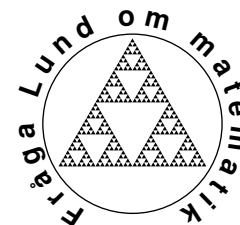




LUNDS
UNIVERSITET



Matematikcentrum

Matematik NF

Representation av heltal med kvadratiska former i två variabler

KJELL ELFSTRÖM

Innehåll

Förord	1
Modulär ekvivalens	2
Kedjebråk	3
Enkla kedjebråk	5
Avståndet från värdet till en konvergent	8
Modulärt ekvivalenta kedjebråk	9
Kroppen $\mathbb{Q}(\sqrt{d})$	11
Kvadratisk irrationella tal	12
Moduler	13
Ordningar	14
Koefficientringar	19
Element med föreskriven norm	20
Modulärt ekvivalenta kvadratisk irrationella tal	24
Reella kvadratisk irrationella tal	25
Icke-reella kvadratisk irrationella tal	29
Kvadratiska former i två variabler	30
Bibliografi	34

Förord

Syftet med arbetet är att studera hur man löser diofantiska ekvationer av formen

$$px^2 + qxy + ry^2 = m,$$

där p , q , r och m är heltal. Man säger att m representeras av den kvadratiska formen $px^2 + qxy + ry^2$. En välkänd ekvation av denna form är Pells ekvation $x^2 - Dy^2 = 1$, där D är ett positivt heltal, som inte är kvadraten på ett heltal. Den allmänna teorin för representation av heltal med kvadratiska former i n variabler har jag studerat i [1]. Detta

avspeglas i texten, då jag behållit mycket av terminologin, även beteckningar i flertalet fall. Eftersom jag begränsar mig till studiet av kvadratiska former i två variabler, har jag kunnat undvika att använda mycket av den algebraiska teori, som förekommer i [1]. Detta gäller i synnerhet teorin för ändligtgenererade fria abelska grupper och kroppsutvidgningar. Användning av kedjebråk utgör ett väsentligt inslag i lösandet av kvadratiska diofantiska ekvationer i två obekanta. Här har jag i stor utsträckning hämtat inspiration från [2]. Teorin för rent periodiska kedjebråk och reducerade kvadratisk irrationella tal har tillkommit.

Modulär ekvivalens

Definition 1 Vi betecknar med $GL(2, \mathbf{Z})$ mängden av 2×2 -matriser R med heltals-element, sådana att $\det R = \pm 1$. Vi kallar sådana matriser unimodulära.

Sats 1 $GL(2, \mathbf{Z})$ är en grupp under matrismultiplikation.

Bevis Det är klart att $E \in GL(2, \mathbf{Z})$, om E är enhetsmatrisen. Om $R \in GL(2, \mathbf{Z})$, följer det av Cramers regel att R^{-1} har heltalselement. Det följer nu av produktsatsen för determinanter att $R^{-1} \in GL(2, \mathbf{Z})$. Av samma sats följer det också att $RS \in GL(2, \mathbf{Z})$, om $R \in GL(2, \mathbf{Z})$ och $S \in GL(2, \mathbf{Z})$. ■

Definition 2 Om

$$R = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2, \mathbf{Z}),$$

och $\xi \in \mathbf{C} \cup \{\infty\}$, definierar vi $R\xi$ genom

$$R\xi = \begin{cases} \frac{a\xi+b}{c\xi+d} & \text{om } \xi \neq \infty \text{ och } c\xi+d \neq 0, \\ \infty & \text{om } \xi \neq \infty \text{ och } c\xi+d = 0, \\ \frac{a}{c} & \text{om } \xi = \infty \text{ och } c \neq 0, \\ \infty & \text{om } \xi = \infty \text{ och } c = 0. \end{cases}$$

Sats 2 Om $\xi \in \mathbf{C} \cup \{\infty\}$, så gäller det att $E\xi = \xi$, om E är enhetsmatrisen, och att $R(S\xi) = (RS)\xi$, om $R \in GL(2, \mathbf{Z})$ och $S \in GL(2, \mathbf{Z})$.

Bevis Att $E\xi = \xi$ är trivialt. Antag att

$$R = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \text{och} \quad S = \begin{bmatrix} e & f \\ g & h \end{bmatrix}.$$

Om $\xi \in \mathbf{C}$, $g\xi+h \neq 0$ och $cS\xi+d \neq 0$, så är

$$\begin{aligned} R(S\xi) &= \frac{aS\xi+b}{cS\xi+d} = \frac{a\frac{e\xi+f}{g\xi+h}+b}{c\frac{e\xi+f}{g\xi+h}+d} = \frac{a(e\xi+f)+b(g\xi+h)}{c(e\xi+f)+d(g\xi+h)} \\ &= \frac{(ae+bg)\xi+af+bh}{(ce+dg)\xi+cf+dh} = (RS)\xi. \end{aligned}$$

Eftersom $\det R \neq 0$, kan det inte gälla att $a\xi+b=c\xi+d=0$, om $\xi \in \mathbf{C}$. För alla $\xi \in \mathbf{C} \cup \{\infty\}$ gäller det alltså att $R\xi \rightarrow R\xi$, då $\zeta \rightarrow \xi$, varav $R(S\xi) = (RS)\xi$. ■

Definition 3 Två element ξ och ζ i $\mathbf{C} \cup \{\infty\}$ säges vara modulärt ekvivalenta, $\xi \sim \zeta$, om det finns en matris $R \in GL(2, \mathbf{Z})$, sådan att $\xi = R\zeta$.

Sats 3 Modulär ekvivalens är en ekvivalensrelation på $\mathbf{C} \cup \{\infty\}$.

Bevis Påståendet följer direkt av sats 2. ■

Sats 4 Låt $\xi \in \mathbf{C}$. Då gäller det att $\xi \sim \infty$, om och endast om $\xi \in \mathbf{Q}$.

Bevis Det är klart att $\xi \in \mathbf{Q}$, om $\xi \sim \infty$. Antag att $\xi = a/c$, där a och c är relativt prima heltal. Då finns det heltal b och d , sådana att $ad - bc = 1$. Det gäller då att $\det R = 1$, där

$$R = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

och att $R\infty = \xi$. ■

Sats 5 Om $\xi \in \mathbf{C} \setminus \mathbf{Q}$, och $R \in \text{GL}(2, \mathbf{Z})$, så är $\text{sgn}(\text{Im } R\xi) = (\det R) \text{sgn}(\text{Im } \xi)$.

Bevis Om $\xi = x + iy$, $x \in \mathbf{R}$, $y \in \mathbf{R}$, och

$$R = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

så är

$$R\xi = \frac{ax + b + iay}{cx + d + icy} = \frac{(ax + b)(cx + d) + acy^2 + i(ad - bc)y}{(cx + d)^2 + (cy)^2}. \quad \blacksquare$$

Kedjebråk

Definition 4 Med ett kedjebråk skall vi mena en ändlig följd (a_0, \dots, a_N) , eller en oändlig följd (a_0, a_1, \dots) , av reella tal, sådan att alla element utom möjligen a_0 är positiva. Vi kallar kedjebråket ändligt eller oändligt beroende på om följen är ändlig eller oändlig.

Definition 5 För ett ändligt kedjebråk (a_0, \dots, a_N) definierar vi dess värde $[(a_0, \dots, a_N)]$ rekursivt genom

$$[(a_0)] = a_0, \quad [(a_0, a_1, \dots, a_N)] = a_0 + \frac{1}{[(a_1, \dots, a_N)]}, \quad N \geq 1.$$

Vi kommer i fortsättningen oftast att utelämna de inre parenteserna.

Sats 6 Om $1 \leq n \leq N$, så gäller det att $[a_0, \dots, a_N] = [a_0, \dots, a_{n-1}, [a_n, \dots, a_N]]$.

Bevis Vi bevisar påståendet med induktion över N . Om $N = 1$, är $n = 1$, och påståendet följer direkt av definitionen. Antag att $N \geq 2$, och att påståendet är sant för kedjebråk (a_0, \dots, a_M) , där $M = N - 1$. Om $n = 1$, följer påståendet av definitionen. Antag att $2 \leq n \leq N$. Då är

$$[a_0, \dots, a_{n-1}, [a_n, \dots, a_N]] = [a_0, [a_1, \dots, a_{n-1}, [a_n, \dots, a_N]]]$$

enligt definitionen och

$$[a_1, \dots, a_{n-1}, [a_n, \dots, a_N]] = [a_1, \dots, a_{n-1}, a_n, \dots, a_N]$$

enligt induktionsantagandet, och det följer att

$$[a_0, \dots, a_{n-1}, [a_n, \dots, a_N]] = [a_0, \dots, a_{n-1}, a_n, \dots, a_N]. \quad \blacksquare$$

Definition 6 För ändliga kedjebraök a definierar vi $p(a)$ och $q(a)$ rekursivt genom

$$\begin{aligned} p((a_0)) &= a_0, & p((a_0, a_1)) &= a_1 a_0 + 1, \\ q((a_0)) &= 1, & q((a_0, a_1)) &= a_1, \end{aligned}$$

och

$$\begin{aligned} p((a_0, \dots, a_N)) &= a_N p((a_0, \dots, a_{N-1})) + p((a_0, \dots, a_{N-2})), \\ q((a_0, \dots, a_N)) &= a_N q((a_0, \dots, a_{N-1})) + q((a_0, \dots, a_{N-2})), \end{aligned}$$

då $N \geq 2$.

I fortsättningen utelämnar vi oftast det ena paret av parenteser.

Sats 7 Det gäller att

$$[a_0, \dots, a_N] = \frac{p(a_0, \dots, a_N)}{q(a_0, \dots, a_N)}.$$

Bevis Vi visar påståendet med induktion över N . Om $N = 0$ eller $N = 1$ är påståendet trivialt. Antag att $N \geq 2$, och att påståendet är sant för kedjebraök (a_0, \dots, a_M) , där $M < N$. Då är

$$[a_0, \dots, a_N] = [a_0, \dots, a_{N-2}, [a_{N-1}, a_N]] = \frac{p(a_0, \dots, a_{N-2}, [a_{N-1}, a_N])}{q(a_0, \dots, a_{N-2}, [a_{N-1}, a_N])}.$$

Då $N = 2$, ger detta att

$$\begin{aligned} [a_0, \dots, a_N] &= \frac{p(a_0, [a_1, a_2])}{q(a_0, [a_1, a_2])} = \frac{a_0[a_1, a_2] + 1}{[a_1, a_2]} = \frac{a_0 a_1 + \frac{a_0}{a_2} + 1}{a_1 + \frac{1}{a_2}} = \frac{a_2(a_1 a_0 + 1) + a_0}{a_2 a_1 + 1} \\ &= \frac{a_2 p(a_0, a_1) + p(a_0)}{a_2 q(a_0, a_1) + q(a_0)} = \frac{p(a_0, a_1, a_2)}{q(a_0, a_1, a_2)}, \end{aligned}$$

och då $N \geq 3$, ger det att

$$\begin{aligned} [a_0, \dots, a_N] &= \frac{[a_{N-1}, a_N] p(a_0, \dots, a_{N-2}) + p(a_0, \dots, a_{N-3})}{[a_{N-1}, a_N] q(a_0, \dots, a_{N-2}) + q(a_0, \dots, a_{N-3})} \\ &= \frac{\left(a_{N-1} + \frac{1}{a_N}\right) p(a_0, \dots, a_{N-2}) + p(a_0, \dots, a_{N-3})}{\left(a_{N-1} + \frac{1}{a_N}\right) q(a_0, \dots, a_{N-2}) + q(a_0, \dots, a_{N-3})} \\ &= \frac{a_N(a_{N-1} p(a_0, \dots, a_{N-2}) + p(a_0, \dots, a_{N-3})) + p(a_0, \dots, a_{N-2})}{a_N(a_{N-1} q(a_0, \dots, a_{N-2}) + q(a_0, \dots, a_{N-3})) + q(a_0, \dots, a_{N-2})} \\ &= \frac{a_N p(a_0, \dots, a_{N-1}) + p(a_0, \dots, a_{N-2})}{a_N(q(a_0, \dots, a_{N-1}) + q(a_0, \dots, a_{N-2}))} = \frac{p(a_0, \dots, a_N)}{q(a_0, \dots, a_N)}. \quad \blacksquare \end{aligned}$$

Definition 7 Om $a = (a_0, \dots, a_N)$ eller $a = (a_0, a_1, \dots)$ är ett kedjebraök, och $n \leq N$ i det ändliga fallet, definierar vi $p_n(a) = p(a_1, \dots, a_n)$, $q_n(a) = q(a_1, \dots, a_n)$ och kallar talet

$$[a_0, \dots, a_n] = \frac{p_n(a)}{q_n(a)}$$

för den n :e konvergenten till a . Vi definierar också matrisen $R_n(a)$ genom

$$R_0(a) = \begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix}, \quad R_n(a) = \begin{bmatrix} p_n(a) & p_{n-1}(a) \\ q_n(a) & q_{n-1}(a) \end{bmatrix}, \quad n \geq 1,$$

och kallar $R_n(a)$ den n :e konvergentmatrisen till a .

Sats 8 Det gäller att

$$R_n(a) = R_{n-1}(a) \begin{bmatrix} a_n & 1 \\ 1 & 0 \end{bmatrix}, \quad n \geq 1.$$

Bevis Påståendet följer direkt av definition 6. ■

Vi kommer att skriva p_n , q_n och R_n , när detta inte kan leda till missförstånd. Vi kommer också att underförstå att $n \leq N$, då det gäller ändliga kedjebråk.

Korollarium 1 Det gäller att $\det R_n = (-1)^{n-1}$, då $n \geq 0$.

Bevis Påståendet följer av produktsatsen för determinanter. ■

Korollarium 2 Det gäller att

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}, \quad n \geq 1, \quad (1)$$

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_{n-1} q_n}, \quad n \geq 1, \quad (2)$$

$$p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n, \quad n \geq 2, \quad (3)$$

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{(-1)^n a_n}{q_{n-2} q_n}, \quad n \geq 2. \quad (4)$$

Bevis Formel (1) följer av korollarium 1, och (2) är bara en omformulering av (1). Formel (3) följer av att

$$\begin{aligned} p_n q_{n-2} - p_{n-2} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-2} - p_{n-2} (a_n q_{n-1} + q_{n-2}) \\ &= a_n (p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) = (-1)^n a_n, \end{aligned}$$

och (4) är en omformulering av (3). ■

Sats 9 Sätt $r_n = p_n/q_n$. Det gäller då att r_{2n} är strängt växande, r_{2n+1} strängt avtagande, och $r_{2m} < r_{2n+1}$, $m \geq 0$, $n \geq 0$.

Bevis Eftersom $a_n > 0$ då $n \geq 1$, och $q_n > 0$, då $n \geq 0$, följer de två första påståendena av (4) i korollarium 2. Enligt (2) har vi att $r_{2n} < r_{2n+1}$ och $r_{2n} < r_{2n-1}$. Om $2m < 2n + 1$, får vi att $r_{2m} \leq r_{2n} < r_{2n+1}$. Om $2m > 2n + 1$, får vi $r_{2m} < r_{2m-1} \leq r_{2n+1}$. ■

Enkla kedjebråk

Definition 8 Ett kedjebråk (a_0, \dots, a_N) eller (a_0, a_1, \dots) säges vara enkelt, om dess element är heltal.

Sats 10 Antag att a är ett enkelt kedjebråk. Då gäller det att p_n och q_n är relativt prima heltal, och att $R_n \in \text{GL}(2, \mathbf{Z})$. Det gäller också att $0 < q_0 \leq q_1$, och $q_n < q_{n+1}$, om $n \geq 1$. Om $a_0 \geq 0$, gäller det att $p_0 \geq 0$, och $p_n < p_{n+1}$, då $n \geq 0$.

Bevis Det följer av definition 6 att p_n och q_n är heltal. Av det $R_n = p_n q_{n-1} - q_n p_{n-1} = \pm 1$, följer det att $R_n \in \text{GL}(2, \mathbf{Z})$ och att p_n och q_n är relativt prima. De övriga påståendena följer också av definitionen. ■

Sats 11 Om a är ett enkelt kedjebråk, och $\xi > 0$, så är

$$[a_0, \dots, a_{n-1}, \xi] = R_{n-1}(a)\xi, \quad n \geq 1.$$

I det ändliga fallet förutsätter vi att $n \leq N$.

Bevis Påståendet följer av sats 7, definition 6 och att $R_{n-1}(a) = R_{n-1}(a_0, \dots, a_{n-1}, \xi)$. ■

Sats 12 Låt a vara ett enkelt oändligt kedjebråk. Då gäller det att $r_n = [a_0, \dots, a_n]$ har ett gränsvärde då $n \rightarrow \infty$.

