Lezione 22

Prerequisiti: Lezioni 20, 21.

Fattorizzazione di ideali.

Teorema 22.1 Sia A un dominio di Dedekind, e sia I un suo ideale proprio non nullo. Allora esistono unici ideali primi non nulli $P_1,...,P_r$ a due a due distinti ed unici numeri interi positivi $n_1,...,n_r$ tali che

$$I = P_1^{n_1} \cdots P_r^{n_r} . \qquad (*)$$

La decomposizione (*) si dice *fattorizzazione* di I.

Dimostrazione: Proviamo dapprima l'esistenza. Supponiamo per assurdo che l'insieme S degli ideali propri non nulli di A che non ammettono una decomposizione (*) sia non vuoto. Essendo, in base alla Definizione 20.18, A noetheriano, in virtù della condizione b) della Definizione 18.1, S ammette allora un elemento massimale I. Sia I_0 un ideale massimale contenente I. Allora I_0 è un ideale primo non nullo. Quindi, per la Proposizione 21.8, esiste un ideale frazionario J tale che $A \subset J$ e $I_0 J = A$. Segue che

$$I = IA \subset IJ \subset I_0 J = A ,$$

quindi IJ è un ideale intero. Inoltre $IJ \neq I$: lo si dimostra procedendo come nell'ultima parte della dimostrazione della Proposizione 21.8. Infine, IJ è un ideale proprio. Infatti, se fosse $IJ = A$, allora sarebbe $I_0 J = IJ$, da cui $I_0 JI = IJI$, e dunque $I_0 = I$, il che è impossibile, dato che $I_0 \notin S$. Stante la massimalità di I, IJ è quindi prodotto di ideali primi non nulli. Allora lo stesso vale per $IJI_0 = I$, assurdo. Proviamo ora l'unicità della decomposizione (*). Supponiamo che si abbia

$$P_1^{n_1} \cdots P_r^{n_r} = Q_1^{m_1} \cdots Q_s^{m_s} , \qquad (1)$$

ove P_i, Q_j sono ideali primi non nulli e n_i, m_j sono interi positivi. Poiché il prodotto a primo membro è contenuto in P_1, lo stesso vale per il prodotto a secondo membro. Dunque, in virtù della Proposizione 21.1 b), si ha che $Q_j \subset P_1$ per qualche j. Ma, essendo Q_j un ideale massimale in virtù della Definizione 20.18, segue che $Q_j = P_1$. Per concludere la dimostrazione, si moltiplichino entrambi i membri di (1) per P_1^{-1} e si proceda per induzione. □

Osservazione 22.2 Il Teorema 22.1 stabilisce, per i domini di Dedekind, una proprietà di fattorizzazione unica valida non per gli elementi (non nulli e non invertibili), ma per gli ideali (diversi dall'ideale nullo e dall'anello stesso). La dimostrazione ricalca fedelmente quella del Teorema Fondamentale dell'Aritmetica, oppure l'analoga argomentazione con cui si prova che l'anello dei polinomi in un indeterminata a coefficienti in un campo è un UFD (vedi Algebra 2, Teorema 19.7). In effetti, in un PID (che, in base alla Proposizione 19.4 di Algebra 2, è sempre un UFD) gli ideali primi non nulli sono tutti e soli gli ideali della forma (p), ove p è un elemento primo: ne deriva che l'esistenza ed unicità della fattorizzazione di un generico ideale proprio non nullo (a) equivale alla analoga proprietà dell'elemento a (che è necessariamente non nullo e non invertibile): se

$$a = p_1 \cdots p_r$$

è la fattorizzazione di a, allora

$$(a) = (p_1) \cdots (p_r)$$

è la fattorizzazione dell'ideale (a).

L'esistenza ed unicità della fattorizzazione stabilite dal Teorema 22.1 valgono però, per una classe di anelli più ampia di quella dei PID e degli UFD: l'Osservazione 20.16 mostra, infatti, che non tutti i domini di Dedekind sono UFD.

Corollario 22.3 Per ogni ideale non nullo I di un dominio di Dedekind A esiste un ideale frazionario J tale che $IJ = A$.

