Antike Konstruktionsprobleme

von Christian Hercher, Aachen

1 Motivation

Im antiken Griechenland wurde Mathematik hauptsächlich durch Geometrie betrieben. Dabei ließen sie als Konstruktionswerkzeuge einzig einen Zirkel und ein unmakiertes Lineal[1] zu. Es stellten sich natürlich sofort Fragen, was damit konstruierbar ist und was nicht.

So entstanden auch die drei klassischen Konstruktionsprobleme:

- Das Problem der Würfelverdopplung: Ist es möglich zu einem gegebenen Würfel die Kantenlänge eines neuen Würfels zu konstruieren, welcher genau das doppelte Volumen des ersten besitzt?
- Das Problem der Quadratur des Kreises: Ist es möglich zu einem vorgegebenem Kreis ein flächengleiches Quadrat zu konstruieren?

  und schließlich
- Das Problem der Winkeldrittelung: Ist es möglich zu einem (beliebig!) vorgegebenen Winkel einen weiteren zu konstruieren, der genau ein Drittel der Größe des Ausgangswinkels besitzt?

In diesem Artikel werden wir uns hauptsächlich mit einem vierten Problem beschäftigen und nach dessen Klärung zu den drei hier genannten zurückkehren:

- Das „n-Eck-Problem“: Für welche natürlichen Zahlen n ist ein regelmäßiges n-Eck konstruierbar?

2 Konstruktionen in der Ebene

Wir wollen im Folgenden die mächtigen Werkzeuge der Algebra auf unsere Probleme anwenden. Dafür müssen wir allerdings unsere geometrischen Überlegungen auf Objekte übertragen, mit denen wir rechnen können.

Was heißt eigentlich „einen Punkt mit Zirkel und Lineal zu konstruieren“? Nun, das bedeutet, dass man ihn in endlich vielen Konstruktionsschritten aus den vorgegebenen Punkten erhalten kann. Dabei gibt es genau drei mögliche Konstruktionsschritte:

[1] Später fand man heraus, dass schon die Benutzung eines Zirkels allein ausreicht um alle Punkte zu konstruieren, die auch mit Zirkel und Lineal konstruierbar sind. Siehe dazu $\sqrt{\text{WURZEL}}$-Heft . . .„Mascheronische Konstruktionen“.

- Schnitt zweier Geraden durch je zwei schon konstruierte Punkte
- Schnitt zweier Kreise, für die je schon ihr Mittelpunkt und ein Punkt auf ihrer Peripherie konstruiert worden sind
- Schnitt einer Geraden durch zwei schon konstruierte Punkte mit einem Kreis, dessen Mittelpunkt und ein Punkt auf seiner Peripherie im Vorfeld konstruiert wurden.

Zuerst fragen wir uns, welche Streckenlängen wir eigentlich konstruieren können. Dazu benötigen wir eine Bezugsgröße, welche wir durch zwei (voneinander verschiedene) fest vorgegebene Punkte der Ebene erhalten: Wir definieren ihren Abstand als 1. Um nicht später in Schwierigkeiten mit (Maß-) Einheiten zu kommen, lassen wir sie gleich ganz weg.

Man überlegt sich leicht, dass man sehr leicht durch „Aneinandersetzen" Summe und Differenz zweier gegebener Längen konstruieren kann. Mit dem Produkt sieht es schon schwieriger aus: Hier benötigt man den Strahlensatz. Analog lässt sich auch das Reziproke einer Länge (ungleich 0) konstruieren, und so auch der entsprechende Quotient. Und schließlich mithilfe des Höhensatzes auch die zweite Wurzel einer nicht-negativen Länge.

Können wir aber noch weitere Streckenlängen konstruieren? Und welche Punkte der Ebene können wir so erreichen? Um diese Frage zu beantworten identifizieren wir die Ebene mit der komplexen Zahlenebene, und unsere beiden Startpunkte mit den komplexen Zahlen 0 und 1. Da wir im Folgenden sehr viel mit komplexen Zahlen arbeiten werden, möchten wir sie im Folgenden Abschnitt nocheinmal kurz in Erinnerung rufen.

3 Die komplexen Zahlen

Die komplexen Zahlen (mit Zahlbereichssymbol $\mathbb{C}$) werden meist als Paare (a, b) reeller Zahlen eingeführt. Dabei schreibt man der besseren Lesbarkeit später meist $a + ib$ anstatt jener Paardarstellung, wobei i als Symbol mit der Eigenschaft $i^2 = -1$ eingeführt wird.

Dies führt dazu, dass man komplexe Zahlen addiert, wie man es sich vorstellt (also $(a_1+ib_1) + (a_2+ib_2) = (a_1 + a_2)+i\,(b_1 + b_2)\,; \forall a_1, a_2, b_1, b_2 \in \mathbb{R}$) und auch so multipliziert ($((a_1+ib_1)\cdot(a_2+ib_2) = (a_1a_2-b_1b_2)+i(a_1b_2+b_1a_2)\,; \forall a_1, a_2, b_1, b_2 \in \mathbb{R}$). Das Einzige, was man sich beim Ausmultiplizieren merken muss, ist, dass eben $i \cdot i = -1$ ist.

Da damit $(a + ib) \cdot (a - ib) = a^2 - b^2$, also reell ist, kann man auch leicht einen komplexen Bruch durch Erweitern mit dem Komplex-Konjugierten des Nenners (also wie hier das Vorzeichen des Imaginärteils, d. h. dem Vorfaktor zu i, umkehren) vereinfachen und berechnen.

Die Darstellung der komplexen Zahlen als Paare reeller Zahlen bringt den Vorteil einer geometrischen Veranschaulichung mit sich: So interpretiert man die komplexen Zahlen als Punkte in einer Ebene, die man komplexe (oder Gaußsche) Zahlenebene nennt. Dabei wird der Realteil einfach als x-Koordinate und der Imaginärteil als y-Koordinate des Punktes interpretiert.

So ergibt sich auch eine neue Interpretation der Addition zweier komplexer Zahlen als „Addition zweier Punkte“ der Ebene. Gemeint ist dabei folgende Operation: Man ergänze die Menge der drei Punkte Koordinatenursprung, erster Punkt, zweiter Punkt so zu einem Parallelogramm, dass die beiden zu addierenden Punkte auf einer Diagonale des Parallelogramms zu liegen kommen. Dann ist der vierte Punkt des Parallelogramms die Summe der beiden vorgegebenen Punkte.

Aber einen Punkt in der Ebene kann man auch anders eindeutig charakterisieren als durch seine (kartesischen) Koordinaten. Es genügen auch die folgenden zwei Informationen: Der Abstand vom Koordinatenursprung und der Winkel zwischen der Verbindung Koordinatenursprung-Punkt und der positiven x-Achse. Diese nennt man dann auch die Polar-Koordinaten des betrachteten Punktes.

Dies liefert uns umgekehrt auch eine andere Darstellung für komplexe Zahlen, die wir später noch brauchen werden: $r\cdot(\cos\varphi + i\cdot\sin\varphi)$, mit $r \geq 0$ und $0 \leq \varphi < 2\Pi$. Dies erhalten wir aus den Definitionen der Winkelfunktionen am Einheitskreis. Dabei ist zu bemerken, dass der Ausdruck in Klammern eine komplexe Zahl mit Betrag Eins (also genau Eins vom Koordinatenursprung entfernt) ist.

