JOCHEN HEINLOTH

ALGEBRA

Inhaltsverzeichnis

Einleitung

Diese Notizen sind nicht als Skript gedacht, sondern eher als Hilfestellung zur Erinnerung an die Vorlesung. Während des Semesters ist es schwierig, zusätzlich zur Vorlesung ein Buch zu schreiben – Sie können gerne einmal versuchen selbst eine Vorlesung im Computer aufzuschreiben, dann sehen Sie vielleicht, was ich meine – daher werden Sie hier auch mehr Tippfehler finden als mir lieb ist.

Hinweise zu Fehlern und Tippfehlern nehme ich gerne entgegen, zum Beispiel per email oder das Moodle-Forum.

Als Literaturquellen finden Sie in der Bibliothek viele Bücher mit dem Titel „Algebra" viele davon sind online verfügbar, beispielsweise die Bücher seien hier die Bücher von Bosch [1]*, Chambert-Loir* [2] *und Cox* [3] *genannt, in die ich gerne hineinschaue. Zudem gibt es eine Vielzahl von Skripten, zum Beispiel von den Autoren, die Sie in der Linearen Algebra schon kennen gelernt haben, Ulrich Görtz* [4]*, Wolfgang Soergel* [5]*, vielleicht gefällt Ihnen auch das Skript von Lukas Pottmeyer* [6]*.*

Sie werden sehen, dass die Quellen fast den gleichen Inhalte umfassen, aber unterschiedlich erklären, welche Darstellung Ihnen persönlich am leichtesten zugänglich ist, wird von Ihren Vorlieben und Vorkenntnissen abhängen.

Nachdem der Ausgangspunkt der linearen Algebra die Lösung linearer Gleichungssysteme war, ist der Ausgangspunkt für die Algebra die Suche nach Lösungen von nicht-linearen Gleichungen. Es ist dabei noch nützlicher als in der linearen Algebra, das Rechnen mit Buchstaben ernst zu nehmen; in dem Sinne, dass wir dem Rechnen mit Symbolen einen eigenständigen Sinn geben, ohne bei Variablen nur an Platzhalter für „Zahlen" zu denken.

Bei den komplexen Zahlen haben Sie das bei der Zahl i schon gesehen. Dieser Gesichtspunkt hat sich nach und nach immer stärker als nützlich erwiesen, weil uns die damit einhergehende etwas abstraktere Sprache ermöglicht, einige kompliziert aussehende Probleme in den Griff zu bekommen.

Ich habe in der Vorlesung zweierlei Ziele. Einerseits möchte ich Ihnen erklären, wie Algebra einige klassische Probleme recht einfach lösen kann. Beispielsweise kennen Sie sicher die Redewendungen von der „Quadratur des Kreises", vielleicht wissen Sie auch, dass es irgendein Problem bei der „Dreiteilung eines Winkels" gibt, oder Sie haben schon einmal gehört, dass es angeblich im Gegensatz zu quadratischen Gleichungen für Polynome 5ten Grades keine Lösungsformel gibt.

[1] Siegfried Bosch. *Algebra*. Springer Spektrum, Berlin, 2020. URL `https://doi.org/10.1007/978-3-662-61649-9`

[2] Antoine Chambert-Loir. *A field guide to algebra*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2005. URL `https://doi.org/10.1016/s0012-365x(05)00124-x`

[3] David A. Cox. *Galois theory*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2012. ISBN 978-1-118-07205-9. URL `https://doi.org/10.1002/9781118218457`

[4] Ulrich Görtz. Algebra. Vorlesungsskript, 2022. URL `https://math.ug/lecture-notes.html`

[5] Wolfgang Soergel. Algebra und zahlentheorie. Vorlesungsskript, 2022. URL `http://home.mathematik.uni-freiburg.de/soergel/Skripten/XXAL.pdf`

[6] Lukas Pottmeyer. Algebra. Vorlesungsskript, 2015. URL `https://www.esaga.uni-due.de/f/lukas.pottmeyer/Algebra_Skript.pdf`

Ein erstes Ziel der Vorlesung ist, zu verstehen, was es mit diesen Fragen auf sich hat. Für einige davon brauchen wir wenig mehr als lineare Algebra, für andere dann wirklich neue Werkzeuge.

