

Esempi di calcoli espliciti in Teoria dei Numeri

Note dal Corso di Teoria dei Numeri,
di Andrea Mori

Versione Maggio 2003

Lo scopo di queste note è di illustrare come, nei casi più semplici, metodi elementari permettano di calcolare in pratica il **gruppo delle classi** ed il **gruppo delle unità** di un campo di numeri.

1 Il gruppo delle classi

Sia K un campo di numeri (cioè un'estensione algebrica finita del campo razionale \mathbb{Q}) e denotiamo A l'anello degli interi di K .

L'anello A è un dominio di Dedekind e l'insieme \mathcal{I} degli ideali frazionari non nulli di K è un gruppo rispetto alla moltiplicazione. Tra gli ideali frazionari, quelli della forma $A\alpha$ si dicono *principali*. L'insieme \mathcal{P} degli ideali principali costituisce un sottogruppo di \mathcal{I} . Il **gruppo delle classi** è il quoziente

$$C = \mathcal{I}/\mathcal{P}.$$

Il gruppo delle classi C fornisce una misura della complessità dell'aritmetica di K nel senso dell'osservazione

$$A \text{ è un dominio a fattorizzazione unica } \iff C = \{1\}$$

che segue dall'equivalenza $\text{PID} \iff \text{UFD}$ nell'ambito dei domini di Dedekind. Vale il

Teorema 1.1 (Dirichlet). *Il gruppo delle classi C è finito.*

Correntemente, questo risultato si fa discendere dai due fatti seguenti:

- (Minkowski) Esiste una costante M che dipende solo da K , tale che ogni classe in C possiede un rappresentante $I \subseteq A$ tale che $N(I) < M$.
- Per ogni $N > 0$ esistono solo un numero finito di ideali $I \subseteq A$ tali che $N(I) < N$.

Ricordiamo anche che la norma $N(I)$ di un ideale $I \subseteq A$ è per definizione il numero degli elementi in A/I . Inoltre:

- Per ogni $I, J \subseteq A$ vale l'uguaglianza $N(IJ) = N(I)N(J)$ e pertanto la mappa norma si estende a \mathcal{I} per moltiplicatività.

- Un ideale $I \subseteq A$ è principale se e soltanto se esiste $x \in I$ tale che $N(I) = N_{K/\mathbb{Q}}(x)$.

Se K è un'estensione di grado n e discriminante δ con r_1 immersioni reali e r_2 immersioni complesse (a meno di coniugio) in modo che $n = r_1 + 2r_2$ la costante M di Minkowski sopra citata è

$$M = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |\delta|^{1/2} \quad (1)$$

Campi Quadratici Consideriamo ora il caso dei campi quadratici ($n = 2$). Senza perdita di generalità scriviamo $K = \mathbb{Q}(\sqrt{m})$ con $m \in \mathbb{Z}$ privo di fattori quadratici. Sappiamo che l'anello degli interi è

$$A = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{se } m \equiv 2, 3 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] & \text{se } m \equiv 1 \pmod{4} \end{cases}$$

e corrispondentemente

$$\delta = \begin{cases} 4m & \text{se } m \equiv 2, 3 \pmod{4} \\ m & \text{se } m \equiv 1 \pmod{4} \end{cases}.$$

Possiamo allora esplicitare la costante di Minkowski M in (1) osservando che $r_2 = 0$ se $m > 0$ e $r_2 = 1$ se $m < 0$. Otteniamo la tabella

$$\begin{array}{ccc} & m > 0 & m < 0 \\ m \equiv 1 \pmod{4} & \frac{1}{2}\sqrt{m} & \frac{2}{\pi}\sqrt{|m|} \\ m \equiv 2, 3 \pmod{4} & \sqrt{m} & \frac{4}{\pi}\sqrt{|m|} \end{array}$$

Prima di procedere con i calcoli espliciti è necessario ottenere qualche informazione più precisa sulla decomposizione degli ideali in A . In particolare, siccome gli ideali in A di norma t sono esattamente quelli che contengono t , ci servirà sapere come si decompone l'ideale At . Per il Teorema Fondamentale dell'Aritmetica, basterà conoscere la decomposizione degli ideali Ap con p primo. Il prossimo risultato risponde esattamente a questa domanda.

Proposizione 1.2. *Si hanno i casi seguenti:*

- se $p|m$ allora $Ap = (p, \sqrt{m})^2$.
- se m è dispari, allora

$$A2 = \begin{cases} (2, 1 + \sqrt{m})^2 & \text{se } m \equiv 3 \pmod{4} \\ (2, \frac{1+\sqrt{m}}{2})(2, \frac{1-\sqrt{m}}{2}) & \text{se } m \equiv 1 \pmod{8} \\ \text{è primo} & \text{se } m \equiv 5 \pmod{8} \end{cases}$$

- Se p è dispari e non divide m , allora

$$Ap = \begin{cases} (p, a + \sqrt{m})(p, a - \sqrt{m}) & \text{se } m \equiv a^2 \pmod{p} \\ \text{è primo} & \text{se } m \text{ non è un quadrato modulo } p \end{cases}$$

Inoltre, nei casi in cui la decomposizione è data da due fattori, questi sono distinti.

