JOCHEN HEINLOTH

ALGEBRA

Inhaltsverzeichnis

Vorwort

Im Wintersemester 2023/24 habe ich im Anschluss an die Grundvorlesungen einmal wieder die Vorlesung „Algebra“ gehalten. Dabei habe ich die Reihenfolge der Vorlesungsinhalte im Vergleich zu den üblichen Quellen etwas verändert. Da das einerseits sowohl die Anzahl der Teilnehmenden als auch die Ergebnisse in der Abschlussklausur sehr positiv beeinflusst hat, aber andererseits auf den ersten Blick weniger strukturiert als die Standardbücher zur Vorlesung erscheinen mag, möchte ich den Grund für diese Umordnung hier kurz erklären.

Für mich ist Algebra eine besonders schöne Vorlesung, weil hier einige ganz naheliegende Grundfragen zu Zahlen und der Lösbarkeit von Gleichungen, die auf den ersten Blick schwer zu fassen sind, in moderner Sprache plötzlich sehr klare Antworten finden und darüber hinaus die Techniken, die dafür entwickelt wurden, für erstaunlich viele andere Fragestellungen nützlich geworden sind. Außerdem ist in der Algebra der Schritt zu offenen Problemen an vielen Stellen klein.

In Gesprächen mit Studierenden und Kolleg:innen aus anderen Bereichen wurde mir leider der fast gegenteilige Eindruck vermittelt, dass Algebra eine besonders schwer zugängliche, abstrakte Vorlesung sei, bei der zudem nicht so klar wäre, wozu die ganze Theorie überhaupt gut ist.

Dass die Theoriebildung in der Wahrnehmung der Vorlesung oft einen so starken Schwerpunkt einnimmt, hat mich überrascht. Ein Blick in die deutschsprachigen Standardbücher zum Thema erklärt das Problem allerdings recht gut, denn hier steht in der Tat die Theoriebildung manchmal sehr im Vordergrund, was an die „Kunstaufräumen“ Bücher von Ursus Wehrli erinnern könnte.

Ich habe mir daher für die Vorlesung vorgenommen, das Prinzip mathematische Konzepte erst dann einzuführen, nachdem wir interessanten Beispielen begegnet sind, für diese Vorlesung beizubehalten. In dieser Reihenfolge fällte es mir leichter zu erklären, dass sich viele überraschende Resultate der Algebra schon mit sehr wenig Aufwand erklären lassen.

Meine Hoffnung ist, dass diese Herangehensweise nicht nur früher im Semester zu interessanten Ergebnissen führt, sondern gleichzeitig auch der Art, wie ich selbst über Mathematik nachdenke näher kommt. In meiner eigenen Arbeit sind immer offenen Fragen der Ausgangspunkt, neue Definitionen entstehen dabei nur selten

und wenn, dann immer langsam. Das Phänomen, dass eine Definition zu erst da ist und ich danach nach Beispielen suchen muss, ist mir selbst nur in mathematischen Texten, nie bei der eigenen Arbeit begegnet.

An einigen Stellen hatten die Studierenden in der Vorlesung dann noch den dringenden Wunsch, zunächst weitere Beispiele oder Anwendungen zu sehen. Darauf bin ich meist eingegangen, was dieses Skript allerdings etwas mehr durcheinander gebracht hat, als ursprünglich geplant war.

Um das etwas auszugleichen, habe ich am Ende der Kapitel kurz die entstandene Theorie zusammen gestellt. Eigentlich würde ich mir dabei wünschen, dass den Studierenden am Ende der Vorlesung die sortierte Darstellung in den Lehrbüchern zum Nachschlagen leichter zugänglich erscheint.

Die Bücher „Galois theory“[1] von D. Cox und „A field guide to algebra“[2] von A. Chambert-Loir verfolgen eine sehr ähnliche Herangehensweise wie diese Notizen und waren mir darum bei der Vorbereitung besonders nützlich.

Wie bei allen Skripten möchte ich mich bei all denjenigen bedanken, die mir mit Anregungen, Korrekturen und Gesprächen geholfen haben. Die Gespräche beim gemeinsamen Kaffee und die Rückmeldung der Studierenden waren mir eine große Hilfe. Viele der Korrekturen erreichten mich anonym über die Moodle-Seite, stellvertretend für alle diese Rückmeldunegn hier ein Dank an Herrn Lensing für die vielen Hinweise.

[1] 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

[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

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 am 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 über das Moodle-Forum.

Als Literaturquellen finden Sie in der Bibliothek viele Bücher mit dem Titel „Algebra", viele davon sind auch online verfügbar. Als Beispiele von Büchern zu Vorlesung seien hier die Bücher von Bosch [3], Chambert-Loir [4] und Cox [5] genannt, in die ich bei der Vorbereitung 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 [6], Wolfgang Soergel [7], vielleicht gefällt Ihnen auch das Skript von Lukas Pottmeyer [8]. Ich habe bei der Vorbereitung auch in den Skripten von Gerard van der Geer gelesen, die ich vor längerer Zeit als Grundlage für eine ähnliche Vorlesung verwendet hatte.

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

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

[4] 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

[5] 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

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

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

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

Worum geht es? 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 allgemeine Lösungsformel gibt.

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 Galoiskorrepondenz – erklärt auf sehr elegante Weise einerseits, wie sich eine Frage, die in der Sprache von Lösungen von Gleichungen schwer erklärbar aussieht, in eine äquivalente Frage in Termen der Struktur der Menge aller Symmetrien des Problems – der Galoisgruppe – übersetzen lässt. 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 Galoiskorrespondenz, die umgekehrt auch erklären, dass wir über Körper geometrisch nachdenken können, was Sie womöglich überrascht.

Diese Beobachtung hat es ins Kino geschafft: Im Film *„A beautiful mind“* erklärt jemand *„I believe I can show that Galois extensions are covering spaces“*. Die deutsche Synchronisation hat den Satz leider völlig entstellt.

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 eine Stelle irgendwo zwischen 1,2 und 1,3 auf der Zahlengeraden zu denken.

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

Konstruierbare Zahlen

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 z *mit 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:

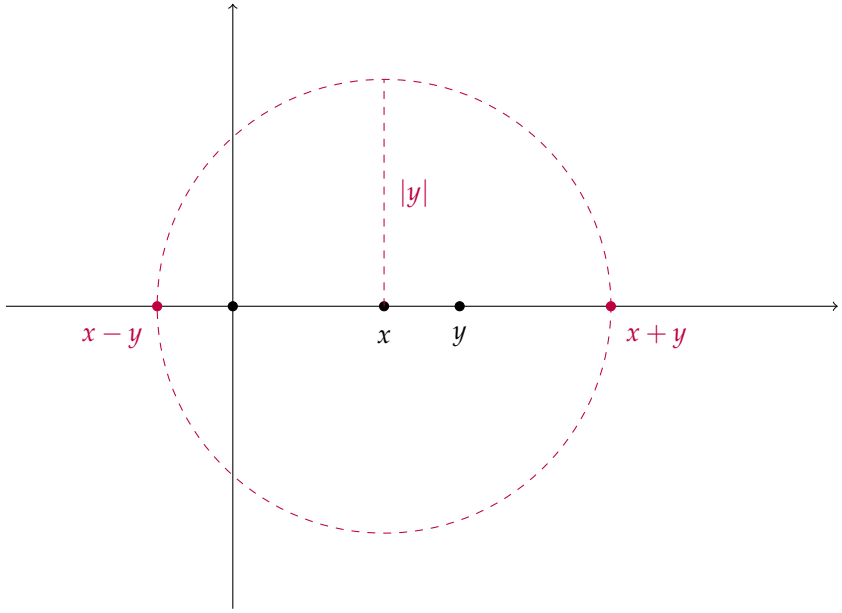
1′. (Addition von komplexen Zahlen) Sind komplexe Zahlen $a, b \in \mathbb{C}$ in $\mathcal{C}(M)$, so auch $a+b$ und $a-b$.

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!

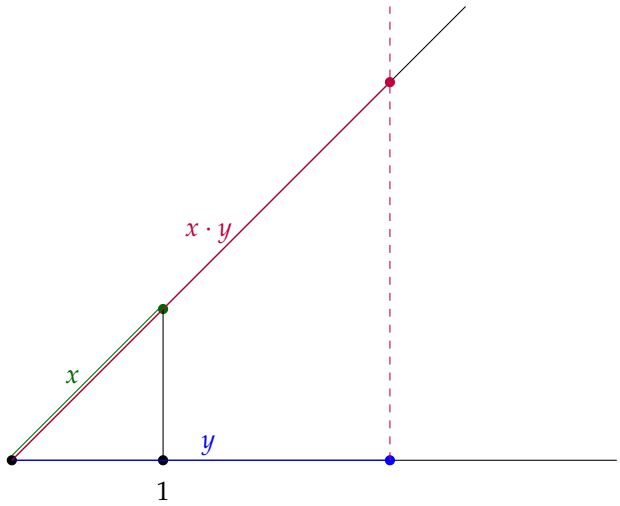
Skizzen für die Konstruktionen.

1. (Addition)

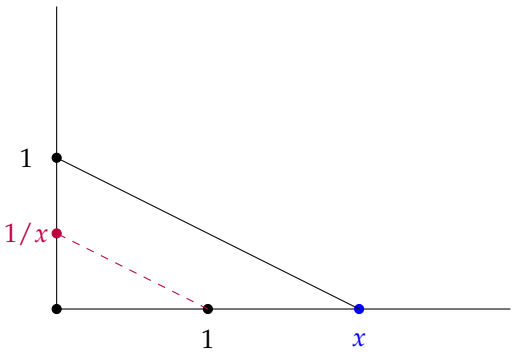


2. (Multiplikation)

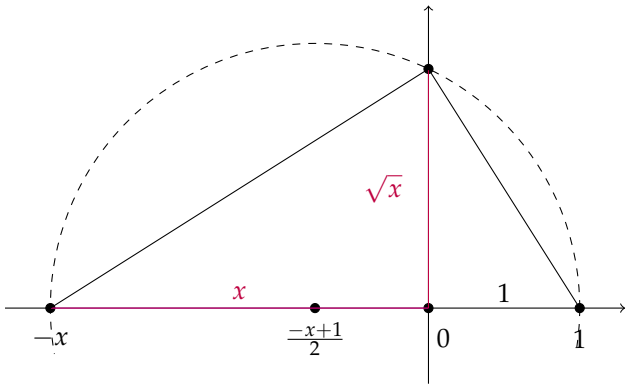
In dieser Konstruktion verwenden wir, dass wir mit Zirkel und Lineal die Parallele einer Gerade, durch einen beliebigen gegebenen Punkt konstruieren können. Können Sie sich überlegen, Sie wie das geht?



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

$$a_1x + b_1y = c_1$$
$$a_2x + b_2y = c_2$$

haben wir in der linearen Algebra eine Formel gefunden.

2. Ist

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

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

$$(x-x_0)^2 + (y-y_0)^2 = r_0^2$$
$$(x-x_1)^2 + (y-y_1)^2 = r_1^2$$

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

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

Hier ist außerdem $a^2 - b^2 x \neq 0$ denn sonst wäre $x = (\frac{a}{b})^2$ ein Quadrat.

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 $\mathbb{Q} \subset \mathbb{Q}(i)$ und $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ kennengelernt.

2. Ist $M \subset \mathbb{C}$ eine Teilmenge, so bezeichnen wir mit $\mathbb{Q}(M) \subseteq \mathbb{C}$ 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.

In der Vorlesung haben Sie gefragt, wieso wir hier plötzlich Brüche benötigen, obwohl das bei $K(\sqrt{x})$ nicht nötig war.

Die erste Antwort ist, dass wir für das Teilen in diesem Fall einen Trick verwendet haben, für den ich für allgemeine Zahlen zunächst keinen Ersatz sehe. Um sicher zu sein, dass wir wirklich einen Körper bekommen, nehmen wir daher die Quotienten einfach hinzu.

Wir werden darauf aber noch zurück kommen und sehen dass wir die Brüche genau dann wirklich brauchen, wenn eines der Elemente von M „transzendent“ ist, d.h. nicht als Nullstelle von Polynomen mit Koeffizienten in $\mathbb{Q}$ vorkommt.

Charakterisierung konstruierbarer Zahlen

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*

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

mit $z \in K_n$ 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. Für quadratische Erweiterungen ist das plausibel, denn

$$\begin{aligned} K(\sqrt{\alpha}) &= \{a + b\sqrt{\alpha} \mid a, b \in K\} \\ K(\sqrt{\alpha})(\sqrt{\beta}) &= \{c + d\sqrt{\beta} \mid c, d \in K(\sqrt{\alpha})\} \\ &= \{(a + b\sqrt{\alpha}) + (a' + b'\sqrt{\alpha})\sqrt{\beta} \mid a, b, a', b' \in K\} \\ &= \{a + b\sqrt{\alpha} + a'\sqrt{\beta} + b'(\sqrt{\alpha}\sqrt{\beta}) \mid a, b, a', b' \in K\}. \end{aligned}$$

Damit ist $1, \sqrt{\alpha}, \sqrt{\beta}, (\sqrt{\alpha}\sqrt{\beta})$ zumindest ein Erzeugendensystem dieses K-Vektorraums.

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 auf der rechten Seite der Gleichung jeweils endlich sind.

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.

Damit haben wir die Aussage für Fall, dass $\dim_{K_1} K_2$ und $\dim_{K_2} K_3$ endlich sind gezeigt. Ist $\dim_{K_1} K_2$ unendlich, so enthält K_2 eine unendliche Menge K_1-linear unabhängiger Vektoren, also gilt das erst recht für $K_3 \supseteq K_2$. Ist $\dim_{K_2} K_3$ unendlich, so enthält K_3 eine unendliche Menge K_2-linear unabhängiger Vektoren, die sind dann aber erst recht für K_1-linear unabhängig. Also ist für den Fall, dass die rechte Seite der Gleichung unendlich ist, auch die linke unendlich. □

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

Hinzufügen von Nullstellen

Wir sollten uns also überlegen, dass $1, \sqrt[3]{2}, \sqrt[3]{2}^2$ Zahlen sind, die über $\mathbb{Q}$-linear unabhängig sind. Das möchte ich mir gerne auf eine Art überlegen, die uns später noch weiter hilft, Sie können aber gerne versuchen, sich das einmal selbst direkt zu überlegen.

Ich finde es hierfür in jedem Fall hilfreich, mich zunächst – wie bei den komplexen Zahlen – auf den Standpunkt zu stellen, dass wir $\alpha = \sqrt[3]{2}$ zunächst als Symbol betrachten könnten, für das wir nur die Rechenregel $\alpha^3 = 2$ festgelegt haben. 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

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

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

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

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

1. $\mathbb{Q}[x]/(x^3 - 2)\mathbb{Q}[x]$ 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

$$K = \mathbb{Q}[x]/(x^3 - 2)\mathbb{Q}[x]$$

ein Körper ist.

In der Vorlesung hatten Sie noch gefragt, warum $\sqrt[3]{2} \notin \mathbb{Q}$ nicht rational ist. Das funktionert wie das Argument für $\sqrt{2}$ durch Widerspruch: Angenommen

$$\sqrt[3]{2} = \frac{a}{b}$$

wäre ein gekürzter Bruch, d.h. a, b sind teilerfremde ganze Zahlen, dann wäre

$$2 = (\sqrt[3]{2})^3 = \frac{a^3}{b^3}$$

also

$$2b^3 = a^3$$

und damit a^3 durch 2 teilbar und also $a = 2a'$. Dann ist aber

$$a^3 = 2^3 a'^3 = 2b^3,$$

d.h.

$$b^3 = 2^2 a'^3$$

und damit wie zuvor auch b durch 2 teilbar. Das ist ein Widerspruch zur Annahme, das a, b teilerfremd sind.

Das Argument funktioniert genauso für alle $n-$ten Wurzeln aus Primzahlen.

3. Der Körper $K = \mathbb{Q}[x]/(x^3-2)\mathbb{Q}[x]$ 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 $= 2 \geq \mathrm{Grad}(a(x)$ 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:

$$\begin{array}{rl} 3x^4 \quad + 2x \; + 1 = \Big(x^2 - 2\Big) \Big(3x^2 + 6\Big) + 2x + 13 \cdot \\ \underline{-\,3x^4 + 6x^2} \\ \quad 6x^2 + 2x \; + 1 \\ \underline{-\,6x^2 \qquad + 12} \\ \quad 2x + 13 \end{array}$$

Satz 8 (Euklidischer Algorithmus für Polynome)**.** *Sind $p(x), q(x) \in K[x]$ Polynome so existiert ein eindeutig bestimmter größter gemeinsamer Teiler $\mathrm{ggT}(p(x), q(x)) \in K[x]$, d.h. ein normiertes Polynom $\mathrm{ggT}(p, q)$, das*

1. *$p(x)$ und $q(x)$ teilt und*
2. *sich in der Form $\mathrm{ggT}(p, q) = n(x) \cdot p(x) + m(x) \cdot q(x)$ schreiben lässt.*

Ist insbesondere $d(x)$ ein anderes Polynom, das p, q teilt, so teilt es auch $\mathrm{ggT}(p, q)$.

Beweis. Das folgt genau wie der euklidische Algorithmus für ganze Zahlen aus der Division mit Rest. □

Folgerung 9. *Ist $p(x) \in K[x]$ ein nicht-konstantes, irreduzibles Polynom vom Grad d, so ist der Quotientenvektorraum*

$$K[x]/(p(x)) = K[x]/f \sim g \Leftrightarrow g = f + m \cdot p \text{ für ein } m \in K[x]$$

mit den Verknüpfungen

$$\begin{aligned} [a(x)] + [b(x)] &:= [a(x) + b(x)] \qquad \text{und} \\ [a(x)] \cdot [b(x)] &:= [a(x) \cdot b(x)] \qquad \text{für alle } a(x), b(x) \in K[x] \end{aligned}$$

eine Körpererweiterung von K, in der die Restklasse $\alpha := [x]$ eine Nullstelle des Polynoms p ist.

Der Grad dieser Körpererweiterung ist gleich dem Grad des Polynoms p:

$$\dim_K(K[x]/(p(x))) = [(K[x]/(p(x))) : K] = \operatorname{grad}(p).$$

Diese Aussage macht nur formal genau, was wir mit „wir führen für das Symbol x die Rechenregel $p(x) = 0$ ein“ meinen. Das Argument ist darum eigentlich nicht schwer.

Beweis. Zunächst haben wir die Konstruktion so gemacht, dass $\alpha = [x] \in K[x]/(p(x))$ tatsächlich eine Nullstelle von $p(t) = t^d + a_{d-1}t^{d-1} + \cdots + a_1 t + a_0$ ist, denn:

$$\begin{aligned} p([x]) &= [x]^d + a_{d-1}[x]^{d-1} + \cdots + a_1[x] + a_0 && \text{Einsetzen} \\ &= [x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0] && \text{Def. von } +, \cdot \\ &= [p(x)] = [0]. && \text{Def. von } [\ \ ] \end{aligned}$$

Die Aussage $\dim_K(K[x]/(p(x))) = \operatorname{grad}(p) = d$ gilt, weil wir jedes Polynom $a(x) \in K[x]$ eindeutig in der Form

$$a(x) = q(x) \cdot p(x) + r(x)$$

mit $\operatorname{grad}(r(x)) < d$ schreiben können. Darum ist $[a(x)] = [r(x)]$ für ein eideutiges Polynome vom Grad $< d$. Da der Raum der Polynome vom grad $< d$ die Basis $1, x, \ldots, x^{d-1}$ besitzt, sind die Restklassen dieser Elemente auch eine Basis von $K[x]/(p(x))$.

Die Verknüpfungen sind jeweils wohldefiniert: Das Argument hierfür ist genau das gleiche wie für die Operationen für $\mathbb{Z}/N\mathbb{Z}$ und ich möchte Sie daher bitten, sich das noch einmal selbst klar zu machen.

Bis auf die Existenz von multiplikativ inversen Elementen ergeben sich die Körperaxiome damit direkt aus den entsprechenden Eigenschaften der Addition und Multiplikation auf dem Polynomring $K[x]$.

Sei nun $[a(x)] \in K[x]/(p(x))$ eine Restklasse mit $[a(x)] \neq 0$, d.h. $a(x)$ ist nicht durch $p(x)$ teilbar. Für die Existenz eines inversen Elementes, können wir entweder wie zuvor argumentieren:

Da $p(x)$ irreduzibel ist, muss weil $p(x)$ das Polynom $a(x)$ nicht teilt:

$$\operatorname{ggT}(a(x), p(x)) = 1$$

In der Vorlesung hatten Sie um das Argument gebeten, daher hier noch einmal:

Nach Definition bedeutet

$$[\tilde{a}(x)] = [a(x)],$$

dass $\tilde{a}(x) = a(x) + n(x) \cdot p(x)$ für ein $n(x) \in K[x]$ und $[\tilde{b}(x)] = [b(x)]$ bedeutet, dass $\tilde{b}(x) = b(x) + m(x) \cdot p(x)$ für ein $m(x) \in K[x]$. Dann ist aber

$$\begin{aligned} &[\tilde{a}(x)] \cdot [\tilde{b}(x)] = [\tilde{a}(x) \cdot \tilde{b}(x)] \\ &= [(a(x) + n(x)p(x)) + (b(x) + m(x)p(x))] \\ &= [a(x) \cdot b(x) \\ &\quad + \underbrace{(a(x)m(x) + n(x)b(x) + n(x)m(x)p(x))p(x)}_{=[0]}] \\ &= [a(x) \cdot b(x)]. \end{aligned}$$

Also hängt das Resultat der Definition von $\cdot$ nicht von der Wahl der Rpräsentanten $a(x), b(x)$ ab.

gelten. Wir können also mit dem euklidischen Algorithmus $n(x), m(x) \in K[x]$ finden, für die

$$1 = \mathrm{ggT}(a(x), p(x)) = n(x)a(x) + m(x)p(x)$$

gilt. Damit ist

$$[1] = [n(x)][a(x)] + [m(x)p(x)] = [n(x)][a(x)] \in K[x]/(p(x))$$

und also $[n(x)]$ das gesuchte inverse Element.

Alternativ könnten wir mit linearer Algebra argumentieren. Die Abbildung

$$\begin{aligned} a(x)\cdot\colon K[x]/(p(x)) &\to K[x]/(p(x)) \\ [b(x)] &\mapsto [a(x)\cdot b(x)] \end{aligned}$$

ist K-linear und $\ker(a(x)\cdot) = \{0\}$ denn $[a(x)\cdot b(x)] = [0]$ bedeutet, dass das Produkt $a(x)\cdot b(x)$ durch $p(x)$ teilbar ist. Da $p(x)$ irreduzibel ist und $a(x)$ nicht teilt, muss $p(x)$ daher $b(x)$ teilen, also $[b(x)] = 0$ gelten. Also ist die Abbildung injektiv und da $\dim_K K[x]/(p(x)) = d$ endlich ist darum auch surjektiv, d.h. es gibt ein $[b(x)]$ mit $[a(x)\cdot b(x)] = [1]$. □

Bemerkung. Wir haben gerade für jeden Körper K eine Möglichkeit gefunden für ein beliebiges Polynom $f \in K[x]$, das in K keine Nullstelle hat, eine Körpererweiterung $K \subset L = K[x]/(p(x))$ zu konstruieren, in dem f eine Nullstelle hat: Wir können einfach für $p(x)$ einen irreduziblen Teiler von f wählen.

Um Nullstellen von Polynomen zu einem Körper hinzuzufügen, brauchen wir also nicht wie für $\mathbb{Q}$ das Glück, zufällig eine Körpererweiterung $K \subset C$ zu kennen, in der alle Polynome Nullstellen haben.

Bemerkung. In unserem Beispiel ist das Polynom $p(x) = x^3 - 2 \in \mathbb{Q}[x]$ irreduzibel, denn wenn wir $p(x) = a(x)\cdot b(x)$ in nicht konstante Polynome $a(x), b(x) \in \mathbb{Q}[x]$ faktorisieren könnten, müsste $\mathrm{Grad}(a) + \mathrm{Grad}(b) = \mathrm{Grad}(p) = 3$ gelten und also eines der beiden Polynome linear sein. Lineare Polynome haben aber Nullstellen und wir hatten und überlegt, dass $p(x)$ in $\mathbb{Q}$ keine Nullstelle besitzt.

Folgerung 10. *Ist $p(x) \in K[x]$ ein Polynom vom Grad 2 oder 3, so ist $p(x)$ in $K[x]$ irreduzibel, wenn p in K keine Nullstelle besitzt.*

ZURÜCK zu unserer Frage, wieso $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ ist. Auf den ersten Blick haben wir nicht viel gewonnen, weil wir jetzt noch zeigen müssen, dass unsere neue Methode eine Nullstelle von $x^3 - 2$ zu $\mathbb{Q}$ hinzu zu fügen wirklich $\mathbb{Q}(\sqrt[3]{2})$ liefert.

Das ist aber mit einem kleinen Trick gar nicht schwer, denn wir können eine Abbildung zwischen den beiden Körpern

$$\begin{aligned} F\colon \mathbb{Q}[x]/(x^3-2) &\to \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{C} \\ [x] &\mapsto F([x]) := \sqrt[3]{2} \qquad \text{und allgemein} \\ [a(x)] &\mapsto F([a(x)]) := a(\sqrt[3]{2}) \end{aligned}$$

definieren. Das ist wieder wohldefiniert da

$$F([a(x)+n(x)(x^3-2)]) = a(\sqrt[3]{2}) + n(\sqrt[3]{2})\underbrace{(\sqrt[3]{2}^3-2)}_{=0}$$
$$= a(\sqrt[3]{2}) = F([a(x)])$$

und die Abildung ist auch nach Konstruktion surjektiv und $\mathbb{Q}$-linear.

Besser noch: Die Abbildung ist mit $+$ und $\cdot$ verträglich, d.h.

$$F([a]+[b]) = F([a]) + F([b])$$
$$F([a]\cdot[b]) = F([a])\cdot F([b])$$
$$F([0]) = 0$$
$$F([1]) = 1.$$

Die Abbildungsvorschrift ist durch Einsetzen von $\sqrt[3]{2}$ definiert, also für $a, b \in \mathbb{Q}[x]$ als

$$F([a]+[b]) \overset{\text{Def } F}{=} (a+b)(\sqrt[3]{2}) \overset{\text{Def } a+b}{=} a(\sqrt[3]{2}) + b(\sqrt[3]{2}) \overset{\text{Def } F}{=} F([a]) + F([b]).$$

Daraus folgt, dass $\ker(F) = \{0\}$ (in der Vorlesung haben Sie selbst ein Argument dafür gefunden), da wenn $F([a]) = 0$ und $[a] \neq 0$ wäre, dann auch

$$F([1]) = F([a]\cdot[a]^{-1}) = \underbrace{F([a])}_{=0}\cdot F([a]^{-1})$$
$$= 0 \cdot F([a]^{-1}) = 0$$

gelten müsste, aber es ist $F([1]) = 1$.

Darum ist F bijektiv und also ist

$$\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = \dim_{\mathbb{Q}} \mathbb{Q}[x]/(x^3-2) = 3.$$

Damit ist $\sqrt[3]{2}$ nicht konstruierbar!

Das Argument dafür, dass F injektiv ist hat nur verwendet, dass F mit den Körpereigenschaften verträglich war. Da das noch nützlich sein wird, möchte ich das kurz festhalten.

Definition. Ein *Körperhomomorphismus* ist eine Abbildung

$$F\colon K \to L$$

von Körpern K, L so dass für alle $a, b \in K$ gilt, dass

1. $F(a+b) = F(a) + F(b)$
2. $F(a\cdot b) = F(a)\cdot F(b)$
3. und $F(1) = 1$.

Die Eigenschaft $F(0) = 0$ folgt automatisch aus 1.

Folgerung 11. *Körperhomomorphismen $F\colon K \to L$ sind injektiv.*

Beweis. Das haben wir gerade gesehen: Wenn $F(a) = 0$ für ein $a \neq 0$ wäre, dann wäre auch

$$F(1) = F(a\cdot a^{-1}) = \underbrace{F(a)}_{=0}\cdot F(a^{-1})$$
$$= 0,$$

aber es ist $F(1) = 1$. □

Bemerkung. 1. Die Aussage, dass die Abbildung

$$F\colon \mathbb{Q}[x]/(x^3-2) \to \mathbb{Q}(\sqrt[3]{2}),$$

die $[x]$ auf $\sqrt[3]{2}$ abbildet bijektiv ist, erklärt, warum wir mit $\sqrt[3]{2}$ tatsächlich einfach wie mit einem Symbol rechnen können, dass nur die Gleichung $\sqrt[3]{2}^3 = 2$ erfüllt. Das ist am Ende so, wie wir tatsächlich mit diesem Symbol in Formeln umgehen.

2. Bei genauerem Hinschauen, fällt Ihnen vielleicht auch auf, dass es in $\mathbb{C}$ drei verschiedene Zahlen gibt, die die Gleichung $a^3 = 2$ erfüllen, nämlich

$$\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}$$

wobei

$$\zeta_3 = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$$

eine primitive 3-te Einheitswuzel ist, d.h. eine Zahl $\neq 1$, für die $\zeta_3^3 = 1$ gilt.

Der Körper $L = \mathbb{Q}[x]/(x^3-2)$ lässt sich also auf 3 verschiedene Arten in $\mathbb{C}$ einbetten, denn die Abbildungen

$$\begin{aligned} F_2\colon \mathbb{Q}[x]/(x^3-2) &\to \mathbb{Q}(\zeta_3\sqrt[3]{2})\mathbb{C} \\ [a(x)] &\mapsto F([a(x)]) := a(\zeta_3\sqrt[3]{2}) \end{aligned}$$

bzw.

$$\begin{aligned} F_2\colon \mathbb{Q}[x]/(x^3-2) &\to \mathbb{Q}(\zeta_3^2\sqrt[3]{2})\mathbb{C} \\ [a(x)] &\mapsto F([a(x)]) := a(\zeta_3^2\sqrt[3]{2}) \end{aligned}$$

sind ebenfalls Isomorphismen von Körpern.

Das ist vielleicht gar nicht so merkwürdig, denn wenn wir quadratische Gleichungen lösen, kommt in den Formeln auch immer $\pm\sqrt{\ }$ vor, d.h. algebraisch sind beide Wurzeln nicht recht zu unterscheiden. Das passiert erst, wenn wir die Ergebnisse in $\mathbb{R}$ interpretieren.

Genauso können wir uns überlegen, dass sich ein allgemeiner Winkel nicht mit Zirkel und Lineal dreiteilen lässt. Einen Winkel α in der Ebene können wir genau dann konstruieren, wenn wir die komplexe Zahl $e^{i\alpha} = \cos(\alpha) + i\sin(\alpha)$ konstruieren können, denn das ist die eindeutig bestimmte Zahl vom Betrag 1, deren Winkel mit der x-Achse α ist.

Einen Winkel zu dritteln bedeutet also aus $z = e^{i\alpha}$ die Zahl $e^{i\frac{\alpha}{3}} = \cos(\frac{\alpha}{3}) + i\sin(\frac{\alpha}{3})$ zu konstruieren und das ist wiederum eine Zahl w, die $w^3 = z$ erfüllt, d.h., auch hierfür müssen wir eine 3. Wurzel konstruieren.

Da wir uns vielleicht nicht so gerne überlegen möchten, ob das Polynom $x^3 - z$ eine Nullstelle in $\mathbb{Q}(z)$ besitzt, nehmen wir uns einen Winkel α für den der Realteil $\cos(\alpha)$ von $e^{i\alpha}$ rational ist. Zum Beispiel ist das für $\frac{\pi}{3} = 60^\circ$ der Fall, denn

$$e^{i\frac{\pi}{3}} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$$

ist nach dem Satz des Pythagoras die Spitze des gleichseitigen Dreiecks mit Kantenlänge 1 über dem Intervall $[0,1]$.

Auf dem Übungsblatt überlegen Sie sich, dass der Realteil $\cos(\frac{\alpha}{3})$ von $e^{i\frac{\alpha}{3}}$ die Gleichung

$$\cos(\alpha) = 4\cos(\frac{\alpha}{3})^3 - 3\cos(\frac{\alpha}{3})$$

erfüllt. Die Gleichung

$$p(x) = 4x^3 - 3x - \frac{1}{2} = 0$$

hat aber keine Nullstelle in $\mathbb{Q}$, weil

$$2p(\frac{x}{2}) = x^3 - 3x - 1$$

keine Nullstelle besitzt. (Für normierte, ganzzahlige Polynome kommen als Nullstellen nur Teiler des konstanten Koeffizienten in Betracht und ± 1 sind keine Nullstellen).

Wenn Sie das nicht wissen, finden Sie dafür eine Anleitung auf dem Übungsblatt.

FAZIT: Wir haben uns nun eigentlich eine allgemeinere Aussage zu nicht-konstruierbaren Zahlen überlegt.

Behauptung 12. *Ist eine Zahl $z \in \mathbb{C}$ eine Nullstelle eines irreduziblen Polynoms $p(x) \in \mathbb{Q}[x] \setminus \{0\}$ dessen Grad $\neq 2^m$ keine Potenz von 2 ist, dann ist z nicht mit Zirkel und Lineal konstruierbar.*

Beweis. Ist z konstruierbar, so existiert nach der Charakterisierung konstruierbarer Zahlen ein Körperturm

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$$

mit $z \in K_n$ und $[K_i : K_{i-1}] = 2$ für alle $i = 1, \ldots, n$. Dann ist aber einerseits $[K_n : \mathbb{Q}] = 2^n$ (Multiplikativität der Dimension) und andererseits

$$\mathbb{Q} \subset \mathbb{Q}(z) \subseteq K_n$$

und darum auch

$$2^n = [K_n : \mathbb{Q}] = [K_n : \mathbb{Q}(z)] \cdot [\mathbb{Q}(z) : \mathbb{Q}].$$

Darum muss dann $[\mathbb{Q}(z) : \mathbb{Q}]$ ein Teiler von 2^n sein.

Andererseits ist z aber Nullstelle des irreduziblen Polynoms $p(x)$ und darum ist

$$\mathbb{Q}[x]/(p(x)) \xrightarrow{x \mapsto z} \mathbb{Q}(z)$$

ein Isomorphismus von Körpern und es gilt

$$[\mathbb{Q}[x]/(p(x)) : \mathbb{Q}] = \mathrm{Grad}(p).$$

Da $\mathrm{Grad}(p) \neq 2^m$ nach Voraussetzung aber keine Potenz von 2 ist, ist das ein Widerspruch zu Annahme, dass z konstruierbar ist. □

Den Trick, dass Nullstellen von irrreduziblen Polynomen $p(x) \in \mathbb{Q}[x]$ genau den Einbettungen von $\mathbb{Q}[x]/p(x) \to \mathbb{C}$ entsprechen sollten wir auch noch allgemein festhalten.

Folgerung 13. *Ist $K \subseteq L$ eine Körpererweiterung und $p(x) \in K[x]$ ein irreduzibles Polynom, dann definiert jede Nullstelle $\alpha \in L$ von p in L einen Isomorphismus:*

$$\begin{aligned} K[x]/(p(x)) &\to K(\alpha) \subseteq L \\ [a(x)] &\mapsto a(\alpha). \end{aligned}$$

Beweis. Wir können unseren Beweis für den Spezialfall $p(x) = x^3 - 2 \in \mathbb{Q}[x]$ abschreiben:

Die Abbildung ist wohldefiniert, weil $[a(x)] = [\tilde{a}(x)]$ bedeutet, dass $\tilde{a}(x) = a(x) + n(x) \cdot p(x)$ für ein $n(x) \in K[x]$ und also

$$\tilde{a}(\alpha) = a(\alpha) + n(\alpha) \underbrace{p(\alpha)}_{=0} = a(\alpha).$$

Die Abbildung ist mit den Verknüpfungen $+, \cdot$ verträglich, weil das für die Abbildung $a(x) \mapsto a(\alpha)$ gilt und also ist die Abbildung ein Körperhomomorphismus.

Nach Folgerung 11 sind Körperhomomorphismen injektiv, das Bild ist also ein Unterkörper von L, enthält α und ist nach Konstruktion in $K(\alpha)$ enthalten. Da $K(\alpha)$ der kleinste Unterkörper von L ist, der K und α enthält ist die Abbildung also ein Isomorphismus. □

Transzendente Zahlen und die Quadratur des Kreises

Wenn Sie in der Analysis gut aufgepasst haben, können Sie sich vielleicht selbst überlegen, dass nicht alle reelle Zahlen Nullstellen von Polynomen mit rationalen Koeffizienten sind. Das folgt daraus, dass es überabzählbar viele reelle Zahlen gibt.

Hingegen ist die Menge $\mathbb{Q}[x]$ der Polynome mit rationalen Koeffizienten abzählbar und jedes dieser Polynome hat nur endlich viele Nullstellen in $\mathbb{R}$. Es gibt also nur abzählbar viele Zahlen in $\mathbb{R}$ (oder $\mathbb{C}$), die Nullstellen eines irreduziblen Polynoms in $\mathbb{Q}[x]$ sind, aber überabzählbar viele Elemente von $\mathbb{R}$.

Die „meisten“ reellen Zahlen sind also keine Nullstellen von Polynomen mit rationalen Koeffizienten.

In der Vorlesung haben Sie an dieser Stelle sofort die wichtige Frage gestellt, wie Sie herausfinden können, ob eine Zahl nun als Nullstelle eines Polynoms vorkommt oder nicht. Darauf kommen wir gleich noch zurück, die Antwort ist aber dass das ein Beispiel für eine Aussage ist, bei der wir ganz leicht zeigen können, das etwas für „fast alle“ reellen Zahlen gilt, es aber schwer ist, auch nur ein konkretes Beispiel anzugeben. Bevor ich Ihnen Beispiele angebe, möchte ich kurz die Begriffe einführen, die wir verwenden, um „kommt als Nullstelle vor“ und „kommt nicht als Nullstelle vor“ zu unterscheiden.

Definition (algebraisch/transzendent)**.** Ist $K \subseteq L$ eine Körpererweiterung so heißt ein Element $\alpha \in L$

algebraisch (über K), wenn α Nullstelle eines Polynoms $p(x) \in K[x] \setminus \{0\}$ ist, bzw.

transzendent (über K) wenn α keine Gleichung der Form $p(x) = 0$ für ein $p(x) \in K[x] \setminus \{0\}$ erfüllt.

Beispiel 14 (Bekannte transzendente Zahlen)**.** 1. Eine transzendente Zahl, die gebastelt wurde, um ein explizites Besipiel zu haben, ist die Liouville Zahl

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{1}{10^{n!}} &= \frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^6} + \frac{1}{10^{24}} + \frac{1}{10^{120}} + \dots \\ &= 0,110001000000000000000000100000\dots\end{aligned}$$

Das ist eine Zahl in der die Abstände zwischen den Nachkommastellen die nicht 0 sind sehr schnell wachsen. Dadurch lässt sich diese Zahl sehr gut durch rationale Zahlen approximieren. Für algebraische Zahlen geht das nicht, Sie können sich überlegen, dass wenn α eine Nullstelle eines irreduziblen Polynoms $p(x) \in \mathbb{Q}[x]$ vom Grad $d > 1$ ist eine Konstante $c > 0$ existiert, so dass für alle Brüche $\frac{n}{m}$ gilt

$$|\alpha - \frac{n}{m}| \geq \frac{c}{m^d}.$$

Die Liouville Zahl ist gerade so konstruiert, dass diese Bedingung nicht erfüllt ist.

2. Die Zahl $e = \sum_{n=0}^{\infty} \frac{1}{n!}$ ist ebenfalls transzendent. Das ist schwerer zu zeigen. Wenn am Ende des Semesters noch Zeit ist und Sie das lernen möchten, können wir darauf noch einmal zurück kommen. Der Grund ist am Ende auch hier, dass sich diese Zahl zu gut durch Brüche approximieren lässt, weil die Exponentialreihe so gut konvergiert.

3. Die Zahl π ist transzendent. Das wurde von Lindemann mit einem wunderbaren Argument gezeigt: Statt etwas über π zu beweisen, lässt sich ähnlich wie im Punkt davor ein Argument dafür finden, dass für algebraische Zahlen $\alpha \neq 0$ die Zahl e^{α} immer transzendent ist. Dann kann π aber nicht algebraisch sein, weil $e^{i\pi} = -1$ nicht transzendent ist.

   Da dieses Argument so indirekt ist, wissen wir nicht, ob π über $\mathbb{Q}(e)$ transzendent ist oder nicht, d.h. ob es ein Polynom mit Koeffizienten in denen e vorkommen darf gibt, das π als Nullstelle hat. Viele Mathematiker:innen würden wetten, dass das nicht so ist und numerische Experimente bestätigen das, aber es ist noch niemandem eine Methode eingefallen, die das beweisen könnte.

4. Es gibt sehr sehr viele Vermutungen über die Transzendenz von natürlich vorkommenden Zahlen. Zum Beispiel kennen Sie vielleicht die überraschende Formel

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Für die ähnlichen Summen

$$\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k}$$

für ungerade $k > 1$ wird vermutet, dass diese Zahlen transzendent sind (für die geraden kennen wir Formeln in denen nur π vorkommt). Andererseits, was schon der Beweis dafür, dass $\zeta(3) \notin \mathbb{Q}$ nicht rational ist eine große Überraschung.

Der Abstand zwischen den Vermutungen und dem was wir wissen ist also noch sehr groß.

Folgerung 15 (Quadratur des Kreises)**.** *Transzendente Zahlen sind nicht konstruierbar, insbesondere ist die Zahl π nicht konstruierbar. Darum ist es nicht möglich ein Quadrat zu konstruieren, dass den Flächeninhalt des Einheitskreises besitzt.*

Beweis. Da alle konstruierbaren Zahlen algebraisch sind (Satz 5), sind transzendente Zahlen nicht konstruierbar. Da π transzendent ist, ist insbesondere π nicht konstruierbar.

Der Flächeninhalt des Einheitskreises ist π, daher hätte ein Quadrat mit Flächeninhalt π die Kantenlänge $\sqrt{\pi}$. Da π nicht konstruierbar ist, ist auch $\sqrt{\pi}$ nicht konstruierbar. □

Charakterisierung algebraischer Zahlen

Lassen Sie uns kurz einige alternative Charakterisierungen algebraischer Zahlen angeben, die manchmal statt unserer Definition verwendet werden.

Lemma 16. *Ist $K \subseteq L$ eine Körpererweiterung so sind für $\alpha \in L$ die folgenden Aussagen äquivalent:*

1. *α ist algebraisch.*
2. *α ist Nullstelle eines irreduziblen Polynoms $p(x) \in K[x] \setminus \{0\}$.*
3. *$[K(\alpha) : K] = d < \infty$, d.h. die von α erzeugte Körpererweiterung ist ein endlich dimensionaler K-Vektorraum.*

Beweis. Wir zeigen 1. $\Rightarrow$ 2. $\Rightarrow$ 3. $\Rightarrow$ 1., Sie können gerne versuchen, erst zu schauen, ob Sie einige dieser Implikationen selbst einsehen können, bevor Sie weiter lesen.

Zunächst gilt 1. $\Rightarrow$ 2.: Ist α algebraisch, so existiert ein Polynom $p(x) \in K[x] \setminus \{0\}$ mit $p(\alpha) = 0$. Ist p irreduzibel, so gilt 2. Falls nicht, existieren nicht-konstante Polynome $a(x), b(x) \in K[x]$, für die

$$p(x) = a(x) \cdot b(x)$$

gilt. Dann ist aber $0 = p(\alpha) = a(\alpha) \cdot b(\alpha)$ und also $a(\alpha) = 0$ oder $b(\alpha) = 0$. Der Grad der Polynome a, b ist aber kleiner als der Grad von p. Wählen wir also ein Polynom $p(x) \in K[x] \setminus \{0\}$ von minimalem Grad, für das $p(\alpha) = 0$ ist, so ist $p(x)$ irreduzibel.

Insbesondere existiert also auch ein irreduzibles Polynom $p(x)$ mit $p(\alpha) = 0$.

Die Folgerung 2. $\Rightarrow$ 3. haben wir auch schon gesehen, denn ist $p(x) \in K[x] \smallsetminus \{0\}$ irreduzibel und α eine Nullstelle von p, so ist $K[x]/(p(x)) \cong K(\alpha)$ (Folgerung 13) und es gilt also

$$\dim_K K(\alpha) = \dim_K K[x]/(p(x)) = \mathrm{Grad}(p) < \infty.$$

Für die Folgerung 3. $\Rightarrow$ 1. können wir eine Beobachtung wiederverwenden, die Sie bei $\sqrt[3]{2}$ gemacht hatten, das nämlich eine nichttriviale Linearkombination $a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 = 0$ bedeuten würde, dass $\sqrt[3]{2}$ eine Nullstelle des quadratischen Polynoms $a + bx + cx^2$ wäre:

Angenommen es gilt $[K(\alpha) : K] = d < \infty$. Dann müssen die $d + 1$ Elemente $1, \alpha, \ldots, \alpha^d$ des d-dimensionalen K-Vektorraums $K(\alpha)$ linear abhängig sein, d.h., es gibt eine nichttriviale Lösung der Gleichung

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_d\alpha^d = 0.$$

Das bedeutet aber, dass α eine Nullstelle des Polynoms $p(x) = a_0 + a_1 x + \cdots + a_d x^s$ ist. Das zeigt 1. □

Lemma/Definition 17 (Minimalpolynom)**.** *Ist $K \subset L$ eine Körpererweiterung und $\alpha \in L$ algebraisch, so existiert ein eindeutiges normiertes irreduzibles Polynom* $\mathrm{minpol}_\alpha(x) \in K[x]$ *für das* $\mathrm{minpol}_\alpha(\alpha) = 0$ *gilt.*

Dieses Polynom heißt Minimalpolynom *von α (über K).*

Normiert bedeutet, dass der führende Term des Polynoms x^d ist, d.h. das Polynom ist von der Form $x^d + a_{d-1}x^{d-1} + \cdots + a_0$.

Beweis. Wir haben gerade gesehen, dass es ein irreduzibles Polynom $p(x) \in K[x]$ gibt, für das $p(\alpha) = 0$ gilt und nachdem wir dieses mit $\frac{1}{\text{Führender Koeffizient}}$ multiplizieren ist dieses Polynom auch normiert. Wir müssen also nur die Eindeutigkeit zeigen.

Sind $a(x), b(x)$ zwei irreduzible Polynome mit $a(\alpha) = b(\alpha) = 0$, so ist nach dem Euklidischen Algorithmus

$$\mathrm{ggT}(a(x), b(x)) = n(x)a(x) + m(x)b(x)$$

ein normiertes Polynom, das ebenfalls die Nullstelle α besitzt. Da $a(x), b(x)$ aber irreduzibel sind, ist $a(x)$ der einzige nichttriviale Teiler von $a(x)$, also gilt

$$a(x) = \mathrm{ggT}(a(x), b(x)) = b(x).$$

□

Bemerkung. Sie haben in der linearen Algebra schon eine Möglichkeit kennengelernt, das Minimalpolynom einer Zahl zu finden: Ist $[L : K]$ endlich und $\alpha \in L$, so ist die Multiplikation mit α eine K-lineare Abbildung

$$\begin{aligned} \alpha\cdot \colon L &\to L \\ \beta &\mapsto \alpha \cdot \beta. \end{aligned}$$

Nach dem Satz von Cayley-Hamilton erfüllt jede lineare Abbildung ihr charakteristisches Polynom, d.h. α ist eine Nullstelle von

$$\mathrm{charpol}_{\alpha\cdot}(t) = \det(\alpha \cdot - t\,\mathrm{id}_L).$$

Damit ist das Minimalpolynom ein Teiler dieses charakteristischen Polynoms.

Wenn $L = K(\alpha)$ ist, dann ist dieses Polynom vom Grad $[K(\alpha) : K]$ und weil dieser Grad der Gerad des Minimalpolynoms ist, muss in diesem Fall das Minimalpolynom bis auf ein Vorzeichen gleich dem charakteristischen Polynom sein.

