

0. Einleitung und Motivation

Die Vorlesung „Einführung in die Algebra“ verfolgt zwei Ziele. Einerseits wollen wir aus rein algebraischer Sicht das in der Vorlesung „Algebraische Strukturen“ begonnene Studium von Gruppen, Ringen und Körpern fortsetzen. Wir werden demzufolge viele Resultate dieser vorangegangenen Vorlesung benutzen; in diesem Skript verwende ich dazu Referenzen auf mein Skript [G]. Die Ergebnisse der Einführung in die Algebra gehören wie die der Algebraischen Strukturen zum Werkzeugkasten eines jeden Algebraikers; sie werden euch später sicher immer wieder begegnen, wenn ihr vertiefende Vorlesungen im Bereich der Algebra hört.

Andererseits sind diese algebraischen Strukturen ursprünglich natürlich nicht aus purem Interesse an abstrakter Algebra eingeführt worden. Sie dienen vielmehr als Hilfsmittel, um konkrete klassische mathematische Probleme zu lösen, die oftmals sehr anschaulich und geometrisch waren. Im Rahmen dieser Vorlesung werden wir einige dieser klassischen Probleme untersuchen und sie dann nach und nach mit Hilfe der Algebra lösen. Diese anschaulichen und wichtigen Probleme, deren Lösung also das zweite Ziel der „Einführung in die Algebra“ sind, können uns somit im Laufe der Vorlesung als Motivation und Leitfaden dienen. Ich möchte hier einige von ihnen in diesem einführenden Kapitel vorstellen.

Problem 0.1 (Fundamentalsatz der Algebra). Der wohl bekannteste und wichtigste Satz der Algebra ist der sogenannte *Fundamentalsatz der Algebra*, dessen Aussage ihr bereits alle kennt. Er besagt, dass jedes nicht-konstante komplexe Polynom

$$f = t^n + a_{n-1}t^{n-1} + \cdots + a_1t + a_0 \in \mathbb{C}[t]$$

eine Nullstelle hat, also dass es ein $x \in \mathbb{C}$ gibt mit $f(x) = 0$. Hat man eine solche Nullstelle, so kann man das gegebene Polynom natürlich ohne Rest durch $t - x$ teilen und erhält so ein neues Polynom vom Grad $n - 1$, auf das man den Fundamentalsatz erneut anwenden kann. Der Fundamentalsatz ist also äquivalent dazu, dass sich jedes Polynom vom Grad n über \mathbb{C} als Produkt von n linearen Polynomen schreiben lässt. Damit hat ein solches Polynom stets n Nullstellen (von denen einige übereinstimmen können).

Den Fundamentalsatz der Algebra kann man auf viele verschiedene Arten beweisen, z. B. mit Hilfe der Topologie oder der Funktionentheorie. Wir werden in dieser Vorlesung einen algebraischen Beweis geben (siehe Satz 7.25).

Problem 0.2 (Auflösbarkeit von Polynomgleichungen). Wir betrachten wieder eine komplexe polynomiale Gleichung

$$t^n + a_{n-1}t^{n-1} + \cdots + a_1t + a_0 = 0$$

mit $n \geq 1$ und $a_i \in \mathbb{C}$. Wie wir gerade erwähnt haben, hat diese Gleichung nach dem Fundamentalsatz der Algebra genau n Lösungen (von denen einige übereinstimmen können). Für kleines n lassen sich diese Lösungen natürlich leicht explizit angeben: für $n = 1$ hat man einfach

$$t = -a_0,$$

und für $n = 2$ nach der aus der Schule bekannten Formel

$$t = -\frac{a_1}{2} \pm \sqrt{\frac{a_1^2}{4} - a_0}.$$

Für höhere Grade kennt ihr vermutlich keine derartigen Lösungsformeln. In der Schule begnügt man sich z. B. für kubische Polynomgleichungen ja in der Regel mit der Methode, dass man eine Nullstelle „rät“ — sofern dies möglich ist — und diese dann abspaltet, so dass man eine quadratische Gleichung übrig behält, die man dann wieder wie oben lösen kann.

