# Forme quadratiche binarie

Carmelo Antonio Finocchiaro

**Notazioni e terminologia**
Nel corso di queste note, con il termine *anello* si intenderà sempre un anello commutativo con unità.
Il gruppo degli elementi invertibili di un anello $A$ si indicherà con $U(A)$. Un *campo di numeri* sarà un'estensione finita di $\mathbb{Q}$.
Se $K$ è un campo di numeri di grado due su $\mathbb{Q}$ (diremo anche che $K$ è un *campo quadratico*) e $\alpha \in K$, denoteremo con $\alpha'$ il coniugato di $\alpha$ (ovvero l'altra radice del polinomio minimo di $\alpha$ su $\mathbb{Q}$). Se $\alpha \in \mathbb{Q}$, poniamo, per definizione, $\alpha' = \alpha$. Indicheremo la norma e la traccia di $\alpha$ su $\mathbb{Q}$ con $\mathrm{N}(\alpha)$ e $\mathrm{Tr}(\alpha)$, rispettivamente.
Se $A$ è un anello, $M$ un $A-$modulo, $x_1, \ldots, x_n \in M$, allora poniamo

$$< x_1, \ldots, x_n >_A := \left\{ \sum_{i=1}^{n} a_i x_i : a_1, \ldots, a_n \in A \right\}.$$

Se $A = \mathbb{Z}$ (e quindi $M$ è un gruppo abeliano) allora scriveremo $< x_1, \ldots, x_n >$ anziché $< x_1, \ldots, x_n >_{\mathbb{Z}}$.

# 1 Introduzione

Nel corso di queste note, affronteremo il problema della ricerca delle soluzioni intere di equazioni della forma

$$aX^2 + bXY + cY^2 = m, \tag{1}$$

dove $a, b, c, m \in \mathbb{Q}$. Il numero razionale $b^2 - 4ac$ si dice *discriminante dell'equazione* ( o anche *discriminante del polinomio* $aX^2 + bXY + cY^2$).

1.1 Esempio. Consideriamo l'equazione

$$X^2 - 2Y^2 = 7. \tag{2}$$

Osserviamo che le coppie $(\alpha_1, \beta_1) := (3, 1), (\alpha_1' \beta_1') := (5, 3)$ sono soluzioni intere dell'equazione (2). Inoltre è immediatamente visto che, per ogni soluzione intera $(x, y)$ della (2), è soluzione anche $(3x+4y, 2x+3y)$. Dunque, posto, per ogni $n \geq 2$, $(\alpha_{n+1}, \beta_{n+1}) := (3\alpha_n + 4\beta_n, 2\alpha_n + 3\beta_3)$, $(\alpha'_{n+1}, \beta'_{n+1}) := (3\alpha'_n + 4\beta'_n, 2\alpha'_n + 3\beta'_3)$, si ottiene una famiglia di soluzioni della (2). Si può mostrare ogni soluzione della (2) è della forma $(\alpha_n, \beta_n), (\alpha'_n, \beta'_n)$, per quanche $n \geq 1$.

1.2 Osservazione. Consideriamo un polinomio $f := aX^2 + bXY + cY^2 \in \mathbb{Q}[X, Y]$. Detto $D := b^2 - 4ac$ il discriminante del polinomio $f$, è immediatamente visto che $f$ si fattorizza in $\mathbb{Q}(\sqrt{D})[X, Y]$ nel seguente modo

$$f = \left(X + \frac{b + \sqrt{D}}{2a} Y\right) \left(aX + \frac{b - \sqrt{D}}{2} Y\right). \tag{3}$$

(a) Se $D$ è il quadrato di un numero razionale, i fattori di $f$ scritti sopra sono a coeffienti razionali, e quindi la ricerca delle soluzioni dell'equazione $f(X, Y) = m$ $(m \in \mathbb{Q})$ si riconduce facilmente alla teoria delle Equazioni Diofantee lineari.

(b) Supponiamo adesso che $D$ non sia il quadrato di alcun numero razionale. Pertanto esistono, e sono univocamente determinati da $D$, un numero razionale positivo $s$ e un numero intero $d$ distinto da 1 privo di fattori quadratici tale che $D = s^2 d$. Quindi si ha

$$f = \frac{1}{a} \left(aX + \frac{b + s\sqrt{d}}{2} Y\right) \left(aX + \frac{b - s\sqrt{d}}{2} Y\right). \tag{4}$$

Si osservi che, in questo caso gli elementi $\alpha := a, \beta := \dfrac{b + s\sqrt{d}}{2}$ sono linearmente indipendenti su $\mathbb{Q}$.

Introduciamo adesso uno strumento algebrico che avrà un ruolo centrale nella teoria che esporremo.

1.3 Definizione. *Siano $K$ un campo numerico e $\mathcal{B}$ una base di $K$ su $\mathbb{Q}$. Il sottogruppo additivo di $K$ generato (liberamente) dall'insieme $\mathcal{B}$ si dice* modulo *di $K$.*

Siano $K$ un campo di numeri e $M$ un modulo di $K$. Allora, per definizione, esiste una base $\{\alpha_1, \ldots, \alpha_n\}$ di $K$ su $\mathbb{Q}$ tale che

$$M =< \alpha_1, \ldots, \alpha_n >= \left\{ \sum_{i=1}^{n} m_i \alpha_i : m_1, \ldots, m_n \in \mathbb{Z} \right\}.$$

1.4 Esempio. Sia $f := aX^2 + bXY + cY^2 \in \mathbb{Q}[X, Y]$. Se il discriminante di $f$ non è il quadrato di alcun numero razionale e $d$ è il numero intero considerato in (1.2(b)), allora, per quanto visto in (1.2(b)), è possibile associare al polinomio $f$ il modulo $M =< \alpha, \beta >$ di $\mathbb{Q}(\sqrt{d})$, con $\alpha := a, \beta := \dfrac{b + s\sqrt{d}}{2}$.

L'importanza dei moduli per la ricerca delle soluzioni intere delle equazioni da noi considerate è data dal seguente semplice risultato.

1.5 Proposizione. *Si consideri l'equazione $aX^2 + bXY + cY^2 = m$, con $a, b, c, m \in \mathbb{Q}$, e sia $D$ il discriminante. Assumiamo che $D$ non sia il quadrato di alcun numero razionale, e sia $D = s^2 d$, dove $s$ è un numero razionale positivo e $d$ è un intero privo di fattori quadratici. Siano inoltre $\alpha, \beta$ come in (1.2(b)). Considerato il modulo $M :=< \alpha, \beta >$ di $\mathbb{Q}(\sqrt{d})$, allora $(x, y)$ è soluzione intera dell'equazione $aX^2 + bXY + cY^2 = m$ se e soltanto se $x\alpha + y\beta \in M$ e $\mathrm{N}(x\alpha + y\beta) = am$.*

Dimostrazione. La condizione $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ equivale a $x\alpha + y\beta \in M$, poiché $\alpha, \beta$ sono linearmente indipendenti su $\mathbb{Q}$. Inoltre si ha $\beta' = \dfrac{b - s\sqrt{d}}{2}$ e quindi, per (1.2(b)), $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ è soluzione dell'equazione $aX^2 + bXY + cY^2 = m$ se e soltanto se $x\alpha + y\beta \in M$ e $m = \dfrac{1}{a}\mathrm{N}(\alpha x + \beta y)$. □

# 2 Moduli di campi numerici

Per (1.5), la nozione di modulo è centrale nella ricerca delle soluzioni intere di equazioni del tipo (1), in quanto tali soluzioni corrispondono agli elementi del modulo associato all'equazione che hanno una fissata norma.
Esporremo adesso alcune proprietà di base per i moduli di campi numerici. Ricordiamo alcuni fatti preliminari di Teoria dei Campi.

2.1 Definizione. *Sia $L/K$ un'estensione di campi finita e sia $\mathcal{B} := \{x_1, \ldots, x_n\}$ una base di $L$ su $K$. Diremo* discriminante della base $\mathcal{B}$*, e lo indicheremo*

*con $D(\mathcal{B})$, il determinante della matrice di elemento generico* $\mathrm{Tr}_{L/K}(x_i x_j)$, $i, j \in \{1, \ldots, n\}$.

Ricordiamo il seguente risultato di base sui discriminanti.

2.2 Teorema. *Siano $L/K$ un'estensione finita di campi, e $\mathcal{B} := \{x_1, \ldots, x_n\}$ una base di $L$ su $K$. Allora valgono le seguenti asserzioni.*

(a) *Il discriminante $D(\mathcal{B})$ è un elemento di $K$.*

(b) *Se $\mathcal{C} := \{y_1, \ldots, y_n\}$ è una base di $L$ su $K$, e $C := (c_{ij})$ è la matrice di passaggio dalla base $\mathcal{B}$ alla base $\mathcal{C}$ (ovvero $y_i = \sum_{j=1}^{n} c_{ij} x_j$, $i = 1, \ldots, n$), si ha $D(\mathcal{C}) = (\det C)^2 D(\mathcal{B})$.*

(c) *Se $L/K$ è un'estensione di campi separabile, allora $D(\mathcal{B}) \neq 0$.*

2.3 Corollario. *Siano $K$ un campo di numeri e $\mathcal{B} := \{x_1, \ldots, x_n\}$ una sua base intera. Allora $D(\mathcal{B}) \in \mathbb{Z}$.*

Dimostrazione. Poiché $x_1, \ldots, x_n$ sono interi su $\mathbb{Z}$, allora è intero su $\mathbb{Z}$ anche il discriminante di $\mathcal{B}$. Dunque, per (2.2(a)), si ha $D(\mathcal{B}) \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$. □.

2.4 Proposizione. *Siano $K$ un campo di numeri, $\mathcal{B} := \{x_1, \ldots, x_n\}$, $\mathcal{C} := \{y_1, \ldots, y_n\}$ due basi di $K$ su $\mathbb{Q}$, e consideriamo i moduli $M :=< x_1, \ldots, x_n >$, $N :=< y_1, \ldots, y_n >$ di $K$. Allora $M = N$ se e soltanto la matrice di passaggio dalla base $\mathcal{B}$ alla base $\mathcal{C}$ appartiene a* $\mathrm{GL}_n(\mathbb{Z})$.

