Dr. Silke Hartlieb, Prof. Dr. Luise Unger

Kurs 01320

Algebra und ihre Anwendungen

LESEPROBE

Fakultät für
Mathematik und Informatik

FernUniversität in Hagen

Inhaltsverzeichnis

Studierhinweise

Bevor es losgeht, möchten wir kurz vorstellen, worum es im Kurs „Algebra und ihre Anwendungen“ geht. Dazu wiederholen wir zunächst, was wir zu dem Begriff „Algebra“ im ersten Mathematikkurs der Fakultät für Mathematik und Informatik, dem Kurs „Mathematische Grundlagen“ bereits berichtet haben.

Das Wort Algebra entstand aus dem Titel eines arabischen Werks, dessen Verfasser, Muhammed ibn Musa Alchwarizmi, im ersten Viertel des 9. Jahrhunderts unserer Zeitrechnung gelebt hat. Aus dem Namen Alchwarizmi leitet sich der in der Informatik und Mathematik übliche Begriff des „Algorithmus“ her. Sie sehen Alchwarizmi hier auf einer sowjetischen Briefmarke, die 1983 zu Ehren seines 1200-jährigen Geburtstags herausgegeben wurde.

Der Titel des Werkes lautete:„Aldschebr walmukabala“. Dabei bedeutet „dschebr“ Wiederherstellung und „mukabala“ Gegenüberstellung, und die Bedeutung dieser Worte ist nach dem Mathematikhistoriker Moritz Cantor (1829–1920) die folgende:

„Wiederherstellung ist genannt, wenn eine Gleichung derart geordnet wird, dass auf beiden Seiten des Gleichheitszeichens nur positive Glieder sich finden; Gegenüberstellung sodann, wenn Glieder gleicher Natur nach vollzogener Gegenüberstellung nur noch auf der einen Seite vorkommen, wo sie eben im Überschusse vorhanden waren.“

Der Name des Gebietes Algebra verweist also auf die Kunst, Gleichungen zu lösen. Algebra ist mithin die mathematische Wissenschaft, die sich mit dem Lösen von Gleichungen beschäftigt.

Natürlich müssen wir spezifizieren, um welche Art von Gleichungen es eigentlich geht. Es gibt in der Mathematik die verschiedensten Formen von Gleichungen, etwa Differentialgleichungen, Integralgleichungen, Funktionalgleichungen und eben auch algebraische Gleichungen. Eine typische algebraische Gleichung ist zum Beispiel die Polynomgleichung

$$x^3 - 5x^2 + 11x - 6 = 0,$$

und man fragt sich etwa, für welche Werte von x diese Gleichung eine Lösung besitzt und wie viele Lösungen es gibt. In Analogie zur Linearen Algebra, wo man die Lösungsmengen von Systemen spezieller algebraischer Gleichungen (nämlich linearer Gleichungen) untersucht, gibt es auch Teilgebiete der Algebra, die sich mit der Struktur der Lösungsmengen von Systemen nicht linearer, algebraischer Gleichungen in mehreren Unbestimmten beschäftigen.

Kommen wir nun zum zweiten Teil des Kurstitels: Anwendungen der Algebra. Es ist irgendwie klar, dass eine Wissenschaft, die sich das Lösen von Gleichungen auf die Fahnen schreibt, viele Anwendungen haben wird, und dieses Gefühl täuscht nicht. Viele Teilgebiete der Mathematik tragen den Begriff „Algebra“ bereits in ihrem Titel. Die Algebraische Zahlentheorie untersucht zahlentheoretische Probleme mit algebraischen Mitteln. Sie grenzt sich damit von der Elementaren, der Analytischen und der Algorithmischen Zahlentheorie ab. Zum Thema Algebraische Zahlentheorie werden Sie in diesem Kurs nichts finden. Die Algebraische Geometrie untersucht die Lösungsmengen von Systemen nicht linearer algebraischer Gleichungen in mehreren Unbestimmten. Sie verwendet dabei Methoden der so genannten kommutativen Algebra. Wir werden in die Anfänge der Algebraischen Geometrie beziehungsweise der kommutativen Algebra in Kurseinheit 7 einführen. In der Computeralgebra geht es darum, Algorithmen zu entwickeln, die in vertretbarem Zeitaufwand Lösungen von (wie auch immer gearteten) Gleichungen finden. Anders als in der Numerik, wo versucht wird, gute Näherungslösungen zu finden, sind in der Computeralgebra exakte Lösungen gefordert. Die Computeralgebra ist in den letzten 20 Jahren zu einem riesigen Forschungsgebiet der Mathematik und Informatik geworden und in diesem Kurs können wir bestenfalls Teilaspekte vorstellen. Wir haben uns dafür entschieden, den Schwerpunkt auf endliche Körper beziehungsweise Polynomringe über endlichen Körpern zu legen, da diese in praktischen Anwendungen immer wieder benötigt werden. Im zweiten Teil von Kurseinheit 4 und in Kurseinheit 5 konzentrieren wir uns auf diese Themen – in den Kurseinheiten 2 und 3 stellen wir die mathematischen Grundlagen dafür zur Verfügung.

Andere Anwendungsgebiete der Algebra sind die Kryptografie (über die wir in diesem Kurs auch nichts schreiben) oder die Codierungstheorie. Bei der Codierungstheorie geht es um Folgendes: Stellen wir uns vor, wir hätten einen Sender und einen Empfänger von Informationen, wobei allerdings klar ist, dass es bei der Übertragung der Nachrichten höchstwahrscheinlich zu einer Verfälschung kommen wird (etwa die Bodenstation eines Satelliten, die den Satelliten zu einer Kursänderung bewegen will, wobei die übermittelten Daten unterwegs durch atmosphärisches Rauschen verfälscht werden können). Wie kann man die Nachricht so absichern, dass der Empfänger erkennt, dass ein Fehler aufgetreten ist (und den Sender um erneutes Schicken bitten kann) oder, besser noch, wie kann ein Fehler automatisch korrigiert werden? Die Codierungstheorie ist ein interdisziplinäres Forschungsgebiet der Mathematik, Informatik und Elektrotechnik. Wichtige mathematische Säulen sind die Lineare Algebra und die Algebra mit endlichen Körpern. In die Codierungstheorie werden wir in Kurseinheit 6 einführen.

Neben den bisher genannten Anwendungen der Algebra gibt es auch ganz kleine, quasi anrührende aber nicht minder spektakuläre Anwendungen von Algebra; und das führt schon zu einem Überblick über die erste Kurseinheit. Es gibt drei berühmte Probleme, die fragen, ob gewisse geometrische Konstruktionen unter der Einhaltung gewisser Spielregeln möglich sind oder nicht. Nicht, dass eine geglückte Konstruktion praktische Folgen hätte; diese Fragen sind reine Gedankenspielereien. Aber sie haben Intellektuelle über 2500 Jahre lang fasziniert, und sie konnten erst in der zweiten Hälfte des 19. Jahrhunderts beantwortet werden. Und zwar, indem die Geometrie in Algebra übersetzt wurde. Eine angenommene mögliche Konstruktion würde die Existenz einer Nullstelle eines speziellen Polynoms (also der Lösung einer speziellen algebraischen Gleichung) zur Folge haben, und man konnte zeigen, dass eine solche Lösung nicht existieren konnte. Details finden Sie in Kapitel 1.

Ob ein Polynom eine Nullstelle hat oder nicht, hängt davon ab, welche Lösungen wir akzeptieren. Das Polynom $T^2 - 2$ hat keine Nullstellen in $\mathbb{Z}$ oder in $\mathbb{Q}$, aber $\pm\sqrt{2}$ sind Nullstellen in $\mathbb{R}$. Das Polynom $T^2 + 2$ hat auch keine Nullstellen in $\mathbb{R}$, wohl aber in $\mathbb{C}$. Der so genannte Hauptsatz der Algebra besagt, dass jedes Polynom mit Koeffizienten in $\mathbb{C}$ (also zum Beispiel ein Polynom, dessen Koeffizienten alle in $\mathbb{Z}$ liegen) immer eine Nullstelle in $\mathbb{C}$ hat. Da man mit jeder Nullstelle λ den Faktor $T - \lambda$ von dem Ausgangspolynom abspalten kann, bedeutet dies, dass über $\mathbb{C}$ jedes Polynom in Linearfaktoren zerfällt. Der erste lückenlose Beweis des Hauptsatzes der Algebra wird dem Mathematiker und Astronomen Johann Carl Friedrich Gauß (1777-1855) zugeschrieben. Heutzutage sind etwa 50 verschiedene Beweise dieses Satzes bekannt. In der Regel wird er in einem eleganten Dreizeiler in der Funktionentheorie bewiesen. Wir werden in Kapitel 2 einen ziemlich neuen

Beweis vorstellen, der im Jahr 2003 von dem in den USA arbeitenden niederländischen Mathematiker Harm Derksen gefunden wurde. Das, was uns an diesem Beweis fasziniert, ist, dass er nur eine kleine, völlig unkritische Zutat aus der Analysis benötigt, und dann nur noch Methoden der Linearen Algebra verwendet. Wir könnten diesen Beweis problemlos in Kurseinheit 8 des Kurses „Lineare Algebra“ übernehmen.

Kapitel 1

Die klassischen griechischen Konstruktionsprobleme

Bevor es losgeht, möchte ich noch kurz einige Notationen festlegen. Mit $\mathbb{N}$ bezeichnen wir die Menge der natürlichen Zahlen, also $\mathbb{N} = \{1, 2, 3, \dots\}$, mit $\mathbb{N}_0$ die natürlichen Zahlen mit 0, mit $\mathbb{Z}$ die Menge der ganzen Zahlen, mit $\mathbb{Q}$ die Menge der rationalen Zahlen, mit $\mathbb{R}$ die Menge der reellen Zahlen und mit $\mathbb{C}$ die Menge der komplexen Zahlen. Abstrakte Körper bezeichnen wir mit $\mathbb{K}$, $\mathbb{F}$, $\mathbb{L}$ oder $\mathbb{M}$.

1.1 Konstruierbare Zahlen

Nehmen wir an, wir wollten geometrische Konstruktionen vornehmen. Als Hilfsmittel stehen uns dabei nur ein Lineal ohne Maßeinheiten und ein Zirkel zur Verfügung.

Wir stellen uns folgende Ausgangsfrage:

1.1.1 Frage: Gegeben sei eine Strecke der Länge 1. Für welche Werte $a \in \mathbb{R}$ können wir mit Zirkel und Lineal eine Strecke der Länge a konstruieren?

Dabei dürfen wir nur folgende Konstruktionen in der Ebene verwenden:

1.1.2 Fundamentale Konstruktionen:

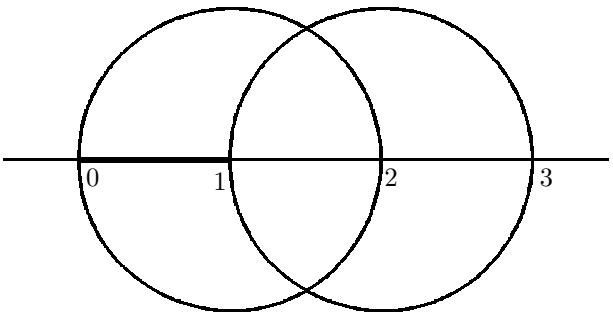
1. Wenn zwei Punkte gegeben sind, dürfen wir eine Gerade durch sie zeichnen.
2. Wenn zwei Punkte gegeben sind, dürfen wir die Verbindungsstrecke zwischen ihnen ziehen.

3. Wenn ein Punkt und eine Strecke gegeben sind, dürfen wir um den Punkt einen Kreis schlagen, dessen Radius die Länge der Strecke ist.

1.1.3 Definition: Eine reelle Zahl $a \in \mathbb{R}$ heißt **konstruierbar**, wenn eine Strecke der Länge $|a|$ aus einer Strecke der Länge 1 mit Hilfe von endlich vielen der fundamentalen Konstruktionen aus 1.1.2 mit Zirkel und Lineal konstruiert werden kann.

Dabei bezeichnet $|a|$ den Absolutbetrag einer reellen Zahl a.

1.1.4 Beispiel: Die Zahl -3 ist konstruierbar. Um das einzusehen, müssen wir eine Strecke der Länge $|-3| = 3$ aus einer Strecke der Länge 1 mit Hilfe von endlich vielen fundamentalen Konstruktionen basteln. Wir bezeichnen die Randpunkte der Strecke der Länge 1 mit 0 und 1. Durch 0 und 1 dürfen wir eine Gerade ziehen. Jetzt nehmen wir die Länge der vorgegebenen Strecke als Radius in unseren Zirkel und schlagen um 1 einen Kreis vom Radius 1. Dieser schneidet unsere Gerade in zwei Punkten, nämlich in 0 und einem weiteren Punkt, den wir 2 nennen. Jetzt schlagen wir um 2 einen Kreis vom Radius 1. Dieser schneidet die Gerade in zwei Punkten, nämlich in 1 und einem weiteren Punkt, den wir 3 nennen. Die Strecke zwischen 0 und 3 hat die Länge 3, und dies zeigt, dass -3 konstruierbar ist. Die folgende Graphik veranschaulicht unsere Konstruktion:



1.1.5 Aufgabe: Beweisen Sie, dass $\frac{1}{2}$ konstruierbar ist.

1.1.6 Vereinbarung: Wir wollen einen Punkt als eine Strecke der Länge 0 interpretieren. Damit ist die Zahl 0 konstruierbar, denn mit der vorgegebenen Strecke der Länge 1 haben wir auch deren Randpunkte gegeben, und diese sind mit dieser Vereinbarung Strecken der Länge 0.

Bei unserer Untersuchung der Frage 1.1.1, welche Zahlen $a \in \mathbb{R}$ konstruierbar sind, beginnen wir mit folgender Beobachtung:

1.1.7 Beobachtung: Alle Zahlen $a \in \mathbb{Z}$ sind konstruierbar.

Beweis: Mit unserer Vereinbarung ist 0 konstruierbar.

Unsere vorgegebene Strecke hat die Länge 1, daher können wir 1 und damit auch -1 konstruieren. Wie in Beispiel 1.1.4 benennen wir die Randpunkte der vorgegebenen Strecke mit 0 und 1 und ziehen durch 0 und 1 eine Gerade g. Jetzt nehmen wir die Länge 1 als Radius in unseren Zirkel und können jede natürliche Zahl n konstruieren, indem wir diese Länge n mal auf der Geraden g abtragen. Damit sind auch alle Zahlen in $\mathbb{Z}$ konstruierbar, denn nach Definition ist mit n auch $-n$ konstruierbar. □

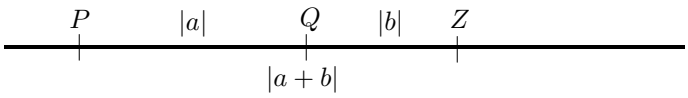
Die folgende Proposition zeigt, wie wir aus bereits konstruierten Zahlen mit Hilfe der Grundrechenarten weitere konstruieren können.

