KAPITEL 9

Konstruierbarkeit mit Zirkel und Lineal

1. Konstruktionen mit Zirkel und Lineal - Konstruierbare Punkte

Zugrunde liegt $\mathbb{R}^2 = \{(x,y) : x, y \in \mathbb{R}\}$.

- $\mathbb{R}^2$ betrachten wir als **Ebene**, die Elemente von $\mathbb{R}^2$ werde **Punkte** genannt.
- Den **Abstand** zweier Punkte P, Q schreiben wir als $|PQ|$. Ist $P = (x_P, y_P)$ und $Q = (x_Q, y_Q)$, so ist
$$|PQ| = \sqrt{(x_P - x_Q)^2 + (y_P - y_Q)^2}.$$
- Zu zwei verschiedenen Punkten P, Q bezeichne $G(P,Q)$ die **Gerade durch** P **und** Q. Ist $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$, so lässt sich die Gerade durch die Gleichung
$$(x_Q - x_P)(y - y_P) = (y_Q - y_P)(x - x_P)$$
beschreiben.
- Mit $K(P,r)$ wird der **Kreis mit Mittelpunkt** P **und Radius** r bezeichnet. Dabei ist P ein Punkt und $r \in \mathbb{R}_{>0}$. Ist $P = (x_P, y_P)$, so lässt sich der Kreis durch die Gleichung
$$(x - x_P)^2 + (y - y_P)^2 = r^2$$
beschreiben.

Gegeben sei eine Menge von Punkten $M \subseteq \mathbb{R}^2$, wobei wir voraussetzen, dass M die Punkte $(0,0)$ und $(1,0)$ enthält. Es soll erklärt werden, was es heißt, dass sich ein Punkt $P \in \mathbb{R}^2$ aus M mit **Zirkel und Lineal konstruieren** lässt:

Definition. *Gegeben sei eine Menge $M \subseteq \mathbb{R}^2$ mit $(0,0), (1,0) \in M$. Wir sagen, P* **lässt sich aus** M **mit Zirkel und Lineal konstruieren***, wenn es Mengen $M_0, M_1, \ldots, M_n \subseteq \mathbb{R}^2$ gibt mit*
$$M = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \quad \text{und} \quad P \in M_n,$$
sodass M_{i+1} aus M_i durch einen der drei folgenden **elementaren Konstruktionsschritte** *hervorgeht:*

(i) *Sind $P_1, Q_1, P_2, Q_2 \in M_i$ mit $P_1 \neq Q_1$, $P_2 \neq Q_2$ und $G(P_1,Q_1) \neq G(P_2,Q_2)$, und schneiden sich die Geraden in genau einem Punkt $P_{i,1}$, so setzen wir*
$$M_{i+1} = M_i \cup \{P_{i,1}\}.$$

(ii) *Sind $P_1, Q_1, P, P_2, Q_2 \in M_i$ mit $P_1 \neq Q_1$ und $P_2 \neq Q_2$, so betrachten wir die Gerade $G = G(P_1,Q_1)$ und den Kreis $K = K(P, |P_2Q_2|)$. (Beachte: Der Radius muss als Abstand zweier Punkte aus M_i auftreten.) Gerade und Kreis können sich in 0, 1 oder 2 Punkten schneiden, d.h.*
$$|G(P_1,Q_1) \cap K(P, |P_2Q_2|)| \in \{0,1,2\}.$$
Schnittpunkte können wir zu M_i hinzunehmen, d.h. sind $P_{i,1}, \ldots, P_{i,r} \in G(P_1,Q_1) \cap K(P, |P_2Q_2|)$, so setzen wir
$$M_{i+1} = M_i \cup \{P_{i,1}, \ldots, P_{i,r}\}.$$

Datei: kt_konstruierbarkeit.tex. Version vom 8.7.2024

(iii) *Sind* $P_1, Q_1, R_1, P_2, Q_2, R_2 \in M_i$ *mit* $P_1 \neq P_2$, $Q_1 \neq R_1$ *und* $Q_2 \neq R_2$, *so betrachten wir die Kreise* $K(P_1, |Q_1R_1|)$ *und* $K(P_2, |Q_2R_2|)$. *Da die Mittelpunkte* P_1, P_2 *verschieden sind, können sich die Kreise in* 0, 1 *oder* 2 *Punkten schneiden. Wir können wählen*

$$P_{i,1}, \dots, P_{i,r} \in K(P_1, |Q_1R_1|) \cap K(P_2, |Q_2R_2|)$$

und setzen dann

$$M_{i+1} = M_i \cup \{P_{i,1}, \dots, P_{i,r}\}.$$

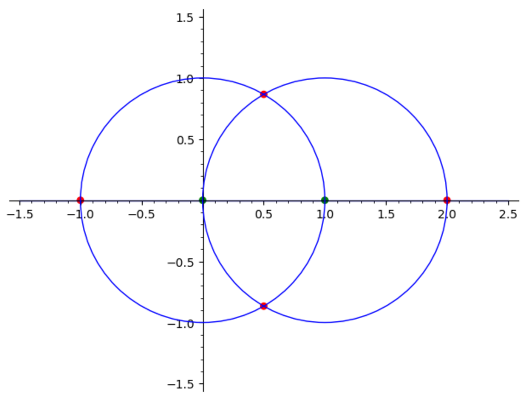
Beispiel: Wir starten mit $M = \{(0,0), (1,0)\}$. Wir wollen sehen, wie wir die Punkte $(0,1)$ und $(1,1)$ aus M konstruieren können. Wir setzen $M_0 = M = \{(0,0), (1,0)\}$.

