3 Die klassischen griechischen Konstruktionsprobleme

Aus der griechischen Antike sind folgende geometrische Konstruktionsprobleme überliefert.

- Wie teilt man einen (beliebig vorgegebenen) Winkel in drei gleiche Teile?
- Wie kann man zu einem gegebenen Würfel einen Würfel konstruieren, der das doppelte Volumen besitzt?
- Wie konstruiert man zu einem gegebenen Kreis ein Quadrat gleichen Flächeninhalts?
- Wie konstruiert man ein regelmäßiges n-Eck?

(Wenn man von den drei klassischen Konstruktionsproblemen redet, sind es die drei ersten.)
Hierzu muss man wissen, dass die Griechen als Hilfsmittel nur „Zirkel und Lineal“ zuließen und auch mit diesen Hilfsmittel nur die folgenden Operationen erlaubten.

Operation 1, Lineal Durch zwei gegebene Punkte kann man eine Gerade legen.

Operation 2, Zirkel Man kann einen Kreis zeichnen, wobei der Mittelpunkt P_0 ein bereits konstruierter Punkt ist und der Radius r gleich dem Abstand von P_0 zu einem anderen bereits konstruierten Punkt P_1 ist.

Neue Punkte erhält man als Schnittpunkte von den konstruierten Geraden oder Kreisen. Ein Punkt gilt als konstruierbar, wenn er durch eine endliche Anzahl von Anwendungen der Operationen 1 und 2 konstruierbar ist.

Übung 3.1. Gegeben seien zwei Punkte. Konstruieren Sie den Mittelpunkt.

Übung 3.2. Überlegen Sie sich, dass Sie mit unendlich vielen Schritten aus zwei Punkten mit Abstand 1 alle beliebigen reellen Abstände konstruieren können.

Übung 3.3. Bequemer ist es, statt Operation 2 folgendes zuzulassen:
Man kann einen Kreis zeichnen, wobei der Mittelpunkt P_0 ein bereits konstruierter Punkt ist und der Radius r gleich dem Abstand von zwei anderen bereits konstruierten Punkt P_1 und P_2 ist. Zeigen Sie, dass man diese Übertragung des Radius aus Operation 2 herleiten kann.

Über Jahrhunderte zweifelte niemand daran, dass für diese Probleme eine Lösung existiert, d.h. dass man nur lange genug nach ihr suchen müsse. Heute hingegen weiß man, dass für die ersten drei Probleme *keine* Lösung existiert. Und gerade dies ist für Nichtmathematiker häufig unvorstellbar.
Wir beschäftigen uns mit einem *Beweis*, dass die obigen Probleme im allgemeinen unlösbar sind.
Die Lösungsstrategie besteht darin, dass wir das geometrische Problem in ein äquivalentes algebraisches Problem umformulieren. Wir zeigen dann, dass das algebraische Problem keine Lösung hat.

Obwohl wir in der zweidimensionalen Geometrie denken, ist es bequemer, sich vorzustellen, dass wir bestimmte reelle Zahlen konstruieren wollen. Kann man zwei Punkte mit Abstand a konstruieren, sagen wir, dass wir die reelle Zahl a konstruieren können. Wir formulieren obige Probleme in diesem Sinne um.

- Bei der Würfelverdoppelung reicht es, $\sqrt[3]{2}$ zu konstruieren.
- Bei der Quadratur des Kreises reicht es, $\sqrt{\pi}$ zu konstruieren.
- Bei der Winkeldreiteilung reicht es, zu gegebenem Winkel α die Zahl $\cos(\alpha/3)$ zu konstruieren. Da wir zeigen werden, dass die Winkeldreiteilung allgemein nicht möglich ist, reicht es, für einen bestimmten Winkel zu zeigem, dass sie nicht möglich ist. Für $\alpha = 60^0$ sieht man, dass es ausreicht, eine Nullstelle von $f(x) = 8x^3 - 6x - 1$ (oder mit $y = 2x$ von $f(y) = y^3 - 3y - 1$) zu konstruieren.
- Bei den n-Ecken reicht es analog, $\cos(\frac{360^0}{n})$ zu konstruieren.