Es gibt jedoch auch für $n = 3$ noch eine explizite Lösungsformel. In der Schule betrachtet man sie in der Regel nicht, weil sie zum einen ein bisschen zu kompliziert ist, um sie sich merken zu können, und sie zum anderen erfordert, dass man dritte Wurzeln aus komplexen Zahlen ziehen kann. Es handelt sich hierbei um die im 16. Jahrhundert gefundene **Cardanische Formel**

$$t = \sqrt[3]{-q + \sqrt{q^2 + p^3}} + \sqrt[3]{-q - \sqrt{q^2 + p^3}}, \quad (*)$$

wobei

$$p = \frac{3a_1 - a_2^2}{9} \quad \text{und} \quad q = \frac{a_2^3}{27} - \frac{a_1 a_2}{6} + \frac{a_0}{2}$$

(und in $(*)$ die „richtigen“ komplexen dritten Wurzeln gewählt werden müssen — für jede der beiden dritten Wurzeln gibt es ja drei Möglichkeiten, aber nur 3 der insgesamt $3 \cdot 3 = 9$ Kombinationsmöglichkeiten liefern in der Tat eine Nullstelle des Polynoms).

In der Tat gibt es auch für den Fall $n = 4$ noch eine (natürlich noch komplizierte) Lösungsformel im obigen Stil, d. h. ein Verfahren, das aus den gegebenen Koeffizienten a_i der Gleichung durch Körperoperationen (Addition, Subtraktion, Multiplikation und Division) und Ziehen beliebiger Wurzeln die exakten Lösungen bestimmt. Diese sogenannte Formel von Ferrari wurde ebenfalls bereits im 16. Jahrhundert gefunden.

Natürlich haben die Mathematiker dann nach entsprechenden Formeln für höhere Grade gesucht — allerdings erfolglos. Es hat sehr lange gedauert, bis Abel im 19. Jahrhundert erkannte, dass es für $n \geq 5$ keine derartige Lösungsformel geben kann. Dieses überraschende Resultat benötigt zum Beweis natürlich ganz andere Methoden als im Fall $n \leq 4$, wo man eine konkrete Formel einfach angeben und ihre Korrektheit nachrechnen kann. Obwohl man dies von der Problemstellung her gar nicht vermuten würde, benötigt man hierzu Gruppentheorie. Wir werden in Definition 5.10 und Lemma 5.11 (a) einem Polynom f vom Grad n eine Untergruppe G der symmetrischen Gruppe S_n zuordnen und die Frage, ob sich die Nullstellen von f aus den Koeffizienten durch Körperoperationen und Wurzelziehen bestimmen lassen, in Definition 8.6 und Folgerung 8.12 in eine gewisse Eigenschaft der Untergruppe G übersetzen. Von dieser Eigenschaft können wir in Folgerung 8.10 dann zeigen, dass sie für Untergruppen von S_n für $n \leq 4$ stets erfüllt ist, für $n \geq 5$ jedoch nicht.

Wir sollten aber noch einmal deutlich betonen, dass dies natürlich *nicht* bedeutet, dass Polynomgleichungen vom Grad $n \geq 5$ keine exakten Lösungen besitzen — das wäre ja auch ein Widerspruch zum Fundamentalsatz. Es bedeutet nur, dass sich die exakten Lösungen im Allgemeinen nicht mehr durch Körperoperationen und fortgesetztes Wurzelziehen aus den Koeffizienten des Polynoms berechnen lassen.

Problem 0.3 (Konstruktionen mit Zirkel und Lineal). Ein sehr klassisches (und zunächst geometrisch erscheinendes) Problem ist die Konstruktion bestimmter Objekte in der Ebene mit Zirkel und Lineal, wie ihr sie sicher schon in der Schule durchgeführt habt. Dabei seien die folgenden beiden **Elementarkonstruktionen** erlaubt:

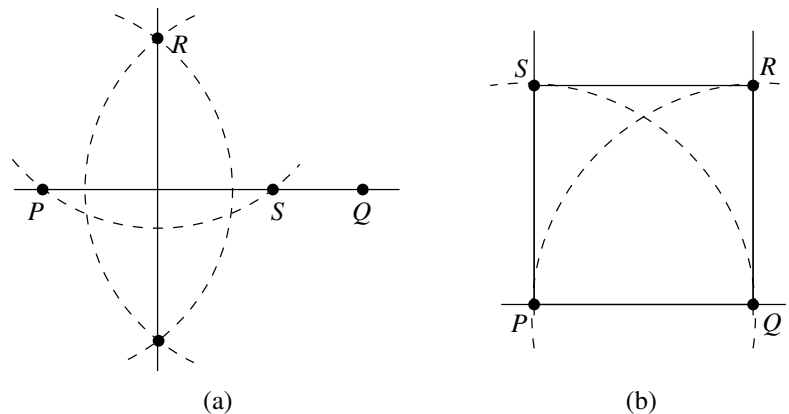
- man zeichnet mit dem Lineal eine Gerade durch P und Q (wobei P und Q zwei bereits konstruierte Punkte sind);
- man zeichnet mit dem Zirkel einen Kreis durch P mit Radius \overline{QR} (wobei P , Q und R drei bereits konstruierte Punkte sind).

Bei diesen beiden Operationen entstehende Schnittpunkte aus Geraden und Kreisen gelten dann als konstruiert.

Ein paar Beispiele solcher möglichen Konstruktionen sind:

- (a) Gegeben seien eine Gerade PQ und ein Punkt R (der auf der Geraden PQ liegen darf oder auch nicht). Man konstruiere die Gerade durch R , die auf PQ senkrecht steht.

Lösung: Man zeichne einen Kreis um R mit Radius \overline{PR} ; die beiden Schnittpunkte mit der gegebenen Geraden seien P und S . Mit dem gleichen Radius zeichne man nun zwei Kreise um P und S . Die Verbindungslinie der Schnittpunkte dieser beiden Kreise ist dann die gesuchte Gerade. Die Konstruktion ist im Bild unten links dargestellt.



- (b) Man konstruiere ein Quadrat.

Lösung: Man starte mit einer beliebigen Strecke \overline{PQ} . Dann konstruiere man wie in (a) die Senkrechten zu PQ durch P und Q und trage die Strecke PQ auf diesen beiden Senkrechten mit dem Zirkel ab. Die Konstruktion ist im Bild oben rechts dargestellt.

Es gibt aber auch einige geometrische Probleme, deren Lösung mit Zirkel und Lineal trotz jahrhundertelanger Suche nicht gefunden werden konnte, und von denen man erst viel später mit Hilfe der Algebra zeigen konnte, dass sie in der Tat nicht lösbar sind:

- (A) (**Quadratur des Kreises**) Zu einem gegebenen Kreis konstruiere man ein Quadrat mit gleichem Flächeninhalt. Dies ist mit Zirkel und Lineal nicht möglich — in der Tat steht der Begriff der „Quadratur des Kreises“ umgangssprachlich ja auch für ein unlösbares Problem. Hat der ursprüngliche Kreis den Radius a und das gesuchte Quadrat die Seitenlänge b , so verlangen wir offensichtlich $\pi a^2 = b^2$, wir wollen aus einer Strecke der Länge a also eine Strecke der Länge $b = \sqrt{\pi}a$ konstruieren. Wir werden dieses Problem in Beispiel 2.23 genauer untersuchen.
- (B) (**Würfelverdoppelung**) Zu einem gegebenen Würfel konstruiere man einen Würfel doppelten Volumens. (Damit ist gemeint: es sei die Seitenlänge a eines solchen Würfels gegeben; man konstruiere die Seitenlänge $\sqrt[3]{2}a$ des Würfels mit dem doppelten Volumen.) Auch diese Konstruktion ist mit Zirkel und Lineal nicht möglich, wie wir in Beispiel 2.23 beweisen werden.
- (C) (**Konstruktion des regelmäßigen n -Ecks**) Zu gegebenem n konstruiere man ein regelmäßiges n -Eck mit Zirkel und Lineal (wie wir es z. B. für $n = 4$ in (b) oben getan haben). Wir werden in Folgerung 3.33 und 7.8 sehen, dass dies nur für bestimmte n möglich ist — z. B. ist es für $n = 3, 4, 5, 6, 8, 10$ möglich, für $n = 7$ und $n = 9$ jedoch nicht.

