Konstruierbarkeit mit Zirkel und Lineal – ein Vorspiel zur Galois-Theorie

Klaus Pommerening

Oktober 1979 – Überarbeitung April 2020

Zusammenfassung

Üblicherweise werden im Rahmen eines Algebra-Kurses die elementargeometrischen Aufgaben der Konstruierbarkeit mit Zirkel und Lineal als Anwendungen der Galois-Theorie vorgestellt. An diesem Vorgehen ist im Prinzip nichts auszusetzen – es verschleiert aber, dass dieser Themenbereich viel elementarer behandelt werden kann. Umgekehrt kann er dann dazu dienen, die Galois-Theorie zu motivieren.

Diese Note führt das in drei Stufen vor[1].

Stufe 1

Hier treten Körper als Teilkörper des reellen Zahlkörpers $\mathbb{R}$ auf; der abstrakte Körperbegriff wird am Rande verwendet, ist aber nicht wirklich notwendig. Weiterhin werden aus der ebenen analytischen Geometrie die Gleichungen von Geraden und Kreisen und aus der elementaren Algebra das Lösen von quadratischen Gleichungen gebraucht.

Das Ergebnis dieser Stufe ist die Reduktion der Konstruierbarkeit auf das sukzessive Lösen von quadratischen Gleichungen.

Stufe 2

Hier werden als Methoden eingesetzt:

- einfaches Rechnen mit Polynomen,
- die Cosinus-Funktion (für die Winkeldreiteilung und die regelmäßigen Vielecke),
- die komplexen Einheitswurzeln (für die regelmäßigen Vielecke),
- nicht zwingend, aber nützlich für das Siebzehneck: die zyklische Gruppe der Ordnung 16 als multiplikative Gruppe $\mathbb{F}_{17}^{\times}$.

[1] Übungsaufgaben sind unsystematisch eingestreut.

Damit kann man als Ergebnisse die Konstruktionen des regelmäßigen Fünf- und Siebenecks herleiten sowie die Unmöglichkeitsbeweise für die Konstruktion der Würfelverdoppelung, der Winkeldreiteilung und des regelmäßigen Sieben- und Neunecks, kurz: für alle Aufgaben, die auf kubische Gleichungen führen.

Stufe 3

Hier wird etwas mehr abstrakte Algebra ins Spiel gebracht:

- Automorphismen von zyklischen Gruppen und von Körpern,
- die Körpergradformel (wird hier bewiesen),
- die Charakteristik eines Körpers (nicht wesentlich),
- die endlichen Körper $\mathbb{F}_p$,
- die Teilbarkeit von Polynomen (Divisionsalgorithmus, euklidischer Algorithmus, Irreduzibilität – die Irreduzibilität der relevanten Kreisteilungspolynome wird hier bewiesen),
- Homomorphismen, insbesondere die Substitution von Polynomen und die Koeffizientenreduktion.

Hiermit lässt sich dann die Konstruktion der regelmäßigen Vielecke befriedigend abhandeln, und die dabei auftretenden Türme von quadratischen Körpererweiterungen führen ganz zwanglos zur Grundidee der Galois-Theorie: der Korrespondenz von Zwischenkörpern und Untergruppen der Automorphismengruppe.

Ausblick

Die (moderne) Theorie der Algorithmen stellt allgemein die Frage:

> *Läßt sich ein Problem mit gegebenen Mitteln in endlich vielen Schritten lösen?*

Die überhistorische Bedeutung der klassischen Probleme „Konstruktion mit Zirkel und Lineal“ und „Auflösung von Gleichungen durch Radikale“ liegt darin, dass erstmals solche Fragen negativ entschieden werden konnten – es hat also keinen Sinn, weiterhin nach Verfahren dafür zu suchen. Diese Probleme haben daher einen exemplarischen Charakter, auch wenn sie selbst inhaltlich nicht von überragender Bedeutung sind. Allgemein scheint es ungeheuer schwer zu sein, nicht-triviale Unmöglichkeitsbeweise zu finden, man denke nur an das berühmte Problem $\mathbf{P} \stackrel{?}{=} \mathbf{NP}$.

1 Fragestellung und algebraische Beschreibung

1.1 Einleitung: Konstruierbare Größen

Objekte der Betrachtung

Unsere Objekte sind *Punkte, Geraden, Strecken, Kreise, Winkel* in der Ebene, die wir als reellen zweidimensionalen Raum $\mathbb{R}^2$ interpretieren. Wir gehen davon aus, dass die Koordinatenachsen und die Einheitslänge gegeben sind. Unsere Objekte werden sämtlich durch reelle Zahlen ausgedrückt, die auch negativ sein können und die wir als Strecken (-längen) interpretieren, siehe Abbildung 1:

Punkte werden duch zwei Koordinaten, also zwei Strecken, beschrieben.

Geraden werden duch zwei Punkte, also vier Strecken, beschrieben.

Kreise werden duch Mittelpunkt und Radius, also drei Strecken, beschrieben.

Winkel werden duch ihren Cosinus, also eine Strecke, beschrieben.

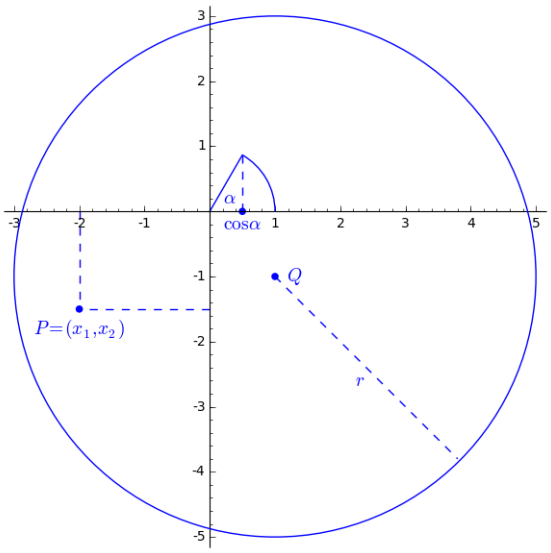

Abbildung 1: Beschreibung des Punkts P, des Kreises um Q mit Radius r und des Winkels α

Allgemeine Aufgabenstellung

Gegeben ist eine endliche Menge $M \subseteq \mathbb{R}$ von Strecken – und damit implizit

- alle Punkte, deren Koordinaten in M liegen,

- alle Geraden durch zwei solche Punkte,
- alle Kreise um solche Punkte, deren Radius auch in M liegt,
- alle Winkel, deren Cosinus in M liegt.

Die Einheitslänge wird durch $1 \in M$ repräsentiert.

Gesucht ist eine weitere Strecke x (oder mehrere) durch Konstruktion mit Zirkel und Lineal aus den gegebenen Größen, also den Elementen von M.

Beispiel: Gegeben ist ein Dreieck, also drei Punkte bzw. sechs reelle Zahlen, gesucht ist sein Schwerpunkt, siehe Abbildung 4.

Konstruktionsschritte

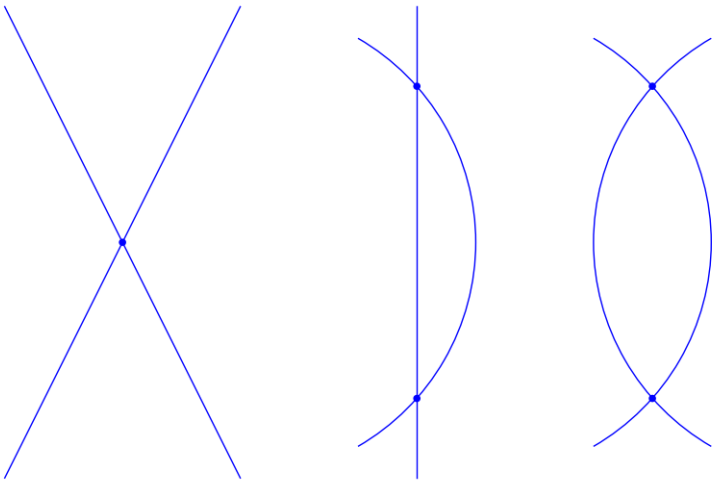

Abbildung 2: Schnitt zweier Geraden, einer Geraden mit einem Kreis und zweier Kreise

Die Konstruktion mit Zirkel und Lineal bedeutet die Ausführung von elementaren Schritten dreier Typen, siehe Abbildung 2:

1. Bestimmung des Schnittpunkts zweier Geraden,
2. Bestimmung der Schnittpunkte einer Geraden und eines Kreises,
3. Bestimmung der Schnittpunkte zweier Kreise.

Dadurch entsteht aus M eine Obermenge $M' \supseteq M$ von direkt (in einem Schritt) konstruierbaren Strecken. Da M endlich ist und somit nur endlich viele verschiedene Geraden und Kreise beschreiben kann, ist auch M' wieder endlich. Sukzessiv erhalten wir eine aufsteigende Folge von endlichen Mengen

$$M \subseteq M' \subseteq M^{(2)} \subseteq \ldots \subseteq M^{(n)} \subseteq \ldots \subseteq \mathbb{R}.$$

Definition. Eine Strecke $x \in \mathbb{R}$ heißt **aus M (mit Zirkel und Lineal) konstruierbar**, wenn es ein $n \in \mathbb{N}$ gibt mit $x \in M^{(n)}$.

Beispiel: Konstruktion des Schwerpunkts eines Dreiecks. Hier besteht M aus den Koordinaten $a_1, a_2, b_1, b_2, c_1, c_2$ der Ecken des gegebenen Dreiecks und ihren Abständen, den Seitenlängen d_1, d_2, d_3 des Dreiecks. D. h. $M = \{a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2, d_3\}$.

