Algebra, WS 2021/22

Ulrich Görtz

Version vom 3. Juli 2022.

Online-Version des Skripts: https://math.ug/algebra-ws2122/

Ulrich Görtz

Universität Duisburg-Essen
Fakultät für Mathematik
45117 Essen

ulrich.goertz@uni-due.de

Ich freue mich über Kommentare und Berichtigungen.

Ich bedanke mich für Bemerkungen/Korrekturen bei Lukas Fußangel, Johannes Höffner, Jan Renner.

Gesetzt in der Schrift Vollkorn[3] von F. Althausen mit LuaLaTeX, TikZ und anderen TEX-Paketen. Einige Abbildungen wurden mit IPE[4] erstellt. Die HTML-Version wird mit plasTeX[5] erzeugt.

[1] https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.de
[2] https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de
[3] http://vollkorn-typeface.com/
[4] http://ipe.otfried.org/
[5] https://github.com/plastex/plastex

Inhaltsverzeichnis

KAPITEL 1

Einleitung

1.1. Inhalt der Vorlesung

Die Vorlesung *Algebra* besteht aus meiner Sicht im wesentlichen aus

- der Untersuchung von Körpern und sogenannten Körpererweiterungen; im Fokus steht dabei die Frage, wann ein Polynom in einer Unbestimmten mit Koeffizienten in einem Körper K in K oder einem Erweiterungskörper von K eine Nullstelle hat (oder sogar vollständig in Linearfaktoren zerfällt) und
- zu diesem Zweck einem (im Vergleich zur Linearen Algebra) systematischeren Studium des Begriffs der Gruppe, das wir an den Anfang der Vorlesung stellen.

Ein Erweiterungskörper eines Körpers K ist ein Körper L, derart dass K ein Teilkörper von L ist, d.h. es gilt $K \subseteq L$ und die Addition und Multiplikation auf K sind durch Einschränkung der entsprechenden Verknüpfungen auf L gegeben. Wir nennen das Paar $K \subseteq L$ dann auch eine *Körpererweiterung* und schreiben oft L/K.

Neben den konkreten Sätzen (siehe unten) ist ein wichtiges Lernziel der Vorlesung der Umgang mit »abstrakten mathematischen Strukturen«. An mehreren Stellen ist der Abstraktionsgrad höher als in der Linearen Algebra, das bedeutet, dass es schwieriger ist, ein »Gefühl« für die entsprechenden Begriffe zu entwickeln, damit man wirklich mit ihnen umgehen kann. Zusätzlich ist es so, dass der Stoff der Algebra-Vorlesung (wie bei fast allen Mathematik-Vorlesungen, und ähnlich wie in anderen Fächern) über ungefähr 200 Jahre hin immer weiter optimiert und in eine stromlinienförmige Gestalt gebracht wurde. Das hat den Vorteil, dass man in der zur Verfügung stehenden Zeit zu mehreren wichtigen und teilweise (mathematisch gesehen) spektakulären Ergebnissen kommen kann, deren Beweise alles andere als offensichtlich sind, aus vielen Schritten bestehen und in teils überraschender Art verschiedene Konzepte zusammenbringen. Der Nachteil liegt allerdings auch auf der Hand: Es ist nicht von vorneherein offensichtlich, welche Bedeutung einige Ergebnisse aus der ersten Vorlesungshälfte später haben werden und warum dieser oder jener Begriff überhaupt eingeführt wird (auch wenn ich mir Mühe geben werde, das jeweils an Ort und Stelle zu motivieren).