1.1.8 Proposition: Seien a und b zwei konstruierbare Zahlen. Dann sind $a + b$, $a - b$ und ab konstruierbar. Ist $b \neq 0$, so ist auch $\frac{a}{b}$ konstruierbar.

Beweis: Nach Annahme lassen sich zwei Strecken $\overline{PQ}$ und $\overline{RS}$ der Längen $|a|$ beziehungsweise $|b|$ konstruieren. Dabei bezeichnen P und Q beziehungsweise R und S die Randpunkte der Strecken. Wir müssen zeigen, dass wir Strecken der Länge $|a + b|$, $|a - b|$, $|ab|$ und $\left|\frac{a}{b}\right|$ konstruieren können; letzteres allerdings nur, falls $b \neq 0$ ist. Dabei können wir annehmen, dass a und b beide $\neq 0$ sind, denn anderenfalls wäre das Resultat 0 (also konstruierbar) oder a beziehungsweise b, und von denen wissen wir ja, dass sie konstruierbar sind. Wir gehen jetzt die einzelnen Rechnungen getrennt durch.

1. Wir zeigen, dass $|a + b|$ konstruierbar ist. Dabei unterscheiden wir verschiedene Fälle.

   1. Fall: Es sind $a > 0$ und $b > 0$. Wir ziehen durch P und Q eine Gerade g, nehmen die Länge b als Radius in unseren Zirkel und schlagen um Q einen Kreis mit Radius $|b| = b$. Der Kreis schneidet g in dem Punkt Z, der auf der zu P entgegengesetzten Seite von Q auf der Geraden g liegt, und die Strecke $\overline{PZ}$ hat die Länge $a + b = |a + b|$ (vergleiche folgende Skizze).



   2. Fall: Es sind $a < 0$ und $b < 0$. Dann gelten $-a > 0$ und $-b > 0$ und

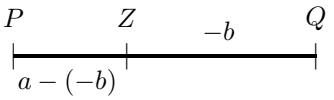
$a + b < 0$, also

$$|a + b| = -(a + b) = -a - b = -a + (-b).$$

Wir konstruieren wie im ersten Fall eine Strecke der Länge $(-a) + (-b) = |a + b|$, und dies zeigt, dass $a + b$ konstruierbar ist.

3. Fall: Es sind $a > 0$ und $b < 0$, also $-b = |b| > 0$. Hier unterscheiden wir wieder zwei Fälle.

   (a) Es ist $a + b \geq 0$, also $|a + b| = a + b = a - (-b)$. Wir ziehen durch P und Q die Verbindungsstrecke $\overline{PQ}$, nehmen die Länge $-b$ in den Zirkel und schlagen um Q einen Kreis mit Radius $-b$. Der Kreis schneidet $\overline{PQ}$ in Z, und die Strecke $\overline{PZ}$ hat die Länge $|a + b| = a - (-b)$ (vergleiche folgende Skizze).

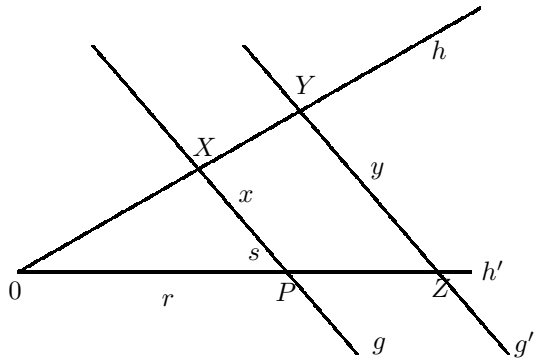


   (b) Es ist $a + b < 0$, also $|a + b| = -(a + b) = -a - b = -a + (-b) = (-b) - a > 0$. Wie im Fall (a) konstruieren wir eine Strecke der Länge $|a + b|$, und es folgt, dass $a + b$ konstruierbar ist.

4. Fall: Es ist $a < 0$ und $b > 0$. Wir benennen a und b um, und wie im dritten Fall folgt, dass $a + b$ konstruierbar ist.

2. Es ist $a - b = a + (-b)$. Wenn b konstruierbar ist, dann ist $-b$ konstruierbar, und im ersten Teil des Beweises haben wir gezeigt, dass $a+(-b)$ konstruierbar ist.

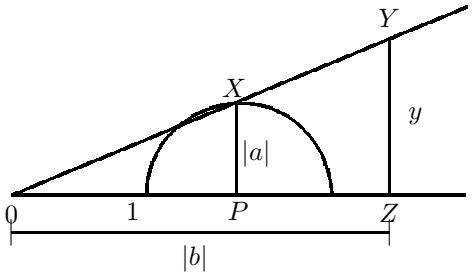
3. Zum Beweis, dass eine Strecke der Länge $|ab| = |a| \cdot |b|$ konstruierbar ist, erinnere ich an den Strahlensatz. Gegeben seien zwei Strahlen h und h', die von zwei Parallelen g und g' mit Schnittpunkten X, P und Y und Z geschnitten werden:



Seien x die Länge der Stecke $\overline{XP}$, y die Länge der Strecke $\overline{YZ}$, r die Länge der Strecke $\overline{0P}$ und s die Länge der Strecke $\overline{0Z}$. Der Strahlensatz besagt, dass dann $\frac{x}{r} = \frac{y}{s}$ ist.

Kommen wir nun zur Konstruktion von $|ab| = |a| \cdot |b|$.

Wir zeichnen eine Strecke $\overline{0P}$ der Länge 1 und legen durch 0 und P eine Gerade h. Wir schlagen um P einen Kreis K mit Radius $|a|$. Wir errichten auf P die Senkrechte g zur Geraden h (wie man das mit Zirkel und Lineal bewerkstelligt, müssen Sie in Aufgabe 1.1.9 zeigen). Diese schneidet K im Punkt X. Die Strecke $\overline{PX}$ hat die Länge $|a|$. Wir zeichnen die Gerade h' durch 0 und X. Wir schlagen um 0 einen Kreis mit Radius $|b|$. Dieser schneidet h im Punkt Z. Wir zeichnen die Parallele g' zu g durch Z (wie das mit Zirkel und Lineal gemacht werden kann, sollen Sie in Aufgabe 1.1.10 zeigen). Sei Y der Schnittpunkt mit h'. Sei y die Länge von $\overline{YZ}$.

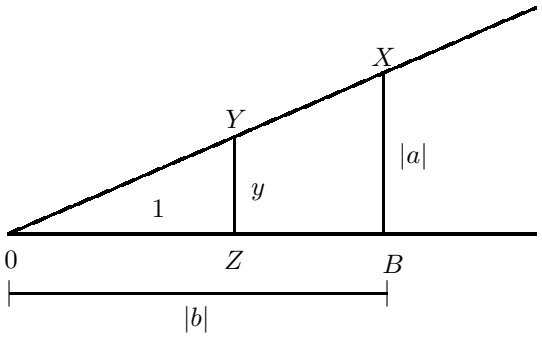


Mit dem Strahlensatz gilt

$$\frac{y}{|b|} = \frac{|a|}{1}, \text{ also } y = |a| \cdot |b| = |ab|.$$

Es folgt, dass ab konstruierbar ist.

4. Sei $b \neq 0$. Wir konstruieren eine Strecke der Länge $\frac{|a|}{|b|} = \left|\frac{a}{b}\right|$. Betrachten wir folgende Skizze.



Wir zeichnen eine Strecke $\overline{0B}$ der Länge $|b|$ und legen durch 0 und B eine Gerade h. Um B schlagen wir einen Kreis K mit Radius $|a|$. Wir errichten in B die Senkrechte zu h, diese schneidet K in X. Wir zeichnen die Gerade h' durch 0 und X. Wir schlagen um 0 einen Kreis mit Radius 1. Sei Z der Schnittpunkt mit h. Wir errichten auf Z die Senkrechte zu h. Diese schneidet h' in Y. Sei y die Länge der Strecke $\overline{YZ}$. Mit dem Strahlensatz gilt

$$y = \frac{|a|}{|b|} = \left|\frac{a}{b}\right|,$$

also ist $\frac{a}{b}$ konstruierbar.

□

1.1.9 Aufgabe: Sei g eine Gerade, und sei P ein Punkt auf g. Konstruieren Sie mit Zirkel und Lineal die Senkrechte zu g durch P.

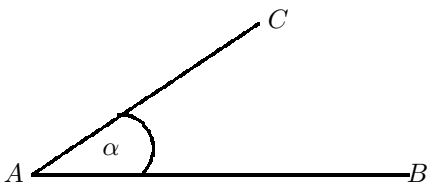
1.1.10 Aufgabe: Sei g eine Gerade, und sei X ein Punkt, der nicht auf g liegt. Konstruieren Sie mit Zirkel und Lineal eine Parallele durch X zu g.

Als Folgerung aus Beobachtung 1.1.7 und Proposition 1.1.8 erhalten wir:

1.1.11 Korollar: Alle Zahlen in $\mathbb{Q}$ sind konstruierbar.

Beweis: Mit 1.1.7 ist jede ganze Zahl konstruierbar, und mit 1.1.8 ist dann jeder Bruch $\frac{a}{b}$ mit $a, b \in \mathbb{Z}$ und $b \neq 0$ konstruierbar. Somit ist jede rationale Zahl konstruierbar. □

1.1.12 Notation: Sei α der folgende durch die Strecken $\overline{AB}$ und $\overline{AC}$ eingeschlossene Winkel.



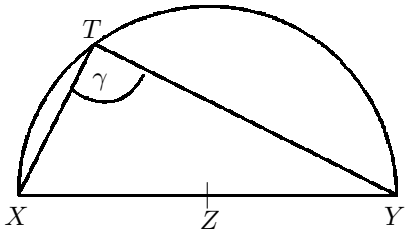
Wir bezeichnen α auch mit $\alpha = \angle BAC$.

Dazu folgende Faustregel. Der Scheitelpunkt des Winkels steht in der Mitte. Der erste Buchstabe ist B, denn wenn wir die Strecke $\overline{AB}$ um den Winkel α gegen den Uhrzeigersinn drehen, landen wir auf der Strecke $\overline{AC}$.

Neben den rationalen Zahlen gibt es aber noch weitere reelle Zahlen, die konstruierbar sind. Dies zu zeigen werden wir jetzt in Angriff nehmen. Zum Beweis brauchen wir allerdings noch drei klassische Ergebnisse der Geometrie, die Sie vermutlich schon aus dem Mittelstufenunterricht kennen. Zum Beweis verwenden wir, dass die Summe der Winkel in einem ebenen Dreieck 180° beträgt.

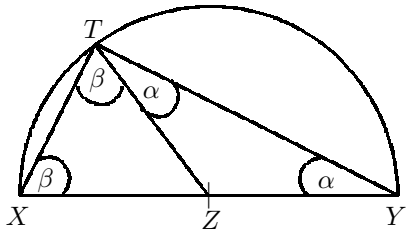
1.1.13 Satz: (Satz von Thales)

Sei T ein Punkt auf einem Halbkreis mit Mittelpunkt Z, und seien X und Y die Schnittpunkte des Durchmessers durch Z mit dem Halbkreis, also:



Dann ist der Winkel $\gamma = \angle XTY$ ein rechter Winkel.

Beweis: Die Strecken $\overline{XZ}$, $\overline{TZ}$ und $\overline{YZ}$ haben dieselbe Länge, also sind die Dreiecke XZT und TZY gleichschenklig.



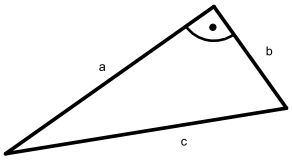
Es folgt $\angle ZXT = \angle XTZ (= \beta)$ und $\angle ZTY = \angle TYZ (= \alpha)$. Es folgt

$$180° = 2\alpha + 2\beta, \text{ also } 90° = \alpha + \beta = \angle XTY.$$

□

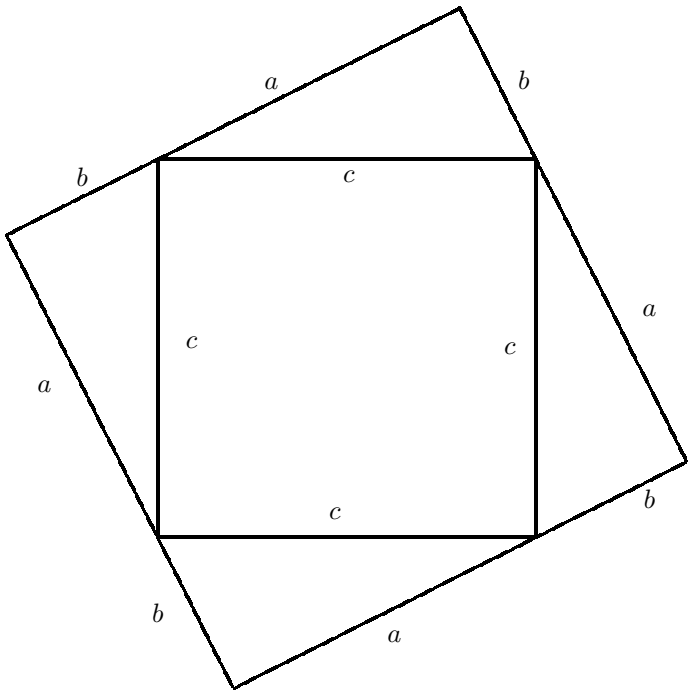
1.1.14 Satz: (Pythagoras)

Gegeben sei ein rechtwinkliges Dreieck mit Seitenlängen a, b, c wie folgt:



Dann gilt $a^2 + b^2 = c^2$.

Beweis: Wir betrachten folgende Skizze:



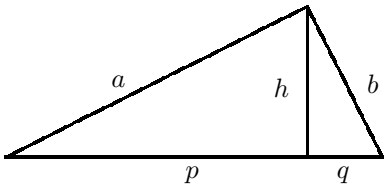
Der Flächeninhalt des großen Quadrats ist $(a+b)^2$, der der vier Dreiecke $\frac{ab}{2}$, der des kleinen Quadrats ist c^2. Es folgt

$$c^2 = (a+b)^2 - 4\frac{ab}{2} = a^2 + 2ab + b^2 - 2ab = a^2 + b^2.$$

□

1.1.15 Satz: (Höhensatz von Euklid)

Gegeben sei ein rechtwinkliges Dreieck mit Höhe der Länge h:



Dann gilt $h^2 = pq$.