Schritt 1: Für jede der drei Seiten wird durch die beiden Endpunkte jeweils der Kreis geschlagen, der durch den anderen Endpunkt geht, und die beiden Schnittpunkte dieser beiden Kreise bestimmt[2]. Deren Koordinaten, also sechs Koordinatenpaare, zu M hinzugefügt, liegen in M'.

Schritt 2: Für jede der drei Seiten wird duch die beiden Kreis-Schnittpunkte die Gerade gezogen, und deren Schnittpunkte mit der jeweiligen Dreiecksseite bestimmt. Das ergibt drei neue Koordinatenpaare, die in $M^{(2)}$ liegen, siehe Abbildung 3.

Schritt 3: Wir verbinden zwei der eben bestimmten Seitenmittelpunkte mit der jeweils gegenüberliegenden Ecke durch eine Gerade und bestimmen den Schnittpunkt dieser beiden Geraden. Dessen Koordinaten $x_1, x_2 \in M^{(3)}$ sind die Lösung unserer Aufgabe, siehe Abbildung 4.

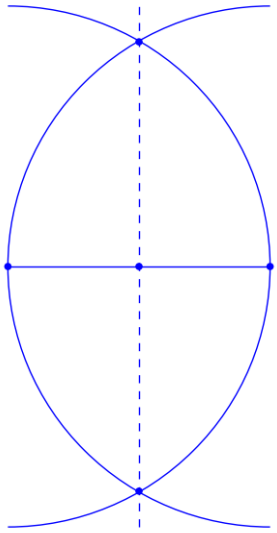

Abbildung 3: Mittelpunkt einer Strecke in zwei Schritten

[2]Die Mittelpunkte dieser Kreise haben Koordinaten in M. Die Radien sind die Seitenlängen, also auch Elemente von M. Natürlich kann man die Radien in dieser Konstruktion auch willkürlich wählen, aber das würde unser Modell unnötig verkomplizieren.

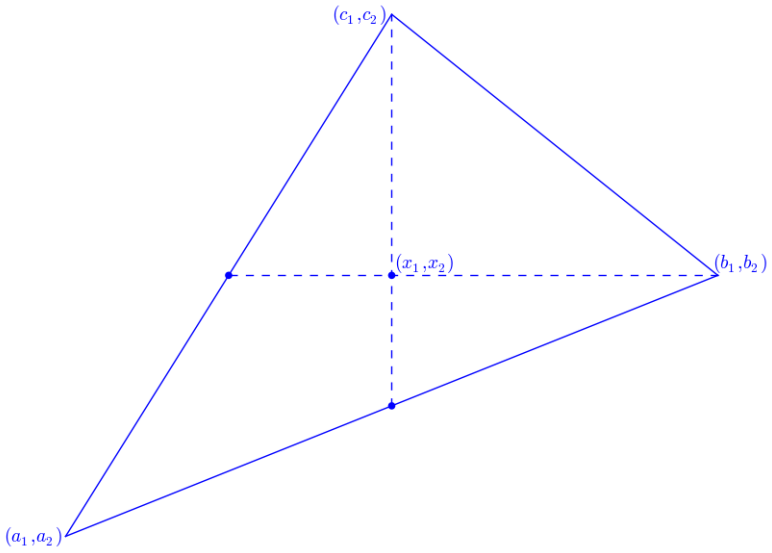

Abbildung 4: Schwerpunkt eines Dreiecks

1.2 Übergang zur Algebra

Eine endliche Menge $M \subseteq \mathbb{R}$ von reellen Zahlen sei gegeben (mit $1 \in M$). Wir bilden den Zahlkörper $K = \mathbb{Q}(M)$, den kleinsten Teilkörper von $\mathbb{R}$, der M enthält. Er besteht aus allen Zahlen, die sich rational, also durch endlich viele Operationen $+$, $-$, $\times$, $/$, aus Elementen von $\mathbb{Q}$ und M bilden lassen.

Hilfssatz 1 *Sei $x \in \mathbb{R}$.*

(i) *Ist $x \in K$, so ist x aus M konstruierbar.*

(ii) *Ist $x^2 \in K$, so ist x aus M konstruierbar.*

Beweis. Da x aus M durch endlich viele rationale Operationen und (im Fall (ii)) eine Quadratwurzel entsteht, ist für $a, b \in M$, $a \neq 0$ zu zeigen, dass $a + b$, $a - b$, $a \cdot b$, $1/a$ und $\sqrt{a}$ aus M konstruierbar sind. Das geschieht in den Abbildungen 5–8. $\diamond$

Hilfssatz 2 (i) *Jede Gerade durch zwei verschiedene Punkte $\in K^2$ hat eine Gleichung der Form*

$$ax + by = c \quad \textit{mit } a, b, c \in K,\ a, b \textit{ nicht beide } 0.$$

(ii) *Jeder Kreis um einen Punkt $\in K^2$ mit Radius $\in K$ hat eine Gleichung der Form*

$$x^2 + ax + y^2 + by = c \quad \textit{mit } a, b, c \in K.$$

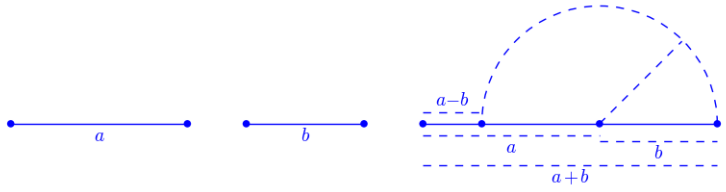

Abbildung 5: Summe und Differenz zweier Strecken

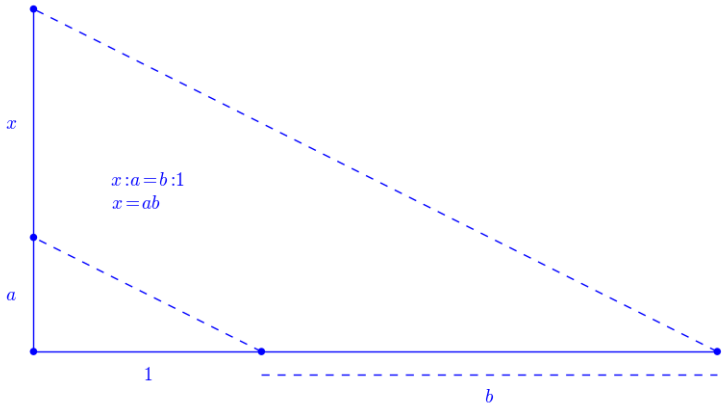

Abbildung 6: Produkt zweier Strecken (Ähnlichkeitssatz)

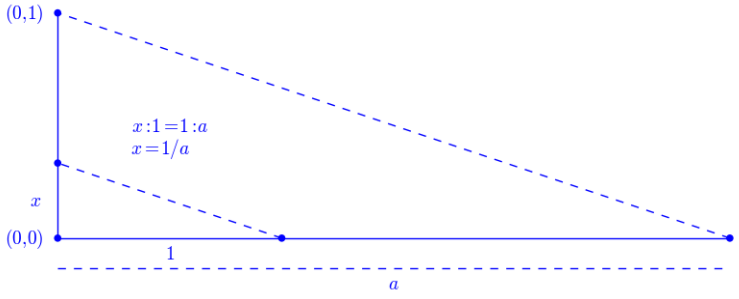

Abbildung 7: Inverses einer Strecke (Ähnlichkeitssatz)

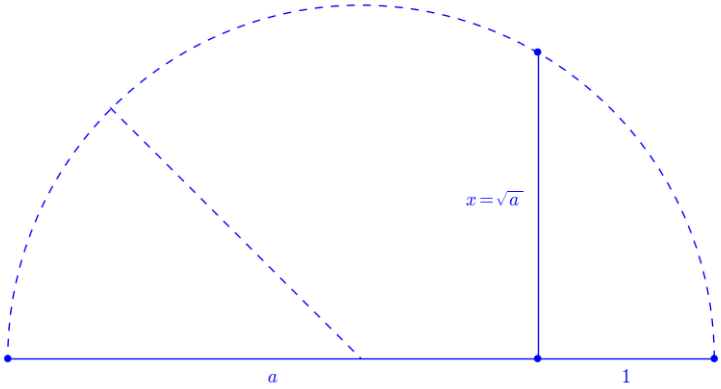

Abbildung 8: Quadratwurzel aus einer Strecke (Höhensatz)

Beweis. (i) Die Gerade durch zwei verschiedene Punkte (x_1, y_1) und $(x_2, y_2) \in K^2$ besteht genau aus den Punkten $(x, y) = (x_1, y_1) + t \cdot (x_2 - x_1, y_2 - y_1)$ mit beliebigem $t \in \mathbb{R}$. Sei etwa $x_2 \neq x_1$ (im Falle $y_2 \neq y_1$ argumentiert man analog). Dann ist $t = (x - x_1)/(x_2 - x_1)$, also

$$y = y_1 + \frac{x - x_1}{x_2 - x_1} \cdot (y_2 - y_1).$$

Die Behauptung folgt mit

$$a = y_2 - y_1, \quad b = x_2 - x_1 \neq 0, \quad c = x_1 \cdot (y_2 - y_1)\,.$$

(ii) Der Kreis um $(x_0, y_0) \in K^2$ mit Radius $r \in K$ besteht genau aus den Punkten (x, y) mit

$$(x - x_0)^2 + (y - y_0)^2 = r^2.$$

Daraus folgt die Behauptung durch die Umformung

$$x^2 - 2x_0\, x + y^2 - 2y_0\, y = -x_0^2 - y_0^2 + r^2.$$

$\diamond$

Aufgaben

1. Die Menge aller aus M konstruierbaren Zahlen (Strecken) ist ein Körper.

1.3 Quadratwurzel-Erweiterungen

Definition. Eine Körpererweiterung $L \supseteq K$ heißt **Quadratwurzel-Erweiterung**, wenn es eine Kette

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_m = L$$

von Körpern[3] und $\delta_i \in K_i$ gibt mit $\delta_i^2 \in K_{i-1}$ und $K_i = K_{i-1}(\delta_i)$ für $i = 1, \ldots, m$.