Außerdem spiegelt so eine Vorlesung nicht wider, wie sich eine mathematische Theorie entwickelt. Das könnte man mit einer Stadtführung vergleichen, wo typischerweise nur die schönen und besonders sehenswerten Ecken gezeigt werden, aber nicht die Sackgassen mit den heruntergekommenen Häusern…

> Mathematik ist kein vorsichtiger Gang auf einer gut geräumten Straße, sondern eine Reise in eine fremde Wildnis, in der sich die Entdecker oft verlaufen.
>
> W.S. Anglin

Dennoch ist es, um Mathematik zu lernen, wichtig, auf eigene Faust auch einmal Sackgassen und Irrwege kennenzulernen, Fehler zu machen, *eigene* Beweise zu finden (auch wenn sie im Nachhinein betrachtet vielleicht unnötig umständlich sind), usw. Auch das muss und wird in der Veranstaltung abgedeckt werden, und zwar – Sie ahnen es wahrscheinlich – durch die Bearbeitung der Hausaufgaben und den Besuch der Übungsgruppen.

Damit, dass die Ergebnisse tiefliegender sind als in den Anfängervorlesungen, geht einher, dass sie weiter entfernt sind von konkreten Anwendungen. Während Methoden der Linearen Algebra »überall« benötigt werden, ist beispielsweise die Tatsache, dass das regelmäßige 17-Eck mit Zirkel und Lineal konstruierbar ist, nicht jedoch das regelmäßige 7-Eck, zwar die Lösung eines mathematischen Problems, das die Mathematik seit über 2000 Jahren beschäftigt hat, und auch insofern interessant, als der Lösungsweg unerwartet und trotz seiner Komplexität auch extrem elegant ist. Für die Praxis hat diese Sache aber keinerlei Bedeutung. Es gibt zwar durchaus Anwendungen, die auf den Ergebnissen der Algebra bzw. auf darauf aufbauenden Theorien beruhen (die Kryptographie mit elliptischen Kurven ist ein häufig genanntes Beispiel, auch in der Kodierungstheorie spielt die Theorie der (endlichen) Körper eine Rolle), aber diese benötigen dann oft noch deutlich mehr Theorie (zum Beispiel die algebraische Geometrie). Daher beschäftigen sich auch die *Ergänzungen* im Skript größtenteils mit innermathematischen Themen und Ausblicken.

> Es kann nicht geleugnet werden, daß ein großer Teil der elementaren Mathematik von erheblichem praktischen Nutzen ist. Aber diese Teile der Mathematik sind, insgesamt betrachtet, ziemlich langweilig. Dies sind genau diejenigen Teile der Mathematik, die den geringsten ästhetischen Wert haben. Die »echte« Mathematik der »echten« Mathematiker, die Mathematik von Fermat, Gauß, Abel und Riemann ist fast völlig »nutzlos«.
>
> G. H. Hardy[a]

[a] Zur Sicherheit der Hinweis: Die im Skript eingestreuten Zitate sollten in erster Linie zur Auflockerung dienen. Auch wenn ich jedenfalls bei den meisten davon finde, dass sie einen wahren Kern haben oder es wenigstens lohnenswert ist, darüber nachzudenken, wie die jeweilige Aussage gemeint ist, stimme ich definitiv nicht jedem zu.

> Alle Pädagogen sind sich darin einig: Man muß vor allem tüchtig Mathematik treiben, weil ihre Kenntnis fürs praktische Leben größten direkten Nutzen gewährt.
>
> Felix Klein

Das soll aber nicht heißen, dass die Themen dieser Vorlesung nicht interessant wären – im Gegenteil ist aus meiner Sicht die *Algebra* eine der schönsten Vorlesungen des Mathematikstudiums, weil, wie schon angedeutet, die Lösungen mehrerer Probleme erklärt werden können, die über Jahrhunderte Mathematiker∗innen fasziniert haben und die mit der Theorie der Galois-Erweiterungen sehr durchsichtig dargestellt werden können. Die Kraft der mathematischen Abstraktion kommt hier noch weitaus stärker zum Tragen als in der Linearen Algebra (oder den Anfängervorlesungen der Analysis), wo die allermeisten Begriffe und Ergebnisse (auch) einen konkreten, »rechnerischen« Zugang erlauben.

