Konstruktionen mit Zirkel und Lineal

Mathematik am Samstag, 23. März 2013

Lukas-Fabian Moser

Einführung

Bereits in der Antike wurden intensiv die Möglichkeiten der Lösung geometrischer Probleme nur mit Zirkel und Lineal studiert, und die entsprechenden Begriffe und Resultate (das Fällen von Loten, Winkelhalbierung, Thaleskreis usw.) sind bis heute fester Teil des mathematischen Schulstoffes. Einige Probleme konnten jedoch weder in der Antike noch später gelöst werden; die berühmtesten sind:

- Das *Problem der Würfelverdoppelung*: Konstruiere die Seitenlängen zweier Würfel, deren Volumina sich verhalten wie zwei zu eins.

  (Angeblich wurde diese Aufgabe den Bewohnern der Insel Delos vom Delphischen Orakel gestellt, als diese um Rat zur Bekämpfung einer Pestepidemie fragten; man nennt es daher auch das *Delische Problem*.)

- Die Konstruktion eines regelmäßiges n-Ecks für vorgegebenes $n \geqslant 3$.

  (Die Fälle $n = 3, 4, 5$ sind klassisch und bis auf $n = 5$ auch heute Schulstoff. Durch Winkelhalbierung ist es außerdem stets möglich, aus einem n-Eck ein $2n$-Eck zu machen, so daß man sich auf *ungerades* n beschränken kann. Mit elementaren Argumenten kann man noch weiter reduzieren auf den Fall, daß n eine Primzahlpotenz ist.)

- Die Drittelung eines beliebigen Winkels.

  (Ist sie möglich, so kann man aus einem n-Eck auch ein $3n$-Eck konstruieren; insbesondere ist dann beispielsweise das regelmäßige Neuneck konstruierbar.)

- Die *Quadratur des Kreises*, also die Kontruktion eines Quadrates und eines Kreises mit gleichem Flächeninhalt.

Erst im 19. Jahrhundert konnte man beweisen, daß alle diese Probleme (in ihrer allgemeinsten Form) nicht lösbar sind. Dies kann natürlich nur gelingen, wenn man sich von der Untersuchung spezifischer Konstruktionsvorgänge verabschiedet und vielmehr die prinzipiellen Möglichkeiten und Begrenzungen dieses Werkzeuges untersucht. Wie das möglich ist, soll im folgenden erklärt werden.

1 Formalisierung

Die „Spielregeln“ sind folgendermaßen festgelegt: Das Lineal darf nur zum Zeichnen der Geraden durch zwei schon bekannte Punkte verwendet werden, der Zirkel nur zum Zeichnen des Kreises um einen schon bekannten Mittelpunkt, dessen Radius gleich dem Abstand zweier ebenfalls schon bekannter Punkte ist. Ein Punkt gilt dabei als bekannt, wenn er seinerseits Schnittpunkt von schon konstruierten Kreisen bzw. Geraden ist. Indem wir unser Augenmerk weg von den Kreisen und Geraden und hin zu den Punkten richten, kann man die Spielregeln folgendermaßen zusammenfassen: Eine Konstruktion mit Zirkel und Lineal ist ein Vorgang, mit dem in jedem Schritt neue Punkte gewonnen werden, und zwar als Schnittpunkte von Kreisen bzw. Geraden, die durch schon früher konstruierte Punkte gegeben sind. Wie kann man das nun formalisieren?

Wir bezeichnen mit E die Zeichenebene. Für $x_1 \neq x_2 \in E$ bezeichnen wir mit $L(x_1, x_2) \subset E$ die Gerade, die durch x_1 und x_2 verläuft. Sind $u, x_1, x_2 \in E$, so bezeichnet $K(u; x_1, x_2) \subset E$ den Kreis mit Mittelpunkt u, dessen Radius durch den Abstand der Punkte x_1 und x_2 gegeben ist.[1]

Definition. Es sei $T \subset E$ eine Punktmenge in der Ebene. Ein Punkt $a \in E$ heißt *aus T direkt konstruierbar*, wenn $a \in T$ gilt *(„Was schon konstruiert ist, ist konstruierbar!“)*, oder wenn eine der folgenden Bedingungen erfüllt ist:

i) Es gibt $t_1, t_2, s_1, s_2 \in T$ mit $t_1 \neq t_2$ und $s_1 \neq s_2$, so daß $L(t_1, t_2) \neq L(s_1, s_2)$ gilt und a in beiden enthalten ist.

ii) Es gibt $t_1, t_2, s_1, s_2, u \in T$ mit $s_1 \neq s_2$, so daß a sowohl in $C(u; t_1, t_2)$ als auch in $L(s_1, s_2)$ enthalten ist.

iii) Es gibt $t_1, t_2, s_1, s_2, u, v \in T$, so daß $C(u; t_1, t_2) \neq C(v; s_1, s_2)$ gilt und a in beiden enthalten ist.

Die Menge der direkt aus T konstruierbaren Punkte bezeichnen wir mit $\mathscr{K}^1(T)$.