Damit können wir eine erste Fassung des Konstruierbarkeitskriteriums formulieren:

Satz 1 *Die Strecke $x \in \mathbb{R}$ ist genau dann aus der endlichen Menge $M \subseteq \mathbb{R}$ konstruierbar, wenn x Element einer Quadratwurzel-Erweiterung von $\mathbb{Q}(M)$ ist.*

Beweis. Die Richtung „$\Longleftarrow$“ folgt direkt aus Hilfssatz 1 (ii), weil x durch endlich viele Operationen $+$, $-$, $\times$, $/$ und $\sqrt{\ }$ aus M entsteht.

Für die umgekehrte Richtung „$\Longrightarrow$“ zeigen wir zu gegebenem Körper $K \subseteq \mathbb{R}$, dass jeder der elementaren Konstruktionsschritte aus 1.1 Elemente von K oder einer quadratischen Erweiterung $K(\sqrt{a})$ für ein geeignetes Element $a \in K$ liefert.

(i) Der Schnittpunkt zweier Geraden: Ihre Gleichungen seien $ax + by = c$ und $dx + ey = f$. Sie sind genau dann nicht parallel, wenn die Determinante $ae - bd \neq 0$ ist. Der Schnittpunkt ist dann

$$(x, y) = \left(\frac{ce - bf}{ae - bd}, \frac{af - cd}{ae - bd} \right) \in K^2.$$

(ii) Schnitt von Kreis (mit Gleichung $x^2 + ax + y^2 + by = c$) und Gerade (mit Gleichung $dx + ey = f$): Sei etwa $d \neq 0$. Dann folgt für jeden Schnittpunkt (x, y) aus der Geradengleichung, dass $x = (f - ey)/d$. Dieses in die Kreisgleichung eingesetzt ergibt eine quadratische Gleichung für y über K. Also gibt es (falls überhaupt Schnittpunkte existieren) ein $\delta \in \mathbb{R}$ mit $\delta^2 \in K$, und $x, y \in K(\delta)$.[4]

(iii) Der Schnitt zweier Kreise mit Gleichungen

$$\begin{aligned} x^2 + ax + y^2 + by &= c\,, \\ x^2 + dx + y^2 + ey &= f\,, \end{aligned}$$

wird durch Differenzbildung der beiden Gleichungen,

$$(a - d)\, x + (b - e)\, y = c - f\,,$$

auf den Fall (ii) zurückgeführt. $\diamond$

Wie beim Themenkreis der Auflösung von Gleichungen durch Radikale stoßen wir auch hier auf die algebraische Aufgabe, einen Überblick über mögliche Zwischenkörper zu bekommen, die im Prinzip durch die Galois-Theorie gelöst wird, hier aber viel einfacher ist.

Aufgaben

1. Bestimme eine minimale Kette von quadratischen Erweiterungen für $\sqrt{2} + \sqrt{3}$ über dem Körper $\mathbb{Q}$ der rationalen Zahlen.

[3] Wenn $\operatorname{char} K \neq 2$, könnte man auch sagen: durch eine Kette von quadratischen Erweiterungen. In Charakteristik 2 ist das etwas problematisch, aber im momentanen Kontext ohne Belang.

[4] Es könnte, z. B. aus einem früheren Konstruktionsschritt, schon $\delta \in K$ sein. Das schadet nicht.

2 Anwendung auf konkrete Konstruktionsaufgaben

2.1 Regelmäßige Vielecke

Bezeichnen wir die Aussage „das regelmäßige n-Eck ist mit Zirkel und Lineal konstruierbar“ als $\mathcal{K}(n)$, so gilt (vergleiche Abbildung 9 und Satz 1):

$$\begin{aligned} \mathcal{K}(n) &\iff x = \cos\frac{2\pi}{n} \text{ ist aus } M = \{1\} \text{ konstruierbar.} \\ &\iff x \text{ liegt in einer Quadratwurzel-Erweiterung von } \mathbb{Q}. \end{aligned}$$

Aus x gewinnt man die „erste“ Ecke des n-Ecks durch Errichtung einer Senkrechten (die Verbindung von x bis zum Schnittpunkt ζ mit dem Einheitskreis)[5]. Die übrigen Ecken erhält man, indem man die Strecke zwischen 1 und ζ so lange rund um den Kreis abträgt, bis man wieder am Anfang angelangt ist. Das bedeutet jedesmal, den Schnitt zweier Kreise zu bestimmen.

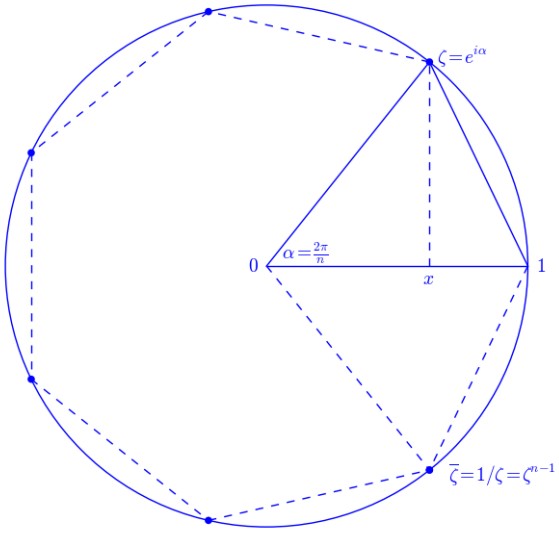

Abbildung 9: Die primitive n-te Einheitswurzel ζ und das regelmäßige n-Eck in der komplexen Ebene

Hilfssatz 1 (i) *Gilt $\mathcal{K}(n)$ und ist $m|n$ ein Teiler, so gilt auch $\mathcal{K}(m)$.*

(ii) *Sind m und n teilerfremd und gelten $\mathcal{K}(m)$ und $\mathcal{K}(n)$, so gilt auch $\mathcal{K}(mn)$.*

(iii) *Ist $n = p_1^{r_1} \cdots p_m^{r_m}$ die Primzerlegung, so gilt:*

$$\mathcal{K}(n) \iff \mathcal{K}(p_i^{r_i}) \quad \textit{für alle } i = 1, \ldots m.$$

[5]Das ist natürlich schon ein Folge mehrerer elementarer Konstruktionsschritte.

(iv) *Gilt $\mathcal{K}(n)$, so auch $\mathcal{K}(2n)$.*

(v) *$\mathcal{K}(2^r)$ für alle r.*

(vi) *$\mathcal{K}(3)$.*

Beweis. (i) Man konstruiert das n-Eck und lässt überflüssige Ecken weg.

(ii) Es gibt ganze Zahlen a und b mit $am + bn = 1$. Trägt man fortlaufend b-mal den Winkel $\alpha = 2\pi/m$ und a-mal den Winkel $\beta = 2\pi/n$ auf[6], so gelangt man zum Winkel

$$b\alpha + a\beta = \frac{2b\pi}{m} + \frac{2a\pi}{n} = \frac{2bn\pi + 2am\pi}{mn} = \frac{2\pi}{mn}\,,$$

der das mn-Eck charakterisiert.

(iii) ist eine unmittelbare Folge aus (i) und (ii).

(iv) Man halbiert den Winkel $\alpha = 2\pi/n$, indem man wie in Abbildung 3 die Verbindung von 1 und $\zeta = e^{2\pi/n}$ (in der komplexen Ebene) halbiert.

(v) folgt mit (iv) aus $\mathcal{K}(2)$ (oder $\mathcal{K}(4)$).

(vi) $\cos 2\pi/3 = -1/2$ ist sogar rational. $\diamond$

Nach Hilfssatz 1 bleiben als „Problemfälle“ nur die Eckenzahlen p^r mit einer Primzahl $p \neq 2$ und einem natürlichen Exponenten $r \geq 1$. Der erste davon ist $p = 5$, $r = 1$. Von diesem handelt der nächste Abschnitt 2.2.

2.2 Beispiel: das regelmäßige Fünfeck

Hier spielt die fünfte Einheitswurzel $\zeta = e^{2\pi i/5} \in \mathbb{C}$ die entscheidende Rolle[7]. Sie ist Nullstelle des Polynoms $X^5 - 1 = (X - 1)\,(X^4 + X^3 + X^2 + X + 1)$. Da $\zeta^5 = 1$, aber $\zeta \neq 1$ (und natürlich auch $\zeta \neq 0$), erfüllt ζ die Relation

$$(1) \qquad \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0 \quad \text{oder äquivalent} \quad \zeta^2 + \zeta + 1 + \frac{1}{\zeta} + \frac{1}{\zeta^2} = 0.$$

Ein wichtiger Zwischenschritt ist die Substitution von de Moivre[8]:

$$y = \zeta + \frac{1}{\zeta} \quad \text{also} \quad y^2 = \zeta^2 + 2 + \frac{1}{\zeta^2}.$$

Wie man in Abbildung 9 sieht, ist $y = 2x = 2\cos\alpha$, wo $\alpha = 2\pi/5$ das Argument von ζ in Polarkoordinaten ist. Aus der Relation (1) für ζ wird somit die quadratische Gleichung

$$y^2 + y - 1 = 0$$

[6] falls diese Anzahl a oder b positiv ist, geht man im positiven Sinn vorwärts, sonst umgekehrt.