Dimostrazione. Se $M = N$, basta tenere presente che le matrici del cambiamento di base sono a coefficienti interi e che il loro prodotto è la matrice identica. Viceversa, sia $\mathbf{x} := (x_1, \ldots, x_n)^t$, $\mathbf{y} := (y_1, \ldots, y_n)^t$. Allora $\mathbf{y} = C\mathbf{x}$, per qualche matrice $C \in \mathrm{GL}_n(\mathbb{Z})$. Allora è immediatamente visto che $x_1, \ldots, x_n \in N$, e quindi $M \subseteq N$. Viceversa, si ha $\mathbf{y} = C^{-1}\mathbf{x}$. Poiché, ovviamente, $C^{-1} \in \mathrm{GL}_n(\mathbb{Z})$, si ha analogamente $N \subseteq M$. □

2.5 Corollario. *Siano $K$ un campo di numeri $M$ un modulo di $K$. Se $\mathcal{B}$ e $\mathcal{C}$ sono basi di $K$ su $\mathbb{Q}$ tali che $M =< \mathcal{B} >=< \mathcal{C} >$, allora $(D(\mathcal{B})) = (D(\mathcal{C}))$.*

Dimostrazione. Basta applicare (2.2(b)), e tenere presente (2.5). □

Quanto appena visto, ci permette di dare la seguente definizione.

2.6 Definizione. *Siano $K$ un campo di numeri e $M$ un modulo di $K$. Detta $\mathcal{B}$ una base di $K$ su $\mathbb{Q}$ tale che $< \mathcal{B} >= M$, diremo* discriminante del modulo $M$ *il numero razionale $\Delta(M) := D(\mathcal{B})$.*

2.7 Osservazione. Siano $K$ un campo di numeri e $M$ un modulo di $K$. Da (2.3) segue subito che, se $\mathcal{B}$ è una base intera di $K$ su $\mathbb{Q}$ tale che $M =< \mathcal{B} >$, allora $\Delta(M) \in \mathbb{Z}$.

Ricordiamo il seguente risultato di Algebra Commutativa, di immediata verifica.

2.8 Proposizione. *Sia $L/F$ un'estensione di campi, $A$ un sottoanello di $L$ il cui campo dei quozienti sia $F$. Allora, se $\alpha \in L$ è algebrico su $F$, esiste un elemento non nullo $a \in A$ tale che $a\alpha$ è intero su $A$.*

2.9 Corollario. *Siano $K$ un campo di numeri e $\alpha \in K$. Allora esiste un numero intero $d \neq 0$ tale che $\alpha d \in \mathcal{O}_K$.*

Dimostrazione. Basta applicare (2.8) ($A = \mathbb{Z}$, $F = \mathbb{Q}$, $L = K$). □

Possiamo adesso dimostrare una importante caratterizzazione dei moduli di un campo di numeri.

2.10 Teorema. *Siano $K$ un campo di numeri e $M$ un sottoinsieme di $K$. Allora le seguenti condizioni sono equivalenti.*

(i) *$M$ è un modulo di $K$.*

(ii) *$M$ è un sottogruppo additivo di $K$ che contiene una base di $K$ su $\mathbb{Q}$, e inoltre esiste un intero $k \neq 0$ tale che $kM \subseteq \mathcal{O}_K$.*

Dimostrazione. (i)$\Longrightarrow$(ii). Supponiamo che $M$ sia un modulo di $K$, e sia $\mathcal{B} := \{x_1, \ldots, x_n\}$ una base di $K$ su $\mathbb{Q}$ tale che $< \mathcal{B} >= M$. Stante (2.9), per ogni $i \in \{1, \ldots, n\}$, esiste un intero $m_i \neq 0$ tale che $m_i x_i \in \mathcal{O}_K$. Allora, posto $k := \prod_{i=1}^{n} m_i$, si ha $kM = k < \mathcal{B} >\subseteq \mathcal{O}_K$, come è immediatamente visto ricordando che $\mathcal{O}_K$ è un sottoanello di $K$ contenente $\mathbb{Z}$. Questo basta per provare la condizione (ii).
(ii)$\Longrightarrow$ (i). Supponiamo che $M$ soddisfi la condizione (ii). Fissata una base $\mathcal{C} := \{z_1, \ldots, z_n\}$ contenuta in $M$, si ha immediatamente $\{kz_i : i = 1, \ldots, n\} \subseteq M \cap \mathcal{O}_K$, essendo $M$ un sottogruppo additivo di $K$ e $kM \subseteq \mathcal{O}_K$. Inoltre, è subito visto che l'insieme $\{kz_i : i = 1, \ldots, n\}$ è una base di $K$ su $\mathbb{Q}$,

e quindi $D(\{kz_1,\ldots,kz_n\})$ è un numero intero non nullo, in virtù di (2.2(c)) e (2.3). Inoltre, poiché $\mathrm{Tr}(kz_ikz_j) = k^2\mathrm{Tr}(z_iz_j)$, per ogni $i,j \in \{1,\ldots,n\}$, si ha $D(\{kz_1,\ldots,kz_n\}) = k^{2n}D(\mathcal{C})$. Quindi, per ogni base $\mathcal{C}$ di $K$ su $\mathbb{Q}$ contenuta in $M$, il denominatore del numero razionale non nullo $D(\mathcal{C})$ (cf. (2.2(a,c))) è un divisore di $k^{2n}$. Inoltre, per ipotesi, esiste una base $\mathcal{B}$ di $K$ su $\mathbb{Q}$ contenuta in $M$. Dunque l'insieme

$$\{|D(\mathcal{C})| : \mathcal{C} \text{ base di } K \text{ su } \mathbb{Q}, \mathcal{C} \subseteq M, |D(\mathcal{C})| \leq |D(\mathcal{B})|\}$$

è finito e non vuoto (contiene $|D(\mathcal{B})|$), e pertanto esiste una base $\mathcal{C}^* := \{\alpha_1,\ldots,\alpha_n\}$ di $K$ su $\mathbb{Q}$ contenuta in $M$ tale che $|D(\mathcal{C}^*)|$ è minimo. Sarà sufficiente mostrare che $< \mathcal{C}^* >= M$. L'inclusione $< \mathcal{C}^* > \subseteq M$ è evidente, essendo $M$ un sottogruppo additivo di $K$. Viceversa, supponiamo, per assurdo, che esista un elemento $\gamma \in M \setminus < \mathcal{C}^* >$. Allora esistono, univocamente determinati, numeri razionali $x_1,\ldots,x_n$, non tutti interi, tali che $\gamma = \sum_{i=1}^n x_i\alpha_i$. Possiamo assumere che $x_1 \notin \mathbb{Z}$. Dunque, esistono un numero intero $y_1$ e un numero razionale $y_2$ strettamente compreso fra 0 e 1 tali che $x_1 = y_1 + y_2$. Posto $\alpha_1^* := \gamma - y_1\alpha_1$, $\alpha_j^* := \alpha_j$, per $j \in \{2,\ldots,n\}$, si verifica immediatamente che l'insieme $\mathcal{E} := \{\alpha_1^*,\ldots,\alpha_n^*\}$ è una base di $K$ su $\mathbb{Q}$ contenuta in $M$ (si osservi che, essendo $M$ un sottogruppo additivo di $K$, si ha $\alpha_1^* = \gamma - y_1\alpha_1 \in M$). Inoltre, posto

$$C := \begin{pmatrix} y_2 & x_2 & \ldots & x_n \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix},$$

si ha immediatamente $(\alpha_1^*,\ldots,\alpha_n^*)^t = C(\alpha_1,\ldots,\alpha_n)^t$. Dunque, per (2.2(b)), si ha $|D(\mathcal{E})| = (\det C)^2|D(\mathcal{C}^*)| = y_2^2|D(\mathcal{C}^*)| < |D(\mathcal{C}^*)|(\leq |D(\mathcal{B})|)$, una contraddizione. Questo completa la dimostrazione. □

2.11 Definizione. *Siano $K$ un campo di numeri e $M$ un modulo di $K$. Allora l'insieme*

$$\mathcal{O}_M := \{x \in K : xM \subseteq M\}$$

*si dice* l'anello dei coeffienti di $M$.

2.12 Osservazione. Siano $K$ un campo di numeri e $M$ un modulo di $K$.

(a) Si verifica immediatamente che $\mathcal{O}_M$ è un anello contenente $\mathbb{Z}$ come sottoanello.

(b) Se $\alpha \in M$ e $\epsilon$ è un elemento di $\mathscr{O}_M$ di norma 1, allora $\epsilon\alpha \in M$, per definizione, e inoltre $\mathrm{N}(\epsilon\alpha) = \mathrm{N}(\alpha)$.

2.13 Proposizione. *Siano $K$ un campo di numeri e $M$ un modulo di $K$. Allora $\mathscr{O}_M$ è un sottoanello di $\mathcal{O}_K$.*

Dimostrazione. Fissiamo $x \in \mathscr{O}_M$, e sia $\{\alpha_1, \ldots, \alpha_n\}$ una base di $K$ su $\mathbb{Q}$ tale che $< \alpha_1, \ldots, \alpha_n >= M$. Allora, per definizione, $x\alpha_i \in M$, per ogni $i \in \{1, \ldots, n\}$. Esistono allora interi $m_{ij}$, $i, j \in \{1, \ldots, n\}$ tali che $x\alpha_i = \sum_{j=1}^{n} m_{ij}\alpha_j$. Segue immediatamente che $(\alpha_1, \ldots, \alpha_n)$ è una soluzione non nulla del sistema lineare omogeneo

$$(x - m_{ii})Y_i + \sum_{j \neq i} m_{ij}Y_j = 0 \qquad i = 1, \ldots, n,$$

e pertanto la matrice dei coefficienti di questo sistema deve avere determinante nullo. Allora è evidente che lo sviluppo di tale determinante fornisce un'equazione di dipendenza integrale di $x$ su $\mathbb{Z}$. □

2.14 Proposizione. *Siano $K$ un campo di numeri, $x \in K$, $M$ un modulo di $K$, e $\{\alpha_1, \ldots, \alpha_n\}$ una base di $K$ su $\mathbb{Q}$ tale che $M =< \alpha_1, \ldots, \alpha_n >$. Allora $x \in \mathscr{O}_M$ se e soltanto se $x\alpha_i \in M$, per ogni $i \in \{1, \ldots, n\}$.*

Dimostrazione. Per definizione, se $x \in \mathscr{O}_M$, allora $x\alpha_i \in M$, per ogni $i = 1, \ldots, n$. Viceversa, supponiamo che $x\alpha_1, \ldots, x\alpha_n \in M$, e fissiamo un elemento $\gamma \in M$. Per definizione, $\gamma = \sum_{i=1}^{n} m_i\alpha_i$, per opportuni $m_1, \ldots, m_n \in \mathbb{Z}$. Dunque, si ha $x\gamma = \sum_{i=1}^{n} m_i(x\alpha_i) \in M$, essendo $M$ un sottogruppo additivo di $K$. Quindi $x \in \mathscr{O}_M$. □

2.15 Proposizione. *Siano $K$ un campo di numeri, $M$ un modulo di $K$, $x \in K$. Allora esiste un numero naturale non nullo $n$ tale che $nx \in \mathscr{O}_M$.*