- Für die elementaren Konstruktionsschritte können wir die Gerade $G((0,0),(1,0))$ und die Kreise $K((0,0), |(0,0)(1,0)|)$ und $K((1,0), |(0,0)(1,0)|)$ betrachten, die sich durch die Gleichungen

$$y = 0, \quad x^2 + y^2 = 1, \quad (x-1)^2 + y^2 = 1$$

beschreiben lässen. Die Schnittpunkte sind

$$(1,0), \quad (-1,0), \quad (0,0), \quad (2,0), \quad (\frac{1}{2}, \frac{\sqrt{3}}{2}), \quad (-\frac{1}{2}, \frac{\sqrt{3}}{2}).$$

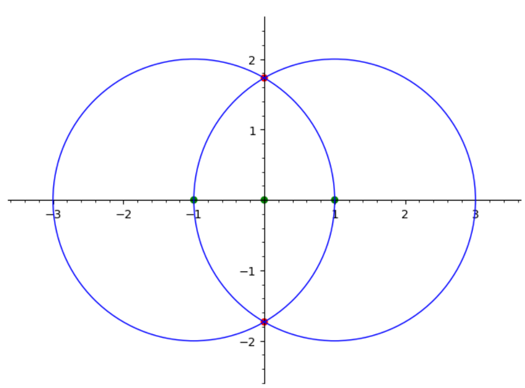


Wir wollen aber zunächst nur den Punkt $(-1,0)$ zu M hinzunehmen:

$$M_1 = \{(0,0), (1,0), (-1,0)\}.$$

- Wir schneiden die Kreise um $(-1,0)$ und $(1,0)$ mit Radius $2 = |(1,0)(-1,0)|$:

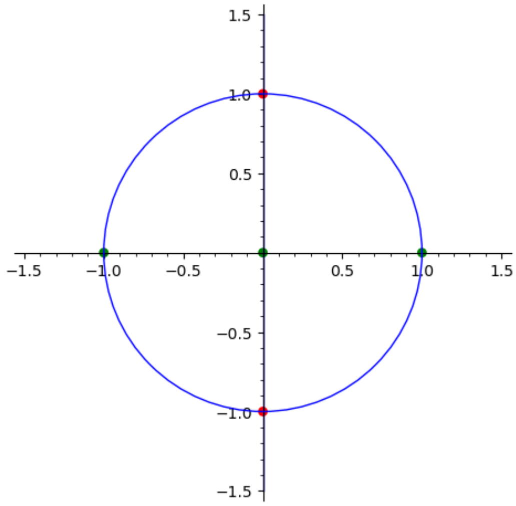
$$K((1,0),2) \cap K((-1,0),2) = \{(0,\sqrt{3}), (0,-\sqrt{3})\}.$$



Wir nehmen den Punkt $(0,\sqrt{3})$ hinzu:

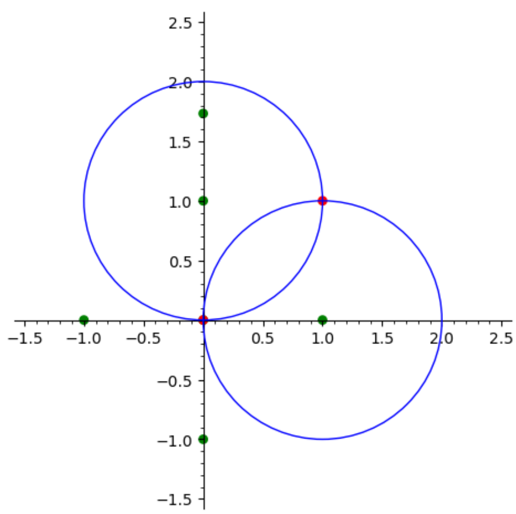
$$M_2 = \{(0,0), (1,0), (-1,0), (0,\sqrt{3})\}.$$

- Wir schneiden nun die Gerade durch $(0,0)$ und $(0,\sqrt{3})$ mit dem Kreis um $(0,0)$ vom Radius $1 = |(1,0)(0,0)|$ und erhalten die Schnittpunkte $(0,1)$ und $(0,-1)$:



  Wir nehmen die Punkte $(0,1)$ und $(0,-1)$ zu M_2 hinzu:
$$M_3 = \{(0,0),(1,0),(-1,0),(0,\sqrt{3}),(0,1),(0,-1)\}.$$

- Wegen $(1,0),(0,1) \in M_3$ und $1 = |(1,0)(0,0)|$ können wir die Kreise um $(1,0)$ und $(0,1)$ vom Radius 1 schneiden:
$$K((1,0),1) \cap K((0,1),1) = \{(0,0),(1,1)\}.$$



  Wir nehmen den Punkt $(1,1)$ zu M_3 hinzu:
$$M_4 = \{(0,0),(1,0),(-1,0),(0,\sqrt{3}),(0,1),(-1,0),(1,1)\}.$$

Bemerkung: Wenn wir im Folgenden sagen, dass ein Punkt P konstruierbar ist, so meint dies, dass er mit Zirkel und Lineal aus einer Menge M konstruierbar ist. Ist nichts zur Menge M ausgesagt, so ist immer $M = \{(0,0),(1,0)\}$ gemeint.

LEMMA. (1) *Ist (a,b) ein konstruierbarer Punkt, so sind auch die Punkte*
$$(\pm a, \pm b), \quad (\pm b, \pm a), \quad (\pm a, 0), \quad (0, \pm a), \quad (\pm b, 0), \quad (0, \pm b)$$
konstruierbar.

(2) *Sind $(a,0)$ und $(b,0)$ konstruierbare Punkte, so ist auch (a,b) konstruierbar.*

Beweis:

(1)
- – Wir betrachten die Kreise mit den Mittelpunkten $(0,0)$ und $(1,0)$, die durch den Punkt (a,b) gehen. Dann schneiden sich die Kreise in (a,b) und $(a,-b)$. Also ist auch $(a,-b)$ konstruierbar.
  – Wir betrachten die Kreise mit den Mittelpunkten $(0,0)$ und $(0,1)$, die durch den Punkt (a,b) gehen. Dann schneiden sich die Kreise in den Punkten (a,b) und $(-a,b)$. Also ist auch $(-a,b)$ konstruierbar.
  – Der Kreis mit Mittelpunkt $(0,0)$, der durch (a,b) geht, schneidet die Gerade, die durch $(0,0)$ und (a,b) in den Punkten (a,b) und $(-a,-b)$. Also ist auch $(-a,-b)$ konstruierbar.