[7] Wir identifizieren hier ganz zwanglos $\mathbb{C}$ mit der Ebene $\mathbb{R}^2$.

[8] Abraham de Moivre, 1667–1754

für y, die von $y = (-1 \pm \sqrt{5})/2$ erfüllt wird. Das ergibt für $x = \cos\alpha$ (das ja positiv sein muss) die Lösung

$$x = \frac{-1+\sqrt{5}}{4} = \frac{(-1+\sqrt{5})(1+\sqrt{5})}{4\,(1+\sqrt{5})} = \frac{1}{1+\sqrt{5}} \in \mathbb{Q}(\sqrt{5})\,. \tag{2}$$

Da dieser Körper eine Quadratwurzel-Erweiterung von $\mathbb{Q}$ ist, haben wir insbesondere gezeigt:

Satz 1 *Es gilt $\mathcal{K}(5)$, d. h., das regelmäßige Fünfeck ist mit Zirkel und Lineal konstruierbar.*

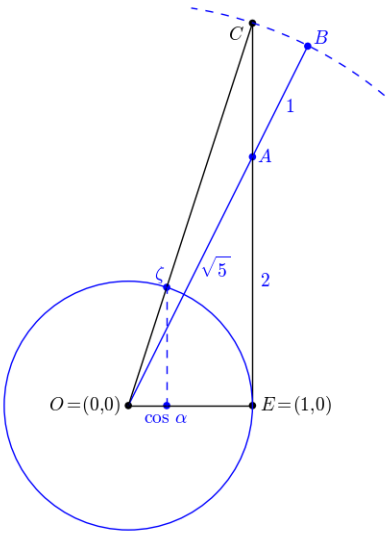

Abbildung 10: Eine Konstruktion des regelmäßigen Fünfecks

Aber die Lösungsgleichung (2) beweist nicht nur die Existenz, sondern führt auch tatsächlich zu einem expliziten Konstruktionsverfahren, siehe Abbildung 10:

1. Konstruiere das rechtwinklige Dreieck (O, E, A) mit den Katheten 1 und 2. Die Hypothenuse $\overline{OA}$ hat dann die Länge $\sqrt{5}$ nach dem Satz von Pythagoras[9].

2. Verlängere die Hypothenuse um 1, was den Punkt B ergibt.

3. Schneide den Kreis um O durch B mit der verlängerten Kathete $\overline{EA}$, was den Punkt C ergibt.

[9]Wir brauchen also nicht die etwas kompliziertere Konstruktion der Quadratwurzel aus Abbildung 8 zu bemühen.

4. Die Strecke $\overline{OC}$ hat dann wie $\overline{OB}$ die Länge $1+\sqrt{5}$, d. h., ihr Winkel mit $\overline{OE}$ hat den Cosinus $1/(1+\sqrt{5}) = x$. Ihr Schnittpunkt mit dem Einheitskreis ist also (als komplexe Zahl interpretiert) die gesuchte Einheitswurzel ζ, also die nächste Ecke des Fünfecks.

2.3 Das regelmäßige Siebzehneck

Die Konstruktion des regelmäßigen 17-Ecks wurde von Gauss 1796 im Rahmen seiner Dissertation gefunden und erregte damals ziemliches Aufsehen. Niemand hatte geglaubt, dass es über das Fünfeck hinaus noch weitere konstruierbare Vielecke (mit primer Eckenzahl) geben könnte. Die Herleitung hier ist ziemlich elementar (im Rahmen der Theorie der Einheitswurzeln), wird aber geheimnisvoll bleiben. Was wirklich passiert, werden wir später nochmal von einem höheren Standpunkt aus betrachten.

Ausgangspunkt ist die primitive 17. Einheitswurzel $\varepsilon = e^{2\pi i/17}$. Als Nullstelle $\neq 1$ des Polynoms $X^{17}-1 = (X-1)(1+X+\cdots+X^{16})$ erfüllt sie die Relation

$$1+\varepsilon+\cdots+\varepsilon^{16} = 0, \tag{3}$$

die alle siebzehn 17. Einheitswurzeln 1, ε, …, ε^{16} miteinander verbindet[10]. Die entscheidende Idee von Gauss (von ihm natürlich völlig anders ausgedrückt) war, dass die multiplikative Gruppe $G = \mathbb{F}_{17}^{\times}$ des Körpers $\mathbb{F}_{17} = \mathbb{Z}/17\mathbb{Z}$ zyklisch ist und vom Element 3 erzeugt wird, denn die sukzessiven Potenzen von 3 in $\mathbb{F}_{17}$ sind:

Exponent:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Potenz:	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Wir schreiben nun $\varepsilon_\nu := \varepsilon^{3^\nu}$ für $\nu = 0,\dots 15$, d. h., wir durchlaufen die 16 Einheitswurzeln $\neq 1$ in der Reihenfolge $\varepsilon_0,\dots,\varepsilon_{15} =$

$$\varepsilon,\ \varepsilon^3,\ \varepsilon^9,\ \varepsilon^{10},\ \varepsilon^{13},\ \varepsilon^5,\ \varepsilon^{15},\ \varepsilon^{11},\ \varepsilon^{16},\ \varepsilon^{14},\ \varepsilon^8,\ \varepsilon^7,\ \varepsilon^4,\ \varepsilon^{12},\ \varepsilon^2,\ \varepsilon^6,$$

und halten die Gleichung (3) in der Form fest, dass $\varepsilon_0+\cdots+\varepsilon_{15} = -1$. Wir bilden nun die „Gaußschen Perioden“, siehe Tabelle 1, und finden unsere gesuchte Größe $x = \cos(2\pi/17)$ unter ihnen als $2x = x_{31} = \varepsilon+\varepsilon^{16}$.

Die weiterführende Beobachtung ist nun, dass die Perioden jeder Länge „quadratisch über den Perioden der doppelten Länge“ sind. Das bedeutet dann, dass x als Periode der Länge 2 durch eine Quadratwurzel-Erweiterung von $K_0 = \mathbb{Q}$ eingefangen ist. Das gehen wir jetzt Schritt für Schritt durch.

Schritt 1: Es ist $x_{11}+x_{12} = -1$ nach (3). In dem durch eine Doppelsumme ausgedrückten Produkt

$$x_{11}\cdot x_{12} = \sum_{a\in A}\sum_{b\in B}\varepsilon^{a+b}$$

[10] und die Großmutter aller „Gaußschen Summen“ ist

$$
\begin{array}{lcll}
x_{11} & = & \varepsilon_0+\varepsilon_2+\cdots+\varepsilon_{14} & = & \varepsilon+\varepsilon^9+\varepsilon^{13}+\varepsilon^{15}+\varepsilon^{16}+\varepsilon^8+\varepsilon^4+\varepsilon^2 \\
x_{12} & = & \varepsilon_1+\varepsilon_3+\cdots+\varepsilon_{15} & = & \varepsilon^3+\varepsilon^{10}+\varepsilon^5+\varepsilon^{11}+\varepsilon^{14}+\varepsilon^7+\varepsilon^{12}+\varepsilon^6 \\
x_{21} & = & \varepsilon_0+\varepsilon_4+\varepsilon_8+\varepsilon_{12} & = & \varepsilon+\varepsilon^{13}+\varepsilon^{16}+\varepsilon^4 \\
x_{22} & = & \varepsilon_1+\varepsilon_5+\varepsilon_9+\varepsilon_{13} & = & \dots \\
x_{23} & = & \varepsilon_2+\varepsilon_6+\varepsilon_{10}+\varepsilon_{14} & = & \varepsilon^9+\varepsilon^{15}+\varepsilon^8+\varepsilon^2 \\
x_{24} & = & \varepsilon_3+\varepsilon_7+\varepsilon_{11}+\varepsilon_{15} & = & \dots \\
x_{31} & = & \varepsilon_0+\varepsilon_8 & = & \varepsilon+\varepsilon^{16} \\
\vdots & & & & \\
x_{35} & = & \varepsilon_4+\varepsilon_{12} & = & \varepsilon^{13}+\varepsilon^4 \\
\vdots & & & &
\end{array}
$$

Tabelle 1: Die Gaußschen Perioden für das Siebzehneck

treten 64 Summanden auf, und $\varepsilon^{17}=\varepsilon^0$ ist nicht dabei. Daher kommt ein Summand ε^k mindestens viermal vor (mit $1\le k\le 16$). Es kommen also in den Exponenten der Summe mindestens vier verschiedene Kombinationen

$$k=a_1+b_1=a_2+b_2=a_3+b_3=a_4+b_4 \quad \text{mit } a_i,b_i\in\mathbb{F}_{17}$$

vor. Da die Gruppe $\mathbb{F}_{17}^\times$ zyklisch von der Ordnung 16 ist, ist jeder andere Summand ein ε^{rk} mit $2\le r\le 16$. Der Exponent rk kommt aber auch mindestens viermal vor in den Kombinationen $rk=ra_i+rb_i \bmod 17$, die alle verschieden sind. (Wäre etwa $ra_1=ra_2$ im Körper $\mathbb{F}_{17}$, so auch schon $a_1=a_2$.) Das geht nur, wenn in der Summe jeder Exponent genau viermal vorkommt. Also ist

$$x_{11}\cdot x_{12}=4\cdot\sum_{s=1}^{16}\varepsilon^s=-4.$$

(Das kann man natürlich auch durch explizites Ausmultiplizieren berechnen, ohne den endlichen Körper $\mathbb{F}_{17}$ bemühen zu müssen.) Also sind x_{11} und x_{12} die beiden Nullstellen des Polynoms $X^2+X-4\in\mathbb{Q}[X]$, also

$$x_{11},x_{12} \;=\; -\frac{1}{2}\pm\sqrt{\frac{1}{4}+4} \;=\; \frac{-1\pm\sqrt{17}}{2} \;\in K_1=\mathbb{Q}(\sqrt{17}).$$

Schritt 2: Es ist $x_{21}+x_{23}=x_{11}$, und weil beim Ausmultiplizieren des Produkts $x_{21}\cdot x_{23}$ sechzehn Summanden entstehen, unter denen $\varepsilon,\dots\varepsilon^{16}$ alle vertreten sind, ist $x_{21}\cdot x_{23}=-1$. Also sind x_{21} und x_{23} die Nullstellen des Polynoms $X^2-x_{11}X-1\in K_1[X]$ und somit in einer Quadratwurzel-Erweiterung $K_2\supseteq K_1$ enthalten.