Mit ein bisschen Mußе und Kenntnis der Additionstheoreme der Winkelfunktionen rechnet man auch schnell Folgendes nach:

$$r_1(\cos\varphi_1 + i\sin\varphi_1)\cdot r_2(\cos\varphi_2 + i\sin\varphi_2) = r_1r_2\cdot(\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2))\,.$$

Dies bedeutet also, dass wir zwei komplexe Zahlen ganz einfach multiplizieren können: Wir multiplizieren ihre Beträge r und addieren ihre Argumente φ.

Aus algebraischer Sicht ist noch interessant, dass $\mathbb{C}$ ein algebraisch abgeschlossener Körper ist, d. h. jedes nicht-konstante Polynom mit Koeffizienten aus $\mathbb{C}$ mindestens eine Nullstelle besitzt und so in Linearfaktoren zerfällt.

4 Konstruktionen in der Ebene II

Damit können wir nun zurückkehren zu unserer Frage, welche Punkte in der Ebene denn konstruierbar sind. Dabei identifizieren wir unsere Ebene,

in der wir unsere Konstruktionen ausführen, mit der komplexen Zahlenebene derart, dass die beiden uns vorgegebenen Punkte in der Ebene gerade die komplexen Zahlen Null und Eins sind.

Wie wir oben bereits gesehen haben, sind alle rationalen Längen konstruierbar, d. h. insbesondere also alle rationalen Zahlen. Damit ergibt sich also für unsere weiteren Überlegungen keinen Unterschied, wenn wir uns nicht nur diese beiden Punkte, sondern gleich alle rationalen Zahlen als „Startwerte“ vorgeben, denn jede einzelne rationale Zahl ist ja in endlich vielen Konstruktionsschritten aus den beiden „eigentlichen Startwerten“ Null und Eins konstruierbar.

Wie wir weiter oben schon gesehen haben, können wir leicht aus zwei schon konstruierten komplexen Zahlen ihre Summe konstruieren. Wie schaut es mit ihrem Produkt aus? Nun, das Produkt der Beträge haben wir schon oben geklärt, und auch die Summe der Argumente φ ist sehr leicht zu bestimmen. Damit ist auch das Produkt zweier komplexer Zahlen konstruierbar, und mit

$$\frac{1}{a+ib} = \frac{a-ib}{(a+ib)(a-ib)} = \frac{a-ib}{a^2+b^2} = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}$$

auch das Reziproke einer komplexen Zahl ungleich Null, also auch jeder (sinnvolle) Quotient zweier schon konstruierter komplexer Zahlen.

Aber auch die beiden Quadratwurzeln, d. h. Lösungen der Gleichung $z^2 = a + ib$ lassen sich aus einer schon konstruierten Zahl $a + ib$ konstruieren. Dazu schaue man sich die Multiplikationsformel für komplexe Zahlen in ihrer Polarkoordinatendarstellung an und führe sich noch einmal vor Augen, wie man einen vorgegebenen Winkel konstruktiv halbiert.

Somit können wir bisher sagen, dass wir mindestens die komplexen Zahlen konstruieren können, welche durch Ausführen von endlich vielen Operationen der Grundrechenarten (+,-,*,:) und des Quadratwurzelziehens aus den rationalen Zahlen zu erhalten sind.

Die Frage, die sich gleich daran anschließt, ist natürlich: Sind dies alle konstruierbaren komplexen Zahlen, oder können wir noch weitere konstruieren? Die Antwort darauf lautet: Ja, dies sind alle.

Denn schauen wir uns unsere drei möglichen Konstruktionsschritte an: Der Schnitt zweier Geraden lässt sich als Lösung einer linearen Gleichung erhalten. Dabei werden beim Lösen dieser Gleichung die Koeffizienten, die den Verlauf der Geraden beschreiben, (welche i W. nur Real- und Imaginärteile unserer schon konstruierten Zahlen sind) nur durch die Grundrechenarten zum Ergebnis verknüpft. Hier wird noch nicht einmal die Operation des Quadratwurzelziehens benötigt.

Hinweis: Offenbar ist eine komplexe Zahl genau dann konstruierbar, wenn es ihr Real- und Imaginärteil auch sind.

Analog schauen wir uns die anderen beiden Konstruktionsschritte (Schnitt von Kreis mit Gerade und Schnitt von zwei Kreisen) an. Hier ergeben sich quadratische Gleichungen, aber auch jene lassen sich durch Anwenden der uns gegebenen Operationen der Grundrechenarten und Quadratwurzelziehens in endlich vielen Schritten lösen.

Wir können also in allen möglichen Fällen die neu konstruierten komplexen Zahlen wiederum in endlich vielen Schritten durch Anwenden der Grundrechenarten und des Quadratwurzelziehens aus den rationalen Zahlen erhalten, wenn dies für die Punkte, welche die Objekte (Gerade bzw. Kreis), die wir hier zum Schnitt brachten, definierten, auch schon galt.

Zusammenfassend können wir damit sagen: Es lassen sich genau diejenigen komplexen Zahlen konstruieren, welche wir in endlich vielen Schritten durch Anwenden der Grundrechenarten und des Quadratwurzelziehens aus den rationalen Zahlen erhalten können!

5 Gruppen, Körper, Vektorräume

Diese Eigenschaft, die wir gerade hergeleitet haben, wollen wir im Folgenden etwas genauer – algebraischer – fassen um dann ein besseres Kriterium uns erarbeiten zu können. Dafür müssen wir uns nun aber ersteinmal mit den Grundlagen und Begriffen der Algebra beschäftigen, um dann ihre mächtigen Werkzeuge für unser Problem nutzen zu können.

Starten wir mit dem Begriff der *Gruppe*: Darunter wollen wir eine Menge G mit einer binären Verknüpfung $\circ$ auf ihr (d. h. man ordnet jedem Paar (a, b) von Elementen aus G eine Verknüpfung $a \circ b$ aus G zu) verstehen, wenn diese gewisse Eigenschaften erfüllt:

- Existenz eines neutralen Elements: $\exists e \in G : a \circ e = e \circ a = a,\ \forall a \in G$,
- Existenz des inversen Elements: $\forall a \in G\ \exists b \in G : a \circ b = b \circ a = e$ und
- Assoziativität: $\forall a, b, c \in G : a \circ (b \circ c) = (a \circ b) \circ c$.

Gilt zusätzlich die Kommutativität, d. h. $a \circ b = b \circ a, \forall a, b \in G$, so nennen wir $(G, \circ)$ auch kommutative Gruppe. Ist klar, welche Verknüpfung wir meinen, so sagen wir auch nur „G ist eine (kommutative) Gruppe“.

Als Beispiel seien die ganzen Zahlen mit ihrer Addition genannt. Informell gesprochen ist also eine Gruppe eine Menge mit einer Operation, die dort „gut“ funktioniert. Diese Verknüpfung muss aber nicht notwendigerweise irgendetwas mit den üblichen Verknüpfungen wie Addition zu tun haben. Dazu mache man sich z. B. klar, dass die Menge der bijektiven Funktionen

(d. h. eineindeutig und ganz $\mathbb{R}$ als Wertebereich) bezüglich der Verknüpfung des Hintereinanderausführens eine Gruppe bilden!

Eine Gruppe war eine Menge mit einer Verknüpfung, die gewisse Eigenschaften erfüllte. Was man nun machen kann, ist eine zweite Verknüpfung hinzunehmen. Verhält sich dort dann auch alles „ordentlich“, so erhalten wir einen Körper[2]:

Eine Menge K mit zwei binären Verknüpfungen $+$, $\cdot$ nennen wir *Körper*, wenn folgende Eigenschaften erfüllt sind:

- „gutes Verhalten“ bezügl. Addition: K ist mit $+$ eine kommutative Gruppe, wobei wir das additiv-neutrale Element 0 nennen wollen[3],
- „gutes Verhalten“ bezügl. Multiplikation: $K\backslash\{0\}$ ist mit $\cdot$ eine kommutative Gruppe und
- Distributivgesetz: $\forall a, b, c \in K : a \cdot (b + c) = a \cdot b + a \cdot c$.