Dimostrazione: Supponiamo $p|m$. Si ha allora $(p, \sqrt{m})^2 = (p^2, p\sqrt{m}, m) \subseteq Ap$.

D'altronde, siccome m è privo di fattori quadrati, $p = \text{MCD}(p^2, m)$. Allora per l'identità di Bezout $p \in (p, \sqrt{m})^2$ ottenendo così l'inclusione opposta.

Esattamente allo stesso modo si trattano i casi in cui m è dispari e congruo a 3 modulo 4 o a 1 modulo 8, oppure p dispari con m non divisibile per p e quadrato modulo p .

Negli altri casi occorre dimostrare che l'ideale Ap è primo. Supponiamo p dispari e Ap non primo. Siccome $N_{K/\mathbb{Q}}(p) = p^2$, ogni fattore proprio \mathfrak{p} di Ap deve avere norma p . Pertanto $A/\mathfrak{p} \simeq \mathbb{Z}/\mathbb{Z}p$. Per costruzione l'equazione $x^2 - m$ ha soluzione in A e quindi in ogni suo quoziente. Ma nelle ipotesi correnti l'equazione non è risolvibile in $\mathbb{Z}/\mathbb{Z}p$, da cui si ha la contraddizione.

Il caso $p = 2$ si tratta in modo analogo. Poichè ora $m \equiv 1 \pmod{4}$, l'equazione di secondo grado da considerare è quella soddisfatta dall'intero $\frac{1}{2}(1 + \sqrt{m})$ cioè $x^2 - x + \frac{1}{4}(1 - m)$.

Infine, la non uguaglianza dei due fattori nei casi $m \equiv 1 \pmod{8}$ e m quadrato modulo p se p è dispari e non divide m è del tutto chiara. ■

Abbiamo così completato i requisiti necessari per il calcolo vero e proprio che, in ciascun caso, procederà come segue:

1. determinazione della costante di Minkowski M ;
2. determinazione, usando la Proposizione 1.2, degli ideali primi di norma $< M$;
3. determinazione delle relazioni tra gli ideali del punto precedente e quindi della struttura del gruppo delle classi C .

Distinguiamo tra campi quadratici immaginari ($m < 0$) e reali ($m > 0$).

Campi Quadratici Immaginari

$[m = -1]$ $K = \mathbb{Q}(i)$, $A = \mathbb{Z}[i]$, $M = \frac{4}{\pi} \sim 1.27$. Dunque $C = \{\bar{A}\}$ e A è un PID.

$[m = -2]$ $K = \mathbb{Q}(\sqrt{-2})$, $A = \mathbb{Z}[-2]$, $M = \frac{4}{\pi}\sqrt{2} \sim 1.8$. Dunque $C = \{\bar{A}\}$ e A è un PID.

$[m = -3]$ $K = \mathbb{Q}(\sqrt{-3})$, $A = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-3})]$, $M = \frac{2}{\pi}\sqrt{3} \sim 1.1$. Dunque $C = \{\bar{A}\}$ e A è un PID.

$[m = -5]$ $K = \mathbb{Q}(\sqrt{-5})$, $A = \mathbb{Z}[\sqrt{-5}]$, $M = \frac{4}{\pi}\sqrt{5} \sim 2.84$. Siccome $A_2 = (2, \sqrt{-5})^2$, l'unico ideale di norma 2 è $I = (2, \sqrt{-5})$ che non è principale in quanto non possiede elementi di norma 2 perchè le equazioni

$$a^2 + 5b^2 = \pm 2$$

non hanno soluzioni in \mathbb{Z}^2 . Dunque $C = \langle \bar{I} \rangle \simeq \mathbb{Z}/2\mathbb{Z}$.

$[m = -6]$ $K = \mathbb{Q}(\sqrt{-6})$, $A = \mathbb{Z}[\sqrt{-6}]$, $M = \frac{4}{\pi}\sqrt{6} \sim 3.11$. Si ha

$$A_2 = (2, \sqrt{-6})^2 = I^2, \quad A_3 = (3, \sqrt{-6})^2 = J^2$$

con $IJ = A\sqrt{-6}$ principale. pertanto $C = \langle \bar{I} \rangle \simeq \mathbb{Z}/2\mathbb{Z}$.

[$m = -7$] $K = \mathbb{Q}(\sqrt{-7})$, $A = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-7})]$, $M = \frac{2}{\pi}\sqrt{7} \sim 1.68$. Dunque $C = \{\bar{A}\}$ e A è un PID.

