Lezione 24

Prerequisiti: Lezioni 22, 23.

Il gruppo delle classi di ideali.

Sia K un campo numerico.
In questa sezione proveremo che il gruppo delle classi di ideali $Cl(D_K)$ introdotto nella Definizione 22.16 è finito. Ricordiamo che, in base all'Osservazione 22.18, esso è formato da classi di ideali interi.

Lemma 24.1 Il gruppo delle classi ideali $Cl(D_K)$ è finito se e solo se esiste una costante C tale che ogni classe di ideali contenga un ideale di norma al più C.

Dimostrazione: Supponiamo che $Cl(D_K)$ sia finito, diciamo $Cl(D_K) = \{[I_1],...,[I_n]\}$. Allora si prenda $C = \max_{i=1,..,n} N(I_i)$. Per dimostrare l'implicazione contraria, basta provare che esiste solo un numero finito di ideali la cui norma sia al più C. Per ogni ideale proprio non nullo I, se $I = P_1^{n1} \cdots P_r^{nr}$ è la sua fattorizzazione, allora, in virtù della moltiplicatività della norma di ideali (vedi Teorema 23.17), si ha $N(I) = N(P_1)^{n1} \cdots N(P_r)^{nr}$. Ma, in base al Corollario 23.24, ogni fattore a secondo membro è la potenza di un primo. Poiché esiste solo un numero finito di potenze di primi minori o uguali a C, in virtù dell'Esercizio 23.26 segue che è finito il numero degli ideali di D_K tali che $N(I) \le C$. □

Lemma 24.2 Esiste una costante C tale che per ogni ideale non nullo I di D_K esiste $\alpha \in I$, $\alpha \neq 0$ con $|N(\alpha)| \le CN(I)$.

Dimostrazione: Sia $\alpha_1,...,\alpha_n$ una base di D_K su $\mathbf{Z}$. Sia I un ideale proprio non nullo di D_K, e sia m un intero tale che $m^n \le N(I) < (m+1)^n$. Consideriamo

$$S = \left\{ \sum_{i=1}^{n} m_i \alpha_i \,\middle|\, 0 \le m_i \le m, m_i \in \mathbf{Z} \right\} \subset D_K .$$

Poiché $|S| = (m+1)^n > N(I) = (D_K : I)$, esistono $x, y \in S$ distinti tali che $\alpha = x - y \in I$. Sia $\alpha = \sum_{i=1}^{n} m_i \alpha_i$, con $0 \le |m_i| \le m, m_i \in \mathbf{Z}$ per ogni $i = 1,..,n$. Allora, in base all'Osservazione 23.10, dette $\sigma_1,...,\sigma_n$ le immersioni di K in un'estensione algebricamente chiusa di $\mathbf{Q}$ (ad esempio $\mathbf{C}$), si ha

$$|N(\alpha)| = \prod_{i=1}^{n} |\sigma_i(\alpha)| \le \prod_{i=1}^{n} \sum_{j=1}^{n} |m_j| |\sigma_i(\alpha_j)| \le m^n C \le N(I)C,$$

ove si è posto $C = \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\alpha_j)|$. □

Sia C come nella dimostrazione del Lemma 24.2.

Lemma 24.3 Ogni elemento di $Cl(D_K)$ contiene un ideale di norma al più C.

Dimostrazione: Sia $\gamma \in Cl(D_K)$. Allora, in base all'Osservazione 22.18, esiste un ideale I di D_K tale che $[I] = \gamma^{-1}$. In base al Lemma 24.2 esiste $\alpha \in I$ tale che $\frac{|N(\alpha)|}{N(I)} \le C$. Allora $J = I^{-1}(\alpha) \subset D_K$ è un ideale di D_K tale che $IJ = (\alpha)$, e $[J] = [I]^{-1} = \gamma$. Inoltre, data la moltiplicatività della norma, $N(J) = \frac{|N(\alpha)|}{N(I)} \le C$. □

Dai Lemmi 24.1, 24.2 e 24.3 segue

Teorema 24.4 $Cl(D_K)$ è finito.

