1. Körper und Körpererweiterungen

Wir beginnen nun mit dem eigentlichen Studium von Gruppen, Ringen und Körpern. Die in der Einleitung vorgestellten Probleme haben dabei zunächst einmal hauptsächlich mit Körpern (und dabei insbesondere mit dem Körper der komplexen Zahlen) zu tun. Auch die geometrisch erscheinenden Fragestellungen zu Konstruktionen mit Zirkel und Lineal aus Problem 0.3 werden wir in Satz 1.12 über gewisse Unterkörper von $\mathbb{C}$ in die Sprache der Algebra übersetzen. Im Gegensatz zu den „Algebraischen Strukturen“, wo wir zunächst Gruppen und später dann Ringe und Körper untersucht haben, wollen wir daher hier den umgekehrten Weg gehen, zuerst Körper studieren und uns erst später genauer mit Gruppen beschäftigen.

Aus den „Algebraischen Strukturen“ wisst ihr sicher noch, was ein Körper ist: eine Menge K mit zwei Verknüpfungen „$+$“ und „$\cdot$“, so dass $(K,+)$ eine abelsche Gruppe (mit neutralem Element $0 = 0_K$) ist, $(K\backslash\{0\},\cdot)$ ebenfalls eine abelsche Gruppe (mit neutralem Element $1 = 1_K$) ist, und das Distributivgesetz gilt [G, Definition 7.6 (b) und Bemerkung 7.7 (b)]. Wir wollen hier nun den in der Praxis besonders wichtigen Fall untersuchen, dass zwei solche Körper ineinander liegen.

Definition 1.1 (Körpererweiterungen)**.** Sind K und L zwei Körper mit $K \subset L$, so heißt K **Teilkörper** bzw. **Unterkörper** von L, und L **Erweiterungskörper** von K. Wir schreiben dies auch als $K \leq L$ oder L/K und sagen, L/K (gesprochen: „L über K“) ist eine **Körpererweiterung**. Im Fall $K \leq Z \leq L$ nennt man Z einen **Zwischenkörper** der Körpererweiterung L/K.

Beachte also, dass L/K für zwei Körper K und L *keine mathematische Konstruktion* wie etwa einen Faktorring bezeichnet, sondern nur eine andere (und letztlich historisch bedingte) Schreibweise für die Relation $K \subset L$ ist.

Beispiel 1.2.

(a) Natürlich gilt $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

(b) Für jede Primzahl p wissen wir, dass $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ (mit den von $\mathbb{Z}$ induzierten Operationen) ein Körper mit p Elementen ist [G, Satz 7.10]. Diese Körper sind keine Teilkörper von $\mathbb{R}$.

(c) Die Menge der reellen *rationalen Funktionen*

$$\mathbb{R}(t) := \left\{ t \mapsto \frac{f}{g} : \ f,g \in \mathbb{R}[t] \text{ mit } g \neq 0 \right\}$$

ist ein Körper, der $\mathbb{R}$ (als konstante Funktionen) als Unterkörper enthält. Analog kann man $\mathbb{Q}(t)$ und $\mathbb{C}(t)$ als die Körper rationaler oder komplexer rationaler Funktionen definieren.

Bemerkung 1.3.

(a) Ist L ein Körper und $K \subset L$ eine Teilmenge von L, so ist K offensichtlich genau dann ein Unterkörper von L, wenn gilt

- $0,1 \in K$, und
- für alle $x,y \in K$ liegen auch $x+y$, $-x$, $x \cdot y$ und (für $x \neq 0$) x^{-1} in K (d. h. K ist abgeschlossen bezüglich der Körperoperationen).

Dies beweist man genauso wie das Untergruppen- oder Unterringkriterium in den „Algebraischen Strukturen“ [G, Satz 3.3 und 7.23].

(b) Ist $f : K \to L$ ein beliebiger Morphismus von Körpern, so ist f bereits injektiv: ist nämlich $x \in K$ mit $x \neq 0$, so ist nach Definition eines Körperhomomorphismus [G, Definition 7.25 (a)].

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

und damit notwendigerweise $f(x) \neq 0$. Es folgt unmittelbar $\operatorname{Ker} f = \{0\}$, d. h. f ist injektiv. Wir können damit K durch die Abbildung f als Unterkörper von L auffassen. *Jeder Körperhomomorphismus führt also automatisch zu einer Körpererweiterung.*

(c) Es seien L ein Körper sowie $K_i \leq L$ Unterkörper für alle i aus einer beliebigen Indexmenge I. Dann ist nach (a) klar, dass auch der Durchschnitt $\bigcap_{i \in I} K_i$ wieder ein Unterkörper von L ist — da alle K_i die 0 und 1 enthalten sowie abgeschlossen unter den Körperoperationen sind, gilt dies natürlich auch für den Durchschnitt. (Möchte man dies formal aufschreiben, müsste man dies analog zum Fall von Untergruppen in [G, Bemerkung 3.9 (b)] tun.)