Dimostrazione: Se $I = A, J = A$. Sia $I \neq A$. Se $I = P_1^{n_1} \cdots P_r^{n_r}$ è una fattorizzazione di I, allora si può prendere $J = P_1^{-n_1} \cdots P_r^{-n_r}$ (essendo $P^{-n} = (P^{-1})^n$). Si ricorda che l'inverso di un ideale primo non nullo esiste in virtù della Proposizione 21.8. □

Esempio 22.4 Nel dominio di Dedekind $\mathbf{Z}[i\sqrt{5}]$ proviamo che vale la seguente fattorizzazione

$$(6) = P_1 P_2 P_3 P_4, \tag{2}$$

ove $P_1 = (2, 1 + i\sqrt{5})$, $P_2 = (2, 1 - i\sqrt{5})$, $P_3 = (3, 1 + i\sqrt{5})$, $P_4 = (3, 1 - i\sqrt{5})$ sono ideali primi di $\mathbf{Z}[i\sqrt{5}]$. Si verifica infatti che $\mathbf{Z}[i\sqrt{5}]/P_1 \cong \mathbf{Z}[i\sqrt{5}]/P_2 \cong \mathbf{Z}_2$, e $\mathbf{Z}[i\sqrt{5}]/P_3 \cong \mathbf{Z}[i\sqrt{5}]/P_4 \cong \mathbf{Z}_3$ (provare per esercizio). Proviamo (2). Si ha che

$$P_3 P_4 = ((3) + (1 + i\sqrt{5}))((3) + (1 - i\sqrt{5})) = (9) + (3 + 3i\sqrt{5}) + (3 - 3i\sqrt{5}) + (6) = (3) \tag{3}$$

dove l'ultima uguaglianza si prova facilmente verificando le due inclusioni.

Analogamente si prova che

$$P_1 P_2 = (2). \tag{4}$$

Quindi, infine,

$$P_1 P_2 P_3 P_4 = (2)(3) = (6).$$

La decomposizione (2) è unica, in virtù del Teorema 22.2. Non è però unica la decomposizione di 6 in fattori irriducibili in $\mathbf{Z}[i\sqrt{5}]$. Infatti, come sappiamo dall'Osservazione 18.18 di Algebra 2,

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

sono due distinte decomposizioni. Esse corrispondono alle seguenti decomposizioni dell'ideale (6):

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

Queste non sono, però, decomposizioni in ideali primi: ad esempio, l'ideale (2) non è primo perché 2 non è un elemento primo di $\mathbf{Z}[i\sqrt{5}]$. Esse scaturiscono dalla (2) raggruppando opportunamente i fattori, infatti, oltre alla (3) e alla (4) si ha:

$$(1+i\sqrt{5}) = P_1P_3, \quad (1-i\sqrt{5}) = P_2P_4.$$

Nota storica La moderna teoria degli ideali nasce da qui: l'idea di introdurre gli ideali per recuperare, per gli anelli D_K che non sono UFD, una proprietà di fattorizzazione unica, risale all'Ottocento, ed è del matematico tedesco Ernst Eduard Kummer (1810-1893). Egli studiò i campi ciclotomici (ossia i campi numerici del tipo $K = Q(\omega)$, ove $\omega \neq 1$ è un radice p-esima dell'unità, essendo p un numero primo) nel tentativo di dimostrare l'Ultimo Teorema di Fermat. I dettagli possono essere trovati in [Ri], mentre un cenno alla teoria di Kummer è contenuto in [B], Capitoli 1 e 2.

A Kummer risale anche il seguente criterio pratico di fattorizzazione di alcuni ideali degli ideali D_K. Nel suo enunciato viene presupposta la proprietà stabilita nella Proposizione 19.8.