[1] Die Bedingung $x_1 \neq x_2$ kann man zusätzlich verlangen, aber das ändert nichts an dem erhaltenen Konstruierbarkeitsbegriff. – Man kann sich auch auf den Fall $u = x_1$ beschränken, also verbieten, den Zirkel erst einzustellen und dann neu einzustechen. Es stellt sich aber heraus, daß diese Einschränkung der Möglichkeiten nur die Zahl der nötigen Konstruktionsschritte erhöht; darum verzichten wir auf sie.

Nach Definition gilt $T \subset \mathscr{K}^1(T)$. Wir schreiben $\mathscr{K}^2(T) := \mathscr{K}^1(\mathscr{K}^1(T))$ für die in zwei Schritten aus T konstruierbaren Punkte und allgemein rekursiv $\mathscr{K}^n(T) := \mathscr{K}^1(\mathscr{K}^{n-1}(T))$. Dann haben wir eine aufsteigende Kette von Teilmengen

$$T =: \mathscr{K}^0(T) \subset \mathscr{K}^1(T) \subset \mathscr{K}^2(T) \subset \dots .$$

Definition. Die Menge $\mathscr{K}(T) := \bigcup_{n \geqslant 0} \mathscr{K}^n(T)$ nennen wir die Menge der *aus T konstruierbaren* Punkte.

Jede Konstruktion muß mit irgendwelchen gegebenen Punkten beginnen: Es ist schnell zu sehen, daß $\mathscr{K}(\emptyset) = \emptyset$ ist, und außerdem, daß aus $|T| = 1$ folgt $\mathscr{K}^1(T) = T$, also induktiv $\mathscr{K}^n(T) = T$ und damit $\mathscr{K}(T) = T$. Man kann also nur dann wirklich zu konstruieren beginnen, wenn man mindestens zwei Startpunkte gegeben hat (und dann ergibt sich tatsächlich eine ganze Welt konstruierbarer Punkte, denn man kann schnell zeigen, daß aus $|T| \geqslant 2$ folgt $|\mathscr{K}(T)| = \infty$).

2 Algebraisierung: Die komplexen Zahlen

Um nun zu entscheiden, welche Konstruktionsaufgaben mit Zirkel und Lineal lösbar sind (und wenn ja, wie?), müssen wir die Struktur der Menge $\mathscr{K}(T)$ für eine gegebene Startmenge T untersuchen. Dies gelingt mit algebraischen Methoden, wobei der Weg zur Verknüpfung mit der Algebra darin besteht, auf der Zeichenebene E algebraische Operationen zu definieren.

Stellen wir uns also E von nun an als die Ebene $E = \mathbb{R}^2$ vor. Dann haben wir nicht nur einen ausgezeichneten Ursprungspunkt $(0, 0)$, sondern können auch Punkte mit Vektoren identifizieren und sie folglich addieren und vervielfachen. Leistungsfähig wird diese Theorie durch eine weitere Rechenoperation, die wir auf der Ebene E definieren können, nämlich die Multiplikation: Dazu beschreiben wir einen Punkt a der Ebene nicht nur durch seine Koordinaten (x, y), sondern durch seinen *Betrag* $|a|$ und sein *Argument* $\measuredangle a$, den Winkel von der positiven x-Achse im Gegenuhrzeigersinn zu a (wobei man pragmatischerweise $\measuredangle 0 := 0$ definiert; der Zusammenhang zwischen Koordinaten und Betrag/Argument ist durch die Formeln $x = |a| \cdot \cos \measuredangle a$, $y = |a| \cdot \sin \measuredangle a$ gegeben).

Definition. Das *Produkt* zweier Punkte $a, b \in E$ ist der (eindeutig bestimmte) Punkt $c \in E$ mit $|c| = |a| \cdot |b|$ und $\measuredangle c = \measuredangle a + \measuredangle b$. Man schreibt $c =: a \cdot b =: ab$.

2.1 Satz. *Für die Verknüpfungen $+$ und $\cdot$ auf E gelten die folgenden Rechenregeln für alle $a, b, c \in E$:*

i) $ab = ba$, $a + b = b + a$ *(Kommutativität)*

ii) $(a + b) + c = a + (b + c)$, $(ab)c = a(bc)$ *(Assoziativität)*

iii) $a(b+c) = ab + ac$ *(Distributivität)*

iv) Für die Punkte $0 := (0,0)$ *und* $1 := (1,0)$ *gilt* $0 + a = a$ *und* $1 \cdot a = a$.

v) Ist $a \neq 0$*, so gibt es ein (automatisch eindeutig bestimmtes)* d *mit* $ad = 1$*; wir schreiben* $\frac{1}{a} := d$.

Beweisskizze. Der einzige Punkt, der etwas Mühe erfordert, ist die Distributivität – dies ist aber (so gefährlich solche Wertungen sind) die wichtigste Rechenregel, denn erst durch sie wird ein Zusammenhang zwischen Addition und Multiplikation hergestellt, die ansonsten völlig unabhängig voneinander existieren würden. Zum ihrem Beweis kann man sich auf die zwei Fälle beschränken, daß $|a| = 1$ oder $\measuredangle a = 0$ ist; im einen Fall muß man dann die Drehinvarianz, im anderen die Streckinvarianz der geometrischen Definition der Vektoraddition beweisen. □

Man formuliert den Satz so, daß E mit den Verknüpfungen $+$ und $\cdot$ einen sogenannten *Körper* bildet, den *Körper der Komplexen Zahlen* (die übliche Notation, wenn man nicht wie wir Elementargeometrie treiben möchte, lautet $\mathbb{C} := E$). In einem Körper kann man bezüglich aller Grundrechenarten hantieren wie mit den gewöhnlichen rationalen oder reellen Zahlen. Der Körper E besitzt sogar, im Unterschied zu $\mathbb{R}$, zu jedem Element eine Quadratwurzel, wie man geometrisch sehen kann: nämlich durch Wurzelung des Betrages und Halbierung des Arguments der gegebenen Zahl!