Einen einfachen Fall hiervon erhält man, wenn man einfach *alle* Unterkörper von L miteinander schneidet. Dies führt zur folgenden Definition.

Definition 1.4 (Primkörper)**.** Ist L ein Körper, so heißt der Durchschnitt

$$P(L) := \bigcap_{K \leq L} K$$

über alle Teilkörper von L der **Primkörper** von L. Nach Bemerkung 1.3 (c) gilt stets $P(L) \leq L$.

Beispiel 1.5. Wir wollen den Primkörper von $L = \mathbb{R}$ berechnen. Es sei dazu $K \leq \mathbb{R}$ beliebig. Nach Definition eines Teilkörpers sind dann zunächst 0 und 1 in K, wegen der Abgeschlossenheit bezüglich Addition und Subtraktion dann auch $2 = 1+1$, $3 = 1+1+1$, ... und analog alle ganzen Zahlen, und wegen der Abgeschlossenheit bezüglich der Division schließlich auch alle Brüche $\frac{p}{q}$ mit $p, q \in \mathbb{Z}$, $q \neq 0$. Für jeden solchen Teilkörper K gilt also $K \supset \mathbb{Q}$.

Damit muss auch der Durchschnitt $P(\mathbb{R})$ aller dieser Teilkörper $\mathbb{Q}$ umfassen. Andererseits ist aber $\mathbb{Q}$ natürlich einer der Teilkörper von $\mathbb{R}$, über den in der Definition von $P(\mathbb{R})$ der Schnitt gebildet wird. Also folgt auch die umgekehrte Inklusion $P(\mathbb{R}) \subset \mathbb{Q}$ und damit schließlich $P(\mathbb{R}) = \mathbb{Q}$.

Genauso ergibt sich natürlich auch für die komplexen Zahlen $P(\mathbb{C}) = \mathbb{Q}$. Dies ist kein Zufall — es gibt nur sehr wenige verschiedene Möglichkeiten für Primkörper, wie wir gleich in Aufgabe 1.11 sehen werden. Für dieses Resultat benötigen wir noch den Begriff der Charakteristik eines Körpers, der die wohl wichtigste Eigenschaft eines Körpers beschreibt.

Definition 1.6 (Charakteristik eines Körpers)**.** Es sei K ein Körper. Für $n \in \mathbb{Z}$ setzen wir wie üblich

$$n \cdot 1_K := \underbrace{1_K + \cdots + 1_K}_{n\text{-mal}} \quad \in K$$

(wobei dieser Ausdruck für $n < 0$ natürlich als $(-n)$-fache Aufsummierung von -1_K zu verstehen ist). Gibt es ein $n > 0$, so dass $n \cdot 1_K = 0_K$ ist, so heißt das kleinste solche n die **Charakteristik** $\operatorname{char} K$ von K. Andernfalls setzt man $\operatorname{char} K := 0$.

Beispiel 1.7.

(a) Natürlich ist $\operatorname{char}\mathbb{Q} = \operatorname{char}\mathbb{R} = \operatorname{char}\mathbb{C} = 0$ und $\operatorname{char}\mathbb{Z}_p = p$ für alle Primzahlen p.

(b) Ist L/K eine Körpererweiterung, so gilt stets $\operatorname{char} K = \operatorname{char} L$ (da $1_K = 1_L$ und $0_K = 0_L$ ist und somit $n \cdot 1_K = 0_K$ genau dann in K gilt wenn $n \cdot 1_L = 0_L$ in L ist).

Bemerkung 1.8. Möchte man Definition 1.6 „algebraisch eleganter“ ausdrücken, so könnte man dies auch so formulieren: man betrachtet den Ringhomomorphismus $\mathbb{Z} \to K$, $n \mapsto n \cdot 1_K$. Der Kern dieses Morphismus ist ein Ideal von $\mathbb{Z}$ [G, Lemma 8.4] und damit von der Form (m) für ein eindeutig bestimmtes $m \in \mathbb{N}$ [G, Beispiel 8.3 (a)]. Diese Zahl m heißt dann die Charakteristik von K. Beachte, dass diese alternative Definition gleichermaßen in den Fällen $m > 0$ und $m = 0$ funktioniert.

