

Ruhr-Universität Bochum
Fakultät für Mathematik

Zur Konstruktion regelmäßiger Vielecke

– MASTERARBEIT –

vorgelegt von:	Erik Sprungala
Matrikelnummer:	108019237122
Erstgutachter:	Prof. Dr. Christian Stump
Zweitgutachter:	Jun.-Prof. Dr. Marie Brandenburg
Abgabefrist:	07.07.2026

Inhaltsverzeichnis

1	Einleitung	1
2	Regelmäßige Vielecke und Einheitswurzeln	3
2.1	Darstellungsformen von Punkten in der Kartesischen Ebene . . .	4
2.2	Die Einheitswurzeln	5
3	Konstruierbarkeit mit Zirkel und Lineal	13
3.1	Euklids elementare Konstruktionsschritte	13
3.2	Der Körper der konstruierbaren Zahlen	18
3.3	Die Bedeutung konstruierbarer Zahlen für die Konstruierbarkeit des regelmäßigen Vielecks	24
4	Regelmäßige Vielecke mit wenigen Ecken	27
4.1	Das regelmäßige Drei- und Viereck	27
4.2	Das regelmäßige Fünfeck	29
4.3	Das regelmäßige Sechseck und regelmäßige $2n$ -Ecke	31
4.4	Das problematische Siebeneck	33
5	Algebraische Grundlagen der Konstruierbarkeit	35
5.1	Algebraische Zahlen und das Minimalpolynom	36
5.2	Irreduzible Polynome	39
5.3	Körpererweiterungen	45
5.4	Konstruierbare Zahlen	53
6	Welche n-Ecke sind konstruierbar?	61
6.1	Das regelmäßige mn -Eck	61
6.2	Nicht konstruierbare p -Ecke	63
6.3	Konstruierbare p -Ecke	71
6.4	Das regelmäßige p^2 -Eck ist nicht konstruierbar	78
6.5	Der Satz von Gauß-Wantzel	80

1 Einleitung

Die Geometrie gehört zu den ältesten Teilgebieten der Mathematik und prägte bereits früh die Entwicklung des mathematischen Denkens. Unser Blick geht dabei zwar nicht in die Zeit der ersten Auseinandersetzungen mit der Mathematik, also die der Babylonier und der alten Ägypter zurück, aber immerhin in die Zeit um 600 v. Chr. in das antike Griechenland [Toe10, S. 1].

Die alten Griechen nutzten die Mathematik erstmals nicht nur für praktische und wirtschaftliche Interessen, sondern stellten sie unter einen wissenschaftlichen Anspruch. Ihre Methodik des Beweisens lieferte dabei die Grundlage der modernen Mathematik, indem durch klar strukturierte logische Argumentationen zum ersten Mal universell gültige mathematische Aussagen getroffen werden konnten. Nicht zuletzt - und in diesem Sinne kommen wir wieder zur Geometrie zurück - seien dabei der Satz des Pythagoras und der Satz des Thales genannt, die heutzutage zweifelsohne jedem Schüler und jeder Schülerin mit einem Schulabschluss bekannt sein dürften [Toe10, S. 1-2].

Eine Vielzahl weiterer geometrischer Erkenntnisse der alten Griechen findet sich in Euklids Buch 'Die Elemente' wieder, welches er um das Jahr 300 v. Chr. verfasste. Dazu gehörten die Kongruenz- und Strahlensätze, das Teilen einer Strecke in gleich große Abschnitte und die Halbierung des Winkels. Eine faszinierende Leistung, die sich in besonderem Maße dadurch auszeichnete, dass die alten Griechen dazu nur Zirkel und Lineal nutzten, um Kreise zu zeichnen und Punkte zu verbinden [Beu18, S. 235].

Aus der genauen Untersuchung der Arbeit mit Zirkel und Lineal entstand für die alten Griechen eine Reihe faszinierender mathematischer Fragestellungen, deren Beantwortung über 2000 Jahre dauern sollte:

- Ist es möglich, einen Winkel in drei gleich große Winkel zu zerteilen?
- Kann zu einem gegebenen Kreis ein Quadrat mit demselben Flächeninhalt gefunden werden?
- Kann das Volumen eines gegebenen Würfels verdoppelt werden?
- Welche regelmäßigen n -Ecke sind konstruierbar?

[Beu18, S. 235-236]

Die letztgenannte dieser antiken Fragestellungen der Geometrie wollen wir in dieser Arbeit genauer betrachten. Wann genau ist es möglich, ein geometrisches Gebilde mit einer festen natürlichen Eckenanzahl n , dessen Innenwinkel und Seitenlängen überall gleich groß sind, nur mit der Hilfe von Lineal und Zirkel zu konstruieren?

Für eine geringe Anzahl an Ecken wurden schnell Lösungen für eine Konstruktion gefunden. Für das regelmäßige 7-Eck und das regelmäßige 17-Eck blieben die Konstruktionsversuche jedoch über mehr als zwei Jahrtausende erfolglos.

Im Jahr 1796 machte es sich daher einer der größten Mathematiker der Geschichte zur Aufgabe, eine Lösung für das antike Problem der Konstruktion regelmäßiger Vielecke zu finden. Die Rede ist vom deutschen Mathematiker Carl Friedrich Gauß, dem im Alter von nur 19 Jahren eines Morgens im Urlaub in Braunschweig die Idee zur Konstruktion des regelmäßigen 17-Ecks in den Kopf kam [Beu18, S. 244].

Der entscheidende Durchbruch bestand darin, den Ausdruck $\cos\left(\frac{2\pi}{17}\right)$ durch verschachtelte Quadratwurzeln darzustellen. Dies gelang Gauß mithilfe der Darstellung

$$\begin{aligned} \cos\left(\frac{2\pi}{17}\right) = \frac{1}{16} & \left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} \right. \\ & \left. + \sqrt{68 + 12\sqrt{17} + 2(\sqrt{17} - 1)\sqrt{34 - 2\sqrt{17}} - 16\sqrt{34 + 2\sqrt{17}}} \right) \end{aligned}$$

[Ben25, S. 196].

Die bahnbrechende Konstruktion des 17-Ecks motivierte Gauß dazu, statt eines Studiums der alten Sprachen ein Studium der Mathematik anzustreben [Toe10, S. 305]. Es wäre also gut möglich gewesen, dass es einen der größten Mathematiker aller Zeiten niemals Mathematiker geworden wäre, wenn schon die alten Griechen bei der Konstruktion des regelmäßigen 17-Ecks Erfolg gehabt hätten.

Nur fünf Jahre später, im Jahr 1801, veröffentlichte Gauß das Lehrbuch *Disquisitiones Arithmeticae*, in dem ihm eine Kategorisierung der Konstruierbarkeit regelmäßiger Vielecke gelang [Beu18, S. 244].

Zugegeben, Gauß hatte im Vergleich zu den alten Griechen einen entscheidenden Vorteil. Seine Konstruktionen nutzten die Mittel der *Analytischen Geometrie*, die ihren Ursprung allerdings erst im 17. Jahrhundert beim französischen Mathematiker René Descartes fanden. Die analytische Geometrie schuf dabei eine Brücke zwischen Geometrie und Algebra und machte es somit möglich, Punkte mithilfe einer Koordinatisierung durch Zahlen darzustellen und geometrische Objekte durch eine oder mehrere Gleichungen zu beschreiben.

Um zu überprüfen, ob ein Punkt (a, b) auf einem Kreis mit Mittelpunkt (x_0, y_0) und Radius r liegt, reichte es nun aus, dass seine Koordinaten die Kreisgleichung $(x - x_0)^2 + (y - y_0)^2 = r^2$ erfüllten [Beu18, S. 236].

2 Regelmäßige Vielecke und Einheitswurzeln

Auch die Herangehensweise dieser Arbeit wird sich an den modernen Mitteln der analytischen Geometrie bedienen, um die geometrischen Problemstellungen der alten Griechen in algebraische Problemstellungen zu überführen. Begeben wir uns also auf die Spuren von Gauß und den alten Griechen und widmen uns den drei wichtigsten Fragen dieser Arbeit:

- Welche regelmäßigen Vielecke sind konstruierbar?
- Welche Konstruktionsschritte sind nötig, um ein bestimmtes regelmäßiges Vieleck zu konstruieren?
- Wie sieht die geometrische Konstruktion eines regelmäßigen Vielecks in der Praxis aus?

Die erste Frage ist das zentrale Anliegen dieser Arbeit. Die zweite und dritte Frage werden wir exemplarisch für einige Vielecke untersuchen, um typische Muster in der Konstruktion regelmäßiger Vielecke zu finden. Dabei wird sich zeigen, dass die Konstruierbarkeit regelmäßiger Vielecke eng mit der algebraischen Struktur bestimmter komplexer Zahlen zusammenhängt.

Die Arbeit orientiert sich dabei hauptsächlich an den Büchern *Das Geheimnis der transzendenten Zahlen* von F. Toennissen [Toe10] und *Zahlen, Formeln und Gleichungen* von A. Beutelspacher [Beu18].

2 Regelmäßige Vielecke und Einheitswurzeln

Um die grundlegende Verbindung zwischen Geometrie und Algebra herstellen zu können, die für die Untersuchung regelmäßiger Vielecke von zentraler Bedeutung ist, betrachten wir zunächst die geometrische Definition eines regelmäßigen Vielecks.

Definition 2.1. [Beu18, S. 244] Sei $n \geq 3$. Ein konvexes Vieleck (n -Eck) heißt **regelmäßig**, falls für die paarweise verschiedenen Eckpunkte

$$A_0, \dots, A_{n-1} \in \mathbb{R}^2$$

folgende Eigenschaften erfüllt sind:

- Alle Seitenlängen sind gleich, d.h.

$$|A_0A_1| = |A_1A_2| = \dots = |A_{n-2}A_{n-1}| = |A_{n-1}A_0|.$$

- Alle Innenwinkel sind kongruent, d.h.

$$\angle A_0A_1A_2 = \angle A_1A_2A_3 = \dots = \angle A_{n-2}A_{n-1}A_0 = \angle A_{n-1}A_0A_1.$$

2 Regelmäßige Vielecke und Einheitswurzeln

Ein regelmäßiges Vieleck ist somit ein geometrisches Objekt mit n gleich langen Seiten und n gleich großen Innenwinkeln.

Bemerkung 2.2. Sämtliche folgenden Betrachtungen beziehen sich auf regelmäßige Vielecke. Wird im weiteren Verlauf der Arbeit von einem *Vieleck* oder einem *n-Eck* gesprochen, so ist damit stets ein regelmäßiges Vieleck mit n Ecken gemeint.

Unser erstes Ziel wird nun darin bestehen, die Menge der Eckpunkte

$$A_0, \dots, A_{n-1} \in \mathbb{R}^2$$

eines regelmäßigen Vielecks explizit zu bestimmen.

2.1 Darstellungsformen von Punkten in der Kartesischen Ebene

Es wird sich in der Suche nach den Koordinaten der Eckpunkte eines regelmäßigen Vielecks als äußerst nützlich erweisen, die Punkte der kartesischen Ebene auf eine etwas andere Art zu beschreiben. Wir identifizieren die Ebene $\mathbb{R}^2$ daher mit der komplexen Zahlenebene $\mathbb{C}$, indem wir jedem Punkt $(x, y) \in \mathbb{R}^2$ die komplexe Zahl

$$z = x + iy \in \mathbb{C}$$

zuordnen. Die komplexen Zahlen lassen sich zudem mithilfe ihres euklidischen Abstands zum Ursprung und einem Winkel $\varphi \in [0, 2\pi)$ eindeutig darstellen.

Definition 2.3 (Polarkoordinaten). [Toe10, S. 276] Sei $z \in \mathbb{C} \setminus \{0\}$. Dann existieren eindeutig bestimmte Zahlen $r \in \mathbb{R}_{>0}$ und $\varphi \in [0, 2\pi)$ mit

$$z = r(\cos \varphi + i \sin \varphi).$$

Dabei ist $r = |z|$ der **euklidische Abstand** von z zum Ursprung und φ heißt **Argument** von z .

Zur weiteren Vereinfachung der Darstellung eines Punktes $(x, y) \in \mathbb{R}^2$ verwenden wir eine grundlegende Beziehung aus der Analysis.

Satz 2.4 (Eulersche Formel). Für alle $\varphi \in \mathbb{R}$ gilt

$$e^{i\varphi} = \cos \varphi + i \sin \varphi.$$

2 Regelmäßige Vielecke und Einheitswurzeln

Der Beweis der Eulerschen Formel nutzt eine Reihe von Kenntnissen aus der Analysis und findet sich unter anderem in [Kri11, S. 5]. Das Resultat folgt unmittelbar aus den Potenzreihendarstellungen des Sinus, des Kosinus und der Exponentialfunktion.

Zusammenfassend lassen sich die gesuchten Eckpunkte

$$A_0, \dots, A_{n-1} \in \mathbb{R}^2$$

über die Identifikation $\mathbb{R}^2 \cong \mathbb{C}$ als komplexe Zahlen auffassen und in Polarkoordinaten darstellen. Dabei gilt

$$\begin{aligned} A_k &= x_k + iy_k \\ &= r_k(\cos \varphi_k + i \sin \varphi_k) \\ &= r_k e^{i\varphi_k} \end{aligned}$$

für $r_k = \sqrt{x_k^2 + y_k^2}$ und $\varphi_k \in [0, 2\pi)$. Während r_k dabei den euklidischen Abstand zum Ursprung definiert, beschreibt das Argument φ_k den Winkel, den A_k mit der positiven reellen Zahlenachse einschließt.

Die alternative Darstellung der kartesischen Koordinaten wird sich im weiteren Verlauf der Arbeit als wesentliches Hilfsmittel bei der Untersuchung regelmäßiger Vielecke erweisen.

2.2 Die Einheitswurzeln

Die Beschreibung des regelmäßigen Vielecks durch seine Eckpunkte und die Darstellung dieser Eckpunkte in der komplexen Zahlenebene bieten die Grundlage für die ersten algebraischen Untersuchungen dieser Arbeit. Hierzu benötigen wir die folgende Definition.

Definition 2.5 (Die Einheitswurzeln). [Beu18, S. 325] *Die Lösungen der Gleichung*

$$z^n = 1$$

*mit $n \in \mathbb{N}$ heißen **n-te Einheitswurzeln**.*

Die n -ten Einheitswurzeln sind daher genau die Nullstellen des Polynoms

$$P(z) = z^n - 1.$$

Satz 2.6. *Die n -ten Einheitswurzeln sind von der Form*

$$z_k = e^{2\pi i k/n}, \quad k = 0, \dots, n-1.$$

2 Regelmäßige Vielecke und Einheitswurzeln

Beweis. Sei $z \in \mathbb{C}$ eine Lösung der Gleichung $z^n = 1$.

Da $z = 0$ diese Gleichung nicht erfüllt, ist $z \neq 0$ und es existieren nach Definition 2.3 Zahlen $r > 0$ und $\varphi \in [0, 2\pi)$ mit

$$z = re^{i\varphi}.$$

Dann gilt

$$z^n = (re^{i\varphi})^n = r^n e^{in\varphi} \stackrel{!}{=} 1.$$

Nach der Euler-Formel (2.4) gilt

$$e^{2\pi ik} = \cos(2\pi k) + i \cdot \sin(2\pi k) = 1 + i \cdot 0 = 1.$$

für alle $k \in \mathbb{Z}$. Somit erhalten wir die Gleichung

$$r^n e^{in\varphi} = 1 = e^{2\pi ik}$$

für ein geeignetes $k \in \mathbb{Z}$. Ein Vergleich der Beträge ergibt

$$r^n = 1$$

und ein Vergleich der Argumente führt uns zur Gleichung

$$n\varphi = 2\pi k.$$

Da r eine positive reelle Zahl ist, gilt $r = 1$. Zusätzlich ist

$$\varphi = \frac{2\pi k}{n}$$

und somit

$$z = e^{2\pi ik/n}.$$

Durch Einsetzen in die Gleichung

$$z^n = 1$$

erhalten wir

$$(e^{2\pi ik/n})^n = e^{2\pi ik} = 1.$$

Folglich ist jede komplexe Zahl von der Form

$$e^{2\pi ik/n} \quad \text{mit} \quad k \in \mathbb{Z}$$

eine Lösung der Gleichung

$$z^n = 1.$$

2 Regelmäßige Vielecke und Einheitswurzeln

Sei nun $l \in \mathbb{Z}$. Dann gilt

$$e^{2\pi i(k+ln)/n} = e^{2\pi ik/n} \cdot e^{2\pi il} = e^{2\pi ik/n}.$$

Somit werden alle Lösungen bereits durch

$$z_k = e^{2\pi ik/n}, \quad k = 0, \dots, n-1$$

erfasst. Da alle Zahlen z_k paarweise verschieden sind, handelt es sich dabei genau um die n -ten Einheitswurzeln. $\square$

Zusammenfassend haben wir mit $P(z) = z^n - 1$ ein Polynom mit n komplexen Nullstellen gefunden. Unsere gesuchten regelmäßigen Vielecke basieren genau auf dieser Anzahl von Eckpunkten. Mithilfe der folgenden Aussagen stellen wir nun einen direkten Zusammenhang zwischen den n -ten Einheitswurzeln und regelmäßigen Vielecken her.

Definition 2.7 (Der Einheitskreis). *Die Menge*

$$S^1 = \{z \in \mathbb{C} : |z| = 1\}$$

*heißt **Einheitskreis**.*

Lemma 2.8. *Die n -ten Einheitswurzeln*

$$z_k = e^{2\pi ik/n}, \quad k = 0, \dots, n-1,$$

liegen auf dem Einheitskreis. Für die Argumente

$$\varphi_k = \frac{2\pi k}{n}$$

der n -ten Einheitswurzeln gilt zudem

$$\varphi_{k+1} - \varphi_k = \frac{2\pi}{n}$$

für alle k .

Beweis. Für jede n -te Einheitswurzel z_k haben wir im Beweis von Satz 2.6 die Gleichheit

$$r_k = |z_k| = 1$$

gezeigt.

Weiter ist das Argument von z_k gegeben durch

$$\varphi_k = \frac{2\pi k}{n}.$$

2 Regelmäßige Vielecke und Einheitswurzeln

Für aufeinanderfolgende Indizes k und $k + 1$ ergibt sich daher

$$\varphi_{k+1} - \varphi_k = \frac{2\pi(k+1)}{n} - \frac{2\pi k}{n} = \frac{2\pi}{n}.$$

Die Einheitswurzeln liegen folglich alle auf dem Einheitskreis und ihre Argumente zerlegen das Intervall $[0, 2\pi)$ in n gleich große Teilintervalle. $\square$

Die Vorbereitungen des Lemmas münden im folgenden Satz.

Satz 2.9. *Die n -ten Einheitswurzeln*

$$z_k = e^{2\pi i k/n}, \quad k = 0, \dots, n-1,$$

bilden die Eckpunkte eines regelmäßigen n -Ecks im Einheitskreis.

Beweis. Ein regelmäßiges n -Eck hat nach Definition 2.1 mindestens drei Ecken. Sei daher $n \geq 3$. Dann sind

$$z_k = e^{2\pi i k/n} \quad \text{mit} \quad k \in \{0, \dots, n-1\}$$

die n -ten Einheitswurzeln. Nach dem vorherigen Lemma gilt für alle diese k

$$|z_k| = 1.$$

Folglich liegen die n -ten Einheitswurzeln alle auf dem Einheitskreis.

Weiterhin sind die Argumente der Punkte gegeben durch

$$\varphi_k = \frac{2\pi k}{n},$$

sodass für alle k

$$\varphi_{k+1} - \varphi_k = \frac{2\pi}{n}$$

gilt.

Damit gilt für alle Winkel $\angle z_k 0 z_{k+1}$

$$\angle z_k 0 z_{k+1} = \frac{2\pi}{n}.$$

Betrachten wir nun die Dreiecke $\triangle(0, z_k, z_{k+1})$, so gilt für alle k :

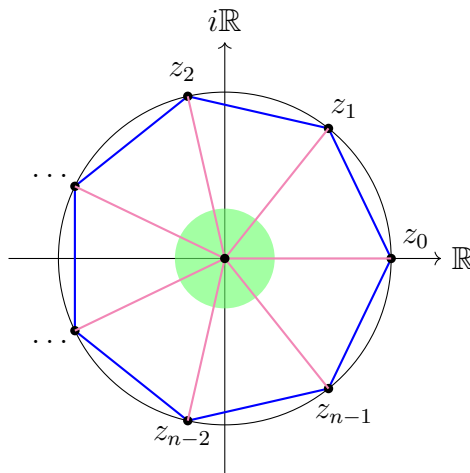
- $|z_{k-1}| = |z_k| = |z_{k+1}| = 1$,
- $\angle z_{k-1} 0 z_k = \angle z_k 0 z_{k+1}$.

2 Regelmäßige Vielecke und Einheitswurzeln

Da alle z_k den gleichen euklidischen Abstand vom Ursprung haben, sind die Dreiecke $\triangle(0, z_k, z_{k+1})$ folglich nicht nur alle gleichschenkelig, sondern nach dem Kongruenzsatz Seite-Winkel-Seite auch alle kongruent zueinander. Daraus folgt allerdings insbesondere die Gleichheit

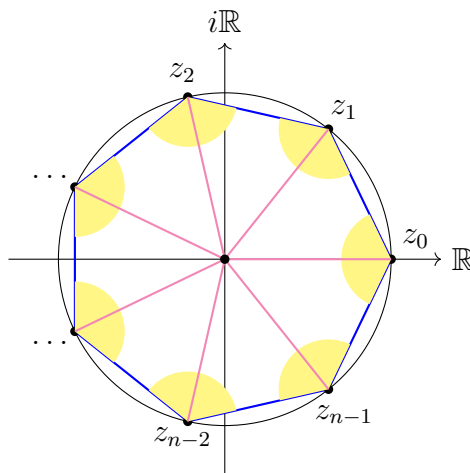
$$|z_{k-1} - z_k| = |z_k - z_{k+1}|$$

für alle k .



Alle Strecken zwischen z_k und z_{k+1} sind folglich gleich lang. Da diese aber genau die Seitenlängen unseres gesuchten Vielecks darstellen, sind auch diese alle gleich lang.

Außerdem stimmen die Innenwinkel aller Dreiecke $\triangle(0, z_k, z_{k+1})$ überein. Da jeder Innenwinkel des Vielecks die Summe zweier entsprechender Winkel benachbarter Dreiecke ist (siehe folgende Abbildung), sind auch alle Innenwinkel des Vielecks gleich groß.



2 Regelmäßige Vielecke und Einheitswurzeln

Die Punktmenge $z_0, \dots, z_{n-1}$ definiert daher ein Vieleck mit gleich langen Seiten und gleich großen Innenwinkeln. Ein solches Vieleck ist nach Definition 2.1 regelmäßig. $\square$

Mit unseren ersten Bemühungen, die Geometrie und die Algebra miteinander zu verknüpfen, haben wir somit durch die n -ten Einheitswurzeln n -Punkte gefunden, die gemeinsam die Eckpunkte eines regelmäßigen n -Ecks definieren.

Können wir die Betrachtung der Konstruktion regelmäßiger Vielecke nun schon abschließen?

Im Rahmen unserer bisherigen Ausführungen zeichnen wir die Eckpunkte $e^{2\pi ik/n}$ auf dem Einheitskreis der komplexen Zahlenebene ein, verbinden die benachbarten Eckpunkte miteinander und erhalten ein Vieleck mit gleichen Innenwinkeln und gleichen Seitenlängen.

Diese Anleitung zur Konstruktion regelmäßiger Vielecke mag zwar auf den ersten Blick schlüssig sein, lässt allerdings den wichtigen Fakt außer Acht, dass wir die Eckpunkte des regelmäßigen n -Ecks nur mit Hilfe von Zirkel und Lineal konstruieren können.

Es stellt sich daher die Frage:

Können wir die Punkte $e^{2\pi ik/n}$ im Allgemeinen nur unter der Verwendung von Zirkel und Lineal für alle $n \in \mathbb{N}$ erreichen?

Bevor wir im folgenden Kapitel untersuchen, welche Optionen wir unter der Bedingung der Nutzung von Lineal und Zirkel überhaupt haben, um neue Punkte zu konstruieren, halten wir eine wichtige geometrische Eigenschaft der n -ten Einheitswurzeln fest. Dazu benötigen wir die folgende Definition:

Definition 2.10 (Komplexe Konjugation). *Für eine komplexe Zahl*

$$z = x + iy$$

*ist ihre **komplex konjugierte Zahl** $\bar{z}$ definiert als*

$$\bar{z} = x - iy.$$

Geometrisch entspricht die komplexe Konjugation der Spiegelung an der reellen Zahlenachse.