Die neuen Werkzeuge sind dabei das zweite Ziel und der eigentliche Grund, wieso die Algebra für die Mathematik so wichtig geworden ist. Das Hauptresultat der Vorlesung – die sogenannte Galois-Korrepondenz – erklärt auf sehr elegante Weise einerseits, wie sich eine Frage, die in der Sprache von Lösungen von Gleichungen schwer erklärbar aussieht eine äquivalente Formulierung in Termen der Struktur der Menge aller Symmetrien des Problems – der Galoisgruppe – hat. Das sieht zunächst abstrakter aus, lässt sich aber viel leichter angreifen.

Dieses Resultat erklärt die Struktur der oben erwähnten klassischen Probleme recht schön und hat darum in vielen Bereichen der Mathematik Anwendungen gefunden: Dass einer der ersten Reflexe in der Mathematik mittlerweile ist, zunächst nach den Symmetrien von Problemen zu suchen und diese zu verstehen, habe ich schon erwähnt. Es gibt sowohl in der Geometrie als auch beim Studium von Differentialgleichungen Versionen der Galois-Korrespondenz, die umgekehrt auch erklären, dass wir über Körper geometrisch nachdenken können, was Sie hoffentlich überrascht.

Schließlich lassen sich viele der offenen Fragen der Zahlentheorie in Termen von Galoisgruppen formulieren. Wenn Sie in die Liste der verschiedenen Jahrgänge von Fields-Medallien schauen, werden Ihnen sehr häufig Gruppen und Galoisgruppen begegnen, spätestens wenn Sie die Mathematik hinter den Auszeichnungen anschauen. Am Ende der Vorlesung ist hoffentlich Zeit für einen Ausblick in eine dieser Richtungen.

Von Konstruktionen mit Zirkel und Lineal zu Körpererweiterungen

Zum Einstieg möchte ich erklären wieso die Frage welche Zahlen (bzw. welche Längen und Winkel) sich mit Zirkel und Lineal konstruieren lassen ein Anlass ist, um Zahlbereichserweiterungen anzuschauen. Diese sind insbesondere Vektorräume und lineare Algebra erklärt uns dann mittels einer Dimensionsformel recht schnell ein Hindernis dafür zum Beispiel $\sqrt[3]{2}$ zu konstruieren. Ein Trick wird dabei sein, $\sqrt[3]{2}$ einmal wie die komplexe Zahl i einfach als Symbol sagen wir a mit einer Rechenregel (in diesem Fall $a^3 = 2$) zu betrachten, statt an die Stelle auf der Zahlengerade zu denken.

Keine Sorge, wir werden zwar einige grundlegende Konstruktionen explizit sehen, aber nur wenige Knobelaufgaben mit komplizierten Konstruktionen lösen.

Wie formalisieren wir was Konstruktionen mit Zirkel und Lineal sind? Wir betrachten die Ebene $\mathbb{R}^2 = \mathbb{C}$ als komplexe Zahlenebene und schreiben Punkte entsprechend entweder als $z = a + ib$ oder als Punkt mit Koordinaten $P = (a, b)$.

Gegeben eine Menge von Punkten $M \subseteq \mathbb{C} = \mathbb{R}^2$, die $\{0, 1\}$ enthält, zum Beispiel $M = \{0, 1\}$, so erlauben uns Zirkel und Lineal aus M wie folgt neue Punkte zu konstruieren:

1. (Geraden schneiden) Gegeben 4 Punkte $A, B, C, D \in M$, so können wir den Schnittpunkt P der Geraden AB und CD mit dem Lineal konstruieren.

2. (Gerade und Kreis schneiden) Gegeben 5 Punkte $A, B, C, D, E \in M$ so können wir die Schnittpunkte der Geraden AB mit dem Kreis mit Mittelpunkt C und Radius $\overline{DE}$ konstruieren.

