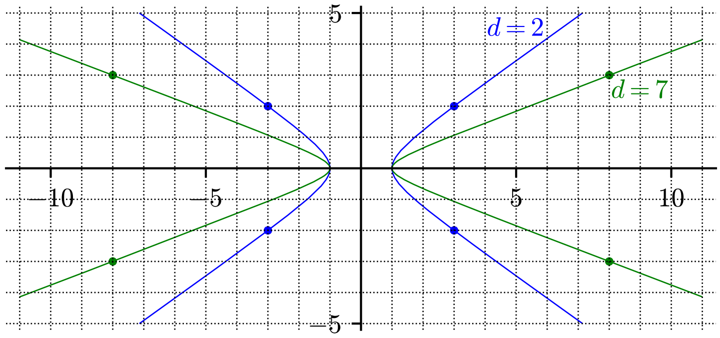
1. Die Pell Gleichung

Pell Gleichung: $\quad x^2 - dy^2 = 1 \quad (d \in \mathbb{N}^+ \text{ kein Quadrat})$



$$x^2 - dy^2 = (x + \sqrt{d}y)(x - \sqrt{d}y)$$

Satz 1 (Dirichlet Lemma)**.** *Sei $x \in \mathbb{R}$ und $N \in \mathbb{N}^+$. Dann gibt es $p, q \in \mathbb{Z}$ teilerfremd mit*

$$\left| x - \frac{p}{q} \right| \leqslant \frac{1}{q(N+1)} \quad \text{und} \quad 1 \leqslant q \leqslant N.$$

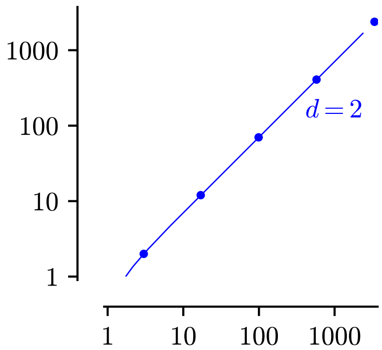
Korollar 2. *Sei $x \in \mathbb{R} \backslash \mathbb{Q}$. Dann gibt es unendlich viele $p, q \in \mathbb{Z}$ teilerfremd mit $|qx - p| < \frac{1}{q}$.*

Theorem 3. *Die Pell Gleichung $x^2 - dy^2 = 1$, $0 < d \neq n^2$, hat eine nichttriviale Lösung $(x, y) \in \mathbb{Z}^2$.*

Korollar 4. *Die Pell Gleichung $x^2 - dy^2 = 1$, $0 < d \neq n^2$, hat unendlich viele Lösungen $(x, y) \in \mathbb{Z}^2$.*

Die Lösungen von $x^2 - 2y^2 = 1$:

$$(\pm 3, \pm 2), (\pm 17, \pm 12), (\pm 99, \pm 70), (\pm 577, \pm 408), (\pm 3363, \pm 2378), \ldots$$



2. Quadratische Zahlkörper und Zahlringe

Zahlkörper: endliche Körpererweiterungen von $\mathbb{Q}$
quadratischen Zahlkörper: $\mathbb{Q}(\sqrt{d})$ $(d \in \mathbb{Z}\backslash\{0,1\}$ quadratfrei$)$

$$\mathbb{Q}(\sqrt{d}) = \mathbb{Q} + \mathbb{Q}\sqrt{d} = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$$

Konjugation, Norm, Spur:

$$\begin{aligned} \overline{\square} : \quad & \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d}) \\ & z = a + b\sqrt{d} \mapsto \overline{z} := a - b\sqrt{d} \end{aligned}$$