1.2. Wichtige Sätze und Folgerungen

Einige wichtige Sätze, die wir im Laufe der Vorlesung beweisen werden, sind die folgenden. Zum Teil fehlt uns im Moment allerdings noch die Terminologie, um ihren Inhalt präzise zu beschreiben.

- Die Sylow-Sätze geben über die Untergruppen einer Gruppe Aufschluss, deren Ordnung eine Primzahlpotenz ist.
- Der Satz von Gauß besagt, dass der Polynomring über einem faktoriellen Ring selbst faktoriell ist und gibt eine genaue Beschreibung der irreduziblen Elemente darin (in Termen der Irreduzibilität im Polynomring über dem Quotientenkörper des Grundrings).
- Sind $K \subseteq L \subseteq M$ Teilkörper, und ist $x \in M$ Nullstelle eines normierten Polynoms mit Koeffizienten in L, so dass jeder dieser Koeffizienten Nullstelle eines normierten Polynoms mit Koeffizienten in K ist, so ist auch x Nullstelle eines normierten Polynoms mit Koeffizienten in K.
- Ist K ein Körper, so existiert ein algebraisch abgeschlossener Erweiterungskörper von K.
- Zu jeder Primzahlpotenz $q = p^r$ (mit $r \geq 1$) existiert ein Körper mit q Elementen (und dieser ist bis auf Isomorphie eindeutig bestimmt).
- Der *Hauptsatz der Galois-Theorie*, der eine Bijektion zwischen den Zwischenkörpern einer galoisschen Körpererweiterung und den Untergruppen der sogenannten Galois-Gruppe dieser Erweiterung angibt und damit einen Zusammenhang zwischen der Theorie der Körpererweiterungen und der Gruppentheorie herstellt.

Als »Anwendungen« werden wir am Ende der Vorlesung dann

- einen Beweis des Fundamentalsatzes der Algebra geben (also zeigen, dass der Körper der komplexen Zahlen algebraisch abgeschlossen ist), der nur ganz wenige Zutaten aus der Analysis benötigt (dass es ganz ohne Analysis nicht gehen kann, ist insofern klar, als die komplexen Zahlen von ihrer Natur aus ein »analytisches« Objekt sind),
- zeigen, dass es Polynomgleichungen mit Koeffizienten in $\mathbb{Q}$ gibt, deren Nullstellen (in $\mathbb{R}$ bzw. $\mathbb{C}$) nicht mit den Grundrechenarten und dem Ziehen n-ter Wurzeln hingeschrieben werden können. (Man sagt, diese Gleichungen seien nicht »auflösbar durch Radikale«.) Insbesondere kann es keine allgemeine Lösungsformel ähnlich der Lösungsformel für quadratische Gleichungen im allgemeinen Fall geben. Wir werden auch sehen, warum dieses Phänomen nur in Grad ≥ 5 auftritt (und Methoden entwickeln, mit denen man die bekannten Lösungsformeln für Polynome vom Grad 3 und vom Grad 4 systematisch herleiten kann). Siehe auch die Einführung des Buchs [**Bo-A**] von Bosch, in dem das Thema ausführlich und auch aus historischer Sicht beleuchtet wird.
- Wir werden verschiedene klassische Konstruktionsprobleme (»Konstruktion mit Zirkel und Lineal«) diskutieren und zum Beispiel sehen, dass die Verdoppelung des Würfels nicht möglich ist, dass der Satz von Lindemann über die Transzendenz von π zeigt, dass die *Quadratur des Kreises* unmöglich ist, und ein Kriterium dafür beweisen, dass das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar ist.
- Einen konzeptionellen Beweis des quadratischen Reziprozitätsgesetzes geben, eines Grundpfeilers der Zahlentheorie, das in der Klassenkörpertheorie weitreichend verallgemeinert wird und insofern als Wegweiser auch für aktuelle Forschung in Zahlentheorie und benachbarten Gebieten betrachtet werden kann.

Sie sehen ja aus, als hätten Sie die Quadratur des Kreises gelöst!