****Teorema 22.5** (*Criterio di Kummer*) Sia K un campo numerico, e sia $D_K = \mathbf{Z}[\alpha]$. Sia $f(x) \in \mathbf{Z}[x]$ il polinomio minimo di α su **Q**. Sia, inoltre, p un numero primo (in **Z**). Indicata con $\overline{f(x)}$ la riduzione di $f(x)$ modulo p, siano $f_1(x),\dots,f_r(x) \in \mathbf{Z}[x]$ monici tali che $\overline{f_1(x)},\dots,\overline{f_r(x)}$ siano irriducibili in $\mathbf{Z}_p[x]$, a due a due distinti, e, per opportuni interi positivi $n_1,\dots,n_r$, si abbia

$$\overline{f(x)} = \overline{f_1(x)}^{n_1}\cdots\overline{f_r(x)}^{n_r}.$$

Allora, posto, per ogni $i = 1,\dots,r$, $P_i = (p, f_i(\alpha))$,

$$(p) = P_1^{n_1}\cdots P_r^{n_r}$$

è una fattorizzazione dell'ideale principale (p) in $\mathbf{Z}[\alpha]$. In particolare, se $\overline{f(x)}$ è irriducibile in $\mathbf{Z}_p[x]$, allora l'ideale (p) è primo in $\mathbf{Z}[\alpha]$.

Dimostrazione: [Mi], Theorem 3.41.

Osservazione 22.6 Il Teorema 22.5 permette di determinare la fattorizzazione di ogni ideale principale (m) di D_K, ove m è un intero maggiore di 1. Se

$$m = p_1^{u_1}\cdots p_s^{u_s}$$

è la fattorizzazione di m in **Z**, allora si ha

$$(m) = (p_1)^{u_1}\cdots(p_s)^{u_s}.$$

Si applica quindi il Teorema 22.5 ad ognuno degli ideali (p_i).

Vediamo alcune applicazioni.

Esempio 22.7 Ricaviamo la fattorizzazione di (6) in $\mathbf{Z}[i\sqrt{5}]$, già esaminata nell'Esempio 22.4. Dalla fattorizzazione $6 = 2 \cdot 3$ in **Z**, si ricava la decomposizione

$$(6) = (2) \cdot (3).$$

Il polinomio minimo di $\alpha = i\sqrt{5}$ su **Q** è $f(x) = x^2 + 5$, la cui riduzione modulo 2 ha la fattorizzazione

$$\overline{f(x)} = x^2 + \overline{1} = (x + \overline{1})^2,$$

mentre la fattorizzazione modulo 3 è

$$\overline{f(x)} = x^2 + \overline{2} = (x + \overline{1})(x + \overline{2}).$$

In base al Teorema 22.5 si ha che

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

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

Si ricava la fattorizzazione

$$(6) = (2, 1 + i\sqrt{5})^2 (3, 1 + i\sqrt{5})(3, 2 + i\sqrt{5}),$$

che coincide con quella precedentemente trovata: infatti $(2, 1 + i\sqrt{5}) = (2, 1 - i\sqrt{5})$, e $(3, 2 + i\sqrt{5}) = (3, 1 - i\sqrt{5})$.

Il procedimento che abbiamo appena effettuato si estende facilmente ad un arbitrario campo quadratico. Diamo di seguito, senza dimostrazione, un risultato in tal senso.

Proposizione 22.8 Sia m un intero privo di quadrati tale che $m \equiv 2$ o $m \equiv 3$ (mod 4). Sia $K = \mathbf{Q}(\sqrt{m})$. Sia p un numero primo.

a) Se esiste $a \in \mathbf{Z}$ tale che $a^2 \equiv m \pmod{p}$, allora

$$(p) = (p, a + \sqrt{m}) \cdot (p, a - \sqrt{m}).$$

b) Altrimenti (p) è un ideale primo.

Esercizio 22.9 Determinare i numeri primi che sono elementi primi di $\mathbf{Z}[i]$.

<u>Svolgimento</u>: Sia p un numero primo. Allora p è un elemento primo di $\mathbf{Z}[i]$ se e solo se (p) è un ideale primo di $\mathbf{Z}[i]$. In base alla Proposizione 22.8 ciò avviene se e solo se la congruenza

$x^2 \equiv -1 \pmod p$ non ha soluzione, se e solo se $p \equiv 3 \pmod 4$: l'ultima equivalenza è un noto risultato di teoria dei numeri elementare (vedi, ad esempio, [PC], pag. 195 e seguenti). Quindi i numeri interi che sono primi in $\mathbf{Z}[i]$ sono: 3, 7, 19, 23, 31,... Ad esempio, il numero 5 non è primo, perché non è irriducibile: infatti una sua decomposizione non banale è $5=(2+i)(2-i)$. Ricordiamo che $\mathbf{Z}[i]$ è un dominio euclideo (vedi Algebra 2, Proposizione 16.4) quindi è un PID (vedi Algebra 2, Proposizione 16.5), e in un PID le nozioni di elemento primo ed elemento irriducibile coincidono (vedi Algebra 2, Corollario 18.21).