2 Regelmäßige Vielecke und Einheitswurzeln

Bemerkung 2.11. Für $z, z_1, z_2 \in \mathbb{C}$ gelten die folgenden Rechenregeln für das komplex Konjugierte:

- $z + \bar{z} = 2 \operatorname{Re}(z)$,
- $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$,
- $\overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$,
- $z^{-1} = \frac{\bar{z}}{|z|^2}$.

Proposition 2.12. Für eine komplexe Zahl $z = \cos \varphi + i \sin \varphi$ mit $\varphi \in [0, 2\pi)$ auf dem Einheitskreis gilt

$$z + z^{-1} = 2 \cos \varphi.$$

Beweis. Sei $z = \cos \varphi + i \sin \varphi$ mit $\varphi \in [0, 2\pi)$ eine komplexe Zahl auf dem Einheitskreis. Aus den Rechenregeln zum komplex Konjugierten folgt dann direkt

$$z + z^{-1} = z + \frac{\bar{z}}{|z|^2} = z + \bar{z} = 2 \operatorname{Re}(z) = 2 \cos \varphi.$$

□

Bemerkung 2.13. Diese leicht zu beweisende Aussage ist von überraschend großer Bedeutung für das Konstruieren regelmäßiger Vielecke. Unter anderem zeigt die Proposition, dass sich für die n -ten Einheitswurzeln

$$z_k = e^{2\pi i k/n}$$

Paare (z_k, z_{n-k}) bilden lassen, für die

$$z_k + z_{n-k} = 2 \cos \left(\frac{2\pi k}{n} \right)$$

gilt [Toe10, S. 300-301]. Dies folgt aus der Gleichung

$$\begin{aligned} z_{n-k} &= e^{2\pi i(n-k)/n} \\ &= e^{2\pi i} \cdot e^{-2\pi i k/n} \\ &= e^{-2\pi i k/n} \\ &= \cos \left(-\frac{2\pi k}{n} \right) + i \cdot \sin \left(-\frac{2\pi k}{n} \right) \\ &= \cos \left(\frac{2\pi k}{n} \right) - i \cdot \sin \left(\frac{2\pi k}{n} \right) \\ &= \bar{z}_k = z_k^{-1} \end{aligned}$$

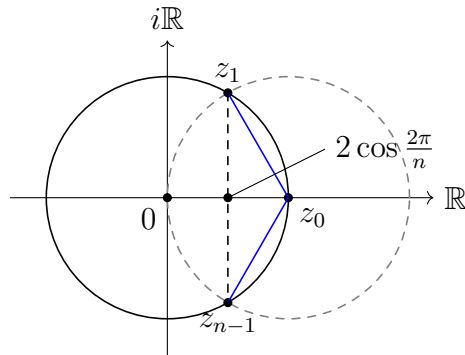
und der besagten Proposition 2.12.

2 Regelmäßige Vielecke und Einheitswurzeln

Die Addition eines Paares von Nullstellen (z_k, z_{n-k}) führt somit zwei komplexe n -te Einheitswurzeln auf die reelle Zahl

$$2 \cos \frac{2\pi k}{n}$$

zurück.



Wir werden in der Konstruktion des regelmäßigen Fünfecks in Kapitel 4.2 und in vielen weiteren Konstruktionen einen großen Nutzen aus dieser Eigenschaft ziehen können. Bevor wir allerdings mit dem Konstruieren regelmäßiger n -Ecke beginnen können, müssen wir im folgenden Kapitel untersuchen, wie wir mithilfe von Zirkel und Lineal neue Punkte in der komplexen Zahlenebene konstruieren können.

3 Konstruierbarkeit mit Zirkel und Lineal

Nachdem wir gezeigt haben, dass die n -ten Einheitswurzeln die Eckpunkte eines regelmäßigen n -Ecks im Einheitskreis bilden, stellt sich nun die zentrale Frage, ob wir diese Punkte im Allgemeinen mit Zirkel und Lineal konstruieren können. Um diese Frage präzise untersuchen zu können, müssen wir zunächst klären, was unter der Konstruierbarkeit eines Punktes mit Zirkel und Lineal zu verstehen ist.

3.1 Euklids elementare Konstruktionsschritte

Ausgehend von einem Axiomensystem leitete Euklid in seinem bekanntesten Werk *Die Elemente* eine Reihe wichtiger Eigenschaften für geometrische Objekte her. Dabei reduzierte Euklid die erlaubten Konstruktionsschritte mit Zirkel und Lineal auf nur wenige elementare Grundoptionen. Daher ist es naheliegend, dass wir unsere Untersuchungen zur Konstruierbarkeit gewisser Punkte in der komplexen Zahlenebene $\mathbb{C}$ mit den elementarsten Objekten der Geometrie beginnen.

Definition 3.1 (Gerade). *Seien $p, q \in \mathbb{C}$ mit $p \neq q$. Dann bezeichnen wir mit*

$$g_{p,q} := \{p + t(q - p) \mid t \in \mathbb{R}\}$$

*die eindeutige **Gerade** durch p und q .*

Definition 3.2 (Kreis). *Sei $p \in \mathbb{C}$ und $r \in \mathbb{R}_{>0}$. Dann bezeichnen wir mit*

$$K_r(p) := \{z \in \mathbb{C} \mid |z - p| = r\}$$

*den **Kreis** mit Mittelpunkt p und Radius r .*

Mithilfe der möglichst klein gewählten Startmenge

$$\mathcal{M} = \{0, 1\} \subset \mathbb{C}$$

und den Definitionen von Gerade und Kreis können wir nun drei elementare Optionen definieren, um mit Zirkel und Lineal weitere Punkte zur Menge $\mathcal{M}$ hinzuzufügen:

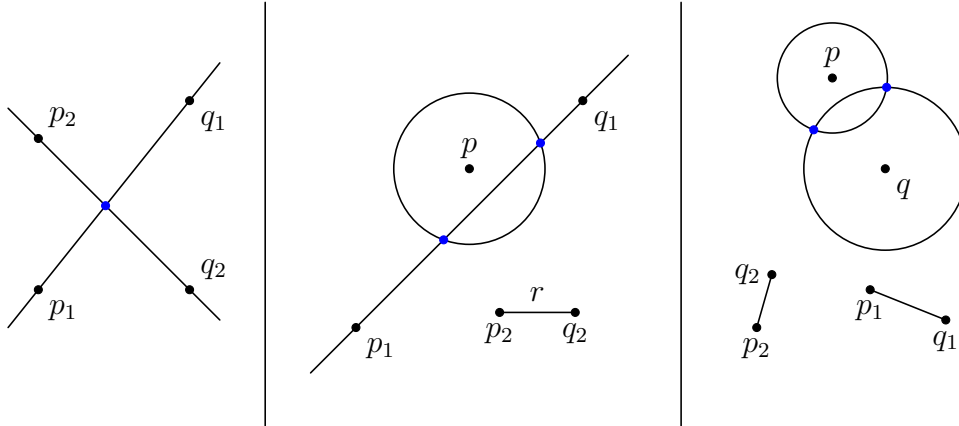
Definition 3.3 (Elementare Erweiterungen von $\mathcal{M}$). *[Toe10, S. 284] Sei $\mathcal{M} \subset \mathbb{C}$ eine bereits konstruierte Punktmenge. Dann lässt sich $\mathcal{M}$ durch die folgenden Konstruktionen schrittweise erweitern:*

3 Konstruierbarkeit mit Zirkel und Lineal

- **Typ 1** (zwei Geraden): Sind $p_1, p_2, q_1, q_2 \in \mathcal{M}$ mit $p_i \neq q_i$ für $i \in \{1, 2\}$, so lässt sich $\mathcal{M}$ um den eindeutigen Schnittpunkt der Geraden g_{p_1, q_1} und g_{p_2, q_2} erweitern, sofern die Geraden verschieden sind und sich schneiden.
- **Typ 2** (Gerade und Kreis): Sind $p, p_1, p_2, q_1, q_2 \in \mathcal{M}$ mit $p_1 \neq q_1$, so lässt sich $\mathcal{M}$ um alle existierenden Punkte des Schnitts $g_{p_1, q_1} \cap K_{|p_2 - q_2|}(p)$ erweitern.
- **Typ 3** (zwei Kreise): Sind $p, p_1, p_2, q, q_1, q_2 \in \mathcal{M}$ mit $p \neq q$, so lässt sich $\mathcal{M}$ um alle existierenden Punkte des Schnitts $K_{|p_1 - q_1|}(p) \cap K_{|p_2 - q_2|}(q)$ erweitern.

Bemerkung 3.4. In der euklidischen Ebene schneiden sich zwei nicht-identische, nicht-parallele Geraden in genau einem Punkt. Zwei Kreise sowie eine Gerade und ein Kreis schneiden sich hingegen in keinem, einem oder zwei Punkten.

Geometrisch lassen sich die elementaren Erweiterungen von $\mathcal{M}$ wie folgt darstellen:



Definition 3.5 (Konstruierbare Punkte und Zahlen). Wir bezeichnen mit

$$\text{Con}(\mathcal{M})$$

die Menge aller Punkte der komplexen Zahlenebene, die sich ausgehend von der Startmenge

$$\mathcal{M} = \{0, 1\}$$

durch endlich viele elementare Erweiterungen aus Definition 3.3 konstruieren lassen.

Ein Punkt $z \in \mathbb{C}$ heißt **konstruierbar**, falls

$$z \in \text{Con}(\mathcal{M})$$

3 Konstruierbarkeit mit Zirkel und Lineal

gilt.

Eine reelle Zahl $x \in \mathbb{R}$ heißt **konstruierbar**, falls der Punkt

$$(x, 0) \in \mathbb{C}$$

konstruierbar ist.

Aus der Startmenge

$$\mathcal{M} = \{0, 1\}$$

lassen sich durch elementare Erweiterungen zunächst nur wenige neue Punkte gewinnen. Die Punkte 0 und 1 definieren eine eindeutige Gerade, die der algebraischen Gleichung

$$y = 0$$

genügt. Da unser Vorrat an Punkten zur Konstruktion weiterer Geraden nun bereits aufgebraucht ist, wenden wir uns den konstruierbaren Kreisen zu. Für $z = x + iy \in \mathbb{C}$ genügt der Kreis $K_1(0)$ der Gleichung

$$|z|^2 = x^2 + y^2 = 1.$$

Durch das Einsetzen von $y = 0$ in diese Gleichung erhalten wir

$$x^2 = 1$$

und somit

$$x_1 = 1 \quad \text{und} \quad x_2 = -1.$$

Wir haben durch eine elementare Erweiterung vom Typ 2 unseren ersten neuen Punkt konstruiert, den Punkt $(-1, 0)$ [Toe10, S. 285]. Folglich gilt

$$\{(0, 0), (1, 0), (-1, 0)\} \subset \text{Con}(\mathcal{M}).$$

Durch elementare Erweiterungen vom Typ 3 und Typ 1 können wir nun noch weitere Punkte der Menge $\text{Con}(\mathcal{M})$ konstruieren.

Wir betrachten für eine Erweiterung vom Typ 3 die Kreise $K_1(-1)$ und $K_1(0)$. Diese genügen den Gleichungen

$$x^2 + y^2 = 1, \tag{1}$$

$$(x + 1)^2 + y^2 = 1. \tag{2}$$

Durch das Gleichsetzen von 1 und 2 erhalten wir

$$\begin{aligned} x^2 + y^2 &= (x + 1)^2 + y^2 \\ \Leftrightarrow x^2 &= x^2 + 2x + 1 \\ \Leftrightarrow 2x &= -1 \\ \Leftrightarrow x &= -\frac{1}{2} \end{aligned}$$

3 Konstruierbarkeit mit Zirkel und Lineal

und dieses Ergebnis liefert uns mit dem Einsetzen in 1

$$y_{1,2} = \pm \frac{\sqrt{3}}{2}.$$

Die Schnittpunkte der Kreise $K_1(0)$ und $K_1(-1)$ sind also genau die Punkte

$$z_1 = -\frac{1}{2} + i \cdot \frac{\sqrt{3}}{2} \quad \text{und} \quad z_2 = -\frac{1}{2} - i \cdot \frac{\sqrt{3}}{2}.$$

Wir haben somit zwei bemerkenswerte konstruierbare Punkte gefunden [Toe10, S. 285]. Zum einen liegen die Punkte nicht mehr auf der reellen Zahlenachse, zum anderen ist der Imaginärteil von z_1 und z_2 nicht mehr rational! Wir werden uns schon bald mit einer algebraischen Charakterisierung konstruierbarer Punkte auseinandersetzen, wollen aber nun noch kurz ausnutzen, dass wir durch die neu konstruierten Punkte auch erstmals zwei Geraden miteinander schneiden können. Definiert durch die Punkte $(0,0)$, $(1,0)$ und $(-\frac{1}{2}, \frac{\sqrt{3}}{2})$, $(-\frac{1}{2}, -\frac{\sqrt{3}}{2})$ genügen die eindeutigen Geraden den Gleichungen

$$\begin{aligned} y &= 0 \\ x &= -\frac{1}{2} \end{aligned}$$

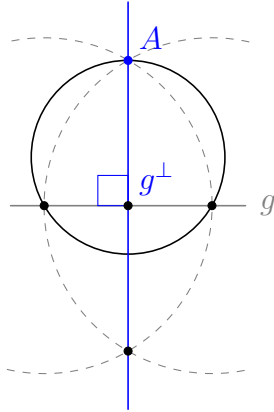
und liefern somit direkt den Schnittpunkt $(-\frac{1}{2}, 0)$. Die Konstruierbarkeit der Zahl $-\frac{1}{2}$ ist, nachdem wir den Punkt $(-\frac{1}{2}, \frac{\sqrt{3}}{2})$ konstruiert haben, tatsächlich nur wenig überraschend. Hierbei können wir uns bekannte Hilfsmittel aus der Geometrie zunutze machen.

Satz 3.6. [Toe10, S. 282] *Durch das wiederholte Schneiden von Geraden und Kreisen sind insbesondere folgende geometrische Konstruktionen möglich:*

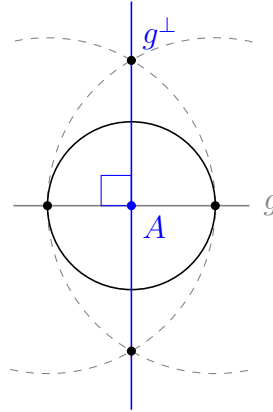
1. *Das Fällen des Lots eines Punkts A auf eine Gerade g ,*
2. *Das Konstruieren einer Senkrechten $g^\perp$ durch einen Punkt A auf einer Geraden g ,*
3. *Die Konstruktion einer Geraden h , die zu einer anderen Geraden g parallel verläuft,*
4. *Die Halbierung eines gegebenen Winkels,*
5. *Das Konstruieren des Mittelpunkts einer gegebenen Strecke.*

Beweisidee. Die Konstruierbarkeit sei anhand der folgenden Zeichnungen verdeutlicht.

(1)

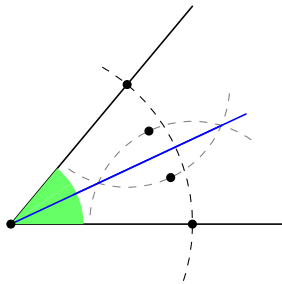


(2)

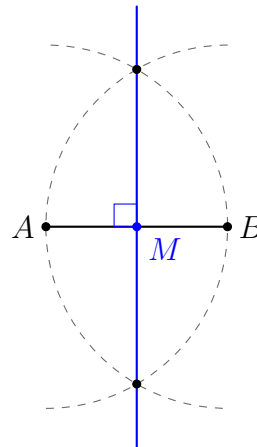


(3) Die Konstruktion der Parallelen ist eine Kombination der Konstruktionen (1) und (2).

(4)



(5)



Da innerhalb der einzelnen Konstruktionsschritte nur auf den Schnitt von zwei Geraden, zwei Kreisen und einer Geraden mit einem Kreis zurückgegriffen wird, lassen sich all diese Konstruktionen mit Zirkel und Lineal durchführen. $\square$

Aus den bisher konstruierten Punkten

$$\left\{ (-1, 0), (0, 0), \left(-\frac{1}{2}, 0\right), (1, 0), \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right), \left(-\frac{1}{2}, -\frac{\sqrt{3}}{2}\right) \right\} \subset \text{Con}(\mathcal{M})$$

lassen sich durch Satz 3.6 problemlos zusätzliche konstruierbare Punkte ableiten. Zum Beispiel lässt sich mit 3.6(2) eine Senkrechte zur x-Achse durch

den Ursprung bilden. Diese verläuft identisch zur y-Achse. Wegen

$$\left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right) \in \text{Con}(\mathcal{M})$$

liegt, durch das Fällen des Lots auf die y-Achse, auch

$$\left(0, \frac{\sqrt{3}}{2}\right) \in \text{Con}(\mathcal{M}).$$

Durch die Möglichkeit der Streckenhalbierung liegen daher auch

$$\left(0, \frac{\sqrt{3}}{4}\right), \left(0, \frac{\sqrt{3}}{8}\right), \left(0, \frac{\sqrt{3}}{16}\right), \dots$$

in $\text{Con}(\mathcal{M})$. Ohne Zweifel lassen sich mit diesen geometrischen Hilfsmitteln schon eine Reihe verschiedener Punkte konstruieren. Weiterhin nur einzelne Punkte zu konstruieren, wäre allerdings nicht sonderlich mathematisch wertvoll. Daher lohnt sich die Suche nach einer algebraischen Struktur, die uns vorgibt, wann genau ein allgemeiner Punkt $(x, y) \in \mathbb{C}$ konstruierbar ist. Eine solche Struktur wollen wir im folgenden Kapitel finden.

3.2 Der Körper der konstruierbaren Zahlen

Die bisherigen Ausführungen des Kapitels haben verdeutlicht, dass neue Punkte in der komplexen Zahlenebene nur durch das wiederholte Schneiden zweier Geraden, zweier Kreise oder eines Kreises mit einer Geraden konstruiert werden können. Geraden und Kreise sind daher als geometrische Objekte von zentraler Bedeutung für die Konstruierbarkeit der n -ten Einheitswurzeln. Jedoch wurde auch klar, dass durch eine algebraische Betrachtung der Geraden und Kreise sowie ihrer Schnittpunkte eine genaue Betrachtung konstruierbarer Punkte in $\mathbb{C}$ in hohem Maße vereinfacht wird. Insbesondere werden wir zeigen, dass die Menge der konstruierbaren Zahlen eine starke algebraische Struktur besitzt. Dazu definieren wir zunächst einige basale Objekte aus der Algebra.

Definition 3.7 (Gruppe). [FS25, S. 54] Eine Menge G zusammen mit einer Verknüpfung $*$ heißt **Gruppe** $(G, *)$, wenn die Abbildung

$$*: G \times G \rightarrow G, \quad (a, b) \mapsto a * b$$

die folgenden Eigenschaften erfüllt:

- Für alle $a, b, c \in G$ gilt

$$(a * b) * c = a * (b * c). \quad (\text{Assoziativität})$$

3 Konstruierbarkeit mit Zirkel und Lineal

- Es gibt ein neutrales Element $e \in G$, sodass für alle $a \in G$ gilt:

$$e * a = a * e = a. \quad (\text{Neutrales Element})$$

- Zu jedem $a \in G$ existiert ein eindeutiges $a^{-1} \in G$ mit

$$a * a^{-1} = a^{-1} * a = e. \quad (\text{Inverse Elemente})$$

Eine Gruppe $(G, *)$ heißt **abelsch**, falls zusätzlich für alle $a, b \in G$

$$a * b = b * a$$

gilt.

Definition 3.8 (Ring). [FS25, S. 67] Eine Menge R mit den Verknüpfungen $+$ und $\cdot$ heißt **Ring** $(R, +, \cdot)$, falls für die Abbildungen

$$+ : R \times R \rightarrow R, \quad (a, b) \mapsto a + b$$

$$\cdot : R \times R \rightarrow R, \quad (a, b) \mapsto a \cdot b$$

folgende Eigenschaften erfüllt sind:

- $(R, +)$ ist eine abelsche Gruppe mit neutralem Element $0 \in R$.
- Für alle $a, b, c \in R$ gilt

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c. \quad (\text{Assoziativität})$$

- Für alle $a, b, c \in R$ gilt

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \quad \text{und} \\ (a + b) \cdot c &= a \cdot c + b \cdot c. \end{aligned} \quad (\text{Distributivität})$$

Definition 3.9 (Körper). [FS25, S. 69] Eine Menge K mit den Verknüpfungen $+$ und $\cdot$ heißt **Körper** $(K, +, \cdot)$, falls für die Abbildungen

$$+ : K \times K \rightarrow K, \quad (a, b) \mapsto a + b$$

$$\cdot : K \times K \rightarrow K, \quad (a, b) \mapsto a \cdot b$$

folgende Eigenschaften erfüllt sind:

- $(K, +)$ ist eine abelsche Gruppe mit neutralem Element 0 .
- $(K \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe mit neutralem Element 1 .

3 Konstruierbarkeit mit Zirkel und Lineal

- Für alle $a, b, c \in K$ gilt

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \quad \text{und} \\ (a + b) \cdot c &= a \cdot c + b \cdot c. \end{aligned} \quad (\text{Distributivität})$$

Unser Ziel vor dem ersten kurzen algebraischen Einschub dieses Unterkapitels bestand darin, die Konstruierbarkeit verschiedener Punkte in der komplexen Zahlenebene $\mathbb{C}$ genauer beschreiben zu können. Tatsächlich besitzen die konstruierbaren Zahlen die mächtige algebraische Struktur eines Körpers.

Satz 3.10 (Der Körper der konstruierbaren Zahlen). *[Beu18, S. 237-238]*
Sind die Zahlen $a, b \in \mathbb{R}$ konstruierbar, so sind es auch die Zahlen

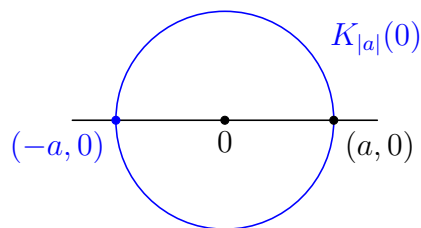
1. $-a$,
2. $a + b$,
3. $a \cdot b$ und
4. $\frac{b}{a}$ (für $a \neq 0$).

Insbesondere bilden die konstruierbaren Zahlen einen Körper.

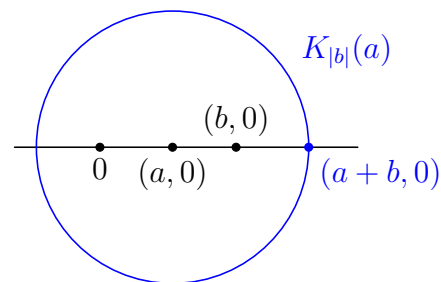
Beweis.

1. Sei a eine konstruierbare Zahl, d.h. der Punkt $(a, 0) \in \mathbb{C}$ ist konstruierbar. Der Schnitt der x-Achse mit dem Kreis $K_{|a|}(0)$ liefert somit sofort den gesuchten Punkt $(-a, 0)$.

(1)



(2)



2. Seien a, b konstruierbare Zahlen, d.h. die Punkte $(a, 0)$ und $(b, 0)$ sind konstruierbar. Insbesondere lässt sich somit der Kreis $K_{|b|}(a)$ zeichnen, welcher die x-Achse in den Punkten $(a-b, 0)$ und $(a+b, 0)$ schneidet. Somit ist auch die Zahl $a+b$ konstruierbar.

