Il problema della fattorizzazione nei domini di Dedekind

Stefania Gabelli

Dipartimento di Matematica, Università degli Studi Roma Tre

Note per i corsi di Algebra Commutativa – a.a. 2010/2011

Indice

1 Preliminari **3**
1.1 Il carattere di finitezza 4
1.2 Ideali frazionari 5

2 Divisibilità in un dominio **7**
2.1 Massimo comune divisore 9
2.2 Domini a fattorizzazione unica 10
2.3 Domini di Bezout e a ideali principali 12
2.4 Domini euclidei 14

3 Domini di Dedekind **16**
3.1 Domini noetheriani 16
3.2 Dipendenza integrale 23
3.3 Domini di valutazione discreta 26
3.4 Domini di Dedekind 31

4 Fattorizzazione in ideali primi **33**
4.1 Ideali invertibili 33
4.2 Fattorizzazione in ideali primi 35
4.3 Il Gruppo delle Classi 37

5 Anelli di Interi Algebrici **38**
5.1 Anelli di interi quadratici 43
5.2 Fattorizzazione negli anelli di interi quadratici 48
5.2.1 Fattorizzazione in ideali primi 50
5.2.2 Esempi 51

Introduzione

Nel 1847, G. Lamè presentò all'Accademia di Parigi una sua dimostrazione dell'Ultimo Teorema di Fermat. Essa si basava sul fatto che gli anelli di interi ciclotomici fossero a fattorizzazione unica, ovvero sul fatto che ogni intero ciclotomico (non nullo e non invertibile) si potesse fattorizzare in modo essenzialmente unico nel prodotto di interi ciclotomici irriducibili.

Come fu osservato da J. Liouville, tale supposizione non aveva nessun fondamento. Infatti E. Kummer, venuto a conoscenza del problema sollevato da Liouville, mostrò con un esempio che talvolta gli interi ciclotomici possono essere fattorizzati in più modi. Tuttavia Kummer riuscì a dimostrare che in certi casi l'unicità della fattorizzazione poteva essere ripristinata introducendo dei *numeri ideali*.

In una sua fondamentale memoria del 1871, R. Dedekind osservò poi che la funzione dei numeri ideali di Kummer poteva essere svolta più generalmente in tutti gli anelli di interi algebrici da particolari sottoinsiemi, che egli chiamò ancora *ideali*.

Dedekind dimostrò che, in ogni anello di interi algebrici, un ideale proprio si può sempre fattorizzare in modo unico nel prodotto di ideali primi, anche nei casi in cui il teorema di fattorizzazione unica fallisca per gli elementi.

Astraendo le proprietà degli anelli di interi algebrici, negli anni '20 del 1900, E. Noether ha poi introdotto i *Domini di Dedekind*, ovvero gli anelli commutativi unitari integri che sono caratterizzati dalle seguenti tre proprietà:

(a) Ogni ideale è finitamente generato (ovvero l'anello è noetheriano), (b) Ogni ideale primo non nullo è massimale, (c) l'anello è integralmente chiuso.

I domini di Dedekind sono precisamente quelli in cui ogni ideale proprio è prodotto di ideali primi.

Queste note costituiscono un'introduzione ai domini di Dedekind. Dopo avere richiamato brevemente alcune proprietà fondamentali dei domini noetheriani e integralmente chiusi, caratterizzeremo i domini di Dedekind come quei domini in cui ogni ideale non nullo è invertibile o, equivalentemente, ogni ideale proprio è prodotto di ideali primi. Per applicare questa teoria e fornire esempi di domini di Dedekind che non sono a fattorizzazione unica, introdurremo poi la classe degli anelli di interi algebrici e in particolare considereremo gli anelli di interi quadratici.

1 Preliminari

Se non specificato altrimenti, tutti gli anelli considerati sono anelli commutativi unitari che non sono campi. Se A è un dominio con campo dei quozienti K, un sopra-anello di A è un dominio B tale che $A \subseteq B \subseteq K$.

Daremo per acquisiti i concetti e le tecniche di base dell'Algebra Commutativa. Tuttavia ricordiamo qui alcune nozioni che useremo nel seguito.

1.1 Il carattere di finitezza

Sia A un anello commutativo unitario. Un sottoinsieme non vuoto S di A si chiama una *parte moltiplicativa* se è moltiplicativamente chiuso, cioè se $x, y \in S$ implica $xy \in S$ e si dice che S è *saturata* se vale anche il viceversa, cioè $x, y \in S$ se e soltanto se $xy \in S$.

Un'applicazione del lemma di Zorn mostra che $S \subseteq A$ è una parte moltiplicativa saturata se e soltanto se il suo complementare $A \setminus S$ è unione di ideali primi [6, Exercise 5.7].

Se S è una parte moltiplicativa, con usuale notazione indichiamo con A_S l'*anello delle frazioni di A rispetto ad S*, ovvero $A_S = \{\frac{a}{s}\,;\ a \in A, s \in S\}$ e, se P è un ideale primo di A, poniamo $A_P := A_{A\setminus P}$. L'anello A_P si chiama la *localizzazione di A rispetto all'ideale P*.

Si vede facilmente che gli ideali di A_S sono tutti e soli gli ideali estesi da A, cioè gli ideali del tipo $I_S = \{\frac{x}{s}\,;\ x \in I, s \in S\}$, dove $I \subseteq A$ è un ideale di A. Inoltre $I_S = A_S$ se e soltanto se I non interseca S [6, Lemma 5.24]. Se S non ha zero-divisori, in particolare A è un dominio, $I_S = IA_S$ è l'ideale di A_S generato dagli elementi di I.

Ricordiamo che se $A = \cap A_\lambda$ è una intersezione di domini, si dice che questa intersezione ha il *carattere di finitezza* se ogni elemento non nullo $x \in A$ è non invertibile al più in un numero finito di A_λ. Se A è un'intersezione di localizzazioni rispetto a una famiglia di ideali primi, cioè $A = \cap_\lambda A_{P_\lambda}$, il carattere di finitezza equivale a dire che ogni elemento non nullo x di A appartiene al più ad un numero finito di ideali primi P_λ.

Proposizione 1.1 *Sia A un dominio e sia $\{A_\lambda\}$ una famiglia di sopraanelli di A tali che $A = \cap A_\lambda$ e questa intersezione abbia il carattere di finitezza. Se $S \subseteq A$ è una parte moltiplicativa, allora $A_S = \cap (A_\lambda)_S$ e questa intersezione ha il carattere di finitezza.*

Dimostrazione: Chiaramente $A_S \subseteq B := \cap (A_\lambda)_S$. Mostriamo che $A_S = B$. Sia $x \in B$ non nullo. Poiché B è contenuto nel campo dei quozienti di A, possiamo scrivere $x = \frac{a}{b}$, con $a, b \in A$. Allora $a, b \in A_\lambda$ per ogni λ e quando b è invertibile in A_λ si ha $x \in A_\lambda$. Dunque, se b è invertibile in tutti gli A_λ, $x \in A$. Altrimenti, per il carattere di finitezza, esistono soltanto un numero finito di indici $\lambda_1, \ldots, \lambda_n$ tali che $x \notin A_{\lambda_i}$. Ma poiché $x \in (A_{\lambda_i})_S$, esiste $s \in S$ tale che $sx \in A_{\lambda_i}$ per ogni $i = 1, \ldots, n$. In conclusione, $sx \in \cap A_\lambda = A$ e dunque $x \in A_S$.

Per provare il carattere di finitezza dell'intersezione $\cap (A_\lambda)_S$, osserviamo che se a è invertibile in A_λ, allora $x := \frac{a}{b}$ è invertibile in $(A_\lambda)_S$. Infatti, sia

$x := \frac{a}{b} = \frac{x_\lambda}{s_\lambda}$, con $x_\lambda \in A_\lambda$ e $s_\lambda \in S$. Poiché $as_\lambda = x_\lambda b$ è invertibile in $(A_\lambda)_S$, allora x_λ è invertibile in $(A_\lambda)_S$ e $x(s_\lambda x_\lambda^{-1}) = 1$ con $s_\lambda x_\lambda^{-1} \in (A_\lambda)_S$. □

1.2 Ideali frazionari

Nello studio delle proprietà aritmetiche dei domini ha grande importanza la nozione di ideale frazionario.

Se A è un dominio con campo dei quozienti K, un *ideale frazionario* di A è un A-sottomodulo I di K tale che $dI \subseteq A$, per qualche elemento non nullo $d \in A$. Quindi I è un ideale frazionario di A se e soltanto se $I = d^{-1}J$, dove $0 \neq d \in A$ e $J \subseteq A$ è un ideale. Segue dalla definizione che ogni A-sottomodulo di un ideale frazionario è ancora un ideale frazionario.

Le proprietà elencate nelle seguenti due proposizioni sono di facile verifica.

Proposizione 1.2 *Siano I, J ideali frazionari di A. Allora*

(a) $IJ := \{\sum_{i=1}^{n} x_i y_i \,;\; x_i \in I\,, y_i \in J\,, n \geq 1\}$;

(b) $I \cap J$;

(c) $I + J := \{x + y \,;\; x \in I\,, y \in J\}$

sono ideali frazionari. □

Dati due A-sottomoduli I, J di K, poniamo

$$(I : J) := (I :_K J) := \{x \in K \,;\; xJ \subseteq I\}\,;$$

$$(I :_A J) := (I :_K J) \cap A = \{x \in A \,;\; xJ \subseteq I\}.$$

Con questa notazione, un A-sottomodulo I di K è un ideale frazionario di A se e soltanto se $(A : I) \neq (0)$.

Proposizione 1.3 *Siano I, J, H ideali frazionari di A. Allora:*

(a) $(I : J)$ *è un ideale frazionario di A e $(I :_A J)$ è un ideale di A;*

(b) $(I : JH) = ((I : J) : H)$;

(c) $(xI : J) = x(I : J)$ *e* $(I : xJ) = x^{-1}(I : J)$, *per ogni elemento non nullo $x \in K$.*

Inoltre, per ogni famiglia di ideali frazionari $\{H_i\}$:

(d) $(\cap H_i : J) = \cap(H_i : J)$;

(e) $(I : \sum H_i) = \cap(I : H_i)$. □

Proposizione 1.4 *Siano I e J due ideali frazionari non nulli di A. Allora I e J sono isomorfi come A-moduli se e soltanto se $I = xJ$, con $x \in K \setminus \{0\}$.*

Dunque l'ideale frazionario $(I : J)$ è A-linearmente isomorfo al modulo $Hom_A(J, I)$ degli A-omomorfismi di J in I. Inoltre, $(I : I)$ è isomorfo all'anello degli A-endomorfismi di I.

Dimostrazione: Per ogni $x \in (I : J)$, la moltiplicazione per x

$$\mu_x : J \longrightarrow I\,; \quad a \mapsto ax$$

è un A-omomorfismo ed è iniettivo se $x \neq 0$.

Allora, se $x \in K \setminus \{0\}$ e $I = xJ$, si ha che $x \in (I : J)$ e $I = \mu_x(J)$ è isomorfo a J. Viceversa, sia $\varphi \in Hom_A(J, I)$ non nullo. Mostriamo che, per ogni $a, b \in J \setminus \{0\}$, $a^{-1}\varphi(a) = b^{-1}\varphi(b)$. Allora, posto $z := a^{-1}\varphi(a)$, per ogni $b \in J$ potremo scrivere $\varphi(b) = zb = \mu_z(b)$, da cui $\varphi = \mu_z$ è la moltiplicazione per z e $\varphi(J) = zJ$.

Sia $d \in A$ non nullo tale che $dJ \subseteq R$ e siano $a_1 := da$, $b_1 := db \in A$. Allora per A-linearità,

$$\varphi(a) = \varphi(\frac{a_1}{d}) = a_1\varphi(\frac{1}{d}) = \frac{a_1}{b_1}\varphi(\frac{b_1}{d}) = \frac{a_1}{b_1}\varphi(b)$$

da cui,

$$a^{-1}\varphi(a) = a^{-1}\frac{a_1}{b_1}\varphi(b) = \frac{d}{b_1}\varphi(b) = b^{-1}\varphi(b).$$

Per quanto appena visto, l'applicazione

$$\Psi : (I : J) \longrightarrow Hom_A(J, I)\,;\ x \mapsto \mu_x.$$

è A-lineare e biiettiva. Infine, $(I : I)$ e $End_A(I) := Hom_A(I; I)$ sono anelli e $\Psi : (I : I) \longrightarrow End_A(I)$ è anche un isomorfismo di anelli. □

Osservazione 1.5 Poiché, come appena visto, l'ideale frazionario $(A : I)$ è A-isomorfo a $Hom_A(I, A)$, esso si chiama anche il *duale* di I.

Se I è un ideale frazionario di A, I è isomorfo ad un ideale intero J e gli anelli degli endomorfismi di I e J coincidono. Infatti risulta $I = d^{-1}J$, con $0 \neq d \in A$ e $J \subseteq A$ ed inoltre $(I : I) = (J : J)$.

È evidente che gli A-sottomoduli ciclici di K (cioè quelli del tipo xA, con $x \in K$) sono ideali frazionari. Più generalmente, abbiamo il seguente risultato.

Proposizione 1.6 *Sia A un dominio con campo dei quozienti K. Ogni A-sottomodulo di K finitamente generato è un ideale frazionario di A.*

Dimostrazione: Sia $I := x_1A + \cdots + x_nA$, con $x_i := \frac{a_i}{b_i} \in K$. Allora posto $d := b_1 \dots b_n$ si ha $dI \subseteq A$. □

Il seguente risultato è una versione del Lemma di Nakayama per i domini.

Proposizione 1.7 *Sia A un dominio con campo dei quozienti K e siano I, J ideali frazionari non nulli di A. Se I è finitamente generato e $IJ = I$, allora $1 \in J$. In particolare, se $J \subseteq A$, allora $J = A$.*

Dimostrazione: Sia $I = x_1A + \cdots + x_nA$, con $0 \neq x_i \in K$. Se $I = IJ = x_1J + \cdots + x_nJ$, allora per ogni $i = 1, \dots, n$ possiamo scrivere $x_i = x_1y_{i1} + \cdots + x_ny_{in}$, $y_{ij} \in J$. Da cui $\sum_j(\delta_{ij} - y_{ij})x_j = 0$, dove δ_{ij} è il simbolo di Kronecker. Allora il sistema lineare $\sum_j(\delta_{ij} - y_{ij})X_j = 0$ ha soluzioni non nulle in K e perciò $\det(\delta_{ij} - y_{ij}) = 0$. Ma, calcolando, risulta $\det(\delta_{ij} - y_{ij}) = 1 - z$, con $z \in J$; perciò $1 = z \in J$. □

Proposizione 1.8 *Siano I, J ideali frazionari di A e $S \subseteq A$ una parte moltiplicativa. Allora $(I : J)A_S \subseteq (IA_S : JA_S)$. Se inoltre J è finitamente generato, $(I : J)A_S = (IA_S : JA_S)$.*

Dimostrazione: È evidente che $(I : J)A_S \subseteq (IA_S : JA_S)$. Inoltre, sia $J := \sum x_iA$ finitamente generato. Allora $(IA_S : JA_S) = (IA_S : \sum x_iA_S) = \cap(IA_S : x_iA_S) = \cap x_i^{-1}IA_S = \cap(I : x_iA)A_S = (I : \sum x_iA)A_S = (I : J)A_S$. □

Proposizione 1.9 *Se A è un dominio, allora per ogni ideale frazionario I di A risulta $I = \cap\{IA_M\,;\ M \in \mathrm{Max}(A)\}$; in particolare $A = \cap\{A_M\,;\ M \in \mathrm{Max}(A)\}$. Dunque $I = J$ se e soltanto se $IA_M = JA_M$ per ogni ideale massimale M.*

Dimostrazione: Chiaramente $I \subseteq \cap\{IA_M\,;\ M \in \mathrm{Max}(A)\}$. Viceversa, fissato M, sia $x := \frac{a}{s} \in IA_M$, con $a \in I$ e $s \in A \setminus M$. Allora $s \in (I :_A x) \setminus M$, da cui $(I :_A x) \nsubseteq M$. Perciò, se $x \in \cap\{IA_M\,;\ M \in \mathrm{Max}(A)\}$, si ha $(I :_A x) \nsubseteq M$, per ogni $M \in \mathrm{Max}(A)$. Da cui $(I :_A x) = A \ni 1$ e $x = 1x \in I$. □

Osservazione 1.10 Anche se $(I : J)A_M \subsetneq (IA_M : JA_M)$ per qualche $M \in \mathrm{Max}(A)$, si ha comunque $(I : J) = \cap(I : J)A_M = \cap(IA_M : JA_M)$. Infatti $I = \cap IA_M$ e $(I : J) = (\cap IA_M : J) = \cap(IA_M : J) = \cap(IA_M : JA_M)$.

2 Divisibilità in un dominio

Per definire in un anello commutativo unitario A una buona teoria della divisibilità, è conveniente assumere che A non abbia zero-divisori, cioè che A sia un dominio.

Dati due elementi x, y di un dominio A, si dice che y *divide* x in A se esiste un elemento $z \in A$ tale che $x = yz$. In tal caso si dice anche che y è un *divisore* o un *fattore* di x in A e che x è un *multiplo* di y. Lo zero di A divide soltanto se stesso ma è diviso da ogni elemento di A, infatti $0x = 0$ per ogni $x \in A$.

Gli elementi invertibili di A sono i divisori dell'unità moltiplicativa di A, denotata con 1. Indicheremo al solito con $\mathcal{U}(A)$ il gruppo moltiplicativo degli elementi invertibili di A.

Si dice che y è *associato* a x in A se esiste un elemento $u \in \mathcal{U}(A)$ tale che $y = ux$. Si verifica subito che questa è una relazione di equivalenza su A e che x e y sono associati se e soltanto se si dividono reciprocamente.

Ogni elemento $x \in A$ è diviso dagli elementi invertibili di A e dai suoi associati. Infatti $x = 1x = u(u^{-1}x)$, per ogni $u \in \mathcal{U}(A)$. Un divisore di x non invertibile e non associato a x si chiama un *divisore proprio* di x.

Notiamo che y divide x se e soltanto se $\langle x \rangle \subseteq \langle y \rangle$. Quindi x e y sono associati se e soltanto se $\langle x \rangle = \langle y \rangle$ e y è un divisore proprio di x se e soltanto se $\langle x \rangle \subsetneq \langle y \rangle \neq A$.

Un elemento x di A si chiama un *elemento irriducibile* se x è non nullo e non invertibile e non ha divisori propri. Un elemento non nullo che ha divisori propri si dice *riducibile*. Un *elemento primo* di A è un elemento x non nullo e non invertibile tale che, scelti comunque $y, z \in A$, quando x divide yz allora x divide y oppure x divide z. Quindi, per induzione su $n \geq 2$, un elemento primo x che divide un prodotto $y_1 y_2 \dots y_n$ divide almeno uno dei fattori y_i.

Proposizione 2.1 *Sia A un dominio e sia $x \in A$ un elemento non nullo e non invertibile. Allora x è un elemento primo se e soltanto se l'ideale principale $\langle x \rangle$ è un ideale primo.*

Dimostrazione: Segue direttamente dalle definizioni. □

Proposizione 2.2 *In un dominio A, ogni elemento primo è irriducibile.*

Dimostrazione: Sia $p \in A$ un elemento primo. Se $p = xy$, allora p divide x oppure y. Nel primo caso, p e x sono associati e y è invertibile. Nel secondo caso, p e y sono associati e x è invertibile. Quindi p non ha divisori propri. □

Esempio 2.3 **(1)** Gli elementi irriducibili di $\mathbb{Z}$ sono esattamente i numeri primi e i loro opposti e coincidono con gli elementi primi.

(2) Se K è un campo, per la formula del grado, gli elementi invertibili di $K[X]$ sono tutte e sole le costanti non nulle. Dunque un polinomio non costante $f(X) \in K[X]$ è irriducibile se e soltanto se gli unici suoi divisori sono le costanti non nulle ed i polinomi del tipo $cf(X)$, con $c \in K^*$.

Ne segue che un polinomio non nullo $f(X) \in K[X]$ è riducibile su K se e soltanto se $f(X)$ ha un divisore $g(X) \in K[X]$ tale che $1 \leq \deg g(X) < \deg f(X)$. In particolare, se $\deg f(X) = 1$, allora $f(X)$ è irriducibile.

2.1 Massimo comune divisore

Se A è un dominio e $x, y \in A$ sono non entrambi nulli, un massimo comune divisore di x e y è un divisore comune di x e y diviso da ogni altro divisore comune. Precisamente, un elemento $d \in A$ è un *massimo comune divisore* di x e y se:

(1) d divide x e y;

(2) Se d' divide x e y, allora d' divide d.

Un massimo comune divisore di x e y, se esiste, non è univocamente determinato. Infatti dalla proprietà (2) segue subito che se $d \in A$ è un massimo comune divisore, lo sono anche tutti gli elementi di A associati a d.

Nell'impossibilità di privilegiare un particolare massimo comune divisore di due elementi, se d è un *qualsiasi* massimo comune divisore di x e y, si usa scrivere $(x, y) = d$. Se gli unici divisori comuni di x e y sono gli elementi invertibili di A, si scrive $(x, y) = 1$ e si dice che x e y sono elementi *coprimi*.

Lemma 2.4 *Sia A un dominio. Un elemento $q \in A$, non nullo e non invertibile, è irriducibile se e soltanto se, per ogni $x \in A$, q divide x oppure $(x, q) = 1$.*

Dimostrazione: Poiché gli unici divisori di q sono gli elementi invertibili di A e gli elementi associati a q, se q non divide x, gli unici divisori comuni di x e q sono gli elementi invertibili. Quindi $(x, q) = 1$. □

Diremo che A è un *dominio con il massimo comune divisore* se due qualsiasi elementi non nulli di A hanno un massimo comune divisore.

Proposizione 2.5 (Lemma di Euclide) *Sia A un dominio con il massimo comune divisore e siano $x, y, z \in A$ elementi non nulli. Se x divide yz e $(x, y) = 1$, allora x divide z.*

Dimostrazione: Si verifica facilmente che $(xz, yz) = z(x, y)$. Allora, se $(x, y) = 1$ e x divide yz, si ha che x divide $(xz, yz) = z(x, y) = z$. □

Corollario 2.6 *Sia A un dominio con il massimo comune divisore e sia $p \in A$. Allora p è un elemento primo se e soltanto se p è un elemento irriducibile.*

Dimostrazione: Sia p un elemento irriducibile di A e supponiamo che p divida xy. Se p non divide x, allora $(p, x) = 1$ (Lemma 2.4) e quindi p divide y per il Lemma di Euclide (Proposizione 2.5). Viceversa, in ogni dominio un elemento primo è irriducibile (Proposizione 2.2). □

2.2 Domini a fattorizzazione unica

Un dominio A si chiama *atomico* se ogni elemento non nullo e non invertibile $x \in A$ può essere fattorizzato nel prodotto di un numero finito di elementi irriducibili (non necessariamente distinti):

$$x = p_1 p_2 \dots p_n, \quad \text{con } p_i \text{ irriducibile per } i = 1, \dots, n.$$

Questa proprietà è garantita dalla condizione della catena ascendente sugli ideali principali. Si dice che un dominio A soddisfa la *condizione della catena ascendente sugli ideali principali* se ogni catena di ideali principali propri di A

$$\langle x_1 \rangle \subseteq \langle x_2 \rangle \subseteq \dots \subseteq \langle x_i \rangle \subseteq \dots$$

è stazionaria, cioè se esiste un (minimo) intero $n \geq 1$ tale che $\langle x_n \rangle = \langle x_m \rangle$ per $m \geq n$.