Wenn wir genau schauen, dann sehen wir hier nicht nur zwei Verknüpfungen (Addition und Multiplikation), sondern aufgrund der Existenz der jeweiligen inversen Elemente auch ihre Umkehroperationen (Subtraktion und Division). Deswegen können wir informell auch sagen, dass ein Körper also eine Menge ist, in der alle vier Grundrechenarten „funktionieren“. Beispiele für Körper sind somit die rationalen Zahlen $\mathbb{Q}$, die reellen Zahlen $\mathbb{R}$ oder auch die komplexen Zahlen $\mathbb{C}$.

Wir sehen schon: Mit einem Körper können wir ganz gut den Umgang mit den Grundrechenarten beschreiben. Deshalb werden gewisse Teilmengen der komplexen Zahlen, die auch Körper darstellen, im weiteren Verlauf für uns eine große Rolle spielen.

Und schließlich benötigen wir noch eine dritte algebraische Struktur, die mehr ist als nur eine Gruppe, aber nicht notwendigerweise selbst ein Körper ist, nämlich die des Vektorraums:

Sei V eine Menge mit einer binären Verknüpfung $\circ$ und K ein Körper bezüglich $+, \cdot$. Dann nennen wir V einen *K-Vektorraum*, wenn folgende Eigenschaften erfüllt sind:

- additive Struktur von V: V ist bezügl. $\circ$ eine kommutative Gruppe,
- Existenz einer äußeren Multiplikation: Für jedes $v \in V$ und $a \in K$ ist $a \cdot v \in V$,

[2] Dieser Begriff hat nichts mit einer geometrischen Figur zu tun. Im Englischen heißt diese algebraische Struktur auch „field“, sodass man sich da nicht von falschen Assoziationen leiten lassen sollte.

[3] Man orientiert sich bei der Bezeichnung an den „normalen“ Operationen Addition und Multiplikation, sodass das neutrale Element bezügl. Mutliplikation auch 1 genannt wird; auch wenn diese Elemente nicht unbedingt die reellen Zahlen 0 und 1 sein müssen...

- neutrales Element: Für das neutrale Element 1 bezügl. der Multiplikation von K gilt: $1 \cdot v = v$,
- „Assoziativität“: $\forall a, b \in K, v \in V : a \cdot (b \cdot v) = (a \cdot b) \cdot v$ und
- Distributivitäten: $\forall a, b \in K, v, w \in V : (a + b) \cdot v = (a \cdot v) \circ (b \cdot v)$ und $a \cdot (v \circ w) = (a \cdot v) \circ (a \cdot w)$.

Im Folgenden werden wir der Einfachheit halber auch für die Addition der Vektoren $+$ schreiben, auch wenn es sich um eine andere Addition handelt als die im Körper K.

Ein K-Vektorraum V ist also - wieder informell gesprochen - eine Menge, in der eine Verknüpfung (z. B. die Addition) „gut funktioniert“, die aber sich auch gut mit einer Multiplikation „von außen“, durch Elemente aus K verträgt.

Wenn man sich die Definition noch einmal kurz anschaut, so stellt man fest, dass jeder Körper K offenbar ein Vektorraum über sich selbst ist. Auch wenn wir Tupel (z. B. Paare, Tripel, ...) von Elementen aus K bilden und dann „komponentenweise“ verknüpfen (also z. B. $(a, b)+(c, d) = (a+c, b+d)$ und $f \cdot (a, b) = (f \cdot a, f \cdot b)$), bildet auch diese Menge (wie im Beispiel $\mathbb{R}^2$ als Menge von Paaren reeller Zahlen) einen $(\mathbb{R})$-Vektorraum. So kann man sich dann auch diesen Vektorraum entsprechend veranschaulichen. Aber Vorsicht! Diese Darstellung klappt nur für diesen speziellen Vektorraum und ist keine gute Vorstellung für den allgemeinen Begriff. So bilden z. B. auch die Polynome mit reellen Koeffizienten und einem maximalen Grad n einen $\mathbb{R}$-Vektorraum. Und Polynome sich als „Pfeile“, oder ähnliches vorzustellen, ist nicht unbedingt verständnisfördernd...

Wir haben also nun die Strukturen „Gruppe“, „Körper“ und „Vektorraum“ definiert. Im weiteren Verlauf dieses Artikels werden wir uns hauptsächlich mit den Eigenschaften von Körpern beschäftigen. Dafür benötigen wir aber zuerst noch ein wenig an Grundwissen über Vektorräume:

Sei V ein K-Vektorraum. Das neutrale Element der Gruppenstruktur von V nennen wir „Nullvektor“ und bezeichnen ihn auch mit 0. Eine endliche Menge $\{v_1, v_2, \ldots, v_n\}$ von Vektoren aus V nennen wir *linear unabhängig*, wenn die Gleichung $0 = a_1 \cdot v_1 + a_2 \cdot v_2 + \cdots + a_n \cdot v_n$ mit $a_1, \ldots, a_n \in K$ nur für $a_1 = a_2 = \cdots = a_n = 0$ erfüllt ist. Gibt es noch mindestens noch eine andere Belegung der a_k's, sodass diese Summe (Linearkombination) den Nullvektor ergibt, nennen wir sie linear abhängig.

Ähnlich nennen wir eine solche endliche Menge von Vektoren *Erzeugendensystem von* V, wenn für jeden Vektor $v \in V$ eine Linearkombination der Vektoren dieser Menge existiert, die v ergibt, es also $a_1, \ldots, a_n \in K$ gibt, sodass $v = a_1 \cdot v_1 + a_2 \cdot v_2 + \cdots + a_n \cdot v_n$ gilt.

Ein linear unabhängiges Erzeugendensystem von V nennt man auch eine *Basis von* V. Beispielsweise wäre die Menge $\{(0;1),(1;0)\}$ eine Basis von $\mathbb{R}^2$ als $\mathbb{R}$-Vektorraum. Basen sind im Normalfall nicht eindeutig bestimmt, aber ein Satz der linearen Algebra liefert uns: Die Anzahl der Elemente einer Basis eines Vektorraums ist für jede solche Basis gleich. Diese Anzahl nennt man *Dimension* des Vektorraums. So hat $\mathbb{R}^2$ die Dimension 2 als $\mathbb{R}$-Vektorraum.

6 Körpererweiterungen

Gegeben sei ein Körper L. Eine Teilmenge K von L, die bezüglich der gleichen Verknüpfungen wieder ein Körper ist, nennen wir Teil- (oder Unter-) Körper von L. Umgekehrt nennen wir L einen *Erweiterungskörper* von K und schreiben L/K (sprich „L über K“).

Wenn wir uns noch einmal die Definition des Vektorraums anschauen, dann können wir nun L als K-Vektorraum auffassen: Wir „vergessen“ dabei etwas von der multiplikativen Struktur von L, wie man beliebige Elemente aus L miteinander multiplizieren kann, sondern merken uns nur, wie eine Multiplikation mit einem Element aus K funktioniert.

Für diesen Vektorraum von L über dem Körper K können wir nun die Dimension bestimmen. Diese bezeichnen wir als Grad der Körpererweiterung und schreiben $[L:K]$. Dabei ist diese Zahl also ein Maß dafür, um wie viel L größer ist als K. So ist z. B. $[\mathbb{C}:\mathbb{R}]=2$, aber $[\mathbb{R}:\mathbb{Q}]=\infty$.