Definition 3.1. *Sei $\mathbb{K}$ die Menge der konstruierbaren reellen Zahlen.*

Satz 3.2. *Die Menge der konstruierbaren Zahlen $\mathbb{K}$ ist ein Körper.*

Beweis. Wir können mit Zirkel und Lineal addieren, subtrahieren, multiplizieren und dividieren (siehe Übung). Es folgt dann natürlich $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{R}$.
Exemplarisch behandeln wir die Multiplikation:
Gegeben seien die Streckenlängen 1, a und b. Gesucht ist eine Strecke der Länge ab. Wir tragen auf einer Geraden die Strecke $|OA| = a$ und $|OB| = 1$ ab. Über B konstruieren wir die Senkrechte auf die Gerade durch A und B und tragen darauf die Strecke $|BQ| = b$ ab. Wir zeichnen die Gerade durch O und Q. Wir konstruieren die Parallele zu BQ durch A. Den Schnittpunkt mit der Geraden durch O und Q nennen wir P. Nach den Strahlensätzen ist $|AP| : a = b : 1$, also $|AP| = ab$.
Die Divison verwendet die gleiche Figur und die Strahlensätze. Siehe Übung.

Übung 3.4. Zeigen Sie, dass man mit Zirkel und Lineal addieren und subtrahieren und dividieren kann.

Gibt es noch weitere Operationen, die wir konstruieren können? Ja, wir können mittels Euklids Höhensatz Wurzeln ziehen.
Gegeben seien Strecken der Längen a und der Länge 1. Gesucht sei eine Strecke der Länge $\sqrt{a}$. Wir konstruieren eine Strecke AQ der Länge $a + 1$. Hierbei sei $a = |AB|$ und $1 = |BQ|$. Wir konstruieren den Mittelpunkt M der Strecke AQ und einen Kreis um M mit Radius $|MA|$. Wir errichten eine Senkrechte zu AQ durch B. Der Schnittpunkt P der Senkrechten mit dem Kreis ergibt ein rechtwinkliges Dreieck APQ (Satz von Thales). Nach dem Höhensatz gilt: $|BP|^2 = a \cdot 1$. Also ist $|BP| = \sqrt{a}$.
Daher gilt:
Die Menge der konstruierbaren Zahlen $\mathbb{K}$ ist ein Körper, der alle (endlich iterierten) quadratischen Erweiterungen von $\mathbb{Q}$ enthält. Insbesondere ist also z.B. $\sqrt[8]{\sqrt{2} + 5\sqrt{7} + 2} + \frac{3}{11}\sqrt{14}$ konstruierbar.

Man kann aber nun zeigen, dass man außer derartigen Zahlen keine weiteren mehr erhalten kann.

Satz 3.3. *Die Menge der konstruierbaren Zahlen $\mathbb{K}$ ist gleich dem Körper, der alle (endlich iterierten) quadratischen Erweiterungen von $\mathbb{Q}$ enthält, also gleich dem reell quadratisch abgeschlossenen Körper über $\mathbb{Q}$.*

Der Beweis analysiert, auf welche Weise neue Punkte konstruiert werden: Schnitt von einer Gerade mit einer anderen Gerade führt auf eine lineare Gleichung, Schnitt von Gerade mit Kreis führt auf eine quadratische Gleichung, und Schnitt von Kreis mit Kreis führt ebenfalls auf eine Gleichung vom Grad 2 (und nicht etwa 4 !).
Hieraus folgt

Satz 3.4. *Sei $\alpha \in \mathbb{K}$. Dann ist $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ eine Zweierpotenz.*

Hierbei bezeichnet $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ den Körpererweiterungsgrad. Man bestimmt zu α das Minimalpolynom. $\mathbb{Q}(\alpha)$ ist (bezüglich Inklusion) der kleinste Körper, der $\mathbb{Q}$ und α enthält.