Bevis Det gäller enligt sats 9, att r_{2n} är strängt växande, och eftersom $r_{2n} \leq r_1$, också att r_{2n} är uppåt begränsad. På samma sätt följer det att r_{2n+1} är strängt avtagande och nedåt begränsad. Följderna r_{2n} och r_{2n+1} har därför var sitt gränsvärde ξ och ζ . Enligt korollarium 2 är

$$|r_{2n+1} - r_{2n}| = \frac{1}{q_n q_{n+1}},$$

och eftersom q_n , $n \geq 1$, är en strängt växande följd av positiva heltal, så gäller det att $|r_{2n+1} - r_{2n}| \rightarrow 0$ då $n \rightarrow \infty$, vilket visar att $\xi = \zeta$. ■

Definition 9 Med värdet $[a_0, a_1, \dots]$ av det oändliga enkla kedjebråket (a_0, a_1, \dots) skall vi mena gränsvärdet i sats 12.

Sats 13 Om $\xi = [a_0, a_1, \dots]$ är värdet av ett enkelt oändligt kedjebråk, så är

$$\frac{p_{2n}}{q_{2n}} < \xi < \frac{p_{2n+1}}{q_{2n+1}}, \quad n \geq 0.$$

Bevis Beviset av sats 12 visar att p_{2n}/q_{2n} växer strängt mot ξ och att p_{2n+1}/q_{2n+1} avtar strängt mot ξ . ■

Sats 14 Antag att $\xi = [a_0, \dots, a_N, \zeta]$, där $N \geq 1$, och $\zeta \geq 1$, eller att $\xi = [a_0, a_1, \dots]$. Här är (a_0, \dots, a_N) och (a_0, a_1, \dots) enkla kedjebråk. Då gäller det att $a_0 < \xi < a_0 + 1$ och därför att $a_0 = \lfloor \xi \rfloor$ och $\xi \notin \mathbf{Z}$.

Bevis För ändliga kedjebråk ger sats 9 att

$$a_0 = \frac{p_0}{q_0} < [a_0, \dots, a_N, \xi] < \frac{p_1}{q_1} = a_0 + \frac{1}{a_1} \leq a_0 + 1, \quad N \geq 1.$$

För oändliga kedjebråk ger sats 13 att

$$a_0 = \frac{p_0}{q_0} < \xi < \frac{p_1}{q_1} = a_0 + \frac{1}{a_1} \leq a_0 + 1. \quad \blacksquare$$

Definition 10 Låt a vara ett ändligt eller oändligt enkelt kedjebråk. Med den n :e fullständiga konvergenten, $n \leq N$ i det ändliga fallet, skall vi mena värdet $a'_n = [a_n, \dots, a_N]$ respektive $a'_n = [a_n, a_{n+1}, \dots]$.

Sats 15 Låt ξ vara värdet av ett enkelt kedjebråk a . Då är

$$\xi = a'_0, \quad \xi = R_{n-1}a'_n = [a_0, \dots, a_{n-1}, a'_n], \quad n \geq 1,$$

där vi som vanligt antar, att $n \leq N$, om a är ändligt.

Bevis Det följer av sats 11, att $[a_0, \dots, a_{n-1}, a'_n] = R_{n-1}a'_n$. I det ändliga fallet följer påståendet nu av att $\xi = [a_0, \dots, a_{n-1}, a'_n]$ enligt sats 6. I det oändliga fallet följer det att $\xi = R_{n-1}a'_n$, om vi låter $N \rightarrow \infty$ och använder att $\zeta \mapsto R_{n-1}\zeta$ är en kontinuerlig funktion på intervallet $(0, \infty)$. ■

Sats 16 Antag att $[a_0, \dots, a_N, \xi] = [b_0, \dots, b_N, \zeta]$, där (a_0, \dots, a_N) och (b_0, \dots, b_N) är enkla kedjebråk och $\xi \geq 1$ och $\zeta \geq 1$ är reella tal. Då är $(a_0, \dots, a_N) = (b_0, \dots, b_N)$ och $\xi = \zeta$. Det gäller också att $[\xi] = [\zeta]$.

Bevis Vi använder induktion över N . Vi noterar att heltalsdelen av $[a_0, \xi]$ är a_0 , om $\xi > 1$. Om $\xi > 1$ och $\zeta > 1$, följer det att $a_0 = b_0$, och därför är $\xi = \zeta$. Om $\xi = \zeta = 1$, är påståendet trivalt. Om en av ξ och ζ är lika med 1 och den andra större än 1, så kan det inte gälla att $[a_0, \xi] = [b_0, \zeta]$. Påståendet är alltså sant då $N = 0$. Antag nu att påståendet är sant då $N < M$, där $M \geq 1$, och att $[a_0, \dots, a_M, \xi] = [b_0, \dots, b_M, \zeta]$. Då är

$$[a_0, [a_1, \dots, a_M, \xi]] = [b_0, [b_1, \dots, b_M, \zeta]],$$

varför $a_0 = b_0$ och $[a_1, \dots, a_M, \xi] = [b_1, \dots, b_M, \zeta]$. Induktionsantagandet ger nu att $(a_1, \dots, a_M) = (b_1, \dots, b_M)$ och $\xi = \zeta$. Det sista påståendet i satsen är trivalt. ■

Sats 17 Kedjebråken förutsätts vara enkla.

1. Om $[a_0, \dots, a_N] = [b_0, \dots, b_N]$, så är $(a_0, \dots, a_N) = (b_0, \dots, b_N)$.
2. Om $[a_0, \dots, a_N] = [b_0, \dots, b_M]$, $M > N$, så är $M = N + 1$, $b_M = 1$, $a_N = b_N + 1$, och om $N > 0$, så är $(a_0, \dots, a_{N-1}) = (b_0, \dots, b_{N-1})$.
3. Ett ändligt och ett oändligt kedjebråk har inte samma värde.
4. Om två oändliga kedjebråk har samma värde, är de lika.

Bevis Vi använder sats 16 i samtliga fall.

1. Påståendet följer direkt av satsen.
2. Det gäller att $a_N = [b_N, \dots, b_M]$, och om $N > 0$, att $(a_0, \dots, a_{N-1}) = (b_0, \dots, b_{N-1})$. Om $M > N + 1$, eller $b_{N+1} > 1$, är detta inte möjligt, eftersom $[b_N, \dots, b_M]$ då inte är ett heltal.
3. Om $[a_0, \dots, a_N] = [b_0, b_1, \dots]$, så är $a_N = [b_N, b_{N+1}, \dots]$, vilket är omöjligt, eftersom $[b_N, b_{N+1}, \dots]$ inte är ett heltal.
4. Om $[a_0, a_1, \dots] = [b_0, b_1, \dots]$, så är $(a_0, \dots, a_n) = (b_0, \dots, b_n)$ och $a'_{n+1} = b'_{n+1}$ för alla naturliga tal n . I synnerhet är $a_n = b_n$. ■

Sats 18

1. Varje rationellt tal är värdet av precis två olika enkla ändliga kedjebråk, ett med ett jämnt antal konvergenter, ett med ett udda antal.
2. Varje irrationellt tal är värdet av precis ett enkelt oändligt kedjebråk.
3. Värdet av ett enkelt ändligt kedjebråk är rationellt. Värdet av ett enkelt oändligt kedjebråk är irrationellt.

Bevis 1. Det följer av sats 17 att ett rationellt tal inte är värdet av fler än två olika enkla kedjebråk. Om $\xi \in \mathbf{Z}$, så är $\xi = [\xi] = [\xi - 1, 1]$, varmed påståendet är bevisat i det fallet. Om $\xi < 1$ och $\xi \notin \mathbf{Z}$, så är $\xi = a_0 + 1/\zeta = [a_0, \zeta]$, där $a_0 = \lfloor \xi \rfloor$, och $\zeta > 1$. Om $a_N \geq 2$ och (a_0, \dots, a_N) är enkelt, så är också $(a_0, \dots, a_N - 1, 1)$ ett enkelt kedjebråk.

Det räcker därför att vi visar att varje rationellt tal $\xi > 1$ är värdet av ett enkelt kedjebråk (a_0, \dots, a_N) , i vilket $a_0 \geq 1$ och $a_N \geq 2$. Vi kan skriva $\xi = m/n$, där $m > n > 0$ är heltal. Vi visar påståendet med induktion över n . Om $n = 1$, är $\xi \geq 2$ ett heltal, och $\xi = [\xi]$. Antag att påståendet är sant, då $\xi = p/r$ och $1 \leq r < n$. Om $\xi = m/n > 1$ är ett heltal, vet vi att påståendet är sant. Annars ger divisionsalgoritmen att $m = qn + r$, där $1 \leq r < n$. Om $\zeta = n/r$, så är $\zeta > 1$. Vi har att $\xi = q + 1/\zeta = [q, \zeta]$, och påståendet följer av induktionsantagandet.

2. Om ξ är irrationellt, så är $\zeta = \xi - \lfloor \xi \rfloor$ irrationellt, och därför också $1/\zeta$. Definiera talföljderna (a_n) och (ξ_n) rekursivt genom

$$\xi_0 = \xi, \quad a_0 = \lfloor \xi_0 \rfloor, \quad \xi_n = \frac{1}{\xi_{n-1} - a_{n-1}}, \quad a_n = \lfloor \xi_n \rfloor, \quad n \geq 1.$$

Att $a_0 \in \mathbf{Z}$, $\xi_n > 1$ och $a_n \in \mathbf{Z}_+$, då $n \geq 1$, kan visas med induktion. Vi visar att $\xi = [a_0, \dots, a_n, \xi_{n+1}]$, då $n \geq 0$. Då $n = 0$, är $[a_0, \dots, a_n, \xi_{n+1}] = [\lfloor \xi \rfloor, \xi_1] = \lfloor \xi \rfloor + \xi - \lfloor \xi \rfloor = \xi$. Antag att påståendet är sant då $n = m - 1 \geq 0$. Då är

$$[a_0, \dots, a_m, \xi_{m+1}] = [a_0, \dots, a_{m-1}, [a_m, \xi_{m+1}]] = [a_0, \dots, a_{m-1}, \xi_m] = \xi.$$

Påståendet följer av induktionsprincipen. För det enkla oändliga kedjebråket (a_0, a_1, \dots) gäller att $p_n = p_n(a_0, \dots, a_n, \xi_{n+1})$ och $q_n = q_n(a_0, \dots, a_n, \xi_{n+1})$. Om $\zeta = [a_0, a_1, \dots]$, gäller det att

$$\frac{p_{2n}}{q_{2n}} < \xi < \frac{p_{2n+1}}{q_{2n+1}}, \quad \frac{p_{2n}}{q_{2n}} \rightarrow \zeta \quad \text{då} \quad n \rightarrow \infty, \quad \frac{p_{2n+1}}{q_{2n+1}} \rightarrow \zeta \quad \text{då} \quad n \rightarrow \infty,$$

och det följer att $\xi = \zeta$. Entydigheten följer av sats 17.

3. Det första påståendet är självklart. Det andra följer av att om värdet av ett enkelt oändligt kedjebråk vore rationellt, skulle detta värde också vara värdet av ett enkelt ändligt kedjebråk, vilket motsäger sats 17. ■

Avståndet från värdet till en konvergent

Sats 19 Låt ξ vara värdet av ett enkelt oändligt kedjebråk och p_n/q_n en konvergent. Då gäller det att

$$\left| \xi - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}.$$

Bevis Det gäller enligt sats 13 att

$$\frac{p_n}{q_n} < \xi < \frac{p_{n+1}}{q_{n+1}} \quad \text{eller} \quad \frac{p_{n+1}}{q_{n+1}} < \xi < \frac{p_n}{q_n}.$$

Därför är

$$\left| \xi - \frac{p_n}{q_n} \right| < \left| \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \right| = \frac{|p_{n+1}q_n - p_nq_{n+1}|}{q_nq_{n+1}} = \frac{1}{q_nq_{n+1}} \leq \frac{1}{q_n^2}$$

enligt korollarium 2 och sats 10. ■

Sats 20 Låt ξ vara värdet av ett enkelt oändligt kedjebråk. För varje $n \in \mathbf{N}$ gäller minst ett av påståendena

$$\left| \xi - \frac{p_{2n}}{q_{2n}} \right| < \frac{1}{2q_{2n}^2} \quad \text{och} \quad \left| \xi - \frac{p_{2n+1}}{q_{2n+1}} \right| < \frac{1}{2q_{2n+1}^2}.$$

Bevis Om påståendet är falskt, gäller det enligt korollarium 2 att

$$\frac{1}{q_{2n}q_{2n+1}} = \frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} = \frac{p_{2n+1}}{q_{2n+1}} - \xi + \xi - \frac{p_{2n}}{q_{2n}} \geq \frac{1}{2q_{2n+1}^2} + \frac{1}{2q_{2n}^2},$$

vilket ger att $(q_{2n+1} - q_{2n})^2 \leq 0$. Detta är bara möjligt, om $n = 0$ och $a_1 = 1$, och då är $q_0 = q_1 = 1$. I detta fall är

$$0 < \frac{p_1}{q_1} - \xi = a_0 + 1 - \left(a_0 + \frac{a'_2}{1 + a'_2} \right) = \frac{1}{1 + a'_2} < \frac{1}{2} = \frac{1}{2q_1^2},$$

vilket visar att påståendet är sant även i detta fall. ■

Sats 21 Antag att p och $q \neq 0$ är heltal, att ξ är ett irrationellt tal och att

$$\left| \xi - \frac{p}{q} \right| < \frac{1}{2q^2}.$$

Då är p/q en konvergent till det enkla kedjebråk, vars värde är ξ .

Bevis Det gäller att

$$\frac{p}{q} - \xi = \frac{\delta\varepsilon}{q^2},$$

där $0 < \delta < 1/2$ och $\varepsilon = \pm 1$. Om p/q är ett heltal, och $\varepsilon = -1$, så är $p/q = \lfloor \xi \rfloor$, och vi är klara. Annars ger sats 18 att $p/q = [a_0, \dots, a_n]$ är värdet av ett enkelt kedjebråk, för vilket $n \geq 1$ och $\varepsilon = (-1)^{n-1}$. Definiera nu talet ζ genom $\xi = R_n\zeta$, där

$$R_n = \begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix}$$

är den n :e konvergentmatrisen till (a_0, \dots, a_n) . Då är $p_n/q_n = p/q$, och

$$\frac{\delta\varepsilon}{q_n^2} = \frac{p_n}{q_n} - \xi = \frac{p_n}{q_n} - \frac{p_n\zeta + p_{n-1}}{q_n\zeta + q_{n-1}} = \frac{p_nq_{n-1} - p_{n-1}q_n}{q_n(q_n\zeta + q_{n-1})} = \frac{\varepsilon}{q_n(q_n\zeta + q_{n-1})},$$

varav

$$\zeta = \frac{1}{\delta} - \frac{q_{n-1}}{q_n} > 2 - 1 = 1.$$

Eftersom $\xi = [a_0, \dots, a_n, \zeta]$, ger sats 16, att $p_n/q_n = p/q$ är den n :e konvergenten i det enkla kedjebråk, vars värde är ξ . ■

Modulärt ekvivalenta kedjebråk

Sats 22 Om $\xi = [a_0, a_1, \dots]$ är värdet av ett enkelt oändligt kedjebråk, så gäller det att $\xi \sim a'_n$ för alla naturliga tal n .

Bevis Att $\xi \sim a'_0$ är trivialt, och om $n \geq 1$, är $\xi = R_{n-1}a'_n$, och $R_{n-1} \in \text{GL}(2, \mathbf{Z})$. ■

Lemma 1 Antag att $\xi = [a_0, a_1, \dots]$ är värdet av ett enkelt oändligt kedjebråk, att $\zeta > 1$ är ett irrationellt tal, och p, q, r och s är heltal, sådana att $q > s > 0$ och

$$R = \begin{bmatrix} p & r \\ q & s \end{bmatrix} \in \text{GL}(2, \mathbf{Z})$$

Om det gäller att $\xi = R\zeta$, så är $R = R_n$ och $\zeta = a'_{n+1}$ för något positivt heltal n .