Dimostrazione. Fissiamo una base $\{\alpha_1, \ldots, \alpha_n\}$ di $K$ su $\mathbb{Q}$ tale che $M =< \alpha_1, \ldots, \alpha_n >$. Allora esistono numeri razionali $r_{ij}$, $i, j \in \{1, \ldots, n\}$ tali che $x\alpha_i = \sum_{j=1}^{n} r_{ij}\alpha_j$, per ogni $i = 1, \ldots, n$. Se $n$ è un denominatore comune alle frazioni $r_{ij}$, $i, j \in \{1, \ldots, n\}$, allora $(nx)\alpha_i \in M$, per ogni $i = 1, \ldots, n$. Per concludere la dimostrazione, basta quindi applicare (2.14). □

2.16 Corollario. *Siano $K$ un campo di numeri e $M$ un modulo di $K$. Allora $\mathscr{O}_M$ è un modulo di $K$.*

DIMOSTRAZIONE. $\mathscr{O}_K$ è ovviamente un sottogruppo additivo di $K$. Inoltre, se $\{\alpha_1, \ldots, \alpha_n\}$ è una base di $K$ su $\mathbb{Q}$, allora esistono numeri naturali $m_1, \ldots, m_n$ non nulli tali che $m_1\alpha_1, \ldots, m_n\alpha_n \in \mathscr{O}_M$, stante (2.15), ed è subito visto che $\{m_1\alpha_1, \ldots, m_n\alpha_n\}$ è una base di $K$ su $\mathbb{Q}$. Inoltre $\mathscr{O}_M$ è un sottoanello di $\mathcal{O}_K$, in virtù di (2.13). Allora, per concludere la dimostrazione basta applicare (2.10). □

2.17 DEFINIZIONE. *Sia $K$ un campo di numeri. Un sottoinsieme di $K$ si dice* ordine di $K$ *se è simultaneamente un anello e un modulo di $K$.*

2.18 ESEMPIO. Stante (2.16), l'anello dei coefficienti di un modulo di un campo numerico $K$ è un ordine di $K$.

2.19 PROPOSIZIONE. *Siano $K$ un campo di numeri e $A$ un sottoinsieme di $K$. Allora le seguenti condizioni sono equivalenti.*

(i) *$A$ è un ordine di $K$.*

(ii) *Esiste un modulo di $K$ il cui anello dei coefficienti è $A$.*

*Se valgono le precedenti condizioni, si ha $\mathscr{O}_A = A$.*

DIMOSTRAZIONE. (ii)$\Longrightarrow$(i) è una conseguenza immediata di (2.16) (o di (2.18)).
(i)$\Longrightarrow$(ii). Essendo, in particolare, $A$ un modulo, l'insieme $\mathscr{O}_A$ è un anello, e pertanto basterà dimostrare che $\mathscr{O}_A = A$. Ma questo è ovvio, perché $x \in A$ se e soltanto se $xA \subseteq A$ (si tenga presente che $1 \in A$). Questo conclude la dimostrazione. □

2.20 ESEMPIO. Sia $d$ un intero privo di fattori quadratici. Consideriamo il modulo $M =: < 1, \sqrt{d} >$ di $\mathbb{Q}(\sqrt{d})$. Allora è immediatamente visto che $M$ è anche un sottoanello di $\mathbb{Q}(\sqrt{d})$, ovvero un ordine di $\mathbb{Q}(\sqrt{d})$. Allora $\mathscr{O}_M = M$, in virtù di (2.19).

2.21 DEFINIZIONE. *Siano $K$ un campo di numeri e $M, N$ moduli di $K$. Si dice che $M, N$ sono* simili *se esiste un elemento $\alpha \in K$ non nullo tale che $M = \alpha N$.*

L'importanza della precedente definizione è data dal seguente semplice e utile risultato.

2.22 Proposizione. *Siano $K$ un campo di numeri e $M, N$ moduli di $K$ simili. Allora $\mathscr{O}_M = \mathscr{O}_N$.*

Dimostrazione. Per ipotesi, esiste un elemento non nullo $\alpha \in K$ tale che $M = \alpha N$. Se $x \in \mathscr{O}_N$, allora $xN \subseteq N$, e si ha $xM = x\alpha N \subseteq \alpha N = M$. Dunque $x \in \mathscr{O}_M$. Questo prova che $\mathscr{O}_N \subseteq \mathscr{O}_M$. Viceversa, basta osservare che $N = \alpha^{-1}M$ e usare il precedente argomento, scambiando i ruoli di $N$ e $M$. □

# 3 Moduli su campi quadratici

In virtù di (1.5), si rivela cruciale lo studio dei moduli dei campi quadratici e dei loro anelli dei coeffienti. Ricordiamo il seguente risultato ben noto.

3.1 Teorema. *Siano $d$ un intero privo di fattori quadratici e $K := \mathbb{Q}(\sqrt{d})$. Allora $\mathcal{O}_K =< 1, \omega_d >$, dove*

$$\omega_d := \begin{cases} \sqrt{d} & \text{se } d = 2, 3 (\text{mod } 4) \\ \dfrac{1+\sqrt{d}}{2} & \text{se } d = 1 (\text{mod } 4) \end{cases}$$

Il prossimo risultato descrive i possibili anelli dei coefficienti dei moduli di un campo quadratico.

3.2 Teorema. *Siano $d$ un intero privo di fattori quadratici, $M$ un modulo di $\mathbb{Q}(\sqrt{d})$ e $\omega_d$ come in (3.1). Allora esiste un numero naturale $\mathscr{L}$ tale che $\mathscr{O}_M =< 1, \mathscr{L}\omega_d >$. Si può scegliere $\mathscr{L}$ come il più piccolo numero naturale non nullo tale che $\mathscr{L}\omega_d \in \mathscr{O}_M$.*

Dimostrazione. In virtù di (2.15), l'insieme $\{n \in \mathbb{N}\backslash\{0\} : n\omega_d \in \mathscr{O}_M\}$ è non vuoto, e quindi ha minimo $\mathscr{L}$. Poiché, in particolare, $1 \in \mathscr{O}_M$, si ha immediatamente $< 1, \mathscr{L}\omega_d > \subseteq \mathscr{O}_M$. Sia adesso $\gamma \in \mathscr{O}_M$. Poiché, stante (2.13), $\mathscr{O}_M$ è un sottoanello di $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, esistono $s, t \in \mathbb{Z}$ tali che $\gamma = s + t\omega_d$ (cf. (3.1)). Possiamo scegliere adesso numeri interi $q, r$ tali che $t = q\mathscr{L} + r$, con $0 \leq r < \mathscr{L}$. Poiché $s \in \mathbb{Z} \subseteq \mathscr{O}_M$, segue subito $\gamma - s = t\omega_d \in \mathscr{O}_M$, Poiché, inoltre, $q\mathscr{L}\omega_d \in \mathscr{O}_M$, si ha $t\omega_d - q\mathscr{L}\omega_d = r\omega_d \in \mathscr{O}_M$. Dunque, per come è stato scelto $\mathscr{L}$, si deve avere $r = 0$, e quindi $\gamma = s + q\mathscr{L}\omega_d \in < 1, \mathscr{L}\omega_d >$. Questo completa la dimostrazione. □

3.3 Corollario. *Siano $d$ e $\omega_d$ come in (3.1), $A$ un sottoinsieme di $\mathbb{Q}(\sqrt{d})$. Allora le seguenti condizioni sono equivalenti.*

(i) *$A$ è un ordine di $\mathbb{Q}(\sqrt{d})$.*

(ii) *Esiste un intero $\mathscr{L} > 0$ tale che $A = {}^{\mathscr{L}}\mathscr{O} :=< 1, \mathscr{L}\omega_d >$.*

*In particolare, tutti e soli gli anelli dei coefficienti di moduli di $\mathbb{Q}(\sqrt{d})$ sono della forma $< 1, \mathscr{L}\omega_d >$, con $\mathscr{L} \in \mathbb{N}\backslash\{0\}$.*

Dimostrazione. (i)$\Longrightarrow$(ii). Basta applicare (2.19) e (3.2).
(ii)$\Longrightarrow$(i). Sia $\mathscr{L} \in \mathbb{N}\backslash\{0\}$. Allora ${}^{\mathscr{L}}\mathscr{O}$ è ovviamente un modulo di $\mathbb{Q}(\sqrt{d})$, perché $\{1, \mathscr{L}\omega_d\}$ è una base di $\mathbb{Q}(\sqrt{d})$ su $\mathbb{Q}$. Inoltre è subito visto che ${}^{\mathscr{L}}\mathscr{O}$ è un sottoanello di $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Questo completa la dimostrazione. □

3.4 Osservazione. Siano $K$ un campo quadratico, $\{\alpha, \beta\}$ una base di $K$ su $\mathbb{Q}$. Si vede immediatamente che $\alpha \neq 0$ e che, posto $\gamma := \beta/\alpha$, $\{1, \gamma\}$ è una base di $K$ su $\mathbb{Q}$. Dunque $\gamma$ ha necessariamente grado due su $\mathbb{Q}$, e quindi esiste un unico polinomio $a_\gamma X^2 - bX + c \in \mathbb{Z}[X]$, con $a_\gamma, b, c$ privi di fattori in comune distinti da 1, che si annulla in $\gamma$.

3.5 Lemma. *Siano $K$ un campo quadratico e $\{1, \gamma\}$ una base di $K$ su $\mathbb{Q}$. Allora, considerato il modulo $M :=< 1, \gamma >$ di $K$, si ha $\mathscr{O}_M =< 1, a_\gamma\gamma >$, dove $a_\gamma$ è il numero intero considerato in (3.4).*

Dimostrazione. Fissiamo un elemento $\eta \in K$. Per definizione, esistono, e sono unici, $x, y \in \mathbb{Q}$ tali che $\eta = x + y\gamma$. In virtù di (2.14), $\eta \in \mathscr{O}_M$ se e soltanto se $\eta, \eta\gamma \in M$. Con le notazioni di (3.4), si ha immediatamente $\gamma^2 = \dfrac{b\gamma - c}{a}$. Quindi $\eta, \eta\gamma$ appartengono a $M$ se e soltanto se $x, y \in \mathbb{Z}$ e $\eta\gamma = \left(x + \dfrac{b}{a_\gamma}y\right)\gamma - \dfrac{c}{a_\gamma}y \in M$, ovvero se e soltanto se $x, y, \dfrac{b}{a_\gamma}y, \dfrac{c}{a_\gamma}y \in \mathbb{Z}$. Poiché $a_\gamma, b, c$ non hanno fattori comuni distinti da 1, le precedenti condizioni equivalgono a $x, y \in \mathbb{Z}$ e $a_\gamma$ divide $y$. L'asserto segue immediatamente. □

Nel prossimo risultato determineremo l'anello dei coefficienti del modulo associato a un polinomio $f := aX^2 - bXY + cY^2 \in \mathbb{Z}[X, Y]$ (cf. (1.4)), dove $a, b, c$ non hanno fattori in comune distinti da 1 e il discriminante di $f$ non sia un quadrato.