  Wir haben also nun alle Punkt $(a,-b)$, $(-a,b)$, $(-a,-b)$ konstruiert.
- – Die Geraden $G((a,b),(a,-b))$ und $G((0,0),(1,0))$ schneiden sich in $(a,0)$. Analog sieht man, dass auch $(-a,0)$ konstruierbar ist.
  – Die Geraden $G((a,b),(-a,b))$ und $G((0,0),(0,1))$ schneiden sich in $(0,b)$, sodass auch $(0,b)$ konstruierbar ist. Genauso sieht man, dass auch $(0,-b)$ konstruierbar ist.
- – Der Kreis mit Mittelpunkt $(0,0)$ durch $(a,0)$ schneidet die Gerade $G((0,0),(0,1))$ im Punkt $(0,a)$. Auf die gleiche Weise sieht man, dass auch die Punkte $(0,\pm a)$ und $(\pm b,0)$ konstruierbar sind.

(2)
- Der Kreis mit Mittelpunkt $(0,0)$ durch $(b,0)$ schneidet die Gerade durch $(0,0)$ und $(0,1)$ im Punkt $(0,b)$. Also ist auch $(0,b)$ konstruierbar.
- Der Kreis mit Mittelpunkt $(a,0)$ durch $(0,0)$ schneidet die Gerade $y=0$ im den Punkten $(0,0)$ und $(2a,0)$. Also ist auch $(2a,0)$ konstruierbar. Der Kreis mit Mittelpunkt $(0,0)$, der durch $(2a,0)$ geht, wird durch die Gleichung
$$x^2+y^2=4a^2$$
beschrieben. Der Kreis mit Mittelpunkt $(2a,0)$, der durch $(0,0)$ geht, wird durch
$$(x-2a)^2+y^2=4a^2, \quad \text{also} \quad x^2-4ax+4a^2+y^2=4a^2$$
beschrieben. Wir wollen den Schnitt, also die gemeinsamen Lösungen der beiden Gleichungen bestimmen. Subtraktion der Gleichungen liefert $-4ax+4a^2=0$, also $x=a$. Es bleibt die Gleichung $y^2=3a^2$. Wir erhalten also die Schnittpunkte
$$(a,\pm\sqrt{3}a).$$
Damit können wir die Gerade $x=a$ konstruieren.
- Genauso können wir die Gerade $y=b$ konstruieren.
- Der Schnitt der Geraden $x=a$ und $y=b$ liefert den Punkt (a,b), der demzufolge konstruierbar ist. ■

Lemma. *Sei $M\subseteq\mathbb{R}^2$ eine Menge von Punkten mit $(0,0),(1,0)\in M$. Dazu betrachten wir die Menge reeller Zahlen*
$$M'=\{a\in\mathbb{R}:(a,b)\in M\}\cup\{b\in\mathbb{R}:(a,b)\in M\}$$
und die Menge von Punkten
$$M''=\{(a,0):a\in M'\}.$$
Dann gilt: Ein Punkt $P\in\mathbb{R}^2$ ist genau dann aus M konstruierbar, wenn P aus M'' konstruierbar ist.

Der Beweis folgt direkt mit dem vorangegangenen Lemma.

Bemerkung: Nach den vorangegangenen Überlegungen nennen wir einen Punkt $P\in\mathbb{R}^2$ **aus einer Menge** $M\subseteq\mathbb{R}$ **konstruierbar**, wenn sich P aus der Punktmenge $\{(a,0):a\in M\}$ mit Zirkel und Lineal konstruieren lässt.

2. Konstruierbare reelle Zahlen

Definition. *Sei M eine Menge von Punkten aus $\mathbb{R}^2$ oder eine Menge von Zahlen $M \subseteq \mathbb{R}$ mit $(0,0),(1,0) \in M$ bzw. $0,1 \in M$.*

(1) *Eine reelle Zahl $a \in \mathbb{R}$ heißt aus M mit Zirkel und Lineal* **konstruierbar**, *wenn $(a,0)$ aus M mit Zirkel und Lineal konstruierbar ist.*
(2) *Sei $\mathbb{K}(M)$* **die Menge der aus M konstruierbaren reellen Zahlen**. *Im Fall $M = \{(0,0),(1,0)\}$ oder $M = \{0,1\}$ schreiben wir dafür auch einfach $\mathbb{K}$.*

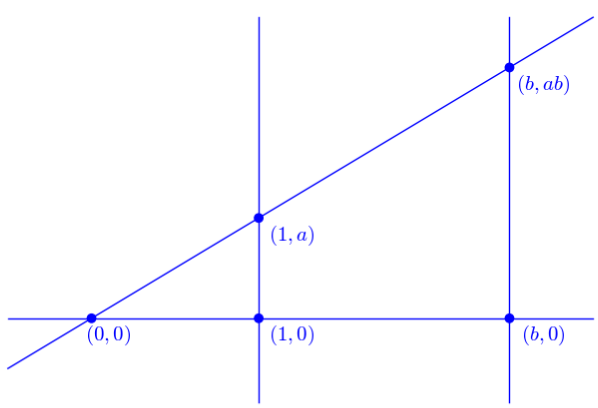
Wir zeigen nun, dass die konstruierbaren reellen Zahlen eine schöne algebraische Struktur haben.

Addition und Subtraktion: Sind $(a,0)$ und $(b,0)$ aus M konstruierbar, so auch $(\pm a \pm b, 0)$.

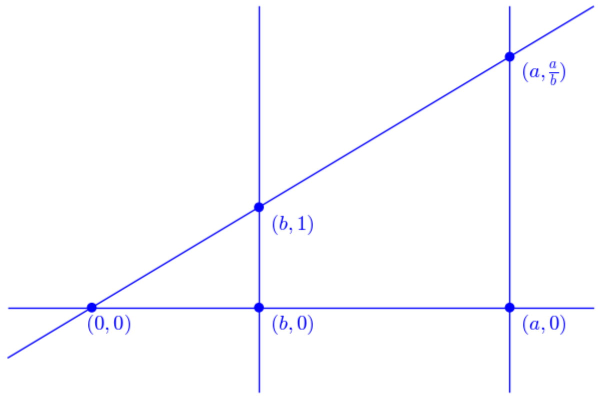
- Ist $(a,0)$ konstruierbar (und $a \neq 0$), so schneidet der Kreis mit Mittelpunkt $(0,0)$ durch $(a,0)$ die Gerade $x = 0$ in den Punkten $(\pm a, 0)$. Daher ist auch $(-a,0)$ konstruierbar. Wir können daher für das Folgende o.E. $a > 0$ und $b > 0$ annehmen.
- Sei $a > 0$ und $b > 0$. Der Kreis mit Mittelpunkt $(a,0)$ und Radius b schneidet die Gerade $x = 0$ in den Punkten $(a+b,0)$ und $(a-b,0)$. Also sind die Punkte $(a+b,0)$ und $(a-b,0)$ konstruierbar. Mit dem ersten Teil ist dann klar, dass auch die Punkte $(-a-b,0)$ und $(-a+b,0)$ konstruierbar sind.