Tuttavia un dominio atomico non soddisfa necessariamente la condizione della catena ascendente sugli ideali principali.

Proposizione 2.7 *Se A è un dominio che soddisfa la condizione della catena ascendente sugli ideali principali, allora A è atomico.*

Dimostrazione: Supponiamo che la tesi non sia vera e sia $\mathcal{S}$ l'insieme degli ideali principali propri $\langle a \rangle$ di A tali che a non possa essere fattorizzato in elementi irriducibili. Per la condizione della catena ascendente, $\mathcal{S}$ ha un elemento massimale $\langle x \rangle$, perché altrimenti sarebbe possibile costruire una catena infinita di ideali principali generati da elementi di $\mathcal{S}$

$$\langle x_1 \rangle \subsetneq \langle x_2 \rangle \subsetneq \dots \subsetneq \langle x_i \rangle \subsetneq \dots.$$

Poiché x non può essere primo, altrimenti sarebbe banalmente fattorizzabile, possiamo scrivere $x = yz$, con y, z fattori propri di x. Allora $\langle x \rangle \subsetneq \langle y \rangle$ e $\langle x \rangle \subsetneq \langle z \rangle$. Per la massimalità di $\langle x \rangle$, ne segue che y e z possono essere fattorizzati nel prodotto di un numero finito di elementi irriducibili. Ma allora anche x può essere fattorizzato. Questa è una contraddizione. □

Un dominio A si dice un *dominio a fattorizzazione unica* se soddisfa le due seguenti condizioni:

(1) A è atomico;

(2) Se $x = p_1 \dots p_n = q_1 \dots q_m$ sono due fattorizzazioni dello stesso elemento di A in elementi irriducibili (non necessariamente distinti), allora $n = m$ e gli elementi q_i possono essere rinumerati in modo tale che p_i e q_i siano associati per $i = 1, \dots, n$.

Si usa esprimere la proprietà (2) dicendo che la fattorizzazione in elementi irriducibili è *unica, a meno dell'ordine e di elementi invertibili.*

Esempio 2.8 (1) Il *Teorema Fondamentale dell'Aritmetica* asserisce che l'anello degli interi $\mathbb{Z}$ è un dominio a fattorizzazione unica. L'esistenza di una fattorizzazione in numeri primi si può dimostrare per induzione sul modulo.

(2) Se A è un dominio a fattorizzazione unica, ogni elemento non nullo di A ha un numero finito di divisori non associati tra loro. Quindi se $\mathcal{U}(A)$ è un insieme finito, ogni elemento non nullo ha un numero finito di divisori.

Infatti, sia $x \in A \setminus \{0\}$. Se $x \in \mathcal{U}(A)$, i suoi divisori sono tutti associati tra di loro, e associati a 1. Se $x \notin \mathcal{U}(A)$ e $x = p_1 \dots p_n$ è una fattorizzazione di x in elementi irriducibili, ogni divisore proprio di x deve essere associato a un elemento del tipo $p_{i_1} \dots p_{i_m}$ con $m \leq n$.

Se A è un dominio a fattorizzazione unica e $x, y \in A$ sono due elementi non nulli e non invertibili, considerando tutti i fattori irriducibili sia di x che di y, possiamo scrivere $x = p_1^{a_1} \dots p_n^{a_n}$ e $y = p_1^{b_1} \dots p_n^{b_n}$, dove $p_1, \dots, p_n$ sono elementi irriducibili distinti e $a_i, b_i \geq 0$, per $i = 1, \dots, n$.

Proposizione 2.9 *Sia A un dominio a fattorizzazione unica. Allora A è un dominio con il massimo comune divisore. Inoltre, se*

$$x = p_1^{a_1} \dots p_n^{a_n}, \quad y = p_1^{b_1} \dots p_n^{b_n},$$

dove $p_1, \dots, p_n$ sono elementi irriducibili distinti di A e $a_i, b_i \geq 0$, per $i = 1, \dots, n$, si ha $(x, y) = p_1^{m_1} \dots p_n^{m_n}$, dove $m_i := \min\{a_i, b_i\}$, per $i = 1, \dots, n$.

Dimostrazione: È una semplice verifica, osservando che se uno tra gli elementi x e y è invertibile si ha $(x, y) = 1$. □

Teorema 2.10 *Le seguenti condizioni sono equivalenti per un dominio A:*

(i) *A è un dominio a fattorizzazione unica;*

(ii) *A è atomico e ogni elemento irriducibile di A è un elemento primo;*

(iii) *A soddisfa la condizione della catena ascendente sugli ideali principali ed ogni elemento irriducibile di A è un elemento primo;*

(iv) *A è un dominio atomico con il massimo comune divisore;*

(v) *A soddisfa la condizione della catena ascendente sugli ideali principali ed è un dominio con il massimo comune divisore;*

(vi) *Ogni elemento non nullo e non invertibile di A si fattorizza in un numero finito di elementi primi;*

(vii) *Ogni ideale primo non nullo di A contiene un elemento primo;*

(viii) *Ogni ideale primo di A minimale su un ideale principale è principale.*

Dimostrazione: (i) $\Rightarrow$ (iv) segue dal Proposizione 2.9.

(iv) $\Rightarrow$ (ii) è il Corollario 2.6.

(ii) $\Rightarrow$ (i) Supponiamo che $p_1 \dots p_r = q_1 \dots q_s$, dove i p_i e q_j sono elementi irriducibili per $i = 1, \dots, r$ e $j = 1, \dots, s$. Poiché p_1 è un elemento primo di A, allora p_1 divide uno degli elementi q_j. A meno di riordinare i fattori q_j, possiamo supporre che p_1 divida q_1. Allora, essendo p_1 e q_1 entrambi irriducibili, essi devono essere associati, cioè deve essere $q_1 = up_1$, con $u \in \mathcal{U}(A)$. Quindi, cancellando p_1, risulta $p_2 \dots p_r = uq_2 \dots q_s$. Così proseguendo, si ottiene che $r = s$ e, a meno dell'ordine, gli elementi p_i e q_i sono associati per $i = 1, \dots, r$.

(iii) $\Rightarrow$ (ii) e (v) $\Rightarrow$ (iv) seguono dalla Proposizione 2.7.

(ii) $\Rightarrow$ (iii) e (iv) $\Rightarrow$ (v) Via (i), basta dimostrare che un un dominio a fattorizzazione unica A soddisfa la condizione della catena ascendente sugli ideali principali. Questo segue dal fatto che $\langle x \rangle \subseteq \langle y \rangle$ se e soltanto se y divide x ed inoltre ogni elemento non nullo $x \in A$ ha un numero finito di divisori non associati tra loro (Esempio 2.8 (2)).

(ii) $\Rightarrow$ (vi) è chiaro.

(vi) $\Rightarrow$ (ii) A è atomico, perché gli elementi irriducibili sono primi. Sia q un elemento non nullo e non invertibile di A. Se $q = p_1 \dots p_n$ si fattorizza in $n \geq 2$ elementi primi allora q non è irriducibile. Quindi ogni elemento irriducibile è primo.

(vii) $\Rightarrow$ (vi) Sia $S := \{up_1^{a_1} \dots p_n^{a_n} \,;\, u \in \mathcal{U}(A)\,, p_i \text{ primo e } a_i \geq 0\} \subseteq A$. Chiaramente S è una parte moltiplicativa non vuota ed è saturata. Allora se $a \notin S$, l'ideale $\langle a \rangle$ non interseca S, quindi è contenuto in un ideale primo di A che non interseca S. Poiché per ipotesi ogni ideale primo non nullo di A interseca S, deve essere $a = 0$. In conclusione $S = A \setminus \{0\}$ e questo basta.

(vi) $\Rightarrow$ (viii) Sia $0 \neq x \in A$. Se P è un ideale primo contenente x, allora P contiene un fattore primo p di x. Dunque $x \in \langle p \rangle \subseteq P$ e, per la minimalità di P, $\langle p \rangle = P$.

(viii) $\Rightarrow$ (vii) Se P è un ideale primo non nullo e $0 \neq x \in P$, P contiene un ideale primo minimale su x, che è principale per ipotesi. Quindi P contiene un elemento primo. □

Corollario 2.11 *Se A è un dominio a fattorizzazione unica, ogni ideale primo di altezza uno di A è principale.*

2.3 Domini di Bezout e a ideali principali

Se $d = (x, y)$ è un massimo comune divisore di x e y ed è possibile scrivere $d = ax + by$ per opportuni $a, b \in A$, questa espressione si chiama una *identità di Bezout* per d.

Proposizione 2.12 *Dati due elementi non nulli x, y di un dominio A, le seguenti condizioni sono equivalenti:*

(i) $\langle x, y\rangle =: \langle d\rangle$ *è un ideale principale;*

(ii) $(x, y) = d$ *e* $d = ax + by$*, per opportuni* a*,* $b \in A$ *(cioè esiste un massimo comune divisore di* x *e* y *ed una identità di Bezout per esso).*

Dimostrazione: Ricordiamo che d divide x e y se e soltanto se $\langle x, y\rangle \subseteq \langle d\rangle$.

(i) $\Rightarrow$ (ii) Se $\langle x, y\rangle = \langle d\rangle$, d divide x, y e $d = ax + by$, per a, $b \in A$. Dunque ogni d' che divide x e y divide d e segue che $(x, y) = d$.

(ii) $\Rightarrow$ (i) Se $(x, y) = d$, $\langle x, y\rangle \subseteq \langle d\rangle$ e se $d = ax + by$, $\langle d\rangle \subseteq \langle x, y\rangle$. □

Un dominio si dice *a ideali principali* se ogni suo ideale è principale. Inoltre, un dominio che soddisfa le condizioni equivalenti della Proposizione 2.12 si chiama un *dominio di Bezout*. Dunque, per induzione sul numero dei generatori, un dominio A è di Bezout se e soltanto se ogni ideale finitamente generato è principale.

Corollario 2.13 *Se* A *è un dominio a ideali principali, allora* A *è un dominio di Bezout.*

Proposizione 2.14 *Sia* A *un dominio in cui ogni ideale primo è principale (in particolare un dominio a ideali principali) e sia* $p \in A$ *un elemento non nullo e non invertibile. Le seguenti condizioni sono equivalenti:*

(i) $\langle p\rangle$ *è un ideale massimale;*

(ii) $\langle p\rangle$ *è un ideale primo;*

(iii) p *è un elemento primo di* A*;*

(iv) p *è un elemento irriducibile di* A*.*

Dimostrazione: (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) sono sempre vere.

(iv) $\Rightarrow$ (i) Sia p un elemento irriducibile di A e sia $M := \langle q\rangle$ un ideale massimale tale che $p \in M$. Allora q divide p e q non è invertibile. Dunque q è associato a p e ne segue che $\langle p\rangle = \langle q\rangle = M$ è un ideale massimale. □

Proposizione 2.15 *Un dominio a ideali principali è un dominio a fattorizzazione unica.*

Dimostrazione: Sia A un dominio a ideali principali. Poiché ogni elemento irriducibile di A è primo (Proposizione 2.14), per il Teorema 2.10, basta far vedere che A soddisfa la condizione della catena ascendente sugli ideali principali. Sia

$$\langle x_1\rangle \subseteq \langle x_2\rangle \subseteq \ldots \subseteq \langle x_i\rangle \subseteq \ldots$$

una catena di ideali principali e sia $I := \bigcup_{i\geq 1}\langle x_i\rangle$. Si vede facilmente che I è un ideale di A e quindi I è principale per ipotesi. Se $I = \langle x\rangle$, per definizione $x \in \langle x_n\rangle$ per qualche $n \geq 1$. Ne segue che $I = \langle x_n\rangle = \langle x_m\rangle$ per $m \geq n$. □

Si dice che un dominio A ha *dimensione uno* se ogni ideale primo non nullo di A è massimale. La Proposizione 2.14 implica che ogni dominio a ideali principali ha dimensione uno. Vedremo nel Paragrafo 3.1 che un dominio a fattorizzazione unica è a ideali principali se e soltanto se ha dimensione uno (Corollario 3.13).

Esempio 2.16 (1) Se A è un dominio a fattorizzazione unica, per il così detto *Lemma di Gauss*, ogni anello di polinomi su A è un dominio a fattorizzazione unica. In particolare ogni anello di polinomi a coefficienti in un campo o nell'anello degli interi $\mathbb{Z}$ è un dominio a fattorizzazione unica.

(2) Se A è un dominio ma non è un campo, l'anello dei polinomi $A[X]$ non è mai ad ideali principali; ad esempio, l'anello dei polinomi $\mathbb{Z}[X]$ non è a ideali principali, anche se lo è $\mathbb{Z}$.

Infatti, se $a \in A$ è non nullo e non invertibile, l'ideale $\langle a, X\rangle = \{ac + Xf(X)\,; c \in A, f(X) \in A[X]\}$ non è principale. Per vedere questo, supponiamo che $\langle a, X\rangle = \langle g(X)\rangle$. Allora il polinomio $g(X)$, dividendo la costante a, deve essere un polinomio costante per la formula del grado. Inoltre, poiché $g(X)$ divide X e X è monico, deve essere $g(X) := u$ invertibile in A. Ma allora $\langle a, X\rangle = \langle u\rangle = A$, mentre $1 \notin \langle a, X\rangle$.

In modo simile si vede che, se K è un campo e $n \geq 2$, l'anello $K[X_1, \ldots, X_n]$ non è a ideali principali. Ad esempio, poiché le indeterminate sono elementi irriducibili, l'ideale $\langle X_1, X_2\rangle$ non è principale.

2.4 Domini euclidei

Una classe importante di domini a ideali principali (e quindi a fattorizzazione unica) sono i domini euclidei.

Una *funzione euclidea* su dominio A è un'applicazione $\phi : A \setminus \{0\} \longrightarrow \mathbb{N}$ tale che, per ogni a, $b \in A \setminus \{0\}$:

(1) Se a divide b, allora $\phi(a) \leq \phi(b)$;

(2) (Divisione euclidea) esistono q, $r \in A$ (detti rispettivamente *quoziente* e *resto*) tali che $a = bq + r$ e $r = 0$ oppure $\phi(r) < \phi(b)$.

Se sul dominio A esiste una funzione euclidea ϕ, A si chiama un *dominio euclideo rispetto a* ϕ.

Esempio 2.17 L'anello degli interi $\mathbb{Z}$ è euclideo rispetto al modulo, l'anello dei polinomi $K[X]$ a coefficienti in un campo è euclideo rispetto al grado e l'anello degli *interi di Gauss* $\mathbb{Z}[i]$ è euclideo rispetto alla norma complessa (vedi il successivo Paragrafo 5.2).

Il resto della divisione euclidea non è sempre unico. Anzi, si può dimostrare che il resto è unico se e soltanto se A è isomorfo ad un anello di polinomi $K[X]$, mentre esistono al più soltanto due resti se e soltanto se A è isomorfo a $\mathbb{Z}$.

Proposizione 2.18 *Un dominio euclideo A è a ideali principali. Precisamente, ogni ideale non nullo $I \subseteq A$ è principale, generato da un elemento di valutazione minima.*

Dimostrazione: Sia $I \subseteq A$ non nullo. Allora il sottoinsieme $\{\phi(x)\,;\ 0 \neq x \in I\}$ di $\mathbb{N}$ è non vuoto e perciò esiste un elemento non nullo $a \in I$ di valutazione minima $\phi(a)$. Per ogni elemento non nullo $y \in I$, possiamo scrivere $y = aq + r$. Poiché $r \in I$, non puó essere $\phi(r) < \phi(a)$; quindi $r = 0$ e y è un multiplo di a. □

Proposizione 2.19 *Sia A un dominio euclideo rispetto alla funzione ϕ e sia $x \in A \setminus \{0\}$. Allora:*

(1) $\phi(x) \geq \phi(1)$.

(2) *Se y divide x e $\phi(x) = \phi(y)$, allora x e y sono associati.*

(3) *x è invertibile se e soltanto se $\phi(x) = \phi(1)$.*

Dimostrazione: (1) Poiché $x = x1$, si ha $\phi(x) = \phi(x1) \geq \phi(1)$.

(2) Sia $y = xz$. Poiché $y \in \langle x \rangle$, se $\phi(y) = \phi(x)$, allora y ha valutazione minima nell'ideale $\langle x \rangle$. Dunque y genera l'ideale $\langle x \rangle$ ed è per questo associato a x.

(3) Se x è invertibile, allora $xz = 1$ e $\phi(1) = \phi(xz) \geq \phi(x)$. Quindi per (1) vale l'uguaglianza. Il viceversa segue da (2) per $y = 1$. □

Osservazione 2.20 Se A è un dominio euclideo, un massimo comune divisore di due elementi $x, y \in A$ si può calcolare con l'*algoritmo euclideo delle divisioni successive*. Precisamente, se

$$\begin{aligned}
x &= yq_1 + r_1\,, && r_1 = 0 \text{ oppure } \phi(r_1) < \phi(x);\\
y &= r_1q_2 + r_2\,, && r_2 = 0 \text{ oppure } \phi(r_2) < \phi(r_1);\\
&\cdots\cdots && \cdots\cdots\\
r_{n-2} &= r_{n-1}q_n + r_n\,, && r_n = 0 \text{ oppure } \phi(r_n) < \phi(r_{n-1});\\
r_{n-1} &= r_nq_{n+1}.
\end{aligned}$$

Allora un massimo comune divisore $d := (x, y)$ è l'ultimo resto non nullo r_n (notiamo che il procedimento ha termine perché $\phi(x) > \phi(r_1) > \phi(r_2) > \ldots$ è una successione strettamente decrescente di interi positivi).

Inoltre, dalla successione di uguaglianze:

$$\begin{aligned}
r_n &= r_{n-2} - q_nr_{n-1};\\
r_{n-1} &= r_{n-3} - q_{n-1}r_{n-2};\\
&\cdots\cdots
\end{aligned}$$

per sostituzioni successive, si ottiene esplicitamente una identità di Bezout per d.

3 Domini di Dedekind

Astraendo le proprietà degli anelli di interi algebrici, E. Noether ha chiamato *domini di Dedekind* i domini A che verificano le seguenti tre proprietà:

(1) Ogni ideale di A è finitamente generato;

(2) Ogni elemento del campo dei quozienti K che è radice di un polinomio monico a coefficienti in A appartiene ad A;

(3) Ogni ideale primo non nullo di A è massimale.

In questo capitolo studieremo questa importante classe di domini e le loro proprietà di fattorizzazione.

3.1 Domini noetheriani

Gli anelli noetheriani prendono il nome da Emmy Noether, per i suoi fondamentali contributi alla Teoria degli Ideali (*Idealtheorie in Ringbereichen*, 1921). Lo studio di questi anelli ha avuto origine nell'ambito della Geometria Algebrica dallo studio delle k-algebre finitamente generate (quozienti di anelli di polinomi in un numero finito di indeterminate a coefficienti in un campo k). In questo contesto, ci interessano le proprietà di divisibilità dei domini noetheriani.

Ricordiamo la definizione. Sia A un anello commutativo unitario. Un A-modulo M si dice un *modulo noetheriano* se ogni sotto A-modulo di M è finitamente generato. Inoltre A si dice un *anello noetheriano* se è noetheriano come A-modulo.

Notando che i sotto A-moduli di un anello commutativo unitario A sono precisamente gli ideali di A, possiamo anche definire un *anello noetheriano* come un anello commutativo unitario i cui ideali sono finitamente generati.

Proposizione 3.1 *Sia A un anello commutativo unitario e M un A-modulo. Le seguenti condizioni sono equivalenti:*

(i) *M (rispettivamente A) è noetheriano;*

(ii) (Principio del massimo) *Ogni insieme non vuoto di sotto A-moduli di M (rispettivamente di ideali di A) ha un elemento massimale rispetto all'inclusione;*

(iii) (Condizione della catena ascendente) *Ogni catena ascendente di sotto A-moduli di M (rispettivamente di ideali di A)*

$$N_0 \subseteq N_1 \subseteq \ldots \subseteq N_k \subseteq \ldots$$

è stazionaria, cioè esiste un (minimo) intero $h \geq 0$ tale che $N_h = N_k$ per $k \geq h$.

Dimostrazione: (i) $\Rightarrow$ (iii) Sia $\{N_k\}_{k\geq 0}$ una catena di sotto A-moduli di M e sia $N = \bigcup_{k\geq 0} N_k$ la loro unione. Poiché $N = \alpha_1 A + \cdots + \alpha_t A$ è finitamente generato, esiste un (minimo) intero $h \geq 0$ tale che $\alpha_i in N_h$ per $i = 1, \ldots, t$. Allora $N_h = N_k = N$ per ogni $k \geq h$.

(iii) $\Rightarrow$ (ii) Sia $\mathcal{S}$ un insieme non vuoto di sotto A-moduli di M e supponiamo che $\mathcal{S}$ non abbia elementi massimali rispetto all'inclusione. Allora dato $N_0 \in \mathcal{S}$, esiste $N_1 \in \mathcal{S}$ tale che $N_0 \subsetneq N_1$. Poiché N_1 non è massimale in $\mathcal{S}$, esiste $N_2 \in S$ tale che $N_0 \subsetneq N_1 \subsetneq N_2$. Così procedendo, si ottiene una catena ascendente di sotto A-moduli di M

$$N_0 \subseteq N_1 \subseteq \ldots \subseteq N_k \subseteq \ldots$$

che non è stazionaria.

(ii) $\Rightarrow$ (i) Supponiamo che $N \subseteq M$ sia un sotto A-modulo che non è finitamente generato e sia $\mathcal{S}$ l'insieme dei sotto A-moduli di M contenuti in N che sono finitamente generati. Poiché il modulo nullo appartiene ad $\mathcal{S}$, $\mathcal{S}$ è non vuoto e quindi per ipotesi ha un elemento massimale L. Se $L \subsetneq N$, dato $x \in N \setminus L$, il sotto A-modulo $L' := L + xA$ di M è ancora finitamente generato e contenuto in N. Ma $L \subsetneq L'$, contro la massimalità di L. $\square$

Il seguente risultato è di grande utilità teorica nello studio degli anelli noetheriani.

Teorema 3.2 (Teorema di Cohen) *Un anello A è noetheriano se e soltanto se ogni ideale primo di A è finitamente generato.*

Dimostrazione: Sia $\mathcal{S}$ l'insieme degli ideali di A che non sono finitamente generati. Se A non è noetheriano, $\mathcal{S}$ è non vuoto. Mostriamo che $\mathcal{S}$ ha elementi massimali e che questi sono ideali primi; in questo modo otteremo una contraddizione.