Dies sagte (angeblich ...[a]) Oberstleutnant von dem Busche zu seinem Freund Ferdinand Lindemann[b], als er ihn eines Abends in außergewöhnlich guter Stimmung antraf. Der Grund für Lindemanns gute Laune war, dass er just an diesem Tag die Transzendenz (Definition 4.9) der Kreiszahl π bewiesen hatte. Wie wir sehen werden (und wie Lindemann natürlich wusste) folgt daraus mit der Theorie der Körpererweiterungen, wie wir sie in der Vorlesung kennenlernen werden, dass die »Quadratur des Kreises mit Zirkel und Lineal« nicht möglich ist (Satz 4.47).

[a] `https://epub.ub.uni-muenchen.de/4546/1/4546.pdf`
[b] `https://de.wikipedia.org/wiki/Ferdinand_von_Lindemann`

1.3. Vorkenntnisse

Gute Kenntnisse der Linearen Algebra werden benötigt, allerdings weniger die »Feinheiten« der Theorie von Vektorräumen und ihrer Homomorphismen (auch wenn der Dimensionsbegriff, mit dem wir den *Grad* einer Körpererweiterung definieren werden, wichtig ist und wir auch auf die Eigenwerttheorie für Vektorraumendomorphismen zurückgreifen werden), sondern vor allem:

- der Begriff der Gruppe,
- der Begriff des (kommutativen) Rings und des Körpers, und zum Beispiel des Polynomrings, des Quotientenkörpers eines Integritätsrings und des faktoriellen Rings,
- die Konstruktion des Quotienten einer Gruppe nach einem Normalteiler und eines Rings nach einem Ideal (und seine Eigenschaften, vor allem der Homomorphiesatz).

Menschen, die von der Algebra nichts wissen, können sich auch nicht die wunderbaren Dinge vorstellen, zu denen man mit Hilfe der genannten Wissenschaft gelangen kann.

G. W. Leibniz

Auch wenn wir die in der Linearen Algebra schon behandelten Themen teilweise wiederholen werden, werden diese ziemlich schnell abgehandelt, und es ist wichtig, dass Sie, was diese Begriffe angeht, schnell »arbeitsfähig« sind, also mit diesen Begriffen ohne langes Nachdenken umgehen können, weil wir weiter darauf aufbauen werden. Das gilt in besonderem Maße für die Quotienten von Gruppen und Ringen. Diese spielen in allen Kapiteln eine sehr wichtige Rolle – wiederholen Sie gegebenenfalls noch einmal, was wir in der Linearen Algebra dazu schon gelernt haben. Die Bildung des Quotienten eines Vektorraums nach einem Untervektorraum kann hier vielleicht auch noch einmal nützlich sein, weil sie besser geometrisch veranschaulicht werden kann.

Als konkrete Beispiele von Körpern sollten Ihnen $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ und die Körper $\mathbb{F}_p$ (p eine Primzahl) geläufig sein.

Aus der Analysis benötigen wir nicht viel. In Abschnitt 5.5.3 benutzen wir den Zwischenwertsatz aus der reellen Analysis. In der zweiten Vorlesungshälfte ist es nützlich, grundlegende Eigenschaften der komplexen Exponentialfunktion $\exp\colon \mathbb{C} \to \mathbb{C}^\times$ zu kennen; insbesondere werden uns die sogenannten n-ten Einheitswurzeln $\exp(\frac{2\pi ki}{n})$ ($n \in \mathbb{N}_{>0}$, $k \in \{0, \ldots, n-1\}$) begegnen, die so heißen, weil es genau die Zahlen in $\mathbb{C}$ sind, deren n-te Potenz gleich 1 ist.

KAPITEL 2

Gruppen

2.1. Gruppen, Gruppenhomomorphismen, Untergruppen

Wir beginnen die Vorlesung Algebra damit, den Begriff der Gruppe, den wir in der Linearen Algebra bereits kennengelernt haben, etwas systematischer und ausführlicher zu studieren.