Wir wir gesehen haben, benötigen wir sinnvolle Konstruktionen immer mindestens zwei gegebene Startpunkte – welche, ist im Prinzip egal, da man durch Drehen und Strecken aus einem gegebenen Punktepaar ein beliebiges anderes gegebenes Punktepaar machen kann. Wir vereinbaren daher, immer $0, 1 \in T$ anzunehmen. Unter dieser Voraussetzung lassen sich die (ja ebenfalls geometrisch definierten) komplexen Grundrechenarten alle mit Zirkel und Lineal durchführen:

2.2 Satz (Rechnen mit Zirkel und Lineal)**.** *Es sei* $T \subset \mathbb{C}$ *eine beliebige Teilmenge mit* $0, 1 \in T$*, und es sei* $\mathscr{K} := \mathscr{K}(T)$*. Dann gilt für alle* $a, b \in \mathscr{K}$*:*

$$a + b \in \mathscr{K}\,, \quad -a \in \mathscr{K}\,,$$
$$a \cdot b \in \mathscr{K}\,, \quad \frac{1}{a} \in \mathscr{K} \text{ (falls } a \neq 0\text{)}.$$

$\mathscr{K}$ *ist also ebenfalls ein Körper (ein Unterkörper von* E*).*

Beweis. Wir geben teilweise nur Beweisskizzen:

i) *Negatives:* $-a$ ist (für $a \neq 0$) der zweite Schnittpunkt von $C(0;0,a)$ und $L(0,a)$.

ii) *Summe:* $a + b$ ist einer der beiden Schnittpunkte von $C(a;0,b)$ und $C(b;0,a)$, sofern $a \neq 0$ und $a \neq b$ ist. $a + a = 2a$ ist der zweite Schnittpunkt von $C(a;0,a)$ und $L(0,a)$.

iii) *Produkt:* Die Richtung des Vektors von ab erhält man durch Winkelübertragung, eine Strecke der Länge $|a| \cdot |b|$ mittels zentrischer Streckung (also durch Konstruktion einer Parallelen).

iv) *Kehrwert:* Die Richtung des Vektors von a^{-1} ergibt sich wieder durch Winkelübertragung, und die Länge ebenfalls durch zentrische Streckung. □

2.3 Satz (Wurzelziehen mit Zirkel und Lineal)**.** *Es sei $T \subset \mathbb{C}$ eine beliebige Teilmenge mit $0, 1 \in T$, und es sei $\mathscr{K} := \mathscr{K}(T)$. Dann ist für jedes $a \in \mathscr{K}$ auch $\sqrt{a} \in \mathscr{K}$.*

Beweisskizze. Zum Wurzelziehen benötigt man zum einen eine Winkelhalbierung, zum anderen die Konstruktion einer Strecke der Länge $\sqrt{a}$. Ersteres ist klassischer Schulstoff; letzteres ermöglicht der Höhensatz des Pythagoras, der wiederum durch den Satz von Thales anwendbar wird. □

Wir vereinbaren, von nun an unter einer Konstruktion mit Zirkel und Lineal stets eine von den beiden Punkten $\{0, 1\}$ ausgehende Konstruktion zu verstehen, und schreiben kurz $\mathscr{K} := \mathscr{K}(\{0, 1\})$. Die Struktur eines Körpers auf der Menge $\mathscr{K}$ ermöglicht nun eine viel genauere Beschreibung ihrer Struktur; dazu müssen wir jedoch mehr über Körper wissen.

3 Körper und quadratische Erweiterungen

Ein Körper ist, wie gesagt, eine Teilmenge $F \subset E$ mit $0, 1 \in F$, für die mit $a, b \in F$ auch $a + b, -a, a \cdot b$ und (falls $a \neq 0$) auch $\frac{1}{a}$ in F liegen. Beispiele für Körper sind E selbst und $\mathscr{K}$, aber auch $\mathbb{Q}$ und $\mathbb{R}$ (wobei wir eine reelle Zahl a als das Element $(a, 0)$ von E auffassen).