Bevis Talet p/q är inte ett heltal, eftersom $q > 1$ och $(p, q) = 1$. Enligt sats 18 är p/q värdet av två enkla ändliga kedjebråk, ett med ett udda antal och ett med ett jämnt konvergener, och antalet konvergener är i båda fallen minst 2. Vi kan alltså välja ett enkelt kedjebråk $b = (b_0, \dots, b_n)$, sådant att det $R = (-1)^{n-1}$ och $p/q = [b_0, \dots, b_n] = p_n/q_n$, där vi med p_n/q_n här avser den n :e konvergenten till b . Eftersom $(p_n, q_n) = (p, s) = 1$, $q_n > 0$ och $q > 0$, så är $p = p_n$ och $q = q_n$. Vi får att

$$p_n s - q_n r = p s - q r = (-1)^{n-1} = p_n q_{n-1} - p_{n-1} q_n.$$

Detta ger att $q_n \mid p_n(s - q_{n-1})$, och eftersom $(p_n, q_n) = 1$, att $q_n \mid (s - q_{n-1})$. Eftersom

$$-q_n \leq -q_{n-1} < s - q_{n-1} < q_n - q_{n-1} < q_n,$$

måste det gälla att $s - q_{n-1} = 0$, varav $s = q_{n-1}$ och $r = p_{n-1}$. Vi får alltså att

$$\xi = \frac{p_n \zeta + p_{n-1}}{q_n \zeta + q_{n-1}} = [b_0, \dots, b_n, \zeta].$$

Vi har att $\xi = [a_0, \dots, a_n, a'_{n+1}]$, och sats 16 ger att $\zeta = a'_{n+1}$ och $[a_0, \dots, a_n] = [b_0, \dots, b_n]$. Det gäller alltså också att p_{n-1}/q_{n-1} och p_n/q_n är den $(n-1)$:a och n :e konvergenten till (a_0, a_1, \dots) . ■

Sats 23 Låt $\xi = [a_0, a_1, \dots]$ och $\zeta = [b_0, b_1, \dots]$ vara värdena av två enkla oändliga kedjebråk. Då gäller det att $\xi \sim \zeta$, om och endast om $a'_n = b'_m$ för några naturliga tal m och n .

Bevis Om $a'_n = b'_m$, gäller det att $\xi \sim a'_n \sim b'_m \sim \zeta$. Antag nu att $\xi \sim \zeta$. Då är $\zeta = R\xi$, där

$$R = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{GL}(2, \mathbf{Z}).$$

Eftersom $R\xi = (-R)\xi$, kan vi antaga att $c\xi + d > 0$. Om vi sätter $S_n = R_n(a_0, a_1, \dots)$, så är $\xi = S_{n-1}a'_n$ för varje heltal $n \geq 1$. Vi får att $\zeta = RS_{n-1}a'_n$. Om p_n/q_n är den n :e konvergenten till (a_0, a_1, \dots) , så är

$$RS_{n-1} = \begin{bmatrix} e_{n-1} & f_{n-1} \\ g_{n-1} & h_{n-1} \end{bmatrix} = \begin{bmatrix} ap_{n-1} + bq_{n-1} & ap_{n-2} + bq_{n-2} \\ cp_{n-1} + dq_{n-1} & cp_{n-2} + dq_{n-2} \end{bmatrix}.$$

Enligt sats 19 finns det tal δ_n , $n = 0, 1, \dots$, sådana att $|\delta_n| < 1$ och

$$p_n = \xi q_n + \frac{\delta_n}{q_n}.$$

Vi får att

$$g_{n-1} = (c\xi + d)q_{n-1} + \frac{c\delta_{n-1}}{q_{n-1}}, \quad h_{n-1} = (c\xi + d)q_{n-2} + \frac{c\delta_{n-2}}{q_{n-2}}.$$

Eftersom $q_n \rightarrow \infty$ då $n \rightarrow \infty$, så gäller det för alla stora n , att $h_{n-1} > 0$. Vidare är, enligt sats 10, $q_{n-1} - q_{n-2} \geq 1$, om $n \geq 3$. Det följer att

$$g_{n-1} - h_{n-1} = (c\xi + d)(q_{n-1} - q_{n-2}) + \frac{c\delta_{n-1}}{q_{n-1}} - \frac{c\delta_{n-2}}{q_{n-2}} \geq (c\xi + d) + \frac{c\delta_{n-1}}{q_{n-1}} - \frac{c\delta_{n-2}}{q_{n-2}},$$

om $n \geq 3$, och vi ser att $g_{n-1} > h_{n-1} > 0$ för alla stora n . Enligt lemma 1 är alltså a'_n också en fullständig konvergent till (b_0, b_1, \dots) för alla tillräckligt stora n . ■

Kroppen $\mathbf{Q}(\sqrt{d})$

Definition 11 Ett heltal $d \neq 1$ säges vara kvadratfritt, om det inte för något primtal p gäller att $p^2 \mid d$.

Sats 24 Om d är ett kvadratfritt heltal, och $x^2 = d$, så är x irrationellt.

Bevis Om $d < 0$, är påståendet trivialt, eftersom ekvationen $x^2 = d$ då saknar reella rötter. Antag att $d \geq 2$. Enligt aritmetikens fundamentalsats är $d = p_1 \dots p_n$ en produkt av olika primtal. Om $x \in \mathbf{Q}$, så är $x = a/b$ för några heltal a och b . Det gäller då att $db^2 = a^2$. I primtalsfaktoriseringen av db^2 förekommer p_1 ett udda antal gånger och i faktoriseringen av a^2 ett jämnt antal gånger. Eftersom detta strider mot aritmetikens fundamentalsats, är satsen bevisad. ■

Definition 12 Låt d vara ett kvadratfritt heltal. Vi betecknar med $\mathbf{Q}(\sqrt{d})$ mängden $\{x + y\sqrt{d}; x, y \in \mathbf{Q}\}$, där \sqrt{d} är en godtycklig rot till ekvationen $x^2 = d$.

Vi noterar att definitionen inte beror på vilken av rötterna x_1 och x_2 vi väljer, eftersom $x_1 = -x_2$.

Sats 25 Om d är ett kvadratfritt heltal, så är $\mathbf{Q}(\sqrt{d})$ en kropp och ett tvådimensionellt vektorrum över \mathbf{Q} .

Bevis Eftersom 0, 1 och -1 är element i $\mathbf{Q}(\sqrt{d})$, räcker det att visa att $\alpha + \beta$ och $\alpha\beta$ tillhör $\mathbf{Q}(\sqrt{d})$, om α och β tillhör $\mathbf{Q}(\sqrt{d})$, och att $1/\alpha \in \mathbf{Q}(\sqrt{d})$, om $\alpha \in \mathbf{Q}(\sqrt{d}) \setminus \{0\}$. Om $\alpha = x + y\sqrt{d}$ och $\beta = z + w\sqrt{d}$, följer detta av att $\alpha + \beta = (x + z) + (y + w)\sqrt{d}$, $\alpha\beta = xz + dyw + (xw + yz)\sqrt{d}$, och

$$\frac{1}{\alpha} = \frac{x}{x^2 - dy^2} - \frac{y}{x^2 - dy^2}\sqrt{d}.$$

Eftersom d är kvadratfritt, så är $x^2 - dy^2 = 0$, bara då $x = y = 0$, vilket betyder att $\alpha = 0$. Eftersom \sqrt{d} är irrationellt, så är 1, \sqrt{d} en bas för $\mathbf{Q}(\sqrt{d})$ över \mathbf{Q} . ■

Definition 13 Om $\alpha = x + y\sqrt{d} \in \mathbf{Q}(\sqrt{d})$, definierar vi konjugatet, spåret och normen av α genom

$$\alpha' = x - y\sqrt{d}, \quad \text{Sp}(\alpha) = \alpha + \alpha' = 2x, \quad N(\alpha) = \alpha\alpha' = x^2 - dy^2.$$

Sats 26 Det gäller att

1. $\alpha \mapsto \alpha'$ är en automorfism på $\mathbf{Q}(\sqrt{d})$,
2. $\alpha \mapsto \text{Sp}(\alpha)$ är en grupphomomorfism $\mathbf{Q}(\sqrt{d}) \rightarrow \mathbf{Q}$,
3. $\alpha \mapsto N(\alpha)$ är en grupphomomorfism $\mathbf{Q}(\sqrt{d})^* \rightarrow \mathbf{Q}^*$,
4. $\alpha' = \alpha$, om och endast om $\alpha \in \mathbf{Q}$.

Bevis Alla påståenden är direkta konsekvenser av definition 13. ■

Sats 27 Om d och e är olika kvadratfria tal, så är $\mathbf{Q}(\sqrt{d}) \cap \mathbf{Q}(\sqrt{e}) = \mathbf{Q}$.

Bevis Antag att $\alpha = x + y\sqrt{d} = z + w\sqrt{e}$, där x, y, z och w är rationella tal. Då är

$$(x - z)^2 = (w\sqrt{e} - y\sqrt{d})^2 = y^2d + w^2e - 2yw\sqrt{d}\sqrt{e}.$$

Om $yw \neq 0$, kan vi lösa ut $\sqrt{d}\sqrt{e}$, kvadrera och få att $de = a^2$ för något heltal a . Eftersom d och e är olika kvadratfria tal, finns det ett primtal, som förekommer precis en gång i faktoriseringen av de . Det måste därför gälla att $yw = 0$. Detta visar att $y = 0$ eller $w = 0$, varför $\alpha \in \mathbf{Q}$. ■

Efter sats 27 kan vi tala om konjugatet, spåret och normen av ett tal i $\bigcup \mathbf{Q}(\sqrt{d})$, där unionen tas över alla kvadratfria heltal, utan att referera till d .

Definition 14 Om \sqrt{d} betecknar den positiva kvadratroten, då $d > 0$, och $\sqrt{d} = i\sqrt{|d|}$, då $d < 0$, definierar vi $\text{Rat } \alpha = x$ och $\text{Irr } \alpha = y$, om $\alpha = x + y\sqrt{d}$.

Kvadratisk irrationella tal

Definition 15 Med diskriminanten $D(\varphi(t))$ av $\varphi(t)$, där $\varphi(t) = at^2 + bt + c \in \mathbf{Z}[t]$, skall vi mena talet $b^2 - 4ac$.

Definition 16 Med ett kvadratisk irrationellt tal menas ett tal $\alpha \in \mathbf{C} \setminus \mathbf{Q}$, sådant att $\varphi(\alpha) = 0$ för något polynom $\varphi(t) = at^2 + bt + c \in \mathbf{Z}[t]$.

Sats 28 Låt $\alpha \in \mathbf{C}$. Då är α kvadratisk irrationellt, om och endast om $\alpha \in \mathbf{Q}(\sqrt{d}) \setminus \mathbf{Q}$ för något kvadratfritt heltal d .

Bevis Antag först att α är kvadratisk irrationellt. Då är α nollställe till ett polynom $\varphi(t) = at^2 + bt + c \in \mathbf{Z}[t]$. Om $D = D(\varphi(t))$, så är därför

$$\alpha = \frac{-b \pm \sqrt{D}}{2a}.$$

Eftersom $\alpha \notin \mathbf{Q}$, så kan inte D vara ett kvadrattal, och därför är $D = e^2d$, där e är ett heltal och d är kvadratfritt. Detta visar att $\alpha \in \mathbf{Q}(\sqrt{d})$.

Antag nu att $\alpha \in \mathbf{Q}(\sqrt{d}) \setminus \mathbf{Q}$. Det gäller enligt sats 26 att

$$(t - \alpha)(t - \alpha') = t^2 - (\text{Sp}(\alpha))t + N(\alpha) \in \mathbf{Q}[t].$$

Det finns därför heltal a, b, c och e , sådana att

$$\varphi(t) = e(t - \alpha)(t - \alpha') = at^2 + bt + c \in \mathbf{Z}[t],$$

och det gäller att $\varphi(\alpha) = 0$. ■

Sats 29 Varje kvadratisk irrationellt tal α är nollställe till ett entydigt bestämt polynom $\varphi(t) = at^2 + bt + c \in \mathbf{Z}[t]$, om vi kräver att $(a, b, c) = 1$ och $a > 0$.

Bevis Om det finns två sådana polynom $\varphi(t)$ och $\psi(t)$, så är båda irreducibla över \mathbf{Q} . Därför finns relativt prima heltal e och f , sådana att $e\varphi(t) = f\psi(t)$, och det följer av förutsättningarna att $e = f = 1$. ■

Definition 17 Om α är kvadratisk irrationellt, så betecknar vi polynomet $\varphi(t)$ i sats 29 med $\varphi_\alpha(t)$.

Sats 30 Om $\psi(t) \in \mathbf{Q}[t]$, och $\psi(\alpha) = 0$, där α är ett kvadratisk irrationellt tal, så är $\psi(\alpha') = 0$.

Bevis Antag att $\psi(t) = xt^2 + yt + z$, där x, y och z är rationella tal. Då är

$$\psi(\alpha') = x(\alpha')^2 + y\alpha' + z = x'(\alpha')^2 + y'\alpha' + z' = (x\alpha^2 + y\alpha + z)' = (\psi(\alpha))' = 0$$

enligt sats 26. ■

Sats 31 Antag att $\gamma \in k = \mathbf{Q}(\sqrt{d})$, och låt $\Psi : k \rightarrow k$ vara den lineära avbildning, för vilken $\Psi(\xi) = \gamma\xi$, $\xi \in k$. Dess karakteristiska polynom är

$$\psi(t) = (t - \gamma)(t - \gamma') = t^2 - \text{Sp}(\gamma)t + N(\gamma)$$

och har rationella koefficienter.

Bevis Antag att α, β är en bas för k över \mathbf{Q} . Då är $\Psi(\alpha) = x\alpha + y\beta$ och $\Psi(\beta) = z\alpha + w\beta$ för några rationella tal x, y, z och w . Avbildningens matris med avseende på basen α, β är lika med

$$\begin{bmatrix} x & z \\ y & w \end{bmatrix},$$

och dess karakteristiska polynom $\psi(t) = (x - t)(w - t) - yz$ har rationella koefficienter. Det gäller att

$$\psi(\gamma) \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} w - \gamma & -y \\ -z & x - \gamma \end{bmatrix} \begin{bmatrix} x - \gamma & y \\ z & w - \gamma \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix},$$

och

$$\begin{bmatrix} x - \gamma & y \\ z & w - \gamma \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} x\alpha + y\beta - \gamma\alpha \\ z\alpha + w\beta - \gamma\beta \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix},$$

vilket visar att $\psi(\gamma) = 0$. Om γ är irrationellt, följer det att $\psi(\gamma') = 0$, och påståendet följer av faktorsatsen. Om $\gamma \in \mathbf{Q}$, så är $x = w = \gamma$ och $y = z = 0$, varför $\psi(t) = (t - \gamma)^2$. ■

Moduler

Definition 18 Låt A vara en additiv undergrupp av $\mathbf{Q}(\sqrt{d})$. Vi säger att A är en modul, om $A = \langle \alpha, \beta \rangle = \{x\alpha + y\beta; x, y \in \mathbf{Z}\}$ för några element α och β i $\mathbf{Q}(\sqrt{d})$, och det gäller att α och β är lineärt oberoende över \mathbf{Q} .

Sats 32 Om $A = \langle \alpha, \beta \rangle$ är en modul, och α och β är lineärt oberoende, gäller det att varje element $\gamma \in A$ kan skrivas $\gamma = x\alpha + y\beta$ med entydigt bestämda heltal x och y .

Bevis Om $\gamma = x\alpha + y\beta = z\alpha + w\beta$, så är $(x - z)\alpha + (y - w)\beta = 0$. Eftersom α och β är lineärt oberoende, är $x - z = y - w = 0$. ■

Definition 19 Om A är en modul, och $\xi \in \mathbf{Q}(\sqrt{d})$, definierar vi $\xi A = \{\xi\gamma; \gamma \in A\}$.

Sats 33 Om A är en modul, och $\xi \neq 0$, så är ξA en modul.

Bevis Om $A = \langle \alpha, \beta \rangle$, där α och β är lineärt oberoende över \mathbf{Q} , så är $\xi A = \langle \xi\alpha, \xi\beta \rangle$, och $\xi\alpha$ och $\xi\beta$ är lineärt oberoende, eftersom $\xi \neq 0$. ■

Definition 20 Om A är en modul, definierar vi $A' = \{\gamma'; \gamma \in A\}$.

Sats 34 Om A är en modul, så är A' en modul.

Bevis Man inser lätt, att om α och β är lineärt oberoende, så är α' och β' lineärt oberoende, och om $A = \langle \alpha, \beta \rangle$, så är $A' = \langle \alpha', \beta' \rangle$. ■

Definition 21 Om A och B är moduler, och $A = \xi B$, för något $\xi \neq 0$ i $\mathbf{Q}(\sqrt{d})$, säger vi att A och B är ekvivalenta och skriver $A \sim B$.

Sats 35 Ekvivalens mellan moduler är en ekvivalensrelation.

Bevis Det gäller att $A = 1A$, vilket visar att $A \sim A$. Om $A \sim B$, så är $A = \xi B$, där $\xi \neq 0$. Det följer att $B = \xi^{-1}A$, varför $B \sim A$. Om $A \sim B$ och $B \sim C$, så är $A = \xi B$ och $B = \zeta C$. Det följer att $A = \xi\zeta C$, vilket visar att $A \sim C$. ■

Ordningar

Definition 22 En ordning i $\mathbf{Q}(\sqrt{d})$ är en modul, som innehåller 1, och är en underring till $\mathbf{Q}(\sqrt{d})$.

Sats 36 Om Ω är en ordning i $\mathbf{Q}(\sqrt{d})$, och $\gamma \in \Omega$, så gäller det att $\text{Sp}(\gamma)$ och $N(\gamma)$ är heltal.