Lemma 1.9. *Ist die Charakteristik eines Körpers ungleich Null, so ist sie eine Primzahl.*

Beweis. Angenommen, K wäre ein Körper mit $\operatorname{char} K = n = p \cdot q$, wobei $1 < p, q < n$. Dann wäre

$$0_K = \underbrace{1_K + \cdots + 1_K}_{n\text{-mal}} = \underbrace{(1_K + \cdots + 1_K)}_{p\text{-mal}} \cdot \underbrace{(1_K + \cdots + 1_K)}_{q\text{-mal}}.$$

Da Körper aber keine Nullteiler außer der 0 besitzen [G, Lemma 7.8 (c)], folgt daraus bereits $p \cdot 1_K = 0_K$ oder $q \cdot 1_K = 0_K$ — im Widerspruch dazu, dass n die *kleinste* positive Zahl mit $n \cdot 1_K = 0_K$ sein soll. Also kann es keine Darstellung $n = p \cdot q$ wie oben geben, d. h. n ist eine Primzahl. □

Bemerkung 1.10. Ob man hauptsächlich Körper der Charakteristik Null oder solche positiver Charakteristik betrachtet, hängt sehr vom jeweiligen Anwendungsgebiet der Algebra ab. So werden wir für die in der Einleitung genannten Probleme hauptsächlich Unterkörper von $\mathbb{C}$, also solche mit Charakteristik Null benötigen, während z. B. in der Gruppentheorie oder Zahlentheorie die Körper mit positiver Charakteristik eine weit größere Rolle spielen. Es ist eine besondere Stärke der Algebra, dass sie in weiten Teilen beide Fälle mit derselben Theorie behandeln kann, obwohl sich Körper mit positiver Charakteristik in der Praxis sehr deutlich von denen mit Charakteristik Null unterscheiden.

Der Zusammenhang zwischen der Charakteristik eines Körpers und seinem Primkörper ist sehr einfach, wie die folgende Aufgabe zeigt.

Aufgabe 1.11. Es sei K ein Körper. Man zeige:

(a) Ist $\operatorname{char} K = 0$, so ist $P(K)$ isomorph zu $\mathbb{Q}$. Jeder Körper der Charakteristik 0 ist also ein Erweiterungskörper von $\mathbb{Q}$.

(b) Ist $\operatorname{char} K = p > 0$, so ist $P(K)$ isomorph zu $\mathbb{Z}_p$. Jeder Körper der Charakteristik $p > 0$ ist also ein Erweiterungskörper von $\mathbb{Z}_p$.

(Hinweis: Untersuche den bereits in Bemerkung 1.8 erwähnten Ringhomomorphismus $\mathbb{Z} \to K$, $n \mapsto n \cdot 1_K$.)

Als Anwendung der gerade eingeführten Begriffe wollen wir nun sehen, wie sich die Probleme der Auflösbarkeit von Polynomgleichungen und der Konstruktionen mit Zirkel und Lineal aus der Einleitung in die Sprache der Körpererweiterungen übersetzen lassen. Bei den Konstruktionen mit Zirkel und Lineal müssen wir dabei zunächst einmal sehen, wie diese überhaupt mit Körpern zusammenhängen. Die Grundidee hierfür ist, die Zeichenebene mit der Ebene der komplexen Zahlen $\mathbb{C}$ zu identifizieren. Wir starten nun mit einer Menge $M \subset \mathbb{C}$ von ursprünglich gegebenen Punkten. Diese Menge wird in der Regel recht klein sein, muss aber natürlich mindestens zwei Punkte enthalten, da sonst überhaupt keine Elementarkonstruktionen wie in Problem 0.3 ausführbar sind (sowohl um eine Gerade als auch um einen Kreis zu zeichnen braucht man ja mindestens zwei Punkte). Wir können die komplexe Ebene daher so mit der Zeichenebene identifizieren, dass die Punkte $0 \in \mathbb{C}$ und $1 \in \mathbb{C}$ in M liegen. Der entscheidende Punkt ist nun, dass die Menge *aller* aus M konstruierbaren Punkte ein Unterkörper von $\mathbb{C}$ ist.

Satz 1.12. *Es sei $M \subset \mathbb{C}$ mit $0, 1 \in M$ gegeben. Weiterhin bezeichne $\hat{M} \subset \mathbb{C}$ die Menge aller aus M mit Zirkel und Lineal konstruierbaren Punkte der Ebene. Dann gilt:*

(a) *$\hat{M}$ ist ein Körper mit $\mathbb{Q} \leq \hat{M} \leq \mathbb{C}$.*

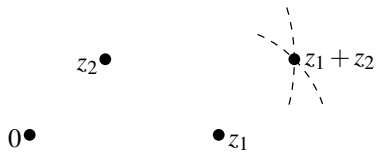
(b) *Ist $z \in \hat{M}$, so liegt auch die zu z konjugiert komplexe Zahl $\bar{z}$ in $\hat{M}$.*

(c) *Ist $z \in \hat{M}$, so liegen auch die beiden komplexen Quadratwurzeln $\pm\sqrt{z}$ in $\hat{M}$.*