Beispiel 18. Für das Beispiel $\mathbb{R} \subset \mathbb{C}$ und das Element $\alpha = i \in \mathbb{C}$ ist die Matrix der Multiplikation $i\cdot$ bezüglich der Basis $1, i$ von $\mathbb{C}$ gleich $I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ und

$$\text{charpol}_I(t) = \det(\begin{pmatrix} -t & -1 \\ 1 & -t \end{pmatrix}) = t^2 + 1$$

ist das Minimalpolynnom von i.

Struktur von $K(\alpha)$ für transzendente α

Für algebrische Elemente α haben wir die Struktur von $K(\alpha)$ in Termen von Polynomen als Quotienten $K[x]/(p(x))$ verstehen können. Ist $\alpha \in L$ transzendent, so ist die analoge Abbildung:

$$\begin{aligned} K[x] &\to L \\ p(x) &\mapsto p(\alpha) \end{aligned}$$

nach Definition injektiv, denn $p(\alpha) = 0$ gilt dann nur für das Nullpolynom.

Die Abbildung ist weiter mit $+, \cdot$ verträglich und darum kann das Bild kein Körper sein, da es im Polynomring keine multiplikativen Inversen für Polynome vom Grad ≥ 1 gibt.

Genauso, wie wir die Konstruktion von $\mathbb{Z}/p\mathbb{Z}$ abschreiben konnten, um $K[x]/(p(x))$ zu konstruieren, können wir aber auch die Konstruktion des Körpers der rationalen Zahlen $\mathbb{Q}$ aus $\mathbb{Z}$ abschreiben um aus $K[x]$ einen Körper zu konstruieren.

Die Bezeichnung „rationale Funktionen“ ist etwas irreführend, da wir hier die formalen Terme meinen. Ein Ausdruck der Form $\frac{p(x)}{q(x)}$ definiert nur auf $K \setminus$ Nullstellen von q eine Abbildung.

Die Bezeichnung klärt immerhin die sehr merkwürdige Bezeichnung „ganzrationale Funktionen“ die in Schulbüchern statt „Polynome“ verwendet wird.

Definition. Die Menge

$$K(x) := \left\{ \frac{p(x)}{q(x)} \mid p(x), q(x) \in K[x], q(x) \neq 0 \right\} / \sim$$

wobei $\sim$ die Äquivalenzrelation

$$\frac{a(x)}{b(x)} \sim \frac{c(x)}{d(x)} \Leftrightarrow a(x)d(x) - b(x)c(x) = 0$$

bezeichnet ist mit den Verknüpfungen $+, \cdot$ die durch die Rechenregeln für Bruchrechnung

$$\begin{aligned} \frac{a(x)}{b(x)} + \frac{c(x)}{d(x)} &:= \frac{a(x)d(x) + b(x)c(x)}{b(x)d(x)} \\ \frac{a(x)}{b(x)} \cdot \frac{c(x)}{d(x)} &:= \frac{a(x)c(x)}{b(x)d(x)} \end{aligned}$$

gegeben sind ein Körper, genannt der *Körper der rationalen Funktionen*.

FÜR DEN NACHWEIS, dass die Verknüpfungen wohldefiniert sind und die Körperaxiome erfüllen, können wir einfach den Beweis, den wir für die rationalen Zahlen verwendet haben abschreiben und dabei überall die auftretenden ganzen Zahlen a, b, c, d durch Polynome $a(x), b(x), c(x), d(x)$ ersetzen. Bitte überzeugen Sie sich selbst davon, dass das tatsächlich funktioniert.

DAMIT KÖNNEN wir nun für jedes transzendente Element $\alpha \in L$ einer Körpererweiterung $K \subset L$ die Abbildung $K[x] \to K(\alpha) \subset L$ die durch $p(x) \mapsto p(\alpha)$ gegeben ist auf $K(x)$ fortsetzen:

$$\begin{aligned} f\colon K(x) &\to K(\alpha) \subseteq L \\ \frac{p(x)}{q(x)} &\mapsto \frac{p(\alpha)}{q(\alpha)} \end{aligned}$$

ist wohldefiniert, weil einerseits für alle $q(x) \in K[x] \smallsetminus \{0\}$ gilt, dass $q(\alpha) \neq 0$ – das war genau die Bedingung transzendent zu sein – und andererseits in jedem Körper die Rechenregeln für die Bruchrechnung gelten (das hatten wir in der linearen Algebra nachgeprüft). Gilt also $\frac{a(x)}{b(x)} \sim \frac{c(x)}{d(x)}$, d.h. $a(x)d(x) - b(x)c(x) = 0$ dann ist

$$\frac{a(\alpha)}{b(\alpha)} - \frac{c(\alpha)}{d(\alpha)} = \frac{a(\alpha)d(\alpha) - b(\alpha)c(\alpha)}{b(\alpha)d(\alpha)} = \frac{0}{b(\alpha)d(\alpha)} = 0.$$

Die Abbildung ist ein Körperhomomorphismus, also injektiv. Das Bild liegt in $K(\alpha)$ und enthält α und K, da $K(\alpha)$ der kleinste Unterkörper von L mit diesen Eigenschaften ist, muss die Abbildung also auch surjektiv und damit ein Isomorphismus sein.

Damit haben wir auch für transzendente Elemente α die Struktur des Körpers $K(\alpha)$ bestimmt: Dieser Körper ist immer eine Kopie des Körpers der rationalen Funktionen.

Folgerung 19. *Ist $K \subseteq L$ eine Körpererweiterung und $\alpha \in L$ ein Element, dann sind äquivalent:*

1. *α ist transzendent*
2. *Die Abbildung $K[x] \to L$ die durch $x \mapsto \alpha$ und $p(x) \mapsto p(\alpha)$ gegeben ist, ist injektiv.*
3. *Die Vorschrift $\frac{p(x)}{q(x)} \mapsto \frac{p(\alpha)}{q(\alpha)}$ definiert einen Isomorphismus*
$$K(x) \cong K(\alpha).$$
4. *$K(\alpha)$ ist ein unendlich dimensionaler K-Vektorraum.*

Beweis. Wir haben uns gerade 1. $\Rightarrow$ 2. $\Rightarrow$ 3. überlegt. Die Implikation 3. $\Rightarrow$ 4. ist klar, da $K(x)$ ein unendlichdimensionaler K-Vektorraum ist, denn $K(x)$ enthält den Polynomring. Und 4. $\to$ 1. folgt weil für algebraische Elemente $K(\alpha)$ endlichdimensional ist. □

DIE KONSTRUKTION die aus $\mathbb{Z}$ den Körper $\mathbb{Q}$ und aus dem Polynomring $K[x]$ den Körper $K(x)$ macht, ist noch allgemeiner nützlich. Das möchte ich kurz vorstellen.

Sie erinnern sich (hoffentlich?) aus der linearen Algebra, dass ein kommutativer Ring mit 1, ein Zahlbereich (also eine Menge mit Rechenoperationen $+, \cdot$)ist, in dem alle Körperaxiom bis auf die Existenz von multiplikativen inversen Elementen gelten. Also zum Beispiel $\mathbb{Z}$, $K[x]$ oder auch Polynomringe in mehreren Variablen $K[x_1, \ldots, x_n]$.

KONVENTION: In dieser Vorlesung meine ich mit „Ring“ immer einen kommutativen Ring mit 1. Wenn einmal nicht-kommutative Ringe vorkommen sollten, werde ich „nicht-kommutativer Ring“ oder „nicht notwendig kommutativer Ring“ schreiben.

WIR KÖNNTEN für einen beliebigen Ring R versuchen die Definition von oben abzuschreiben:

$$Q(R) := \left\{ \frac{a}{b} \mid a, b \in R, b \neq 0 \right\} / \sim$$

wobei $\sim$ die Äquivalenzrelation

$$\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow ad - bc = 0$$

ist.

FRAGE: Wird das mit den Rechenregeln $+, \cdot$ für Brüche immer ein Körper?

Vergleiche auch mit Aufgabe 1 Blatt 4!

DENKEN SIE darüber einmal nach, bevor Sie weiter lesen.

In der Vorlesung hatten Sie bemerkt, dass schon in der Definition für die Multiplikation

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$$

benötigt wird, dass in R der Satz vom Nullprodukt gilt, d.h. aus $bd = 0$ sollte $b = 0$ oder $d = 0$ folgen.

Das stimmt aber beispielsweise in $\mathbb{Z}/4\mathbb{Z}$ nicht, da dort $[2] \cdot [2] = [4] = [0]$ gilt. Genauso wissen Sie das für $\mathbb{Z}/10\mathbb{Z}$. Für Quotienten von Polynomringen haben wir das gleiche Problem, wenn wir $K[x]/(x(x-1)), K[x,y]/(xy)$ oder $K[x]/(x^2)$ betrachten.

Der Ring $K[x]/(x^2)$ ist tatsächlich nützlich, wenn wir hier über x als Symbol nachdenken, das nicht 0 ist, aber $x^2 = 0$ gilt, das gibt der Idee dass x dann ein „sehr kleines“ Element ist eine algebraische Bedeutung und diese ist tatsächlich nützlich, um in der Algebra analytische Argumente ganz ohne Abschätzungen zu ermöglichen.

Ringe in denen der Satz vom Nullprodukt gilt, heißen nullteilerfrei.

Definition. Ein Ring R heißt *nullteilerfrei*, wenn für alle $a, b \in R$ gilt dass

$$(a \cdot b = 0) \Rightarrow (a = 0 \text{ oder } b = 0).$$

In nullteilerfreien Ringen lässt sich der Beweis, dass $\mathbb{Q}$ ein Körper ist nun aber wirklich abschreiben:

Lemma/Definition 20. *Ist R ein nullteilerfreier Ring, so ist die Menge*

$$Q(R) := \left\{ \frac{a}{b} \mid a, b \in R, b \neq 0 \right\} / \sim$$

wobei $\sim$ die Äquivalenzrelation

$$\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow ad - bc = 0$$

ist, zusammen mit den Verknüpfungen:

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}$$
$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$$

ein Körper.

$Q(R)$ heißt Quotientenkörper von R.

Die Aufgabe nachzuschauen, dass sich der Beweis für die rationalen Zahlen abschreiben lässt und damit einen Beweis dieses Lemmas liefert, überlasse ich Ihnen.

Nachdem die Mehrheit von Ihnen in der Vorlesung zunächst der Meinung war, dass die Konstruktion für beliebige Ringe funktioniert, sind Sie jetzt hoffentlich misstrauisch genug, um das ernsthaft nachprüfen zu wollen.

Bemerkung. Wir erhalten mit dieser Konstruktion also auch Quotientenkörper

$$K(x_1, \ldots, x_n) := Q(K[x_1, \ldots, x_n])$$

von Polynomringen in mehreren Variablen.

Das wird für uns noch nützlich sein, weil wir die Frage nach einer Lösungsformel für allgemeine Gleichungen der Form

$$x^3 + ax^2 + bx + c = 0$$

als Frage für den Körper $K(a,b,c)$ in dem a,b,c formale Symbole verstehen können.

Diese Erkenntnis, die vielleicht ganz naheliegend erscheint, wenn Sie das einmal gelesen haben, war lange Zeit ein echtes Hindernis für die Beantwortung der Frage, ob es solche Formeln geben kann.

Jeder Körper enthält einen der Körper $\mathbb{Q}$ oder $\mathbb{F}_p$

Die Struktur, dass für Körpererweiterungen der Form $K(\alpha)$ der Homomorphismus $K[x] \to K(\alpha)$ der $x \to \alpha$ abbildet entweder

1. injektiv ist und dann gilt $K(x) \cong K(\alpha)$, oder
2. einen Kern hat und dann gilt dass $K[x]/(p(x)) \cong K(\alpha)$ für ein irreduzibles Polynom $p(x) \in K[x]$

können wir noch einmal für $\mathbb{Z}$ statt $K[x]$ wiederfinden. Um das zu formulieren möchte ich eine abkürzende Notation einführen.

Notation 21. Ist p eine Primzahl so bezeichnen wir mit $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ den Restklassenkörper mit p Elementen.

Der Buchstabe $\mathbb{F}$ wurde wegen der englishen Bezeichnung „field“ für „Körper“ gewählt.

Wir werden gleich sehen, dass es (bis auf natürliche Isomorphie) nur einen Körper mit p Elementen gibt.

Behauptung 22. *Für jeden Körper K (und jeden kommutativen Ring R mit 1) definiert die induktive Vorschrift*

$$\begin{aligned} f\colon \mathbb{Z} &\to K \\ 1 &\mapsto f(1) := 1_K && \text{und induktiv} \\ n+1 &\mapsto f(n+1) := f(n)+1 && \text{also } n \mapsto \underbrace{1+1+\cdots+1}_{n-mal} \\ -n &\mapsto f(-n) := -f(n) && \text{und } f(0) = 0. \end{aligned}$$

einen Ringhomomorphismus.

Ist K ein Körper so gilt entweder

1. *f ist injektiv und dann setzt sich f zu einem Körperhomomorphismus*

$$f\colon \mathbb{Q} \hookrightarrow K$$

fort, oder

2. *$\operatorname{Ker}(f) = \{n \mid f(n) = 0\} = p \cdot \mathbb{Z}$ für eine Primzahl p und in diesem Fall induziert f einen Körperhomomorphismus*

$$\begin{aligned} \overline{f}\colon \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} &\hookrightarrow K \\ [a] &\mapsto \overline{f}([a]) := f(a). \end{aligned}$$

Bevor wir das erklären kurz ein Begriff und ein paar Beispiele.

Definition. Die *Charakteristik* eines Körpers K ist die Zahl $p \in \mathbb{N}_0$ für die gilt, dass

$$\ker(f\colon \mathbb{Z} \to K) = p \cdot \mathbb{Z}.$$

Wir schreiben kurz $\operatorname{char}(K) = p$.

Die Charakteristik eines Körpers ist also genau dann > 0 wenn es eine Zahl $n > 0$ gibt, so dass

$$n \cdot 1 = \underbrace{1+1+\cdots+1}_{n-\text{mal}} = 0$$

ist und genau dann 0, wenn K die ganzen Zahlen $\mathbb{Z}$ und damit auch die rationalen Zahlen $\mathbb{Q}$ enthält.

Beispiel 23. 1. Die Körper $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}(i), \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(x)$ haben Charakteristik 0.

2. Die Körper $\mathbb{F}_p, \mathbb{F}_p(x)$ haben Charakteristik p.

3. Auf dem Übungsblatt haben Sie einen Körper mit 27 Elementen konstruiert, nämlich

$$K = \mathbb{F}_3[x]/(x^3 - x + 1).$$

Dieser Körper enthält $\mathbb{F}_3$, insbesondere gilt in K, dass $1+1+1 = [3] = 0$. Also hat dieser Körper auch die Charakteristik 3.

Beweis der Behauptung. Wenn Sie in der Analysis einmal mit Induktion bewiesen haben, dass in den ganzen Zahlen tatsächlich das Assoziativ-, Kommutativ- und Distributivgesetz gelten, empfinden Sie die Behauptung, dass f ein Ringhomomorphismus ist, das also

$$f(n+m) = f(n) + f(m) \text{ und } f(n \cdot m) = f(m+m+\ldots m) = f(n) \cdot f(m)$$

gilt, wahrscheinlich etwas, das Sie einerseits mit einem langweiligen Induktionsbeweis aufschreiben könnten und andererseits intuitiv (hoffentlich?) einsichtig ist, da die Definition liefert, das $f(n) = \underbrace{f(1)+\cdots+f(1)}_{n-\text{mal}}$ und der Vergleich dieser Formeln für $n+m$ und $n \cdot m$ damit liefert was zu zeigen ist.

Ich möchte Sie darum bitten, sich selbst davon zu überzeugen, dass f diese Eigenschaften erfüllt. Fragen Sie nach, wenn Sie damit Schwierigkeiten haben sollten, oder Sie nach Abkürzungen für das formale Argument suchen möchten.

Ist nun f injektiv, so ist $\ker(f) = \{0\}$ und damit die Abbildung

$$\frac{a}{b} \mapsto \frac{f(a)}{f(b)} \in K$$

wohldefiniert. Das liefert die gewünschte Einbettung $\mathbb{Q} \hookrightarrow K$.

Ist f nicht injektiv, d.h. es gibt $a \neq b \in \mathbb{Z}$ mit $f(a) = f(b)$, also $f(a-b) = 0 = f(0)$. Dann ist also $\ker(f) \neq \{0\}$. Wir wollen zeigen, dass $\ker(f)$ dann aus den Vielfachen einer Primzahl besteht, also $\ker(f) = p \cdot \mathbb{Z}$

Der Kern erfüllt aber die Eigenschaften:

1. $a, b \in \ker(f) \Rightarrow a + b \in \ker(f)$, denn dann ist $f(a+b) = f(a) + f(b) = 0 + 0 = 0$,

2. $a \in \ker(f), n \in \mathbb{Z} \Rightarrow na \in \ker(f)$, denn $f(na) = f(n) \cdot f(a) = f(n) \cdot 0 = 0$.

Damit ist aber für $a, b \in \ker(f)$ nach dem euklidischen Algorithmus auch

$$\mathrm{ggT}(a,b) = na + mb \in \ker(f).$$

Ist also $a > 0$ die kleinste natürliche Zahl mit $a \in \ker(f)$ so muss $\ker(f) = a \cdot \mathbb{Z}$ sein.

Damit ist die Abbildung

$$\begin{aligned} \overline{f} \colon \mathbb{Z}/a\mathbb{Z} &\hookrightarrow K \\ [b] &\mapsto \overline{f}([b]) := f(b) \end{aligned}$$

ein wohldefinierter Ringhomomorphismus und gerade so gemacht, dass $\overline{f}$ injektiv ist, denn

$$f(b) = 0 \Leftrightarrow b \in \ker(f) = a\mathbb{Z}.$$

Da K nullteilerfrei ist, muss dann aber auch $\mathbb{Z}/a\mathbb{Z}$ nullteilerfrei sein und das gilt genau dann wenn a eine Primzahl ist. Das war zu zeigen. □

Folgerung 24. *Ist K ein endlicher Körper*[9] *so ist die Anzahl der Elemente von K eine Potenz einer Primzahl:*

$$\#K = p^n$$

wobei $p = \mathrm{char}(K)$ und $n \in \mathbb{N}$.

[9] „endlicher Körper"=Körper mit endlich vielen Elementen

Beweis. Ist K endlich, so ist $\mathrm{char}(k) = p > 0$, da es keine injektive Abbildung von $\mathbb{Z}$ in eine endliche Menge gibt.

Wir haben gerade gezeigt, dass K dann

$$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \hookrightarrow K$$

den Körper $\mathbb{F}_p$ enthält. Insbesondere erhält K damit die Struktur eines $\mathbb{F}_p$-Vektorraums, der endlich und daher insbesondere endlichdimensional ist. Das bedeutet, dass die Wahl einer Basis einen Isomorphismus

$$K \cong \mathbb{F}_p^n$$

von $\mathbb{F}_p$ Vektorräumen definiert und es gilt

$$\#\mathbb{F}_p^n = \#\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mid a_i \in \mathbb{F}_p \} = p^n.$$

□

Bemerkung. 1. Die Folgerung besagt insbesondere, dass es keinen Körper mit 10 Elementen gibt.

2. Wir werden später noch sehen, dass es für jede Primzahlpotenz p^n tatsächlich einen Körper $\mathbb{F}_{p^n}$ mit p^n Elementen gibt und dieser bis auf Isomorphie eindeutig bestimmt ist.

   Für $p^n = 2^8 = 256$ wird dieser Körper in allen QR-Codes verwendet. Wenn Sie einen QR-Code scannen, Ihr Mobiltelefon den zugehörigen Link anzeigt, hat dafür in $\mathbb{F}_{256}$ gerechnet. Wir kommen darauf noch zurück.

Kreisteilung

Zum Abschluss des Kapitels zu Konstruktionen mit Zirkel und Lineal, möchte ich noch kurz zur Frage kommen, welche regelmäßigen N-Ecke konstruierbar sind. Ich finde es bemerkenswert, dass diese mittlerweile vielleicht etwas altmodisch erscheinenden Frage, uns zufällig auf sehr interessante mathematische Objekte geführt hat.

In einem regelmäßigen N-Eck ist der Winkel zwischen zwei Eckpunkten, gemessen am Mittelpunk des N-Ecks gerade

$$\frac{360^\circ}{N} = \frac{2\pi}{N}.$$

Ein regelmäßiges N-Eck ist also genau dann konstruierbar, wenn wir die komplexen Zahl mit Betrag 1 und Winkel $\frac{2\pi}{N}$ zur x-Achse konstruieren können, also

$$\zeta_N := e^{i\frac{2\pi}{N}}.$$

Die Zahlen

$$1, \zeta_N, \zeta_N^2, \dots, \zeta_N^{N-1},$$

also

$$1, e^{i\frac{2\pi}{N}}, e^{i\frac{2\pi 2}{N}}, \dots, e^{i\frac{2\pi(N-1)}{N}}$$

sind dann die Eckpunkte eines regelmäßigen N-Echs, da der Winkel zwischen zwei aufeinanderfolgenden gerade $\frac{2\pi}{N}$ ist.

FAZIT: Es ist genau dann möglich ein regelmäßiges N-Eck zu konstruieren, wenn die N-te Einheitswurzel $\zeta_N = e^{i\frac{2\pi}{N}}$ konstruierbar ist.

Wir sollten also zunächst prüfen, ob $[\mathbb{Q}(\zeta_N) : \mathbb{Q}] \stackrel{?}{=} 2^n$ eine Potenz von 2 ist.

Für $N = 3, 4, 5, 6$ hatten Sie schon Konstruktionen gefunden, hierfür muss das also stimmen.

SEHEN SIE EIN POLYNOM in $\mathbb{Q}[x]$ das ζ_N als Nullstelle besitzt?

HAT IHR POLYNOM eine Nullstelle in $\mathbb{Q}$?

Es gilt $\zeta_N^N = 1$ also ist ζ_N ein Nullstelle von $p(x) = X^N - 1$.

Das Polynom erfüllt aber auch $p(1) = 0$, also können wir $(x-1)$ ausklammern:

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

Aufgabe 1. Wenn N keine Primzahl ist, können Sie weitere Teiler von $x^N - 1$ finden.

Behauptung 25. *Ist p eine Primzahl, so ist das Polynom*

$$\Phi_p(x) := \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

irreduzibel und daher das Minimalpolynom von ζ_p.

Insbesondere gilt dann $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.

Φ ist der griechische Buchstabe Phi. Wieso sich dieser für Kreisteilungspolynome eingebürgert hat, weiß ich nicht genau, aber das Symbol ist ein geteilter Kreis.

Folgerung 26. *Ist p eine Primzahl die nicht von der Form $p = 2^n + 1$ ist, so ist es nicht möglich ein regelmäßiges p-Eck mit Zirkel und Lineal zu konstruieren.*

Bemerkung. 1. Wir wissen schon, dass regelmäßige p-Eck für die ersten Primzahlen $2, 3, 5$ konstruierbar ist, die Folgerung besagt, dass das für $7, 11, 13, ?, 19, 23, 29, 31, \ldots$ nicht möglich ist. Für $p = 17 = 16 + 1$ schließt die Folgerung nicht aus, dass ζ_{17} konstruierbar ist.

2. Die Frage, ob es tatsächlich möglich ist ein regelmäßiges 17 Eck zu konstruieren, war sehr lange offen. Dazu müssten wir $e^{\frac{2\pi}{17}} = \cos(\frac{2\pi}{17}) + i\sin(\frac{2\pi}{17})$ konstruieren, wofür es genügen würde $\cos(\frac{2\pi}{17})$ durch iteriertes Wurzelziehen zu beschreiben. Es war eine Überraschung, als Gauß eine Lösung für das Problem fand:

$$\cos(\frac{2\pi}{17}) = \frac{1}{16}\Big(-1 + \sqrt{17} + \sqrt{2(17+\sqrt{17})} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{2(17-\sqrt{17})} - 2\sqrt{2(17+\sqrt{17})}}\Big).$$

Ich denke, diese Formel lässt sich nicht ohne zusätzliche Einsicht finden.

Vielleicht fällt Ihnen auch auf, dass in der Formel $\sqrt{17}$ eine tragende Rolle spielt, genau wie bei Ihrer Formel für $\cos(\frac{2\pi}{5})$ vom 1. Übungsblatt die Zahl $\sqrt{5}$ wesentlich war. Das ist kein Zufall.

3. Mit der Galois-Korrespondenz werden wir genau bestimmen können, für welche N das regelmäßige N-Eck konstruierbar ist. Insbesondere geht das für alle Primzahlen der Form $2^n + 1$ und wir bekommen damit auch eine Anleitung, wie wir eine Konstruktion für gegebenes $p = 2^n + 1$ finden könnten.

Lassen Sie uns das allgemeine Resultat zunächst an einem Beispiel ausprobieren, das Sie schon kennen. Wieso ist

$$\frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1$$

in $\mathbb{Q}[x]$ irreduzibel? Und können wir dazu ein Argument finden, das eine Chance hat, für alle p zu funktionieren?

Ein Trick ist, auf der linken Seite zu sagen: Ich teile eigentlich lieber durch x als $x-1$ und $p(x)$. Setzen wir $x = y+1$, also $y = x-1$, dann wird

$$P(y) = \frac{(y+1)^5 - 1}{y} = \frac{y^5 + 5y^4 + 10y^3 + 10y^2 + 5y + 1 - 1}{y}$$
$$= y^4 + 5y^3 + 10y^2 + 10y + 5.$$

Von diesem komplizierteren Polynom ist es leicht zu sehen, dass es irreduzibel ist, wenn Sie sich an das Übungsblatt erinnern, auf dem Sie gezeigt haben:

Lemma 27. *(Lemma von Gauß) Ist $f(x) \in \mathbb{Z}[x]$ ein primitives Polynom so ist $f(x)$ genau dann irreduzibel in $\mathbb{Q}[x]$ wenn es in $\mathbb{Z}[x]$ irreduzibel ist.*

primitiv=ggT(Koeffizienten)=1.

Warum hilft das weiter? Nun, angenommen

$$= y^4 + 5y^3 + 10y^2 + 10y + 5 = a(y) \cdot b(y)$$

wobei $a(x) = \sum a_i x^i, b(x) = \sum b_j x^j \in \mathbb{Z}[x]$. Rechnen wir dann modulo 5, dann ist

$$[a(y)] \cdot [b(y)] = y^4 \in \mathbb{F}_5[x]$$

Das bedeutet aber, dass

$$[a(y)] = y^k, [b(y)] = y^\ell \in \mathbb{F}_5[y].$$

Also ist $[a_0] = [b_0] = 0 \in \mathbb{F}_5$, d.h. a_0, b_0 sind beide durch 5 teilbar. Das kann nicht sein, denn $a_0 b_0 = 5$.

Lemma 28 (Eisensteinkriterium)**.** *Ist $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ ein primitives Polynom und p eine Primzahl so dass*

1. *$a_{n-1}, \ldots, a_0$ durch p teilbar sind, aber*
2. *a_0 nicht durch p^2 teilbar ist.*

Dann ist $p(x)$ in $\mathbb{Q}[x]$ irreduzibel.

Beweis. Das Argument des Beispiels funktioniert allgemein: Wegen des Lemmas von Gauß genügt es zu zeigen, dass es keine nichtkonstanten Polynome $b(x) = b_m x^m + \cdots + b_1 x + b_0, c(x) = c_\ell x^\ell + \cdots + c_1 x + c_0 \in \mathbb{Z}[x]$ gibt mit $f(x) = b(x)c(x)$.

Angenommen wir hätten eine solche Faktorisierung, dann würde für die Restklassen $\overline{b}(x), \overline{c}(x), \overline{f}(x) \in \mathbb{F}_p[x]$ der Polynome modulo p gelten, dass

$$\overline{b}(x)\overline{c}(x) = \overline{f}(x) = [a_n]x^n$$

mit $a_n \neq 0$ weil f primitiv war. Da die einzigen Teiler des Polynoms x^n die Polynome der Form x^m sind[10], folgt dass $\overline{b}(x) = [b_m]x^m, \overline{c}(x) = [c_\ell]x^\ell$ mit $\ell + m = n$. Insbesondere ist $[b_0] = [c_0] = 0 \in \mathbb{F}_p$. Dann ist aber $b_0 c_0 = a_0$ durch p^2 teilbar, was im Widerspruch zur Annahme steht. □

[10] Ist Ihnen das klar?

Damit können wir den Beweis für die Irreduzibilität von $\Phi_5(x) = \frac{x^5-1}{x-1}$ für jede Primzahl wiederverwenden.

Beweis der Behauptung zum Minimalpolynom von ζ_p. Es genügt zu zeigen, dass

$$\begin{aligned} f(y) = \Phi(y+1) &= \frac{(y+1)^p - 1}{y} \\ &= \frac{(\sum_{k=0}^{p} \binom{p}{k} y^k) - 1}{y} = \sum_{k=1}^{p} \binom{p}{k} y^{k-1} \\ &= y^{p-1} + \binom{p}{p-1} x^{p-2} + \cdots + \binom{p}{2} y + p \end{aligned}$$

irreduzibel ist. Für die Binomialkoeffizienten kennen wir aber die Formel

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

in denen der Nenner durch p teilbar ist, aber der Zähler für $1 \leq k < p$ nicht. Also erfüllt f die Voraussetzung des Eisensteinkriteriums und ist darum irreduzibel. □

Bemerkung (Forbenius-Homomorphismus)**.** Die Beobachtung, dass die Binomialkoeffizienten $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ für $1 \leq k \leq p-1$ durch p teilbar sind, bedeutet, dass diese in jedem Körper der Charakteristik p gleich 0 sind, denn dann gilt $[p] = 0$. Die allgemeine binomische Formel

$$\begin{aligned} (x+y)^p &= \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} \\ &= x^p + px^{p-1}y + \binom{p}{p-2} x^{p-2}y^2 + \cdots + \binom{p}{2} x^2 y^{p-2} + pxy^{p-1} + y^p \end{aligned}$$

vereinfacht sich also in Körpern der Charakteristik $p > 0$ zur skandalösen Formel

$$(x+y)^p = x^p + y^p \in K[x] \text{ wenn } \operatorname{char}(K) = p.$$

Das bedeutet, dass die Abbildung

$$\begin{aligned} \operatorname{Frob}_p \colon K &\to K \\ a &\mapsto \operatorname{Frob}_p(a) := a^p \end{aligned}$$

ein Körperhomomorphismus ist, denn

$$1^p = 1, (a+b)^p = a^p + b^p, (a \cdot b)^p = a^p \cdot b^p.$$

Insbesondere gilt in $\mathbb{F}_p$, dass

$$a^p = a$$

für alle a, denn für $\mathbb{Z}/p\mathbb{Z}$ ist jeder Körperhomomorphismus $F \colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ eindeutig durch $F(1) = 1$ bestimmt.

Nachtrag: Eindeutigkeit der Primfaktorzerlegung ($\mathbb{Z}, K[x], \dots$)

Wir haben gerade verwendet, dass die einzigen Teiler von x^n im Polynomring $K[x]$ die Polynome der Form $c \cdot x^m$ mit $m \leq n, c \in K \setminus \{0\}$ sind. Wahrscheinlich konnten Sie sich das selbst überlegen. Das ist aber auch eine Gelegenheit, um uns zu überlegen, warum es sowohl in den ganzen Zahlen $\mathbb{Z}$ als auch dem Polynomring $K[x]$ eine eindeutige Zerlegung in Primfaktoren gibt.

Lassen Sie uns zunächst versuchen, zu formulieren, was wir damit meinen. In $\mathbb{Z}$ sind Primzahlen p durch $\pm 1, \pm p$ teilbar, die Zahl $-p$ ist also genauso wenig faktorisierbar wie $p = (-1) \cdot (-p)$ und Polynomen können wir immer durch Elemente in $K \setminus 0$ teilen. Kurz, Faktorisierungen $f = a \cdot b$ werden immer nur bis auf Elemente eindeutig sein, durch die wir teilen können. Darum führen wir die folgenden Sprechweisen ein.

Definition. 1. Die *Einheiten* R^* in einem Ring R ist die Teilmenge der Elemente, die ein multiplikatives inverses besitzen:

$$R^* := \{r \in R \mid \exists r^{-1} \in R \text{ s.d. } r \cdot r^{-1} = 1\}.$$

2. Ein Element $r \in R \setminus \{0\}$ eines nullteilerfreien Rings R heißt *irreduzibel* wenn r keine Einheit ist und aus $r = a \cdot b$ in R folgt, dass entweder a oder b eine Einheit ist.

Beispiel 29. 1. Die Einheiten in $\mathbb{Z}$ sind $\mathbb{Z}^* = \{\pm 1\}$, in einem Körper K ist $K^* = K \setminus \{0\}$ und die Einheiten in $K[x]$ sind K^*, d.h. die konstanten Polynome $\neq 0$.

2. Es ist nicht immer ganz offensichtlich, welche Elemente eines Rings multiplikative Inverse besitzen und welche nicht. Zum Beispiel ist[11]

$$\mathbb{Z}[i]^* = \{\pm 1, \pm i\},$$

aber in $\mathbb{Z}[\sqrt{2}]$ ist $\sqrt{2}$ keine Einheit, dafür gilt aber

$$(1+\sqrt{2})(1-\sqrt{2}) = 1 - 2 = -1$$

also $(1+\sqrt{2})^{-1} = -(1-\sqrt{2})$. Darum ist $(1+\sqrt{2})$ in $\mathbb{Z}[\sqrt{2}]$ eine Einheit und damit auch alle Potenzen $(1+\sqrt{2})^n$. Die sind alle verschieden, weil $|1+\sqrt{2}| > 1$.

[11] Das ist eine Knobelaufgabe für Sie.

Was soll „jedes Element besitzt eine eindeutige Primfaktorzerlegung“ bedeuten? In $\mathbb{Z}$ können wir jedes Element schreiben als

$$n = (\pm 1) \cdot p_1 \cdot \dots \cdot p_m.$$

Definition. Ein nullteilerfreier Ring R besitzt eindeutige Primfaktorzerlegungen wenn für jedes Element $r \in R \setminus \{0\}$ gilt:

1. r lässt sich als Produkt

$$r = \varepsilon \cdot p_1 \cdot \dots \cdot p_m$$

schreiben, wobei $p_1, \dots, p_m \in R$ irreduzible Elemente und $\varepsilon \in R^*$ sind und

2. diese Schreibweise eindeutig bis auf Permutation der p_i und Multiplikation mit Einheiten ist.

Solche Ringe heißen *faktoriell*.

Auf englisch ist die Bezeichung UFD für „unique factoization domain“ üblich.

Behauptung 30 (Eindeutigkeit der Primfaktorzerlegung)**.** *Die Ringe der ganzen Zahlen $\mathbb{Z}$ und Polynomringe $K[x]$ mit Koeffizienten in einem Körper sind faktoriell.*

Außerdem gilt: Ist R faktoriell, so auch der Polynomring $R[x]$ mit Koeffizienten in R.

Bemerkung. Die Implikation (R faktoriell)$\Rightarrow$ ($R[x]$ faktoriell) zeigt, dass auch in $\mathbb{Z}[x]$, in Polynomringen in mehreren Variablen $K[x_1, \dots, x_n]$ und auch in $\mathbb{Z}[x_1, \dots, x_n]$ eindeutige Primfaktorzerlegungen gibt.

Für mehrere Variablen ist das nicht so offensichtlich, zum Beispiel sehen Sie vielleicht schon ür $(a+b)(c+d) = ac + bd + ad + bc$ nicht gleich, dass Sie nicht auch andere lineare Terme ausklammern können.

Beweis für ganze Zahlen und Polynomringe. Ist R einer der Ringe $\mathbb{Z}$ oder $K[x]$, so können wir die *Existenz* von Faktorisierungen mit Induktion (entweder über $|r|$ für $R = \mathbb{Z}$ oder $\operatorname{Grad}(r)$ für $R = K[x]$) zeigen:

Ist $a \in R^*$ eine Einheit, so ist nichts zu zeigen. (Das zeigt auch den Induktionsanfang $|r| = 1$, bzw. $\operatorname{Grad}(r) = 0$.)

Ist $r \in R \setminus \{0\}$, so ist entweder r irreduzibel, oder wir können r schreiben als $r = a \cdot b$ mit $a, b \in R \setminus R^*$.

Dann gilt im Fall $R = \mathbb{Z}$ dass $1 < |a| < |r|$ und $1 < |b| < |r|$ und im Fall $R = K[x]$ gilt $\operatorname{Grad}(a) < \operatorname{Grad}(r), \operatorname{Grad}(b) < \operatorname{Grad}(r)$. Also besitzen a, b nach Induktionsvoraussetzung Faktorisierungen in irreduzible Elemente.

Die *Eindeutigkeit* folgt ebenso mit Induktion (diesmal über die Länge m einer Faktorisierung $r = \varepsilon \cdot p_1 \cdot \dots \cdot p_m$) aus der Aussage:

Für die Ringe $\mathbb{Z}, K[x]$ gilt: Ist $p \in R$ irreduzibel und teilt p ein Produkt $a \cdot b$ in R, so teilt p einen der Faktoren.

Das gilt, da aus der Voraussetzung $p | a \cdot b$ im Quotienten $R/(p)$ die Gleichung $0 = [a] \cdot [b]$ wird. Da wir sowohl für Primzahlen als auch für irreduzible Polynome gesehen haben, dass $R/(p)$ ein Körper ist, folgt daraus $[a] = 0$ oder $[b] = 0$. Also ist a oder b durch p teilbar.

Haben wir also zwei Faktorisierungen

$$\varepsilon \cdot p_1 \cdot \dots \cdot p_m = \varepsilon' \cdot q_1 \cdot \dots \cdot q_\ell$$

so teilt p_m die rechte Seite, also auch einen der Faktoren q_i, d.h. $q_i = \epsilon'' p_m$.

Dann können wir aber beide Seiten durch p_m teilen und erhalten zwei kürzere, gleiche Zerlegungen, die nach Induktion bis auf Reihenfolge und Einheiten übereinstimmen. □

Um zu zeigen, dass für jeden faktoriellen Ring R auch der Polynomring $R[x]$ faktoriell ist, können wir das Argument, dass Sie auf

dem Übungsblatt genutzt haben, um zu zeigen, dass für primitive Polynome $p(x) \in \mathbb{Z}[x]$ alle Teiler $\mathbb{Q}[x]$ schon Teiler in $\mathbb{Z}[x]$ definieren wiederverwenden. Dort war die Strategie:

1. Das Produkt primitiver Polynome ist wieder primitiv. (Argument: sonst hätte $\mathbb{Z}/p\mathbb{Z}[x]$ Nullteiler).
2. Ist $p(x) = a(x)b(x)$ eine Zerlegung in $\mathbb{Q}$, dann können wir beide Seiten mit dem Hauptnenner der rechten Seite multiplizieren, um eine Zerlegung von $Np(x)$ in $\mathbb{Z}$ in primitive Polynome zu erhalten, wegen 1. muss dann $N = 1$ gelten.

Das Argument funktioniert in faktoriellen Ringen genauso, weil wir dort auf Grund der eindeutigen Primfaktorzerlegung wieder von primitiven Polynomen sprechen können und jedes Polynom $p(x) \in Q(R)[x]$ mit einer bis auf Einheiten eindeutigen Zahl $c \in \mathbb{Q}$ multiplizieren können, so dass $c \cdot p(x) \in R[x]$ primitiv ist.

Lassen Sie uns einmal üben, diese informelle Beobachtung zu formalisieren:

Definition. Sei R ein faktorieller Ring. Ein Polynom $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ heißt *primitiv* wenn es kein irreduzibles Element $p \in R$ gibt, das alle a_i teilt.

Notation 31. In einem Ring R schreiben wir $p|a$ für *p teilt a*, d.h. $p, a \in R$ und es gibt ein Element $c \in R$ mit $a = p \cdot c$.

Damit können wir den ersten Schritt unseres Arguments für faktorielle Ringe formulieren:

Lemma 32. *Ist R ein faktorieller Ring und sind $a(x), b(x) \in R[x]$ primitive Polynome, so ist auch das Produkt $a(x) \cdot b(x)$ primitiv.*

Beweis. Angenommen $a(x) \cdot b(x)$ ist nicht primitiv, dann gibt es ein irreduzibles Element $p \in R$, das alle Koeffizienten des Polynoms teilt, d.h. die Restklasse des Polynoms in $R/pR[x]$ verschwindet:

$$[0] = [a(x) \cdot b(x)] = [a(x)] \cdot [b(x)].$$

Der Ring R/pR ist aber nach dem Übungsblatt 4 nullteilerfrei, denn in faktoriellen Ringen gilt wegen der Eindeutigkeit der Zerlegung in irreduzible Elemente, dass

$$(p \mid c \cdot d) \Rightarrow (p|c \text{ oder } p|d).$$

Also ist auch $R/pR[x]$ nullteilerfrei (denn der führende Koeffizient eines Produktes von Polynomen ist das Produkt der führenden Koeffizienten der Polynome). Dann muss aber $[a(x)] = 0$ oder $[b(x)] = 0$ gelten, was im Widerspruch zur Annahme, dass $a(x), b(x)$ primitiv waren steht. □

Um das Argument, dass wir aus Zerlegungen in $\mathbb{Q}[x]$ auch Zerlegungen in $\mathbb{Z}[x]$ bekommen zu übertragen, müssen wir nur „Hauptnenner“ übersetzen:

Lemma 33. *Ist R ein faktorieller Ring, so lässt sich jedes Element $a \in Q(R)$ in der Form*

$$a = \epsilon \prod_{i=1}^{r} p_i^{n_i}$$

schreiben, wobei $\epsilon \in R^*$, $p_1, \dots, p_r$ paarweise teilerfremde irreduzible Elemente von R und $n_i \in \mathbb{Z} \setminus \{0\}$ sind.

Diese Zerlegung ist bis auf Reihenfolge und Multiplikation mit Skalaren eindeutig.

Beweis. Da wir nach Konstruktion jedes Element $a \in Q(R)$ im Quotientenkörper in der Form $\frac{b}{d}$ mit $b, d \in R, d \neq 0$ schreiben können und b, d eine Zerlegung in irreduzible Elemente besitzen, folgt die Existenz einer Zerlegung von a.

Die Eindeutigkeit folgt auch aus der Eindeutigkeit in R, da wir für zwei Zerlegungen

$$\epsilon \prod_{i=1}^{r} p_i^{n_i} = \epsilon' \prod_{j=1}^{k} q_j^{m_j}$$

die Gleichung mit den Termen mit negativen Exponenten multiplizieren können und damit zwei Zerlegungen in R erhalten. □

Damit können wir nun zeigen, dass für einen faktoriellen Ring R der Polynomring $R[x]$ wieder faktoriell ist.

Beweis (Polynomring wieder faktoriell). Ist R faktoriell und $a(x) \in R[x] \subset Q(R)[x]$ ein Polynom. Da Polynomringe über Körpern faktoriell sind, können wir $a(x)$ in $Q(R)[x]$ in irreduzible Polynome faktorisieren.

$$a(x) = c \prod_{i=1}^{n} q_i(x) \in Q(R)[x].$$

Für jedes der Polynome $q_i(x)$ existiert ein $c_i \in Q(R)$, so dass $c_i q_i(x) \in R[x]$ primitiv ist.[12] Ersetzen wir q_i durch $c_i q_i(x)$ und c durch $c / \prod c_i$, so erhalten wir also

$$a(x) = c \prod_{i=1}^{n} q_i(x) \in Q(R)[x]$$

mit primitiven Polynomen $q_i(x)$, die sogar in $Q(R)[x]$ irreduzibel sind, also erst recht in $R[x]$.

Schreiben wir nun $c = \epsilon \prod_{i=j}^{r} p_j^{n_j}$ als Produkt von irreduziblen Elementen in R und multiplizieren die Gleichung mit dem Nenner N von c erhalten wir

$$Na(x) = (cN) \prod_{i=1}^{n} q_i(x).$$

Da N keinen der Faktoren von cN teilt, muss N alle Koeffizienten von $\prod_{i=1}^{n} q_i(x)$ teilen, aber dieses Produkt ist nach unserem Lemma wieder primitiv. Also ist $N = 1$ und wir haben

$$a(x) = \epsilon \prod_{j=1}^{r} p_j^{n_j} \prod_{i=1}^{n} q_i(x)$$

[12] In der Vorlesung haben wir diese Behauptung auf Ihren Wunsch hin noch einmal genauer ausgearbeitet.

als Produkt von irreduziblen Elementen geschrieben.

Die Eindeutigkeitsaussage folgt, da die Zerlegung in irreduzible Elemente in $Q(R)[x]$ und R jeweils eindeutig bis auf Reihenfolge und Multiplikation mit Einheiten ist. □

Beispiel 34. Die Aussage, dass $K[x]$ für jeden Körper faktoriell ist, können wir auf interessante Weise verwenden, um zu zeigen, dass ein Polynom in $\mathbb{Z}[x]$ und damit wegen des Lemmas zu primitiven Polynomen auch in $\mathbb{Q}[x]$ irreduzibel ist. Zum Beispiel ist das (primitive) Polynom

$$p(x) = x^5 + x^2 - x + 4,$$

in $\mathbb{Z}[x]$ und damit auch in $\mathbb{Q}[x]$ irreduzibel, denn:

1. modulo 2, also in $\mathbb{F}_2[x]$ ist

   $$x^5 + x^2 - x + 4 = x^5 + x^2 - x = (x^4 + x - 1)x$$

   und die Faktoren $(x^4 + x - 1)$ und x sind irreduzibel, denn $(x^4 + x - 1)$ ist nicht durch ein lineares Polynom teilbar, da es in $\mathbb{F}_2$ keine Nullstelle hat und das einzige irreduzible Polynom vom Grad 2 in $\mathbb{F}_2[x]$ ist $x^2 + x + 1$, aber $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq (x^4 + x - 1) \in \mathbb{F}_2[x]$, also ist der Ausdruck auch nicht durch Polynome vom Grad 2 teilbar.

2. modulo 3, also in $\mathbb{F}_3[x]$ ist

   $$x^5 + x^2 - x + 1 = (x^2 + 1)(x^3 - x + 1).$$

   Von beiden Faktoren haben Sie sich schon überlegt, dass diese in $\mathbb{F}_3[x]$ irreduzibel sind, da die Elemente von $\mathbb{F}_3$, also $0, 1, -1$ jeweils keine Nullstellen sind.

Wäre $p(x) = a(x)b(x)$ eine Faktorisierung in $\mathbb{Z}[x]$ so müssten die Faktoren modulo 2 also Grad 1 und 4 haben, modulo 3 die Grade $2, 3$ und außerdem muss $\mathrm{Grad}(a) + \mathrm{Grad}(b) = 5$ gelten. Das ist nicht möglich.

Damit möchte ich den Abschnitt über konstruierbare Zahlen zunächst beenden, auf einige der Fragen kommen wir später noch einmal zurück.

Rückblick: Welche allgemeinen Konzepte haben wir kennen gelernt?

Anlässlich der klassischen Fragen haben wir in diesem Kapitel eine Reihe von Begriffen und allgemeinen Resultaten kennengelernt:

1. Körpererweiterungen
   - Grad einer Erweiterung: $[L : K] = \dim_K L$.
   - Multiplikativität der Dimension $[K_2 : K_1][K_1 : K_0] = [K_2 : K_0]$.
   - Charakteristik eines Körpers.

- Endliche Körper haben p^n Elemente.
- Elemente hinzufügen (=adjungieren) $K(\alpha)$.
- Formales Hinzufügen von Nullstellen als Quotienten:

$$K[x]/(p(x))$$

- Algebraische und transzendente Elemente.
- Minimalpolynome.