3. (Kreise schneiden) Gegeben 6 Punkte $A, B, C, D, E, F \in M$, so können wir die Schnittpunkte der Kreise mit Mittelpunkten A und B und Radien $\overline{CD}, \overline{EF}$ konstruieren.

Bemerkung. Es gibt relativ viele Varianten der erlaubten Konstruktionen, manche Quellen sind etwas strikter bei den erlaubten Konstruktionen, das führt aber zu den gleichen Ergebnissen, nur mit längeren Bastelanleitungen.

Definition 1 (Konstruierbare Zahlen)**.** Wir sagen, dass sich eine komplexe Zahl *zmit Zirkel und Lineal aus der Menge M konstruieren lässt*, wenn z durch eine Folge der oben angegebenen Konstruktionen konstruiert werden kann. Die Menge der *aus M konstruierbaren Zahlen* bezeichnen wir mit $\mathcal{C}(M)$, für $M = \{0, 1\}$ nennen wir $\mathcal{C}(\{0.1\}) = \mathcal{C}$ auch die *Menge der konstruierbaren Zahlen*.

Algebra in Geometrie übersetzen

Damit wir in der Algebra ankommen, sollten wir uns zunächst davon zu überzeugen, dass wir mit Zirkel und Lineal die Grundrechenarten und Wurzeln konstruieren können.

Ich gebe zunächst eine Liste von Behauptungen an, um Sie dazu zu ermuntern, selbst nachzudenken, wie Sie die entsprechende Operation vielleicht konstruieren könnten. Das macht mehr Spaß, als gleich die Antwort zu sehen.

Behauptung 2 (Rechen mit Zirkel und Lineal). *Sei $M \subset \mathbb{C}$ eine Teilmenge, die $\{0, 1\}$ enthält.*

1. *(Addition von reellen Zahlen) Sind reelle Zahlen $a, b \in \mathbb{R}$ in $\mathcal{C}(M)$, so auch $a + b$ und $a - b$.*

2. *(Multiplikation von reellen Zahlen) Sind reelle Zahlen $a, b \in \mathbb{R}$ in $\mathcal{C}(M)$, so auch $a \cdot b$.*

3. *(Division) Ist eine reelle Zahl $a \neq 0$ in $\mathcal{C}(M)$ so auch $\frac{1}{a}$.*

4. *(Wurzeln) Ist eine reelle Zahl $a \neq 0$ in $\mathcal{C}(M)$ so auch $\sqrt{a}$.*

5. *(Real und Imaginärteil) Eine komplexe Zahl $z = a + ib$ ist genau dann konstruierbar wenn a, b konstruierbar sind.*

Die konstruierbaren Zahlen $\mathcal{C}(M) \subseteq \mathbb{C}$ sind also insbesondere ein Körper, der $\mathbb{Q}$ und $\mathbb{Q}(i) := \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$ enthält.

Aufgabe. Zeigen Sie, dass in der Behauptung auch gilt:

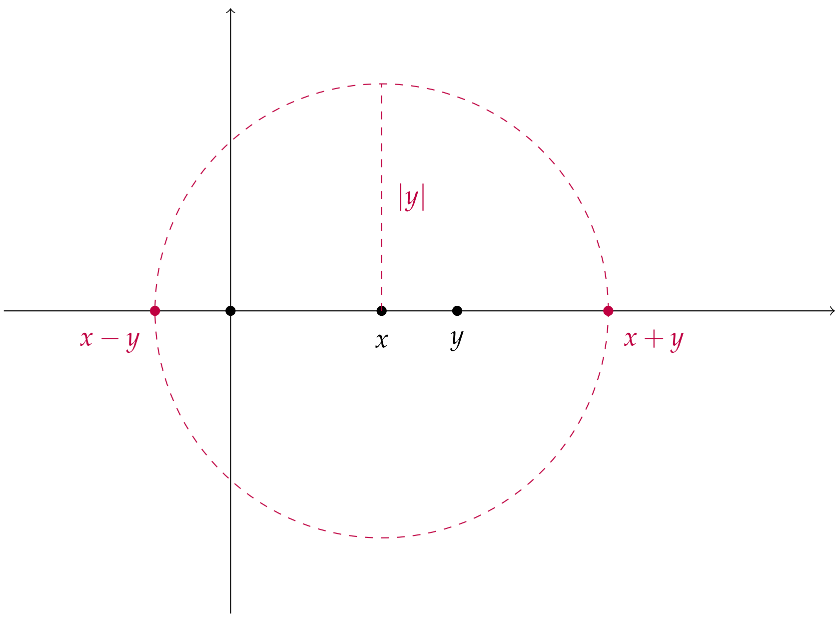
1'. (Addition von komplexen Zahlen) Sind komplexe Zahlen $a, b \in \mathbb{C}$ in $\mathcal{C}(M)$, so auch $a + b$ und $a - b$.