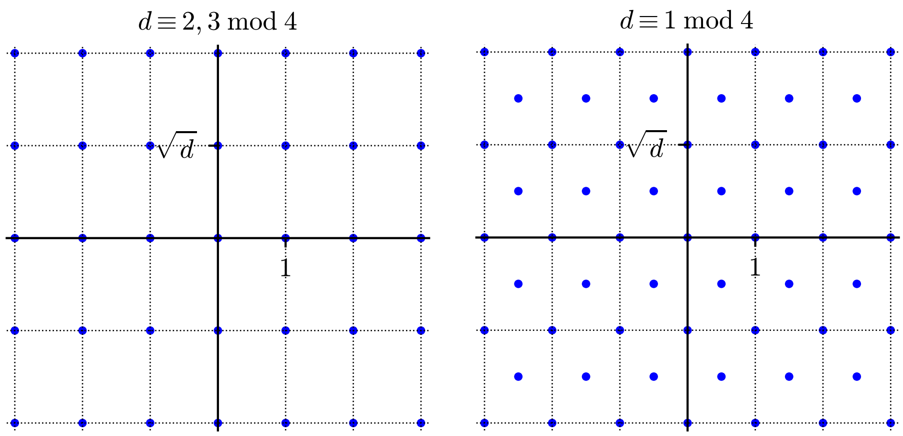
$$\begin{aligned} N : \quad & \mathbb{Q}(\sqrt{d}) \to \mathbb{Q} \\ & z = a + b\sqrt{d} \mapsto a^2 - db^2 = z \cdot \overline{z} \end{aligned} \qquad \begin{aligned} \mathrm{tr} : \quad & \mathbb{Q}(\sqrt{d}) \to \mathbb{Q} \\ & z = a + b\sqrt{d} \mapsto 2a = z + \overline{z} \end{aligned}$$

$$N(z \cdot w) = N(z) \cdot N(w) \qquad \mathrm{tr}(z + w) = \mathrm{tr}(z) + \mathrm{tr}(w)$$

Definition 5. $\mathcal{O}_d := \{z \in \mathbb{Q}(\sqrt{d}) \mid \mathrm{tr}(z) \in \mathbb{Z}, N(z) \in \mathbb{Z}\} \subseteq \mathbb{Q}(\sqrt{d})$ *heißt* quadratischer Zahlring.

Lemma 6. *$\mathcal{O}_d$ ist tatsächlich ein Unterring, und es gilt:*

- $\mathcal{O}_d = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} = \mathbb{Z} + \mathbb{Z}\sqrt{d}$ *falls* $d \equiv 2, 3 \bmod 4$
- $\mathcal{O}_d = \{\frac{a+b\sqrt{d}}{2} \mid a, b \in \mathbb{Z}$ *und* $a \equiv b \bmod 2\} = \mathbb{Z} + \mathbb{Z}\omega$ *mit* $\omega = \frac{1+\sqrt{d}}{2}$ *falls* $d \equiv 1 \bmod 4$



3. Einheiten in quadratischen Zahlringen

Lemma 7. *Für* $z \in \mathcal{O}_d$ *ist* $z \in \mathcal{O}_d^\times \iff N(z) = \pm 1$.

Korollar 8. *Für* $a, b \in \mathbb{Z}$ *gilt:*

- $a + b\sqrt{d} \in \mathcal{O}_d^\times \iff a^2 - db^2 = \pm 1$ *falls* $d \equiv 2, 3 \bmod 4$
- $\frac{a+b\sqrt{d}}{2} \in \mathcal{O}_d^\times \iff a^2 - db^2 = \pm 4$ *falls* $d \equiv 1 \bmod 4$

Satz 9. *Im imaginär-quadratischen Fall $d < 0$ sind alle Einheiten Einheitswurzeln. Konkret:*

$$\mathcal{O}_{-1}^\times = \langle \xi_4 \rangle \qquad \mathcal{O}_{-3}^\times = \langle \xi_6 \rangle \qquad \mathcal{O}_d^\times = \langle \xi_2 \rangle = \pm 1 \quad \text{für } d \leqslant -5 \text{ oder } d = -2$$

Lemma 10. *Im reellquadratischen Fall $d > 0$ ist $\mathcal{O}_d^\times \cap (1, M)$ endlich für alle $M > 1$.*

Satz 11. *Im reellquadratischen Fall $d > 0$ gibt es $\varepsilon \in \mathcal{O}_d^\times, \varepsilon \neq \pm 1$, sodass $\mathcal{O}_d^\times = \{\pm\varepsilon^k \mid k \in \mathbb{Z}\}$.*

Theorem 12. *Sei $d \in \mathbb{Z}\backslash\{0,1\}$ quadratfrei und $U \subseteq \mathcal{O}_d$ die multiplikative Gruppe der Einheitswurzeln im Ganzzahlring $\mathcal{O}_d$ des Körpers $\mathbb{Q}(\sqrt{d})$. Dann gilt:*

$$\mathcal{O}_d^\times \cong \begin{cases} U & d < 0 \\ U \times \mathbb{Z} & d > 0 \end{cases}$$

Die Pell Gleichung

Die Gleichung $x^2 - dy^2 = 1$ mit $d \in \mathbb{N}^+$ heißt Pell-Gleichung.