3.6 Teorema. *Si consideri il polinomio* $f := aX^2 - bXY + cY^2 \in \mathbb{Z}[X,Y]$, *con* $a, b, c$ *numeri interi privi di fattori comuni distinti da* 1 *e tali che il discriminante* $D := b^2 - 4ac$ *di* $f$ *non sia il quadrato di un numero intero. Sia* $d$ *un numero intero privo di fattori quadratici e* $\mathscr{L}$ *un numero naturale non nullo tali che* $D = \mathscr{L}^2 d$. *Allora, considerato il modulo* $M :=< a, \frac{b + \mathscr{L}\sqrt{d}}{2} >$ *associato a* $f$, *si ha*

$$\mathscr{O}_M = \begin{cases} < 1, \frac{\mathscr{L}}{2}\omega_d > & \text{se } d = 2, 3 (\text{mod } 4) \\ < 1, \mathscr{L}\omega_d > & \text{se } d = 1 (\text{mod } 4) \end{cases},$$

*dove* $\omega_d$ *è il numero definito in (3.1).*

Dimostrazione. Poniamo $\alpha := \frac{b + \mathscr{L}\sqrt{d}}{2a}$ e consideriamo il modulo $M_1 :=< 1, \alpha >$ di $\mathbb{Q}(\sqrt{d})$. Allora i moduli $M, M_1$ sono simili, ovviamente, e quindi, a norma di (2.22) e (3.5), si ha $\mathscr{O}_M = \mathscr{O}_{M_1} =< 1, a\alpha >=< 1, \frac{b + \mathscr{L}\sqrt{d}}{2} >$ (si osservi che $\alpha$ è radice di del polinomio $aX^2 + bX + c$). Si ha

$$\mathscr{L}^2 d = b^2 - 4ac = b^2 (\text{mod } 4). \tag{5}$$

Se $d = 3 (\text{mod } 4)$, allora $b^2 + \mathscr{L}^2 = 0 (\text{mod } 4)$, e quindi $b^2 = \mathscr{L}^2 = 0 (\text{mod } 4)$, poiché $x^2 = 0, 1 (\text{mod } 4)$, per ogni $x \in \mathbb{Z}$. Dunque $b, \mathscr{L}$ sono numeri pari. Se $d = 2 (\text{mod } 4)$, allora da (5) segue immediatamente che $2\mathscr{L}^2 = b^2 (\text{mod } 4)$, e, in particolare, $b, \mathscr{L}$ sono pari. Resta così provato che, se $d = 2, 3 (\text{mod } 4)$, allora $b, \mathscr{L}$ sono pari. Dunque $\frac{b + \mathscr{L}\sqrt{d}}{2} \in < 1, \frac{\mathscr{L}}{2}\omega_d >$, e quindi $\mathscr{O}_M \subseteq < 1, \frac{\mathscr{L}}{2}\omega_d >$. L'altra inclusione è immediata. Dunque $\mathscr{O}_M =< 1, \frac{\mathscr{L}}{2}\omega_d >$ se $d = 2, 3 (\text{mod } 4)$.
Se $d = 1 (\text{mod } 4)$, allora da (5) segue che $\mathscr{L}^2 = b^2 (\text{mod } 4)$. Poiché $\mathscr{L}^2 - b^2$ è, in particolare, pari, si ha che $\mathscr{L}, b$ sono o entrambi pari o entrambi dispari, e quindi $\frac{b - \mathscr{L}}{2} \in \mathbb{Z}$. Dunque $\frac{d + \mathscr{L}\sqrt{d}}{2} = \frac{b - \mathscr{L}}{2} + \mathscr{L}\omega_d$. Questo prova che $\mathscr{O}_M =< 1, \mathscr{L}\omega_d >$, se $d = 1 (\text{mod } 4)$. □

3.7 Osservazione. In virtù di (1.5), il problema di determinare le soluzioni intere di un'equazione quadratica $aX^2 - bXY + cY^2 = m$ e equivalente a trovare gli elementi di un opportuno modulo $M$ di un opportuno campo

quadratico $K$ la cui norma è un numero intero fissato. Osserviamo che, stante (2.12(b)), a partire da un elemento $\alpha$ di $M$ di norma fissata, allora tutti gli elementi della forma $\epsilon\alpha$, dove $\epsilon \in \mathscr{O}_M$ ha norma 1, appartengono a $M$ e hanno la stessa norma di $\alpha$.

In virtù di (3.7), per risolvere il problema della determinazione delle soluzioni intere di equazioni della forma (1) è cruciale determinare tutti gli elementi di norma 1 dell'anello dei coefficienti di un modulo.

3.8 Lemma. *Siano $K$ un campo di numeri e $A$ un sottoanello di $\mathcal{O}_K$. Allora si ha $\mathrm{N}(\alpha)\alpha^{-1} \in A$, per ogni $\alpha \in A\backslash\{0\}$.*

Dimostrazione. Per ipotesi, esistono elementi $c_0, \ldots, c_{n-1} \in \mathbb{Z}$ $(n \geq 1)$ tali che $\alpha^n + c_{n-1}\alpha^{n-1} + \ldots + c_0 = 0$. Allora, come è bene noto, si ha $\mathrm{N}(\alpha) = \pm c_0$. Allora $\pm\mathrm{N}(\alpha)\alpha^{-1} = \alpha^{n-1} + c_{n-1}\alpha^{n-2} + c_1 \in A$, essendo $A$ un anello. □

3.9 Proposizione. *Siano $K$ un campo di numeri, $A$ un sottoanello di $\mathcal{O}_K$ e $\epsilon \in A$. Allora Allora $\epsilon$ è invertibile in $A$ se e soltanto se $\mathrm{N}(\epsilon) = \pm 1$. In particolare, se $M$ un modulo di $K$, allora $U(\mathscr{O}_M) = \{\epsilon \in \mathscr{O}_M : \mathrm{N}(\epsilon) = \pm 1\}$.*

Dimostrazione. Sia $\epsilon$ un elemento invertibile di $A$. Allora, poiché $\epsilon^{-1} \in A$, si ha $\mathrm{N}(\epsilon), \mathrm{N}(\epsilon^{-1}) \in \mathbb{Z}$. Poiché, inoltre, $\mathrm{N}(\epsilon)\mathrm{N}(\epsilon^{-1}) = 1$, segue immediatamente $\mathrm{N}(\epsilon) = \pm 1$.
Viceversa, sia $\epsilon$ un elemento di $A$ tale che $\mathrm{N}(\epsilon) = \pm 1$. Allora $\pm\epsilon^{-1} \in A$, stante (3.8). Dunque $\epsilon \in U(A)$. L'ultima parte dell'asserzione è una conseguenza immediata di (2.13). □

La precedente caratterizzazione ci permette si spostare il problema nella determinazione di alcuni elementi invertibili (quelli di norma 1) dell'anello dei coefficienti di un modulo. Ovviamente, restringeremo la nostra indagine ai moduli sui campi quadratici. A norma di (3.3), sarà sufficiente determinare gli invertibili degli anelli della forma ${}^{\mathscr{L}}\mathscr{O} :=< 1, \mathscr{L}\omega_d >$, dove $d, \omega_d$ sono come in (3.1) e $\mathscr{L}$ è un intero positivo.

3.10 Proposizione. *Preserviamo le notazioni di (3.3) e (3.1), e siano $x, y \in \mathbb{Z}$. Allora l'elemento $x + y\mathscr{L}\omega_d$ è invertibile in ${}^{\mathscr{L}}\mathscr{O}$ se e soltanto se $x^2 - \mathscr{L}^2 d y^2 = \pm 1$, quando $d = 2, 3 (\mathrm{mod}\ 4)$, oppure se $x^2 + \mathscr{L}xy + \dfrac{1-d}{4}\mathscr{L}^2 y^2 = \pm 1$, quando $d = 1 (\mathrm{mod}\ 4)$.*

DIMOSTRAZIONE. Stante (3.9), basta determinare $x, y \in \mathbb{Z}$ in modo che $\mathrm{N}(x + y\mathscr{L}\omega_d) = (x + y\mathscr{L}\omega_d)(x + y\mathscr{L}\omega'_d) \pm 1$. Se $d = 2, 3 (\mathrm{mod}\ 4)$, allora $\omega'_d = -\sqrt{d}$. Dunque $\mathrm{N}(x + y\mathscr{L}\omega_d) = x^2 - \mathscr{L}^2 y^2 d$. Se $d = 1 (\mathrm{mod}\ 4)$, allora $\omega'_d = \dfrac{1 - \sqrt{d}}{2}$ e quindi

$$\mathrm{N}(x + y\mathscr{L}\omega_d) = x^2 + \frac{1}{4}\mathscr{L}^2 y^2 + \mathscr{L}xy - \frac{\mathscr{L}^2 y^2 d}{4} = x^2 + \mathscr{L}xy + \frac{1-d}{4}\mathscr{L}^2 y^2.$$

Questo conclude la dimostrazione. □

Vedremo adesso che, nel caso $d < 0$, sarà molto semplice determinare gli invertibili di ${}^{\mathscr{L}}\mathscr{O}$. Nel caso $d > 0$ la risposta a tale questione sarà molto più articolata, e per nulla banale.