2.1.1. Vorkenntnisse. Sie sollten jedenfalls die Definition einer Gruppe, von kommutativen bzw. abelschen Gruppen, von Gruppenhomomorphismen und -isomorphismen, und von Kern und Bild eines Gruppenhomomorphismus kennen. Beispiele für Gruppen, die in der Linearen Algebra eine Rolle gespielt haben, sind insbesondere die symmetrischen Gruppen S_n und die allgemeine und spezielle lineare Gruppe über einem Körper K, $GL_n(K)$ und $SL_n(K)$. Wichtige Gruppenhomomorphismen waren die Signumabbildung sgn: $S_n \to \{1, -1\}$ sowie die Determinante $GL_n(K) \to K^\times$. Schauen Sie gegebenenfalls noch einmal in die Skripte zur LA1 (Kapitel LA1.8) und LA2 (Abschnitt LA2.18.3).

Für Gruppen G und H bezeichnen wir mit $\mathrm{Hom}(G,H)$ (oder mit $\mathrm{Hom}_{\mathrm{Gruppen}}(G,H)$, wenn wir betonen wollen, dass wir Homomorphismen *von Gruppen* betrachten) die Menge aller Gruppenhomomorphismen $G \to H$.

Wir haben gezeigt, dass ein Gruppenhomomorphismus genau dann ein Isomorphismus ist, wenn er bijektiv ist, und dass ein Gruppenhomomorphismus genau dann injektiv ist, wenn er trivialen Kern hat.

Eine Teilmenge H einer Gruppe G heißt eine Untergruppe, wenn H nicht leer ist und bezüglich der Gruppenverknüpfung und bezüglich der Bildung des Inversen abgeschlossen ist. Das ist genau dann der Fall, wenn die Verknüpfung auf G auf H eine Verknüpfung induziert, für die die Gruppenaxiome erfüllt sind.

Der Durchschnitt von Untergruppen einer Gruppe ist wieder eine Untergruppe. Ist $M \subseteq G$ eine Teilmenge einer Gruppe G, so ist also der Durchschnitt aller Untergruppen von G, die M enthalten, eine Untergruppe von G, und zwar die kleinste Untergruppe, die M enthält. Wir bezeichnen sie mit $\langle M\rangle$ und nennen sie die *von M erzeugte Untergruppe*.

Ein wichtiger Spezialfall, den wir in Abschnitt 2.4 genauer untersuchen werden, ist der, dass M aus einem einzigen Element $g \in G$ besteht. In diesem Fall ist (für multiplikativ geschriebenes G)

$$\langle g\rangle := \langle\{g\}\rangle = \{g^i;\ i \in \mathbb{Z}\}$$

die Menge aller Potenzen $1 = g^0, g, g^2, g^3, \ldots, g^{-1}, g^{-2} := (g^{-1})^2, \ldots$ von g. Dabei kann es natürlich, je nach Gruppe und gewähltem Element, passieren, dass einige dieser Potenzen gleich sind (und dann ist $\langle g\rangle$ eine endliche Menge).

Wir schreiben, wenn nichts anderes gesagt wird, in diesem Kapitel Gruppen multiplikativ, schreiben also die Gruppenverknüpfung als Multiplikation ($g \cdot h$ oder einfach gh). (Gruppen wie $\mathbb{Z}$ und die Quotienten $\mathbb{Z}/n$ sind aber natürlich Gruppen bezüglich der Addition und werden auch additiv geschrieben.)

2.1.2. Beispiele von Gruppen. Allgemein und besonders in der Algebra-Vorlesung sind Gruppen wichtig, die aus Bijektionen einer Menge auf sich bzw. aus den Automorphismen eines Objekts bestehen. Auch aus historischer Sicht war die Betrachtung solcher Bijektionen entscheidend für die Entwicklung des Gruppenbegriffs.