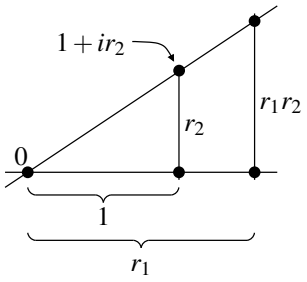
01

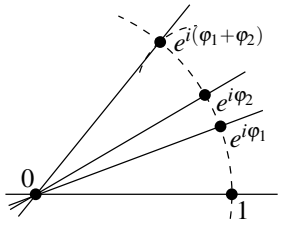
Beweis. Da 0 und 1 nach Voraussetzung in $\hat{M}$ liegen, müssen wir nach Bemerkung 1.3 (a) nur zeigen, dass $\hat{M}$ abgeschlossen unter den Körperoperationen, der komplexen Konjugation und dem Ziehen von Quadratwurzeln ist, d. h. dass sich diese algebraischen Operationen mit Zirkel und Lineal durchführen lassen (dass $\hat{M}$, wie in (a) zusätzlich noch behauptet, ein Erweiterungskörper von $\mathbb{Q}$ ist, folgt aus Aufgabe 1.11 (a)). Wir zeigen diese Abgeschlossenheit exemplarisch für die Addition, die Multiplikation und das Wurzelziehen, da die anderen Fälle analog (bzw. einfacher) sind.

- *Addition:* Es seien $z_1, z_2 \in \hat{M}$, also konstruierbar. Der Punkt $z_1 + z_2$ ist offensichtlich der, der die drei Punkte 0, z_1 und z_2 zu einem Parallelogramm vervollständigt. Diesen kann man konstruieren, indem man einen Kreis um z_1 mit Radius $|z_2|$ (also dem Abstand von 0 nach z_2) und einen um z_2 mit Radius $|z_1|$ (also dem Abstand von 0 nach z_1) zeichnet: der Punkt $z_1 + z_2$ ist dann einer der beiden Schnittpunkte dieser Kreise. Also ist auch $z_1 + z_2 \in \hat{M}$.



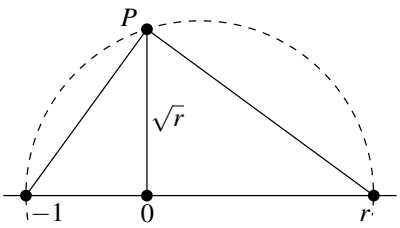
- *Multiplikation:* Es seien wieder $z_1, z_2 \in \hat{M}$ konstruierbar; wir müssen zeigen, dass auch $z_1 z_2$ konstruierbar ist. Dazu stellen wir diese beiden Zahlen in Polarkoordinaten $z_1 = r_1 e^{i\varphi_1}$ und $z_2 = r_2 e^{i\varphi_2}$ dar. Wegen $z_1 z_2 = r_1 r_2 e^{i(\varphi_1+\varphi_2)}$ müssen wir also mit Zirkel und Lineal die Beträge der beiden Zahlen multiplizieren und die Winkel addieren können. Um die Beträge zu multiplizieren (siehe das Bild unten links), zeichnen wir in den Punkten 1 und r_1 zur reellen Achse senkrechte Geraden wie in Problem 0.3 (a). Auf der ersten Senkrechten tragen wir dann nach oben die Länge r_2 ab (d. h. wir konstruieren den Punkt $1+ir_2$). Die Gerade durch 0 und $1+ir_2$ schneidet die zweite Senkrechte dann nach dem Strahlensatz im Punkt $r_1 + ir_1 r_2$, d. h. in einem Punkt, der von r_1 die Länge $r_1 r_2$ hat.

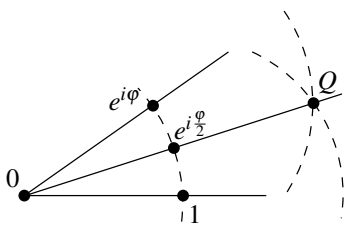




Um die Winkel zu addieren (siehe das Bild oben rechts), zeichnen wir einfach einen Kreis mit Radius 1 um den Nullpunkt und einen mit Radius $|e^{i\varphi_1} - 1|$ (also dem Abstand der bereits konstruierten Punkte 1 und $e^{i\varphi_1}$) um $e^{i\varphi_2}$; einer der Schnittpunkte dieser beiden Kreise definiert dann den Punkt $e^{i(\varphi_1+\varphi_2)}$, also die addierten Winkel.