Wir betrachten im Folgenden spezielle Körpererweiterungen. Greifen wir uns für einen Körper K eine Zahl α heraus, die nicht in K liegt, so können wir uns nach dem „kleinsten“ Körper L fragen, der sowohl alle Elemente aus K als auch α enthält. Dieser existiert, ist eindeutig bestimmt und wird mit $L=K(\alpha)$ (sprich: „K adjungiert α“) bezeichnet. Er zeichnet sich also dadurch aus, dass jeder Körper, der α und K enthält, diesen als Teilkörper besitzt. Anders herum kann man ihn aber auch als „Abschluss“ der Menge $\{1;\alpha\}$ unter Addition, Multiplikation, additiver Inversenbildung und multiplikativer Inversenbildung (für Elemente ungleich 0) definieren.

Dabei müssen natürlich aufgrund der Abgeschlossenheit der Multiplikation insbesondere alle Potenzen $\alpha^k, k\in\mathbb{Z}$ von α in L enthalten sein. Ist die Menge $\left\{\alpha^k \middle| 0\le k\le n\right\}$ für irgendein $n\in\mathbb{N}$ linear abhängig über K, so nennen wir α algebraisch über K. Wir wählen dabei das n, für welches diese Menge linear abhängig wird, minimal. Dann existieren also $a_k, 0\le k\le n$, nicht alle gleich 0 (und $a_n\neq 0$, da n minimal), sodass $0=a_0\cdot\alpha^0+\cdots+a_n\cdot\alpha^n$ gilt. Nach Division durch a_n und mit $b_k:=\frac{a_k}{a_n}$ sieht man, dass also α Nullstelle des Polynoms $m_\alpha(X):=X^n+b_{n-1}X^{n-1}+\cdots+b_0$ mit Koeffizienten $b_0,\ldots,b_{n-1}$ aus K ist.

Dieses Polynom mit Koeffizienten aus K ist nach Konstruktion eindeutig bestimmt. Des Weiteren ist es irreduzibel über K, d. h. durch kein nichtkonstantes Polynom kleineren Grades mit Koeffizienten aus K teilbar, denn wäre es dies, dann wäre α auch Nullstelle eines Polynoms kleineren Grades und damit n nicht minimal gewählt. Umgekehrt ist aber jedes Polynom mit Koeffizienten aus K, welches α als Nullstelle besitzt, durch $m_\alpha(X)$ teilbar. Deshalb nennt man dieses Polynom auch das Minimalpolynom von α (über K).

In jenem Fall der linearen Abhängigkeit bei minimal gewähltem n ist aber die Menge $\left\{ \alpha^k \middle| 0 \leq k < n \right\}$ schon eine Basis von $K(\alpha)$, da es auch ein Erzeugendensystem ist. Dazu müssen wir nur zeigen, dass mit zwei Elementen aus $K(\alpha)$, die als Linearkombination von Elementen aus der obigen Menge darstellbar sind, auch deren Summe, Produkt, das jeweils additive und auch multiplikative Inverse (wenn das zu invertierende Element ungleich 0 ist) jeweils solch eine Linearkombination ist. Die Summe und das additive Inverse sind klar; für das Produkt multipliziere man einfach die beiden Summen aus, stelle die höheren Potenzen von α durch eine Linearkombination aus den kleineren Potenzen dar und fasse wieder zusammen.

Einzig für die Darstellbarkeit des multiplikativen Inversen müssen wir uns kurz gedanken machen. Um das multiplikative Inverse zu dem Element $A := a_0 \cdot \alpha_0 + \ldots a_{n-1} \cdot \alpha^{n-1}$ mit $a_0, \ldots a_{n-1} \in K$, nicht alle gleich 0 zu bestimmen, multiplizieren wir dieses mit dem Element $U := u_0 \cdot \alpha_0 + \ldots u_{n-1} \cdot \alpha^{n-1}$ mit noch zu bestimmenden Koeffizienten u_0 bis u_{n-1}. Dabei erhalten wir (nach entsprechender Reduktion der α-Potenzen und Zusammenfassen den Wert des Produkts zu $t_0 \cdot \alpha_0 + \ldots t_{n-1} \cdot \alpha^{n-1}$, wobei die t_j linear von den u_0 bis u_{n-1} abhängen. Dieses Produkt soll nun genau Eins sein, d. h. es muss gelten $t_0 = 1$ und $t_j = 0$ für $1 \leq j \leq n-1$. Wir erhalten also ein lineares Gleichungssystem in n Variablen und n Gleichungen, welches in dem Fall, dass nicht gleichzeitig alle a_j verschwinden, eine eindeutige Lösung besitzt. Dann ist U das multiplikative Inverse zu A, sodass also die Menge der K-Linearkombinationen der Menge $M = \left\{ \alpha^k \middle| 0 \leq k < n \right\}$ abgeschlossen ist unter allen vier Grundrechenarten (wenn der Divisor verschieden ist von Null), sodass sie genau den Körper $K(\alpha)$ darstellt und M damit eine Basis dieses Körpers ist.

Insbesondere ist der Grad der Körpererweiterung $[K(\alpha) : K]$ im Fall, dass α algebraisch über K ist, genau der Grad des Minimalpolynoms m_α von α über K.

Beispiel: Wir wählen $K = \mathbb{Q}$ und $\alpha = \sqrt{2}$. Wie sieht nun $K(\alpha) = \mathbb{Q}\left(\sqrt{2}\right)$ aus?

Nun, das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$ ist offensichtlich $X^2 - 2$. Dieses hat Grad Zwei, d. h., die Menge $\{1; \sqrt{2}\}$ ist linear unabhängig über $\mathbb{Q}$.

Damit ist also $\mathbb{Q}\left(\sqrt{2}\right) = \left\{ a + b\sqrt{2} \middle| \, a, b \in \mathbb{Q} \right\}$. Und tatsächlich ist $\frac{1}{a+b\sqrt{2}} = \frac{a}{a^2-2b^2} - \sqrt{2}\frac{b}{a^2-2b^2}$ auch von dieser Form.
Betrachtet man nun wieder allgemein zwei Körpererweiterungen L/K und M/L, so ist natürlich auch K ein Teilkörper von M. So kann man nun die drei Körpererweiterungsgrade $[L : K]$, $[M : L]$ und $[M : K]$ miteinander in Beziehung bringen. Dies tut der

Satz 1 (Gradsatz:)**.** *Für die Grade der Körpererweiterungen L/K und M/L gilt:*

$$[L : K] \cdot [M : L] = [M : K] \, .$$

Beweis. Sei $[L : K] = n$ und $[M : L] = m$. Dann gibt es also eine Basis $\{l_1, l_2, \ldots, l_m\}$ von M als L-Vektorraum. Das heißt, jedes Element $x \in M$ kann eindeutig dargestellt werden als

$$x = a_1 \cdot l_1 + a_2 \cdot l_2 + \cdots + a_m \cdot l_m = \sum_{j=1}^{m} a_j \cdot l_j, \text{ mit } a_1, a_2, \ldots, a_m \in L \, .$$