Beweis. Jede konstruierbare Zahl ist in endlich vielen Schritten konstruierbar, liegt also in einer n-fach iterierten quadratischen Körpererweiterung von $\mathbb{Q}$. Aufgrund des Turmsatzes der Körpertheorie folgt mit einer Reihe von Zwischenkörpern $[Q_n : Q] = [Q_n : Q_{n-1}] \cdot [Q_{n-1} : Q_{n-2}] \cdots [Q_1 : Q] = 2^n$. Der Turmsatz selbst folgt aus der linearen Algebra durch Angeben einer Basis.
Beispiel: $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ hat $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ als Basis über $\mathbb{Q}$:

Satz 3.5. *Wenn ein kubisches Polynom mit rationalen Koeffizienten keine rationalen Nullstellen hat, dann ist keine der Nullstellen mit Zirkel und Lineal konstruierbar.*
Oder:
Sei α Nullstelle von einem (über $\mathbb{Q}$) irreduziblen Polynom vom Grad 3 mit ganzzahligen Koeffizienten. Dann ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ und damit ist α nicht konstruierbar.

Satz 3.6. *Die Polynome $f_1 : x^3 - 2$ und $f_2 : 8x^3 - 6x - 1$ sind irreduzibel. Daraus folgt:*

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3, \quad [\mathbb{Q}(\cos(20^0)) : \mathbb{Q}] = 3.$$

Satz 3.7. *Die Zahl π ist transzendent, (Lindemann, 1882), d.h. sie ist niemals Nullstelle eines Polynoms mit ganzzahligen Koeffizienten. Daraus folgt:*

$$[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = \infty.$$

Aus den obigen Sätzen folgt nun unmittelbar, dass man mit Zirkel und Lineal den Winkel von 60^0 nicht in drei gleiche Teile zerlegen kann, dass man die Würfelverdoppelung nicht konstruieren kann und dass man zu einem Kreis kein flächengleiches Quadrat konstruieren kann. Die Versuche von Laien, dies dennoch zu tun, sind zwangsläufig zum Scheitern verurteilt, bzw. können allenfalls gute Näherungslösungen sein.

Hinweis: Ist α Nullstelle von einem Polynom mit Grad=Zweierpotenz, dann ist aber noch nicht klar, ob man α auch durch eine Verkettung von quadratischen Wurzeln darstellen kann. Dies führt auf komplizierte Fragen, die allgemein im Rahmen der Galoistheorie gelöst werden. Die Galoistheorie verlagert schwierige Fragen über Zwischenkörper auf einfachere Fragen von Untergruppen der (endlichen) Galoisgruppe des zugehörigen Polynoms.
Die Untergruppenstruktur der Galoisgruppe ist isomorph (nur auf den Kopf gestellt) zur Untergruppenstruktur der Zwischenkörper zwischen $\mathbb{Q}(\alpha)$ und $\mathbb{Q}$. Im Falle von kubischen Polynomen benötigt man aber keine Galoistheorie, wie wir gesehen haben.
Im Alter von 18 Jahren gelang es Gauß (1796), die Konstruierbarkeit des regelmäßigen 17-Ecks zu beweisen. (Dies wird manchmal als der erste wesentliche Beitrag zur Geometrie nach Euklid bewertet.)
Allgemein führt das regelmäßige n-Eck auf das sogenannte Kreisteilungspolynom vom Grad $\varphi(n)$, wobei $\varphi(n)$ die Eulerfunktion ist.
Ist nun n eine Primzahl der Form $2^r + 1$, so ist $\varphi(n)$ eine Zweierpotenz. (In der Zahlentheorie beweist man, dass eine derartige Primzahl sogar die Form $2^{2^k} + 1$ haben muss.) Und für diese speziellen Kreisteilungspolynome bewies Gauß, dass sie durch sukzessive quadratische Gleichungen gelöst werden können.
Es gilt der folgende Satz:

Satz 3.8. *[ohne Beweis] Das regelmäßige n-Eck kann genau dann mit Zirkel und Lineal konstruiert werden, wenn die Primfaktorzerlegung von n die folgende Form hat:*

$$n = 2^r p_1 p_2 \cdots p_s,$$

wobei $r, s \geq 0$ und die p_i verschiedene Primzahlen der Form $2^{2^{r_i}} + 1$ sind.