Beweis: Wir wenden den Satz von Pythagoras auf alle Dreiecke an: Es gilt

$$a^2 + b^2 = (p+q)^2 = p^2 + 2pq + q^2,$$

sowie

$$a^2 = h^2 + p^2 \text{ und } b^2 = h^2 + q^2.$$

Einsetzen liefert

$$h^2 + p^2 + h^2 + q^2 = p^2 + 2pq + q^2.$$

Wir vereinfachen und erhalten

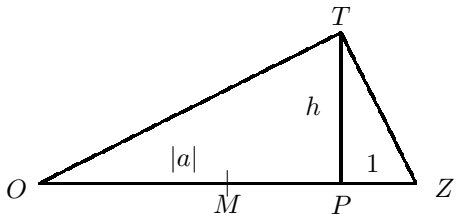
$$2h^2 = 2pq, \text{ also } h^2 = pq.$$

□

Wenden wir uns jetzt wieder der Frage zu, welche Zahlen konstruierbar sind.

1.1.16 Proposition: Sei $a \in \mathbb{R}$ konstruierbar. Dann ist $\sqrt{|a|}$ konstruierbar.

Beweis: Wir betrachten eine Strecke $\overline{OP}$ der Länge $|a|$. Wir zeichnen durch O und P eine Gerade und schlagen um P einen Kreis mit Radius 1. Dies liefert eine Strecke $\overline{OZ}$ der Länge $|a| + 1$. Jetzt errichten wir auf P die Senkrechte g und halbieren die Strecke $\overline{OZ}$ (mit Proposition 1.1.8 ist diese Konstruktion mit Zirkel und Lineal möglich). Der Mittelpunkt der Strecke $\overline{OZ}$ sei M. Wir schlagen um M einen Kreis mit Radius $\frac{|a|+1}{2}$. Sei T der Schnittpunkt des Kreises mit g. Der Satz von Thales garantiert, dass das Dreieck OTZ rechtwinklig ist. Die Strecke $\overline{TP}$ ist die Höhe. Sei h die Länge der Höhe. Dann haben wir folgende Situation:



Mit dem Höhensatz von Euklid gilt $h^2 = |a| \cdot 1$, also $h = \sqrt{|a|}$. □

1.1.17 Aufgabe: Beweisen Sie, dass $\frac{4}{3}\sqrt{\sqrt{6} + \sqrt{1 + 2\sqrt{7}}}$ konstruierbar ist.

Proposition 1.1.16 zeigt, dass es unendlich viele konstruierbare Zahlen gibt, die irrational sind. Ich erinnere nämlich an folgendes Ergebnis, das im Kurs „Elementare Zahlentheorie mit Maple“ bewiesen wird:

1.1.18 Proposition: Seien m und n natürliche Zahlen. Sei $n \geq 2$.

Wenn $\sqrt[n]{m}$ rational ist, dann liegt $\sqrt[n]{m}$ schon in $\mathbb{N}$.

Wenden wir dieses Ergebnis auf Quadratwurzeln an, so sehen wir, dass $\sqrt{|a|}$ mit $|a| \in \mathbb{N}$ genau dann rational ist, wenn $|a|$ eine Quadratzahl ist.

Fassen wir unsere bisherigen Überlegungen noch einmal zusammen. Wir haben bisher gezeigt, dass jede Zahl $a \in \mathbb{R}$, die durch sukzessives Anwenden von Grundrechenarten $+$, $-$, $\cdot$, $:$ und Quadratwurzelziehen aus bereits konstruierten Zahlen entsteht, konstruierbar ist. Was wir noch nicht wissen, und was wir in Abschnitt 1.3 zeigen werden, ist, dass alle konstruierbaren Zahlen so entstehen.

1.2 Drei klassische Konstruktionsprobleme

Es wird Zeit zu verraten, warum das Problem, welche Zahlen konstruierbar sind, so faszinierend ist. Das hat unter anderem historische Gründe, denn dieses Problem hat die Mathematik fast 2500 Jahre beschäftigt, bevor es befriedigend gelöst werden konnte. Es gibt drei klassische Konstruktionsprobleme, die vermutlich um 500 vor unserer Zeitrechnung in Griechenland gestellt wurden und seitdem die Mathematik gefesselt haben. Diese Probleme haben gemeinsam, dass die Größen, nach deren Konstruktion gefragt wurde, nicht mit Zirkel und Lineal konstruiert werden können (dass dies so ist, weiß man allerdings erst seit etwa 150 Jahren). Wie soll

man beweisen, dass eine Zahl nicht konstruierbar ist? Natürlich kann man beweisen, dass eine vorgelegte Konstruktion nicht das Gewünschte leistet, aber wie soll man beweisen, dass es keine wie auch immer geartete Konstruktionsmöglichkeit für die vorgegebene Größe gibt?

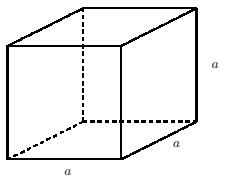
Faszinierend ist auch, dass eine Lösung dieses rein geometrischen Problems der Konstruierbarkeit von Zahlen mit Methoden gefunden wurde, die auf den ersten Blick nichts mit Geometrie zu tun haben. Gelöst wurde es mit Methoden der Algebra, wobei die klassische Algebra sich mit dem Lösen von Gleichungen befasst, zu deren Formulierung nur endlich viele Rechenoperationen (Addition, Subtraktion, Multiplikation, Division) erforderlich sind. Eine typische Frage der klassischen Algebra ist etwa, ob, wie viele und welche Lösungen einer Gleichung der Form $x^5 - 4x^2 + 3x - 5 = 0$ existieren.

In Abschnitt 1.3 werden wir die klassischen Konstruktionsprobleme lösen; jetzt will ich sie erst einmal vorstellen.

1.2.1 Das Deli'sche Problem

Der Sage nach war die Stadt Athen von einer Seuche bedroht. Die Bürger schickten eine Delegation zum Orakel von Delphi, um den Gott Apollo um Rat zu fragen, wie sie sich schützen sollten. Apollo forderte zur Abwendung der Seuche die Verdoppelung seines Altars in Würfelform dem Volumen nach.

Analysieren wir den Wunsch. Angenommen, der Altar habe die Kantenlänge a.



Dann hat er das Volumen a^3. Der hypothetische verdoppelte Würfel hätte das Volumen $2a^3$, also die Kantenlänge $\sqrt[3]{2a^3} = a\sqrt[3]{2}$, und diese müssten wir konstruieren können. Die Zahl a ist konstruierbar (sie ist ja schon konstruiert als Kantenlänge des Altars).

Damit stellt sich die Frage: Ist $\sqrt[3]{2}$ konstruierbar?

1.2.2 Die Quadratur des Kreises

Gegeben sei ein Kreis mit konstruierbarem Radius r. Der Flächeninhalt dieses Kreises beträgt πr^2. Ist es möglich, ein Quadrat mit Zirkel und Lineal zu konstruieren, dessen Flächeninhalt ebenfalls πr^2 ist?

Wäre dies möglich, so müssten wir ein Quadrat der Seitenlänge $r\sqrt{\pi}$, insbesondere müssten wir $\sqrt{\pi}$ konstruieren können.

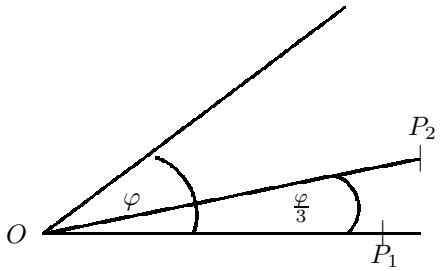
1.2.1 Aufgabe: Seien a und $a\sqrt{b}$ konstruierbar. Beweisen Sie, dass $\sqrt{b}$ konstruierbar ist.

Die Frage ist also: Ist $\sqrt{\pi}$ konstruierbar?

1.2.3 Die Dreiteilung von beliebigen Winkeln

Dieses Problem ist etwas anders als die bisherigen. Bei den Problemen oben geht es darum, zu überprüfen, ob eine konkret gegebene Zahl konstruierbar ist. Bei der Dreiteilung von Winkeln geht es darum, ob ein beliebiger vorgegebener Winkel mit Hilfe von Zirkel und Lineal gedrittelt werden kann.

Genauer: Gegeben sei ein beliebiger vorgegebener Winkel φ:



Die Frage lautet: Können wir immer einen Punkt P_2 so konstruieren, dass der Winkel $\angle P_1OP_2$ die Größe $\frac{\varphi}{3}$ hat?

1.2.4 Über Winkeldreiteiler und Kreisquadriererinnen

Wir werden in dieser Kurseinheit zeigen, dass die klassischen griechischen Konstruktionsprobleme nicht lösbar sind. Mit anderen Worten, es gibt keine wie auch immer gestaltete Konstruktion mit Zirkel und Lineal, die einen Kreis quadriert, einen Würfel dem Volumen nach verdoppelt oder einen 60°-Winkel in drei gleiche

Teile teilt. Solche Unmöglichkeitsbeweise sind für mathematische Laien nur schwer nachvollziehbar, und daher gibt es überraschend viele Leute, die einen Satzanfang der Form „Es ist nicht möglich,...“ als „Bis jetzt haben wir es noch nicht hingekriegt,...“ übersetzen. Es gibt also auch heute noch etliche Personen, die ihre vermeintlich geglückten Konstruktionen an mathematische Fachbereiche schicken, und dann sehr enttäuscht sind (oder sehr böse werden), wenn man ihnen mitteilt, dass man nicht gewillt sei, dies genauer anzusehen, da die Konstruktion sowieso falsch sein müsse. Eine Kollegin an der Norwegischen Technischen Universität in Trondheim hat mir erzählt, dass ein Winkeldreiteiler versucht hat, die Universität zu verklagen, weil sie ihm angeblich seine Konstruktion geklaut habe. Es gibt sogar Bücher über die schönsten falschen Konstruktionsversuche.

Eine besonders eifrige (verbale) Kreisquadriererin scheint Angela Merkel zu sein.

Die Frankfurter Rundschau meldete am 13. 11. 2005, dass Frau Merkel die Schwierigkeiten bei den Koalitionsverhandlungen mit CSU und SPD dadurch beschrieben hat, dass sie schwieriger seien als die Quadratur des Kreises, dass sie sozusagen der „Kubatur der Kugel“ entsprechen würden.

Vergleichsweise gelassen blickte Frau Merkel der deutschen EU-Ratspräsidentschaft entgegen. In einem Interview mit der Süddeutschen Zeitung äußerte sie sich am 5.11.2006 über die Probleme der EU, die bevorstehende deutsche Ratspräsidentschaft und Probleme mit Ankara mit den Worten „Wir müssen die Quadratur des Kreises schaffen“.

1.3 Der Hauptsatz über konstruierbare Zahlen

Wir werden in diesem Abschnitt unsere Ausgangsfrage, welche reellen Zahlen konstruierbar sind, umformulieren und in einen algebraischen Kontext überführen.

1.3.1 Unterkörper

Wir haben in der Linearen Algebra bereits Körper und Ringe kennen gelernt. Wir hatten auch definiert, was ein Unterring eines Ringes ist. Ganz analog definieren wir jetzt Unterkörper von Körpern.

1.3.1 Definition: Sei $\mathbb{K}$ ein Körper. Eine Teilmenge $\mathbb{F}$ von $\mathbb{K}$ heißt **Unterkörper** von $\mathbb{K}$, wenn $\mathbb{F}$ mit der Addition und der Multiplikation in $\mathbb{K}$ ein Körper ist. Ist $\mathbb{F}$ ein Unterkörper von $\mathbb{K}$, so wird $\mathbb{K}$ eine **Körpererweiterung** (oder **Erweite-**

rungskörper oder **Oberkörper**) von $\mathbb{F}$ genannt. Ein **echter Unterkörper** von $\mathbb{K}$ ist ein Unterkörper $\mathbb{F}$, der eine echte Teilmenge von $\mathbb{K}$ ist.

Ähnlich wie das Unterraumkriterium in der Linearen Algebra beweist man das folgende nützliche Unterkörperkriterium:

1.3.2 Bemerkung: (Unterkörperkriterium)

Sei $\mathbb{K}$ ein Körper, und sei $\mathbb{F}$ eine Teilmenge von $\mathbb{K}$. Genau dann ist $\mathbb{F}$ ein Unterkörper von $\mathbb{K}$, wenn gilt:

1. Für alle $a, b \in \mathbb{F}$ liegen $a + b$, $a - b$, ab in $\mathbb{F}$. Ist $b \neq 0$, so liegt $\frac{a}{b}$ in $\mathbb{F}$.
2. Es ist $1 \in \mathbb{F}$.

Beweis:

$\Rightarrow$ Sei $\mathbb{F}$ ein Unterkörper von $\mathbb{K}$. Dann erfüllt $\mathbb{F}$ nach Definition die Bedingung 1. Auch die zweite Bedingung ist erfüllt, denn $\mathbb{F}$ hat nach Definition eines Körpers ein Einselement $e \in \mathbb{F}$, für das $ea = ae = a$ für alle $a \in \mathbb{F}$ gilt. Es ist also insbesondere $ee = e = 1e$. Multiplikation mit e^{-1} liefert $e = 1$.

$\Leftarrow$ Sei $\mathbb{F}$ eine Teilmenge von $\mathbb{K}$, die die Bedingungen 1. und 2. erfüllt. Nach Voraussetzung liegt das neutrale Element 1 der Multiplikation in $\mathbb{F}$. Mit der ersten Bedingung liegt auch $1 - 1 = 0$ in $\mathbb{F}$, somit enthält $\mathbb{F}$ das neutrale Element der Addition. Mit $a \in \mathbb{F}$ liegt auch $0 - a = -a$ in $\mathbb{F}$, jedes Element aus $\mathbb{F}$ besitzt also ein additives Inverses in $\mathbb{F}$. Ist $b \neq 0$, so liegt $1 \cdot \frac{1}{b} = \frac{1}{b}$ in $\mathbb{F}$, somit besitzt jedes Element $\neq 0$ in $\mathbb{F}$ ein inverses Element in $\mathbb{F}$. Die übrigen Bedingungen folgen, weil sie schon in $\mathbb{K}$ gelten.

□

Als Folgerung aus Proposition 1.1.8 erhalten wir:

1.3.3 Korollar: Die Menge $\mathbb{M}$ der konstruierbaren Zahlen ist ein Unterkörper von $\mathbb{R}$.

Beweis: Nach Definition ist $\mathbb{M}$ eine Teilmenge von $\mathbb{R}$. Das Element 1 liegt in $\mathbb{M}$, denn es ist nach Annahme eine Strecke der Länge 1 gegeben. Proposition 1.1.8 besagt, dass auch die erste Bedingung des Unterkörperkriteriums erfüllt ist. □

1.3.4 Aufgabe: Sei $\mathbb{F}$ ein Unterkörper von $\mathbb{C}$. Beweisen Sie, dass $\mathbb{Q}$ ein Unterkörper von $\mathbb{F}$ ist.