Schritt 3: Ebenso sind x_{22} und x_{24} die Nullstellen des Polynoms $X^2-x_{12}X-1$ aus $K_1[X]\subseteq K_2[X]$ und somit in einer Quadratwurzel-Erweiterung $K_3\supseteq K_2$ enthalten.

Schritt 4: Schließlich ist $x_{31}+x_{35}=x_{21}$ und

$$x_{31}\cdot x_{35}=\varepsilon^5+\varepsilon^{14}+\varepsilon^3+\varepsilon^{12}=\varepsilon_2+\varepsilon_6+\varepsilon_{10}+\varepsilon_{14}=x_{22},$$

also sind x_{31} und x_{35} die Nullstellen des Polynoms $X^2 - x_{21}X + x_{22} \in K_3[X]$ und somit in einer Quadratwurzel-Erweiterung $K_4 \supseteq K_3$ enthalten.

Also liegt $x = x_{31}/2$ in der Quadratwurzel-Erweiterung K_4 von $\mathbb{Q}$, und damit ist bewiesen:

Satz 2 *Es gilt $\mathcal{K}(17)$, d. h., das regelmäßige Siebzehneck ist mit Zirkel und Lineal konstruierbar.*

Bemerkungen

1. Neben DE MOIVRE hatte auch COTES[11] sich vor GAUSS mit der „Kreisteilungsgleichung“ $x^{n-1} + \cdots + 1 = 0$ befasst und bemerkt, dass sie sich durch die Substitution $y = x + 1/x$ auf eine Gleichung vom Grad $(n-1)/2$ reduziert (bei ungeradem n).

2. Die moderne Sicht[12] auf die Gaußschen Perioden für die n-ten Einheitswurzeln wird die Untergruppen H der Gruppe $G = (\mathbb{F}/n\mathbb{F})^\times$ und ihre Nebenklassen $aH \in G/H$ für $a \in G$ in den Fokus rücken. Die zugehörigen Gaußschen Perioden haben dann die Form
$$\sum_{\nu \in aH} \varepsilon^\nu.$$

Aufgaben

1. Was wird bei der Substitution $y = x+1/x$ aus einer Kreisteilungsgleichung geraden Grades?

2. Finde mit Hilfe der Gaußschen Perioden Ausdrücke für die 5. Einheitswurzeln durch Quadratwurzeln.

3. Finde mit Hilfe der Gaußschen Perioden Ausdrücke für die 7. Einheitswurzeln durch Quadrat- und Kubikwurzeln.

2.4 Weitere Konstruktionsprobleme

Würfelverdoppelung

Gegeben ist ein (dreidimensionaler) Würfel der Kantenlänge 1, der also auch das Volumen 1 hat.

Gesucht ist ein Würfel vom Volumen 2; genauer gesagt, soll seine Kantenlänge x konstruiert werden. Sie erfüllt die Gleichung

$$x^3 = 2. \tag{4}$$

[11] Roger Cotes, 1682–1716

[12] die die Galois-Theorie im Spezialfall vorwegnimmt

Winkeldreiteilung

Gegeben ist der Winkel α.

Gesucht der Winkel $\beta = \alpha/3$. Aus der elementaren Trigonometrie ist die Beziehung

$$\underbrace{\cos\alpha}_{a} = 4\,\cos^3\beta - 3\,\underbrace{\cos\beta}_{x}$$

bekannt, also $4\,x^3 - 3x - a = 0$, oder für $y = 2x$ über $\mathbb{Q}(a)$:

$$y^3 - 3y - 2a = 0. \tag{5}$$

Insbesondere für den Winkel $\alpha = 60^\circ$ ist $2a = 2\cos\alpha = 1 \in \mathbb{Z}$, für den Winkel $\alpha = 120^\circ$ ist $2a = 2\cos\alpha = -1 \in \mathbb{Z}$.

Konstruktion des Neunecks

Hier ist der Winkel $360^\circ/9 = 40^\circ$ zu konstruieren. Das ist äquivalent zur Dreiteilung des Winkels $\alpha = 120^\circ$ mit $\cos\alpha = -1/2$.

Konstruktion des Siebenecks

Hier spielt die siebte Einheitswurzel $\zeta = e^{2\pi i/7}$ die Hauptrolle. Auf die Gleichung

$$\zeta^3 + \zeta^2 + \zeta + 1 + \frac{1}{\zeta} + \frac{1}{\zeta^2} + \frac{1}{\zeta^3} = 0$$

wird die de-Moivresche Transformation $y = 2x = \zeta + \frac{1}{\zeta}$ angewendet. Da

$$y^3 = \zeta^3 + 3\zeta + \frac{3}{\zeta} + \frac{1}{\zeta^3}\,, \quad y^2 = \zeta^2 + 2 + \frac{1}{\zeta^2}\,,$$

ergibt sich für y als zu lösende Gleichung

$$y^3 + y^2 - 2y - 1 = 0. \tag{6}$$

Alle diese Konstruktionsaufgaben führen also auf Gleichungen dritten Grades und werden durch den folgenden Satz 3 erledigt.

Quadratur des Kreises

Gegeben ist der Einheitskreis. Seine Fläche ist π.

Gesucht ist ein Quadrat der Fläche π. Seine Seitenlänge ist also $\sqrt{\pi}$. Sie wäre genau dann konstruierbar, wenn π konstruierbar wäre. Da π aber transzendent ist (was hier nicht bewiesen wird), also überhaupt keiner Polynomgleichung über $\mathbb{Q}$ genügt, ist das nicht der Fall.

2.5 Gleichungen dritten Grades

Die Unmöglichkeit von Konstruktionsproblemen, die auf Gleichungen dritten Grades führen, wird durch den folgenden Satz gesichert, dessen elementarar Beweis in dieser Form auf LANDAU[13] 1897 zurückgeht. Verwendet wird, dass für eine einfache Quadratwurzel-Erweiterung $K \subseteq K(\delta)$ die Abbildung $a + b\delta \mapsto a - b\delta$ ein Automorphismus von L ist.

Satz 3 *Sei $K \subseteq \mathbb{R}$ ein Teilkörper. Das Polynom*

$$f = X^3 + a\,X^2 + bX + c \;\in K[X]$$

habe keine Nullstelle in K. Dann gibt es keine Quadratwurzel-Erweiterung von K, in der f eine Nullstelle hat.

Beweis. Angenommen doch. Sei dann

$$K = K_0 \subset K_1 \subset \ldots \subset K_m$$

eine Kette von echten einfachen Quadratwurzel-Erweiterungen mit minimalem m, so dass K_m eine Nullstelle x von f enthält. Da f keine Nullstelle in K_0 hat, ist $m \geq 1$. Sei $K_m = K_{m-1}(\sqrt{r})$ mit $r \in K_{m-1}$.

Sei σ der nicht-triviale Automorphismus $u + v\sqrt{r} \mapsto u - v\sqrt{r}$ von K_m über K_{m-1}. Dann ist

$$f(\sigma x) = (\sigma x)^3 + a\,(\sigma x)^2 + b\,(\sigma x) + c = \sigma f(x) = 0.$$

Ist $x = p + q\sqrt{r}$ mit $p, q \in K_{m-1}$, $q \neq 0$, so ist $\sigma x = p - q\sqrt{r} \neq x$. Die Summe der drei Nullstellen von f ist $-a$, also ist die dritte Nullstelle

$$y = -a - x - \sigma x = a - 2p.$$

Diese liegt aber in K_{m-1}, Widerspruch. $\diamond$

Anmerkung. Etwas mehr Körpertheorie vorausgesetzt, siehe Abschnitt 3.3, verkürzt sich das Argument so: Der Grad von K_m über K ist eine Zweierpotenz, also auch der Grad von K_m über K_{m-1}. Daher kann ein über K_{m-1} irreduzibles Polynom vom Grad 3 in K_m keine Nullstelle haben.

Korollar 1 *Die Würfelverdoppelung mit Zirkel und Lineal ist unmöglich.*

Beweis. Die reelle dritte Wurzel $\sqrt[3]{2}$ ist nicht rational, erst recht nicht die beiden nichtreellen dritten Wurzeln aus 2. $\diamond$

Für die beiden übrigen Probleme, Winkeldreiteilung und Siebeneck, ziehen wir noch einen weiteren Satz hinzu.