[$m = -10$] $K = \mathbb{Q}(\sqrt{-10})$, $A = \mathbb{Z}[\sqrt{-10}]$, $M = \frac{4}{\pi}\sqrt{10} \sim 4.02$. Siccome $A_2 = (2, \sqrt{-10})^2$, l'unico ideale di norma 2 è $I = (2, \sqrt{-10})$ che non è principale in quanto non possiede elementi di norma 2 perchè le equazioni

$$a^2 + 10b^2 = \pm 2$$

non hanno soluzioni in \mathbb{Z}^2 . Inoltre, $-10 \equiv 2$ non è un quadrato modulo 3: l'ideale A_3 è primo e non esistono ideali di norma 3. Dunque $C = \langle \bar{I} \rangle \simeq \mathbb{Z}/2\mathbb{Z}$.

[$m = -11$] $K = \mathbb{Q}(\sqrt{-11})$, $A = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-11})]$, $M = \frac{2}{\pi}\sqrt{11} \sim 2.11$. Siccome $-11 \equiv 5 \pmod{8}$ l'ideale A_2 è primo e non esistono ideali di norma 2. Dunque $C = \{\bar{A}\}$ e A è un PID.

[$m = -13$] $K = \mathbb{Q}(\sqrt{-13})$, $A = \mathbb{Z}[\sqrt{-13}]$, $M = \frac{4}{\pi}\sqrt{13} \sim 4.59$. Siccome $A_2 = (2, \sqrt{-13})^2$, l'unico ideale di norma 2 è $I = (2, \sqrt{-13})$ che non è principale in quanto non possiede elementi di norma 2 perchè le equazioni

$$a^2 + 13b^2 = \pm 2$$

non hanno soluzioni in \mathbb{Z}^2 . Inoltre, $-13 \equiv 2$ non è un quadrato modulo 3: l'ideale A_3 è primo e non esistono ideali di norma 3. Dunque $C = \langle \bar{I} \rangle \simeq \mathbb{Z}/2\mathbb{Z}$.

[$m = -14$] $K = \mathbb{Q}(\sqrt{-14})$, $A = \mathbb{Z}[\sqrt{-14}]$, $M = \frac{4}{\pi}\sqrt{14} \sim 4.76$. Si hanno le decomposizioni

$$A_2 = (2, \sqrt{-14})^2 = I^2, \quad A_3 = (3, 1 + \sqrt{-14})(3, 1 - \sqrt{-14}) = J_1 J_2.$$

Le classi \bar{A} , \bar{I} , \bar{J}_1 e \bar{J}_2 sono tutte distinte in C . Infatti

1. Gli ideali I , J_1 e J_2 non sono principali, mancando elementi di norma 2 o 3 in quanto le equazioni

$$a^2 + 14b^2 = \pm 2, \pm 3$$

non hanno soluzioni in \mathbb{Z}^2 .

2. $\bar{I} \neq \bar{J}_1$ (o \bar{J}_2) perchè A_3 è l'unico ideale principale di norma 9 ed allora $J_1^2 \neq A_3$ non è principale.
3. $\bar{J}_1 \neq \bar{J}_2$ perchè altrimenti C risulterebbe un gruppo con tre elementi, contraddicendo $\bar{I}^2 = \bar{A}$.

Infine, siccome $\bar{J}_1^2 \neq \bar{A}$ deve essere $C = \langle \bar{J}_1 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$.

[$m = -15$] $K = \mathbb{Q}(\sqrt{-15})$, $A = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-15})]$, $M = \frac{2}{\pi}\sqrt{15} \sim 2.46$. Si ha la decomposizione

$$A_2 = \left(2, \frac{1 + \sqrt{-15}}{2}\right) \left(2, \frac{1 - \sqrt{-15}}{2}\right) = IJ.$$

Gli ideali I e J non sono principali (non ci sono elementi di norma 2) ma I^2 e J^2 lo sono, ad esempio $I^2 = (\frac{1 + \sqrt{-15}}{2})$. Pertanto l'unica possibilità di avere un gruppo è che risulti $\bar{I} = \bar{J}$ e dunque $C = \langle \bar{I} \rangle \simeq \mathbb{Z}/2\mathbb{Z}$.

[$m = -17$] $K = \mathbb{Q}(\sqrt{-17})$, $A = \mathbb{Z}[\sqrt{-15}]$, $M = \frac{4}{\pi}\sqrt{17} \sim 5.24$. Si hanno le decomposizioni

$$A2 = (2, 1 + \sqrt{-17})^2 = I^2, \quad A3 = (3, 1 + \sqrt{-17})(3, 1 - \sqrt{-17}) = J_1 J_2$$

con I , J_1 e J_2 non principali, in mancanza di elementi di norma 2 o 3. Inoltre $A5$ è primo in quanto $-17 \equiv 2 \pmod{5}$ non è un quadrato.