2'. (Multiplikation von komplexen Zahlen) Sind komplexe Zahlen $a, b \in \mathbb{C}$ in $\mathcal{C}(M)$, so auch $a \cdot b$.

VERSUCHEN SIE BITTE EINMAL SELBST herauszufinden, wie sich einige der oben genannten Zahlen konstruieren lassen bevor Sie umblättern!

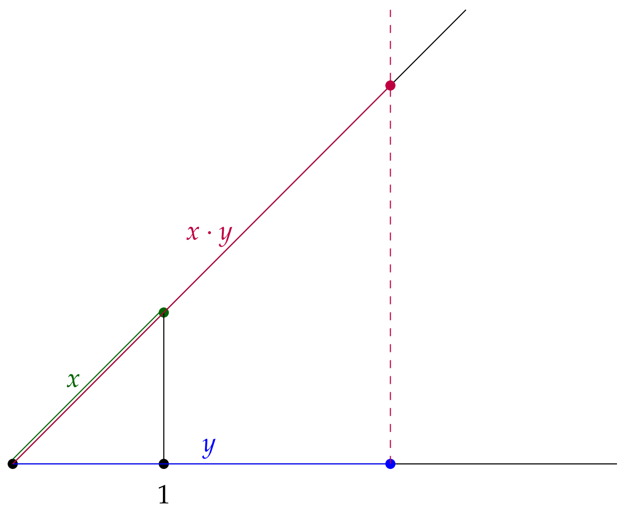
Skizzen für die Konstruktionen.

1. (Addition)

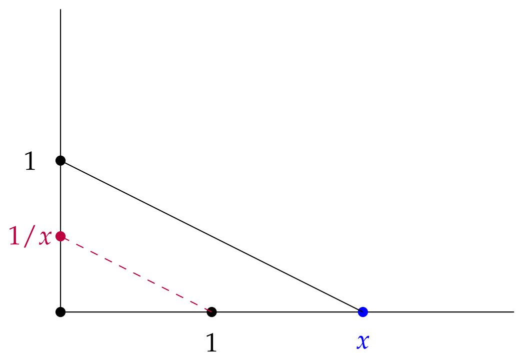


2. (Multiplikation)

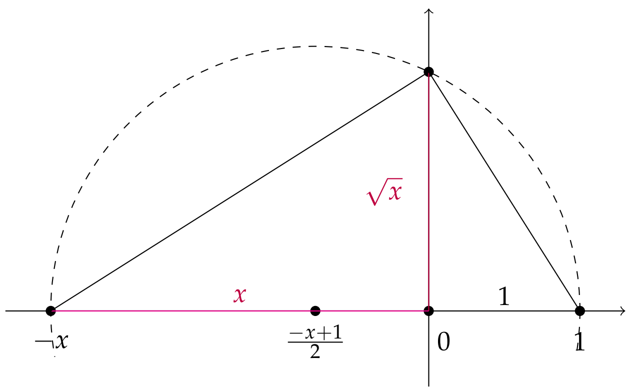
In dieser Konstruktion verwenden wir, dass wir mit Zirkel und Lineal die Parallele einer Gerade, durch einen beliebigen gegebenen Punkt konstruieren können. Können Sie sich überlegen, Sie wie das geht?