Analog existiert auch eine Basis $\{k_1, k_2, \ldots, k_n\}$ von L als K-Vektorraum. Da die a_j Elemente von L sind, gibt es also für jedes solche $a_j, 1 \leq j \leq m$ eindeutig bestimmte Koeffizienten $b_{1,j}$ bis $b_{n,j}$ aus K, sodass $a_j = b_{1,j} \cdot k_1 + \cdots + b_{n,j} \cdot k_n = \sum_{h=1}^{n} b_{h,j} \cdot k_h$ ist.
Setzen wir dies ein, so erhalten wir, dass sich jedes x aus M eindeutig darstellen lässt als

$$x = \sum_{j=1}^{m} \sum_{h=1}^{m} b_{h,j} \cdot (k_h \cdot l_j) \, .$$

Damit bildet die Menge $\{k_h \cdot l_j | 1 \leq h \leq n, 1 \leq j \leq m\}$ eine Basis von M als K-Vektorraum (da die Koeffizienten $b_{h,j}$ ja alle aus K sind). Diese Basis enthält genau nm Elemente, sodass $[M : K] = nm = [M : L] \cdot [L : K]$ gilt. □

Bemerkung: Man kann sich diesen Satz also quasi als „Multiplikation zweier Brüche“ merken. Jedoch ist auch dies wieder nur eine informelle Sichtweise, denn es finden hier ja gar keine Divisionen statt! Insbesondere sagt dieser Satz aber auch aus, dass der Grad der Erweiterung eines Zwischenkörpers L über dem Grundkörper K immer ein Teiler des Erweiterungsgrads $[M : K]$ sein muss.

Und wozu dies nun alles? Nun, wenn wir zwei schon konstruierte komplexe Zahlen a und b aus einem Körper K nehmen und diese mit den Grundrechenarten miteinander verknüpfen, dann wird das Ergebnis aufgrund der

Definition des Körpers auf jeden Fall wieder in K liegen. Wenden wir jedoch einmalig die Operation des Quadrat-Wurzelziehens an, so liegt das Ergebnis nicht mehr notwendigerweise in K, wohl aber in einem Erweiterungs-Körper L mit $[L : K] = 2$, denn das Minimalpolynom dieses Ergebnisses ist ja offenbar vom Grad Zwei.

Umgekehrt lassen sich aber auch dann alle Elemente aus L konstruieren, wenn sich die aus K alle konstruieren lassen: Für ein beliebiges Element $\beta \in L$ ist ja $K(\beta)$ ein Zwischenkörper zur Erweiterung L/K, also muss der Grad der Erweiterung von $K(\beta)$ über K ein Teiler von $[L : K] = 2$ sein. Da dieser Grad aber gleich dem Minimalpolynom von β über K ist, ist dieses entweder linear oder quadratisch. Da aber mit unseren Konstruktionsmitteln sowohl jede lineare als auch quadratische Gleichung gelöst werden kann, ist damit auch β, und damit jedes Element aus L, konstruierbar, wenn jedes Element aus K konstruierbar ist.

Zusammen genommen ergibt sich also folgender

Satz 2. *Es lassen sich genau diejenigen komplexen Zahlen mit Zirkel und unmakiertem Lineal konstruieren, die in einem Erweiterungskörper L von $\mathbb{Q}$ mit $[L : \mathbb{Q}] = 2^n$ für ein $n \in \mathbb{N}$ liegen.*

Beweis. Wir zeigen zuerst, dass sich all diese Zahlen konstruieren lassen, und zeigen dann, dass keine weiteren konstruierbar sind. Dazu gehen wir induktiv vor: Für $n = 0$ ergeben sich nur die rationalen Zahlen, von denen wir schon gezeigt haben, dass sie konstruierbar sind. Seien also nun alle Zahlen eines Körpers K (mit $[K : \mathbb{Q}] = 2^k$) konstruierbar und L ein Erweiterungskörper von K mit $[L : K] = 2$. Nach der Bemerkung von eben sind dann auch alle Elemente von L konstruierbar, und nach dem Gradsatz ist $[L : \mathbb{Q}] = 2^{k+1}$.

Umgekehrt ist offenbar jede konstruierbare Zahl Element eines solchen Körpers, denn in jedem Konstruktionsschritt wird entweder eine lineare oder quadratische Gleichung mit Koeffizienten aus bisher schon konstruierten Zahlen gelöst, d. h., entweder man bleibt in dem Körper oder geht zu einem Erweiterungskörper vom Grad Zwei (also nach dem Gradsatz einer Zweierpotenz über $\mathbb{Q}$) über, in welchem man sich dann befindet. □

7 Einheitswurzeln

Wir haben nun ein sehr gutes Kriterium dafür hergeleitet, wann eine komplexe Zahl konstruierbar ist. Dies ist nämlich genau dann der Fall, wenn sie algebraisch ist und ihr Minimalpolynom über $\mathbb{Q}$ den Grad einer Zweierpotenz hat. Nun wollen wir dieses so gewonnene Wissen nutzen, um unsere Probleme (zuerst unser n-Eck-Problem) zu lösen.

Um ein regelmäßiges n-Eck bestimmter Seitenlänge zu konstruieren, muss man zwei Dinge bewerkstelligen: Man muss die vorgegebene Seitenlänge und die notwendigen Winkel konstruieren können. Da wir aber konstruierte Figuren zentrisch um einen konstruierbaren Faktor strecken können (dies überlegt man sich schnell), genügt uns also für festes n die Konstruktion eines bestimmten n-Ecks um daraus durch zentrische Streckung alle entsprechend konstruierbaren n-Ecke beliebiger, konstruierbarer Größe zu erhalten.

Regelmäßige n-Ecke haben die Eigenschaft, dass sie einen Umkreis besitzen, und dass die Strecken Eckpunkt-Umkreismittelpunkt den Vollwinkel am Umkreismittelpunkt in n gleich große Winkel der Größe $\frac{2\pi}{n}$ zu zerlegen. Deshalb ist es ausreichend einen solchen Winkel zu konstruieren bzw. die Werte $\sin\frac{2\pi}{n}$ und $\cos\frac{2\pi}{n}$, oder aber $\zeta_n := \cos\frac{2\pi}{n} + i \cdot \sin\frac{2\pi}{n}$. Umgekehrt überlegt man sich aber auch recht schnell, dass man mit ζ_n ein regelmäßiges n-Eck konstruieren kann. Die Aufgaben sind also äquivalent.

Was können wir nun über ζ_n aussagen? Mit der Multiplikationsformel für komplexe Zahlen in ihrer Polarkoordinatendarstellung erkennen wir, dass $\zeta_n^n = 1$ ist, und auch, dass n der kleinste positive Exponent ist, für den dies gilt. Also sind insbesondere die Werte ζ_n^k mit $1 \leq k \leq n$ alle paarweise verschieden, und wegen $\left(\zeta_n^k\right)^n = \left(\zeta_n^n\right)^k = 1$ allesamt Nullstellen des Polynoms $X^n - 1$ bzw. Lösungen der Gleichung $X^n = 1$. Aus diesem Grund nennt man sie auch die n-ten Einheitswurzeln. Da dies n verschiedene Werte sind und ein Polynom n-ten Grades im Bereich der komplexen Zahlen genau so viele Nullstellen besitzt (Vielfachheiten entsprechend gezählt), sind die ζ_n^k also genau die n-ten Einheitswurzeln, d. h., es gilt $X^n - 1 = (X - \zeta_n^1) \ldots (X - \zeta_n^n)$.

Für jeden Teiler d von n ist aber natürlich ζ_n^d (und Potenzen davon) nicht nur eine n-te Einheitswurzel, sondern auch eine $\frac{n}{d}$-te Einheitswurzel. Diejenigen Einheitswurzeln, welche nur n-te Einheitswurzeln (aber nicht auch gleichzeitig welche von niedrigerer Ordnung) sind, nennen wir primitive Einheitswurzeln. Dies sind also dann offenbar genau diejenigen Potenzen von ζ_n, welche einen Exponenten besitzen, der teilerfremd zu n ist.