Gauß bewies hierbei die Existenz der Konstruktion, also dass es sich um eine hinreichende Bedingung handelt. Erst viel später bewies Wantzel die viel einfachere Notwendigkeit der angegebenen Bedingung. (Diese war Gauß wohl bekannt, wenn auch er sie nicht bewies.)
Insbesondere folgt also die Konstruierbarkeit für die Fermatschen Primzahlen: $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$. Weitere Fermatschen Primzahlen sind nicht bekannt.

Übung 3.5. Konstruieren Sie das regelmäßige n-Eck mit Zirkel und Lineal für $n = 2, 3, 4, 5, 6, 8, 10, 12, 15, 16$.

Übung 3.6. Aus Satz 3.8 folgt, dass das regelmäßige 7 und 9-Eck nicht konstruiert werden kann. Beweisen Sie:

a) leicht: Das regelmäßige 9-Eck kann nicht konstruiert werden.

b) nicht so leicht: Das regelmäßige 7 Eck kann nicht konstruiert werden. Tipp: Denken Sie sich, dass Sie eine komplexe Zahl z suchen, mit $z^7 = 1$. Reduzieren Sie dies mit $t = z + \frac{1}{z}$ auf ein irreduzibles kubisches Polynom.

Übung 3.7. Seien m und n teilerfremd. Wenn das regelmäßige m und n-Eck konstruiert werden kann, dann auch das mn-Eck.

Übung 3.8. Sei p eine ungerade Primzahl. Zeigen Sie, dass das regelmäßige p^2-Eck nicht konstruiert werden kann.

Lösung der vorstehenden Übungsaufgabe

Satz 3.9. *Sei $p > 2$ eine Primzahl. Dann ist das reguläre p^2-Eck nicht mit Zirkel und Lineal konstruierbar.*

Beweis. Damit eine Zahl (bzw. ein Punkt) konstruierbar ist, muß sie in einer Körpererweiterungen über $\mathbb{Q}$ liegen, die den Grad 2^i hat (notwendiges Kriterium; für hinreichend benötigtman noch, dass diese Körpererweiterung als eine Kette von jeweils quadratischen Erweiterungen dargestellt werden kann.)
Es reicht also zu zeigen, dass $\zeta = e^{2\pi i/p^2}$ niemals in einer Körpererweiterung vom Grad 2^i liegt.
ζ ist Nullstelle des Polynoms $z^{p^2} - 1$. Dieses kann zerlegt werden in $z^{p^2} - 1 = (z^p - 1)(z^{p(p-1)} + z^{p(p-2)} + \cdots + z^{2p} + z^p + 1)$. Wir zeigen, dass $f(z) = z^{p(p-1)} + z^{p(p-2)} + \cdots + z^{2p} + z^p + 1$ über $\mathbb{Q}$ irreduzibel ist. Dann ist klar, dass f das Minimalpolynom von ζ ist. Der Körpererweiterungsgrad ist damit $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p(p-1)$, also keine Zweierpotenz. (betrachtet man den Erweiterungsgrad für den Kosinus- bzw. Sinuswert von $2\pi/p^2$, so entspricht das einer rellen (nicht komplexen) Körpererweiterung von $\mathbb{Q}$ vom Grad $p(p-1)/2$.)

Lemma 3.1. $f(z) = z^{p(p-1)} + z^{p(p-2)} + \cdots + z^{2p} + z^p + 1$ *ist irreduzibel über* $\mathbb{Q}$.

Wir verwenden hierzu:
a) Ein Polynom das über $\mathbb{Z}$ irreduzibel ist, ist auch über $\mathbb{Q}$ irreduzibel. (Lemma von Gauß.)
b) Den Satz von Eisenstein.

Satz 3.10 (Eisensteinsches Irreduzibilitätskriterium). *Sei $g \in \mathbb{Z}[x]$ ein Polynom mit $g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Weiter sei p eine Primzahl. Wenn die folgenden Bedingungen erfüllt sind*

$$\begin{aligned} i) &\quad a_n \not\equiv 0 \bmod p \\ ii) &\quad a_i \equiv 0 \bmod p \text{ für } i = 0, \cdots, n-1 \\ iii) &\quad a_0 \not\equiv 0 \bmod p^2, \end{aligned}$$

dann ist g irreduzibel über $\mathbb{Q}$. (Dies ist ein hinreichendes, aber kein notwendiges Kriterium.)