- *Quadratwurzeln:* Wir arbeiten wieder mit Polarkoordinaten und suchen also zu $z = re^{i\varphi}$ die Zahl $\sqrt{r}\, e^{i\frac{\varphi}{2}}$, d. h. wir müssen die Wurzel aus r sowie zu φ den halben Winkel $\frac{\varphi}{2}$ konstruieren. Für die Wurzel aus r zeichnet man wie im Bild unten links einen Kreis mit Durchmesser $r+1$ von $-1 \in \mathbb{C}$ nach $r \in \mathbb{C}$; es sei P dann der Schnittpunkt dieses Kreises mit der positiven imaginären Achse. Nach bekannter Schulgeometrie ist das Dreieck mit den Eckpunkten P, -1 und r dann rechtwinklig, so dass aus dem Höhensatz folgt, dass die Strecke von 0 nach P gleich der Wurzel aus dem Produkt der Streckenlängen von -1 nach 0 und von 0 nach r, also gleich $\sqrt{r}$ ist.





Für die Winkelhalbierung zeichne man einfach wie im Bild oben rechts zwei Kreise mit Radius 1 und Mittelpunkten 1 sowie $e^{i\varphi}$; ist dann Q ein Schnittpunkt dieser beiden Kreise, so halbiert die Strecke von 0 nach Q offensichtlich den Winkel φ. □

Wir haben die geometrische Frage der Konstruierbarkeit gewisser Punkte der Ebene damit also auf die algebraische Frage zurückgeführt, ob diese Punkte — aufgefasst als komplexe Zahlen — in bestimmten Erweiterungskörpern von $\mathbb{Q}$ bzw. Unterkörpern von $\mathbb{C}$ liegen. Daher sollten wir als

Nächstes nun sehen, wie wir solche Körper zwischen $\mathbb{Q}$ und $\mathbb{C}$ algebraisch am besten beschreiben können.

Die grundlegende Idee hierfür kennt ihr in anderen Fällen bereits aus den „Algebraischen Strukturen“: um Untergruppen einer gegebenen Gruppe G zu konstruieren, kann man eine beliebige Teilmenge $M \subset G$ wählen und die davon erzeugte Untergruppe $\langle M \rangle$ betrachten. Formal kann man $\langle M \rangle$ als den Durchschnitt aller Untergruppen U mit $U \supset M$ definieren; anschaulich ist es einfach die kleinste Untergruppe von G, die M enthält [G, Definition 3.11 und Lemma 3.12]. Analog gibt es in Ringen das von einer Teilmenge erzeugte Ideal, also das kleinste Ideal, das diese gegebene Menge enthält [G, Definition 8.5 und Lemma 8.6].

Ganz genauso können wir nun Körper konstruieren, die zwischen zwei gegebenen Körpern K und L (oben also zwischen $\mathbb{Q}$ und $\mathbb{C}$) liegen:

Definition 1.13 (Körperadjunktion, einfache Körpererweiterungen)**.** Es seien $K \leq L$ Körper und $M \subset L$ eine beliebige Menge. Dann ist

$$K(M) := \bigcap_{\substack{K \leq Z \leq L \\ Z \supset M}} Z,$$

also der Durchschnitt aller Unterkörper von L, die sowohl K als auch die Menge M enthalten, nach Beispiel 1.3 (c) ein Körper mit $K \leq K(M) \leq L$. Anschaulich ist $K(M)$ der kleinste Unterkörper von L, der K und M enthält. Man kann $K(M)$ daher als den von M über K erzeugten Körper bezeichnen. Aus historischen Gründen ist jedoch die Sprechweise üblicher, dass $K(M)$ aus K durch **Adjunktion** der Elemente von M entsteht; man spricht $K(M)$ daher oft als „K adjungiert M“.

Ist $M = \{a_1, \ldots, a_n\}$ eine endliche Menge, so schreibt man statt $K(\{a_1, \ldots, a_n\})$ aus Bequemlichkeit in der Regel $K(a_1, \ldots, a_n)$. Besteht M sogar nur aus einem Element a, so nennt man $K(a)/K$ eine **einfache Körpererweiterung**.

Bemerkung 1.14 (Explizite Formel für Körperadjunktionen)**.** Analog zu [G, Aufgabe 3.14 und Definition 8.5] im Fall von Untergruppen bzw. Idealen kann man auch im Fall von Körpern eine explizite Formel für $K(M)$ hinschreiben. Betrachten wir der Einfachheit halber zunächst eine einfache Körpererweiterung, also $K(a)$ für ein $a \in L$ mit $K \leq L$, so gilt

$$K(a) = \left\{ \frac{f(a)}{g(a)} : \ f, g \in K[t] \text{ mit } g(a) \neq 0 \right\}.$$

Denn einerseits muss jeder Körper, der sowohl K als auch a enthält, wegen der Abgeschlossenheit bezüglich der Körperoperationen alle Ausdrücke der Form $\frac{f(a)}{g(a)}$ mit $f, g \in K[t]$ und $g(a) \neq 0$ enthalten; andererseits ist die rechte Seite der obigen Gleichung aber offensichtlich schon ein Körper, da sie selbst abgeschlossen unter den Körperoperationen ist. Damit ist dies also in der Tat der kleinste Körper, der K und a enthält, d. h. es ist genau $K(a)$.