3 Konstruierbarkeit mit Zirkel und Lineal

3. Seien zunächst $a, b \geq 0$ konstruierbare Zahlen. Schneiden wir die konstruierbare, zur y-Achse identisch verlaufende Gerade g mit den Kreisen $K_1(0)$ und $K_b(0)$, so erhalten wir die Punkte $(0, 1)$ und $(0, b)$. Sei h die eindeutige Gerade durch die Punkte $(0, 1)$ und $(a, 0)$. Da wir nach Satz 3.6 auch Parallelen zu einer bestehenden Geraden durch einen konstruierbaren Punkt bilden können, bilden wir nun eine Parallele h' zu h durch den Punkt $(0, b)$. Da h die x-Achse schneidet, schneidet auch h' die x-Achse in einem bislang nicht weiter bestimmten Punkt $(x, 0)$. Nun machen wir uns den aus der Schule bekannten Strahlensatz mit Zentrum $(0, 0)$ zunutze. Dieser liefert die Gleichung

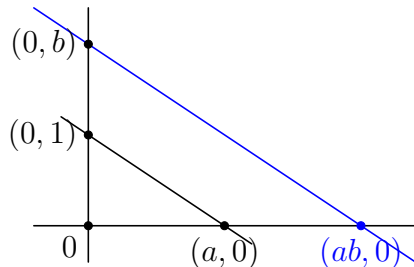
$$\frac{1}{b} = \frac{a}{x}$$

und somit

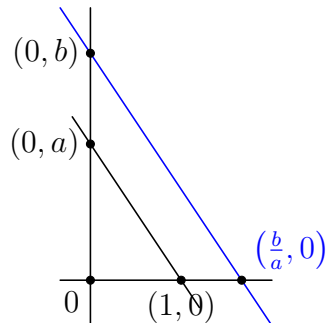
$$x = ab.$$

Wir haben daher den Punkt $(a \cdot b, 0)$ konstruiert. Für beliebige Vorzeichen folgt die Aussage mit Teil (1).

(3)



(4)



4. Seien zunächst a, b konstruierbare Zahlen mit $a \neq 0$ und $b > 0$. Ähnlich wie im Beweis zu 3 bilden wir eine Parallele g' durch $(0, b)$ zur Geraden g durch die Punkte $(0, a)$ und $(1, 0)$. g' schneidet die x-Achse in einem Punkt $(x, 0)$. Für das Zentrum $(0, 0)$ ergibt sich aus dem Strahlensatz die Gleichung

$$\frac{b}{a} = \frac{x}{1}$$

und somit

$$x = \frac{b}{a}.$$

3 Konstruierbarkeit mit Zirkel und Lineal

Damit können wir auch den Punkt

$$\left(\frac{b}{a}, 0\right)$$

für $a \neq 0$ konstruieren. Für allgemeine Vorzeichen von b folgt die Aussage wieder mit Teil (1).

Da die Menge der konstruierbaren Zahlen eine Teilmenge von $\mathbb{R}$ ist, können wir die üblichen Rechenoperationen auf $\mathbb{R}$ auf diese Menge einschränken. Da insbesondere aufgrund der gewählten Startmenge $\mathcal{M} = \{0, 1\}$ die Zahlen 0 und 1 konstruierbar sind und die Menge der konstruierbaren Zahlen unter Addition, Multiplikation sowie der Bildung additiver und multiplikativer Inversen abgeschlossen ist, bilden die konstruierbaren Zahlen einen Körper. $\square$

Die Eigenschaft der konstruierbaren Zahlen, ein Körper zu sein, ist in der Tat von großer Bedeutung. Wir können zunächst festhalten:

Korollar 3.11. *Für $\text{Con}(\mathcal{M})$ gelten die folgenden Inklusionen:*

1. $\mathbb{Q} \times \{0\} \subset \text{Con}(\mathcal{M})$,
2. $\mathbb{Q}^2 \subset \text{Con}(\mathcal{M})$.

Beweis.

1. Da die konstruierbaren Zahlen nach Satz 3.10 einen Körper bilden, folgt die Eigenschaft $\mathbb{Q} \times \{0\} \subset \text{Con}(\mathcal{M})$ direkt aus den geltenden Körpereigenschaften.
2. Im Beweis zu Satz 3.10 haben wir gesehen, dass auch der Punkt $(0, 1)$ konstruierbar ist. Sei $q \in \mathbb{Q}$. Dann schneiden sich die y-Achse und der Kreis $K_q(0)$ insbesondere im Punkt $(0, q)$. Wir können also auch alle Punkte $(0, r)$ für ein rationales r konstruieren. Bilden wir für $r, q \in \mathbb{Q}$ durch $(q, 0)$ eine Senkrechte bezüglich der x-Achse und durch $(0, r)$ eine Senkrechte bezüglich der y-Achse, so schneiden sich die entstehenden Geraden im Punkt $(q, r) \in \mathbb{Q}^2$.

$\square$

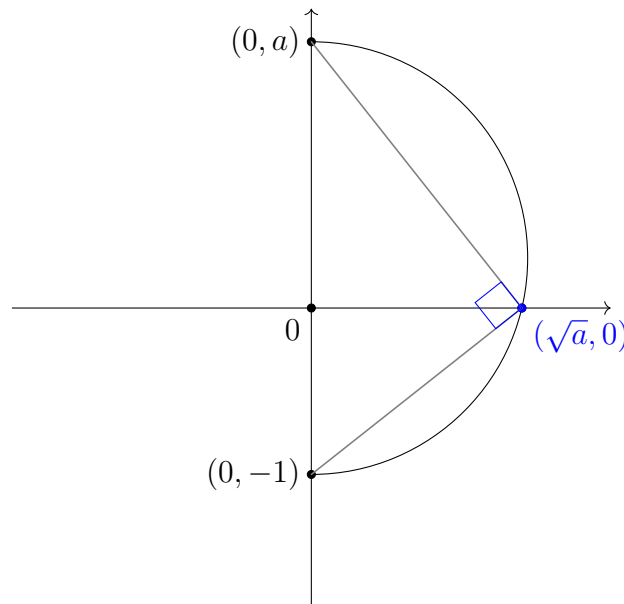
Wir können folglich alle Punkte mit rationalem Real- und Imaginärteil in der komplexen Zahlenebene mit Zirkel und Lineal konstruieren.

Eine exakte Beschreibung der Menge $\text{Con}(\mathcal{M})$ haben wir mit dem Korollar allerdings noch nicht gefunden, denn schon zu Beginn dieses Kapitels haben wir gezeigt, dass unter anderem der Punkt $(0, \frac{\sqrt{3}}{2}) \notin \mathbb{Q}^2$ konstruierbar ist. Der folgende Satz zeigt daher eine weitere wichtige Eigenschaft der konstruierbaren Zahlen.

3 Konstruierbarkeit mit Zirkel und Lineal

Satz 3.12. [Beu18, S. 238] Ist eine Zahl $a \in \mathbb{R}_{\geq 0}$ konstruierbar, so ist auch ihre Quadratwurzel $\sqrt{a}$ konstruierbar.

Beweis. Sei a eine positive konstruierbare Zahl. Da $(0, -1) \in \mathbb{Q}^2$ liegt und wir in Satz 3.10 gesehen haben, dass auch der Punkt $(0, a)$ konstruierbar ist, bilden wir den Thaleskreis über der Strecke zwischen $(0, -1)$ und $(0, a)$. Der Thaleskreis schneidet die positive x-Achse notwendigerweise in einem Punkt $(x, 0)$. Das Dreieck aus diesen drei Punkten ist rechtwinklig. Unter Anwendung des Höhensatzes [Toe10, S. 8] erhalten wir somit die Gleichung $x^2 = a \cdot 1$ und damit $x = \sqrt{a}$. $\square$



Auch die Quadratwurzeln gehören somit zu den konstruierbaren Zahlen. Mit $\sqrt{2}$ und $\sqrt{3}$ finden wir leicht zwei Beispiele für konstruierbare irrationale Zahlen. Diese Erkenntnis kann im Allgemeinen allerdings als gute Nachricht aufgefasst werden. Wir können nicht nur alle rationalen Zahlen konstruieren, sondern auch jede beliebige Quadratwurzel aus einer positiven konstruierbaren Zahl.

Wir werden für die Betrachtung der allgemeinen regelmäßigen Vielecke noch weitere Hilfsmittel benötigen. Die bisherigen Hilfsmittel reichen jedoch bereits aus, um einige unserer gesuchten Vielecke konstruieren zu können. Bevor wir uns in Kapitel 4 diesen Konstruktionen widmen, wollen wir im nächsten Unterkapitel ein zentrales Kriterium für die Konstruierbarkeit eines regelmäßigen Vielecks festhalten.

3.3 Die Bedeutung konstruierbarer Zahlen für die Konstruktion des regelmäßigen Vielecks

Kapitel 2 hat uns gezeigt, dass wir die Frage der Konstruktion regelmäßiger Vielecke auf die Konstruktion bestimmter Punkte, der n -ten Einheitswurzeln, auslagern können. Das bisherige Kapitel 3 hat uns das zentrale Resultat geliefert, dass die Menge der konstruierbaren Zahlen einen Körper bildet. Dieser erlaubt es uns, neben den Rechenoperationen $+$, $-$, $\cdot$, $\div$ auch beliebige Wurzeln $\sqrt[n]{\cdot}$ aus einer positiven konstruierbaren Zahl zu ziehen. Zudem konnten wir zeigen, dass wir unter anderem zu einem gegebenen konstruierbaren Punkt auf einer Geraden eine Senkrechte konstruieren können. Diese Resultate erlauben es uns, unsere spezifische Frage nach der Konstruktion der n -ten Einheitswurzeln noch genauer einzugrenzen.

Satz 3.13. [Toe10, S. 300] *Ein Punkt $z = x + iy \in S^1$ ist mit Zirkel und Lineal genau dann konstruierbar, wenn die reelle Zahl $\operatorname{Re}(z) = x$ konstruierbar ist.*

Beweis. Der Beweis des Satzes ist eine einfache Folgerung aus den bisherigen Resultaten. Sei dazu zunächst $z = x + iy \in \mathbb{C}$ eine komplexe Zahl auf dem Einheitskreis mit einem konstruierbaren Realteil $\operatorname{Re}(z) = x$. Das bedeutet, dass der Punkt $(x, 0)$ konstruierbar ist. Nun lässt sich nach Satz 3.6 eine Senkrechte $g^\perp$ durch den Punkt $(x, 0)$ bezüglich der x -Achse bilden. Aufgrund der Kreisgleichung $x^2 + y^2 = 1$ des Einheitskreises gilt $|\operatorname{Re}(z)| \leq 1$.

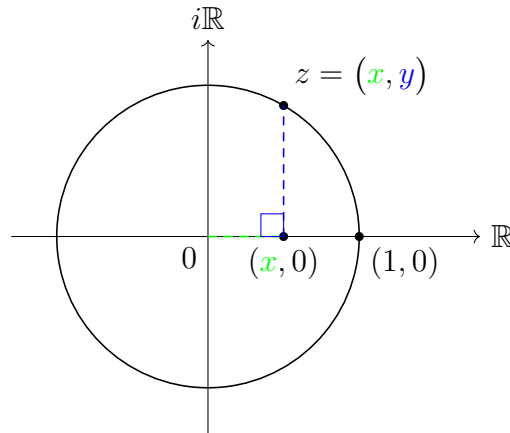
1. Fall: $|\operatorname{Re}(z)| = 1$

Dann gilt wegen $x^2 + y^2 = 1$ schon $\operatorname{Im}(z) = 0$ und die Konstruktion von $\operatorname{Re}(z)$ ist somit gleichbedeutend mit der Konstruktion von z .

2. Fall: $|\operatorname{Re}(z)| < 1$

Dann liegt der konstruierbare Punkt im Inneren des Einheitskreises. Wir erhalten somit zwei Schnittpunkte zwischen $g^\perp$ und S^1 . Einer dieser Punkte ist der gesuchte Punkt $z = x + iy \in \mathbb{C}$.

3 Konstruierbarkeit mit Zirkel und Lineal



Sei umgekehrt ein Punkt $z = x + iy$ auf dem Einheitskreis konstruierbar. Dann können wir nach Satz 3.6 das Lot des Punktes auf die x -Achse fällen. Die dabei entstehende Gerade schneidet die x -Achse im Punkt $(x, 0)$. Daher ist die reelle Zahl $\operatorname{Re}(z) = x$ ebenfalls konstruierbar. $\square$

Das nachfolgende Resultat liefert uns ein exaktes Kriterium, wann das regelmäßige n -Eck mit Zirkel und Lineal konstruiert werden kann. Wir werden im Laufe dieser Arbeit immer wieder darauf zurückkommen. Deswegen erhält der folgende Satz seine Bezeichnung als Hauptsatz der ersten drei Kapitel.

Hauptsatz 3.14. [Toe10, S. 300] Ist die Zahl

$$\cos\left(\frac{2\pi}{n}\right)$$

konstruierbar, so sind alle n -ten Einheitswurzeln und damit das regelmäßige n -Eck konstruierbar.

Beweis. Nach Kapitel 2 stellen die n -ten Einheitswurzeln

$$z_k = e^{2\pi i k/n}, \quad k = 0, \dots, n-1$$

die Eckpunkte eines regelmäßigen n -Ecks im Einheitskreis dar. Aufgrund der Gleichheit

$$e^{i\varphi} = \cos \varphi + i \cdot \sin \varphi$$

folgt wegen $z_k \in S^1$ und aus Satz 3.13, dass es ausreicht, die Konstruierbarkeit von

$$\cos \frac{2\pi k}{n}, \quad k = 0, \dots, n-1$$

zu zeigen. Für $k = 0$ gilt dabei für alle $n \in \mathbb{N}$

$$\cos \frac{2\pi \cdot 0}{n} = \cos 0 = 1.$$

3 Konstruierbarkeit mit Zirkel und Lineal

Der Punkt $(1, 0)$ ist somit ein Eckpunkt jedes regelmäßigen Vielecks im Einheitskreis. Sei nun die Zahl $\cos(2\pi/n)$ konstruierbar. Dann ist nach Satz 3.13 auch

$$z_1 = \cos \frac{2\pi}{n} + i \cdot \sin \frac{2\pi}{n}$$

konstruierbar. Mit

$$|z_1 - z_0| = |z_1 - 1|$$

erhalten wir insofern den eindeutigen Abstand zweier Eckpunkte unseres regelmäßigen n -Ecks. Durch die Definition regelmäßiger Vielecke gilt

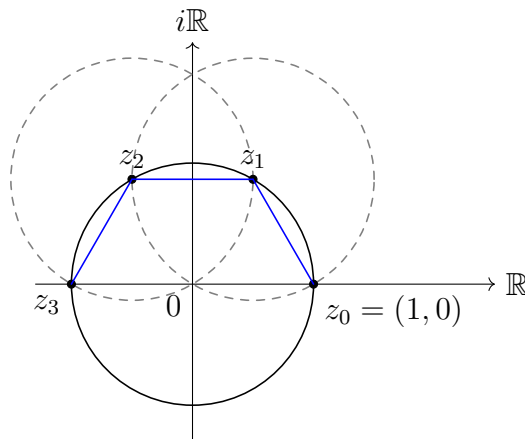
$$|z_{k-1} - z_k| = |z_k - z_{k+1}|$$

für alle k und somit

$$S^1 \cap K_{|z_1 - z_0|}(z_k) = \{z_{k-1}, z_{k+1}\}.$$

Iterativ erhalten wir deshalb durch den Schnitt von S^1 mit dem konstruierbaren Kreis $K_{|z_1 - z_0|}(z_1)$ den bekannten Punkt z_0 und den neuen Eckpunkt z_2 . Den nächsten Eckpunkt z_3 erhalten wir durch das Schneiden von S^1 mit dem Kreis $K_{|z_1 - z_0|}(z_2)$. Dieses Verfahren setzen wir fort, bis alle Eckpunkte $z_0, \dots, z_{n-1}$ gefunden wurden. $\square$

Die folgende Abbildung zeigt das Verfahren zur Konstruktion weiterer Eckpunkte, exemplarisch für die Ecken z_0, z_1, z_2 und z_3 des regelmäßigen Sechsecks:



Die Konstruierbarkeit des Punktes z_1 , der dieses iterative Verfahren für das regelmäßige Sechseck erlaubt, werden wir im folgenden Kapitel genauer betrachten.

Wir haben es nun endlich geschafft, die Konstruierbarkeit eines regelmäßigen Vielecks von der Konstruierbarkeit einer einzigen Zahl abhängig zu machen. Gelingt es uns im Folgenden, die Zahl $\cos 2\pi/n$ mithilfe einer Kombination der Verknüpfungen $+$, $-$, $\cdot$, $\div$ und $\sqrt{\cdot}$ durch rationale Zahlen darzustellen, so können wir eindeutig feststellen, ob das regelmäßige n -Eck konstruierbar ist.

4 Regelmäßige Vielecke mit wenigen Ecken

Kapitel 2 und Kapitel 3 haben die theoretischen Grundlagen für die Untersuchung der Konstruierbarkeit regelmäßiger Vielecke geschaffen. Um zu überprüfen, inwieweit die bisherigen Resultate bereits zur Konstruktion konkreter Vielecke ausreichen, betrachten wir in diesem Kapitel zunächst regelmäßige Vielecke mit wenigen Ecken. Unser Ziel wird es dabei sein, alle regelmäßigen Vielecke mit bis zu sieben Ecken zu konstruieren und dabei mögliche Grenzen der bisherigen Methoden sichtbar zu machen.

Wir beginnen mit der Konstruktion des regelmäßigen 3- und 4-Ecks, also des gleichseitigen Dreiecks und des Quadrats.

4.1 Das regelmäßige Drei- und Viereck

Für das besagte regelmäßige Dreieck benötigen wir die dritten Einheitswurzeln und somit die Nullstellen des Polynoms

$$z^3 - 1.$$

Da wir bereits gezeigt haben, dass jedes Polynom der Form

$$z^n - 1$$

für $n \in \mathbb{N}$ eine triviale Nullstelle $z_0 = 1$ besitzt, erhalten wir durch Polynomdivision

$$(z^3 - 1) \div (z - 1) = z^2 + z + 1.$$

Da dieser Schritt schlussendlich in allen Konstruktionen regelmäßiger n -Ecke getätigt werden wird, halten wir fest, dass das Polynom

$$z^n - 1$$

durch die triviale Nullstelle $z_0 = 1$ immer als

$$(z - 1)(z^{n-1} + z^{n-2} + \cdots + z + 1)$$

4 Regelmäßige Vielecke mit wenigen Ecken

darstellbar ist und wir daher immer nach den Nullstellen des Polynoms

$$z^{n-1} + z^{n-2} + \dots + z + 1$$

suchen.

Kommen wir zurück zum Polynom

$$z^2 + z + 1.$$

Dieses besitzt die Nullstellen

$$z_1 = -\frac{1}{2} + i \cdot \frac{\sqrt{3}}{2} \quad \text{und} \quad z_2 = -\frac{1}{2} - i \cdot \frac{\sqrt{3}}{2}.$$

Ohne explizit nach dem Wert von

$$\cos\left(\frac{2\pi}{3}\right)$$

gesucht zu haben, konnten wir diesen bereits durch die Berechnung der dritten Einheitswurzeln bestimmen. Genauer gesagt gilt

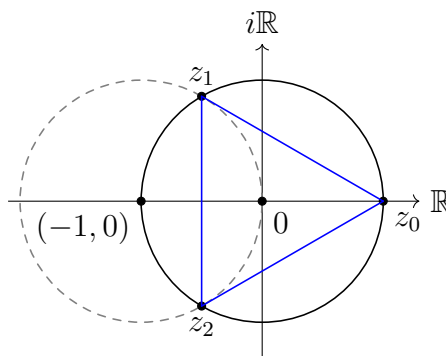
$$\cos\frac{2\pi}{3} = -\frac{1}{2}.$$

Dieser Wert lässt sich zweifelsohne durch eine Verkettung rationaler Zahlen mit den Verknüpfungen $+$, $-$, $\cdot$, $\div$ und $\sqrt{}$ schreiben, da schon $-\frac{1}{2}$ in den rationalen Zahlen liegt.

Das regelmäßige Dreieck ist somit das erste konstruierbare regelmäßige Vieleck [Str19, S. 17-18]. Tatsächlich haben wir eine geometrische Konstruktion der dritten Einheitswurzeln bereits in Kapitel 3.1 gesehen. Dort haben wir mithilfe des Schnitts des Einheitskreises mit dem Kreis $K_1(-1)$ die einzigen nicht-trivialen Eckpunkte

$$z_1 = -\frac{1}{2} + i \cdot \frac{\sqrt{3}}{2} \quad \text{und} \quad z_2 = -\frac{1}{2} - i \cdot \frac{\sqrt{3}}{2}$$

des regelmäßigen Dreiecks bereits konstruiert.



4 Regelmäßige Vielecke mit wenigen Ecken

Die Konstruktion des regelmäßigen 4-Ecks (des Quadrats) stellt uns vor noch weniger Herausforderungen, denn es gilt

$$\cos \frac{2\pi}{4} = \cos \frac{\pi}{2} = 0$$

und da der Punkt $(0, 0)$ zu unserer Startmenge $\mathcal{M} = \{(0, 0), (1, 0)\}$ gehört, ist der Eckpunkt z_1 problemlos mithilfe einer Senkrechten zur x-Achse durch den Ursprung konstruierbar.

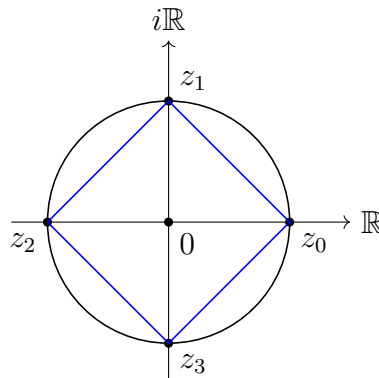
Auch hier lassen sich alternativ die Nullstellen des Polynoms

$$z^4 - 1$$

durch die Zerlegung

$$z^4 - 1 = (z - 1)(z - i)(z + 1)(z + i)$$

schnell bestimmen [Str19, S. 18-19].



Die Konstruierbarkeit von gleichseitigen Dreiecken und Quadraten ist nicht sonderlich überraschend, da diese Vielecke zu den wichtigsten geometrischen Figuren der Geschichte zählen. Die Konstruktionen waren daher auch schon im alten Griechenland bekannt.

4.2 Das regelmäßige Fünfeck

Die fünften Einheitswurzeln konnten wir bislang nur durch

$$z_k = e^{2\pi i k/5}$$

für $k = 0, \dots, 4$ darstellen. Jedoch ließ sich bisher lediglich für die triviale Nullstelle $z_0 = 1$ verifizieren, ob der Realteil

$$\cos\left(\frac{2\pi k}{5}\right)$$

4 Regelmäßige Vielecke mit wenigen Ecken

dieser komplexen Nullstellen durch die erlaubten Rechenoperationen $+$, $-$, $\cdot$, $\div$ und $\sqrt{\cdot}$ aus den rationalen Zahlen konstruierbar ist.

Betrachten wir das Polynom

$$z^5 - 1,$$

welches alle fünften Einheitswurzeln als Nullstellen besitzt, so können wir die triviale Nullstelle $z_0 = 1$ herausteilen und erhalten das Polynom

$$(z^5 - 1) : (z - 1) = z^4 + z^3 + z^2 + z + 1$$

mit den Nullstellen $z_1, \dots, z_4$. Da $z = 0$ keine Nullstelle des Polynoms ist, gilt

$$\begin{aligned} z^4 + z^3 + z^2 + z + 1 &= 0 & | \div z^2 \\ z^2 + z + 1 + z^{-1} + z^{-2} &= 0. \end{aligned}$$

Wegen der Gleichheit

$$(z + z^{-1})^2 = z^2 + 2 + z^{-2}$$

können wir unsere Gleichung auch wie folgt darstellen:

$$(z + z^{-1})^2 + (z + z^{-1}) - 1 = 0.$$

Nun lässt sich leicht erkennen, dass wir den Ausdruck $z + z^{-1}$ durch

$$u = z + z^{-1}$$

substituieren können. Die Substitution führt in Verbindung mit 2.12 und 2.13 unmittelbar zu einer Reduktion der vier komplexen Nullstellen auf zwei reelle Nullstellen, denn für z_1 und z_4 gilt

$$u_1 = z_1 + z_1^{-1} = z_1 + z_4 = 2 \cos \frac{2\pi}{5}$$

und analog für z_2 und z_3

$$u_2 = z_2 + z_2^{-1} = z_2 + z_3 = 2 \cos \frac{4\pi}{5}.$$

Die reellen Lösungen der durch die Substitution entstandenen quadratischen Gleichung

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

können wir nun schnell bestimmen. Die Berechnung ergibt

$$u_1 = \frac{-1 + \sqrt{5}}{2} \quad \text{und} \quad u_2 = \frac{-1 - \sqrt{5}}{2}.$$

Da

$$\cos\left(\frac{2\pi}{5}\right) > 0 \quad \text{und} \quad \cos\left(\frac{4\pi}{5}\right) < 0$$

gilt, entspricht die positive Nullstelle

$$u_1 = \frac{-1 + \sqrt{5}}{2}$$

dem Ausdruck

$$2 \cos\left(\frac{2\pi}{5}\right).$$

Somit gilt

$$\cos \frac{2\pi}{5} = \frac{-1 + \sqrt{5}}{4}$$

und das regelmäßige Fünfeck ist nach dem Hauptsatz 3.14 konstruierbar [Toe10, S. 300-301].