L'ideale $J_1^2 = (9, 1 + \sqrt{-17}) \neq A3$ non è principale perchè 3 è l'unico elemento di norma 9. Stesso dicasi per J_2^2 . Possiamo allora procedere come nel caso $m = -14$ per concludere che $C = \langle \bar{J}_1 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$.

[$m = -19$] $K = \mathbb{Q}(\sqrt{-19})$, $A = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-19})]$, $M = \frac{2}{\pi}\sqrt{19} \sim 2.77$. Siccome $-19 \equiv 5 \pmod{8}$, l'ideale $A2$ è primo. Dunque $C = \{\bar{A}\}$ e A è un PID.

[$m = -21$] $K = \mathbb{Q}(\sqrt{-21})$, $A = \mathbb{Z}[\sqrt{-21}]$, $M = \frac{4}{\pi}\sqrt{21} \sim 5.8$. Si hanno le decomposizioni

$$A2 = (2, 1 + \sqrt{-21})^2 = I^2, \quad A3 = (3, \sqrt{-21})^2 = J^2$$

e

$$A5 = (5, 2 + \sqrt{-21})(5, 2 - \sqrt{-21}) = P_1 P_2$$

in quanto $-21 \equiv 2^2 \pmod{5}$. Osserviamo che:

1. Mancando elementi di norma 2, 3, 5, 6, 10 o 15 gli ideali I , J , P_1 , P_2 , IJ , IP_i e JP_i sono tutti non principali ($i = 1, 2$).
2. $P_1^2 = (2 + \sqrt{-21})$ e $P_2^2 = (2 - \sqrt{-21})$ sono principali.
3. Dalle relazioni $\bar{P}_1^2 = \bar{P}_2^2 = \bar{P}_1 \bar{P}_2 = \bar{A}$ segue $\bar{P}_1 = \bar{P}_2$ (chiamiamo \bar{P} questa classe).

Ne segue che le quattro classi $\{\bar{A}, \bar{I}, \bar{J}, \bar{P}\}$ sono tutte distinte e siccome ogni elemento ha quadrato banale, $C \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

[$m = -23$] $K = \mathbb{Q}(\sqrt{-23})$, $A = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-23})]$, $M = \frac{2}{\pi}\sqrt{19} \sim 3.09$. Si hanno le decomposizioni

$$A2 = (2, \frac{1 + \sqrt{-23}}{2})(2, \frac{1 - \sqrt{-23}}{2}) = I_1 I_2$$

e

$$A3 = (3, 1 + \sqrt{-23})(3, 1 - \sqrt{-23}) = J_1 J_2$$

in quanto $-23 \equiv 1^2 \pmod{3}$. Siccome le equazioni

$$a^2 + 23b^2 = 16, 36$$

hanno soluzioni solo per $b = 0$, gli ideali I_1^2 , I_2^2 , J_1^2 e J_2^2 non sono principali.

D'altra parte $I_1 J_1 = (\frac{1 + \sqrt{-23}}{2})$ e $I_2 J_2 = (\frac{1 - \sqrt{-23}}{2})$ sono principali. Dunque C risulta generato da \bar{I}_1 ed in assenza di altri elementi, $C = \langle \bar{I}_1 \rangle \simeq \mathbb{Z}/3\mathbb{Z}$.

[$m = -26$] $K = \mathbb{Q}(\sqrt{-26})$, $A = \mathbb{Z}[\sqrt{-26}]$, $M = \frac{4}{\pi}\sqrt{26} \sim 6.49$. Si hanno le decomposizioni $A2 = (2, \sqrt{-26})^2 = I^2$ e, siccome $-26 \equiv 1^2 \pmod{3}$ e $-26 \equiv 2^2 \pmod{5}$,

$$A3 = (3, 1 + \sqrt{-26})(3, 1 - \sqrt{-26}) = P_1 P_2$$

e

$$A3 = (3, 2 + \sqrt{-26})(3, 2 - \sqrt{-26}) = Q_1 Q_2$$

Osserviamo che:

1. Mancando elementi di norma 2, 3 o 5 gli ideali I , P_1 , P_2 , Q_1 e Q_2 sono tutti non principali.
2. Gli ideali P_1^2 , P_2^2 , Q_1^2 e Q_2^2 sono non principali perchè non si hanno soluzioni delle equazioni $a^2 + 26b^2 = 9$ o 25 con $b \neq 0$.
3. $Q_1^6 = (109 + 12\sqrt{-26})$ è la più piccola potenza di Q_1 che risulti principale, in quanto le equazioni

$$a^2 + 26b^2 = 5^k$$

sono prive di soluzioni con $b \neq 0$ per $0 < k < 6$.

4. Nel gruppo C si ha $\bar{I} = \bar{Q}_1^3$ e $\bar{P}_1 = \bar{Q}_1^4$ perchè $IQ_1^3 = (4 - 3\sqrt{-26})$ e $P_1Q_1^2 = (7 + \sqrt{-26})$ sono principali.