Multiplikation und Division: Seien $(a,0)$ und $(b,0)$ konstruierbar. Dabei können wir nach den vorangegangenen Überlegungen o.E. $a > 0$ und $b > 0$ annehmen.

-
  - Wir konstruieren die Senkrechte auf $x = 0$ durch den Punkt $(1,0)$ und schneiden mit dem Kreis $K((1,0),a)$. Einer der Schnittpunkte ist $(1,a)$.
  - Wir können jetzt die Gerade durch $(0,0)$ und $(1,a)$ konstruieren, also $y = ax$.
  - Wir konstruieren die Senkrechte auf $y = 0$ durch den Punkt $(b,0)$, also $x = b$.
  - Wir schneiden nun $y = ax$ mit $x = b$ und erhalten den Punkt (b,ab), also ab.



-
  - Wir konstruieren die Senkrechte auf $x = 0$ durch den Punkt $(b,0)$ und schneiden diese mit dem Kreis $K((b,0),1)$. Einer der Schnittpunkte ist $(b,1)$.
  - Wir konstruieren die Gerade durch $(0,0)$ und $(b,1)$, also $y = \frac{x}{b}$.
  - Wir konstruieren die Senkrechte auf $y = 0$ durch den Punkt $(a,0)$, also $x = a$.
  - Wir schneiden nun $y = \frac{x}{b}$ mit $x = a$ und erhalten den Punkt $(a, \frac{a}{b})$, insbesondere also $\frac{b}{a}$.



Damit erhalten wir:

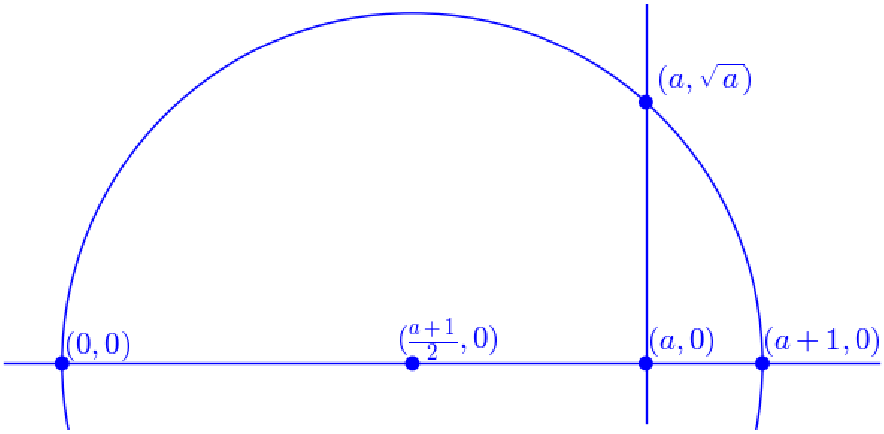
Satz. *Sei M eine Menge von Punkten aus $\mathbb{R}^2$ oder eine Menge von Zahlen $M \subseteq \mathbb{R}$ mit $(0,0),(1,0) \in M$ bzw. $0,1 \in M$.*

(1) *$\mathbb{K}(M)$ ist ein Körper (mit $\mathbb{Q} \subseteq \mathbb{K}(M)$).*
(2) *Ist $a \in \mathbb{K}(M)$, d.h. ist a eine aus M konstruierbare reelle Zahl, so auch alle Zahlen aus $\mathbb{Q}(a)$.*

Der Körper $\mathbb{K}(M)$ ist auch abgeschlossen unter Wurzelziehen - soweit dies möglich ist:

Wurzelziehen: Sei $a > 0$ gegeben. Wir nehmen an, dass $(a, 0)$ konstruierbar ist.

- Wir konstruieren den Punkt $(a+1, 0)$, dann damit $(\frac{a+1}{2}, 0)$. (Entweder mit Division oder durch Konstruktion der Mittelsenkrechten.)
- Wir konstruieren den Kreis mit Mittelpunkt $(\frac{a+1}{2}, 0)$, der durch $(0,0)$ geht, also
$$(x - \frac{a+1}{2})^2 + y^2 = (\frac{a+1}{2})^2,$$
was auch in der Form
$$x^2 - (a+1)x + y^2 = 0$$
geschrieben werden kann.
- Wir konstruieren die Senkrechte auf $y = 0$ durch den Punkt $(a, 0)$, also $x = a$.
- Wir schneiden den Kreis mit der Senkrechten:
$$x = a \quad \text{und} \quad x^2 - (a+1)x + y^2 = 0.$$
Wir erhalten $x = a$ und
$$y^2 = -a^2 + (a+1)a = a,$$
also die Punkte
$$(a, \pm\sqrt{a}).$$
Also ist $(a, \sqrt{a})$ konstruierbar, und damit auch $\sqrt{a}$.



Damit haben wir folgende Aussage gezeigt:

Satz. *Es gilt:*

$$a \in \mathbb{K}(M) \cap \mathbb{R}_{>0} \quad \Longrightarrow \quad \sqrt{a} \in \mathbb{K}(M).$$

Wir wollen die konstruierbaren Zahlen nun noch genauer anschauen.