L'esistenza di elementi massimali in $\mathcal{S}$ segue dal Lemma di Zorn. Infatti, sia $\mathcal{C} := \{I_\lambda\}$ una catena di ideali di $\mathcal{S}$ e sia $I := \cup I_\lambda$. Allora I non è finitamente generato, altrimenti risulterebbe $I = I_{\lambda_0}$ per qualche ideale $I_{\lambda_0} \in \mathcal{C}$ e quindi I_{λ_0} sarebbe finitamente generato, mentre $I_{\lambda_0} \in \mathcal{S}$. Perciò I è un maggiorante per $\mathcal{C}$ e dunque $\mathcal{S}$ ha elementi massimali.

Sia dunque M un elemento massimale di $\mathcal{S}$. Notiamo che $M \neq A$, perché $A = (1) \notin \mathcal{S}$. Supponiamo che M non sia un ideale primo e siano $x, y \in A \setminus M$ tali che $xy \in M$. Allora $M \subsetneq \langle M, x\rangle$, così che, per la massimalità di M in $\mathcal{S}$, $\langle M, x\rangle$ è finitamente generato. Analogamente, poiché $M \subseteq (A :_A x)$ e $y \in (M :_A x) \setminus M$, anche $(M :_A x)$ è un ideale finitamente generato. Siano $m_1 + a_1 x, \ldots, m_s + a_s x$ i generatori di $\langle M, x\rangle$ (con $m_i \in M$ e $a_i \in A$) e $b_i, \ldots, b_t \in A$ i generatori di $(M :_A x)$ e consideriamo l'ideale I generato da $m_1, \ldots, m_s, xb_1, \ldots, xb_t$. Certamente $I \subseteq M$. Mostriamo che $I = M$ e quindi M è finitamente generato.

Sia $z \in M$. Poiché $M \subseteq \langle M, x\rangle$, possiamo scrivere $z = \sum c_i(m_i + a_i x) = \sum c_i m_i + x\sum c_i a_i$, $c_i \in A$. Ne segue che $x\sum c_i a_i \in M$ e dunque $\sum c_i a_i \in (M :_A x)$, da cui $\sum c_i a_i = \sum d_i b_i$, $d_i \in A$. Finalmente, $z = \sum c_i m_i + x\sum c_i a_i = \sum c_i m_i + \sum d_i(x b_i) \in I$. Quindi $I = M$.

In conclusione, se M non è primo, esso è finitamente generato e dunque $M \notin \mathcal{S}$. Contraddizione. □

Richiamiamo ora alcune proprietà di base degli anelli noetheriani che ci saranno necessarie nel seguito; in particolare alcune proprietà di trasporto della noetherianità ed il fatto che ogni ideale proprio di un anello noetheriano ha un numero finito di primi minimali. Per una trattazione più approfondita rimandiamo a [1, 6]. Il seguente teorema è un caposaldo della teoria.

Teorema 3.3 (Teorema della Base, D. Hilbert, 1888) *Se A è un anello noetheriano e $X_1, \ldots, X_n$, $n \geq 1$, sono indeterminate indipendenti su A, l'anello di polinomi $A[X_1, \ldots, X_n]$ è un anello noetheriano. In particolare, gli anelli di polinomi $\mathbb{Z}[X_1, \ldots, X_n]$ e $k[X_1, \ldots, X_n]$, dove k è un campo, sono noetheriani.*

Dimostrazione: Per induzione sul numero delle indeterminate, basta dimostrare che, se A è noetheriano, lo è anche $A[X]$. Useremo le condizioni equivalenti date nella Proposizione 3.1.

Per ogni ideale non nullo I di $A[X]$ e per ogni $n \geq 0$, consideriamo il sottoinsieme $C_n(I)$ di A formato dai coefficienti direttori di tutti i polinomi di grado n appartenenti ad I e dallo zero. Si verifica facilmente che $C_n(I)$ è un ideale di A e che, se $I_1 \subseteq I_2$, si ha $C_n(I_1) \subseteq C_n(I_2)$. Inoltre

$$C_0(I) \subseteq C_1(I) \subseteq \ldots \subseteq C_j(I) \subseteq \ldots$$

Infatti, se $f(X) \in I$, anche $Xf(X) \in I$. Allora, data una catena di ideali di $A[X]$

$$I_0 \subseteq I_1 \subseteq \ldots \subseteq I_k \subseteq \ldots$$

per ogni k, $j \geq 0$, si hanno le catene di ideali di A

$$C_0(I_k) \subseteq C_1(I_k) \subseteq \ldots \subseteq C_j(I_k) \subseteq C_{j+1}(I_k) \subseteq \ldots$$

$$C_j(I_0) \subseteq C_j(I_1) \subseteq \ldots \subseteq C_j(I_k) \subseteq C_j(I_{k+1}) \subseteq \ldots$$

Poiché A è noetheriano, l'insieme di ideali $S := \{C_j(I_k)\}_{j,k\geq 0}$ ha un elemento massimale $C_p(I_q)$. Quindi in particolare $C_p(I_k) = C_p(I_q)$ per ogni $k \geq q$. D'altra parte, le catene di ideali

$$\{C_0(I_k)\}_{k\geq 0}\,; \quad \{C_1(I_k)\}_{k\geq 0}\,; \quad \ldots\,; \quad \{C_{p-1}(I_k)\}_{k\geq 0}$$

stazionano. Quindi esiste un intero $q' \geq 0$ tale che $C_j(I_k) = C_j(I_{q'})$ per $j = 1, \ldots, p-1$ e $k \geq q'$. In definitiva, se $m := \max(q, q')$, si ha

$$C_j(I_k) = C_j(I_m) \quad \text{per ogni} \quad j \geq 0\,, k \geq m.$$

Per finire, mostriamo che questo implica che $I_k = I_m$ per $k \geq m$ e quindi che la catena di ideali $\{I_j\}_{j\geq 0}$ di $A[X]$ staziona. Supponiamo che $I_m \subsetneq I_k$ e sia $f(X) := a_n X^n + \cdots + a_0$, $a_n \neq 0$, un polinomio di grado minimo in $I_k \setminus I_m$. Poiché $a_n \in C_n(I_k) = C_n(I_m)$, esiste un polinomio $g(X) \in I_m$ di grado n e coefficiente direttore a_n. Ma allora il polinomio $f(X) - g(X)$ ha grado strettamente minore di n e $f(X)-g(X) \in I_k \setminus I_m$, contro la minimalità di n. □

Osservazione 3.4 Se A è noetheriano, un anello di polinomi $A[\mathbf{X}]$ in infinite indeterminate $\mathbf{X} := \{X_\lambda\}$ su A non è noetheriano, perché l'ideale $\langle \mathbf{X} \rangle$ generato da tutte le indeterminate non è finitamente generato.

Proposizione 3.5 *Sia M un R-modulo e sia N un sotto A-modulo di M. Allora M è noetheriano se e soltanto se N è noetheriano ed il modulo quoziente M/N è noetheriano.*

Inoltre, se R è un anello noetheriano e $I \subseteq R$ è un ideale, l'anello quoziente R/I è noetheriano.

Dimostrazione: Supponiamo che M sia noetheriano. Ogni sottomodulo di N è anche un sottomodulo di M. Quindi è finitamente generato su R. Inoltre, ogni sottomodulo di M/N è del tipo L/N, dove L è un sottomodulo di M contenente N. Allora se L è finitamente generato, anche L/N lo è.

Se poi R è un anello noetheriano, ogni ideale di R/I è finitamente generato come R-modulo e quindi anche come R/I-modulo.

Viceversa, sia L un sottomodulo di M. Per ipotesi $L \cap N$ e $(L + N)/N$ sono finitamente generati. Per l'isomorfismo canonico $L/(L \cap N) \cong (L + N)/N$, L è finitamente generato modulo l'ideale $L \cap N$ e quindi è finitamente generato. □

Corollario 3.6 *Siano $M_1, \ldots, M_n$ R-moduli. Allora la somma diretta $M_1 \oplus \cdots \oplus M_n$ è un R-modulo noetheriano se e soltanto se $M_1, \ldots, M_n$ sono noetheriani.*

In particolare, se R è un anello noetheriano, R^n è un R-modulo noetheriano.

Dimostrazione: Per induzione su n, basta dimostrare il caso $n = 2$. Sia $M := M_1 \oplus M_2$. Allora M_1 si immerge canonicamente in M tramite l'isomorfismo $M_1 \cong M_1 \oplus \{0\}$ e M_2 è canonicamente isomorfo a $M/(M_1 \oplus \{0\})$. Quindi basta applicare la Proposizione 3.5. □

Corollario 3.7 *Sia A un anello noetheriano. Allora*

(1) *Ogni A-modulo finitamente generato $M := x_1 A + \cdots + x_n A$ è noetheriano.*

(2) *Ogni A-algebra finitamente generata $D := A[x_1, \ldots, x_n]$ è un anello noetheriano.*

Dimostrazione: (1) L'applicazione

$$A^n \longrightarrow M\,; \quad (c_1, \ldots, c_n) \mapsto x_1c_1 + \cdots + x_nc_n$$

è un omomorfismo A-lineare suriettivo. Allora M è A-isomorfo ad un quoziente di A^n ed in quanto tale è un A-modulo noetheriano (Proposizioni 3.6 e 3.5(1)).

(2) L'anello di polinomi $A[X_1, \ldots, X_n]$ è noetheriano (Teorema 3.3). Poiché l'applicazione

$$A[X_1, \ldots, X_n] \longrightarrow D\,; \quad X_i \mapsto x_i$$

è un omomorfismo suriettivo, D è un quoziente di $A[X_1, \ldots, X_n]$ ed in quanto tale è noetheriano (Proposizione 3.5(1)) □

Proposizione 3.8 *Sia S una parte moltiplicativa di A. Se A è un anello noetheriano, l'anello delle frazioni A_S è noetheriano.*

Dimostrazione: Tutti gli ideali di A_S sono estesi, cioè del tipo JA_S con J un ideale di A. Inoltre se J è finitamente generato anche JA_S lo è. □

Per la proposizione precedente, un anello noetheriano è localmente noetheriano. Ma la noetherianità *non è una proprietà locale*; infatti esistono molti esempi di anelli localmente noetheriani che non sono noetheriani. Tuttavia mostriamo ora che un dominio localmente noetheriano col carattere di finitezza è noetheriano.

Proposizione 3.9 *Sia A un anello e $I \subseteq A$ un ideale. Se I_M è finitamente generato, per ogni ideale massimale M, e ogni elemento non nullo di A è contenuto al più in un numero finito di ideali massimali, allora I è finitamente generato.*

In particolare, se A è un dominio, A_M è noetheriano, per ogni ideale massimale M, e l'intersezione $A := \cap A_M$ ha il carattere di finitezza, allora A è noetheriano.

Dimostrazione: Sia I un ideale di A. Vogliamo far vedere che I è finitamente generato. Per ipotesi I è contenuto in un numero finito di ideali massimali $M_1, \ldots, M_n$ e $I_{M_i} = (J_i)_{M_i}$ con $J_i \subseteq I$ finitamente generato. Sia $J := J_1 + \cdots + J_n$. Chiaramente $J \subseteq I$ e J è finitamente generato. Inoltre $I_{M_i} = (J_i)_{M_i} \subseteq J_{M_i} \subseteq I_{M_i}$, da cui $I_{M_i} = J_{M_i}$ per ogni i. Quindi, se $I \neq J$, J è contenuto in qualche ideale massimale diverso da $M_1, \ldots, M_n$.

Siano $M_1, \ldots, M_n, M_{n+1}, \ldots M_{n+k}$, $k \geq 1$, gli ideali massimali contenenti J. Poiché $I \nsubseteq M_{n+j}$, allora $I \nsubseteq M_{n+1} \cup \cdots \cup M_{n+k}$ (Prime Avoidance). Sia

$x \in I \setminus (M_{n+1} \cup \cdots \cup M_{n+k})$ e $J' := J + xA$. Allora $J \subseteq J' \subseteq I$, gli unici ideali massimali di A contenenti J' sono $M_1, \ldots, M_n$ e ancora $I_{M_i} = J_{M_i} = J'_{M_i}$ per ogni i. Ne segue che $I = J'$ è finitamente generato. □

Osserviamo che, se A è un dominio noetheriano, l'intersezione $A := \cap A_M$ non ha necessariamente il carattere di finitezza. Infatti ad esempio l'anello di polinomi $\mathbb{Z}[X]$ è noetheriano, ma l'elemento X è contenuto in tutti gli ideali massimali del tipo $\langle X, p \rangle$, $p \in \mathbb{Z}$ primo. Tuttavia vale il seguente risultato.

Proposizione 3.10 *Sia $I \neq (0)$ un ideale proprio di un anello A. Se ogni primo minimale di I è finitamente generato, allora I ha un numero finito di primi minimali.*

In particolare in un anello noetheriano ogni ideale proprio ha un numero finito di ideali primi minimali e quindi un dominio noetheriano di dimensione uno ha il carattere di finitezza.

Dimostrazione: Sia I un ideale proprio di A e sia $\mathrm{Min}(I) := \{P_\lambda\}$ la famiglia dei primi minimali di I. Se esistono $P_1, \ldots, P_n \in \mathrm{Min}(I)$ tali che $P_1 \ldots P_n \subseteq I$, allora ogni primo minimale di I contiene uno dei P_i e quindi per minimalità è uguale a P_i. Dunque $\mathrm{Min}(I) := \{P_1, \ldots, P_n\}$.

Supponiamo dunque che $P_{\lambda_1} \ldots P_{\lambda_n} \nsubseteq I$, per ogni scelta di $P_{\lambda_i} \in \mathrm{Min}(I)$, e consideriamo l'insieme di ideali

$$\mathcal{S} := \{J\,;\ I \subseteq J,\ P_{\lambda_1} \ldots P_{\lambda_n} \nsubseteq J,\ \text{per ogni } P_{\lambda_i} \in Min(I)\}.$$

$\mathcal{S}$ è non vuoto perché $I \in \mathcal{S}$. Applichiamo il Lemma di Zorn per mostrare che $\mathcal{S}$ ammette un elemento massimale.

Sia $\mathcal{C} := \{J_\alpha\} \subseteq \mathcal{S}$ una catena di ideali e sia $J := \cup J_\alpha$. Allora $J \in \mathcal{S}$. Infatti, poiché ogni P_{λ_i} è finitamente generato, anche ogni prodotto $P_{\lambda_1} \ldots P_{\lambda_n}$ lo è. Dunque se $P_{\lambda_1} \ldots P_{\lambda_n} \subseteq J$, esiste un ideale J_{α_0} della catena che contiene $P_{\lambda_1} \ldots P_{\lambda_n}$, mentre $J_{\alpha_0} \in \mathcal{S}$. Perciò ogni catena di $\mathcal{S}$ ha un maggiorante e $\mathcal{S}$ ha un elemento massimale M.

Mostriamo ora che M è un ideale primo. Siano $x, y \in A \setminus M$. Poiché $\langle M, x \rangle, \langle M, y \rangle \notin \mathcal{S}$, esistono primi minimali $P_1, \ldots, P_n, Q_1, \ldots, Q_m$ di I tali che $P_1 \ldots P_n \subseteq \langle M, x \rangle$ e $Q_1 \ldots Q_m \subseteq \langle M, y \rangle$. Allora $P_1 \ldots P_n Q_1 \ldots Q_m \subseteq \langle M, xy \rangle$. Dunque $\langle M, xy \rangle \notin \mathcal{S}$, ovvero $M \neq \langle M, xy \rangle$ e $xy \notin M$. In conclusione M è primo.

Ma, essendo $I \in \mathcal{S}$ ed M massimale in $\mathcal{S}$, si ha $I \subseteq M$ e dunque se M è primo esso contiene qualche primo minimale di I e allora $M \notin \mathcal{S}$. Questa contraddizione mostra che deve essere $\mathcal{S} = \emptyset$. Dunque $\mathrm{Min}(I)$ è finito. □

Notiamo che, se si assume che A sia noetheriano, per dimostrare la proposizione precedente il Lemma di Zorn non è necessario. Inoltre il fatto che in un anello noetheriano ogni ideale proprio ha un numero finito di primi

minimali discende anche dall'esistenza di una decomposizione primaria [1, Cap. 7].

Finalmente diamo alcune proprietà di divisibilità.

Proposizione 3.11 *Ogni dominio noetheriano è atomico.*

Dimostrazione: Segue dalla Proposizione 2.7, perché un anello noetheriano verifica in particolare la condizione della catena ascendente sugli ideali principali (Proposizione 3.1). □

Corollario 3.12 *Sia A un dominio noetheriano. Le seguenti proprietà sono equivalenti:*

(i) *A è un dominio con il massimo comune divisore;*

(ii) *A è un dominio a fattorizzazione unica;*

(iii) *Ogni ideale primo di altezza uno di A è principale.*

Dimostrazione: (i) $\Rightarrow$ (ii) Poiché un dominio noetheriano è atomico, A ha il massimo comune divisore se e soltanto se è a fattorizzazione unica (Teorema 2.10).

(ii) $\Rightarrow$ (iii) Poiché in un dominio Noetheriano gli ideali primi di altezza uno coincidono con gli ideali primi minimali sugli ideali principali (Principal Ideal Theorem) [6], possiamo ancora applicare il Teorema 2.10. □

Corollario 3.13 *Le seguenti proprietà sono equivalenti per un dominio A:*

(i) *A è un dominio a ideali principali;*

(ii) *Ogni ideale primo di A è principale;*

(iii) *A è un dominio a fattorizzazione unica di dimensione uno;*

(iv) *A è un dominio di Bezout noetheriano.*

Dimostrazione: (i) $\Leftrightarrow$ (iv) segue dalle definizioni.

(i) $\Rightarrow$ (iii) segue dalle Proposizioni 2.14 e 2.15.

(iii) $\Rightarrow$ (ii) Sia $M \neq (0)$ un ideale primo (ovvero massimale) di A. Per il Teorema 2.10, M contiene un ideale primo P principale, ma essendo A di dimensione uno, deve essere $M = P$.

(ii) $\Rightarrow$ (i) A è noetheriano per il Teorema di Cohen (Teorema 3.2). Sia $I \neq (0)$ un ideale proprio di A e sia $M_1 := \langle q_1 \rangle$ un ideale massimale contenente I. Allora $I_1 := q_1^{-1} I \subseteq A$ e $I = M_1 I_1$. Se $I_1 \neq A$, ripetendo il procedimento otteniamo $I_1 = M_2 I_2$ per qualche ideale massimale $M_2 := \langle q_2 \rangle$ e $I = M_1 M_2 I_2$. Così proseguendo, poiché la catena di ideali $I \subseteq I_1 \subseteq I_2 \subseteq \ldots$ staziona, per un certo n si ha $I_{n+1} = A$ e $I_n = M_n$. Allora $I = M_1 \ldots M_n = \langle q_1 \rangle \ldots \langle q_n \rangle = \langle q_1 \ldots q_n \rangle$ è principale. □

3.2 Dipendenza integrale

La nozione di dipendenza integrale è fondamentale in Algebra Commutativa.

Data un'estensione di anelli $A \subseteq B$, un elemento $x \in B$ si dice *intero su* A se x è radice di un polinomio monico a coefficienti in A, ovvero se esistono $a_{n-1}, \ldots, a_0 \in A$ tali che

$$f(x) := x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0.$$

L'espressione $f(x) = 0$ si chiama un *relazione di dipendenza integrale* per x su A. Si dice che B *è intero su* A, o che *l'estensione* $A \subseteq B$ *è intera*, se ogni elemento $x \in B$ è intero su A.

Ricordiamo alcune prime proprietà. Il caso che più ci interessa è quello in cui B sia un dominio; per il caso più generale e approfondimenti rimandiamo a [1, 6].

Proposizione 3.14 *Sia $A \subseteq B$ un'estensione di anelli. Le seguenti proprietà sono equivalenti per un elemento $x \in B$:*

(i) *x è intero su A;*

(ii) *$A[x]$ è un A-modulo finitamente generato;*

(iii) *Esiste un sotto A-modulo finitamente generato M di B tale che $xM \subseteq M$ e $\mathrm{Ann}_B M := \{b \in B\,;\, bM = (0)\} = (0)$.*

Dimostrazione: (i) $\Rightarrow$ (ii) Sia $f(x) := x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ una relazione di dipendenza integrale per x. Allora $A[x] = \sum x^i A$ è generato su A da $1, x, \ldots, x^{n-1}$.

(ii) $\Rightarrow$ (iii) Basta prendere $M := A[x]$, tenuto conto che $1 \in A[x] =: M$ e allora se $bM = 0$, per $b \in B$, si ha $b = b1 = 0$.

(iii) $\Rightarrow$ (i) Siano $b_1, \ldots, b_n \in B$ i generatori di M. Se $xM \subseteq M$, allora $xb_i = \sum_j a_{ij}b_j$ ($a_{ij} \in A$, $i, j = 1, \ldots, n$), da cui $\sum_j (\delta_{ij}x - a_{ij})b_j = 0$, dove δ_{ij} è il simbolo di Kronecker. Moltiplicando a sinistra per l'aggiunta della matrice $(\delta_{ij}x - a_{ij})$ (che ha valori in B), vediamo che $\det(\delta_{ij}x - a_{ij})b_j = 0$, per ogni b_j. Dunque $\det(\delta_{ij}x - a_{ij}) \in \mathrm{Ann}_B M$ e $f(x) := \det(\delta_{ij}x - a_{ij}) = 0$. Questa è una relazione di dipendenza integrale per x. □

Dalla Proposizione precedente segue, per induzione su $n \geq 1$, che se $x_1, \ldots, x_n \in B$ sono interi su A, allora $A[x_1, \ldots, x_n]$ è un A-modulo finitamente generato. Basta osservare che, se x_i è intero su A, lo è anche su $A[x_1, \ldots, x_{i-1}]$.

Notiamo che se A è un campo, x è intero su A se e soltanto se è algebrico su A. Mostriamo ora che le estensioni intere di campi sono campi.

Proposizione 3.15 *Sia $A \subseteq B$ un'estensione intera di anelli. Allora B è un campo se e soltanto se A è un campo.*

Dimostrazione: Sia $x \in B$ non nullo e sia $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, $a_i \in A$, una relazione di dipendenza integrale su A di grado minimo. Allora, poiché B è integro, deve necessariamente essere $a_0 \neq 0$. Se A è un campo, $a_0^{-1} \in A$ e, moltiplicando per $a_0^{-1}x^{-1}$, si ottiene $x^{-1} = -a_0^{-1}(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1) \in B$.