Wir suchen die ganzzahligen Lösungen $(x,y) \in \mathbb{Z}^2$.
$(1,0)$ und $(-1,0)$ heißen triviale Lösungen.

Wichtig: $x^2 - dy^2 = (x + \sqrt{d}\,y)(x - \sqrt{d}\,y)$

Wenn $d = n^2$ mit $n \in \mathbb{N}$ dann folgt für jede Lösung:

$$1 = x^2 - dy^2 = (x+ny)(x-ny)$$

$$\Rightarrow x+ny = x-ny \quad \Rightarrow y = 0$$

Satz 1 (Dirichlet Lemma). *Sei $x \in \mathbb{R}$ und $N \in \mathbb{N}^+$. Dann gibt es $p, q \in \mathbb{Z}$ teilerfremd mit*

$$\underbrace{\left|x - \frac{p}{q}\right| \leqslant \frac{1}{q(N+1)}} \quad \text{und} \quad 1 \leqslant q \leqslant N.$$

<u>Beweis</u> $\quad |qx - p| \leq \frac{1}{N+1}$

$[y] := y - \lfloor y \rfloor$

Betrachte die $N+1$ Zahlen $0, [x], [2x], \dots, [Nx] \in [0,1)$.
Teile $[0,1)$ in die $N+1$ Intervalle

$$\left[\frac{j}{N+1}, \frac{j+1}{N+1}\right) \qquad j = 0, \dots, N$$

auf.

Wenn im letzten Intervall eine Zahl liegt, gibt es $1 \leq q \leq N$ ganz mit $\frac{N}{N+1} \leq [qx] < 1$.

$p := \lceil qx \rceil$. $\Rightarrow |p - qx| \leq \frac{1}{N+1}$

Ansonsten gibt es nach dem Schubfachprinzip $0 \leq r < s \leq N$ sodass $|[rx] - [sx]| < \frac{1}{N+1}$.

$q := s - r$, $p := \lfloor sx \rfloor - \lfloor rx \rfloor$.

$$\Rightarrow |qx - p| = |sx - rx - \lfloor sx \rfloor + \lfloor rx \rfloor| = |[sx] - [rx]| < \frac{1}{N+1}.$$

$\square$

Korollar 2. *Sei $x \in \mathbb{R} \backslash \mathbb{Q}$. Dann gibt es unendlich viele $p, q \in \mathbb{Z}$ teilerfremd mit $|qx - p| < \frac{1}{q}$.*

Beweis

Nach dem letzten Satz gibt es solche $p, q \in \mathbb{Z}$.
Angenommen es gibt nur endlich viele, genannt (p_i, q_i).

$$\varepsilon := \min_i |q_i x - p_i| > 0$$

Aber nach dem letzten Satz mit $N \geq \frac{1}{\varepsilon}$ gibt es p, q teilerfremd mit

$$|qx - p| < \frac{1}{N} \leq \varepsilon \,. \; \lightning$$

$\square$

Theorem 3. *Die Pell Gleichung $x^2 - dy^2 = 1$, $0 < d \neq n^2$, hat eine nichttriviale Lösung $(x, y) \in \mathbb{Z}^2$.*

Beweis

Nach letztem Korollar gibt es unendlich viele $(x, y) \in \mathbb{N}^2$ teilerfremd mit $|x - y\sqrt{d}| < \frac{1}{y} \leq 1$.

