Prof. Dr. H. Brenner Osnabrück SS 2015

Elemente der Algebra

Vorlesung 26

Konstruktion von Quadratwurzeln

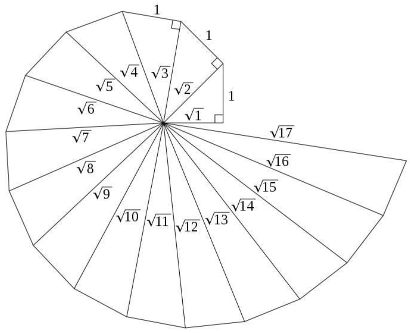
Wenn man sich zwei Punkte 0 und 1 vorgibt und man die dadurch definierte Gerade mit $\mathbb{R}$ identifiziert, so wird diese Gerade durch 0 in zwei Hälften (Halbgeraden) unterteilt, wobei man dann diejenige Hälfte, die 1 enthält, als positive Hälfte bezeichnet. Aus solchen positiven reellen Zahlen kann man mit Zirkel und Lineal die Quadratwurzel ziehen.

Lemma 26.1. *Es sei G eine mit zwei Punkten 0 und 1 markierte Gerade, die wir mit den reellen Zahlen identifizieren. Es sei $a \in G_+$ eine positive reelle Zahl. Dann ist die Quadratwurzel $\sqrt{a}$ aus $0,1,a$ mittels Zirkel und Lineal konstruierbar.*

Beweis. Wir zeichnen den Kreis mit Mittelpunkt 0 durch 1 und markieren den zweiten Schnittpunkt dieses Kreises mit G als -1. Wir halbieren die Strecke zwischen -1 und a gemäß Lemma 25.6 und erhalten den konstruierbaren Punkt $M = \frac{a-1}{2} \in G$. Der Abstand von M zu a als auch zu -1 ist dann $\frac{a+1}{2}$. Wir zeichnen den Kreis mit Mittelpunkt M und Radius $\frac{a+1}{2}$ und markieren einen der Schnittpunkte des Kreises mit der zu G senkrechten Geraden H durch 0 als x. Wir wenden den *Satz des Pythagoras* auf das Dreieck mit den Ecken $0, x, M$ an. Daraus ergibt sich

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

Also repräsentiert (der Abstand von 0 zu) x die Quadratwurzel aus a. $\square$



Die Spirale des Theodorus. In dieser Weise kann man alle Quadratwurzeln von natürlichen Zahlen konstruieren.

Die nächste Aussage bedeutet, dass man zu einem gegebenen Rechteck ein flächengleiches Quadrat konstruieren kann.

Korollar 26.2. *Es sei ein Rechteck in der Ebene gegeben. Dann lässt sich mit Zirkel und Lineal ein flächengleiches Quadrat konstruieren.*

Beweis. Die Längen der Rechteckseiten seien a und b. Wir wählen einen Eckpunkt des Rechtecks als Nullpunkt und verwenden die Geraden durch die anliegenden Rechteckseiten als Koordinatenachsen. Wir wählen willkürlich einen Punkt 1 ($\neq 0$) auf einer der Achsen und schlagen einen Kreis um den Nullpunkt durch den Eckpunkt auf der anderen Achse, so dass beide Seitenlängen auf der mit 0 und 1 markierten Achse liegen. Darauf führen wir die Multiplikation ab nach Lemma 25.8 durch. Aus diesem Produkt zieht man nun gemäß Lemma 26.1 die Quadratwurzel und erhält somit $\sqrt{ab}$. Mit dieser Streckenlänge konstruiert man ein Quadrat, dessen Flächeninhalt gleich dem Flächeninhalt des vorgegebenen Rechtecks ist. $\square$

Man beachte, dass im Beweis der vorstehenden Aussage die Zahl ab von der Wahl der 1 abhängt, nicht aber $\sqrt{ab}$ und damit natürlich auch nicht die Seitenlänge des konstruierten Quadrats.

Konstruierbare und algebraische Zahlen

Wir wollen nun die konstruierbaren Zahlen algebraisch mittels quadratischer Körpererweiterungen charakterisieren. Unter einer reell-quadratischen Körpererweiterung eines Körpers $K \subseteq \mathbb{R}$ verstehen wir eine quadratische Körpererweiterung $K \subseteq K'$ mit $K' \subseteq \mathbb{R}$, die sich also innerhalb der reellen Zahlen abspielt. Eine solche Körpererweiterung ist nach Lemma 24.2 gegeben durch die Adjunktion einer Quadratwurel einer positiven reellen Zahl $\sqrt{c}$ mit $c \in K$, $\sqrt{c} \notin K$. Es gilt die Isomorphie

$$K[\sqrt{c}] \cong K[X]/(X^2 - c)\,.$$

Lemma 26.3. *Sei $K \subseteq \mathbb{R}$ ein Körper. Es sei $P \in \mathbb{C}$ ein Punkt, der sich aus $K^2 = K + Ki$ in einem Schritt konstruieren lässt. Dann liegen die Koordinaten von P in einer reell-quadratischen Körpererweiterung von K.*