Viceversa, sia B un campo e sia $x \in A$, $x \neq 0$. Allora $x^{-1} \in B$ è intero su A e dunque $x^{-m} + a_{m-1}x^{-(m-1)} + \cdots + a_1x^{-1} + a_0 = 0$, con $a_i \in A$. Moltiplicando per x^{m-1}, si ottiene $x^{-1} = -(a_{m-1} + \cdots + a_1x^{m-2} + a_0x^{m-1}) \in A$. □

Proposizione 3.16 *Sia $A \subseteq B$ un'estensione intera di domini. Allora:*

(1) *Se $I \subseteq B$ è un ideale e $J := I \cap A$, $\frac{B}{I}$ è intero su $\frac{A}{J}$. Inoltre, se I e J sono ideali primi, I è massimale se e soltanto se J è massimale.*

(2) *Se $S \subseteq A$ è una parte moltiplicativa, B_S è intero su A_S.*

Dimostrazione: (1) Poiché l'applicazione $\frac{A}{J} \longrightarrow \frac{B}{I}$, $a + J \mapsto a + I$ è iniettiva, possiamo identificare $\frac{A}{J}$ con la sua immagine in $\frac{B}{I}$. Sia $x \in B$ non nullo e sia $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, con $a_i \in A$, una relazione di dipendenza integrale per x. Riducendo modulo I, otteniamo una relazione di dipendenza integrale per $x + I$ su $\frac{A}{J}$.

L'ultima affermazione segue dalla Proposizione 3.15.

(2) Sia $\frac{x}{s} \in B_S$, $x \in B$, $s \in S$. Se $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, con $a_i \in A$, è una relazione di dipendenza integrale per x, allora moltiplicando per $\frac{1}{s^n}$, otteniamo una relazione di dipendenza integrale per $\frac{x}{s}$ su A_S: $(\frac{x}{s})^n + \frac{a_{n-1}}{s}(\frac{x}{s})^{n-1} + \cdots + \frac{a_0}{s^n} = 0$. □

La dipendenza integrale è una proprietà transitiva.

Proposizione 3.17 *Siano $A \subseteq B \subseteq C$ estensioni di anelli. Se C è intero su B e B è intero su A, allora C è intero su A.*

Dimostrazione: Applichiamo la Proposizione 3.14. Sia $x \in C$ e sia $x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$ una relazione di dipendenza integrale per x su B. Allora x è intero su $A' := A[b_0, \ldots, b_{n-1}]$. Poiché ogni b_i è intero su A, A' è un A-modulo finitamente generato e dunque anche $M := A'[x]$ è un A-modulo finitamente generato. Poiché $x \in (M : M)$ e $\mathrm{Ann}_C M = (0)$ (perché $1 \in M$), allora x è intero su A. □

Denotiamo con $\overline{A}_B$ l'insieme degli elementi $x \in B$ interi su A; chiaramente $A \subseteq \overline{A}_B$. A si dice *integralmente chiuso in* B se $A = \overline{A}_B$, cioè se ogni elemento di B che è intero su A appartiene ad A.

Corollario 3.18 *Sia $A \subseteq B$ un'estensione di anelli. L'insieme $\overline{A}_B$ degli elementi di B interi su A è un anello integralmente chiuso in B.*

Dimostrazione: Applichiamo la Proposizione 3.14. Siano $x, y \in B$ interi su A. Allora $M := A[x, y] \subseteq B$ è un A-modulo finitamente generato. Poiché $x - y$, $xy \in (M : M)$ e $\mathrm{Ann}_B\, M = (0)$ (perché $1 \in M$), $x - y$, xy sono interi su A. Che $\overline{A}_B$ è integralmente chiuso in B segue subito dalla definizione e dalla Proposizione 3.17. □

L'anello $\overline{A}_B$ si chiama la *chiusura integrale* di A in B. Se A è un dominio con campo dei quozienti K, poniamo semplicemente $\overline{A} := \overline{A}_K$. Diciamo inoltre che $\overline{A}$ è la *chiusura integrale* di A e che A è *integralmente chiuso* se $A = \overline{A}$.

Corollario 3.19 *Sia A un dominio con campo dei quozienti K e sia $x \in K$. Le seguenti condizioni sono equivalenti:*

(i) *x è intero su A;*

(ii) *Esiste un ideale non nullo finitamente generato I di A tale che $x \in (I : I)$.*

Quindi

$$\overline{A} = \cup\{(I : I);\ I \subseteq A \text{ ideale finitamente generato}\}$$

ed A è integralmente chiuso se e soltanto se $A = (I : I)$, per ogni ideale $I \subseteq A$ finitamente generato.

Dimostrazione: Segue dalla Proposizione 3.14, tenuto conto che un A-sottomodulo di K finitamente generato è un ideale frazionario di A ed inoltre che se $J := dI$, con $d \in A \setminus \{0\}$ e $I \subseteq A$ un ideale, allora $(J : J) = (I : I)$. □

Per un dominio, la proprietà di essere integralmente chiuso *è una proprietà locale.*

Proposizione 3.20 *Sia A un dominio con campo dei quozienti K.*

(1) *Se A è integralmente chiuso, ogni anello di frazioni A_S è integralmente chiuso.*

(2) *Se $\{A_\lambda\}$ è una famiglia di domini integralmente chiusi in K, il dominio $A = \cap A_\lambda$ è integralmente chiuso.*

(3) *A è integralmente chiuso se e soltanto se A_M è integralmente chiuso per ogni ideale massimale M.*

Dimostrazione: (1) Ogni ideale di A_S è esteso, cioè del tipo IA_S per qualche ideale di A. Inoltre IA_S è finitamente generato se e soltanto se lo è I. Allora se A è integralmente chiuso, usando la Proposizione 1.8, per ogni IA_S finitamente generato si ha $A_S = (I : I)A_S = (IA_S : IA_S)$. Quindi A_S è integralmente chiuso.

(2) Se $x \in K$ è intero su A, lo è anche su ogni A_λ. Se ogni A_λ è integralmente chiuso, allora, $x \in \cap A_\lambda = A$ ed A è integralmente chiuso.

(3) Segue da (1) e (2), tenendo conto che $A = \cap\{A_M\,;\ M \in \mathrm{Max}(A)\}$ (Proposizione 1.9). □

Proposizione 3.21 *Ogni dominio con il massimo comune divisore è integralmente chiuso.*

Dimostrazione: Sia $x := \frac{a}{b} \in K$, a, $0 \neq b \in A$. Per l'esistenza del massimo comune divisore possiamo supporre che a e b siano coprimi. Se $f(x) := x^n + c_{n-1}x^{n-1} + \cdots + c_0 = 0$ è una relazione di dipendenza integrale per x, si ha $b^n f(x) = a^n + bc_{n-1}a^{n-1} + \cdots + b^n c_0 = 0$, ovvero $a^n = bc$, $c \in A$. Allora b divide a^n in A, ma allo stesso tempo è coprimo con a. Per il lemma di Euclide (Proposizione 2.5), vediamo che b deve essere invertibile in A e quindi $x \in A$. □

Una proprietà importante delle estensioni intere di un anello A è quella di avere la stessa dimensione di A. Per i nostri scopi ci basta sapere che se un dominio A ha dimensione uno, cioè ogni ideale primo non nullo di A è massimale, anche $\overline{A}$ ha dimensione uno.

Proposizione 3.22 *Sia $A \subseteq B$ un'estensione intera di domini. Se A ha dimensione uno, anche B ha dimensione uno.*

Dimostrazione: B non è un campo, perché non lo è A (Proposizione 3.15). Sia $Q \subseteq B$ un ideale primo non nullo e sia $P := Q \cap A$. Allora $B_{A\setminus P}$ è intero su A_P (Proposizione 3.16(2)) e $QB_{A\setminus P} \neq B_{A\setminus P}$ è un ideale primo di $B_{A\setminus P}$ tale che $QB_{A\setminus P} \cap A_P = PA_P$ è l'ideale massimale di A_P. Ne segue che $QB_{A\setminus P}$ è massimale in $B_{A\setminus P}$ (Proposizione 3.16(1)) e dunque Q è massimale in B. □

3.3 Domini di valutazione discreta

Esempi di domini di Bezout che non sono necessariamente principali sono i *domini di valutazione*. Una approfondita trattazione di questi anelli si trova in [5, Chapter III], oppure negli appunti in rete di S. Gabelli [4]. Qui ricordiamo le definizioni e qualche proprietà che ci sarà necessaria nello studio dei Domini di Dedekind.

Un dominio A con campo delle frazioni K si chiama un *dominio di valutazione* se, per ogni $x \in K$, si ha che $x \in A$ oppure $x^{-1} \in A$.

Ricordiamo che se un anello A ha un unico ideale massimale M si dice che A è *anello locale* e si scrive $A := (A, M)$. Si vede facilmente che A è un anello locale se e soltanto se l'insieme $A \setminus \mathcal{U}(A)$ è un ideale (massimale) [1, Proposition 1.6].

Proposizione 3.23 *Le seguenti proprietà sono equivalenti per un dominio A.*

(i) *A è un dominio di valutazione;*

(ii) *Gli ideali (frazionari) principali di A sono linearmente ordinati;*

(iii) *Gli ideali (frazionari) di A sono linearmente ordinati;*

(iv) *A è un dominio di Bezout locale.*

Dimostrazione: (i) $\Rightarrow$ (ii) Siano x, $y \in K$. Se $xy^{-1} \in A$, allora $xA \subseteq yA$. Altrimenti $(xy^{-1})^{-1} = x^{-1}y \in A$ e quindi $yA \subseteq xA$.

(ii) $\Rightarrow$ (iii) Siano I e J due ideali (frazionari) di A. Se $x \in J \setminus I$, per ogni $y \in I$ si ha $\langle y \rangle \subseteq \langle x \rangle$. Quindi $I \subseteq \langle x \rangle \subseteq J$.

(iii) $\Rightarrow$ (iv) A è locale perché in ogni dominio due ideali massimali che sono comparabili coincidono.

Siano x, $y \in A$. Se $\langle x \rangle \subseteq \langle y \rangle$ si ha $\langle x, y \rangle = \langle y \rangle$. Altrimenti $\langle y \rangle \subseteq \langle x \rangle$ e perciò $\langle x, y \rangle = \langle x \rangle$. Ne segue che A è di Bezout (Proposizione 2.12).

(iv) $\Rightarrow$ (ii) Sia M l'ideale massimale di A e siano x, $y \in A$. Supponiamo che $I := \langle x, y \rangle = \langle d \rangle$. Allora $d^{-1}I = A$ e quindi, posto $w := d^{-1}x$, $z := d^{-1}y$, risulta $1 = aw + bz$ per opportuni a, $b \in A$. Siccome $1 \notin M$, $aw \notin M$ oppure $bz \notin M$. Se $aw \notin M$, allora aw è invertibile in A; quindi $z = z(aw)(aw)^{-1} = w(az)(aw)^{-1} \in \langle w \rangle$. Segue che $\langle z \rangle \subseteq \langle w \rangle$ e dunque $\langle y \rangle \subseteq \langle x \rangle$. Analogamente, se $bz \notin M$ allora $\langle x \rangle \subseteq \langle y \rangle$.

(ii) $\Rightarrow$ (i) Sia $x = \frac{a}{b} \in K$. Gli ideali $\langle a \rangle$ e $\langle b \rangle$ sono comparabili per ipotesi. Se $\langle a \rangle \subseteq \langle b \rangle$, allora $xA \subseteq A$ e $x \in A$. Altrimenti $A \subseteq xA$ e quindi $x^{-1} \in A$. □

Corollario 3.24 *Un dominio di valutazione è integralmente chiuso.*

Dimostrazione: Poiché un dominio di valutazione è di Bezout (Proposizione 3.23), allora è integralmente chiuso per la Proposizione 3.21. □

Osservazione 3.25 Un'intersezione di domini di valutazione con stesso campo dei quozienti è un dominio integralmente chiuso (Proposizione 3.20(2)). Krull ha dimostrato che la chiusura integrale di un dominio A in un campo F è l'intersezione di tutti i domini di valutazione di F contenenti A [1, Corollary 5.22].

Proposizione 3.26 *Sia A un dominio di valutazione. Allora ogni sopra-anello di A è un dominio di valutazione ed è la localizzazione di A rispetto ad un ideale primo. In particolare, se A ha dimensione uno, allora A non ha sopra-anelli propri.*

Dimostrazione: Sia B un sopra-anello di A. Se $x \notin B$, allora $x \notin A$; quindi $x^{-1} \in A \subseteq B$. Ne segue che B è un dominio di valutazione. In particolare B è locale. Sia M l'ideale massimale di B e sia $P := M \cap A$. Mostriamo che $A_P = B$. Chiaramente $A_P \subseteq B$. Viceversa, sia $x \in B \setminus A$. Poiché $x^{-1} \in A \subseteq B$, allora x è invertibile in B. Dunque $x^{-1} \in A \setminus M = A \setminus P$. Ne segue che $x \in A_P$. □

Un dominio di valutazione noetheriano si chiama un *dominio di valutazione discreta*, in breve un DVR.

Teorema 3.27 *Le seguenti proprietà sono equivalenti per un dominio A:*

(i) *A è un dominio di valutazione discreta (cioè un dominio di valutazione noetheriano);*

(ii) *A è un dominio di valutazione a ideali principali;*

(iii) *A è un dominio locale a ideali principali;*

(iv) *A è un dominio locale di dimensione uno il cui ideale massimale è principale;*

(v) *Esiste $t \in A$ (*parametro uniformizzante*) tale che, per ogni elemento non nullo $x \in A$ si ha $x = ut^n$, con $u \in \mathcal{U}(A)$ e $n \geq 0$ univocamente determinati;*

(vi) *Esiste $t \in A$ tale che, per ogni ideale non nullo I di A, $I = \langle t^n \rangle$ con $n \geq 0$;*

(vii) *A è un dominio locale e, se M è il suo ideale massimale, tutti e soli gli ideali non nulli di A sono gli ideali M^n, $n \geq 0$;*

(viii) *A è un dominio locale noetheriano integralmente chiuso di dimensione uno.*

Dimostrazione: (i) $\Rightarrow$ (ii) perché un dominio di valutazione è di Bezout, cioè ogni ideale finitamente generato è principale (Proposizione 3.23).

(ii) $\Rightarrow$ (i) e (ii) $\Rightarrow$ (iii) sono evidenti.

(iii) $\Rightarrow$ (iv) perché un dominio a ideali principali ha dimensione uno (Proposizione 2.14).

(iv) $\Rightarrow$ (v) Poiché A ha un unico ideale massimale, per il Teorema di Cohen (Teorema 3.2), A è noetheriano. Sia t un generatore dell'ideale massimale M di A. Se $x \in A$ è invertibile, allora $x = xt^0$. Altrimenti $x \in M$,

quindi $x = x_1 t$ con $x_1 \in A$. Se x_1 non è invertibile, possiamo scrivere $x_1 = x_2 t$, con $x_2 \in A$ e dunque $x = x_2 t^2$. Così proseguendo, otteniamo una catena di ideali principali

$$\langle x \rangle \subseteq \langle x_1 \rangle \subseteq \langle x_2 \rangle \subseteq \ldots \subseteq \langle x_k \rangle \subseteq \ldots .$$

Per noetherianità, tale catena staziona, cioè $\langle x_n \rangle = \langle x_{n+1} \rangle$ per qualche intero $n \geq 0$. Allora $x_n = u$ è invertibile e $x = ut^n$ (altrimenti per costruzione $x_n = x_{n+1} t$ e $\langle x_n \rangle \subsetneq \langle x_{n+1} \rangle$).

Per l'unicità, se $x = ut^n = vt^m$, allora $(u - v)t^{n-m} = 0$, da cui $u = v$ e $n = m$.

(v) $\Rightarrow$ (vi) Per ipotesi $x = ut^n \in A$ è invertibile se e soltanto se $n = 0$. Sia I un ideale proprio di A e sia $S := \{k \geq 1 \,;\ \text{tali che } ut^k \in I\}$. Se n è il minimo intero in S, allora $I = \langle t^n \rangle$.

(vi) $\Rightarrow$ (vii) È evidente che A è locale con ideale massimale $M = \langle t \rangle$. Inoltre se $I = \langle t^n \rangle$ allora $I = M^n$.

(vii) $\Rightarrow$ (vi) Si ha $M \neq M^2$, altrimenti $M = M^n$ per ogni $n \geq 1$ e M sarebbe l'unico ideale proprio non nullo del dominio A, il che è impossibile. Sia $t \in M \setminus M^2$. Poiché $\langle t \rangle = M^k$ per qualche $k \geq 1$, allora $k = 1$. Ovvero $M = \langle t \rangle$ e $M^n = \langle t^n \rangle$.

(vi) $\Rightarrow$ (ii) A è evidentemente ad ideali principali. Inoltre gli ideali di A sono linearmente ordinati. Quindi A è un dominio di valutazione per la Proposizione 3.23.

(ii) $\Rightarrow$ (viii) A è evidentemente noetheriano ed ha dimensione uno perché è a ideali principali (Proposizione 2.14). Infine A è locale per la Proposizione 3.23 e integralmente chiuso per il Corollario 3.24.

(viii) $\Rightarrow$ (iv) Basta mostrare che l'ideale massimale di A è principale. Sia $x \in A$ un elemento non nullo. Poiché M è l'unico ideale primo non nullo di A, allora l'ideale principale $I := \langle x \rangle$ ha radicale M. Poiché M è finitamente generato, le potenze di M sono tutte distinte (Proposizione 1.7). Inoltre I contiene una potenza M^n di M. Perciò, scegliendo n minimale, $M^{n-1} \nsubseteq I$. Sia $y \in M^{n-1} \setminus I$, così che $yM \subseteq M^n \subseteq I$ e $\frac{y}{x} M \subseteq A$. Mostriamo che $\frac{y}{x} M = A$ e dunque $M = \langle \frac{x}{y} \rangle$. Se $\frac{y}{x} M \neq A$, necessariamente $\frac{y}{x} M \subseteq M$ e $\frac{y}{x} \subseteq (M : M)$ è intero su A. Poiché A è integralmente chiuso, allora $\frac{y}{x} \in A$ e $y \in I$. Contraddizione. $\square$

Osservazione 3.28 La terminologia *dominio di valutazione* deriva dal fatto che ad ogni dominio di valutazione A si può associare una valutazione sul suo campo dei quozienti K e viceversa ad ogni valutazione su K resta associato un dominio di valutazione con campo dei quozienti K nel seguente modo.

Un gruppo abeliano $(G, *)$ è un *gruppo (totalmente) ordinato* se in esso è definita una relazione $\leq$ di ordine (totale) compatibile con l'operazione, cioè tale che:

$$x \leq x' \,,\ y \leq y' \Rightarrow x * y \leq x' * y'.$$

Se G è un gruppo additivo ordinato e α è un simbolo, possiamo estendere l'operazione di G e la sua relazione di ordine all'insieme $G \cup \{\alpha\}$ ponendo, per ogni $x \in G$:

$$x < \alpha\,; \quad x * \alpha = \alpha * x = \alpha.$$

In notazione additiva, si usa porre $\alpha = \infty$, mentre in notazione moltiplicativa si usa $\alpha = 0$.

Se K è un campo e G è un gruppo additivo totalmente ordinato, una applicazione suriettiva $v : K \longrightarrow G \cup \{\infty\}$ si dice una *valutazione su* K se

$$\begin{gathered} v(x) = \infty \text{ se e soltanto se } x = 0; \\ v(xy) = v(x) + v(y), \text{ per ogni } x, y \in K; \\ v(x + y) \geq \min\{v(x), v(y)\}. \end{gathered}$$

In notazione moltiplicativa, $v : K \longrightarrow G \cup \{0\}$ è una valutazione se:

$$\begin{gathered} v(x) = 0 \text{ se e soltanto se } x = 0; \\ v(xy) = v(x)v(y), \text{ per ogni } x, y \in K; \\ v(x + y) \leq \max\{v(x), v(y)\}. \end{gathered}$$

Se A è un dominio con campo dei quozienti K, il gruppo moltiplicativo quoziente $\Delta(A) = \dfrac{K^*}{U(A)}$ si dice il *gruppo di divisibilità* di A. $\Delta(A)$ è un gruppo ordinato moltiplicativo rispetto alla relazione

$$xU(A) \leq yU(A) \iff xy^{-1} \in A.$$

Allora:

(1) Se v è una valutazione su un campo K, l'insieme $A_v := \{x \in K\,; v(x) \geq 0\}$ è un anello di valutazione con ideale massimale $M_v := \{x \in K\,; v(x) > 0\}$.

(2) Se (V, M) è un anello di valutazione con campo dei quozienti K, il suo gruppo di divisibilità $\Delta(V)$ è totalmente ordinato e l'applicazione $v : V \longrightarrow \Delta(V) \cup \{0\}$ definita da

$$v(0) = 0 \text{ e } v(x) = xU(V) \text{ per } x \in K^*$$

è una valutazione su K, il cui anello di valutazione A_v coincide con V.

(3) Un dominio di valutazione V è un DVR se e soltanto se $\Delta(V)$ è ordinatamente isomorfo all'anello degli interi $\mathbb{Z}$.

Riguardo a (3) notiamo che se A è un DVR, ogni elemento non nullo del campo dei quozienti K è del tipo $\frac{ut^n}{vt^m} = wt^k$, con $w \in \mathcal{U}(A)$ e $k \in \mathbb{Z}$. Allora una valutazione su K a valori in $\mathbb{Z}$ resta definita ponendo $wt^k \mapsto k$.

3.4 Domini di Dedekind

Un *dominio di Dedekind* si definisce come un dominio noetheriano, integralmente chiuso di dimensione uno. Questa nozione globalizza quella di dominio di valutazione discreta, nel senso del risultato seguente.

Teorema 3.29 *Le seguenti condizioni sono equivalenti per un dominio A:*

(i) *A è un dominio di Dedekind (cioè un dominio noetheriano, integralmente chiuso di dimensione uno);*

(ii) *A_M è un dominio di valutazione discreta, per ogni ideale massimale M di A, e l'intersezione $A = \cap A_M$ ha il carattere di finitezza;*

(iii) *A è un dominio noetheriano e A_M è un dominio di valutazione discreta, per ogni ideale massimale M di A.*

(iv) *A ha dimensione uno ed esiste una famiglia di domini di valutazione discreta $\{V_\lambda\}$ in K tale che $A = \cap V_\lambda$ con il carattere di finitezza.*

Dimostrazione: (i) $\Rightarrow$ (ii) A_M è noetheriano di dimensione uno (Proposizione 3.8) ed è integralmente chiuso (Proposizione 3.20(1)). Dunque è un DVR per il Teorema 3.27.

(ii) $\Rightarrow$ (iii) segue dalla Proposizione 3.9.

(iii) $\Rightarrow$ (i) Poiché A_M ha dimensione uno per ogni M, anche A ha dimensione uno. Inoltre A è integralmente chiuso per la Proposizione 3.20(3).

(ii) $\Rightarrow$ (iv) è chiaro.

(iv) $\Rightarrow$ (ii) Sia M un ideale massimale di A. Allora, per il carattere di finitezza dell'intersezione, si ha $A_M = (\cap V_\lambda)_{A\setminus M} = \cap((V_\lambda)_{A\setminus M})$ (Proposizione 1.1). Ma poiché V_λ è un DVR, $(V_\lambda)_{A\setminus M}$ può essere uguale soltanto a V_λ oppure al campo dei quozienti K (Proposizione 3.26). Inoltre, sempre per il carattere di finitezza, $(V_\lambda)_{A\setminus M} = V_\lambda$ soltanto per un numero finito di indici λ. Perció $A_M = V_1 \cap \cdots \cap V_n$ è intersezione di un numero finito di anelli di valutazione discreta, ognuno centrato su M. Ne segue che $A_M = V_1 = \cdots = V_n$ [5, Theorem 22.8].