1.3.2 Quadratische Erweiterungen

Sei $\mathbb{F}$ ein Unterkörper von $\mathbb{R}$, und sei $k \in \mathbb{F}$, $k > 0$, fest gewählt. Wir bezeichnen mit $\mathbb{F}(\sqrt{k})$ die Menge

$$\mathbb{F}(\sqrt{k}) = \{a + b\sqrt{k} \mid a, b \in \mathbb{F}\}.$$

Ausgesprochen wird $\mathbb{F}(\sqrt{k})$ als „F adjungiert Wurzel k“.

Analysieren wir diese Menge:

- Immer gilt $\mathbb{F} \subseteq \mathbb{F}(\sqrt{k})$, denn sei $a \in \mathbb{F}$ ein beliebiges Element. Wir haben oben gesehen, dass $0 \in \mathbb{F}$ gilt. Mit $b = 0$ gilt dann

  $$a = a + 0 \cdot \sqrt{k} \in \mathbb{F}(\sqrt{k}),$$

  das heißt, jedes Element aus $\mathbb{F}$ liegt auch in $\mathbb{F}(\sqrt{k})$. Somit gilt $\mathbb{F} \subseteq \mathbb{F}(\sqrt{k})$, wie behauptet.

- Angenommen, $\sqrt{k} \in \mathbb{F}$, zum Beispiel $\mathbb{F} = \mathbb{Q}$ und $k = \frac{1}{4}$. Mit der ersten Bedingung des Unterkörperkriteriums gilt $b\sqrt{k} \in \mathbb{F}$ für alle $b \in \mathbb{F}$, und dann auch $a + b\sqrt{k} \in \mathbb{F}$ für alle $a \in \mathbb{F}$. Es folgt, dass jedes Element $a + b\sqrt{k}$ bereits in $\mathbb{F}$ liegt. Es folgt also $\mathbb{F}(\sqrt{k}) \subseteq \mathbb{F}$. Nun hatten wir aber gerade überlegt, dass immer $\mathbb{F} \subseteq \mathbb{F}(\sqrt{k})$ gilt. Zusammen bedeutet dies, dass $\mathbb{F} = \mathbb{F}(\sqrt{k})$ ist, sofern $\sqrt{k} \in \mathbb{F}$ ist.

- Angenommen, $\sqrt{k} \notin \mathbb{F}$, also zum Beispiel $\mathbb{F} = \mathbb{Q}$ und $k = 2$. Da $\sqrt{k} = 0 + 1 \cdot \sqrt{k} \in \mathbb{F}(\sqrt{k})$, denn $1, 0 \in \mathbb{F}$, aber $\sqrt{k} \notin \mathbb{F}$, folgt, dass $\mathbb{F} \neq \mathbb{F}(\sqrt{k})$ ist. In dieser Situation ist $\mathbb{F}$ in $\mathbb{F}(\sqrt{k})$ echt enthalten.

In jedem Fall ist $\mathbb{F}(\sqrt{k})$ ein Körper, wie in der folgenden Proposition gezeigt wird.

1.3.5 Proposition: Sei $\mathbb{F}$ ein Unterkörper von $\mathbb{R}$. Sei $k \in \mathbb{F}$, $k > 0$. Dann ist $\mathbb{F}(\sqrt{k})$ ein Unterkörper von $\mathbb{R}$.

Beweis: Wenn $\sqrt{k} \in \mathbb{F}$, dann sind wir schon fertig, denn wir haben oben gesehen, dass dann $\mathbb{F}(\sqrt{k}) = \mathbb{F}$ ist, und $\mathbb{F}$ ist nach Annahme ein Unterkörper von $\mathbb{R}$.

Wir werden also im Folgenden annehmen, dass $\sqrt{k} \notin \mathbb{F}$ gilt.

Da $\sqrt{k} \in \mathbb{R}$, $\mathbb{F} \subseteq \mathbb{R}$, und da $\mathbb{R}$ ein Unterkörper von $\mathbb{R}$ ist, folgt mit der ersten Bedingung des Unterkörperkriteriums, dass $b\sqrt{k} \in \mathbb{R}$ und $a + b\sqrt{k} \in \mathbb{R}$ für alle $a, b \in \mathbb{F}$ gilt. Wir haben also $\mathbb{F}(\sqrt{k}) \subseteq \mathbb{R}$.

Da $1 \in \mathbb{F}$ und $\mathbb{F} \subseteq \mathbb{F}(\sqrt{k})$, folgt $1 \in \mathbb{F}(\sqrt{k})$, die zweite Bedingung des Unterkörperkriteriums. Wir müssen also nur noch die erste Bedingung überprüfen.

Seien $a+b\sqrt{k}$ und $a'+b'\sqrt{k}$ mit $a,a',b,b' \in \mathbb{F}$ beliebige Elemente in $\mathbb{F}(\sqrt{k})$. Dann gilt

$$(a+b\sqrt{k})+(a'+b'\sqrt{k}) = \underbrace{(a+a')}_{\in\mathbb{F}} + \underbrace{(b+b')}_{\in\mathbb{F}}\sqrt{k},$$

und es folgt, dass $(a+b\sqrt{k})+(a'+b'\sqrt{k})$ in $\mathbb{F}(\sqrt{k})$ liegt.

Analog gilt

$$(a+b\sqrt{k})-(a'+b'\sqrt{k}) = \underbrace{(a-a')}_{\in\mathbb{F}} + \underbrace{(b-b')}_{\in\mathbb{F}}\sqrt{k} \in \mathbb{F}(\sqrt{k})$$

und

$$(a+b\sqrt{k})\cdot(a'+b'\sqrt{k}) = \underbrace{(aa'+bb'k)}_{\in\mathbb{F}} + \underbrace{(ab'+a'b)}_{\in\mathbb{F}}\sqrt{k} \in \mathbb{F}(\sqrt{k}).$$

Sei nun $a'+b'\sqrt{k} \neq 0$. Es bleibt zu zeigen, dass $\frac{a+b\sqrt{k}}{a'+b'\sqrt{k}} \in \mathbb{F}(\sqrt{k})$ gilt. Um unsere Rechnungen gleich zu vereinfachen, zeigen wir zunächst, dass auch $a'-b'\sqrt{k} \neq 0$ ist. Dazu nehmen wir an, dass $a'-b'\sqrt{k}=0$ ist. Dann gilt

$$0 \neq a'+b'\sqrt{k} = a'+b'\sqrt{k}-0 = a'+b'\sqrt{k}-(a'-b'\sqrt{k}) = 2b'\sqrt{k}.$$

Es ist also $2b'\sqrt{k} \neq 0$, und es folgt $b' \neq 0$. Wir können also die Gleichung $a'-b'\sqrt{k}=0$ durch b' teilen und erhalten

$$\frac{a'}{b'} - \sqrt{k} = 0, \text{ also } \sqrt{k} = \frac{a'}{b'}.$$

Da $\mathbb{F}$ ein Unterkörper von $\mathbb{R}$ ist, und da $a',b' \in \mathbb{F}$ gilt, folgt $\frac{a'}{b'} = \sqrt{k} \in \mathbb{F}$, und das ist ein Widerspruch, denn wir hatten angenommen, dass $\sqrt{k} \notin \mathbb{F}$ gilt. Dieser Widerspruch zeigt, dass $a'-b'\sqrt{k} \neq 0$ ist.

Wir wissen also jetzt, dass $a'-b'\sqrt{k} \neq 0$ ist, und wir können den Ausdruck $\frac{a'-b'\sqrt{k}}{a'-b'\sqrt{k}} = 1$ bilden. Dann gilt

$$\begin{aligned}
\frac{a+b\sqrt{k}}{a'+b'\sqrt{k}} &= \frac{(a+b\sqrt{k})(a'-b'\sqrt{k})}{(a'+b'\sqrt{k})(a'-b'\sqrt{k})} \\
&= \frac{aa'-ab'\sqrt{k}+a'b\sqrt{k}-bb'k}{a'^2-b'^2k} \\
&= \underbrace{\frac{aa'-bb'k}{a'^2-b'^2k}}_{\in\mathbb{F}} + \underbrace{\frac{a'b-ab'}{a'^2-b'^2k}}_{\in\mathbb{F}}\sqrt{k} \in \mathbb{F}(\sqrt{k}).
\end{aligned}$$

Es gilt also auch die erste Bedingung des Unterkörperkriteriums, und es folgt, dass $\mathbb{F}(\sqrt{k})$ ein Unterkörper von $\mathbb{R}$ ist. □

1.3.6 Aufgabe: Schreiben Sie die Ergebnisse der folgenden Rechnungen in der Form $a + b\sqrt{3}$ mit $a, b \in \mathbb{Q}$:

1. $(2 + 8\sqrt{3})(1 - 6\sqrt{3})$,
2. $\frac{1}{8-4\sqrt{3}}$,
3. $\frac{4+3\sqrt{3}}{6-5\sqrt{3}}$.

Wir hatten oben bereits gesehen, dass $\mathbb{F} \neq \mathbb{F}(\sqrt{k})$ ist, sofern $\sqrt{k} \notin \mathbb{F}$ gilt. In dieser Situation erhält $\mathbb{F}(\sqrt{k})$ eine spezielle Bezeichnung:

1.3.7 Definition: Sei $\mathbb{F}$ ein Unterkörper von $\mathbb{R}$, und sei $k \in \mathbb{F}$ mit $k > 0$ und $\sqrt{k} \notin \mathbb{F}$. Dann wird $\mathbb{F}(\sqrt{k})$ eine **reell-quadratische Erweiterung** von $\mathbb{F}$ genannt.

Kommen wir nun mit dieser neuen Terminologie zu den konstruierbaren Zahlen zurück.

1.3.8 Proposition: Angenommen, wir haben eine endliche Folge $\mathbb{Q} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_{n-1} \subseteq \mathbb{F}_n$ von Unterkörpern von $\mathbb{R}$ gegeben, sodass $\mathbb{F}_{j+1}$ für alle $0 \leq j < n$ eine reell-quadratische Erweiterung von $\mathbb{F}_j$ ist. Dann ist jedes $a \in \mathbb{F}_n$ konstruierbar.

Beweis: Wir beweisen die Behauptung mit Induktion nach n. Im Induktionsanfang sei $n = 0$. Dann ist die Behauptung, dass alle Elemente in $\mathbb{F}_0 = \mathbb{Q}$ konstruierbar sind, und das haben wir in Korollar 1.1.11 bereits bewiesen. Der Induktionsanfang ist also richtig.

Die Induktionsannahme ist, dass die Behauptung für ein $n \geq 0$ richtig ist, dass also alle Elemente in $\mathbb{F}_n$ konstruierbar sind.

Im Induktionsschritt müssen wir zeigen, dass alle Elemente in $\mathbb{F}_{n+1}$ konstruierbar sind, sofern $\mathbb{F}_{n+1}$ eine reell-quadratische Erweiterung von $\mathbb{F}_n$ ist. Sei also

$$\mathbb{F}_{n+1} = \mathbb{F}_n(\sqrt{k_n}) = \{a_n + b_n\sqrt{k_n} \mid a_n, b_n \in \mathbb{F}_n\},$$

wobei $k_n \in \mathbb{F}_n$, $k_n > 0$ und $\sqrt{k_n} \notin \mathbb{F}_n$ gilt. Sei a ein beliebiges Element in $\mathbb{F}_{n+1}$. Dann gibt es Elemente $a_n, b_n \in \mathbb{F}_n$ mit $a = a_n + b_n\sqrt{k_n}$. Nach Induktionsannahme sind a_n, b_n und k_n konstruierbar. Mit Proposition 1.1.16 ist $\sqrt{k_n}$ konstruierbar. Aus Proposition 1.1.8 folgt, dass $b_n\sqrt{k_n}$ konstruierbar ist, und wieder mit Proposition 1.1.8 ist dann auch $a_n + b_n\sqrt{k_n}$ konstruierbar. Damit sind alle Elemente in $\mathbb{F}_{n+1}$ konstruierbar. □

1.3.9 Definition: Eine endliche Folge $\mathbb{Q} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_{n-1} \subseteq \mathbb{F}_n$ von Unterkörpern von $\mathbb{R}$ mit der Eigenschaft, dass $\mathbb{F}_{j+1}$ für alle $0 \leq j < n$ eine reell-quadratische Erweiterung von $\mathbb{F}_j$ ist, wird ein **reell-quadratischer Körperturm** in $\mathbb{R}$ genannt.

1.3.10 Aufgabe: Sei $\mathbb{F}$ ein Unterkörper von $\mathbb{R}$, und seien $k, k' \in \mathbb{F}$ mit $k, k' > 0$ und $k \neq k'$.

Beweisen Sie, dass $(\mathbb{F}(\sqrt{k}))(\sqrt{k'}) = (\mathbb{F}(\sqrt{k'}))(\sqrt{k})$ ist.

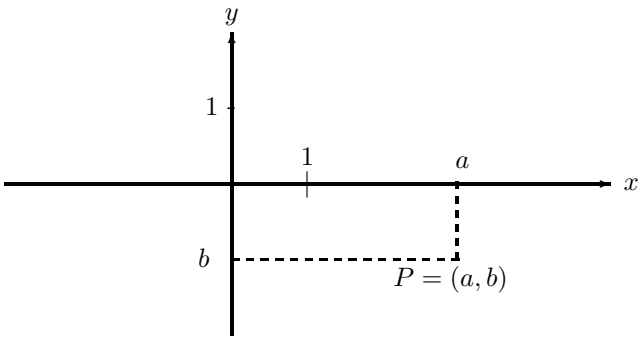
1.3.11 Aufgabe: Untersuchen Sie, ob die folgenden Zahlen in $((\mathbb{Q}(\sqrt{2}))(\sqrt{3}))(\sqrt{5})$ liegen:

1. $4 + 8\sqrt{12}$,
2. $\sqrt{6} + 3\sqrt{15}$,
3. $\sqrt{10} + \sqrt{30}$.

1.3.3 Eine algebraische Charakterisierung konstruierbarer Zahlen

Proposition 1.3.8 besagt, dass gewisse Zahlen konstruierbar sind, nämlich diejenigen, die in einem reell-quadratischen Körperturm, ausgehend von $\mathbb{Q}$ liegen. Es stellt sich die Frage, ob es weitere konstruierbare Zahlen gibt. Wir werden in diesem Abschnitt sehen, dass dies nicht der Fall ist.