3.1 Proposition. *Ist $F \subset E$ ein Körper, so gilt $\mathbb{Q} \subset F$.*

Beweis. Aus 1 in F folgt induktiv $a \in F$ für alle $a \in \mathbb{N}$ und dann auch für alle $a \in \mathbb{Z}$. Weiter ergibt sich $\frac{1}{a} \in F$ für alle $0 \neq a \in \mathbb{Z}$ und schließlich $\frac{a}{b} = a \cdot \frac{1}{b} \in F$ für alle $a, b \in \mathbb{Z}$, $b \neq 0$. □

3.2 Beispiel. *Die Menge $\left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$ ist ein Körper, den man als $\mathbb{Q}(\sqrt{2})$ bezeichnet.*

Beweis. Nicht offensichtlich sind nur die Abgeschlossenheit unter Multiplikation und die Existenz von Inversen. Für ersteres genügt die Rechnung $(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = ac + 2bd + (ad + bc)\sqrt{2}$, für letzteres die etwas trickreichere Darstellung

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{b}{a^2 - 2b^2}\sqrt{2}$$

für $a + b\sqrt{2} \neq 0$. Damit diese Rechnung korrekt ist, dürfen wir nicht mit 0 erweitert haben, wir müssen also $a - b\sqrt{2}$ nachweisen. Ist $b = 0$, so sind wir nach Voraussetzung fertig; andernfalls

würde aus $a - b\sqrt{2} = 0$ folgen $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$, und schon die alten Griechen wußten, daß $\sqrt{2}$ keine rationale Zahl ist.[2] □

Dieses Beispiel läßt sich ausdehnen zu einem allgemeinen Verfahren, um Körper zu vergrößern:

3.3 Satz. *Es sei $F \subset E$ ein Körper, und es sei $\alpha \in E$ Lösung einer quadratischen Gleichung $x^2 + px + q = 0$ mit $p, q \in F$. Dann ist die Menge $F(\alpha) := \{a + b\alpha \mid a, b \in F\}$ wieder ein Körper.*

Man nennt den Körper $F(\alpha)$ eine *quadratische Erweiterung* von F.[3]

Beweis. Wir unterscheiden zwei Fälle: Ist $\alpha \in F$, so gilt $F(\alpha) = F$, so daß nichts zu beweisen ist. Wir können uns also auf den interessanteren Fall beschränken, daß $\alpha \notin F$ ist.

Der Beweis verläuft nun ähnlich wie im letzten Beispiel, nur noch etwas trickreicher: Für Produkte ergibt sich

$$(a + b\alpha) \cdot (c + d\alpha) = ac + bd\alpha^2 + (ad + bc)\alpha = (ac - bdq) + (ad - bc - p)\alpha \in F(\alpha),$$

wobei wir die Beziehung $\alpha^2 = -q - p\alpha$ verwendet haben. Für die Existenz von Inversen verwenden wir einen Trick: Es sei $\beta := -p - \alpha$; nach dem Satz von Vieta ist β ebenfalls eine Nullstelle des gleichen Polynoms, und es gilt $\alpha \cdot \beta = q$. Für $a + b\alpha \neq 0$ können wir nun rechnen

$$\begin{aligned}\frac{1}{a + b\alpha} &= \frac{a + b\beta}{(a + b\alpha)(a + b\beta)} = \frac{a - b(p + \alpha)}{a^2 + b^2\alpha\beta + ab(\alpha + \beta)} = \frac{(a - bp) - b\alpha}{a^2 + qb^2 - pab} \\ &= \frac{a - bp}{a^2 + qb^2 - pab} - \frac{b}{a^2 + qb^2 - pab}\alpha.\end{aligned}$$

Dieser letzte Ausdruck liegt nun sicher in $F(\alpha)$; wir müssen nur wieder sicherstellen, daß wir nicht mit Null erweitert haben: Wäre aber $a + b\beta = 0$, so folgt (wegen $a + b\alpha \neq 0$) auf jeden Fall $b \neq 0$, daraus aber $\beta = -\frac{a}{b} \in F$ und weiter $\alpha = -p - \beta \in F$, aber diesen Fall haben wir oben schon behandelt. □

4 Die algebraische Charakterisierung konstruierbarer Punkte

Mit diesen Begriffen können wir eine präzise Charakterisierung des Körpers der konstruierbaren Zahlen geben:

[2] Auch ohne die Kenntnis dieses Satzes wäre die Aussage richtig: Denn dann wäre einfach $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}$.

[3] Für Kenner: Man beachte, daß wir – in der üblichen Terminologie – eigentlich eine Erweiterung vom Grad *höchstens* 2 definiert haben.

4.1 Satz (Hauptsatz über konstruierbare Zahlen)**.** *Ein Punkt $a \in E$ liegt genau dann im Körper $\mathscr{K}$ der konstruierbaren Zahlen, wenn es eine Kette*

$$\mathbb{Q} = F_0 \subset K_1 \subset \cdots \subset F_n \subset E$$

von Körpern gibt, so daß $a \in F_n$ gilt und jedes F_i eine quadratische Erweiterung von F_{i-1} ist, d.h. $F_i = F_{i-1}(\alpha_i)$ für eine Zahl $\alpha_i \in E$, die Lösung einer quadratischen Gleichung mit Koeffizienten in F_{i-1} ist.

Mit etwas mehr algebraischem Aufwand kann man daraus folgern:

4.2 Folgerung. *Ist eine Zahl $a \in E$ konstruierbar, so ist a Lösung einer Polynomgleichung mit rationalen Koeffizienten. Ist der Grad dieser Polynomgleichung* minimal *gewählt, so ist er eine Zweierpotenz.*

Beweisskizze. Man zeigt, daß in einer Körperkette wie im Hauptsatz der Körper F_i ein Vektorraum über dem Körper $\mathbb{Q}$ von der Dimension 2^i ist. Insbesondere ist diese Dimension *endlich*; die Potenzen $1, a, a^2, \ldots$ eines Elementes a können also nicht $\mathbb{Q}$-linear unabhängig sein, und das bedeutet genau die Existenz einer Gleichung wie angegeben.