Bevis Antag att $\Omega = \langle \alpha, \beta \rangle$, där α och β är lineärt oberoende över \mathbf{Q} . Då är α, β också en bas för vektorrummet $\mathbf{Q}(\sqrt{d})$ över \mathbf{Q} . Om Ψ är avbildningen, definierad genom $\Psi(\xi) = \gamma\xi$, så gäller det att $\Psi(\alpha) = x\alpha + y\beta$ och $\Psi(\beta) = z\alpha + w\beta$ för några heltal x, y, z och w , eftersom $\gamma\alpha$ och $\gamma\beta$ är element i Ω . Avbildningens karakteristiska polynom $\psi(t)$ har därför heltalskoefficienter, och påståendet följer av sats 31. ■

Definition 23 Vi definierar $\overline{\Omega} = \{\xi \in \mathbf{Q}(\sqrt{d}); \text{Sp}(\xi) \in \mathbf{Z}, N(\xi) \in \mathbf{Z}\}$.

Lemma 2 Om $\text{Sp}(\omega)$ och $N(\omega)$ är heltal, så är $\omega^2 = a\omega + b$ för några heltal a och b .

Bevis Polynomet $\varphi(t) = (t - \omega)(t - \omega')$ har heltalskoefficienter, och $\varphi(\omega) = 0$. ■

Sats 37 $\overline{\Omega}$ är en ordning, och $\overline{\Omega} = \langle 1, \omega \rangle$, där

$$\omega = \begin{cases} \frac{1 + \sqrt{d}}{2}, & \text{om } d \equiv 1 \pmod{4}, \\ \sqrt{d}, & \text{om } d \equiv 2 \pmod{4}, \text{ eller } d \equiv 3 \pmod{4}. \end{cases}$$

Bevis Antag att $\xi = x + y\sqrt{d} \in \overline{\Omega}$, där x och y är rationella tal. Då är $2x$ och $x^2 - dy^2$ heltal. Sätt $m = 2x$, och antag att $y = p/q$, där p och $q > 0$ är relativt prima heltal. Då gäller det att

$$\frac{m^2}{4} - \frac{dp^2}{q^2} = r \in \mathbf{Z},$$

och $4dp^2 = q^2(m^2 - 4r)$. Om $p = 0$, så är $r = 1$. Eftersom $(p, q) = 1$, gäller det i vilket fall som helst att $q^2 \mid 4d$, och eftersom d är kvadratfritt, att $q = 1$ eller $q = 2$. Därför är $y = n/2$, där $n \in \mathbf{Z}$. Att

$$N(\xi) = \frac{m^2}{4} - \frac{dn^2}{4} \in \mathbf{Z}$$

är ekvivalent med att

$$m^2 - dn^2 \equiv 0 \pmod{4}.$$

Eftersom d är kvadratfritt, så är $d \not\equiv 0 \pmod{4}$.

Antag att $d \equiv 1 \pmod{4}$. Då gäller det att $m^2 \equiv n^2 \pmod{4}$, vilket är ekvivalent med att $m \equiv n \pmod{2}$, så att $m = n + 2k$, för något heltal k . Därför är

$$\xi = \frac{m}{2} + \frac{n}{2}\sqrt{d} = k + n\frac{1 + \sqrt{d}}{2}.$$

Omvänt, om ξ är av denna form, så gäller det att $\text{Sp}(\xi) = 2k + n \in \mathbf{Z}$ och

$$N(\xi) = \left(k + n\frac{1 + \sqrt{d}}{2}\right) \left(k + n\frac{1 - \sqrt{d}}{2}\right) = k^2 + nk + n^2\frac{1 - d}{4} \in \mathbf{Z},$$

eftersom $d \equiv 1 \pmod{4}$. I detta fall är alltså $\overline{\Omega} = \langle 1, \omega \rangle$, där

$$\omega = \frac{1 + \sqrt{d}}{2}.$$

Antag att $d \equiv 2 \pmod{4}$ eller $d \equiv 3 \pmod{4}$. Om n är udda, så är $n^2 \equiv 1 \pmod{4}$, och $d \equiv m^2 \pmod{4}$. Detta ger att $d \equiv 0 \pmod{4}$ eller $d \equiv 1 \pmod{4}$, vilket strider mot förutsättningarna. De måste alltså gälla, att n är jämnt, så att $n^2 \equiv 0 \pmod{4}$, och detta visar att också m är jämnt. Därför är både x och y heltal. Det följer att $\overline{\Omega} = \langle 1, \omega \rangle$, där $\omega = \sqrt{d}$.

Det är klart att $\overline{\Omega}$ är en modul, och efter lemma 2 också att $\overline{\Omega}$ är en ring. ■

Sats 38 Låt ω vara som i sats 37. Om f är ett positivt heltal, så är $\Omega_f = \langle 1, f\omega \rangle$ en ordning i $\mathbf{Q}(\sqrt{d})$, och varje ordning i $\mathbf{Q}(\sqrt{d})$ är av formen Ω_f för något positivt heltal f .

Bevis Eftersom $f\omega \in \overline{\Omega}$, så är $\text{Sp}(f\omega)$ och $N(f\omega)$ heltal. Det följer av lemma 2 att Ω_f är en ring. Låt Ω vara en ordning i $\mathbf{Q}(\sqrt{d})$. Då är $\Omega \subseteq \overline{\Omega}$ enligt sats 36. Varje element i Ω är därför av formen $x + y\omega$, där x och y är heltal. Eftersom Ω är en ring, så gäller det att $\mathbf{Z} \subseteq \Omega$. Det kan inte vara så, att $\Omega = \mathbf{Z}$, eftersom Ω innehåller två lineärt oberoende element. Det finns därför ett minsta positivt heltal f , sådant att $f\omega \in \Omega$. Om $x + y\omega \in \Omega$, så kan vi dividera y med f , och få att $y = qf + r$, där $0 \leq r < f$. Det gäller då att $x + y\omega - x - qf\omega = r\omega \in \Omega$, och det är möjligt bara om $r = 0$, eftersom f är minimalt. Det gäller alltså att $x + y\omega = x + qf\omega \in \Omega_f$. ■

Korollarium 3 Om Ω är en ordning, och $\gamma \in \Omega$, så gäller det att $\gamma' \in \Omega$.

Bevis Påståendet följer av att $(f\omega)' \in \Omega_f$. ■

Lemma 3 Låt α, β, γ och η vara element i $\mathbf{Q}(\sqrt{d})$, och antag att

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = R \begin{bmatrix} \gamma \\ \eta \end{bmatrix}, \quad R = \begin{bmatrix} p & r \\ q & s \end{bmatrix} \in \text{GL}(2, \mathbf{Z}).$$

Då är $\text{Sp}(\alpha^2) \text{Sp}(\beta^2) - (\text{Sp}(\alpha\beta))^2 = \text{Sp}(\gamma^2) \text{Sp}(\eta^2) - (\text{Sp}(\gamma\eta))^2$.

Bevis Det gäller att

$$\begin{aligned} \text{Sp}(\alpha^2) &= p^2 \text{Sp}(\gamma^2) + r^2 \text{Sp}(\eta^2) + 2pr \text{Sp}(\gamma\eta), \\ \text{Sp}(\beta^2) &= q^2 \text{Sp}(\gamma^2) + s^2 \text{Sp}(\eta^2) + 2qs \text{Sp}(\gamma\eta), \\ \text{Sp}(\alpha\beta) &= pq \text{Sp}(\gamma^2) + rs \text{Sp}(\eta^2) + (ps + qr) \text{Sp}(\gamma\eta). \end{aligned}$$

Man ser att

$$\begin{bmatrix} \text{Sp}(\alpha^2) & \text{Sp}(\alpha\beta) \\ \text{Sp}(\alpha\beta) & \text{Sp}(\beta^2) \end{bmatrix} = R \begin{bmatrix} \text{Sp}(\gamma^2) & \text{Sp}(\gamma\eta) \\ \text{Sp}(\gamma\eta) & \text{Sp}(\eta^2) \end{bmatrix} R^t,$$

och påståendet följer av produktsatsen för determinanter. ■

Sats 39 Om $\langle \alpha, \beta \rangle = \langle \gamma, \eta \rangle$ är en ordning, så är

$$\text{Sp}(\alpha^2) \text{Sp}(\beta^2) - (\text{Sp}(\alpha\beta))^2 = \text{Sp}(\gamma^2) \text{Sp}(\eta^2) - (\text{Sp}(\gamma\eta))^2.$$

Bevis Det finns en matris R , som i lemma 3, och därför följer påståendet av lemma 3. ■

Definition 24 Med diskriminanten $D(\Omega)$, där Ω är en ordning, skall vi mena talet

$$\text{Sp}(\alpha^2) \text{Sp}(\beta^2) - (\text{Sp}(\alpha\beta))^2,$$

där α och β är element i $\mathbf{Q}(\sqrt{d})$, sådana att $\Omega = \langle \alpha, \beta \rangle$. Vi definierar också $D_f = D(\Omega_f)$, $f \in \mathbf{Z}_+$.

Sats 40 Om $d \equiv 1 \pmod{4}$, så är $D_f = f^2d$, och om $d \equiv 2 \pmod{4}$ eller $d \equiv 3 \pmod{4}$, så är $D_f = 4f^2d$.

Bevis Antag att $d \equiv 1 \pmod{4}$. Då är

$$\text{Sp}(\omega) = \text{Sp}\left(\frac{1+\sqrt{d}}{2}\right) = 1, \quad \text{Sp}(\omega^2) = \text{Sp}\left(\frac{1+d}{4} + \frac{\sqrt{d}}{2}\right) = \frac{1+d}{2},$$

varav

$$\text{Sp}(1^2) \text{Sp}((f\omega)^2) - (\text{Sp}(1 \cdot f\omega))^2 = 2 \cdot f^2 \cdot \frac{1+d}{2} - f^2 = f^2d.$$

Om $d \equiv 2 \pmod{4}$ eller $d \equiv 3 \pmod{4}$, så är

$$\text{Sp}(\omega) = \text{Sp}(\sqrt{d}) = 0, \quad \text{Sp}(\omega^2) = \text{Sp}(d) = 2d,$$

och $D_f = 4f^2d$. ■

Vi noterar att en ordning är entydigt bestämd av sin diskriminant.

Sats 41 Om Ω är en ordning, och $\varepsilon \in \Omega$, så gäller det att ε är inverterbart i ringen Ω , om och endast om $N(\varepsilon) = \pm 1$.

Bevis Om ε är inverterbart, så finns det ett element $\delta \in \Omega$, sådant att $\delta\varepsilon = 1$. Då är $N(\delta)N(\varepsilon) = N(\delta\varepsilon) = N(1) = 1$, och det följer att $N(\varepsilon) = \pm 1$, eftersom $N(\delta)$ och $N(\varepsilon)$ båda är heltal. Omvänt, om $N(\varepsilon) = \pm 1$, så är $\varepsilon\varepsilon' = \pm 1$, och eftersom $\pm\varepsilon' \in \Omega$ enligt korollarium 3, så är ε inverterbart. ■

Sats 42 Då $d = -1$ och $f = 1$, är de inverterbara elementen i $\Omega_f \pm 1$ och $\pm i$. Då $d = -3$ och $f = 1$, är de ± 1 och $(\pm 1 \pm i\sqrt{3})/2$. För övriga värden på $d < 0$ och f är de enda inverterbara elementen ± 1 .

Bevis Vi noterar att $N(\xi) \geq 0$, då $\xi \in \mathbf{Q}(\sqrt{d})$ och $d < 0$. Sätt $\varepsilon = x + yf\omega$, och antag att ε är inverterbart. Då är $N(\varepsilon) = 1$. Antag att $d < 0$ och $d \equiv 1 \pmod{4}$. Då är $\omega = (1 + \sqrt{d})/2$, och

$$\begin{aligned} N(\varepsilon) &= x^2 + xyf(\omega + \omega') + y^2f^2\omega\omega' \\ &= x^2 + xyf + y^2f^2\frac{1+|d|}{4} = \frac{(2x + yf)^2 + y^2f^2|d|}{4} \geq 0. \end{aligned}$$

Om $y = 0$, så är $x = \pm 1$.

Antag att $y \neq 0$. Om $f \geq 2$, så är $y^2f^2|d| \geq 12$, eftersom $d \leq -3$. Om $f = 1$ och $d \leq -7$, så är $y^2f^2|d| \geq 7$. I dessa fall är alltså ± 1 de enda inverterbara elementen. Antag att $d = -3$ och $f = 1$. Då är

$$N(\varepsilon) = \frac{(2x + y)^2 + 3y^2}{4}.$$

Det gäller alltså att $y = \pm 1$, och $2x + y = \pm 1$. Förutom ± 1 , är alltså också $(\pm 1 \pm i\sqrt{3})/2$ inverterbara.

Antag nu att $d < 0$, och $d \equiv 2 \pmod{4}$ eller $d \equiv 3 \pmod{4}$. Nu är $\omega = \sqrt{d}$, och $N(\varepsilon) = x^2 + y^2f^2|d| \geq 0$. Om $y = 0$, så är $x = \pm 1$. Om $y \neq 0$, och $d < -1$ eller $f > 1$, så är $N(\varepsilon) > 1$. Om $y \neq 0$, $d = -1$ och $f = 1$, så är $N(\varepsilon) = 1$, bara då $x = 0$ och $y = \pm 1$. ■

Sats 43 Om $d > 1$, så finns det ett inverterbart element $\varepsilon > 1$ i Ω_f , sådant att varje inverterbart element i Ω_f är av formen $\pm\varepsilon^n$ för något heltal n . Det gäller att $\varepsilon = (1 + \sqrt{5})/2$, om $d = 5$ och $f = 1$. Annars är $\varepsilon = x + yf\omega$ för några relativt prima positiva heltal x och y . Om $\eta = z + wf\omega > 1$ är inverterbart, så är $x \leq z$ och $y \leq w$. Om $N(\varepsilon) = 1$, så är $N(\eta) = 1$ för alla inverterbara element η . Om $N(\varepsilon) = -1$, så är $N(\pm\varepsilon^n) = 1$, om och endast om n är jämnt.

Bevis Vi visar först att det finns ett inverterbart element $\eta > 1$. Sätt $\alpha = f\omega$ och $\xi = -\alpha'$. Då är $\xi > 0$. Låt (a_0, a_1, \dots) vara kedjebraaket vars värde är ξ . Enligt sats 13 är $a_0 \geq 0$, och därför är $p_n > 0$ och $q_{n+1} > q_n > 0$, då $n \geq 1$, enligt sats 10. Enligt sats 19 gäller det att

$$\left| \xi - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}, \quad n \geq 0.$$

Det finns alltså oändligt många olika par (p, q) av positiva heltal, sådana att

$$\left| \xi - \frac{p}{q} \right| < \frac{1}{q^2}.$$

Olikheten ger att

$$\left| \xi - \frac{p}{q} \right| \left| \xi' - \frac{p}{q} \right| < \frac{1}{q^2} \left| \xi' - \frac{p}{q} \right|,$$

varav

$$|(p + q\alpha)(p + q\alpha')| = |(q\xi - p)(q\xi' - p)| < \left| \xi' - \frac{p}{q} \right| \leq |\xi' - \xi| + \left| \xi - \frac{p}{q} \right| < |\xi' - \xi| + 1.$$

Eftersom $N(p + q\alpha) = (p + q\alpha)(p + q\alpha') \in \mathbf{Z}$, så finns det ett heltal m och oändligt många par av positiva heltal (p, q) , sådana att $|m| < |\xi' - \xi| + 1$ och $N(p + q\alpha) = m$. Det finns därför två olika par (p, q) och (r, s) av positiva heltal, sådana att

$$p \equiv r \pmod{m}, \quad q \equiv s \pmod{m}, \quad N(p + q\alpha) = N(r + s\alpha) = m.$$

Eftersom $\alpha > 0$, kan vi välja talen p, q, r och s så, att $0 < r + s\alpha < p + q\alpha$. Då är

$$\eta = \frac{p + q\alpha}{r + s\alpha} > 1,$$

och $N(\eta) = 1$. Att $\eta \in \Omega_f$ följer av att

$$\begin{aligned} \eta - 1 &= \frac{p + q\alpha}{r + s\alpha} - 1 = \frac{p - r + (q - s)\alpha}{r + s\alpha} = \frac{mg + mh\alpha}{r + s\alpha} \\ &= \frac{m(g + h\alpha)(r + s\alpha')}{(r + s\alpha)(r + s\alpha')} = (g + h\alpha)(r + s\alpha') \end{aligned}$$

för några heltal g och h .

Låt nu $\eta = x + yf\omega$ vara ett godtyckligt inverterbart element i Ω_f , sådant att $\eta > 1$. Det gäller att $\omega - \omega' > 0$. Eftersom $\eta\eta' = \pm 1$, så är $\eta' < 1$, vilket ger att $yf(\omega - \omega') = \eta - \eta' > 0$. Detta visar att $y > 0$. Då $d \equiv 2 \pmod{4}$ eller $d \equiv 3 \pmod{4}$, så är $f\omega' = -f\sqrt{d} < -1$. Då $d \equiv 1 \pmod{4}$, är $f\omega' = f(1 - \sqrt{d})/2 < -1$, utom då $d = 5$ och $f = 1$. I detta fall är $f\omega' < 0$. Eftersom $|x + yf\omega'| = |\eta'| < 1$, så är $x > 0$, utom då $d = 5$ och $f = 1$, i vilket fall $x \geq 0$.