Die Konstruktion von Zahlen spielt sich in der euklidischen Ebene $\mathbb{R}^2$ ab. Wir stellen uns vor, dass diese Ebene mit einem rechtwinkligen Koordinatensystem versehen ist, und dass jeder Punkt P eindeutig durch seine Koordinaten (a, b) gegeben ist:



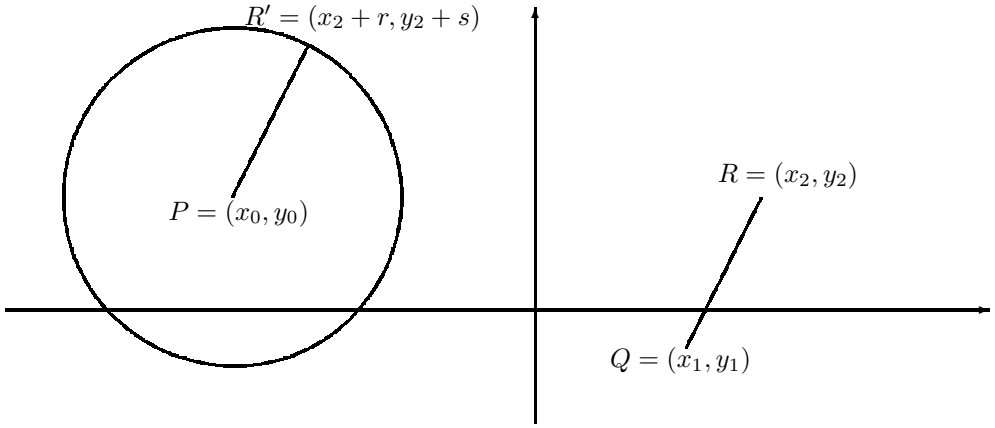
1.3.12 Aufgabe: Beweisen Sie, dass ein Punkt $P = (a, b)$ in $\mathbb{R}^2$ genau dann mit Zirkel und Lineal konstruierbar ist, wenn a und b konstruierbare Zahlen sind.

1.3.13 Definition: Sei $\mathbb{F}$ ein Unterkörper von $\mathbb{R}$.

1. Die **Ebene von** $\mathbb{F}$ besteht aus denjenigen Punkten (x, y) der euklidischen Ebene $\mathbb{R}^2$, für die $x \in \mathbb{F}$ und $y \in \mathbb{F}$ gilt.
2. Eine **Gerade in** $\mathbb{F}$ ist eine Gerade in $\mathbb{R}^2$, die mindestens zwei verschiedene Punkte in der Ebene von $\mathbb{F}$ enthält.
3. Ein **Kreis in** $\mathbb{F}$ ist ein Kreis in $\mathbb{R}^2$, sodass der Mittelpunkt und mindestens ein Punkt auf der Kreislinie in der Ebene von $\mathbb{F}$ liegen.

1.3.14 Bemerkung: Sei $\mathbb{F}$ ein Unterkörper von $\mathbb{R}$, und seien P, Q und R Punkte in der Ebene von $\mathbb{F}$. Sei a die Länge der Strecke $\overline{QR}$, und sei K der Kreis um P mit Radius a. Dann ist K ein Kreis in $\mathbb{F}$.

Beweis: Anschaulich gesprochen verschieben wir die Strecke $\overline{QR}$ so, dass Q auf P geschoben wird. Genauer: Seien $P = (x_0, y_0)$, $Q = (x_1, y_1)$ und $R = (x_2, y_2)$. Sei $r = x_0 - x_1$ und $s = y_0 - y_1$. Dann gilt $r, s \in \mathbb{F}$, und $(x_1 + r, y_1 + s) = (x_0, y_0)$. Der Punkt $R' = (x_2 + r, y_2 + s)$ liegt ebenfalls in der Ebene von $\mathbb{F}$, denn $x_2 + r$ und $y_2 + s$ liegen in $\mathbb{F}$. Die Längen der Strecken $\overline{QR}$ und $\overline{PR'}$ sind gleich. Somit liegt R' auf K, und es folgt, dass K ein Kreis in $\mathbb{F}$ ist.



□

Das folgende Lemma gibt Geraden- beziehungsweise Kreisgleichungen für Geraden beziehungsweise Kreise in $\mathbb{F}$ an.

1.3.15 Lemma: Sei $\mathbb{F}$ ein Unterkörper von $\mathbb{R}$.

1. Sei g eine Gerade in $\mathbb{F}$. Dann gibt es $a, b, c \in \mathbb{F}$ mit
$$g = \{(x, y) \in \mathbb{R}^2 \mid ax + by + c = 0\}.$$

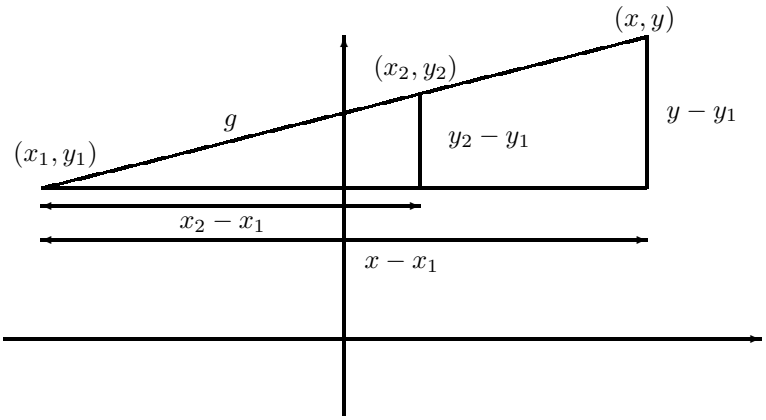
2. Sei K ein Kreis in $\mathbb{F}$. Dann gibt es $a, b, c \in \mathbb{F}$ mit
$$K = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 + ax + by + c = 0\}.$$

Beweis:

1. Sei g eine Gerade in $\mathbb{F}$. Nach Definition gibt es mindestens zwei verschiedene Punkte (x_1, y_1) und (x_2, y_2) in g mit $x_1, x_2, y_1, y_2 \in \mathbb{F}$.

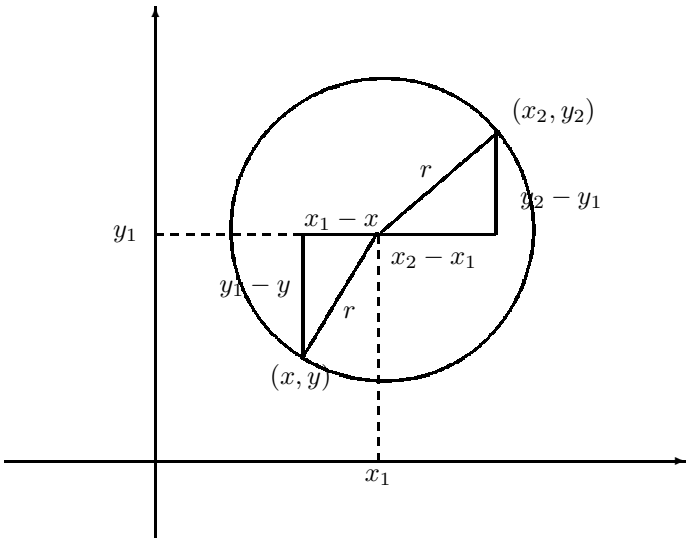
   Wir nehmen zunächst an, dass $x_1 = x_2$ ist. Dann ist g parallel zur y-Achse, enthält also alle Punkte (x, y) mit $x = x_1$ und $y \in \mathbb{R}$ beliebig. Mit $a = 1$, $b = 0$ und $c = -x_1$ gilt $a, b, c \in \mathbb{F}$ und
   $$g = \{(x, y) \in \mathbb{R}^2 \mid ax + by + c = 0\}.$$

   Wir nehmen jetzt an, dass $x_1 \neq x_2$ gilt. Betrachten wir folgende Skizze:



   Die Steigung von g kann durch $\frac{y_2-y_1}{x_2-x_1}$ berechnet werden. Mit dem Strahlensatz gilt für jeden weiteren Punkt (x, y) auf g die Beziehung $\frac{y-y_1}{x-x_1} = \frac{y_2-y_1}{x_2-x_1}$. Umformen ergibt $(y_2 - y_1)x + (x_1 - x_2)y + (y_1x_2 - x_1y_2) = 0$. Mit $a = y_2 - y_1$, $b = x_1 - x_2$ und $c = y_1x_2 - x_1y_2$ gilt $a, b, c \in \mathbb{F}$ und
   $$g = \{(x, y) \in \mathbb{R}^2 \mid ax + by + c = 0\}.$$

2. Sei (x_1, y_1) der Mittelpunkt des Kreises. Dieser liegt nach Annahme in der Ebene von $\mathbb{F}$. Sei (x_2, y_2) in der Ebene von $\mathbb{F}$ und auf der Kreislinie. Sei r der Radius des Kreises.



Mit dem Satz des Pythagoras gilt $r^2 = (x_2 - x_1)^2 + (y_2 - y_1)^2$. Ein Punkt (x, y) liegt genau dann auf dem Kreis, wenn gilt

$$\underbrace{(x_1 - x)^2}_{=(x-x_1)^2} + \underbrace{(y - y_1)^2}_{=(y_1-y)^2} = r^2 = (x_2 - x_1)^2 + (y_2 - y_1)^2,$$

also

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

Durch Umformen erhalten wir

$$x^2 + y^2 - 2x_1x - 2y_1y + (2x_1x_2 - x_2^2 + 2y_1y_2 - y_2^2) = 0.$$

Mit $a = -2x_1$, $b = -2y_1$ und $c = 2x_1x_2 - x_2^2 + 2y_1y_2 - y_2^2$ gilt $a, b, c \in \mathbb{F}$ und

$$K = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 + ax + by + c = 0\}.$$

□

1.3.16 Notation: Sei $\mathbb{F}$ ein Unterkörper von $\mathbb{R}$. Sei g eine Gerade in $\mathbb{F}$, und sei K ein Kreis in $\mathbb{F}$. Die Gleichungen $ax + by + c = 0$ und $x^2 + y^2 + ax + by + c = 0$ aus Lemma 1.3.15 werden die **Geradengleichung** von g beziehungsweise die **Kreisgleichung** von K genannt.

Bei der Konstruktion von Punkten mit Zirkel und Lineal, die wir benötigen, um Zahlen zu konstruieren, müssen wir folgendermaßen vorgehen:

- Wir müssen Geraden durch bereits konstruierte Punkte zum Schnitt bringen, oder
- wir müssen eine Gerade durch bereits konstruierte Punkte mit einem Kreis, dessen Mittelpunkt ein bereits konstruierter Punkt ist und dessen Radius die Länge einer Strecke zwischen bereits konstruierten Punkten ist, schneiden, oder
- wir müssen zwei Kreise, deren Mittelpunkte bereits konstruiert sind, und deren Radien Längen von Strecken zwischen bereits konstruierten Punkten sind, zum Schnitt bringen.

Welche Eigenschaften die jeweiligen Schnittpunkte haben, ist Thema des folgenden Lemmas.

1.3.17 Lemma: Sei $\mathbb{F}$ ein Unterkörper von $\mathbb{R}$.

1. Der Schnittpunkt von zwei Geraden in $\mathbb{F}$ liegt in der Ebene von $\mathbb{F}$.
2. Die Schnittpunkte einer Gerade in $\mathbb{F}$ mit einem Kreis in $\mathbb{F}$ liegen in der Ebene von $\mathbb{F}$ oder in der Ebene einer reell-quadratischen Erweiterung von $\mathbb{F}$.
3. Die Schnittpunkte von zwei verschiedenen Kreisen in $\mathbb{F}$ liegen in der Ebene von $\mathbb{F}$ oder in der Ebene einer reell-quadratischen Erweiterung von $\mathbb{F}$.

Beweis:

1. Seien g und g' zwei sich schneidende Geraden in $\mathbb{F}$ mit Geradengleichungen $a_1x + b_1y + c_1 = 0$ und $a_2x + b_2y + c_2 = 0$. Mit Lemma 1.3.15 liegen a_1, b_1, c_1, a_2, b_2 und c_2 in $\mathbb{F}$. Der Schnittpunkt (x, y) der Geraden muss beide Gleichungen erfüllen. Beachten Sie, dass a_1 und b_1 nicht beide gleichzeitig 0 sein können. Nehmen wir an, dass $a_1 \neq 0$ ist. Wir formen nach x um und erhalten $x = -\frac{b_1}{a_1}y - \frac{c_1}{a_1}$. Einsetzen in die zweite Gleichung liefert

$$a_2\left(-\frac{b_1}{a_1}y - \frac{c_1}{a_1}\right) + b_2y + c_2 = 0.$$

   Diese Gleichung können wir nach y umformen und erhalten $y \in \mathbb{F}$. Setzen wir dies in die erste Gleichung ein, so folgt $x \in \mathbb{F}$, also (x, y) in der Ebene von $\mathbb{F}$. Analog argumentieren wir, wenn $a_1 = 0$ und $b_1 \neq 0$ ist.

2. Sei g eine Gerade in der Ebene von $\mathbb{F}$ mit Geradengleichung $a_1x+b_1y+c_1 = 0$ und $a_1, b_1, c_1 \in \mathbb{F}$. Sei K ein Kreis in der Ebene von $\mathbb{F}$ mit der Kreisgleichung $x^2+y^2+a_2x+b_2y+c_2 = 0$ und $a_2, b_2, c_2 \in \mathbb{F}$. Wir setzen voraus, dass g und K sich schneiden, dass es also ein $(x, y) \in \mathbb{R}^2$ gibt, das beide Gleichungen erfüllt.

Wieder sind in der Geradengleichung nicht a_1 und b_1 beide gleichzeitig 0, und wir nehmen an, dass $b_1 \neq 0$ ist. Dann können wir die Geradengleichung nach y umformen und erhalten

$$y = -\frac{a_1}{b_1}x - \frac{c_1}{b_1}.$$

Wir setzen y in die Kreisgleichung ein und erhalten

$$\begin{aligned} 0 &= x^2 + \left(-\tfrac{a_1}{b_1}x - \tfrac{c_1}{b_1}\right)^2 + a_2x + b_2\left(-\tfrac{a_1}{b_1}x - \tfrac{c_1}{b_1}\right) + c_2 \\ &= (1 + \tfrac{a_1^2}{b_1^2})x^2 + (a_2 + 2\tfrac{a_1c_1}{b_1^2} - \tfrac{a_1b_2}{b_1})x + (\tfrac{c_1^2}{b_1^2} - \tfrac{b_2c_1}{b_1} + c_2). \end{aligned}$$

Es ist $1 + \frac{a_1^2}{b_1^2} \neq 0$, denn $\frac{a_1^2}{b_1^2} \geq 0$, das heißt, wir können diese Gleichung durch $1 + \frac{a_1^2}{b_1^2}$ teilen und erhalten

$$x^2 + \tilde{a}x + \tilde{b} = 0.$$

Genau interessieren uns die Koeffizienten $\tilde{a}$ und $\tilde{b}$ nicht, wichtig ist nur, dass sie in $\mathbb{F}$ liegen.