Insbesondere $x \leq 1 + y\sqrt{d}$.

$$\Rightarrow |x^2 - dy^2| = |x + y\sqrt{d}|\,|x - y\sqrt{d}| = \frac{x + y\sqrt{d}}{y}$$

$$\leq \frac{1 + 2y\sqrt{d}}{y} \leq 1 + 2\sqrt{d}$$

Nach dem Schubfachprinzip gibt es $M \in [-1-2\sqrt{d}, 1+2\sqrt{d}]$ ganz sodass $x^2 - dy^2 = M$ unendlich viele teilerfremde Lösungen hat.

$M \neq 0$ da $\sqrt{d} \notin \mathbb{Q}$. Da $(\mathbb{Z}/M\mathbb{Z})^2$ endlich ist, gibt es zwei verschiedene Lösungen $(x_1, y_1), (x_2, y_2) \in \mathbb{N}^2$ mit $x_1 \equiv x_2 \mod M$ und $y_1 \equiv y_2 \mod M$.

$$A := x_1 x_2 - y_1 y_2 d$$
$$B := x_2 y_1 - x_1 y_2$$

sodass $A + B\sqrt{d} = (x_1 + y_1\sqrt{d})(x_2 - y_2\sqrt{d})$.

$$\Rightarrow A^2 - dB^2 = (A + B\sqrt{d})(A - B\sqrt{d}) = (x_1^2 - d y_1^2)(x_2^2 - d y_2^2)$$
$$= M \cdot M = M^2$$

$$A \equiv x_1^2 - y_1^2 d \equiv 0 \mod M$$
$$B \equiv x_1 y_2 - x_1 y_2 \equiv 0 \mod M$$

$$A =: M\tilde{A} \qquad (\tilde{A}, \tilde{B} \in \mathbb{N})$$
$$B =: M\tilde{B}$$

$$\tilde{A}^2 - d\tilde{B}^2 = \frac{1}{M^2}(A^2 - dB^2) = 1$$

Die Lösung ist nichttrivial, da

$$\tilde{B} = 0 \Rightarrow B = 0 \Rightarrow x_2 y_1 = x_1 y_2 \Rightarrow \frac{x_1}{y_1} = \frac{x_2}{y_2} \quad ↯$$

$\square$

Korollar 4. *Die Pell Gleichung* $x^2 - dy^2 = 1$, $0 < d \neq n^2$, *hat unendlich viele Lösungen* $(x, y) \in \mathbb{Z}^2$.

<u>Beweis</u>

Sei $(x, y) \in \mathbb{Z}^2$ eine nichttriviale Lösung.

$$x_n := \frac{(x+y\sqrt{d})^n + (x-y\sqrt{d})^n}{2} \in \mathbb{Z}$$

$$y_n := \frac{(x+y\sqrt{d})^n - (x-y\sqrt{d})^n}{2\sqrt{d}} \in \mathbb{Z}$$

sodass
$$x_n + y_n\sqrt{d} = (x+y\sqrt{d})^n$$
$$x_n - y_n\sqrt{d} = (x-y\sqrt{d})^n.$$

$$\Rightarrow x_n^2 - dy_n^2 = (x_n + y_n\sqrt{d})(x_n - y_n\sqrt{d})$$
$$= (x+y\sqrt{d})^n (x-y\sqrt{d})^n$$
$$= (x^2 - dy^2)^n = 1$$

Die Lösungen sind alle verschieden, da

$$|x_n + y_n\sqrt{d}| = |x+y\sqrt{d}|^n \quad \text{und} \quad |x+y\sqrt{d}| \neq 1$$

da falls $|x+y\sqrt{d}| = 1$ folgt

$$1 = (x+y\sqrt{d})(x-y\sqrt{d})$$

also $x+y\sqrt{d} = x-y\sqrt{d}$, also $y=0$. $\lightning$

$\square$

Quadratische Zahlkörper & Zahlringe

$\mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Z}$ heißt quadratischer Zahlkörper.

$d = 0,1 \Rightarrow \mathbb{Q}(\sqrt{d}) = \mathbb{Q}$

Falls $n^2 \mid d$ mit $n \in \mathbb{N}$, dann

$$\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(n\sqrt{d/n^2}) = \mathbb{Q}\left(\sqrt{\frac{d}{n^2}}\right).$$

Also setzen wir voraus, dass $d \neq 0,1$ und d quadratfrei.