3. (Division – $1/x$)



4. (Wurzel) Vielleicht kennen Sie aus der Schule noch den Höhensatz, der die Länge der eingetragenen Höhe des rechtwinkligen Dreiecks in der Skizze berechnet.



Falls nicht, sollten Sie diese Höhe einmal selbst ausrechnen, das geht auf viele Arten: Wenn Sie am liebsten Rechnen, können Sie den Satz des Pythagoras auf alle rechtwinkligen Dreiecke in der Skizze anwenden, wenn Sie lieber geometrisch argumentieren, können Sie die Seitenverhältnisse ähnlicher Dreiecke vergleichen. □

Geometrie in Algebra übersetzen

UMGEKEHRT können wir für alle mit Zirkel und Lineal möglichen Konstruktionen jeweils Formeln für die Koordinaten der Schnittpunkte aufstellen, in denen nur die Grundrechenarten und Wurzeln vorkommen, denn Geraden sind durch lineare Gleichungen und Kreise durch quadratische Gleichungen gegeben:

1. Für den Schnittpunkt zweier Geraden

$$\begin{aligned} a_1x + b_1y &= c_1 \\ a_2x + b_2y &= c_2 \end{aligned}$$

haben wir in der linearen Algebra eine Formel gefunden.

2. Ist

$$\begin{aligned} L &= \{(x,y) \in \mathbb{R}^2 \mid ax + by = c\} \text{ eine Gerade und} \\ K_r(P) &= \{(x,y) \in \mathbb{R}^2 \mid (x-x_0)^2 + (y-y_0)^2 = r^2\} \end{aligned}$$

ein Kreis mit Radius r um $P = (x_0, y_0)$, so sind die Koordinaten der Schnittpunkte als Nullstellen eines quadratischen Polynoms bestimmt. Diese lassen sich mit einer Wurzel ausrechnen.

3. Das Gleiche gilt für zwei Kreise, denn für zwei Kreisgleichungen

$$\begin{aligned} (x-x_0)^2 + (y-y_0)^2 &= r_0^2 \\ (x-x_1)^2 + (y-y_1)^2 &= r_1^2 \end{aligned}$$

ist die Differenz der Gleichungen linear, weil die quadratischen Terme für beide Kreise x^2 und y^2 sind. Das führt die Berechnung des Schnitts auf die Rechnung unter 2. zurück.

Aufgabe. Wenn Sie geometrisch zwei Kreise schneiden, sehen Sie, dass die Verbindungsgerade der Schnittpunkte senkrecht auf der Verbindungsgeraden der Mittelpunkte liegt. Überlegen Sie sich mit Hilfe der linearen Algebra einmal, dass die Geradengleichung, die wir in 3. gefunden haben tatsächlich eine Gerade beschreibt, die senkrecht auf $\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} - \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$ steht.

Wir haben also gesehen, dass wir den Körper der konstruierbaren Zahlen aus den rationalen Zahlen erhalten können, indem wir zu den rationalen Zahlen induktiv Wurzeln hinzufügen. Wie bei den komplexen Zahlen ist aber für einen Körper $K \subset \mathbb{C}$ und $x \in K$ mit $\sqrt{x} \in \mathbb{C}$, $\sqrt{x} \notin K$ die Menge

$$K(\sqrt{x}) := \{a + b\sqrt{x} \mid a, b \in K\} \subseteq \mathbb{C}$$

wieder ein Körper, denn die Menge ist sicher ein 2-dimensionaler K-Vektorraum und es gilt

$$(a + b\sqrt{x}) \cdot (c + d\sqrt{x}) = (ac + bdx) + (ad + bc)\sqrt{x} \in K(\sqrt{x})$$

und

$$\begin{aligned} \frac{1}{a + b\sqrt{x}} &= \frac{a - b\sqrt{x}}{(a + b\sqrt{x})(a - b\sqrt{x})} \\ &= \frac{a - b\sqrt{x}}{(a^2 - b^2 x)} \\ &= \frac{a}{(a^2 - b^2 x)} - \frac{b}{(a^2 - b^2 x)}\sqrt{x} \in K(\sqrt{x}) \quad \text{falls } (a, b) \neq (0, 0). \end{aligned}$$

Definition 3 (Körpererweiterungen)**.** Eine *Körpererweiterung* eines Körpers K ist ein Körper L, der K enthält, d.h. $K \subseteq L$ und die Verknüpfungen $+, \cdot$ von L stimmen auf K mit den Rechenoperationen auf K überein.