2. Körperhomomorphismen:
   - sind automatisch injektiv.
   - Körperhomomorphismen $K[x]/p(x) \to L$ entsprechen Nullstellen von p in $L \supset K$.
   - Frobenius-Homomorphismus falls $\mathrm{char}(K) = p > 0$.
3. Nullteilerfreie Ringe, Körper der rationalen Funktionen $K(x)$ und Quotientenkörper $Q(R)$ von nullteilerfreien Ringen R.
4. Irreduzibilität von Polynomen:
   - Gauß-Lemma: Irreduzibilität in $\mathbb{Q}[x]$ und $\mathbb{Z}[x]$.
   - Eisensteinkriterium.
   - Beispiel: Einheitswurzeln und Kreisteilungskörper $\mathbb{Q}(\zeta_N)$.
   - Faktorielle Ringe/Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}, K[x]$.
   - R faktoriell $\Rightarrow R[x]$ faktoriell. (Argument: Schreibe Beweis des Gauß-Lemmas für R statt $\mathbb{Z}$ und $Q(R)$ statt $\mathbb{Q}$ ab.)

Von kubischen Gleichungen zur Galoiskorrespondenz

Unser nächstes Ziel ist, zu verstehen, wie wir Lösungsformeln für die Nullstellen von Polynomen $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ finden können und warum die Symmetrien der Nullstellen einerseits für Polynome vom Grad ≤ 4 eine systematische Methode liefern, wie wir Formeln finden können und andererseits für Grad ≥ 5 ein Hindernis dafür erklären.

Beispiele: Grad 2 *und* 3

Quadratische Gleichungen

Lassen Sie uns einfach anfangen. Sie kennen vielleicht mehrere Methoden eine quadratische Gleichung

$$f(x) = x^2 + px + q = 0$$

zu lösen. In der Vorlesung haben wir die folgenden Möglichkeiten gesammelt:

p, q-Formel = quadratische Ergänzung: Die binomische Formel

$$(x + a)^2 = x^2 + 2ax + a^2$$

erklärt uns, dass wir Gleichungen der Form $x^2 + 2ax + a^2 = b$ durch Wurzelziehen als $x = \pm\sqrt{b} - a$ lösen können. Also ist

Bei den Umformungen verwenden wir, dass $2 \neq 0 \in K$, d.h. die Rechung funktioniert nur in Körpern der Charakteristik $\neq 2$

$$\begin{aligned} x^2 + px + q = 0 \qquad & \Leftrightarrow \\ x^2 + 2\frac{p}{2}x + (\frac{p}{2})^2 = (\frac{p}{2})^2 - q & \\ x_{1/2} = \pm\sqrt{\frac{p^2}{4} - q} - \frac{p}{2}. & \end{aligned}$$

Der Satz von Vieta Sind umgekehrt x_1, x_2 die Nullstellen von $p(x) = x^2 + px + q$, so ist $p(x) = (x - x_1)(x - x_2)$ weil wir Nullstellen ausklammern können. Die Gleichung

$$\begin{aligned} f(x) = (x - x_1)(x - x_2) &= x^2 - (x_1 + x_2)x + x_1x_2 \\ &= x^2 + px + q \end{aligned}$$

besagt also

$$\begin{aligned} x_1 + x_2 &= -p \\ x_1x_2 &= q. \end{aligned}$$

Wir können also auch versuchen, dieses Gleichungssystem zu lösen.

ZURÜCKFÜHREN AUF $x^2 - c = 0$ Statt das Problem auf die binomische Formel zurückzuführen, könnten wir auch den linearen Term der Gleichung entfernen, indem wir $x = y - \frac{p}{2}$ einsetzen:

$$\begin{aligned} f(y - \frac{p}{2}) &= y^2 - py + (\frac{p}{2})^2 + py - p\frac{p}{2} + q \\ &= y^2 - \frac{p^2}{4} + q. \end{aligned}$$

Davon sind die Lösungen $y_{1/2} = \pm\sqrt{\frac{p^2}{4} - q}$, das liefert wieder die p,q-Formel für $x_{1/2}$.

DER TERM IN DER WURZEL $p^2 - 4q$ hat im in Termen der Nullstellen eine einfache Bedeutung: Schreiben wir $p = -(x_1 + x_2), q = x_1x_2$ so ist

$$\begin{aligned} p^2 - 4q &= (x_1 + x_2)^2 - 4x_1x_2 \\ &= x_1^2 + 2x_1x_2 + x_2^2 - 4x_2x_2 \\ &= (x_1 - x_2)^2. \end{aligned}$$

Der Ausdruck $(x_1 - x_2)^2$ heißt *Diskriminante* und entscheidet über jedem Körper, ob $f(x)$ eine doppelte Nullstelle hat, in den reellen Zahlen entscheidet das Vorzeichen des Ausdrucks zudem, ob die Nullstellen reell oder komplex sind.

Kubische Gleichungen

Für kubische Gleichungen

$$f(x) = x^3 + ax^2 + bx + c$$

haben die Ansätze, die wir für quadratische Gleichungen verwendet haben nur teilweise Erfolg.

KUBISCHE ERGÄNZUNG ist nicht immer möglich, denn

$$(x + d)^3 = x^3 + 3dx^2 + 3d^2x + d^3$$

und wir können zwar mit $d = \frac{a}{3}$ den ersten Term in die gewünschte Form bringen, aber das führt dann nur zum Ziel, wenn zufällig $b = 3d^2 = \frac{a^2}{3}$ gilt.

DER SATZ VON VIETA für Gleichungen 3. Grades ergibt

$$\begin{aligned} (x - x_1)(x - x_2)(x - x_3) &= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - (x_1x_2x_3) \\ &= x^3 + ax^2 + bx + c \end{aligned}$$

also das Gleichungssystem

$$\begin{aligned} x_1 + x_2 + x_3 &= -a \\ x_1x_2 + x_1x_3 + x_2x_3 &= b \\ x_1x_2x_3 &= -c. \end{aligned}$$

MIT EINER SUBSTITUTION können wir immerhin der quadratischen Term entfernen: Setzen wir $x = y - \frac{a}{3}$ so erhalten wir

$$\begin{aligned} f(y - \frac{a}{3}) &= y^3 - ay^2 + 3(\frac{a}{3})^2 y - \frac{a^3}{27} \\ &\quad + a(y^2 - 2\frac{a}{3}y + \frac{a^2}{9}) + by - b\frac{a}{3} + c \\ &= y^3 + (-\frac{a^2}{3} + b)y + (\frac{2a^3}{27} - \frac{ab}{3} + c) \\ &= y^3 + py + q. \end{aligned}$$

Vergleichen wir das mit dem Satz von Vieta, gilt für diese Gleichung, dass die Summe der Nullstellen $= 0$ ist, wir hatten $x = y - \frac{a}{3}$ gerade um den Schwerpunkt der Nullstellen verschoben.

WAS NUN? Wenn wir eine Lösungsformel suchen, wollen wir die Nullstellen x_1, x_2, x_3 in Termen der Koeffizienten des Polynoms und $\sqrt{\ }, \sqrt[3]{\ }$ ausdrücken. Die Koeffizienten sind bis auf Vorzeichen gerade

$$\begin{aligned} s_1 &= x_1 + x_2 + x_3 \\ s_2 &= x_1x_2 + x_1x_3 + x_2x_3 \\ s_3 &= x_1x_2x_3. \end{aligned}$$

Bei Bedarf könnten wir annehmen, das $s_1 = 0$ ist.

Das Problem könnte ich also als Erweiterungsproblem für die Ringe

$$\begin{aligned} \mathbb{C}[s_1, s_2, s_3] &\to \mathbb{C}[x_1, x_2, x_3] \\ s_1 &\mapsto x_1 + x_2 + x_3 \\ s_2 &\mapsto x_1x_2 + x_1x_3 + x_2x_3 \\ s_3 &\mapsto x_1x_2x_3 \end{aligned}$$

Wobei wir noch nachprüfen sollten, dass die Abbildung injektiv ist. Darüber denken wir später nach.

auffassen, d.h., wie bei Körpererweiterungen würde ich gerne zu $\mathbb{C}[s_1, s_2, s_3]$ Wurzeln und 3-te Wurzeln hinzufügen, so dass ich am Ende eine Beschreibung von $\mathbb{C}[x_1, x_2, x_3]$ erhalte.

Sie Ausdrücke für s_1, s_2, s_3 sind hierbei symmetrisch in den x_i, d.h. die Ausdrücke ändern sich nicht, wenn wir die Indizes vertauschen:

$$s_i(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}) = s_i(x_1, x_2, x_3) \text{ für alle } \sigma \in S_3.$$

DIE ERSTE FRAGE welche Wurzeln wir hinzufügen können ist dann: Sehe ich einen Ausdruck $p(x_1, x_2, x_3)$ in den x_i, so dass $p(x_1, x_2, x_3)^2$ als Polynom in den s_i geschrieben werden kann, aber $p(x_1, x_2, x_3)$ nicht? Kandidaten dafür wären Ausdrücke p, die nicht symmetrisch sind, für die aber das Quadrat p^2 symmetrisch ist.

Für quadratische Polynome mussten wir nur die Wurzel aus der Diskriminante

$$(x_1 - x_2) = \sqrt{(x_1 - x_2)^2} = \sqrt{p^2 - 4q}$$

hinzufügen.

Das Analogon der Diskriminante für kubische Polynome wäre vielleicht

$$(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$$

denn dieser Ausdruck entscheidet sicher wieder, ob ein Polynom eine doppelte Nullstelle hat. Außerdem gilt für die Wurzel

$$d := (x_1 - x_2)(x_1 - x_3)(x_2 - x_3),$$

dass sich der Ausdruck beim Vertauschen zweier Variablen gerade um ein Vorzeichen ändert. Es gilt also für alle Permutationen $\sigma \in S_3$:

Probieren Sie das aus: Welche Terme ändern das Vorzeichen wenn Sie $1 \leftrightarrow 2$ vertauschen, bzw $1 \leftrightarrow 3$,$2 \leftrightarrow 3$?

$$(x_{\sigma(1)} - x_{\sigma(2)})(x_{\sigma(1)} - x_{\sigma(3)})(x_{\sigma(2)} - x_{\sigma(3)}) = \mathrm{sign}(\sigma)(x_1 - x_2)(x_1 - x_3)(x_2 - x_3).$$

Insbesondere ist das Quadrat dieses Ausdrucks invariant.

Um zu sehen, ob wir $D = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$ in den s_1, s_2, s_3 ausdrücken können, haben wir den Computer, genauer Sage zur Hilfe genommen, damit wir das nicht per Hand ausmultiplizieren müssen.

Das lieferte:

$$\mathrm{expand}(D) = x_1^4x_2^2 - 2x_1^3x_2^3 + x_1^2x_2^4 + \cdots.$$

Um einen Ausdruck in den s_i zu finden, in dem $x_1^4x_2^2$ vorkommt, haben Sie mir $s_1^2s_2^2$ vorgeschlagen (s_3 kann nicht dabei sein, denn das enthält x_3 und in Potenzen von s_2 kommt nur $(x_1x_2)^n$ also nur gleiche Exponenten vor, da $x_1^4x_2^2 = x_1^2(x_1x_2)^2$ liegt es nahe, $s_1^2s_2^2$ auszuprobieren).

Damit hatten wir ausprobiert:

$$\mathrm{expand}(D - s_1^2s_2^2) = -4x_1^4x_2x_3 - 4x_1^3x_2^3 + \cdots.$$

Sie schlugen als nächsten Versuch vor $4s_1^3s_3$ zu subtrahieren, da dieser Ausdruck den Term $4x_1^4x_2x_3 = 4x_1^3(x_1x_2x_3)$ enthält.

Nach einigen Schritten fanden Sie so:

$$D = s_1^2s_2^2 - 4s_1^3s_3 - 4s_2^3 + 18s_1s_2s_3 - 27s_3^2.$$

Ist $s_1 = 0$ vereinfacht sich das zum freundlicheren Term

$$D = -4s_2^3 - 27s_3^2.$$

Für $f(x) = x^3 + px + q$ ist die Diskriminante also

$$-(4p^3 + 27q^2).$$

DAMIT HABEN WIR eine erste Erweiterung

$$\underbrace{\mathbb{C}[s_1, s_2, s_3]}_{\substack{\text{Elemente invariant unter} \\ \text{Vertauschung der } x_i}} \subsetneq \underbrace{\mathbb{C}[s_1, s_2, s_3](d)}_{\substack{\text{Elemente noch invariant unter} \\ \text{zyklischer Vertauschung}}} \subseteq \mathbb{C}[x_1, x_2, x_3]$$

gefunden.

Der Ausdruck $d = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ ist noch unter der zyklischen Vertauschung $1 \to 2 \to 3 \to 1$, also $\sigma = \binom{123}{231}$ invariant, da $\mathrm{sign}(\sigma) = 1$ ist.

Wir suchen noch eine 3. Wurzel also einen Term F, für den $F^3 \in \mathbb{C}[s_1, s_2, s_3](d)$ liegt. Dann muss insbesondere F^3 wieder unter σ invariant sein. Praktisch wäre dazu ein Term für den

$$F(x_2, x_3, x_1) = \zeta_3^{\pm 1} F(x_1, x_2, x_3)$$

gilt, wobei $\zeta_3 = e^{\frac{2\pi i}{3}}$ eine 3-te Einheitswurzel und damit $\zeta_3^3 = 1$ ist.

So ein Term lässt sich leicht raten:

$$s_1'(x_1, x_2, x_3) := x_1 + \zeta_3 x_2 + \zeta_3^2 x_3$$

erfüllt zum Beispiel

$$\begin{aligned} s_1'(x_2, x_3, x_1) &= x_2 + \zeta_3 x_3 + \zeta_3^2 x_1 \\ &= \zeta_3^{-1}(x_1 + \zeta_3 x_2 + \zeta_3^2 x_3) \\ &= \zeta_3^{-1} s_1'(x_1, x_2, x_3). \end{aligned}$$

Und ähnlich erfüllt

$$s_1''(x_1, x_2, x_3) := x_1 + \zeta_3^2 x_2 + \zeta_3 x_3,$$

dass

$$s_1''(x_2, x_3, x_1) = \zeta_3 s_1''(x_1, x_2, x_3).$$

Bemerkung. Wenn Sie sich daran erinnern, dass $1 + \zeta_3 + \zeta_3^2 = 0$ gilt, dann können wir aus den Werten

$$\begin{aligned} s_1(x_1, x_2, x_3) &= x_1 + x_2 + x_3 \\ s_1'(x_1, x_2, x_3) &= x_1 + \zeta_3 x_2 + \zeta_3^2 x_3 \\ s_1''(x_1, x_2, x_3) &= x_1 + \zeta_3^2 x_2 + \zeta_3 x_3 \end{aligned}$$

die Nullstellen x_1, x_2, x_3 sofort ausrechnen, zum Beispiel ist die Summe dieser Zahlen dann $3x_1$, bzw.

$$\begin{aligned} x_1 &= \frac{1}{3}(s_1 + s_1' + s_1'') \\ x_2 &= \frac{1}{3}(s_1 + \zeta_3^2 s_1' + \zeta_3 s_1'') \\ x_3 &= \frac{1}{3}(s_1 + \zeta s_1' + \zeta_3^2 s_1''). \end{aligned}$$

Haben wir unser Polynom zuvor in die vereinfachte Form $f(x) = x^3 + px + q$ gebracht, fallen außerdem die Terme mit $s_1 = 0$ weg.

Sie sollten selbst einmal, zum Beispiel mit Sage versuchen, für

$$R(x_1, x_2, x_3) := (x_1 + \zeta_3 x_2 + \zeta_3^2 x_3)^3$$

einen Ausdruck in $s_1, s_2, s_3, d = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ zu finden. Damit haben Sie dann

$$s_1'(x_1, x_2, x_3) = \sqrt[3]{R(x_1, x_2, x_3)}$$

geschrieben und da s_1'' aus s_1' dadurch entsteht, dass wir x_2 und x_3 vertauschen, erhalten wir damit sofort auch einen Ausdruck für s_1'' indem wir in der Formel d durch $-d$ ersetzen.

Wenn Sie das geschafft haben und $s_1 = 0$ einsetzen, finden Sie Cardanos Formeln für die Lösungen von $f(x) = x^3 + px + q$, nämlich:

$$x_1 = \sqrt[3]{\frac{1}{2}(-q + \sqrt{q^2 + \frac{4p^3}{27}})} + \sqrt[3]{\frac{1}{2}(-q - \sqrt{q^2 + \frac{4p^3}{27}})}$$
$$x_2 = \zeta_3^2\sqrt[3]{\frac{1}{2}(-q + \sqrt{q^2 + \frac{4p^3}{27}})} + \zeta_3\sqrt[3]{\frac{1}{2}(-q - \sqrt{q^2 + \frac{4p^3}{27}})}$$
$$x_3 = \zeta_3\sqrt[3]{\frac{1}{2}(-q + \sqrt{q^2 + \frac{4p^3}{27}})} + \zeta_3^2\sqrt[3]{\frac{1}{2}(-q - \sqrt{q^2 + \frac{4p^3}{27}})}.$$

Hierbei müssen Sie aufpassen, dass die beiden dritten Wurzeln – also die Ausdrücke für s_1', s_2' – nicht unabhängig voneinander gewählt werden können, denn $s_1' \cdot s_1''$ ist invariant unter Permutationen, genauer ist

$$\begin{aligned} s_1' \cdot s_1'' &= (x_1 + \zeta_3 x_2 + \zeta_3^2 x_3)(x_1 + \zeta_3^2 x_2 + \zeta_3 x_3) \\ &= x_1^2 + x_2^2 + x_3^2 + \underbrace{(\zeta + \zeta^2)}_{=-1}(\sum_{i<j} x_i x_j) \\ &= s_1^2 - 3s_2. \end{aligned}$$

Weil wir $s_1 = 0$ angenommen hatten, ergibt sich für die dritten Wurzeln, dass das Produkt $-\frac{p}{3}$ sein.

Aufgabe. Bitte machen Sie einmal die Probe und rechnen nach, dass die Ausdrücke dann tatsächlich die Gleichung $x_i^3 + px_i + q = 0$ erfüllen. Diese Rechnung ist überraschend kurz möglich, versuchen Sie es!

DAMIT haben wir auf recht systematische Weise eine Lösungsformel für kubische Gleichungen gefunden. Es gibt dafür kürzere Herleitungen, die dann aber Tricks verwenden. Die systematische Herangehensweise gefällt mir besser, weil ich mir das Prinzip einerseits gut merken kann und damit weiß, dass ich mir die Formeln notfalls herleiten kann und andererseits haben wir damit auch ein Grundprinzip gefunden, dass wir auch für Gleichungen höheren Grades ausprobieren können. Im nächsten Abschnitt werden wir sehen, was davon allgemein funktioniert und wieso die Struktur der Permutationsgruppe S_n für $n > 4$ ein Hindernis dafür liefert, eine allgemeine Lösungsformel in Termen von Wurzeln zu finden.

Die allgemeine Gleichung und symmetrische Polynome

Für Polynome

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

vom Grad n können wir die Vieta-Berechnung genau wie für $n = 2, 3$ durchführen: Multiplizieren wir

$$(x - x_1)(x - x_2) \cdots (x - x_n)$$

aus, so ist der Koeffizient von x^{n-j} genau die Summe aus allen Möglichkeiten in $n - j$-Faktoren den Summanden x und in allen anderen den Summanden x_i auszuwählen, d.h.:

Wenn Sie noch üben möchten, Formeln zu lesen und Induktionsbeweise aufzuschreiben, können Sie diese Formel noch einmal mit Induktion beweisen.

$$\begin{aligned}(x - x_1)(x - x_2) \cdots (x - x_n) &= \sum_{j=0}^{n} \Big((-1)^j \sum_{\substack{I \subseteq \{1,\dots,n\} \\ \#I = j}} \prod_{i \in I} x_i \Big) x^{n-j} \\ &= \sum_{j=0}^{n} \Big((-1)^j \sum_{1 \le i_1 < i_2 < \cdots < i_j \le n} x_{i_1} x_{i_2} \dots x_{i_j} \Big) x^{n-j}.\end{aligned}$$

Notation 35 (Elementarsymmetrische Polynome)**.** Die Koeffizienten

$$\begin{aligned}s_j(x_1, \dots, x_n) &:= \sum_{1 \le i_1 < i_2 < \cdots < i_j \le n} x_{i_1} x_{i_2} \dots x_{i_j} \\ &= \sum_{\substack{I \subseteq \{1,\dots,n\} \\ \#I = j}} \prod_{i \in I} x_i\end{aligned}$$

für $1 \le j \le n$ in der obigen Formel heißen *elementarsymmetrische Polynome*.

Beispiel 36. Für $j = 1$ finden wir wieder

$$s_1(x_1, \dots, x_n) = x_1 + \cdots + x_n,$$

für $j = n$

$$s_n(x_1, \dots, x_n) = x_1 \cdots x_n.$$

Für $j = 2$ sind wir

$$s_2(x_1, \dots, x_n) = \sum_{1 \le i < j \le n} x_i x_j$$

im Fall $n = 3$ schon begegnet.

Definition. Ist R ein Ring, so heißt ein Polynom $f(x_1, \dots, x_n) \in R[x_1, \dots, x_n]$ *symmetrisch* wenn für alle Permutationen $\sigma \in S_n$ gilt, dass

Erinnerung:

$S_n = \{\sigma \colon \{1, \dots, n\} \to \{1, \dots, n\} \mid \sigma \text{ bijektiv}\}$

$$f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = f(x_1, \dots, x_n).$$

Wir bezeichnen die Menge der symmetrischen Polynome mit

$$R[x_1, \dots, x_n]^{S_n} := \{f \in R[x_1, \dots, x_n] \mid f \text{ symmetrisch}\}.$$

Bemerkung. 1. $R[x_1, \dots, x_n]^{S_n} \subseteq R[x_1, \dots, x_n]$ ist ein Unterring.

2. Die elmentarsymmetrischen Polynome sind symmetrisch, da as Polynom $(x - x_1)(x - x_2) \cdots (x - x_n) \in R[x][x_1, \dots, x_n]$ symmetrisch ist.

3. Für jedes $k \in \mathbb{N}$ ist die Summe der k-ten Potenzen

$$P_k(x_1, \dots, x_n) := x_1^k + x_2^k + \cdots + x_n^k$$

symmetrisch.

Für die Diskriminante hatten wir einen Ausdruck in Termen der symmetrischen Polynome gefunden, indem wir systematisch die „höchste x_1-Potenz“ entfernt haben. Lassen Sie uns das zur Erinnerung an einem einfachen Beispiel ausprobieren. Das Polynom

$$P_2(x_1, \dots, x_n) = x_1^2 + x_2^2 + \cdots + x_n^2$$

ist symmetrisch, Terme mit x_1^2 können wir nur mit $s_1^2 = (x_1 + \cdots + x_2)^2$ erhalten und es ist

$$(x_1 + \cdots + x_2)^2 = x_1^2 + \cdots + x_n^2 + 2\sum_{i<j} x_i x_j.$$

Also ist

$$x_1^2 + x_2^2 + \cdots + x_n^2 = s_1^2 - 2s_2.$$

Das funktioniert allgemein:

Satz 37 (Satz über symmetrische Polynome)**.** *Ist R ein Körper oder $R = \mathbb{Z}$ so lässt sich jedes symmetrische Polynom*

$$p(x_1, \dots, x_n) \in R[x_1, \dots, x_n]^{S_n}$$

eindeutig als Polynom in den $s_j(x_1, \dots, x_n)$ schreiben, d.h. die Abbildung

$$\begin{aligned} R[s_1, \dots, s_n] &\to R[x_1, \dots, x_n]^{S_n} \\ q(s_1, \dots, s_n) &\mapsto q(s_1(x_1, \dots, x_n), \dots, s_n(x_1, \dots, x_n)) \end{aligned}$$

ist ein Isomorphismus.

Wenn Sie den Beweis ganz genau anschauen, werden Sie sehen, dass das Resultat für jeden kommutativen Ring mit 1 stimmt.

Um unsere Verfahren aus den Beispielen allgemein zu formulieren, sollten wir zunächst erklären, was wir mit „größtem Term“ genau meinen.

Zur Vereinfachung kürzen wir die Schreibweise für die Terme von Polynomen ab indem wir für $\underline{d} = (d_1, \dots, d_n) \in \mathbb{N}_0^n$

$$\underline{x}^{\underline{d}} := x_1^{d_1} \cdots x_n^{d_n} = \prod_{i=1}^{n} x_i^{d_i}$$

definieren.

Nennen wir die Variablen a, b, c so ist das die Ordnung, die im Lexikon für Wörter $a^3b^2c = aaabbc$ verwendet wird.

Definition (Lexikographische Ordnung)**.** Sind $\underline{d}, \underline{e} \in \mathbb{N}_0^n$ so schreiben wir

$$\underline{x}^{\underline{d}} >_{lex} \underline{x}^{\underline{e}}$$

wenn $d_1 > e_1$ oder ($d_1 = e_1$ aber $d_2 > e_2$) oder ($d_1 = e_1, d_2 = e_2$ aber $d_3 > e_3$) oder …, d.h. wenn es ein $j \geq 1$ gibt so dass

$$\begin{aligned} d_j &> e_j && \text{und} \\ d_i &= e_i && \text{für alle } i < j. \end{aligned}$$

Bemerkung. 1. Die obige Bedingung können wir äquivalent so formulieren: Es gibt ein $j \geq 1$, so dass

$$\begin{aligned} d_1 + \cdots + d_j &> e_1 + \cdots + e_j && \text{und} \\ d_1 + \cdots + d_i &= e_1 + \cdots + e_i && \text{für alle } i < j. \end{aligned}$$

2. Wir schreiben manchmal auch

$$\underline{d} >^{lex} \underline{e}$$

statt

$$\underline{x}^{\underline{d}} >_{lex} \underline{x}^{\underline{e}}$$

, da die Bedingung nur vom Exponenten abhängt.

Die lexikographische Ordnung hat die Eigenschaften:

1. $>_{lex}$ ist eine Ordnungsrelation, d.h. je zwei Elemente $x^{\underline{d}} \neq x^{\underline{e}} \in \mathbb{N}_0^n$ sind vergleichbar, es gilt dann entweder $x^{\underline{d}} >_{lex} x^{\underline{e}}$ oder $x^{\underline{e}} >_{lex} x^{\underline{d}}$ und die Relation ist transitiv.

2. $>_{lex}$ ist mit Multiplikation von Monomen (also Ausdrücken der Form $\underline{x}^{\underline{d}}$) verträglich, d.h. sind $\underline{d}, \underline{d}', \underline{e} \in \mathbb{N}_0^n$ so gilt

$$(x^{\underline{d}} >_{lex} x^{\underline{e}}) \Rightarrow x^{\underline{d}+\underline{d}'} >_{lex} x^{\underline{e}+\underline{d}'},$$

daraus ergibt sich auch

$$(x^{\underline{d}} >_{lex} x^{\underline{e}} \text{ und } x^{\underline{d}'} >_{lex} x^{\underline{e}'}) \Rightarrow x^{\underline{d}+\underline{d}'} >_{lex} x^{\underline{e}+\underline{e}'}.$$

Beispiel 38. Für die Terme des Polynoms $f(x_1, x_2, x_3) = x_1^3x_2^2 + 5x_1^3x_2x_3 + 3x_1^4x_3 + x_2^{12}x_3 + x_3^+x_1$ gilt

$$x_1^4x_3 >^{lex} x_1^3x_2^2 >^{lex} x_1^3x_2x_3 >^{lex} x_1 >^{lex} x_2^{12}x_3 >^{lex} x_3.$$

Damit können wir jetzt präzise fassen, was wir mit dem „größten“ Term in einem Monom $x^{\underline{d}}$ meinen:

Definition (Führender Term und Multigrad)**.** 1. Wir nennen die Abbildung

$$\underline{\deg}^{lex}\colon K[x_1, \ldots, x_n] \to \mathbb{N}_0^n$$
$$p(\underline{x}) := \sum_{\underline{d} \in \mathbb{N}_0^n} a_{\underline{d}} x^{\underline{d}} \mapsto \underline{\deg}^{lex}(p) := \overset{lex}{\max}\{\underline{d} \mid a_{\underline{d}} \neq 0\}$$

wobei das Maximum hier bezüglich der lexikographischen Ordnung gebildet wird, den (Multi)grad.

2. Ist $\mapsto \underline{\deg}^{lex}(p) = \underline{d}$ so heißt $a_{\underline{d}} x^{\underline{d}}$ *führender Term* des Polynoms und $\mathrm{FKoeff}(p) := a_{\underline{d}}$ *führender Koeffizient*.

Beispiel 39. 1. Für das Polynom $f(x_1, x_2, x_3) = x_1^3x_2^2 + 5x_1^3x_2x_3 + 3x_1^4x_3 + x_2^{12}x_3 + x_3^+x_1$ war der führende Term

$$3x_1^4x_3$$

also

$$\underline{\deg}^{lex}(f) = (4, 0, 1) \text{ und } \mathrm{FKoeff}(f) = 3.$$

2. Der führende Term des j-ten elementarsymmetrischen Polynoms s_j ist
$$x_1 x_2 \cdots x_j$$
und darum
$$\underline{\deg}^{lex}(s_j) = (\underbrace{1,1,\ldots,1}_{j-\text{Einträge}},0,\ldots,0),$$
der führende Koeffizient ist 1. Ich möchte in diesem Kapitel
$$e_{[1,j]} := \underline{\deg}^{lex}(s_j) = (\underbrace{1,1,\ldots,1}_{j-\text{Einträge}},0,\ldots,0).$$
schreiben.

Bemerkung (Der Multigrad ist additiv)**.** Ist R ein nullteilerfreier Ring, so folgt aus der Verträglichkeit der lexikographischen Ordnung mit der Multiplikation von Monomen sofort, dass für $f, g \in R[x_1,\ldots,x_n]$ gilt
$$\underline{\deg}^{lex}(f \cdot g) = \underline{\deg}^{lex}(f) + \underline{\deg}^{lex}(g).$$

Mit diesen Vorbereitungen können wir nun zeigen, dass unser Verfahren für alle symmetrischen Polynome funktioniert.

Beweis des Satzes über symmetrische Polynome. Die Eindeutigkeit ist jetzt leicht, denn:

1. Ist $\underline{m} = (m_1,\ldots,m_n) \in \mathbb{N}_0^n$ so ist
$$\begin{aligned}\underline{\deg}^{lex}(s_1^{m_1}\cdots s_n^{m_n}) &= m_1 e_1 + m_2 e_{[12]} + \cdots + m_n e_{[1n]} \\ &= \sum_{i=1}^{n}(\sum_{k=0}^{n-i} m_{i+k}) e_i.\end{aligned}$$

2. Da die Vektoren $e_1, e_{[12]},\ldots,e_{[1n]}$ in $\mathbb{R}^n$ linear unabhängig sind, ist die Abbildung die für ein $\underline{m} \in \mathbb{N}_0^n$ den Multigrad des Polynoms $s_1^{m_1}\cdot s_n^{m_n}$ berechnet
$$\begin{aligned}\mathbb{N}_0^n &\to \mathbb{N}_0^n \\ \underline{m} &\mapsto m_1 e_1 + m_2 e_{[12]} + \cdots + m_n e_{[1n]}\end{aligned}$$
injektiv. Also ist auch die Abbildung
$$\begin{aligned}R[s_1,\ldots,s_n] &\to R[x_1,\ldots,x_n]^{S_n} \\ q(s_1,\ldots,s_n) = \sum_{\underline{m}} a_{\underline{m}} x^{\underline{m}} &\mapsto q(s_1(x_1,\ldots,x_n),\ldots,s_n(x_1,\ldots,x_n)) \\ &= \sum_{\underline{m}} a_{\underline{m}} s_1^{m_1}\cdot s_n^{m_n}\end{aligned}$$
injektiv, denn alle Summanden haben unterschiedlichen Multigrad und darum ist $q(s_1(x_1,\ldots,x_n),\ldots,s_n(x_1,\ldots,x_n)) \neq 0$ wenn $q \neq 0$.

Für die EXISTENZAUSSAGE können wir induktiv beweisen, dass unser Verfahren funktioniert: Der Multigrad $\underline{d} := \underline{\deg}^{lex}(f)$ eines symmetrischen Polynoms erfüllt

$$d_1 \geq d_2 \geq \cdots \geq d_n$$

da falls in f der Koeffizient von $\underline{x}^{\underline{d}}$ von 0 verschieden ist, wegen der Symmetrie für alle $\sigma \in S_n$ auch der Koeffizient von $x_1^{d_{\sigma(1)}} \cdots x_n^{d_{\sigma(n)}}$ von Null verschieden ist und in der lexikographischen Ordnung der nach Größe sortierte Exponent das größte Monom definiert.

Dann hat aber für $\underline{m} = (m_1, \ldots, m_n)$ das durch $m_n = d_n$ und $m_i := d_i - d_{i+1} \in \mathbb{N}_0$ für $i = 1, \ldots, n-1$ definiert ist das Polynom

$$\underline{\deg}^{lex}(s_1^{m_1} \cdot \cdots \cdot s_n^{m_n}) = \underline{d} = \underline{\deg}^{lex}(f)$$

den gleichen Multigrad wie f, denn den i-ten Eintrag des Multigrades des Produktes hatten wir gerade als $m_i + m_{i+1} + \cdots + m_n$ berechnet und weil $m_i = d_i - d_{i+1}$ ist, heben sich die negativen Terme in der Summe auf und es bleicht d_i übrig.

Für $(d_1, d_2, d_3, d_4) = (7, 4, 2, 1)$ ist:

$$\begin{aligned}(7,4,2,1) &= (3,0,0,0)\\ &+ (2,2,0,0)\\ &+ (1,1,1,0)\\ &+ (1,1,1,1).\end{aligned}$$

Also hat $s_1^3 s_2^2 s_3^1 s_4^1$ den Multigrad $(7, 4, 2, 1)$.

Also ist

$$\underline{\deg}^{lex}(f - \text{Fkoeff}(s_1^{m_1} \cdot s_n^{m_n})) < \underline{d} = \underline{\deg}^{lex}(f).$$

Damit haben wir gezeigt, dass es genügt das Polynom von kleinerem Multigrad $f - \text{Fkoeff}(s_1^{m_1} \cdot s_n^{m_n})$ als Polynom in den s_j zu schreiben.

Wir wären also nach Induktion fertig, wenn wir wüssten, dass jede bezüglich der lexikographischen Ordnung absteigende Folge von Graden

$$\underline{d}^1 >^{lex} \underline{d}^2 >^{lex} \ldots$$

abbricht.

Da es in der lexikographischen Ordnung zu $\underline{d} \in \mathbb{N}_0^n$ in der Regel unendlich viele $\underline{e}$ mit $\underline{d} >^{lex} \underline{e}$ gibt, ist das nicht offensichtlich. Auf dem Übungsblatt überlegen Sie sich, dass das trotzdem stimmt.

IN DER VORLESUNG hatten Sie vorgeschlagen, dass wir einfach beobachten sollten, dass der Totalgrad $\deg(f) := \max\{\sum d_i \mid a_{\underline{d}} \neq 0\}$ in unserem Verfahren nicht größer werden kann, da alle Terme von s_j den gleichen Totalgrad haben. Darum ist die Menge der induktiv auftretenden führenden Koeffizienten endlich, denn es kann in jedem Eintrag höchstens der Totalgrad auftreten. Darum bricht das Verfahren ab und wir können daher f als Polynom in den s_j schreiben. □

Bemerkung. Das Argument aus dem Beweis entspricht tatsächlich unserem Algorithmus:

Ist f symmetrisch mit führendem Term $a\underline{x}^{\underline{d}} = a x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$ mit $d_1 \geq d_2 \cdots \geq d_n$ dann existiert genau ein $\underline{m} \in \mathbb{N}_0^n$ so dass das Produkt $s_1^{m_1} \cdots s_n^{s_m}$ führenden Term $\underline{x}^{\underline{d}}$ hat.

Das symmetrische Polynom $f_1 := f - a s_1^{m_1} \cdots s_n^{s_m}$ hat dann kleineren Multigrad.

Wenden wir das Argument nun auf f_1 an, so bricht die resultierende Folge $f.f_1, f_2, \dots$ von symmetrischen Polynomen ab, d.h. es gibt ein N mit $f_N = 0$.

Lesen wir das Verfahren dann rückwärts, erhalten wir

$$f = a\underline{s}^{\underline{m}} + a_1\underline{s}^{\underline{m}_1} + \dots.$$

Das ist genau das Verfahren, das wir für die Diskriminante verwendet haben.

DA WIR URSPRÜNGLICH an Lösungsformeln in Körpern interessiert waren, wäre es schöner, die Erweiterung

$$K[s_1, \dots, s_n] \cong K[x_1, \dots, x_n]^{S_n} \subseteq K[x_1, \dots, x_n]$$

als Erweiterung der Quotientenkörper

$$K(s_1, \dots, s_n) \subseteq K(x_1, \dots, x_n)$$

zu verstehen. Auch für Elemente von $K(x_1, \dots, x_n)$ wissen wir, was „symmetrisch" bedeuten soll, nämlich:

$$\frac{p(x_{\sigma(1)}, \dots, x_{\sigma(n)})}{q(x_{\sigma(1)}, \dots, x_{\sigma(n)})} \stackrel{!}{=} \frac{p(x_1, \dots, x_n)}{q(x_1, \dots, x_n)} \text{ für alle } \sigma \in S_n.$$

WENN SIE gründlich aufpassen, fragen Sie vielleicht, wieso die linke Seite der Gleichung wohldefiniert ist, da wir eine Formel mit Hilfe eines Repräsentanten für den Bruch aufgeschrieben haben. Damit wir uns nicht wieder über ähnliche Aussagen Gedanken machen müssen, sollten wir einmal formal aufschreiben, warum das hier klar ist:

Lemma 40 (Universelle Eigenschaft von Quotientenkörpern)**.** *Ist R ein nullteilerfreier Ring, L ein Körper und $f\colon R \to K$ ein injektiver Ringhomomorphismus, dann setzt sich f zu einem Körperhomomorphismus*

$$F\colon Q(R) \to L$$
$$\frac{a}{b} \mapsto F(\frac{a}{b}) := \frac{f(a)}{f(b)}$$

fort.

Für uns ist $R = K[x_1, \dots, x_n]$ und $L = K(x_1, \dots, x_n)$ gerade das Beispiel, das uns interessiert. Ringhomomorphismus bedeutete: $f(a \stackrel{+}{\cdot} b) = f(a) \stackrel{+}{\cdot} f(b)$ und $f(1) = 1$.

Beweis. Das finden Sie mittlerweile vielleicht selbst nicht mehr schwer? Wir müssen nur zeigen, dass

$$\frac{a}{b} \sim \frac{c}{d} \Rightarrow F(\frac{a}{b}) \sim F(\frac{c}{d})$$

gilt. Aber $\frac{a}{b} \sim \frac{c}{d}$ bedeutet $ad = bc$ dann ist $f(ad) = f(bc)$ und weil f ein Ringhomomorphsmus ist, folgt daraus $f(a)f(d) = f(b)f(c)$ also $\frac{f(a)}{f(b)} \sim \frac{f(c)}{f(d)}$. □

Da $p(x_1, \dots, x_n) \mapsto p(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ einen Ringhomomorphismus

$$K[x_1, \dots, x_n] \to K[x_1, \dots, x_n] \subseteq K(x_1, \dots, x_n)$$

definiert, folgt also, dass $\frac{p(x_{\sigma(1)}, \dots, x_{\sigma(n)})}{q(x_{\sigma(1)}, \dots, x_{\sigma(n)})}$ auch ein wohldefinierter Ausdruck ist. Wir kürzen das als $\sigma.\frac{p}{q} := \frac{p(x_{\sigma(1)}, \dots, x_{\sigma(n)})}{q(x_{\sigma(1)}, \dots, x_{\sigma(n)})}$ ab.

Folgerung 41 (Satz über symmetrische Funktionen)**.** *Jede symmetrische rationale Funktion ist ein Quotient aus rationalen Polynomen, d.h. der Isomorphismus*

$$K[s_1,\dots,s_n] \cong K[x_1,\dots,x_n]^{S_n} \subset K[x_1,\dots,x_n]$$

induziert einen Isomorphismus

$$K(s_1,\dots,s_n) \cong K(x_1,\dots,x_n)^{S_n} := \left\{ \frac{p}{q} \in K(x_1,\dots,x_n) \mid \sigma.\frac{p}{q} = \frac{p}{q} \text{ für alle } \sigma \in S_n \right\}.$$

Beweis. Das einzige Problem ist, dass aus

$$\frac{p(x_{\sigma(1)},\dots,x_{\sigma(n)})}{q(x_{\sigma(1)},\dots,x_{\sigma(n)})} = \frac{p(x_1,\dots,x_n)}{q(x_1,\dots,x_n)}$$

nicht $p(x_{\sigma(1)},\dots,x_{\sigma(n)}) = p(x_1,\dots,x_n)$ folgt. Zum Beispiel ist sicher $\frac{x_1}{x_1} = \frac{x_2}{x_2}$.

Die Lösung ist einfach, dass wir den Nenner eines Bruchs immer invariant machen können, denn für $q \in K[x_1,\dots,x_n]$ ist das Produkt

$$Q(x_1,\dots,x_n) := \prod_{\sigma\in S_n} q(x_{\sigma(1)},\dots,x_{\sigma(n)})$$

sicher invariant. Setzen wir

$$\widetilde{Q}(x_1,\dots,x_n) := \prod_{\substack{\sigma\in S_n \\ \sigma\neq \mathrm{id}}} q(x_{\sigma(1)},\dots,x_{\sigma(n)})$$

so ist

$$\frac{p}{q} = \frac{p\cdot\widetilde{Q}}{q\cdot\widetilde{Q}} = \frac{p\cdot\widetilde{Q}}{Q}$$

ein Bruch in dem der Nenner ein symmetrisches Polynom ist. Wenn der Bruch selbst symmetrisch ist, folgt für alle Permutationen σ aus $\sigma.\frac{p}{q} = \frac{p}{q}$ dass

$$\sigma.\frac{p\cdot\widetilde{Q}}{Q} = \frac{p\cdot\widetilde{Q}}{Q}, \text{ also } \frac{\sigma.(p\cdot\widetilde{Q})}{(\sigma.Q)} = \frac{p\cdot\widetilde{Q}}{Q}.$$

Wegen der Äquivalenzrelation für Brüche bedeutet das gerade

$$(\sigma.(p\cdot\widetilde{Q}))\cdot Q = (p\cdot\widetilde{Q})\cdot\sigma.Q.$$

Da Q symmetrisch ist gilt $\sigma.Q = Q$ also bedeutet die obige Gleichung

$$(\sigma.(p\cdot\widetilde{Q}))\cdot Q = (p\cdot\widetilde{Q})\cdot Q$$

und weil der Polynomring nullteilerfrei ist, folgt daraus

$$\sigma.(p\cdot\widetilde{Q}) = (p\cdot\widetilde{Q}),$$

d.h. $p\cdot\widetilde{Q}$ ist ebenfalls ein symmetrisches Polynom. □

Bemerkung. Den Trick, den Nenner invariant zu machen, kennen Sie schon aus der Berechnung von Brüchen in den komplexen Zahlen:

$$\frac{a+ib}{c+id} = \frac{(a+ib)(c-id)}{(c+id)(c-id)} = \frac{(a+ib)(c-id)}{c^2+d^2}.$$

Dort haben wir auch den Nenner invariant unter der komplexen Konjugation und damit reell gemacht.

FÜR DIE LÖSUNG von kubischen Gleichungen hatten wir also in der Körpererweiterung

$$K(s_1, s_2, s_3) \subset K(x_1, x_2, x_3)$$

Zwischenkörper gesucht, die unter Teilmengen von Permutationen invariant waren. Das funktioniert auch noch für $n = 4$, aber danach machte das sehr lange Zeit Probleme. Galois hatte dann die Einsicht, dass das auch die einzige Möglichkeit ist, um Zwischenkörper zu finden und außerdem Zwischenkörper die durch Wurzel ziehen entstehen zu besonderen Untergruppen von S_n gehören würden, von denen es für $n > 4$ nicht ausreichend viele gibt.

Das zu zeigen ist unser nächstes Ziel. Da das Rechnen mit vielen Variablen unhandlich ist, verwenden wir die Strategie: Wenn die Rechnung im Beispiel unübersichtlich wird, schauen wir ob der Kern des Arguments in einen übersichtlichen allgemeinen Rahmen passt, den wir leichter verstehen können.

DAS NÄCHSTE ZIEL IST: Zeige, dass für eine Körpererweiterung $K \subset L$, in der wir K als die Teilmenge der unter einer Menge von Symmetrien G invarianten Elemente schreiben können, alle Zwischenkörper durch Untergruppen von G bestimmt sind.

Die Galoisgruppe einer Erweiterung

Für unser Ziel, die Zwischenkörper von Körpererweiterungen durch Symmetrien zu verstehen, sollten wir also den Symmetrien von Körpererweiterungen einen Namen geben.

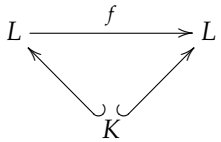
Definition (Galoisgruppe)**.** Ist $K \subseteq L$ eine (endliche) Körpererweiterung so heißt

$$\mathrm{Gal}(L|K) := \left\{ f \colon L \to L \mid \begin{array}{c} f \text{ Körperautomorphismus mit} \\ f(a) = a \text{ für alle } a \in K \end{array} \right\}$$

Galoisgruppe von L über K.

Körperautomorphismus: f bijektiv und $f(a \overset{+}{\cdot} b) = f(a) \overset{+}{\cdot} f(b)$.

Bemerkung. Die Bedingung $f(a) = a$ für alle $a \in K$ schreibe ich gerne als Diagramm



auf und merke mir, dass dieses kommutiert, d.h. es egal ist auf welchem Weg ich Elemente in K nach rechts oben abbilde.

Wir kennen schon eine Reihe von Körperautomorphismen:

Beispiel 42. 1. Für die Körpererweiterung $K(x_1, \ldots, x_n)^{S_n} \subseteq K(x_1, \ldots, x_n)$ definiert jede Permutation $\sigma \in S_n$ einen Automorphismus $\sigma \colon K(x_1, \ldots, x_n) \to K(x_1, \ldots, x_n)$, also ist

$$S_n \subseteq \mathrm{Gal}\left(K(x_1, \ldots, x_n) | K(s_1, \ldots, s_n)\right).$$

Für den Moment ist noch nicht ganz klar, dass das alle Automorphismen sind.

2. Für $\mathbb{R} \subset \mathbb{C}$ ist die komplexe Konjugation

$$\begin{aligned}(\_): \mathbb{C} &\to \mathbb{C}\\ z = a + ib &\mapsto \overline{z} = a + ib\end{aligned}$$

ein Körperautomorphismus und hier ist

$$\mathrm{Aut}(\mathbb{C}|\mathbb{R}) = \{\mathrm{id}, (\_)\}$$

den jeder Körperautomorphismus, der auf $\mathbb{R}$ die Identität ist, ist wegen

$$f(a + ib) = f(a) + f(i)f(b) = a + f(i)b$$

eindeutg durch $f(i)$ bestimmt und dieser Wert muss

$$-1 = f(-1) = f(i^2) = f(i)f(i)$$

erfüllen, aber $z^2 = -1$ hat nur die Lösungen $\pm i$.

3. Das obige Beispiel ist allgemeiner: Ist $p(x) \in K[x]$ irreduzibel, und $K \subseteq L$ eine Körpererweiterung, so ist jeder Körperhomomorphismus

$$f\colon K[x]/(p(x)) \to L,$$

mir $f(a) = a$ für alle $a \in K$ eindeutig durch $f(x)$ bestimmt und dieser Wert muss eine Nullstelle von p in L sein, da $0 = f(0) = f(p(x)) = p(f(x))$.