In conclusione A_M è un DVR per ogni $M \in \mathrm{Max}(A)$ e $A = \cap A_M$ con il carattere di finitezza. □

Osservazione 3.30 (1) Se A_M è un dominio di valutazione discreta per ogni ideale massimale M, non è detto che A sia di Dedekind. Infatti può accadere che l'intersezione $A = \cap A_M$ non abbia il carattere di finitezza [5, Section 36].

(2) Se esiste una famiglia di domini di valutazione discreta $\{V_\lambda\}$ in K tale che $A = \cap V_\lambda$ con il carattere di finitezza, A si chiama un *dominio di Krull* [5, Section 43]. Per il Teorema 3.29, un dominio di Dedekind è precisamente un dominio di Krull di dimensione uno.

Tutti i domini di Krull sono integralmente chiusi e i domini noetheriani e integralmente chiusi sono di Krull; ma un dominio di Krull non è necessariamente noetheriano né di dimensione uno. Ad esempio l'anello di polinomi $k[X_1, \ldots, X_n]$ in n indeterminate a coefficienti in un campo k è un dominio di Krull di dimensione n e l'anello di polinomi $k[X_\alpha]$ in infinite indeterminate su k è un dominio di Krull che non è noetheriano.

Un importante teorema di Mori-Nagata asserisce che la chiusura integrale di un dominio noetheriano è di Krull [2, Theorem 4.3].

(3) Se A_M è un dominio di valutazione, per ogni ideale massimale M, allora A si chiama un *dominio di Prüfer* [5, Chapter IV]. I domini di Dedekind sono precisamente i domini di Prüfer noetheriani o anche i domini che sono allo stesso tempo di Prüfer e di Krull.

In termini di divisibilità, i domini di Dedekind a fattorizzazione unica sono precisamente i domini a ideali principali. Ricordiamo tuttavia che, per la noetherianità, ogni dominio di Dedekind è atomico (Proposizione 3.11).

Teorema 3.31 *Le seguenti condizioni sono equivalenti per un dominio A:*

(i) *A è un dominio a ideali principali;*

(ii) *A è un dominio di Dedekind a fattorizzazione unica.*

Dimostrazione: (i) $\Rightarrow$ (ii) A è noetheriano per il Teorema di Cohen (Teorema 3.2). Inoltre A è a fattorizzazione unica di dimensione uno (Teorema 3.13) e quindi integralmente chiuso per la Proposizione 3.21.

(ii) $\Rightarrow$ (i) per il Teorema 3.13, perché un dominio di Dedekind ha dimensione uno. □

Corollario 3.32 *Le seguenti condizioni sono equivalenti per un dominio di Dedekind A:*

(i) *A è un dominio a ideali principali;*

(ii) *A è un dominio a fattorizzazione unica;*

(iii) *A è un dominio di Bezout;*

(iv) *A è un dominio con il massimo comune divisore.*

Dimostrazione: (i) $\Leftrightarrow$ (ii) per il Teorema 3.31. (i) $\Rightarrow$ (iii) $\Rightarrow$ (iv) segue dalle definizioni (Paragrafo 2.3). (iv) $\Rightarrow$ (ii) perché A è noetheriano (Corollario 3.12). □

4 Fattorizzazione in ideali primi

Vogliamo ora caratterizzare i domini di Dedekind dal punto di vista della Teoria degli Ideali. In particolare, faremo vedere che in un dominio di Dedekind ogni ideale proprio si fattorizza unicamente in ideali primi, anche se fallisce l'unicità della fattorizzazione in elementi irriducibili. Per questo introduciamo il concetto di ideale frazionario invertibile.

4.1 Ideali invertibili

Nel seguito indicheremo con $\mathcal{F}(A)$ l'insieme degli ideali frazionari non nulli del dominio A. Poiché $\mathcal{F}(A)$ è chiuso rispetto alla moltiplicazione di ideali, $\mathcal{F}(A)$ è un semigruppo moltiplicativo commutativo, con unità A.

Un ideale frazionario non nullo I di A si dice *invertibile* se è invertibile nel semigruppo $\mathcal{F}(A)$, cioè se esiste un (unico) ideale frazionario J tale che $IJ = A$.

Notiamo che un ideale invertibile I è *cancellabile*, ovvero, dati $H_1, H_2 \in \mathcal{F}(A)$, si ha $IH_1 \subseteq IH_2$ se e soltanto se $H_1 \subseteq H_2$.

Proposizione 4.1 *Se $I \in \mathcal{F}(A)$ è un ideale invertibile, allora il suo inverso è $(A : I)$. Dunque I è invertibile se e soltanto se $I(A : I) = A$.*

Dimostrazione: Sia $A = IJ$. Allora $J \subseteq (A : I)$ e $A = IJ \subseteq I(A : I) \subseteq A$, da cui $A = I(A : I)$. Per l'unicità dell'inverso, $J = (A : I)$. □

Proposizione 4.2 *Sia I un ideale frazionario invertibile. Allora, per ogni $J, H \in \mathcal{F}(A)$,*

$$(IJ : H) = I(J : H)\,; \quad (H : IJ) = (A : I)(H : J).$$

In particolare $(I : I) = A$.

Dimostrazione: Per la prima uguaglianza, $x \in (IJ : H) \Leftrightarrow xH \subseteq IJ \Leftrightarrow x(A : I)H \subseteq J \Leftrightarrow x(A : I) \subseteq (J : H) \Leftrightarrow x \in I(J : H)$. Da questa, per $H = I$ e $J = A$, otteniamo $(I : I) = A$.

La seconda uguaglianza si prova in modo analogo. □

Proposizione 4.3 *Un ideale frazionario invertibile è finitamente generato.*

Dimostrazione: Sia $I \in \mathcal{F}(A)$ invertibile e sia $J \in \mathcal{F}(A)$ tale che $IJ = A$. Poiché $1 \in IJ$, esistono $x_1, \ldots, x_n \in I$ e $y_1, \ldots, y_n \in J$ tali che $1 = x_1y_1 + \cdots + x_ny_n$. Allora, per ogni $a \in I$, risulta $a = a1 = x_1(ay_1) + \cdots + x_n(ay_n)$. Poiché $ay_i \in IJ = A$, ne segue che $x_1, \ldots, x_n$ generano I. □

Proposizione 4.4 *Se A ha un numero finito di ideali massimali, ogni ideale frazionario invertibile di A è principale.*

Dimostrazione: È sufficiente dimostrare l'asserto per gli ideali interi. Siano $M_1, \ldots, M_n$ gli ideali massimali di A e sia $I \subseteq A$ un ideale invertibile.

Se $n = 1$, A è locale, con ideale massimale $M = M_1$. Poiché I è invertibile, $I \neq IM$. Allora, se $x \in I \setminus IM$, $x(A : I) \subseteq A$ è un ideale che non è contenuto in M. Ne segue che $x(A : I) = A$ e $I = xA$ è principale.

Sia ora $n \geq 2$. Poiché $M_i \not\supseteq \cap_{j \neq i} M_j$ ed I è invertibile, allora $IM_i \not\supseteq I(\cap_{j \neq i} M_j)$ per ogni $i = 1, \ldots, n$. Sia $x_i \in I(\cap_{j \neq i} M_j) \setminus IM_i$ e $x := x_1 + \cdots + x_n$. Allora $x \in I$ e $x \notin IM_i$. Ne segue che $x(A : I) \subseteq A$ e $x(A : I) \not\subseteq M_i$ per ogni i e dunque $x(A : I) = A$ e $I = xA$. □

Proposizione 4.5 *Sia $A \subseteq B$ un'estensione di domini. Se $I \in \mathcal{F}(A)$ è invertibile, allora $IB \in \mathcal{F}(B)$ è invertibile.*

Dimostrazione: Sia $A = IJ$. Allora $B = IJB = (IB)(JB)$. □

Dalla proposizione precedente otteniamo che, se $I \in \mathcal{F}(A)$ è invertibile, per ogni estensione $A \subseteq B$, si ha $(A : I)B = (B : IB)$.

Proposizione 4.6 *Sia I un ideale frazionario non nullo di A. Le seguenti condizioni sono equivalenti:*

(i) *I è un ideale invertibile;*

(ii) *I è finitamente generato e IA_M è principale, per ogni ideale massimale M di A.*

Dimostrazione: (i) $\Rightarrow$ (ii) I è finitamente generato per la Proposizione 4.3. Poiché IA_M è invertibile (Proposizione 4.5) allora esso è principale per la Proposizione 4.4.

(ii) $\Rightarrow$ (i) Poiché I è finitamente generato, per ogni ideale massimale M di A, si ha $(A : I)A_M = (A_M : IA_M)$. Inoltre $I(A : I)A_M = IA_M(A_M : IA_M) = A_M$. Quindi $I(A : I) = A$ (Proposizione 1.9). □

Proposizione 4.7 (1) *Se $I \in \mathcal{F}(A)$ è un ideale invertibile e $I = JH$, con $J, H \in \mathcal{F}(A)$, allora J, H sono ideali invertibili.*

(2) *Se $J \subseteq I \subseteq A$ sono ideali e I è invertibile, allora $J = IH$, per un ideale $H \subseteq A$.*

(3) *Se P, Q sono ideali primi invertibili e $P \subseteq Q$, allora $P = Q$.*

Dimostrazione: (1) $A = I(A : I) = J((A : I)H) = (J(A : I))H$.

(2) Se $J \subseteq I$, allora $H := J(A : I) \subseteq A$. Perciò se I è invertibile, $J = I(A : I)J = IH$.

(3) Se $P \subseteq Q$, per (2), $P = QH$, con $H := (A : Q)P \subseteq A$. Poiché $H \not\subseteq P$ (altrimenti cancellando P sarebbe $(A : Q) = A$) allora $Q \subseteq P$ e $P = Q$. □

4.2 Fattorizzazione in ideali primi

La proprietà che storicamente ha giustificato l'introduzione e lo studio dei domini di Dedekind è la possibilità di fattorizzare gli ideali propri in ideali primi.

Proposizione 4.8 *Sia A un dominio. Allora:*

(1) *Se I è un ideale invertibile e $I = P_1 \dots P_n$ è prodotto di ideali primi, gli ideali primi P_i sono univocamente determinati.*

(2) *Se ogni ideale proprio si fattorizza in ideali primi, ogni ideale primo invertibile è massimale.*

Dimostrazione: (1) Siano $I = P_1 \dots P_n = Q_1 \dots Q_m$ due fattorizzazioni di I in ideali primi, necessariamente invertibili per la Proposizione 4.7(1). Allora $P_1 \dots P_n \subseteq Q_1$ e, a meno dell'ordine, possiamo supporre che sia $P_1 \subseteq Q_1$. Dunque $P_1 = Q_1$ per la Proposizione 4.7(3). Cancellando P_1, otteniamo $P_2 \dots P_n = Q_2 \dots Q_m$ e, proseguendo per ricorsione, concludiamo che $n = m$ e gli ideali P_i e Q_i coincidono, per ogni $i = 1, \dots, k$.

(2) Supponiamo che ogni ideale proprio di A si fattorizzi in ideali primi e sia P un ideale primo non nullo di A; mostriamo che, se P è invertibile, $\langle P, x\rangle = A$, per ogni $x \in A \backslash P$. Per questo, facciamo vedere che, se $x \in A \backslash P$ è tale che $\langle P, x\rangle \neq A$, risulta $P = P\langle P, x\rangle$. Quindi P non può essere invertibile.

Se $\langle P, x\rangle \neq A$, fattorizziamo $\langle P, x\rangle$ e $\langle P, x^2\rangle$ in ideali primi:

$$\langle P, x\rangle = P_1^{a_1} \dots P_n^{a_n}\,; \quad \langle P, x^2\rangle = Q_1^{b_1} \dots Q_m^{b_m}.$$

Applicando (1) all'ideale principale del quoziente A/P generato dalla classe $x^2 + P$, vediamo che $n = m$, $P_i/P = Q_i/P$ e $b_i = 2a_i$ per $i = 1, \dots, n$. Poiché $P \subseteq P_i, Q_i$, allora $P_i = Q_i$ e $\langle P, x^2\rangle = \langle P, x\rangle^2$. Da cui

$$P \subseteq \langle P, x^2\rangle = \langle P, x\rangle^2 = \langle P^2, xP, x^2\rangle \subseteq \langle P^2, x\rangle.$$

Sia $p \in P$ e scriviamo $p = y + ax$, $y \in P^2$, $a \in A$. Allora $ax = p - y \in P$ e, poiché $x \notin P$, deve essere $a \in P$. In conclusione, $P \subseteq P^2 + Px = P\langle P, x\rangle \subseteq P$, da cui $P = P\langle P, x\rangle$. □

Teorema 4.9 *Le seguenti condizioni sono equivalenti per un dominio A:*

(i) *A è un dominio di Dedekind;*

(ii) *Ogni ideale frazionario non nullo di A è invertibile;*

(iii) *Ogni ideale primo non nullo di A è invertibile;*

(iv) *Ogni ideale proprio di A è prodotto di un numero finito di ideali primi (univocamente determinati).*

Dimostrazione: (i) $\Rightarrow$ (ii) Basta considerare ideali $I \subseteq A$. Se A è di Dedekind, ogni ideale I di A è finitamente generato. Inoltre, poiché A_M è un DVR, per ogni ideale massimale M (Teorema 3.29), IA_M è principale. Quindi se I è non nullo, esso è invertibile (Proposizione 4.6).

(ii) $\Rightarrow$ (iii) è chiaro.

(iii) $\Rightarrow$ (iv) A è noetheriano per il Teorema di Cohen (Teorema 3.2), perché gli ideali invertibili sono finitamente generati (Proposizione 4.3). Sia $I \neq (0)$ un ideale proprio di A e sia M_1 un ideale massimale contenente I. Poiché M_1 è invertibile, possiamo scrivere $I = M_1 J_1$ con J_1 un ideale di A (Proposizione 4.7(2)). Se $J_1 \neq A$, sia M_2 un ideale massimale contenente J_1. Allora come prima $J_1 = M_2 J_2$ con J_2 un ideale di A. Poiché la catena $I \subseteq J_1 \subseteq J_2 \subseteq \dots$ staziona, ad un certo punto il procedimento ha termine e $I = M_1 \dots M_k$.

(iv) $\Rightarrow$ (iii) Sia Q un ideale primo non nullo e sia $0 \neq x \in Q$. Se $\langle x \rangle = P_1 \dots P_n$ e la fattorizzazione dell'ideale $\langle x \rangle$ in ideali primi, i P_i essendo invertibili sono massimali per la Proposizione 4.8(2). Allora $Q = P_i$ per qualche i e Q è invertibile.

(iii) $\Rightarrow$ (i) A è noetheriano per il Teorema di Cohen (Teorema 3.2), perché gli ideali invertibili sono finitamente generati (Proposizione 4.3). Inoltre A ha dimensione uno per la Proposizione 4.7(3). Infine, se $M \in \mathrm{Max}(A)$, MA_M è principale per la Proposizione 4.6. Dunque A_M è un DVR (Teorema 3.27). In conclusione A è un dominio di Dedekind (Teorema 3.29). □

Il seguente corollario dice che ogni ideale di un dominio di Dedekind è $(1, \frac{1}{2})$-*generato.*

Corollario 4.10 *Sia A un dominio di Dedekind e $I \subseteq A$ un ideale non nullo. Allora per ogni elemento non nullo $\alpha \in I$, esiste $\beta \in I$ tale che $I = \langle \alpha, \beta \rangle$.*

Dimostrazione: Poiché $\alpha \in I$, si ha $J := \alpha(A : I) \subseteq A$. Mostriamo che esiste $\beta \in I$ tale che $\beta(A : I) + J = \beta(A : I) + \alpha(A : I) = \langle \alpha, \beta \rangle (A : I) = A$, da cui $I = \langle \alpha, \beta \rangle$.

Siano $P_1, \dots, P_n$ gli ideali massimali di A contenenti J. Se $\beta(A : I) + J \neq A$, allora $\beta(A : I) \subseteq \beta(A : I) + J \subseteq P_k$ per qualche $k = 1, \dots, n$. Allora basta trovare un elemento $\beta \in I$ tale che $\beta(A : I) \nsubseteq P_k$ per ogni $k = 1, \dots n$, equivalentemente un elemento $\beta \in I \setminus IP_k$. Per l'unicità della fattorizzazione in ideali primi, si ha $I \neq IP_k$ per ogni k. Quindi se $n = 1$ un tale β esiste. Se $n \geq 2$, poniamo $I_k := IP_1 \dots P_{k-1} P_{k+1} \dots P_n$. Per quanto appena osservato, esiste $\beta_k \in I_k \setminus I_k P_k$. Sia $\beta := \beta_1 + \dots + \beta_n$. Poiché $I_k \subseteq I$, allora $\beta \in I$. D'altra parte $\beta \notin IP_k$ per ogni k. Infatti, se $j \neq k$, si ha $\beta_j \in I_j \subseteq IP_k$ e allora, se $\beta \in IP_k$, anche $\beta_k = \beta - \beta_1 - \dots - \beta_{k-1} - \beta_{k+1} - \dots - \beta_n \in IP_k$. □

Corollario 4.11 *Un dominio di Dedekind con un numero finito di ideali massimali è un dominio a ideali principali.*

Dimostrazione: Segue dal Teorema 4.9 e la Proposizione 4.4. □

Osservazione 4.12 (1) Dal Teorema 4.9, si ottiene che se A è di Dedekind il gruppo $\mathcal{F}(A)$ dei suoi ideali frazionari non nulli è libero, generato dall'insieme degli ideali primi.

Infatti, se $I \in \mathcal{F}(A)$ e $J := dI \subseteq A$, $0 \neq d \in A$, possiamo scrivere dA e J come prodotto di ideali primi univocamente determinati: $dA = P_1^{a_1} \dots P_n^{a_n}$, $J = Q_1^{b_1} \dots Q_m^{b_m}$. Allora $I = P_1^{-a_1} \dots P_n^{-a_n} Q_1^{b_1} \dots Q_m^{b_m} = X_i^{z_1} \dots X_k^{z_k}$ con gli X_i ideali primi univocamente determinati e $z_i \in \mathbb{Z}$, $i = 1, \dots, k$ (dove $X^0 := A$ e $X^{-n} := (A : X)^n = (A : X^n)$).

(2) In un dominio noetheriano A ogni ideale proprio I ha una *decomposizione primaria*, cioè è intersezione di un numero finito di ideali primari [1, Theorem 7.13]. Se poi A ha dimensione uno, questi ideali sono univocamente determinati [1, Theorem 4.10] e dunque, per comassimalità, $I = Q_1 \cap \dots \cap Q_n = Q_1 \dots Q_n$, dove gli ideali Q_i sono primari e univocamente determinati. Tuttavia ricordiamo che, se Q è M-primario, con $M \in \mathrm{Max}(A)$, non è detto che Q sia una potenza di M [1, Example 2, pag. 51].

4.3 Il Gruppo delle Classi

Se A è un dominio, gli ideali frazionari invertibili di A formano un gruppo abeliano moltiplicativo, che denoteremo con $\mathrm{Inv}(A)$. L'insieme $P(A)$ degli ideali frazionari principali non nulli è un sottogruppo di $\mathrm{Inv}(A)$. Resta allora definito il gruppo quoziente $C(A) := \mathrm{Inv}(A)/P(A)$, che si chiama il *gruppo delle classi (di ideali)* o *gruppo di Picard* di A.

Per definizione, due ideali frazionari invertibili I e J di A appartengono alla stessa classe di $C(A)$ se e soltanto se $I = xJ$ per qualche $x \in K$, cioè se e soltanto se I e J sono ideali frazionari isomorfi (Proposizione 1.4). Dunque $C(A)$ è il gruppo delle classi di isomorfismo degli ideali frazionari di A.

Notiamo che in ogni classe di $C(A)$ c'è almeno un ideale intero di A. Infatti, se $I \in \mathrm{Inv}(A) \subseteq \mathcal{F}(A)$ e $dI \subseteq A$ con $d \in A$ non nullo, allora I e dI appartengono alla stessa classe di $C(A)$.

Il gruppo delle classi $C(A)$ è banale, cioè ha un solo elemento, se e soltanto se ogni ideale invertibile I è isomorfo ad A, cioè è principale. In questo caso, si scrive $C(A) = 0$.

Teorema 4.13 *Sia A un dominio di Dedekind. Allora*

(1) *$C(A) = \mathcal{F}(A)/P(A)$ ed è generato dalle classi degli ideali primi non nulli.*

(2) *Le seguenti condizioni sono equivalenti:*

(i) *A è un dominio a ideali principali;*

(ii) *A è un dominio a fattorizzazione unica;*

(iii) *Ogni ideale primo di A è principale;*

(iv) $C(A) = 0$.

Dimostrazione: (1) segue dal Teorema 4.9, (i) $\Leftrightarrow$ (iv).
(2) (i) $\Leftrightarrow$ (ii) per il Teorema 3.31. (i) $\Leftrightarrow$ (iii) $\Leftrightarrow$ (iv) segue da (1). $\square$

Osservazione 4.14 L. Claborn ha dimostrato che per ogni gruppo abeliano G esiste un dominio di Dedekind il cui gruppo delle classi è isomorfo a G [2, Section 14].

5 Anelli di Interi Algebrici

Una classe importante di domini di Dedekind è data dai domini di interi algebrici. In questo paragrafo introdurremo questa classe di domini e ne daremo alcune prime proprietà; per approfondimenti si rimanda a [7]. Useremo alcune nozioni elementari di Teoria dei Campi, per le quali si può vedere ad esempio [3].

Un numero complesso $\alpha \in \mathbb{C}$ si chiama un *numero algebrico* se esiste un polinomio monico $f(X) \in \mathbb{Q}[X]$ tale che $f(\alpha) = 0$. Se $\alpha \in \mathbb{C}$ è algebrico, il polinomio monico $m_\alpha(X) \in \mathbb{Q}[X]$ di grado minimo annullato da α si chiama il *polinomio minimo* di α. Indicando con $\mathbb{Q}(\alpha)$ l'ampliamento semplice di $\mathbb{Q}$ generato da α, si ha che α è algebrico su $\mathbb{Q}$ se e soltanto se $[\mathbb{Q}(\alpha) : \mathbb{Q}] := \dim_{\mathbb{Q}} \mathbb{Q}(\alpha) = n$ è finito; in questo caso risulta $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg m_\alpha(X)$ ed una base di $\mathbb{Q}(\alpha)$ su $\mathbb{Q}$ è $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ [3, Paragrafo 3.4].