Per determinare $Cl(D_K)$ basta quindi determinare tutti gli ideali che hanno norma minore o uguale alla costante C. A questo proposito si deve tenere presente che il valore di quest'ultima dipende strettamente dalla scelta della base di D_K su **Z**.

Esempio 24.5 Sia $K = \mathbf{Q}(\sqrt{2})$. Allora, in base alla Proposizione 19.20, $D_K = \mathbf{Z}[\sqrt{2}]$. Calcoliamo prima C rispetto alla base formata da $\alpha_1 = 1, \alpha_2 = \sqrt{2}$. Le immersioni di K in un campo algebricamente chiuso contenente **Q** sono due $\sigma_1 : a + b\sqrt{2} \mapsto a + b\sqrt{2}$, $\sigma_2 : a + b\sqrt{2} \mapsto a - b\sqrt{2}$. Quindi

$$C = \prod_{i=1}^{2} \sum_{j=1}^{2} |\sigma_i(\alpha_j)| = (|\sigma_1(\alpha_1)| + |\sigma_1(\alpha_2)|)(|\sigma_2(\alpha_1)| + |\sigma_2(\alpha_2)|) = \left(|\sigma_1(1)| + |\sigma_1(\sqrt{2})|\right)\left(|\sigma_2(1)| + |\sigma_2(\sqrt{2})|\right)$$
$$= (1 + \sqrt{2})(1 + \sqrt{2}) = 3 + 2\sqrt{2} \approx 5.8$$

Questo valore può però essere reso più piccolo, ad esempio scegliendo la base $1, -1 + \sqrt{2}$. In tal caso, infatti,

$$C = (1 - 1 + \sqrt{2})(1 + 1 + \sqrt{2}) = 2\sqrt{2} + 2 \approx 4.82 .$$

Esercizio 24.6 Determinare $Cl(\mathbf{Z}[\sqrt{2}])$.

Svolgimento: Utilizzando il risultato dell'Esempio 24.5, determiniamo tutti gli ideali I di $\mathbf{Z}[\sqrt{2}]$ tali che $N(I) \le 4$. In virtù dell'Osservazione 22.18, possiamo limitarci agli ideali interi non nulli, che hanno norma pari ad un intero positivo. Se $N(I) = 1$, allora $I = \mathbf{Z}[\sqrt{2}]$. Consideriamo i restanti casi.

a) $N(I) = 2$. In base al Lemma 23.22, $2 \in I$. Sia $a + b\sqrt{2} \in I$, con $a, b \in \mathbf{Z}$. Allora, in virtù del Corollario 23.20, 2 divide $N(a + b\sqrt{2}) = a^2 - 2b^2$ (vedi Esempio 23.3 b)). Segue che 2 divide a, e quindi $a \in I$. Allora $b\sqrt{2} \in I$. Se tutti i b siffatti fossero pari, allora si avrebbe che $I \subset (2)$, e quindi si avrebbe $I = (2)$. In tal caso, però, sarebbe $N(I) = 4$. Quindi esiste un intero b dispari

siffatto, allora $\sqrt{2} \in I$. Pertanto $(\sqrt{2}) \subset I$; poiché $N((\sqrt{2})) = N(I) = 2$, in virtù del Corollario 23.19, segue che $I = (\sqrt{2})$.

b) $N(I) = 4$. Per ogni $a, b \in \mathbf{Z}$ tali che $a + b\sqrt{2} \in I$ si ha che $4 = N(I)$ divide $N(a + b\sqrt{2}) = a^2 - 2b^2$. Segue che a e b sono entrambi pari. Quindi $I \subset (2)$. Poiché $N(I) = N((2)) = 4$, segue che $I = (2)$.

c) $N(I) = 3$. In base al Corollario 23.18, I è allora un ideale primo, e $3 \in I$, cioè $(3) \subset I$. Però, in base alla Proposizione 22.8, (3) è un ideale primo, perché la congruenza $x^2 \equiv 2 \pmod 3$ non ha soluzione. Ma allora (3) è massimale. Quindi $I = (3)$. Però, in tal caso, sarebbe $N(I) = 9$.