Det finns alltså ett minsta inverterbart element $\varepsilon > 1$. Om $d = 5, f = 1$, så är $\varepsilon = 0 + 1 \cdot \omega = (1 + \sqrt{5})/2$, och det gäller att $N(\eta) = -1$. Annars är $\varepsilon = x + yf\omega$, där x och y är relativt prima positiva heltal. Låt åter $\eta > 1$ vara ett inverterbart element. Då är $1 < \varepsilon \leq \eta$. Låt n vara det största positiva heltal, för vilket $\varepsilon^n \leq \eta$. Då är $1 \leq \eta/\varepsilon^n < \varepsilon$, och därför är $\eta = \varepsilon^n$. I annat fall är nämligen η/ε^n inverterbart, och $1 < \eta/\varepsilon^n < \varepsilon$, vilket strider mot att ε är minimalt. Om $0 < \eta < 1$ är inverterbart, så är $1/\eta > 1$ inverterbart, och därför är $\eta = \varepsilon^n$ för något negativt heltal n . Om $\eta < 0$ är inverterbart, så är $-\eta > 0$ inverterbart, och därför är $\eta = -\varepsilon^n$ för något heltal n .

Om p är ett primtal, som delar x och y , så gäller det att p^2 delar $N(x + yf\omega)$. Detta visar att x och y är relativt prima. Det sista påståendet i satsen är självklart. ■

Definition 25 Vi kallar talet ε i sats 43 för det fundamentala inverterbara elementet i Ω_f .

Sats 44 Antag att $d > 1$. Om $\varepsilon = x + yf\omega$ är det fundamentala inverterbara elementet i Ω_f , så är x/y en av konvergenterna p_n/q_n till det kedjebråk, vars värde är $-f\omega'$. Om $N(p_n + q_nf\omega) = \pm 1$, och $N(p_k + q_kf\omega) \neq \pm 1$, då $k < n$, så är $x = p_n, y = q_n$. Även då $d \equiv 1 \pmod{4}$, och $\Omega = \langle 1, f\sqrt{d} \rangle$, så gäller det för det fundamentala inverterbara elementet $x + yf\sqrt{d}$ i Ω , att x/y är en av konvergenterna i kedjebråket, vars värde är $f\sqrt{d}$.

Bevis Om $d = 5$ och $f = 1$, så är $0 < -f\omega' = (\sqrt{5} - 1)/2 < 1$. Det följer att $a_0 = 0$ i kedjebracket, varför $p_0 = 0 = x$, och $q_0 = 1 = y$. Antag i fortsättningen av beviset att $d \neq 5$ eller $f \neq 1$. Det gäller att

$$\left| \frac{x}{y} + f\omega' \right| = \left| \frac{x + yf\omega'}{y} \right| = \left| \frac{N(x + yf\omega)}{y(x + yf\omega)} \right| = \frac{1}{y(x + yf\omega)}.$$

Om $d \equiv 1 \pmod{4}$, så är $f\omega > 2$, varav $y(x + yf\omega) > y^2f\omega > 2y^2$. Då $d \equiv 2 \pmod{4}$ eller $d \equiv 3 \pmod{4}$, är $\omega = \sqrt{d}$, och $d \geq 2$. Eftersom $N(x + yf\omega) = x^2 - y^2f^2d = \pm 1$, så är $x^2 \geq y^2f^2d - 1 \geq y^2d - 1 \geq y^2d - y^2$, varav $x \geq y\sqrt{d-1}$. Detta ger att

$$y(x + yf\omega) = y(x + yf\sqrt{d}) \geq y(y\sqrt{d-1} + y\sqrt{d}) > 2y^2.$$

I båda fallen gäller det alltså att

$$\left| \frac{x}{y} + f\omega' \right| < \frac{1}{2y^2}.$$

Att x/y är en konvergent följer nu av sats 21. Enligt sats 10 är p_n strängt växande, och eftersom x och y är minimala positiva heltal, följer det att x/y är den första konvergenten p_n/q_n , för vilken $N(p_n + q_nf\omega) = \pm 1$. Eftersom $(x, y) = (p_n, q_n) = 1$, och alla fyra talen är positiva, så är $x = p_n$ och $y = q_n$. ■

Koefficientringar

Definition 26 Koefficientringen Ω_A till en modul A är $\Omega_A = \{\xi \in \mathbf{Q}(\sqrt{d}); \xi A \subseteq A\}$.

Sats 45 Om A är en modul, så gäller det att $1 \in \Omega_A$, och Ω_A är en underring till $\mathbf{Q}(\sqrt{d})$.

Bevis Självklart gäller det att $1 \in \Omega_A$, och att $\alpha - \beta \in \Omega_A$ och $\alpha\beta \in \Omega_A$, om α och β är element i Ω_A . ■

Sats 46 Om Ω är en ordning, så är $\Omega_\Omega = \Omega$. Om A och B är ekvivalenta moduler, så är $\Omega_A = \Omega_B$.

Bevis Om $\xi \in \Omega$, så gäller det att $\xi\Omega \subseteq \Omega$, eftersom Ω är en ring. Om $\xi\Omega \subseteq \Omega$, så gäller det att $\xi = \xi \cdot 1 \in \Omega$. Detta visar att $\Omega_\Omega = \Omega$. Antag att $A = \zeta B$. Då är $B = \zeta^{-1}A$. Om $\xi \in \Omega_A$ och $\beta \in B$, så gäller det att $\alpha = \zeta\beta \in A$. Det medför att $\xi\alpha = \zeta\xi\beta \in A$, varför $\xi\beta \in B$. Det gäller alltså att $\Omega_A \subseteq \Omega_B$. Den omvända inklusionen följer av symmetri. ■

Sats 47 Antag att $\gamma \in \mathbf{Q}(\sqrt{d})$ är irrationellt. Om $\varphi_\gamma(t) = at^2 + bt + c$ och $A = \langle 1, \gamma \rangle$, så är $\Omega_A = \langle 1, a\gamma \rangle$ en ordning, och $D(\Omega_A) = D(\varphi_\gamma(t)) = b^2 - 4ac$.

Bevis Eftersom γ är irrationellt, så är 1 och γ lineärt oberoende över \mathbf{Q} , och utgör därför en bas för $\mathbf{Q}(\sqrt{d})$. Antag att $\xi \in \Omega_A$. Då gäller det att $\xi A \subseteq A$, och $\xi = x + y\gamma \in \mathbf{Q}(\sqrt{d})$, där x och y är rationella tal. Det gäller att $\xi \cdot 1 = x + y\gamma \in A$. Eftersom $A = \langle 1, \gamma \rangle$, så är $x + y\gamma = z + w\gamma$ för några heltal z och w , och eftersom 1 och γ är lineärt oberoende över \mathbf{Q} , så är $x = z$ och $y = w$ båda heltal. Eftersom $\varphi_\gamma(\gamma) = 0$, så gäller det att $\gamma^2 = -(b\gamma + c)/a$. Vi får att

$$\xi\gamma = x\gamma + y\gamma^2 = -\frac{cy}{a} + \left(x - \frac{by}{a}\right)\gamma \in A,$$

av vilket det, som tidigare, följer att cy/a och $x - by/a$ är heltal, och eftersom x och y är heltal, så är by/a ett heltal. Eftersom $a \mid by$, $a \mid cy$ och $(a, b, c) = 1$, så gäller det att $a \mid y$.

Detta visar att $\xi \in \langle 1, a\gamma \rangle$. Om $\xi \in \langle 1, a\gamma \rangle$, så är $\xi = x + ya\gamma$, där x och y är heltal. Det följer direkt att $\xi \cdot 1 \in A$. Eftersom $a\gamma^2 = -b\gamma - c$, så gäller det att $\xi\gamma \in A$. Vi har nu visat att $\Omega_A = \langle 1, a\gamma \rangle$, och därför också att Ω_A är en modul och därmed en ordning. Eftersom $(a\gamma)^2 + b(a\gamma) + ac = 0$, så är $\text{Sp}(a\gamma) = -b$, och $\text{Sp}(a^2\gamma) = \text{Sp}(-b(a\gamma) - ac) = b^2 - 2ac$, av vilket påståendet om diskriminanten följer. ■

Korollarium 4 Om A är en modul, så är Ω_A en ordning. Det gäller att $\Omega_{A'} = \Omega_A$.

Bevis Det första påståendet följer av sats 46 och att $\langle \alpha, \beta \rangle \sim \langle 1, \gamma \rangle$, där $\gamma = \beta/\alpha$. Det andra påståendet följer nu av korollarium 3. ■

Element med föreskriven norm

Sats 48 Låt A vara en modul. Om $A = \langle \alpha_1, \beta_1 \rangle = \langle \alpha_2, \beta_2 \rangle$, $\Omega_A = \langle \gamma_1, \eta_1 \rangle = \langle \gamma_2, \eta_2 \rangle$, och

$$\begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix} = R_1 \begin{bmatrix} \gamma_1 \\ \eta_1 \end{bmatrix}, \quad \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} = R_2 \begin{bmatrix} \gamma_2 \\ \eta_2 \end{bmatrix},$$

där R_1 och R_2 är kvadratiske matriser över \mathbf{Q} av ordning 2, så är $|\det R_1| = |\det R_2|$.

Bevis Matriserna S och T , givna av

$$\begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix} = S \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix}, \quad \begin{bmatrix} \gamma_2 \\ \eta_2 \end{bmatrix} = T \begin{bmatrix} \gamma_1 \\ \eta_1 \end{bmatrix},$$

tillhör $\text{GL}(2, \mathbf{Z})$, och $R_1 = SR_2T$, varav $|\det R_1| = |\det S||\det R_2||\det T| = |\det R_2|$. ■

Definition 27 Låt $A = \langle \alpha, \beta \rangle$ vara en modul, och antag att $\Omega_A = \langle \gamma, \eta \rangle$. Om

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = R \begin{bmatrix} \gamma \\ \eta \end{bmatrix},$$

där R är en kvadratisk matris över \mathbf{Q} av ordning 2, definierar vi $N(A) = |\det R|$.

Sats 49 Låt A vara en modul. Då gäller det att $N(A) \in \mathbf{Q}$, och $N(A) > 0$. Om A är en ordning, så är $N(A) = 1$. Det gäller att $N(\xi A) = |N(\xi)|N(A)$.

Bevis Det första påståendet följer direkt av definitionen, eftersom R är en inverterbar matris med rationella element. Om A är en ordning, så är $\Omega_A = A$ enligt sats 46, och vi kan låta R vara enhetsmatrisen. Antag att $A = \langle \alpha, \beta \rangle$. Enligt sats 31 är $N(\xi)$ den konstanta termen i det karakteristiska polynomet till avbildningen Ψ , definierad genom $\Psi(\zeta) = \xi\zeta$. Om S^t är avbildningens matris med avseende på basen α, β , så är alltså $\det S = N(\xi)$, och

$$\begin{bmatrix} \xi\alpha \\ \xi\beta \end{bmatrix} = S \begin{bmatrix} \alpha \\ \beta \end{bmatrix}.$$

Enligt sats 46 har $A = \langle \alpha, \beta \rangle$ och $\gamma A = \langle \gamma\alpha, \gamma\beta \rangle$ samma koefficientring $\Omega = \langle \gamma, \eta \rangle$. Om

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = R \begin{bmatrix} \gamma \\ \eta \end{bmatrix},$$

så är

$$\begin{bmatrix} \xi\alpha \\ \xi\beta \end{bmatrix} = SR \begin{bmatrix} \gamma \\ \eta \end{bmatrix},$$

varav $N(\xi A) = |\det(SR)| = |\det S||\det R| = |N(\xi)|N(A)$. ■

Sats 50 Om $\varphi_\gamma(t) = at^2 + bt + c$, så är $N(\langle 1, \gamma \rangle) = 1/a$.

Bevis Påståendet följer direkt av sats 47 ■

Definition 28 Om $A = \langle \alpha, \beta \rangle$ och $B = \langle \gamma, \eta \rangle$ är moduler i $\mathbf{Q}(\sqrt{d})$, definierar vi deras produkt genom $AB = \{x\alpha\gamma + y\alpha\eta + z\beta\gamma + w\beta\eta; x, y, z, w \in \mathbf{Z}\}$.

Det är lätt att se att definitionen inte beror på vilka baser vi använder i modulerna, eftersom övergångsmatrisen från en bas till en annan är unimodulär.

Definition 29 Om A är en modul, så definierar vi A^{-1} genom

$$A^{-1} = \frac{1}{N(A)}A',$$

och kallar A^{-1} för inversen till A .

Sats 51 Om A är en modul, så gäller det att $AA^{-1} = \Omega_A$, och $N(A^{-1}) = (N(A))^{-1}$.

Bevis Antag först att $A = \langle 1, \gamma \rangle$. Då är $A' = \langle 1, \gamma' \rangle$, och $N(A) = 1/a$ med beteckningar som i sats 50. Vi får att

$$\begin{aligned} AA^{-1} &= a\{x + y\gamma + z\gamma' + w\gamma\gamma'; x, y, z, w \in \mathbf{Z}\} \\ &= a\{x + y\gamma + z\left(-\gamma - \frac{b}{a}\right) + w\frac{c}{a}; x, y, z, w \in \mathbf{Z}\} \\ &= \{xa - zb + wc + (y - z)a\gamma; x, y, z, w \in \mathbf{Z}\} = \langle 1, a\gamma \rangle = \Omega_A, \end{aligned}$$

eftersom $(a, b, c) = 1$. En godtycklig modul kan skrivas $A = \xi B$, där $B = \langle 1, \gamma \rangle$, och det gäller att $A' = \xi' B'$. Vi har då att

$$AA^{-1} = \frac{1}{N(A)}AA' = \frac{\xi\xi'}{N(A)}BB' = \frac{\xi\xi'N(B)}{N(A)}\Omega_B = \frac{N(\xi)N(B)}{N(A)}\Omega_A = \frac{\pm N(A)}{N(A)}\Omega_A = \Omega_A$$

enligt satserna 46 och 49.

Om $A = \langle \alpha, \beta \rangle$ och $\Omega_A = \langle \gamma, \eta \rangle$, så är $A' = \langle \alpha', \beta' \rangle$ och $\Omega_{A'} = \langle \gamma', \eta' \rangle$, vilket visar att $N(A) = N(A')$. Sats 49 ger nu att $N(A^{-1}) = (N(A))^{-2}N(A) = (N(A))^{-1}$. ■

Definition 30 Modulerna A och B i $\mathbf{Q}(\sqrt{d})$ kallas strikt ekvivalenta, om det finns ett element $\xi \in \mathbf{Q}(\sqrt{d})$, sådant att $A = \xi B$, och $N(\xi) > 0$. Vi skriver i så fall $A \approx B$.

Sats 52 Om $d < 0$, eller om det finns ett inverterbart element $\varepsilon \in \Omega_A$, sådant att $N(\varepsilon) = -1$, så gäller det att $A \sim B$ om och endast om $A \approx B$. Om $d > 0$, $N(\varepsilon) = 1$ för alla inverterbara element i Ω_A , och $A = \xi B$ för något $\xi \in \mathbf{Q}(\sqrt{d})$, för vilket $N(\xi) < 0$, så gäller det att $A \not\approx B$.

Bevis Om $d < 0$, så är $N(\xi) \geq 0$ för alla $\xi \in \mathbf{Q}(\sqrt{d})$, och påståendet är trivialt. Antag att $d > 0$, $N(\varepsilon) = -1$ för något inverterbart element ε i Ω_A , och $A = \xi B$, där $N(\xi) < 0$. Eftersom ε och ε^{-1} båda är element i Ω_A , så är $A = \varepsilon A = \varepsilon\xi B$, och eftersom $N(\varepsilon\xi) > 0$, så gäller det att $A \approx B$. Antag att $A = \xi B = \zeta B$, där $N(\xi)$ och $N(\zeta)$ har olika tecken. Likheten ger att $B = \xi^{-1}\zeta B = \xi\zeta^{-1}B$, vilket visar att både $\xi^{-1}\zeta$ och $\xi\zeta^{-1}$ är element i $\Omega_B = \Omega_A$. Därför är $\varepsilon = \xi^{-1}\zeta$ inverterbart i Ω_A , och $N(\varepsilon) = -1$. ■

Definition 31 Elementen ξ och ζ i modulen A säges vara strikt associerade, om $\xi = \varepsilon\zeta$ för något element $\varepsilon \in \Omega_A$, för vilket $N(\varepsilon) = 1$. Vi skriver då $\xi \cong \zeta$.

Sats 53 Strikt ekvivalens av modulelement i A är en ekvivalensrelation på A .