4.3 Das regelmäßige Sechseck und regelmäßige 2n-Ecke

Um zu prüfen, ob das regelmäßige Sechseck konstruierbar ist, brauchen wir nur die bisherige Polarkoordinatendarstellung der n -ten Einheitswurzeln. Diese sind für den Fall $n = 6$ definiert durch

$$z_k = e^{2\pi i k / 6}$$

für $k \in \{0, \dots, 5\}$. Somit lässt sich z_2 wie folgt darstellen:

$$z_2 = e^{4\pi i / 6} = e^{2\pi i / 3} = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}.$$

Den Wert $\cos \frac{2\pi}{3}$ haben wir allerdings schon bei der Konstruktion des regelmäßigen Dreiecks bestimmt. Somit ist der Eckpunkt z_2 des regelmäßigen Sechsecks konstruierbar. Mithilfe der in Satz 3.6 konstruierten Winkelhalbierenden können wir nun auch die Einheitswurzel z_1 konstruieren.

Durch

$$z_0 = e^{i\varphi_0} \quad \text{mit} \quad \varphi_0 = 0$$

und

$$z_2 = e^{i\varphi_2} \quad \text{mit} \quad \varphi_2 = \frac{2\pi}{3}$$

schließt die Winkelhalbierende des Winkels $\angle z_0 z_2$ genau den Winkel $\varphi_1 = \frac{\pi}{3}$ mit der positiven reellen Zahlenachse ein. Die Winkelhalbierende schneidet den Einheitskreis folglich genau im Punkt

$$z_1 = e^{i\pi/3}.$$

4 Regelmäßige Vielecke mit wenigen Ecken

Durch die Konstruierbarkeit von z_1 ist somit nach dem Hauptsatz 3.14 auch das regelmäßige Sechseck konstruierbar.

Die Winkelhalbierende ermöglicht es nun erstmals, von der konkreten Konstruktion einzelner n -Ecke auf die Konstruierbarkeit allgemeiner regelmäßiger Vielecke zu schließen. Dazu dient der folgende Satz:

Satz 4.1. *[Beu18, S. 245-246] Das regelmäßige n -Eck ist genau dann konstruierbar, wenn das regelmäßige $2n$ -Eck konstruierbar ist.*

Beweis. Sei zunächst das regelmäßige n -Eck konstruierbar. Dann sind insbesondere die n -ten Einheitswurzeln

$$z_k = e^{2\pi i k/n}$$

für $k \in \{0, \dots, n-1\}$ konstruierbar. Die $2n$ -ten Einheitswurzeln sind hingegen die komplexen Zahlen

$$\tilde{z}_k = e^{2\pi i k/2n} = e^{\pi i k/n}$$

für $k \in \{0, \dots, 2n-1\}$. Aufgrund von

$$z_k = \tilde{z}_{2k}$$

sind insbesondere die Punkte $\tilde{z}_0$ und $\tilde{z}_2$ konstruierbar. Nun können wir wie in der Konstruktion des regelmäßigen Sechsecks die Winkelhalbierende des Winkels $\angle \tilde{z}_0 \tilde{z}_2$ konstruieren. Diese schließt mit der positiven reellen Zahlenachse den Winkel $\frac{\pi}{n}$ ein und schneidet somit den Einheitskreis im Punkt $\tilde{z}_1 = e^{i\pi/n}$. Daher ist $\tilde{z}_1$ ebenfalls konstruierbar und somit auch das gesamte $2n$ -Eck.

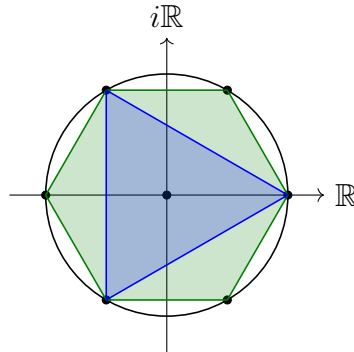
Umgekehrt folgt die Konstruierbarkeit des n -Ecks unmittelbar aus der Konstruierbarkeit des $2n$ -Ecks, denn es gilt

$$\tilde{z}_{2k} = e^{2\pi i k/n} = z_k.$$

□

4 Regelmäßige Vielecke mit wenigen Ecken

Das folgende Bild zeigt die geometrische Lage des n -Ecks und des $2n$ -Ecks am Beispiel des 3- und 6-Ecks:



Aus der Konstruierbarkeit des 3-, 4- und 5-Ecks können wir folglich die Konstruierbarkeit einer Vielzahl weiterer regelmäßiger Vielecke ableiten. So können wir unter anderem das regelmäßige 8-, 10- und 12-Eck konstruieren. Für das regelmäßige 7-, 9- und 11-Eck fehlen uns bislang die Nachweise der Konstruierbarkeit. Ohne dabei zu weit vorgreifen zu wollen, werden sich unsere Untersuchungen schon bald darauf beschränken, warum diese Vielecke nicht konstruierbar sind. Zunächst wollen wir jedoch – wie bereits für die bisherigen Vielecke – einen Konstruktionsversuch für das regelmäßige 7-Eck unternehmen.

4.4 Das problematische Siebeneck

Mit dem regelmäßigen Siebeneck erreichen wir die erste Hürde eines regelmäßigen Vielecks, dessen Konstruierbarkeit die alten Griechen vor über 2000 Jahren mit ihrem geometrischen Zugang nicht eindeutig beweisen oder widerlegen konnten. Auch mit den bislang in dieser Arbeit entwickelten Methoden lässt sich die Frage der Konstruierbarkeit des Siebenecks noch nicht abschließend beantworten. Der nachfolgende Konstruktionsversuch wird jedoch den tieferen Einstieg in die Algebra im folgenden Kapitel motivieren.

Analog zu unseren bisherigen Vielecken beginnen wir unsere Betrachtung mit dem Polynom

$$z^6 + z^5 + z^4 + z^3 + z^2 + z + 1.$$

$z = 0$ ist keine Nullstelle dieses Polynoms. Somit gilt

$$\begin{aligned} z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 &= 0 & | \div z^3 \\ z^3 + z^2 + z + 1 + z^{-1} + z^{-2} + z^{-3} &= 0. \end{aligned}$$

4 Regelmäßige Vielecke mit wenigen Ecken

Zusätzlich halten wir die folgenden Identitäten fest:

- $(z + z^{-1})^3 = z^3 + 3z + 3z^{-1} + z^{-3},$
- $(z + z^{-1})^2 = z^2 + 2 + z^{-2}.$

Die Identitäten ermöglichen die folgende Transformation unserer Gleichung:

$$\begin{aligned} & z^3 + z^2 + z + 1 + z^{-1} + z^{-2} + z^{-3} = 0 \\ \Leftrightarrow & (z + z^{-1})^3 + (z + z^{-1})^2 - 2(z + z^{-1}) - 1 = 0. \end{aligned}$$

Wir können nun, wie schon beim Fünfeck, eine Substitution

$$u = z + z^{-1}$$

vornehmen [Toe10, S. 301]. Die Substitution fasst jeweils zwei zueinander komplex konjugierte Nullstellen zusammen und reduziert das Problem dadurch auf die Bestimmung der drei reellen Lösungen der kubischen Gleichung

$$u^3 + u^2 - 2u - 1 = 0.$$

Die explizite Lösung kubischer Gleichungen stellte lange Zeit ein zentrales Problem der Algebra dar. Im 16. Jahrhundert konnten schließlich allgemeine Lösungsformeln gefunden werden, wobei die Darstellung der Lösungen im Allgemeinen nicht ohne Kubikwurzeln auskommt.

Da diese Lösungsformeln für unsere weitere Untersuchung nicht benötigt werden, verzichten wir in dieser Arbeit auf ihre explizite Herleitung. Eine solche Herleitung der Lösungsformeln findet sich unter anderem bei [Bos23, S. 369-374]. Wir halten jedoch fest, dass die bekannten Lösungsformeln für die Gleichung

$$u^3 + u^2 - 2u - 1 = 0$$

Kubikwurzeln enthalten und somit nicht allein durch rationale Zahlen und die Rechenoperationen $+, -, \cdot, \div$ und Quadratwurzeln beschrieben werden können.

Trotzdem können wir mithilfe unserer Betrachtung darauf schließen, dass sich prinzipiell auch ein expliziter Ausdruck für

$$\cos\left(\frac{2\pi}{7}\right)$$

bestimmen lässt. Aus einer solchen Darstellung lässt sich die Konstruierbarkeit des regelmäßigen Siebenecks allerdings nicht folgern, da unsere bisherigen

Ergebnisse keine Aussagen über die Konstruierbarkeit allgemeiner Kubikwurzeln liefern.

Wir müssen die Frage nach der Konstruierbarkeit des Siebenecks folglich noch etwas zurückstellen. Jedoch hat uns der Konstruktionsversuch aufgezeigt, dass wir für bestimmte Vielecke noch weitere algebraische Grundlagen benötigen. Insbesondere haben wir bislang noch kein Kriterium dafür gefunden, wann ein regelmäßiges Vieleck nicht konstruierbar ist.

Das folgende Kapitel soll daher alle Grundlagen der Algebra zusammenstellen, die für einen Nachweis oder eine Widerlegung der Konstruierbarkeit regelmäßiger Vielecke notwendig sind.

5 Algebraische Grundlagen der Konstruierbarkeit

Durch die grundlegende Betrachtung der bisherigen Kapitel konnten wir bereits eine Reihe wichtiger mathematischer Beobachtungen zur Konstruierbarkeit regelmäßiger n -Ecke festhalten und beweisen. Der Hauptsatz 3.14 reduziert die Frage der Konstruierbarkeit eines regelmäßigen n -Ecks dabei auf die Konstruierbarkeit der reellen Zahl

$$\cos \frac{2\pi}{n}.$$

Es ist uns bereits gelungen, die Konstruierbarkeit einiger n -Ecke zu beweisen. Das regelmäßige Siebeneck hat uns allerdings aufgezeigt, dass wir noch weit davon entfernt sind, die Konstruierbarkeit aller regelmäßiger n -Ecke zu betrachten. Insbesondere fehlt uns bis jetzt ein Kriterium, wann ein regelmäßiges n -Eck nicht konstruierbar ist.

In diesem Kapitel werden wir deutlich tiefer in die Algebra eintauchen. Dabei wollen wir uns an dem Ziel orientieren, exakt bestimmen zu können, wann eine reelle Zahl konstruierbar ist.

5.1 Algebraische Zahlen und das Minimalpolynom

Alle Polynome eines Körpers K lassen sich wie folgt zusammenfassen:

Definition 5.1 (Der Polynomring). *Die Menge*

$$K[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \mid n \in \mathbb{N}_0, a_0, \dots, a_n \in K\}$$

heißt **Polynomring** über K .

Für ein von Null verschiedenes Polynom

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$$

mit $a_n \neq 0$ heißt a_n der **Leitkoeffizient** von P .

Gilt insbesondere $a_n = 1$, so bezeichnen wir das Polynom P als **normiert**.

Der Index $n \in \mathbb{N}_0$ des Leitkoeffizienten heißt **Grad des Polynoms** und wir schreiben

$$\deg(P) = n.$$

Dem Nullpolynom ordnen wir den Grad $-\infty$ zu.

Definition 5.2 (Algebraische Zahlen). *Sei $K \subseteq \mathbb{C}$ ein Körper. Eine komplexe Zahl a heißt **algebraisch** über K , wenn es ein Polynom $P \in K[x] \setminus \{0\}$ gibt, für das*

$$P(a) = 0$$

gilt.

Ist $K = \mathbb{Q}$, so sind die algebraischen Zahlen über $\mathbb{Q}$ die Teilmenge der komplexen Zahlen, die sich als Nullstellen von Polynomen mit rationalen Koeffizienten darstellen lassen.

Für die späteren Hauptresultate dieser Arbeit wird uns meistens die Konstruktion $K = \mathbb{Q}$ ausreichen. Wir werden allerdings im Hauptsatz dieses Kapitels und im abschließenden Kapitel zur Konstruierbarkeit regelmäßiger Vielecke die in der Definition beschriebene Verallgemeinerung über einem beliebigen Körper $K \subset \mathbb{C}$ benötigen.

Die Definition der algebraischen Zahlen erlaubt es uns, das vielleicht wichtigste algebraische Hilfsmittel für die Konstruierbarkeit regelmäßiger Vielecke kennenzulernen. Dieses basiert auf den Erkenntnissen des folgenden Satzes:

Satz 5.3 (Satz über das Minimalpolynom). *[Beu18, S. 222-223] Sei $K \subset \mathbb{C}$ ein Körper und $a \in \mathbb{C}$ algebraisch über K . Dann gilt:*

1. *a ist die Nullstelle unendlich vieler Polynome aus $K[x]$.*

5 Algebraische Grundlagen der Konstruierbarkeit

2. Es gibt ein Polynom $P \neq 0$ kleinsten Grades aus $K[x]$, welches a als Nullstelle besitzt.
3. Es gibt ein eindeutig bestimmtes normiertes Polynom $P \neq 0$ kleinsten Grades aus $K[x]$, welches a als Nullstelle besitzt.

Beweis. 1. Sei $P \in K[x] \setminus \{0\}$, mit der Eigenschaft $P(a) = 0$ und $\tilde{P}(x)$ ein beliebiges weiteres Polynom über dem Körper K . Dann ist auch

$$f(x) := P(x) \cdot \tilde{P}(x)$$

ein Polynom aus $K[x]$ und es gilt

$$f(a) = P(a) \cdot \tilde{P}(a) = 0 \cdot \tilde{P}(a) = 0$$

für jedes Polynom $\tilde{P} \in K[x]$. Da $\tilde{P}$ somit ein beliebiges Polynom aus $K[x]$ ist, gibt es unendlich viele Polynome aus $K[x]$, die a als Nullstelle besitzen.

2. Da a algebraisch ist, gibt es unendlich viele von Null verschiedene Polynome $f \in K[x]$ mit

$$f(a) = 0.$$

Betrachten wir nun die Menge

$$M := \{\deg(f) \mid f \in K[x] \setminus \{0\}, f(a) = 0\}.$$

Für M gilt durch die Definition des Grades eines Polynoms

$$M \subseteq \mathbb{N}.$$

Da jede nichtleere Menge natürlicher Zahlen ein Minimum besitzt, gibt es ein Polynom

$$\tilde{P} \in K[x]$$

mit $\tilde{P}(a) = 0$ und

$$\deg(\tilde{P}) \leq \deg(f) \quad \text{für alle } f \in K[x] \text{ mit } f(a) = 0.$$

3. **Existenz:** Sei $P \neq 0$ ein Polynom von minimalem Grad j aus $K[x]$, also

$$P(x) = a_j x^j + a_{j-1} x^{j-1} + \cdots + a_1 x + a_0$$

mit $a_j \neq 0$. Dann ist auch

$$f(x) = a_j^{-1} \cdot P(x)$$

5 Algebraische Grundlagen der Konstruierbarkeit

ein Polynom aus $K[x]$ und für den Leitkoeffizienten $\tilde{a}_j$ von f gilt

$$\tilde{a}_j = a_j^{-1} \cdot a_j = 1.$$

Somit ist f normiert und es gilt $\deg(f) = j = \deg(P)$. Daher ist f das gesuchte normierte Polynom minimalen Grades.

Eindeutigkeit: Seien

$$\begin{aligned} f(x) &= x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \quad \text{und} \\ g(x) &= x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0 \end{aligned}$$

von Null verschiedene Polynome minimalen Grades n aus $K[x]$, die a als Nullstelle besitzen.

Dann ist

$$(f - g)(x) = (a_{n-1} - b_{n-1})x^{n-1} + \cdots + (a_1 - b_1)x + (a_0 - b_0)$$

ebenfalls ein Polynom aus $K[x]$ und wegen $f(a) = 0 = g(a)$ folgt auch

$$(f - g)(a) = f(a) - g(a) = 0.$$

Da $\deg(f - g) < n$ gilt, muss aufgrund des minimalen Grades von f und g schon

$$(f - g)(x) = 0$$

und somit

$$f = g$$

gelten.

□

Definition 5.4 (Das Minimalpolynom). [Beu18, S. 223] Sei $K \subseteq \mathbb{C}$ ein Körper und a algebraisch über K . Dann existiert nach Satz 5.3(3) ein eindeutiges normiertes Polynom $P \neq 0$ minimalen Grades aus $K[x]$, welches a als Nullstelle besitzt. Dieses Polynom heißt das **Minimalpolynom von a über K** .

Die Definition des Minimalpolynoms erlaubt es uns, die algebraischen Zahlen genauer zu charakterisieren.

Zunächst einmal ist jedes $a \in \mathbb{Q}$ über dem Körper $\mathbb{Q}$ algebraisch, da mit

$$P(x) = x - a$$

mindestens ein Polynom aus $\mathbb{Q}[x]$ gefunden werden kann, für das

$$P(a) = a - a = 0$$

gilt. Wir können sogar unschwer erkennen, dass das besagte normierte Polynom auch das Minimalpolynom von a über $\mathbb{Q}$ ist, denn es gibt, bis auf das ausgeschlossene Nullpolynom, kein Polynom $f \in \mathbb{Q}[x]$ mit $\deg(f) < \deg(P) = 1$ und $f(a) = 0$.

Unter anderem sind aber auch $\sqrt{2}$ und $\sqrt{3}$ algebraisch über $\mathbb{Q}$, da diese die positiven reellen Nullstellen der Polynome

$$g(x) = x^2 - 2 \quad \text{und} \quad h(x) = x^2 - 3$$

sind. g und h sind dabei die jeweiligen Minimalpolynome von $\sqrt{2}$ und $\sqrt{3}$ über $\mathbb{Q}$, denn beide Zahlen sind irrational und daher keine Nullstellen eines linearen Polynoms mit rationalen Koeffizienten.

Tatsächlich sind alle Quadratwurzeln rationaler Zahlen algebraische Zahlen über $\mathbb{Q}$. Vielleicht wird nun schon deutlich, auf welchen Weg wir uns in diesem Kapitel begeben, denn auch für die konstruierbaren Zahlen haben wir bereits gesehen, dass alle rationalen Zahlen und alle Quadratwurzeln aus positiven rationalen Zahlen konstruierbar sind.

Eine große Hürde besteht jedoch in der Suche nach dem Minimalpolynom einer algebraischen Zahl über einem beliebigen Körper $K \subseteq \mathbb{C}$. Zudem wird es, selbst im Fall $K = \mathbb{Q}$, bei einem Polynom höheren Grades sehr kompliziert nachzuweisen, dass es sich tatsächlich um das Minimalpolynom einer algebraischen Zahl handelt. Diesem Problem widmen wir uns im folgenden Unterkapitel.

5.2 Irreduzible Polynome

Über das Minimalpolynom einer algebraischen Zahl a ist es uns gelungen, einen Einstieg in die algebraischen Hilfsmittel zu finden, die wir schon bald dazu verwenden werden, um eindeutig nachzuweisen, welche regelmäßigen Vielecke tatsächlich konstruierbar sind. Da wir allerdings für Polynome höheren Grades und Polynome über einem beliebigen Körper $K \subseteq \mathbb{C}$ noch kein Kriterium gefunden haben, um ein Minimalpolynom einer Zahl a zu finden und zu zeigen, dass es sich dabei wirklich um das Minimalpolynom von a handelt, müssen wir noch tiefer in die Algebra eindringen. Dazu hilft uns die folgende Definition:

Definition 5.5 (irreduzible Polynome). *[Beu18, S. 203] Ein Polynom $f \in K[x]$ heißt **reduzibel** über K , falls sich f als $f = gh$ schreiben lässt, wobei g und h Polynome aus $K[x]$ sind mit $\deg(g) \geq 1$ und $\deg(h) \geq 1$. Ein Polynom $f \in K[x]$ heißt **irreduzibel** über K , falls es nicht reduzibel über K ist.*

Ein Polynom $f \in K[x]$ ist folglich irreduzibel, wenn die Produktschreibweise $f = gh$ bereits impliziert, dass g oder h konstant sind.

5 Algebraische Grundlagen der Konstruierbarkeit

Die Verbindung irreduzibler Polynome zum Minimalpolynom ist unschwer zu erkennen. Dennoch benötigen wir noch ein wenig Vorarbeit, bevor wir deren exakte Beziehungen formulieren können. Wir formalisieren dazu zunächst die bereits in Kapitel 4 verwendete Polynomdivision:

Satz 5.6 (Polynomdivision). *[Beu18, S. 196] Sei K Körper und seien $f, g \in K[x]$. Ist $g \neq 0$, dann gibt es eindeutig bestimmte Polynome $q, r \in K[x]$ mit*

$$f = qg + r \quad \text{und} \quad \deg(r) < \deg(g).$$

Die Polynomdivision ist ein essenzieller Bestandteil unserer algebraischen Untersuchungen. Unter anderem lässt sich mithilfe der Polynomdivision noch exakter bestimmen, wie das Minimalpolynom einer komplexen Zahl a über einem Körper $K \subseteq \mathbb{C}$ mit allen weiteren Polynomen über K zusammenhängt, die a als Nullstelle besitzen.

Lemma 5.7. *[Beu18, S. 224] Sei $K \subseteq \mathbb{C}$ ein Körper und a algebraisch über K . Sei weiterhin f das Minimalpolynom von a über K . Sei zudem $g \in K[x]$ ein weiteres Polynom mit der Nullstelle a .*

Dann gilt $f \mid g$. Das heißt, dass es ein Polynom $q \in K[x]$ mit $g = q \cdot f$ gibt.

Beweis. Mithilfe der Polynomdivision aus Satz 5.6 finden wir Polynome $q, r \in K[x]$ mit

$$g = q \cdot f + r \quad \text{und} \quad \deg(r) < \deg(f).$$

Setzen wir a in diese Gleichung ein, erhalten wir

$$\begin{aligned} g(a) &= q(a) \cdot f(a) + r(a) \\ \Rightarrow 0 &= q(a) \cdot 0 + r(a) \\ \Rightarrow 0 &= r(a). \end{aligned}$$

r besitzt folglich ebenfalls eine Nullstelle in a und es gilt $\deg(r) < \deg(f)$. Da f bereits das Minimalpolynom von a über K ist, muss r daher bereits das Nullpolynom sein. Daher gilt

$$g = q \cdot f.$$

□

Das Lemma zeigt eine weitere nützliche Eigenschaft des Minimalpolynoms einer komplexen Zahl a . Über einem Körper $K \subseteq \mathbb{C}$ erreichen wir durch die Multiplikation des Minimalpolynoms mit einem beliebigen Polynom alle Polynome, die a als Nullstelle besitzen. Damit haben wir nun genug Vorarbeit geleistet, um die direkte Verbindung zwischen dem Minimalpolynom und irreduziblen Polynomen herzustellen.

Satz 5.8. [Beu18, S. 224] Sei $K \subseteq \mathbb{C}$ ein Körper und $a \in \mathbb{C}$. Sei darüber hinaus $f \neq 0$ ein normiertes Polynom aus $K[x]$ mit $f(a) = 0$. Dann gilt: f ist genau dann das Minimalpolynom von a über K , wenn f irreduzibel über K ist.

Beweis. Angenommen, f wäre reduzibel über K . Dann gibt es Polynome $g, h \in K[x]$ mit $1 \leq \deg(g), \deg(h) < \deg(f)$ und $f = gh$. Zudem gilt

$$0 = f(a) = (g \cdot h)(a) = g(a) \cdot h(a).$$

Dann gilt allerdings entweder $g(a) = 0$ oder $h(a) = 0$ und wir hätten mit g oder h ein Polynom mit Nullstelle a gefunden, das einen kleineren Grad als f hat. Dies steht im Widerspruch zur Minimalität des Grades von f .

Sei nun f irreduzibel über K . Da a wegen $f(a) = 0$ algebraisch über K ist, existiert ein Minimalpolynom von a über K . Nehmen wir an, dass f nicht dieses Minimalpolynom von a ist. Da f aber, wie das gesuchte Minimalpolynom, normiert ist, muss das Minimalpolynom einen kleineren Grad als f haben. Sei daher $g \in K[x]$ das Minimalpolynom von a . Dann gilt $1 \leq \deg(g) < \deg(f)$ und $g(a) = 0$. Nach Lemma 5.7 gibt es dann ein weiteres Polynom $q \in K[x]$ mit

$$f = q \cdot g.$$

Dies steht jedoch im Widerspruch zur Irreduzibilität von f . □

Ist a algebraisch über einem Körper $K \subseteq \mathbb{C}$, so haben wir mithilfe irreduzibler Polynome über K nun eine Möglichkeit gefunden, um nachzuweisen, dass es sich bei einem Kandidaten für das Minimalpolynom von a über K auch tatsächlich um das gesuchte Minimalpolynom handelt.