Beachte, dass die Notation hier konsistent ist mit der Bezeichnung $\mathbb{R}(t)$ für den Körper der rationalen Funktionen über $\mathbb{R}$ aus Beispiel 1.2 (c): dieser wird in der Tat über $\mathbb{R}$ von der Identität $t \mapsto t$ erzeugt.

Adjungiert man zu K eine beliebige Menge M, so erhält man mit der gleichen Begründung wie oben die Aussage, dass $K(M)$ die Menge aller Quotienten von Polynomen (in mehreren Variablen) ist, die Koeffizienten in K haben und für deren Variablen man Werte aus M eingesetzt hat.

Beispiel 1.15. Wenn wir die einfache Körpererweiterung $\mathbb{Q}(\sqrt{2})$ über $\mathbb{Q}$ betrachten, so können wir deren Elemente nach Bemerkung 1.14 als die Menge aller Brüche von Polynomen in $\sqrt{2}$ mit rationalen Koeffizienten schreiben. Es gibt für diesen Körper aber eine viel einfachere Darstellung: wir behaupten, dass

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}$$

gilt. Um dies zu zeigen, bemerken wir zunächst, dass jeder Körper, der $\mathbb{Q}$ und $\sqrt{2}$ enthält, wegen der Abgeschlossenheit offensichtlich auch die rechte Seite der obigen Gleichung enthalten muss. Analog zur Begründung in Bemerkung 1.14 reicht es also zu zeigen, dass die rechte Seite bereits ein Körper, also abgeschlossen unter den Körperoperationen, ist. Die Abgeschlossenheit bezüglich

Addition und Subtraktion ist hierbei trivial, die bezüglich Multiplikation und Division ergibt sich aus den elementaren Rechnungen

$$(a+b\sqrt{2})(c+d\sqrt{2}) = \underbrace{(ac+2bd)}_{\in\mathbb{Q}} + \underbrace{(ad+bc)}_{\in\mathbb{Q}}\sqrt{2}$$

und

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \underbrace{\frac{a}{a^2-2b^2}}_{\in\mathbb{Q}} - \underbrace{\frac{b}{a^2-2b^2}}_{\in\mathbb{Q}}\sqrt{2}$$

für alle $a,b,c,d \in \mathbb{Q}$. Wir werden in Lemma 2.10 und Satz 2.14 (b) noch genauer sehen, wie man Körpererweiterungen oft auf viel einfachere Art als in Bemerkung 1.14 explizit beschreiben kann.

Aufgabe 1.16. Es seien L/K eine Körpererweiterung und M_1, M_2 Teilmengen von L. Zeige, dass $(K(M_1))(M_2) = (K(M_2))(M_1) = K(M_1 \cup M_2)$ gilt, d. h. dass es bei der Adjunktion von Mengen nicht auf die Reihenfolge ankommt.

Aufgabe 1.17. Zeige, dass $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ gilt. Gilt auch $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}\cdot\sqrt{3})$?
(Eine Verallgemeinerung dieser Aussage werden wir später in Satz 4.28 beweisen.)

Nachdem wir nun also wissen, wie wir Körpererweiterungen prinzipiell algebraisch beschreiben können, wollen wir jetzt sehen, welche Eigenschaften diese Körpererweiterungen für unsere konkreten Probleme aus der Einleitung haben müssen. Betrachten wir dazu zunächst einmal die Frage der Auflösbarkeit von Polynomgleichungen aus Problem 0.2. Wenn wir die Möglichkeit des Wurzelziehens für einen Moment vernachlässigen und uns fragen würden, ob wir die Nullstellen eines Polynoms $f = t^n + a_{n-1}t^{n-1} + \cdots + a_0$ nur mit Hilfe der Körperoperationen aus den Koeffizienten von f bestimmen können, so könnten wir dies jetzt bereits algebraisch formulieren: dies wäre genau dann der Fall, wenn alle Nullstellen von f in $\mathbb{Q}(a_0,\ldots,a_{n-1})$ liegen — denn dies ist nach Definition 1.13 ja gerade der Körper aller Zahlen, die man aus den Koeffizienten des Polynoms (und unter Verwendung der rationalen Zahlen, die man nach Aufgabe 1.11 (a) immer mit dabei hat) mit den Körperoperationen erzeugen kann.

Wollen wir nun noch zusätzlich Wurzelziehen erlauben, so müssen wir statt $\mathbb{Q}(a_0,\ldots,a_{n-1})$ einfach eine geeignete Körpererweiterung betrachten, in der solche Wurzeln auch vorhanden sind:

Definition 1.18 (Radikalerweiterungen)**.** Es sei L/K eine Körpererweiterung.