Beispiel 4.

1. Sie kennen die Körpererweiterungen $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ und gerade haben wir auch $\mathbb{Q} \subseteq \mathbb{Q}(i)$ und $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ kennengelernt.

2. Ist $M \subset \mathbb{C}$ eine Teilmenge, so bezeichnen wir mit $\mathbb{Q}(M) \subset \mathbb{C}$ den kleinsten Teilkörper von $\mathbb{C}$ der $\mathbb{Q}$ und M enthält.

   Das sind alle komplexen Zahlen z, die sich als Quotienten $\frac{p(m_1,\ldots,m_r)}{q(m'_1,\ldots,m'_\ell)}$ schreiben lassen, wobei $m_i, m'_i \in M$ und $p \in \mathbb{Q}[x_1, \ldots, x_r], q \in \mathbb{Q}[x_1, \ldots, x_\ell]$ Polynome mit Koeffizienten in $\mathbb{Q}$ sind.

   Für jedes M ist $\mathbb{Q} \subseteq \mathbb{Q}(M)$ eine Körpererweiterung.

Da wir gesehen haben, dass wir konstruierbare Zahlen alle induktiv durch die Grundrechenarten und Wurzelziehen beschreiben können, ergibt sich die folgende Charakterisierung konstruierbarer Zahlen in Termen von Körpererweiterungen.

Satz 5 (Charakterisierung konstruierbarer Zahlen). *Eine Zahl $z \in \mathbb{C}$ ist genau dann mit Zirkel und Lineal aus $M \subset \mathbb{C}$ konstruierbar (d.h. $z \in \mathcal{C}(M)$), wenn es eine Kette von Körpererweiterungen*

$$\mathbb{Q}(M) = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n$$

gibt so dass für alle $i = 1, \ldots, n$ der Körper $K_i = K_{i-1}(\sqrt{x_i})$ für ein $x_i \in K_{i-1}$ ist.

Diese Aussage sieht zunächst nicht so aus, als ob das hilfreich wäre, um von einer Zahl zu entscheiden, ob diese konstruierbar ist. Lineare Algebra hilft uns hier aber noch einmal weiter, indem wir uns überlegen, dass die Aussage, dass die Erweiterungen $K_{i-1} \subset K_i$ jeweils 2-dimensionale K_{i-1}-Vektorräume sind, die Dimension von K_n als K_1-Vektorraum bestimmt.

Behauptung 6 (Multiplikativität der Dimension). *Sind $K_1 \subseteq K_2 \subseteq K_3$ Körpererweiterungen, so gilt*

$$\dim_{K_1} K_3 = \dim_{K_1} K_2 \cdot \dim_{K_2} K_3.$$

Beweis. Wir beweisen die Aussage für den Fall, dass die Dimensionen jeweils endlich sind. Wenn Sie den Beweis in diesem Fall verstanden haben, sehen Sie auch, dass im Fall, dass eine der vorkommenden Dimensionen unendlich sein sollte, auf beiden Seiten der Gleichung eine der Dimensionen unendlich sein muss.

Sei $x_1, \ldots, x_n \in K_2$ eine Basis des K_1-Vektorraums K_2 und $y_1, \ldots, y_m \in K_3$ eine Basis des K_2-Vektorraums K_3.

Dann behaupte ich, dass die Menge $\{x_i y_j\}_{\substack{i=1,\ldots n\\ j=1,\ldots m}}$ eine Basis des K_1-Vektorraums K_3 ist.