Un *campo numerico* è un ampliamento finito di $\mathbb{Q}$, cioè un campo $K \subseteq \mathbb{C}$ tale che $[K : \mathbb{Q}] := \dim_{\mathbb{Q}} K$ sia finito. Il *Teorema dell'Elemento Primitivo* ci assicura che un campo numerico è un ampliamento semplice di $\mathbb{Q}$ [3, Teorema 5.3.13]. L'insieme $\mathcal{A}$ di tutti i numeri algebrici è un sottocampo di $\mathbb{C}$ ed è l'unione di tutti i campi numerici; tuttavia non è un ampliamento finito di $\mathbb{Q}$ [3, Paragrafo 3.6.1].

Un numero complesso α si chiama un *intero algebrico* se è intero su $\mathbb{Z}$, cioè se esiste un polinomio monico $f(X) \in \mathbb{Z}[X]$ tale che $f(\alpha) = 0$. Per quanto visto nel Paragrafo 3.2, gli interi algebrici costituiscono esattamente la chiusura integrale di $\mathbb{Z}$ in $\mathbb{C}$. Denotiamo con $\mathcal{O}$ l'anello di tutti gli interi algebrici; chiaramente $\mathcal{O}$ è contenuto nel campo $\mathcal{A}$ di tutti i numeri algebrici. Se K è un campo numerico, gli interi algebrici appartenenti a K costituiscono la chiusura integrale di $\mathbb{Z}$ in K. Un anello che si ottiene in questo modo si chiama un *anello di interi algebrici* e si denota con $\mathcal{O}_K$. Notiamo che $\mathcal{O}_K = \mathcal{O} \cap K$ e che $\mathcal{O}$ è l'unione di tutti gli anelli di interi algebrici .

Proposizione 5.1 *Sia $\alpha \in \mathbb{C}$ algebrico su $\mathbb{Q}$ con polinomio minimo $m_\alpha(X)$. Allora:*

(1) $\alpha \in \mathcal{O}$ *se e soltanto se* $m_\alpha(X) \in \mathbb{Z}[X]$.

(2) $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$.

(3) *Esiste* $n > 0$ *tale che* $n\alpha \in \mathcal{O}$.

Dimostrazione: (1) Sia $\alpha \in \mathbb{C}$ con polinomio minimo $m(X) := m_\alpha(X)$ su $\mathbb{Q}$. Se $\alpha \in \mathcal{O}$, esiste un polinomio monico $f(X) \in \mathbb{Z}[X]$ tale che $f(\alpha) = 0$; quindi $m(X)$ divide $f(X)$ in $\mathbb{Q}[X]$. Scriviamo $f(X) = m(X)g(X)$, $g(X) \in \mathbb{Q}[X]$. Moltiplicando per un denominatore comune d di $m(X)g(X)$, otteniamo $df(X) = m_1(X)g_1(X)$, con $m_1(X), g_1(X) \in \mathbb{Z}[X]$. Poiché $f(X)$ è monico e quindi primitivo, per il Lemma di Gauss, deve essere $d = c(df) = c(m_1)c(g_1)$ (dove $c(h)$ denota il *contenuto* del polinomio $h(X) \in \mathbb{Z}[X]$, cioè il massimo comune divisore dei coefficienti di $h(X)$). Per il teorema di fattorizzazione unica in $\mathbb{Z}$, possiamo scrivere $d = ab$ con $a, b \in \mathbb{Z}$, tali che a divide $c(m_1)$ e b divide $c(g_1)$. Dunque $f(X) = \frac{1}{d}m_1(X)g_1(X) = \frac{1}{a}m_1(X)\frac{1}{b}g_1(X)$ con $m_2(X) := \frac{1}{a}m_1(X)$, $g_2(X) := \frac{1}{b}g_1(X) \in \mathbb{Z}[X]$ associati rispettivamente a $m(X)$ e $g(X)$ su $\mathbb{Q}$. Scrivendo $m_2(X) = \lambda m(X)$, $\lambda \in \mathbb{Q}$, otteniamo che $f(X) = \lambda m(X)g_2(X)$. Poiché $f(X)$ e $m(X)$ sono monici, uguagliando i coefficienti direttori vediamo che deve essere $\lambda = 1$, cioè $m(X) = m_2(X) \in \mathbb{Z}[X]$.

Viceversa, se $m(X) \in \mathbb{Z}[X]$, allora α è intero su $\mathbb{Z}$ e quindi $\alpha \in \mathcal{O}$.

(2) $\alpha \in \mathcal{O} \cap \mathbb{Q}$ se e soltanto se, per il punto (1), il suo polinomio minimo è $X - a$, con $a \in \mathbb{Z}$, ovvero $\alpha = a \in Z$.

(3) Sia $\alpha \in \mathbb{C}$ tale che $\alpha^r + c_{r-1}\alpha^{r-1} + \cdots + c_0 = 0$ con $c_i \in \mathbb{Q}$, $i = 0, \ldots, r$. Se $n \geq 1$ è un comune denominatore dei coefficienti c_i, moltiplicando per n^r otteniamo $(n\alpha)^r + c_{r-1}n(n\alpha)^{r-1} + \cdots + c_0 n^r = 0$. Poiché $nc_i \in \mathbb{Z}$ per ogni i, $n\alpha$ è intero su $\mathbb{Z}$ e perciò appartiene a $\mathcal{O}$. □

Se α è algebrico su $\mathbb{Q}$, il grado del suo polinomio minimo si chiama anche il *grado di* α. Due numeri algebrici si dicono *coniugati su* $\mathbb{Q}$ se essi hanno lo stesso polinomio minimo su $\mathbb{Q}$. Quindi il numero dei coniugati distinti di un numero algebrico è uguale al suo grado.

Sia ora K un campo di numeri, $\alpha \in K$ e $\sigma : K \longrightarrow \mathbb{C}$ un'immersione di campi. Se $f(\alpha) = 0$, allora $\sigma(f(\alpha)) = f(\sigma(\alpha)) = 0$. Dunque $\sigma(\alpha)$ è coniugato ad α. Se poi $K = \mathbb{Q}(\theta)$ e θ' è coniugato a θ, si verifica subito che l'applicazione

$$\sigma : K \longrightarrow \mathbb{C}\,; \quad f(\theta) \mapsto f(\theta')$$

è un'immersione di campi. Dunque le immersioni di K in $\mathbb{C}$ sono esattamente $n := [K : \mathbb{Q}] = \deg m_\theta(X)$ e sono determinate dai coniugati di θ su $\mathbb{Q}$ [3, Paragrafo 4.2].

Se le immersioni di K in $\mathbb{C}$ sono $\sigma_1, \ldots, \sigma_n$ e $\alpha \in K$, poniamo

$$T_K(\alpha) := \sigma_1(\alpha) + \cdots + \sigma_n(\alpha)\,; \quad N_K(\alpha) := \sigma_1(\alpha) \ldots \sigma_n(\alpha).$$

$T_K(\alpha)$ e $N_K(\alpha)$ si chiamano rispettivamente la *traccia* e la *norma* di α in K [3, Paragrafo 5.3.6]. È evidente che questi valori dipendono dalla scelta del campo K; quando K è fissato e non ci sono ambiguità, porremo semplicemente $T(\alpha) := T_K(\alpha)$ e $N(\alpha) := N_K(\alpha)$.

Poiché i σ_i sono omomorfismi di campi, risulta

$$N(\alpha\beta) = N(\alpha)N(\beta)\,; \quad T(x\alpha + y\beta) = xT(\alpha) + yT(\beta),$$

per ogni $\alpha, \beta \in K$ e $x, y \in \mathbb{Q}$.

Il polinomio

$$f_\alpha(X) := (X - \sigma_1(\alpha)) \dots (X - \sigma_n(\alpha)) = X^n - T(\alpha)X^{n-1} + \dots + (-1)^n N(\alpha)$$

si chiama il *polinomio di α rispetto a K*.

Notiamo che se α ha grado d su $\mathbb{Q}$, con polinomio minimo $m_\alpha(X)$, allora d divide n e $f_\alpha(X) = m_\alpha(X)^{\frac{n}{d}}$. Infatti α ha d coniugati distinti $\alpha_1 := \sigma_1(\alpha) = \alpha, \dots, \alpha_d := \sigma_d(\alpha)$, ognuno ripetuto n/d volte tra i $\sigma_i(\alpha)$.

Il *discriminante* di α si definisce come $\Delta(\alpha) := \prod_{1 \le i < j \le d} (\alpha_i - \alpha_j)^2$ (dove d è il grado di α) ed è un elemento (non nullo) di $\mathbb{Q}$, perché è una funzione simmetrica delle radici del polinomio minimo di α su $\mathbb{Q}$.

La matrice

$$V(\alpha) := (\alpha_i^j)_{\substack{1 \le i \le d \\ 0 \le j \le d-1}} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_d \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_d^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{d-1} & \alpha_2^{d-1} & \cdots & \alpha_d^{d-1} \end{pmatrix}.$$

si chiama la *matrice di Vandermonde* di $\alpha_1 := \alpha, \dots, \alpha_d$. Un semplice calcolo mostra che $\det V(\alpha) = \prod_{1 \le i < j \le d} (\alpha_i - \alpha_j)$, dunque $\Delta(\alpha) = (\det V(\alpha))^2$.

Proposizione 5.2 *Sia K un campo numerico. Allora:*

(1) *$K = \mathbb{Q}(\theta)$ con $\theta \in \mathcal{O}_K$;*

(2) *Se $\alpha \in \mathcal{O}_K$, i coniugati di α sono interi algebrici;*

(3) *Se $\alpha \in \mathcal{O}_K$, $N(\alpha)$, $T(\alpha) \in \mathbb{Z}$;*

(4) *Se $\alpha \in \mathcal{O}_K$, $\Delta(\alpha) \in \mathbb{Z}$.*

Dimostrazione: (1) Per il Teorema dell'Elemento Primitivo, sappiamo che $K = \mathbb{Q}(\alpha)$ è un ampliamento semplice di $\mathbb{Q}$. Per la Proposizione 5.1(2), $\theta := n\alpha \in \mathcal{O}_K$ per qualche $n \ge 1$ e allora $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$.

(2) Se $\alpha \in \mathcal{O}_K$ e $m(X) := m_\alpha(X)$ è il polinomio minimo di α su $\mathbb{Q}$, $m(X)$ ha coefficienti interi. Poiché i coniugati di α sono le radici di $m(X)$, essi sono interi su $\mathbb{Z}$ (Proposizione 5.1(1)).

(3) Se $\alpha \in \mathcal{O}_K$ ha grado d su $\mathbb{Q}$ con polinomio minimo $m(X) := m_\alpha(X)$, allora $m(X) \in \mathbb{Z}[X]$ e $f_\alpha(X) = m(X)^d \in \mathbb{Z}[X]$. Poiché $N(\alpha)$ e $T(\alpha)$ sono coefficienti di $f_\alpha(X)$, allora $N(\alpha)$, $T(\alpha) \in \mathbb{Z}$.

(4) Se $\alpha \in \mathcal{O}_K$ e $m(X) := m_\alpha(X)$ è il polinomio minimo di α su $\mathbb{Q}$, $m(X) \in \mathbb{Z}[X]$ e $\Delta(\alpha)$ è una funzione simmetrica delle radici di $m(X)$, ovvero è una funzione algebrica dei coefficienti di $m(X)$. Dunque $\Delta(\alpha) \in \mathbb{Z}$. □

Corollario 5.3 *Sia $\alpha \in \mathcal{O}_K$. Allora*

(1) *$N(\alpha) = 0$ se e soltanto se $\alpha = 0$;*

(2) *$|N(\alpha)| = 1$ se e soltanto se α è invertibile in $\mathcal{O}_K$;*

(3) *$|N(\alpha)| = p$ è un numero primo, allora α è irriducibile.*

Dimostrazione: (1) segue dalla definizione.

(2) Poiché la norma è moltiplicativa, se $\alpha\beta = 1$, allora $N(\alpha)N(\beta) = N(1) = 1$, da cui $N(\alpha) = \pm 1$. Viceversa, ricordando che $N(\alpha) \in \mathbb{Z}$ è il prodotto dei coniugati di α, indicando con β il prodotto dei coniugati di α diversi da α, risulta $N(\alpha) = \alpha\beta = \pm 1$. Dunque $\beta = \alpha^{-1} \in K$ ed inoltre $\beta \in \mathcal{O}_K$ (Proposizione 5.2(2)). Ne segue che α è invertibile in $\mathcal{O}_K$.

(3) Se $\alpha = \beta\gamma$, allora $N(\alpha) = N(\beta)N(\gamma) = p$. Quindi o $N(\beta) = \pm 1$ e β è invertibile, oppure $N(\gamma) = \pm 1$ e γ è invertibile. □

Vogliamo dimostrare ora che gli anelli di interi algebrici sono domini di Dedekind.

Proposizione 5.4 *Sia K un campo numerico. Allora K (risp. $\mathcal{A}$) è il campo dei quozienti di $\mathcal{O}_K$ (risp. di $\mathcal{O}$). Quindi i domini $\mathcal{O}_K$ e $\mathcal{O}$ sono domini integralmente chiusi.*

Dimostrazione: Se $x \in K$, esiste $n \geq 1$ tale che $nx \in \mathcal{O}_K$ (Proposizione 5.1(1)). Dunque $x = nx/n$ appartiene al campo dei quozienti di $\mathcal{O}_K$. Dal momento che il campo $\mathcal{A}$ è l'unione di tutti i campi numerici, $\mathcal{A}$ è il campo dei quozienti di $\mathcal{O}$.

Poiché poi $\mathcal{O}_K$ è la chiusura integrale di $\mathbb{Z}$ in K, $\mathcal{O}_K$ è un dominio integralmente chiuso (Corollario 3.18). Analogamente, $\mathcal{O}$ è la chiusura integrale di $\mathbb{Z}$ in $\mathbb{C}$. Perciò esso è integralmente chiuso in $\mathbb{C}$ e quindi anche in $\mathcal{A}$. □

Teorema 5.5 *Sia K un campo numerico di grado n su $\mathbb{Q}$. Allora:*

(1) *Esistono $x_1, \ldots, x_n \in K$ tali che $\mathcal{O}_K \subseteq x_1\mathbb{Z} + \cdots + x_n\mathbb{Z}$.*

(2) *$\mathcal{O}_K$ è un dominio di Dedekind.*

Dimostrazione: (1) Per la Proposizione 5.2, risulta $K = \mathbb{Q}(\theta)$ con $\theta \in \mathcal{O}_K$ e $\Delta := \Delta(\theta) \in \mathbb{Z}$. Una base di K su $\mathbb{Q}$ è $\{1, \theta, \ldots, \theta^{n-1}\}$. Dunque, per ogni $y \in \mathcal{O}_K$, si ha $y = \sum_{i=1}^{n} a_i \theta^i$, $a_i \in \mathbb{Q}$. Chiaramente $x_i := \frac{\theta^i}{\Delta} \in K$ e $y = \sum_{i=1}^{n} (a_i \Delta) x_i$, con $a_i \Delta \in \mathbb{Q}$. Allora ci basta far vedere che $a_i \Delta \in \mathbb{Z}$ per ogni $i = 1, \ldots, n$.

Siano $\theta_1 := \theta, \theta_2, \ldots, \theta_n \in \mathcal{O}_K$ i coniugati di θ su $\mathbb{Q}$ (Proposizione 5.2) e consideriamo gli elementi $y_j := \sum a_i \theta_j^i$, per $j = 1, \ldots, n$. Osserviamo che poiché gli elementi θ_j sono tutti coniugati tra loro, anche gli elementi y_j lo sono. Allora essi sono tutti interi su $\mathbb{Z}$, perché lo è $y_1 = y$.

Vediamo le relazioni $y_j := \sum a_i \theta_j^i$ come un sistema lineare su $\mathcal{O}_K$ in $a_1, \ldots, a_n$. La matrice di questo sistema è la matrice di Vandermonde di $\theta_1, \theta_2, \ldots, \theta_n$, il cui determinante è $d := \prod_{k>j} (\theta_k - \theta_j)$. Inoltre, per la regola di Cramer, $a_i d$ è il determinante della matrice ottenuta dalla matrice di Vandermonde sostituendo la i-sima colonna con la colonna $y_1, \ldots, y_n$. Allora, poiché gli elementi θ_i e y_i sono interi su $\mathbb{Z}$, anche $a_i d$ e d lo sono. Infine, essendo $d^2 = \Delta$, otteniamo che $a_i \Delta = a_i d \cdot d \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$.

(2) Per il punto (1), $\mathcal{O}_K$ è uno $\mathbb{Z}$-sottomodulo di uno $\mathbb{Z}$-modulo finitamente generato $B := x_1\mathbb{Z} + \cdots + x_n\mathbb{Z}$. Poiché B è noetheriano (Corollario 3.7(1)), $\mathcal{O}_K$ è uno $\mathbb{Z}$-modulo finitamente generato e quindi anche una $\mathbb{Z}$-algebra finitamente generata; dunque è un dominio noetheriano (Corollario 3.7(2)). Inoltre $\mathcal{O}_K$ è integralmente chiuso in K (Corollario 3.18) ed essendo intero su $\mathbb{Z}$ ha dimensione uno (Proposizione 3.22). In conclusione $\mathcal{O}_K$ è un dominio di Dedekind. □

Osservazione 5.6 Più generalmente, si può dimostrare che, se A è un dominio di Dedekind con campo dei quozienti K e F è un ampliamento finito di K, allora la chiusura integrale di A in F è ancora un dominio di Dedekind. Se poi F è separabile su K, allora tale chiusura integrale è anche una A-algebra finitamente generata [5, Section 41].

Poiché come appena visto gli anelli di interi algebrici sono domini di Dedekind, in questo caso il problema della fattorizzazione si riduce a classificare quali di questi anelli sono euclidei o a ideali principali (Corollario 3.32). Il teorema seguente dà un criterio teorico generale.

Teorema 5.7 (1) *L'anello $\mathcal{O}_K$ è a ideali principali se e soltanto se, comunque scelti $\alpha, \beta \in \mathcal{O}_K$ non nulli, con $\beta \nmid \alpha$, esistono $\gamma, \delta \in \mathcal{O}_K$ tale che*

$$0 < |N(\alpha\gamma - \beta\delta)| < |N(\beta)|.$$

(2) *L'anello $\mathcal{O}_K$ è euclideo rispetto al modulo della norma se e soltanto se, comunque scelti $\alpha, \beta \in \mathcal{O}_K$ non nulli, con $\beta \nmid \alpha$ e $|N(\alpha)| \geq |N(\beta)|$, esiste $\delta \in \mathcal{O}_K$ tale che*

$$0 < |N(\alpha - \beta\delta)| < |N(\beta)|.$$

Dimostrazione: (1) Supponiamo che $\mathcal{O}_K$ sia a ideali principali e siano α, $\beta \in \mathcal{O}_K$ tali che $\beta \nmid \alpha$. Se $I := \langle \alpha, \beta \rangle = \langle \omega \rangle$, possiamo scrivere $\alpha = \tau\omega$, $\beta = \sigma\omega$ con σ non invertibile (perché $\beta \nmid \alpha$). Allora $N(\beta) = N(\sigma)N(\omega)$ con $|N(\sigma)| > 1$ e dunque $0 < |N(\omega))| < |N(\beta)|$. Ma essendo $\omega \in I$, si ha $\omega = \alpha\gamma - \beta\delta$ per opportuni γ, $\delta \in \mathcal{O}_K$.

Viceversa, sia $I \subseteq \mathcal{O}_K$ un ideale non nullo e sia $\omega \in I$ con $|N(\omega)|$ minimale. Se $\alpha \in I$ è non nullo e $\omega \nmid \alpha$, esistono γ, $\delta \in \mathcal{O}_K$ tale che $0 < |N(\alpha\gamma - \omega\delta)| < |N(\omega)|$. Ma poiché $\alpha\gamma - \omega\delta \in I$, questo è impossibile per la minimalità di $|N(\omega)|$. Perciò ω divide α e $I = \langle \omega \rangle$.

(2) Se $\mathcal{O}_K$ è euclideo rispetto al modulo della norma e $\beta \nmid \alpha$, per l'algoritmo della divisione $\alpha = \beta\delta + \rho$ con $\rho = \alpha - \beta\delta \neq 0$ e $0 < |N(\rho)| < |N(\beta)|$.

Viceversa, mostriamo che, sotto le ipotesi date, il modulo della norma è una funzione euclidea su $\mathcal{O}_K \setminus \{0\}$. Poiché la norma è moltiplicativa, per questo basta far vedere che, dati α, $\beta \in \mathcal{O}_K$ non nulli, si può effettuare la divisione euclidea di α per β.

Se β divide α, il quoziente è α/β e il resto è zero. Se $|N(\alpha)| < |N(\beta)|$, il quoziente è zero e il resto è α. Se infine α e β soddisfano le ipotesi, δ è il quoziente e $\alpha - \beta\delta$ è il resto della divisione. □

Osservazione 5.8 Se $\mathcal{O}_K$ è euclideo rispetto al modulo della norma, per effettuare la divisione di α per β si può procedere nel modo seguente. Posto $\eta := \alpha/\beta$, se $\eta \notin \mathcal{O}_K$, si cerca $\delta \in \mathcal{O}_K$ tale che $|N(\eta - \delta)| < 1$ (δ esiste per il Teorema 5.7(2)). Allora $\eta = \delta + (\eta - \delta)$ e, moltiplicando per β, si ottiene $\alpha = \delta\beta + (\eta - \delta)\beta$. Inoltre $\rho := (\eta - \delta)\beta = \alpha - \delta\beta \in \mathcal{O}_K$ e $|N(\rho)| = |N(\eta - \delta)||N(\beta)| < |N(\beta)|$.

Un risultato fondamentale della Teoria dei Numeri ci assicura che il gruppo delle classi di ideali di un anello di interi algebrici è un gruppo finito [7, Chapter 9]. La cardinalità di $C(\mathcal{O}_K)$ si chiama il *numero delle classi* di $\mathcal{O}_K$. Quindi $\mathcal{O}_K$ è a ideali principali se e soltanto se il suo numero delle classi è uguale a uno (Teorema 4.13).

Nel prossimo paragrafo studieremo il caso particolare degli anelli di interi quadratici.

5.1 Anelli di interi quadratici

Se K è un campo numerico tale che $[K : \mathbb{Q}] = 2$, risulta $K = \mathbb{Q}(\sqrt{d})$ per qualche intero $d \neq 0, 1$ privo di fattori quadratici. In questo caso, l'anello degli interi $\mathcal{O}_K$ si chiama un *anello di interi quadratici*.

Se $\alpha := x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, $x, y \in \mathbb{Q}$, gli unici elementi coniugati ad α su $\mathbb{Q}$ sono α e $\overline{\alpha} := x - y\sqrt{d}$ e risulta

$$T(\alpha) := \alpha + \overline{\alpha} = 2x\,, \quad N(\alpha) := \alpha\overline{\alpha} = x^2 - y^2 d.$$

Il polinomio minimo di α su $\mathbb{Q}$ è

$$m_\alpha(X) = (X-\alpha)(X-\overline{\alpha}) = X^2 - T(\alpha)X + N(\alpha);$$

dunque $\alpha \in \mathcal{O}_K$ se e soltanto se $T(\alpha)$, $N(\alpha) \in \mathbb{Z}$ (Proposizione 5.1(1)).