Esercizio 22.10 Sapendo che, per $K=\mathbf{Q}(\sqrt[3]{2})$, $D_K=\mathbf{Z}[\sqrt[3]{2}]$, trovare una fattorizzazione di (5) in $\mathbf{Z}[\sqrt[3]{2}]$.

Svolgimento: Applichiamo il Teorema 22.5. Il polinomio minimo di $\sqrt[3]{2}$ su $\mathbf{Q}$ è $f(x)=x^3-2$. La sua riduzione modulo 5 è

$$\overline{f(x)}=x^3+\overline{3},$$

ed ha, in $\mathbf{Z}_5$, radice $\overline{3}$. Si ha allora

$$\overline{f(x)}=(x+\overline{2})(x^2+\overline{3}x+\overline{4}),$$

dove il secondo fattore è irriducibile su $\mathbf{Z}_5$, perché ivi privo di radici. Segue che

$$(5)=(5,2+\sqrt[3]{2})(5,4+3\sqrt[3]{2}+\sqrt[3]{4}).$$

Estendiamo ora il risultato stabilito nel Teorema 22.1 ad un qualunque ideale frazionario proprio non nullo di un dominio di Dedekind.

Proposizione 22.11 Sia A un dominio di Dedekind. Sia I un suo ideale frazionario proprio non nullo. Allora esistono unici ideali primi non nulli $P_1,\ldots,P_r$ a due a due distinti ed unici numeri interi non nulli $n_1,\ldots,n_r$ tali che

$$I=P_1^{n_1}\cdots P_r^{n_r} \qquad (**)$$

Dimostrazione: Basta supporre che I sia un ideale frazionario proprio non intero. Sia a un denominatore di I, così che $I=(a)^{-1}aI$. Gli ideali interi (propri, non nulli) (a) ed aI di A si decompongono, in virtù del Teorema 22.1, nel prodotto di ideali primi non nulli. Ciò prova l'esistenza di una decomposizione (**). L'unicità si prova come nella dimostrazione del Teorema 22.1, passando ad esponenti positivi (per moltiplicazioni con opportuni ideali primi). □

Osservazione 22.12 Abbiamo così stabilito che ogni ideale frazionario non nullo di un dominio di Dedekind A ammette un inverso: si ha che $A^{-1}=A$, e, se I è un ideale frazionario proprio non nullo, di fattorizzazione $I=P_1^{n_1}\cdots P_r^{n_r}$, allora $I^{-1}=P_1^{-n_1}\cdots P_r^{-n_r}$.

Abbiamo quindi raggiunto lo scopo che ci eravamo prefissi al termine della lezione precedente.

Corollario 22.13 L'insieme degli ideali frazionari non nulli di un dominio di Dedekind A è un gruppo abeliano moltiplicativo (denotato $I(A)$).

Definizione 22.14 Sia A un dominio d'integrità, sia K un suo campo dei quozienti. Un ideale frazionario di A si dice *principale* se è del tipo $A\alpha$ per qualche $\alpha \in K$. Scriveremo, per semplicità, (α).

Proposizione 22.15 L'insieme $P(A)$ degli ideali frazionari principali non nulli di un dominio di Dedekind A è un sottogruppo di $I(A)$.

Dimostrazione: Poiché $A=(1)$, $A \in P(A)$. Siano $I=(\alpha), J=(\beta) \in P(A)$. Allora $IJ^{-1}=(\alpha)(\beta)^{-1}=(\alpha\beta^{-1}) \in P(A)$. □

Definizione 22.16 Il gruppo quoziente $Cl(A)=I(A)/P(A)$ è detto *gruppo delle classi di ideali* di A. Il suo ordine è detto *numero delle classi di ideali.*

Il gruppo moltiplicativo abeliano $Cl(A)$ ci dà una misura di quanto un dominio di Dedekind A si discosti dall'essere un PID (o, equivalentemente, un UFD, in base al Corollario 20.20).