Da $x^2 + \tilde{a}x + \tilde{b} = 0$, ist x Nullstelle dieser quadratischen Gleichung, also ist

$$x = \underbrace{-\frac{\tilde{a}}{2}}_{\in\mathbb{F}} + \frac{1}{2}\sqrt{\underbrace{\tilde{a}^2 - 4\tilde{b}}_{\in\mathbb{F}}} \text{ oder } x = \underbrace{-\frac{\tilde{a}}{2}}_{\in\mathbb{F}} - \frac{1}{2}\sqrt{\underbrace{\tilde{a}^2 - 4\tilde{b}}_{\in\mathbb{F}}}.$$

Da sich g und K schneiden, muss $\tilde{a}^2 - 4\tilde{b} \geq 0$ sein. Setze $k = \tilde{a}^2 - 4\tilde{b}$. Dann folgt $x \in \mathbb{F}$ im Fall $k = 0$ oder $x \in \mathbb{F}(\sqrt{k})$ im Fall $k > 0$.

Falls $\sqrt{k} \in \mathbb{F}$, also $\mathbb{F}(\sqrt{k}) = \mathbb{F}$, so folgt $x \in \mathbb{F}$, und die Gleichung $y = -\frac{a_1}{b_1}x - \frac{c_1}{b_1}$ liefert $y \in \mathbb{F}$, und (x, y) liegt in der Ebene von $\mathbb{F}$. Falls $\sqrt{k} \notin \mathbb{F}$, liefert die Gleichung $y = -\frac{a_1}{b_1}x - \frac{c_1}{b_1}$, dass $y \in \mathbb{F}(\sqrt{k})$ liegt. Dann liegt der Punkt (x, y) in der Ebene von $\mathbb{F}(\sqrt{k})$.

Analog argumentieren wir, wenn $b_1 = 0$ und $a_1 \neq 0$ ist.

3. Seien K_1 und K_2 Kreise in $\mathbb{F}$ mit Kreisgleichungen $x^2+y^2+a_1x+b_1y+c_1 = 0$ und $x^2 + y^2 + a_2x + b_2y + c_2 = 0$, wobei a_1, b_1, c_1, a_2, b_2 und c_2 in $\mathbb{F}$ liegen. Wir subtrahieren die Gleichungen und erhalten

$$(a_1 - a_2)x + (b_1 - b_2)y + (c_1 - c_2) = 0.$$

Falls $a_1 = a_2$ und $b_1 = b_2$, so folgt $c_1 = c_2$, und die Kreise sind gleich, was ausgeschlossen war. Wir können also annehmen, dass $a_1 - a_2 \neq 0$ oder

$b_1 - b_2 \neq 0$ gilt. Wir suchen dann Punkte $(x, y) \in \mathbb{R}^2$, die sowohl die Gleichung $(a_1 - a_2)x + (b_1 - b_2)y + (c_1 - c_2) = 0$ als auch die Gleichung $x^2 + y^2 + a_2x + b_2y + c_2 = 0$ erfüllen. Das ist aber gerade die Situation, die wir in 2. diskutiert haben, und es folgt auch in diesem Fall, dass die Schnittpunkte (x, y) von K_1 und K_2 in der Ebene von $\mathbb{F}$ oder der Ebene einer reell-quadratischen Erweiterung von $\mathbb{F}$ liegen.

□

1.3.18 Proposition: Sei $a \in \mathbb{R}$ konstruierbar.

Dann gibt es einen reell-quadratischen Körperturm $\mathbb{Q} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_n$ mit $a \in \mathbb{F}_n$.

Beweis: Sei $a \in \mathbb{R}$ konstruierbar. Dann gibt es eine Strecke der Länge $|a|$, deren Randpunkte aus einer Strecke der Länge 1 mit Hilfe von endlich vielen Schritten mit Zirkel und Lineal konstruiert werden können. Seien $P_0, P_1, \ldots, P_r$ die Punkte, die bei dieser Konstruktion benötigt werden, aufgelistet in der Reihenfolge ihrer Konstruktion. Der erste Konstruktionsschritt ist vorgegeben: Wir zeichnen eine Strecke der Länge 1. Wir können annehmen, dass der Punkt P_0 im Koordinatenursprung liegt, also $P_0 = (0, 0)$, und dass $P_1 = (1, 0)$ ist. Die Punkte P_0 und P_1 liegen in der Ebene von $\mathbb{Q}$. Der Punkt P_r ist der letzte Punkt, der für die Konstruktion der Strecke der Länge $|a|$ verwendet wird. Für alle $0 \leq i \leq r$ bezeichne $\mathbb{F}_i$ den Körper, in dessen Ebene P_i liegt. Wir erhalten damit eine Folge

$$\mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_r$$

von Körpern in $\mathbb{R}$. Sei $1 < i < r$. Die Ebene von $\mathbb{F}_i$ enthält auch alle Punkte P_j mit $j \leq i$, und P_{i+1} entsteht als Schnittpunkt von Geraden beziehungsweise Geraden mit Kreisen beziehungsweise Kreisen in $\mathbb{F}_i$. Lemma 1.3.17 besagt, dass $\mathbb{F}_{i+1} = \mathbb{F}_i$ ist oder dass $\mathbb{F}_{i+1}$ eine reell-quadratische Erweiterung von $\mathbb{F}_i$ ist. Streichen wir nun in der Folge $\mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_r$ alle diejenigen $\mathbb{F}_i$ mit $\mathbb{F}_i = \mathbb{F}_{i+1}$, so erhalten wir einen reell-quadratischen Körperturm

$$\mathbb{Q} \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_s,$$

und die Punkte $P_0, \ldots, P_r$ liegen in der Ebene von $\mathbb{F}_s$. Im letzten Konstruktionsschritt zeichnen wir die Strecke der Länge $|a|$ zwischen einem Punkt P_k, $0 \leq k < r$ und P_r. Sei $P_k = (x, y)$ und $P_r = (c, d)$, wobei $x, y, c, d \in \mathbb{F}_s$ gilt. Dann ist $|a| = \sqrt{(x-c)^2 + (y-d)^2} \in \mathbb{F}_s(\sqrt{(x-c)^2 + (y-d)^2})$. Also liegt $|a|$ in $\mathbb{F}_s$ oder in einer reell-quadratischen Erweiterung von $\mathbb{F}_s$. In beiden Fällen erhalten wir, wie behauptet, einen reell-quadratischen Körperturm (mit $n = s$ oder $n = s + 1$). □

Das zentrale Ergebnis dieses Abschnitts, für das wir allerdings schon alle Vorarbeiten geleistet haben, ist:

1.3.19 Korollar: (Hauptsatz über konstruierbare Zahlen in $\mathbb{R}$)

Sei $a \in \mathbb{R}$. Die folgenden beiden Aussagen sind äquivalent:

1. a ist konstruierbar.

2. Es gibt einen reell-quadratischen Körperturm $\mathbb{Q} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_n$ mit $a \in \mathbb{F}_n$.

Beweis: Die Implikation 1. $\Rightarrow$ 2. ist Proposition 1.3.18, und die Implikation 2. $\Rightarrow$ 1. haben wir in 1.3.8 gezeigt. □

Der Hauptsatz über konstruierbare Zahlen ist eine rein algebraische Charakterisierung konstruierbarer Zahlen: Eine Zahl a ist genau dann konstruierbar, wenn sie in einem reell-quadratischen Körperturm liegt. Wenn wir also wissen, dass a diese Eigenschaft hat, dann ist gewährleistet, dass a konstruierbar ist; wie eine solche Konstruktion aussehen könnte, ist unklar – darüber macht der Satz keine Aussage. Man könnte meinen, dass der Hauptsatz das Problem nur verlagert und anders formuliert, jedoch nicht angreifbarer macht. Überraschenderweise ist dies nicht der Fall. Man kann den Hauptsatz nämlich auch anders lesen. Wenn wir beweisen können, dass eine Zahl a aus irgendeinem Grund nicht in einem reell-quadratischen Körperturm liegen kann, dann wissen wir, dass es keine wie auch immer geartete Konstruktion von a mit Zirkel und Lineal geben kann. Dieser Schritt fehlte den Griechen für eine Lösung der klassischen Konstruktionsprobleme.

1.4 Die Lösung der klassischen Konstruktionsprobleme

Im 19. Jahrhundert, also mehr als 2000 Jahre nach ihrer Formulierung, wurden die klassischen Konstruktionsprobleme gelöst. Mit Hilfe der im letzten Abschnitt entwickelten Methoden wurde gezeigt, dass diese Konstruktionen mit Zirkel und Lineal nicht möglich sind.

1.4.1 Das Deli'sche Problem

Wir haben in Abschnitt 1.2.1 bereits gesehen, dass das Deli'sche Problem sich auf die Frage reduzieren lässt, ob $\sqrt[3]{2}$ konstruierbar ist. Wir werden in diesem Abschnitt zeigen, dass dies nicht der Fall ist. Wir beginnen mit einem Lemma.

1.4.1 Lemma: Sei $\mathbb{F}$ ein Unterkörper von $\mathbb{R}$. Sei $\mathbb{F}(\sqrt{k})$ eine reell-quadratische Erweiterung von $\mathbb{F}$.

Wenn $\sqrt[3]{2}$ in $\mathbb{F}(\sqrt{k})$ liegt, dann liegt $\sqrt[3]{2}$ schon in $\mathbb{F}$.

Beweis: Sei $\sqrt[3]{2} \in \mathbb{F}(\sqrt{k})$. Dann gibt es $a, b \in \mathbb{F}$ mit

$$a + b\sqrt{k} = \sqrt[3]{2}.$$

Die Behauptung des Lemmas ist, dass $b = 0$ ist. Es gilt

$$2 = (a + b\sqrt{k})^3 = (a^3 + 3ab^2k) + (3a^2b + b^3k)\sqrt{k}.$$

Wäre $3a^2b + b^3k \neq 0$, so könnten wir diese Gleichung nach $\sqrt{k}$ umformen, und es würde folgen, dass $\sqrt{k}$ in $\mathbb{F}$ liegt. Nach Annahme ist dies nicht der Fall, denn $\mathbb{F}(\sqrt{k})$ ist eine reell-quadratische Erweiterung von $\mathbb{F}$. Es folgt, dass $3a^2b + b^3k = b(3a^2 + b^2k) = 0$ ist. Wegen $k > 0$ folgt daraus $b = 0$. □

1.4.2 Satz: Die Verdoppelung des Würfels ist mit Zirkel und Lineal nicht möglich.

Beweis: Angenommen, die Verdoppelung des Würfels mit Zirkel und Lineal wäre möglich. Dann ist $\sqrt[3]{2}$ konstruierbar. Der Hauptsatz über konstruierbare Zahlen besagt, dass es einen reell-quadratischen Körperturm

$$\mathbb{Q} \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_n$$

so gibt, dass $\sqrt[3]{2} \in \mathbb{F}_n$ gilt. Wenden wir Lemma 1.4.1 auf $\mathbb{F}_n$ an, so erhalten wir $\sqrt[3]{2} \in \mathbb{F}_{n-1}$, und wiederholtes Anwenden des Lemmas liefert $\sqrt[3]{2} \in \mathbb{Q}$. Proposition 1.1.18 besagt, dass $\sqrt[3]{2}$ in $\mathbb{N}$ liegt, ein Widerspruch, denn $1 < \sqrt[3]{2} < 2$. Dieser Widerspruch zeigt, dass unsere Annahme, die Verdoppelung des Würfels mit Zirkel und Lineal wäre möglich, falsch gewesen ist. □

1.4.3 Aufgabe: Ist die Verdreifachung des Würfels mit Zirkel und Lineal möglich?

1.4.2 Die Quadratur des Kreises

Wie wir in Abschnitt 1.2.2 gezeigt haben, reduziert sich das Problem der Quadratur des Kreises auf das Problem, ob $\sqrt{\pi}$ konstruierbar ist. Dieses Problem ist deutlich schwerer als die beiden anderen klassischen Probleme, und es wurde auch erst 1882 durch einen Satz des deutschen Mathematikers Ferdinand von Lindemann bewiesen. Sie sehen hier den Grabstein des Ehepaares Lisbeth und Ferdinand von Lindemann, auf dem zur Erinnerung an Lindemanns Beitrag zur Lösung des Quadraturproblems ein Kreis, ein Quadrat und π zu finden ist.

Der Satz von Lindemann ist ein Satz über Nullstellen von Polynomen.

1.4.4 Satz: (Satz von Lindemann)

Es gibt kein Polynom vom Grad ≥ 0 in $\mathbb{Q}[T]$, das π als Nullstelle besitzt.

Als Abfallprodukt des Satzes von Lindemann halten wir noch ganz schnell fest:

1.4.5 Korollar: Die Kreiszahl π ist keine rationale Zahl.

Beweis: Wäre π rational, so wäre $T - \pi$ ein Polynom in $\mathbb{Q}[T]$, das π als Nullstelle enthält. Das ist aber ein Widerspruch zum Satz von Lindemann. □

Der Beweis des Satzes von Lindemann ist trickreich, und wir werden ihn in diesem Kurs zum Glauben lassen.

Wie nun der Satz von Lindemann in die Lösung des Quadraturproblems eingeht, werden wir jetzt zeigen. Wir beginnen mit einem Lemma.

1.4.6 Lemma: Sei $\mathbb{F}$ ein Unterkörper von $\mathbb{R}$, und sei $\mathbb{F}(\sqrt{k})$ eine reell-quadratische Erweiterung von $\mathbb{F}$. Sei c eine Nullstelle eines Polynoms p in $\mathbb{F}(\sqrt{k})[T]$ vom Grad n.

Dann ist c Nullstelle eines Polynoms vom Grad $2n$ in $\mathbb{F}[T]$.