Beweis. Wir gehen die drei Möglichkeiten durch, einen Punkt aus K^2 in einem Schritt zu konstruieren. Es sei P der Schnittpunkt von zwei verschiedenen Geraden G_1 und G_2, die über K definiert sind. Es sei also $G_1 = \{(x,y) |\, a_1x + b_1y + c_1 = 0\}$ und $G_2 = \{(x,y) |\, a_2x + b_2d + c_2 = 0\}$ mit $a_1, b_1, c_1, a_2, b_2, c_2 \in K$. Dann gehört der Schnittpunkt zu K^2 und seine Koordinaten gehören zu K. Sei G eine über K definierte Gerade und C ein über K definierter Kreis. Dann ist $G = \{(x,y) |\, ax + by + c = 0\}$ und $C = \{(x,y) |\, (x-r)^2 + (y-s)^2 = d\}$ mit $a, b, c, r, s, d \in K$. Wir können annehmen, dass $b \neq 0$ ist, so dass die Geradengleichung auf die Form $y = ux + v$ gebracht werden kann. Einsetzen von dieser Gleichung in die Kreisgleichung ergibt eine quadratische Gleichung für x über K. Die reellen Koordinaten der (eventuell komplexen) Lösungen davon liegen in einer quadratischen Erweiterung von K. Das gilt dann auch für die zugehörigen Lösungen für y. Seien nun C_1 und C_2 zwei über K definierte verschiedene Kreise. Es seien

$$C_1 = \left\{(x,y) | \, (x-r_1)^2 + (y-s_1)^2 - a_1 = 0\right\}$$

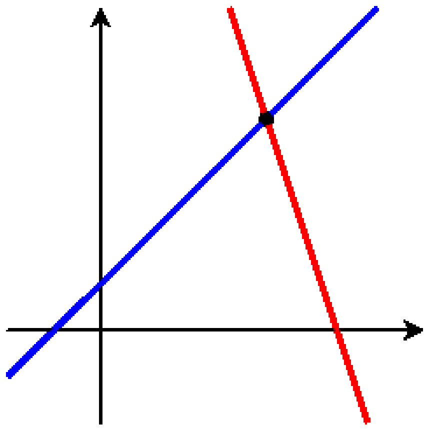
und

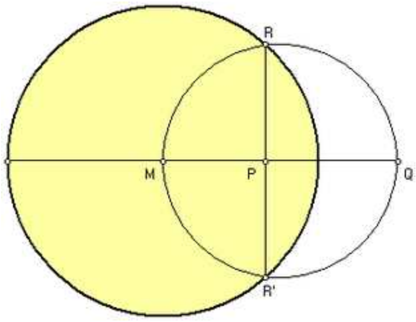
$$C_2 = \left\{(x,y) | \, (x-r_2)^2 + (y-s_2)^2 - a_2 = 0\right\}$$

die Kreisgleichungen. Ein Schnittpunkt der beiden Kreise muss auch jede Linearkombination der beiden Gleichungen erfüllen. Wir betrachten die Differenz der beiden Gleichungen, die die Gestalt

$$x(-2r_1 + 2r_2) + r_1^2 - r_2^2 + y(-2s_1 + 2s_2) + s_1^2 - s_2^2 - a_1 + a_2 = 0$$

besitzt. D.h. dies ist eine Geradengleichung, und die Schnittpunkte der beiden Kreise stimmen mit den Schnittpunkten eines Kreises mit dieser Geraden überein. Wir sind also wieder im zweiten Fall. $\square$





Beispiel 26.4. Wir betrachten die beiden Kreise mit den Kreisgleichungen

$$x^2 + y^2 = 1 \text{ und } (x-2)^2 + y^2 = 3.$$

Die Differenz der beiden Gleichungen ist

$$x^2 - (x-2)^2 + 2 = 0$$

bzw.

$$4x = 2 \text{ und somit } x = \frac{1}{2}\,.$$

Die Schnittpunkte der beiden Kreise müssen also auch auf der durch $x = \frac{1}{2}$ gegebenen Geraden liegen. Setzt man diese Geradenbedingung in die erste Kreisgleichung ein, so erhält man

$$y^2 \,=\, 1 - x^2 \,=\, 1 - \frac{1}{4} \,=\, \frac{3}{4},$$

also

$$y = \pm\frac{\sqrt{3}}{2}\,.$$

Satz 26.5. *Es sei $P \in \mathbb{C}$ eine komplexe Zahl. Dann ist P eine konstruierbare Zahl genau dann, wenn es eine Kette von reell-quadratischen Körpererweiterungen*

$$\mathbb{Q} \subset K_1 \subset K_2 \subset \ldots \subset K_n$$

derart ibt, dass die Koordinaten von P zu K_n gehören.