Wir wollen nun im Folgenden das Polynom betrachten, welches genau das Produkt $(X - \zeta)$ ist, wobei ζ über alle primitiven n-ten Einheitswurzeln läuft. Dieses Polynom wollen wir mit $\Phi_n(X)$ bezeichnen. Da dessen Grad gerade die Anzahl der zu n teilerfremden natürlichen Zahlen zwischen 1 und n ist und jene Anzahl als Eulersche φ-Funktion bekannt ist, gilt also $\operatorname{grad}(\Phi_n(X)) = \varphi(n)$.

Als nächstes stellen wir mit den Gedanken von eben fest, dass jede n-te Einheitswurzel für genau einen Teiler d von n eine primitive d-te Einheitswurzel ist, und umgekehrt jede primitive d-te Einheitswurzel eine n-te Einheitswur-

zel ist. Also ist $X^n - 1 = \prod_{d|n} \Phi_d(X)$ bzw.

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{d|n, d\neq n} \Phi_d(X)}, n > 1.$$

Dies liefert uns eine Möglichkeit die $\Phi_n(X)$ rekursiv zu berechnen, mit dem Startwert $\Phi_1(X) = X - 1$. Induktiv zeigt man mit dieser Berechnungsvorschrift, dass die $\Phi_n(X)$ jeweils normierte Polynome mit rationalen Koeffizienten sind. Beim zweiten Hinschauen stellt man dann sogar noch fest, dass bei der Polynomdivision aufgrund der Normierung auch keine Nenner auftreten können, sodass sogar alle Koeffizienten von $\Phi_n(X)$ ganzzahlig sind!

Da $\Phi_n(X)$ nur Koeffizienten aus dem Grundkörper ($\mathbb{Q}$) besitzt, normiert ist und nach Konstruktion ζ_n als Nullstelle besitzt, bleibt nur noch zu zeigen, dass es irreduzibel (über dem Grundkörper) ist, damit wir es als Minimalpolynom von ζ_n bestätigen können.

Sei also $m_{\zeta_n}(X)$ das Minimalpolynom von ζ_n über $\mathbb{Q}$. Dann ist nach obiger Bemerkung also $\Phi_n(X)$ und damit auch $X^n - 1$ durch $m_{\zeta_n}(X)$ teilbar. Es genügt offenbar zu zeigen, dass für jedes zu n teilerfremde k auch ζ_n^k Nullstelle von $m_{\zeta_n}(X)$ ist, denn dann wäre dessen Grad mindestens so groß wie die Anzahl der verschiedenen Nullstellen, also $\varphi(n)$, und damit wäre $m_{\zeta_n}(X) = \Phi_n(X)$. Und dafür genügt es wiederum zu zeigen, dass für eine primitive n-te Einheitswurzel ζ und eine zu n teilerfremde Primzahl p stets aus $m_{\zeta_n}(\zeta) = 0$ auch $m_{\zeta_n}(\zeta^p) = 0$ folgt, denn mit ζ ist auch ζ^p eine primitive n-te Einheitswurzel, und durch sukzessive Multiplikation des Exponenten mit zu n teilerfremden Primzahlen kann man jedes ζ_n^m mit $\operatorname{ggt}(n, m) = 1$ darstellen.

Nehmen wir also an, dies wäre nicht der Fall. Also existiert erst einmal ein nicht-konstantes Polynom $g(X)$ mit rationalen Koeffizienten, sodass $\Phi_n(X) = m_{\zeta_n}(X) \cdot g(X)$ ist. Nach dem Lemma von Gauß[4] können wir ohne Beschränkung der Allgemeinheit annehmen, dass die Koeffizienten der beiden Polynome im Produkt auf der rechten Seite der Gleichung ganzzahlig sind. Nach Annahme ist ζ nun Nullstelle von $m_{\zeta_n}(X)$, aber nicht ζ^p. Da dies aber eine primitive n-te Einheitswurzel und damit Nullstelle von $\Phi_n(X)$ ist, muss es also eine Nullstelle von $g(X)$ sein. Damit ist gleichzeitig also ζ eine Nullstelle des Polynoms $g(X^p)$, sodass sich auch $g(X^p) = m_{\zeta_n}(X) \cdot h(X)$ mit einem Polynom $h(X)$ mit ganzzahligen Koeffizienten schreiben lässt.

Betrachten wir diese Gleichung nun modulo p (d. h. reduzieren alle auftretenden Koeffizienten der Polynome modulo p, betrachten also nur ihre

[4] Dieses Lemma besagt, dass ein Polynom mit ganzzahligen Koeffizienten genau dann irreduzibel über $\mathbb{Q}$ ist, wenn es dies auch schon über $\mathbb{Z}$ ist, sich also nicht als Produkt zweier Polynome niedrigeren Grades mit nur ganzzahligen Koeffizienten darstellen lässt.

Reste bei der Division mit Rest durch p), so erhält man $g(X^p) \equiv g(X)^p \pmod{p}$, da die beim Ausmultiplizieren der Summe auftretenden Binomialkoeffizienten $\binom{p}{k}$ für alle $0 < k < p$ durch p teilbar sind (und so bei einer Betrachtung modulo p) verschwinden, und nur die „Randterme“ übrig bleiben. Also gilt $g(X)^p \equiv m_{\zeta_n}(X) \cdot h(X) \pmod{p}$. Also ist modulo p das Poylnom $g(X)^p$ durch das Polynom $m_{\zeta_n}(X)$ teilbar, d. h. insbesondere, dass es aufgrund der eindeutigen Zerlegung von Polynomen in irreduzible Faktoren ein nicht-konstantes Polynom $k(X)$ mit ganzzahligen Koeffizenten geben muss, sodass es Polynome $l_1(X)$ und $l_2(X)$ mit ganzzahligen Koeffizenten gibt, die $g(X) \equiv k(X) \cdot l_1(X) \pmod{p}$ und $m_{\zeta_n}(X) \equiv k(X) \cdot l_2(X) \pmod{p}$ erfüllen.

Wie wir bei der Definition von $\Phi_n(X)$ durch die Rekursionsformel schon gesehen haben, gilt die Gleichheit $X^n - 1 = \Phi_n(X) \cdot o(X)$, wobei $o(X)$ als Produkt von Polynomen $\Phi_d(X)\ , d|n\ , d < n$ mit ganzzahligen Koeffizienten wiederum ein solches Polynom ist. Setzen wir die vorhergehenden Erkenntnisse ein, so erhalten wir damit:

$$\begin{aligned} X^n - 1 &= \Phi_n(X) \cdot o(X) = m_{\zeta_n}(X) \cdot g(X) \cdot o(X) \\ &\equiv k(X) \cdot l_2(X) \cdot k(X) \cdot l_1(X) \cdot o(X) = (k(X))^2 \cdot r(X) \pmod{p}\ . \end{aligned}$$

Insbesondere besitzt also $X^n - 1$ mehrfache Nullstellen modulo p, was aber nicht sein kann, da $(X^n - 1)' = n \cdot x^{n-1} \not\equiv 0 \pmod{p}$ wegen der Teilerfremdheit von n und p nur für $X = 0$ verschwindet, was aber keine Nullstelle von $X^n - 1$ ist. Also hat dieses Polynom keine mehrfachen Nullstellen, was den gewünschten Widerspruch liefert. Damit ist $\Phi_n(X)$ irreduzibel und somit auch das Minimalpolynom von ζ_n. □

8 Eulersche φ-Funktion und Fermat-Primzahlen

Wie wir eben gesehen haben, ist dieses Minimalpolynom $\Phi_n(X)$ der Zahl ζ_n über $\mathbb{Q}$, die es zu konstruieren gilt um ein regelmäßiges n-Eck zu konstruieren, genau vom Grad $\varphi(n)$. Damit hat auch die Körpererweiterung $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ den Grad $\varphi(n)$ und damit ist auch der Grad jeder Körpererweiterung der rationalen Zahlen, die ζ_n enthält, durch $\varphi(n)$ teilbar. Da aber genau die Punkte bzw. Zahlen konstruierbar sind, die in Körpererweiterungen mit Grad einer Zweierpotenz über den rationalen Zahlen liegen, sind also genau diejenigen n-Ecke konstruierbar, für die $\varphi(n)$ ein Teiler einer Zweierpotenz, d. h. selbst eine Zweierpotenz ist!