Beweis: Sei c Nullstelle des Polynoms

$$p = (a_0 + b_0\sqrt{k}) + (a_1 + b_1\sqrt{k})T + \cdots + (a_{n-1} + b_{n-1}\sqrt{k})T^{n-1} + (a_n + b_n\sqrt{k})T^n$$

mit $a_i, b_i \in \mathbb{F}$ für alle $0 \leq i \leq n$, und a_n und b_n sind nicht beide 0. Dann gilt

$$(a_0 + b_0\sqrt{k}) + (a_1 + b_1\sqrt{k})c + \cdots + (a_{n-1} + b_{n-1}\sqrt{k})c^{n-1} + (a_n + b_n\sqrt{k})c^n = 0.$$

Ausmultiplizieren und Umsortieren liefert

$$a_0 + a_1c + \cdots + a_{n-1}c^{n-1} + a_nc^n = -\sqrt{k}(b_0 + b_1c + \cdots + b_{n-1}c^{n-1} + b_nc^n).$$

Wir quadrieren beide Seiten und erhalten

$$a_0^2 + \tilde{a}_1c + \cdots + \tilde{a}_{2n-1}c^{2n-1} + a_n^2c^{2n} = k(b_0^2 + \tilde{b}_1c + \cdots + \tilde{b}_{2n-1}c^{2n-1} + b_n^2c^{2n}).$$

Wie die Koeffizienten $\tilde{a}_i$ und $\tilde{b}_i$, $1 \leq i \leq 2n-1$, genau aussehen, interessiert uns nicht. Wichtig ist nur, dass sie in $\mathbb{F}$ liegen. Es folgt

$$(a_0^2 - b_0^2k) + (\tilde{a}_1 - \tilde{b}_1k)c + \cdots + (\tilde{a}_{2n-1} - \tilde{b}_{2n-1}k)c^{2n-1} + (a_n^2 - b_n^2k)c^{2n} = 0.$$

Somit ist c Nullstelle von

$$q = (a_0^2 - b_0^2k) + (\tilde{a}_1 - \tilde{b}_1k)T + \cdots + (\tilde{a}_{2n-1} - \tilde{b}_{2n-1}k)T^{2n-1} + (a_n^2 - b_n^2k)T^{2n}.$$

Es bleibt zu zeigen, dass q den Grad $2n$ hat. Wäre $a_n^2 - b_n^2k = 0$, so würde $a_n^2 = b_n^2k$, also $a_n = \pm b_n\sqrt{k}$ folgen. Das ist aber ein Widerspruch, denn $a_n \in \mathbb{F}$ und $b_n\sqrt{k} \notin \mathbb{F}$. Somit ist q ein Polynom in $\mathbb{F}[T]$ vom Grad $2n$, das c als Nullstelle besitzt. □

1.4.7 Proposition: Sei c eine konstruierbare Zahl. Dann ist c Nullstelle eines Polynoms in $\mathbb{Q}[T]$.

Beweis: Sei c konstruierbar. Der Hauptsatz über konstruierbare Zahlen, Korollar 1.3.19, besagt, dass es einen reell-quadratischen Körperturm $\mathbb{Q} = \mathbb{F}_0 \subseteq \cdots \subseteq \mathbb{F}_n$ gibt, sodass $c \in \mathbb{F}_n$ gilt. Das Element c ist Nullstelle des Polynoms $T - c \in \mathbb{F}_n[T]$. Lemma 1.4.6 besagt, dass c Nullstelle eines Polynoms vom Grad 2 in $\mathbb{F}_{n-1}[T]$ ist. Wiederholtes Anwenden des Lemmas liefert, dass c Nullstelle eines Polynoms vom Grad 2^n in $\mathbb{Q}[T]$ ist. □

1.4.8 Aufgabe: Geben Sie ein Beispiel dafür, dass die Umkehrung von Proposition 1.4.7 im Allgemeinen falsch ist.

Kombinieren wir jetzt Proposition 1.4.7 und den Satz von Lindemann, so erhalten wir:

1.4.9 Korollar: Die Quadratur des Kreises ist unmöglich.

Beweis: Angenommen, sie wäre möglich. Dann ist $\sqrt{\pi}$ konstruierbar, also ist auch $\pi = \sqrt{\pi}\sqrt{\pi}$ konstruierbar. Proposition 1.4.7 besagt, dass π Nullstelle eines Polynoms in $\mathbb{Q}[T]$ ist, ein Widerspruch zum Satz von Lindemann. □

1.4.10 Aufgabe: Nehmen wir an, die „Kubatur der Kugel“ wäre das Problem, mit Zirkel und Lineal einen Würfel zu konstruieren, dessen Volumen dem einer vorgegebenen Kugel entspricht. Ist die Kubatur der Kugel möglich?

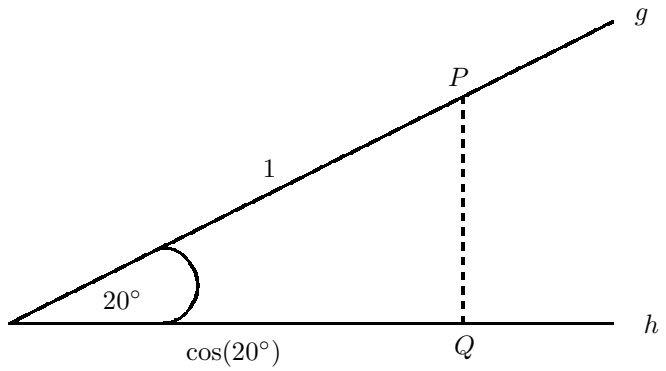
1.4.3 Die Dreiteilung beliebiger Winkel

Wir werden in diesem Abschnitt zeigen, dass die Dreiteilung beliebiger Winkel mit Zirkel und Lineal nicht möglich ist. Dazu müssen wir zeigen, dass es mindestens einen Winkel α gibt, der nicht gedrittelt werden kann. Wir werden dies für den Winkel $\alpha = 60°$ machen. Der Beweis zerfällt in mehrere Schritte, wobei Sie den ersten selbst machen müssen:

1.4.11 Aufgabe: Beweisen Sie, dass ein Winkel von 60° mit Zirkel und Lineal konstruierbar ist.

1.4.12 Bemerkung: Wenn ein 60°-Winkel mit Zirkel und Lineal dreiteilbar ist, dann ist $\cos(20°)$ eine konstruierbare Zahl.

Beweis: Laut Aufgabe 1.4.11 ist ein Winkel von 60° konstruierbar. Könnten wir 60° dreiteilen, so wäre ein Winkel von 20° konstruierbar. Sei O der Scheitel dieses Winkels, der durch die Strahlen g und h eingeschlossen wird. Wir schlagen um O einen Kreis vom Radius 1. Dieser schneidet g im Punkt P. Jetzt fällen wir das Lot von P auf h. Dieses schneidet h im Punkt Q. Die Strecke $\overline{OQ}$ hat die Länge $\cos(20°)$ (vergleiche Skizze).



□

1.4.13 Lemma: Wenn $\cos(20°)$ konstruierbar ist, dann ist eine Nullstelle des Polynoms $p = T^3 - 3T - 1$ konstruierbar.

Beweis: Wir verwenden die Additionstheoreme der Winkelfunktionen. Es gilt

$$\begin{aligned} \cos(\alpha+\beta) &= \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta), \\ \sin(\alpha+\beta) &= \cos(\alpha)\sin(\beta) + \sin(\alpha)\cos(\beta) \end{aligned}$$

und $(\sin(\alpha))^2 + (\cos(\alpha))^2 = 1$ und $\cos(60°) = \frac{1}{2}$.

Sei $\gamma = 20°$. Dann gilt

$$\begin{aligned} \tfrac{1}{2} &= \cos(3\gamma) = \cos(2\gamma+\gamma) = \cos(2\gamma)\cos(\gamma) - \sin(2\gamma)\sin(\gamma) \\ &= \cos(\gamma+\gamma)\cos(\gamma) - \sin(\gamma+\gamma)\sin(\gamma) = (\cos(\gamma))^3 - 3(\sin(\gamma))^2\cos(\gamma) \\ &= (\cos(\gamma))^3 - 3(1-(\cos(\gamma))^2)\cos(\gamma) = 4(\cos(\gamma))^3 - 3\cos(\gamma). \end{aligned}$$

Es folgt $4(\cos(\gamma))^3 - 3\cos(\gamma) - \frac{1}{2} = 0$, also $8(\cos(\gamma))^3 - 6\cos(\gamma) - 1 = 0$ und damit

$$(2\cos(\gamma))^3 - 3(2\cos(\gamma)) - 1 = 0.$$

Somit ist $2\cos(\gamma)$ eine Nullstelle von $p = T^3 - 3T - 1$. Da wir annehmen, dass $\cos(\gamma)$ konstruierbar ist, folgt, dass $2\cos(\gamma)$ konstruierbar ist. Somit ist eine Nullstelle des Polynoms $p = T^3 - 3T - 1$ konstruierbar. □

1.4.14 Lemma: Sei $\mathbb{F}$ ein Unterkörper von $\mathbb{R}$, und sei $\mathbb{F}(\sqrt{k})$ eine reell-quadratische Erweiterung von $\mathbb{F}$. Sei c eine Nullstelle von $p = T^3 - 3T - 1$.

Wenn c in $\mathbb{F}(\sqrt{k})$ liegt, dann gibt es eine Nullstelle c' von p in $\mathbb{F}$.

Beweis: Sei $c \in \mathbb{F}(\sqrt{k})$. Dann gibt es $a, b \in \mathbb{F}$ mit $c = a + b\sqrt{k}$. Wenn $b = 0$ ist, dann liegt schon c in $\mathbb{F}$, und wir sind fertig. Wir können also annehmen, dass $b \neq 0$ ist. Nach Annahme gilt

$$(a + b\sqrt{k})^3 - 3(a + b\sqrt{k}) - 1 = 0.$$

Ausmultiplizieren liefert

$$(a^3 + 3ab^2k - 3a - 1) + (3a^2b + b^3k - 3b)\sqrt{k} = 0.$$

Wäre $3a^2b + b^3k - 3b \neq 0$, so könnten wir nach $\sqrt{k}$ auflösen und erhielten $\sqrt{k} \in \mathbb{F}$, ein Widerspruch. Es gilt also $3a^2b + b^3k - 3b = 0$, und damit

$$3a^2 + b^2k - 3 = 0 \text{ und } a^3 + 3ab^2k - 3a - 1 = 0.$$

Wir formen die erste Gleichung nach b^2k um und setzen in die zweite ein. Das ergibt

$$a^3 + 3a(3 - 3a^2) - 3a - 1 = 0, \text{ also } -8a^3 + 6a - 1 = 0, \text{ also } (-2a)^3 - 3(-2a) - 1 = 0.$$

Somit ist $-2a$ eine Nullstelle von p, und es ist $-2a \in \mathbb{F}$. □

1.4.15 Lemma: Sei c eine Nullstelle des Polynoms $T^3 - 3T - 1$. Dann gilt $c \notin \mathbb{Q}$.

Beweis: Angenommen, es gibt $a, b \in \mathbb{Z}$ mit $b \neq 0$, sodass $c = \frac{a}{b}$ eine Nullstelle von p ist. Da 0 keine Nullstelle von $T^3 - 3T - 1$ ist, gilt $a \neq 0$. Wir wollen ferner annehmen, dass a und b ausgekürzt sind. Dann gilt

$$\frac{a^3}{b^3} - \frac{3a}{b} - 1 = 0, \text{ also } a^3 - 3ab^2 - b^3 = 0.$$

Umformen nach a^3 beziehungsweise b^3 liefert

$$a^3 = b(3ab + b^2) \text{ und } b^3 = a(a^2 - 3b^2).$$

Aus der ersten dieser Gleichungen folgt: Wenn es eine Primzahl q gibt, die b teilt, so teilt q auch a^3 und damit auch a. Da a und b keine gemeinsamen Teiler außer 1 und -1 haben, folgt, dass b nicht von einer Primzahl geteilt wird, also $b = 1$ oder $b = -1$ sein muss. Analog folgt aus der zweiten Gleichung, dass $a = 1$ oder $a = -1$ sein muss. Damit ist $\frac{a}{b} = 1$ oder $\frac{a}{b} = -1$. Das ist ein Widerspruch, denn weder 1 noch -1 ist Nullstelle von $T^3 - 3T - 1$. □

Jetzt haben wir aber alle Puzzleteile zusammen, um die Unmöglichkeit des Winkeldreiteilungsproblems zu beweisen.

1.4.16 Satz: Die Dreiteilung eines 60°-Winkels ist mit Zirkel und Lineal nicht möglich.

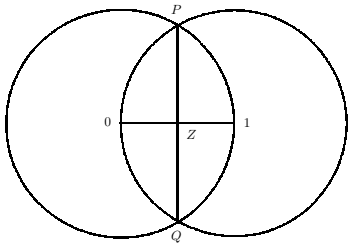
Beweis: Angenommen, eine solche Konstruktion wäre möglich. Aus Bemerkung 1.4.12 und Lemma 1.4.13 folgt, dass eine Nullstelle c von $p = T^3 - 3T - 1$ konstruierbar ist. Der Hauptsatz über konstruierbare Zahlen besagt, dass es einen reell-quadratischen Körperturm $\mathbb{Q} = \mathbb{F}_0 \subseteq \cdots \subseteq \mathbb{F}_n$ gibt, sodass $c \in \mathbb{F}_n$ gilt. Wenden wir Lemma 1.4.14 wiederholt an, so folgt, dass es eine Nullstelle $\tilde{c}$ von $T^3 - 3T - 1$ in $\mathbb{Q}$ gibt. Dies widerspricht aber Lemma 1.4.15. □

Lösungen der Aufgaben

Lösungen der Aufgaben in 1.1

Aufgabe 1.1.5

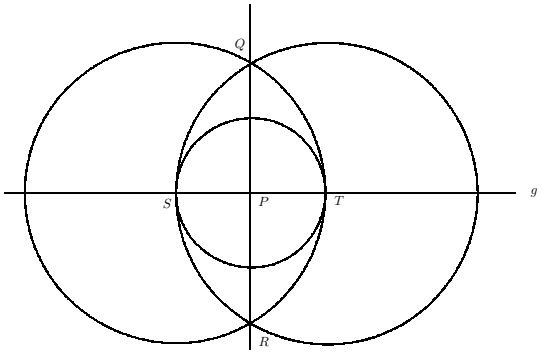
Wir zeichnen eine Strecke der Länge 1, deren Randpunkte wir 0 und 1 nennen. Jetzt nehmen wir die Länge 1 in unseren Zirkel und schlagen um 0 und 1 Kreise mit Radius 1. Diese Kreise schneiden sich in P und Q. Wir verbinden P und Q. Die Strecke $\overline{PQ}$ schneidet die Strecke zwischen 0 und 1 in Z, und Z ist der Mittelpunkt der Strecke $\overline{01}$.



Es folgt, dass die Strecke $\overline{0Z}$ die Länge $\frac{1}{2}$ hat. Somit ist $\frac{1}{2}$ konstruierbar.

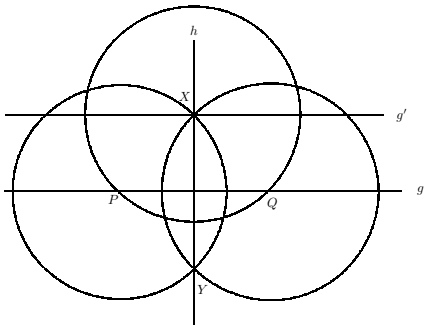
Aufgabe 1.1.9

Gegeben sind g und P. Wir schlagen um P einen Kreis mit Radius 1. Dieser schneidet g in S und T. Jetzt schlagen wir um S und um T jeweils einen Kreis vom Radius $\overline{ST}$. Die Kreise schneiden sich in Q und R. Die Gerade durch Q und R ist die Senkrechte zu g durch P.