Umgekehrt definiert aber auch jede Nullstelle $\alpha \in L$ von p einen Homomophismus

$$\begin{aligned}\mathrm{Ausw}_\alpha\colon :\, K[x]/(p(x)) &\to L\\ q(x) &\mapsto q(\alpha).\end{aligned}$$

Insbesondere ist also

$$\mathrm{Aut}((K[x]/(p(x)))|K) \cong \{z \in K[x]/(p(x)) \mid p(z) = 0\}.$$

4. Für $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3 - 2)$ hatten wir gesehen, dass $x^3 - 2$ in $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ nur eine einzige Lösung hat, da die anderen beiden Nullstellen komplex sind. Die Galoisgruppe kann also klein sein.

5. Umgekehrt, sind für jede Primzahl p, die Nullstellen des Polynoms

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

gerade die p-ten Einheitswurzeln $e^{\frac{2\pi i}{p}k}$ für $k = 0, \ldots, p - 1$ und wir hatten gesehen, dass $(x^{p-1} + \cdots + x + 1)$ irreduzibel ist.

In $L = \mathbb{Q}[x]/(x^{p-1} + \cdots + x + 1)$ sind aber alle Potenzen von x wieder Nullstellen von $x^p - 1$, denn

$$(x^k)^p = (x^p)^k = (1)^k = 1.$$

und da $x^k \neq 1$ für $1 \leq k \leq p-1$, sind das also die $p-1$ Nullstellen von $(x^{p-1}+\cdots+x+1)$ in L, das Polynom zerfällt also in L schon in Linearfaktoren und

$$\mathrm{Gal}(L|\mathbb{Q}) \cong \{(f_k) \mid f_k(x) := x^k \text{ für } k = 1,\dots,p-1\}.$$

6. Für $\sqrt[3]{2}$ wäre das im Körper $\mathbb{Q}(\zeta_3)$ ähnlich. Das Polynom x^3-2 hat in diesem Körper keine Nullstelle (sonst bekämen wir einen Körperhomomorphismus $\mathbb{Q}[x]/(x^3-2) \to \mathbb{Q}(\zeta_3)$, aber $\dim_{\mathbb{Q}} \mathbb{Q}[x]/x^3-2 = 3 > 2 = \dim_{\mathbb{Q}} \mathbb{Q}[x]/(x^2+x+1) = \dim_{\mathbb{Q}} \mathbb{Q}(\zeta_3)$), ist also weil der Grad 3 ist irreduzibel. In $\mathbb{Q}(\zeta_3)[x]/(x^3-2)$ sind aber $x, \zeta_3 x, \zeta_3^2 x$ drei verschiedene Nullstellen von x^3-2.

Zerfällungskörper

Die Anzahl der Körperautomorphismen einer Erweiterung der Form $K[x]/p(x)$ hängt also davon ab, wie viele Nullstellen das Polynom p in dieser Erweiterung hat. Sind das nicht alle, so zerfällt p in der Erweiterung nicht in Linearfaktoren, aber dann können wir einfach Nullstellen der irreduziblen Faktoren induktiv hinzufügen. Körper die so entstehen bekommen den Namen Zerfällungskörper.

Definition. Ist K ein Körper und $g(x) \in K[x]$ ein Polynom, so heißt eine Erweiterung $K \subset L$ *Zerfällungskörper von* g wenn gilt

1. Das Polynom g zerfällt in $L[x]$ in Linearfaktoren und
2. sind $\alpha_1,\dots,\alpha_n \in L$ die Nullstellen von g in L, so gilt $K(\alpha_1,\dots,\alpha_n) = L$.

Lemma 43 (Existenz und Eindeutigkeit von Zerfällungskörpern)**.**

1. *Ist K ein Körper, so existiert zu jedem Polynom $g(x) \in K[x]$ ein Zerfällungskörper L von g.*

   Genauer können wir L als Kette von Körpererweiterungen

   $$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_d = L$$

   konstruieren, wobei $K_j = K_{j-1}[t]/(p_j(t))$ für einen irreduziblen Teiler $p_j(x)$ von $g(x)$ in $K_{j-1}[x]$ ist.

2. *Zerfällungskörper sind bis auf Isomorphie eindeutig bestimmt, d.h. sind $K \subseteq L_1, K \subseteq L_2$ zwei Zerfällungskörper von $g(x) \in K[x]$ so existiert ein Körperisomorhismus $F\colon L_1 \to L_2$ mit $F(a) = a$ für alle $a \in K$.*

Bemerkung. Für Körper die in $\mathbb{C}$ enthalten sind, könne wir Zerfällungskörper finden, indem wir einfach die Nullstellen in $\mathbb{C}$ hinzufügen. Für Körper wir $K(x)$, selbst $\mathbb{C}(x)$ ist es vielleicht nicht so klar, wie wir diese in einen Körper einbetten können, in dem alle Polynome Nullstellen besitzen. Darum ist die abstrakte Methode Nullstellen formal hinzuzufügen praktisch.

DIE BEWEISIDEE IST: Wenn $g(x)$ einen irreduziblen Faktor $p(x)$ besitzt, dann ist $K_1 := K[t]/(p(t))$ eine Körpererweiterung, in der $p(x)$ nach Konstruktion eine Nullstelle – nämlich t besitzt. Zerfällt $p(x)$ in K_1 noch nicht vollständig in Linearfaktoren, so fügen wir genauso eine Nullstelle eines irreduziblen Faktors zu K_1 hinzu. Da der Grad der irreduziblen Faktoren in jedem Schritt kleiner wird, bricht diese Prozess ab. Lassen Sie uns das formal aufschreiben.

Beweis des Lemmas. Zur *Existenz* können wir induktiv – durch Induktion über den Grad des Polynoms – zu jedem Polynom $g(x) \in K[x]$ einen Zerfällungskörper konstruieren.

Hat $g(x)$ Grad 0 oder 1, so ist nichts zu zeigen. Hat $g(x)$ Grad 2, so ist g entweder irreduzibel, dann ist $K[x]/g(x)$ ein Zerfällungskörper, oder g zerfällt schon in $K[x]$ in Linearfaktoren.

Ein allgemeines $g(x)$ können wir als Produkt von irreduziblen Polynomen schreiben, d.h.

$$g(x) = c \cdot \prod_{j=1}^{k} p_j(x), \text{ wobei } c \in K, p_j(x) \in K[x] \text{ irreduzibel.}$$

Dann ist $K \subset K_1 := K[t]/(p_1(t))$ eine Körpererweiterung in der $p_1(x)$ die Nullstelle $\alpha_1 = [t]$ besitzt, also

$$g(x) = (x - t)g_1(x)$$

gilt. Nach Induktionsannahme besitzt das Polynom $g_1(x) \in K_1[x]$ einen Zerfällungkörper $K_1 \subseteq K_d$.

Dann zerfällt $g_1(x)$ also auch $g(x) = (x - t)g_1(x)$ in K_d in Linearfaktoren und sind $\alpha_2, \ldots, \alpha_d$ die Nullstellen von g_1 in K_d so gilt

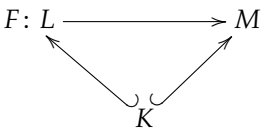
$$\begin{aligned} K_d &= K_1(\alpha_2, \ldots, \alpha_d) && K_d \text{ Zerfällungskörper von } g_1 \\ &= K(\alpha_1)(\alpha_2, \ldots, \alpha_d) && K_1 = K(\alpha_1) \\ &= K(\alpha_1, \ldots, \alpha_d). \end{aligned}$$

Also ist K_d ein Zerfällungskörper für $g(x)$.

Die *Eindeutigkeit* folgt genauso induktiv aus unserer Konstruktion: Ist $K \subseteq L_2$ ein weiterer Zerfällungskörper von $g(x)$ und ist $p_1(x)$ ein irreduzibler Teiler von $g(x)$, so besitzt $p_1(x)$ in L_2 eine Nullstelle α_1.

Diese definiert mittels $t \mapsto \alpha_1$ einen Körperhomomorphismus $K_1 = K[t]/(p_1(t)) \hookrightarrow L_2$. Dann sind aber $K_1 = K[t]/(p_1(t)) \hookrightarrow L_2$ und $K_1 \subseteq K_d$ Zerfällungskörper von $g_1(x) = \frac{g(x)}{x-t} \in K_1[x]$ und da $\text{Grad}(g_1(x)) < \text{Grad}(g(x))$ gilt, sind diese nach Induktion isomorph. □

Folgerung 44. *Ist $K \subset L$ ein Zerfällungskörper eines Polynoms $g(x) \in K[x]$, $K \subset M$ eine andere Körpererweiterung und*



ein Körperhomomorphismus mit $F(a) = a$ für alle $a \in K$, dann ist das Bild $F(L) \subseteq M$ ein Zerfällungkörper von g, d.h. $F(L) = K(\alpha_1, \dots, \alpha_d)$ wobei α_j die Nullstellen von g in M sind.

Beweis. Da F ein Körperhomomorphismus ist, gilt für jede Nullstelle $\beta \in L$ von g, dass

$$0 = F(0) = F(g(\beta)) = g(F(\beta))$$

also ist $F(\beta)$ wieder eine Nullstelle von g. Da L von Nullstellen von g erzeugt ist, ist also auch $F(L)$ von Nullstellen von g erzeugt und da g in L in Linearfaktoren zerfällt, gilt das auch in $F(L)$. □

Ein Knackpunkt für die Galoiskorrespondenz ist eine sehr wundersame Eigenschaft von Zerfällungskörpern.

Satz 45 (Zerfällungskörperwunder)**.** *Ist $K \subseteq L$ ein Zerfällungskörper eines Polynoms $g(x) \in K[x]$ und $p(x) \in K[x]$ ein beliebiges irreduzibles Polynom, das in L eine Nullstelle besitzt, dann zerfällt auch p in L vollständig in Linearfaktoren.*

Ich möchte hierfür zwei Beweise erklären: Einen, der unsere Symmetrieargumente nutzt und die fehlenden Nullstellen konstruiert und einen zweiten, der nur die abstrakte Konstruktion von Zerfällungskörpern verwendet.

Erster Beweis: Ist L ein Zerfällungskörper des Polynoms g und $g(x) = c\prod_{j=1}^{d}(x - \alpha_j)$ die Zerlegung von g in Linearfaktoren, so gilt $L = K(\alpha_1, \dots, \alpha_d)$. Insbesondere sind die Koeffizienten von $\frac{1}{c}g(x)$ – also die elementarsymmetrischen Polynome in $\alpha_1, \dots, \alpha_d$ – in K.

Ist $p(x)$ irreduzibel und $p(\alpha) = 0$ für ein $\alpha \in L$, so können wir, weil L von den α_j erzeugt ist α als Polynom in den α_i schreiben

$$\alpha = f(\alpha_1, \dots, \alpha_d) \text{ für ein } f \in K[x_1, \dots, x_d].$$

Das Polynom $(x - \alpha) = (x - f(\alpha_1, \dots, \alpha_d)) \in L[x]$ hat leider Koeffizienten in L, aber setzen wir

$$G(x) := \prod_{\sigma \in S_d} (x - f(x_{\sigma(1)}, \dots, x_{\sigma(d)})) \in K[x][x_1, \dots, x_d],$$

so sind ist dieses Polynom in den x_i symmetrisch, d.h. die Koeffizienten von $G(x)$ sind symmetrische Polynome in den x_j.

Da die elementarsymmetrischen Polynome in den α_j in K liegen, hat darum das Polynom

$$q(x) = \prod_{\sigma \in S_d} (x - f(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(d)})) \in K[x]$$

Koeffizienten in K und es besitzt in L die Nullstelle $\alpha = f(\alpha_1, \dots, \alpha_d)$. Also teilt $p(x)$ das Polynom $q(x)$. Da $q(x)$ nach Konstruktion in L in Linearfaktoren zerfällt, gilt das auch für $p(x)$. □

Zweiter Beweis. Sei $L \subseteq M$ ein Zerfällungskörper von $p(x)$ über L und $\beta \in M$ eine beliebige Nullstelle von $p(x)$ in M. Wir müssen zeigen, das $\beta \in L$ gilt.

Die Abbildung $t \mapsto \beta$ definiert eine Einbettung

$$F_1 \colon K_1 := K[t]/(p(t)) \hookrightarrow M.$$

Da $p(x)$ in L eine Nullstelle α besitzt, definiert $t \mapsto \alpha$ auch eine Einbettung

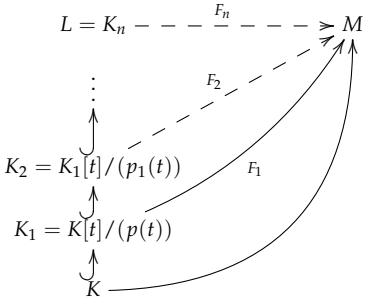
$$G \colon K[t]/(p(t)) \hookrightarrow L \subseteq M.$$

Da L auch ein Zerfällungskörper von $g(x)$ über $K[t]/(p(t))$ ist, gibt es einen Körperturm

$$K[t]/(p(t)) \subseteq K_2 \subseteq K_n = L$$

in dem $K_j = K_{j-1}[x]/(p_j(x))$ jeweils durch Hinzufügen einer Nullstelle eines irreduziblen Teilers $p_j(x)$ von $g(x)$ entsteht.

Induktive Konstruktion



Da p_j in L und damit auch in M in Linearfaktoren zerfällt, können wir induktiv durch die Wahl einer Nullstelle, die Abbildung $F_{j-1} \colon K_{j-1} \to M$ zu einer Abbildung $F_j \colon K_j \to M$ fortsetzen.

Für jede Abbildung $F_n \colon L = K_n \to M$, mit $F_n(a) = a$ für alle $a \in K$ ist das Bild $F_n(L) = K(\alpha_1, \ldots, \alpha_n)$ von den Nullstellen von g erzeugt (Folgerung 44). Nach Konstruktion ist aber $\beta \in F_n(L)$, also ist $\beta \in K(\alpha_1, \ldots, \alpha_n)$. □

Separable Polynome

Die Konstruktion aus dem vorigen Abschnitt erklärt uns auch, dass Zerfällungskörper eines Polynoms genau dann viele Automorphismen haben, wenn das Polynom viele verschiedene Nullstellen hat. Zum Beispiel war $K(s_1, \ldots, s_n) \subseteq K(x_1, \ldots, x_n)$ der Zerfällungskörper des allgemeinen Polynoms

$$p(x) = x^n - s_1 x_{n-1} + \cdots \pm s_n$$

und dieses Poylnom hatte n verschiedene Nullstellen, die wir beliebig vertauschen können. Wir sollten uns noch überlegen, dass irreduzible Polynome in der Regel keine doppelten Nullstellen haben können.

Definition (Separable Polynome)**.** Ein Polynom $f(x) \in K[x]$ vom Grad d heißt *separabel*, wenn f in einem Zerfällungskörper d paarweise verschiedene Nullstellen besitzt.

In der Analysis haben Sie gelernt, dass wir mit Hilfe der Ableitung testen können, ob eine doppelte Nullstelle vorliegt. Das stimmt auch algebraisch. In der linearen Algebra hatten wir dafür die formale Ableitung eines Polynoms $p(x) = \sum_{j=0}^{n} a_j x^j$ durch die übliche Rechenregel definiert:

$$\begin{aligned} p'(x) &:= \sum_{j=1}^{n} j a_j x^{j-1} \\ &= n a_n x^{n-1} + (n-1) a_{n-1} x^{n-1} + \cdots + 2a_2 x + a_1 \end{aligned}$$

und festgestellt, dass für diese Ableitung die üblichen Rechenregeln gelten, insbesondere gilt die Produktregel $(fg)' = f'g + fg'$.

Behauptung 46. *Ist K ein Körper, so ist $f(x) \in K[x]$ genau dann separabel wenn* $\mathrm{ggT}(f, f') = 1$ *gilt.*

Insbesondere ist ein irreduzibles Polynom $p(x)$ genau dann separabel wenn $p'(x) \neq 0$.

Bemerkung. Diese Aussage ist aus zwei Gründen interessant.

1. Für Körper der Charakteristik $p > 0$ fallen beim Ableiten alle Terme der Form x^{mp} weg, es ist daher bemerkenswert, dass die Ableitung dennoch die Vielfachheit der Nullstellen kennt.

2. Den $\mathrm{ggT}(f, f')$ können wir mit dem euklidischen Algorithmus sehr schnell berechnen. Damit können wir also herauszufinden, ob ein Polynom von größerem Grad eine mehrfache Nullstelle hat, ohne die Nullstellen zu bestimmen. Das Bestimmen der Nullstellen wäre in der Regel ohnehin keine Option.

Beweis. In einem Zerfällungkörper ist wegen der Eindeutigkeit der Zerlegung in irreduzible Elemente der $\mathrm{ggT}(f, f')$ das Produkt der Linearfaktoren von f, die f' teilen.

Ist in einem Zerfällungskörper $f(x) = (x-a)^2 g(x)$ so ist

$$f'(x) = 2(x-a)g(x) + (x-a)^2 g'(x) = (x-a)(2g(x) + (x-a)g'(x))$$

und also $(x-a)$ ein Teiler von $\mathrm{ggT}(f, f')$.

Ist umgekehrt $(x-a)$ eine einfache Nullstelle von f, d.h. $f(x) = (x-a)g(x)$ mit $g(a) \neq 0$, so ist $f'(x) = g(x) + (x-a)g'(x)$ und also $f'(a) = g(a) \neq 0$. Also ist $(x-a)$ dann kein Teiler von $\mathrm{ggT}(f, f')$. □

Folgerung 47. *1. Ist K ein Körper der Charakteristik 0, so sind alle irreduziblen Polynome in $K[x]$ separabel.*

2. Ist $\mathrm{char}(K) = p > 0$, so ist ein irreduzibles Polynom $f(x) \in K[x]$ genau dann inseparabel (d.h. nicht separabel), wenn

$$f(x) = g(x^p)$$

für ein Polynom $g(x) \in K[x]$.

3. Ist K ein endlicher Körper, so ist jedes irreduzible Polynom in $K[x]$ separabel.

Beweis. 1. Ist $\mathrm{char}(K) = 0$, so ist $p'(x) = 0 \Leftrightarrow p(x)$ konstant, also gilt dann $\mathrm{ggT}(p, p') = 1$.

2. Nach dem Lemma muss für ein inseparables irreduzibles Polynom $p(x) = \sum_{j=0}^{n} a_j x^j$ gelten, dass $p'(x) = 0$ ist, d.h. $j a_j = 0$. Also muss

$$a_j \neq 0 \Rightarrow j \text{ ist durch } p \text{ teilbar}$$

gelten. Also ist $p(x) = \sum_{k=0}^{m} a_{mp} x^{mp} = \sum_{k=0}^{m} a_{mp} (x^p)^m$. Das war zu zeigen.

3. Jeder endliche Körper der Charakteristik p ist eine endliche Erweiterung von $\mathbb{F}_p$. In $\mathbb{F}_p$ ist ein Polynom der Form $g(x^p)$ nicht irreduzibel, da dann $g(x^p) = g(x)^p$ gilt.

   Ist $\mathbb{F}_p \subset K$ eine endliche Erweiterung und $f(x) \in K[x]$ irreduzibel, so ist $f(x)$ ein Teiler des Minimalpolynoms von $t \in K[t]/(f(t))$ über $\mathbb{F}_p$. Da irreduzible Polynome über $\mathbb{F}_p$ separabel sind, ist auch der Teiler $f(x)$ separabel.

□

Beispiel 48. Das vorerst einzige Beispiel eines inseparablen irreduziblen Polynoms, das Ihnen im Moment einfallen könnte wäre das Polynom $f(x) = x^p - t$ in $\mathbb{F}_p(t)[x]$.

Für dieses Polynom ist die Erweiterung

$$\mathbb{F}_p(t) \subseteq \mathbb{F}_p(t)[s]/(s^p - t) \cong \mathbb{F}_p(s)$$

ein Zerfällungskörper, weil wegen $p = 0 \in \mathbb{F}_p$ die Gleichung

$$(x - s)^p = x^p - s^p = x^p - t \in \mathbb{F}_p(s)$$

gilt. Das Polynom hat in $\mathbb{F}_p(s)$ also nur die einzige Nullstelle s und daher besitzt die Erweiterung auch keine sichtbaren Symmetrien.

Dieses Beispiel ist weniger esoterisch, als Sie vielleicht denken. Es war für uns schon mehrfach nützlich Aussagen über $\mathbb{Q}$ auf Aussagen über $\mathbb{Z}$ zu reduzieren und dann modulo p zu rechnen. Dabei treten immer wieder Polynome dieser Art auf.

Glücklicherweise war das universelle Polynom in $K(s_1, \ldots, s_n)[x]$ für alle K separabel, darum wird das Problem für unsere Suche nach einer Lösungsformel zunächst keine Rolle spielen.

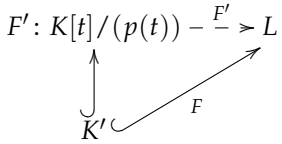
Bemerkung. Körper K in denen alle irreduziblen Polynome separabel sind heißen *perfekt*. Nach de obigen Folgerung sind alle Körper der Charakteristik 0, also alle Körper, die $\mathbb{Q}$ enthalten perfekt, ebenso alle endlichen Körper.

Es gilt außerdem, dass sich alle anderen Körper wenigstens in einen perfekten Körper einbetten lassen – vielleicht kommen wir darauf später noch zurück. Das spielt zum Beispiel in den Arbeiten von Peter Scholze eine große Rolle.

Im Beweis zum Zerfällungskörperwunder, haben wir induktiv Körperhomomorphismen mittels der charakterisierenden Eigenschaft von Quotienten $K[t]/(p(t))$ konstruiert, nämlich, dass Körperhomomorphismen aus dem Quotienten durch Nullstellen von p gegeben sind (Folgerung 13). Lassen Sie uns diese Aussage noch einmal formulieren:

Bemerkung. Ist K' ein Körper und $p(x) \in K'[x]$ ein irreduzibles Polynom und $F\colon K' \hookrightarrow L$ ein Körperhomomorphismus, dann

entsprechen Fortsetzungen



mit $F'(a) = F(a)$ für alle $a \in K'$ genau den Nullstellen des Polynoms $p(x)$ in L.

Hierbei fassen wir $p(x) \in K'[x]$ via F als Polynom mit Koeffizienten in L auf.

In der Vorlesung wollten Sie das Argument hierzu noch einmal sehen:

Beweis. Ist $p(t) = \sum_{j=0}^{n} a_j x^j$ ein irreduzibles Polynom vom Grad n, so sind die Elemente $1, t, \dots, t^{n-1}$ eine Basis des K-Vektorraums $K'[t]/(p(t))$. Da für Körperhomomorphismen F' gilt, dass

$$F'(t^k) = F'(\underbrace{t \cdots t}_{k-\text{Faktoren}}) = F'(t) \cdots F'(t) = (F'(t))^k$$

sind Körperhomomorphismen $F' \colon K'[t]/(p(t)) \to L$ mit $F'(a) = F(a)$ für alle $a \in K'$ durch $F'(t) = \alpha \in L$ eindeutig bestimmt.

Ist umgekehrt $\alpha \in L$ ein Element, so ist die Auswertungsabbildung $F' \colon K'[t] \to L$, die durch $t \mapsto \alpha$ gegeben ist, genau dann auf dem Quotienten $K'[t]/(p(t)) \to L$ wohldefiniert, wenn

$$\begin{aligned} 0 = F'(0) &= F'(p(t)) \\ &= F'(\sum_{j=0}^{n} a_j t^j) \\ &= \sum_{j=0}^{n} F'(a_j) F'(t)^j \\ &= \sum_{=0}^{n} F(a_j) \alpha^j \end{aligned}$$

gilt, d.h. wenn α eine Nullstelle des Polynoms $\sum_{=0}^{n} F(a_j) x^j$ in L ist, also eine Nullstelle von p in L. □

Mit diesem Argument können wir Zerfällungskörper separabler Polynome dadurch charakterisieren, dass sie viele Automorphismen besitzen.

Satz 49 (Charakterisierung von Zerfällungskörpern)**.** *Eine endliche Körpererweiterung $K \subseteq L$, dann ist*

$$\#\operatorname{Aut}(L|K) \leq [L : K]$$

und L ist genau dann der Zerfällungskörper eines separablen Polynoms $f \in K[x]$ wenn

$$\#\operatorname{Aut}(L|K) = [L : K].$$

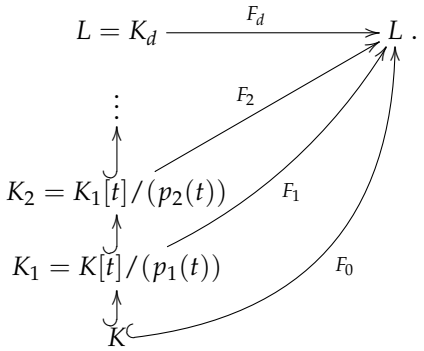
Bemerkung. Ist $\mathrm{char}(K) = 0$, oder allgemeiner K perfekt, so können wir in der obigen Aussage „Zerfällungskörper eines separablen Polynoms“ durch „Zerfällungskörper eines Polynoms“ ersetzen, denn wir können f immer als Produkt $f = c\prod_{j=1}^{r} p_j^{n_j}$ von paarweise teilerfremden irrdeuziblen Polynomen p_j schreiben. Dann ist ein Zerfällungskörper von f auch ein Zerfällungskörper des Produktes $\prod_{j=1}^{r} p_j$. Dieses Polynom ist dann separabel, da irreduzible Polynome in perfekten Körpern separabel sind und die p_j teilerfremd sind.

Beweis. Ist $K \subset L$ eine endliche Körpererweiterung, so können wir $L = K(\alpha_1, \ldots, \alpha_d)$ als Kette von Körpererweiterungen

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_d = L$$

schreiben, in der wir jeweils ein Element hinzufügen, d.h. $K_j = K_{j-1}(\alpha_j) \cong K_{j-1}[t]/(p_j(t))$ für ein irreduzibles Polynom p_j.

Damit definiert jeder Körperautomorphismus $F\colon L \to L$ mit $F(a) = a$ für alle $a \in K$ ein Diagramm von Körperhomomorphismen



Wir haben aber gerade gesehen, dass es zu jedem F_{j-1} höchstens $\mathrm{Grad}(p_j)$ viele Fortsetzungen F_j gibt. Also existieren höchstens

$$\prod_{j=1}^{d} \mathrm{Grad}(p_j) = \prod_{j=1}^{d} [K_j : K_{j-1}] = [L : K]$$

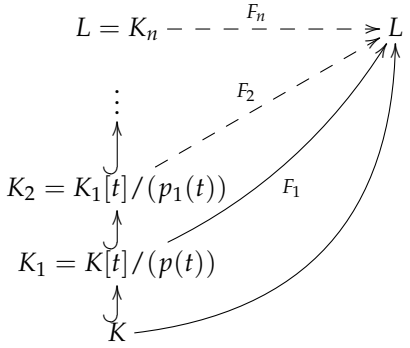
Körperhomomorphismen $F\colon L \to L$ mit $F(a) = a$ für alle $a \in K$. Das zeigt die erste Behauptung.

Ist $K \subset L$ ein Zerfällungskörper eines separablen Polynoms $f(x) \in K[x]$, so können wir L als Kette von Körpererweiterungen

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_d = L$$

schreiben, wobei $K_j = K_{j-1}[t]/(p_j(t))$ für einen irreduzibler Teiler $p_j(x)$ von $f(x)$ in $K_{j-1}[x]$ ist.

Nach unserer Bemerkung gibt es im Turm



induktiv zu jedem $F_{j-1}\colon K_{j-1} \to L$ genau so viele Fortsetzungen $F_j\colon K_j \to L$ wie es Nullstellen von p_j in L gibt. Da p_j ein Teiler von f ist, und f nach Voraussetzung Grad f paarweise verschiedene Nullstellen in L besitzt, so ist p_j separabel und zerfällt in L. Also gibt es $\mathrm{Grad}(p_j) = [K_j : K_{j-1}]$ viele Fortsetzungen.

Da zudem jeder Körperhomomorphismus $F_n\colon L \to L$ injektiv ist und $\dim_K(L) = [L : K] < \infty$, ist F automatisch ein Isomorphismus.

Also ist

$$\#\,\mathrm{Aut}(L|K) = \prod_{j=1}^{d} \mathrm{Grad}(p_j) = [L : K].$$

Sei umgekehrt $K \subset L = K(\alpha_1, \ldots, \alpha_d)$ eine endliche Körpererweiterung, für die $\#\,\mathrm{Aut}(L|K) = [L : K]$ gilt. Ich behaupte, dass dann die Minimalpolynome $\mathrm{minpol}_{\alpha_j}(x)$ separabel sind und in L in Linearfaktoren zerfallen.

Sei dazu $p(x) = \mathrm{minpol}_{\alpha_j}(x)$das Minimalpolynom von α_j.

Dann ist $K \subseteq K_1 := K[t]/(p_j(t)) \subseteq L$ und wir können diese Erweiterung wieder zu einer Kette

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_d = L$$

fortsetzen in der in jedem Schritt ein Element adjungiert wird.
Das Argument von zuvor besagt, dass es nur dann $[L : K]$ viele Körperautomorphismen in $\mathrm{Aut}(L/K)$ geben kann, wenn $p(x)$ in L $\mathrm{Grad}(p)$ viele paarweise verschiedene Nullstellen besitzt, d.h. p ist separabel und zerfällt in L in Linearfaktoren. Da dies für alle j gilt, ist L ein Zerfällungskörper des Produktes der Minimalpolynome der α_j. Da diese irreduzibel sind, sind die p_j entweder teilerfremd, oder gleich. Sind $p_1, \ldots, p_r$ die auftertenden paarweise verschiedenen Minimalpolynome, so ist L der Zerfällungskörper des Produktes $\prod_{j=1}^{r} p_j$ und dieses Polynom ist separabel. Das war zu zeigen. □

Im Beweis haben wir außerdem gesehen, dass für einen Zerfällungskörper eines separablen Polynoms, alle Minimalpolynome von Elementen wieder separabel sind. Daraus ergibt sich , dass der Begriff „separabel“ für Körpererweiterungen sinnvoll ist. Das ist für uns für den Moment nicht ganz so interessant, weil wir schon wissen, dass irreduzible Polynome ohnehin fast automatisch separabel sind, aber da wir die Aussage gerade schon eingesehen haben, sei es hier noch einmal festgehalten:

Folgerung 50. *Ist $K \subseteq L = K(\alpha_1, \ldots, \alpha_n)$ eine endliche Körpererweiterung, dann sind die folgenden Bedingungen äquivalent:*

1. *Die Minimalpolynome der Elemente $\alpha_1, \ldots, \alpha_n$ sind separabel.*
2. *Für jedes Element $\alpha \in L$ ist das Minimalpolynom von α separabel.*

Beweis. Den Beweis möchte ich Ihnen als Übungsaufgabe überlassen, um zu sehen, ob Sie das Argument aus dem vorigen Satz verstanden haben. □

Der Vollständigkeit halber nun noch die offizielle Definition des Begriffs der separablen Körpererweiterung.

Definition. Ein Element einer algebraischen Körpererweiterung $K \subseteq L$ heißt *separabel* wenn sein Minimalpolynom separabel ist.

Eine Körpererweiterung $K \subset L$ heißt *separabel* wenn alle Elemente von L separabel sind.

Die Galoiskorrespondenz – Version 1

Damit können wir nun die Aussage zeigen, dass alle Zwischenkörper von Zerfällungskörpern separabler Polynome, also insbesondere alle Zwischenkörper unserer allgemeinen Erweiterung $K(s_1, \ldots, s_n) \subseteq K(x_1, \ldots, x_n)$ durch Untergruppen der Symmetriegruppe $\mathrm{Aut}(L|K)$ bestimmt sind.

Notation 51. Ist $K \subseteq L$ eine Körpererweiterung und $H \subseteq \mathrm{Aut}(L|K)$ eine Untergruppe so bezeichnen wir mit

$$L^H := \{\alpha \in L \mid \sigma(\alpha) = \alpha \text{ für alle } \sigma \in H\}$$

die Teilmenge der Elemente von L, die unter den Symmetrien in H invariant sind.

$H \subseteq G$ Untergruppe bedeutet H ist eine Teilmenge, die mit der Verknüpfung von G selbst wieder eine Gruppe ist, d.h.

1. Das neutrale Element e von G ist in H.
2. Zu je zwei Elementen $h_1, h_2 \in H$ ist auch $h_1 \cdot h_2 \in H$.
3. Zu jedem $h \in H$ ist auch $h^{-1} \in H$.

Bitte prüfen Sie selbst einmal nach, dass $K \subseteq L^H \subset L$ dann immer ein Zwischenkörper ist.

Satz 52 (Galoiskorrespondenz)**.** *Sei $K \subseteq L$ ein Zerfällungskörper eines separablen Polynoms, dann sind die Abbildungen*

$$\left\{K' \mid \begin{array}{c} K \subseteq K' \subseteq L \\ \textit{Zwischenkörper} \end{array}\right\} \begin{array}{c} \longrightarrow \\ \longleftarrow \end{array} \{H \subseteq \mathrm{Aut}(L|K) \mid H \textit{ Untergruppe}\}$$

$$K' \mapsto \mathrm{Aut}(L|K')$$

$$L^H \hookleftarrow H$$

zueinander inverse Bijektionen und es gilt

$$[L^H : K] = \frac{\#\,\mathrm{Aut}(L|K)}{\#H} \textit{ und } [L : L^H] = \#H.$$

Bemerkung. Da die endliche Menge $\mathrm{Aut}(L|K)$ nur endlich viele Teilmengen hat, gibt es insbesondere nur endlich viele Untergruppen von $\mathrm{Aut}(L|K)$. Der Satz erklärt also insbesondere, dass es nur endlich viele Teilkörper $K \subseteq K' \subseteq L$ gibt.

Das ist etwas überraschend, da es (wenn K unendlich ist) in der Regel unendlich viele K-Untervektorräume von L gibt.

Beweis. Schritt 1: Die Aussage über den Grad der Körpererweiterungen haben wir schon gesehen, denn für jeden Teilkörper $K \subseteq K' \subseteq L$, ist $K' \subset L$ auch der Zerfällungkörper des eines separablen Polynoms für das $K \subset L$ der Zerfällungkörper war. Nach der Charakterisierung von Zerfällungkörpern gilt dann $\#\operatorname{Aut}(L|K') = [L : K']$ und wegen der Multiplikativität des Körpergrades gilt dann auch

$$[K' : K] = \frac{[L : K]}{[L : K']} = \frac{\#\operatorname{Aut}(L|K)}{\#\operatorname{Aut}(L|K')}.$$

Insbesondere ist dieser Bruch eine ganze Zahl.

Schritt 2: Lassen Sie uns nun zeigen, dass die Komposition

$$K' \mapsto H = \operatorname{Aut}(L|K') \mapsto L^H = L^{\operatorname{Aut}(L|K')}$$

ein Isomorphismus ist, d.h. wir zeigen, dass $K' = L^{\operatorname{Aut}(L|K')}$.

Zunächst ist nach Definition

$$K' \subseteq L^{\operatorname{Aut}(L|K')} = \{\alpha \in L \mid \sigma(\alpha) = \alpha \text{ für alle } \sigma \in \operatorname{Aut}(L|K')\}.$$

Da $K' \subseteq L$ und $L^{\operatorname{Aut}(L|K')} \subseteq L$ Zerfällungskörper eines separablen Polynoms sind, gilt also nach der Charakterisierung von Zerfällungkörpern:

$$\begin{aligned}
\#\operatorname{Aut}(L|K') = [L : K'] &\geq [L : L^{\operatorname{Aut}(L|K')}] && \text{weil } K' \subseteq L^{\operatorname{Aut}(L|K')} \\
&= \#\operatorname{Aut}(L|L^{\operatorname{Aut}(L|K')}) && \text{weil } L^{\operatorname{Aut}(L|K')} \subseteq L \text{ Zerfällungskörper} \\
&\geq \#\operatorname{Aut}(L|K') && \text{weil } \operatorname{Aut}(L|K') \subseteq \operatorname{Aut}(L|L^{\operatorname{Aut}(L|K')}).
\end{aligned}$$

Also muss in allen Schritten Gleichheit gelten und insbesondere $[L : K'] = [L : L^{\operatorname{Aut}(L|K')}]$. Daraus folgt aber $K' = L^{\operatorname{Aut}(L|K')}$, da $K' \subseteq L^{\operatorname{Aut}(L|K')}$.

Da es eine Nachfrage hierzu gab: Im letzten Schritt haben wir verwendet dass nach Definition für $G < \operatorname{Aut}(L|K)$ gilt, dass $G \subseteq \operatorname{Aut}(L|L^G)$, da in der Definition von L^G die Aussage $g(a) = a$ für alle $a \in L^G$ enthalten ist.

Schritt 3: Lassen Sie uns nun zeigen, dass die Komposition

$$H \mapsto L^H \mapsto \operatorname{Aut}(L|L^H)$$

ein Isomorphismus ist, d.h. wir zeigen, dass $H = \operatorname{Aut}(L|L^H)$.

Wieder gilt nach Definition, dass $H \subseteq \operatorname{Aut}(L|L^H)$ und wir wissen nach Schritt 2. schon, dass $L^H = L^{\operatorname{Aut}(L|L^H)}$ und nach Schritt 1., dass $\#\operatorname{Aut}(L|L^H) = [L : L^H]$. Damit genügt es zu zeigen, dass $[L : L^H] \leq \#H$ gilt. Diese Aussage gilt allgemein und wir formulieren diese darum als Lemma. □

Lemma 53 (Artin's Lemma – Version 1)**.** *Sei L ein Körper und $H \subseteq \operatorname{Aut}(L)$ eine endliche Untergruppe der Körperautomorphismen von L. Dann gilt*

$$[L : L^H] \leq \#H.$$

Beweis. Sei $n = \#H$. Angenommen $\alpha_1, \ldots, \alpha_{n+1}$ wären L^H-linear unabhängige Elemente von L, dann hätte das lineare Gleichungssystem mit $\#H = n$ Gleichungen in $n+1$ Variablen, das entsteht in dem wir für jedes $\sigma \in H$ die Gleichung

$$\sum_{i=1}^{n+1} \sigma(\alpha_i) x_i = 0$$

betrachten, eine nicht triviale Lösung. Sei $\begin{pmatrix} x_1 \\ \vdots \\ x_{n+1} \end{pmatrix} \in L^{n+1}$ eine nichttriviale Lösung mit einer minimalen Anzahl von Koordinaten $\neq 0$. Nach umnummerieren können wir dann annehmen, dass $x_1 \neq 0$ ist und dann auch, dass $x_1 = 1$ gilt.

Da die Elemente $\alpha_1, \ldots, \alpha_{n+1}$ nach Definition über L^H linear unabhängig sind, ist

$$\underline{x} := \begin{pmatrix} x_1 \\ \vdots \\ x_{n+1} \end{pmatrix} \notin (L^H)^n \subseteq L^n.$$

Sie nun $\tau \in H$ ein Element mit $\tau(\underline{x}) = \begin{pmatrix} \tau(x_1) \\ \vdots \\ \tau(x_{n+1}) \end{pmatrix} \neq \underline{x}$. Dann ist $\tau(\underline{x}$ wieder eine Lösung des Gleichungssystems, denn es gilt wegen $\sum_{i=1}^{n+1} \sigma(\alpha_i)x_i = 0$ dass

$$\begin{aligned} 0 &= \tau(\sum_{i=1}^{n+1} \sigma(\alpha_i)x_i) \\ &= \sum_{i=1}^{n+1} \tau(\sigma(\alpha_i)x_i) \\ &= \sum_{i=1}^{n+1} \tau(\sigma(\alpha_i))\tau(x_i) \\ &= \sum_{i=1}^{n+1} (\tau \circ \sigma)(\alpha_i)\tau(x_i). \end{aligned}$$

Da die Menge

$$\{\tau \circ \sigma \mid \sigma \in H\} = H$$

ist folgt, dass $\tau(\underline{x})$ in der Tat eine weitere Lösung des Gleichungssystems ist.

Dann ist aber auch die Differenz $\underline{x} - \tau(\underline{x})$ wieder eine Lösung der Gleichung, für die nun aber wegen $\tau(1) = 1$ eine weitere Koordinate $= 0$ ist. Da $\tau(\underline{x}) \neq \underline{x}$ nicht 0 ist, ist das ein Widerspruch zur Annahme, dass die Anzahle der Koordinaten $\neq 0$ für den Vektor $\underline{x}$ minimal war. □

Notation 54. Zur Abkürzung schreiben wir $H < G$ für „$H \subseteq G$ ist eine Untergruppe“.

Beispiel 55 (Gleichung 3. Grades)**.** Zur Lösung der allgemeinen Gleichung 3. Grades hatten wir die Erweiterung

$$L = \mathbb{Q}(x_1, x_2, x_3) \supset \mathbb{Q}(x_1, x_2, x_3)^{S_3} \cong \mathbb{Q}(s_1, s_2, s_3) =: K$$

angeschaut und gesehen, dass L der Zerfällungskörper des Polynoms

$$f(x) = x^3 - s_1x^2 + s_2x - s_3 \in \mathbb{Q}(s_1, s_2, s_3)[x]$$

ist, das in L die Gleichung

$$f(x) = \prod_{i=1}^{3}(x - x_i)$$

gilt.

(Hier könnte $\mathbb{Q}$ irgendein Körper sein, aber ich möchte die Körpererweiterung gern $L|K$ nennen.)

Nach Konstruktion ist $S_3 \subseteq \mathrm{Aut}(L|K)$ und $L^{S_3} = K$, also liefert die Galoiskorrespondenz noch ein Argument dafür, dass

$$\mathrm{Aut}(L|K) = S_3$$

und also $[L : K] = \#S_3 = 3! = 6$.

Um für dieses Beispiel die Galoiskorrespondenz zu verstehen, sollten wir zunächst alle Untergruppen von S_3 bestimmen.

Wir verwenden die Zykelschreibweise für Elemente von S_n damit ist

$$S_3 = \{\mathrm{id}, (12), (13), (23), (123), (132)\}.$$

Die möglichen Untergruppen sind

1. $\{\mathrm{id}\}$
2. Die kleinste Untergruppe, die (12) enthält ist $\{\mathrm{id}, (12)\}$ weil $(12)^2 = \mathrm{id}$. Das gilt genauso für die anderen Elemente der Form (i, j), damit finden wir 3 Untergruppen mit 2 Elementen:
$$H_{12} = \{\mathrm{id}, (12)\}, H_{13} = \{\mathrm{id}, (13)\}, H_{23} = \{\mathrm{id}, (23)\}.$$
3. Die kleinste Untergruppe, die (123) enthält ist $\{\mathrm{id}, (123), (132)\}$ weil $(123)^2 = (132)$ und $(123)^3 = \mathrm{id}$. Das gilt genauso für (132) damit finden wir 1 Untergruppe mit 3 Elementen:
$$A_3 = \{\mathrm{id}, (123), (132)\}.$$
Das sind genau die Elementevon S_3 mit $\mathrm{sign}(\sigma) = 1$.
4. Wenn eine Untergruppe zwei Elemente der Form (ij) enthält, dann auch das dritte und damit sogar alle Elemente. Genauso enthält eine Untergruppe, die (ij) und (123) enthält schon alle Elemente, d.h S_3 ist die einzige Untergruppe mit mehr als 3 Elementen.

Die Zwischenkörper sind:

1. $L^{H_{12}} = \mathbb{Q}(s_1, s_2, s_3)(x_3)$ denn x_3 ist ein Element von L, das unter der Vertauschung $x_1 \leftrightarrow x_2$ invariant ist und $[\mathbb{Q}(s_1, s_2, s_3)(x_3) : \mathbb{Q}(s_1, s_2, s_3)] = 3$ da x_3 eine Nullstelle des irreduziblen Polynoms $f(x) = x^3 - s_1x^2 + s_2x - s_3$ ist.
2. $L^{A_3} = \mathbb{Q}(s_1, s_2, s_3)(\sqrt{D})$ wobei $\sqrt{D} = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$.
3. $L^{S_3} = K$.

Das erstaunliche ist, dass wir hier gar nicht rechnen müssen: Die Körper sind alle Unterkörper, die unter den gegebenen Elementen invariant sind und enthalten jeweils ein Element, das nicht unter den anderen Permutationen invariant ist.

ZYKELSCHREIBWEISE: Wir gruppieren die Zahlen $1, \ldots, n$ so hintereinander, dass hinter jeder Zahl, die Zahl steht auf die diese abgebildet wird und die Gruppen einzuklammern, bei denen die letzte Zahl, wieder auf die erste abgebildet wird, also

$(1,2)(3,4,5)$ für $1 \to 2 \to 1, 3 \to 4 \to 5 \to 3$.

Die Konvention ist, dass wir Zykel der Länge 1, d.h. die Zahlen, die auf sich selbst abgebildet werden weglassen:

schreibe $(1,2)$ statt $(1,2)(3)(4)(5)$.

FRAGE: Für welche der Unterkörper L^H ist die Erweiterung $L^H|K$ selbst ein Zerfällungskörper?

ANTWORT: Nur L^{A_3}. Denn in den Körpern

$$\mathbb{Q}(s_1, s_2, s_3)(x_i)$$

hat das Polynom $f(x)$ eine Nullstelle, zerfällt aber noch nicht.

Hingegen ist L^{A_3} der Zerfällungkörper von $x^2 = D$.

UM WEITERE BEISPIELE UND ANWENDUNGEN der Galoiskorrespondenz zu verstehen, müssen wir einerseits Erweiterungen L/K finden, für die wir die Galoisgruppe

WENN WIR in Lösungsformeln n-te Wurzeln verwenden und annehmen, dass unser Körper alle n-ten Einheitswurzeln enthält (und also $\mathrm{char}(K)$ nicht n teilt wenn $\mathrm{char}(K) > 0$ sein sollte), dann ist $K(\sqrt[n]{a})/K$ immer ein Zerfällungkörper, weil wir mit einer n-ten Wurzel α auch n-verschiedene $\zeta_n^k \alpha$ Wurzeln finden. Es wäre also gut, zu klären, ob wir an der Untergruppe $H < G$ ablesen können, ob der Zwischenkörper der Form L^H selbst ein Zerfällungkörper sein kann.

Wir wissen schon einiges hierfür:

1. $L^H|K$ ist genau dann ein Zerfällungskörper, wenn
$$[L^H : K] = \#\,\mathrm{Aut}(L^H|K).$$
2. $[L^H : K] = \frac{\#\,\mathrm{Aut}(L/K)}{\#H}$.
3. Jeder Körperhomomorphismus $F_H \in \mathrm{Aut}(L^H|K)$ lässt sich zu einem $F \in \mathrm{Aut}(L|K)$ fortsetzen.
4. Ist $L^H|K$ ein Zerfällungskörper eines Polynoms $g(x)$, dann bildet jeder Körperhomomorphismus $F \in \mathrm{Aut}(L|K)$ den Zwischenkörper L^H in sich ab, denn F bildet Nullstellen von g auf Nullstellen von g ab, und da L^H von den Nullstellen erzeugt ist, ist dann auch das Bild $F(L^H)$ wieder von Nullstellen von g erzeugt.

Bemerkung. Ist $H < G = \mathrm{Aut}(L|K)$ eine Untergruppe und $g \in \mathrm{Aut}(L|K)$ ein Element, dann gilt für alle $a \in L^H$, dass $g(a) \in L^{gHg^{-1}}$ und $gHg^{-1} = \{h' \mid h' = ghg^{-1} \text{ für ein } g \in G\} < G$ ist wieder eine Untergruppe.

Beweis. Beide Aussagen ergeben sich einfach durch Ausschreiben der Definitionen:

Ist $a \in L^H$, so gilt nach Definition $h(a) = a$ für alle $h \in H$. Dann gilt aber für $h' = ghg^{-1}$ dass

$$h'(g(a)) = ghg^{-1}(g(a)) = gh(g^{-1}(g(a))) = g(h(a)) = g(a).$$

Also ist dann $g(a) \in L^{gHg^{-1}}$.