Wir haben also unser geometrisches Problem mithilfe eines nicht unbedingt kleinen, aber dafür mächtigen algebraischen Apparats auf ein simples zah-

lentheoretisches Problem zurückgeführt! Im Folgenden müssen wir also nun nur noch die Eigenschaften der Eulerschen φ-Funktion studieren.

Wie können wir nun für eine konkrete natürliche Zahl n den Wert $\varphi(n)$ berechnen? Dazu stellen wir nun gewisse Rechenregeln auf:

Sei p eine Primzahl. Da damit 1 und p die einzigen Teiler von p sind, sind also alle natürlichen Zahlen von 1 bis $p-1$ teilerfremd zu p (da sie ja nicht durch p teilbar sind). Also ist $\varphi(p)$, die Anzahl der zu p teilerfremden Zahlen zwischen inklusive 1 und p, genau gleich $p-1$.

Analog können wir nun auch die φ-Funktion an einer Primzahlpotenz p^k auswerten: Da alle Teiler größer als 1 von p^k durch p teilbar sind, ist eine Zahl genau dann nicht teilerfremd zu p^k, wenn sie durch p teilbar ist. Davon gibt es im Bereich von 1 bis p^k genau p^{k-1} Stück. Ergo ist $\varphi\left(p^k\right) = p^k - p^{k-1} = (p-1) \cdot p^{k-1}$.

Haben wir nun zwei teilerfremde natürliche Zahlen n und m (z. B. Primzahlpotenzen zu verschiedenen Primzahlen), von denen wir schon die Funktionswerte der φ-Funktion kennen, so können wir daraus auch den Funktionswert $\varphi(nm)$ berechnen. Dazu überlegen wir uns, dass eine Zahl genau dann teilerfremd zu dem Produkt nm ist, wenn es teilerfremd zu beiden Faktoren ist. Des Weiteren ist eine Zahl teilerfremd zu n (analog zu m), wenn es bei der Division mit Rest durch n (bzw. m) auch der Rest ist. Es sind also genau diejenigen natürlichen Zahlen im Bereich von 1 bis nm teilerfremd zu nm, deren Reste bei der Division mit Rest durch n teilerfremd zu n und deren Reste bei der Division mit Rest durch m teilerfremd zu m sind.

Da jeder Zahl zwischen 1 und nm genau ein Paar von solchen Resten zugeordnet werden kann, und umgekehrt jedem Paar solcher Reste eine Zahl zwischen 1 und nm, genügt es uns also die Anzahl solcher Paare von Resten zu bestimmen, deren erste Komponente teilerfremd zu n und zweite teilerfremd zu m ist. In der ersten Komponente kann man $\varphi(n)$ mögliche Wahlen von zu n teilerfremden Resten treffen, in der zweiten analog $\varphi(m)$. Da die beiden Auswahlprozesse, welcher dieser zu n bzw. m teilerfremden Reste in den beiden Komponenten stehen können, unabhängig voneinander sind, liefert uns dies also insgesamt $\varphi(n) \cdot \varphi(m)$ solche Paare, also genau so viele wie zu nm teilerfremde natürliche Zahlen zwischen 1 und nm. Damit ist also $\varphi(nm) = \varphi(n)\varphi(m)$, für teilerfremde n, m. (Der geneigte Leser möge für sich die Frage stellen und beantworten, wo diese Überlegung für nicht-teilerfremde n, m versagt.)

Fassen wir die beiden letzten Ergebnisse zusammen, so können wir aus der Primfaktorzerlegung einer natürlichen Zahl n sehr leicht den Wert $\varphi(n)$ berechnen: Ist nämlich $n = p_1^{a_1} \dots p_k^{a_k}$ mit Primzahlen $p_1, \dots, p_k$ und positiven

ganzen Zahlen $a_1, \ldots, a_k, k$, so ist

$$\begin{aligned}\varphi(n) &= \varphi\left(p_1^{a_1} \cdots p_k^{a_k}\right) = \varphi\left(p_1^{a_1}\right) \cdots \varphi\left(p_k^{a_k}\right) \\ &= (p_1 - 1) \cdots (p_k - 1) \cdot p_1^{a_1 - 1} \cdots p_k^{a_k - 1} \ .\end{aligned}$$

Was bedeutet dies nun für unser Problem? Wir hatten festgestellt, dass genau diejenigen n-Ecke sich konstruieren lassen, für welche $\varphi(n)$ eine Zweierpotenz ist. Wir sehen nun, dass für jeden ungeraden Primfaktor p von n, der mit einer Vielfachheit größer als 1 in der Primfaktorzerlegung von n auftritt, der Wert $\varphi(n)$ trotzdem noch durch p teilbar ist. Also dürfen ungerade Primfaktoren nur in der ersten Potenz in der Primfaktorzerlegung von n erscheinen. Des Weiteren ist dann aber auch noch $\varphi(n)$ durch $p-1$ teilbar. Da $\varphi(n)$ aber eine Zweierpotenz sein muss, und diese nur Zweierpotenzen als Teiler besitzen, muss also $p - 1$ auch eine Zweierpotenz sein, d. h., p muss die Form $2^k + 1$ besitzen!

Nun kommen aber für dieses k nicht alle natürlichen Zahlen infrage. Kann man nämlich dieses k zerlegen in $k = 2^m \cdot u$ mit einer ungeraden, natürlichen Zahl u und einer natürlichen Zahl m, so ist $2^k + 1 = \left(2^{2^m}\right)^u + 1^u$ durch $2^{2^m} + 1$ teilbar. Für $u > 1$ ist dies aber ein nicht-trivialer Teiler von $2^k + 1$, sodass dies keine Primzahl sein kann. Also muss k selbst eine reine Zweier-Potenz sein, und damit $p = 2^{2^m} + 1$ für eine nicht-negative ganze Zahl m gelten. Primzahlen dieser Form nennt man auch Fermat-Primzahlen. Pierre de Fermat vermutete, dass alle Zahlen dieser Form prim seien, da er dies für $m = 0$ bis 4 bestätigen konnte. Doch Euler konnte nachweisen, dass diese Aussage schon für $m =$ falsch ist. Bis heute weiß man, dass alle weiteren Zahlen dieser Form bis $m = 32$ zusammengesetzt sind. Es ist bisher keine weitere Primzahl jener Form bekannt, und es wird angenommen, dass es keine weiteren gibt. Bewiesen jedoch ist dies nicht.