In definitiva $C = \langle \bar{Q}_1 \rangle \simeq \mathbb{Z}/6\mathbb{Z}$

Campi Quadratici Reali

[$m = 2$] $K = \mathbb{Q}(\sqrt{2})$, $A = \mathbb{Z}[2]$, $M = \sqrt{2} \sim 1.4$. Dunque $C = \{\bar{A}\}$ e A è un PID.

[$m = 3$] $K = \mathbb{Q}(\sqrt{3})$, $A = \mathbb{Z}[3]$, $M = \sqrt{3} \sim 1.7$. Dunque $C = \{\bar{A}\}$ e A è un PID.

[$m = 5$] $K = \mathbb{Q}(\sqrt{5})$, $A = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{5})]$, $M = \frac{1}{2}\sqrt{5} \sim 1.11$. Dunque $C = \{\bar{A}\}$ e A è un PID.

[$m = 6$] $K = \mathbb{Q}(\sqrt{6})$, $A = \mathbb{Z}[\sqrt{6}]$, $M = \sqrt{6} \sim 2.4$. Si ha la decomposizione $A2 = (2, \sqrt{6})^2$ e l'equazione

$$a^2 - 6b^2 = \pm 2$$

ha soluzioni $a = \pm 2$, $b = \pm 1$. Dunque $(2, \sqrt{6}) = (2 + \sqrt{6})$ è principale: $C = \{\bar{A}\}$ e A è un PID.

[$m = 7$] $K = \mathbb{Q}(\sqrt{7})$, $A = \mathbb{Z}[\sqrt{7}]$, $M = \sqrt{7} \sim 2.64$. Si ha la decomposizione $A2 = (2, 1 + \sqrt{7})^2$ e l'equazione

$$a^2 - 7b^2 = \pm 2$$

ha soluzioni $a = \pm 3$, $b = \pm 1$. Dunque $(2, 1 + \sqrt{7}) = (3 + \sqrt{7})$ è principale: $C = \{\bar{A}\}$ e A è un PID.

[$m = 10$] $K = \mathbb{Q}(\sqrt{10})$, $A = \mathbb{Z}[\sqrt{10}]$, $M = \sqrt{10} \sim 3.16$. Si hanno decomposizioni $A2 = (2, \sqrt{10})^2 = I^2$ e

$$A3 = (3, 1 + \sqrt{10})(3, 1 - \sqrt{10}) = J_1 J_2$$

in quanto $10 \equiv 1^2 \pmod{3}$. Le equazioni

$$a^2 - 10b^2 = \pm 2, \pm 3$$

non hanno soluzioni in \mathbb{Z}^2 perchè 2 e 3 non sono quadrati modulo 5. Dunque I , J_1 e J_2 non sono principali. D'altra parte l'ideale IJ_1 che ha norma 6 è principale in quanto $IJ_1 = (2 - \sqrt{10})$. Dunque $\bar{I} = \bar{J}_2$ in C e $C \simeq \mathbb{Z}/2\mathbb{Z}$.

[$m = 11$] $K = \mathbb{Q}(\sqrt{11})$, $A = \mathbb{Z}[\sqrt{11}]$, $M = \sqrt{11} \sim 3.31$. Si ha la decomposizione $A2 = (2, 1 + \sqrt{11})^2$ e l'equazione

$$a^2 - 11b^2 = \pm 2$$

ha soluzioni $a = \pm 3$, $b = \pm 1$. Dunque $(2, 1 + \sqrt{11}) = (3 + \sqrt{11})$ è principale. Inoltre $11 \equiv 2 \pmod{3}$ non è un quadrato e l'ideale $A3$ è primo. Dunque $C = \{\bar{A}\}$ e A è un PID.

[$m = 13$] $K = \mathbb{Q}(\sqrt{13})$, $A = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{13})]$, $M = \frac{1}{2}\sqrt{13} \sim 1.8$. Dunque $C = \{\bar{A}\}$ e A è un PID.

[$m = 14$] $K = \mathbb{Q}(\sqrt{14})$, $A = \mathbb{Z}[\sqrt{14}]$, $M = \sqrt{14} \sim 3.74$. Si ha la decomposizione $A2 = (2, \sqrt{14})^2$ e l'equazione

$$a^2 - 14b^2 = \pm 2$$

ha soluzioni $a = \pm 4$, $b = \pm 1$. Dunque $(2, \sqrt{14}) = (4 + \sqrt{14})$ è principale. Inoltre $14 \equiv 2 \pmod{3}$ non è un quadrato e l'ideale $A3$ è primo. Dunque $C = \{\bar{A}\}$ e A è un PID.