Zu Beginn dieses Kapitels wollten wir zudem für Polynome höheren Grades über dem Körper $\mathbb{Q}$ herleiten, wie sich möglichst einfach das Minimalpolynom einer komplexen Zahl $a \in \mathbb{C}$ finden lässt. Daher wollen wir nun zeigen, dass wir einen Kandidaten für das Minimalpolynom über $\mathbb{Q}$ bereits durch dessen Irreduzibilität über $\mathbb{Z}$ bestätigen können. Dazu benötigen wir allerdings noch einige Vorbereitungen.

Definition 5.9 (Primitive Polynome). Sei

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

ein Polynom aus $\mathbb{Z}[x]$.

Das Polynom f heißt **primitiv**, wenn für den größten gemeinsamen Teiler seiner Koeffizienten

$$\text{ggT}(a_0, a_1, \dots, a_n) = 1$$

gilt.

Wir zeigen zunächst eine wichtige Eigenschaft primitiver Polynome:

Lemma 5.10. *Seien*

$$f(x), g(x) \in \mathbb{Z}[x]$$

primitive Polynome. Dann ist auch das Produkt

$$f(x)g(x)$$

primitiv.

Beweis. Seien

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \\ g(x) &= b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 \end{aligned}$$

primitive Polynome aus $\mathbb{Z}[x]$. Angenommen, das Produkt

$$h(x) := f(x) \cdot g(x) = c_{m+n} x^{m+n} + \cdots + c_1 x + c_0$$

mit

$$c_k = \sum_{i=0}^k a_i b_{k-i}$$

ist nicht primitiv. Dann existiert eine Primzahl p , die alle Koeffizienten von h teilt. Da f und g primitiv sind, gibt es jeweils einen kleinsten Index $r \in \{0, \dots, n\}$ beziehungsweise $s \in \{0, \dots, m\}$ mit

$$p \nmid a_r \quad \text{und} \quad p \nmid b_s.$$

Wir betrachten nun den Koeffizienten von x^{r+s} des Polynoms h . Dieser ist von der Form

$$c_{r+s} = a_0 b_{r+s} + a_1 b_{r+s-1} + \cdots + a_r b_s + \cdots + a_{r+s} b_0.$$

Nach unserer Wahl gilt allerdings für alle $i < r$ und für alle $j < s$

- $p \mid a_i$ und
- $p \mid b_j$.

Tatsächlich enthalten fast alle Summanden der obigen Summe entweder ein solches a_i oder ein solches b_j . Wir können feststellen, dass

$$a_r b_s$$

5 Algebraische Grundlagen der Konstruierbarkeit

der einzige Summand ist, der somit nicht unbedingt von p geteilt wird. Wegen

$$p \nmid a_r \quad \text{und} \quad p \nmid b_s$$

ist $a_r b_s$ allerdings tatsächlich nicht durch p teilbar und somit - aufgrund der Teilbarkeit jedes weiteren Summanden durch p - auch der Koeffizient c_{r+s} nicht. Dies ist allerdings ein Widerspruch zur Annahme, dass p alle Koeffizienten von h teilt. Somit ist das Produkt fg zweier primitiver Polynome f und g wieder primitiv. $\square$

Bemerkung 5.11. Der Beweis des Lemmas zeigt sogar eine stärkere Aussage:

Teilt eine Primzahl p alle Koeffizienten eines Produkts zweier Polynome aus $\mathbb{Z}[x]$, so teilt p bereits alle Koeffizienten eines der beiden Polynome.

Ein wichtiges Resultat liefert das folgende *Lemma von Gauß*.

Lemma 5.12 (Lemma von Gauß). *[Beu18, S. 206-207] Sei*

$$f(x) \in \mathbb{Z}[x]$$

ein primitives Polynom.

Ist f über $\mathbb{Q}$ reduzibel, so ist f bereits über $\mathbb{Z}$ reduzibel.

Beweis. Sei $f \in \mathbb{Z}[x]$ ein primitives Polynom, das über $\mathbb{Q}$ reduzibel ist. Dann existieren Polynome

$$\begin{aligned} g(x) &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \\ h(x) &= b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 \end{aligned}$$

in $\mathbb{Q}[x]$ mit

$$f(x) = g(x) \cdot h(x).$$

Da die Koeffizienten a_i und b_j rational sind, finden wir eine minimale natürliche Zahl $r \in \mathbb{N}$, sodass es Polynome

$$g_1, h_1 \in \mathbb{Z}[x]$$

mit

$$r \cdot f(x) = g_1(x) h_1(x)$$

gibt.

1. Fall: $r = 1$:

Dann gilt bereits

$$f(x) = g_1(x) \cdot h_1(x)$$

für Polynome $g_1, h_1 \in \mathbb{Z}[x]$. Also ist f auch über $\mathbb{Z}$ reduzibel.

2. Fall: $r > 1$:

Ist $r > 1$, so gibt es eine Primzahl p mit

$$p \mid r.$$

Die natürliche Zahl r teilt logischerweise alle Koeffizienten des Polynoms

$$r \cdot f(x).$$

Dann teilt allerdings auch schon p alle Koeffizienten und wegen

$$r \cdot f(x) = g_1(x)h_1(x)$$

teilt p auch alle Koeffizienten des Polynoms $g_1(x)h_1(x)$.

Nach der Bemerkung zu Lemma 5.10 teilt p somit alle Koeffizienten von g_1 oder von h_1 . Ohne Einschränkung sei g_1 das Polynom, dessen Koeffizienten alle von p geteilt werden. Somit existiert ein weiteres Polynom

$$g_2(x) \in \mathbb{Z}[x]$$

mit

$$g_1(x) = p \cdot g_2(x).$$

Folglich gilt:

$$r \cdot f(x) = g_1(x)h_1(x) = p \cdot g_2(x)h_1(x).$$

Dividieren wir diese Gleichung durch p , so erhalten wir

$$\frac{r}{p}f(x) = g_2(x)h_1(x).$$

Dies ist allerdings ein Widerspruch zur Voraussetzung, denn r sollte die kleinste natürliche Zahl sein, die eine Zerlegung von

$$r \cdot f(x)$$

in zwei Polynome über $\mathbb{Z}[x]$ erlaubt. □

Das Lemma von Gauß eröffnet uns eine völlig neue Betrachtung irreduzibler Polynome. Wollen wir zeigen, dass ein Polynom über $\mathbb{Q}$ irreduzibel ist, dann reicht es bereits aus, die Irreduzibilität des Polynoms über $\mathbb{Z}$ zu zeigen. Die Aussage des Lemmas wird im Abschlusskapitel eine zentrale Rolle spielen.

5.3 Körpererweiterungen

Unsere ersten Auseinandersetzungen mit konstruierbaren Zahlen in Kapitel 3 haben verdeutlicht, dass die Menge der konstruierbaren Zahlen einen Körper bildet. Insbesondere haben wir gezeigt, dass alle rationalen Zahlen aus der möglichst klein gewählten Startmenge $\mathcal{M} = \{0, 1\}$ konstruierbar sind. Allerdings reicht der Körper $\mathbb{Q}$ nicht aus, um alle konstruierbaren Zahlen zu beschreiben. Wir konnten zum Beispiel zeigen, dass auch alle Quadratwurzeln positiver rationaler Zahlen, die nicht unbedingt wieder in $\mathbb{Q}$ liegen, konstruierbar sind. Damit stellen sich wichtige Fragen für unsere weitere Betrachtung:

- Können wir eine genauere Darstellung für den Körper der konstruierbaren Zahlen finden?
- Sind noch weitere Rechenoperationen neben dem Verknüpfen rationaler Zahlen durch $+$, $-$, $\cdot$, $\div$ und $\sqrt{\cdot}$ erlaubt, um weitere Zahlen zu konstruieren?

Beide Fragen lassen sich nicht unmittelbar beantworten. Daher werden wir im Sinne dieses Kapitels zunächst einige algebraische Vorarbeiten leisten, die wir in diesem Unterkapitel genauer betrachten. Im folgenden Unterkapitel werden wir dann beide Fragen nahezu parallel beantworten.

Einen Einstieg in unsere Betrachtungen liefert die folgende Definition:

Definition 5.13 (Unterkörper und Körpererweiterungen). *[Beu18, S. 225] Sei L ein Körper und $K \subseteq L$. Ist K bezüglich der von L induzierten Addition und Multiplikation selbst ein Körper, so heißt K ein **Unterkörper** von L . In diesem Fall nennen wir den Körper L eine **Körpererweiterung** (oder einen **Oberkörper**) von K .*

Anhand der Definition lässt sich unschwer erkennen, dass der Körper $\mathbb{Q}$ ein Unterkörper des Körpers $\mathbb{R}$ ist. Diese Eigenschaften können wir sogar noch genauer ausführen:

Satz 5.14. *[Beu18, S. 225-226] Jeder Unterkörper von $\mathbb{R}$ enthält den Körper $\mathbb{Q}$. Damit ist $\mathbb{Q}$ der kleinste Unterkörper von $\mathbb{R}$.*

Beweis. Sei K ein Unterkörper von $\mathbb{R}$. Da K ein Körper ist, gilt

$$0 \in K \quad \text{und} \quad 1 \in K.$$

Da K unter der Addition abgeschlossen ist, sind daher auch die Elemente

$$1, 1 + 1, 1 + 1 + 1, \dots$$

5 Algebraische Grundlagen der Konstruierbarkeit

in K . Folglich gilt $\mathbb{N}_0 \subset K$.

Der Körper K enthält auch alle additiven Inversen seiner Elemente. Folglich gilt wegen $\mathbb{N} \subset K$ auch $\mathbb{Z} \subset K$. Zusätzlich enthält K auch alle multiplikativen Inversen seiner Elemente und es gilt $\mathbb{Q} \subseteq K$. $\square$

Mit dem Körper der konstruierbaren Zahlen haben wir in Satz 3.10 bereits einen Unterkörper von $\mathbb{R}$ kennengelernt, der alle rationalen Zahlen enthält. Wir halten zunächst eine weitere wichtige Eigenschaft von Unterkörpern fest:

Lemma 5.15. *[Beu18, S. 227] Seien $K_1, K_2, \dots$ Unterkörper von $\mathbb{C}$. Dann ist auch ihr Durchschnitt*

$$K := K_1 \cap K_2 \cap \dots$$

wieder ein Unterkörper.

Beweis. Da $K_1, K_2, \dots$ Körper sind, sind $0, 1 \in K_i$ für alle i und somit auch $0, 1 \in K$.

Seien nun $a, b \in K$. Dann gilt schon $a, b \in K_i$ für alle i . Da alle K_i abgeschlossen unter der Addition sind, ist auch $a + b \in K_i$ für alle i . Daher muss $a + b$ auch in K liegen. Analog ist K abgeschlossen unter der Multiplikation. Sei nun $c \in K$. Dann ist $c \in K_i$ für alle i und somit auch $-c$ in jedem K_i , da alle K_i Körper sind. Folglich gilt auch $-c \in K$. Analog finden wir in jedem Unterkörper K_i zu einem Element $d \in K \setminus \{0\}$ ein multiplikatives Inverses d^{-1} , das somit auch in jedem K_i liegt. d^{-1} liegt daher auch in K . $\square$

Die Tatsache, dass wir die Menge $\mathcal{M}$ aus Definition 3.3 sukzessive durch das Schneiden von Geraden und Kreisen erweitern können, motiviert die folgende Definition:

Definition 5.16 (Adjunktion einer Zahl). *[Beu18, S. 227] Sei K ein Unterkörper von $\mathbb{C}$ und $a \in \mathbb{C}$. Sei zudem $\mathcal{K}$ die Menge aller Unterkörper von $\mathbb{C}$, die K und a enthalten. Dann definieren wir*

$$K(a) := \bigcap_{U \in \mathcal{K}} U.$$

*Wir sagen, dass die Menge $K(a)$ durch die **Adjunktion** von a zu K entsteht. Entsprechend definieren wir für $a_1, a_2, \dots, a_n \in \mathbb{C}$:*

Sei $\mathcal{K}$ die Menge aller Unterkörper von $\mathbb{C}$, die den Unterkörper K von $\mathbb{C}$ sowie $a_1, a_2, \dots, a_n$ enthalten. Dann ist

$$K(a_1, a_2, \dots, a_n) := \bigcap_{U \in \mathcal{K}} U$$

die Menge, die durch Adjunktion von $a_1, \dots, a_n$ aus K entsteht.

5 Algebraische Grundlagen der Konstruierbarkeit

Beschränken wir uns auf den Körper $\mathbb{Q}$, lässt sich die Adjunktion algebraischer Zahlen gut auf unser Erkenntnisinteresse zurückführen. Wir wissen schon, dass unsere gesuchte Zahl

$$\cos \frac{2\pi}{n}$$

häufig nicht rational ist. Allerdings wissen wir auch, dass es in bestimmten Fällen möglich ist, den gesuchten Ausdruck durch rationale Zahlen und Quadratwurzeln aus rationalen Zahlen darzustellen. Wenn wir also geschickt einige Quadratwurzeln zum Körper $\mathbb{Q}$ adjungieren, lässt sich möglicherweise eine Körpererweiterung finden, die

$$\cos \frac{2\pi}{n}$$

enthält.

Auch für die Adjunktion einer Zahl zu einem Körper wollen wir zunächst einige Eigenschaften festhalten.

Lemma 5.17. *[Beu18, S. 228] Sei K ein Unterkörper von $\mathbb{C}$ und a algebraisch über K . Dann ist $K(a)$ ein Körper und es gibt keinen Unterkörper M von $\mathbb{C}$, der a enthält und für den*

$$K \subsetneq M \subsetneq K(a)$$

gilt.

Beweis. $K(a)$ ist nach Definition 5.16 ein Durchschnitt von Unterkörpern von $\mathbb{C}$ und somit nach Lemma 5.15 ein Körper.

Sei nun M ein Unterkörper von $\mathbb{C}$ mit $a \in M$. Da $K(a)$ der Durchschnitt aller Unterkörper von $\mathbb{C}$ ist, die a enthalten, muss bereits $K(a) \subseteq M$ gelten. $\square$

Wir wollen die Gestalt des Körpers $K(a)$ nun genauer bestimmen. Dabei gelingt es uns sehr genau, die Form aller Elemente des Körpers zu beschreiben. Wir können sogar den Körper $K(a)$ mit dem Minimalpolynom von a über K in Beziehung setzen.

Satz 5.18. *[Beu18, S. 228-229] Sei K ein Unterkörper von $\mathbb{C}$ und a algebraisch über K . Sei darüber hinaus m der Grad des Minimalpolynoms von a über K . Dann gilt*

$$K(a) = \{b_0 + b_1a + \cdots + b_{m-1}a^{m-1} \mid b_0, b_1, \dots, b_{m-1} \in K\}.$$

5 Algebraische Grundlagen der Konstruierbarkeit

Beweis. Sei

$$L := \{b_0 + b_1a + \cdots + b_{m-1}a^{m-1} \mid b_0, b_1, \dots, b_{m-1} \in K\}.$$

Wir zeigen zunächst, dass die Menge L einen Unterkörper von $\mathbb{C}$ bildet. Offensichtlich ist L bezüglich der Addition eine Gruppe. Des Weiteren gelten alle notwendigen Rechengesetze, weil L eine Teilmenge von $\mathbb{C}$ ist.

Das Minimalpolynom f von a über K hat nach Voraussetzung den Grad m .

Daher gilt

$$f(a) = a^m + b_{m-1}a^{m-1} + \cdots + b_1a + b_0 = 0.$$

Folglich können wir die Potenz a^m über die Gleichung

$$a^m = -b_{m-1}a^{m-1} - \cdots - b_1a - b_0$$

darstellen. Analog lässt sich somit auch jede höhere Potenz a^k mit $k > m$ durch eine Linearkombination aus $1, a, \dots, a^{m-1}$ mit Koeffizienten aus K darstellen. Daher ist L unter der Multiplikation abgeschlossen.

Das Finden von multiplikativen Inversen in der Menge L ist etwas technischer und benötigt einige weitere Resultate aus der Algebra. Im Sinne der Fokussierung in dieser Arbeit sei daher an dieser Stelle auf den vollständigen Beweis der Existenz der multiplikativen Inversen in [Beu18, S. 228-229] verwiesen, der im dortigen Kapitel 6.5 [Beu18, S. 208-213] vorbereitet wird. Die Menge L ist somit ein Körper.

Nun lassen sich die beiden zu zeigenden Inklusionen

$$L \subseteq K(a) \quad \text{und} \quad K(a) \subseteq L$$

leicht folgern.

Zum einen gilt

$$b = 1 \cdot b + 0 \cdot a + \cdots + 0 \cdot a^{m-1} \in L$$

für jedes $b \in K$. Zum anderen finden wir eine Darstellung

$$a = 0 + 1 \cdot a + \cdots + 0 \cdot a^{m-1} \in L.$$

Nach Definition 5.16 entsteht $K(a)$ als Schnitt aller Körper, die K und a enthalten. Wir haben aber soeben gezeigt, dass L alle Elemente des Körpers K und a enthält. Daher folgt

$$K(a) \subseteq L.$$

Sei nun $c \in L$. Dann ist c von der Form

$$c = b_0 + b_1a + \cdots + b_{m-1}a^{m-1}$$

5 Algebraische Grundlagen der Konstruierbarkeit

mit Koeffizienten

$$b_0, b_1, \dots, b_{m-1} \in K.$$

Alle Koeffizienten und a liegen nach Definition 5.16 in $K(a)$. Damit liegt auch $c \in K(a)$ und es gilt

$$L \subseteq K(a).$$

□

Die besondere Struktur der Menge $K(a)$ erinnert nicht zufällig an Linearkombinationen der Menge

$$B = \{1, a, a^2, \dots, a^{n-1}\}$$

mit Koeffizienten aus K . Tatsächlich werden wir im Folgenden insbesondere den K -Vektorraum $K(a)$ betrachten. Diese Betrachtung ist aufgrund des folgenden Lemmas möglich:

Lemma 5.19. *Sei K ein Unterkörper eines Körpers L . Dann ist L ein Vektorraum über K .*

Beweis. Da L ein Körper ist, bildet $(L, +)$ eine abelsche Gruppe und wir können die Addition im Körper L als Vektorraumaddition auffassen.

Die Skalarmultiplikation definieren wir durch

$$K \times L \rightarrow L, \quad (\lambda, x) \mapsto \lambda x.$$

Da $K \subseteq L$ gilt und L unter der Multiplikation abgeschlossen ist, ist diese Abbildung wohldefiniert.

Die Distributivgesetze, die Assoziativität der Multiplikation und die Eigenschaft

$$1 \cdot x = x$$

folgen unmittelbar aus den Körperaxiomen von L . Folglich ist L ein K -Vektorraum. □

Für die Situation des Lemmas halten wir nun die folgende Definition fest:

Definition 5.20 (Grad einer Körpererweiterung). *[Beu18, S. 230] Sei K ein Unterkörper eines Körpers L und n die Dimension des Vektorraums L über K . Wir nennen n den **Grad der Körpererweiterung** von L über K und führen dafür die Kurzschreibweise*

$$n = [L : K]$$

ein.

5 Algebraische Grundlagen der Konstruierbarkeit

Die Definition erlaubt es uns, das nächste bedeutende Resultat kompakt zusammenzufassen:

Satz 5.21 (Dimension einer algebraischen Erweiterung). *[Beu18, S. 230] Sei K ein Unterkörper von $\mathbb{C}$ und a algebraisch über K . Sei zudem n der Grad des Minimalpolynoms von a über K . Dann besitzt der Vektorraum $K(a)$ über dem Körper K die Basis*

$$B = \{1, a, a^2, \dots, a^{n-1}\}.$$

Folglich gilt $[K(a) : K] = n$.

Beweis. Um zu zeigen, dass

$$B = \{1, a, a^2, \dots, a^{n-1}\}$$

eine Basis von $K(a)$ über K ist, muss B linear unabhängig und ein Erzeugendensystem von $K(a)$ sein.

Aus der expliziten Mengendarstellung von $K(a)$ aus Satz 5.18 folgt unmittelbar, dass B ein Erzeugendensystem von $K(a)$ ist.

Auch die lineare Unabhängigkeit von B ist problemlos nachweisbar.

Seien $b_0, b_1, \dots, b_{n-1} \in K$ mit

$$b_0 + b_1 a + \dots + b_{n-1} a^{n-1} = 0. \quad (3)$$

Zu zeigen ist, dass dann schon $b_i = 0$ für alle i gilt.

Wir betrachten das Polynom

$$f(x) = b_0 + b_1 x + \dots + b_{n-1} x^{n-1} \in K[x].$$

Für dieses gilt wegen (3) $f(a) = 0$ und zusätzlich $\deg(f) < n$. Das Minimalpolynom von a über K ist allerdings nach Voraussetzung vom Grad n . Somit muss f bereits das Nullpolynom sein und für alle $i \in \{0, \dots, n-1\}$ gilt somit $b_i = 0$. $\square$

Eine Körpererweiterung von K konnten wir nun schon genau charakterisieren. Tatsächlich können wir auch zwei Körpererweiterungen in einem wichtigen Resultat miteinander in Beziehung setzen:

Satz 5.22 (Gradsatz für Körpererweiterungen). *[Beu18, S. 230-232] Seien K und L zwei Unterkörper von $\mathbb{C}$ mit $K \subseteq L$. Dann gilt*

$$[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}]$$

5 Algebraische Grundlagen der Konstruierbarkeit

Beweis. Seien $[L : K] = m$ und $[K : \mathbb{Q}] = n$. Für den Vektorraum L über dem Körper K gibt es daher eine Basis

$$A = \{a_1, \dots, a_m\}.$$

Analog gibt es für den Vektorraum K über dem Körper $\mathbb{Q}$ eine Basis

$$B = \{b_1, \dots, b_n\}.$$

Wir konstruieren nun aus den Basen A und B eine Basis C des Vektorraums L über dem Körper $\mathbb{Q}$.

Die Zahlen a_i aus der Basis A sind Elemente des Körpers L . Wegen $K \subseteq L$ sind allerdings auch alle b_j aus der Basis B Elemente des Körpers L . Wir können über L folglich die Produkte $a_i \cdot b_j$ betrachten. Wir erhalten aufgrund von $i \in \{1, \dots, m\}$ und $j \in \{1, \dots, n\}$ $n \cdot m$ Produkte, die wieder in L liegen. Wir zeigen nun, dass die Menge

$$C := \{a_i \cdot b_j \mid i \in \{1, \dots, m\}, j \in \{1, \dots, n\}\}$$

eine Basis von L über $\mathbb{Q}$ ist. Dazu müssen wir nachweisen, dass C ein Erzeugendensystem und linear unabhängig ist.

Erzeugendensystem: Sei $a \in L$. Da A eine Basis von L über K ist, existieren $k_1, \dots, k_m \in K$ mit

$$a = k_1 a_1 + \dots + k_m a_m.$$

Wir können nun mithilfe der Basis B von K über dem Körper $\mathbb{Q}$ auch jedes der $k_i \in K$ als Linearkombination ausdrücken:

$$\begin{aligned} k_1 &= r_{11} b_1 + \dots + r_{1n} b_n, \\ k_2 &= r_{21} b_1 + \dots + r_{2n} b_n, \\ &\dots \\ k_m &= r_{m1} b_1 + \dots + r_{mn} b_n. \end{aligned}$$

Wir erhalten

$$\begin{aligned} a &= k_1 a_1 + \dots + k_m a_m \\ &= (r_{11} b_1 + \dots + r_{1n} b_n) a_1 + \dots + (r_{m1} b_1 + \dots + r_{mn} b_n) a_m \\ &= r_{11} \cdot a_1 b_1 + r_{1n} \cdot a_1 b_n + \dots + r_{m1} \cdot a_m b_1 + \dots + r_{mn} \cdot a_m b_n \\ &= \sum_{\substack{i=1, \dots, m \\ j=1, \dots, n}} r_{ij} \cdot a_i b_j. \end{aligned}$$

5 Algebraische Grundlagen der Konstruierbarkeit

Wegen $r_{ij} \in \mathbb{Q}$ und $a_i b_j \in L$ für alle i, j ist C ein Erzeugendensystem von L über $\mathbb{Q}$.

lineare Unabhängigkeit: Seien $r_{ij} \in \mathbb{Q}$ mit $\sum_{j=1, \dots, n} r_{ij} \cdot a_i b_j = 0$.