Die Teilmenge $gHg^{-1} \subseteq G$ ist eine Untergruppe, denn:

1. Das neutrale Element ist enthalten: $\mathrm{id} = g\,\mathrm{id}\,g^{-1} \in gHg^{-1}$.

2. Sind $h_1' = gh_1g^{-1} \in gHg^{-1}$ und $h_2' \in gh_2g^{-1} \in gHg^{-1}$ so auch $h_1'h_2'$, denn

$$h_1'h_2' = gh_1 \underbrace{g^{-1}g}_{=\mathrm{id}} h_2g^{-1} = g\underbrace{h_1h_2}_{\in H}g^{-1} \in gHg^{-1}.$$

3. Ist $h' = ghg^{-1}$, so ist $h'^{-1} = gh^{-1}g^{-1}$, da

$$gh\underbrace{g^{-1}g}_{=\mathrm{id}}h^{-1}g^{-1} = g\underbrace{hh^{-1}}_{=\mathrm{id}}g^{-1} = gg^{-1} = \mathrm{id}\,.$$

   Also ist mit h' auch $h'^{,-1} \in gHg^{-1}$.

□

Definition (Normalteiler)**.** Ist $(G,\cdot)$ eine Gruppe, dann heißen Untergruppen $H < G$ für die gilt, dass

$$gHg^{-1} = H \text{ für alle } g \in G$$

Normalteiler, oder *normale Untergruppe*.

Die Eigenschaft Normalteiler zu sein ist, wie wir im Beispiel S_3 gesehen haben sehr besonders, der Name ist der folgenden Eigenschaft geschuldet.

Lemma 56 (Charakterisierende Eigenschaft von Normalteilern)**.**

1. *Für jede Untergruppe $H < G$ ist die Relation $\sim_H$ auf G, die durch $g \sim_H g' :\Leftrightarrow g' = g \cdot h$ für ein $h \in H$ gegeben ist, eine Äquivalenzrelation und wir schreiben*
$$G/H := G/\sim_H .$$

2. *Eine Untergruppe $H < G$ einer Gruppe G ist genau dann ein Normalteiler wenn die Verknüpfung*
$$\begin{aligned} \cdot\colon G/H \times G/H &\to G/H \\ [g_1]\cdot[g_2] &:= [g_1 \cdot g_2] \end{aligned}$$
   eine wohldefinierte Gruppenstruktur auf G/H ist.

Beweis. 1. Nur auf Anfrage. In der Vorlesung hatten wir uns das kurz in Worten klar gemacht.

2. Damit die Verknüpfung wohldefiniert ist, müssen wir zeigen, dass aus $g_1' = g_1h_1, g_2' = g_2h_2$ mit $h_1, h_2 \in H$ folgt, dass $g_1'g_2' = g_1g_2 \cdot h$ für ein $h \in H$. Aber

$$\begin{aligned} g_1'g_2' &= g_1h_1g_2h_2 \\ &= g_1g_2g_2^{-1}h_1g_2h_2 \\ &= g_1g_2(g_2^{-1}h_1g_2)h_2 \overset{!}{=} g_1g_2h \end{aligned}$$

und multiplizieren wir die letzte Gleichung von links mit $(g_1 g_2)^{-1}$ und von rechts mit h_2^{-1} erhalten wir

$$(g_2^{-1} h_1 g_2) \stackrel{!}{=} h h_2^{-1} \in H.$$

Die Verknüpfung ist also genau dann wohldefiniert, wenn $g_2^{-1} h_1 g_2 \in H$ für alle $g_2 \in G, h_1 \in H$. Das bedeutet aber gerade, dass $ghg^{-1} \in H$ für alle $g \in G, h \in H$ gilt und das ist wie behauptet die Bedingung, dass H ein Normalteiler ist.

Wenn Die Verknüpfung wohldefiniert ist, dann erfüllt diese alle Rechenregeln, die für $\cdot$ galten, also ist G/H dann wieder eine Gruppe.

□

Behauptung 57. *Ist $L|K$ ein Zerfällungskörper eines separablen Polynoms und $H < \mathrm{Aut}(L|K)$ eine Untergruppe, dann ist $L^H|K$ genau dann ein Zerfällungskörper, wenn für alle $g \in \mathrm{Aut}(L|K)$ gilt, dass*

$$gHg^{-1} = H.$$

Das wurde in der Vorlesung vertagt, weil Sie zunächst mehr Beispiele sehen wollten, obwohl wir das mit den voranstehenden Argumenten eigentlich schon gezeigt haben. Wir kommen darauf nach den Beispielen zurück (Satz 71).

Rückblick: Welche allgemeinen Konzepte und Resultate haben wir kennen gelernt?

Auf der Suche nach Lösungsformeln für Nullstellen von Polynomen haben wir eine Reihe von allgemeinen Begriffen und Resultaten kennengelernt:

1. Polynome und Symmetrische Polynome
   - Elementarsymmetrische Polynome (Diese liefern Zusammenhang zwischen Nullstellen und Koeffizienten eines Polynoms)
   - Lexikographische Ordnung auf Polynomen
   - Satz über symmetrische Polynome: Jedes symmetrische Polynom lässt sich eindeutig als Polynom in den elementarsymmetrischen Polynomen schreiben. (Der Beweis liefert einen Algorithmus dafür.)
   - Satz über symmetrische Funktionen
   - Separable Polynome, Test mittels formaler Ableitung
   - Irreduzible Polynome sind in Charakteristik 0 und in endlichen Körpern automatisch separabel.
2. Körpererweiterungen und Konstruktion von Körpern
   - Universelle Eigenschaft von Quotientenkörpern
   - Körperautomorphismen und Galoisgruppe

- Zerfällungskörper, Existenz (Konstruktion) und Eindeutigkeit
- Zerfällungskörperwunder (Trick: Körperketten durch hinzufügen einzelner Elemente aufbauen)
- Charakterisierung von separablen Zerfällungskörpern über $\#\operatorname{Aut}(L|K) = [L : K]$.
- Separable Erweiterungen, Charakterisierung davon.
- Perfekte Körper
- Galoiskorrespondenz: Für separable Zerfällungskörper entsprechen Zwischenkörper genau Untergruppen der Galoisgruppe
- Artin's Lemma
- Lösungsformel für Gleichung 3. Grades mittels Galoiskorrespondenz.

3. Gruppen
   - Normalteiler

Anwendungen der Galoiskorrespondenz

Sie hatten sich ganz zu Recht Beispiele für die Galoiskorrespondenz gewünscht. Dafür müssen wir natürlich ersteinmal Zerfällungskörper finden, in denen wir genug über die Galoisgruppe wissen, um deren Untergruppen verstehen zu können.

Galoiskorrrespondenz und Kreisteilung

Wenn wir anfangen darüber nachzudenken, werden wir sehen, dass die Galoiskorrespondenz ein schönes Beispiel dafür ist, dass schöne Resultate, die beim Versuch eine bestimmte Frage zu beantworten gefunden worden, meistens gleichzeitig auch Probleme auflösen, die uns schon begegnet sind.

Die ersten Körpererweiterungen, die wie gefunden haben entstanden durch Wurzelziehen. Für n-te Wurzeln erhalten wir damit erst dann Zerfällungskörper, wenn wir noch die n-ten Einheitswurzeln hinzufügen.

Die Galoisgruppe der p-ten Einheitswurzeln

Ist $n = p$ eine Primzahl, so haben wir gesehen, dass das Minimalpolynom der p-ten Einheitswurzel $\zeta_p = e^{\frac{2\pi i}{p}}$ über $\mathbb{Q}$ gerade

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-1} + \cdots + x + 1$$

ist und $\mathbb{Q}(\zeta_p) \cong \mathbb{Q}[x]/(\Phi_p(x))$ ist ein Zerfällungskörper des Polynoms Φ_p, da die Potenzen ζ_p^k von ζ_p (bzw. die Potenzen $[x]^k$ der Restklasse $[x] \in \mathbb{Q}[x]/(\Phi_p(x))$) für $k = 0, \ldots, p-1$ die p verschiedenen Nullstellen von $x^p - 1 = \Phi_p(x)(x-1)$ sind.

Wir wissen also:

1. $\mathbb{Q}(\zeta_p)|\mathbb{Q}$ ist ein Zerfällungskörper eines separablen Polynoms.
2. $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$, also ist nach der Charakterisierung von Zerfällungskörpern (Satz 49) $\#\operatorname{Aut}(\mathbb{Q}(\zeta_p)|\mathbb{Q}) = p - 1$
3. Jede Nullstelle $\alpha \in \mathbb{Q}(\zeta_p)$ des Polynoms Φ_p definiert einen Körperhomomorphismus

$$\begin{aligned} \mathbb{Q}(\zeta_p) \cong \mathbb{Q}[x]/(\Phi_p(x)) &\to \mathbb{Q}(\zeta_p) \\ x &\mapsto \alpha \end{aligned}$$

der also einen Ausdruck $a_{p-1}\zeta_p^{p-1} + \cdots + a_1\zeta_p + a_0$ auf $a_{p-1}\alpha^{p-1} + \cdots + a_1\alpha + a_0$ abbildet.

4. Da die Nullstellen von ϕ_p gerade die Zahlen $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$ sind, gibt es also für $k = 1, \ldots, p-1$ einen Körperautomorphismus

$$\begin{aligned} \sigma_k \colon \mathbb{Q}(\zeta_p) &\to \mathbb{Q}(\zeta_p) \\ \zeta_p &\mapsto \sigma_k(\zeta_p) := \zeta_p^k. \end{aligned}$$

Behauptung 58. *Für jede Primzahl p definiert die Abbildung*

$$\begin{aligned} \mathrm{Aut}(\mathbb{Q}(\zeta_p)|\mathbb{Q}) &\to ((\mathbb{Z}/p\mathbb{Z})^*, \cdot) \\ \sigma &\mapsto k \end{aligned}$$

wobei k die eindeutig bestimmte Restklasse ist, für die $\sigma(\zeta_p) = \zeta^k$ gilt, einen Isomorphismus von Gruppen.

Beweis. Wir haben gerade schon gesehen, dass die Abbildung surjektiv ist, da zu jedem k der Körperhomomorphismu σ_k gerade so definiert war, dass $\sigma_k(\zeta_p) = \zeta_p^k$ gilt.

Die Abbildung ist ein Gruppenhomomorphismus, denn gilt für $\sigma, \tau \in \mathrm{Aut}(\mathbb{Q}(\zeta_p)|\mathbb{Q})$, dass $\sigma(\zeta_p) = \zeta^k, \tau(\zeta_p) = \zeta_p^\ell$, so gilt

$$\begin{aligned} \sigma \circ \tau(\zeta_p) &= \sigma(\tau(\zeta_p)) \\ &= \sigma(\zeta_p^\ell) && \tau(\zeta_p) = \zeta_p^\ell \text{ eingesetzt} \\ &= \sigma(\zeta_p)^\ell && \sigma \text{ Körperhomomorphismus} \\ &= (\zeta_p^k)^\ell && \sigma(\zeta_p) = \zeta^k \text{ eingesetzt} \\ &= \zeta_p^{k\cdot\ell}. \end{aligned}$$

Also wird in der Tat $\sigma \circ \tau$ auf $k \cdot \ell$ abgebildet.

Die Abbildung ist damit einerseits automatisch bijektiv, da die beiden Mengen gleich viele Elemente haben, andererseits könnten wie das auch direkt sehen, da die Automorphismen eindeutig durch den Wert auf dem erzeugenden Element ζ_p bestimmt sind. □

Beispiele: Das 5-Eck und das 17-Eck

Beispiel 59 (p=5)**.** Lassen Sie uns für $p = 5$ alle Untergruppen der Galoisgruppe $\mathrm{Aut}(\mathbb{Q}(\zeta_5)|\mathbb{Q}) \cong ((\mathbb{Z}/5\mathbb{Z})^*, \cdot)$ bestimmen, indem wir zunächst schauen, was die kleinsten Unterguppen H_a der Gruppe $G = ((\mathbb{Z}/5\mathbb{Z})^*, \cdot)$ sind, die ein gegebenes Element $a \in G$ enthalten:

Element	$H_a = \{1, a, a^2, \ldots\}$
[1]	$H_1 = \{[1]\}$
[2]	$H_2 = \{[1], [2], [4] = [-1], [8] = [3]\} = G$
[3]	$H_3 = \{[1], [3], [9] = [4], [12] = [2]\} = G$
[4]	$H_4 = \{[1], [4]\}$

Damit ist $H_4 < G = (\mathbb{Z}/5\mathbb{Z})^*$ die einzige Untergruppe die nicht $\{1\}$ oder G selbst ist.

Für die Körpererweiterung $L = \mathbb{Q}(\zeta_5)|\mathbb{Q} = K$ ist also L^{H_4} der einzige Zwischenkörper $K \subsetneq L^{H_4} \subsetneq L$.

Den Unterkörper

$$L^{H_4} = \{\alpha \in \mathbb{Q}(\zeta_5) \mid \sigma_4(\alpha) = \alpha\}$$

können wir ausrechnen, denn $\sigma_4(\zeta_5) = \zeta_5^4$ also ist

$$\begin{aligned}
\zeta_5^k &\mapsto \sigma_4(\zeta_5^k) = \zeta_5^{4k} \\
\zeta_5 &\to \zeta_5^4 \\
\zeta_5^2 &\to \zeta_5^8 = \zeta_5^3 \\
\zeta_5^3 &\to \zeta_5^{12} = \zeta_5^2 \\
\zeta_5^4 &\to \zeta_5^{16} = \zeta_5.
\end{aligned}$$

Außerdem wissen wir, dass $\zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4$ eine Basis des $\mathbb{Q}$-Vektorraums $\mathbb{Q}(\zeta_5)$ ist, denn das gilt für $1, \zeta_5, \zeta_5^2, \zeta_5^3$ (weil $1, [x], [x^2], [x^3]$ ein Basis von $\mathbb{Q}[x]/(\Phi_5(x))$ ist) und

$$1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0.$$

Also sind die invarianten Elemente Linearkombinationen von

$$\alpha_2 = (\zeta_3 + \zeta_3^4) \text{ und } \alpha_1 = (\zeta_3^2 + \zeta_3^3).$$

Und für diese Elemente gilt

$$\sigma_2(\alpha_2) = \alpha_1, \sigma_2(\alpha_1) = \alpha_2.$$

Damit ist

$$p(x) = (x - \alpha_2)(x - \alpha_1)$$

ein Polynom, das unter σ_2 und damit unter G invariant ist, also das Minimalpolynom von α_2 in $\mathbb{Q}[x]$. Wir können das ausrechnen

$$\begin{aligned}
\alpha_1 + \alpha_2 &= \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = -1 \\
\alpha_1 \cdot \alpha_2 &= (\zeta_3^2 + \zeta_3^3)(\zeta_3^1 + \zeta_3^4) \\
&= \zeta_3^3 + \zeta_3^6 + \zeta_3^4 + \zeta_3^7 \\
&= \zeta_5^3 + \zeta_5 + \zeta_5^4 + \zeta_5^2 = -1.
\end{aligned}$$

Also ist $p(x) = x^2 + x - 1$ und daher

$$\alpha_{2,1} = \pm\sqrt{1 + \frac{1}{4}} - \frac{1}{2} = \frac{\pm\sqrt{5} - 1}{2}.$$

Da der Realteil von ζ_5 positiv ist, ist α_2 die positive Lösung der Gleichung.

Damit ist $L^{H_2} = \mathbb{Q}(\sqrt{5})$.

So finden wir die Konstruktion eines regelmäßigen 5-Ecks aus der Galoiskorrespondenz:

1. Der einzige quadratische Zwischenkörper von $\mathbb{Q} \subset \mathbb{Q}(\zeta_5)$ ist $\mathbb{Q}(\sqrt{5})$.
2. Wir können $\sqrt{5}$ konstruieren und
$$\alpha_2 = \zeta_5 + \zeta_5^4 = \zeta_5 + \overline{\zeta_5} = 2\mathrm{Re}(\zeta_5).$$
3. ζ_5 ist dann der Schnittpunkt der Senkrechten durch $\mathrm{Re}(\zeta_5)$ und dem Einheitskreis.

WIR SOLLTEN also probieren, ob das auch für $p = 17$ funktioniert.

Beispiel 60. Die Galoisgruppe $\mathrm{Aut}(\mathbb{Q}(\zeta_{17})|\mathbb{Q})$ ist

$$\mathrm{Aut}(\mathbb{Q}(\zeta_{17})|\mathbb{Q}) \cong ((\mathbb{Z}/17\mathbb{Z})^*, \cdot).$$

Die von einem Element erzeugten Untergruppen sind:

Element	$H_a = \{1, a, a^2, \dots\}$
$[1]$	$H_1 = \{[1]\}$
$[2]$	$H_2 = \{[1], [2], [4], [8], [16] = [-1], [-2], [-4], [-8]\}$
$[3]$	$H_3 = \{[1], [3], [9], [10], [13], [5], [15], [11], [16], [14], [8], [7], [4], [12], [2], [6]\} = G$

Die Potenzen von $[3]$ liefern also alle Elemente von $\mathbb{Z}/17\mathbb{Z}^*$, d.h. die Abbildung

$$\begin{aligned} F\colon (\mathbb{Z}/16\mathbb{Z}, +) &\to (\mathbb{Z}/17\mathbb{Z}^*, \cdot) \\ k &\mapsto F(k) = [3]^k \end{aligned}$$

ist ein surjektiver Gruppenhomomorphismus (da

$$F(k+\ell) = [3]^{k+\ell} = [3]^k[3]^\ell = F(k) \cdot F(\ell)).$$

Da beide Seiten 16 Elemente haben ist F ein Isomorphismus.

Das hilft uns weiter, denn die Untergruppen von $(\mathbb{Z}/16\mathbb{Z}, +)$ kennen wir: Ist $H < \mathbb{Z}/16\mathbb{Z}$ eine Untergruppe, so ist das Urbild in $\mathbb{Z}$

$$\widetilde{H} := \{a \in \mathbb{Z} \mid [a] \in H\} < \mathbb{Z}$$

eine Untergruppe. Aber Untergruppen von $\mathbb{Z}$ sind immer von der Form $n\mathbb{Z}$ für ein $n \in \mathbb{Z}$, weil für $a, b \in \widetilde{H} < \mathbb{Z}$ nach dem euklidischen Algorithmus auch $\mathrm{ggT}(a, b) = ma + m'b \in \widetilde{H}$ liegt, und darum $\widetilde{H} = n\mathbb{Z}$ für die kleinste positive Zahl $n \in \widetilde{H}$. Da das Urbild $\widetilde{H}$ von $H < \mathbb{Z}/16\mathbb{Z}$ außerdem $16\mathbb{Z}$ enthält, kommen für $\widetilde{H} = n\mathbb{Z}$ nur Zahlen n die Teiler von 16 sind in Frage, d.h. alle Untergruppen $H < \mathbb{Z}/16\mathbb{Z}$ sind

$$\{0\} < 8\mathbb{Z}/16\mathbb{Z} < 4\mathbb{Z}/16\mathbb{Z} < 2\mathbb{Z}/16\mathbb{Z} < \mathbb{Z}/16\mathbb{Z}.$$

Bevor wir das verwenden, um uns zu überlegen wie wir mit dieser Information überraschend leicht eine Formel für ζ_{17}, also die komplizierte Formel für $\cos(\frac{2\pi}{17})$ finden können, möchte ich kurz festhalten was wir uns gerade über Untergruppen überlegt haben.

Einschub: Zyklische Gruppen

Der Trick um alle Unterguppen von $\mathrm{Aut}(\mathbb{Q}(\zeta_{17})|\mathbb{Q})$ zu finden war zu bemerken, dass $(\mathbb{Z}/17\mathbb{Z})^*$ von einem Element – der Restklasse $[3]$ – erzeugt war. Gruppen mit dieser Eigenschaft heißen zyklisch.

Definition. Eine endliche Gruppe $(H, \cdot)$ heißt *zyklisch* wenn es ein Element $h \in H$ gibt, so dass

$$H = \{e, h, h^2, \dots, h^{\#H-1}\},$$

d.h. so dass jedes Element von H eine Potenz von h ist.

Eine Element $h \in H$ das die obige Eigenschaft besitzt heißt *erzeugendes Element* der Gruppe.

Bemerkung. Eine endliche Gruppe G mit N Elementen ist genau dann zyklisch, wenn Sie isomorph zu $(\mathbb{Z}/N\mathbb{Z}, +)$ ist. Daher kommt der Name.

Beweis. Ist nämlich G zyklisch und $h \in G$ ein erzeugendes Element, so definiert

$$\begin{aligned} f\colon (\mathbb{Z}/N\mathbb{Z}, +) &\to G \\ [a] &\mapsto h^a \end{aligned}$$

einen Isomorphismus von Gruppen:

1. f ist wohldefiniert weil für $a' = a + mN$ gilt

$$h^{a'} = h^{a+mN} = h^a \cdot h^{mN} = h^a \cdot (h^N)m = h^a \cdot e = h^a.$$

2. f ist wegen des Potenzrechengesetzes

$$f(a+b) = h^{a+b} = h^a \cdot h^b = f(a) \cdot f(b)$$

ein Homomorphismus.

3. f ist nach Definiton bijektiv, weil die Elemente $e = h^0, h, h^2, \ldots, h^{N-1}$ nach Definition genau alle Elemente von G sind.

Ist umgekehrt $f\colon (\mathbb{Z}/N\mathbb{Z}, +) \to G$ ein Isomorphismus, so ist das Element $h = f(1)$ ein Erzeugendes Element von H, da 1 ein Erzeugendes Element von $(\mathbb{Z}/N\mathbb{Z}, +)$ ist. □

Bemerkung. Wegen des obigen Resultates, wird eine unendliche Gruppe H darum manchmal zyklisch genannt, wenn H isomorph zu $(\mathbb{Z}, +)$ ist.

Lemma 61. *Die Untergruppen $H < (\mathbb{Z}/N\mathbb{Z}, +)$ sind genau die Untergruppen der Form $d\mathbb{Z}/N\mathbb{Z} < \mathbb{Z}/N\mathbb{Z}$ für die d ein Teiler von N ist.*

Beweis. Das Argument das wir oben für $\mathbb{Z}/16\mathbb{Z}$ gesehen haben, können wir abschreiben: Ist $H < \mathbb{Z}/N\mathbb{Z}$ eine Untergruppe, so ist das Urbild in $\mathbb{Z}$

$$\widetilde{H} := \{a \in \mathbb{Z} \mid [a] \in H\} < \mathbb{Z}$$

eine Untergruppe.

Untergruppen von $\mathbb{Z}$ sind immer von der Form $d\mathbb{Z}$ für ein $d \in \mathbb{Z}$, weil für $a, b \in \widetilde{H} < \mathbb{Z}$ nach dem euklidischen Algorithmus auch $\mathrm{ggT}(a,b) = ma + m'b \in \widetilde{H}$ liegt, und darum $\widetilde{H} = d\mathbb{Z}$ für die kleinste positive Zahl $d \in \widetilde{H}$.

Da das Urbild $\widetilde{H}$ von $H < \mathbb{Z}/N\mathbb{Z}$ außerdem $N\mathbb{Z}$ enthält, kommen für $\widetilde{H} = d\mathbb{Z}$ nur Zahlen d die N teilen in Frage. □

Die Galoiskorrespondenz und das regelmäßige 17-Eck

Zurück zu $\mathbb{Q}(\zeta_{17})$: Die Unterkörper $\mathbb{Q}(\zeta_{17})^H$ für die Untergruppen $H_8, H_4, H_2 \subseteq \mathrm{Aut}(\mathbb{Q}(\zeta_{17})|\mathbb{Q})$ mit $8, 4, 2$ Elementen können wir nun genau wie für ζ_5 leicht ausrechnen und den Körperturm

$$\mathbb{Q} \subsetneq \mathbb{Q}(\zeta_{17})^{H_8} \subsetneq \mathbb{Q}(\zeta_{17})^{H_4} \subsetneq \mathbb{Q}(\zeta_{17})^{H_2} \subsetneq \mathbb{Q}(\zeta_{17})$$

als Kette von expliziten quadratischen Erweiterungen schreiben:

1. Die Gruppe $G = \mathrm{Aut}(\mathbb{Q}(\zeta_{17})|\mathbb{Q})$ ist vom Automorphismus $\sigma\colon \mathbb{Q}(\zeta_{17}) \to \mathbb{Q}$ der durch $\sigma(\zeta_{17}) = \zeta_{17}^3$ gegeben ist erzeugt. Also ist $H_8 < G$ von σ^2, also der Abbildung für die $\sigma^2(\zeta_{17}) = \zeta_{17}^9$ gegeben ist erzeugt.

   Genau wie für $p = 5$ sind die Elemente

   $\mathbb{Z}/17\mathbb{Z}^* = \{[1], [3], [9], [10], [13], [5], [15], [11], [16], [14], [8], [7], [4], [12], [2], [6]\}$

$$\begin{aligned}
\alpha_1 &= \zeta_{17} + \sigma^2(\zeta_{17}) + \sigma^4(\zeta_{17}) + \cdots + \sigma^{14}(\zeta_{17}) \\
&= \sum_{k=0}^{7} \sigma^{2k}(\zeta_{17}) \\
&= \zeta_{17}^1 + \zeta_{17}^9 + \zeta_{17}^{13} + \zeta_{17}^{15} + \zeta_{17}^{16} + \zeta_{17}^8 + \zeta_{17}^4 + \zeta_{17}^2, \\
\alpha_2 &= \sigma(\zeta_{17}) + \sigma^3(\zeta_{17}) + \sigma^5(\zeta_{17}) + \cdots + \sigma^{15}(\zeta_{17}) \\
&= \sum_{k=0}^{7} \sigma^{2k+1}(\zeta_{17}) \\
&= \zeta_{17}^3 + \zeta_{17}^{10} + \zeta_{17}^5 + \zeta_{17}^{11} + \zeta_{17}^{14} + \zeta_{17}^7 + \zeta_{17}^{12} + \zeta_{17}^6
\end{aligned}$$

   per Konstruktion invariant unter σ^2 – liegen also in $\mathbb{Q}(\zeta_{17})^{H_8}$ – und werden unter σ vertauscht, also ist

$$p(x) = (x - \alpha_1)(x - \alpha_2) = x^2 - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2 \in \mathbb{Q}[x]$$

   da die Koeffizienten unter σ invariant sind. Das Polynom ist also das Minimalpolynom von α_1 und α_2 und wir können das ausrechnen:

$$\begin{aligned}
\alpha_1 + \alpha_2 &= \sum_{k=1}^{16} \zeta_{17}^k \\
&= -1 \quad \text{da } 1 + \zeta_{17} + \zeta_{17}^2 + \cdots + \zeta_{17}^{16} = 0. \\
\alpha_1 \cdot \alpha_2 &= \Big(\sum_{k=0}^{7} \sigma^{2k}(\zeta_{17})\Big)\Big(\sum_{k=0}^{7} \sigma^{2k+1}(\zeta_{17})\Big) \\
&= \cdots = -4
\end{aligned}$$

   Das Ergebnis ist plausibel, da beim Ausmultiplizieren der Summen insgesamt $64 = 4 \cdot 16$ Potenzen von ζ_{17} entstehen und die einzige Gleichung für die Einheitswurzeln die wir kennen ist die aus dem ersten Rechenschritt.

   Die Nullstellen von $p(x) = x^2 + x - 4$ sind

$$\alpha_{1,2} = \pm\sqrt{4 + \frac{1}{4}} - \frac{1}{2} = \frac{\pm\sqrt{17} - 1}{2}.$$

   Also ist $\mathbb{Q}(\zeta_{17})^{H_8} \cong \mathbb{Q}[t]/(t^2 + 1 - 4) \cong \mathbb{Q}(\sqrt{17})$.

2. Für $\mathbb{Q}(\zeta_{17})^{H_4}, \mathbb{Q}(\zeta_{17})^{H_2}$ können wir ganz genauso vorgehen: Die Summen $\beta_1 = \sum_{k=0}^{3} \sigma^{4k}(\zeta_{17})$ und $\beta_2 = \sum_{k=0}^{3} \sigma^{4k+2}(\zeta_{17})$

sind invariant unter σ^4, liegen also in $\mathbb{Q}(\zeta_{17})^{H_4}$ und werden unter σ^2 vertauscht, damit ist $(x-\beta_1)(x-\beta_2) \in \mathbb{Q}(\zeta_{17})^{H_8}$ das Minimalpolynom der β_i usw.

Auf dem Übungsblatt können Sie sich davon überzeugen, dass das tatsächlich ganz algorithmisch auf die Formel für $\cos(\frac{2\pi}{17}) = \mathrm{Re}(\zeta_{17})$ führt.

Endliche Untergruppen der multiplikativen Gruppe und regelmäßige p-Ecke

DER KNACKPUNKT in den Berechnungen der Untergruppen von $(\mathbb{Z}/p\mathbb{Z})^*$ war, dass wir für $p = 5$ und $p = 17$ jeweils zufällig gefunden haben, dass diese Gruppen zyklisch sind.

Das ist tatsächlich immer so:

Satz 62 (Endliche Untergruppen der multiplikativen Gruppe eines Körpers sind zyklisch)**.** *Ist K ein Körper und $H < (K^*, \cdot)$ eine endliche Untergruppe der multiplikativen Gruppe $(K^*, \cdot)$, so ist H eine zyklische Gruppe.*

Insbesondere ist für jeden endlichen Körper $\mathbb{F}$, die multiplikative Gruppe $(\mathbb{F}^*, \cdot)$ zyklisch und damit ist $((\mathbb{Z}/p\mathbb{Z})^*, \cdot)$ für alle Primzahlen p eine zyklische Gruppe.

Wir werden das gleich noch beweisen, es ist vielleicht in sofern plausibel, als $\alpha^n = 1$ in einem Körper bedeutet, dass α eine $n-$te Einheitswurzel ist und die Gruppe der $n-$ten Einheitswurzeln ist in $\mathbb{C}$ sichtbar eine zyklische Gruppe.

ZUNÄCHST möchte ich das Resultat aber verwenden, um uns zu überlegen, welche regelmäßigen p-Ecke konstruierbar sind. Wir wissen nämlich schon, dass ζ_p genau dann konstruierbar ist, wenn ζ_p in einem Körperturm

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = L$$

enthalten ist, bei dem alle Schritte quadratische Erweiterungen sind.

Behauptung 63. *Ist p eine Primzahl, so ist das regelmäßige p-Eck genau dann konstruierbar, wenn p eine Primzahl der Form $p = 2^{2^n} + 1$ ist.*

Beweis. 1. Damit ζ_p konstruierbar ist, muss $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ eine Potenz von 2 sein, also $p = 2^M + 1$ für ein $M \in bZ$.

2. Ist umgekehrt $p = 2^M + 1$ eine Primzahl, so ist

   $$\mathrm{Aut}(\mathbb{Q}(\zeta_p)|\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z}^*, \cdot) \cong (\mathbb{Z}/(p-1)\mathbb{Z}, +) = (\mathbb{Z}/2^M\mathbb{Z}, +)$$

   eine zyklische Gruppe der Ordnung 2^M und diese enthält die Kette von Untergruppen

   $$\{0\} < (2^{M-1}\mathbb{Z}/2^M\mathbb{Z}, +) < \cdots < (2^2\mathbb{Z}/2^M\mathbb{Z}, +) < (2\mathbb{Z}/2^M\mathbb{Z}, +) < (\mathbb{Z}/2^M\mathbb{Z}, +).$$

   Die Galoiskorrespondenz besagt, dass die zugehörigen Unterkörper von $\mathbb{Q}(\zeta_p)$ dann wie gewünscht einen Turm von quadratischen Erweiterungen liefern.

3. Ist $p = 2^M + 1$ eine Primzahl, so ist $M = 2^n$ notwendigerweise selbst eine Potenz von 2, denn ist $M = a \cdot b$ ein Produkt mit b ungerade, so ist das Polynom

$$(x^{a\cdot b} + 1) = \left((x^a)^b + 1\right)$$

nicht irreduzibel, da -1 eine Nullstelle ist, also

$$y^b + 1 = (y - 1)(y^{b-1} - y^{b-2} + \cdots + 1).$$

Also ist dann

$$\begin{aligned}(x^{a\cdot b} + 1) &= ((x^a)^b + 1) \\ &= (x^a - 1)((x^a)^{b-1} - (x^a)^{b-2} + \cdots + 1)\end{aligned}$$

und insbesondere

$$2^{a\cdot b} + 1 = (2^a - 1)((2^a)^{b-1} - (2^a)^{b-2} + \cdots + 1).$$

Also hat M keine ungeraden Teiler, ist also eine Potenz von 2.

□

Bemerkung (Fermat-Primzahlen)**.** Primzahlen der Form $p = 2^{2^n} + 1$, also zum Beispiel $3 = 2 + 1, 5 = 4 + 1, 17 = 16 + 1, 257 = 2^8 + 1, 65537 = 2^{16} + 1$ heißen Fermat-Primzahlen, weil Fermat festgestellt hatte, dass diese Beispiele alle Primzahlen sind und vermutete, dass dann wohl alle diese Zahlen Primzahlen sein sollten.

Für 257 hatten wir das in der Vorlesung im Kopf nachgerechnet, für 65537 ist das gerade noch per Hand möglich, da $\sqrt{(2^{16} + 1)} < 2^8 + 1 = 257$ ist und es nicht so viele Primzahlen bis 257 gibt.

Für die nächste Fermatzahl $2^{32} + 1 = 4.294.967.297$ war das per Hand nicht so leicht, aber Euler hat dann den Faktor 641 gefunden.

Mit Computerhilfe wurden mittlerweile sehr viele der folgenden Fermatzahlen ausprobiert und dabei immer faktorisiert. Bisher wurde keine einzige weitere Fermatprimzahl gefunden! Ob es tatsächlich keine weitere gibt ist eine ebenso offene Frage.

Beweis von Satz 62 (Endliche Untergruppen der multiplikativen Gruppe sind zyklisch). Sei $H < (K^*, \cdot)$ eine Untergruppe mit$N = \#H$ Elementen. Wir wissen schon, dass die Ordnung jedes Elementes von H ein Teile der Gruppenordnung N ist, d.h. alle Elemente $a \in H$ erfüllen die Gleichung $a^N = 1$. Die Elemente von H sind also N-verschiedene Nullstellen des Polynoms

$$p(x) = X^N - 1,$$

sind also genau die N-ten Einheitswurzeln in K. Ist $K \subseteq \mathbb{C}$ ein Teilkörper der komplexen Zahlen, sind wir damit schon fertig, denn die N-ten Einheitswurzeln in $\mathbb{C}$ sind eine zyklische Gruppe, die von $e^{\frac{2\pi i}{N}}$ erzeugt ist.

Für einen abstrakten Körper müssen wir einen anderen Weg finden, ein Element der Ordnung N in H zu finden. Sei $a \in H$ ein Element maximaler Ordnung n, dann teilt n die Gruppenordnung N

und es genügt zu zeigen, dass die Ordnung aller anderen Elemente n teilt, denn dann sind die N Elemente von H Nullstellen von $x^n - 1$ und dann muss $n = N$ sein.

Angenommen $b \in H$ ist ein Element der Ordnung m, die n nicht teilt. Ich behaupte, dass wir aus a und b ein Element der Ordnung $\mathrm{kgV}(n, m)$ konstruieren können. Das ist ein Widerspruch zur Annahme, dass n die maximale Ordnung von Elementen von H war.

Um ein Element der Ordnung $\mathrm{kgV}(n, m)$ zu konstruieren schreiben wir

$$\mathrm{kgV}(n, m) = n' \cdot m',$$

wobei m' das Produkt über die Primfaktoren von m ist, die in m mit größerer Potenz als in n vorkommen und n' das Produkt über die Primfaktoren von n ist die in n mit mindestens gleicher Potenz wie in m vorkommen, d.h.

$$n = n' \cdot n''$$
$$m = m' \cdot m''$$

so dass $m''|n', n''|m'$ und n', m' sind teilerfremd.

Dann hat

$$a' := a^{n''} \text{ hat Ordnung } n' \text{ und}$$
$$b' := b^{m''} \text{ hat Ordnung } m'.$$

Damit hat dann aber $a'b'$ die Ordnung $n' \cdot m'$, denn einerseits ist

$$(a'b')^{n' \cdot m'} = (a^{n''n'})^{m'} (b^{m' \cdot m''})^{n'} = 1 \cdot 1 = 1.$$

Und für $1 \leq k < n'm'$ ist

$$(a'b')^k = \underbrace{(a^{n''})^k}_{\text{Ordnung teilt } n'} \cdot \underbrace{((b^{m''})^k}_{\text{Ordnung teilt } m'}.$$

Ein Produkt zweier Elemente von teilerfremder Ordnung kann aber nicht 1 sein, da die Ordnung von c gleich der Ordnung von c^{-1} ist und $cd = 1$ bedeutet, dass $d = c^{-1}$ ist. Daher müssen die beiden Faktoren beide einzeln 1 sein, d.h. k muss durch die teilerfremden Zahlen n' und m' teilbar sein, ist also ein Vielfaches von $n'm'$. Das Zeigt, dass die Ordnung von $a'b'$ genau $n' \cdot m'$ ist. □

Definition. Ein Element $\zeta_N \in K$ eines Körpers K heißt *primitive N-te Einheitswurzel* wenn $\zeta_N^N = 1$ und $\zeta_N^k \neq 1$ für $1 \leq k < N$ gilt.

Bemerkung. 1. Primitive N-te Einheitswurzeln sind die erzeugenden Elemente der Gruppe der N-ten Einheitswurzeln.

2. Ist ζ_N eine primitive N-te Einheitswurzel, so ist eine Potenz ζ_N^a genau dann wieder eine Primitive $N-$te Einheitswurzel, wenn a, N teilerfremd sind.

Beweis. Für eine primitive N-te Einheitswurzel ist ζ_N^m genau dann 1 wenn $m = n \cdot N$ ein Vielfachest von N ist, da für $m = nN + k$ gilt $\zeta_N^{nN+k} = (\zeta_N^N)^n \cdot \zeta_N^k = \zeta_N^k$.

Also ist für $(\zeta_N^a)^k = \zeta_N^{ak}$ genau dann 1, wenn N das Produkt ak teilt und diese Bedinung ist genau dann äquivalent dazu dass N die Zahl k teilt, wenn a und N teilerfremd sind. Also ist ζ_N^a genau dann wieder eine Primitive $N-$te Einheitswurzel, wenn a, N teilerfremd sind. □

Exkurs: Alle endlichen Körper und QR-Codes

Folgerung 64. *Bis auf Isomorphie existiert für jede Potenz $q = p^n$ einer Primzahl p genau ein Körper $\mathbb{F}_q$ mit $q = p^n$ Elementen, nämlich der Zerfällungskörper des separablen Polynoms $x^{q-1} - 1 \in \mathbb{F}_p[x]$.*

Beweis. Auf dem Übungszettel hatten Sie sich schon überlegt, dass der Zerfällungskörper des Polynoms $x^q - x = x(x^{q-1} - 1)$ genau q Elemente besitzt, da die Nullstellen dieses Polynoms wegen der merkwürdigen binomischen Formel $(x + y)^p = x^p + y^p$ in Körpern in denen $p = 0$ gilt, selbst schon einen Körper bilden. Das Zeigt die Existenz eines Körpers mit $q = p^n$ Elementen.

Die Eindeutigkeit folgt, weil wir gerade gezeigt haben, dass für endliche Körper k die Multiplikative Gruppe k^* eine zyklische Gruppe ist und darum alle Elemente von k^* Nullstellen von $x^{\#k-1} - 1$ sind. Da wir schon gesehen haben, dass die Anzahl der Elemente eines endlichen Körper immer eine Primzahlpotenz p^n ist, ist also jeder endliche Körper ein Zerfällungskörper eines Polynoms der Form $x^{q-1} - 1$ und Zerfällungskörper sind bis auf Isomorphie eindeutig bestimmt. □

Bemerkung (Der endliche Körper $\mathbb{F}_{256}$ und QR-Codes)**.** Der endliche Körper $\mathbb{F}_{256}$ mit 256 Elementen lässt sich als

$$\mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x^2 + 1)$$

schreiben, d.h. die Elemente lassen sich eindeutig als Linearkombination

$$a = b_0 + b_1[x] + \cdots + b_7[x]^7$$

mit $b_0, \ldots, b_7 \in \{0, 1\}$ schreiben. Um zu zeigen, dass das ein Körper ist, müssen wir nur überlegen, dass das Polynom $x^8 + x^4 + x^3 + x^2 + 1 \in \mathbb{F}_2[x]$ irreduzibel ist. Das ist per Hand möglich, da wir nur prüfen müssen, dass es keine irreduziblen Teiler vom Grad ≤ 4 gibt und es gibt nicht so viele irreduzible Polynome vom Grad ≤ 4 in $\mathbb{F}_2[x]$. Das Polynom ist dabei gerade so gewählt, dass die Restklasse $[x]$ ein erzeugendes Element der multiplikativen Gruppe $\mathbb{F}_{256}^*$ ist.

In dieser Form wird der Körper für QR-Codes verwendet. Das Grundprinzip hierfür ist ein sogenannter Reed-Solomon Code (RS-Code), eine ebenso geniale wie einfache Idee. Das ursprüngliche Problem ist, für einen Informationsvektor $\underline{x} = (x_1, \ldots, x_n)$ einen längeren Vektor

$$F(x_1, \ldots, x_n) = (y_1, \ldots, y_n, y_{n+1}, \ldots, y_{n+m})$$

so auszuwählen und abzuspeichern, dass sich für unterschiedliche Vektoren $(x_1, \dots, x_n) \neq (x'_1, \dots, x'_n)$ die Ergebnisvektoren $F(\underline{x}), F(\underline{x}')$ an möglichst vielen Stellen unterscheiden.

Damit können wir nämlich auch wenn einige der Koordinaten $(y_1, \dots, y_n, y_{n+1}, \dots, y_{n+m})$ unlesbar werden, den Vektor $\underline{x}$ zurückberechnen, nämlich als den eindeutigen Vektor im Bild von F, für den $F(\underline{x})$ an den anderen Stellen übereinstimmt.

Dazu müssten wir also eine Abbildung

$$F\colon k^n \to k^{n+m}$$

finden, für die sich je zwei Bildvektoren an vielen Stellen unterscheiden. Wählen wir eine lineare Abbildung F, so bedeutet das einfach, dass für einen Vektor $\underline{x} \neq \underline{0}$ der Bildvektor viele Einträge $\neq 0$ hat.

Die Idee für RS-Codes ist, $k^n \cong k[x]_{\leq n-1}$ als Vektorraum der Polynome vom Grad $\leq n-1$ aufzufassen und als Abbildung F die Auswertung an Werten $a_1, \dots, a_{n+m} \in k$ zu verwenden:

$$(c_0, \dots, c_{n-1}) \mapsto p_c(x) = c_0 + c_1 x + \dots + c_{n-1} x^{n-1} \mapsto \begin{pmatrix} p_c(a_1) \\ p_c(a_2) \\ \vdots \\ p_c(a_{n+m}) \end{pmatrix} =: F(\underline{c}).$$

Da Polynome vom Grad $n-1$ höchstens $n-1$ Nullstellen besitzen, hat $F(\underline{c})$ für $\underline{c} \neq 0$ mindestens $m+1$ von 0 verschiedene Koordinaten.

Für QR-Codes wird $k = \mathbb{F}_{256}$ verwendet, weil dieser Körper einerseits hinreichend viele Elemente besitzt, um an unterschiedlichen Werten auswerten zu können und andererseits die Elemente als ein Byte abgespeichert werden können.

Je nach Format der QR-Codes können damit bis zu 30% fehlerhafter Koordinaten korrigiert werden. In der Abbildung sehen Sie ein Muster in dem die Koordinatenbytes abgelegt werden und zusätzlich markiert die Teile des QR-Codes die für die Technik zuständig sind, um Orientierung (die Kästchen), schwarz-weiß Kontrast (die abwechselnd schwarz-weiße horizontale und vertikale Linie) und Codierungsmethode (rot markiert) festzulegen.

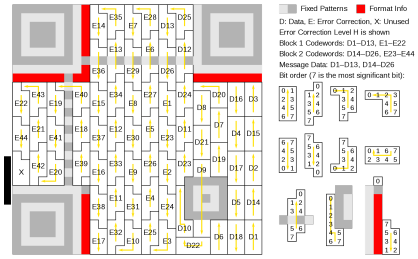


Abbildung 1: Grafik aus Wikipedia entnommen, der englische Artikel ist recht detailliert.

Einheitswurzeln, N-Ecke und N-te Wurzeln

Mit unserem Wissen über die Galoiskorrespondenz und die Struktur der Automotphismengruppe $\mathrm{Aut}(\mathbb{Q}(\zeta_p)|\mathbb{Q})$ können wir nun klären, welche N-Ecke sich mit Zirkel und Lineal konstruieren lassen.

Satz 65. *Ein regelmäßiges N-Eck ist genau dann konstruierbar, wenn* $N = 2^n \prod_{i=1}^{m} p_i$ *ein Produkt einer Potenz von* 2 *und paarweise verschiedener Fermat-Primzahlen* p_i *ist.*

Da die einzigen bekannten Fermat-Primzahlen $3, 5, 17, 257, 65537$ sind, ist es ein glücklicher Zufall, dass $12 = 2^2 \cdot 3$ und $60 = 2^2 \cdot 3 \cdot 5$ konstruierbar sind, was für Ziffernblätter von Uhren praktisch ist.

Beweis. Wir haben schon gesehen, dass:

1. Ein N Eck kann nur dann konstruierbar sein, wenn $[\mathbb{Q}(\zeta_N) : \mathbb{Q}] = 2^n$ eine Potenz von 2 ist (Satz 5).

2. Ist p eine Primzahl, so ist ein regelmäßiges p-Eck genau dann konstruierbar, wenn p eine Fermat-Primzahl (oder $p = 2$) ist (Behauptung 63).

3. Ist $N = n \cdot m$ ein Produkt und das regelmäßige N-Eck konstruierbar, so auch das regelmäßige n-Eck, da $\zeta_N^m = \zeta_n$. Ist also ein regelmäßiges N-Eck konstruierbar, so sind 2 und Fermat-Primzahlen die einzigen möglichen Primfaktoren.

4. $[\mathbb{Q}(\zeta_{p^2}) : \mathbb{Q}] = p(p-1)$, weil wir auf einem Übungsblatt nachgerechnet hatten, dass $\Phi_{p^2}(x) = \frac{x^{p^2}-1}{x^p-1}$ das Minimalpolynom von ζ_{p^2} ist. Da $p(p-1)$ für $p \neq 2$ keine Potenz von 2 ist, ist ein regelmäßiges p^2-Eck nur für $p = 2$ konstruierbar.

5. Ist $N = n \cdot m$ ein Produkt teilerfremder Zahlen n, m und sind ζ_n, ζ_m konstruierbar, so auch ζ_N: Das gilt da die Ordnung von $\zeta_n \cdot \zeta_m$ gerade $\mathrm{kgV}(n, m) = nm$ ist. Daher ist $\zeta_n \cdot \zeta_m$ eine primitive N-te Einheitswurzel und also ist ζ_N konstruierbar.

Das zeigt die Behauptung. □

FÜR JEDE NATÜRLICHE ZAHL N können wir nicht nur entscheiden, ob ζ_N konstruierbar ist, sondern wir können ähnlich wie für Primzahlen die Galoisgruppe von $\mathbb{Q}(\zeta_N)|\mathbb{Q}$ bestimmen.

Ist nämlich $\sigma \in \mathrm{Aut}(\mathbb{Q}(\zeta_N)|\mathbb{Q})$, so ist σ eindeutig durch den Wert von $\sigma(\zeta_N)$ bestimmt, da σ ein Körperhomomorphismus ist und jedes Element von $\mathbb{Q}(\zeta_N)$ als $\mathbb{Q}$-Linearkombination der Potenzen von ζ_N geschrieben werden kann und $\sigma(\zeta_N^a) = \sigma(\zeta_N)^a$ gilt.