Für die Aussage über den Grad der Gleichung zeigt man allgemein: Liegt a in einem Körper, der als $\mathbb{Q}$-Vektorraum n-dimensional ist, so ist der minimale Grad einer rationalen Gleichung für a ein Teiler von n (dies ist der *Gradsatz*). □

4.3 Folgerung. *Das Problem der Würfelverdoppelung ist nicht lösbar.*

Beweis. Aufgrund der Volumenformel $A^3 = 2a^3$ ist die Möglichkeit der Konstruktion äquivalent zur Gültigkeit der Aussage $\sqrt[3]{2} \in \mathscr{K}$. Ich behaupte aber, daß die Gleichung $x^3 - 2 = 0$, die $\sqrt[3]{2}$ als Lösung besitzt, minimalen Grad unter allen solchen Gleichungen hat: da 3 keine Zweierpotenz ist, folgt damit $\sqrt[3]{2} \notin \mathscr{K}$.

Angenommen, f wäre ein Polynom über $\mathbb{Q}$ vom Grad < 3 mit $f(\sqrt[3]{2}) = 0$. Wäre $\deg f = 1$, so wäre $\sqrt[3]{2} \in \mathbb{Q}$, und das ist (wie schon die alten Griechen wußten) falsch. Wäre $\deg f = 2$, so könnten wir schreiben $x^3 - 2 = gf + h$ mit $\deg h < 2$. Einsetzen von $\sqrt[3]{2}$ liefert $0 = h(\sqrt[3]{2})$, aber wegen $\deg h < 2$ folgt $h = 0$. Also ist $x^3 - 2 = gf$, und es folgt $\deg g = 1$. Aber damit besitzt g eine rationale Nullstelle, die damit auch eine Lösung von $x^3 - 2$ ist – Widerspruch. □

4.4 Folgerung. *Das Problem der Quadratur des Kreises ist nicht lösbar.*

Beweis. Die Möglichkeit einer solchen Konstruktion ist aufgrund der Flächenformel $a^2 = r^2\pi$ äquivalent zur Gültigkeit der Aussage $\sqrt{\pi} \in \mathscr{K}$, die wiederum äquivalent zur Aussage $\pi \in \mathscr{K}$ ist. Aber π ist *niemals* Lösung einer Polynomgleichung mit rationalen Koeffizienten; dies hat Ferdinand Lindemann (später Professor am Mathematischen Institut der Münchener Universität) im Jahr 1882 bewiesen. □

Eine weitere Anwendung betrifft die Möglichkeit der Konstruktion des regelmäßigen n-Ecks. Diese ist sicherlich äquivalent zur Konstruktion der Zahl ζ_n mit $|\zeta_n| = 1$ und $\measuredangle\zeta_n = 2\pi/n$. Nun kann man aber beweisen:

4.5 Lemma (über die Kreisteilungsgleichung)**.** *Der minimale Grad einer rationalen Gleichung für ζ_n ist die Zahl $\varphi(n) := n \cdot \prod_{p|n}(1 - \frac{1}{p})$, wobei sich das Produkt über alle Primteiler von n erstreckt.*

Ist $n = p_1^{e_1} \cdot \ldots \cdot p_n^{e_n}$ (mit $e_i \geqslant 1$) die Primfaktorzerlegung von n, so gilt

$$\varphi(n) = \prod_{i=1}^{n}(p_i^{e_i} - p_i^{e_i-1}) = \prod_{i=1}^{n} p_i^{e_i-1} \cdot (p_i - 1).$$

Wann ist diese Zahl einer Zweierpotenz? Es dürfen keine ungeraden Faktoren vorkommen. Ist also p_i eine *ungerade* Primzahl, so muß $e_i - 1 = 0$ sein, also $e_i = 1$, und außerdem muß $p_i - 1$ eine Zweierpotenz sein. Ist p_i gerade, also die Primzahl 2, so ist der Faktor $2^{e_i-1} \cdot 1$ stets eine Zweierpotenz. Das bedeutet:

4.6 Folgerung. *Damit das regelmäßige n-Eck konstruierbar sein kann, muß $n = 2^e \cdot p_1 \cdot \ldots \cdot p_n$ sein, wobei die p_i paarweise verschiedene ungerade Primzahlen sind, für die $p_i - 1$ eine Zweierpotenz ist.*

4.7 Folgerung. *Das regelmäßige Neuneck ist nicht mit Zirkel und Lineal konstruierbar. Insbesondere ist die Dreiteilung des Winkels im Allgemeinen mit Zirkel und Lineal nicht möglich.*