3.11 PROPOSIZIONE. *Preserviamo le notazioni di (3.3) e (3.1), e sia $d < 0$. Allora $U({}^{\mathscr{L}}\mathscr{O}) \supsetneq \{1, -1\}$ se e soltanto se si verifica uno dei seguenti casi:*

(1) *$d = -1, \mathscr{L} = 1$. In questo caso si ha*

$$U({}^{\mathscr{L}}\mathscr{O}) = \{\pm 1, \pm i\}.$$

(2) *$d = -3, \mathscr{L} = 1$. In questo caso si ha*

$$U({}^{\mathscr{L}}\mathscr{O}) = \left\{\pm 1, \frac{\pm 1 \pm i\sqrt{3}}{2}\right\}.$$

DIMOSTRAZIONE. Si ha $x^2 - d\mathscr{L}y^2 \geq 0$, per ogni $x, y \in \mathbb{Z}, \mathscr{L} \in \mathbb{N}\backslash\{0\}$. Dunque, se $d = 2, 3 (\mathrm{mod}\ 4)$, allora $\epsilon := x + y\mathscr{L}\omega_d$ è invertibile in ${}^{\mathscr{L}}\mathscr{O}$ se e soltanto se

$$x^2 + |d|\mathscr{L}^2 y^2 = 1. \tag{6}$$

Se $|d| > 1$ o $\mathscr{L}^2 > 1$, e inoltre $y \neq 0$, allora $x^2 + |d|\mathscr{L}^2 y^2 \geq |d|\mathscr{L}^2 y^2 > 1$, e quindi (6) non ammette soluzioni. Pertanto, se $|d| > 1, \mathscr{L}^2 > 1$, allora $\epsilon$ è invertibile in ${}^{\mathscr{L}}\mathscr{O}$ se e soltanto se $y = 0$. Segue che $\epsilon = x = \pm 1$. Se $|d| = \mathscr{L}^2 = 1$, la (6) diventa $x^2 + y^2 = 1$. Le uniche soluzioni intere di questa equazione sono $(\pm 1, 0), (0, \pm 1)$. Dunque, nel caso $|d| = \mathscr{L}^2 = 1$ gli invertibili di ${}^{\mathscr{L}}\mathscr{O}$ sono $\pm 1, \pm i$.
Si verifica immediatamente che

$$x^2 + \mathscr{L}xy + \frac{1-d}{4}\mathscr{L}^2 y^2 = \left(x + \frac{\mathscr{L}y}{2}\right)^2 + \frac{|d|\mathscr{L}^2 y^2}{4} \geq 0,$$

poiché $d < 0$. Allora, nel caso $d = 1(\text{mod } 4)$, $\epsilon$ è invertibile se e soltanto se

$$\left(x + \frac{\mathscr{L}y}{2}\right)^2 + \frac{|d|\mathscr{L}^2y^2}{4} = 1. \tag{7}$$

Se $|d| > 4$ e $y \neq 0$, allora $\dfrac{|d|\mathscr{L}^2y^2}{4} > 1$ e (7) non ammette soluzioni. Dunque, se $|d| > 4$ $\epsilon$ è invertibile in ${}^{\mathscr{L}}\mathscr{O}$ se e soltanto se $y = 0$, ovvero $\epsilon = \pm 1$. Essendo $d$ un intero negativo congruo 1 modulo 4, allora $|d| \leq 4$ equivale a $d = -3$. Se $\mathscr{L}^2 > 1$ e $y \neq 0$, allora $\dfrac{|d|\mathscr{L}^2y^2}{4} = \dfrac{3\mathscr{L}^2y^2}{4} > 1$, e (7) non ammette soluzioni. Dunque, se $d = -3, \mathscr{L}^2 > 1$, allora $\epsilon$ è invertibile in ${}^{\mathscr{L}}\mathscr{O}$ se e soltanto se $y = 0$. Segue $\epsilon = \pm 1$. Infine sia $\mathscr{L} = 1, d = -3$. Allora (7) diventa

$$\left(x + \frac{y}{2}\right)^2 + \frac{3y^2}{4} = 1.$$

Se $|y| > 2$, allora $\dfrac{3y^2}{4} > 1$, e quindi (7) non ammette soluzioni. Nel caso $\mathscr{L} = 1, d = -3, y \in \{\pm 1, 0\}$, si verifica senza difficoltà che gli unici invertibili di ${}^{\mathscr{L}}\mathscr{O}$ sono $\pm 1, \dfrac{\pm 1 \pm i\sqrt{3}}{2}$. Il risultato è adesso completamente provato. □

Per determinare esplicitamente gli invertibili di ${}^{\mathscr{L}}\mathscr{O}$ nel caso $d > 0$, useremo il seguente teorema chiave.

3.12 Teorema. *Sia $d_0$ un numero naturale non nullo che non sia il quadrato di alcun numero intero. Allora l'insieme delle soluzioni intere dell'equazione (detta di Pell) $X^2 - d_0Y^2 = 1$ è infinito.*

3.13 Corollario. *Preserviamo le notazioni di (3.3) e (3.1), e sia $d > 0$. Allora l'insieme $U({}^{\mathscr{L}}\mathscr{O})$ degli invertibili di ${}^{\mathscr{L}}\mathscr{O}$ è infinito.*

Dimostrazione. Si ha $< 1, \mathscr{L}\sqrt{d} >\subseteq {}^{\mathscr{L}}\mathscr{O}$. Questo è evidente se $d = 2, 3(\text{mod } 4)$ (infatti in questo caso $\omega_d = \sqrt{d}$). Sia adesso $d = 1(\text{mod } 4)$ e fissiamo $x, y \in \mathbb{Z}$. Essendo $\omega_d = \dfrac{1 + \sqrt{d}}{2}$, si ha

$$x + y\mathscr{L}\sqrt{d} = x + y\mathscr{L}(2\omega_d - 1) = x - \mathscr{L}y + (2y)\mathscr{L}\omega_d \in {}^{\mathscr{L}}\mathscr{O}.$$

Poiché, per ipotesi, $d$ è privo di fattori quadratici, $\mathscr{L}^2d$ non è il quadrato di alcun numero intero, e quindi, a norma di (3.12) l'insieme delle soluzioni

intere dell'equazione $X^2 - (\mathscr{L}^2 d)Y^2 = 1$ è infinito. Dunque esistono infinite coppie $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ tali che $\mathrm{N}(x + y\mathscr{L}\sqrt{d}) = x^2 - (\mathscr{L}^2 d)y^2 = 1$. Allora, da quanto osservato all'inizio della dimostrazione e da (3.9) segue l'asserto. □

3.14 Lemma. *Preserviamo le notazioni di (3.3) e (3.1), e sia $r$ un numero reale maggiore di* 1. *Allora l'insieme $U({}^{\mathscr{L}}\mathscr{O}) \cap ]1, r[$ è finito.*

Dimostrazione. Sia $\epsilon$ un elemento invertibile in ${}^{\mathscr{L}}\mathscr{O}$ tale che $1 < \epsilon < r$. Ovviamente, $\epsilon$ è radice del polinomio $f := X^2 - \mathrm{Tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\epsilon) + \mathrm{N}(\epsilon)$, e inoltre, per (3.3) e (2.13), $f$ è a coefficienti interi. Poiché $\epsilon$ è invertibile in ${}^{\mathscr{L}}\mathscr{O}$, allora $\mathrm{N}(\epsilon) = \pm 1$, e quindi $|\epsilon'| = |\epsilon|^{-1} = \epsilon^{-1} < 1$, essendo $\epsilon > 1$. Quindi si ha $|\mathrm{Tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\epsilon)| = |\epsilon + \epsilon'| \leq |\epsilon| + |\epsilon'| < r + 1$. Allora esiste un intero $n$ tale che $|n| < r + 1$ tale che $\epsilon$ è radice del polinomio $X^2 - nX \pm 1$. Per concludere la dimostrazione basta osservare che

$$U({}^{\mathscr{L}}\mathscr{O}) \cap ]1, r[ \subseteq T := \{x \in \mathbb{C} : x^2 - nX \pm 1 = 0, \text{ per qualche } n \in \mathbb{Z}, |n| < r+1\}$$

e tenere presente che $T$ è finito. □

3.15 Lemma. *Preserviamo le notazioni di (3.3) e (3.1), e sia $d > 0$. Allora esiste un invertibile in ${}^{\mathscr{L}}\mathscr{O}$ che è maggiore di* 1.

Dimostrazione. Mostriamo intanto che $U({}^{\mathscr{L}}\mathscr{O})$ possiede un elemento positivo. In virtù di (3.13), esiste un elemento $\delta \in U({}^{\mathscr{L}}\mathscr{O})$ distinto da $\pm 1$. Se $\delta > 0$, abbiamo finito, altrimenti baste considerare l'elemento (invertibile) $-\delta$.
Per quanto appena visto, fissiamo un elemento $\epsilon \in U({}^{\mathscr{L}}\mathscr{O}) \cap ]0, +\infty[$. Se $\epsilon > 1$, non vi è nulla da dimostrare. Se $\epsilon \in ]0, 1[$, allora l'elemento $\epsilon^* := \epsilon^{-1}$ è un invertibile di ${}^{\mathscr{L}}\mathscr{O}$ maggiore di 1. □

3.16 Corollario. *Preserviamo le notazioni di (3.3) e (3.1), e sia $d > 0$. Allora l'insieme degli invertibili di ${}^{\mathscr{L}}\mathscr{O}$ maggiori di* 1 *ha minimo.*

Dimostrazione. In virtù di (3.15), esiste un numero reale $r$ maggiore di 1 che è invertibile in ${}^{\mathscr{L}}\mathscr{O}$. Allora l'insieme $U({}^{\mathscr{L}}\mathscr{O}) \cap ]1, r]$ è non vuoto e finito, alla luce di (3.14), e pertanto esso ha minimo $\epsilon$. Segue immediatamente che $\epsilon$ è il minimo di $U({}^{\mathscr{L}}\mathscr{O}) \cap ]1, +\infty[$. □

3.17 Definizione. *Preserviamo le notazioni di (3.3) e (3.1), e sia $d > 0$. Il minimo di $U({}^{\mathscr{L}}\mathscr{O}) \cap ]1, +\infty[$ si dice* unità fondamentale di ${}^{\mathscr{L}}\mathscr{O}$.

Il seguente risultato indica l'importanza della precedente definizione.