(a) Ist $L = K(a)$ für ein $a \in L$, also $L/K = K(a)/K$ eine einfache Körpererweiterung, so heißt $K(a)/K$ eine **einfache Radikalerweiterung**, falls es ein $n \in \mathbb{N}_{>0}$ gibt mit $a^n \in K$. Man spricht in diesem Fall auch von einer **einfachen n-Radikalerweiterung** und kann sich dies so vorstellen, dass $K(a)$ aus K durch Adjunktion einer n-ten Wurzel entsteht.

(b) Ist L/K beliebig, so nennt man L/K eine **Radikalerweiterung**, falls es eine endliche Kette von Körpern

$$K = K_0 \leq K_1 \leq \cdots \leq K_m = L$$

gibt, so dass jedes K_i/K_{i-1} für $i = 1,\ldots,m$ eine einfache Radikalerweiterung ist (d. h. wenn L aus K durch fortgesetzte Adjunktion von Wurzeln entsteht). Ist jede dieser Körpererweiterungen eine einfache n-Radikalerweiterung (für dasselbe n), so nennt man L/K auch eine **n-Radikalerweiterung**.

Beispiel 1.19.

(a) Die Körpererweiterung $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ aus Beispiel 1.15 ist offensichtlich eine einfache 2-Radikalerweiterung, denn $(\sqrt{2})^2 = 2 \in \mathbb{Q}$.

(b) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{1+\sqrt{2}})/\mathbb{Q}$ ist eine Radikalerweiterung, denn in der Kette

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{1+\sqrt{2}}\right)$$

ist jeder Schritt eine einfache Radikalerweiterung (im zweiten Schritt wird die dritte Wurzel des Elements $1+\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ adjungiert).

Mit dieser Definition können wir nun unser Problem der Auflösbarkeit von Polynomgleichungen exakt formulieren:

Definition 1.20. Ein komplexes Polynom $f = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 \in \mathbb{C}[t]$ heißt **auflösbar**, wenn es eine Radikalerweiterung von $\mathbb{Q}(a_0, \ldots, a_{n-1})$ gibt, die alle Nullstellen von f enthält (also „wenn sich alle Nullstellen von f aus den Koeffizienten mit Hilfe der Körperoperationen und komplexem Wurzelziehen exakt berechnen lassen“).

Beispiel 1.21. Jedes komplexe Polynom $f = t^2 + a_1 t + a_0$ vom Grad 2 ist auflösbar, denn seine Nullstellen $-\frac{a_1}{2} \pm \sqrt{\frac{a_1^2}{4} - a_0}$ liegen offensichtlich in der Radikalerweiterung $\mathbb{Q}\left(a_0, a_1, \sqrt{\frac{a_1^2}{4} - a_0}\right)$ von $\mathbb{Q}(a_0, a_1)$. Genauso zeigt die Cardanische Formel aus Problem 0.2, dass jedes Polynom vom Grad 3 auflösbar ist. Wie bereits angekündigt werden wir in Aufgabe 8.14 jedoch sehen, dass es auch Polynome gibt, die nicht auflösbar sind.

Nach der Auflösbarkeit von Polynomgleichungen wollen wir nun zum Schluss dieses Kapitels auch die Konstruktionsprobleme mit Zirkel und Lineal aus Problem 0.3 in die Sprache der Algebra übersetzen. Das wesentliche Ergebnis hierfür ist natürlich Satz 1.12, der im Prinzip besagt, dass man Körperoperationen und Quadratwurzelziehen in der komplexen Ebene geometrisch durchführen kann. Die Fragestellung ist hier also sehr ähnlich zur Auflösbarkeit von Polynomgleichungen, nur dass wir in diesem Fall lediglich Quadratwurzeln und nicht beliebige Wurzeln zulassen. Dies führt zu folgendem Satz, der der Definition 1.20 eines auflösbaren Polynoms sehr ähnlich sieht.

Satz 1.22. *Es sei $M \subset \mathbb{C}$ mit $0, 1 \in M$ gegeben. Ein Punkt $z \in \mathbb{C}$ ist genau dann aus M mit Zirkel und Lineal konstruierbar, wenn z in einer 2-Radikalerweiterung von $\mathbb{Q}(M \cup \overline{M})$ liegt. (Hierbei bezeichnet $\overline{M}$ die Menge aller komplex konjugierten Zahlen zu Elementen aus M.)*

Beweis.

„$\Leftarrow$“ ist genau Satz 1.12: Zahlen in einer 2-Radikalerweiterung von $\mathbb{Q}(M \cup \overline{M})$ sind nach Definition 1.18 genau diejenigen, die sich aus M mit Hilfe der Körperoperationen, komplexer Konjugation und Ziehen von Quadratwurzeln erzeugen lassen — und solche Punkte sind nach Satz 1.12 alle mit Zirkel und Lineal konstruierbar.