Bevis Påståendet följer direkt av definitionen. ■

Definition 32 Om $\xi \in A$, där A är en modul, så skriver vi $\hat{\xi} = \{\zeta \in A; \xi \cong \zeta\}$. Vi skriver också $\hat{A} = \{\hat{\xi}; \xi \in A\}$.

Sats 54 Om A är en modul och $\xi \cong \zeta$, där ξ och ζ är element i A , så är $N(\xi) = N(\zeta)$.

Bevis Det finns ett inverterbart element $\varepsilon \in \Omega_A$, sådant att $N(\varepsilon) = 1$ och $\xi = \varepsilon\zeta$. Därför är $N(\xi) = N(\varepsilon)N(\zeta) = N(\zeta)$. ■

Definition 33 Om A är en modul, och $\xi \in A$, sätter vi $N(\hat{\xi}) = N(\xi)$.

Lemma 4 Låt A och B vara moduler med samma koefficientring, och antag att ξ och ζ är element i A med positiv norm. Då gäller det att $\xi B = \zeta B$, om och endast om $\xi \cong \zeta$.

Bevis Om $\xi B = \zeta B$, så är $\zeta^{-1}\xi B = B$ och $\xi^{-1}\zeta B = B$, vilket visar att $\zeta^{-1}\xi$ och $\xi^{-1}\zeta$ båda är element i Ω_B . Det följer också att $\zeta^{-1}\xi$ är inverterbart i Ω_B , eftersom $(\zeta^{-1}\xi)^{-1} \in \Omega_B$. Omvänt, om $\zeta^{-1}\xi \in \Omega_B$ är inverterbart, så gäller det att $\xi^{-1}\zeta \in \Omega_B$. Därför gäller det att $\zeta^{-1}\xi B \subseteq B$ och $\xi^{-1}\zeta B \subseteq B$, av vilket det följer att $\xi B = \zeta B$. ■

Sats 55 Låt A vara en modul, m ett positivt heltal,

$$S = \{\hat{\xi} \in \hat{A}; N(\hat{\xi}) = mN(A)\},$$

$$V = \{B; B \text{ modul}, B \subseteq \Omega_B, B \approx A^{-1}, N(B) = m\},$$

och sätt $F(\hat{\xi}) = \xi A^{-1}$. Då är $F : S \rightarrow V$ en bijektion.

Bevis Det följer direkt av lemma 4 att F är väldefinierad.

Vi visar nu att $V_F \subseteq V$. Eftersom $N(\xi) = mN(A) > 0$, så gäller det att $F(\hat{\xi}) \approx A^{-1}$. Vidare är $N(F(\hat{\xi})) = N(\xi)N(A^{-1}) = mN(A)(N(A))^{-1} = m$. Eftersom $\xi \in A$, så gäller det att $\xi\Omega_A \subseteq A$. Vi får att $\xi A^{-1}A = \xi\Omega_A \subseteq A$, vilket visar att $F(\hat{\xi}) = \xi A^{-1} \subseteq \Omega_A = \Omega_B$. Detta visar att $V_F \subseteq V$.

Om $B \in V$, så är $B = \xi A^{-1}$ för något element ξ , för vilket $N(\xi) > 0$. Vi får att $\xi \in BA$, och eftersom $B \subseteq \Omega_B = \Omega_A$, att $\xi \in A$. Eftersom $N(B) = m$ och $N(\xi) > 0$, så är $N(\xi) = |N(\xi)| = N(B)N(A) = mN(A)$. Detta visar att F är surjektiv.

Antag slutligen att $F(\hat{\xi}) = F(\hat{\zeta})$. Då är $\xi A^{-1} = \zeta A^{-1}$, och lemma 4 ger att $\xi \cong \zeta$, vilket betyder att $\hat{\xi} = \hat{\zeta}$. F är alltså injektiv. ■

Lemma 5 Om k är ett positivt heltal, så är k det minsta positiva heltalet i modulen $k\langle 1, \gamma \rangle$.

Bevis Om $l > 0$ är ett heltal i $k\langle 1, \gamma \rangle$, så finns det heltal x och y , sådana att $l = xk + yk\gamma$. Eftersom γ är irrationellt, så är $y = 0$, och $k \mid l$. ■

Lemma 6 Om $\langle 1, \gamma_1 \rangle = \langle 1, \gamma_2 \rangle$, och

$$-\frac{1}{2} \leq \text{Rat } \gamma_i < \frac{1}{2}, \quad \text{Irr } \gamma_i > 0, \quad i = 1, 2,$$

så är $\gamma_1 = \gamma_2$.

Bevis Det gäller att

$$\gamma_1 = x_1 + y_1\gamma_2 = x_1 + y_1(x_2 + y_2\gamma_1) = x_1 + x_2y_1 + y_1y_2\gamma_1,$$

där x_1, x_2, y_1, y_2 är heltal. Därför är $y_1y_2 = 1$. Enligt förutsättningarna är $y_1 > 0$, och det följer att $y_1 = 1$, varav $\gamma_1 = x_1 + \gamma_2$, och förutsättningarna ger nu att $x_1 = 0$. ■

Lemma 7 Om B är en modul, sådan att $B \subseteq \Omega_B$, så finns ett positivt heltal k och ett element γ , sådana att $B = k\langle 1, \gamma \rangle$, $-1/2 \leq \text{Rat } \gamma < 1/2$ och $\text{Irr } \gamma > 0$.

Bevis Det gäller att $B = \langle \alpha, \beta \rangle$ för några element α, β . Eftersom $\alpha' \in \Omega_B$, så gäller det att $N(\alpha) = \alpha\alpha' \in B$. Eftersom $N(\alpha) \in \mathbf{Z}$, så finns det ett positivt heltal i B . Låt k vara det minsta av dem. Då är k det minsta positiva rationella talet i B , eftersom alla rationella tal i Ω_B är heltal. Vi kan skriva $k = x\alpha + y\beta$ för några heltal x och y , och det måste vara så, att $(x, y) = 1$, ty annars skulle det finnas ett mindre positivt rationellt tal i B än k . Det finns därför heltal z och w , sådana att $xw - yz = 1$. Om $k\gamma = z\alpha + w\beta$, så gäller det alltså att $B = k\langle 1, \gamma \rangle$. Eftersom $\langle 1, \gamma \rangle = \langle 1, \pm\gamma + l \rangle$ för alla heltal l , kan vi välja γ så, att $-1/2 \leq \text{Rat } \gamma < 1/2$ och $\text{Irr } \gamma > 0$. ■

Sats 56 Låt A vara en modul, m ett positivt heltal, och antag att $D(\Omega_A) = D$. Låt

$$T = \{[a, b, c, s]; a, b, c, s \in \mathbf{Z}, a, s > 0, -a \leq b < a, (a, b, c) = 1, b^2 - 4ac = D, m = as^2\},$$

$$W = \{B; B \text{ modul}, B \subseteq \Omega_B, D(\Omega_B) = D, N(B) = m\},$$

och sätt $G([a, b, c, s]) = as\langle 1, \gamma \rangle$, där

$$\gamma = \frac{-b + \sqrt{D}}{2a}.$$

Då är $G : T \rightarrow W$ en bijektion. Med \sqrt{D} avses den positiva roten, om $D > 0$, och $i\sqrt{|D|}$, om $D < 0$.

Bevis Det gäller att $a(t - \gamma)(t - \gamma') = at^2 + bt + c$, vilket visar att $D(\varphi_\gamma(t)) = D$. Om $B = as\langle 1, \gamma \rangle$, så är $\Omega_B = \langle 1, a\gamma \rangle$ enligt sats 47, vilket visar att $B \subseteq \Omega_B$. Enligt samma sats är $D(\Omega_B) = D$. Enligt sats 50 är $N(as\langle 1, \gamma \rangle) = (as)^2/a = as^2 = m$. Detta visar att $V_G \subseteq W$.

Antag att $G([a_1, b_1, c_1, s_1]) = G([a_2, b_2, c_2, s_2])$. Då är $a_1s_1 = a_2s_2$ enligt lemma 5. Därför är $\langle 1, \gamma_1 \rangle = \langle 1, \gamma_2 \rangle$, vilket enligt sats 50 medför att $a_1 = a_2$, och därför är också $s_1 = s_2$. Lemma 6 ger att $\gamma_1 = \gamma_2$, och det medför att $b_1 = b_2$, och därför är också $c_1 = c_2$. Vi har nu visat att G är injektiv.

Vi visar slutligen att G är surjektiv. Låt $B \in W$. Enligt lemma 7 finns det ett positivt heltal k och ett element γ , sådana att $B = k\langle 1, \gamma \rangle$, $-1/2 \leq \text{Rat } \gamma < 1/2$ och $\text{Irr } \gamma > 0$. Antag att $\varphi_\gamma(t) = at^2 + bt + c$. Då är $(a, b, c) = 1$. Enligt sats 47 är $\Omega_B = \Omega_{\langle 1, \gamma \rangle} = \langle 1, a\gamma \rangle$, och eftersom $D(\varphi_\gamma(t)) = D(\Omega_B) = D$, kan vi skriva

$$\gamma = \frac{-b + \sqrt{D}}{2a},$$

där $a > 0$ och $-a \leq b < a$. Eftersom $k\langle 1, \gamma \rangle \subseteq \langle 1, a\gamma \rangle$, så gäller det att $a \mid k$, och eftersom k och a är positiva, finns det ett positivt heltal s , sådant att $k = as$. Det gäller att $m = N(B) = k^2/a$ enligt sats 50, varav $m = as^2$. ■

Korollarium 5 Om A är en modul och m ett positivt heltal, så har ekvationen

$$N(\hat{\xi}) = mN(A), \quad \hat{\xi} \in \hat{A},$$

bara ändligt många lösningar.

Bevis Det är lätt att se, att mängden T i sats 56 är ändlig, Därför är också W ändlig. Påståendet följer nu av att $V \subseteq W$ och att S och V har lika många element, där S och V är som i sats 55. ■

Modulärt ekvivalenta kvadratisk irrationella tal

Sats 57 Om $\gamma \sim \eta$, och ett av talen γ och η är kvadratisk irrationellt, så är också det andra kvadratisk irrationellt. Det gäller i så fall att $\gamma \in \mathbf{Q}(\sqrt{d})$ och $\eta \in \mathbf{Q}(\sqrt{d})$ för något kvadratfritt heltal d , och att $D(\varphi_\gamma(t)) = D(\varphi_\eta(t))$. Om $\gamma = R\eta$, där

$$R = \begin{bmatrix} p & r \\ q & s \end{bmatrix} \in \text{GL}(2, \mathbf{Z}),$$

och $\varphi_\gamma(t) = at^2 + bt + c$, så är $\varphi_\eta(t) = \pm(et^2 + ft + g)$, där

$$\begin{bmatrix} e \\ f \\ g \end{bmatrix} = S \begin{bmatrix} a \\ b \\ c \end{bmatrix}, \quad S = \begin{bmatrix} p^2 & pq & q^2 \\ 2pr & ps + rq & 2qs \\ r^2 & rs & s^2 \end{bmatrix}.$$

Bevis Det första påståendet följer av sats 4. Det är klart att $\gamma \in \mathbf{Q}(\sqrt{d})$ för något kvadratfritt heltal d , och eftersom $\mathbf{Q}(\sqrt{d})$ är en kropp gäller det också att $\eta \in \mathbf{Q}(\sqrt{d})$. Det gäller att

$$\begin{aligned} 0 &= (q\eta + s)^2 \varphi(\gamma) = a(p\eta + r)^2 + b(p\eta + r)(q\eta + s) + c(q\eta + s)^2 \\ &= (p^2a + pqb + q^2c)\eta^2 + (2pra + (ps + rq)b + 2qsc)\eta + r^2a + rsb + s^2c, \end{aligned}$$

vilket visar att $e\eta^2 + f\eta + g = 0$. Direkt uträkning visar att

$$\det S = p^3s^3 - 3p^2rqs^2 + 3pr^2q^2s - q^3r^3 = (ps - rq)^3 = (\det R)^3 = \pm 1.$$

Eftersom $(a, b, c) = 1$, visar detta att $(e, f, g) = 1$, varav $\varphi_\eta(t) = \pm(et^2 + ft + g)$. Slutligen är

$$\begin{aligned} f^2 - 4eg &= (2pra + (ps + rq)b + 2qsc)^2 - 4(p^2a + pqb + q^2c)(r^2a + rsb + s^2c) \\ &= (p^2s^2 + r^2q^2 - 2prqs)(b^2 - 4ac) = (ps - rq)^2(b^2 - 4ac) \\ &= (\det A)^2(b^2 - 4ac) = b^2 - 4ac. \quad \blacksquare \end{aligned}$$

Sats 58 Antag att γ och η är kvadratisk irrationella tal. Då gäller det att $\gamma \sim \eta$, om och endast om $\langle 1, \gamma \rangle \sim \langle 1, \eta \rangle$. Om det gäller att $\gamma = R\eta$, där

$$R = \begin{bmatrix} e & f \\ g & h \end{bmatrix} \in \text{GL}(2, \mathbf{Z}),$$

så är

$$\langle 1, \gamma \rangle = \frac{1}{g\eta + h} \langle 1, \eta \rangle.$$

Bevis Antag att $\gamma = R\eta$, där

$$R = \begin{bmatrix} e & f \\ g & h \end{bmatrix} \in \text{GL}(2, \mathbf{Z}).$$

Då är

$$\langle 1, \gamma \rangle = \left\langle \frac{g\eta + h}{g\eta + h}, \frac{e\eta + f}{g\eta + h} \right\rangle = \frac{1}{g\eta + h} \langle g\eta + h, e\eta + f \rangle \subseteq \frac{1}{g\eta + h} \langle 1, \eta \rangle.$$

Eftersom $eh - fg = \pm 1$, så är

$$\begin{aligned} \eta &= \pm(eh - fg)\eta = \pm(-f(g\eta + h) + h(e\eta + f)), \\ 1 &= \pm(eh - fg) = \pm(e(g\eta + h) - g(e\eta + f)), \end{aligned}$$

vilket visar att

$$\langle 1, \gamma \rangle = \frac{1}{g\eta + h} \langle 1, \eta \rangle.$$

Antag nu att $\langle 1, \gamma \rangle = \xi \langle 1, \eta \rangle = \langle \xi, \xi\eta \rangle$. Då är

$$\begin{bmatrix} \gamma \\ 1 \end{bmatrix} = R \begin{bmatrix} \xi\eta \\ \xi \end{bmatrix}, \quad \begin{bmatrix} \xi\eta \\ \xi \end{bmatrix} = S \begin{bmatrix} \gamma \\ 1 \end{bmatrix},$$

där

$$R = \begin{bmatrix} e & f \\ g & h \end{bmatrix}, \quad S = \begin{bmatrix} k & l \\ m & n \end{bmatrix}$$

är matriser med heltalselement. Därför är $RS = E$, och det följer att $(\det R)(\det S) = 1$. Eftersom elementen i matriserna är heltal, så är $\det R = \pm 1$. Det gäller slutligen att

$$\gamma = \frac{\gamma}{1} = \frac{e\xi\eta + f\xi}{g\xi\eta + h\xi} = \frac{e\eta + f}{g\eta + h} = R\eta,$$

vilket visar att $\gamma \sim \eta$. ■

Reella kvadratisk irrationella tal

Definition 34 Det enkla oändliga kedjebråket (a_0, a_1, \dots) säges vara periodiskt, om det finns naturliga tal m och n , $n > m$, sådana att $a'_n = a'_m$. Det säges vara rent periodiskt, om $a'_n = a'_0$ för något positivt heltal n .

Sats 59 Antag att (a_0, a_1, \dots) är ett enkelt kedjebråk, och att $a'_n = a'_m$, där $n > m$. Då är $a'_{n+k} = a'_{m+k}$ för alla naturliga tal k . Om $k \geq m$ och $j \in \mathbf{N}$, så är $a'_{k+j(n-m)} = a'_k$. Om $i \geq m$, så finns det ett naturligt tal k , sådant att $m \leq k < n$, och $a'_i = a'_k$.

Bevis Det gäller att a'_{m+k} och a'_{n+k} är den k :e fullständiga konvergenten i (a_m, a_{m+1}, \dots) respektive (a_n, a_{n+1}, \dots) . Eftersom $[a_m, a_{m+1}, \dots] = [a_n, a_{n+1}, \dots]$, så ger sats 16 att $a'_{m+k} = a'_{n+k}$. Om $k \geq m$, så är $k - m \geq 0$, och vi får

$$a'_{k+(n-m)} = a'_{n+(k-m)} = a'_{m+(k-m)} = a'_k.$$

Det följer nu med induktion över j , att $a'_{k+j(n-m)} = a'_k$, $j \geq 0$. Vi dividerar $i - m$ med $n - m$ och får att $i - m = j(n - m) + r$, där $0 \leq r < n - m$. Det följer att $m \leq k = m + r < n$, och att $a'_k = a'_{k+j(n-m)} = a'_i$. ■

Sats 60 Antag att γ är värdet av ett enkelt oändligt kedjebråk (a_0, a_1, \dots) . Då gäller det att γ är kvadratisk irrationellt, om och endast om (a_0, a_1, \dots) är periodiskt.