Ein Beweis des Gaußschen Lemmas und des Satzes von Eisenstein steht z.B. in Stewart, Galoistheory.

Beweis (des Lemmas). Wir substituieren $z = t+1$. Es ist wegen des kleinen Satzes von Fermat $(t+1)^p \equiv (t+1) \equiv (t^p+1) \bmod p$. Daher ist

$$\begin{aligned}
f(z) &= (t+1)^{p(p-1)} + (t+1)^{p(p-2)} + \cdots + (t+1)^2p + (t+1)^p + 1 \\
&\equiv (t^p+1)^{p-1} + (t^p+1)^{p-2} + \cdots + (t^p+1)^2 + (t^p+1)^1 + 1 \bmod p \\
&\equiv \sum_{i=0}^{p-1} \sum_{j=0}^{i} \binom{i}{j} t^{pj} \bmod p \\
&\equiv \sum_{j=0}^{p-1} t^{pj} \sum_{i=j}^{p-1} \binom{i}{j} \bmod p \\
&\equiv \sum_{j=0}^{p-1} t^{pj} \binom{p}{j+1} \bmod p
\end{aligned}$$

Die Binomialkoeffizienten $\binom{p}{i}$ sind für $1 \le i \le p-1$ durch p teilbar (Produktdarstellung von $\dfrac{p!}{(p-i)!i!}$ beachten.)
Daher sind die Bedingungen i) und ii) erfüllt. Wegen $a_0 = p$ ist auch iii) erfüllt.
Bsp: für $p = 5$:
$1+(1+x)^5+(1+x)^{10}+(1+x)^{15}+(1+x)^{20} = (5+50x+350x^2+1725x^3+6425x^4+18760x^5+43975x^6+84075x^7+132450x^8+172975x^9+187760x^{10}+169325x^{11}+126425x^{12}+77625x^{13}+38775x^{14}+15505x^{15}+4845x^{16}+1140x^{17}+190x^{18}+20x^{19}+x^{20})$.

$$1 + (1+x)^5 + (1+x)^{10} + (1+x)^{15} + (1+x)^{20}$$

$$\begin{array}{llllll}
\equiv & 1+ & (1+x^5)+ & (1+x^5)^2+ & (1+x^5)^3+ & (1+x^5)^4 \bmod 5 \\
= & 1+ & +1 & +1 & +1 & +1 \\
 & & +x^5 & +2x^5 & +3x^5 & +4x^5 \\
 & & & +x^{10} & +3x^{10} & +6x^{10} \\
 & & & & +x^{15} & +4x^{15} \\
 & & & & & +x^{20}
\end{array}$$

$$= 5 + 10x^5 + 10x^{10} + 5x^{15} + x^{20} \bmod 5$$

Literatur:

Ian Stewart, Galois Theory, Chapman & Hall, London, Second Edition 1989. (Ein hervorragend lesbares Buch, enthält über die Galoistheorie hinaus Kapitel über die Konstruktionsprobleme, die Transzendenz von π und behandelt z.B. auch das regelmäßige 17-Eck im Detail.)

Jahrbuch Überblicke Mathematik 1976, BI Wissenschaftsverlag Mannheim, 1976. Hrsg. von Fuchssteiner, Kulisch, Laugwitz, Liedl. Darin der Aufsatz von D. Laugwitz: Unlösbarkeit geometrischer Konstruktionsaufgaben - Braucht man dazu moderne Algebra? S. 201-204.

C. Hadlock, Field Theory and its classical problems, Carus Mathematical Monographs, vol. 19, 1978.

A. Jones, S. Morris, K. Pearson, Abstract Algebra and Famous Impossibilities, Springer, 1991, New York.

D. Duncan, W. Barnier, On trisection, quintisection ... etc., American Mathematical Monthly, vol. 89, 1992, p. 693.