Wir müssen zeigen, dass dann schon

$$r_{11} = \dots = r_{m1} = \dots = r_{1n} = \dots = r_{mn} = 0$$

gilt. Betrachten wir daher die Summe genauer. Wie wir bereits gesehen haben, gilt

$$\begin{aligned} & \sum_{\substack{i=1, \dots, m \\ j=1, \dots, n}} r_{ij} \cdot a_i b_j \\ &= r_{11} \cdot a_1 b_1 + r_{1n} \cdot a_1 b_n + \dots + r_{m1} \cdot a_m b_1 + \dots + r_{mn} \cdot a_m b_n \\ &= (r_{11} b_1 + \dots + r_{1n} b_n) a_1 + \dots + (r_{m1} b_1 + \dots + r_{mn} b_n) a_m. \end{aligned}$$

Da $B = \{b_1, \dots, b_n\}$ eine Basis von K über $\mathbb{Q}$ ist, liegen alle Linearkombinationen

$$r_{11} b_1 + \dots + r_{1n} b_n, \dots, r_{m1} b_1 + \dots + r_{mn} b_n$$

in K . Damit ist die Summe

$$\sum_{\substack{i=1, \dots, m \\ j=1, \dots, n}} r_{ij} \cdot a_i b_j$$

eine Linearkombination der Basis $A = \{a_1, \dots, a_m\}$ von L über K . Da diese Summe nach Voraussetzung gleich 0 ist, müssen schon alle Koeffizienten Null sein, das heißt

$$\begin{aligned} r_{11} b_1 + \dots + r_{1n} b_n &= 0, \\ \dots \\ r_{m1} b_1 + \dots + r_{mn} b_n &= 0. \end{aligned}$$

Wie bereits erwähnt sind die linken Seiten dieser Gleichungen Linearkombinationen der Basis B von K über $\mathbb{Q}$. Da auch diese 0 ergeben sollen, müssen alle Koeffizienten

$$r_{11}, \dots, r_{1n}, \dots, r_{m1}, \dots, r_{mn}$$

5 Algebraische Grundlagen der Konstruierbarkeit

schon Null sein. Daher ist C auch linear unabhängig und somit eine Basis von L über $\mathbb{Q}$. Für die Dimensionen der jeweiligen Vektorräume gilt folglich

$$[L : \mathbb{Q}] = m \cdot n = [L : K] \cdot [K : \mathbb{Q}].$$

□

Die Aussage des Satzes ist zentral für unsere kommenden Betrachtungen der Konstruktion regelmäßiger Vielecke. Das folgende Beispiel verdeutlicht einen wichtigen Zusammenhang:

Beispiel 5.23. *Seien wie in der Situation von Satz 5.22 $K = \mathbb{Q}(a)$ und $L = \mathbb{Q}(a, b)$ mit $K \subseteq L$. Dann gilt*

$$[\mathbb{Q}(a, b) : \mathbb{Q}] = [\mathbb{Q}(a, b) : \mathbb{Q}(a)] \cdot [\mathbb{Q}(a) : \mathbb{Q}].$$

Wir können folglich die Dimension einer algebraischen Erweiterung von $\mathbb{Q}$ mit zwei algebraischen Zahlen a und b bestimmen, indem wir den Grad der Erweiterung $\mathbb{Q}(a)$ über $\mathbb{Q}$ betrachten und diesen mit dem Grad der Erweiterung von $\mathbb{Q}(a, b)$ über $\mathbb{Q}(a)$ vergleichen. Die Erweiterung von $\mathbb{Q}(a, b)$ über $\mathbb{Q}(a)$ ist allerdings nichts anderes als eine Erweiterung des Körpers $\mathbb{Q}(a)$ mit der algebraischen Zahl b . Wir können folglich immer weiter algebraische Zahlen $a_1, \dots, a_n$ zu Unterkörpern von $\mathbb{C}$ adjungieren und auf die Dimension der Körpererweiterung zurückschließen, indem wir die Dimensionen der einzelnen Körpererweiterungen betrachten.

Wir sind nun am Ende unserer algebraischen Vorbereitungen für die Untersuchung der Konstruierbarkeit regelmäßiger Vielecke angekommen. Den Begriff der Körpererweiterung haben wir jedoch noch nicht mit den konstruierbaren Zahlen verbunden. Dieser wichtigen Verknüpfung widmen wir daher ein eigenes Unterkapitel.

5.4 Konstruierbare Zahlen

Im Folgenden wollen wir die gesamten Ausführungen dieses Kapitels auf unser Erkenntnisinteresse zurückführen. Wir haben im Hauptsatz 3.14 bereits gesehen, dass das regelmäßige Vieleck genau dann konstruierbar ist, wenn wir die Zahl

$$\cos \frac{2\pi}{n}$$

konstruieren können. Wir konnten aus einer minimal gewählten Startmenge $\mathcal{M} = \{0, 1\}$ weitere Punkte und Zahlen in der kartesischen Ebene konstruieren. Die Erweiterungen der Menge $\mathcal{M}$ umfassten dabei die Schnittpunkte, die

durch das Schneiden zweier Geraden (Typ 1), einer Geraden mit einem Kreis (Typ 2) und zweier Kreise (Typ 3) entstanden, welche mithilfe der Punkte aus $\mathcal{M}$ konstruierbar waren. Wir konnten bislang schon eine Vielzahl wichtiger Erkenntnisse für die konstruierbaren Zahlen aus diesen Schnittgebilden ableiten, wie zum Beispiel, dass die konstruierbaren Zahlen einen Körper bilden. Zum Abschluss des Kapitels 4 wurde allerdings klar, dass wir beispielsweise noch nicht bestimmen konnten, inwiefern auch ein Ausdruck der Form $\sqrt[3]{\cdot}$ im Allgemeinen konstruierbar ist. Mit den Vorarbeiten dieses Kapitels ist es nun allerdings möglich, die konstruierbaren Zahlen genau zu charakterisieren. Wir werfen dafür noch einmal einen genaueren Blick auf unsere elementaren Optionen zur Konstruktion neuer Punkte.

Satz 5.24. *[Beu18, S. 239 -240] Sei K ein Unterkörper von $\mathbb{R}$. Dann gelten die folgenden Aussagen:*

1. *Schneiden sich zwei verschiedene aus K konstruierbare Geraden in einem Schnittpunkt $(x, y) \in \mathbb{R}^2$, so gilt $x, y \in K$.*
2. *Schneiden sich ein aus K konstruierbarer Kreis und eine aus K konstruierbare Gerade, so liegen die Koordinaten der Schnittpunkte in einem Unterkörper $K(\sqrt{q})$ für ein nicht-negatives $q \in K$.*
3. *Schneiden sich zwei verschiedene aus K konstruierbare Kreise, so liegen die Koordinaten der Schnittpunkte in einem Unterkörper $K(\sqrt{q})$ für ein nicht-negatives $q \in K$.*

Beweis. 1. Seien $g_1 : y = mx + b$ und $g_2 : y = m'x + b'$ zwei verschiedene, sich schneidende Geraden und $b, b', m, m' \in K$. Dann können g_1 und g_2 nicht parallel sein. Daher gilt $m \neq m'$ und somit $m - m' \neq 0$. Daraus folgt

$$\begin{aligned} mx + b &= m'x + b' \\ \Leftrightarrow (m - m')x &= b' - b \\ \Leftrightarrow x_s &= \frac{b' - b}{m - m'} \end{aligned}$$

und mit

$$y_s = m \frac{b' - b}{m - m'} + b$$

erhalten wir den eindeutigen Schnittpunkt (x_s, y_s) . Da K ein Körper ist und $b, b', m, m' \in K$ gilt, liegen somit auch die Koordinaten des Schnittpunkts wieder in K .

5 Algebraische Grundlagen der Konstruierbarkeit

2. Gegeben seien eine Gerade

$$y = mx + b$$

und ein Kreis

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

mit $b, m, r, x_0, y_0 \in K$. Durch das Einsetzen von $y = mx + b$ in die Kreisgleichung erhalten wir

$$\begin{aligned} & (x - x_0)^2 + (mx + b - y_0)^2 = r^2 \\ \Leftrightarrow & (1 + m^2)x^2 + (2m(b - y_0) - 2x_0)x + x_0^2 + (b - y_0)^2 - r^2 = 0. \end{aligned}$$

Durch die Lösungsformel

$$x_{1,2} = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}$$

für eine quadratische Gleichung der Form $Ax^2 + Bx + C = 0$ mit $A, B, C \in \mathbb{R}$ erhalten wir für

$$\begin{aligned} A &:= 1 + m^2, \\ B &:= 2m(b - y_0) - 2x_0, \\ C &:= x_0^2 + (b - y_0)^2 - r^2 \end{aligned}$$

die gesuchten Lösungen unserer Gleichung. Da sich die Gerade und der Kreis schneiden, ist die Diskriminante $B^2 - 4AC =: q$ nicht-negativ.

Da b, m, r, x_0, y_0 in K liegen und K ein Körper ist, liegen $A, B, C \in K$ und somit auch $q \in K$. Die Koordinaten des Schnittpunkts beziehungsweise der Schnittpunkte der Geraden und des Kreises liegen allerdings nicht zwangsläufig wieder in K , da $\sqrt{q}$ nicht unbedingt in K liegt. Mit Sicherheit liegen die Koordinaten des Schnittpunkts beziehungsweise der Schnittpunkte dann allerdings im Körper $K(\sqrt{q})$.

3. Seien

$$\begin{aligned} K_1 &: (x - x_1)^2 + (y - y_1)^2 = r_1^2 \\ K_2 &: (x - x_2)^2 + (y - y_2)^2 = r_2^2 \end{aligned}$$

5 Algebraische Grundlagen der Konstruierbarkeit

zwei verschiedene, sich schneidende Kreise und $r_1, r_2, x_1, x_2, y_1, y_2 \in K$. Durch Subtraktion der beiden Gleichungen erhalten wir

$$2(x_2 - x_1)x + 2(y_2 - y_1)y = r_1^2 - r_2^2 - x_1^2 + x_2^2 - y_1^2 + y_2^2.$$

Da die Kreise verschieden sind, verschwinden die Koeffizienten der linearen Gleichung nicht gleichzeitig. Somit beschreibt die Gleichung eine Gerade durch den beziehungsweise die Schnittpunkte der beiden Kreise.

Damit können wir die Betrachtung des Schnittpunkts zweier Kreise auf die Betrachtung des Schnittpunkts einer Geraden mit einem Kreis zurückführen. Nach Aussage (2) liegen die Koordinaten aller Schnittpunkte zweier Kreise folglich für ein nicht-negatives $q \in K$ im Körper $K(\sqrt{q})$. $\square$

Korollar 5.25. *Sei K ein Unterkörper von $\mathbb{R}$ und $q \in K$ mit $q \geq 0$. Dann gilt*

$$[K(\sqrt{q}) : K] \leq 2.$$

Beweis. Sei $q \in K$ mit $q \geq 0$. Liegt auch $\sqrt{q}$ in K , so gilt

$$K(\sqrt{q}) = K$$

und daher

$$[K(\sqrt{q}) : K] = 1.$$

Gilt $\sqrt{q} \notin K$, dann hat das Minimalpolynom von $\sqrt{q}$ über dem Körper K nicht den Grad 1. Mit

$$P(x) = x^2 - q$$

finden wir allerdings ein normiertes Polynom vom Grad 2 mit Koeffizienten aus K und

$$P(\sqrt{q}) = 0.$$

Daher gilt für $\sqrt{q} \notin K$

$$[K(\sqrt{q}) : K] = 2.$$

$\square$

Wir kommen nun zum zentralen Resultat unserer algebraischen Betrachtungen. Es beruht darauf, dass wir mit $\mathbb{Q}$ bereits einen Körper kennen, dessen Elemente wir alle konstruieren können. Alle weiteren Elemente liegen daher in Körpererweiterungen, die durch das Schneiden von Geraden und Kreisen, wie in Satz 5.24, entstehen. Schlussendlich können wir damit den folgenden Hauptsatz dieses Kapitels festhalten:

5 Algebraische Grundlagen der Konstruierbarkeit

Hauptsatz 5.26 (Konstruierbare Zahlen). *[Beu18, S. 240-241] Eine reelle Zahl a ist genau dann konstruierbar, wenn es Unterkörper*

$$K_0, K_1, \dots, K_n$$

von $\mathbb{R}$ gibt, sodass

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n \subseteq \mathbb{R} \quad \text{mit} \quad a \in K_n$$

gilt, wobei für die Grade der Körpererweiterungen

$$[K_{i+1} : K_i] \leq 2$$

für $i \in \{0, \dots, n-1\}$ gilt.

*Eine solche Folge ineinander geschachtelter Unterkörper heißt **Körperturm**.*

Beweis. Sei zunächst a eine konstruierbare Zahl. Dann entsteht a nach endlich vielen Konstruktionsschritten aus den Operationen gemäß der Definition 3.3.

Nach Satz 3.10 bilden die konstruierbaren Zahlen einen Körper der nach Korollar 3.11 mindestens alle rationalen Zahlen enthält. Wir beginnen daher mit dem Unterkörper

$$K_0 = \mathbb{Q}.$$

Ist $a \in K_0$, so liegt a bereits im Körperturm

$$\mathbb{Q} = K_0 \subseteq \mathbb{R}.$$

Sei daher $a \notin K_0$. In Satz 5.24 haben wir gezeigt, dass die Koordinaten neu konstruierter Punkte beim Schneiden von Geraden und Kreisen aus einem Unterkörper K stets entweder wieder in K oder in einer Körpererweiterung der Form

$$K(\sqrt{q})$$

mit $[K(\sqrt{q}) : K] = 2$ für ein nicht-negatives $q \in K$ liegen.

Entstehen im ersten Konstruktionsschritt neue Punkte, deren Koordinaten nicht bereits in K_0 liegen, so liegen ihre Koordinaten in einer Körpererweiterung K_1 mit

$$[K_1 : K_0] = 2.$$

Analog liegen die Koordinaten aller Punkte, die im nächsten Konstruktionsschritt entstehen, entweder bereits in K_1 oder in einer Körpererweiterung K_2 mit

$$[K_2 : K_1] = 2.$$

5 Algebraische Grundlagen der Konstruierbarkeit

Induktiv erhalten wir auf diese Weise einen Körperturm

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s \subseteq \mathbb{R}$$

mit

$$[K_{i+1} : K_i] \leq 2$$

für $i \in \{0, \dots, s-1\}$.

Da jeder Konstruktionsschritt höchstens eine Quadratwurzeladjunktion erzeugt und die Konstruktion von a nur endlich viele Schritte umfasst, entsteht somit nach endlich vielen Körpererweiterungen ein Unterkörper K_n mit

$$a \in K_n.$$

Seien umgekehrt $K_0, K_1, \dots, K_n$ Unterkörper von $\mathbb{R}$ wie im Hauptsatz und $a \in K_n$. Durch Induktion nach n können wir nun zeigen, dass a konstruierbar ist.

Induktionsanfang. Sei $n = 0$. Dann gilt

$$K_n = K_0 = \mathbb{Q}.$$

Nach Korollar 3.11 sind alle rationalen Zahlen konstruierbar, also ist auch a konstruierbar.

Induktionsschritt. Sei nun die Behauptung für $n-1$ richtig. Dann ist jedes $w \in K_{n-1}$ konstruierbar.

Gilt

$$[K_n : K_{n-1}] = 1,$$

so folgt bereits

$$K_n = K_{n-1}.$$

Damit ist insbesondere $a \in K_n$ konstruierbar.

Sei nun

$$[K_n : K_{n-1}] = 2.$$

Nach Satz 5.24 existiert dann ein Element

$$q = \sqrt{d_{n-1}} \geq 0$$

mit $d_{n-1} \in K_{n-1}$, sodass $K_n = K_{n-1}(q)$ gilt.

Da q nicht in K_{n-1} liegt, kann das Minimalpolynom von q über dem Körper K_{n-1} nicht den Grad 1 besitzen. Für das Polynom $P(x) = x^2 - d_{n-1}$ mit Koeffizienten $1, d_{n-1} \in K_{n-1}$ gilt allerdings $P(q) = 0$. Damit ist q algebraisch

5 Algebraische Grundlagen der Konstruierbarkeit

über dem Körper K_{n-1} und das Minimalpolynom von q besitzt über K_{n-1} den Grad 2. Nach Satz 5.18 ist der Körper K_n dann wie folgt darstellbar:

$$K_n = K_{n-1}(q) = \{b_0 + qb_1 \mid b_0, b_1 \in K_{n-1}\}.$$

Wegen $d_{n-1} \in K_{n-1}$ ist d_{n-1} nach Induktionsvoraussetzung konstruierbar. Somit ist auch

$$q = \sqrt{d_{n-1}}$$

nach Satz 3.12 konstruierbar.

Da außerdem nach der Induktionsvoraussetzung alle Elemente aus K_{n-1} konstruierbar sind, sind insbesondere b_0 und b_1 konstruierbar. Aufgrund der Konstruierbarkeit von q folgt somit nach Satz 3.10, dass auch

$$a = b_0 + qb_1$$

konstruierbar ist. □

Der Hauptsatz dieses Kapitels führt uns ganz nah an unser Erkenntnisinteresse heran. Wir können nun die Konstruierbarkeit einer reellen Zahl a_n darauf zurückführen, ob diese in einem Körperturm

$$\mathbb{Q} \subseteq \mathbb{Q}(a_1) \subseteq \mathbb{Q}(a_1, a_2) \subseteq \cdots \subseteq \mathbb{Q}(a_1, \dots, a_n) \subseteq \mathbb{R}$$

liegt. Dabei sind alle a_i positive Quadratwurzeln aus den vorherigen Unterkörpern. Zusammen mit dem Gradsatz 5.22 und dem Korollar 5.25 erhalten wir aus dem Hauptsatz zudem eine notwendige Bedingung für die Konstruierbarkeit einer reellen Zahl.

Satz 5.27. *[Beu18, S. 241] Ist eine reelle Zahl a konstruierbar, dann gilt notwendigerweise*

$$[\mathbb{Q}(a) : \mathbb{Q}] = 2^k$$

für eine natürliche Zahl $k \in \mathbb{N}_0$.

Beweis. Sei a eine konstruierbare reelle Zahl. Dann liegt a nach dem Hauptsatz 5.26 in einem Unterkörper K von $\mathbb{R}$, für den es einen Körperturm

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n = K \subseteq \mathbb{R}$$

mit $[K_{i+1} : K_i] \leq 2$ gibt.

Nach dem Gradsatz für Körpererweiterungen 5.22 gilt

$$[K : \mathbb{Q}] = [K_1 : K_0] \cdot [K_2 : K_1] \cdot \cdots \cdot [K : K_{n-1}].$$

5 Algebraische Grundlagen der Konstruierbarkeit

Jeder dieser Faktoren ist entweder gleich 1 oder gleich 2, daher gilt

$$[K : \mathbb{Q}] = [K_1 : K_0] \cdot [K_2 : K_1] \cdot \dots \cdot [K : K_{n-1}] = 2^s$$

für eine natürliche Zahl $s \in \mathbb{N}_0$.

Da $a \in K$ liegt, gilt nach der Definition 5.16

$$\mathbb{Q}(a) \subseteq K.$$

Nun können wir erneut den Gradsatz 5.22 anwenden. Es gilt

$$2^s = [K : \mathbb{Q}] = [K : \mathbb{Q}(a)] \cdot [\mathbb{Q}(a) : \mathbb{Q}].$$

Da das Produkt

$$[K : \mathbb{Q}(a)] \cdot [\mathbb{Q}(a) : \mathbb{Q}]$$

somit eine Zweierpotenz ist, müssen wegen der eindeutigen Primfaktorzerlegung schon beide Faktoren Zweierpotenzen sein. Daher gilt

$$[\mathbb{Q}(a) : \mathbb{Q}] = 2^m$$

für ein $m \in \mathbb{N}_0$ mit $m \leq s$. □

Mithilfe der wichtigen Erkenntnisse dieses Kapitels sind wir nun bereit, genau zu kategorisieren, welche regelmäßigen Vielecke tatsächlich konstruierbar sind. Wir können durch den Hauptsatz und den eben bewiesenen Satz sogar alle antiken Fragestellungen aus der Einleitung dieser Arbeit beantworten. Dieser Aufgabe nahm sich im Jahr 1837 auch der französische Mathematiker Pierre Wantzel an [Beu18, S. 241]. Nicht umsonst trägt der Hauptsatz über die Konstruierbarkeit regelmäßiger Vielecke daher den Namen *Satz von Gauß-Wantzel*. Bevor wir im folgenden Kapitel den *Satz von Gauß-Wantzel* beweisen und somit abschließend herausstellen, welche regelmäßigen Vielecke konstruierbar sind, wollen wir zum Abschluss dieses Kapitels noch einen kurzen Blick auf die weiteren antiken Fragestellungen der Griechen werfen.

Satz 5.28 (Die unmögliche Würfelverdopplung). [Beu18, S. 242] *Es ist nicht möglich mit Zirkel und Lineal einen Würfel des Volumens 2 zu konstruieren.*

Beweis. Die Kantenlänge eines Würfels mit einem Volumen von 2 beträgt $\sqrt[3]{2}$. Das Minimalpolynom von $\sqrt[3]{2}$ über dem Körper $\mathbb{Q}$ ist $P(x) = x^3 - 2$. Damit gilt $\deg(P) = 3$ und nach Satz 5.27 ist die Zahl $\sqrt[3]{2}$ nicht konstruierbar. □

Auf ähnliche Weise lässt sich zeigen, dass auch die Quadratur des Kreises und die Dreiteilung eines gegebenen Winkels im Allgemeinen nicht möglich sind. Unter anderem lässt sich zum Einheitskreis mit dem Flächeninhalt π kein Quadrat mit identischem Flächeninhalt konstruieren. Ebenso lässt sich ein Winkel von 60° nicht in drei 20° Winkel aufteilen [Beu18, S. 242-243].

Auch für die regelmäßigen Vielecke werden wir im abschließenden Kapitel dieser Arbeit herausfinden, dass nicht alle solcher n -Ecke tatsächlich konstruierbar sind. Es wird uns allerdings gelingen, explizit zu bestimmen, von welcher Form eine natürliche Zahl n sein muss, damit das regelmäßige n -Eck konstruierbar ist.

6 Welche n -Ecke sind konstruierbar?

Das abschließende Kapitel dieser Arbeit soll sich der allgemeinen Konstruierbarkeit regelmäßiger Vielecke widmen. Dabei werden wir mit dem *Satz von Gauß-Wantzel* eine explizite Darstellungsform einer natürlichen Zahl n herleiten, die eindeutig bestimmt, ob das zugehörige regelmäßige n -Eck konstruierbar ist oder nicht. Die geometrischen und algebraischen Vorarbeiten der Kapitel 3 und 5 werden uns dabei sehr hilfreiche Zwischenresultate liefern.

Zunächst sei daran erinnert, dass wir bereits im Satz 4.1 aus Kapitel 4 eine erste Verallgemeinerung der Konstruierbarkeit regelmäßiger Vielecke bewiesen haben. Genauer besagte der Satz, dass ein regelmäßiges n -Eck genau dann konstruierbar ist, wenn auch das regelmäßige $2n$ -Eck konstruierbar ist.

6.1 Das regelmäßige mn -Eck

Wir beginnen dieses Kapitel mit einem vergleichbaren Resultat, das allerdings nicht nur eine wichtige Eigenschaft für konstruierbare Vielecke beweist, sondern zugleich auch eine klare Richtung für unsere weiteren Untersuchungen vorgibt. Etwas überraschend werden wir dazu ein wichtiges Resultat der Zahlentheorie benötigen.

Satz 6.1. [Toe10, S. 305] Seien $m, n \geq 3$ teilerfremd. Dann gilt: Das regelmäßige n -Eck und m -Eck sind genau dann konstruierbar, wenn das regelmäßige $m \cdot n$ -Eck konstruierbar ist.

Beweis. Seien $m, n \geq 3$ teilerfremde natürliche Zahlen.