Abbiamo così concluso che gli ideali non nulli di norma al più 4 sono (1), (2), $(\sqrt{2})$. Essi sono rappresentanti di tutte le classi di $Cl(\mathbf{Z}[\sqrt{2}])$. Segue che tutti gli ideali di D_K sono principali, cioè $\left|Cl(\mathbf{Z}[\sqrt{2}])\right| = 1$, ossia $\mathbf{Z}[\sqrt{2}]$ è un PID.

Esercizio 24.7 Provare che $\left|Cl(\mathbf{Z}[i\sqrt{5}])\right| = 2$.

Svolgimento: Calcoliamo la costante C corrispondente alla base $1, i\sqrt{5}$ di $\mathbf{Z}[i\sqrt{5}]$ su $\mathbf{Z}$:

$$C = (1 + \left|i\sqrt{5}\right|)(1 + \left|-i\sqrt{5}\right|) = (1 + \sqrt{5})^2 = 6 + 2\sqrt{5} \approx 10.47 < 11.$$

È sufficiente determinare tutti gli ideali interi di norma minore o uguale a 10 per avere un rappresentante in ogni classe di $Cl(\mathbf{Z}[i\sqrt{5}])$. Questi sono prodotti di ideali primi P tali che $N(P) = p^m$, con p un numero primo minore o uguale a 7 (vedi Corollario 23.24). Allora $p \in P$, cioè $(p) \subset P$. Allora, in virtù della Proposizione 21.1 b), P contiene uno degli ideali primi (che sono massimali) della fattorizzazione di (p) e quindi coincide con esso. Quindi possiamo restringere la nostra ricerca agli ideali che sono prodotti degli ideali primi che compaiono nelle fattorizzazioni di (2), (3), (5), (7). Utilizzando il criterio di Kummer (Teorema 22.5) si trova:

$$\begin{array}{lcccl} (2) & = & (2,1 + i\sqrt{5})^2 & = & P_1^{\,2} \\ (3) & = & (3,1 + i\sqrt{5})(3,1 - i\sqrt{5}) & = & P_3 P_4 \\ (5) & = & (i\sqrt{5})^2 & = & P_5^{\,2} \\ (7) & = & (7,3 + i\sqrt{5})(7,3 - i\sqrt{5}) & = & P_6 P_7 \end{array}$$

Le prime due fattorizzazioni erano già state verificate negli Esempi 22.4 e 22.7. Ricordiamo che l'ideale P_1 non è principale. (vedi l'Esempio 23.21). Analogamente si prova che non sono principali gli ideali P_3, P_4, P_6, P_7. Proviamo che questi appartengono alla stessa classe di P_1. Anzitutto osserviamo che, in $Cl(\mathbf{Z}[i\sqrt{5}])$,

$$[P_1]^2 = [(2)] = [(1)], \quad \text{da cui} \quad [P_1] = [P_1]^{-1} \tag{1}$$

Quindi ricordiamo dall'Esempio 22.4 che $P_1 P_3 = (1 + i\sqrt{5})$ e $P_1 P_4 = (1 - i\sqrt{5})$, per cui

$$[P_3] = [(1+i\sqrt{5})][P_1]^{-1} = [(1+i\sqrt{5})][P_1] = [P_1], \quad \text{e} \quad [P_4] = [(1-i\sqrt{5})][P_1]^{-1} = [P_1].$$

Per completare la verifica, occorre provare che gli ideali P_1P_6 e P_1P_7 sono principali. Si verifica facilmente che

$$P_1P_6 = (3+i\sqrt{5}).$$

Analogamente si prova che

$$P_1P_7 = (3-i\sqrt{5}).$$

Pertanto, la classe di ogni ideale avente norma al più 10 è una potenza di $[P_1]$, cioè, in base alla (1), coincide con $[(1)]$ oppure $[P_1]$. Queste sono allora tutte le classi di ideali di $\mathbf{Z}[i\sqrt{5}]$, cioè $\left|Cl(\mathbf{Z}[i\sqrt{5}])\right| = 2$.