[$m = 15$] $K = \mathbb{Q}(\sqrt{15})$, $A = \mathbb{Z}[\sqrt{15}]$, $M = \sqrt{15} \sim 3.87$. Si hanno decomposizioni

$$A2 = (2, 1 + \sqrt{15})^2 = I^2, \quad A3 = (3, \sqrt{15})^2 = J^2$$

Le equazioni $a^2 - 15b^2 = \pm 2, \pm 3$ non hanno soluzioni in \mathbb{Z}^2 perchè 2 e 3 non sono quadrati modulo 5. Dunque I e J non sono principali. Però l'ideale IJ che ha norma 6 è principale in quanto $IJ = (3 + \sqrt{15})$. Dunque $\bar{I} = \bar{J}^{-1} = \bar{J}$ in C e $C \simeq \mathbb{Z}/2\mathbb{Z}$.

[$m = 17$] $K = \mathbb{Q}(\sqrt{17})$, $A = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{17})]$, $M = \frac{1}{2}\sqrt{17} \sim 2.06$. Si ha la decomposizione

$$A2 = (2, \frac{1 + \sqrt{17}}{2})(2, \frac{1 - \sqrt{17}}{2}) = I_1 I_2.$$

La ricerca di elementi interi di norma ± 2 è equivalente alla ricerca di soluzioni intere dell'equazione

$$a^2 - 17b^2 = \pm 8.$$

Essa ha soluzioni $a = \pm 5$, $b = \pm 1$. Pertanto $I_1 = (\frac{5 + \sqrt{17}}{2})$ è principale e dunque $C = \{\bar{A}\}$ e A è un PID.

[$m = 19$] $K = \mathbb{Q}(\sqrt{19})$, $A = \mathbb{Z}[\sqrt{19}]$, $M = \sqrt{19} \sim 4.3$. Si hanno decomposizioni
 $A_2 = (2, 1 + \sqrt{19})^2 = I^2$ e

$$A_3 = (3, 1 + \sqrt{19})(3, 1 - \sqrt{19}) = J_1 J_2$$

in quanto $19 \equiv 1^2 \pmod{3}$. Le equazioni

$$a^2 - 19b^2 = \pm 2, \pm 3$$

hanno soluzioni $a = \pm 13$, $b = \pm 3$ e $a = \pm 4$, $b = \pm 1$ rispettivamente. Dunque $I = (13 + 3\sqrt{19})$ e $J_1 = (4 + \sqrt{19})$ sono principali: $C = \{\bar{A}\}$ e A è un PID.

[$m = 21$] $K = \mathbb{Q}(\sqrt{21})$, $A = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{21})]$, $M = \frac{1}{2}\sqrt{21} \sim 2.29$. Siccome $21 \equiv 5 \pmod{8}$ l'ideale A_2 è primo. Dunque $C = \{\bar{A}\}$ e A è un PID.

[$m = 22$] $K = \mathbb{Q}(\sqrt{22})$, $A = \mathbb{Z}[\sqrt{22}]$, $M = \sqrt{22} \sim 4.3$. Si hanno decomposizioni
 $A_2 = (2, \sqrt{22})^2 = I^2$ e

$$A_3 = (3, 1 + \sqrt{22})(3, 1 - \sqrt{22}) = J_1 J_2$$

in quanto $22 \equiv 1^2 \pmod{3}$. Le equazioni

$$a^2 - 19b^2 = \pm 2, \pm 3$$

hanno soluzioni $a = \pm 14$, $b = \pm 3$ e $a = \pm 5$, $b = \pm 1$ rispettivamente. Dunque $I = (14 + 3\sqrt{22})$ e $J_1 = (5 + \sqrt{22})$ sono principali: $C = \{\bar{A}\}$ e A è un PID.

[$m = 23$] $K = \mathbb{Q}(\sqrt{23})$, $A = \mathbb{Z}[\sqrt{23}]$, $M = \sqrt{23} \sim 4.79$. Si hanno la decomposizioni

$$A_2 = (2, 1 + \sqrt{23})(2, 1 - \sqrt{23}) = I_1 I_1.$$

L'ideale A_3 è primo in quanto $23 \equiv 2 \pmod{3}$ non è un quadrato. L'equazione

$$a^2 - 23b^2 = \pm 2$$

ha soluzione $a = \pm 5$, $b = \pm 1$ e dunque $I_1 = (5 + \sqrt{23})$ è principale: $C = \{\bar{A}\}$ e A è un PID.

[$m = 26$] $K = \mathbb{Q}(\sqrt{26})$, $A = \mathbb{Z}[\sqrt{26}]$, $M = \sqrt{26} \sim 5.09$. Si hanno decomposizioni
 $A_2 = (2, \sqrt{26})^2 = I^2$ e

$$A_5 = (3, 1 + \sqrt{26})(3, 1 - \sqrt{26}) = J_1 J_2$$

in quanto $26 \equiv 1^2 \pmod{5}$. D'altra parte A_3 è primo in quanto $26 \equiv 2 \pmod{3}$ non è un quadrato. Le equazioni

$$a^2 - 26b^2 = \pm 2, \pm 5$$

sono prive di soluzioni in \mathbb{Z}^2 in quanto 2, 5, 8 e 11 non sono quadrati modulo 13. Dunque I , J_1 e J_2 non sono principali. L'ideale di norma 10 $IJ = (1 + \sqrt{26})$ è principale e dunque $C = \langle \bar{I} \rangle \simeq \mathbb{Z}/2\mathbb{Z}$.