Aufgabe 1.1.10

Gegeben sind g und X. Wir schlagen um X einen Kreis mit einem Radius $n \in \mathbb{N}$, sodass der Kreis die Gerade g in zwei Punkten P und Q schneidet. Wir schlagen um P und um Q Kreise mit dem Radius der Länge n. Die Kreise schneiden sich in X und Y. Wir ziehen die Gerade h durch X und Y. Diese Gerade ist senkrecht zu g. Jetzt errichten wir wie in Aufgabe 1.1.9 in X die Senkrechte g' zu h. Diese Senkrechte ist parallel zu g.



Aufgabe 1.1.17 Es gilt

$$
\begin{array}{lcl}
7 \text{ ist konstruierbar} & \Rightarrow & \sqrt{7} \text{ ist konstruierbar} \\
2 \text{ ist konstruierbar} & \Rightarrow & 2\sqrt{7} \text{ ist konstruierbar} \\
1 \text{ ist konstruierbar} & \Rightarrow & 1+2\sqrt{7} \text{ ist konstruierbar} \\
 & \Rightarrow & \sqrt{1+2\sqrt{7}} \text{ ist konstruierbar} \\
6 \text{ ist konstruierbar} & \Rightarrow & \sqrt{6} \text{ ist konstruierbar} \\
 & \Rightarrow & \sqrt{6}+\sqrt{1+2\sqrt{7}} \text{ ist konstruierbar} \\
 & \Rightarrow & \sqrt{\sqrt{6}+\sqrt{1+2\sqrt{7}}} \text{ ist konstruierbar} \\
\frac{4}{3} \text{ ist konstruierbar} & \Rightarrow & \frac{4}{3}\sqrt{\sqrt{6}+\sqrt{1+2\sqrt{7}}} \text{ ist konstruierbar.}
\end{array}
$$

Lösung der Aufgabe in 1.2

Aufgabe 1.2.1

Da a und 1 konstruierbar sind, ist $\frac{1}{a}$ konstruierbar. Da $a\sqrt{b}$ und $\frac{1}{a}$ konstruierbar sind, ist $\frac{1}{a}a\sqrt{b} = \sqrt{b}$ konstruierbar.

Lösungen der Aufgaben in 1.3

Aufgabe 1.3.4

Wir beweisen zunächst mit Induktion nach n, dass jede natürliche Zahl n in $\mathbb{F}$ liegt.

Im Induktionsanfang sei $n_0 = 1$. Da $\mathbb{F}$ ein Unterkörper von $\mathbb{C}$ ist, liegt 1 in $\mathbb{F}$, und es gilt der Induktionsanfang.

Sei nun $n \geq 1$, und sei $n \in \mathbb{F}$. Da n und 1 in $\mathbb{F}$ liegen, folgt, dass $n+1$ in $\mathbb{F}$ liegt. Mit dem Prinzip der vollständigen Induktion folgt, dass alle natürlichen Zahlen in $\mathbb{F}$ liegen, also $\mathbb{N} \subseteq \mathbb{F}$.

Wir wissen bereits, dass $0 = 1-1$ in $\mathbb{F}$ liegt. Es bleibt zu zeigen, dass alle negativen Zahlen in $\mathbb{F}$ liegen. Dazu sei $n \in \mathbb{N}$. Da $\mathbb{F}$ ein Körper ist, liegt $0 - n = -n$ in $\mathbb{F}$. Es folgt $\mathbb{Z} \subseteq \mathbb{F}$.

Sei $\frac{a}{b}$ mit $a \in \mathbb{Z}$ und $b \in \mathbb{Z}$, $b \neq 0$. Da a und b in $\mathbb{F}$ liegen, liegt auch $\frac{a}{b}$ in $\mathbb{F}$, und es folgt, dass $\mathbb{Q} \subseteq \mathbb{F}$ gilt. Somit sind die rationalen Zahlen in jedem Unterkörper von $\mathbb{C}$ enthalten.

Aufgabe 1.3.6

1. Es gilt

$$\begin{aligned}(2+8\sqrt{3})(1-6\sqrt{3}) &= 2-12\sqrt{3}+8\sqrt{3}-48\cdot 3 = 2-144+(8-12)\sqrt{3}\\ &= -142+(-4)\sqrt{3} = -142-4\sqrt{3}.\end{aligned}$$

2. Es gilt

$$\begin{aligned}\tfrac{1}{8-4\sqrt{3}} &= \tfrac{8+4\sqrt{3}}{(8-4\sqrt{3})(8+4\sqrt{3})} = \tfrac{8+4\sqrt{3}}{64-16\cdot 3} = \tfrac{8+4\sqrt{3}}{16}\\ &= \tfrac{1}{2}+\tfrac{1}{4}\sqrt{3}.\end{aligned}$$

3. Es gilt
$$\begin{aligned}\frac{4+3\sqrt{3}}{6-5\sqrt{3}} &= \frac{(4+3\sqrt{3})(6+5\sqrt{3})}{(6-5\sqrt{3})(6+5\sqrt{3})} = \frac{24+20\sqrt{3}+18\sqrt{3}+15\cdot 3}{36-25\cdot 3} \\ &= -\frac{23}{13} - \frac{38}{39}\sqrt{3}.\end{aligned}$$

Aufgabe 1.3.10

Sei $a+b\sqrt{k'} \in (\mathbb{F}(\sqrt{k}))(\sqrt{k'})$, wobei $a, b \in \mathbb{F}(\sqrt{k})$ gilt. Dann gibt es $x, y, x', y' \in \mathbb{F}$ mit $a = x + y\sqrt{k}$ und $b = x' + y'\sqrt{k}$. Es folgt
$$\begin{aligned}a + b\sqrt{k'} &= x + y\sqrt{k} + (x' + y'\sqrt{k})\sqrt{k'} = x + y\sqrt{k} + x'\sqrt{k'} + y'\sqrt{k}\sqrt{k'} \\ &= \underbrace{x + x'\sqrt{k'}}_{\in\mathbb{F}(\sqrt{k'})} + \underbrace{(y + y'\sqrt{k'})}_{\in\mathbb{F}(\sqrt{k'})}\sqrt{k}.\end{aligned}$$

Es folgt $a+b\sqrt{k'} \in (\mathbb{F}(\sqrt{k'}))(\sqrt{k})$, und damit $(\mathbb{F}(\sqrt{k}))(\sqrt{k'}) \subseteq (\mathbb{F}(\sqrt{k'}))(\sqrt{k})$, denn jedes Element der linken Menge liegt auch in der rechten.

Jetzt machen wir das umgekehrt und beginnen mit $a+b\sqrt{k} \in (\mathbb{F}(\sqrt{k'}))(\sqrt{k})$, wobei $a, b \in \mathbb{F}(\sqrt{k'})$ gilt. Dann gibt es $x, y, x', y' \in \mathbb{F}$ mit $a = x+y\sqrt{k'}$ und $b = x'+y'\sqrt{k'}$. Es folgt
$$\begin{aligned}a + b\sqrt{k} &= x + y\sqrt{k'} + (x' + y'\sqrt{k'})\sqrt{k} = x + y\sqrt{k'} + x'\sqrt{k} + y'\sqrt{k'}\sqrt{k} \\ &= \underbrace{x + x'\sqrt{k}}_{\in\mathbb{F}(\sqrt{k})} + \underbrace{(y + y'\sqrt{k})}_{\in\mathbb{F}(\sqrt{k})}\sqrt{k'}.\end{aligned}$$

Somit gilt $a+b\sqrt{k} \in (\mathbb{F}(\sqrt{k}))(\sqrt{k'})$, und damit $(\mathbb{F}(\sqrt{k'}))(\sqrt{k}) \subseteq (\mathbb{F}(\sqrt{k}))(\sqrt{k'})$. Es folgt $(\mathbb{F}(\sqrt{k'}))(\sqrt{k}) = (\mathbb{F}(\sqrt{k}))(\sqrt{k'})$, die Behauptung.

Aufgabe 1.3.11

1. Es ist $4 + 8\sqrt{12} = 4 + 8\sqrt{4\cdot 3} = 4 + 16\sqrt{3} \in \mathbb{Q}(\sqrt{3})$. Weiter gilt $\mathbb{Q}(\sqrt{3}) \subseteq ((\mathbb{Q}(\sqrt{3}))(\sqrt{2}))(\sqrt{5}) = ((\mathbb{Q}(\sqrt{2}))(\sqrt{3}))(\sqrt{5})$, also $4+8\sqrt{12} \in ((\mathbb{Q}(\sqrt{2}))(\sqrt{3}))(\sqrt{5})$.
2. Es ist
$$\sqrt{6} + 3\sqrt{15} = \underbrace{\sqrt{2}\sqrt{3}}_{\in(\mathbb{Q}(\sqrt{2}))(\sqrt{3})} + \underbrace{3\sqrt{3}}_{\in(\mathbb{Q}(\sqrt{2}))(\sqrt{3})}\sqrt{5},$$
also $\sqrt{6} + 3\sqrt{15} \in ((\mathbb{Q}(\sqrt{2}))(\sqrt{3}))(\sqrt{5})$.
3. Es ist $\sqrt{10}+\sqrt{30} = \underbrace{(\sqrt{2} + \sqrt{2}\sqrt{3})}_{\in(\mathbb{Q}(\sqrt{2}))(\sqrt{3})}\sqrt{5}$, also $\sqrt{10}+\sqrt{30} \in ((\mathbb{Q}(\sqrt{2}))(\sqrt{3}))(\sqrt{5})$.

Aufgabe 1.3.12

Sei $P = (a, b)$ konstruierbar. Wir fällen von P das Lot auf die x-Achse und auf die y-Achse (diese Konstruktionen sind mit Zirkel und Lineal durchführbar). Dies liefert die Punkte $(a, 0)$ und $(0, b)$. Die Strecken zwischen dem Koordinatenursprung $(0, 0)$ und $(0, a)$ und zwischen $(0, 0)$ und $(0, b)$ sind $|a|$ beziehungsweise $|b|$. Somit sind a und b konstruierbar.

Seien umgekehrt a und b konstruierbar. Wir schlagen um den Koordinatenursprung $(0, 0)$ einen Kreis vom Radius $|a|$. Dieser schneidet die x-Achse in $(|a|, 0)$ und $(-|a|, 0)$. Analog schlagen wir um $(0, 0)$ einen Kreis vom Radius $|b|$. Dieser schneidet die y-Achse in $(0, |b|)$ und $(0, -|b|)$. Jetzt errichten wir in $(a, 0)$ und $(0, b)$ die Senkrechten zur x- beziehungsweise y-Achse. Diese Senkrechten schneiden sich in $P = (a, b)$. Somit ist P mit Zirkel und Lineal konstruierbar.

Lösungen der Aufgaben in 1.4

Aufgabe 1.4.3

Nein, die Verdreifachung des Würfels ist mit Zirkel und Lineal nicht möglich, wie wir jetzt zeigen werden.

Angenommen, sie wäre möglich. Wie bei der Verdoppelung des Würfels hätte dies die Konstruierbarkeit von $\sqrt[3]{3}$ zur Folge.

Wir zeigen zunächst: Wenn $\sqrt[3]{3} \in \mathbb{F}(\sqrt{k})$ für einen Unterkörper $\mathbb{F}$ von $\mathbb{R}$, ein $k \in \mathbb{F}$ und $\sqrt{k} \notin \mathbb{F}$, so liegt $\sqrt[3]{3}$ schon in $\mathbb{F}$. Sei also $\sqrt[3]{3} \in \mathbb{F}(\sqrt{k})$. Dann gibt es $a, b \in \mathbb{F}$ mit $\sqrt[3]{3} = a + b\sqrt{k}$. Es ist

$$3 = (a + b\sqrt{k})^3 = (a^3 + 3ab^2k) + (3a^2b + b^3k)\sqrt{k}.$$

Wäre $3a^2b + b^3k \neq 0$, so könnten wir nach $\sqrt{k}$ auflösen und erhielten $\sqrt{k} \in \mathbb{F}$, ein Widerspruch. Es ist also $3a^2b + b^3k = 0$, und wir erhalten $b(3a^2 + b^2k) = 0$. Wegen $k > 0$ ist somit $b = 0$, also $\sqrt[3]{3} \in \mathbb{F}$.

Da wir annehmen, dass $\sqrt[3]{3}$ konstruierbar ist, gibt es einen reell-quadratischen Körperturm $\mathbb{Q} \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_n$ mit $\sqrt[3]{3} \in \mathbb{F}_n$. Wie wir gerade überlegt haben, folgt daraus induktiv, dass $\sqrt[3]{3}$ in $\mathbb{Q}$ liegt. Das ist aber nach 1.1.18 ein Widerspruch, denn $\sqrt[3]{3}$ ist keine natürliche Zahl. Dieser Widerspruch zeigt, dass $\sqrt[3]{3}$ nicht konstruierbar ist.

Aufgabe 1.4.8

Die Zahl $\sqrt[3]{2}$ ist nicht konstruierbar, denn sonst wäre die Würfelverdoppelung möglich. Aber $\sqrt[3]{2}$ ist Nullstelle von $T^3 - 2 \in \mathbb{Q}[T]$.

Aufgabe 1.4.10

Nein, die Kubatur des Würfels ist nicht möglich. Das Volumen einer Kugel beträgt $\frac{4}{3}\pi r^3$, wobei r der Radius ist. Wir können annehmen, dass r konstruierbar ist. Das Volumen eines Würfels ist a^3, wobei a die Seitenlänge ist. Wäre die Kubatur des Würfels möglich, so müssten wir eine Strecke der Länge $a = r\sqrt[3]{\frac{4}{3}\pi}$ konstruieren. Dann wäre auch $\sqrt[3]{\frac{4}{3}\pi}$ konstruierbar, also auch $\sqrt[3]{\frac{4}{3}\pi} \cdot \sqrt[3]{\frac{4}{3}\pi} \cdot \sqrt[3]{\frac{4}{3}\pi} = \frac{4}{3}\pi$. Es folgt, dass π konstruierbar ist, und das ist ein Widerspruch zum Satz von Lindemann.

Aufgabe 1.4.11

Es reicht, ein gleichseitiges Dreieck zu konstruieren. In ihm sind alle Winkel gleich groß, und da die Winkelsumme 180° beträgt, ist jeder der Winkel ein 60°-Winkel. Diese Konstruktion lässt sich wie folgt durchführen. Wir haben eine Strecke der Länge 1 gegeben, deren Endpunkte wir O und P nennen. Wir schlagen um O und P Kreise vom Radius 1. Diese Kreise schneiden sich in den Punkten Z und Z'. Das Dreieck mit den Eckpunkten O, P und Z ist gleichseitig.