3.18 Teorema. *Preserviamo le notazioni di (3.3) e (3.1), e sia $d > 0$. Se $\epsilon$ è l'unità fondamentale di ${}^{\mathscr{L}}\mathscr{O}$, allora $U({}^{\mathscr{L}}\mathscr{O}) = \{\pm\epsilon^n : n \in \mathbb{Z}\}$.*

Dimostrazione. L'inclusione $\{\pm\epsilon^n : n \in \mathbb{Z}\} \subseteq U({}^{\mathscr{L}}\mathscr{O})$ è ovvia. Fissiamo adesso un elemento $\epsilon^* \geq 1$ invertibile in ${}^{\mathscr{L}}\mathscr{O}$. Essendo, per definizione, $\epsilon > 1$, la successione di numeri reali $\{\epsilon^n : n \in \mathbb{N}\}$ diverge. Ne segue che l'insieme il sottoinsieme

$$\{n \in \mathbb{N}\backslash\{0\} : \epsilon^m > \epsilon^* \text{ per ogni } m \geq n\}$$

di $\mathbb{N}$ è non vuoto e quindi ha minimo $\nu(\geq 1)$. In particolare, si ha $\epsilon^{\nu-1} \leq \epsilon^* < \epsilon^\nu$, e quindi $1 \leq \epsilon^*\epsilon^{1-\nu} < \epsilon$. Essendo $\epsilon^*\epsilon^{1-\nu} \geq 1$ un elemento invertibile di ${}^{\mathscr{L}}\mathscr{O}$ e $\epsilon$ l'unità fondamentale di ${}^{\mathscr{L}}\mathscr{O}$, dalla definizione segue $\epsilon^*\epsilon^{1-\nu} = 1$, e quindi $\epsilon^* = \epsilon^{\nu-1}$. Questo prova che $U({}^{\mathscr{L}}\mathscr{O}) \cap [1, +\infty[ \subseteq \{\epsilon^n : n \in \mathbb{N}\}$.
Fissiamo adesso un arbitrario elemento $\widetilde{\epsilon}$ invertibile in ${}^{\mathscr{L}}\mathscr{O}$. Usando un argomento pressoché identico a quello dato nella dimostrazione di (3.15), si vede che uno degli elementi (invertibili) $\widetilde{\epsilon}, \widetilde{\epsilon}^{-1}, -\widetilde{\epsilon}, (-\widetilde{\epsilon}^{-1})$ non è minore di uno. L'asserto segue pertanto applicando quanto provato nella prima parte della dimostrazione. □

3.19 Corollario. *Preserviamo le notazioni di (3.3) e (3.1), e sia $U^+({}^{\mathscr{L}}\mathscr{O})$ l'insieme degli invertibili di ${}^{\mathscr{L}}\mathscr{O}$ di norma 1.*

(a) *Se $d > 0$ e $\epsilon$ è l'unità fondamentale di ${}^{\mathscr{L}}\mathscr{O}$, allora*

$$U^+({}^{\mathscr{L}}\mathscr{O}) = \begin{cases} U({}^{\mathscr{L}}\mathscr{O}) & \text{se } \mathrm{N}(\epsilon) = 1 \\ \{\pm\epsilon^{2n} : n \in \mathbb{Z}\} & \text{se } \mathrm{N}(\epsilon) = -1. \end{cases}$$

(b) *Se $d < 0$, allora $U^+({}^{\mathscr{L}}\mathscr{O}) = U({}^{\mathscr{L}}\mathscr{O})$.*

Dimostrazione. (a) è una conseguenza immediata di (3.18) e del fatto che $\mathrm{N}(\pm\epsilon^k) = \mathrm{N}(\epsilon)^k$, per ogni $k \in \mathbb{Z}$. (b) segue subito da (3.11). □

I prossimi risultati sono preliminari per la ricerca dell'unità fondamentale di ${}^{\mathscr{L}}\mathscr{O}$.

3.20 Lemma. *Preserviamo le notazioni di (3.3) e (3.1), e sia $d > 0$. Se $\eta := x + y\mathscr{L}\omega_d$ è un invertibile di ${}^{\mathscr{L}}\mathscr{O}$ $(x, y \in \mathbb{Z})$ e $\eta > 1$, allora $x \geq 0, y > 0$, e si ha $x = 0$ se e soltanto se $d = 5, \mathscr{L} = 1, \eta = \omega_5$.*

DIMOSTRAZIONE. Poiché $\eta$ è invertibile in ${}^{\mathscr{L}}\mathscr{O}$, si ha $\mathrm{N}(\eta) = \eta\eta' = \pm 1$, stante (3.9). Segue immediatamente $\eta' = \pm\eta^{-1}$, e pertanto $\eta - \eta' = \eta \mp \eta^{-1} > 0$, essendo $\eta > 1$ e $\eta^{-1} < 1$. Inoltre, $\omega_d, \omega'_d \in \mathbb{R}$ e $\omega_d - \omega'_d > 0$, poiché $d > 0$. Allora, dal fatto che $\eta - \eta' = y\mathscr{L}(\omega_d - \omega'_d) > 0$, segue subito che $y > 0$.
Osserviamo adesso che $1 > \eta^{-1} = |\eta|^{-1} = |\eta'| = |x + y\mathscr{L}\omega'_d|$. Si deduce subito che $x \geq 0$. Infatti, se così non fosse (ovvero se $x \leq -1$), dalla disuguaglianza $y\mathscr{L}\omega'_d < 0$ seguirebbe $x + y\mathscr{L}\omega'_d < -1$. Dunque resta da mostrare che, se $x = 0$, allora $d = 5, \mathscr{L} = 1, \eta = \omega_5$. Se $x = 0$, si ha $\mathrm{N}(\eta) = y^2\mathscr{L}^2\omega_d\omega'_d = \pm 1$. Poiché

$$\omega_d\omega'_d = \begin{cases} -d & \text{se } d = 2, 3 (\mathrm{mod}\ 4) \\ \dfrac{1-d}{4} & \text{se } d = 1 (\mathrm{mod}\ 4) \end{cases},$$

si ha $d = 1 (\mathrm{mod}\ 4)$ (altrimenti si avrebbe $\pm 1 = y^2\mathscr{L}^2(-d)$, contro il fatto che $d \geq 2$). Inoltre, il caso $d > 5$ non si può presentare, perché si avrebbe $\dfrac{1-d}{4} < -1$ e quindi $|y^2\mathscr{L}^2\omega_d\omega'_d| > 1$. Dovendo essere $d \leq 5$ e $d = 1 (\mathrm{mod}\ 4)$, si ha $d = 5$, e quindi $\mathrm{N}(\eta) = y^2\mathscr{L}^2(-1) = -1$. Allora $\mathscr{L} = 1, y = \pm 1$, e infine $\eta = \omega_5$, essendo $\eta > 1$. Questo completa la dimostrazione. □

3.21 LEMMA. *Preserviamo le notazioni di (3.3) e (3.1), e sia $d > 0$. Se $\eta := x + y\mathscr{L}\omega_d$ $(x, y \in \mathbb{Z})$ è un invertibile di ${}^{\mathscr{L}}\mathscr{O}$, $\eta > 1$ e $x \neq 0$, allora $x$ è l'intero più vicino al numero (irrazionale) $-y\mathscr{L}\omega'_d$.*

DIMOSTRAZIONE. Alla luce di (3.20), si ha $x, y \geq 1$ e, essendo $\omega_d > 1, \mathscr{L} \geq 1$, segue immediatamente $\eta > 2$. Poiché, stante (3.9), $\mathrm{N}(\eta) \pm 1$, si ottiene $|\eta'| = \eta^{-1} < \dfrac{1}{2}$ e, equivalentemente, $-y\mathscr{L}\omega'_d - \dfrac{1}{2} < x < -y\mathscr{L}\omega'_d + \dfrac{1}{2}$. Segue subito l'asserto. □

3.22 LEMMA. *Preserviamo le notazioni di (3.3) e (3.1), e sia $d > 0$. Sia $\eta := x + y\mathscr{L}\omega_d$ $(x, y \in \mathbb{Z})$ è un invertibile di ${}^{\mathscr{L}}\mathscr{O}$ tale che $\eta > 1$ e $x \neq 0$. Allora, posto, per ogni $n \in \mathbb{N}\backslash\{0\}$, $\eta^n = x_n + y_n\mathscr{L}\omega_d$, si ha*

$$0 < x_1 := x < x_2 < \dots \qquad 0 < y_1 := y < y_2 < \dots.$$

DIMOSTRAZIONE. L'asserzione segue procedendo per induzione su $n$, tenendo presente (3.20), e osservando che $\eta^n = (x_1x_{n-1} + \mathscr{L}^2 d y_1 y_{n-1}) + (x_1y_{n-1} + y_1x_{n-1})\mathscr{L}\omega_d$ se $d = 2, 3 (\mathrm{mod}\ 4)$, mentre $\eta^n = (x_1x_{n-1} + \dfrac{d-1}{4}\mathscr{L}^2 y_1y_{n-1}) + (x_1y_{n-1} + y_1x_{n-1} + \mathscr{L}y_1y_{n-1})\mathscr{L}\omega_d$ se $d = 1 (\mathrm{mod}\ 4)$, per ogni $n \in \mathbb{N}\backslash\{0\}$. □

Il seguente importante Teorema fornisce un algoritmo per determinare l'invertibile principale dell'anello dei coefficienti di un modulo di $\mathbb{Q}(\sqrt{d})$, nel caso $d > 0$.

3.23 Teorema. *Preserviamo le notazioni di (3.3) e (3.1), e sia $d > 0$, $(\mathscr{L}, d) \neq (1, 5)$. Per ogni $y \in \mathbb{N}\backslash\{0\}$, sia $x_y$ il numero intero più vicino a $-y\mathscr{L}\omega'_d$. Allora l'insieme $V := \{y \in \mathbb{N}\backslash\{0\} : x_y + y\mathscr{L}\omega_d \in U({}^{\mathscr{L}}\mathscr{O})\}$ è non vuoto e, detto $z$ il suo minimo, l'unità fondamentale di ${}^{\mathscr{L}}\mathscr{O}$ è $x_z + z\mathscr{L}\omega_d$.*

Dimostrazione. Sia $\epsilon := x + y\mathscr{L}\omega_d$ l'unità fondamentale di ${}^{\mathscr{L}}\mathscr{O}$. Stante (3.21), $x$ è l'intero più vicino al numero irrazionale $-y\mathscr{L}\omega'_d$. In altri termini, $y \in V$. Sia adesso $n$ un arbitrario elemento di $V$. Allora $\eta := x_n + n\mathscr{L}\omega_d$ è invertibile in ${}^{\mathscr{L}}\mathscr{O}$ ed è maggiore di 2, come visto nella dimostrazione di (3.21). Dunque, in virtù di (3.18), esiste un intero positivo $r$ tale che $\eta = \epsilon^r$. Alla luce di (3.22) segue immediatamente $x_n \geq x_y, n \geq y$. Questo completa la dimostrazione. □

# 4 Elementi di norma fissata in un modulo

Adesso usiamo la teoria illustrata fino ad ora per risolvere il problema della ricerca degli elementi di un modulo di un campo quadratico aventi norma fissata. Come visto in (1.5), questo problema è di fatto equivalente al problema della ricerca delle soluzioni intere della forma (1). Il prossimo risultato mostra che la questione è abbastanza semplice per moduli di $\mathbb{Q}(\sqrt{d})$, nel caso $d < 0$.