1. Die Menge ist ein Erzeugendensystem, denn jedes Element $v \in K_3$ lässt sich nach Voraussetzung als K_2-Linearkombination

$$v = \sum_{j=1}^{m} b_j y_j$$

mit $b_j \in K_2$ schreiben und jedes $b_j \in K_2$ lässt sich als K_1-Linearkombination

$$b_j = \sum_{i=1}^{n} a_{ij} x_i$$

schreiben. Also ist

$$\begin{aligned} v &= \sum_{j=1}^{m} b_j y_j \\ &= \sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij} x_i y_j. \end{aligned}$$

2. Die Menge ist linear unabhängig, denn ist

$$\sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij} x_i y_j = 0,$$

so ist

$$\sum_{j=1}^{m} \underbrace{\Big(\sum_{i=1}^{n} a_{ij}x_i\Big)}_{=:b_j\in K_2} y_j = 0$$

eine K_2-Linearkombination. Da die y_j aber eine Basis des K_2-Vektorraums K_3 sind, muss also

$$\Big(\sum_{i=1}^{n} a_{ij}x_i\Big) = b_j = 0 \text{ für alle } j$$

gelten und da die x_i eine Basis des K_1-Vektorraums K_2 sind, ist dann auch $a_{ij} = 0$ für alle i, j.

$\square$

Die Formel wird etwas übersichtlicher wird wenn wir

$$[L : K] := \dim_K L$$

abkürzen, denn dann gilt also

$$[K_3 : K_1] = [K_3 : K_2] \cdot [K_2 : K_1].$$

Die Dimension der Körpererweiterung heißt auch *Grad*, wir werden noch sehen woher der Name kommt.

Definition (Grad einer Körpererweiterung)**.** Ist $K \subset L$ eine Körpererweiterung, so heißt

$$\dim_K L =: [L : K]$$

der *Grad* der Körpererweiterung.

Ausblick: Wir können und jetzt leicht überlegen, dass $\sqrt[3]{2}$ nicht mit Zirkel und Lineal konstruierbar ist:

1. Für den Körperturm $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n$ aus der Charakterisiserung konstruierbarer Zahlen gilt $\dim_{\mathbb{Q}} K_n = 2^n$ und darum gilt auch für alle Teilkörper $\mathbb{Q} \subset L \subset K_n$, dass $\dim_{\mathbb{Q}} L$ ein Teiler von 2^n ist, also $\dim_{\mathbb{Q}} L = 2^m$ für ein $m \leq n$.

2. Wenn wir jetzt zeigen können, dass

$$\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = 3$$

gilt. So wäre $[\mathbb{Q}(\sqrt[3]{2}]$ kein Teiler von 2^n und darum $\sqrt[3]{2} \notin \mathcal{C}$ nicht konstruierbar.

Wir sollten uns also überlegen, dass $1, \sqrt[3]{2}, \sqrt[3]{2}^2$ Zahlen sind, die $\mathbb{Q}$-linear unabhängig sind. Dafür finde ich es hilfreich, mich zunächst – wie bei den komplexen Zahlen – auf den Standpunkt zu stellen, dass ich $\alpha = \sqrt[3]{2}$ zunächst als Symbol betrachten möchte, für das ich nur die Rechenregel $\alpha^3 = 2$ festlege. Wir wissen schon, wie wir das mit Hilfe einer Äquivalenzrelation, bzw. mit Quotientenvektorräumen formalisieren können: Wir führen auf dem Polynomring $\mathbb{Q}[x]$ die Äquivalenzrelation

$$\begin{aligned} a(x) \sim_{\sqrt[3]{2}} b(x) :\Leftrightarrow b(x) &= a(x) + m(x) \cdot (x^3 - 2) \\ &\text{für ein } m(x) \in \mathbb{Q}[x] \end{aligned}$$

ein und betrachten

$$K := \mathbb{Q}[x]/\sim_{\sqrt[3]{2}}.$$

Das ist gleichbedeutend damit, dass wir in $\mathbb{Q}[x]$ den Untervektorraum der Vielfachen von $x^3 - 2$

$$(x^3 - 2) := \{p(x) \cdot (x^3 - 2) \mid p(x) \in \mathbb{Q}[x]\}$$

betrachten und dazu den Quotientenraum

$$\mathbb{Q}[x]/(x^3 - 2) \cong \mathbb{Q}[x]/\sim_{\sqrt[3]{2}}$$

bilden. Dafür möchte ich mir jetzt gerne die folgenden Dinge überlegen:

1. $\mathbb{Q}[x]/(x^3 - 2)$ ist ein 3-dimensionaler $\mathbb{Q}$-Vektorraum mit Basis $[1], [x], [x^2]$.