Notiamo che, quando $d < 0$, la norma di un numero $\alpha \in \mathbb{Q}(\sqrt{d})$ coincide con la norma complessa.

Proposizione 5.9 *Sia $K := \mathbb{Q}(\sqrt{d})$, con $d \in \mathbb{Z}$ privo di fattori quadratici. Allora*

$$\mathcal{O}_K = \mathbb{Z}[\omega_d]$$

dove

$$\omega_d = \sqrt{d} \text{ se } d \not\equiv 1 \mod 4\,; \quad \omega_d = \frac{1+\sqrt{d}}{2} \text{ se } d \equiv 1 \mod 4.$$

Dimostrazione: In ogni caso, $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$. Se $\alpha \in \mathbb{Q}(\sqrt{d})$, possiamo scrivere $\alpha = \frac{a+b\sqrt{d}}{c}$ con $\mathrm{MCD}\{a,b,c\} = 1$. Ora $\alpha \in \mathcal{O}_K$ se e soltanto se

$$T(\alpha) = \frac{2a}{c} \in \mathbb{Z}\,, \quad N(\alpha) = \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z}.$$

Sia $\alpha \in \mathcal{O}_K$ e sia $p \in \mathbb{Z}$ un primo che divide c. Se p divide a, guardando alla norma, p^2 divide $b^2 d$ e, poiché d è privo di fattori quadratici, p divide b. Questo contraddice $\mathrm{MCD}\{a,b,c\} = 1$. Quindi $\mathrm{MCD}(a,c) = 1$ e $c = 1, 2$.

Se $c = 1$, $\alpha \in \mathbb{Z}[\sqrt{d}]$. Se $c = 2$, a deve essere dispari (perché $\mathrm{MCD}(a,c) = 1$) e allora anche b deve essere dispari (perché $N(\alpha) \in \mathbb{Z}$, e quindi se b è pari lo sarebbe anche a). Mostriamo che $\alpha := \frac{a+b\sqrt{d}}{2}$, con a e b dispari è un intero se e soltanto se $d \equiv 1 \mod 4$.

Ora a e b sono entrambi dispari se e soltanto se $a^2 \equiv 1 \equiv b^2 \mod 4$. Allora $N(\alpha) = \frac{a^2 - b^2 d}{4} \in \mathbb{Z}$ se e soltanto se $a^2 - b^2 d \equiv 1 - d \equiv 0 \mod 4$, ovvero $d \equiv 1 \mod 4$.

In conclusione, se $d \not\equiv 1 \mod 4$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ e, se $d \equiv 1 \mod 4$, $O_K = \{\frac{a+b\sqrt{d}}{2}\,;\ a, b \text{ con la stessa parità}\}$.

Finalmente, se $d \equiv 1 \mod 4$, posto $\omega_d := \frac{1+\sqrt{d}}{2}$, risulta $\mathcal{O}_K = \mathbb{Z}[\omega_d]$. Infatti $\omega_d \in \mathcal{O}_K$. Viceversa, $\sqrt{d} = 2\omega_d - 1$ e dunque

$$\frac{a+b\sqrt{d}}{2} = \frac{a+b(2\omega_d - 1)}{2} = \frac{a-b}{2} + b\omega_d.$$

Poiché a e b hanno la stessa parità, $\frac{a-b}{2} \in \mathbb{Z}$ e quindi $\mathcal{O}_K \subseteq \mathbb{Z}[\omega_d]$. □

Esempio 5.10 Per $d = -1$, l'anello degli interi di $\mathbb{Q}(i)$ è l'*anello degli interi di Gauss* $\mathbb{Z}[i]$.

Osserviamo che $\mathbb{Z}[\omega_d]$ è uno $\mathbb{Z}$-modulo libero di rango 2, con base $\{1, \omega_d\}$. Infatti 1 e ω_d sono linearmente indipendenti su $\mathbb{Q}$ e quindi anche su $\mathbb{Z}$.

Proposizione 5.11 *Se $G \subseteq \mathbb{Z}[\omega_d]$ è un sottogruppo additivo, risulta $G = n\mathbb{Z} + (a + m\omega_d)\mathbb{Z}$, dove $n, m \geq 0$ sono tali che $n\mathbb{Z} = G \cap \mathbb{Z}$, $m\mathbb{Z} = \{y \in \mathbb{Z}\,;\ x + y\omega_d \in G\}$ e $a \in \mathbb{Z}$.*

In particolare, ogni ideale non nullo $I \subseteq \mathbb{Z}[\omega_d]$ è uno $\mathbb{Z}$-modulo libero di rango 2. Infatti $I = n\mathbb{Z} \oplus (a + m\omega_d)\mathbb{Z}$ con $a \in \mathbb{Z}$ e con n, $m > 0$.

Dimostrazione: Poiché $G \cap \mathbb{Z}$ è un sottogruppo di $\mathbb{Z}$, esso è generato da un intero $n \geq 0$. Sia poi $H := \{y \in \mathbb{Z}\,;\ x + y\omega_d \in G\}$. Si vede subito che H è un sottogruppo di $\mathbb{Z}$ e quindi $H = m\mathbb{Z}$, $m \geq 0$. Poiché $m \in H$, esiste $a \in \mathbb{Z}$ tale che $a + m\omega_d \in G$. Chiaramente $n\mathbb{Z} + (a + m\omega_d)\mathbb{Z} \subseteq G$. Per l'inclusione inversa, sia $x + y\omega_d \in G$. Allora $y = mz$, $z \in \mathbb{Z}$, e $(x + y\omega_d) - z(a + m\omega_d) = x - za \in G \cap \mathbb{Z}$. Dunque $x - za = wn$, $w \in \mathbb{Z}$, e si ha $x + y\omega_d = wn + z(a + m\omega_d) \in n\mathbb{Z} + (a + m\omega_d)\mathbb{Z}$.

Sia poi $I \subseteq \mathbb{Z}[\omega_d]$ un ideale non nullo. Poiché I è un sottogruppo additivo di $\mathbb{Z}[\omega_d]$, possiamo scrivere come sopra $I = n\mathbb{Z} + (a + m\omega_d)\mathbb{Z}$. Se $0 \neq \alpha \in I$, allora $0 \neq \alpha\overline{\alpha} = N(\alpha) \in I \cap \mathbb{Z} = n\mathbb{Z}$. Dunque $n > 0$. Inoltre $N(\alpha)\omega_d \in I$ e quindi $N(\alpha) \in H = m\mathbb{Z}$. Dunque $m > 0$. Ne segue che n e $a + m\omega_d$ sono linearmente indipendenti su $\mathbb{Q}$ e quindi anche su $\mathbb{Z}$. □

Osservazione 5.12 Dati due interi m, $n > 0$ e $a \in \mathbb{Z}$, un semplice calcolo mostra che $1, \omega_d \in G := n\mathbb{Z} + (a + m\omega_d)\mathbb{Z}$ (ovvero $G = \mathbb{Z}[\omega_d]$) se e soltanto se $n = m = 1$. Invece può accadere che l'ideale $\langle n, a + m\omega_d\rangle$ sia tutto il dominio $\mathbb{Z}[\omega_d]$ per $(n, m) \neq (1, 1)$.

Ad esempio, per $d = 3$, $G := 7\mathbb{Z} + (5 + 2\sqrt{3})\mathbb{Z} \neq \mathbb{Z}[\sqrt{3}]$, ma $\langle 7, 5 + 2\sqrt{3}\rangle = \mathbb{Z}[\sqrt{3}]$. Infatti $N(5 + 2\sqrt{3}) = 25 - 12 = 13 \in I$ e dunque $1 = 2 \cdot 7 - 13 \in I$.

Per la Proposizione 5.11, ogni ideale di $\mathbb{Z}[\omega_d]$ è generato al più da 2 elementi. Se $I := \langle \alpha, \beta\rangle \subseteq \mathbb{Z}[\omega_d]$ è un ideale non nullo, poniamo $\overline{I} := \langle \overline{\alpha}, \overline{\beta}\rangle = \{\overline{\gamma}\,;\ \gamma \in I\}$ e consideriamo l'ideale $I\overline{I} = \langle \alpha\overline{\alpha}, \alpha\overline{\beta}, \overline{\alpha}\beta, \beta\overline{\beta}\rangle$. Notiamo che $\alpha\overline{\alpha} = N(\alpha)$, $\alpha\overline{\beta} + \overline{\alpha}\beta = T(\alpha\overline{\beta})$, $\beta\overline{\beta} = N(\beta)$ sono numeri interi appartenenti ad I (non tutti nulli) e indichiamo con $N := \mathrm{MCD}(N(\alpha), T(\alpha\overline{\beta}), N(\beta))$ il massimo comune divisore positivo di questi interi.

Proposizione 5.13 *Con le notazioni precedenti, se $I \subseteq \mathbb{Z}[\omega_d]$ è un ideale non nullo, si ha $I\overline{I} = N\mathbb{Z}[\omega_d]$.*

Dimostrazione: Poiché $N \in I\overline{I}$ (per l'identità di Bezout), allora $N\mathbb{Z}[\omega_d] \subseteq I\overline{I}$. Per l'inclusione opposta, mostriamo che N divide i generatori di $I\overline{I}$. Per definizione, N divide $N(\alpha), T(\alpha\overline{\beta}), N(\beta)$. Verifichiamo che N divide $\alpha\overline{\beta}$ e il suo coniugato $\overline{\alpha}\beta$ in $\mathbb{Z}[\omega_d]$ (Lemma di Hurwitz). Per questo basta far vedere che $\alpha\overline{\beta}/N \in \mathbb{Z}[\omega_d]$, ovvero che $N(\alpha\overline{\beta}/N), T(\alpha\overline{\beta}/N) \in \mathbb{Z}$. Questo è vero,

perché $T(\alpha\overline{\beta}/N) = T(\alpha\overline{\beta})/N \in \mathbb{Z}$ ed inoltre $N(\alpha\overline{\beta}/N) = (\alpha\overline{\beta})(\overline{\alpha}\beta)/N^2 = (N(\alpha)/N)(N(\beta)/N) \in \mathbb{Z}$. □

Se $I \subseteq \mathbb{Z}[\omega_d]$ è un ideale non nullo, il numero positivo N tale che $I\overline{I} = N\mathbb{Z}[\omega_d]$ si chiama la *norma di* I e si indica con $N(I)$. Notiamo che $N(I) = N(\overline{I})$, infatti $\overline{\overline{I}} = I$.

Proposizione 5.14 *Sia $I \subseteq \mathbb{Z}[\omega_d]$ un ideale non nullo con norma $N(I)$. Allora:*

(1) $N(I) \in I$.

(2) *Se $\gamma \in I$, allora $N(I)$ divide $N(\gamma)$.*

(3) *Se $I = \langle\alpha\rangle$, allora $N(I) = |N(\alpha)|$.*

(4) $N(I) = 1$ *se e soltanto se* $I = \mathbb{Z}[\omega_d]$.

(5) $N(IJ) = N(I)N(J)$.

(6) *Se $J \subseteq I$, allora $N(I)$ divide $N(J)$.*

Dimostrazione: (1) $I\overline{I} = N(I)\mathbb{Z}[\omega_d] \subseteq I$.

(2) Poiché $\overline{\gamma} \in \overline{I}$, allora $N(\gamma) = \gamma\overline{\gamma} \in I\overline{I} = N(I)\mathbb{Z}[\omega_d]$.

(3) Se $I = \langle\alpha\rangle$, allora $\overline{I} = \langle\overline{\alpha}\rangle$ e $N(I)\mathbb{Z}[\omega_d] = I\overline{I} = \langle\alpha\overline{\alpha}\rangle = N(\alpha)\mathbb{Z}[\omega_d]$. Dunque $N(I) = N(\alpha)u$, con $u \in \mathbb{Z}[\omega_d]$ invertibile. Ma allora $u \in \mathbb{Q}\cap\mathbb{Z}[\omega_d] = \mathbb{Z}$ e $N(I) = \pm N(\alpha)$.

(4) Se $N(I) = 1$, allora $1 \in I$ per (1). Viceversa, se $1 \in I$, allora $N(I)$ divide $N(1) = 1$ per (3) e quindi $N(I) = 1$.

(5) Si verifica subito che $\overline{IJ} = \overline{I}\,\overline{J}$. Quindi $N(IJ) = IJ\overline{IJ} = IJ\overline{I}\,\overline{J} = N(I)N(J)$.

(6) Poiché I e J sono invertibili, se $J \subseteq I$ allora I divide J (Proposizione 4.7) e quindi $N(I)$ divide $N(J)$ per (5). □

Osservazione 5.15 Se $I \subseteq \mathbb{Z}[\omega_d]$ è un ideale non nullo e, con le notazioni della Proposizione 5.11, risulta $I = n\mathbb{Z} \oplus (a + m\omega_d)\mathbb{Z} = \langle n, a + m\omega_d\rangle$, allora $N(I) = mn$ e $N(I)$ è uguale all'indice di I in $\mathbb{Z}[\omega_d]$.

Infatti, $\overline{I} = \langle n, a + m\overline{\omega}_d\rangle$ e quindi i generatori di $I\overline{I}$ sono:

- $n^2 \in \mathbb{Z}$,
- $(a + m\omega_d)(a + m\overline{\omega}_d) = a^2 + amT(\omega_d) + m^2N(\omega_d) \in \mathbb{Z}$,
- $n(a + m\omega_d) = na + nm\omega_d \in \mathbb{Z} + mn\omega_d\mathbb{Z}$

ed infine, notando che $\overline{\omega}_d = T(\omega_d) - \omega_d$,

- $n(a + m\overline{\omega}_d) = na + nm\overline{\omega}_d = na + nmT(\omega_d) - mn\omega_d \in \mathbb{Z} + mn\omega_d\mathbb{Z}$.

In conclusione, $I\overline{I} = N(I)\mathbb{Z}[\omega_d] \subseteq \mathbb{Z} + mn\omega_d\mathbb{Z}$. Ora $N(I)\omega_d \in I\overline{I} \subseteq \mathbb{Z} + mn\omega_d\mathbb{Z}$ e quindi mn divide $N(I)$. D'altronde $n(a + m\omega_d) = na + mn\omega_d \in I\overline{I} = N(I)\mathbb{Z}[\omega_d]$; perciò $N(I)$ divide mn. Trattandosi di due interi positivi, $N(I) = mn$.

Infine, le classi laterali distinte di I sono rappresentate dagli interi algebrici $r + s\omega_d$ con $0 \leq r \leq n-1$ e $0 \leq s \leq m-1$. Dunque $|\mathbb{Z}[\omega_d]/I| = mn = N(I)$.

Proposizione 5.16 *In $\mathbb{Z}[\omega_d]$ ci sono al più un numero finito di ideali di norma fissata $N > 0$.*

Dimostrazione: Poiché $\mathbb{Z}[\omega_d]$ è un dominio di Dedekind, ogni suo elemento non nullo è contenuto in un numero finito di ideali massimali (Teorema 3.29) e dunque, poiché ogni ideale è prodotto finito di ideali primi (Teorema 4.9), anche in un numero finito di ideali. Allora basta notare, come sopra, che se $N = N(I)$ deve essere $N \in I$. □

Proposizione 5.17 *Esiste una costante positiva C_d, dipendente soltanto da d, tale che ogni ideale non nullo $I \subseteq \mathbb{Z}[\omega_d]$ contiene un elemento $\gamma \neq 0$ con $|N(\gamma)| \leq C_d N(I)$. Precisamente possiamo porre*

$$C_d := 1 + |T(\omega_d)| + |N(\omega_d)|.$$

Dimostrazione: Sia $N := N(I)$ la norma dell'ideale I e sia k il più grande intero tale che $k \leq \sqrt{N}$, così che $k^2 \leq N \leq (k+1)^2$. Scriviamo $I = n\mathbb{Z} \oplus (a + m\omega_d)\mathbb{Z}$ con $a \in \mathbb{Z}$ e $m, n > 0$ (Proposizione 5.11). Allora, come nell'Osservazione 5.15, si ha $N = mn$.

Consideriamo l'insieme $S := \{x + y\omega_d \,;\, 0 \leq x \leq k,\, 0 \leq y \leq k\} \subseteq \mathbb{Z}[\omega_d]$. Allora $|S| = (k+1)^2 > mn$. Per $i = 0, \ldots, m-1$, definiamo $S_i := \{x + y\omega_d \in S \,;\, y \equiv i \mod m\}$. Poiché $S = \bigcup_i S_i$, almeno uno di questi insiemi deve avere più di n elementi. Sia tale insieme $S_j := \{x_1 + y_1\omega_d, \ldots, x_h + y_h\omega_d\}$, dove $h > n$ e $y_s \equiv j \mod m$ per $s = 1, \ldots, h$. Poniamo $t_s := x_s - \frac{a(y_s - j)}{m}$, $s = 1, \ldots, h$, e notiamo che $t_s \in \mathbb{Z}$. Poiché $h > n$, esistono due indici $s_1 < s_2$ tali che $t_{s_1} \equiv t_{s_2} \mod n$. Consideriamo $\alpha := x_{s_1} + y_{s_1}\omega_d$, $\beta := x_{s_2} + y_{s_2}\omega_d$. Allora $\alpha, \beta \in S$ e $\alpha \neq \beta$.

Una semplice verifica mostra che $\gamma := \frac{t_{s_1} - t_{s_2}}{n} n + \frac{y_{s_1} - y_{s_2}}{m}(a + m\omega_d) = \alpha - \beta \in I \setminus \{0\}$. Poiché $\alpha,\, \beta \in S$, possiamo scrivere $\gamma = u + v\omega_d$ con $|u|$, $|v| \leq k$. Allora

$$\begin{aligned} |N(\gamma)| &= |(u + v\omega_d)(u + v\overline{\omega}_d)| = |u^2 + uvT(\omega_d) + v^2 N(\omega_d)| \\ &\leq u^2 + |uvT(\omega_d)| + |v^2 N(\omega_d)| \leq (1 + |T(\omega_d)| + |N(\omega_d)|)k^2 \\ &\leq C_d N(I). \qquad \square \end{aligned}$$

Teorema 5.18 *Il gruppo delle classi di ideali di $\mathbb{Z}[\omega_d]$ è finito.*

Dimostrazione: Con le notazioni della proposizione precedente, facciamo vedere che ogni classe di ideali può essere rappresentata da un ideale $J \subseteq \mathbb{Z}[\omega_d]$ tale che $N(J) \leq C_d$. Sia $I \subseteq \mathbb{Z}[\omega_d]$ un ideale non nullo e $0 \neq \alpha \in \overline{I}$ tale che $|N(\alpha)| \leq C_d N(\overline{I})$ (Proposizione 5.17). Poiché $\langle\alpha\rangle \subseteq \overline{I}$, allora $\langle\alpha\rangle = \overline{I}J$

con $J \subseteq \mathbb{Z}[\omega_d]$ (Proposizione 4.7(2)). Dunque $\alpha I = N(I)J$ e perciò I e J rappresentano la stessa classe. Inoltre, applicando la Proposizione 5.14, $C_d N(\bar{I}) \geq |N(\alpha)| = N(\bar{I}J) = N(\bar{I})N(J)$. Dunque $N(J) \leq C_d$.

Per la Proposizione 5.16, possiamo allora concludere che il numero delle classi di ideali è finito. □

Osservazione 5.19 La norma di un ideale I di $\mathcal{O}_K$ si definisce come l'indice di I in $\mathcal{O}_K$, cioè $N(I) = |\mathcal{O}_K/I|$ (che si dimostra essere finito). Per l'osservazione precedente, questa nozione coincide con quella data per gli anelli di interi quadratici. Notando che $N(I)(1 + I) = I$, vediamo che in ogni caso $N(I) \in I$. Inoltre si può dimostrare che valgono anche tutte le proprietà della Proposizione 5.14.

Per dimostrare più generalmente che il gruppo delle classi di un anello di interi algebrici $\mathcal{O}_K$ è finito, si può procedere come nel caso quadratico, facendo vedere che in $\mathcal{O}_K$ ci sono al più un numero finito di ideali di norma fissata e che esiste una costante positiva C_K tale che ogni classe di ideali può essere rappresentata da un ideale non nullo $I \subseteq \mathcal{O}_K$ con $N(I) \leq C_K$. Un teorema di H. Minkowski ci assicura che questo è vero, scegliendo $C_K := \frac{n!}{n^n}(\frac{4}{\pi})^t \sqrt{|\ \Delta\ |}$, dove, se $K = \mathbb{Q}(\theta)$, n è il grado di θ, $2t$ è il numero dei coniugati non reali di θ e Δ è il discriminante del campo K [7, Chapter 9].

Nel caso degli interi quadratici, risulta $C_K \leq C_d$ e dunque la costante di Minkowski dà una stima migliore. Infatti, se $d \not\equiv 1 \mod 4$, si ha $\omega_d = \sqrt{d}$ e quindi $C_d = 1 + |d|$. Se invece $d \equiv 1 \mod 4$, si ha $\omega_d = \frac{1+\sqrt{d}}{2}$ e quindi $C_d = 2 + |\frac{1-d}{4}|$. Inoltre risulta $t = 0$ se $d > 0$ e $t = 1$ se $d < 0$; dunque la costante di Minkowski è $C := \frac{1}{2}\sqrt{|\ \Delta\ |}$ per $d > 0$ e $C := (\frac{2}{\pi})\sqrt{|\ \Delta\ |}$ per $d < 0$. Infine $\Delta = \Delta(\omega_d) = d$ se $d \equiv 1 \mod 4$ e $\Delta = \Delta(\omega_d) = 4d$ altrimenti.

5.2 Fattorizzazione negli anelli di interi quadratici

Lo studio della fattorizzazione negli anelli di interi quadratici ha coinvolto molti matematici e non è stata ancora completata.

Questo problema è stato tuttavia completamente risolto per $d < 0$. Dickson (1927) ha determinato i valori negativi di d per cui $\mathbb{Z}[\omega_d]$ è euclideo rispetto alla norma e Dubois-Steger (1958) hanno dimostrato che, per $d < 0$, se $\mathbb{Z}[\omega_d]$ è euclideo, allora lo è rispetto alla norma. Sempre per d negativo, la classificazione degli anelli di interi quadratici a ideali principali è dovuta a Stark (1967).

Teorema 5.20 *Sia $d < 0$. Allora:*

(1) *L'anello degli interi quadratici $\mathbb{Z}[\omega_d]$ è euclideo soltanto per*

$$d = -1, -2, -3, -7, -11.$$

In questo caso $\mathbb{Z}[\omega_d]$ è euclideo rispetto alla norma.

(2) *L'anello degli interi quadratici* $\mathbb{Z}[\omega_d]$ *è a ideali principali e non euclideo soltanto per*

$$d = -19, -43, -67, -163.$$

Esempio 5.21 Quando $\mathbb{Z}[\omega_d]$ è euclideo, per effettuare la divisione si può procedere come nell'Osservazione 5.8, come si fa usualmente nell'anello degli interi di Gauss $\mathbb{Z}[i]$. Facciamo un esempio per $d = -2$.