Lemma. *Seien $P_1, P_2, P_3, P_4, P_5 \in \mathbb{R}^2$ mit $P_1 \neq P_2$ und $P_4 \neq P_5$. Sei $G = G(P_1, P_2)$ und $K = K(P_3, |P_4P_5|)$. Wir schreiben $P_i = (\alpha_i, \beta_i)$.*

(1) *Die Gerade $G(P_1, P_2)$ wird beschrieben durch die Gleichung*

$$(\beta_1 - \beta_2)x + (\alpha_2 - \alpha_1)y = \alpha_2\beta_1 - \alpha_1\beta_2.$$

Im Fall $\alpha_1 \neq \alpha_2$ kann man auch die Gleichung

$$y = \frac{\beta_1 - \beta_2}{\alpha_1 - \alpha_2}x + \frac{\alpha_1\beta_2 - \alpha_2\beta_1}{\alpha_1 - \alpha_2}$$

verwenden. Im Fall $\alpha_1 = \alpha_2$ kann man die Gleichung

$$x = \alpha_1$$

verwenden. Die Gerade lässt sich also in der Form

$$ax + by = c \quad \text{mit} \quad a, b, c \in \mathbb{Q}(\alpha_1, \alpha_2, \beta_1, \beta_2)$$

schreiben.

(2) *Der Kreis $K(P_3, |P_4P_5|)$ wird beschrieben durch die Gleichung*

$$(x - \alpha_3)^2 + (y - \beta_3)^2 = (\alpha_4 - \alpha_5)^2 + (\beta_4 - \beta_5)^2.$$

Der Kreis lässt sich also in der Form

$$x^2 + y^2 + ax + by = c \quad \text{mit} \quad a, b, c \in \mathbb{Q}(\alpha_3, \beta_3, \alpha_4, \beta_4, \alpha_5, \beta_5)$$

schreiben.

Beweis: Hier sind nur einige bekannte Sachen aufgeschrieben und etwas umgeformt worden. ■

Lemma. (i) *Seien $P_1, P_2, P_3, P_4 \in \mathbb{R}^2$ mit $P_i = (\alpha_i, \beta_i)$, $P_1 \neq P_2$, $P_3 \neq P_4$ und $G(P_1, P_2) \neq G(P_3, P_4)$. Sei $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_4, \beta_1, \ldots, \beta_4)$. Dann haben die Geraden höchstens einen Schnittpunkt. Ist (α, β) ein Schnittpunkt, so gilt*

$$\alpha, \beta \in L, \quad \text{also} \quad L(\alpha, \beta) = L.$$

(ii) *Seien* $P_1, P_2, P_3, P_4, P_5 \in \mathbb{R}^2$ *mit* $P_i = (\alpha_i, \beta_i)$*, sodass* $G(P_1, P_2)$ *eine Gerade und* $K(P_3, |P_4P_5|)$ *ein Kreis ist. Sei* $L = \mathbb{Q}(\alpha_1, \dots, \alpha_5, \beta_1, \dots, \beta_5)$*. Dann schneiden sich Gerade und Kreis höchstens in* 2 *Punkten. Ist* (α, β) *ein Schnittpunkt, so gilt*

$$L(\alpha, \beta) = L \quad \textit{oder} \quad [L(\alpha, \beta) : L] = 2.$$

(iii) *Sind* $P_1, \dots, P_6$ *Punkte im* $\mathbb{R}^2$ *mit* $P_i = (\alpha_i, \beta_i)$*, sodass* $K(P_1, |P_2P_3|)$ *und* $K(P_4, |P_5P_6|)$ *zwei verschiedene Kreise sind. Sei* $L = \mathbb{Q}(\alpha_1, \dots, \alpha_6, \beta_1, \dots, \beta_6)$*. Dann schneiden sich die Kreise in höchstens* 2 *Punkten. Ist* (α, β) *ein Schnittpunkt, so gilt*

$$L(\alpha, \beta) = L \quad \textit{oder} \quad [L(\alpha, \beta) : L] = 2.$$

Beweis:

(i) Die Geraden werden beschrieben durch die Gleichungen

$$(\beta_1 - \beta_2)x + (\alpha_2 - \alpha_1)y = \alpha_2\beta_1 - \alpha_1\beta_2 \quad \text{und} \quad (\beta_3 - \beta_4)x + (\alpha_4 - \alpha_3)y = \alpha_4\beta_3 - \alpha_3\beta_4.$$

Wenn die Geraden nicht identisch sind, gibt es höchstens einen Schnittpunkt, der durch das Gleichungssystem

$$\begin{pmatrix} \beta_1 - \beta_2 & \alpha_2 - \alpha_1 \\ \beta_3 - \beta_4 & \alpha_4 - \alpha_3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha_2\beta_1 - \alpha_1\beta_2 \\ \alpha_4\beta_3 - \alpha_3\beta_4 \end{pmatrix}$$

eindeutig bestimmt ist. Für einen Schnittpunkt (α, β) gilt dann

$$\alpha, \beta \in \mathbb{Q}(\alpha_1, \dots, \alpha_4, \beta_1, \dots, \beta_4).$$

(ii)

Dies muss noch ausgeführt werden. Aufgabe H37 zeigt ein Beispiel.

(iii)

Die muss noch ausgeführt werden. Aufgabe P61 zeigt ein Beispiel.

■

Der folgende Satz gibt vereint die vorangegangenen Überlegungen zu einem Konstruierbarkeitskriterium:

Satz. *Sei* $M \subseteq \mathbb{R}$ *mit* $0, 1 \in M$*. Eine reelle Zahl* $\alpha \in \mathbb{R}$ *ist genau dann aus* M *konstruierbar, wenn es Körper*

$$\mathbb{Q}(M) = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n \subseteq \mathbb{R}$$

gibt mit

$$[K_i : K_{i-1}] = 2 \textit{ für } i = 1, \dots, n \quad \textit{und} \quad \alpha \in K_n.$$

Beweis:

(1) Sei α aus M konstruierbar, wobei wir jetzt M als Teilmenge von $\mathbb{R}^2$ mit $(0,0), (1,0) \in M$ auffassen. Es gibt dann Mengen $M_0, M_1, \dots, M_n \subseteq \mathbb{R}^2$ mit

$$M = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \quad \text{und} \quad (\alpha, 0) \in M_n,$$

sodass M_{i+1} aus M_i durch elementare Konstruktionsschritte entsteht. Sei

$$K_i = \mathbb{Q}(\widetilde{M_i}) \quad \text{mit} \quad \widetilde{M_i} = \{a \in \mathbb{R} : (a, b) \in M_i\} \cup \{b \in \mathbb{R} : (a, b) \in M_i\}.$$