Die Galoistheorie, die zum Beweis solcher Aussagen (und auch für die Lösung der Probleme 0.1 und 0.2) nötig ist und die wir in dieser Vorlesung behandeln werden, stammt aus dem frühen 19. Jahrhundert, ist also ebenfalls schon relativ alt. Dennoch gibt es übrigens immer noch viele Hobbymathematiker, die die Galoistheorie nicht verstehen bzw. ihre Ergebnisse nicht glauben, und die immer noch versuchen, diese Konstruktionsaufgaben zu lösen und auf diese Art berühmt zu werden. An vielen bekannten Universitäten gibt es daher sogar Mitarbeiter, deren Aufgabe es (unter anderem) ist, die dort zahlreich ankommenden Briefe solcher Hobbymathematiker mit ihren angeblichen Lösungen zu beantworten.

Aufgabe 0.4. Auf einem Blatt Papier sei ein gleichseitiges Dreieck gegeben. Konstruiert daraus ein flächengleiches Quadrat mit Zirkel und Lineal.

Aufgabe 0.5. In dieser Aufgabe bezeichnen $ABCDE$ im Uhrzeigersinn die Ecken eines regelmäßigen Fünfecks.

- (a) Man zeige, dass \overline{AB} die Strecke \overline{AC} im „goldenen Schnitt“ teilt, d. h. dass

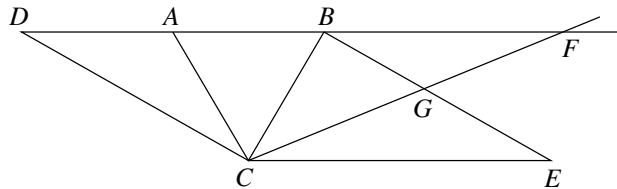
$$\frac{\overline{AB}}{\overline{AC}} = \frac{\overline{AC} - \overline{AB}}{\overline{AB}}$$

gilt, und schlieÙe daraus, dass $\overline{AC} = \frac{1}{2}(\sqrt{5} + 1) \cdot \overline{AB}$.

- (b) Auf einem Blatt Papier sei nur die Strecke \overline{AB} gegeben. Mit Hilfe von (a) konstruiere man daraus das gesamte Fünfeck $ABCDE$ mit Zirkel und Lineal.

Aufgabe 0.6. Stellt euch vor, ihr seid am Fachbereich Mathematik der TU Kaiserslautern angestellt und bekommt einen Brief von einem Hobbymathematiker, der den Unmöglichkeitbeweis der Würfelverdoppelung mit Zirkel und Lineal nicht versteht und meint, doch eine Lösung gefunden zu haben. Er schreibt:

Es sei \overline{AB} die gegebene Kantenlänge des ursprünglichen Würfels. Konstruiere den Punkt C so, dass ABC ein gleichseitiges Dreieck ist. Nun sei $D \neq B$ der Punkt auf der Geraden AB mit $\overline{AD} = \overline{AB}$. Vervollständige die Strecken \overline{BD} und \overline{CD} zu einem Parallelogramm $BDCE$. Nun zeichne eine Gerade durch C so, dass $\overline{FG} = \overline{AB}$, wobei F und G die Schnittpunkte dieser Geraden mit AB und BE bezeichnen. Wie man leicht nachrechnet ist dann $\overline{CG} = \sqrt[3]{2} \cdot \overline{AB}$ die gesuchte Kantenlänge des Würfels mit dem doppelten Volumen.



Was schreibt ihr ihm zurück? Liefert seine Konstruktion überhaupt die richtige Lösung, d. h. stimmt es wirklich dass $\overline{CG} = \sqrt[3]{2} \cdot \overline{AB}$? Wenn ja, widerspricht seine Konstruktion dann nicht der in Problem 0.3 (B) angegebenen Unmöglichkeitssage?