Beweis. Die Zahl $n = 9$ enthält den ungeraden Primfaktor 3 doppelt. □

Die Frage lautet nun jedenfalls: Für welche ungeraden Primzahlen p ist $p-1$ eine Zweierpotenz, also $p = 2^s + 1$? Man kann die Suche einschränken, wenn man beobachtet, daß der Exponent s selbst eine Zweierpotenz sein muß: Denn besitzt s einen ungeraden Teiler $u \geqslant 3$, also $s = ut$, so gilt $2^s + 1 = (2^t)^u + 1^u = (2^t + 1) \cdot (\ldots)$ nach der geometrischen Summenformel, und $1 < 2^t + 1 < 2^s + 1$, so daß $2^s + 1$ nicht prim sein kann. Wir suchen also Primzahlen der Form $F_f := 2^{2^f} + 1$, sogenannte *Fermatsche* Primzahlen. In der folgenden Tabelle

f	0	1	2	3	4	5
$F_f = 2^{2^f} + 1$	3	5	17	257	65.537	$4.294.967.297 = 641 \cdot 6.700.417$

sind die ersten fünf Zahlen tatsächlich Primzahlen, und Fermat vermutete deswegen im Jahre 1637, die Zahlen F_f seien *stets* Primzahlen. Leonhard Euler fand jedoch im Jahre 1732 den Teiler 641 von F_5, womit die Vermutung widerlegt war. Erstaunlicherweise sind bis heute keine weiteren Fermatschen Primzahlen gefunden worden – auf jeden Fall sind F_5 bis F_{32} nicht prim.

Tatsächlich ist die Aussage in der Folgerung sogar eine Äquivalenz: Für jedes n der angegebenen Form ist das regelmäßige n-Eck tatsächlich konstruierbar. Dies hat als erster Gauß bewiesen; für einen Beweis würden wir jedoch mehr algebraische Techniken benötigen, um beweisen zu können, daß Körperketten wie im Hauptsatz in diesem Fall tatsächlich stets existieren. Heute formuliert man diese Sätze und Beweise mit Hilfe der sogenannten *Galoistheorie*. Insbesondere gilt:

4.8 Satz (Gauß)**.** *Das regelmäßige Siebzehneck ist mit Zirkel und Lineal konstruierbar.*

5 Der Beweis des Hauptsatzes

Die Hauptarbeit beim Beweis des Satzes verschieben wir in das folgende Lemma. Dazu benötigen wir noch eine Notation: Für einen Punkt $a \in E$ bezeichnet man mit $\overline{a}$ den Punkt, der entsteht, wenn man a an der x-Achse spiegelt; mit $a = (x, y)$ ist also $\overline{a} = (x, -y)$. Für eine Teilmenge $T \subset E$ schreiben wir $\overline{T} := \{\overline{a} \,|\, a \in T\}$ für ihr Spiegelbild entlang der x-Achse.

5.1 Lemma. *Es sei $F \subset E$ ein Körper.*

i) Gilt $F \subset \mathscr{K}$, und ist $F \subset F(\alpha)$ eine quadratische Erweiterung, so gilt auch $F(\alpha) \subset \mathscr{K}$.

ii) Ist $T \subset F$ eine Teilmenge, so liegt jedes Element von $\mathscr{K}^1(T)$ in einer quadratischen Erweiterung von F, sofern $i \in F$ und $\overline{T} \subset F$ gilt.

Die unterstrichene Bedingung in (ii) ist leider notwendig. Zum besseren Verständnis des Argumentes ignorieren wir sie im Beweis des Hauptsatzes zunächst und zeigen hinterher, wie man sie berücksichtigen kann.

Beweis des Hauptsatzes. Immer dann. Wegen $\mathbb{Q} \subset \mathscr{K}$ folgt durch wiederholte Anwendung von Punkt i) des Lemmas sofort $F_n \subset \mathscr{K}$ und damit $a \in \mathscr{K}$.

Nur dann. Wir zeigen durch Induktion nach n, daß die Aussage für jedes Element von $\mathscr{K}^n(\{0, 1\})$ stimmt, wobei die Aussage für $n = 0$ trivial ist (denn $0, 1 \in \mathbb{Q}$). Sei die Aussage nun für $n - 1$ gezeigt, und es sei $a \in \mathscr{K}^n(\{0, 1\})$. Dann gibt es eine endliche (genauer: höchstens sechselementige) Teilmenge $T \subset \mathscr{K}^{n-1}(\{0, 1\})$ mit $a \in \mathscr{K}^1(T)$. Indem wir die Induktionsvoraussetzung nacheinander auf jedes Element T anwenden, erhalten wir einen Körper F, der Spitze einer Kette quadratischer Erweiterungen von $\mathbb{Q}$ ist, für den $T \subset F$ gilt. Teil ii) des Lemmas zeigt dann (wenn wir die unterstrichene Bedingung ignorieren), daß a in einer quadratischen Erweiterung von F liegt, und wir sind fertig.

Um die korrekte Form des Lemmas zu verwenden, müssen wir unser Argument ein wenig verfeinern. Offensichtlich gilt: Ist T symmetrisch zur x-Achse, so auch $\mathscr{K}^1(T)$; induktiv folgt daraus, daß jedes $\mathscr{K}^n(\{0, 1\})$ symmetrisch zur x-Achse ist. Durch Ersetzen von T durch $T \cup \overline{T}$ können wir deswegen erzwingen, daß $T = \overline{T}$ ist, und dann folgt aus $T \subset F$ auch $\overline{T} \subset F$.