Wir müssen nochmals die elementaren Konstruktionsschritte betrachten. Dabei können wir annehmen, dass bei jedem Schritt nur ein Punkt $P_{i+1} = (\alpha_{i+1}, \beta_{i+1})$ dazukommt:

$$M_{i+1} = M_i \cup \{P_{i+1}\} = M_i \cup \{(\alpha_{i+1}, \beta_{i+1})\}, \quad \text{und damit} \quad K_{i+1} = K_i(\alpha_{i+1}, \beta_{i+1}).$$

(i) Seien $P_1, P_2, P_3, P_4 \in M_i$, sodass $G(P_1, P_2)$ und $G(P_3, P_4)$ nichtidentische und nichtparallele Geraden sind. Sie schneiden sich in einem Punkt (α, β). Ist $P_i = (\alpha_i, \beta_i)$, so gilt nach dem vorangegangenen Lemma:

$$\alpha, \beta \in \mathbb{Q}(\alpha_1, \dots, \alpha_4, \beta_1, \dots, \beta_4),$$

und damit wegen $\alpha_1, \dots, \alpha_4, \beta_1, \dots, \beta_4 \in K_i$

$$\alpha, \beta \in K_i,$$

und damit

$$K_{i+1} = K_i(\alpha, \beta) = K_i.$$

(ii) Seien $P_1, P_2, P_3, P_4, P_5 \in M_i$ mit $P_i = (\alpha_i, \beta_i)$, sodass $G(P_1, P_2)$ eine Gerade und $K(P_3, |P_4P_5|)$ ein Kreis ist. Mit $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_5, \beta_1, \ldots, \beta_5)$ gilt für einen möglichen Schnittpunkt (α, β)

$$L(\alpha, \beta) = L \quad \text{oder} \quad [L(\alpha, \beta) : L] = 2.$$

Dann folgt natürlich auch für $K_{i+1} = K_i(\alpha, \beta)$

$$K_{i+1} = K_i \quad \text{oder} \quad [K_{i+1} : K_i] = 2.$$

(iii) Seien $P_1, P_2, P_3, P_4, P_5, P_6 \in M_i$ mit $P_i = (\alpha_i, \beta_i)$, sodass $K(P_1, |P_2P_3|)$ und $K(P_4, |P_5P_6|)$ nicht identische Kreise sind. Sie schneiden sich dann höchstens in zwei Punkten. Ist (α, β) ein Schnittpunkt und $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_6, \beta_1, \ldots, \beta_6)$, so gilt

$$L(\alpha, \beta) = L \quad \text{oder} \quad [L(\alpha, \beta) : L] = 2.$$

Dann folgt auch für $K_{i+1} = K_i(\alpha, \beta)$

$$K_{i+1} = K_i \quad \text{oder} \quad [K_{i+1} : K_i] = 2.$$

Wir erhalten dann

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n \quad \text{mit} \quad \alpha \in K_n \quad \text{und} \quad [K_{i+1} : K_i] \in \{1, 2\}.$$

Streichen wir aus der Körperkette K_{i+1}, falls $K_{i+1} = K_i$ gilt, so können wir $[K_{i+1} : K_i] = 2$ erreichen, wie behauptet.

(2) Sei umgekehrt eine Körperkette

$$\mathbb{Q}(M) = K_0 \subsetneq K_1 \subsetneq K_2 \cdots \subsetneq K_n$$

gegeben mit

$$[K_{i+1} : K_i] = 2.$$

Dann gibt es $\alpha_i \in K_i$ mit

$$K_{i+1} = K_i(\sqrt{\alpha_i}).$$

Wir beweisen durch Induktion, dass K_i aus konstruierbaren Zahlen besteht. Für $K_0 = \mathbb{Q}(M)$ ist das klar. Sei nun $i \geq 0$ und bereits gezeigt, dass K_i aus konstruierbaren Zahlen besteht. Wegen $\alpha_i \in K_i$ ist auch $\sqrt{\alpha_i}$ konstruierbar, also auch $K_{i+1} = K_i(\sqrt{\alpha_i})$. Dies beweist die Behauptung. ∎

Folgerung. *Sei $\alpha \in \mathbb{R}$.*

(1) *Ist α konstruierbar (aus $\{0, 1\}$), so ist α algebraisch über $\mathbb{Q}$ von 2-Potenzgrad, d.h.*

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n \text{ für ein } n \in \mathbb{N}_0.$$

(2) *Ist α konstruierbar aus $M \subseteq \mathbb{R}$, so ist α algebraisch über $\mathbb{Q}(M)$ von 2-Potenzgrad, d.h.*

$$[\mathbb{Q}(M, \alpha) : \mathbb{Q}(M)] = 2^n \text{ für ein } n \in \mathbb{N}_0.$$

Beweis:

(1) Seien $\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq K_2 \subsetneq \cdots \subsetneq K_n$ mit $[K_{i+1} : K_i] = 2$ und $\alpha \in K_n$. Dann ist

$$[K_n : \mathbb{Q}] = [K_n : K_{n-1}] \cdot \ldots [K_3 : K_2] \cdot [K_2 : K_1] \cdot [K_1 : \mathbb{Q}] = 2^n.$$

Wegen $\alpha \in K_n$ folgt die Behauptung nun aus

$$2^n = [K_n : \mathbb{Q}] = [K_n : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}].$$

(2) Dies beweist man genau wie (1). ∎

Mit dem Grad-Kriterium lässt sich nun leicht zeigen, dass einige klassische Probleme nicht lösbar sind:

Folgerung. *Folgende Zahlen lassen sich nicht mit Zirkel und Lineal konstruieren:*

(1) *(Quadratur des Kreises) $\sqrt{\pi}$.*
(2) *(Würfelverdoppelung) $\sqrt[3]{2}$.*

Beweis:

(1) $\sqrt{\pi}$ ist transzendent über $\mathbb{Q}$, also ist $\sqrt{\pi}$ keine konstruierbare Zahl.
(2) $\sqrt[3]{2}$ hat das Minimalpolynom $f = x^3 - 2$ über $\mathbb{Q}$, hat also Grad 3 über $\mathbb{Q}$. Daher ist $\sqrt[3]{2}$ keine konstruierbare Zahl.