Bevis Antag först att (a_0, a_1, \dots) är periodiskt, så att $a'_n = a'_m$, där $n > m$. Eftersom det då gäller att $a'_{n+k} = a'_{m+k}$, $k \geq 0$, kan vi antaga att $m \geq 3$. Om p_n/q_n är den n :e konvergenten, så gäller det att

$$\gamma = \frac{p_{m-1}a'_m + p_{m-2}}{q_{m-1}a'_m + q_{m-2}} = \frac{p_{m-1}a'_n + p_{m-2}}{q_{m-1}a'_n + q_{m-2}} = \frac{p_{n-1}a'_n + p_{n-2}}{q_{n-1}a'_n + q_{n-2}},$$

vilket ger att

$$a'_n(q_{m-1}\gamma - p_{m-1}) = p_{m-2} - q_{m-2}\gamma, \quad a'_n(q_{n-1}\gamma - p_{n-1}) = p_{n-2} - q_{n-2}\gamma.$$

Det följer att

$$a'_n(q_{n-1}\gamma - p_{n-1})(p_{m-2} - q_{m-2}\gamma) = a'_n(q_{m-1}\gamma - p_{m-1})(p_{n-2} - q_{n-2}\gamma),$$

varav

$$e\gamma^2 + f\gamma + g = 0,$$

där

$$\begin{aligned} e &= q_{m-1}q_{n-2} - q_{n-1}q_{m-2}, \\ f &= p_{m-2}q_{n-1} + p_{n-1}q_{m-2} - p_{n-2}q_{m-1} - p_{m-1}q_{n-2}, \\ g &= p_{m-1}p_{n-2} - p_{n-1}p_{m-2}. \end{aligned}$$

Om $e = f = 0$, så är

$$\frac{p_{m-2}}{q_{m-2}} + \frac{p_{n-1}}{q_{n-1}} = \frac{p_{n-2}}{q_{n-2}} + \frac{p_{m-1}}{q_{m-1}},$$

vilket enligt korollarium 2 ger att

$$\frac{(-1)^{n-2}}{q_{n-1}q_{n-2}} = \frac{(-1)^{m-2}}{q_{m-1}q_{m-2}}.$$

Detta är omöjligt, eftersom q_n , $n \geq 1$, är strängt växande. Eftersom γ är irrationellt, är därför $e \neq 0$, och γ är kvadratisk irrationellt.

Antag nu att γ är kvadratisk irrationellt, och att $\varphi_\gamma(t) = et^2 + ft + g$. Det gäller att

$$\gamma = \frac{p_{n-1}a'_n + p_{n-2}}{q_{n-1}a'_n + q_{n-2}}, \quad n \geq 2.$$

Det gäller enligt sats 57 att $D(\varphi_{a'_n}(t)) = D(\varphi_\gamma(t))$, och $\varphi_{a'_n}(t) = \pm(e_nt^2 + f_nt + g_n)$, där

$$\begin{aligned} e_n &= ep_{n-1}^2 + fp_{n-1}q_{n-1} + gq_{n-1}^2, \\ f_n &= 2ep_{n-1}p_{n-2} + f(p_{n-1}q_{n-2} + p_{n-2}q_{n-1}) + 2gq_{n-1}q_{n-2}, \\ g_n &= ep_{n-2}^2 + fp_{n-2}q_{n-2} + gq_{n-2}^2. \end{aligned}$$

Enligt sats 19 finns det tal δ_n , sådana att $|\delta_n| < 1$ och

$$p_{n-1} = \gamma q_{n-1} + \frac{\delta_{n-1}}{q_{n-1}}.$$

Detta ger att

$$\begin{aligned}
|e_n| &= \left| e \left(\gamma q_{n-1} + \frac{\delta_{n-1}}{q_{n-1}} \right)^2 + f q_{n-1} \left(\gamma q_{n-1} + \frac{\delta_{n-1}}{q_{n-1}} \right) + g q_{n-1}^2 \right| \\
&= \left| (e\gamma^2 + f\gamma + g)q_{n-1}^2 + 2e\gamma\delta_{n-1} + e\frac{\delta_{n-1}^2}{q_{n-1}^2} + f\delta_{n-1} \right| \\
&= \left| 2e\gamma\delta_{n-1} + e\frac{\delta_{n-1}^2}{q_{n-1}^2} + f\delta_{n-1} \right| \leq 2|e||\gamma| + |e| + |f|, \\
|g_n| &= |e_{n-1}| \leq 2|e||\gamma| + |e| + |f|, \\
f_n^2 &= 4e_n g_n + f^2 - 4eg \leq 4|e_n||g_n| + |f^2 - 4eg| \leq 4(2|e||\gamma| + |e| + |f|)^2 + |f^2 - 4eg|.
\end{aligned}$$

Det finns därför bara ändligt många olika polynom $\varphi_{a'_n}(t)$. Därför finns det tre olika positiva heltal n_1, n_2 och n_3 , sådana att $\varphi_{a'_{n_1}}(t) = \varphi_{a'_{n_2}}(t) = \varphi_{a'_{n_3}}(t)$, och det gäller att minst två av talen a'_{n_1}, a'_{n_2} och a'_{n_3} är lika. ■

Definition 35 Ett reellt kvadratisk irrationellt tal γ säges vara reducerat, om $\gamma > 1$ och $-1 < \gamma' < 0$.

Lemma 8 Om γ är reducerat och

$$\gamma = a + \frac{1}{\eta},$$

där $a \in \mathbf{Z}$ och $\eta > 1$, så är också η reducerat.

Bevis Eftersom $\gamma > 1$, är $a \geq 1$. Vi har också att

$$\gamma' = a + \frac{1}{\eta'} < 0,$$

varav

$$-\frac{1}{\eta'} > a \geq 1,$$

och det följer att $-1 < \eta' < 0$. ■

Lemma 9 Om γ är ett irrationellt kvadratisk tal, så finns det högst ett heltal a , sådant att $a + 1/\gamma$ är reducerat.

Bevis Om $a + 1/\gamma$ är reducerat, så är $-1 < a + 1/\gamma' < 0$. Det följer att $a < -1/\gamma' < a + 1$, och att $a = \lfloor -1/\gamma' \rfloor$. ■

Sats 61 Antag att det kvadratisk irrationella talet γ är värdet av det enkla oändliga kedjebråket (a_0, a_1, \dots) . Då gäller det att (a_0, a_1, \dots) är rent periodiskt, om och endast om γ är reducerat.

Bevis Antag att (a_0, a_1, \dots) är rent periodiskt, så att $a'_0 = a'_n$ för något positivt heltal n . Då är $a_n \geq 1$, och det följer att $\gamma = a'_0 = a'_n > 1$. Om $n = 1$, så är

$$\gamma = a_0 + \frac{1}{\gamma}.$$

Det följer att $\gamma^2 - a_0\gamma - 1 = 0$, och sambandet mellan rötter och koefficienter ger att $\gamma\gamma' = -1$, varav påståendet följer i detta fall. Låt annars p_n/q_n vara den n :e konvergenten. Då gäller det att

$$\gamma = \frac{p_{n-1}\gamma + p_{n-2}}{q_{n-1}\gamma + q_{n-2}}.$$

Vi får nu $q_{n-1}\gamma^2 + (q_{n-2} - p_{n-1})\gamma - p_{n-2} = 0$, och sambandet mellan rötter och koefficienter ger att

$$-\gamma' = \frac{p_{n-2}}{\gamma q_{n-1}}.$$

Eftersom $a_0 \geq 1$, är $0 < p_{n-2} < p_{n-1}$ och $0 < q_{n-2} \leq q_{n-1}$ enligt sats 10. Detta ger att

$$\frac{p_{n-2}}{q_{n-1}} > 0, \quad \frac{p_{n-2}}{q_{n-1}} \leq \frac{p_{n-1}}{q_{n-1}}, \quad \frac{p_{n-2}}{q_{n-1}} \leq \frac{p_{n-2}}{q_{n-2}}.$$

Eftersom det enligt sats 13 gäller att

$$\gamma > \frac{p_{n-1}}{q_{n-1}} \quad \text{eller} \quad \gamma > \frac{p_{n-2}}{q_{n-2}},$$

och därmed

$$\gamma > \frac{p_{n-2}}{q_{n-1}},$$

så ger detta att $0 < -\gamma' < 1$. Det gäller alltså att γ är reducerat.

Antag nu att $\gamma = a'_0$ är reducerat. Eftersom

$$a'_n = a_n + \frac{1}{a'_{n+1}},$$

följer det av lemma 8 att a'_n är reducerat för alla naturliga tal n . Enligt sats 60 är kedjebråket (a_0, a_1, \dots) periodiskt, varför $a'_m = a'_n$ för några naturliga tal $m < n$. Låt m vara det minsta naturliga talet, för vilket det finns ett sådant naturligt tal n . Antag att $m > 0$. Då är

$$a'_{m-1} = a_{m-1} + \frac{1}{a'_m} = a_{m-1} + \frac{1}{a'_n} \quad \text{och} \quad a'_{n-1} = a_{n-1} + \frac{1}{a'_n}$$

båda reducerade. Enligt lemma 9 är därför $a_{m-1} = a_{n-1}$, och det följer att $a'_{m-1} = a'_{n-1}$, vilket strider mot att m är minimalt. Alltså är $m = 0$, och kedjebråket är rent periodiskt. ■

Sats 62 Låt γ vara ett reellt kvadratisk irrationellt tal, och definiera rekursivt (γ_n) genom

$$\gamma_0 = \gamma, \quad \frac{1}{\gamma_{n+1}} = \gamma_n - \lfloor \gamma_n \rfloor, \quad n \geq 0.$$

Då finns det naturliga tal $m < n$, sådana att $\gamma_m = \gamma_n$. Det gäller att $\gamma_m, \dots, \gamma_{n-1}$ är reducerade, och $\gamma \sim \gamma_m$. Om $\eta \sim \gamma$, och η är reducerat, så gäller det att $\eta = \gamma_k$ för något heltal k , för vilket $m \leq k \leq n-1$.

Bevis Det gäller att $\gamma_n = a'_n$, där (a_0, a_1, \dots) är det enkla kedjebråk, vars värde är γ . Enligt sats 60 är kedjebråket periodiskt, och det följer att $\gamma_m = \gamma_n$ för några naturliga tal $m < n$. Det är klart att $\gamma \sim \gamma_m$. Det gäller enligt sats 59, att $\gamma_{m+k} = \gamma_{n+k}$ då $k \in \mathbf{N}$. Eftersom γ_{m+k} är den 0:e och γ_{n+k} den $(n-m)$:e fullständiga konvergenten i kedjebråket, vars värde är γ_{m+k} , gäller det enligt sats 61, att γ_{m+k} är ett reducerat tal, då $k \geq 0$. I synnerhet är $\gamma_m, \dots, \gamma_{n-1}$ reducerade.

Antag att $\eta \sim \gamma$, och att η är reducerat. Om η är värdet av det enkla kedjebråket (b_0, b_1, \dots) , så ger sats 23 att $b'_i = a'_j = \gamma_j$ för några naturliga tal i och j . Det gäller därför att $b'_{i+l} = \gamma_{j+l}$ för alla naturliga tal l . Eftersom (b_0, b_1, \dots) är rent periodiskt, kan vi välja l , så att $b'_{i+l} = b'_0 = \eta$ och $j+l \geq m$. Enligt sats 59 är $\gamma_{j+l} = \gamma_k$ för något k , sådant att $m \leq k \leq n-1$, och vi har att $\eta = \gamma_k$. ■

Icke-reella kvadratisk irrationella tal

Definition 36 Låt γ vara ett icke-reellt komplext tal. Man säger att γ är reducerat, om $\text{Im } \gamma > 0$, och antingen

$$|\gamma| > 1, \quad -\frac{1}{2} < \text{Re } \gamma < 0, \quad \text{eller} \quad |\gamma| \geq 1, \quad 0 \leq \text{Re } \gamma \leq \frac{1}{2}.$$

Lemma 10 Antag att γ är ett icke-reellt reducerat tal, och att $\zeta = x + y\gamma \neq 0$, där x och y är heltal.

1. Då är $|\zeta| \geq 1$.
2. Om $y \neq 0$, så är $|\zeta| \geq |\gamma|$.
3. Om $y \neq 0$ och $|\zeta| = |\gamma|$, så är antingen $\zeta = \pm\gamma$, eller $\text{Re } \gamma = 1/2$ och $\zeta = \pm(\gamma - 1)$.
4. Om $|\gamma| = 1$, och $\gamma \neq \frac{1+i\sqrt{3}}{2}$, så är $|\zeta| = 1$, bara då $\zeta = \pm 1$, eller $\zeta = \pm\gamma$.
5. Om $\gamma = \frac{1+i\sqrt{3}}{2}$, så är $|\zeta| = 1$, bara då $\zeta = \pm 1$, eller $\zeta = \frac{\pm 1 \pm i\sqrt{3}}{2}$.

Bevis Skriv $\gamma = a + bi$, där a och b är reella tal. Då är $\zeta = x + ay + iby$, och

$$|\zeta|^2 = (x + ay)^2 + (by)^2.$$

Eftersom $a^2 \leq 1/4$ och $a^2 + b^2 \geq 1$, så är $b^2 \geq 3/4$.

Antag att $y = 0$. Då är $x \neq 0$, och $|\zeta| = |x| \geq 1$.

Antag att $|y| \geq 2$. Då är

$$|\gamma|^2 = a^2 + b^2 \leq 1/4 + b^2 \leq b^2 + b^2 < 4b^2 \leq y^2 b^2 \leq |\zeta|^2,$$

vilket visar att $|\zeta| > |\gamma|$.

Antag att $|y| = 1$. Då är $|\zeta|^2 = (x + ya)^2 + b^2 = x^2 + 2yxa + |\gamma|^2 = |\gamma|^2$, bara då $x^2 + 2yxa = x(x + 2ya) = 0$. Om $x = 0$, så är $\zeta = \pm\gamma$. Om $x = -2ya$, så är $\text{Re } \gamma = a = 1/2$, eftersom $y = \pm 1$ och $x \in \mathbf{Z}$. Därför är också $x = -y$, och därmed $\zeta = \pm(\gamma - 1)$. Enligt förutsättningarna är $x(x + 2ya) \geq 0$, och därför gäller det att $|\zeta| \geq |\gamma|$.

De tre första påståendena i satsen följer nu av att $|\gamma| \geq 1$.

I det fjärde påståendet är $\text{Re } \gamma \neq 1/2$, och i det femte är $\text{Re } \gamma = 1/2$. Dessa påståenden följer därför av de tre första. ■

Sats 63 Om de icke-reella kvadratisk irrationella talen γ och η är reducerade, och $\gamma \sim \eta$, så är $\gamma = \eta$.

Bevis Enligt sats 58 är $\langle 1, \gamma \rangle \sim \langle 1, \eta \rangle$. Det finns därför ett komplext tal ξ , sådant att $\langle 1, \gamma \rangle = \xi \langle 1, \eta \rangle$. Eftersom $\xi \in \langle 1, \gamma \rangle$, så ger lemma 10 att $|\xi| \geq 1$, och eftersom $1/\xi \in \langle 1, \eta \rangle$, så ger samma lemma att $|\xi| \leq 1$. Det gäller alltså att $|\xi| = 1$. Modulerna $\langle 1, \gamma \rangle$ och $\langle 1, \eta \rangle$ innehåller därför lika många element med absolutbeloppet 1. Enligt lemma 10 kan detta antal bara vara 2, 4 eller 6. Om det är 6, så är $\gamma = \eta = (1 + i\sqrt{3})/2$. Om antalet är 2, så är $\xi = \pm 1$, varför $\langle 1, \gamma \rangle = \langle 1, \eta \rangle$. Enligt lemma 10 är $|\gamma| \geq |\eta|$ och $|\eta| \geq |\gamma|$, vilket ger att $|\gamma| = |\eta|$. Eftersom γ och η båda är reducerade, ger lemma 10 att $\gamma = \eta$. Antag att antalet är 4. Det gäller då att γ är något av talen $\pm\xi$ och $\pm\xi\eta$. Om $\gamma = \pm\xi$, så gäller det att $\gamma\eta \in \langle 1, \gamma \rangle$. Enligt lemma 10 är antingen $\gamma\eta = \pm 1$ eller $\gamma\eta = \pm\gamma$. I det sista fallet är

$\eta = \pm 1$, vilket strider mot att η är reducerat. Det kan av samma skäl inte heller vara så, att $\gamma\eta = 1$, och $\gamma\eta = -1$ är bara möjligt då $\gamma = \eta = i$. I annat fall är $\gamma = \pm\xi\eta$, och då gäller att $\gamma/\eta \in \langle 1, \gamma \rangle$. Det gäller då att $\gamma/\eta = \pm 1$ eller $\gamma/\eta = \pm\gamma$. Man inser att endast $\gamma/\eta = 1$ kan gälla, och då är $\gamma = \eta$. ■

Sats 64 Låt γ vara ett icke-reellt kvadratisk irrationellt tal, och definiera (γ_n) genom

$$\gamma_0 = (\operatorname{sgn}(\operatorname{Im} \gamma))\gamma + m_0, \quad \gamma_{n+1} = -\frac{1}{\gamma_n} + m_{n+1}, \quad n \geq 0,$$

där heltalet m_n väljs så, att $-1/2 < \operatorname{Re} \gamma_n \leq 1/2$. Då finns det ett naturligt tal n , sådant att γ_n är reducerat, och $\gamma \sim \gamma_n$.