Schließlich ersetzen wir noch F durch $F(i)$ (dies ist wegen $i^2 + 1 = 0$ eine quadratische Erweiterung von F), um $i \in F$ zu erzwingen – damit sind die Voraussetzungen des Lemmas tatsächlich erfüllt. □

Beweis des Lemmas.

i) Es genügt zu zeigen, daß $\alpha \in \mathscr{K}$ ist. Aber α ist Lösung einer quadratischen Gleichung $X^2 + pX + q = 0$ mit $p, q \in F$; nach der quadratischen Lösungsformel gilt also

$$\alpha = \frac{-p \pm \sqrt{p^2 - 4q}}{2}.$$

Wir haben schon gesehen, daß man in $\mathscr{K}$ Quadratwurzeln ziehen kann; damit folgt aus $p, q \in F \subset \mathscr{K}$ auch $\alpha \in \mathscr{K}$.

ii) Die Voraussetzung impliziert: Ist $t = (t^x, t^y) \in T$, so sind $\frac{1}{2}(t+\overline{t}) = t^x$ und $\frac{1}{2i}(t-\overline{t}) = t^y$ in F enthalten.

Ist $a \in T$, so ist nichts zu zeigen. Also ist a Schnittpunkt von Geraden bzw. Kreisen, die durch Punkte aus T definiert werden. Wir unterscheiden Fälle, je nachdem, wie a gegeben ist:

a) Angenommen, a ist Schnittpunkt der (nicht parallelen) Geraden $L(t_1, t_2)$ und $L(s_1, s_2)$ mit $t_1, t_2, s_1, s_2 \in T$. Das bedeutet, daß es $\lambda, \mu \in \mathbb{R}$ gibt mit

$$t_1 + \lambda(t_2 - t_1) = s_1 + \mu(s_2 - s_1),$$

oder in Koordinaten:

$$\begin{pmatrix} t_1^x - s_1^x \\ t_1^y - s_1^y \end{pmatrix} = \begin{pmatrix} s_2^x - s_1^x & t_1^x - t_2^x \\ s_2^y - s_1^y & t_1^y - t_2^y \end{pmatrix} \begin{pmatrix} \mu \\ \lambda \end{pmatrix}.$$

Dies ist ein lineares Gleichungssystem, deren (wegen der Nichtparallelität der Geraden) eindeutig bestimmte Lösung (μ, λ) sich durch die vier Grundrechenarten aus den Koeffizienten bestimmen lassen. Die Koeffizienten liegen aber nach unserer Vorbemerkung alle in F, und damit folgt $\mu, \lambda \in F$, also auch $a = t_1 + \lambda(t_2 - t_1) \in F$. (In diesem Fall sind wir also ohne eine Körpererweiterung ausgekommen.)

b) Angenommen, a ist Schnittpunkt des Kreises $C(u; t_1, t_2)$ und der Geraden $L(s_1, s_2)$ mit $u, t_1, t_2, s_1, s_2 \in T$. Wir bemerken, daß der quadrierte Kreisradius

$$r^2 = (t_1 - t_2) \cdot \overline{t_1 - t_2} = t_1\overline{t_1} + t_2\overline{t_2} - t_1\overline{t_2} - t_2\overline{t_1}$$

in F liegt. Die Bedingung lautet nun, daß es ein $\mu \in \mathbb{R}$ gibt mit $a = s_1 + \mu(s_2 - s_1)$ und

$$\begin{aligned} r^2 &= |a - u|^2 = |s_1 - u + \mu(s_2 - s_1)|^2 \\ &= |s_1 - u|^2 + \mu^2 |s_2 - s_1|^2 + \mu \cdot (s_1 - u)(s_2 - s_1) \cdot (\overline{s_1} - \overline{u}) \cdot (\overline{s_2} - \overline{s_1}). \end{aligned}$$

Das zeigt, daß μ Lösung einer quadratischen Gleichung ist, deren Koeffizienten allesamt in F liegen. Also ist $K(\mu)$ eine quadratische Erweiterung von F, und es gilt $a = s_1 + \mu(s_2 - s_1) \in K(\mu)$, was zu beweisen war.

c) Angenommen, a ist Schnittpunkt der (voneinander verschiedenen) Kreise $C(u; t_1, t_2)$ und $C(v; s_1, s_2)$. Das bedeutet, daß

$$r^2 := |t_1 - t_2|^2 = |a - u|^2 = |a|^2 + |u|^2 - 2(au)^x \qquad \text{(I)}$$
$$\text{und} \quad s^2 := |s_1 - s_2|^2 = |a - v|^2 = |a|^2 + |v|^2 - 2(av)^x \qquad \text{(II)}$$

gilt. Subtrahieren wir diese Gleichungen voneinander, heben sich die Terme $|a|^2$ auf, und wir erhalten

$$r^2 - s^2 = |u|^2 - |v|^2 + 2(a(v - u))^x. \qquad \text{(III)}$$

Schreibt man Gleichung (III) in Koordinaten aus, entpuppt sie sich als Gleichung einer gewissen Geraden, auf der a liegen muß, und bei genauem Hinsehen zeigt sich, daß diese Gerade durch zwei Punkte definiert ist, die samt ihren Konjugierten in F liegen. Da das Gleichungssystem aus den Gleichungen (I) und (III) äquivalent zum ursprünglichen System aus Gleichungen (I) und (II) ist, sind wir damit (gegebenenfalls nach Vergrößern von T) genau im Fall b), den wir schon behandelt haben. □

6 Konstruktionen ohne Zirkel und Lineal

Hisashi Abe gab in den 1970er Jahren eine Konstruktion des Drittels eines gegebenen Winkels an, die sogar gänzlich *ohne* die Verwendung von Zirkel und Lineal auskommt: Stattdessen werden die üblichen Techniken des Origami, der japanischen Papierfaltkunst, auf das Zeichenpapier angewandt.