Siano $\alpha := 5 + 2i\sqrt{2}$, $\beta := 2 + i\sqrt{2}$. Allora $N(\alpha) = 25 + 8 = 33$ e $N(\beta) = 4 + 2 = 6$, da cui β non divide α. Poniamo $\eta = \frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{N(\beta)} = \frac{14 - i\sqrt{2}}{6}$. Allora per $\delta := 2$ si ha $\eta - \delta = \frac{2 - i\sqrt{2}}{6}$ e $N(\eta - \delta) = \frac{1}{6} < 1$. Moltiplicando per β, otteniamo $\beta(\eta - \delta) = \alpha - 2\beta = \frac{(2 + i\sqrt{2})(2 - i\sqrt{2})}{6} = 1$ e finalmente $\alpha = 2\beta + 1$.

I valori positivi di d per i quali $\mathbb{Z}[\omega_d]$ è euclideo rispetto alla norma sono stati determinati in tappe successive da vari matematici. La lista è stata poi finalmente completata da Inkeri (1949) e Chatland-Daveport (1950) indipendentemente. È però da notare che, se d è positivo, $\mathbb{Z}[\omega_d]$ può essere euclideo senza esserlo rispetto alla norma; ad esempio questo accade per $d = 69$ (Clark, 1994). La classificazione degli anelli di interi quadratici reali che sono euclidei rispetto ad algoritmi diversi dalla norma non è stata ancora completata.

Teorema 5.22 *Se* $d \geq 2$*, l'anello degli interi quadratici* $\mathbb{Z}[\omega_d]$ *è euclideo rispetto alla norma soltanto per*

$$d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

La classificazione degli anelli di interi quadratici reali che sono a ideali principali (equivalentemente a fattorizzazione unica) presenta ancora molti problemi aperti. Ad esempio non è ancora noto se esistono infiniti anelli di interi quadratici con questa proprietà. La maggiore difficoltà si incontra per $d \equiv 1 \mod 4$, quando $\omega_d = \frac{1 + \sqrt{d}}{2}$. È invece facile dimostrare che, sempre se $d \equiv 1 \mod 4$, l'anello $\mathbb{Z}[\sqrt{d}]$ non è mai a fattorizzazione unica.

Per $2 \leq d < 100$, ci sono 38 valori (su 60) per i quali $\mathbb{Z}[\omega_d]$ è un dominio a ideali principali.

Teorema 5.23 *Se* $2 \leq d < 100$*, l'anello degli interi quadratici* $\mathbb{Z}[\omega_d]$ *è a ideali principali soltanto per*

$$d = 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, 38, 41, 43, 46, 47,$$
$$53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97.$$

5.2.1 Fattorizzazione in ideali primi

Poiché gli anelli di interi algebrici sono domini di Dedekind, ogni ideale proprio si fattorizza unicamente in ideali primi. Diamo ora un metodo per fattorizzare un ideale nel caso degli anelli di interi quadratici $\mathbb{Z}[\omega_d]$. A tal fine ricordiamo che negli anelli di Dedekind, se $I \subseteq J$ sono ideali non nulli, allora J divide I. In particolare, in $\mathbb{Z}[\omega_d]$, I divide l'ideale principale generato da $N(I)$, perché $N(I) \in I$.

Passo 1. Se $N(I) = p$ è un numero primo, allora I è un ideale primo.

Infatti, la norma di ideali è moltiplicativa (Proposizione 5.14). Quindi se $I = P_1 \dots P_n$, $n \geq 2$, è la fattorizzazione di I in ideali primi (non necessariamente distinti), allora $N(I) = N(P_1) \dots N(P_n)$ non è un numero primo.

Passo 2. Se $P \subseteq \mathbb{Z}[\omega_d]$ è un ideale primo non nullo, allora $N(P) = p$, oppure $N(p) = p^2$, per qualche numero primo $p \in \mathbb{Z}$.

Infatti, se $P \subseteq \mathbb{Z}[\omega_d]$ è un ideale primo, allora $P \cap \mathbb{Z}$ è un ideale primo di $\mathbb{Z}$ e perciò $P \cap \mathbb{Z} = p\mathbb{Z}$ con p numero primo. Poiché $p \in P$, allora $N(P)$ divide $N(p) = p^2$ (Proposizione 5.14), da cui la conclusione.

Passo 3. Se P ha norma prima uguale a p, allora P divide l'ideale principale $p\mathbb{Z}[\omega_d]$. Precisamente $p\mathbb{Z}[\omega_d] = P\overline{P}$. Dunque P e $\overline{P}$ sono i soli ideali primi di norma p.

Infatti, per definizione, $N(P)\mathbb{Z}[\omega_d] := P\overline{P} = p\mathbb{Z}[\omega_d]$ e, per l'unicità della fattorizzazione, non ci sono altri primi di norma p.

Passo 4. Esiste un ideale primo di norma prima p se e soltanto se esiste $a \in \mathbb{Z}$ tale che p divida $N(a+\omega_d)$. In questo caso i soli ideali primi di norma p sono $P := p\mathbb{Z} \oplus (a+\omega_d)\mathbb{Z} = \langle p, a+\omega_d \rangle$ e $\overline{P} = \langle p, a+\overline{\omega_d} \rangle$.

Per vedere questo, sia $N(P) = p$. Scrivendo $P = n\mathbb{Z} \oplus (a+m\omega_d)\mathbb{Z}$, come nella Proposizione 5.11, risulta $N(P) = mn$ (Osservazione 5.15). Poiché $P \cap \mathbb{Z} = n\mathbb{Z} \neq \mathbb{Z}$ è un ideale primo, allora $n = p$ e $m = 1$, da cui $P = p\mathbb{Z} \oplus (a+\omega_d)\mathbb{Z} = \langle p, a+\omega_d \rangle$, con $a \in \mathbb{Z}$ e $p = N(P)$ che divide $N(a+\omega_d)$ (perché $a+\omega_d \in P$).

Viceversa, supponiamo che p divida $N(a+\omega_d)$. Verifichiamo che il sottogruppo additivo $G := p\mathbb{Z} + (a+\omega_d)\mathbb{Z}$ di $\mathbb{Z}[\omega_d]$ è un ideale. Poiché G è additivamente chiuso, basta far vedere che $p\omega_d$, $\omega_d(a+\omega_d) \in G$. Ma $p\omega_d = -ap + p(a+\omega_d) \in G$ e $\omega_d(a+\omega_d) = -N(a+\omega_d) + (a+T(\omega_d))(a+\omega_d) \in G$, perché per ipotesi p divide $N(a+\omega_d)$. Poiché p e $a+\omega_d$ sono linearmente indipendenti su $\mathbb{Z}$, per quanto visto nell'Osservazione 5.15, concludiamo che l'ideale $p\mathbb{Z} \oplus (a+\omega_d)\mathbb{Z} = \langle p, a+\omega_d \rangle$ ha norma p.

Passo 5 (ramificazione). Se $p \in \mathbb{Z}$ è un numero primo, allora l'ideale $p\mathbb{Z}[\omega_d]$ è prodotto al più di due ideali primi distinti. Precisamente

(a) Se non esistono ideali primi di norma p, l'ideale $p\mathbb{Z}[\omega_d]$ è primo. In questo caso, p si chiama un *primo inerte*.

(b) Se esiste un ideale primo P di norma p, allora gli ideali primi di norma p sono solamente P e $\overline{P}$ e si ha $p\mathbb{Z}[\omega_d] = P\overline{P}$.

Se $P = \overline{P}$, $p\mathbb{Z}[\omega_d] = P^2$ e p si chiama un *primo ramificato*, se invece $P \neq \overline{P}$, p si chiama un *primo decomposto*.

Questo segue da quanto visto nei passi precedenti.

Passo 6. Sia $I \neq (0)$ un ideale proprio e $N(I) := N = p_1 \dots p_n$ la fattorizzazione di $N(I)$ in numeri primi. Allora $N\mathbb{Z}[\omega_d] = I\overline{I} = p_1\mathbb{Z}[\omega_d] \dots p_n\mathbb{Z}[\omega_d]$ e quindi un ideale primo di $\mathbb{Z}[\omega_d]$ che divide I deve dividere uno (e uno solo) degli ideali principali $p_i\mathbb{Z}[\omega_d]$. Dunque, per fattorizzare I in ideali primi, si deve studiare la ramificazione dei numeri primi p_i, come nei Passi (4) e (5).

5.2.2 Esempi

(1) Poiché i domini di interi algebrici sono noetheriani, ogni loro elemento non nullo si fattorizza in elementi irriducibili. Per fattorizzare un elemento $0 \neq x \in \mathbb{Z}[\omega_d]$, si può osservare che la norma di elementi è moltiplicativa; allora se $x = p_1 \dots p_n$ è una fattorizzazione propria in elementi irriducibili, la norma di p_i deve essere un divisore proprio della norma di x.

Ad esempio, sia $d = -6$. Poiché $d \equiv 2 \mod 4$, si ha $\omega_d = i\sqrt{6}$. Se $x = 10$, allora $N(x) = 100 = 2^2 \cdot 5^2$ e gli eventuali fattori propri irriducibili $q := a + bi\sqrt{6}$ di 10 devono avere norma $N(q) = a^2 + 6b^2 =: n$ che divide propriamente 100.

Per $n = 4$, troviamo $q = 2$, per $n = 25$ troviamo $q = 5$, per $n = 10$ troviamo $q = 2 \pm i\sqrt{6}$, altrimenti non ci sono soluzioni.

Si vede subito che $10 = 2 \cdot 5 = (2 + i\sqrt{6})(2 - i\sqrt{6})$ e che $2, 5, 2 \pm i\sqrt{6}$ sono irriducibili (perché in $\mathbb{Z}[i\sqrt{6}]$ non ci sono elementi di norma 2 o 5).

Poiché gli elementi invertibili di $\mathbb{Z}[i\sqrt{6}]$ sono soltanto 1 e -1 (quelli la cui norma è uguale ad 1), vediamo che $2, 5, 2 \pm i\sqrt{6}$ non sono elementi associati. Quindi il dominio $\mathbb{Z}[i\sqrt{6}]$ non è a fattorizzazione unica (equivalentemente, non è a ideali principali).

(2) Lo studio della ramificazione in $\mathbb{Z}[\omega_d]$ è legato a quello delle forme quadratiche. Infatti, come visto sopra, se P è un ideale primo di $\mathbb{Z}[\omega_d]$ che ha norma p, deve essere $P = \langle p, a + \omega_d \rangle$ con p che divide $N(a + \omega_d)$. Allora, per cercare gli ideali primi di norma p, dobbiamo risolvere la congruenza quadratica $N(x + \omega_d) \equiv 0 \mod p$. Notiamo che

$$\langle p, a + \omega_d \rangle = \langle p, b + \omega_d \rangle \quad \Leftrightarrow \quad a \equiv b \mod p.$$

Quindi p è inerte, ramificato o decomposto a seconda che questa congruenza abbia rispettivamente nessuna, una o due soluzioni modulo p.

Illustriamo questo procedimento con alcuni esempi.

(2a) Consideriamo l'anello degli interi di Gauss $\mathbb{Z}[i]$, anello degli interi di $\mathbb{Q}(i)$. In questo caso $\omega_d = i$ e, per cercare gli ideali di norma p, dobbiamo

risolvere la congruenza $x^2 + 1 \equiv 0 \mod p$. Non è difficile vedere che, se $p \geq 3$, questa congruenza ha soluzioni se e soltanto se $p \equiv 1 \mod 4$ e, per un teorema di Fermat, questo equivale a dire che p è somma di due quadrati. Infatti, poiché $\mathbb{Z}[i]$ è a ideali principali, cercare gli ideali di norma p equivale a cercare gli elementi di norma p e per questo, dobbiamo risolvere l'equazione $N(x + yi) = x^2 + y^2 = p$. Se ci sono soluzioni, allora $p = (x + yi)(x - yi)$.

In definitiva:

• Se $p = 2$, l'equazione ha soluzioni $x = y = 1$ e quindi $2 = (1+i)(1-i)$. Ma poiché $i + i$ e $1 - i = -i(1 + i)$ sono elementi associati, allora $2\mathbb{Z}[i] = (1 + i)^2\mathbb{Z}[i]$ (ovvero 2 è ramificato).

• Se $p \equiv 1 \mod 4$, si ha $p\mathbb{Z}[i] = (x + yi)\mathbb{Z}[i](x - yi)\mathbb{Z}[i]$, per opportuni $x, y \in \mathbb{Z}$ (ovvero p è ramificato);

• Se $p \equiv 3 \mod 4$, l'ideale $p\mathbb{Z}[i]$ è primo (ovvero p è inerte).

(2b) Sia $d = -17$. Poiché $d \equiv 3 \mod 4$, si ha $\omega_d = i\sqrt{17}$. Allora $N(a + i\sqrt{17}) = a^2 + 17$ e, per cercare gli ideali di norma p, dobbiamo risolvere la congruenza $x^2 + 17 \equiv 0 \mod p$.

Ad esempio:

• Se $p = 2$, otteniamo $x^2 + 17 \equiv x^2 + 1 \equiv (x + 1)^2 \equiv 0 \mod 2$, che ha l'unica soluzione $a \equiv 1 \mod 2$. Quindi l'unico ideale primo di norma 2 è $P := \langle 2, 1 + i\sqrt{17}\rangle$ (2 è un primo ramificato).

• Se $p = 3$, otteniamo $x^2 + 17 \equiv x^2 - 1 \equiv 0 \mod 3$, che ha soluzioni $a \equiv 1, 2 \mod 3$. Allora gli ideali primi di norma 3 sono $Q := \langle 3, 1 + i\sqrt{17}\rangle$ e $\overline{Q} = \langle 3, 1 - i\sqrt{17}\rangle = \langle 3, 2 + i\sqrt{17}\rangle$ (3 è un primo decomposto).

• Se $p = 5$, otteniamo $x^2+17 \equiv x^2+2 \equiv 0 \mod 5$, che non ha soluzioni. Quindi non ci sono ideali primi di norma 5 (5 è un primo inerte).

Siccome $30 = 2 \cdot 3 \cdot 5$, la decomposizione in ideali primi dell'ideale principale $30\mathbb{Z}[i\sqrt{17}]$ è $30\mathbb{Z}[i\sqrt{17}] = 5P^2Q\overline{Q}$.

Ricordiamo che $\mathbb{Z}[i\sqrt{17}]$ non è un dominio a ideali principali (Teorema 5.20). Infatti gli ideali P, Q e $\overline{Q}$ non sono principali, perché in $\mathbb{Z}[i\sqrt{17}]$ non ci sono elementi di norma 2 oppure 3.

(2c) Sia $d = 5$. Poiché $d \equiv 1 \mod 4$, si ha $\omega_5 = \frac{1+\sqrt{5}}{2}$. Allora $N(a + \omega_5) = a^2 + a - 1$ e, per cercare gli ideali di norma p, dobbiamo risolvere la congruenza $x(x + 1) \equiv 1 \mod p$.

Ad esempio:

• Se $p = 2, 3, 7$, non ci sono soluzioni (questi sono primi inerti).

• Se $p = 5$, abbiamo l'unica soluzione $a \equiv 2 \mod 5$; quindi l'unico primo di norma 5 è $P := \langle 5, 2 + \omega_5\rangle$ (5 è un primo ramificato).

• Se $p = 11$, abbiamo le due soluzioni $a \equiv 3, 7 \mod 11$; quindi gli ideali primi di norma 11 sono $Q := \langle 11, 3 + \omega_5\rangle$ e $\overline{Q} = \langle 11, 3 + \overline{\omega_5}\rangle = \langle 11, 7 + \omega_5\rangle$ (11 è un primo decomposto).

Ricordiamo tuttavia che $\mathbb{Z}[\omega_5]$ è un dominio euclideo (Teorema 5.22) e dunque tutti i suoi ideali sono principali.

Ad esempio, poiché $N(\sqrt{5}) = -5$ si ha che $\sqrt{5}$ è irriducibile e, poiché $5 = (\sqrt{5})^2$, per l'unicità della fattorizzazione in ideali primi, deve essere $P := \langle 5, 2+\omega_5\rangle = \langle\sqrt{5}\rangle$. Similmente, risulta $N(4+\sqrt{5}) = (4+\sqrt{5})(4-\sqrt{5}) = 11$ e si può verificare che $Q := \langle 11, 3+\omega_5\rangle = \langle 4-\sqrt{5}\rangle$.

(3) L'anello di interi quadratici $\mathbb{Z}[i\sqrt{5}]$, anello degli interi di $\mathbb{Q}(i\sqrt{5})$, non è a ideali principali. Infatti, procedendo come nell'Esempio (1), si può verificare che $6 = 2\cdot 3 = (1+i\sqrt{5})(1-i\sqrt{5})$ con $2, 3, 1\pm i\sqrt{5}$ elementi irriducibili non associati. Per fattorizzare (unicamente) l'ideale $6\mathbb{Z}[i\sqrt{5}]$ in ideale primi, cerchiamo gli ideali di norma 2 e 3.

• Se $N(P) = 2$, deve essere $P = \langle 2, a+i\sqrt{5}\rangle$, con a soluzione della congruenza $x^2 \equiv -5 \equiv 1 \mod 2$. Allora $a \equiv 1 \mod 2$ e $P = \langle 2, 1+\sqrt{5}\rangle = \overline{P}$ è l'unico ideale di norma 2.

• Se $N(Q) = 3$, deve essere $Q = \langle 3, a+i\sqrt{5}\rangle$, con a soluzione della congruenza $x^2 \equiv -5 \equiv 1 \mod 3$. Allora $a \equiv 1, 2 \mod 3$ e gli ideali primi di norma 3 sono $Q = \langle 3, 1+\sqrt{5}\rangle$ e $\overline{Q} = \langle 3, 1-\sqrt{5}\rangle = \langle 3, 2+\sqrt{5}\rangle$.

In conclusione, $6\mathbb{Z}[i\sqrt{5}] = P^2Q\overline{Q}$. Notiamo anche che $(1+i\sqrt{5})\mathbb{Z}[i\sqrt{5}] = PQ$ e $(1-i\sqrt{5})\mathbb{Z}[i\sqrt{5}] = \overline{PQ} = P\overline{Q}$.

Poiché $\mathbb{Z}[i\sqrt{5}]$ non è a ideali principali, il Gruppo delle Classi di $\mathbb{Z}[i\sqrt{5}]$ è non banale. Per calcolarlo, possiamo procedere come indicato dal Teorema 5.18, cercando le classi distinte degli ideali la cui norma è limitata da una fissata costante. Come nell'Osservazione 5.19, possiamo poi scegliere la costante di Minkowski, che in questo caso è $C_K := (\frac{2}{\pi})\sqrt{|\Delta|} = \frac{4}{\pi}\sqrt{5} < 3$, e quindi cercare gli ideali I di norma uguale a 1 e 2.

• Se $N(I) = 1$, allora $I = (1)$.

• Se $N(I) = 2$, allora I è primo e, come visto sopra, $I =: P = \langle 2, 1+i\sqrt{5}\rangle$.

In conclusione il Gruppo delle Classi di $\mathbb{Z}[i\sqrt{5}]$ ha due elementi, precisamente $C(\mathbb{Z}[i\sqrt{5}]) = \{[(1)], [P]\}$. (Si può verificare direttamente che P non è principale, perché in $\mathbb{Z}[i\sqrt{5}]$ non ci sono elementi $\alpha = x+iy\sqrt{5}$ tali che $N(\alpha) = x^2+5y^2 = 2$).

Notiamo che la costante C_{-5} della Proposizione 5.17 è uguale a $1+|-5| = 6$. Scegliendo questa costante, si devono cercare gli ideali di norma 2, 3, 4, 5 e 6. Tuttavia, poiché il Gruppo delle Classi è generato dalle classi degli ideali primi (Teorema 4.13), per determinarlo è sufficiente trovare gli ideali primi di $\mathbb{Z}[i\sqrt{5}]$ con tali possibili norme e le loro relazioni modulo il gruppo degli ideali principali:

• L'unico ideale primo che divide l'ideale $2\mathbb{Z}[i\sqrt{5}]$ è (come visto sopra) l'ideale $P = \overline{P}$, che ha norma 2. Quindi non ci sono ideali primi di norma 4.

• Gli ideali di norma 3 sono gli ideali primi Q e $\overline{Q}$ trovati sopra; ma poiché gli ideali $P^2 = 2\mathbb{Z}[i\sqrt{5}]$, $PQ = (1+i\sqrt{5})\mathbb{Z}[i\sqrt{5}]$ e $P\overline{Q} = (1-i\sqrt{5})\mathbb{Z}[i\sqrt{5}]$ sono principali, allora $[Q] = [P] = [\overline{Q}]$.

• Se $N(I) = 5$, allora I deve essere l'ideale primo $\langle 5, a+i\sqrt{5}\rangle$, con a soluzione della congruenza $x^2 \equiv -5 \equiv 0 \mod 5$. Dunque $a \equiv 0 \mod 5$ e $I = i\sqrt{5}\mathbb{Z}[i\sqrt{5}]$ è un ideale principale. Quindi $[I] = [(1)]$.

• Se esiste un ideale I con $N(I) = 6 = 2 \cdot 3$, allora I non può essere primo. D'altra parte I esiste e, come visto sopra, risulta $I = PQ = (1+i\sqrt{5})\mathbb{Z}[i\sqrt{5}]$, oppure $I = P\overline{Q} = (1-i\sqrt{5})\mathbb{Z}[i\sqrt{5}]$. In ogni caso, I è principale e $[I] = [(1)]$.

Alla fine, con più calcoli, arriviamo alla stessa conclusione che $C(\mathbb{Z}[i\sqrt{5}]) = \{[(1)], [P]\}$.

Un risultato di Carlitz (1960) afferma che il numero delle classi di un anello di interi quadratici è uguale a 2 se e soltanto se tutte le fattorizzazioni di un elemento non nullo x in elementi irriducibili hanno lo stesso numero di fattori. I domini con questa proprietà si chiamano domini *metà fattoriali*. Altri domini di interi quadratici metà fattoriali si ottengono per $d = -6, \pm 10, -13, \pm 15, \ldots$ etc. [7, Table10.2].

Riferimenti bibliografici

[1] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[2] R. M. Fossum, *The divisor class group of a Krull domain*, Springer-Verlag, 1973.

[3] S. Gabelli, *Teoria delle Equazioni e Teoria di Galois*, Springer, 2008.

[4] S. Gabelli, *Introduzione alla Teoria delle Valutazioni*, http://www.mat.uniroma3.it/users/gabelli/dispense/Valutazioni.pdf

[5] R. Gilmer, *Multiplicative Ideal Theory*, Dekker, New York, 1972.

[6] R.Y. Sharp, *Steps in Commutative Algebra*, London Math. Soc. Student Texts 51, 1990.

[7] I. Stewart and D. Tall, *Algebraic Number Theory and Fermat Last Theorem* (third edition), Peters, 2002