6 Welche n-Ecke sind konstruierbar?

Seien zunächst das regelmäßige m -Eck und n -Eck konstruierbar. Dann sind insbesondere die n -ten Einheitswurzeln

$$z_k = e^{2\pi i k/n}$$

für $k \in \{0, \dots, n-1\}$ und die m -ten Einheitswurzeln

$$\tilde{z}_l = e^{2\pi i l/m}$$

für $l \in \{0, \dots, m-1\}$ konstruierbar. Genauer sind die reellen Zahlen

$$\cos \frac{2\pi}{n} \quad \text{und} \quad \cos \frac{2\pi}{m}$$

und damit die Winkel

$$\alpha = \frac{2\pi}{m} \quad \text{und} \quad \beta = \frac{2\pi}{n}$$

konstruierbar. Nach dem Lemma von Bézout [Küh25, S. 2-3] existieren zu zwei gegebenen teilerfremden Zahlen ganze Zahlen a, b mit

$$an + bm = 1.$$

Multiplizieren wir diese Gleichung mit $\frac{2\pi}{mn}$, erhalten wir

$$(an + bm) \cdot \frac{2\pi}{mn} = a \cdot \frac{2\pi}{m} + b \cdot \frac{2\pi}{n} = \frac{2\pi}{mn}.$$

Indem wir den konstruierbaren Winkel α a -mal und den konstruierbaren Winkel β b -mal abtragen, erhalten wir folglich einen Winkel $\gamma = \frac{2\pi}{mn}$. Diesen Winkel können wir im mathematisch positiven Sinne bezüglich der positiven reellen Zahlenachse und mit dem Scheitelpunkt im Ursprung abtragen. Der dabei entstehende Strahl schneidet den Einheitskreis im Punkt

$$z = e^{2\pi i/mn} = \cos \frac{2\pi}{mn} + i \cdot \sin \frac{2\pi}{mn}.$$

Dieser Punkt ist die erste nicht-triviale mn -te Einheitswurzel. Damit ist das regelmäßige $m \cdot n$ -Eck konstruierbar.

Sei nun das regelmäßige $m \cdot n$ -Eck konstruierbar. Dann sind insbesondere die $m \cdot n$ -ten Einheitswurzeln

$$z_k = e^{2\pi i k/mn}$$

für $k \in \{0, \dots, mn-1\}$ konstruierbar. Da somit auch

$$z_n = e^{2\pi i n/mn} = e^{2\pi i/m} \quad \text{und} \quad z_m = e^{2\pi i m/mn} = e^{2\pi i/n}$$

konstruierbar sind, folgt aus dem Satz 3.13 und dem Hauptsatz 3.14, dass auch das regelmäßige m -Eck und das regelmäßige n -Eck konstruierbar sind. $\square$

Bemerkung 6.2. Interpretieren wir den Beweis der Rückrichtung des Satzes geometrisch, so erhalten wir das regelmäßige n -Eck beziehungsweise das regelmäßige m -Eck aus dem regelmäßigen $m \cdot n$ -Eck, indem wir jede m -te beziehungsweise jede n -te Ecke des $m \cdot n$ -Ecks miteinander verbinden.

Die Rückrichtung des Satzes genügt dabei sogar einer stärkeren Formulierung als im Satz, denn wir haben die Teilerfremdheit der Zahlen n und m dort nicht verwenden müssen. Aus der Konstruierbarkeit des regelmäßigen $m \cdot n$ -Ecks können wir für natürliche Zahlen $m, n \geq 3$ daher immer die Konstruierbarkeit des regelmäßigen m -Ecks und des regelmäßigen n -Ecks folgern.

Die im ersten Teil des Satzes notwendige Teilerfremdheit der natürlichen Zahlen $m, n \geq 3$ deutet darauf hin, dass es besonders interessant ist, regelmäßige p -Ecke für eine Primzahl $p \geq 3$ zu betrachten, denn zwei verschiedene Primzahlen müssen nach ihrer Definition bereits teilerfremd zueinander sein.

6.2 Nicht konstruierbare p -Ecke

Wir werden einige Resultate benötigen, um schlussendlich auf die Konstruierbarkeit regelmäßiger p -Ecke für eine Primzahl p schließen zu können. Wir halten zunächst fest, dass p zumindest eine ungerade Primzahl sein muss, da wir für ein allgemeines n -Eck die Eigenschaft $n \geq 3$ gefordert haben.

Unsere Ausführungen werden dabei schon bald in einem spannenden Resultat münden: Nicht jedes p -Eck ist für eine ungerade Primzahl p konstruierbar!

Definition 6.3 (Primitive Einheitswurzeln). *Sei $n \in \mathbb{N}$. Eine komplexe Zahl $z \in \mathbb{C}$ heißt primitive n -te Einheitswurzel, wenn*

$$z^n = 1$$

gilt und zugleich für alle $k \in \mathbb{N}$ mit

$$1 \leq k < n$$

die Ungleichung

$$z^k \neq 1$$

erfüllt ist.

Wir benötigen nun ein Kriterium, wann eine p -te Einheitswurzel einer ungeraden Primzahl p primitiv ist. Ein solches Kriterium lässt sich leicht finden.

Satz 6.4. *Sei p eine Primzahl und*

$$z_k = e^{2\pi i k/p}$$

6 Welche n-Ecke sind konstruierbar?

mit

$$1 \leq k < p$$

eine nicht-triviale p -te Einheitswurzel.

Dann ist z_k eine primitive p -te Einheitswurzel.

Beweis. Nach Satz 2.6 ist z_k eine p -te Einheitswurzel, also eine Nullstelle des Polynoms

$$P(z) = z^p - 1.$$

Angenommen, es gibt ein $m \in \mathbb{N}$ mit

$$1 \leq m < p$$

und

$$(z_k)^m - 1 = 0.$$

Dann gilt

$$(e^{2\pi i k/p})^m = e^{2\pi i k m/p} = 1.$$

Diese Gleichung ist genau dann erfüllt, wenn

$$\frac{km}{p}$$

eine ganze Zahl ist. p muss also ein Teiler des Produkts $k \cdot m$ sein.

Da p eine Primzahl ist und zusätzlich

$$1 \leq k < p$$

gilt, müssen p und k teilerfremd sein. Wenn p aber den Faktor k nicht teilt, muss

$$p \mid m$$

gelten. Dies ist jedoch ein Widerspruch, da aus

$$1 \leq m < p$$

bereits folgt, dass p kein Teiler von m ist.

Folglich gilt für alle

$$1 \leq m < p$$

die Ungleichung

$$(z_k)^m \neq 1$$

und die p -te Einheitswurzel z_k ist primitiv. □

6 Welche n-Ecke sind konstruierbar?

Bis auf die triviale p -te Einheitswurzel $z_0 = 1$ sind folglich alle p -ten Einheitswurzeln primitiv. Wir zeigen nun, dass wir sogar alle primitiven p -ten Einheitswurzeln durch eine einzige primitive p -te Einheitswurzel darstellen können.

Satz 6.5. *Sei p eine Primzahl und*

$$z_k = e^{2\pi i k/p}$$

mit

$$1 \leq k < p$$

die primitiven p -ten Einheitswurzeln. Dann ist

$$M = \{z_k, z_k^2, \dots, z_k^{p-1}\}$$

die Menge aller primitiven p -ten Einheitswurzeln.

Beweis. Wir wissen bereits, dass es genau $p-1$ primitive p -te Einheitswurzeln gibt. Daher bleibt zu zeigen, dass die Elemente der Menge M paarweise verschiedene primitive p -te Einheitswurzeln sind. Nach Voraussetzung ist z_k eine p -te Einheitswurzel, daher gilt

$$z_k^p = 1$$

und somit auch

$$(z_k^m)^p = (z_k^p)^m = 1^m = 1$$

für $1 \leq m < p$. Die Menge M enthält folglich nur p -te Einheitswurzeln. Angenommen, es existieren Indizes $i, j \in \{1, \dots, p-1\}$ mit

$$z_k^i = z_k^j.$$

Dividieren wir die Gleichung durch z_k^j , erhalten wir

$$z_k^{i-j} = 1.$$

Da z_k primitiv ist, gilt

$$i - j \equiv 0 \pmod{p}.$$

Das ist allerdings wegen $i, j \in \{1, \dots, p-1\}$ nur für

$$i = j$$

möglich. Folglich gilt

$$M = \{z_1, \dots, z_{p-1}\}.$$

□

6 Welche n-Ecke sind konstruierbar?

Die primitiven p -ten Einheitswurzeln stellen ein zentrales Hilfsmittel für die Untersuchung der Konstruierbarkeit regelmäßiger Vielecke dar. Da der Beweis für ein notwendiges Kriterium für die Konstruierbarkeit des p -Ecks recht umfangreich ist, beweisen wir zuvor noch ein kurzes Hilfslemma.

Lemma 6.6. *Sei $n \geq 3$ und*

$$z_1 = e^{2\pi i/n}.$$

Dann gilt

$$[\mathbb{Q}(z_1) : \mathbb{Q}(\cos \frac{2\pi}{n})] = 2.$$

Beweis. In Proposition 2.12 haben wir gesehen, dass eine komplexe Zahl auf dem Einheitskreis in ihrer Polarkoordinatendarstellung die Gleichung

$$z + z^{-1} = 2 \cos \varphi$$

erfüllt. Da z_1 auf dem Einheitskreis liegt, gilt daher

$$z_1 + z_1^{-1} = 2 \cos \frac{2\pi}{n}.$$

Wir definieren

$$\alpha := \cos \frac{2\pi}{n}$$

und erhalten somit durch elementare Umformungen die Gleichung

$$z_1^2 - 2\alpha z_1 + 1 = 0.$$

Das Polynom

$$P(x) = x^2 - 2\alpha x + 1$$

ist ein normiertes Polynom über dem Körper $\mathbb{Q}(\alpha)$. Für dieses gilt

$$P(z_1) = 0.$$

z_1 ist somit algebraisch über $\mathbb{Q}(\alpha)$. Da $z_1 \in \mathbb{C} \setminus \mathbb{R}$ liegt und somit $z_1 \notin \mathbb{Q}(\alpha)$ gilt, ist P bereits das Minimalpolynom von z_1 über $\mathbb{Q}(\alpha)$. Daher gilt

$$[\mathbb{Q}(z_1) : \mathbb{Q}(\alpha)] = 2.$$

□

Satz 6.7. *[Beu18, S. 303-304] Ist das p -Eck konstruierbar, so muss die Primzahl p bereits von der Form*

$$p = 2^k + 1$$

für ein $k \in \mathbb{N}$ sein.

6 Welche n-Ecke sind konstruierbar?

Beweis. Wir betrachten zunächst das Polynom

$$F(x) = x^p - 1.$$

Die Nullstellen des Polynoms sind genau die p -ten Einheitswurzeln. Das Polynom ist reduzibel über $\mathbb{Q}$ mit der Zerlegung

$$F(x) = (x - 1)(x^{p-1} + x^{p-2} + \cdots + x + 1).$$

Der erste der beiden Faktoren ist das Polynom

$$g(x) = x - 1.$$

Die Nullstelle dieses Polynoms ist die triviale p -te Einheitswurzel $z_0 = 1$. Alle weiteren p -ten Einheitswurzeln müssen daher die Nullstellen des Polynoms

$$h(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

sein. Diese sind nach Lemma 6.4 genau die primitiven p -ten Einheitswurzeln. Wir zeigen nun, dass das Polynom h irreduzibel über $\mathbb{Q}$ ist.

Angenommen, h ist reduzibel über $\mathbb{Q}$. Da alle Koeffizienten von h aus $\mathbb{Z}$ kommen, ist h nach dem Lemma von Gauß (5.12) auch über $\mathbb{Z}$ reduzibel. Es gibt also eine Zerlegung

$$h(x) = f(x) \cdot r(x)$$

mit $f, r \in \mathbb{Z}[x]$ und $1 \leq \deg(f), \deg(r) < \deg(h) = p - 1$. Dabei sei f irreduzibel über $\mathbb{Z}$. Diese Eigenschaften können wir voraussetzen, da wir h so lange zerlegen können, bis nur irreduzible Faktoren übrig bleiben. Einer dieser Faktoren ist dann unser Polynom f und alle anderen Faktoren sind das Polynom r .

Da h normiert ist, müssen auch f und r normiert sein. Setzen wir $x = 1$ ein, so erhalten wir:

$$p = h(1) = f(1) \cdot r(1).$$

Die Faktoren $f(1)$ und $r(1)$ sind ganze Zahlen. Somit gilt entweder

$$f(1) = p \quad \text{und} \quad r(1) = 1$$

oder

$$f(1) = -p \quad \text{und} \quad r(1) = -1.$$

Die anderen Fälle $f(1) = \pm 1$ und $r(1) = \pm p$ decken wir durch das Vertauschen der Rollen von f und r ab.

6 Welche n-Ecke sind konstruierbar?

Da das Polynom h alle primitiven p -ten Einheitswurzeln als Nullstellen besitzt, muss auch f mindestens in einem z_j mit $j \in \{1, \dots, p-1\}$ eine Nullstelle haben. Sei $k \in \{1, \dots, p-1\}$. Dann ist nach Lemma 6.5 auch z_j^k eine Nullstelle von h und somit entweder von f oder r .

Angenommen, z_j^k ist eine Nullstelle von r , das heißt,

$$r(z_j^k) = 0.$$

Wir definieren ein weiteres Polynom

$$R(x) := r(x^k).$$

Dann gilt

$$R(z_j) = r(z_j^k) = 0.$$

Das Polynom f ist irreduzibel über $\mathbb{Z}$ und z_j eine Nullstelle von f . Daher ist f das Minimalpolynom von z_j über $\mathbb{Z}$ und teilt somit nach Lemma 5.7 das Polynom R . Es gibt also eine Darstellung

$$R(x) = f(x) \cdot r_1(x)$$

für $r_1 \in \mathbb{Z}[x]$. Dann gilt allerdings bezogen auf die obige Fallunterscheidung

$$R(1) = r(1^k) = r(1) = \pm 1$$

und

$$R(1) = f(1)r_1(1) = \pm p \cdot r_1(1).$$

Somit muss

$$1 = p \cdot r_1(1)$$

gelten. Da r_1 allerdings nur ganzzahlige Werte annehmen kann, ist dies ein Widerspruch dazu, dass z_j^k eine Nullstelle von r ist. Somit ist z_j^k für jedes $k \in \{1, \dots, p-1\}$ eine Nullstelle von f . Anders ausgedrückt: Alle primitiven p -ten Einheitswurzeln sind Nullstellen von f . Es gibt allerdings genau $p-1$ verschiedene primitive p -te Einheitswurzeln. Daher gilt

$$\deg(f) = \deg(h).$$

Dies ist ein weiterer Widerspruch, diesmal zu $\deg(f) < \deg(h)$ und damit zur Reduzibilität von h . Das Polynom

$$h(x) = x^{p-1} + x^{p-2} + \dots + x + 1$$

ist daher irreduzibel über $\mathbb{Z}$ und somit nach dem Lemma von Gauß (5.12) auch irreduzibel über $\mathbb{Q}$. Insbesondere ist f somit das Minimalpolynom von z_1 über $\mathbb{Q}$.

6 Welche n-Ecke sind konstruierbar?

Daher gilt

$$[\mathbb{Q}(z_1) : \mathbb{Q}] = p - 1$$

und nach Lemma 6.6

$$[\mathbb{Q}(z_1) : \mathbb{Q}(\cos \frac{2\pi}{p})] = 2.$$

Somit muss nach dem Gradsatz 5.22 die folgende Gleichheit gelten:

$$p-1 = [\mathbb{Q}(z_1) : \mathbb{Q}] = [\mathbb{Q}(z_1) : \mathbb{Q}(\cos \frac{2\pi}{p})] \cdot [\mathbb{Q}(\cos \frac{2\pi}{p}) : \mathbb{Q}] = 2 \cdot [\mathbb{Q}(\cos \frac{2\pi}{p}) : \mathbb{Q}]$$

Da das p -Eck konstruierbar ist, folgt nach Satz 5.27

$$\frac{p-1}{2} = [\mathbb{Q}(\cos \frac{2\pi}{p}) : \mathbb{Q}] = 2^k$$

für ein $k \in \mathbb{N}_0$. Folglich ist p von der Form

$$p = 2^{k+1} + 1.$$

Mit $m := k + 1$ erhalten wir die Darstellung

$$p = 2^m + 1.$$

für ein $m \in \mathbb{N}$. □

Der Beweis des Satzes ist zwar sehr technisch, wird uns aber schon bald dabei helfen, ein weiteres großes Resultat nahezu identisch zu beweisen. Betrachten wir aber zunächst die Zahlen der Form $2^m + 1$ für ein $m \in \mathbb{N}$ genauer. Für den Fall $m = 3$ fällt auf, dass es sich bei

$$p = 2^3 + 1 = 9$$

überhaupt nicht um eine Primzahl handelt. Wir können daher die Aussage des Satzes noch weiter präzisieren, indem wir eine notwendige Bedingung für die Primzahl-Eigenschaft der Zahlen $2^m + 1$ finden.

Satz 6.8. *Sei p eine ungerade Primzahl.*

Ist das regelmäßige p -Eck konstruierbar, so gilt

$$p = 2^{2^n} + 1$$

für ein $n \in \mathbb{N}_0$.

6 Welche n-Ecke sind konstruierbar?

Beweis. Sei das regelmäßige p -Eck für eine ungerade Primzahl p konstruierbar. Nach dem vorherigen Satz gilt dann bereits

$$p = 2^s + 1$$

für ein $s \in \mathbb{N}$.

Wir zeigen nun, dass s selbst eine Zweierpotenz sein muss.

Angenommen, s ist keine Zweierpotenz. Dann besitzt s einen ungeraden Teiler $m > 1$. Somit gibt es ein $r \in \mathbb{N}$ mit

$$s = rm.$$

Für p finden wir eine Faktorisierung

$$p = 2^s + 1 = 2^{rm} + 1 = (2^r)^m + 1 = (2^r + 1)((2^r)^{m-1} - (2^r)^{m-2} + \dots - 2^r + 1).$$

Für den ersten Faktor gilt

$$1 < 2^r + 1 < 2^{rm} + 1 = p.$$

Wir haben folglich einen echten Teiler von p gefunden, der größer als 1 ist. Das ist ein Widerspruch dazu, dass es sich bei p um eine Primzahl handelt. Folglich muss p bereits von der Form

$$p = 2^{2^n} + 1$$

für ein $n \in \mathbb{N}_0$ sein. □

Die soeben bewiesenen Sätze 6.7 und 6.8 liefern uns eine Antwort auf eine der großen Fragestellungen dieser Arbeit.

Nicht jedes regelmäßige n -Eck ist mit Zirkel und Lineal konstruierbar!

Ist p eine Primzahl, so können wir sogar exakt bestimmen, dass die Konstruktion des p -Ecks für alle Primzahlen, die nicht bereits von der Form

$$p = 2^{2^n} + 1$$

für ein $n \in \mathbb{N}_0$ sind, nicht möglich ist. Wir erhalten somit auch eine Antwort darauf, warum sowohl unser Versuch der Konstruktion des Siebenecks in Kapitel 4.4 als auch die Versuche der alten Griechen nicht erfolgreich waren. Es gibt keine Zahl $k \in \mathbb{N}_0$ mit

$$7 = 2^{2^k} + 1.$$

Folglich ist die Konstruktion eines regelmäßigen Siebenecks mit Zirkel und Lineal nicht möglich.

Betrachten wir daher, welche p -Ecke überhaupt noch konstruierbar sein können und setzen verschiedene natürliche Zahlen in unsere aufgestellte Gleichung ein:

$$\begin{aligned}n = 0 : \quad p_0 &= 2^{2^0} + 1 = 3, \\n = 1 : \quad p_1 &= 2^{2^1} + 1 = 5, \\n = 2 : \quad p_2 &= 2^{2^2} + 1 = 17, \\n = 3 : \quad p_3 &= 2^{2^3} + 1 = 257, \\n = 4 : \quad p_4 &= 2^{2^4} + 1 = 65537, \\n = 5 : \quad p_5 &= 2^{2^5} + 1 = 4.294.967.297 .\end{aligned}$$

Für die Zahlen p_0, p_1, p_2, p_3 und p_4 konnte der französische Mathematiker *Pierre de Fermat* nachweisen, dass es sich tatsächlich um Primzahlen handelt [Toe10, S. 313]. Daher werden die Primzahlen der Form

$$p = 2^{2^n} + 1$$

auch als **Fermatsche Primzahlen** bezeichnet.

Die Suche nach weiteren Fermatschen Primzahlen bleibt jedoch bis heute ohne Erfolg. So konnten beispielsweise durch die Zerlegung

$$4.294.967.297 = 641 \cdot 6.700.417$$

zwei echte Teiler der Zahl p_5 gefunden werden. Allgemein konnte die Vermutung, dass es keine weiteren Fermatschen Primzahlen gibt, allerdings noch nicht bewiesen werden.

6.3 Konstruierbare p-Ecke

Wir haben im letzten Unterkapitel gezeigt, dass das p -Eck für alle Primzahlen, die nicht von der Form

$$p = 2^{2^n} + 1$$

sind, nicht konstruierbar ist. Daher stellt sich unweigerlich die Frage, ob zumindest die regelmäßigen Vielecke, deren Eckenanzahl einer Fermatschen Primzahl entspricht, konstruierbar sind. Für $p_0 = 3$ und $p_1 = 5$ haben wir

die Konstruierbarkeit des regelmäßigen Dreiecks und des regelmäßigen Fünfecks bereits in Kapitel 4.1 und Kapitel 4.2 nachgewiesen. Tatsächlich lässt sich zeigen, dass das regelmäßige p -Eck für alle Fermatschen Primzahlen p konstruierbar ist.

Satz 6.9. *(ohne Beweis) Sei p eine ungerade Primzahl. Dann sind die folgenden Aussagen äquivalent:*

1. *Das p -Eck ist konstruierbar.*
2. *p ist eine Fermatsche Primzahl der Form*

$$p = 2^{2^n} + 1$$

für ein $n \in \mathbb{N}_0$

Die Implikation

$$(1) \Rightarrow (2)$$

haben wir bereits im vorherigen Kapitel bewiesen. Der Beweis ließ sich dabei mit elementaren Methoden der Algebra und Zahlentheorie führen. Betrachten wir die Implikation

$$(2) \Rightarrow (1),$$

so müssen wir nach dem Hauptsatz 5.26 zeigen, dass die reelle Zahl

$$\cos \frac{2\pi}{p}$$

für eine Fermatsche Primzahl p in einem Körperturm

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n \subseteq \mathbb{R}$$

mit $\cos \frac{2\pi}{p} \in K_n$ und $[K_{i+1} : K_i] \leq 2$ liegt. Dieser Beweis benötigt weiterführende algebraische Methoden aus der Galoistheorie, die auf den französischen Mathematiker *Évariste Galois* zurückzuführen sind. Im Sinne der Übersichtlichkeit und des elementaren Zugangs zur Algebra, den wir in dieser Arbeit gewählt haben, ist diese interessante Implikation der einzige Beweis, den wir in dieser Arbeit nicht führen werden. Wir wollen jedoch trotzdem die Arbeit von Carl Friedrich Gauß würdigen, der erstmals zeigen konnte, dass alle p -Ecke für Fermatsche Primzahlen p tatsächlich konstruierbar sind. Deswegen betrachten wir in diesem Kapitel den bahnbrechenden Beweis der Konstruierbarkeit des regelmäßigen 17-Ecks, der Gauß dazu bewegte, sich statt eines Studiums der alten Sprachen der Mathematik zu widmen. Innerhalb des Beweises können wir Strukturen festhalten, die sich schlussendlich auf

6 Welche n-Ecke sind konstruierbar?

die Beweise der Konstruierbarkeit des regelmäßigen p -Ecks für die weiteren Fermatschen Primzahlen $p_3 = 257$ und $p_4 = 65537$ übertragen lassen. Der nachfolgende Beweis der Konstruierbarkeit des regelmäßigen 17-Ecks ist daher mehr als nur ein Beispiel für die Konstruktion eines Körperturms für die reelle Zahl

$$\cos \frac{2\pi}{17}$$

nach den Bedingungen des Hauptsatzes 5.26.

Das regelmäßige 17-Eck

Zur Konstruktion bedienen wir uns einer Erkenntnis, die uns bereits bei der Konstruktion des regelmäßigen Fünfecks in Kapitel 4.2 geholfen hat. Die vergleichbaren Ideen in der Konstruktion sind dabei nur wenig überraschend, da auch $p_1 = 5$ eine Fermatsche Primzahl ist.