[13] Edmund Landau, 1877–1938

Satz 4 *Sei $f = X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$ ein normiertes ganzzahliges Polynom mit $n \geq 1$. Dann liegt jede rationale Nullstelle $x \in \mathbb{Q}$ von f schon in $\mathbb{Z}$ und ist Teiler von a_n.*

Beweis. Sei $x = p/q$ mit teilerfremden ganzen Zahlen $p, q \in \mathbb{Z}$. Dann gilt

$$\left(\frac{p}{q}\right)^n + a_1 \left(\frac{p}{q}\right)^{n-1} + \cdots + a_n = 0\,,$$

$$p^n + a_1 p^{n-1} q + \cdots + a_n q^n = 0\,,$$

$$q \cdot (a_1 p^{n-1} + \cdots + a_n q^{n-1}) = -p^n.$$

Wegen der Teilerfremdheit folgt $q = \pm 1$. Da dann

$$p \cdot (p^{n-1} \pm a_1 p^{n-2} q \pm \cdots) = \pm a_n,$$

folgt $x = \pm p | a_n$. $\diamond$

Korollar 2 *Die Winkel $60°$ und $120°$ sind nicht mit Zirkel und Lineal dreiteilbar.*

Beweis. Hätten die Polynome $Y^3 - 3Y \pm 1$ rationale Nullstellen, so könnten das nach Satz 4 nur die ganzen Zahlen ± 1 sein. Diese sind aber keine Nullstellen. Nach Satz 3 gibt es daher auch in keiner Quadratwurzel-Erweiterung von $\mathbb{Q}$ eine Nullstelle. $\diamond$

Korollar 3 *Das regelmäßige Neuneck ist nicht mit Zirkel und Lineal konstruierbar.*

Beweis. Sonst wäre der Winkel $120°$ dreiteilbar. $\diamond$

Korollar 4 *Das regelmäßige Siebeneck ist nicht mit Zirkel und Lineal konstruierbar.*

Beweis. Für das Polynom $Y^3 + Y^2 - 2Y - 1$ gilt das gleiche Argument wie bei Korollar 2. $\diamond$

Aufgaben

1. Warum sind $\sqrt[3]{3}$ und $\sqrt[3]{4}$ nicht konstruierbar? Verallgemeinerung?
2. Welche Winkel sind dreiteilbar? Finde unendlich viele Winkel mit rationalem Cosinus, die nicht dreiteilbar sind.
3. Finde einen Winkel, der nicht fünfgeteilt werden kann.
4. Für $n \in \mathbb{N}$ ist der Winkel $n°$ genau dann konstruierbar, wenn $3|n$.

5. Drücke mit Hilfe der Gaußschen Perioden für das Siebeneck die siebten Einheitswurzeln durch Quadrat- und Kubikwurzeln aus.

6. Zeige, dass das regelmäßige Elfeck nicht konstruierbar ist.

7. Verallgemeinere die Überlegungen der beiden vorangehenden Aufgaben zu einem Kriterium für Konstruktionsprobleme, die auf Gleichungen fünften Grades führen.

2.6 Historische Bemerkungen

1. Carl Friedrich Gauss (1777–1855) fand die Konstruktionsmöglichkeit des regelmäßigen Siebzehnecks 1796 (als 18-Jähriger) und verallgemeinerte dies zu einer gründlichen Untersuchung der Einheitswurzeln („Kreisteilung“), die in

   C. F. Gauss: *Disquisitiones arithmeticae*. Fleischer, Leipzig 1801.

   veröffentlicht wurde (in lateinisch) und als grundlegendes Werk der Zahlentheorie gilt. Er formulierte darin auch die notwendige und hinreichende Bedingung für die Konstruierbarkeit des regelmäßigen n-Ecks allgemein, bewies strenggenommen aber nur die Notwendigkeit dieser Bedingung.

2. Der vollständige Beweis findet sich erstmals bei Pierre Wantzel (1814–1848):

   P. Wantzel: Recherches sur les moyens de reconnaître si un problème de géométrie peut se resoudre avec la règle et le compas. J. Math. Pures Appl. 2 (1837), 366–372.

   Hier gab er ebenfalls die Beweise für die Winkeldreiteilung und die Würfelverdoppelung.

3. Edmund Landau (1877–1938) formulierte 1897 den einfachen elementaren Trick aus Satz 3 für Gleichungen dritten Grades; erstmals veröffentlicht wurde er in

   H. Weber, J. Wellstein: *Encyklopädie der Elementar-Mathematik I – Elementare Algebra und Analysis*. Teubner, Leipzig 1903.

3 Einordnung in die Galois-Theorie

3.1 Grundidee: Permutation der Nullstellen

Lagrange[14] brachte die Frage nach der Auflösung von Polynomgleichungen einen entscheidenden Schritt weiter durch die Idee, Permutationen der Nullstellen zu studieren und daraus Hilfsgrößen zu gewinnen, die bei der Auflösung helfen. Sinngemäß:

> Permutiere die Nullstellen und finde Ausdrücke, die bei einigen, aber nicht bei allen Permutationen invariant sind.

[14] Joseph-Louis Lagrange, 1736–1813; in Turin als Giuseppe Lodovico Lagrangia geboren

Er publizierte diese Idee und daraus folgende Lösungsansätze in:

> J. L. LAGRANGE: *Réflexions sur la résolution algébrique des equations.* Nouveaux Mémoires de l'Academie royale des Sciences et Belles-Lettres de Berlin, années 1770 et 1771.

Auch andere Mathematiker wie VANDERMONDE[15] verfolgten in dieser Zeit ähnliche Ideen, drangen aber nicht so tief in die Materie ein wie LAGRANGE.

3.2 Die Gaußschen Perioden als Invarianten

LAGRANGE kannte die Gaußschen Perioden natürlich noch nicht. Ob GAUSS umgekehrt die Schrift von LAGRANGE 1796 schon kannte, ist unklar[16]; er könnte seinen Ansatz auch unabhängig intuitiv entwickelt haben.

In der Bezeichnung von Tabelle 1 betrachten wir als Beispiel die Periode

$$x_{21} = \varepsilon + \varepsilon^{13} + \varepsilon^{16} + \varepsilon^4.$$

Die zyklische Gruppe der 17. Einheitswurzeln wird von jedem ihrer Elemente außer 1 erzeugt. Jede Zuordnung $\varepsilon \mapsto \varepsilon^r$ für $r = 1, \ldots, 16$ erzeugt also einen Automorphismus σ_r dieser Gruppe durch $\varepsilon^j \mapsto \varepsilon^{rj}$. Speziell σ_2 schickt x_{21} nach

$$\varepsilon^2 + \varepsilon^9 + \varepsilon^{15} + \varepsilon^8 = x_{23}\,,$$

und σ_4 bewirkt

$$x_{21} \mapsto \varepsilon^4 + \varepsilon + \varepsilon^{13} + \varepsilon^{16} = x_{21}\,,$$

lässt x_{21} also invariant. Ähnlich sind auch die anderen Perioden „teilweise invariant", d. h. unter einer Untergruppe. Diese Untergruppen kennen wir alle:

Hilfssatz 1 *Sei $G = \langle g \rangle$ eine endliche zyklische Gruppe mit erzeugendem Element g und von der Ordnung $\#G = n$. Dann ist jede Untergruppe $H \leq G$ zyklisch, und zwar $H = \langle g^d \rangle$ für $d = n/\#H$.*

Beweis. Sei $d \geq 1$ minimal mit $g^d \in H$. Ist nun $h = g^s \in H$ ein beliebiges Element von H, so liefert die Division mit Rest $s = qd + r$ mit $0 \leq r < d$. Dann ist

$$g^r = g^{s-qd} = g^s\,(g^d)^{-q} \in H.$$

Wegen der Minimalität von d muss $r = 0$ sein, und $h \in \langle g^d \rangle$. $\diamond$

Damit konstruieren wir einen Turm von Körpererweiterungen[17]:

[15] Alexandre-Théophile Vandermonde, 1735–1796

[16] Immerhin war Lagrange ja an der Akademie in Berlin tätig.

[17] in der Ausdrucksweise des nächsten Abschnitts 3.3 jeweils vom Grad 2

Grad	Untergruppe	Körper
16	$\mathbf{1}$	$\mathbb{Q}(\varepsilon)$
|	|	|
8	$\langle\sigma^8\rangle$	$\mathbb{Q}(x_{31},\ldots,x_{38})$
|	|	|
4	$\langle\sigma^4\rangle$	$\mathbb{Q}(x_{21},x_{22},x_{23},x_{24})$
|	|	|
2	$\langle\sigma^2\rangle$	$\mathbb{Q}(x_{11},x_{12})$
|	|	|
1	G	$\mathbb{Q}$

Die Einheitswurzeln $\varepsilon,\ldots,\varepsilon^{16}$ bilden eine Vektorraum-Basis von $\mathbb{Q}(\varepsilon)$ über $\mathbb{Q}$, und die σ_j, $j=1,\ldots,16$, lassen sich zu Körperautomorphismen von $\mathbb{Q}(\varepsilon)$ über $\mathbb{Q}$ fortsetzen, die $\mathbb{Q}$ elementweise festlassen. Durch die Gaußsche Nummerierung $\varepsilon_\nu=\varepsilon^{3^\nu}$ für $\nu=0,\ldots 15$ wird die Basis umgeordnet, und der Automorphismus σ_8 bewirkt[18]:

$$\varepsilon\mapsto\varepsilon^{16},\quad\text{also }\varepsilon_0\mapsto\varepsilon_8,\quad\text{allgemein }\varepsilon_\nu\mapsto\varepsilon_{\nu+8}\,.$$

Für ein beliebiges Element x des Körpers $\mathbb{Q}(\varepsilon)$ gilt also

$$x=\sum_{\nu=0}^{15}a_\nu\varepsilon_\nu\ \overset{\sigma_8}{\mapsto}\ \sum_{\nu=0}^{15}a_\nu\varepsilon_{\nu+8}\,.$$

Daran erkennen wir, wann x unter σ_8 invariant ist:

$$\begin{aligned}\sigma_8x=x\ &\iff\ a_\nu=a_{\nu+8}\quad\text{für }\nu=0,\ldots,7\\ &\iff\ x\text{ Linearkombination von }x_{31},\ldots,x_{38}\,.\end{aligned}$$

Der Körper $\mathbb{Q}(x_{31},\ldots,x_{38})$ besteht also genau aus den Invarianten der Untergruppe $\langle\sigma^8\rangle$. Genauso besteht auf jeder Etage des Turms der Körper in der rechten Spalte genau aus den Invarianten der Untergruppe in der mittleren Spalte.