2. Das Argument das wir verwendet hatten, um uns zu überlegen, dass $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, liefert und auch, dass $K = \mathbb{Q}[x]/(x^3 - 2)$ ein Körper ist.

3. Der Körper $K = \mathbb{Q}[x]/(x^3 - 2)$ ist eine andere Beschreibung von $\mathbb{Q}(\sqrt[3]{2})$, genauer ist die Abbildung

$$\begin{aligned} A\colon \mathbb{Q}[x]/(x^3 - 2) &\to \mathbb{Q}(\sqrt[3]{2}) \\ [a(x)] &\mapsto a(\sqrt[3]{2}) \end{aligned}$$

ein Isomorphismus.

Erinnerung: Euklidischer Algorithmus für Polynome

In der linearen Algebra hatten wir uns mittels Polynomdivision überlegt, dass wir Polynome mit Rest Teilen können.

Satz 7 (Teilen mit Rest für Polynome). *Sind $a(x), b(x) \in K[x]$ Polynome mit Koeffizienten in einem Körper K, so existieren eindeutige Polynome $q(x), r(x) \in K[x]$ mit $\mathrm{Grad}(r(x)) < \mathrm{Grad}(a(x))$ so dass*

$$b(x) = q(x) \cdot a(x) + r(x).$$

Beispiel: Für $b(x) = 3x^4 + 2x + 1$ und $a(x) = x^2 - 2$, ist

$$\begin{aligned} &(3x^4 + 2x + 1) - 3x^2 \cdot (x^2 - 2) \\ &= 3x^4 + 2x + 1 - (3x^4 - 6x^2) \\ &= 6x^2 + 2x + 1 \end{aligned}$$

Das Ergebnis hat Grad $= 2 \geq \text{Grad}(a(x)$ also weiter:

$$\begin{aligned}
&(6x^2 + 2x + 1) - 6 \cdot (x^2 - 2) \\
&= 6x^2 + 2x + 1 - 6x^2 + 12 \\
&= 2x + 13.
\end{aligned}$$

Also ist

$$b(x) = (3x^2 + 6)a(x) + 2x + 13.$$

Das können wir als Polynomdivision auch so schreiben:

$$\begin{array}{rrrl}
3x^4 & + 2x & + 1 & = \left(x^2 - 2\right)\left(3x^2 + 6\right) + 2x + 13. \\
\underline{-\,3x^4 + 6x^2} & & & \\
6x^2 & + 2x & + 1 & \\
\underline{-\,6x^2} & & \underline{+\,12} & \\
 & 2x & + 13 &
\end{array}$$

Glossar mathematischer Symbole und Begriffe

Literaturverzeichnis

Siegfried Bosch. *Algebra*. Springer Spektrum, Berlin, 2020. URL https://doi.org/10.1007/978-3-662-61649-9.

Antoine Chambert-Loir. *A field guide to algebra*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2005. URL https://doi.org/10.1016/s0012-365x(05)00124-x.

David A. Cox. *Galois theory*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2012. ISBN 978-1-118-07205-9. URL https://doi.org/10.1002/9781118218457.

Ulrich Görtz. Algebra. Vorlesungsskript, 2022. URL https://math.ug/lecture-notes.html.

Lukas Pottmeyer. Algebra. Vorlesungsskript, 2015. URL https://www.esaga.uni-due.de/f/lukas.pottmeyer/Algebra_Skript.pdf.

Wolfgang Soergel. Algebra und zahlentheorie. Vorlesungsskript, 2022. URL http://home.mathematik.uni-freiburg.de/soergel/Skripten/XXAL.pdf.