Bevis Det gäller att $\gamma_0 = R_0\gamma$ och $\gamma_{n+1} = R_{n+1}\gamma_n$, där

$$R_0 = \begin{bmatrix} \operatorname{sgn}(\operatorname{Im} \gamma) & m_0 \\ 0 & 1 \end{bmatrix}, \quad R_{n+1} = \begin{bmatrix} m_{n+1} & -1 \\ 1 & 0 \end{bmatrix}, \quad n \geq 0,$$

och det $R_0 = \operatorname{sgn}(\operatorname{Im} \gamma)$, det $R_{n+1} = 1$, då $n \geq 0$. Därför är $\gamma \sim \gamma_n$ för varje naturligt tal n . Enligt sats 5 är $\operatorname{Im} \gamma_n > 0$, och enligt konstruktionen är $-1/2 < \operatorname{Re} \gamma_n \leq 1/2$, för varje naturligt tal n . Låt $\psi(t) = \varphi_\gamma(t) = a^2 + bt + c$ och $\psi_n(t) = \varphi_{\gamma_n}(t) = a_n t^2 + b_n t + c_n$, då $n \geq 0$, och sätt $D = b^2 - 4ac$. Då är $D < 0$, eftersom γ är icke-reellt, och $D(\psi_n(t)) = D$, då $n \geq 0$, enligt sats 57.

Antag att $|\gamma_n| < 1$ då $n \geq 0$. Då är

$$\gamma_{n+1} = \frac{-1 + \gamma_n m_{n+1}}{\gamma_n} = \frac{|\gamma_n|^2 m_{n+1} - \operatorname{Re} \gamma_n + i \operatorname{Im} \gamma_n}{|\gamma_n|^2},$$

vilket visar att $\operatorname{Im} \gamma_{n+1} > \operatorname{Im} \gamma_n$, $n \geq 0$. Vi kan skriva

$$\gamma_n = \frac{-b_n + i\sqrt{|D|}}{2a_n},$$

och $\operatorname{Im} \gamma_n \geq \operatorname{Im} \gamma_0$ ger att $0 < a_n \leq a_0$. Att $-1/2 < \operatorname{Re} \gamma_n \leq 1/2$ medför att $|b_n| \leq a_n \leq a_0$. Enligt sats 57 är $c_{n+1} = a_n$, vilket visar att $|c_n| \leq a_0$, då $n \geq 1$. Det måste alltså finnas två olika naturliga tal $n_1 < n_2$, sådana att $\psi_{n_1}(t) = \psi_{n_2}(t)$, och då är också $\gamma_{n_1} = \gamma_{n_2}$. Eftersom detta strider mot att $\operatorname{Im} \gamma_{n_1} < \operatorname{Im} \gamma_{n_2}$, så måste det vara så, att $|\gamma_n| \geq 1$ för något naturligt tal n . Om $|\gamma_n| > 1$, så är γ_n reducerat, och vi är klara. Om $|\gamma_n| = 1$, och $0 \leq \operatorname{Re} \gamma_n \leq 1/2$, så är också γ_n reducerat. Antag att $|\gamma_n| = 1$ och $-1/2 < \operatorname{Re} \gamma_n < 0$. Då är $\gamma_{n+1} = m_{n+1} - \operatorname{Re} \gamma_n + i \operatorname{Im} \gamma_n$. Eftersom $0 < -\operatorname{Re} \gamma_n < 1/2$, så är $m_{n+1} = 0$, och vi finner att $\gamma_{n+1} = -\operatorname{Re} \gamma_n + i \operatorname{Im} \gamma_n$. Det gäller att $|\gamma_{n+1}| = |\gamma_n| = 1$ och $0 < \operatorname{Re} \gamma_{n+1} < 1/2$, varför γ_{n+1} är reducerat. ■

Kvadratiska former i två variabler

Definition 37 Den kvadratiska formen $F(x, y) = px^2 + qxy + ry^2$, där p, q och r är heltal, säges vara primitiv, om $(p, q, r) = 1$ och polynomet $pt^2 + qt + r$ är irreducibelt över \mathbf{Q} . Talet $q^2 - 4pr$ kallas formens diskriminant.

Eftersom $\varphi(t) = pt^2 + qt + r$ är irreducibelt över \mathbf{Q} , så är dess nollställen $-\gamma$ och $-\gamma'$ kvadratisk irrationella tal. Vi kan skriva $\varphi(t) = p(t + \gamma)(t + \gamma')$, och får att

$$F(x, y) = y^2 \varphi\left(\frac{x}{y}\right) = p(x + y\gamma)(x + y\gamma')$$

Om $p > 0$, följer det av sats 50, att $N(A) = 1/p$, där $A = \langle 1, \gamma \rangle$, och vi kan skriva

$$F(x, y) = \frac{N(x + y\gamma)}{N(A)} = \frac{N(x\alpha + y\beta)}{N(A)},$$

där $\alpha = 1$ och $\beta = \gamma$. Om $p < 0$ och $D = D(\varphi(t)) > 0$, sätter vi $A = \sqrt{D}\langle 1, \gamma \rangle = \langle \alpha, \beta \rangle$, där $\alpha = \sqrt{D}$ och $\beta = \gamma\sqrt{D}$. Då är $N(A) = |N(\sqrt{D})|/(-p) = -D/p$, och

$$F(x, y) = \frac{p(x\alpha + y\beta)(x\alpha' + y\beta')}{-D} = \frac{N(x\alpha + y\beta)}{N(A)}.$$

Om m är ett positivt heltal, kan vi alltså skriva ekvationen

$$F(x, y) = m$$

som

$$N(x\alpha + y\beta) = mN(A).$$

Exempel 1 Pells ekvation är en ekvation av formen $x^2 - Dy^2 = 1$, där D är ett positivt heltal, som inte är kvadraten på ett heltal. Ekvationen kan skrivas

$$N(x + y\sqrt{D}) = 1,$$

och vi kan lösa den genom att använda satserna 43 och 44. Vi illustrerar detta då $D = 13$. Vi sätter $\omega = \sqrt{13}$ och bestämmer konvergenterna i kedjebråksutvecklingen av $-\omega' = \omega$.

n	0	1	2	3	4
ω_n	$\sqrt{13}$	$\frac{3 + \sqrt{13}}{4}$	$\frac{1 + \sqrt{13}}{3}$	$\frac{2 + \sqrt{13}}{3}$	$\frac{1 + \sqrt{13}}{4}$
a_n	3	1	1	1	1
p_n	3	4	7	11	18
q_n	1	1	2	3	5
$p_n^2 - 13q_n^2$	-4	3	-3	4	-1

Vi ser att det fundamentala inverterbara elementet är $\varepsilon = 18 + 5\sqrt{13}$ och att $N(\varepsilon) = -1$. Det gäller att $\varepsilon^2 = 649 + 180\sqrt{13}$, och lösningen ges av

$$x + y\sqrt{13} = \pm\varepsilon^{2n} = \pm(649 + 180\sqrt{13})^n, \quad n \in \mathbf{Z}.$$

Vi får att

$$x - y\sqrt{13} = (x + y\sqrt{13})' = (\pm(649 + 180\sqrt{13})^n)' = \pm(649 - 180\sqrt{13})^n, \quad n \in \mathbf{Z},$$

och därför

$$\begin{bmatrix} x \\ y \end{bmatrix} = \pm \begin{bmatrix} \frac{(649 + 180\sqrt{13})^n + (649 - 180\sqrt{13})^n}{2} \\ \frac{(649 + 180\sqrt{13})^n - (649 - 180\sqrt{13})^n}{2\sqrt{13}} \end{bmatrix}, \quad n \in \mathbf{Z}.$$

Vi noterar att uttrycket för x är en jämn funktion och att uttrycket för y är en udda funktion av n . Lösningarna kan därför också skrivas

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \pm \frac{(649 + 180\sqrt{13})^n + (649 - 180\sqrt{13})^n}{2} \\ \pm \frac{(649 + 180\sqrt{13})^n - (649 - 180\sqrt{13})^n}{2\sqrt{13}} \end{bmatrix}, \quad n \in \mathbf{N}.$$

Vi noterar också att lösningarna $[x, y]$, för vilka både x och y är naturliga tal, ges av

$$x_n + y_n\sqrt{13} = (649 + 180\sqrt{13})^n, \quad n \in \mathbf{N}.$$

Vi har

$$\begin{aligned} x_{n+1} + y_{n+1}\sqrt{13} &= (649 + 180\sqrt{13})(x_n + y_n\sqrt{13}) \\ &= 649x_n + 2340y_n + (180x_n + 649y_n)\sqrt{13}, \quad n \in \mathbf{N}, \end{aligned}$$

vilket ger oss följande rekursionsformel.

$$\begin{bmatrix} x_0 \\ y_0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 649x_n + 2340y_n \\ 180x_n + 649y_n \end{bmatrix}, \quad n \in \mathbf{N}.$$

Vi har också sett att ekvationen $x^2 - 13y^2 = -1$ har en lösning. Samtliga lösningar till denna ekvation ges av $x + y\sqrt{13} = \pm \varepsilon^{2n+1}$, $n \in \mathbf{Z}$.

Exempel 2 Vi vill finna lösningarna till ekvationen

$$F(x, y) = 14x^2 - 32xy + 17y^2 = 9.$$

Ekvationen $14t^2 - 32t + 17 = 0$ har rötterna $-(-16 \pm 3\sqrt{2})/14$, och vi kan skriva

$$F(x, y) = \frac{(x\alpha + y\beta)(x\alpha' + y\beta')}{14} = \frac{N(x\alpha + y\beta)}{N(A)},$$

där

$$\alpha = 14, \quad \beta = -16 + 3\sqrt{2}, \quad A = \langle \alpha, \beta \rangle.$$

Vi har att $A = 14\langle 1, \gamma \rangle$, där $\gamma = (-16 + 3\sqrt{2})/14$, och $\Omega_A = \langle 1, 14\gamma \rangle = \langle 1, \omega \rangle$, där $\omega = 3\sqrt{2}$ enligt sats 47. Vi bestämmer det fundamentala inverterbara elementet i Ω_A , som vi gjorde i exempel 1, och finner att det är $\varepsilon = 17 + 12\sqrt{2}$ och att $N(\varepsilon) = 1$. Nästa steg är att använda sats 56 och finna mängden W , som finns angiven i satsen. Vi börjar med att bestämma a, b, c, s , som i mängden T . Eftersom $D = 32^2 - 4 \cdot 14 \cdot 17 = 72$ och $m = 9$, skall vi ha

$$-a \leq b < a, \quad (a, b, c) = 1, \quad b^2 - 4ac = 72, \quad as^2 = 9, \quad a, s > 0.$$

Lösningarna finns angivna i följande tabell.

s	a	b	c
3	1	0	-18
1	9	-6	-1
1	9	0	-2
1	9	6	-1

Detta ger oss fyra moduler B i mängden W . Dessa är

$$3 \left\langle 1, 3\sqrt{2} \right\rangle, \quad 9 \left\langle 1, \frac{1 + \sqrt{2}}{3} \right\rangle, \quad 9 \left\langle 1, \frac{\sqrt{2}}{3} \right\rangle, \quad 9 \left\langle 1, \frac{-1 + \sqrt{2}}{3} \right\rangle.$$

Vi skall nu bestämma mängden V i sats 55 genom att avgöra vilka av dessa, som är strikt ekvivalenta med A^{-1} . Vi noterar att $A^{-1} = \frac{1}{14} \cdot 14\langle 1, \gamma' \rangle = \langle 1, \gamma' \rangle$. Vi börjar med att använda sats 62 för att finna de reducerade element, som är ekvivalenta med $\eta = \gamma'$. För

den sakens skull bestämmer vi de fullständiga konvergenterna i kedjebråket till η , tills vi finner en period. Vi kommer också att behöva nämnarna q_n i konvergenterna.

n	0	1	2	3	4	5
η_n	$\frac{-16 - 3\sqrt{2}}{14}$	$\frac{4 + \sqrt{2}}{3}$	$-3 + 3\sqrt{2}$	$\frac{4 + 3\sqrt{2}}{2}$	$4 + 3\sqrt{2}$	$\frac{4 + 3\sqrt{2}}{2}$
q_n	1	1	2	9	74	305

Vi finner att de reducerade elementen är η_3, η_4 . Det gäller att

$$\eta = \frac{p_{n-1}\eta_n + p_{n-2}}{q_{n-1}\eta_n + q_{n-2}}$$

enligt sats 15 och enligt sats 58 att

$$A^{-1} = \langle 1, \eta \rangle = \frac{1}{2\eta_3 + 1} \langle 1, \eta_3 \rangle = \frac{1}{9\eta_4 + 2} \langle 1, \eta_4 \rangle.$$

Vi utvecklar nu vart och ett av de irrationella baselementen λ i modulerna B , tills vi får en reducerad fullständig konvergent. Om denna är ett av elementen η_3 och η_4 , så är motsvarande modul ekvivalent med A^{-1} .

n	0	1
λ_n	$3\sqrt{2}$	$\frac{4 + 3\sqrt{2}}{2}$
q_n	1	4

n	0	1	2
λ_n	$\frac{1 + \sqrt{2}}{3}$	$-3 + 3\sqrt{2}$	$\frac{4 + 3\sqrt{2}}{2}$
q_n	1	1	5

n	0	1	2
λ_n	$\frac{\sqrt{2}}{3}$	$\frac{3\sqrt{2}}{2}$	$4 + 3\sqrt{2}$
q_n	1	2	17

n	0	1	2
λ_n	$\frac{-1 + \sqrt{2}}{3}$	$3 + 3\sqrt{2}$	$\frac{4 + 3\sqrt{2}}{2}$
q_n	1	7	29

Vi får

$$B_1 = 3 \left\langle 1, 3\sqrt{2} \right\rangle = \frac{3}{\eta_3} \langle 1, \eta_3 \rangle = \frac{3(2\eta_3 + 1)}{\eta_3} A^{-1} = (-6 + 9\sqrt{2})A^{-1},$$

$$B_2 = 9 \left\langle 1, \frac{1 + \sqrt{2}}{3} \right\rangle = \frac{9}{\eta_3 + 1} \langle 1, \eta_3 \rangle = \frac{9(2\eta_3 + 1)}{\eta_3 + 1} A^{-1} = (12 + 3\sqrt{2})A^{-1},$$

$$B_3 = 9 \left\langle 1, \frac{\sqrt{2}}{3} \right\rangle = \frac{9}{2\eta_4 + 1} \langle 1, \eta_4 \rangle = \frac{9(9\eta_4 + 2)}{2\eta_4 + 1} A^{-1} = (18 + 15\sqrt{2})A^{-1},$$

$$B_4 = 9 \left\langle 1, \frac{-1 + \sqrt{2}}{3} \right\rangle = \frac{9}{7\eta_3 + 1} \langle 1, \eta_3 \rangle = \frac{9(2\eta_3 + 1)}{7\eta_3 + 1} A^{-1} = (24 - 15\sqrt{2})A^{-1}.$$

Av elementen

$$\xi_1 = -6 + 9\sqrt{2}, \quad \xi_2 = 12 + 3\sqrt{2}, \quad \xi_3 = 18 + 15\sqrt{2}, \quad \xi_4 = 24 - 15\sqrt{2}$$

är det bara ξ_2 och ξ_4 , som har positiv norm. Eftersom Ω_A saknar inverterbara element med negativ norm, så är bara B_2 och B_4 strikt ekvivalenta med A^{-1} enligt sats 52. Samtliga lösningar till ekvationen $F(x, y) = 9$ ges därför av

$$x\alpha + y\beta = \pm \varepsilon^n \xi_i, \quad n \in \mathbf{Z}, \quad i = 2, 4.$$

Observerar vi att $\xi_2 = (3 + 2\sqrt{2})\xi_4$, och att $(3 + 2\sqrt{2})^2 = \varepsilon$, får vi den något enklare lösningsformeln

$$14x - 16y + 3y\sqrt{2} = \pm(3 + 2\sqrt{2})^n(24 - 15\sqrt{2}).$$

Bibliografi

- [1] Borevich, Shafarevich, *Number Theory*, Academic Press, 1966
- [2] Hardy, Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, 1938