Proposizione 22.17 Un dominio di Dedekind A è un PID se e solo se $|Cl(A)|=1$.

Dimostrazione: Sia A un PID. Allora ogni ideale intero di A è principale. Sia I un ideale frazionario non nullo di A e sia a un suo denominatore. Allora aI è un ideale intero, per cui $aI=(b)$ per qualche $b \in A$. Segue che $I=(a^{-1}b)$ è un ideale frazionario principale. Quindi $I(A)=P(A)$, cioè $|Cl(A)|=1$.

Viceversa, sia $|Cl(A)|=1$. Allora, in particolare, ogni ideale intero I di A è un ideale frazionario principale, ossia $I=(\alpha)$ per qualche $\alpha \in K$. Ma allora $\alpha \in I \subset A$, quindi I è l'ideale principale intero di A generato da α. Quindi A è un PID. □

Verificheremo più avanti che, ad esempio, $|Cl(\mathbf{Z}[i\sqrt{5}])|=2$.

Osservazione 22.18 Si può dare una definizione alternativa di $Cl(A)$. Sull'insieme $Int(A)$ degli ideali interi non nulli del dominio di Dedekind A (con campo dei quozienti K) introduciamo la seguente relazione binaria:

$$\forall I,J \in Int(A), \quad I \sim J \Leftrightarrow \exists \alpha \in K \ \text{ tale che } \ I=\alpha J .$$

È facile verificare che ~ è una relazione di equivalenza. Consideriamo l'applicazione

$$\begin{aligned} \varphi : Int(A) &\to I(A)/P(A) = Cl(A) \\ I &\mapsto IP(A) \end{aligned}$$

Proviamo che φ è suriettiva. Sia I un ideale frazionario di A non nullo. Allora esiste $a \in A$ non nullo tale che aI sia un ideale intero di A, e quindi

$$\varphi(aI)=aIP(A)=I(a)P(A)=IP(A),$$

dove l'ultima uguaglianza segue dal fatto che $(a) \in P(A)$. Inoltre, per ogni $I, J \in Int(A)$, si ha che $\varphi(I) = \varphi(J)$ se e solo se $IJ^{-1} \in P(A)$ se e solo se esiste $\alpha \in K$ tale che $IJ^{-1} = (\alpha)$, se e solo se esiste $\alpha \in K$ tale che $I = \alpha J$ se e solo se $I \sim J$.
Segue che φ induce una biiezione

$$\varphi^* : Int(A)/\sim \; \to Cl(A).$$

Ponendo, per ogni $I, J \in Int(A)$, $[I][J] = [IJ]$, ad imitazione dell'identità $(IP(A))(JP(A)) = IJP(A)$ di $Cl(A)$, si munisce $Int(A)/\sim$ di una struttura di gruppo moltiplicativo isomorfo a $Cl(A)$. Essa è una realizzazione equivalente del gruppo delle classi di ideali di A.

Prima di procedere con la teoria del gruppo delle classi di ideali, vediamo di stabilire un'importante proprietà dell'aritmetica degli ideali nei domini di Dedekind, che corrisponde a una ben nota proprietà di divisibilità dei numeri interi: un numero che divide altri due numeri divide anche la loro somma. Questa proprietà ci sarà utile nella Lezione 25. Premettiamo la seguente:

Osservazione 22.19 Sia A un dominio di Dedekind, siano I, J suoi ideali non nulli. Se I divide J, cioè esiste un ideale I' tale che $II' = J$, allora $J \subset I$. Viceversa, se $J \subset I$, allora sia $L = I^{-1}J \subset I^{-1}I = A$. L è un ideale di A tale che $J = LI$, per cui I divide J. Abbiamo così provato la regola fondamentale:

$$I \text{ divide } J \Leftrightarrow I \text{ contiene } J.$$

Esercizio 22.20 Sia A un dominio di Dedekind. Siano I,J,L ideali di A. Provare che se L divide I e L divide J, allora L divide $I + J$.

Svolgimento: Supponiamo che L divida I. Allora $I \subset L$. Se L divide J, allora $J \subset L$. Quindi $I + J \subset L$, cioè L divide $I + J$.