Wir gruppieren jeweils zwei der 17-ten Einheitswurzeln wie folgt:

$$\begin{aligned} 2 \cos \alpha &= z_1 + z_1^{-1} = z_1 + z_{16}, \\ 2 \cos 2\alpha &= z_2 + z_2^{-1} = z_2 + z_{15}, \\ &\dots \\ 2 \cos 8\alpha &= z_8 + z_8^{-1} = z_8 + z_9 \end{aligned}$$

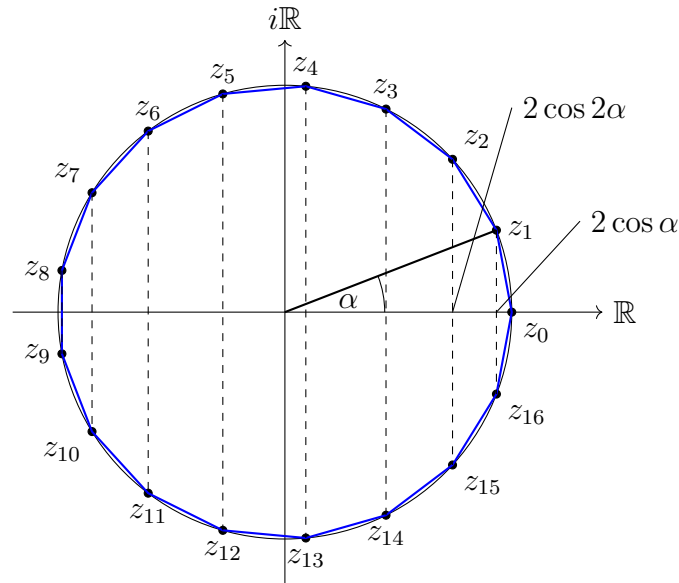
für $\alpha = \frac{2\pi}{p}$.

Der nächste Schritt beinhaltet die geniale Idee von Gauß. Seien $a_1, a_2 \in \mathbb{R}$ mit

$$\begin{aligned} a_1 &= 2 \cos \alpha + 2 \cos 2\alpha + 2 \cos 4\alpha + 2 \cos 8\alpha \quad \text{und} \\ a_2 &= 2 \cos 3\alpha + 2 \cos 5\alpha + 2 \cos 6\alpha + 2 \cos 7\alpha. \end{aligned}$$

Vergleichbare Summen werden wir im Verlauf dieses Beweises immer wieder auffinden. Sie werden auch **Gaußsche Bahnen** oder **Gaußsche Perioden** genannt [Toe10, S. 306].

6 Welche n-Ecke sind konstruierbar?



Wir machen uns nun zunutze, dass wir das Minimalpolynom aller nicht-trivialen p -ten Einheitswurzeln bereits kennen. Es ist von der Form

$$f(x) = x^{p-1} + x^{p-2} + \dots + 1.$$

Somit gilt

$$f(z_k) = z_k^{p-1} + \dots + z_k + 1 = 0$$

für alle $k \in \{1, \dots, p-1\}$. Dabei stellt nach Satz 6.5 jeder Summand genau eine der p -ten Einheitswurzeln dar. Da 17 eine Primzahl ist und wir in den obigen Gaußschen Bahnen alle 17-ten Einheitswurzeln, bis auf die triviale Einheitswurzel $z_0 = 1$, aufsummiert haben, gilt

$$a_1 + a_2 = -1.$$

Wir können a_1 und a_2 auch multiplizieren. Das Produkt enthält dabei jede nicht-triviale 17-te Einheitswurzel genau viermal. Wir erhalten daher eine zweite Gleichung

$$a_1 \cdot a_2 = -4.$$

Damit sind a_1 und a_2 die Nullstellen des Polynoms

$$g(x) = (x - a_1)(x - a_2) = x^2 - (a_1 + a_2)x + a_1a_2 = x^2 + x + 4.$$

Anhand der obigen Zeichnung erkennen wir unschwer den Zusammenhang $a_1 > a_2$ und erhalten für die Nullstellen der quadratischen Funktion g die expliziten Lösungen

$$a_1 = \frac{-1 + \sqrt{17}}{2} \quad \text{und} \quad a_2 = \frac{-1 - \sqrt{17}}{2}.$$

6 Welche n-Ecke sind konstruierbar?

Vielleicht lässt sich nun schon erkennen, wie wir den Korperturm aus dem Hauptsatz 5.26 aufbauen wollen, denn g ist das Minimalpolynom von a_1 , weil $\sqrt{17}$ eine irrationale Zahl ist. Daher gibt es einen Korperturm

$$\mathbb{Q} \subseteq \mathbb{Q}(a_1) \subseteq \mathbb{R}$$

mit $[\mathbb{Q}(a_1) : \mathbb{Q}] = 2$ und $a_1, a_2 \in \mathbb{Q}(a_1)$. Nun zerlegen wir auf ähnliche Weise die Gaußsche Bahn a_1 in

$$\begin{aligned} b_1 &= 2 \cos \alpha + 2 \cos 4\alpha \quad \text{und} \\ b_2 &= 2 \cos 2\alpha + 2 \cos 8\alpha \end{aligned}$$

mit $b_1 > b_2$. Für die Summe $b_1 + b_2$ gilt

$$b_1 + b_2 = a_1.$$

Das Produkt $b_1 b_2$ schreiben wir exemplarisch konkret aus. Es gilt:

$$\begin{aligned} b_1 b_2 &= (2 \cos \alpha + 2 \cos 4\alpha) \cdot (2 \cos 2\alpha + 2 \cos 8\alpha) \\ &= (z_1 + z_{16} + z_4 + z_{13}) \cdot (z_2 + z_{15} + z_8 + z_9) \\ &= (z_1 + z_1^{16} + z_1^4 + z_1^{13}) \cdot (z_1^2 + z_1^{15} + z_1^8 + z_1^9) \\ &= z_1^3 + z_1^{16} + z_1^9 + z_1^{10} + z_1 + z_1^{14} + z_1^7 + z_1^8 + \\ &\quad z_1^6 + z_1^2 + z_1^{12} + z_1^{13} + z_1^{15} + z_1^{11} + z_1^4 + z_1^5 = -1. \end{aligned}$$

Somit sind b_1 und b_2 die Nullstellen des Polynoms

$$h_1(x) = (x - b_1)(x - b_2) = x^2 - (b_1 + b_2)x + b_1 b_2 = x^2 - a_1 x - 1$$

mit Koeffizienten aus $\mathbb{Q}(a_1)$. Daher gilt in jedem Fall $[\mathbb{Q}(a_1, b_1) : \mathbb{Q}(a_1)] \leq 2$. Wir erhalten

$$b_1 = \frac{a_1 + \sqrt{a_1^2 + 4}}{2} \quad \text{und} \quad b_2 = \frac{a_1 - \sqrt{a_1^2 + 4}}{2}.$$

Dabei gibt es einen Korperturm

$$\mathbb{Q} \subseteq \mathbb{Q}(a_1) \subseteq \mathbb{Q}(a_1, b_1) \subseteq \mathbb{R}$$

mit $b_1, b_2 \in \mathbb{Q}(a_1, b_1)$ für welchen nach dem Gradsatz 5.22 $[\mathbb{Q}(a_1, b_1) : \mathbb{Q}] = 2^k$ für ein $k \in \{1, 2\}$ gilt.

Für unseren letzten Schritt benötigen wir zwei Zerlegungen Gaußscher Bahnen. Zunächst zerlegen wir a_2 in

$$\begin{aligned} c_1 &= 2 \cos 3\alpha + 2 \cos 5\alpha \quad \text{und} \\ c_2 &= 2 \cos 6\alpha + 2 \cos 7\alpha. \end{aligned}$$

6 Welche n-Ecke sind konstruierbar?

Wir erhalten sofort

$$c_1 + c_2 = a_2$$

und $c_1 > c_2$. Für das Produkt $c_1 c_2$ gilt

$$c_1 c_2 = -1.$$

Erneut finden wir ein quadratisches Polynom mit den Nullstellen c_1 und c_2 . Es ist von der Form

$$h_2(x) = x^2 - a_2 x - 1$$

mit Koeffizienten aus $\mathbb{Q}(a_1, b_1)$. Die expliziten Nullstellen von h_2 sind

$$c_1 = \frac{a_2 + \sqrt{a_2^2 + 4}}{2} \quad \text{und} \quad c_2 = \frac{a_2 - \sqrt{a_2^2 + 4}}{2}.$$

Als letzten Schritt zerlegen wir nun b_1 in

$$d_1 = 2 \cos \alpha \quad \text{und}$$

$$d_2 = 2 \cos 4\alpha.$$

Dabei gelten $d_1 > d_2$, $d_1 + d_2 = b_1$ und

$$\begin{aligned} d_1 d_2 &= 2 \cos \alpha \cdot 2 \cos 4\alpha \\ &= (z_1 + z_1^{16})(z_1^4 + z_1^{13}) \\ &= z_1^5 + z_1^{14} + z_1^3 + z_1^{12} \\ &= 2 \cos 3\alpha + 2 \cos 5\alpha \\ &= c_1. \end{aligned}$$

Wir erhalten ein weiteres quadratisches Polynom mit den Nullstellen d_1 und d_2 . Es ist von der Form

$$h_3(x) = x^2 - b_1 x + c_1$$

mit den expliziten Nullstellen

$$d_1 = \frac{b_1 + \sqrt{b_1^2 - 4c_1}}{2} \quad \text{und} \quad d_2 = \frac{b_1 - \sqrt{b_1^2 - 4c_1}}{2}.$$

Wegen

$$\frac{d_1}{2} = \cos \frac{2\pi}{17}$$

6 Welche n-Ecke sind konstruierbar?

haben wir nun unser Ziel erreicht. Setzen wir alle explizit berechneten Ausdrücke ein, so erhalten wir die Darstellung

$$\cos\left(\frac{2\pi}{17}\right) = \frac{1}{16} \left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + \sqrt{68 + 12\sqrt{17} + 2(\sqrt{17} - 1)\sqrt{34 - 2\sqrt{17}} - 16\sqrt{34 + 2\sqrt{17}}} \right).$$

Wir besitzen nun zwei äquivalente Möglichkeiten, die Konstruierbarkeit des 17-Ecks zu folgern. Im Sinne der Kapitel 2 bis 4 ist der gesuchte Ausdruck

$$\frac{d_1}{2} = \cos \frac{2\pi}{17}$$

ausschließlich mithilfe von rationalen Zahlen und den Verknüpfungen $+$, $-$, $\cdot$, $\div$ und $\sqrt{}$ darstellbar. Gleichbedeutend gibt es einen Körperturm der Form

$$\mathbb{Q} \subseteq \mathbb{Q}(a_1) \subseteq \mathbb{Q}(a_1, b_1) \subseteq \mathbb{Q}(a_1, b_1, c_1) \subseteq \mathbb{Q}(a_1, b_1, c_1, d_1) \subseteq \mathbb{R}$$

mit $\cos \frac{2\pi}{17} \in \mathbb{Q}(a_1, b_1, c_1, d_1)$ und

$$[\mathbb{Q}(a_1, b_1, c_1, d_1) : \mathbb{Q}] = 2^k$$

für ein $k \in \{1, \dots, 4\}$. Daher ist die reelle Zahl $\cos \frac{2\pi}{17}$ und somit das 17-Eck konstruierbar [Toe10, S. 305-308].

Das regelmäßige 257-Eck und das 65537-Eck

Das Verfahren zur konkreten Konstruktion weiterer p -Ecke ähnelt für eine Fermatsche Primzahl p dem Vorgehen für das regelmäßige 17-Eck. Gauß zeigte zwar, dass jedes dieser p -Ecke konstruierbar ist, entwarf aber keine Vorschrift für eine konkrete Konstruktion des 257-Ecks und des 65537-Ecks.

Ein Verfahren zur Konstruktion des 257-Ecks beschrieb der Deutsche *Friedrich Julius Richelot* in seiner Dissertation im Jahr 1832. Schließlich war es *Johann Gustav Hermes*, dem im Jahr 1889 eine Konstruktion des 65537-Ecks gelang. Die mehrere hundert Seiten lange Konstruktionsvorschrift hatte den deutschen Mathematiker dabei 10 Jahre lang beschäftigt. Sein Werk reichte er in einem Koffer an der Universität Göttingen ein. Bis auf einen kurzen Bericht in den Göttinger Nachrichten - fünf Jahre nach dessen Einreichung - wurde sein Werk allerdings zu seinen Lebzeiten kaum gewürdigt. Das Werk ist jedoch bis heute erhalten geblieben und erhielt somit, über 100 Jahre später, noch seinen ehrenvollen Platz im Museum der Universität Göttingen [Toe10, S. 314].

6.4 Das regelmäßige p^2 -Eck ist nicht konstruierbar

Wir sind nun fast in der Lage, allgemein zu bestimmen, wann das regelmäßige n -Eck für eine natürliche Zahl $n \geq 3$ konstruierbar ist. Der letzte vorbereitende Satz betrachtet nun das p^2 -Eck für eine ungerade Primzahl p . Bevor wir den Satz zum p^2 -Eck beweisen können, betrachten wir zur Vorbereitung kurz, welche der p^2 -ten Einheitswurzeln primitiv sind.

Lemma 6.10. *Sei p eine ungerade Primzahl. Dann gelten die folgenden Aussagen:*

1. *Für $j \in \{1, \dots, p^2\}$ ist eine p^2 -te Einheitswurzel z_j genau dann primitiv, wenn bereits $p \nmid j$ gilt.*
2. *Ist z_j eine primitive p^2 -te Einheitswurzel, so ist auch z_j^k für*

$$\text{ggT}(k, p^2) = 1$$

primitiv.

Beweis. 1. Sei zunächst $j \in \{1, \dots, p^2\}$ mit $p \mid j$. Dann ist p ein Teiler von j und es gilt $j = pm$ für ein $m \in \{1, \dots, p\}$. Daraus folgt

$$z_j = z_{pm} = e^{2\pi i mp/p^2} = e^{2\pi i m/p}.$$

Daher ist z_j eine p -te Einheitswurzel und es gilt

$$(z_j)^p = e^{2\pi i mp/p} = e^{2\pi i m} = 1.$$

Wegen $p < p^2$ sind daher alle p^2 -ten Einheitswurzeln

$$z_p, z_{2p}, \dots, z_{p^2}$$

nicht primitiv.

Sei nun $j \in \{1, \dots, p^2\}$ mit $p \nmid j$. Dann sind alle z_j p^2 -te Einheitswurzeln. Angenommen, es gibt ein $s \in \{1, \dots, p^2 - 1\}$ mit

$$(z_j)^s = 1.$$

Dann gilt

$$\left(e^{2\pi i j/p^2}\right)^s = e^{2\pi i js/p^2} = 1.$$

Diese Gleichung ist für

$$\frac{js}{p^2} \in \mathbb{Z}$$

erfüllt. Wegen $p \nmid j$ muss daher $p^2 \mid s$ gelten. Dies ist allerdings ein Widerspruch zu $s \in \{1, \dots, p^2 - 1\}$.

6 Welche n-Ecke sind konstruierbar?

2. Seien nun z_j eine primitive p^2 -te Einheitswurzel und $\text{ggT}(k, p^2) = 1$. Dann gilt

$$(z_j)^k = e^{2\pi i jk/p^2} = z_{jk}.$$

Nach Voraussetzung gilt $p \nmid k$ und nach der ersten Aussage des Lemmas $p \nmid j$. Da weder j noch k durch p teilbar sind, ist auch jk nicht durch p teilbar. Daher ist z_{jk} nach Teil (1) primitiv.

□

Wir sind nun bereit, das letzte vorbereitende Resultat auf dem Weg zum *Satz von Gauß-Wantzel* zu formulieren.

Satz 6.11. [Toe10, S. 309] *Sei p eine ungerade Primzahl. Dann ist das p^2 -Eck nicht konstruierbar.*

Beweis. Der Satz lässt sich nahezu vollständig mit der Argumentation des Satzes 6.7 zum p -Eck beweisen. Der einzige Unterschied besteht darin, dass wir diesmal das Polynom

$$F(x) = x^{p^2} - 1$$

betrachten und es in die Polynome

$$\begin{aligned} g(x) &= x^p - 1 \quad \text{und} \\ h(x) &= x^{p(p-1)} + x^{p(p-2)} + \dots + x^p + 1 \end{aligned}$$

mit

$$F(x) = g(x) \cdot h(x)$$

zerlegen. Die Nullstellen von g sind die p -ten Einheitswurzeln. Alle weiteren p^2 -ten Einheitswurzeln sind nach Lemma 6.10 daher genau die primitiven p^2 -ten Einheitswurzeln. Nun zeigen wir, dass das Polynom

$$h(x) = x^{p(p-1)} + x^{p(p-2)} + \dots + x^p + 1$$

irreduzibel über dem Körper $\mathbb{Q}$ ist. Die nächsten Schritte im Beweis sind, mithilfe beider Aussagen des Lemmas 6.10, vollständig analog zum Beweis von Satz 6.7.

Abschließend erhalten wir daher, dass h insbesondere das Minimalpolynom der primitiven p^2 -ten Einheitswurzel z_1 über $\mathbb{Q}$ ist und folglich

$$[\mathbb{Q}(z_1) : \mathbb{Q}] = p(p-1)$$

gilt. Aufgrund des Gradsatzes 5.22 und des Lemmas 6.6 folgt

$$\begin{aligned} p(p-1) &= [\mathbb{Q}(z_1) : \mathbb{Q}] = [\mathbb{Q}(z_1) : \mathbb{Q}(\cos \frac{2\pi}{p^2})] \cdot [\mathbb{Q}(\cos \frac{2\pi}{p^2}) : \mathbb{Q}] \\ &= 2 \cdot [\mathbb{Q}(\cos \frac{2\pi}{p^2}) : \mathbb{Q}]. \end{aligned}$$

Dementsprechend muss

$$\frac{p(p-1)}{2} = [\mathbb{Q}(\cos \frac{2\pi}{p^2}) : \mathbb{Q}]$$

gelten. Da p ungerade ist, ist $\frac{p(p-1)}{2}$ aber mit Sicherheit keine Zweierpotenz und das regelmäßige p^2 -Eck somit nach Satz 5.27 nicht konstruierbar. $\square$

6.5 Der Satz von Gauß-Wantzel

In diesem Kapitel schließen wir unsere Betrachtung der Konstruierbarkeit regelmäßiger n -Ecke mit Zirkel und Lineal mit dem *Satz von Gauß-Wantzel* ab. Dieser beschreibt für eine natürliche Zahl $n \geq 3$ genau, wann ein regelmäßiges n -Eck konstruierbar ist. Der Satz führt dabei die Erkenntnisse aus

- Satz 4.1 zur Konstruierbarkeit des $2n$ -Ecks,
- Satz 6.1 zur Konstruierbarkeit des mn -Ecks,
- Satz 6.9 zur Konstruierbarkeit des p -Ecks und
- Satz 6.11, der zeigt, dass das p^2 -Eck für eine ungerade Primzahl p nicht konstruierbar ist

zusammen. Bis auf die allgemeine Rückrichtung der Äquivalenz in Satz 6.9, deren Beweis auf Methoden der Galoistheorie beruht, haben wir dabei alle benötigten Resultate detailliert vorbereitet und bewiesen. Kommen wir daher zum faszinierenden Abschlussresultat dieser Arbeit:

Satz 6.12 (Der Satz von Gauß-Wantzel). *[Beu18, S. 247]*

Das regelmäßige n -Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn n von der Gestalt

$$n = 2^k p_1 \dots p_s$$

ist, wobei $k \in \mathbb{N}_0$ ist und $p_1, \dots, p_s$ paarweise verschiedene Fermatsche Primzahlen sind.

Beweis. Sei zunächst n von der Form

$$n = 2^k p_1 \dots p_s$$

für $k \in \mathbb{N}_0$ und paarweise verschiedene Fermatsche Primzahlen $p_1, \dots, p_s$. Dann sind nach Satz 6.9 alle p_i -Ecke für $i \in \{1, \dots, s\}$ konstruierbar. Da alle Fermatschen Primzahlen teilerfremd sind, ist somit nach Satz 6.1 auch das

6 Welche n -Ecke sind konstruierbar?

$p_1 \dots p_s$ -Eck konstruierbar. Schlussendlich folgt aus Satz 4.1, dass auch das $2^k p_1 \dots p_s$ -Eck konstruierbar ist. Wegen

$$n = 2^k p_1 \dots p_s$$

ist somit das n -Eck konstruierbar.

Sei nun das regelmäßige n -Eck mit Zirkel und Lineal konstruierbar und

$$n = 2^k p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$$

die eindeutige Primfaktorzerlegung von n . Angenommen, es gibt einen ungeraden Primfaktor p_i mit

$$e_i \geq 2.$$

Dann gibt es eine Darstellung

$$n = p_i^2 \cdot m$$

für eine ungerade Primzahl p_i und ein $m \in \mathbb{N}$. Ist $m = 1$ oder $m = 2$, so ist das n -Eck genau dann konstruierbar, wenn das p_i^2 -Eck konstruierbar ist. Ist $m \geq 3$, so impliziert die Konstruierbarkeit des n -Ecks nach Satz 6.1 die Konstruierbarkeit des p_i^2 -Ecks und des m -Ecks. Insbesondere muss daher in allen Fällen das p_i^2 -Eck konstruierbar sein. Das ist aber ein Widerspruch zu Satz 6.11. Daher gilt für jeden Faktor $p_i^{e_i}$ der Primfaktorzerlegung von n $e_i = 1$. Daher muss n bereits von der Form

$$n = 2^k p_1 \dots p_r$$

für $k \in \mathbb{N}_0$ und paarweise verschiedene Primzahlen $p_1, \dots, p_r$ sein. Da das n -Eck konstruierbar ist, folgt aus Satz 6.1, dass jedes p_i -Eck konstruierbar ist. Nach Satz 6.9 ist dies nur möglich, wenn jede Primzahl p_i bereits eine Fermatsche Primzahl ist.

Somit besitzt n die Form

$$n = 2^k p_1 \dots p_r$$

für $k \in \mathbb{N}_0$ und paarweise verschiedene Fermatsche Primzahlen $p_1, \dots, p_r$. $\square$

Literatur

- [Ben25] Môtî Ben-Arî. *Mathematische Überraschungen*. Cham: Springer, 2025. ISBN: 978-3-031-76041-9. URL: <https://directory.doabooks.org/handle/20.500.12854/158424>.
- [Beu18] Albrecht Beutelspacher. *Zahlen, Formeln, Gleichungen: Algebra für Studium und Unterricht*. SpringerLink Bücher. Wiesbaden: Springer Spektrum, 2018. ISBN: 978-3-658-16106-4. DOI: 10.1007/978-3-658-16106-4. URL: <http://dx.doi.org/10.1007/978-3-658-16106-4>.
- [Bos23] Siegfried Bosch. *Algebra*. 10. Aufl. 2023. Berlin, Heidelberg: Springer Berlin Heidelberg, 2023. ISBN: 978-3-662-67464-2. DOI: 10.1007/978-3-662-67464-2. URL: <https://nbn-resolving.org/urn:nbn:de:bsz:31-epflicht-3018324>.
- [FS25] Gerd Fischer und Boris Andre Michael Springborn. *Lineare Algebra: Eine Einführung für Studienanfänger*. 20. Auflage 2025. Grundkurs Mathematik. Berlin, Heidelberg: Springer Berlin Heidelberg, 2025. ISBN: 978-3-662-71261-0. DOI: 10.1007/978-3-662-71261-0. URL: <https://nbn-resolving.org/urn:nbn:de:bsz:31-epflicht-3215380>.
- [Kri11] Andreas Kriegl. *Komplexe Analysis*. Vorlesungsskript, Universität Wien. 2011. URL: <https://www.mat.univie.ac.at/~kriegl/Skripten/2011SS.pdf>.
- [Küh25] Stefan Kühnlein. *Algebra und Zahlentheorie: Ausgewählte Fragestellungen und wichtige Konzepte*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2025. ISBN: 978-3-662-71523-9. DOI: 10.1007/978-3-662-71523-9. URL: <https://link.springer.com/book/10.1007/978-3-662-71523-9>.
- [Str19] Heinz Klaus Strick. *Mathematik Ist Schön: Anregungen Zum Anschauen und Erforschen Für Menschen Zwischen 9 und 99 Jahren*. 2., erweiterte und korrigierte Auflage. Berlin: Springer, 2019. ISBN: 978-3-662-59060-7. URL: <https://link.springer.com/book/10.1007/978-3-662-59060-7>.
- [Toe10] Fridtjof Toenniessen. *Das Geheimnis der Transzendenten Zahlen: Eine Etwas Andere Einführung in Die Mathematik*. 2. Auflage. Berlin, Germany: Springer, 2010. ISBN: 978-3-662-58326-5. URL: <https://link.springer.com/book/10.1007/978-3-662-58326-5>.