$\sqrt{d}$ ist Nullstelle von $X^2 - d \in \mathbb{Q}[X]$.

$$\Rightarrow \mathbb{Q}(\sqrt{d}) = \mathbb{Q} + \mathbb{Q}\sqrt{d}$$

Die Konjugation ist

$$\begin{aligned} \overline{\cdot} : \mathbb{Q}(\sqrt{d}) &\longrightarrow \mathbb{Q}(d) \\ a + b\sqrt{d} &\longmapsto a - b\sqrt{d} \end{aligned}$$

$$z \cdot (a+b) = z \cdot a + z \cdot b$$

Bezüglich der Basis $(1, \sqrt{d})$ ist die Multiplikation mit $a + b\sqrt{d}$ gegeben durch $\begin{pmatrix} a & db \\ b & a \end{pmatrix}$.

$z \in \mathbb{C}$ heißt ganz-algebraisch, wenn es Nullstelle eines normierten Polynoms in $\mathbb{Z}[X]$ ist.

$\Leftrightarrow$ Minimalpolynom von z liegt in $\mathbb{Z}[X]$

normiertes

Bei uns: Das Minimalpolynom von $z \in \mathbb{Q}(\sqrt{d})$ ist

$$X - z \quad \text{bzw.} \quad (X-z)(X-\bar{z})$$
$$= X^2 - \mathrm{tr}(z)X + N(z)$$

Definition 5. $\mathcal{O}_d := \{z \in \mathbb{Q}(\sqrt{d}) \mid \mathrm{tr}(z) \in \mathbb{Z}, N(z) \in \mathbb{Z}\} \subseteq \mathbb{Q}(\sqrt{d})$ *heißt* quadratischer Zahlring.

Lemma 7. *$\mathcal{O}_d$ ist tatsächlich ein Unterring, und es gilt:*

- $\mathcal{O}_d = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} = \mathbb{Z} + \mathbb{Z}\sqrt{d}$ *falls* $d \equiv 2, 3 \bmod 4$
- $\mathcal{O}_d = \{\frac{a+b\sqrt{d}}{2} \mid a, b \in \mathbb{Z}$ *und* $a \equiv b \bmod 2\} = \mathbb{Z} + \mathbb{Z}\omega$ *mit* $\omega = \frac{1+\sqrt{d}}{2}$ *falls* $d \equiv 1 \bmod 4$

Beweis

Diese Mengen liegen tatsächlich in $\mathcal{O}_d$.

Sei $\frac{A + B\sqrt{d}}{2} \in \mathcal{O}_d$, $A, B \in \mathbb{Q}$.

$$\Rightarrow A \in \mathbb{Z}, \frac{A^2 - dB^2}{4} \in \mathbb{Z}$$

Insbesondere $A^2 - dB^2 \in \mathbb{Z}$, also $dB^2 \in \mathbb{Z}$,

also $B \in \mathbb{Z}$ da d quadratfrei.

$$\Rightarrow A \in \mathbb{Z}, B \in \mathbb{Z}, A^2 \equiv dB^2 \bmod 4$$

Die einzigen Quadrate in $\mathbb{Z}/4\mathbb{Z}$ sind 0, 1.

$d \equiv 2, 3 \bmod 4 \Rightarrow A^2 \equiv B^2 \equiv 0 \bmod 4$
$\Rightarrow A \equiv B \equiv 0 \bmod 2$

$d \equiv 1 \bmod 4 \Rightarrow A^2 \equiv B^2 \bmod 4$
$\Rightarrow A \equiv B \bmod 2$

$\square$

Lemma 9. *Für $z \in \mathcal{O}_d$ ist* $\quad z \in \mathcal{O}_d^\times \iff N(z) = \pm 1$.