Für $\alpha \in \mathbb{R}$ gilt die Implikation

$$\alpha \text{ konstruierbar} \quad \Longrightarrow \quad [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k \text{ für ein } k \in \mathbb{N}_0.$$

Leider gilt die Rückrichtung $\Longleftarrow$ im Allgemeinen nicht. Eine notwendige und hinreichende Bedingung findet sich im nächsten Abschnitt.

3. Eine algebraische Charakterisierung der Konstruierbarkeit einer reellen Zahl

Es gilt folgender Satz:

SATZ. *Für eine Zahl $\alpha \in \mathbb{R}$ sind folgende frei Bedingungen äquivalent:*

(1) *α ist konstruierbar (aus $\{0, 1\}$).*
(2) *α ist algebraisch über $\mathbb{Q}$ und für die normale Hülle N von $\mathbb{Q}(\alpha)$ gilt $[N : \mathbb{Q}] = 2^k$ für ein $k \in \mathbb{N}_0$.*
(3) *Es gibt eine Galoiserweiterung $K|\mathbb{Q}$ mit $[K : \mathbb{Q}] = 2^l$ für ein $l \in \mathbb{N}_0$ und $\alpha \in K$.*

Beweis folgt. ■

Beispiel: Das Polynom $f = x^4 - x - 1 \in \mathbb{Q}[x]$ ist irreduzibel über $\mathbb{Q}$, es hat zwei reelle Nullstellen $\alpha \approx 1.22$ und $\beta \approx -0.72$. Also gilt

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 = 2^2.$$

Der Zerfällungskörper von f ist die normale Hülle N von α. Man kann zeigen, dass

$$[N : \mathbb{Q}] = 24 = 2^3 \cdot 3$$

gilt. Also ist α nicht konstruierbar. (In einer Staatsexamensaufgabe vom Herbst 2013 soll man - mit Hilfe einiger Teilaufgaben - zeigen, dass α oder β nicht mit Zirkel und Lineal konstruierbar ist.)

4. Regelmäßige n-Ecke

Für $n \in \mathbb{N}_{\geq 3}$ bilden die n Punkte

$$P_{n,j} = \left(\cos(\frac{2\pi}{n} \cdot j), \sin(\frac{2\pi}{n} \cdot j)\right), \quad j = 0, \ldots, n-1$$

die Ecken eines regelmäßigen n-Ecks. Wir haben bereits gesehen, dass dieses regelmäßige n-Eck genau dann konstruierbar ist, wenn

$$\cos(\frac{2\pi}{n})$$

konstruierbar ist.

LEMMA. *Sei $n \in \mathbb{N}_{\geq 3}$ und $\zeta_n = e^{\frac{2\pi i}{n}}$. ($\zeta_n$ ist eine primitive n-te Einheitswurzel und $\mathbb{Q}(\zeta_n)$ der n-te Kreisteilungskörper.) Dann gilt:*

(1) *Es ist*
$$\cos(\frac{2\pi}{n}) = \frac{1}{2}(\zeta_n + \frac{1}{\zeta_n}).$$
(2) *Es ist*
$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\cos(\frac{2\pi}{n}))] = 2 \quad \textit{und} \quad [\mathbb{Q}(\cos(\frac{2\pi}{n})) : \mathbb{Q}] = \frac{1}{2}\varphi(n).$$

Beweis:

(1) Dies folgt aus
$$\zeta_n = e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i\,\sin(\frac{2\pi}{n}) \quad \text{und} \quad \zeta_n^{-1} = e^{-\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) - i\,\sin(\frac{2\pi}{n}).$$

(2) Es ist
$$(x-\zeta_n)(x-\frac{1}{\zeta_n}) = x^2-(\zeta_n+\frac{1}{\zeta_n})x+1 = x^2-2\cos(\frac{2\pi}{n})x+1.$$
Daher ist
$$[\mathbb{Q}(\zeta_n):\mathbb{Q}(\cos(\frac{2\pi}{n}))] \le 2.$$
Wegen $\mathbb{Q}(\cos(\frac{2\pi}{n})) \subseteq \mathbb{R}$ und $\mathbb{Q}(\zeta_n) \not\subseteq \mathbb{R}$ folgt schließlich
$$[\mathbb{Q}(\zeta_n):\mathbb{Q}(\cos(\frac{2\pi}{n}))] = 2.$$
Aus
$$\varphi(n) = [\mathbb{Q}(\zeta_n):\mathbb{Q}] = [\mathbb{Q}(\zeta_n):\mathbb{Q}(\cos(\frac{2\pi}{n}))]\cdot[\mathbb{Q}(\cos(\frac{2\pi}{n})):\mathbb{Q}]$$
folgt dann der Rest. ■

Satz. *Für $n \in \mathbb{N}_{\ge 3}$ ist $\cos(\frac{2\pi}{n})$ (und damit ein regelmäßiges n-Eck) genau dann konstruierbar, wenn $\varphi(n)$ eine 2-Potenz ist.*

Beweis: Sei $\zeta_n = \exp(\frac{2\pi i}{n})$. $\mathbb{Q}(\zeta_n)$ ist galoissch über $\mathbb{Q}$ mit Galoisgruppe
$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \simeq \mathbb{Z}_n^*.$$
Da die Galoisgruppe abelsch ist, ist auch $\mathbb{Q}(\cos(\frac{2\pi}{n}))$ galoissch über $\mathbb{Q}$, insbesondere ist $\mathbb{Q}(\cos(\frac{2\pi}{n}))$ die galoissche Hülle seiner selbst mit
$$[\mathbb{Q}(\cos(\frac{2\pi}{n})):\mathbb{Q}] = \frac{1}{2}\varphi(n).$$
Mit dem zuvor angegebenen Kriterium für Konstruierbarkeit folgt:
$$\begin{aligned}\cos(\frac{2\pi}{n}) \text{ konstruierbar} \quad &\iff \quad [\mathbb{Q}(\cos(\frac{2\pi}{n})):\mathbb{Q}] = 2^k \text{ für ein } k \in \mathbb{N}_0 \quad \iff \\ &\iff \quad \frac{1}{2}\varphi(n) = 2^k \text{ für ein } k \in \mathbb{N}_0 \quad \iff \\ &\iff \quad \varphi(n) = 2^l \text{ für ein } l \in \mathbb{N}.\end{aligned}$$
Dies wollten wir zeigen. ■