Da außerdem $\sigma(1) = 1$ ist, muss also

$$\sigma(\zeta_N)^N = \sigma(\zeta_N^N) = \sigma(1) = 1$$

wieder eine N-te Einheitswurzel sein und sogar eine primitive N-te Einheitswurzel, da

$$\sigma(\zeta_N)^k = 1 \Leftrightarrow \sigma(\zeta_N^k) = 1 \Leftrightarrow \zeta_N^k = 1$$

weil σ bijektiv ist.

Die primitiven N-ten Einheitswurzeln sind aber genau die Zahlen der Form ζ_N^k für die k, N teilerfremd sind (**??** 2.).

Folgerung 66. *Die Abbildung*

$$F\colon \mathrm{Aut}(\mathbb{Q}(\zeta_N)|\mathbb{Q}) \to (\mathbb{Z}/N\mathbb{Z}^*, \cdot)$$
$$\sigma \mapsto F(\sigma) := k \qquad \textit{wobei } k \textit{ durch } \sigma(\zeta_N) = \zeta_N^k \textit{ bestimmt ist,}$$

ist ein injektiver Gruppenhomomorphismus.

Beweis. Da σ durch den Wert $\sigma(\zeta_N)$ bestimmt ist, ist die Abbildung injektiv, wir müssen also nur noch prüfen, dass die Abbildung

ein Homomorphismus ist. Seien also $\sigma, \tau \in \mathrm{Aut}(\mathbb{Q}(\zeta_N)|\mathbb{Q})$ und $F(\sigma) = k, F(\tau) = \ell$, d.h. $\sigma(\zeta_N) = \zeta_N^k, \tau(\zeta_N) = \zeta_N^\ell$. Dann ist

$$\begin{aligned}
\sigma \circ \tau(\zeta_N) &= \sigma(\tau(\zeta_N)) && \text{Definition } \circ \\
&= \sigma(\zeta_N^\ell) && \tau(\zeta_N) = \zeta_N^\ell \\
&= \sigma(\zeta_N)^\ell && \sigma \text{ Körperhomomorphismus} \\
&= (\zeta_N^k)^\ell && \sigma(\zeta_N) = \zeta_N^k \\
&= \zeta_N^{k\cdot\ell} && \text{Potenzgesetz.}
\end{aligned}$$

Also ist $F(\sigma \circ \tau) = k \cdot \ell = F(\sigma) \cdot F(\tau)$. □

Bemerkung. Da $\mathbb{Q}(\zeta_N)|\mathbb{Q}$ ein Zerfällungskörper eines separablen Polynoms ist, gilt $\#\,\mathrm{Aut}(\mathbb{Q}(\zeta_N)|\mathbb{Q}) = [\mathbb{Q}(\zeta_N) : \mathbb{Q}]$. Um zu zeigen, dass die Abbildung aus der Folgerung ein Isomorphismus ist, genügt es also zu zeigen, dass

$$[\mathbb{Q}(\zeta_N) : \mathbb{Q}] = \#(\mathbb{Z}/N\mathbb{Z}^*) =: \varphi(N)$$

gilt. Das überlegen wir uns in der nächsten Vorlesung.

Die Abbildung φ, die durch

$$\begin{aligned}
\varphi(N) &:= \#(\mathbb{Z}/N\mathbb{Z}^*) \\
&= \#\{k \in \{1, \dots, N\} | k, N \text{ teilerfremd}\}
\end{aligned}$$

gegeben ist, heißt *Eulersche-Phi-Funktion*.

Ganz ähnlich wie für $\mathbb{Q}(\zeta_N)|\mathbb{Q}$ können wir die Galoisgruppe von Erweiterungen die durch das hinzufügen N-ter Wurzeln entstehen beschreiben.

Satz 67 (Galoisgruppe von Wurzel-Erweiterungen)**.** *Sei K ein Körper, der eine primitive N-te Einheitswurzel ζ_N enthält und $a \in K$, dann ist die Abbildung*

$$\begin{aligned}
F\colon \mathrm{Aut}(K(\sqrt[N]{a})|K) &\to (\mathbb{Z}/N\mathbb{Z}, +) \\
\sigma &\mapsto F(\sigma) := k \qquad \textit{wobei } k \textit{ durch} \\
&\qquad\qquad\qquad\quad \sigma(\sqrt[N]{a}) = \zeta_N^k \sqrt[N]{a} \textit{ bestimmt ist,}
\end{aligned}$$

ein injektiver Gruppenhomomorphismus, der genau dann ein Isomorphismus ist wenn $x^N - a \in K[x]$ irreduzibel ist.

Beweis. Da zu einer Nullstelle $\sqrt[N]{a}$ von $x^N - a$, auch $\zeta_N^k x^N - a$ für $k = 1, \dots, N$ Nullstellen sind, zerfällt das Polynom $x^N - a$ in $K(\sqrt[N]{a})$ in N verschiedene Linearfaktoren, d.h. $K(\sqrt[N]{a}$ ist ein Zerfällungskörper eines separablen Polynoms.

Jeder Automorphismus $\sigma\,\mathrm{Aut}(K(\sqrt[N]{a})|K)$ bildet Nullstellen von $x^N - a$ auf Nullstellen von $x^N - a$ ab, also ist für alle σ tatsächlich $\sigma(\sqrt[N]{a}) = \zeta_N^k \sqrt[N]{a}$ für ein $k \in \mathbb{Z}/N\mathbb{Z}$, die Abbildung ist also wohldefiniert und injektiv, weil σ durch den Wert auf dem erzeugenden Element $\sqrt[N]{a}$ der Körpererweiterung eindeutig bestimmt ist.

Die Abbildung ist ein Homomoprhismus, da für $\sigma, \tau \in \mathrm{Aut}(K(\sqrt[N]{a}|K)$ wie zuvor gilt, dass wenn $\sigma(\sqrt[N]{a}) = \zeta_N^k \sqrt[N]{a}, \tau(\sqrt[N]{a}) = \zeta_N^\ell \sqrt[N]{a}$ gilt,

dass

$$\begin{aligned}
\sigma\circ\tau(\sqrt[N]{a}) &= \sigma(\tau(\sqrt[N]{a})) && \text{Definition } \circ\\
&= \sigma(\zeta_N^\ell \sqrt[N]{a}) && \tau(\zeta_N)=\zeta_N^\ell\\
&= \zeta_N^\ell\sigma(\zeta_N) && \sigma\sigma(b)=b \text{ für alle } b\in K\\
&= \zeta_N^\ell(\zeta_N^k \sqrt[N]{a}) && \sigma(\sqrt[N]{a})=\zeta_N^k\sqrt[N]{a}\\
&= \zeta_N^{k+\ell}\sqrt[N]{a} && \text{Potenzgesetz.}
\end{aligned}$$

Also ist $F(\sigma\circ\tau)=k+\ell=F(\sigma)+F(\tau)$. □

Kreisteilungspolynome und $\mathrm{Gal}(\mathbb{Q}(\zeta_N)|\mathbb{Q})$

Wir sollten uns noch überlegen, dass die Galoisgruppe der Körperwerweiterung $\mathrm{Aut}(\mathbb{Q}(\zeta_N)|\mathbb{Q})$ tatsächlich isomorph zu $((\mathbb{Z}/N\mathbb{Z})^*,\cdot)$ ist.

Satz 68. *Die Abbildung*

$$\begin{aligned}
F\colon \mathrm{Aut}(\mathbb{Q}(\zeta_N)|\mathbb{Q}) &\to (\mathbb{Z}/N\mathbb{Z}^*,\cdot)\\
\sigma &\mapsto F(\sigma):=k \qquad \textit{wobei } k \textit{ durch } \sigma(\zeta_N)=\zeta_N^k \textit{ bestimmt ist,}
\end{aligned}$$

ist ein Isomorphismus.

Beweis. Da wir schon wissen, dass die Abbildung injektiv ist und $\mathbb{Q}(\zeta_p)|\mathbb{Q}$ der Zerfällungskörper des separablen Polynoms x^N-1 ist, genügt es zu zeigen, dass $[\mathbb{Q}(\zeta_N):\mathbb{Q}]=\#(\mathbb{Z}/N\mathbb{Z}^*)=:\varphi(N)$, d.h. wir müssen Zeigen, dass das Minimalpolynom von ζ_N den Grad $\varphi(N)$ hat.

Wenn das so sein sollte, dann kennen wir das Polynom auch schon, denn die Nullstellen sind dann genau ζ_N^k für $k\in(\mathbb{Z}/N\mathbb{Z})^*$ – da dann die Körperautomorphismen ζ_N genau auf die Nullstellen des Minimalpolynoms abbilden, d.h. das Minimalpolynom sollte dann das folgende Polynom sein:

$$\begin{aligned}
\Phi_N(x) &:= \prod_{k\in(\mathbb{Z}/N\mathbb{Z})^*}(x-\zeta_N^k)\\
&= \frac{\prod_{k=0}^{N-1}(x-\zeta_N^k)}{\prod^{N-1}_{\substack{k=0\\ k,N \text{ nicht teilerfremd}}}(x-\zeta_N^k)}\\
&= \frac{x^N-1}{\prod d|N\Phi_d(x)}.
\end{aligned}$$

Hier haben wir im letzten Schritt verwendet, dass jede Potenz ζ_N^k die nicht selbst eine primitive N-te Einheitswurzel ist, eine primitive d-te Einheitswurzel für einen Teiler d von N ist.

Wir wissen induktiv dass $\Phi_N(x)\in\mathbb{Z}[x]$ ein ganzzahliges, normiertes Polynom ist, denn das gilt sicher für $\Phi_1(x)=x-1$ und nach Konstruktion sind die $\Phi_d(x)$ für $d|N$ teilerfremde Teiler von X^N-1 in $\mathbb{Q}(\zeta_N)[x]$. Da die Polynome Φ_d aber nach Induktion selbst normiert und ganzzahlig sind, sind die Polynome auch schon Teiler in $\mathbb{Z}[x]$.

Es ist bemerkenswert, dass wir zeigen können, dass $\Phi_N(x)$ ganzzahlig ist, ohne das Pordukt auszurechnen. Wenn Sie $\zeta_N=\cos(\frac{frm-e\pi}{N})+i\sin(\frac{frm-e\pi}{N})$ schreiben und das ausmultiplizieren, bekommen Sie sehr kompliziert aussehende Terme. Algebra sagt uns freundlicherweise ohne Mühe, dass das komplizierte Ausdrücke für ganze Zahlen sind.

Dein einzigen guten Trick, um zu zeigen, dass ein Polynom irreduzibel ist, den wir kennengelernt haben, war das Polynom modulo Primzahlen zu betrachten – das Eisensteinkriterium beruhte zum Beispiel auch auf diesem Trick. Das funktionierte, weil wir nach dem Lemma von Gauß wussten, dass es, wenn es fpr ein normiertes Polynom Teiler in $\mathbb{Q}[x]$ gibt, die Teiler schon in $\mathbb{Z}[x]$ gefunden werden können.

Angenommen $\Phi_N(x) = f(x) \cdot g(x)$ mit $f(x), g(x) \in \mathbb{Z}[x]$. Dann ist ζ_N eine Nullstelle eines der Faktoren, zum Beipiel von $f(x)$. Wir müssen zeigen, dass dann auch alle Potenzen ζ_N^k für zu N teilerfremde k ebenfalls Nullstellen von f sind. Wir können das Problem auf den Fall, dass k eine zu N teilerfremde Primzahl ist zurückführen, in dem wir folgendes zeigen:

Behauptung: Ist ζ_N^a eine Nullstelle von $f(x)$ und p eine zu N teilerfremde Primzahl, so ist auch $(\zeta_N^a)^p = \zeta_N^{ap}$ eine Nullstelle von f.

Wäre das nicht so, so wäre $(\zeta_N^a)^p$ eine Nullstelle von $g(x)$, d.h. $g((\zeta_N^a)^p) = 0$. Das beeutet aber, dass ζ_N^a sowohl eine Nullstelle von $g(x^p)$, als auch von $f(x)$ ist, die beiden Polynome $g(x^p)$ und $f(x)$ also nicht teilerfremd in $\mathbb{Z}[x]$ sind.

Die Restklasse des gemeinsamen Teilers in $\mathbb{Z}[x]$ ist dann ein gemeinsamer Teiler der Restklassen $[g](x^p), [f](x) \in \mathbb{Z}/p\mathbb{Z}[x]$. Aber in $\mathbb{Z}/pZ$ gilt wegen der merkwürdigen binoischen Formel $(x+y)^p = x^p + y^p$ in $\mathbb{Z}/p\mathbb{Z}$ dass

$$[g](x^p) = ([g](x))^p.$$

Wegen der Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}/p\mathbb{Z}[x]$ haben dann aber auch $[g](x), [f](x)$ einen gemeinsamen Teiler. Das kann nicht sein, denn das Polynom $x^N - 1$ ist in $\mathbb{Z}/p\mathbb{Z}[x]$ separabel, da es teilerfremd zu seiner Ableitung Nx^{N-1} ist und $[g](x) \cdot [f](x)$ ist nach Konstruktion ein Teiler von $x^N - 1$.

Also ist $\Phi_N(x)$ irreduzibel. □

Auflösbarkeit von Gleichungen und Gruppen

In diesem Kapitel möchte ich nun erklären, wie die Galoiskorrespondenz uns sagt, für welche Polynome wir eine Lösungsformel für die Nullstellen finden können, die nur (n-)te Wurzeln verwendet.

Wir hatten schon gesehen, dass sich die Voraussetzung im Satz zur Galoiskorrespondenz – $L|K$ ist ein Zerfällungskörper eines separablen Polynoms – verschiedene äquivalente Beschreibungen hat:

Lemma/Definition 69. *Für eine endliche Körpererweiterung $L|K$ sind die folgenden Bedingungen äquivalent:*

1. *L ist der Zerfällungskörper eines separablen Polynoms in $K[x]$.*
2. $\#\operatorname{Aut}(L|K) = [L : K]$
3. $K = L^{\operatorname{Aut}(L/K)}$.

Körpererweiterungen die eine (und daher alle) dieser Bedingungen erfüllen heißen Galoiserweiterungen.

Beweis. Die Äquivalenz der Aussagen 1. und 2. war die Charakterisierung von Zerfällungskörpern (Satz 49), die Äquivalenz von 2. und 3. hatten Sie in einer Übungsaufgabe zusammen gesucht, das folgte daraus, dass Satz 49 für alle Erweiterungen die Ungleichung $\#\operatorname{Aut}(L|K) \leq [L:K]$ zeigte und Artin's Lemma umgekehrt $[L:L^H] \leq \#H$ für jede Untergruppe $H < \operatorname{Aut}(L)$ zeigt. □

Notation 70. Ist $L|K$ eine Galoiserweiterung so schreiben wir

$$\operatorname{Gal}(L|K) := \operatorname{Aut}(L|K)$$

für die Galoisgruppe der Erweiterung.

Ist $K \subseteq K' \subseteq L$ eine Kette von Körpererweiterungen, so dass sowohl $L|K$ als auch $K'|K$ Galoiserweiterungen sind, so ist automatisch auch $L|K'$ eine Galoiserweiterung, da K' nach der Galoiskorrespondenz als $K' = L^H$ für eine Untergruppe $H < \operatorname{Aut}(L|K) < \operatorname{Aut}(L)$ geschrieben werden kann. Das bedeutet insbesondere, dass $H < \operatorname{Aut}(L|K')$ und also $K' = L^H = L^{\operatorname{Aut}(L|K')}$ und wir haben gerade gesehen, dass das schon bedeutet, dass $L|K'$ eine Galoiserweiterung ist.

Dann ist die Abbildung

$$\begin{aligned} |_{K'} \colon \operatorname{Gal}(L|K) &\to \operatorname{Gal}(K'|K) \\ \sigma &\mapsto \sigma|_{K'} \colon K' \to K' \end{aligned}$$

wohldefiniert, denn K' ist ein Zerfällungskörper, also von den Nullstellen eines Polynoms $f(x) \in K[x]$ in L erzeugt. Da jeder Körperhomomorphismus $\sigma \in \operatorname{Gal}(L|K)$ Nullstellen von f auf Nullstellen von f abbildet, ist für alle $b \in K'$ auch $\sigma(b) \in K'$, also $\sigma|_{K'} \in \operatorname{Gal}(K'|K)$.

Der Kern dieser Abbildung ist

$$\begin{aligned} \ker(\ \ |_{K'}) &= \{\sigma \in \operatorname{Gal}(L|K) \mid \sigma|_{K'} = \mathrm{id}_{K'}\} \\ &= \operatorname{Aut}(L|K') = \operatorname{Gal}(L|K'). \end{aligned}$$

Insbesondere ist also $\operatorname{Gal}(L|K') \lhd \operatorname{Gal}(L|K)$ als Kern eines Gruppenhomomorphismus ein Normalteiler und die Abbildung $|_{K'}$ induziert einen injektiven Homomorphismus

$$\begin{aligned} Q \colon \operatorname{Gal}(L|K)/\operatorname{Gal}(L|K') &\to \operatorname{Gal}(K'|K) \\ [\sigma] &\mapsto \sigma|_{K'} \colon K' \to K'. \end{aligned}$$

Nach der Galoiskorrepondenz (Satz 52) gilt aber

$$\#\operatorname{Gal}(K'|K) = [K':K] = \frac{\#\operatorname{Gal}(L|K)}{\#\operatorname{Gal}(L|K')} = \#(\operatorname{Gal}(L|K)/\operatorname{Gal}(L|K')).$$

Daher ist Q ein Isomorphismus.

Für den Zwischenkörper $K \subset K' \subset L$ ist $K'|K$ also genau dann eine Galoiserweiterung, wenn $\operatorname{Gal}(L|K') \lhd \operatorname{Gal}(L|K)$ ein Normalteiler ist. Wir haben also gezeigt:

Satz 71 (Galoiskorrespondenz - Version 2)**.** *Ist $K \subseteq L$ eine Galoiserweiterung, so sind die Abbildungen*

$$\left\{K' \mid \begin{array}{c} K \subseteq K' \subseteq L \\ \textit{Zwischenkörper} \end{array}\right\} \underset{\longleftarrow}{\longrightarrow} \{H \subseteq \mathrm{Aut}(L|K) \mid H \textit{ Untergruppe}\}$$
$$K' \mapsto \mathrm{Aut}(L|K')$$
$$L^H \hookleftarrow H$$

zueinander inverse Bijektionen und es gilt:

1. $[L^H : K] = \frac{\#\mathrm{Aut}(L|K)}{\#H}$ *und* $[L : L^H] = \#H$.
2. *Die Erweiterung $L^H|K$ ist genau dann eine Galoiserweiterung wenn $H \lhd \mathrm{Aut}(L|K)$ ein Normalteiler ist.*

In den Beispielen zur Galoiskorrespondenz haben wir außerdem gesehen, dass die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta_N)|\mathbb{Q})$ abelsch (=kommutativ) ist und außerdem falls ein Körper K eine primitive N-te Einheitswurzel $\zeta_N \in K$ enthält für alle $a \in K$ die Erweiterung $K(\sqrt[N]{a})|K$ eine Galoiserweiterung mit abelscher Galoisgruppe. Solche Erweiterungen bekommen zur Abkürzung einen Namen.

Definition 72. Eine *abelsche Körpererweiterung*, ist eine Galoiserweiterung $L|K$ für die $\mathrm{Gal}(L|K)$ eine abelsche Gruppe ist.

Wenn wir also eine Lösungsformel für die Nullstellen eines Polynoms $f \in K[x]$ finden können, die nur die Symbole $+, -, \cdot, :$, $\sqrt[N]{}$ verwendet, so ist der Zerfällungskörper von f in einem Körperturm

$$K = K_0 \subseteq K_1 = K_0(\zeta_N) \subseteq K_2 = K_1(\sqrt[N]{a_1}) \subseteq \cdots \subseteq L = K_r = K_{r-1}(\sqrt[N]{a_{r-1}})$$

enthalten, in dem alle Erweiterungen $K_i|K_{i-1}$ abelsche Erweiterungen sind.

Definition 73. Eine Körpererweiterung $K'|K$ heißt *auflösbar* wenn es einen Erweiterungskörper $L|K$ gibt, der K' enthält und zudem als Kette von abelschen Erweiterungen der Form

Meistens heißen diese Erweiterungen durch Radikale auflösbar

$$K = K_0 \subseteq K_1 = K_0(\zeta_N) \subseteq K_2 = K_1(\sqrt[N]{a_1}) \subseteq \cdots \subseteq L = K_r = K_{r-1}(\sqrt[N]{a_{r-1}})$$

geschrieben werden kann.

In Termen der Galoiskorrespondenz übersetzt sich dieser Begriff als Eigenschaft der Galoisgruppe $\mathrm{Gal}(L|K)$:

Definition. Eine Gruppe $(G, \cdot)$ heißt *auflösbar* wenn G eine Kette von Normalteilern

$$\{e\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_r = G$$

besitzt so dass für alle $i = 1, \ldots r$ die Gruppen G_i/G_{i-1} abelsche Gruppen sind.

Um zu zeigen, dass es für die Nullstellen der allgemeine Gleichung n-ten Grades für $n \geq 5$ keine Formel in Termen von Grundrechenarten und Wurzelziehen gibt, werden wir uns überlegen, dass die symmetrische Gruppe S_n für $n \geq 5$ keine auflösbare Gruppe ist. Als Nebenprodukt wird das für $n = 4$ noch erklären, wie wir für die Gleichung 4-ten Grades eine Formel für die Nullstellen finden können. Zunächst sollten wir uns Beispiele für Gruppen, die diese Eigenschaft erfüllen suchen.

Beispiel 74. 1. Jede abelsche Gruppe A ist auflösbar. Formal ist die Kette $\{e\} \lhd A$ schon eine Kette in der $A/\{e\} \cong A$ eine abelsche Gruppe ist.

2. Für die symmetrische Gruppe S_3 hatten wir bei der Suche nach einer Lösungsformel der Gleichung 3. Grades die Untergruppe

$$\{e\} \lhd A_3 \lhd S_3$$

gefunden, wobei

$$\begin{aligned} A_3 &:= \ker(\operatorname{sign}\colon S_3 \to (\{\pm 1\}, \cdot)) \\ &= \{\sigma \in S_3 \mid \operatorname{sign}(\sigma) = 1\} \\ &= \{\mathrm{id}, (123), (132) = (123)^2\} \cong (\mathbb{Z}/3\mathbb{Z}, +) \end{aligned}$$

eine zyklische Gruppe und insbesondere abelsch ist und sign einen Isomorphismus

$$S_3/A_3 \cong (\{\pm 1\}, \cdot)$$

induziert. Also ist S_3 auflösbar.

3. Auf dem Übungsblatt hatten Sie schon für jeden Körper K die Gruppe der oberen Dreicksmatrizen

$$B_2 := \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in K, ad \neq 0\} < \mathrm{GL}_2(K)$$

angeschaut und die Untergruppe

$$U_2 := \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in K\} \lhd B_2$$

als Normalteiler kennengelernt. Die Abbildung

$$\begin{aligned} G\colon B_2 \to T_2 &:= \{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in K, ad \neq 0\} \\ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} &\mapsto \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \end{aligned}$$

war nämlich wegen

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \circ \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} aa' & ?? \\ 0 & dd' \end{pmatrix}$$

ein surjektiver Gruppenhomomorphismus mit $\ker(G) = U_2$. Die Gruppe T_2 ist abelsch, denn $T_2 \cong K* \times K^*$ und $U_2 \cong (K,+)$ da

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+b' \\ 0 & 1 \end{pmatrix}.$$

4. Ähnlich ist für

$$B_3 := \{ \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \mid a, \ldots, f \in K, adf \neq 0 \} < \mathrm{GL}_3(K)$$

die Gruppe

$$U_3 := \{ \begin{pmatrix} 1 & b & c \\ 0 & 1 & e \\ 0 & 0 & 1 \end{pmatrix} \} \lhd B_3$$

ein Normalteiler, weil U_3 wieder der Kern des Homomorphismus

$$G \colon B_3 \to T_3 := \{ \begin{pmatrix} a & 0 & 0 \\ 0 & d & 0 \\ 0 & 0 & f \end{pmatrix} \mid a, d, f \in K, adf \neq 0 \}$$

$$\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \mapsto \{ \begin{pmatrix} a & 0 & 0 \\ 0 & d & 0 \\ 0 & 0 & f \end{pmatrix}$$

ist. Die Gruppe U_3 ist selbst nicht abelsch, denn

$$\begin{pmatrix} 1 & b & c \\ 0 & 1 & e \\ 0 & 0 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & b' & c' \\ 0 & 1 & e' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+b' & c+c'+be' \\ 0 & 1 & e+e' \\ 0 & 0 & 1 \end{pmatrix}$$

und der blau markierte Term ist nicht symmetrisch in den Termen mit und ohne $'$.

Dafür sehen wir an der Formel (oder auch an der Regel für die Multiplikation von Blockmatrizen) dass die Abbildung

$$Q_2 \colon U_3 \to U_2$$
$$\begin{pmatrix} 1 & b & c \\ 0 & 1 & e \\ 0 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

ein surjektiver Gruppenhomomorphismus ist, also ist

$$\ker(Q_2) = \left\{ \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & e \\ 0 & 0 & 1 \end{pmatrix} \mid c, e \in K \right\} \lhd U_3$$

ein Normalteiler mit

$$U_3 / \ker(Q_2) \cong U_2$$

abelsch und $\ker(Q_2) \cong (K^2, +)$ ist selbst wieder abelsch. Also ist B_3 auflösbar.

Das Argument lässt sich für alle n induktiv auf die Gruppe der oberen Dreiecksmatrizen in $\mathrm{GL}_n(K)$ übertragen, indem Sie in U_n die Gruppen U_m mit $m < n$ als Quotienten auffassen.

Sich auflösbare Gruppen als Untergruppen der oberen Dreiecksmatrizen vorzustellen, ist eine gute Idee, mit etwas Glück begegnet Ihnen dazu noch einmal ein Resultat das das erklärt.

Auf dem Übungsblatt haben Sie ein weiteres Beispiel dafür, wie solche Gruppen als Galoisgruppen vorkommen.

In der Vorlesung haben Sie sich nun noch das Beispiel S_4 gewünscht:

Beispiel 75. Die Gruppe S_4 hat wie alle symmetrischen Gruppen den Normalteiler

$$A_4 := \mathrm{Ker}(\mathrm{sign}) = \{\sigma \in S_n \mid \mathrm{sign}(\sigma) = 1\} \lhd S_4.$$

Die $\frac{\#S_4}{\#\{\pm 1\}} = \frac{4!}{2} = 12$ Elemente von A_4 sind

1. das neutrale Element $e = \mathrm{id}$,
2. die Dreizyklen $(123), (124), (132), (134), (142), (143), (234), (243)$
3. die Doppeltranspositionsn $(12)(34), (13)(24), (14)(23)$.

Das sind 12 Elemente, also alle. Die Normalteilerbedingung

$$\sigma H \sigma^{-1} = H \text{ für alle } \sigma \in S_n$$

bedeutet,dass ein Normalteiler mit einem Element $\tau \in H$ auch alle konjugierten $\sigma\tau\sigma^{-1}$ in H liegen, was genau die Elemente sind bei denen in der Zykelschreibweise die Zahlen vertauscht wurden, d.h. ein Normalteiler, der einen Dreizyklus enthält muss also alle enthalten, damit auch das Produkt

$$(123) \circ (124) = (13)(24)$$

und damit auch alle Doppeltranspositionen. Also ist der einzig mögliche Normalteiler:

$$V_4 := \{e, (12)(34), (13)(24), (14)(23)\}.$$

Diese Teilmenge erfüllt die Normalisatorbedingung, da sie alle Elemente mit gegebener Zykelschreibweise enthält und ist tatsächlich eine abelsche Untergruppe da

$$(12)(34) \circ (13)(24) = (14)(23) = (13)(24) \circ (12)(34)$$

gilt. Damit ist

$$\begin{aligned} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} &\to V_4 \\ (a, b) &\mapsto ((12)(34))^a \circ ((13)(24))^b \end{aligned}$$

ein bijektiver Gruppenhomomorphismus. Also ist

$$\{e\} \lhd V_4 \lhd A_4 \lhd S_4$$

eine Kette von Normalteilern, in der V_4 abelsch ist, $\#A_4/V_4 = 12/4 = 3$ also ist $A_4/V_4 \cong \mathbb{Z}/3\mathbb{Z}$ zyklisch und $S_4/A_4 \cong \{\pm 1\}$ ist ebenfalls abelsch.

Damit ist S_4 auflösbar.

Um den Begriff noch formal etwas zu üben möchte ich kurz Eigenschaften des Begriffs erklären.

Lemma 76 (Untergruppen auflösbarer Gruppen sind auflösbar)**.** *Ist G eine auflösbare Gruppe und $H < G$ eine Untergruppe, so ist H auflösbar.*

Beweis. Nach Voraussetzung ist G auflösbar. Es gibt also eine Kette von Normalteilern

$$\{e\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_r = G$$

so dass die Quotienten G_i/G_{i-1} abelsch sind.

Es ist zu zeigen, dass auch H eine solche Kette enthält. Die einzige Möglichkeit aus den G_i Untergruppen von H zu machen ist vielleicht die Schnitte

$$H_i := H \cap G_i < H$$

zu betrachten. Dann erhalten wir eine Kette von Untergruppen

$$\{e\} = H_0 < H_1 = G_1 \cap H < H_2 = G_2 \cap H < \cdots < H_r = H = H \cap G.$$

Auf dem Übungsblatt hatten Sie sich auch überlegt, dass für einen Normalteiler $N \lhd G$ für jede Untergruppe $H < G$ der Schnitt $H \cap N \lhd H$ wieder ein Normalteiler ist.[13] Also haben wir sogar eine Kette von Normalteilern

$$\{e\} = H_0 \lhd H_1 = G_1 \cap H \lhd H_2 = G_2 \cap H \lhd \cdots \lhd H_r = H = H \cap G.$$

gefunden.

Für jedes $i = 1, \dots r$ ist die Abbildung

$$\begin{aligned} F\colon H_i/H_{i-1} = H \cap G_i / H \cap G_{i-1} &\to G_i/G_{i-1} \\ [h] &\mapsto [h] \end{aligned}$$

ein Gruppenhomomorphismus, der injektiv ist, da $F([h]) = e$ bedeutet, dass $h \in G_{i-1}$, für $h \in H \cap G_i$ bedeutet das aber gerade $h \in H \cap G_{i-1}$, also $[h] = [e] \in H \cap G_i / H \cap G_{i-1}$.

Da G_i/G_{i-1} nach Voraussetzung abelsch ist, ist also auch H_i/H_{i-1} abelsch. □

Bemerkung. Auf dem Übungsblatt zeigen Sie analog, dass für jeden surjektiven Homomorphismus $F\colon G \twoheadrightarrow Q$ ebenso folgt, dass wenn G auflösbar ist auch Q auflösbar ist. Dafür betrachten Sie dann entsprechend die Bilder $F(G_i)$ und überlegen sich, dass diese die gewünschte Kette von Normalteilern in Q liefern.

Wie findet sich ein Normalteiler $N \lhd G$, für den G/N abelsch ist? Wenn es so einen gibt, ist die Quotientenabbildung

$$F\colon G \to G/N =: A$$

[13] Das war nicht scher, denn es ist nur zu zeigen, dass für alle $h \in H$ gilt, dass

$$h(N \cap H)h^{-1} = N \cap H.$$

Da N ein Normalteiler ist, ist $hNh^{-1} = N$, also liegt die linke Seite sicher in N und da $h \in H$ ist, liegt $h(N \cap H)h^{-1}$ sicher in H, also auch in $H \cap N$.

ein Homomorphismus in eine kommutative Gruppe, d.h. es gilt dann für $g, h \in G$:

$$\begin{aligned} F(g \cdot h) &= F(g) \cdot F(h) && F \text{ Homomorphismus} \\ &= F(h) \cdot F(g) && A \text{ kommutativ} \\ &= F(h \cdot g) && F \text{ Homomorphismus.} \end{aligned}$$

Das bedeutet aber, dass $F((gh) \cdot (hg)^{-1}) = F(ghg^{-1}h^{-1}) = e$, d.h. $ghg^{-1}h^{-1} \in \ker(F) = N$.

Notation 77. Für Elemente g, h einer Gruppe G bezeichnen wir mit

$$[g, h] := ghg^{-1}h^{-1}$$

den *Kommutator* von g und h.

Die Untergruppe von G, die von den Kommutatoren, also von allen Elementen der Form $[g, h]$ erzeugt wird heißt *Kommutatoruntergruppe* von G und wird als

$$[G, G] < G$$

notiert.

Bemerkung. 1. Der Kommutator $[g, h] = ghg^{-1}h^{-1}$ ist genau dann das neutrale Element e, wenn $g \cdot h = h \cdot g$ gilt, denn

$$g \cdot h = h \cdot g \Leftrightarrow ghg^{-1}h^{-1} = e.$$

Das erklärt den Namen „Kommutator“.

2. Die Gruppe $[G, G] \lhd G$ ist tatsächlich immer ein Normalteiler.

Der erste Reflex ist vielleicht, das mit der Definition direkt nachzurechnen: Die Elemente von $[G, G]$ sind nach Definition Produkte von Elementen der Form $[g_1, g_2]$. Ist nun $[g_1, g_2] \in [G, G]$ und $g \in G$, so ist

$$\begin{aligned} g \cdot [g_1, g_2] \cdot g^{-1} &= g \cdot g_1 \cdot g_2 \cdot g_1^{-1} \cdot g_2^{-1} \cdot g^{-1} \\ &= gg_1g^{-1}gg_2g^{-1}gg_1^{-1}g^{-1}gg_2^{-1}g^{-1} \\ &= (gg_1g^{-1}) \cdot (gg_2g^{-1}) \cdot (gg_1^{-1}g^{-1}) \cdot (gg_2^{-1}g^{-1}) \\ &= [gg_1g^{-1}, ghg^{-1}] \in [G, G]. \end{aligned}$$

Also gilt für alle $g \in G$, dass $g[G, G]g^{-1} = [G, G]$.

Das Argument ist ein gutes Beispiel dafür, dass es sich oftmals lohnt, noch einmal darüber nachzudenken, was wir gerade gerechnet haben.

Fällt Ihnen eine allgemeinere Aussage ein, die leichter zu beweisen ist? Was ist das Besondere an der Abbildung $h \mapsto g \cdot h \cdot g^{-1}$?

Folgerung 78. *1. Ist $N \lhd G$ ein Normalteiler mit abelscher Quotientengruppe G/N, so enthält N die Kommutatoruntergruppe, d.h.*

$$G/N \text{ abelsch } \Rightarrow [G, G] < N.$$

2. *Ist G eine Gruppe für die $[G,G] = G$ gilt, so ist G nicht auflösbar.*

Beweis. Den ersten Teil der Folgerung haben wir schon nachgerechnet, als wir uns überlegt haben, dass $[G,G] \subseteq \ker(G \to G/N) = N$ gilt.

Der 2. Teil folgt daraus, da wegen 1. folgt, dass G dann keine Normalteiler $N \subsetneq G$ enthalten kann für die G/N abelsch ist. □

Beispiel: Kommutatoruntergruppe der symmetrischen Gruppe

Für die symmetrische Gruppe können wir den Kommutator bestimmen.

Satz 79. *1. Die Kommutatoruntergruppe der symmetrischen Gruppe ist die alternierende Gruppe, d.h. für alle $n \in \mathbb{N}$ gilt*

$$[S_n, S_n] = A_n.$$

Erinnerung:

$$A_n = \{\sigma \in S_n \mid \operatorname{sign}(\sigma) = 1\} = \ker(\operatorname{sign})$$

2. *Ist $n \geq 5$ so gilt*

$$[A_n, A_n] = A_n.$$

Insbesondere sind die Gruppen S_n und A_n für $n \geq 5$ nicht auflösbar.

Vorüberlegung: Um einen Überblick über die Kommutatoren in S_n zu bekommen, brauchen wir einen Überblick über die Elemente von S_n. Aus der linearen Algebra wissen wir noch, das die einfachsten Permutationen die Transpositionen (ij), also die Vertauschungen von 2 Elementen sind. Formal also die Abbildungen $\tau_{ij} \colon \{1,\dots,n\} \to \{1,\dots,n\}$ die durch

$$\begin{aligned} \tau_{ij}(i) &= j \\ \tau_{ij}(j) &= i \\ \tau_{ij}(k) &= k \qquad\qquad \text{für } k \notin \{i,j\}. \end{aligned}$$

Sie wissen auch, dass wir alle Permutationen als Verkettung von Transpositionen schreiben können – durch mehrfaches Vertauschen können Sie jede Unordnung aufräumen, bzw. herstellen. Lassen Sie mich kurz an das formale Argument dazu erinnern:

Lemma 80. *Die Gruppe S_n ist von den Transpositionen erzeugt, d.h. jede Permutation $\sigma \in S_n$ lässt sich als Produkt von Transpositionen schreiben.*

Beweis. Wir zeigen die Aussage mit Hilfe von Induktion über die Größe der Unordnung: Für $\sigma \in S_n$ sei

$$F_\sigma := \#\{i \in \{1,\dots,n\} \mid \sigma(i) = i\}$$

die Anzahl der Fixpunkte der Abbildung σ.

Ist $F_\sigma = n$, so ist $\sigma = \mathrm{id}$ und also das Produkt von 0 Transpositionen.

Ist $F_\sigma = m < n$, so existiert ein $i \in \{1,\dots,n\}$ mit $\sigma(i) = j \neq i$. Dann ist $\sigma^{-1}(i) \neq \sigma^{-1}(j) = i$ also ist $\sigma^{-1}(i)$ ebenfalls kein Fixpunkt von σ.

Dann gilt für

$$\widetilde{\sigma} := (ij) \circ \sigma$$

dass

$$\begin{aligned} (ij) \circ \sigma(i) &= i \\ (ij) \circ \sigma(k) &= \sigma(k) \qquad \text{für alle } k \notin i, \sigma^{-1}(i). \end{aligned}$$

Also besitzt $\widetilde{\sigma}$ wenigstens $m+1$ Fixpunkte, lässt sich also nach Induktion als Produkt von Transpositionen schreiben. Also lässt sich auch $\sigma = (ij) \circ (ij) \circ \sigma = (ij) \circ \widetilde{\sigma}$ als Produkt von Transpositionen schreiben. □

Beweis von Satz 79. 1. Zunächst gilt $[S_n, S_n] \subseteq A_n$, denn für $[\sigma, \tau]$ gilt $[\sigma, \tau] \in \ker(\text{sign}\colon S_n \to (\{\pm 1\}, \cdot))$.

Ist umgekehrt $\sigma \in A_n$ so lässt sich σ als Produkt von Transpositionen

$$\sigma = (i_1 j_1) \circ (i_2 j_2) \circ \cdots \circ (i_m j_m)$$

schreiben und wegen der der Multiplikativität von sign und $\text{sign}((ij)) = -1$ ist die Anzahl m der Permutationen gerade. Es genügt also zu zeigen, dass sich alle Produkte von zwei Transpositionen $(i_1 j_1) \circ (i_2 j_2)$ als Produkt von Kommutatoren schreiben lassen.

(a) Ist $\{i_1, j_1\} = \{i_2, j_2\}$ so ist das Produkt die Identität und es ist nichts zu zeigen.

(b) Haben die Mengen $\{i_1, j_1\}, \{i_2, j_2\}$ ein gemeinsames Element, so genügt es nach umnummerieren das Beispiel $(12) \circ (23)$ zu betrachten. Hierfür gilt

$$(12) \circ (23) = (123)$$

Also

$$[(12), (23)] = (123)^2 = (132).$$

Damit ist $[(13), (23)] = (123)$.

(c) Sind die Mengen $\{i_1, j_1\}, \{i_2, j_2\}$ disjunkt, so genügt es nach umnummerieren das Beispiel $(12) \circ (34)$ zu betrachten. Es gilt

$$(123) \circ (234) = (12)(34)$$

und nach der vorigen Berechnung lassen Sich (123) und (234) als Produkt von Kommutatoren schreiben.

Insbesondere haben wir hiermit gezeigt, dass sich alle Elemente von A_n als Produkt von Dreizyklen (ijk) schreiben lässt, weil das für die Kompositionen von 2 Transpositionen gilt.

2. Nach dem vorigen Teil genügt es zu zeigen, dass sich für $n \geq 5$ alle Dreizyklen als Kommutator von Elementen in A_n schreiben lassen. Wir wissen schon, dass $[(13), (23)] = (123)$ gilt, also gilt auch

$$[(13)(45), (23)(45)] = (123)$$

und Produkte von 2 Transpositionen sind Elemente von A_n.

□

Lassen Sie uns die Beobachtung zu den Erzeugenden von der alternierenden Gruppe aus dem Beweis noch einmal festhalten.

Folgerung 81. *Die alternierende Gruppe A_n ist von Dreizyklen, also Elementen der Form (i,j,k) mit $i,j,k \in \{1,\dots,n\}$ erzeugt.*

Bemerkung. Wir haben auch schon gesehen, dass $[A_4, A_4] = V_4 \lhd A_4$ und $[A_3, A_3] = \{e\}$ weil $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ abelsch ist.

Die alternierende Gruppe A_n ist für $n \geq 5$ eine einfache Gruppe

Mit den Berechnungen von Kommutatoren in S_n können wir jetzt auch die stärkere Aussage, dass A_n für $n \geq 5$ einfach ist, beweisen.

Satz 82. *Die alternierende Gruppe A_n ist für $n \geq 5$ eine einfache Gruppe.*

Beweis. Sei $N \lhd A_n$ ein Normalteiler mit $N \neq \{e\}$, d.h. N ist eine nicht triviale Untergruppe so dass für alle $\sigma \in A_n$

$$\sigma N \sigma^{-1} = N.$$

Wir wollen zeigen, dass dann $N = A_n$ gilt.

Schritt 1: Es genügt zu zeigen, dass N einen Dreizyklus (ijk) enthält.

Das gilt, da die Dreizyklus in A_n für $n \geq 5$ alle konjugiert sind, d.h. alle sind von der Form $\sigma(123)\sigma^{-1}$ für ein $\sigma \in A_n$. Das gilt, da die Aussage in S_n gilt und falls $\operatorname{sign}(\sigma) = -1$ ist, so gilt

$$\begin{aligned}\sigma \circ (123) \circ \sigma^{-1} &= \sigma \circ \big((45) \circ (123) \circ (45)\big) \circ \sigma^{-1} \\ &= (\sigma \circ (45)) \circ (123) (\sigma \circ (45))^{-1}.\end{aligned}$$

Enthält N also einen Dreizyklus, so enthält N wegen $\sigma N \sigma^{-1} = N$ alle Dreizyklus und A_n ist von Dreizyklen erzeugt. Das zeigt die Behauptung.

Schritt 2: N enthält ein Element, dessen Ordnung eine Primzahl ist.

Sei $\sigma \in N$ mit $\sigma \neq 1$, also $\operatorname{Ordnung}(\sigma) = m > 1$. Ist $m = d \cdot p$ für eine Primzahl p, hat σ^d die Ordnung p. Also enthält N ein Element σ, dessen Ordnung eine Primzahl p ist.

Dann hat enthält die Zyklenschreibweise von σ nur Zyklen der Länge p, da Zyklen der Länge k die Ordnung k haben.

Schritt 3: Wenn N ein Element der Ordnung $p > 3$ enthält, so auch einen Dreizyklus.

Für einen Zyklus der Länge $k > 3$ können wir den folgenden Kommutator berechnen:

$$(k \dots 21) \circ (321) \circ (12 \dots k) \circ (123) = (1)(23k)(4)(5) \dots (k-1).$$

Haben wir also eine Element

$$\sigma = (i_1 i_2 \dots i_k)\text{evtl weitere Zyklen} \in N,$$

so sind σ^{-1} und $(i_1 i_2 i_3)^{-1} \circ \sigma \circ (i_1 i_2 i_3)$ Elemente von N und darum auch

$$\sigma^{-1} \circ (i_3 i_2 i_1) \circ \sigma \circ (i_1 i_2 i_3) = (i_1)(i_2 i_3 i_k)(i_4) \dots (i_{k-1})\text{evtl weitere Zyklen}.$$

In der Vorlesung hatten Sie gefragt, woher die Idee kommt für ein gegebenes Element $\sigma \in N$ Elemente der Form $\sigma^{-1} z^{-1} \sigma z$ anuschauen.

Zunächst haben wir nur ein Element $\sigma \in N$ und damit auch die Potenzen σ^a zur Verfügung. Das hilft uns nicht weiter, um die Zyklenschreibweise zu vereinfachen.

Da N ein Normalteiler ist, können wir σ auch konjugiern, also $z\sigma z^{-1}$ anschauen. Das ändert aber nur die Nummerierung der Zyklen, nicht die Länge.

Als nächstes würde ich dann Produkte von σ^a und den konjugierten Elementen $z\sigma z^{-1}$ anschauen.

Enthält also σ nur Zyklen der Länge $p > 3$, so haben wir nun ein Element mit einem Zyklus der Länge 3 und eventuell weiteren Zyklen der Länge $p > 3$, die p-te Potenz dieses Elements ist dann ein Dreizyklus und wir sind fertig.

Schritt 4: Falls N ein Element σ der Ordnung 3 enthält, so ist σ entweder selbst ein Dreizyklus, oder σ ist von der Form

$$(i_1 i_2 i_3)(j_1 j_2 j_3)\cdots .$$

Dann können wir den Kommutator

$$\begin{aligned}&((123)(456))^{-1} \circ (234)^{-1} \circ ((123)(456)) \circ (234)\\ &= (16234)(5)\end{aligned}$$

verwenden, um wie zuvor zu zeigen, dass

$$\sigma^{-1}(i_2 i_3 i_4)^{-1}\sigma(i_2 i_3 i_4) \in N$$

ein Element ist, von dem die 3.te Potenz Ordnung 5 besitzt. Dann enthält N nach Schritt 3 einen Dreizyklus.

Schritt 4: Wenn N ein Element σ der Ordnung 2 enthält, dann ist

$$\sigma = (i_1 j_1)(i_2 j_2)\dots$$

ein Element mit einer geraden Anzahl von Zweizyklen. Hierfür hilft uns dann

$$(12)(34) \circ (345)^{-1} \circ (12)(34) \circ (234) = (1)(2)(354)$$

um ein Element der Ordnung 3 zu finden.

Also enthält N einen Dreizyklus. □

Bemerkung. Der Trick, mit Hilfe von Kommutatoren Permutationen zu vereinfachen ist Ihnen, wenn Sie schon einmal mit einem Zauberwürfel gespielt haben, schon begegnet. Die typischen Zugfolgen, um Kanten oder Ecken zu vertauschen bestehen aus Kommutatoren.

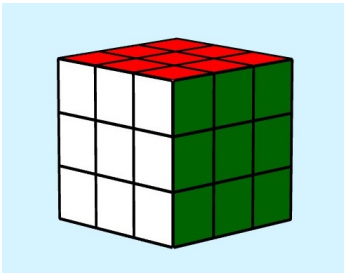


Abbildung 2: Geogebra kennt eine digitale Version des Würfels. Sage kann Ihnen (optimale) Lösungen für einen verdrehten Würfel berechnen.

In der Vorlesung haben wir uns dieser Stelle noch überlegt, warum die Symmetriegruppe des Dodekaeders isomorph zur einfachen Gruppe A_5 ist. Das Geogebra-Applet dazu finden Sie auf der Moodleseite des Kurses.

Wiederholung und Nachträge

Sie hatten an dieser Stelle noch einmal um Beispiele von Zerfällungskörpern und dem Zerfällungskörperwunder gebeten. In der Vorlesung haben wir darum wieder ein Begriffs-Stadt-Land-Fluss ausgefüllt:

Begriff	Definition	Beispiele	Resultate/Anwendungen
Zerfällungskörper			

Beispiel 83.