Wir haben also bisher festgestellt, dass die ungeraden Primfaktoren von n nur Fermat-Primzahlen sein dürfen, und dass diese auch jeweils nur in der ersten Potenz in der Primfaktorzerlegung von n erscheinen dürfen. Umgekehrt stellt man aber auch fest, dass für alle Zahlen n, die diese Voraussetzungen erfüllen, der Wert $\varphi(n)$ eine reine Zweierpotenz ist. Damit gelangen wir zu unserem

Satz 3. *Es lassen sich genau diejenigen n-Ecke mithilfe von Zirkel und Lineal konstruieren, für die n ein Produkt einer Zweierpotenz mit paarweise verschiedenen Fermat-Primzahlen ist.*

9 Randbemerkungen, die anderen Probleme

Diesen Satz bewies zuerst der 17-jährige Gauß in seiner Arbeit „Disquisitiones Arithmeticae“ (veröff. 1801). Dabei hatte er jedoch nicht diese Hilfsmittel der Algebra zur Verfügung, weil hier erst die Begriffsbildung begann.

Nun haben wir also unser Problem, welche regelmäßigen n-Ecke konstruierbar sind, weitestgehend erschöpfend beantwortet (einzig und allein die Frage, ob es noch weitere außer den fünf bekannten Fermat-Primzahlen gibt, ist noch unbeantwortet). Doch was ist mit den übrigen, den originalen Problemen?

Das Problem der Winkeldrittelung können wir leicht negativ beantworten: Da wir kein regelmäßiges Neuneck konstruieren können, ist also insbesondere auch nicht ein Winkel von $\frac{2\pi}{9} = \frac{1}{3} \cdot \frac{2\pi}{3}$ konstruierbar. Da man aber einen Winkel von $\frac{2\pi}{3}$ als „Zentri"-Winkel eines regelmäßigen Dreiecks konstruieren kann, ist jener Winkel also nicht konstruktiv zu dritteln.

Ähnlich ist auch die Würfelverdopplung nicht konstruktiv möglich: Hier müsste man die komplexe Zahl $\sqrt[3]{2}$ konstruieren, welche offenbar das Minimalpolynom $X^3 - 2$ besitzt, sodass jede endliche Körpererweiterung von $\mathbb{Q}$, die $\sqrt[3]{2}$ enthält, einen durch Drei teilbaren Erweiterungsgrad hat. Also ist jene Zahl nicht mit Zirkel und Lineal konstruierbar.

Abschließend noch das Problem der Quadratur des Kreises: Dieses läuft auf die Frage der Konstruierbarkeit der komplexen Zahl $\sqrt{\pi}$ hinaus. Lindemann bewies 1882, dass π nicht algebraisch, d. h. transzendent über $\mathbb{Q}$ ist, es also kein Polynom mit rationalen Koeffizienten gibt, von welchem π eine Nullstelle ist. Damit besitzt die Körpererweiterung $\mathbb{Q}(\pi)/\mathbb{Q}$ einen unendlichen Erweiterungsgrad (weil die Menge $\left\{ \pi^k \middle| k \in \mathbb{Z} \right\}$ linear unabhängig ist). Also ist π nicht konstruierbar, und damit auch nicht $\sqrt{\pi}$. Damit ist auch hier die Antwort negativ: Zu einem vorgegebenem Kreis lässt sich kein flächengleiches Quadrat konstruieren.

10 Ausblick

Unser Zugang zur Beantwortung der gestellten geometrischen Fragen war ein sehr algebraischer. Diese Theorie, welche sich mit den Eigenschaften von Körpererweiterungen beschäftigt, wird zu Ehren des französischen Mathematikers Evariste Galois auch Galois-Theorie genannt. Sie wurde allerdings entwickelt, um eine ganz andere Fragestellung zu bearbeiten, nämlich wann eine polynomielle Gleichung auflösbar ist.

Dabei meint „auflösbar" für eine Gleichung, dass sich jede ihrer Lösungen durch Anwenden einer endlichen Anzahl von Operationen der Grundrechenarten und des n-ten Wurzelziehens (also nicht nur Quadratwurzeln, wie bei der Fragestellung der Konstruierbarkeit) aus den rationalen Zahlen darstellen lässt. Man nennt diejenigen Zahlen, welche so darstellbar sind, Radikale.

Eine polynomielle Gleichung auf Lösungen zu untersuchen ist äquivalent dazu entsprechende Polynome auf Nullstellen zu untersuchen (indem man die Gleichung in der Form $p(X) = 0$ schreibt). Dabei kann man nun jeder

solchen Gleichung eine Körpererweiterung über den rationalen Zahlen zuordnen, nämlich den kleinsten Körper, der sowohl die rationalen Zahlen als auch alle Nullstellen des Polynoms enthält. Diesen Körper nennt man dann auch Zerfällungskörper des Polynoms (weil dies der kleinste Körper ist, in dem das Polynom vollständig in Linearfaktoren zerfällt).

Des Weiteren betrachtet man auf einer Körpererweiterung L/K nun gewisse Abbildungen, die man K-Automorphismen nennt. Eine Abb. $\psi : L \to L$ nennt man K-Automorphismus, wenn sie folgende Bedingungen erfüllt:

- Verträglichkeit mit der Addition auf L: $\forall a, b \in L : \psi(a+b) = \psi(a)+\psi(b)$,
- Verträglichkeit mit der Multiplikation auf L: $\forall a, b \in L : \psi(ab) = \psi(a)\psi(b)$,
- Bijektivität auf L: $\forall a, b \in L : (\psi(a) = \psi(b) \Rightarrow a = b)$ und $\forall b \in L$ $\exists a \in L : \varphi(a) = b$ sowie
- Konstanz auf K: $\forall a \in K : \psi(a) = a$.

Diese K-Automorphismen bilden bezüglich Hintereinanderausführung für eine feste Körpererweiterung L/K eine Gruppe, welche man bei noch einer gegebenen Zusatzvoraussetzung auch Galois-Gruppe nennt. So kann man also jedem Polynom eine Körpererweiterung und jeder Körpererweiterung eine Gruppe zuordnen, insgesamt also jedem Polynom eine bestimmte Gruppe, die etwas über das Verhalten der Nullstellen jenes Polynoms aussagt.

Dabei überträgt sich die Eigenschaft „die entsprechende Polynomialgleichung ist auflösbar“ auf die Gruppe zu „die entsprechende Galois-Gruppe dieses Polynoms ist auflösbar“, wobei „auflösbar“ hier nun eine gruppentheoretische Bedeutung besitzt. Was diese beinhaltet, möchten wir hier jetzt nicht genauer darstellen, jedoch kann man für spezielle Gruppen zeigen, dass sie nicht auflösbar sind, und damit auch nicht die ihnen „zugrunde liegenden“ Polynomialgleichungen. Damit kann man beweisen, dass es keine allgemeinen Lösungsformeln in Radikalen für polynomielle Gleichungen vom Grad fünf, oder höher geben kann. Jedoch kann man trotzdem für jedes gegebene konkrete Polynom nachrechnen, ob sich dessen Lösungen entsprechend angeben lassen, oder nicht. Das Ergebnis ist, dass „die meisten“ polynomiellen Gleichungen vom Grad fünf oder höher, sich nicht entsprechend auflösen lassen!

Wir haben also nun gesehen, dass die Mittel der Algebra, die wir hier genutzt haben, auch fähig und nützlich sind Problemstellungen ganz anderer Themengebiete der Mathematik mit zu beantworten helfen. Umgekehrt gibt es entsprechende Verzweigungen, in denen andere Teilgebiete der Mathematik sich jeweils befruchten, sodass man nach Meinung des Autors dieses Artikels die Mathematik immer als ein Ganzes in ihrer Schönheit begreifen sollte.