Beweis. Es sei $P \in \mathbb{C}$ eine konstruierbare komplexe Zahl. D.h. es gibt eine Folge von Punkten $P_1, \ldots, P_n = P$ derart, dass P_{i+1} aus den Vorgängerpunkten $\{0, 1, P_1, \ldots, P_i\}$ in einem Schritt konstruierbar ist. Es sei $P_i = (a_i, b_i)$ und es sei

$$K_i \,=\, \mathbb{Q}(a_1, b_1, \ldots, a_i, b_i)$$

der von den Koordinaten der Punkte erzeugte Unterkörper von $\mathbb{R}$. Nach Lemma 26.3 liegt K_{i+1} in einer reell-quadratischen Körpererweiterung von K_i (und zwar ist $K_{i+1} = K_i$ oder K_{i+1} ist eine reell-quadratische Körpererweiterung von K_i). Die Koordinaten von P liegen also in K_n, und K_n ist das Endglied in einer Folge von quadratischen Körpererweiterungen von $\mathbb{Q}$. Sei umgekehrt angenommen, dass die Koordinaten eines Punktes $P = (a, b)$ in einer Kette von reell-quadratischen Körpererweiterungen von $\mathbb{Q}$ liegen. Wir zeigen durch Induktion über die Länge der Körperkette, dass die Zahlen in einer solchen Kette aus quadratischen Körpererweiterungen konstruierbar sind. Bei $n = 0$ ist $K_0 = \mathbb{Q}$, und diese Zahlen sind konstruierbar. Sei also schon gezeigt, dass alle Zahlen aus K_n konstruierbar sind, und sei $K_n \subset K_{n+1}$ eine reell-quadratische Körpererweiterung. Nach Lemma 24.2 ist $K_{n+1} = K_n[\sqrt{c}]$ mit einer positiven reellen Zahl $c \in K_n$. Nach Induktionsvoraussetzung ist c konstruierbar und nach Lemma 26.1 ist $\sqrt{c}$ konstruierbar. Daher ist auch jede Zahl $u + v\sqrt{c}$ mit $u, v \in K_n$, konstruierbar. Damit sind die Koordinaten von P konstruierbar und somit ist nach Lemma 25.7 auch P selbst konstruierbar. $\square$

Man kann ebenfalls zeigen, dass eine komplex-algebraische Zahl z genau dann konstruierbar ist, wenn der Grad des Zerfällungskörpers des Minimalpolynoms von z eine Potenz von 2 ist. Dies erfordert jedoch die Galoistheorie. Für viele Anwendungen ist allerdings schon die oben vorgestellte Charakterisierung bzw. die folgenden Korollare ausreichend.

KOROLLAR 26.6. *Eine mit Zirkel und Lineal konstruierbare Zahl ist algebraisch.*

Beweis. Dies folgt direkt aus Satz 26.5, aus Satz 24.4 und aus Satz 23.3. □

KOROLLAR 26.7. *Sei $z \in \mathbb{C}$ eine konstruierbare Zahl. Dann ist der Grad des Minimalpolynoms von z eine Potenz von zwei.*

Beweis. Die Koordinaten der konstruierbaren Zahl z liegen nach Satz 26.5 in einer Folge von reell-quadratischen Körpererweiterungen

$$\mathbb{Q} \subset K_1 \subset K_2 \subset \ldots \subset K_n \,.$$

Diese Kette kann man um die komplex-quadratische Körpererweiterung $K_n \subset K_n[i] = L$ ergänzen mit $z \in L$. Nach der Gradformel ist der Grad von L über $\mathbb{Q}$ gleich 2^{n+1}. Dabei ist $\mathbb{Q}(z) = \mathbb{Q}[z] \subseteq L$ ein Unterkörper und daher ist, wieder nach der Gradformel, der Grad von $\mathbb{Q}[z]$ über $\mathbb{Q}$ ein Teiler von 2^{n+1}, also selbst eine Potenz von 2. □

Abbildungsverzeichnis

Quelle = Spiral of Theodorus.svg , Autor = Benutzer Pbroks13 auf en Wikipedia, Lizenz = CC-by-sa 3.0 2
Quelle = Two Lines.svg , Autor = Benutzer Jim.belk auf Commons, Lizenz = PD 3
Quelle = Inversie.PNG , Autor = Benutzer Lymantria auf Commons, Lizenz = CC-by-sa 3.0 3