1. $\mathbb{C} = \mathbb{R}(i)$ ist ein Zerfällungskörper von $x^2 + 1 \in \mathbb{R}[x]$.
2. $\mathbb{Q}(i)$ ist ein Zerfällungskörper von $x^2 + 1 \in \mathbb{Q}[x]$.
3. $\mathbb{Q}(\sqrt{2})$ ist ein Zerfällungskörper von $x^2 - 2 \in \mathbb{Q}[x]$.
4. Für quadratische Erweiterungen entstehen Zerfällungskörper durch hinzufügen einer Nullstelle.
5. $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ ist ein Zerfällungskörper von $x^3 - 2 \in \mathbb{Q}[x]$.

   Hingegen ist $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ *kein* Zerfällungskörper, weil $x^3 - 2$ in dieser Erweiterung nur eine Nullstelle besitzt.
6. $\mathbb{Q}(\sqrt[n]{a}, \zeta_n)$ ist ein Zerfällungskörper von $x^n - a \in \mathbb{Q}[x]$.
7. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ist ein Zerfällungskörper von $(x^2 - 2)(x^2 - 3) = x^4 - 5x^2 + 5\mathbb{Q}[x]$. Das Minimalpolynom von $\sqrt{2} + \sqrt{3}$ über $\mathbb{Q}$ ist

   $$(x - (\sqrt{2} + \sqrt{3}))(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3}) \in \mathbb{Q}[x].$$

   Davon sagt uns die Galoiskorrespondenz, dass die Koeffizienten in $\mathbb{Q}$ liegen, da diese unter $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ invariant sind.

Bemerkung. Ist $L|K$ eine endliche Galoiserweiterung mit Galoisgruppe $G = \mathrm{Gal}(L|K)$ und $\alpha \in L$, so ist

$$p(x) = \prod_{\sigma \in \mathrm{Gal}(L|K)} (x - \sigma(\alpha)) \in K[x]$$

und wenn die Elemente $\{\sigma(\alpha)\}_{\sigma \in \mathrm{Gal}(L|K)}$ paarweise verschieden sind, so ist dieses Polynom das Minimalpolynom von α.

Beweis. Da für alle $\tau \in \mathrm{Gal}(L|K)$ gilt

$$\begin{aligned}
\tau(p(x)) &= \tau\left(\prod_{\sigma \in \mathrm{Gal}(L|K)} (x - \sigma(\alpha))\right) \\
&= \prod_{\sigma \in \mathrm{Gal}(L|K)} (x - \tau\sigma(\alpha)) && \tau \text{ Körperhomomorphismus} \\
&= \prod_{\sigma' \in \mathrm{Gal}(L|K)} (x - \sigma'(\alpha)) && \sigma' = \tau\sigma \Leftrightarrow \sigma = \tau^{-1}\sigma' \\
&= p(x)
\end{aligned}$$

sind die Koeffizienten von $p(x)$ in $L^{\mathrm{Gal}(L|K)}$ und nach der Galoiskorrespondenz ist $L^{\mathrm{Gal}(L|K)} = K$.

Die Elemente $\sigma(\alpha)$ sind alle auch Nullstellen des Minimalpolynoms von x, da das Minimalpolynom in $K[x]$ liegt und damit ebenfalls invariant unter $\mathrm{Gal}(L|K)$ ist. Wenn die Elemente also paarweise verschieden sind, so ist also $p(x) = \prod_{\sigma \in \mathrm{Gal}(L|K)}(x - \sigma(\alpha))$ ein Teiler des Minimalpolynoms und damit schon gleich dem Minimalpolynom, da $p(x) \in K[x]$ liegt und $p(\alpha) = 0$ erfüllt. □

Das Zerfällungkörperwunder (Satz 45) war die Aussage:

Ist $K \subseteq L$ ein Zerfällungskörper eines Polynoms $g(x) \in K[x]$ und $p(x) \in K[x]$ ein beliebiges irreduzibles Polynom, das in L eine Nullstelle besitzt, dann zerfällt auch p in L vollständig in Linearfaktoren.

Zum Beispiel hatten wir gesehen, dass in $\mathbb{Q}(\sqrt{2},\sqrt{3})$ das in $\mathbb{Q}[x]$ irreduzible Polynom

$$f(x) = x^4 - 10x^2 + 1 \quad = (x - (\sqrt{2}+\sqrt{3}))(x - \sqrt{2}+\sqrt{3})(x+\sqrt{2}-\sqrt{3})(x+\sqrt{2}+\sqrt{3})$$

vollständig in Linearfaktoren zerfällt. Die Galoiskorrespondenz erklärt hier ganz schön, wieso das in diesem Fall stimmt.

Diese Eigenschaft von Zerfällungskörpern hat einen Namen, den ich noch nachtragen muss:

Definition. Eine Körpererweiterung $L|K$ heißt *normal* wenn jedes irreduzible Polynom $p(x) \in K[x]$ das in L eine Nullstelle besitzt, in L vollständig in Linearfaktoren zerfällt.

Bemerkung. Eine endliche Körpererweiterung $L|K$ ist genau dann normal, wenn $L|K$ ein Zerfällungskörper ist.

Beweis. Dass Zerfällungskörper normal sind, ist genau die Aussage des Zerfällungskörperwunders (Satz 45). Ist umgekehrt $L = K(\alpha_1, \dots, \alpha_r)$ eine endliche normale Erweiterung, so ist L der Zerfällungskörper von $f(x) = \prod_{i=1}^{r} \mathrm{minpol}_{\alpha_i}(x)$, denn die Minimalpolynome sind irreduzibel und haben in L eine Nullstelle, zerfallen also weil L normal ist bereits vollständig in Linearfaktoren. □

Beispiel 84. 1. Die unendliche Erweiterung $\mathbb{C}|\mathbb{Q}$ ist normal, da in $\mathbb{C}[x]$ sogar alle Polynome in Linearfaktoren zerfallen.

2. Die unendliche Erweiterung $\mathbb{R}|\mathbb{Q}$ ist nicht normal, da zum Beispiel das irreduzible Polynom $p(x) = x^3 - 2 \in \mathbb{Q}[x]$ in $\mathbb{R}$ nur eine Nullstelle besitzt.

Aufgabe (Knobelaufgabe)**.** Dass die Körpererweiterung $\mathbb{Q} \subset \mathbb{R}$ recht groß aber nicht normal ist hat unangenehme Auswirkungen auf die Körperautomorphismen von $\mathbb{R}$:

Zeigen Sie, dass der einzige Körperautomorphismus $\sigma\colon \mathbb{R} \to \mathbb{R}$ die Identität ist.
Hinweis: Das wäre viel leichter, wenn wir wüssten, dass σ stetig ist. Um zu beweisen, dass das immer der Fall ist könnten Sie zunächst schauen, was Sie über $\sigma(\mathbb{R}_{>0})$ wissen.

Bemerkung: Obwohl es hier nicht nötig ist, möchte ich darauf hinweisen, dass im Gegensatz zu diesem Ergebnis $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$ sehr groß (überabzählbar) ist.

Zur Auflösbarkeit von Gleichungen hatten Sie sich auch noch eine Wiederholung gewünscht.

Definition. Eine Körpererweiterung $L|K$ heißt *durch Radikale auflösbar* wenn es eine Kette von Körpererweiterungen

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n$$

gibt so dass $K_i = K_{i-1}(\sqrt[n_i]{a_i})$ mit $n_i \in \mathbb{N}$ und $a_i \in K_{i-1}$ (dabei lassen wir auch das Hinzufügen von Einheitswurzeln, also $a_i = 1$ zu), so dass $L \subseteq K_n$.

Wenn wir eine Lösungsformel für die Nullstellen eines separablen Polynoms $f(x) \in K[x]$ angeben können, die mit iterierten n-ten Wurzeln auskommt, bedeutet das also, dass der Zerfällungskörper L von f auflösbar ist und umgekehrt lassen sich die Nullstellen genau dann als Formel in $n-$ten Wurzeln ausdrücken, wenn diese in einer auflösbaren Erweiterung liegen.

Für Erweiterungen die durch Wurzelziehen entstehen, haben wir die Galoisgruppe berechnet, indem wir gezeigt haben, dass wenn K eine primitive $n-$te Einheitswurzel enthält, die Galoisgruppe $\mathrm{Gal}(K(\sqrt[n]{a})|K)$ eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z}, +)$ ist (Satz 67). Also sind Galoisgruppen, von Galoiserweiterungen die durch Hinzufügen von Einheitswurzeln und $n-$ten Wurzeln entstehen auflösbar.

Ist $K|L$ ein separabler Zerfällungkörper, der in einer solchen Erweiterung $K|K_n$ enthalten ist, so ist die Galoisgruppe $\mathrm{Gal}(L|K) = \mathrm{Gal}(K_n|K)/\mathrm{Gal}(K_n|L)$ ein Quotient einer auflösbaren Gruppe, also selbst wieder auflösbar.

Darum kann es nur Lösungsformeln für die Nullstellen eines separablen Polynoms $f(x) \in K[x]$ geben, die mit iterierten n-ten Wurzeln auskommen, wenn der Zerfällungskörper L von f durch Radikale auflösbar ist.

Bemerkung. Statt nach einer Lösungsformel für alle Nullstellen eines irreduziblen Polynoms zu fragen, könnten Sie auch nach einer Formel für eine Nullstelle fragen. Diese Frage hat die gleiche Antwort.

Versuchen Sie doch einmal, diese Aussage selbst zu beweisen. Das ist nicht ganz einfach, benötigt aber keine neuen Methoden. Mittlerweile finden Sie die Aussage, dass die beiden Fragen die gleiche Antwort haben, da wir in den Formeln verschiedene $n-$ten Wurzeln algebraisch nicht unterscheiden können und daher eine Lösung für eine Nullstelle immer mehrere Nullstellen liefern muss. Aber das ist natürlich noch kein Beweis.

Gruppenoperationen und erste Resultate zur Struktur endlicher Gruppen

Um zu zählen, wie viele Automorphismen ein Dodekaeder besitzt, also die Anzahl der Elemente der Gruppe

$$\mathrm{Aut}(\text{Dodekaeder}) := \{A \in SO(3) \mid A(\text{Dodekaeder}) = \text{Dodekaeder}\}$$

zu zählen hatten wir wie folgt argumentiert:

1. Der Dodekaeder hat 12 Flächen.
2. Ein Automorphismus kann jede der 12 Flächen nach oben drehen und

3. für jede dieser 12 Flächen gibt es 5 mögliche Ausrichtungen.

Ein Automorphismus ist eindeutig dadurch bestimmt, welche Fläche in welcher Ausrichtung oben liegt, also gibt es $12 \cdot 5 = 60$ Automorphismen.

DAS ARGUMENT war also zu schauen, was die Automorphismen mit den Flächen anstellen. Das ist ein allgemein nützliches Prinzip: Um eine Gruppe zu verstehen, sollten wir versuchen, diese als Symmetrien eines Objektes oder einer Menge zu beschreiben.

In unserem Fall definierte jede Symmetrie $g \in \mathrm{Aut}(\text{Dodekaeder})$ eine Abbildung:

$$g.\colon \{\text{Seitenflächen}\} \to \{\text{Seitenflächen}\}$$

Nummerieren wir die Seitenflächen durch, können wir das als

$$g.\colon \{1,2,3,\dots,12\} \to \{1,2,3,\dots,12\}$$

auffassen. Diese Abbildungen haben die Eigenschaften

1. (Neutrales Element) $e. = \mathrm{id}$, d.h. das neutrale Element definiert die identische Abbildung
2. (Verträglich mit Verknüpfung) Für $g, h \in G$ ist $h. \circ g. = (h \cdot g)$.

Diese Struktur heißt Gruppenoperation, oder Gruppenwirkung:

Definition 85 (Gruppenoperation)**.** Eine *Operation* einer Gruppe G auf einer Menge X ist eine Abbildung

$$\begin{aligned} .\colon G \times X &\to X \\ (g,x) &\mapsto g.x \end{aligned}$$

für die gilt:

1. Für das neutrale Element $e \in G$ gilt
$$e.x = x \text{ für alle } x \in X.$$
2. Für alle $g, h \in G$ gilt:
$$g.(h.x) = (g \cdot h).x \text{ für alle } x \in X.$$

Die zweite Bedingung lese ich als Assoziativgesetz:

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

Zusammen mit der ersten Bedingung ist in diesem Axiom die Aussage versteckt, dass für alle $g \in G$ die Abbildung

$$\begin{aligned} g.\colon X &\to X \\ x &\mapsto g.x \end{aligned}$$

bijektiv ist, da das zu g inverse Element g^{-1} eine inverse Abbildung definiert:

$$\begin{aligned} g^{-1}.(g.x) &= (g^{-1} \cdot g).x && \text{Assoziativität} \\ &= e.x = x && \text{und} \\ g.(g^{-1}.x) &= (g \cdot g^{-1}).x \\ &= e.x = x. \end{aligned}$$

Bemerkung. Eine Operation einer Gruppe G auf einer Menge X anzugeben ist das selbe, wie einen Gruppenhomomorphismus

$$G \to S(X) := \{f \colon X \to X \mid f \text{ bijektiv}\}$$

anzugeben.

Beweis. Ist $. \colon G \times X \to X$ eine Gruppenoperation, so ist für jedes $g \in G$ die Abbildung

$$\begin{aligned} g. \colon X &\to X \\ x &\mapsto g.x \end{aligned}$$

bijektiv, also ist

$$\begin{aligned} G &\to S(X) \\ g &\mapsto g. \colon X \to X \end{aligned}$$

wohldefiniert. Diese Abbildung bildet das neutrale Element e von G auf das neutrale Element id_X von $S(X)$ ab, da $e. = \mathrm{id}_X$ und ist verträglich mit Komposition, da

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

für alle $g, h \in G, x \in X$ gilt, also ist $(g \cdot h). = g. \circ h.$. Darum ist $g \mapsto g.$ ein Gruppenhomomorphismus.

Ist umgekehrt $F \colon G \to S(X)$ ein Gruppenhomomorphismus, so erfüllt die Abbildung

$$\begin{aligned} . \colon G \times X &\to X \\ (g, x) &\mapsto g.x := \underbrace{\underbrace{F(g)}_{\in S(X)}(x)}_{\in X} \end{aligned}$$

die Eigenschaften einer Gruppenoperation, da

$$\begin{aligned} e.x &\overset{Def}{=} F(e)(x) \\ &= \mathrm{id}_X(x) = x && F \text{ Gruppenhomomorphimus.} \end{aligned}$$

und

$$\begin{aligned} g.h.(x) &\overset{Def}{=} F(g)(F(h)(x)) \\ &= (F(g) \circ F(h))(x) && \text{Def } \circ \quad = F(g \cdot h)(x) \quad F \text{ Gruppenhomomorphimus} \\ &= (g \cdot h).(x) && \text{Def } . \end{aligned}$$

Diese beiden Konstruktionen sind nach Definition zueinander invers. □

Beispiel 86.

1. Für die Automorphismengruppe $G = \mathrm{Aut}(\text{Dodekaeder})$ haben wir uns die Operation auf der Menge der Seitenflächen

$$G \times \{\text{Seitenflächen}\} \to \{\text{Seitenflächen}\}$$

angeschaut, die wir nach nummerieren der Seiten als

$$G \times \{1, 2, 3, \ldots, 12\} \to \{1, 2, 3, \ldots, 12\}$$

auffassen können. Das liefert uns einen Homomorphismus $G \to S_{12}$, der sogar injektiv ist, weil nur die Identität alle Seitenflächen fest lässt.

Genauso könnten wir die 20 Ecken nummerieren und einen Homomorphismus $G \to S_{20}$ bekommen, oder wie im Argument, dass $G \cong A_5$ ist die Operation auf den 5 einbeschriebenen Würfeln betrachten.

Der Vorteil der abstrakten Gruppe G gegenüber der Untergruppen von S_n ist, dass wir die Gruppe auf verschiedene Weisen operieren lassen können, die Einbettung in S_5 ist die kleinste Möglichkeit, auf die wir zunächst sicher nicht gekommen wären.

2. In der linearen Algebra hatten wir die Gruppe $\mathrm{GL}_n(K)$ der invertierbaren $n \times n$ Matrizen kennengelernt. Diese operiert zum Beispiel auf K^n:

$$\begin{aligned} \cdot\colon \mathrm{GL}_n(K) \times K^n &\to K^n \\ (A, v) &\mapsto Av \end{aligned}$$

oder auch auf den $n \times m$ Matrizen:

$$\begin{aligned} \circ\colon \mathrm{GL}_n(K) \times \mathrm{Mat}_{n,m}(K) &\to \mathrm{Mat}_{n,m}(K) \\ (A, B) &\mapsto A \circ B. \end{aligned}$$

3. Die Untergruppe[14] der orthogonalen Matrizen mit Determinante 1 $SO(3) < \mathrm{GL}_3(\mathbb{R})$ operiert genauso auf $\mathbb{R}^3$:

$$\begin{aligned} \cdot\colon \mathrm{SO}(3) \times \mathbb{R}^3 &\to \mathbb{R}^3 \\ (A, v) &\mapsto Av \end{aligned}$$

aber da orthogonale Abbildungen Längen erhalten definiert das auch eine Operation auf der 2-Sphäre $S^2 := \{\mathbf{v} \in \mathbb{R}^3 \mid \|v\| = 1\}$:

$$\begin{aligned} \cdot\colon \mathrm{SO}(3) \times S^2 &\to S^2 \\ (A, v) &\mapsto Av. \end{aligned}$$

[14] Erinnerung: Der Satz vom Fußball besagte, dass die Elemente von $SO(3)$ genau die Drehungen sind.

Elemente zählen I: Stabilisatoren und transitive Operationen

In unserer Berechnung der Anzahl der Elemente der Dodekaedergruppe hatten wir gezählt, wie viele Elemente der Gruppe die Oberseite fest lassen. Nummerieren wir die Oberseite mit 1 wären das also die Elemente $g \in G$ mit $g.1 = 1$. Diese Untergruppe heißt *Stabilisator* der Seite.

Definition (Stabilisator eines Elements)**.** Ist $G \times X \to X$ eine Operation einer Gruppe G auf einer Menge X und $x \in X$ ein Element, so heißt

$$\mathrm{Stab}_G(x) := \{g \in G \mid g.x = x\} < G$$

der *Stabilisator* von x in G (oder die Stabilisatoruntergruppe von x in G).

Aufgabe. Der Stabilisator eines Elementes ist tatsächlich eine Untergruppe. Bitte rechnen Sie das einmal selbst mit der Definition nach.

Beispiel 87.

1. Für die Operation der Automorphismengruppe $G = \mathrm{Aut}(\text{Dodekaeder})$ der Menge der Seitenflächen

   $$G \times \{\text{Seitenflächen}\} \to \{\text{Seitenflächen}\}$$

   besteht der Stabilisator einer Fläche genau aus den 5 Drehungen um die Achse durch den Mittelpunkt der Fläche.

2. Im Beispiel der Operation:

   $$\begin{aligned} \cdot\colon \mathrm{GL}_n(K) \times K^n &\to K^n \\ (A, v) &\mapsto Av \end{aligned}$$

   ist der Stabilisator des ersten Einheitsvektors $\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ die Gruppe der invertierbaren Matrizen A mit $A\mathbf{e}_1 = \mathbf{e}_1$, d.h. der Matrizen mit erster Spalte $\mathbf{e}_1$:

   $$\mathrm{Stab}_{\mathrm{GL}_n}(\mathbf{e}_1) = \left\{ A = \begin{pmatrix} 1 & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & \cdots & \vdots \\ 0 & * & \cdots & * \end{pmatrix} \in \mathrm{GL}_n(K) \right\}.$$

Schließlich hatten wir bei Berechnung der Anzahl der Elemente der Dodekaedergruppe noch verwendet, dass wir jede Seite nach oben drehen können, bzw. dass wir die obere Seite auf jede Seite drehen können, d.h. wenn x_0 die obere Seite bezeichnet, so gibt es für alle $x \in \{\text{Seitenflächen}\}$ gibt es ein $g \in G$ mit $g.x_0 = x$.

Definition (transitive Operationen)**.** Eine Gruppenoperation

$$.\colon G \times X \to X$$

heißt *transitiv* wenn für ein $x_0 \in X$ gilt, dass es zu jedem $x \in X$ ein $g \in G$ gibt so dass $g.x_0 = x$.

In dieser Definition hätten wir die Bedingung genauso gut für alle $x_0 \in X$ formulieren können:

Bemerkung. Eine Gruppenoperation ist genau dann transitiv, wenn für jedes Element $x_1 \in X$ gilt, dass es zu jedem $x \in X$ ein $g \in G$ gibt so dass $g.x_1 = x$.

Beweis. Ist die Operation transitiv, $x_0 \in X$ ein Element das die Bedingung der Definition erfüllt und $x_1 \in X$ beliebig, so existiert ein $g_1 \in G$ mit $x_1 = g_1.x_0$ und $g \in G$ mit $x = g.x_0$. Dann gilt aber $x_0 = g_1^{-1}.x_1$ und also:

$$x = g.x_0 = g.(g_1^{-1}.x_1) = (g \cdot g_1^{-1}).x_1.$$

Also gibt es zu jedem $x \in X$ ein $g' \in G$ mit $g'.x_1 = x$. □

Jetzt können wir unser Zählargument allgemein formulieren:

Behauptung 88 (Bahnen-Stabilisatorformel)**.** *Sei* $.: G \times X \to X$ *eine transitive Gruppenoperation und* $x \in X$ *ein Element. Dann definiert die Abbildung*

$$\begin{aligned} .x\colon G &\to X \\ g &\mapsto g.x \end{aligned}$$

eine bijektive Abbildung

$$\begin{aligned} f\colon G/\operatorname{Stab}_G(x) &\to X \\ [g] &\mapsto f([g]) := g.x. \end{aligned}$$

Insbesondere ist

$$\#X = \#(G/\operatorname{Stab}_G) = \frac{\#G}{\#\operatorname{Stab}_G(x)},$$

beziehungsweise

$$\#G = \#X \cdot \#\operatorname{Stab}_G(x).$$

ERINNERUNG: Ist $H < G$ eine Untergruppe, so ist die Quotientenmenge

$$G/H := G/\sim_H \text{ wobei } g \sim_H g' :\Leftrightarrow \exists h \in G \text{ s.d. } g' = gh$$

nur eine Menge mit G-Operation, aber nur dann eine Gruppe, wenn H ein Normalteiler ist.

Im obigen Satz ist der Stabilisator nicht unbedingt ein Normalteiler, der Quotient $G/\operatorname{Stab}_G(x)$ ist darum zunächst nur eine Menge. (Diese Menge war für uns schon einmal nützlich, um zu zeigen, dass die Ordnung eines Elementes immer ein Teiler der Gruppenordnung ist.)

Beweis. Die Abbildung ist wohldefiniert: Ist $[g] = [g']$, so existiert nach Definition ein $h \in \operatorname{Stab}_G(x)$, so dass $g' = g \cdot h$. Darum gilt dann

$$\begin{aligned} f([g']) = g'.x &= (g \cdot h).x && g' = g \cdot h \\ &= g.(h.x) && \text{Gruppenoperation} \\ &= g.(x) && h.x = x \text{ weil } h \in \operatorname{Stab}_G(x) \\ &= g.x = f([g]). \end{aligned}$$

Die Abbildung ist injektiv, denn $f([g]) = f([g'])$ bedeutet

$$\begin{aligned} & g.x = g'.x && \text{wende } g^{-1}. \text{ auf beide Seiten an} \\ \Rightarrow\ & x = (g^{-1} \cdot g').x, \end{aligned}$$

also ist dann $g^{-1} \cdot g' \in \mathrm{Stab}_G(x)$ und damit $g' = g \cdot \underbrace{(g^{-1}g')}_{\in \mathrm{Stab}_G(x)}$, d.h.

$$[g'] = [g].$$

Die Abbildung ist surjektiv, da wir vorausgesetzt hatten, dass die Operation transitiv ist. □

Bemerkung. Die Gleichung der Stabilisator-Bahnen-Formel ist interessant, weil wir je nach Situation unterschiedliche 2 der 3 auftretenden Terme einfach verstehen können und damit den dritten berechnen.

Für die Dodekaedergruppe hatten wir die Gleichung

$$\#G = \#X \cdot \#\mathrm{Stab}_G(x)$$

verwendet, um $\#G$ aus der Anzahl der Seiten und der Anzahl der Elemente des Stabilisators einer Seite zu berechnen.

Das hätte mit den Ecken genauso funktioniert. Umgekehrt können wir damit schnell sehen, dass ein Dodekaeder 30 Kanten haben muss, da der Stabilisator einer Kante nur die Identität und die Drehung um 180° enthält, also

$$\#\{\text{Kanten}\} = \frac{\#G}{\#\mathrm{Stab}_G(x)} = \frac{60}{2} = 30.$$

Bemerkung. Die Bijektion $G/\mathrm{Stab}_G \xrightarrow{\cong} X$ gibt uns auch eine konkrete Beschreibung der Quotientenmenge. Zum Beispiel ist die Operation

$$\begin{aligned} \mathrm{GL}_n \times K^n &\to K^n \\ A, v &\mapsto Av \end{aligned}$$

nicht transitiv, aber fast: $A\mathbf{v} \neq 0$ für alle $\mathbf{v} \in K^n \setminus \{0\}$ und $A0 = 0$, also gibt es kein Element von K^n, so dass sich alle $\mathbf{w} \in K^n$ als $A\mathbf{v} = \mathbf{w}$ schreiben lassen, aber die Operation

$$\begin{aligned} \mathrm{GL}_n \times K^n \setminus \{0\} &\to K^n \setminus \{0\} \\ A, v &\mapsto Av \end{aligned}$$

ist bijektiv, da wir jedes Element $\mathbf{v} \in K^n \setminus \{0\}$ zu einer Basis $\mathbf{v}, \mathbf{v}_2, \ldots, \mathbf{v}_n$ von K^n ergänzen können und damit $A := (\mathbf{v}\mathbf{v}_2 \ldots \mathbf{v}_n) \in \mathrm{GL}_n$ die Eigenschaft $A\mathbf{e}_1 = \mathbf{v}$ erfüllt. Also ist

$$\mathrm{GL}_n \,/\, \mathrm{Stab}_{\mathrm{GL}_n}(\mathbf{e}_1) \cong K^n \setminus \{0\}.$$

Wenn wir die Untergruppe $\mathrm{SO}(3) < \mathrm{GL}_n(\mathbb{R})$ der Drehungen betrachten, so bildet diese die Einheitssphäre

$$S^2 := \{v \in \mathbb{R}^3 \mid \|v\| = 1\}$$

in sich ab:

$$\begin{aligned} \mathrm{SO}(3) \times S^2 &\to S^2 \\ A, v &\mapsto Av \end{aligned}$$

und der Stabilisator des ersten Einheitsvektors ist

$$\mathrm{Stab}_{\mathrm{SO}_3}(\mathbf{e}_1) = \{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & -b & a \end{pmatrix} \mid \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathrm{SO}(2) \} \cong \mathrm{SO}(2).$$

Also ist

$$\mathrm{SO}(3)/\mathrm{SO}(2) \cong S^2.$$

Wenn Sie die Definitionen auspacken, werden Sie feststellen, dass die Abbildung einfach durch

$$\text{Matrix} \mapsto \text{erste Spalte}$$

gegeben ist.

Elemente zählen II: Die Bahnenformel(n)

Unser Hauptbeispiel einer Gruppenoperation ist die Operation der Galoisgruppe eines Zerfällungskörpers eines Polynoms f auf der Menge der Nullstellen von f.

Im Beispiel $f(x) = (x^2-2)(x^2-3) \in \mathbb{Q}[x]$ ist diese Operation sicher nicht transitiv, denn die Galoisgruppe kann die Nullstellen $\pm\sqrt{2}$ und $\pm\sqrt{3}$ nicht vermischen.

Auf englisch „orbit“.

Definition (Bahn eines Elementes)**.** Ist $G \times X \to X$ eine Gruppenoperation und $x_0 \in X$ so heißt die Menge

$$G.x_0 := \{x = g.x_0 \mid g \in G\} \subseteq X$$

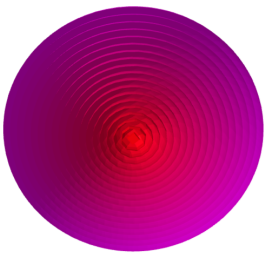
Bahn von x_0.

Beispiel 89. 1. Für unsere Operation $\mathrm{GL}_n \times K^n \to K^n$ haben wir schon gesehen, dass diese zwei Bahnen, nämlich $\mathrm{GL}_n .0 = \{0\}$ und $\mathrm{GL}_n .\mathbf{e}_1 = K^n \smallsetminus \{0\}$ besitzt.

2. Für die Operation $\mathrm{SO}(3) \times \mathbb{R}^3 \to \mathbb{R}_3$ haben wir genauso die Bahn

$$\mathrm{SO}(3).0 = \{0\}$$

und für jeden Vektor $\mathbf{v} \in \mathbb{R}^3 \smallsetminus \{0\}$ gilt $\|A\mathbf{v}\| = \|\mathbf{v}\|$. Da umgekehrt $A.\mathbf{e}_1 = S^2$ und $Ar\mathbf{e}_1 = rA\mathbf{e}_1$ gilt, sind die anderen Bahnen dieser Operation genau die Sphären mit festem Radius r.



Die Bahnen von $SO(3)$ auf $\mathbb{R}^3$ sind konzentrische Sphären.

Lemma/Definition 90 (Menge der Bahnen $G\backslash X$)**.** *Ist $G \times X \to X$ eine Gruppenoperation, so ist die Menge der Bahnen*

$$G\backslash X := \{M \subseteq X \mid M = G.x \text{ für ein } x \in X\}$$

genau die Menge der Äquivalenzklassen bezüglich der Relation

$$x \simeq x' :\Leftrightarrow x' = g.x \text{ für ein } g \in G.$$

Insbesondere sind Bahnen entweder gleich oder disjunkt, d.h. $G.x \cap G.x' \neq \varnothing \Rightarrow G.x = G.x'$.

Beweis. Wenn wir nachrechnen, das die Relation eine Äquivalenzrelation ist, folgt, dass die Äquivalenzklasse eines Elementes $[x] = \{x' \in X \mid x \sim x'\} = G.x$ gerade die Bahn von x ist. Da Äquivalenzklassen entweder gleich oder disjunkt sind, folgt dann der Rest der Behauptung.

Die Axiome für Äquivalenzrelationen rechnen wir leicht nach:

1. reflexiv: Für jedes Element $x \in X$ ist $e.x = x$ also $x \sim x$.

2. transitiv: Die Bedingungen $x \sim x'$ und $x' \sim x''$ bedeuten dass es $g, h \in G$ gibt, so dass $x' = g.x$ und $x'' = h.x'$ also

$$\begin{aligned} x'' &= h.x' \\ &= h.(g.x) \\ &= (h \cdot g).x \end{aligned}$$

   also $x \sim x''$.

symetrisch: Die Bedingung $x \sim x'$ bedeutet, dass es $g \in G$ gibt mit $x' = g.x$. Wenden wir auf diese Gleichung g^{-1}. an erhalten wir

$$\begin{aligned} g^{-1}.x' &= g^{-1}.(g.x) \\ &= (g^{-1} \cdot g).x = e.x = x. \end{aligned}$$

Also $x = g^{-1}.x'$ und das bedeutet $x' \sim x$. □

Da die Operation einer Gruppe auf einer Bahn per Definition transitiv ist, können wir damit die Elemente von X neu zählen:

Satz 91 (Bahnenformel I)**.** *Ist $G \times X \to X$ eine Operation einer endlichen Gruppe auf einer endlichen Menge so gilt:*

$$\#X = \sum_{[x] \in G\backslash X} \#[x] = \sum_{[x] \in G\backslash X} \frac{\#G}{\#\operatorname{Stab}_G(x)} = \#G \cdot \sum_{[x] \in G\backslash X} \frac{1}{\#\operatorname{Stab}_G(x)}.$$

Beweis. Die erste Gleichung ist nur die Zerlegung von X in die Äquivalenzklassen und in der 2. Gleichung haben wir die Bahnen-Stabilisatorformel für die Bahnen $G/\operatorname{Stab}_G(x) \cong G.x = [x]$ (Behauptung 88) verwendet. □

Der Grund dafür diese Aussage als Satz zu formulieren ist die etwas überraschende Nützlichkeit dieser Zählmethode. Zum Beispiel ergibt sich die folgende Aussage über die Struktur von endlichen Gruppen erstaunlich leicht daraus.

Folgerung 92 (Gruppen der Ordnung p^n sind auflösbar)**.** *Sei p eine Primzahl und G eine endliche Gruppe.*

1. *Ist $\#G = p$ so ist $G \cong (\mathbb{Z}/p\mathbb{Z}, +)$ zyklisch und insbesondere abelsch.*

2. *Ist $\#G = p^n$ für ein $n \in \mathbb{N}$, so ist G auflösbar.*

3. *Ist $\#G = p^2$ so ist entweder $G \cong (\mathbb{Z}/p^2\mathbb{Z}, +)$ oder $G \cong (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, +)$. Insbesondere ist G abelsch.*

VORÜBERLEGUNG: Um eine Gruppe zu verstehen, sollten wir Mengen suchen, auf denen die Gruppe operiert. Hier fangen wir leider mit einer abstrakten Gruppe G an, weshalb uns nicht viele Mengen einfallen, auf denen G operieren könnte. Zunächst fällt mir nur G selbst ein, also $X = G$. Lassen wir G einfach durch Multiplikation von links auf $X = G$ operieren, finden wir nur eine Bahn $G.e = G$, was uns nicht weiter hilft.

Eine bessere Operation haben wir schon gefunden als wir $S_4 \to S_3$ konstruiert haben, indem wir S_4 durch Konjugation auf den Doppeltranspositionen $\{(12)(34), (13)(24), (14)(23)\}$ operieren gelassen haben.

MERKE: Jede Gruppe G operiert durch Konjugation auf sich selbst: Für $X := G$ ist

$$\begin{aligned} .: G \times X &\to X \\ (g, x) &\mapsto g.x := g \cdot x \cdot g^{-1} \end{aligned}$$

eine Gruppenoperation, denn für alle $x \in X = G$ gilt $e.x \overset{Def.}{=} e \cdot x \cdot e^{-1} = x$ und für $g, h \in G, x \in X = G$ gilt

$$\begin{aligned} g.(h.x) &= g.(h \cdot x \cdot h^{-1}) \\ &= g \cdot (h \cdot x \cdot h^{-1}) \cdot g^{-1} \\ &= (g \cdot h) \cdot x \cdot (h^{-1} \cdot g^{-1}) \\ &= (g \cdot h) \cdot x \cdot (g \cdot h)^{-1} \\ &= (g \cdot h).x. \end{aligned}$$

Beispiel 93. 1. Für die Gruppe $G = \mathrm{GL}_n(K)$ entspricht $A \mapsto gAg^{-1}$ einem Basiswechsel. Die Bahnen diese Operation haben wir in der linearen Algebra für algebraisch abgeschlossene Körper K berechnet, diese sind genau durch die möglichen Jordannormalformen gegeben, denn zu jeder Matrix gibt es einen Basiswechsel, der die Matrix in Jordannormalform bringt und weil die Jordannormalform durch das charakteristische Polynom, und die Dimension der Kerne $\ker(A - c_i \,\mathrm{id})^m$ wobei $m \leq n$ und c_i Eigenwerte von A sind bestimmt ist, sind zwei Matrizen genau dann zueinander konjugiert, wenn sie die gleiche Jordannormalform besitzen.

2. Für die symmetrische Gruppe S_n haben wir gesehen, das $\tau \mapsto \sigma\tau\sigma^{-1}$ in der Zykelschreibweise von τ die Einträge $1, \ldots, n$ durch $\sigma(1), \ldots, \sigma(n)$ ersetzt. Zwei Permutationen sind also genau dann konjugiert, wenn die Längen der Zyklen in der Zykelschreibweise übereinstimmen. Die Konjugationsklassen in S_n entsprechen also genau den Möglichkeiten n als Summe $n = n_1 + \cdots + n_r$ von natürlichen Zahlen zu schreiben.

Beweis von Folgerung 92. 1. Die erste Aussage kennen wir schon und das hatten Sie in der Vorlesung erklärt: Ist $g \in G \smallsetminus \{e\}$ ein Element so ist die Ordnung von g ein Teiler der Gruppenordnung p, also 1 oder p. Da $g \neq e$ nicht das neutrale Element

ist, ist die Ordnung nicht 1, also ist $\operatorname{ord}(g) = p$ und damit $G = \{e, g, g^2, \ldots, g^{p-1}\}$ eine zyklische Gruppe und damit abelsch.

Die Aussage, dass G abelsch ist, könnten wir auch mit der Bahnenformel einsehen – und das wird uns gleich für 2. weiter helfen: Wir wissen nämlich für die Konjugation von G auf $X = G$:

$$\begin{aligned} p = \#X &= \sum_{[x]\in G\backslash X} \frac{\#G}{\#\operatorname{Stab}_G(x)} \\ &= \#[e] + \sum_{\substack{[x]\in G\backslash X \\ [x]\neq[e]}} \frac{\#G}{\#\operatorname{Stab}_G(x)} \\ &= 1 + \sum_{\substack{[x]\in G\backslash X \\ [x]\neq[e]}} \underbrace{\frac{\#G}{\#\operatorname{Stab}_G(x)}}_{\in\{1,p\}}, \end{aligned}$$

weil $g.e = g \cdot e \cdot g^{-1} = g \cdot g^{-1} = e$. Für alle Elemente $x \in X = G$ teilt die Ordnung der Untergruppe $\operatorname{Stab}_G(x)$ die Ordnung $p = \#G$, ist also p oder 1. Da die Summe aber insgesamt $p - 1$ ergibt, kann $\frac{\#G}{\#\operatorname{Stab}_G(x)} = p$ nicht vorkommen, also muss für alle $x \in X$ gelten, dass $\#\operatorname{Stab}_G(x) = p$ ist, also $\operatorname{Stab}_G(x) = G$.

Das bedeutet aber, dass $gxg^{-1} = x$ für alle $g \in G, x \in X$ also $gx = xg$ für alle $g, x \in G$. Also ist G abelsch.

2. Das Argument aus 1. können wir genauso im Fall $\#G = p^n$ anwenden:

$$\begin{aligned} p^n = \#X &= \sum_{[x]\in G\backslash X} \frac{\#G}{\#\operatorname{Stab}_G(x)} \\ &= \#[e] + \sum_{\substack{[x]\in G\backslash X \\ [x]\neq[e]}} \frac{\#G}{\#\operatorname{Stab}_G(x)} \\ &= 1 + \sum_{\substack{[x]\in G\backslash X \\ [x]\neq[e]}} \underbrace{\frac{\#G}{\#\operatorname{Stab}_G(x)}}_{\in\{1,p,\ldots,p^n\}}. \end{aligned}$$

Weil die linke Seite der Gleichung aber $\equiv 0 \mod p$ ist, muss es ein $[x] \in G\backslash X$ mit $[x] \neq [e]$ geben so dass $\frac{\#G}{\#\operatorname{Stab}_G(x)}$ nicht durch p teilbar ist, also $\frac{\#G}{\#\operatorname{Stab}_G(x)} = 1$ gilt. Das bedeutet aber gerade, dass $gx = xg$ für alle $g \in G$ gilt.

Die Untergruppe

$$Z(G) := \{z \in G \mid zg = gz \text{ für alle } g \in G\} \lhd G$$

ist dann aber ein nichttrivialer, abelscher Normalteiler von G (wir rechnen gleich in Ruhe nach, dass das ein Normalteiler ist). Dann ist aber nach Induktion über n die Quotientengruppe $G/Z(G)$ auflösbar, weil $\#G/Z(G) = p^m$ mit $m < n$ ist. Da $Z(G)$ abelsch ist, ist dann auch G auflösbar.

3. Um zu zeigen, dass eine Gruppe G der Ordnung p^2 immer isomorph zu einer der abelschen Gruppen $\mathbb{Z}/p^2\mathbb{Z}$ oder $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ sind benutzen wir einen Trick: Alle Elemente von G, die nicht das neutrale Element sind, haben entweder Ordnung p oder

Ordnung p^2, da die Ordnung ein Teiler der Gruppenordnung $\#G = p^2$ ist. Enthält G ein Element x der Ordnung p^2, so ist $G = \{e, x, x^2, \dots, x^{p^2-1}\} \cong (\mathbb{Z}/p^2\mathbb{Z}, +)$ zyklisch. Andernfalls haben alle nichttrivialen Elemente von G die Ordnung p.

In Teil 2. haben wir außerdem gezeigt, dass das Zentrum $Z(G) < G$ nicht trivial ist. Sei also $x \in Z(G) \smallsetminus \{e\}$ ein Element und $y \in G \smallsetminus \{e, x, x^2, \dots, x^{p-1}\}$ ein Element, das nicht in der von x erzeugten Untergruppe liegt. Da x im Zentrum von G liegt, kommutiert x mit allen Elementen, insbesondere gilt also $xy = yx$. Dann ist aber die Abbildung

$$\begin{aligned} F\colon \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} &\to G \\ (a, b) &\mapsto x^a y^b \end{aligned}$$

ein Gruppenhomorphismus, da

$$(x^a y^b) \cdot (x^{a'} y^{b'}) = x^a x^{a'} x^a y^b) \cdot (x^{a'} y^{b'}) y^{b'} = x^{a+a'} y^{b+b'}$$

für alle $a, b, a', b' \in \mathbb{Z}/p\mathbb{Z}$ gilt.

Da das Bild von F eine Untergruppe ist, die mehr als p Elemente enthält, die Ordnung von Untergruppen aber die Gruppenordnung $\#G = p^2$ teilt, ist F surjektiv und damit sogar ein Isomorphismus.

□

Wie versprochen hier noch der Nachweis, dass das Zentrum ein Normalteiler ist:

Bemerkung. Ist G eine Gruppe, so ist das Zentrum

$$Z(G) := \{z \in G \mid zg = gz \text{ für alle } g \in G\} \lhd G$$

ein Normalteiler in G.

Beweis. 1. Das Zentrum ist eine Untergruppe:

(a) $e \in Z(G)$ da für alle $g \in G$ gilt dass $e \cdot g = g = g \cdot e$ weil e das neutrale Elemente von G ist.

(b) Sind $a, b \in Z(G)$, so auch $a \cdot b$, da für alle $g \in G$ gilt dass

$$\begin{aligned} a \cdot b \cdot g &= a \cdot g \cdot b && b \in Z(G) \\ &= g \cdot a \cdot b && a \in Z(G). \end{aligned}$$

(c) Ist $a \in Z(G)$, so auch a^{-1}, da für alle $g \in G$ gilt dass – Möchten Sie sich das vielleicht selbst überlegen? Sie können auch hierfür versuchen los zurechnen, das Argument ist nur eine Zeile lang.

2. Das Zentrum ist ein Normalteiler, das für alle $g \in G$ und $z \in Z(G)$ gilt, dass $gzg^{-1} = zgg^{-1} = z$, also gilt $gZ(G)g^{-1} = Z(G)$.

□

MERKE: Das Zentrum einer Gruppe mit p^n Elementen ist nicht trivial. Darum sind Gruppen der Ordnung p^n auflösbar.

Folgerung 94. *Ist G eine Gruppe mit p^n Elementen, so enthält G für alle $m \leq n$ Untergruppen und sogar Normalteiler der Ordnung p^m.*

Beweis. In der Vorlesung habe ich Ihnen das als Übungsaufgabe überlassen. Sie können sich das induktiv überlegen, indem Sie zeigen:

1. Das Zentrum $Z(G)$ enthält ein Element der Ordnung p und damit auch eine Untergruppe $H < Z(G)$ der Ordnung p.
2. Jede Untergruppe $H < Z(G) \lhd G$ des Zentrums $Z(G)$ ist automatisch ein Normalteiler in G.
3. Ist $N \lhd (G/H)$ ein Normalteiler mit p^m Elementen, so ist
$$\tilde{N} := \{g \in G \mid [g] \in N\} < G$$
ein Normalteiler mit $\#H \cdot \#N$ Elementen.

□

Anwendung: Die komplexen Zahlen sind algebraisch abgeschlossen

Mit der Aussage das Gruppen der Ordnung p^n auflösbar sind, können wir versuchen u zeigen, das die komplexen Zahlen $\mathbb{C}$ die einzige algebraische Erweiterung der reellen Zahlen und darum algebraisch abgeschlossen sind. Wir wissen nämlich schon:

1. Jedes Polynom $f(x) \in \mathbb{R}[x]$ von ungeradem Grad besitzt eine Nullstelle in $\mathbb{R}$. Insbesondere müssen irreduzible Polynome $f(x) \in \mathbb{R}[x]$ geraden Grad haben.

   Da jede endliche Körpererweiterung $K|\mathbb{R}$ von einem Element erzeugt ist, ist also $[K : \mathbb{R}]$ notwendig gerade, also
$$[K : \mathbb{R}] = 2^n \cdot m \text{ mit } m \text{ ungerade.}$$
2. Jedes quadratische Polynom in $g(z) \in \mathbb{C}[z]$ besitzt eine Nullstelle in $\mathbb{C}$, denn die pq-Formel gibt uns eine Lösungsformel in Termen einer Wurzel und in $\mathbb{C}$ können wir aus jeder Zahl die Wurzel ziehen. Die komplexen Zahlen besitzen also keine quadratische Körpererweiterung.

Erinnerung: Wurzelziehen in $\mathbb{C}$ ging mittels: Winkel halbieren und Wurzel aus der Länge ziehen, d.h. für $|z| = 1$ und $z \neq -1$ ist
$$\sqrt{z} = \frac{z+1}{|z+1|}$$
und $\sqrt{-1} = i$.

Wenn also $K|\mathbb{R}$ ein Zerfällungskörper eines irreduziblen Polynoms f ist hat die Galoisgruppe $G = \mathrm{Gal}(K\mathbb{R})$
$$\#G = \#\mathrm{Gal}(K|\mathbb{R}) = [K : \mathbb{R}] = 2^n \cdot m$$
Elemente, wobei $m = 2k + 1$ ungerade ist. Wenn wir jetzt zeigen könnten, dass jede Gruppe der Ordnung $2^n \cdot m$ eine Untergruppe $H < G$ der Ordnung 2^n besitzt, könnten wir folgern:

1. Aus der Galoiskorrespondenz wissen wir

$$[K^H : \mathbb{R}] = \frac{\#\mathrm{Gal}(K|\mathbb{R})}{\#H} = \frac{2^n m}{2^n} = m \text{ ist ungerade.}$$

   Da Körpererweiterungen von $\mathbb{R}$ aber geraden Grad haben muss also $m = 1$, also $K^H = \mathbb{R}$ und darum $H = \mathrm{Gal}(K|\mathbb{R})$ gelten. Also ist

$$\#\mathrm{Gal}(K|\mathbb{R}) = 2^n.$$

2. Gruppen der Ordnung 2^n sind aber auflösbar und wegen Folgerung 94 gibt es sogar eine Kette von Normalteilern

$$\{e\} \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_n = \mathrm{Gal}(K|\mathbb{R})$$

   mit $\#H_i/h_{i-1} = 2$ für alle i. Nach der Galoiskorrespondenz entspricht diese Kette einer Kette von Körpererweiterungen

$$K \supseteq K_1 \supseteq \cdots \supseteq K_n = \mathbb{R}$$

   mit $[K_i : K_{i+1}] = 2$ für alle i. Quadratische Erweiterung von $\mathbb{R}$ entstehen aber wegen der pq-Formel durch Wurzelziehen, also ist $\mathbb{C}$ die einzige quadratische Erweiterung von $\mathbb{R}$ und $\mathbb{C}$ hat keine quadratischen Erweiterungen. Darum muss $K = \mathbb{C}$ sein.

Es bleibt also noch zu zeigen, dass jede Gruppe der Ordnung $2^n \cdot m$ eine Untergrupe der Ordnung 2^n besitzt. Das überlegen wir uns im nächsten Abschnitt.

Bemerkung. Sie haben nach der Vorlesung angemerkt, dass das obige Argument den Zwischenwertsatz verwendet hat. Das erzeugt immer wieder einmal die Frage, ob es einen „rein algebraischen" Beweis der Aussage dass $\mathbb{C}$ algebraisch abgeschlossen ist gibt.