Damit ist die Bildung der Gaußschen Perioden aus der Sicht der (historisch später entwickelten) Körpertheorie geklärt.

Aufgaben

1. Beschreibe jede Etage des Erweiterungs-Turms von $\mathbb{Q}(\varepsilon)\supseteq\mathbb{Q}$ durch die Adjunktion einer Quadratwurzel.

3.3 Ausflug: Die Körpergradformel

Eines der einfachsten Ergebnisse der Körpertheorie ist die Körpergradformel. Sie wird uns dabei helfen, die Konstruierbarkeit allgemeinerer regelmäßiger Vielecke zu untersuchen. Sie wurde in dieser Form von DEDEKIND[19] in die Algebra eingeführt. Ist $L\supseteq K$ ein

[18] Die von Gauß intuitiv aufgespürte versteckte Symmetrie der Einheitswurzeln wird also durch die Gruppenoperation leicht verständlich.

[19] Julius Wilhelm Richard Dedekind, 1831–1916

Erweiterungskörper, so ist er auf natürliche Weise ein Vektorraum über K und hat als solcher eine Dimension $\mathrm{Dim}_K L$, die in diesem Kontext auch als Körpergrad bezeichnet wird.

Satz 1 *Seien $M \supseteq L \supseteq K$ Körper. Dann ist*

$$\mathrm{Dim}_K M = \mathrm{Dim}_L M \times \mathrm{Dim}_K L.$$

Beweis. Sei $\{x_i \mid i \in I\}$ eine K-Basis von L und $\{y_j \mid j \in J\}$ eine L-Basis von M. Wir müssen nur zeigen dass

$$\{x_i y_j \mid i \in I, j \in J\}$$

eine K-Basis von M ist.

Sei $z \in M$. Dann ist

$$\begin{aligned} z &= \sum_{j \in J} b_j y_j \quad \text{mit } b_j \in L, \text{ fast alle } b_j = 0, \\ b_j &= \sum_{i \in I} a_{ij} x_i \quad \text{mit } a_{ij} \in K, \text{ fast alle } a_{ij} = 0, \\ z &= \sum_{i \in I, j \in J} a_{ij} x_i y_j, \end{aligned}$$

wobei nur endlich viele Koeffizienten $\neq 0$ sind.

Nun ist noch die lineare Unabhängigkeit zu zeigen. Sei

$$0 = \sum_{i \in I, j \in J} c_{ij} x_i y_j \quad \text{mit } c_{ij} \in K, \text{ fast alle } c_{ij} = 0.$$

Da die y_j linear unabhängig über L sind, folgt $\sum_{i \in I} c_{ij} x_i = 0$ für alle $j \in J$, und weil die x_i linear unabhängig über K sind, weiter $c_{ij} = 0$ für alle $i \in I$ und alle $j \in J$. $\diamond$

Anmerkung. Aus heutiger Sicht ist dieser Satz eine Trivialität. Im 19. Jahrhundert war aber die lineare Algebra nicht so geläufiges mathematisches Grundwissen.

Korollar 1 *Sei $L \supseteq K$ ein Erweiterungskörper von Primzahlgrad. Dann gibt es keinen echten Zwischenkörper.*

Korollar 2 *Sei $L \supseteq K$ eine einfache Quadratwurzel-Erweiterung, also $L = K(\delta)$ mit $\delta \notin K$, $\delta^2 \in K$. Dann ist der Grad $\mathrm{Dim}_K L = 2$. Falls $\mathrm{char}\, K \neq 2$, gilt auch umgekehrt: Ist $\mathrm{Dim}_K L = 2$, so $L \supseteq K$ eine einfache Quadratwurzel-Erweiterung.*

Beweis. Die Menge L' aller Elemente der Form $a + b\delta$ ist unter Addition, Multiplikation und Inversenbildung abgeschlossen, also ein Körper zwischen K und L. Da $\delta \notin K$ und es keinen echten Zwischenkörper gibt, ist $L' = L$.

Für die Umkehrung wählen wir ein beliebiges $\gamma \in L$, $\gamma \notin K$. Dann ist $L = K(\gamma)$ (da es keine echten Zwischenkörper gibt), und $1, \gamma, \gamma^2$ sind linear abhängig über K. Es gibt also eine Linearkombination $a\gamma^2 + b\gamma + c = 0$ mit $a, b, c \in K$, $a \neq 0$, o. B. d. A. $a = 1$. Dann ist[20] $\delta := \gamma + b/2 \in L$, $\delta \notin K$, $L = K(\delta)$, $\delta^2 = \gamma^2 + b\gamma + b^2/4 = b^2/4 - c \in K$. $\diamond$

Damit können wir das Konstruierbarkeitskriterium Satz 1 aus Abschnitt 1.3 in einer zweiten Fassung formulieren:

Korollar 3 *Die Strecke $x \in \mathbb{R}$ ist genau dann aus der endlichen Menge $M \subseteq \mathbb{R}$ konstruierbar, wenn es eine Kette*

$$K = \mathbb{Q}(M) = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_m = L$$

von Körpern gibt mit $x \in L$ und $\mathrm{Dim}_{K_{i-1}} K_i = 2$ für alle $i = 1, \ldots, m$.

3.4 Ausflug: Irreduzible Polynome

Von der Theorie der Minimalpolynome brauchen wir auch nur einen ganz kleinen Ausschnitt:

Satz 2 *Sei $L \supseteq K$ eine Körpererweiterung, und das Element $x \in L$ sei Nullstelle eines irreduziblen Polynoms $f \in K[X]$. Dann ist $\mathrm{Dim}_K K(x) = \mathrm{Grad}\, f$.*

Beweis. Sei o. B. d. A. f normiert, $f = X^n + a_1 X^{n-1} + \cdots + a_n$. Dann ist

$$x^n = -a_1 x^{n-1} - \cdots - a_n x^0 \in \sum_{i=0}^{n-1} K x^i =: M.$$

Die beim Ausmultiplizieren von Summen und Produkten von Elementen aus M auftretenden Potenzen von x lassen sich durch diese Formel alle auf Linearkombinationen der $(\leq n-1)$-ten Potenzen reduzieren. Also ist $M \supseteq K$ ein Erweiterungskörper vom Grad $\mathrm{Dim}_K M \leq n$, und $M = K(x)$.

Wäre nun $\mathrm{Dim}_K M < n$, so gäbe es eine K-Linearkombination von $1, \ldots, x^{n-1}$ mit Wert 0, also ein Polynom $g \in K[X]$ mit Grad $< n$ und $g(x) = 0$. Damit wäre der größte gemeinsame Teiler h von g und f ein nicht-konstanter Teiler von f von echt kleinerem Grad (siehe die folgende Bemerkung), im Widerspruch zur Irreduzibilität. $\diamond$

Bemerkungen

1. Beim Beweis des Satzes haben wir die Teilbarkeitslehre von Polynomen verwendet, insbesondere (implizit) den euklidischen Algorithmus. Aus diesem folgt nämlich: Sind $f, g \in K[X]$ teilerfremde Polynome, so sind sie auch über L, also im Polynomring $L[X]$ teilerfremd.

[20] Hier geht $\mathrm{char}\, K \neq 2$ ein.

2. Man kann Satz 2 auch so interpretieren, dass der Substitutionshomomorphismus $K[X] \longrightarrow L$, $X \mapsto x$, einen Isomorphismus $K[X]/fK[X] \longrightarrow K(x)$ der Körper induziert.

3. Die bekannte Aussage

   Ist $a \in K$ Nullstelle eines Polynoms $f \in K[X]$, so ist das lineare Polynom $X - a$ Teiler von f.

   kann man übrigens viel einfacher beweisen, ohne die Polynomdivision bemühen zu müssen:

Beweis. Dazu betrachten wir den Substitutionshomomorphismus $\tau_a : K[X] \longrightarrow K[X]$, $X \mapsto X + a$. Da $\tau_a f(0) = f(a) = 0$, ist das absolute Glied von $\tau_a f$ Null, also $X | \tau_a f$. Also $X - a = \tau_a^{-1} X \mid f$. $\diamond$

3.5 Ausflug: Ganzzahlige Polynome

Im nächsten Abschnitt 3.6 benötigen wir ein klassisches Irreduzibilitätskriterium für Polynome über $\mathbb{Q}$. Dies wird hier mit Minimalaufwand hergeleitet. Als Hilfergebnis dient die einfachste Version des sogenannten Lemmas von Gauss:

Hilfssatz 2 *Das normierte ganzzahlige Polynom $f \in \mathbb{Z}[X]$ zerfalle in $\mathbb{Q}[X]$ in zwei normierte Polynome $f = gh$ mit $g, h \in \mathbb{Q}[X]$. Dann sind g und h ganzzahlig, $g, h \in \mathbb{Z}[X]$.*

Beweis. Sei $d \in \mathbb{Z}$ der Hauptnenner von g, also $d > 0$ minimal mit $dg \in \mathbb{Z}[X]$. Ebenso sei $e \in \mathbb{Z}$ der Hauptnenner von h. Dann ist $def = (dg)(eh)$ eine Produktzerlegung in $\mathbb{Z}[X]$.