4.1 Proposizione. *Siano $d$ un intero negativo privo di fattori quadratici, $M$ un modulo di $\mathbb{Q}(\sqrt{d})$, $r \in \mathbb{Q}$. Allora l'insieme $\{\eta \in M : \mathrm{N}(\eta) = r\}$ è finito*

Dimostrazione. Siano $\{\alpha, \beta\}$ una base di $\mathbb{Q}(\sqrt{d})$ su $\mathbb{Q}$ tale che $< \alpha, \beta >= M$, e $a, b, c, e$ i numeri razionali tali che $\alpha = a + b\sqrt{d}, \beta = c + e\sqrt{d}$. Allora, per ogni $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, si ha

$$\mathrm{N}(x\alpha + y\beta) = (x\alpha + y\beta)(x\alpha' + y\beta') = (ax + cy)^2 + (bx + ey)^2|d|. \qquad (8)$$

Se $g$ è un denominatore comune alle frazioni $a, b, c, e$, allora il denominatore di $ax+cy, bx+ey$ deve dividere necessariamente $g$. Inoltre, se $\mathrm{N}(x\alpha+y\beta) = r$,

allora $r \geq 0$, e da (8) seguono immediatamente le maggiorazioni

$$|ax + cy| \leq \sqrt{r} \qquad |bx + ey| \leq \sqrt{\frac{r}{|d|}}.$$

Segue subito che, se $\mathrm{N}(x\alpha + y\beta) = r$, allora il numero di scelte possibili per gli interi $x, y$ è finito. Questo conclude la dimostrazione. □

Vedremo fra poco che il caso $d > 0$ sarà molto meno banale. Prima però bisogna fare alcune osservazioni.

4.2 Definizione. *Siano $K$ un campo di numeri e $M$ un modulo di $K$. Diremo che due elementi $x, y \in M$ sono* associati in $M$ *(o che $x$ è* associato con $y$*) se esiste un elemento $\epsilon$ invertibile in $\mathscr{O}_M$ tale che $x = \epsilon y$.*

4.3 Esempio. Consideriamo l'ordine $M :=< 1, \sqrt{2} >$ di $\mathbb{Q}(\sqrt{2})$ (cf. (2.20)). Allora $2 + 3\sqrt{2}$ e $4 - \sqrt{2}$ sono associati in $M$, poiché $-1 + \sqrt{2}$ è un ivertibile di $\mathscr{O}_M = M$ e $4 - \sqrt{2} = (-1 + \sqrt{2})(2 + 3\sqrt{2})$.

4.4 Osservazione. Siano $K$ un campo di numeri e $M$ un modulo di $K$. Allora è immediatamente visto che la relazione su $M$ che identifica elementi associati in $M$ è di equivalenza.

4.5 Definizione. *Siano $K$ un campo di numeri e $M$ un modulo di $K$, $r$ un numero razionale. Diremo che un sottoinsieme $S$ (possibilmente vuoto) di $M$ è* un sistema completo di non associati di norma $r$ *in $M$ se valgono le seguenti condizioni.*

(1) *Elementi distinti di $S$ sono non associati in $M$.*

(2) *Tutti gli elementi di $S$ hanno norma $r$.*

(3) *Per ogni $\eta \in M$ tale che $\mathrm{N}(\eta) = r$, esiste un elemento $x_\eta \in S$ che è associato con $\eta$.*

Il prossimo risultato chiarisce l'importanza della precedente definizione.

4.6 Proposizione. *Siano $K$ un campo di numeri, $M$ un modulo di $K$, $r$ un numero razionale non nullo, $S$ un sistema completo di non associati di norma $r$ per $M$. Allora*

$$\{\eta \in M : \mathrm{N}(\eta) = r\} = \{\epsilon x : \epsilon \in \mathscr{O}_M, N(\epsilon) = 1, x \in S\}$$

DIMOSTRAZIONE. Da (2.12(b)) segue l'inclusione $\supseteq$. Viceversa, sia $\eta \in M$ un elemento di norma $r$. Allora, per definizione, esistono un elemento $x \in S$ e un invertibile $\epsilon$ di $\mathscr{O}_M$ tali che $\eta = \epsilon x$. Inoltre si ha $r = \mathrm{N}(\eta) = \mathrm{N}(\epsilon)\mathrm{N}(x) = \mathrm{N}(\epsilon)r$, e quindi $\mathrm{N}(\epsilon) = 1$, essendo $r \neq 0$. □

Da quanto appena provato si evince che per determinare gli elementi di norma fissata $r$ di un modulo $M$ basta conoscere un sistema completo di non associati di norma $r$ per $M$ e gli invertibili di $\mathscr{O}_M$ aventi norma 1. Nel caso dei campi quadratici, che è il caso di nostro interesse, abbiamo già determinato gli invertibili di un ordine aventi norma 1 (cf. (3.19)). Adesso ci occuperemo della determinazione di un sistema completo di non associati di una certa norma per un modulo. Intanto mostriamo che ogni sistema completo di non associati per un modulo è finito. Il seguente risultato sarà cruciale.

4.7 PROPOSIZIONE. *Siano $K$ un campo di numeri, $A$ un sottoanello di $\mathcal{O}_K$, $c$ un numero naturale non nullo. Se $\alpha, \beta \in A$ sono tali che $|\mathrm{N}(\alpha)| = |\mathrm{N}(\beta)| = c$ e $\alpha, \beta$ non sono associati in $A$, allora le immagini canoniche di $\alpha, \beta$ in $A/(c)$ sono distinte.*

DIMOSTRAZIONE. Fissiamo elementi $\alpha, \beta \in A$ le cui immagini in $A/(c)$ coincidono tali che $|\mathrm{N}(\alpha)| = |\mathrm{N}(\beta)| = c$. Dunque, esiste un elemento $\eta \in A$ tale che $\alpha - \beta = c\eta$. In virtù di (3.8), risulta $\alpha\beta^{-1} - 1 = |\mathrm{N}(\beta)|\beta^{-1}\gamma \in A$, e $1 - \alpha^{-1}\beta = |\mathrm{N}(\alpha)|\alpha^{-1}\gamma \in A$. Segue immediatamente che $\alpha\beta^{-1}, \alpha^{-1}\beta \in A$. Dunque $\alpha, \beta$ sono associati di $A$. □

4.8 LEMMA. *Siano $K$ un campo di numeri, $M$ un modulo di $K$, $c$ un numero naturale non nullo, $N := \{c\eta : \eta \in M\}$. Allora $N$ è un sottogruppo di $M$ e $M/N$ ha $c^{[K:\mathbb{Q}]}$ elementi.*

DIMOSTRAZIONE. Siano $n := [K : \mathbb{Q}]$ e $\{\alpha_1, \ldots, \alpha_n\}$ una base di $K$ su $\mathbb{Q}$ tale che $M =< \alpha_1, \ldots, \alpha_n >$. Allora l'applicazione $\phi : M \longrightarrow (\mathbb{Z}/c\mathbb{Z})^n$, $\sum_{i=1}^n m_1\alpha_i \mapsto ([m_1], \ldots, [m_n])$, è un omomorfismo surgettivo di gruppi tale che $\mathrm{Ker}(\phi) = N$. L'asserto segue immediatamente. □

4.9 PROPOSIZIONE. *Siano $K$ un campo di numeri, $A$ un ordine di $K$, $c$ un numero intero non nullo. Ogni insieme di elementi di $A$ a due a due non associati aventi norma $c$ è finito.*

DIMOSTRAZIONE. Basta applicare (4.7) e (4.8) □

4.10 LEMMA. *Siano $K$ un campo di numeri e $M$ un modulo di $K$. Allora esiste un munero naturale non nullo $k$ tale che $kM \subseteq \mathscr{O}_M$.*

DIMOSTRAZIONE. Sia $\{\alpha_1, \ldots, \alpha_n\}$ una base di $K$ su $\mathbb{Q}$ tale che $M =< \alpha_1, \ldots, \alpha_n >$. Allora, per (2.15), esistono numeri naturali non nulli $m_1, \ldots, m_n$ tali che $m_i\alpha_i \in \mathscr{O}_M$, per ogni $i \in \{1, \ldots, n\}$. Allora, posto $k := m_1, \cdots m_n$, si ha $kM \subseteq \mathscr{O}_M$. □

4.11 COROLLARIO. *Siano $K$ un campo di numeri e $M$ un modulo di $K$, $r$ un numero razionale. Allora ogni insieme di elementi di $M$ a due a due non associati di norma $r$ è finito. Inoltre $M$ ha un sistema completo di non associati di norma $r$.*

DIMOSTRAZIONE. In virtù di (4.10), esiste un numero naturale non nullo $k$ tale che $kM \subseteq \mathscr{O}_M$. Sia adesso $F$ un insieme di elementi di $M$ a due a due non associati aventi tutti norma $r$. Allora, posto $n := [K : \mathbb{Q}]$, $kF$ è un insieme di elementi a due a due non associati dell'ordine $\mathscr{O}_M$ aventi norma $c := k^n r \in \mathbb{Z}$. Dunque $kF$ è finito, per (4.9). Allora la prima parte dell'asserzione segue dal fatto che $\mathrm{Card}(F) = \mathrm{Card}(kF)$.
Sia ora $R$ l'insieme degli elementi di $M$ che hanno norma $r$, e sia $P$ l'insieme delle classi di equivalenza $\gamma$ modulo $(c)$ che hanno un elemento $kx_\gamma$ in $kR$ $(x_\gamma \in R)$. Sia adesso

$$P' := \{\gamma \in P : x_\gamma \text{ non è associato a } x_\delta \text{ per ogni } \delta \in P\backslash\{\gamma\}\}$$

Allora, dalle definizioni, da (4.7) e da (4.4) segue che $\{x_\gamma : \gamma \in P'\}$ è un sistema completo di non associati di $M$ con norma $r$. □

Occupiamoci adesso di determinare un sistema completo di non associati di norma fissata per un campo quadratico. I precedenti risultati ci garantiscono soltanto la finitezza, ma non sono costruttivi. Presenteremo adesso un algoritmo per determinare un sistema completo di non associati (possibilmente vuoto) per moduli di campi quadratici.

4.12 LEMMA. *Siano $d$ un numero naturale privo di fattori quadratici, $M$ un modulo di $\mathbb{Q}(\sqrt{d})$, $\mathscr{L}$ un numero naturale non nullo tale che $\mathscr{O}_M = {}^{\mathscr{L}}\mathscr{O}$ (cf. (3.3)), $\epsilon$ l'unità fondamentale di $\mathscr{O}_M$, $r$ un numero razionale non nullo. Allora, se $\zeta \in M$ ha norma $r$, allora esiste un associato $\zeta_1$ di $\zeta$ tale che* $1 \leq \zeta_1 < \epsilon$ *e* $\dfrac{|r|}{\epsilon} < \zeta_1' \leq |r|$.