„$\Rightarrow$“ Es sei $z \in \hat{M}$ mit Zirkel und Lineal konstruierbar. Wir müssen zeigen, dass sich z aus den Punkten von M mit Hilfe der Körperoperationen, der komplexen Konjugation und komplexer Quadratwurzeln ergibt.

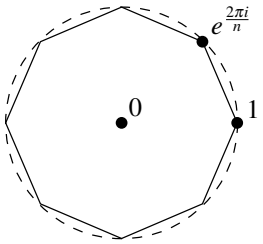
Neue Punkte entstehen bei Elementarkonstruktionen nur dadurch, dass man Schnittpunkte von bereits konstruierten Geraden und / oder Kreisen bestimmt. Geraden und Kreise durch schon konstruierte Punkte werden aber beschrieben durch lineare bzw. quadratische Gleichungen in z und $\bar{z}$, deren Koeffizienten bereits konstruierte Zahlen sind. Die in einer Elementarkonstruktion neu konstruierten Punkte entstehen also stets als Lösungen linearer oder quadratischer Gleichungen mit bereits konstruierten Koeffizienten. Lineare und quadratische Gleichungen lassen sich aber bekanntlich mit Hilfe der Körperoperationen und evtl. Ziehen von Quadratwurzeln lösen. □

Beispiel 1.23 (Konstruktionen mit Zirkel und Lineal, algebraische Fassung)**.** Mit Satz 1.22 können wir die Aufgaben aus Problem 0.3 nun algebraisch formulieren:

(A) (Quadratur des Kreises) In der Ebene sei ein Kreis, o. B. d. A. der Einheitskreis gegeben (der durch den Mittelpunkt 0 und den Punkt 1 auf dem Rand definiert wird). Da dieser Kreis den Flächeninhalt π besitzt, suchen wir also nach einem Quadrat mit Seitenlänge $\sqrt{\pi}$, d. h. wir wollen den Punkt $\sqrt{\pi}$ konstruieren. Nach Satz 1.22 ist die Quadratur des Kreises also genau dann möglich, wenn $\sqrt{\pi}$ in einer 2-Radikalerweiterung von $\mathbb{Q}(0,1) = \mathbb{Q}$ liegt. Offensichtlich ist dies auch äquivalent dazu, dass π in einer 2-Radikalerweiterung von $\mathbb{Q}$ liegt, da man $\sqrt{\pi}$ ja aus π durch Ziehen einer weiteren Quadratwurzel erhält.

(B) (Würfelverdoppelung) Da wir zur Seitenlänge 1 eines Würfels die Seitenlänge $\sqrt[3]{2}$ eines Würfels mit dem doppelten Volumen konstruieren wollen, ist diese Konstruktion analog zu (A) genau dann möglich, wenn $\sqrt[3]{2}$ in einer 2-Radikalerweiterung von $\mathbb{Q}$ liegt.

(C) (Konstruktion des regelmäßigen n-Ecks) Gegeben sei der Mittelpunkt und einer der Eckpunkte des n-Ecks, o. B. d. A. wieder 0 bzw. 1. Offensichtlich genügt es, den ersten weiteren Eckpunkt $e^{\frac{2\pi i}{n}}$ des n-Ecks zu konstruieren, da alle weiteren Eckpunkte dann natürlich rekursiv genauso aus dem jeweils vorhergehenden konstruiert werden können. Also ist die Konstruktion des n-Ecks genau dann möglich, wenn $e^{\frac{2\pi i}{n}}$ in einer 2-Radikalerweiterung von $\mathbb{Q}$ liegt.



Wie schon angekündigt müssen wir also genau wie im Fall der Auflösbarkeit von Polynomgleichungen entscheiden, ob bestimmte Zahlen in gewissen Radikalerweiterungen enthalten sein können oder nicht. Der wesentliche Unterschied besteht darin, dass wir hier nach einer *2-Radikalerweiterung* und nicht nach einer allgemeinen Radikalerweiterung fragen — weil wir beim Auflösen von Gleichungen beliebige Wurzeln zulassen wollen, während man mit Zirkel und Lineal nur Quadratwurzeln ziehen kann.

Bemerkung 1.24. Ist $M \subset \mathbb{C}$ eine Menge mit $0, 1 \in M$, so ergibt sich aus Satz 1.12, dass in jedem Fall alle Punkte der Form $x + iy$ mit $x, y \in \mathbb{Q}$ zu $\hat{M}$ gehören, also konstruierbar sind. Die konstruierbaren Punkte liegen damit „*dicht*“ in der Zeichenebene, d. h. jeder beliebige Punkt der Ebene lässt sich zumindest beliebig genau mit Zirkel und Lineal approximieren.