Beweis

$\boxed{\Rightarrow}$ $zw = 1 \Rightarrow 1 = N(1) = N(zw) = N(z)N(w)$

$\Rightarrow N(z) = \pm 1$

$\boxed{\Leftarrow}$ $\pm 1 = N(z) = z\overline{z} \qquad \Rightarrow z^{-1} = \pm \overline{z}$

Korollar 10. *Für $a, b \in \mathbb{Z}$ gilt:*

- $a + b\sqrt{d} \in \mathcal{O}_d^\times \iff a^2 - db^2 = \pm 1$ *falls* $d \equiv 2, 3 \bmod 4$
- $\frac{a+b\sqrt{d}}{2} \in \mathcal{O}_d^\times \iff a^2 - db^2 = \pm 4$ *falls* $d \equiv 1 \bmod 4$

Beweis

$d \equiv 2,3 \bmod 4 \rightsquigarrow$ genau vorheriges Lemma

$d \equiv 1 \bmod 4$ gilt auch

$$\frac{a+b\sqrt{d}}{2} \in \mathcal{O}_d^\times \iff \left(\frac{a}{2}\right)^2 - d\left(\frac{b}{2}\right)^2 = \pm 1$$

$$\iff a^2 - db^2 = \pm 4 .$$

Und $a^2 - db^2 \equiv 0 \bmod 4$

$\Rightarrow a^2 \equiv b^2 \bmod 4 \Rightarrow a \equiv b \bmod 2$

$\square$

Satz 11. *Im imaginär-quadratischen Fall $d < 0$ sind alle Einheiten Einheitswurzeln. Konkret:*

$\mathcal{O}_{-1}^\times = \langle \xi_4 \rangle \qquad \mathcal{O}_{-3}^\times = \langle \xi_6 \rangle \qquad \mathcal{O}_d^\times = \langle \xi_2 \rangle = \pm 1$ *für $d \leqslant -5$ oder $d = -2$*

Beweis

Die Norm entspricht dem komplexen Absolutbetrag. Da es nur endlich viele Elemente auf dem Einheitskreis gibt (in $\mathcal{O}_d$), ist jedes z mit $N(z) = 1$ eine Einheitswurzel.

$\square$

Lemma 12. *Im reellquadratischen Fall $d > 0$ ist $\mathcal{O}_d^\times \cap (1, M)$ endlich für alle $M > 1$.*

Beweis

Für $e \in \mathcal{O}_d^\times \cap (1, M)$.

$\Rightarrow e\bar{e} = N(e) = \pm 1 \Rightarrow \bar{e} \in (-1, 1)$

$\Rightarrow tr(e) = e + \bar{e} \in (0, M+1)$

$\Rightarrow$ nur endlich viele Möglichkeiten für $N(e)$ und $tr(e)$.

$\Rightarrow e$ ist eine der $4M$ Nullstellen von

$$\{X^2 - aX + b\}_{a \in \{1, \dots, M\}, b \in \{-1, 1\}}$$

$\square$

Satz 13. *Im reellquadratischen Fall $d > 0$ gibt es $\varepsilon \in \mathcal{O}_d^\times, \varepsilon \neq \pm 1$, sodass $\mathcal{O}_d^\times = \{\pm\varepsilon^k \mid k \in \mathbb{Z}\}$.*

Beweis

Es gibt eine nichttriviale Einheit e, da wir eine nichttriviale Lösung der Pellgleichung haben.

O.b.d.A ist $e > 1$. Nach vorherigem Lemma gibt es eine kleinste Einheit $\varepsilon > 1$.

Angenommen es gibt $e \in \mathcal{O}_d$, $e \neq \varepsilon^k$ $\forall k \in \mathbb{Z}$. O.b.d.A. $e > 0$.

$\Rightarrow \varepsilon^k < e < \varepsilon^{k+1}$ mit $k \in \mathbb{Z}$

$\Rightarrow 1 < e\varepsilon^{-k} < \varepsilon$ ↯

$\square$

Theorem 14. *Sei $d \in \mathbb{Z}\backslash\{0, 1\}$ quadratfrei und $U \subseteq \mathcal{O}_d$ die multiplikative Gruppe der Einheitswurzeln im Ganzzahlring $\mathcal{O}_d$ des Körpers $\mathbb{Q}(\sqrt{d})$. Dann gilt:*

$$\mathcal{O}_d^\times \cong \begin{cases} U & d < 0 \\ U \times \mathbb{Z} & d > 0 \end{cases}$$