Man kann zeigen, daß unsere drei bislang zulässig Konstruktionsschritte auch mit Origami durchführbar sind (das Falten von Kreisen ist selbstverständlich nicht möglich, aber Schnittpunkte mit „virtuellen“ Kreisen können durch Falten gewonnen werden). Wenn die Winkeldrittelung nun mit Origami möglich ist, muß es Faltschritte geben, die mächtiger sind als Konstruktionen mit Zirkel und Lineal. Es stellt sich heraus, daß die Konstruktion *doppelter Punkt-auf-Gerade-Spiegelungen* dieser entscheidende Faltschritt ist.

Sind $g := L(t_1, t_2)$ und $h := L(s_1, s_2)$ zwei verschiedene Geraden, und sind $u, v \in E$ zwei verschiedene Punkte, so ist eine *Spiegelung von u auf g und von v auf h* eine Gerade mit der Eigenschaft, daß Spiegelung an dieser Gerade den Punkt u auf die Gerade g und den Punkt v auf die Gerade h abbildet.

Eine solche simultane Spiegelachse muß nicht unbedingt existieren, und falls sie existiert, muß sie nicht eindeutig sein. Jede solche Gerade ist jedoch mit einer direkten Origamioperation durch Falten herstellbar. Solcherart gegebene Geraden gehören also ebenfalls zu den Objekten, deren Schnittpunkte in einer Axiomatik des Origamifaltens zuzulassen sind.

Definiert man nun, ganz analog, zu einer Menge $T \subset E$ die Menge $\mathscr{O}^1(T)$ der direkt aus T faltbaren Punkte und allgemein $\mathscr{O}^n(T) := \mathscr{O}^1(\mathscr{O}^{n-1}(T))$ sowie $\mathscr{O}(T) := \bigcup_n \mathscr{O}^n(T)$ und $\mathscr{O} := \mathscr{O}(\{0,1\})$, so ist $\mathscr{O}$ wieder ein Körper, der *Körper der Origami-faltbaren Zahlen*, und es gilt $\mathscr{K} \subset \mathscr{O}$.

Dann kann man beweisen:

6.1 Satz (Hauptsatz über Origami-faltbare Zahlen)**.** *Ein Punkt $a \in E$ liegt genau dann im Körper $\mathscr{O}$ der Origami-faltbaren Zahlen, wenn es eine Kette*

$$\mathbb{Q} = F_0 \subset K_1 \subset \cdots \subset F_n \subset E$$

von Körpern gibt, so daß $a \in F_n$ gilt und jedes F_i eine quadratische oder kubische Erweiterung von F_{i-1} ist, d.h. $F_i = F_{i-1}(\alpha_i)$ für eine Zahl $\alpha_i \in E$, die Lösung einer quadratischen oder kubischen Gleichung mit Koeffizienten in F_{i-1} ist.

Dabei ist $F(\alpha) = \{a + b\alpha + c\alpha^2 \mid a, b, c \in F\}$, wenn α Lösung einer kubischen Gleichung mit Koeffizienten in F ist; auch dies ist stets ein Körper. Insbesondere kann man mit Origami Kubikwurzeln ziehen, was auch bedeutet:

6.2 Folgerung. *Das Delische Problem ist mit Origami lösbar.*

Mit den gleichen algebraischen Methoden wie im Falle der Konstruktion mit Zirkel und Lineal kann man auch zeigen:

6.3 Folgerung. *Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal faltbar, wenn $\varphi(n)$ nur die Primfaktoren 2 und 3 enthält, und dies ist genau dann der Fall, wenn $n = 2^e \cdot 3^f \cdot p_1 \cdot \ldots \cdot p_n$ ist, wobei die p_i paarweise verschiedene Primzahlen sind, für die $p_i - 1$ nur die Primfaktoren 2 und 3 besitzt.*

Primzahlen dieser Form heißen auch *Pierpont-Primzahlen*, und es ist nicht bekannt, ob es unendlich viele von ihnen gibt. Die ersten von ihnen sind

$$2, 3, 5, 7, 13, 17, 19, 37, \ldots,$$

so daß sich ergibt:

6.4 Folgerung. *Das regelmäßige Siebeneck und das regelmäßige Dreizehneck lassen sich mit Origami konstruieren, das regelmäßige Elfeck jedoch nicht.*

Literatur

Eine für Nichtmathematiker geschriebene Einführung in die Theorie der Konstruierbarkeit und der Lösbarkeit von Gleichungen ist *Bewersdorff, Algebra für Einsteiger (Vieweg)*. Eine umfassende Darstellung der Theorie, inklusive der Origami-Konstruierbarkeit, bietet *Cox, Galois Theory (Wiley)*.