[$m = 29$] $K = \mathbb{Q}(\sqrt{29})$, $A = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{29})]$, $M = \frac{1}{2}\sqrt{29} \sim 2.69$. Siccome $21 \equiv 5 \pmod{8}$ l'ideale A_2 è primo. Si ha la decomposizione

$$A_2 = (2, \frac{1 + \sqrt{29}}{2})(2, \frac{1 - \sqrt{29}}{2}) = I_1 I_2.$$

La ricerca di elementi interi di norma ± 2 è equivalente alla ricerca di soluzioni intere dell'equazione

$$a^2 - 29b^2 = \pm 8.$$

Essa non ha soluzioni perchè 8 e 21 non sono quadrati modulo 29. Pertanto $C = \langle \bar{I}_1 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$.

[$m = 30$] $K = \mathbb{Q}(\sqrt{30})$, $A = \mathbb{Z}[\sqrt{30}]$, $M = \sqrt{30} \sim 5.47$. Si hanno decomposizioni $A_2 = (2, \sqrt{30})^2 = P^2$, $A_3 = (3, \sqrt{30})^2 = Q^2$ e $A_5 = (5, \sqrt{30})^2 = R^2$. Gli ideali P , Q e R non sono principali in quanto le equazioni

$$a^2 - 30b^2 = \pm 2, \pm 3, \pm 5$$

sono prive di soluzioni (per riconoscerlo, ridurre modulo 3 o modulo 5). L'ideale PQ ha norma 6 ed è principale: $PQ = (6 + \sqrt{30})$. Invece l'ideale PR , che ha norma 10, non può essere principale perchè le equazioni

$$a^2 - 30b^2 = \pm 10$$

sono prive di soluzioni: $-10 \equiv 2 \pmod{6}$ non è un quadrato e l'equazione $a^2 + 2b^2 = 10$ non ha soluzioni in $(\mathbb{Z}/16\mathbb{Z})^2$. Dunque $C = \{\bar{A}, \bar{P}, \bar{R}, \bar{P}\bar{R}\} \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

2 Il gruppo delle unità

Per **unità** del campo di numeri K intendiamo l'insieme A^\times degli elementi invertibili nell'anello A degli interi di K . È un gruppo moltiplicativo.

Il risultato seguente permette di riconoscere le unità.

Proposizione 2.1. *le unità in K sono tutti e soli gli elementi di A di norma ± 1 .*

Dimostrazione: Per la moltiplicatività della norma, se $x \in A^\times$ allora $N(x) \in \mathbb{Z}^\times = \{\pm 1\}$.

Viceversa, un elemento $x \in A$ tale che $N(x) = \pm 1$ soddisfa una relazione polinomiale

$$x^n + a_1 x^{n-1} + \dots + a_{n-1} x \pm 1 = 0$$

a coefficienti in \mathbb{Z} . Ne segue che

$$\frac{1}{x} = \mp(x^{n-1} + a_1 x^{n-2} + \dots + a_{n-1}) \in \mathbb{Z}[x] \subseteq A.$$

■

La struttura di A^\times dipende dal tipo delle immersioni di K nel campo \mathbb{C} . Se n è il grado di K scriviamo $n = r_1 + 2r_2$ dove r_1 è il numero delle immersioni reali e r_2 è il numero delle immersioni complesse (a meno di coniugio) e poniamo

$$r = r_1 + r_2 - 1.$$

Denotiamo poi μ_K il gruppo delle radici di 1 in K .

Proposizione 2.2. $\mu(K)$ è un gruppo ciclico finito.

Dimostrazione: Se K possiede immersioni reali, l'asserto è ovvio perchè le sole radici di 1 reali sono ± 1 . Supponiamo $n = 2r_2$. Per ogni $x \in \mu_K$ e per ogni immersione $\sigma: K \hookrightarrow \mathbb{C}$ si ha $|\sigma(x)| = 1$. Dunque nell'immersione canonica di $\iota: K \hookrightarrow \mathbb{C}^{r_2}$ si ha

$$\iota(\mu_K) = \iota(A) \cap \underbrace{(S^1 \times \dots \times S^1)}_{r_2}.$$

Il primo insieme è discreto, il secondo è compatto. Infine, è ben noto che ogni gruppo finito del gruppo moltiplicativo di un campo è ciclico. ■

Vale il risultato seguente.

Teorema 2.3 (Dirichlet). Il gruppo delle unità A^\times è finitamente generato. Più precisamente $A^\times \simeq \mu_K \times \mathbb{Z}^r$.