DIMOSTRAZIONE. Assumiamo intanto $\zeta > 0$. Poichè $\epsilon > 1$, la successione di numeri reali $\{\epsilon^n : n \in \mathbb{N}\}$ diverge, mentre $\{\epsilon^{-n} : n \in \mathbb{N}\}$ converge a zero, e quindi esiste un numero intero $n$ tale che $\epsilon^n \leq \zeta < \epsilon^{m+1}$ (la prima parte della disuguaglianza segue dal fatto che $\zeta > 0$). Si ha immediatamente $1 \leq \epsilon^{-n} < \epsilon$. Allora l'elemento di cui si doveva provare l'esistenza è $\zeta_1 := \epsilon^{-n}\zeta$. Se $\zeta < 0$, basta tenere presente che $-\zeta > 0$ è associato di $\zeta$, e applicare quanto provato nella prima parte della dimostrazione. □

4.13 LEMMA. *Siano $d$ un intero privo di fattori quadratici, $M$ un modulo di $\mathbb{Q}(\sqrt{d})$. Allora esiste un intero positivo $g$ tale che $gM \subseteq < 1, \sqrt{d} >$.*

DIMOSTRAZIONE. Stante (2.10), esiste un numero naturale non nullo $K$ tale che $kM \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})} = < 1, \omega_d >$. Se $d = 2, 3 (\mathrm{mod}\ 4)$ basta scegliere $g := k$. Se $d = 1 (\mathrm{mod}\ 4)$, l'asserto segue prendendo $g := 2k$. □

4.14 TEOREMA. *Siano $d$ un intero positivo privo di fattori quadratici, $M$ un modulo di $\mathbb{Q}(\sqrt{d})$, $g$ un numero naturale non nullo tale che $gM \subseteq < 1, \sqrt{d} >$ (cf. (4.13)), $\epsilon$ l'unità fondamentale di $\mathcal{O}_M$, $r$ un numero razionale non nullo. Siano $p, q$ rispettivamente il massimo intero minore o uguale a $g\dfrac{\epsilon + |r|}{2}$ e il massimo intero minore o uguale a $g\dfrac{\epsilon + |r|}{2\sqrt{d}}$. Poniamo*

$$S_1 := \{\pm n/g : n \in \{0, \ldots, p\}\} \qquad S_2 := \{\pm m/g : g \in \{0, \ldots, q\}\}.$$

*Allora l'insieme degli elementi a due a due non associati aventi norma $r$ dell'insieme*

$$\{a + b\sqrt{d} : (a, b) \in S_1 \times S_2\}$$

*è un sistema completo di non associati (possibilmente vuoto) di norma $r$ per $M$.*

DIMOSTRAZIONE. Sia $\zeta \in M$ un elemento di norma $r$. Per (4.12), esiste un associato $\zeta_1$ di $\zeta$ tale che $1 \leq \zeta_1 < \epsilon$ e $\dfrac{|r|}{\epsilon} < \zeta_1' \leq |r|$. Siano $a, b$ i numeri irrazionali tali che $\zeta_1 = a + b\sqrt{d}$. Essendo

$$a = \frac{\zeta_1 + \zeta_1'}{2} \qquad b = \frac{\zeta_1 - \zeta_1'}{2\sqrt{d}},$$

si hanno immediatamente le stime

$$|a| \leq \frac{\epsilon + |r|}{2} \qquad |b| \leq \frac{\epsilon + |r|}{2\sqrt{d}}.$$

Inoltre, poiché $g\zeta_1 \in < 1, \sqrt{d} >$, i denominatori di $a, b$ devono necessariamente dividere $g$. Dunque $(a, b) \in S_1 \times S_2$. La conclusione segue facilmente. □

4.15 Esempio. Determiniamo tutti gli elementi di norma $r = 7$ del modulo $M := < 1, \sqrt{2} >$. Per (3.1), $M$ è l'anello degli interi di $\mathbb{Q}(\sqrt{2})$, e quindi, essendo un ordine, si ha $\mathscr{O}_M = M$. Applicando (3.23) (con $\mathscr{L} = 1, d = 2$), è facilmente visto che l'unità fondamentale di $M$ è $\epsilon := 1 + \sqrt{2}$. Ovviamente, possiamo scegliere $g = 1$ (perché $M := < 1, \sqrt{2} >$). Si ha

$$g\frac{\epsilon + |r|}{2} = 4,707 \qquad g\frac{\epsilon + |r|}{2\sqrt{d}} = 3,328.$$

In virtù di (4.14), gli elementi di norma 7 a due a due non associati dell'insieme

$$S_0 := \{a + b\sqrt{2} : a \in \{0, \pm 1, \pm 2, \pm 3, \pm 4\}, b \in \{0, \pm 1, \pm 2, \pm 3\}\}$$

costituiscono un sistema completo di non associati di norma 7 per $M$. Non è difficile controllare (disponendo di un calcolatore) che gli unici elementi di norma 7 di $S_0$ sono $\pm 3 \pm \sqrt{2}$. Si verifica immediatamente che $(-3 - \sqrt{2}, 3 + \sqrt{2}), (-3 + \sqrt{2}, 3 - \sqrt{2})$ sono coppie di elementi fra loro associati. Inoltre gli elementi $3+\sqrt{2}, 3-\sqrt{2}$ non sono associati in $M$, perché $\dfrac{3 + \sqrt{2}}{3 - \sqrt{2}} = \dfrac{11}{7} + \dfrac{6}{7}\sqrt{2} \notin \mathscr{O}_M = M$. Dunque $\{3 \pm \sqrt{2}\}$ è un sistema completo di non associati di norma 7 per $M$. Poiché $\mathrm{N}(\epsilon) = -1$, da (3.19) e (4.6) segue immediatamente che l'insieme degli elementi di $M$ con norma 7 è

$$\{\pm(1 + \sqrt{2})^{2n}(3 \pm \sqrt{2}) : n \in \mathbb{Z}\}.$$

4.16 Esempio. Applichiamo adesso tutta la teoria illustrata per determinare l'insieme delle soluzioni intere dell'equazione $X^2 + 3XY - 5Y^2 = 65$. Il discriminante dell'equazione è 29 e, come visto in (1.4), il modulo associato all'equazione è $M := < 1, \dfrac{3 + \sqrt{29}}{2} >$. Stante (1.5), un elemento $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ è soluzione dell'equazione data se e soltanto se $x + y\dfrac{3 + \sqrt{29}}{2}$ è un elemento di $M$ avente norma $r := 65$. In virtù di (3.6), l'anello dei coefficienti di $M$ è $\mathscr{O}_M = < 1, \mathscr{L}\omega_d > = < 1, \dfrac{1 + \sqrt{29}}{2} >$ (nel nostro caso $\mathscr{L} = 1, d = 29$). Inoltre, è immediato rendersi conto che $M = \mathscr{O}_M$. Applicando (3.23), è facile

verificare che l'unità fondamentale di $\mathscr{O}_M$ è $\epsilon := 2 + \omega_{29} = \dfrac{5+\sqrt{29}}{2}$. Infatti, posto $y = 1$, allora $-y\mathscr{L}\omega'_d = \dfrac{\sqrt{29}-1}{2} = 2,19$, e quindi il numero intero più vicino a $-y\mathscr{L}\omega'_d$ è $x_y = 2$. Inoltre l'elemento $x_y + y\mathscr{L}\omega_d$ ha norma $-1$ e quindi è invertibile in $\mathscr{O}_M$ (per (3.9)), e quindi l'unità fondamentale è $2+\omega_d$. Si vede subito che $2M \subseteq < 1, \sqrt{29} >$, quindi possiamo scegliere $g = 2$ (cf. (4.13)). Si ha

$$g\frac{\epsilon + |r|}{2} = 70,20... \qquad g\frac{\epsilon + |r|}{2\sqrt{d}} = 13,04....$$

Dunque, in virtù di (4.14), gli elementi a due a due non associati di norma 65 dell'insieme

$$S_0 := \{a_1/2 + b_1/2\sqrt{29} : a_1, b_1 \in \mathbb{Z}, |a_1| \leq 70, |b_1| \leq 13\}$$

costituiscono un sistema completo di non associati di norma 65 per $M$. Affinché $a_1/2 + b_1/2\sqrt{29}$ abbia norma 65 basta (e occorre che) $a_1^2 - 29b_1^2 = 4 \cdot 65 = 260$. Non è difficile verificare che $(a_1, b_1)$ deve essere uno degli elementi dell'insieme $\{(\pm 17, \pm 1), (\pm 41, \pm 7), (\pm 46, \pm 8)\}$. Allora, si vede che $\left\{\dfrac{17 \pm \sqrt{29}}{2}, \dfrac{41 \pm 7\sqrt{29}}{2}\right\}$ è un sistema completo di non associati di norma 65 per $M$. Osservando che $\dfrac{17+\sqrt{29}}{2} = 7 + \omega_{29}$, $\dfrac{17-\sqrt{29}}{2} = 10 - \omega_{29}$, $\dfrac{41+7\sqrt{29}}{2} = 10 + 7\omega_{29}$, $\dfrac{41-7\sqrt{29}}{2} = 31 - 7\omega_{29}$, si deduce che $I := \{(7,1), (10,-1), (10,7), (31,-7)\}$ sono soluzioni dell'equazione data. Inoltre, l'insieme di tutti gli elementi di $M$ aventi norma 65 è

$$\left\{\pm\frac{17 \pm \sqrt{29}}{2}\epsilon^{2n}, \pm\frac{41 \pm 7\sqrt{29}}{2}\epsilon^{2n} : n \in \mathbb{Z}\right\},$$

in virtù di (3.19) e (4.6). Dunque, per (1.5), un elemento $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ è soluzione dell'equazione assegnata se e soltanto se esistono un numero intero $n$ e un elemento $(x_0, y_0) \in I$ tali che

$$x + y\frac{3+\sqrt{29}}{2} = \pm\left(x_0 + y_0\frac{3+\sqrt{29}}{2}\right)\epsilon^{2n}.$$

Poiché $\epsilon^2 = \dfrac{27+5\sqrt{29}}{2}, \epsilon^{-2} = \dfrac{27-5\sqrt{29}}{2}$, si ha

$$\left(x_0 + y_0\frac{3+\sqrt{29}}{2}\right)\epsilon^2 = 6x_0 + 25y_0 + (5x_0 + 21y_0)\frac{3+\sqrt{29}}{2},$$

$$\left(x_0 + y_0\frac{3+\sqrt{29}}{2}\right)\epsilon^{-2} = 21x_0 - 25y_0 + (6y_0 - 5x_0)\frac{3+\sqrt{29}}{2},$$

e dunque dalle soluzioni iniziali dell'insieme $I$ troviamo un altro insieme $I_1$ di soluzioni

$$I_1 := \{(\pm(6x_0 + 25y_0), \pm(5x_0 + 21y_0)), (\pm(21x_0 - 25y_0), \pm(6y_0 - 5x_0))\}.$$

Procedendo ricorsivamente si trovano tutte le soluzioni dell'equazione data.