Überlegung: Sei $n \in \mathbb{N}_{\ge 3}$. Ist
$$n = 2^e \cdot p_1^{e_1} \dots p_r^{e_r}$$
die Primfaktorzerlegung von n (mit Primzahlen $2 < p_1 < p_2 < \dots < p_r$ und $e_1, \dots, e_r \ge 1$), so gilt
$$\varphi(n) = \varphi(2^e)\cdot\varphi(p_1^{e_1})\dots\varphi(p_r^{e_r}).$$
Es ist
$$\varphi(2^0) = 1, \quad \varphi(2^1) = 1 \quad \text{und} \quad \varphi(2^e) = 2^{e-1} \text{ für } e \ge 2.$$
Für ungerade Primzahlen p_i ist
$$\varphi(p_i) = p_i - 1 \quad \text{und} \quad \varphi(p_i^{e_i}) = p_i^{e_1-1}(p_i-1) \text{ für } e_i \ge 2.$$
Daher folgt:
$$\varphi(n) \text{ ist 2-Potenz} \quad \iff \quad e_i = 1 \text{ und } p_i - 1 \text{ ist 2-Potenz für } i = 1, \dots, r.$$

Definition. *Eine Primzahl $p \ge 3$ heißt* **Fermat-Primzahl**, *wenn*
$$p = 2^e + 1 \textit{ für ein } e \in \mathbb{N}$$
gilt.

Beispiele: Durch Probieren findet man folgende Fermat-Primzahlen:
$$3 = 2^1 + 1, \quad 5 = 2^2 + 1, \quad 17 = 2^4 + 1, \quad 257 = 2^8 + 1, \quad 65537 = 2^{16} + 1.$$

Nun können wir obigen Satz nochmals etwas anders formulieren:

Satz. *Für $n \in \mathbb{N}_{\geq 3}$ ist $\cos(\frac{2\pi}{n})$ (und damit das regelmäßige n-Eck) genau dann konstruierbar, wenn n die Primfaktorzerlegung*
$$n = 2^e \cdot p_1 \dots p_r$$
mit $e \in \mathbb{N}_0$ und $r \geq 0$ paarweise verschiedenen Fermat-Primzahlen p_i hat.

Bemerkung: Wir betrachten die ersten Fermat-Primzahlen. Das gleichseitige 3-Eck kennt man schon aus der Schule. In den Übungen wurde das gleichmäßige 5-Eck konstruiert und dabei die Formel
$$\cos(\frac{2\pi}{5}) = \frac{\sqrt{5} - 1}{4}$$
benutzt. Die nächste Fermat-Primzahl ist 17. Mit Galoistheorie kommt man auf folgende Formel:
$$\cos(\frac{2\pi}{17}) = -1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + \sqrt{68 + 12\sqrt{17} - 4\sqrt{170 + 38\sqrt{17}}}.$$
(Im Prinzip kann man die Formel zur Konstruktion des regelmäßigen 17-Ecks benutzen, da wir wissen, wie man die rechte Seite der Gleichung mit Zirkel und Lineal aus $\{(0,0),(1,0)\}$ konstruieren kann.)

Exkurs: Herleitung der Formel für $\cos(\frac{2\pi}{17})$

5. Konstruierbarkeit von Winkeln

Ein Winkel φ (mit $0 \leq \varphi < 2\pi$) heißt **konstruierbar**, wenn sich drei Punkte Z, S, T finden lassen, sodass die Strahlen $\overrightarrow{ZS}$ und $\overrightarrow{ZT}$ den Winkel φ einschließen. Dann können wir auch den Punkt $(\cos\varphi, \sin\varphi)$ konstruieren, also auch $(\cos\varphi, 0)$. Können wir $(\cos\varphi, 0)$ konstruieren, so auch $(\cos\varphi, \sin\varphi)$, also den Winkel φ. Daher können wir (etwas vereinfacht) sagen: Ein Winkel φ ist genau dann konstruierbar, wenn die reelle Zahl $\cos(\varphi)$ konstruierbar ist.

Ein altes Problem ist die

Winkeldreiteilung: Ist φ ein Winkel, kann man daraus den Winkel $\frac{\varphi}{3}$ konstruieren. Anders formuliert: Kann man aus $\cos(\varphi)$ die Zahl $\cos(\frac{\varphi}{3})$ konstruieren?

Beispiel: Wegen $\cos(\pi) = -1$ und $\cos(\frac{\pi}{3}) = \frac{1}{2}$ ist trivialerweise der Winkel $\frac{\pi}{3}$ aus π konstruierbar.

Beispiel: Wir wollen zeigen, dass sich der Winkel $\frac{\pi}{9}$ nicht aus dem Winkel $\frac{\pi}{3}$ konstruieren lässt. Sei $\beta = \cos(\frac{\pi}{9})$. Mit dem 3-ten Chebyshev-Polynom gilt
$$\cos(\frac{\pi}{3}) = \cos(3\beta) = T_3(\beta) = 4\beta^3 - 3\beta,$$
also
$$4\beta^3 - 3\beta = \frac{1}{2} \quad \text{bzw.} \quad 8\beta^3 - 6\beta - 1 = 0$$
Nun ist aber $f = 8x^3 - 6x - 1 \in \mathbb{Q}[x]$ irreduzibel, was man beispielsweise durch Betrachtung modulo 5 sieht. Daher hat β Grad 3 über $\mathbb{Q}$, also
$$[\mathbb{Q}(\cos(\frac{\pi}{9})) : \mathbb{Q}(\cos(\frac{\pi}{3}))] = 3.$$
$\cos(\frac{\pi}{9})$ ist also aus $\cos(\frac{\pi}{3})$ nicht mit Zirkel und Lineal konstruierbar.

Das letzte Beispiel zeigt, dass es kein allgemeines Verfahren zur Winkeldreiteilung geben kann.