Angenommen, $de > 1$. Dann gibt es eine Primzahl $p | de$. Die Reduktion der Koeffizienten induziert einen Ringhomomorphismus

$$\rho : \mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X] \,.$$

und $0 = \rho(def) = \rho(dg)\,\rho(eh)$. Also muss einer der beiden Faktoren 0 sein, etwa $\rho(dg) = 0$. Das bedeutet aber, dass p alle Koeffizienten von dg teilt. Daher ist auch schon $\frac{d}{p}\, g$ ganzzahlig, im Widerspruch zur Minimalität von d. $\diamond$

Daraus leiten wir das sogenannt Eisensteinsche Irreduzibilitätskriterium ab, das erstmals von Schönemann formuliert und bewiesen wurde:

Satz 3 *Sei $f = X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$. Es gebe eine Primzahl p mit $p | a_1, \ldots, a_n$, aber $p^2 \nmid a_n$. Dann ist f in $\mathbb{Q}[X]$ irreduzibel.*

Beweis. Wenn f zerlegbar ist, können wir es nach Hilfssatz 2 als $f = gh$ schreiben mit normierten

$$g = X^l + \cdots b_l,\ h = X^m + \cdots c_m \in \mathbb{Z}[X].$$

Wir verwenden wieder den Ringhomomorphismus $\rho : \mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X]$. Dann ist $X^n = \rho f = (\rho g)(\rho h)$. Also $\rho g = X^l$ und $\rho h = X^m$. Es folgt $p|b_l$ und $p|c_m$, also $p^2|b_l c_m = a_n$, Widerspruch. $\diamond$

Dieses Kriterium lässt sich (mit einem kleinen Zusatztrick) auf das „Kreisteilungspolynom“

$$\Phi_{p^r} := \underbrace{1 + X^{p^{r-1}} + \cdots + (X^{p^{r-1}})^{p-1}}_{p \text{ Summanden}} = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} \in \mathbb{Q}[X]$$

mit einer Primzahl p und einem Exponenten $r \geq 1$ anwenden: Der Substitutionshomomorphismus τ_1 bewirkt:

$$\Phi_{p^r} \mapsto \Phi_{p^r}(X+1) = \sum_{i=0}^{n} a_i X^i =: f \quad \text{mit } n = p^{r-1}(p-1),\ a_n = 1,\ a_0 = p.$$

Um mithilfe von Satz 2 die Irreduzibilität von Φ_{p^r} zu zeigen, zeigen wir, dass $p|a_i$ für $i = 1, \ldots, a_{n-1}$. Dazu wenden wir die Koeffizientenreduktion $\rho : \mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X]$ an. Es ist

$$\begin{aligned}
\rho \circ \tau_1(X^{p^i} - 1) &= \rho((X+1)^{p^i} - 1) = X^{p^i} \quad \text{für alle } i, \\
\tau_1(X^{p^{r-1}} - 1)\, f &= \tau_1(X^{p^{r-1}} - 1)\, \tau_1 \Phi_{p^r} = \tau_1(X^{p^r} - 1), \\
X^{p^{r-1}} \cdot \rho f &= X^{p^r}, \\
\rho f &= X^{p^r - p^{r-1}}.
\end{aligned}$$

Daher sind alle „Zwischenkoeffizienten“ a_i von f durch p teilbar, und wir haben gezeigt:

Korollar 1 *Das Kreisteilungspolynom $\Phi_{p^r} \in \mathbb{Q}[X]$, p prim, $r \geq 1$, ist irreduzibel.*

3.6 Das regelmäßige n-Eck

Sei $n \geq 3$ und $\zeta = e^{2\pi i/n} \in \mathbb{C}$ die „kanonische“ n-te Einheitswurzel. Wir wissen, dass das regelmäßige n-Eck genau dann mit Zirkel und Lineal konstruierbar ist, wenn $x = \cos(2\pi/n)$ konstruierbar ist, also in einer Quadratwurzel-Erweiterung $L \supseteq \mathbb{Q}$ liegt. Insbesonere ist dann $\mathrm{Dim}_{\mathbb{Q}} \mathbb{Q}(x) \mid \mathrm{Dim}_{\mathbb{Q}} L$ eine Zweierpotenz. Da $x = \frac{1}{2}(\zeta + \frac{1}{\zeta})$, erfüllt ζ die quadratische Gleichung $\zeta^2 - 2x\zeta + 1$ über $\mathbb{Q}(x)$, also hat $\mathbb{Q}(\zeta)$ über $\mathbb{Q}(x)$ den Grad[21] ≤ 2. Zusammengefasst:

Hilfssatz 3 *Wenn das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar ist, so ist der Grad des Körpers $\mathbb{Q}(\zeta)$ über $\mathbb{Q}$ eine Zweierpotenz.*

Satz 4 *Sei p eine Primzahl ≥ 3 und $r \geq 2$. Dann ist das regelmäßige p^r-Eck nicht mit Zirkel und Lineal konstruierbar.*

[21] sogar $= 2$, aber das brauchen wir nicht

Beweis. Die zugehörige Einheitswurzel ζ ist Nullstelle des irreduziblen Kreisteilungspolynoms Φ_{p^r}, denn sie annulliert den Zähler $X^{p^r}-1$, aber nicht den Nenner $X^{p^{r-1}}-1$ – sonst wäre sie nämlich schon p^{r-1}-te Einheitswurzel. Da Φ_{p^r} den ungeraden Grad $p^{r-1}(p-1)$ hat, hat nach Satz 2 auch $\mathbb{Q}(\zeta)$ diesen Grad über $\mathbb{Q}$. Die Behauptung folgt aus Hilfssatz 3. $\diamond$

Im Spezialfall $r=1$ hat $\mathbb{Q}(\zeta)$ den Grad $p-1$ über $\mathbb{Q}$, der gerade ist und allerdings sehr wohl eine Zweierpotenz sein kann. Das ist allerdings selten:

Hilfssatz 4 *Sei $s \in \mathbb{N}$ und $p = 2^s+1$ eine Primzahl. Dann ist s selbst eine Zweierpotenz.*

Beweis. Angenommen, s hat einen ungeraden Teiler, $s = ab$, mit ungeradem $b \geq 3$. Dann hat das Polynom $X^b+1 \in \mathbb{Q}[X]$ die Nullstelle -1, also $X^b+1 = (X+1)\cdot g$ nach der Bemerkung 3 in 3.4. Also ist

$$p = (2^a)^b + 1 = (2^a+1)\, g(2^a).$$

Da p prim und $\neq 2^a+1$ ist, folgt $2^a+1 = 1$, $2^a = 0$, Widerspruch. $\diamond$

Damit ist gezeigt:

Satz 5 *Sei p eine Primzahl, und das regelmäßige p-Eck sei mit Zirkel und Lineal konstruierbar. Dann hat p die Form*

$$p = 2^{2^r}+1 \quad \textit{für eine natürliche Zahl } r \in \mathbb{N}.$$

Zahlen dieser Form heißen **Fermatsche Zahlen** F_r. Es ist

- $F_0 = 2^{2^0}+1 = 3$ prim,
- $F_1 = 2^{2^1}+1 = 5$ prim,
- $F_2 = 2^{2^2}+1 = 17$ prim,
- $F_3 = 2^{2^3}+1 = 257$ prim,
- $F_4 = 2^{2^4}+1 = 65537$ prim,
- $F_5 = 2^{2^5}+1$ nicht prim (mithilfe der Identität $1-X^4 = (1+X)(1-X)(1+X^2)$ von Euler[22] 1732 gefunden):

$$\begin{aligned} 2^{2^5}+1 &= 2^{32}+1 = 16\cdot 2^{28}+1 = (641-625)\cdot 2^{28}+1 \\ &= (1+5\cdot 2^7-5^4)\cdot (2^7)^4+1 \\ &= (1+5\cdot 2^7)\cdot (2^7)^4 + 1 - (5\cdot 2^7)^4 \\ &= \underbrace{(1+5\cdot 2^7)}_{641}\cdot \big((2^7)^4 + (1-5\cdot 2^7)(1+(5\cdot 2^7)^2)\big) \end{aligned}$$

[22] Leonhard Euler, 1707–1783

Bemerkungen

1. FERMAT[23] hatte 1640 vermutet, dass alle Fermatschen Zahlen[24] $F_r = 2^{2^r} + 1$ prim sind.

2. Bis heute (Stand April 2020) kennt man keine weitere Fermatsche Primzahl, weiß aber, dass bis $r = 32$ alle Fermatschen Zahlen, und auch viele mit größerem r, zusammengesetzt sind.

3. Unbekannt ist,

   (a) ob F_{33} prim ist,

   (b) ob es überhaupt weitere Fermatsche Primzahlen (also mit $r \geq 5$) gibt,

   (c) ob unendlich viele der Fermatschen Zahlen zusammengesetzt sind.

4. Ist p eine Fermatsche Primzahl, so kann man die Umkehrung von Satz 5 beweisen, indem man mithilfe der Gaußschen Perioden einen Turm von Körpererweiterungen vom jeweiligen Grad 2 konstruiert (und dabei implizit auch ein konkretes Konstruktionsverfahren aufstellt).

5. Die explizite Konstruktion für das 257-Eck ist beschrieben[25] in

   W. BISHOP: How to construct a regular polygon. Amer. Math. Monthly 85 (1978), 186–188.

[23] Pierre de Fermat, 1607–1665

[24] die natürlich erst später so genannt wurden

[25] und nein – das will wirklich niemand so genau wissen