Auf den ersten Blick ist das eine ganz natürliche Frage, aber auf den zweiten Blick habe ich diese Frage ehrlich gesagt noch nie verstanden: Da wir die komplexen Zahlen mittels der reellen Zahlen definiert haben, werden wir im Beweis notwendig irgendwo entweder die Konstruktion oder eine charakterisierende Eigenschaft der reellen Zahlen – also die Vollständigkeit des geordneten Körpers $\mathbb{R}$ – verwenden müssen. Anders gesagt: Da die Aussage für $\mathbb{Q}(i)$ statt $\mathbb{C}$ falsch ist, wird eine Eigenschaft von $\mathbb{R}$ für das Argument notwendig sein.

Der Zwischenwertsatz scheint mir nun aber eine zur Vollständigkeit äquivalente Aussage zu sein.

Der Sylowsatz

Für das Argument für den Fundamentalsatz der Algebra, zeigen wir die allgemeinere Aussage, dass Gruppen der Ordnng $p^n \cdot m$ wobei p, m teilerfremd sind, immer Untergruppen der Ordnung p^n besitzen.

Satz 95 (Sylow). *Sei p eine Primzahl und G eine endliche Gruppe der Ordnung $\#G = p^n \cdot m$, wobei m, p teilerfremd sind.*

Dann besitzt G eine Untergruppe mit p^n Elementen, je zwei solche Gruppen sind zueinander konjugiert (d.h. sind $S, S' < G$ Untergruppen mit p^n Elementen, so existiert $g \in G$ mit $S' = gSg^{-1}$) und es gilt

$$\#\{S < G \mid \#S = p^n\} \equiv 1 \mod p.$$

Notation 96. Ist $\#G = p^n m$ mit m, p teilerfremd, so heißen Untergruppen $S < G$ mit p^n Elementen *p-Sylowuntergruppen*. Da nach dem Satz je zwei Sylowuntergruppen konjugiert sind, sind p-Sylowuntergruppen isomorph und wir schreiben darum manchmal $\mathrm{Syl}_p(G) < G$ für eine p-Sylowuntergruppe.

Den Beweis dieses Satzes finde ich einerseits ganz wunderbar – die Aussage folgt indem wir G auf einer geschickt gewählten Menge operieren lassen – andererseits kann ich mir aus irgendeinem Grund schlecht merken, was die geschickte Wahl ist.

Beweis des Sylowsatzes (Existenz von Sylowuntergruppen). Die Idee ist wie gesagt, G auf einer geeigneten Menge X operieren zu lassen. Da wir eine Untergruppe mit p^n Elementen suchen, können wir die Menge aller p^n-elementigen Teilmengen ausprobieren:

$$X := \{M \subseteq G \mid \#M = p^n\}.$$

Darauf operiert G mittels

$$\begin{aligned} G \times X &\to X \\ (g, M) &\mapsto g.M := \{g \cdot m \mid m \in M\}. \end{aligned}$$

Die wichtigste Beobachtung ist, dass die Anzahl der Elemente von X nicht durch p teilbar ist, denn die Anzahl der p^n-elementigen Teilmengen ist nach Definition ein Binomialkoeffizient:

$$\#X = \binom{\#G}{p^n} = \binom{p^n m}{p^n} = \frac{(p^n m)(p^n m - 1) \cdots (p^n m - (p^n - 1))}{p^n \ (p^n - 1) \cdots (1)}.$$

Erinnerung

$$\begin{aligned} \binom{n}{k} &= \frac{n(n-1)\cdots(n-(k-1))}{k!} \\ &= \frac{n(n-1)\cdots(n-(k-1))}{k(k-1)\cdots(1)}. \end{aligned}$$

Diese Formel hatte eine einfache Erklärung, erinnern Sie sich?

Nun sind aber für alle $0 \leq \ell < p^n$ die Zahlen $p^n m - \ell$ und $p^n - \ell$ kongruent modulo p^n und darum durch die gleiche Potenz von p teilbar, d.h. im Nennen und Zähler des Binomialkoeffizienten tauchen die gleichen Potenzen von p auf, also ist

$$\#X \not\equiv 0 \mod p.$$

Nach der Bahnenformel ist aber

$$\#X = \sum_{[M] \in G \backslash X} \frac{\#G}{\#\mathrm{Stab}_G(M)}$$

und der Term $\frac{\#G}{\#\mathrm{Stab}_G(M)}$ ist nur dann nicht durch p teilbar, wenn $\#\mathrm{Stab}_G(M) = p^n k$ für ein $k \in \mathbb{N}$. Es existiert also ein $M_0 \in X$ mit $\#\mathrm{Stab}_G(M_0) = p^n k$. Andererseits ist aber

$$\#\mathrm{Stab}_G(M_0) = \{g \in G \mid g \cdot M_0 = M_0\} \leq \#M_0 = p^n$$

denn ist $m \in M_0$ so gibt es für jedes $m' \in M_0 \subseteq G$ genau ein $g \in G$ mit $gm = m'$, nämlich $m' \cdot m^{-1}$. Es gibt also genau $\#M_0 = p^n$ Elemente für die $gm \in M_0$ liegt und $\mathrm{Stab}_G(M_0)$ kann höchstens diese Elemente enthalten.

Also ist $p^n k = \#\mathrm{Stab}_G(M_0) \leq p^n$, d.h. $\#\mathrm{Stab}_G(M_0) = p^n$ und damit ist $\mathrm{Stab}_G(M_0)$ eine Untergruppe mit p^n Elementen. □

Sie können sich jetzt überlegen, dass $M_0 = \mathrm{Stab}_G(M_0) \cdot m_0$ ist. M_0 selbst ist also nicht notwendig selbst eine Untergruppe, aber fast.

MIT DEM ERSTEN TEIL des Sylowsatzes haben wir den Beweis das $\mathbb{C}$ algebraisch abgeschlossen ist, schon vervollständigt.

Folgerung 97 (Fundamentalsatz der Algebra)**.** *Der Körper der komplexen Zahlen $\mathbb{C}$ ist algebraisch abgeschlossen, d.h. jedes nicht konstante Polynom besitzt eine Nullstelle in $\mathbb{C}$.*

Beweis. Im vorigen Abschnitt hatten wir die Aussage mittels der Galoiskorrespondenz und der Aussage dass reelle Polynome ungeraden Grades eine reelle Nullstelle haben darauf zurück geführt zu zeigen, dass jede endliche Gruppe G mit $2^n(2k+1)$ Elementen eine Untergruppe der Ordnung 2^n besitzt. Das wissen wir nun, da G nach dem Sylowsatz eine 2-Sylowuntergruppe enthält. □

Anwendung: Poynome mit Galoisgruppe S_p

Als weitere Anwendung des ersten Teils des Sylowsatzes können wir auch Ihre Frage nach einem expliziten Polynom mit nichtauflösbarer Galoisgruppe S_5 beantworten.

Behauptung 98. *Die Galoisgruppe $\mathrm{Gal}(K|\mathbb{Q})$ des Zerfällungskörpers des irreduziblen Polynoms $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ ist die Symmetrische Gruppe S_5 und insbesondere nicht auflösbar.*

Es gilt allgemeiner: Ist p eine Primzahl und $f(x) \in \mathbb{Q}[x]$ ein irreduzibles Polynom vom Grad p das genau $p-2$ reelle und 2 komplexe Nullstellen besitzt, so ist die Galoisgruppe eines Zerfällungskörpers von f die symmetrische Gruppe S_p.

Beweis. Das Polynom $f(x) = x^5 - 6x + 3$ ist nach dem Eisensteinkriterium (angewendet für die Primzahl 3) irreduzibel. Kurvendiskussion zeigt, das $f(x)$ genau drei reelle Nullstellen besitzt, da die Ableitung

$$f'(x) = 5x^4 - 6$$

die reellen Nullstellen $\pm\sqrt[4]{\frac{6}{5}}$ und die komplexen Nullstellen $\pm i\sqrt[4]{\frac{6}{5}}$ besitzt und

$$f(-\sqrt[4]{\frac{6}{5}}) = -\sqrt[4]{\frac{6}{5}}^5 + 6\sqrt[4]{\frac{6}{5}} + 3 > 0 \qquad \text{sowie}$$
$$f(\sqrt[4]{\frac{6}{5}}) = \sqrt[4]{\frac{6}{5}}^5 - 6\sqrt[4]{\frac{6}{5}} + 3 < 0.$$

Seien nun $\alpha_1, \ldots, \alpha_5 \in \mathbb{C}$ die Nullstellen von f und $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_5)$ der Zerfällungskörper von f. Wir nummerieren die Nullstellen so, dass α_1, α_2 die komplexen Nullstellen und $\alpha_3, \alpha_4, \alpha_5$ die reellen Nullstellen sind.

Da Körperautomorphismen $\sigma \in \mathrm{Gal}(\mathbb{Q}(\alpha_1, \ldots, \alpha_5)|\mathbb{Q})$ eindeutig durch die Bilder der Nullstellen $\sigma(\alpha_i)$ bestimmt sind definiert die Operation der Galoisgruppe auf der Menge der Nullstellen eine Einbettung

$$\mathrm{Gal}(K|\mathbb{Q}) \hookrightarrow S_5.$$

Nach der Galoiskorrespondenz ist $\#\mathrm{Gal}(K|\mathbb{Q}) = [K : \mathbb{Q}]$ (ud das ist ein Teiler von $\#S_5 = 5!$).

Weil f irreduzibel ist, is $\mathbb{Q}[x]/(f(x)) \hookrightarrow K$. Also ist $\#\mathrm{Gal}(K|\mathbb{Q})$ durch 5 teilbar und enthält also nach dem Sylowsatz eine Untergruppe der Ordnung 5 und darum enthält $\mathrm{Gal}(K|\mathbb{Q})$ auch ein Element der Ordnung 5.

Die einzigen Elemente der Ordnung 5 in S_5 sind aber 5-Zyklen, d.h. $\mathrm{Gal}(K|\mathbb{Q})$ enthält einen 5-Zyklus $\sigma = (1, i_2, \ldots, i_5)$. Da 5 eine Primzahl ist, haben auch die Potenzen σ^k für $k < 5$ Ordnung 5 und da eine dieser Potenzen 1 auf 2 abbildet können wir nach umnummerieren der reellen Nullstellen annehmen, dass $\sigma^k = (12345) \in \mathrm{Gal}(K|\mathbb{Q})$ ist.

Die komplexe Konjugation definiert auch ein Element $\tau \in \mathrm{Gal}(K|\mathbb{Q})$ und dieses Element lässt die reellen Nullstellen $\alpha_3, \alpha_4, \alpha_5$ von f fest und vertauscht darum die beiden komplexen α_1, α_2, entspricht also der Transposition $\tau = (12)$.

Eine Untergruppe von S_5, die (12) und (12345) enthält, enthält alle Transpositionen $(ii+1)$ und diese erzeugen S_5, also ist $\mathrm{Gal}(K|\mathbb{Q}) = S_5$. □

Zurück zum Sylowsatz

Bisher haben wir die Existenz von p-Sylowuntergruppen gezeigt, dass diese alle konjugiert – und daher isomorph – sind fehlt noch.

Beweis des zweiten Teils von Satz 95.] Wie im Sylowsatz vorausgesetzt sei p ieder eine Primzahl und G eine Gruppe mit $p^n m$ Elementen, wobei m, p teilerfremd sind.

1. Wir wollen nun zeigen, dass es zu je zwei Untergruppen $S, S' < G$ mit p^n Elementen ein $g \in G$ existiert, mit $gSg^{-1} = S'$.

   Wie im ersten Teil suchen wir dafür wieder eine geeignete Menge auf der G operiert. Die Gleichung $gSg^{-1} = S'$ impliziert, dass für alle $s \in S$ ebenfalls $(gs)Ss^{-1}g^{-1} = gSg^{-1} = S'$ gilt. Ein gesuchtes Element g ist also höchstens bis auf Elemente von S bestimmt. Darum betrachten wir die Menge

   $$X = G/S = \{[g] = M \subseteq G \mid M = gS \text{ für ein } g \in G\}.$$

   Auf dieser Menge operiert G und damit auch die zweite Untergruppe S' durch Multiplikation von links

   $$\begin{aligned} G \times G/S &\to G/S \\ (h, gS) &\mapsto hgS. \end{aligned}$$

Damit ergibt sich das Resultat wieder überraschend einfach: Die Menge $X = G/S$ hat $\frac{\#G}{\#S} = \frac{p^n m}{p^n} = m$ Elemente und m ist teilerfremd zu p. Die Bahnenformel für X besagt dann

$$m = \#X = \sum_{[xS] \in S' \backslash X} \frac{\#S'}{\#\mathrm{Stab}_{S'}(xS)}.$$

Aber die Terme $\frac{\#S'}{\#\mathrm{Stab}_{S'}(xS)}$ sind alle Potenzen von p, es sei denn $\mathrm{Stab}_{S'}(xS) = S'$. Weil $m \not\equiv 0 \mod p$ existiert also ein $xS \in G/S$ so dass $\mathrm{Stab}_{S'}(xS) = S'$, d.h. $s'xS = xS$ für alle $s' \in S'$ also $S'xS = xS$ und damit $S' = xSx^{-1}$. Also ist S' konjugiert zu S und das war zu zeigen.

2. Mit dem Wissen, dass alle p-Sylowuntergruppen konjugiert sind, können wir die Aussage über die Anzahl der Sylowuntergruppen zeigen. Sei $X := \{S' < G \mid \#S' = p^n\}$ die Menge der p-Sylowuntergruppen. Hierauf operiert G als

$$\begin{aligned} G \times X &\to X \\ g, S' &\mapsto gS'g^{-1} \end{aligned}$$

und wir wissen schon, dass diese Operation transitiv ist. Wir benutzen wieder die Bahnenformel für die Operation einer festen Sylowuntegruppe S:

$$\#X = \sum_{[S'] \in S \backslash X} \frac{\#S}{\#\mathrm{Stab}_S([S'])}.$$

Die einzelnen Terme sind wieder Potenzen von p und genau dann 1 wenn $\mathrm{Stab}_S([S']) = S$. Wenn wir zeigen können, dass das nur für $S' = S$ vorkommen kann folgt $\#X \equiv 1 \mod p$.

Sei also S' eine Untergruppe mit $\mathrm{Stab}_S([S']) = S$, d.h. $sS' = S's$ für alle $s \in S$. Das bedeutet aber, dass die Menge $SS' = \{g = ss' \mid s \in S, s' \in S'\} < G$ eine Untergruppe ist. Die Anzahl der Elemente von SS' ist aber eine Potenz von p, da die Gruppe $S \times S'$ transitiv auf dieser Untergruppe operiert, mittels

$$\begin{aligned} (S \times S') \times SS' &\to SS' \\ (s, s'), g &\mapsto sgs'^{-1}. \end{aligned}$$

Da eine Untergruppe von p-Potenzordnung von G aber maximal $p^n = \#S = \#S'$ Elemente besitzen kann muss $S' = SS' = S$ gelten. Das war zu zeigen.

□

Für die Eigenschaften einer Operation:

(a) $e.S = eSe^{-1} = eSe = S$ ist in der Tat die Identische Abbildung und

(b) für die Komposition gilt

$g.(h.S) = g.(hSh^{-1}) = ghSh^{-1}g^{-1} = (gh)S(gh)^{-1} =$

weil $(gh)^{-1} = h^{-1}g^{-1}$ in allen Gruppen gilt.

Sylow selbst hatte dieses Resultat im übrigen tatsächlich gesucht, um das Resultat auf Galoisgruppen anzuwenden, ganz ähnlich wie wir das mit dem Fundamentalsatz der Algebra gemacht hatten. Außerdem ist das Resultat auch nützlich, um transitive Untergruppen von S_n, also Untergruppen $G < S_n$ für die Einschränkung der Operation von S_n auf $G \times \{1, \ldots, n\} \to \{1, \ldots, n\}$ noch immer transitiv

ist, zu verstehen. Diese sind gerade die Untergruppen, die als Galoisgruppen von Zerfällungskörpern von irreduziblen Polynomen auftreten können.

In den Übungsaufgaben werden Sie ausprobieren, wie der Sylowsatz erlaubt zu zeigen, dass Gruppen deren Ordnung nicht durch viele Primzahlen teilbar sind oft auflösbar sind. Mit hinreichend großer Geduld lässt sich damit zum Beispiel zeigen, dass wir mit A_5 die kleinste nicht abelsche einfache Gruppe gefunden hatten.

Das beruht auf der Beobachtung, dass die Aussage über die Anzahl von Sylowuntergruppen manchmal erlaubt zu folgern, dass eine Sylowuntergruppe sogar ein Normalteiler ist.

Wir hatten gesehen, dass die Operation von G auf der Menge der Sylowuntergruppen:

$$\begin{aligned} G \times \{S < G \mid \#S = p^n\} &\to \{S < G \mid \#S = p^n\} \\ (g, S) &\mapsto g.S := gSg^{-1} \end{aligned}$$

transitiv ist und nach der Bahnen-Stabilisatorformel also

$$G/\operatorname{Stab}_G(S) \cong \{S < G \mid \#S = p^n\}$$

ist.

Lassen Sie uns den Stabilisator dieser Operation einmal ausrechnen. Da das eine allgemeiner funktioniert möchte ich das für alle Untergruppen $H < G$ machen, also die Stabilisatoren für die Operation

$$\begin{aligned} G \times \{H < G \mid H \text{ Untergruppe}\} &\to \{H < G \mid H \text{ Untergruppe}\} \\ (g, H) &\mapsto g.H := gHg^{-1} \end{aligned}$$

bestimmen. Nach Definition ist das

$$\begin{aligned} \operatorname{Stab}_G(H) &= \{g \in G \mid g.H = H\} \\ &= \{g \in G \mid gHg^{-1} = H\} \\ &= \{g \in G \mid gH = Hg\} =: N_G(H). \end{aligned}$$

Definition (Normalisator)**.** Der *Normalisator* einer Untergruppe $H < G$ ist

$$N_G(H) := \{g \in G \mid gHg^{-1} = H\} < G$$

dies ist eine Untergruppe, die H enthält.

Bemerkung. 1. Da wir gerade gesehen haben, dass der Normalisator einer Untergruppe als Stabilisator einer Gruppenoperation auftaucht und Stabilisatoren immer Untergruppen sind, müssen wir uns nicht mehr überlegen, dass $N_G(H)$ immer eine Untergruppe ist.

2. Da $H < G$ genau dann ein Normalteiler ist, wenn $gHg^{-1} = H$ für alle $g \in G$ gilt, ist eine Untergruppe genau dann ein Normalteiler wenn $N_G(H) = G$ gilt.

Damit können wir nun Beispiele finden, in denen Sylowuntergruppen aus Teilbarkeitsgründen Normalteiler sind.

Beispiel 99 (Gruppen der Ordnung 6)**.** Ist G eine Gruppe mit 6 Elementen, so existiert nach dem Sylowsatz eine Untergruppe $S < G$ mit 3 Elementen. Wegen den Inklusionen

$$S \leqslant N(G) \leqslant G$$

und da die Ordnung einer Untergruppe immer ein Teiler der Gruppenordnung ist gilt also

$$\#S = 3 | \#N_G(S) | \#G = 6.$$

Also ist $\#N(G) \in \{3, 6\}$. Andererseits ist aber nach dem Sylowsatz

$$\#(G/N_G(S)) = \frac{\#G}{\#N_G(S)} = \frac{6}{\#N_G(S)} \equiv 1 \mod 3.$$

Da $2 \not\equiv 1 \mod 3$ muss also $N_G(S) = G$ gelten, d.h. S ist ein Normalteiler in $N_G(S)$. Insbesondere ist G eine auflösbare Gruppe.

Außerdem wissen wir, dass $S \cong (\mathbb{Z}/3\mathbb{Z}, +)$ und $G/S \cong (\mathbb{Z}/2\mathbb{Z}, +)$ weil Gruppen von Primzahlordnung zyklisch sind. Daraus können Sie sich überlegen, dass G entweder S_3 oder $\mathbb{Z}/6\mathbb{Z}$ ist.

Exkurs: Zählprobleme und die zweite Bahnenformel

Gruppenoperationen tauchen überall dort auf, wo Symmetrien auftauchen. Das passiert bei Abzählproblemen häufig. Wir könnten zum Beispiel fragen wie viele Möglichkeiten es gibt, die Seiten eines Würfel mit zwei verschiedenen Farben einzufärben. Ihnen fallen sicher viele Varianten dieser Frage ein, ob es die Möglichkeiten sind, wie chemische Elemente in einer Reaktion an ein gegebenes Molekül andocken können, die möglichen Armbänder mit gegebener Dekoration usw.

Lassen Sie uns zunächst beim Würfel bleiben: Ein Würfel hat 6 Flächen, also gibt es bei 2 Farben, sagen wir blau und grün, 2^6 mögliche Färbungen. Von diesen sind aber einige gleich, denn die 6 Möglichkeiten eine Seite blau und alle anderen grün einzufärben lassen, liefern alle den gleichen Würfel.

VERSUCHEN SIE einmal sich einen Überblick über alle Möglichkeiten zu verschaffen! Das ist gar nicht so einfach.

WENN WIR das Problem in Termen von Gruppenoperationen beschreiben, können wir leichter eine Methode finden, das systematisch anzugehen.

Dazu beschreiben wir das Problem so: Ist X die Menge der 2^6 möglichen Färbungen für die nummerierten Würfelflächen, so operiert die Automorphismengruppe G des Würfels auf X und die Menge der verschiedenen Würfel ist gerade die Menge der Bahnen $G\backslash X$.

Hat ein gefärbter Würfel gar keine Symmetrie, so taucht dieser $\#G$ mal in der Menge X auf, die beiden einfarbigen Würfel tauchen nur einmal auf, die Bahn hat $\frac{\#G}{\#\mathrm{Stab}_G(W)}$ Elemente. Würden wir also statt Würfeln Paare $(\text{Würfel}, g)$ mit $g \in \mathrm{Stab}_G(\text{Würfel})$ zählen, so würden alle Würfel genau $\#G$-mal auftauchen.

Umgekehrt tauchen für ein $g \in G$ in diesen Paaren ein Würfel W genau dann auf, wenn $g.W = W$. Diese Würfel können wir wieder leicht zählen, denn $g.W = W$ bedeutet gerade, dass die Flächen von W die unter g aufeinander abgebildet werden die gleiche Farbe haben müssen.

Bevor wir das ausführen, schreiben wir diese Diskussion noch einmal formal auf.

Notation 100. Ist $G \times X \to X$ eine Gruppenoperation und $g \in G$ ein Element, so schreiben wir

$$X^g := \{x \in X \mid g.x = x\}$$

für die Menge der Fixpunkte von g auf X.

Satz 101 (Bahnenformel)**.** *Operiert eine endliche Gruppe G auf einer endlichen Menge X, so gilt*

$$\#G\backslash X = \frac{1}{\#G} \sum_{g \in G} \#X^g,$$

d.h. $\#G$ mal Anzahl der Bahnen ist die Summe über die Anzahl der Fixpunkte der Elemente von G.

Bitte schauen Sie nach, dass wir im Beweis nur den Text vor der Formulierung des Satzes in Formeln umschreiben.

Beweis der Bahnenformel. Wir bezeichnen mit

$$I(X) := \{(x, g) \mid x \in X, g \in G, \text{ s.d. } g.x = x\}$$

die Menge der Paare von Elementen zusammen mit einem Element des Stabilisators. Die Elemente dieser Menge zählen wir auf zwei Arten: Entweder wir summieren erst über die Möglichkeiten für x

$$\begin{aligned}
\#I(X) &= \sum_{x \in X} \#\mathrm{Stab}_G(x) \\
&= \sum_{[x] \in G\backslash X} \#[x] \#\mathrm{Stab}_G(x) \\
&= \sum_{[x] \in G\backslash X} \frac{\#G}{\#\mathrm{Stab}_G(x)} \#\mathrm{Stab}_G(x) \\
&= \sum_{[x] \in G\backslash X} \#G = \#G\backslash X \cdot \#G.
\end{aligned}$$

oder über die Möglichkeiten von $g \in G$:

$$\#I(X) = \sum_{g \in G} \#X^g.$$

Also gilt

$$\#G\backslash X \cdot \#G = \sum_{g \in G} \#X^g.$$

□

Beispiel 102. Die Anzahl der mit zwei Farben gefärbten Würfel können wir mit der Formel berechnen: Sei X die Menge der Färbungen des Standardwürfels. Weil alle Elemente von $SO(3)$ Drehungen sind, sind die Elemente der Automorphismengruppe des Standardwürfels gerade:

1. Die Identität $e \in G$: Die Identität lässt jede Färbung unverändert, also $\#X^e = \#X = 2^5$.

2. Drehungen g um $\pm 90°$ um den Mittelpunkt einer Seitenfläche. Diese Drehung lässt eine Färbung genau dann unverändert, wenn die 4 Seiten, die bei der Drehung nicht fest gelassen werden, die gleiche Farbe haben. Mit, Deckel und Boden können wir also nur für 3 Bahnen eine Farbe wählen. Es gilt also
$$\#X^g = 2^3.$$
Von diesen Drehungen gibt es genau 6.

3. Drehungen um 180° um den Mittelpunkt einer Seitenfläche. Diese Drehung lässt eine Färbung genau dann unverändert wenn die beiden gegenüberliegenden Seiten die nicht auf der Drehachse liegen die gleiche Farbe haben: Es gilt also
$$\#X^g = 2^4.$$
Es gibt genau 3 solche Drehungen.

4. Drehungen um 120° um eine Raumdiagonale durch gegenüberliegende Ecken: Diese Drehung lässt eine Färbung genau dann unverändert wenn an die Ecken angrenzenden Flächen die gleiche Farbe haben: Es gilt also
$$\#X^g = 2^2.$$
Es gibt genau 8 solche Drehungen.

5. Drehungen um 180° um eine Achse durch zwei gegnüberliegende Kanten. Diese Drehung lässt eine Färbung genau dann unverändert wenn an die Kanten angrenzenden Flächen die gleiche Farbe haben und die beiden nicht angrenzenden Flächen ebenfalls die gleiche Farbe haben. Es gilt also
$$\#X^g = 2^3.$$
Es gibt genau 6 solche Drehungen.

Insgesamt finden wir also:

$$\begin{aligned}
\#G\backslash X &= \frac{1}{\#G} \cdot \sum_{g \in G} \#X^g \\
&= \frac{1}{24} \cdot \left(\underbrace{2^6}_{g=e} + \underbrace{6 \cdot 2^3}_{90°\text{Seite}} + \underbrace{3 \cdot 2^4}_{180°\text{Seite}} + \underbrace{8 \cdot 2^2}_{120°\text{Ecke}} + \underbrace{6 \cdot 2^3}_{180°\text{ Kante}} \right) \\
&= \frac{1}{3 \cdot 2^3}(3 \cdot 2^5 + 3 \cdot 2^4 + 12 \cdot 2^3) = 2^2 + 2 + 2^2 \\
&= 10.
\end{aligned}$$

Es gibt also 10 verschiedene Färbungen.

Zurück zur Galoiskorrespondenz: $\mathbb{Q}(\zeta_p)$ und das quadratische Reziprozitätsgesetz

Um Konstruktionen für regelmäßige p-Ecke zu finden, hatten wir zunächst einen quadratischen Körper $\mathbb{Q}(\sqrt{a}) \subseteq \mathbb{Q}(\zeta_p)$ gesucht und gefunden:

$p = 3$ $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$, denn $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$ ist selbst quadratisch und wir wissen $\zeta_3 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}, \zeta_3^2 = \overline{\zeta_3} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$. Also ist $\zeta_3 - \zeta_3^2 = i\sqrt{3} = \sqrt{-3}$ und damit $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$.

$p = 5$ $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\zeta_5)$, weil $(\zeta_5 + \zeta_5^4 - (\zeta_3^2 + \zeta_3^3))^2 = 5$.

$p = 17$ $\mathbb{Q}(\sqrt{17}) \subseteq \mathbb{Q}(\zeta_{17})$.

Das ging wie folgt:

1. Die Galoisgruppe

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)|\mathbb{Q}) \cong ((\mathbb{Z}/p\mathbb{Z})^*, \cdot) \cong (\mathbb{Z}/(p-1)\mathbb{Z}, +)$$

   ist überraschenderweise zyklisch (explizit konnten wir ein Erzeugendes aber jeweils nur durch Ausprobieren finden).

2. Nach der Galoiskorrepsondenz entsprechen quadratische Zwischenkörper gerade den Untergruppen $H < \mathrm{Gal}(\mathbb{Q}(\zeta_p)|\mathbb{Q})$ für die $\frac{\#\mathrm{Gal}(\mathbb{Q}(\zeta_p)|\mathbb{Q})}{\#H} = 2$ ist. Da die Untergruppen der zyklischen Gruppe $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$ die zyklischen Untergruppen $(d\mathbb{Z}/(p-1)\mathbb{Z}, +)$ für die Teiler d von $(p-1)$ sind, muss also $H = ((2\mathbb{Z}/(p-1)\mathbb{Z}), +)$ die Untergruppe von $\mathrm{Gal}(\mathbb{Q}(\zeta_p)|\mathbb{Q})$ sein, die vom Quadrat eines Erzeugenden $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)|\mathbb{Q})$ erzeugt wird.

3. Um den quadratischen Zwischenkörper $\mathbb{Q}(\zeta_p)^H$ als $\mathbb{Q}(\sqrt{d})$ zu schreiben, müssen wir also ein Element $\alpha \in \mathbb{Q}(\zeta_p)$ finden, das unter σ^2 invariant ist und für das $\sigma(\alpha) = -\alpha$ gilt, damit das Minimalpolynom $(x - \alpha)(x - \sigma(\alpha))$ von der Form $x^2 - d$ ist.

4. Da $(\mathbb{Q}(\zeta_p)|\mathbb{Q})$ der Zerfällungskörper des Minimalpolynoms von ζ_p ist, operiert die Galoisgruppe transitiv auf den Nullstellen $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$ des Minimalpolynoms $\Phi_p(x) = \frac{x^p-1}{x-1}$, d.h. die Bahn $\zeta_p, \sigma(\zeta_p), \ldots, \sigma^{p-1}(\zeta_p)$ ist eine Liste der Nullstellen und entsprechen hat das Element σ^2 auf dieser Menge zwei Bahnen

$$\{\sigma^{2k}(\zeta_p)\}_{k=0,\ldots,\frac{p-1}{2}-1}, \{\sigma^{2k+1}(\zeta_p)\}_{k=0,\ldots,\frac{p-1}{2}-1}.$$

   Das Element σ vertauscht diese beiden Mengen, also ist

$$\alpha := \underbrace{\sum_{k=0}^{\frac{p-1}{2}-1} \sigma^{2k}(\zeta)}_{\text{Summe über gerade Potenzen}} - \underbrace{\sum_{k=0}^{\frac{p-1}{2}-1} \sigma^{2k+1}(\zeta)}_{\text{Summe über Ungerade Potenzen}}$$

   ein Element von $\mathbb{Q}(\zeta_p)^H$ mit $\alpha^2 = d \in \mathbb{Q}$.

Dieses Element konnten wir in den Beispielen durch die Wahl eines expliziten Erzeugenden σ konkret bestimmen und damit (α^2) ausrechnen, wobei wir in dieser Berechnung jeweils genutzt haben, dass

$$\sum_{k=1}^{p-1} \zeta_p^k = -1$$

weil

$$\sum_{k=0}^{p-1} \zeta_p^k = 0.$$

Wenn Sie aus den Beispielen $p = 3, 5, 17$ noch kein Muster erkennen, sollten Sie ein paar weitere Beispiele ausrechnen, zum Beispiel

$p = 7$ $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{-7}) \subseteq \mathbb{Q}(\zeta_7)$,

$p = 11$ $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{-11}) \subseteq \mathbb{Q}(\zeta_{-11})$,

$p = 13$ $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{13}) \subseteq \mathbb{Q}(\zeta_{13})$.

VIELLEICHT ERKENNEN SIE in der Liste

$$\mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-11}), \mathbb{Q}(\sqrt{13}), \mathbb{Q}(\sqrt{17})$$

das Muster.

Behauptung 103. *Ist p eine ungerade Primzahl, so ist*

- *für $p \equiv 1 \mod 4$*
$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_p)$$
- *für $p \equiv 3 \mod 4$*
$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{-p}) \subseteq \mathbb{Q}(\zeta_p)$$

der eindeutig bestimmte quadratische Unterkörper von $\mathbb{Q}(\zeta_p)$.

Beweis. Wir haben uns gerade überlegt, dass wenn $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)) \cong (\mathbb{F}_p^*, \cdot)$ ein erzeugendes Element ist, das Element

$$\alpha := \underbrace{\sum_{k=0}^{\frac{p-1}{2}-1} \sigma^{2k}(\zeta_p)}_{\text{Summe über gerade Potenzen}} - \underbrace{\sum_{k=0}^{\frac{p-1}{2}-1} \sigma^{2k+1}(\zeta_p)}_{\text{Summe über ungerade Potenzen}}$$

die quadratische Erweiterung erzeugt und $\alpha^2 = d \in \mathbb{Q}$ ist.

Da wir die Galoisautomorphismen $\zeta_p \to \zeta_p^k$ für $k \in \mathbb{F}_p^*$ gut kennen, aber die Erzeugenden σ nicht, ist es praktisch sich zu überlegen, dass wir die Summen in obigem Ausdruck gut kennen:

Beobachtung: Für $b \in \mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$ ist ζ_p^b genau dann von der Form $\sigma^{2k}(\zeta_p)$ – also ein Summand in der geraden Summe – wenn p ein Quadrat in $\mathbb{F}_p^*$ ist. Andernfalls ist ζ_p^k von der Form $\sigma^{2k+1}(\zeta_p)$.

Das ist relativ klar, denn unter dem Isomorphismus $\phi\colon (\mathbb{F}_p^*, \cdot) \xrightarrow{\cong} (\mathbb{Z}/p-1\mathbb{Z}, +)$ übersetzt sich $b = c^2$ in $\phi(c \cdot c) = \phi(c) + \phi(c) = 2\phi(c)$.

Also entsprechen die Quadrate in $\mathbb{F}_p^*$ genau den Elementen von $2\mathbb{Z}/(p-1)\mathbb{Z} \subset \mathbb{Z}/(p-1)\mathbb{Z}$.

Also können wir die Summe umschreiben:

$$\begin{aligned}\alpha &= \underbrace{\sum_{k=0}^{\frac{p-1}{2}-1} \sigma^{2k}(\zeta_p)}_{\text{Summe über gerade Potenzen}} - \underbrace{\sum_{k=0}^{\frac{p-1}{2}-1} \sigma^{2k+1}(\zeta_p)}_{\text{Summe über ungerade Potenzen}} \\ &= \sum_{\substack{b\in\mathbb{F}_p^* \\ b \text{ Quadrat}}} \zeta_p^b - \sum_{\substack{b\in\mathbb{F}_p^* \\ b \text{ kein Quadrat}}} \zeta_p^b.\end{aligned}$$

Notation 104 (Quadratisches Restsymbol)**.** Für $[a] \in (\mathbb{Z}/p\mathbb{Z})^*$ notieren wir

$$\left(\frac{a}{p}\right) := \begin{array}{ll} 1 & a \text{ Quadrat modulo } p \\ -1 & a \text{ kein Quadrat modulo } p \end{array}$$

und nennen diesen Ausdruck das quadratische Restsymbol.

Für $[a] = 0 \in \mathbb{Z}/p\mathbb{Z}$ wird häufig $\left(\frac{a}{p}\right) := 0$ definiert, weil das in den Rechnungen gut passt. Das brauchen wir aber nicht.

Also ist

$$\alpha = \sum_{b\in\mathbb{F}_p^*} \left(\frac{b}{p}\right) \zeta_p^b.$$

Zum Rechnen – und das Muster im Satz – sind zwei Rechenregeln für das Restsymbol nützlich:

1. Für alle a, b gilt:
$$\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$
denn die Aussage „ein Produkt ist genau dann ein Quadrat in $\mathbb{F}_p$, wenn entweder beide oder keiner der Faktoren Quadrate sind“ übersetzt sich in $\mathbb{Z}/(p-1), +$ in die Aussage, dass eine Summe von zwei Elementen genau dann gerade ist, wenn entweder beide Summanden gerade, oder beide Summanden ungerade sind.

2. Für ungerade Primzahlen p gilt
$$\left(\frac{-1}{p}\right) = \begin{array}{ll} 1 & p \equiv 1 \mod 4 \\ -1 & p \equiv 3 \mod 4 \end{array}$$
Das folgt einfach weil für ein Erzeugendes a gilt, dass $(a^{\frac{p-1}{2}})^2 = 1$ ist aber $a^{\frac{p-1}{2}} \neq 1$, also $a^{\frac{p-1}{2}} = -1$. Damit ist -1 genau dann ein Quadrat wenn $\frac{p-1}{2} = 2k$ gerade ist, d.h wenn $p = 4k+1$ gilt.

Die Primzahlen $p \equiv 1 \mod 4$ sind im übrigen auch genau die Primzahlen, die sich als Summe von zwei Quadraten $p = a^2 + b^2$ schreiben lassen,

$$5 = 1+4, 13 = 4+9, 17 = 1+16, \ldots.$$

Das ist eine schöne Knobelaufgabe, die Sie mit etwas Algebra herausbekommen können.

Lassen Sie uns nun endlich $\alpha^2 = \left(\frac{-1}{p}\right) p$ ausrechnen:

$$\begin{aligned}\alpha^2 &= \left(\sum_{b\in\mathbb{F}_p^*} \left(\frac{b}{p}\right) \zeta_p^b\right)^2 \\ &= \sum_{a,b\in\mathbb{F}_p^*} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \zeta_p^a \zeta_p^b \\ &= \sum_{a,b\in\mathbb{F}_p^*} \left(\frac{ab}{p}\right) \zeta_p^{a+b}\end{aligned}$$

Diesen Ausdruck würde ich gerne nach $\left(\frac{ab}{p}\right)$ sortieren. Setzen wir $a' = a/b$ ist:

Das ist ein guter Trick, der erste Versuch wäre $a' = ab$, was nicht so glatt funktioniert.

$$\begin{aligned}\alpha^2 &= \sum_{a,b\in\mathbb{F}_p^*}\left(\frac{ab}{p}\right)\zeta_p^{a+b}\\ &= \sum_{a'\in\mathbb{F}_p^*}\left(\frac{a'b^2}{p}\right)\sum_{b\in\mathbb{F}_p'}\zeta_p^{a'b+b}\\ &= \sum_{a'\in\mathbb{F}_p^*}\left(\frac{a'}{p}\right)\sum_{b\in\mathbb{F}_p'}\zeta_p^{a'b+b}\\ &= \sum_{a'\in\mathbb{F}_p^*}\left(\frac{a'}{p}\right)\sum_{b\in\mathbb{F}_p'}(\zeta_p^{a+1})^b\end{aligned}$$

nun ist aber ζ_p^{a+1} für $a \neq -1$ eine primitive p-te Einheitswurzel und für $a = -1$ ist $\zeta_p^{a+1} = \zeta_p^0 = 1$, also gilt

$$\begin{aligned}\alpha^2 &= \sum_{a'\in\mathbb{F}_p^*}\left(\frac{a'}{p}\right)\sum_{b\in\mathbb{F}_p'}(\zeta_p^{a+1})^b\\ &= \left(\sum_{\substack{a'\in\mathbb{F}_p^*\\ a\neq -1}}\left(\frac{a'}{p}\right)\underbrace{\sum_{b\in\mathbb{F}_p'}(\zeta_p^{a+1})^b}_{=-1}\right) + \left(\frac{-1}{p}\right)\sum_{b\in\mathbb{F}_p^*}1\\ &= \left(\sum_{\substack{a'\in\mathbb{F}_p^*\\ a\neq -1}}\left(\frac{a'}{p}\right)(-1)\right) + \left(\frac{-1}{p}\right)(p-1)\\ &= \left(\sum_{a'\in\mathbb{F}_p^*}\left(\frac{a'}{p}\right)\right)\cdot(-1) + \left(\frac{-1}{p}\right)p\\ &= \left(\frac{-1}{p}\right)p.\end{aligned}$$

Hierbei folgt die letzte Gleichung daraus, dass es in $\mathbb{F}_p$ genauso viele Quadrate wie nicht Quadrate gibt (die beiden Summen in der Definition von α hatten gleich viele Summanden. Damit ist also

$$\alpha = \sum_{b\in\mathbb{F}_p^*}\left(\frac{b}{p}\right)\zeta_p^b = \sqrt{\left(\frac{-1}{p}\right)p}.$$

□

Aus diesem Resultat lässt sich ein sehr überraschendes Ergebnis – das quadratische Reziprozitätsgesetz – ableiten. Für ungerade Primzahlen p, ℓ haben die Fragen ob ℓ ein Quadrat modulo p ist, bzw. ob p ein Quadrat modulo ℓ ist zunächst keinen rechten Zusammenhang. Wenn Sie das in Beispielen anschauen, müssen Sie eine Weile probieren, bevor Sie ein Muster erkennen:

Satz 105 (Quadratisches Reziprozitätsgesetz)**.** *Sind p, ℓ zwei ungerade Primzahlen, so gilt*

$$\left(\frac{\ell}{p}\right) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}} \left(\frac{p}{\ell}\right).$$

Bemerkung. Der Faktor $(-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}$ ist nur dann -1 wenn $\frac{p-1}{2}, \frac{\ell-1}{2}$ beide ungerade sind, d.h. wenn p und ℓ beide kongruent 3 modulo 4 sind.

Das lässt sich auch als $\left(\frac{\ell}{p}\right) = \left(\frac{\left(\frac{-1}{p}\right)p}{\ell}\right)$ formulieren.

Dieses Resultat hat eine lange Geschichte. Euler hatte als erster das Muster erkannt, aber ein vollständiger Beweis gelang erst Gauss, der das Resultat gerne besser verstehen wollte und darum nach immer neuen Beweisen gesucht hat.

Zum Abschluss der Vorlesung möchte ich für dieses Ergebnis gerne einen Beweis vorstellen, der die Galoiskorrespondenz verwendet und damit einen Ausblick auf ein sehr allgemein vermutetes aber noch immer nicht ganz verstandenes Phänomen liefert, das einen sehr merkwürdigen Zusammenhang zwischen der Struktur von Galoisgruppen von Körpererweiterungen und der Arithmetik des Körpers selbst gibt – genannt Langlands-Korrespondenz. Das quadratische Reziprozitätsgesetz war die Keimzelle hiervon.

Im Beweis werden Sie sehen, dass wir einerseits $(\mathbb{Z}/p\mathbb{Z})^*$ als Galoisgruppe interpretieren und andererseits $(\mathbb{Z}/\ell\mathbb{Z})$ als Quotient von $\mathbb{Z} \subseteq \mathbb{Q}$, also als Objekt das zum Körper gehört.

Beweis. Nach unserer Berechnung des quadratischen Unterkörpers von $\mathbb{Q}(\zeta_p)$ ist die Zahl ℓ genau dann ein Quadrat in $\mathbb{F}_p^*$ wenn der zugehörige Körperautomorphismus σ_ℓ der durch $\zeta_p \mapsto \zeta_p^\ell$ bestimmt ist, das Element $\sqrt{\left(\frac{-1}{p}\right)p}$ fest lässt, also

$$\sigma_\ell(\sqrt{\left(\frac{-1}{p}\right)p}) = \sqrt{\left(\frac{-1}{p}\right)p}.$$

Der Automorphismus σ_ℓ permutiert die p-ten Einheitswurzeln und definert daher auch einen Automorphismus von

$$\mathbb{Z}(\zeta_p) = \mathbb{Z}[x]/(x^{p-1} + \cdots + x^2 + x + 1) \subset \mathbb{Q}(\zeta_p)$$

und

$$\sqrt{\left(\frac{-1}{p}\right)p} = \sum_{b \in \mathbb{F}_p^*} \left(\frac{b}{p}\right) \zeta_p^b \in \mathbb{Z}(\zeta_p).$$

Rechnen wir nun modulo ℓ, so erhalten wir einen Isomporphismus

$$\overline{\sigma_\ell} \colon \mathbb{F}_\ell[x]/(x^{p-1} + \cdots + x^2 + x + 1) \to \mathbb{F}_\ell[x]/(x^{p-1} + \cdots + x^2 + x + 1)$$

für den $\overline{\sigma_\ell}([x]) = [x]^\ell$ ist. Weil für alle Elemente $c \in \mathbb{F}_\ell$ gilt dass $c^\ell = c$ ist, ist $\overline{\sigma_\ell}$ einfach der Frobeniushomomorphismus $\overline{\sigma_\ell}([f]) = [f]^\ell$.

Wegen unserer Formel für $\sqrt{\left(\frac{-1}{p}\right)p}$ wir wissen auch, dass $\mathbb{F}_\ell(\sqrt{\left(\frac{-1}{p}\right)p}) \subseteq \mathbb{F}_\ell[x]/(x^{p-1}+\cdots+x^2+x+1)$. Aber die Fixpunkte des Frobenius $f \mapsto f^\ell$ auf einer Körpererweiterung sind genau der Körper $\mathbb{F}_\ell$ selbst, d.h. $[\sqrt{\left(\frac{-1}{p}\right)p}]$ ist genau dann unter $f \mapsto f^\ell$ invariant wenn $\left(\frac{-1}{p}\right)p$ ein Quadrat in $\mathbb{F}_\ell$ ist.

Also ist ℓ genau dann ein Quadrat modulo p wenn $\left(\frac{-1}{p}\right)p$ ein Quadrat in $\mathbb{F}_\ell$ ist. Das war zu zeigen. □

Rückblick: Welche allgemeinen Konzepte und Resultate haben wir gelernt?

Um die Galoiskorrespondenz anzuwenden, sind wir einer Reihe von Techniken und Begriffen begegnet:

1. Gruppen und Gruppenoperationen
   - Zyklische Gruppen
   - Normalteiler
   - Auflösbare Gruppen
   - Einfache Gruppen
   - Das Zentrum einer Gruppe
   - Kommutatoruntergruppe (Beispiele für S_n und A_n)
   - Gruppenoperationen
   - Stabilisatoren, Bahnen, Fixpunkte
   - Normalisator einer Untergruppe
   - Bahnen-Stabilisator-Formel
   - Bahnenformeln
   - Sylowsätze
   - Konjugation, Konjugationsklassen
   - Auflösbarkeit von Gruppen der Ordnung p^n
   - Die alternierenden Gruppen A_n sind für $n \geq 5$ einfach.
2. Kreisteilung und Einheitswurzeln
   - Welche regelmäßigen n-Ecke sind konstruierbar?
   - Körpergrad und Galoisgruppe von $\mathbb{Q}(\zeta_N)|\mathbb{Q}$
   - Eulersche φ-Funktion
   - Kreisteilungspolynome
   - Galoisgruppe von Wurzel-Erweiterungen
3. Körpererweiterungen
   - Galoiserweiterungen (verschiedene Charakterisierungen)
   - Normale Erweiterungen

- Zusammenhang: Normalteiler und normale Erweiterungen
- Abelsche Erweiterungen
- Radikalerweiterungen
- Auflösbarkeit von Körpererweiterungen
- Minimalpolynome und Bahnen von Elementen in Galoiserweiterungen

4. Endliche Körper
   - Konstruktion aller endlichen Körper
   - Multiplikative Gruppe eines endlichen Körpers ist zyklisch
   - $\mathbb{F}_{256}$ steckt in QR-Codes.

Glossar mathematischer Symbole und Begriffe

$[L : K]$ Grad der Körpererweiterung $L|K$

$\dot\cup$ disjunkte Vereinigung, $M = A \dot\cup B$ bedeutet

$$M = A \cup B \text{ und } A \cap B = \varnothing.$$

$H < G$ H ist Untergruppe von G

$N \lhd G$ N ist Normalteiler in G.

$[G : G]$ Kommutatoruntergruppe von G.

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.