Il teorema afferma che è possibile trovare $\epsilon_1, \dots, \epsilon_r \in A^\times$ tali che ogni $\epsilon \in A^\times$ si scrive in modo unico come

$$\epsilon = \mu \epsilon_1^{m_1} \dots \epsilon_r^{m_r}$$

dove $\mu \in \mu_K$ e $m_1, \dots, m_r \in \mathbb{Z}$. Un tale insieme $\{\epsilon_1, \dots, \epsilon_r\}$ si dice **sistema fondamentale di unità** per K .

Campi Quadratici Immaginari. Supponiamo ora $K = \mathbb{Q}(\sqrt{m})$ con $m < 0$ e privo di fattori quadrati. In questa situazione $r_1 = 0$, $r_2 = 0$ e dunque $r = 0$. Allora il gruppo delle unità è finito e

$$A^\times = \mu_K.$$

Si ha la seguente casistica:

- se $m = -1$, allora $|A^\times| = 4$,
- se $m = -3$, allora $|A^\times| = 6$,
- negli altri casi $|A^\times| = 2$.

Infatti, supponiamo dapprima $m \not\equiv 1 \pmod{4}$. Allora $A = \mathbb{Z}[\sqrt{m}]$ e la ricerca delle unità equivale a quella delle soluzioni intere dell'equazione

$$a^2 + |m|b^2 = 1.$$

Per $m < -1$ le uniche soluzioni sono $a = \pm 1, b = 0$, mentre per $m = -1$ si hanno le quattro soluzioni $a = \pm 1, b = 0$ e $a = 0$ e $b = \pm 1$. Se invece $m \equiv 1 \pmod{4}$, allora $A = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{m})]$ e la ricerca delle unità equivale a quella delle soluzioni intere dell'equazione

$$a^2 + |m|b^2 = 4.$$

Per $m = -3$ si hanno 6 soluzioni: $a = \pm 2, b = 0$ e $a = \pm 1$ e $b = \pm 1$. Per $m < -3$ si hanno solo le due soluzioni $a = \pm 2, b = 0$.

Campi Quadratici Reali. Supponiamo ora $K = \mathbb{Q}(\sqrt{m})$ con $m > 0$ e privo di fattori quadrati. In questa situazione $r_1 = 2$, $r_2 = 0$ e dunque $r = 1$. Siccome $\mu_K = \{\pm 1\}$, il gruppo delle unità si può scrivere

$$A^\times = \{\pm 1\} \times \epsilon^{\mathbb{Z}}$$

dove ϵ risulta canonicamente definito dalla condizione $\epsilon > 1$ e prende il nome di **unità fondamentale**.

Data una soluzione $(a, b) \in \mathbb{Z}^2$, $a, b > 0$ di una equazione

$$a^2 - mb^2 = \pm 1, \pm 4 \tag{2}$$

e posto $\eta = a + b\sqrt{m}$, le quattro soluzioni $(\pm a, \pm b)$ corrispondono a $\pm\eta, \pm 1/\eta$. È dunque chiaro che per l'unità fondamentale $\epsilon = a + b\sqrt{m}$ si ha $a > 0, b > 0$.

Lemma 2.4. *Sia $m \neq 5$ e sia $\eta = a + b\sqrt{m} \in A^\times$ con $a, b > 0$. Posto $\eta^n = a_n + b_n\sqrt{m}$, si ha $b_1 < b_2 < b_3 < \dots$*

Dimostrazione: Il risultato si dimostra facilmente per induzione distinguendo i casi $m \equiv 1$ e $m \not\equiv 1 \pmod{4}$. L'ipotesi $m \neq 5$ è necessaria in quanto $\left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{3+\sqrt{5}}{2}$. ■

Questo lemma permette di riconoscere immediatamente che l'unità fondamentale $\epsilon = a + b\sqrt{m}$ corrisponde alla soluzione positiva di (2) con b minimo. Allora per determinare l'unità fondamentale, basta controllare per $b = 1, 2, 3, \dots$ se $mb^2 \pm 1$ o ± 4 è un quadrato nel caso in cui $m \not\equiv 1 \pmod{4}$ o $m \equiv 1 \pmod{4}$ rispettivamente.

Ad esempio:

- $m = 11$, $A = \mathbb{Z}[\sqrt{11}]$. Per $b = 1$ e 2 nessuno dei quattro valori $11b^2 \pm 1$ è un quadrato. Invece $11 \cdot 3^2 + 1 = 100 = 10^2$ e dunque l'unità fondamentale è

$$\epsilon = 10 + 3\sqrt{11}.$$

- $m = 17$, $A = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{17})]$. I valori 17 ± 4 non sono quadrati, però $17 \cdot 2^2 - 4 = 64 = 8^2$ e dunque l'unità fondamentale è

$$\epsilon = 8 + 2\sqrt{17}.$$

Infine, è facile rendersi conto che l'unità fondamentale in $A = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{5})]$ è proprio $\frac{1+\sqrt{5}}{2}$.