BEISPIEL 2.1 (Gruppen bijektiver Abbildungen). (1) Sei X eine Menge. Die Menge $\mathrm{Bij}(X)$ aller bijektiven Abbildungen $X \to X$ ist mit der Komposition von Abbildungen $\mathrm{Bij}(X) \times \mathrm{Bij}(X) \to \mathrm{Bij}(X)$ als Verknüpfung eine Gruppe.

(2) Ist speziell $X = \{1, \ldots, n\}$ für $n \in \mathbb{N}$, so nennen wir $S_n := \mathrm{Bij}(\{1, \ldots, n\})$ die *symmetrische Gruppe*. Siehe auch Abschnitt 2.5.

$\Diamond$

Als Variante der vorherigen Beispielklasse können wir sogenannte Automorphismengruppen von Objekten betrachten, die eine zusätzliche Struktur haben, die zu einem Begriff von Homomorphismus führt.

BEISPIEL 2.2 (Automorphismengruppen). Zu jedem Homomorphismusbegriff (also für Gruppen, Ringe, Vektorräume) haben wir den Begriff von Isomorphismen (d.h. Homomorphismen, die einen Umkehrhomomorphismus besitzen) und Automorphismen (d.h. Isomorphismen, deren Definitions- und Wertebereich übereinstimmen).

Für ein Objekt X mit der gegebenen Struktur (also zum Beispiel eine Gruppe X; oder einen Vektorraum X über einem Körper) setzen wir

$$\mathrm{Aut}(X) = \{f \colon X \to X;\, f \text{ Automorphismus}\}.$$

Die Verkettung von Automorphismen von X ist wieder ein Automorphismus, die Identitätsabbildung von X ist ein neutrales Element bezüglich der Verkettung, und jeder Automorphismus besitzt nach Definition ein Inverses bezüglich der Verkettung. Daher ist $\mathrm{Aut}(X)$ bezüglich der Verkettung von Abbildungen eine Gruppe, die sogenannte Automorphismengruppe von X.

Wenn erforderlich, können wir die Art von Homomorphismen, die wir betrachten möchten, als Index angeben, zum Beispiel $\mathrm{Aut}_{\mathrm{Gruppen}}(X)$ oder $\mathrm{Aut}_{K-\mathrm{Vektorräume}}(X)$. Teilweise sind für diese Automorphismengruppen auch andere Schreibweisen gebräuchlich, zum Beispiel wird die Automorphismengruppe eines K-Vektorraums V manchmal mit $GL_K(V)$ bezeichnet.

Analog können wir beliebige Abbildungen zwischen Mengen als »Mengenhomomorphismen« betrachten; die »Mengenisomorphismen«, also die Abbildungen, die eine Umkehrabbildung besitzen, sind genau die bijektiven Abbildungen. Mit der entsprechenden Definition erhalten wir als »Automorphismengruppe« der Menge X die Gruppe $\mathrm{Bij}(X)$ der Bijektionen $X \to X$. (Diese Sichtweise ist natürlich Kontext von Kategorien, siehe (Ergänzungs-)Abschnitt LA2.18.8.1.) $\Diamond$

Ein Spezialfall, mit dem wir uns später ausführlich beschäftigen werden, ist die Automorphismengruppe einer Körpererweiterung (die wir unter gewissen zusätzlichen Voraussetzungen die *Galois-Gruppe* der Erweiterung nennen werden).

BEMERKUNG 2.3 (Galois-Gruppen). Sei L ein Körper. Die Menge $\mathrm{Aut}(L)$ aller Ringautomorphismen $L \xrightarrow{\sim} L$ ist eine Gruppe (mit der Komposition von Automorphismen als Gruppenverknüpfung). Ist $K \subseteq L$ ein Teilkörper, dann ist die Teilmenge

$$\mathrm{Aut}_K(L) := \{\sigma \in \mathrm{Aut}(L);\, \sigma(x) = x \text{ für alle } x \in K\} \subseteq \mathrm{Aut}(L).$$

eine Untergruppe von $\mathrm{Aut}(L)$. Wir nennen $\mathrm{Aut}_K(L)$ die Automorphismengruppe der Erweiterung L/K.

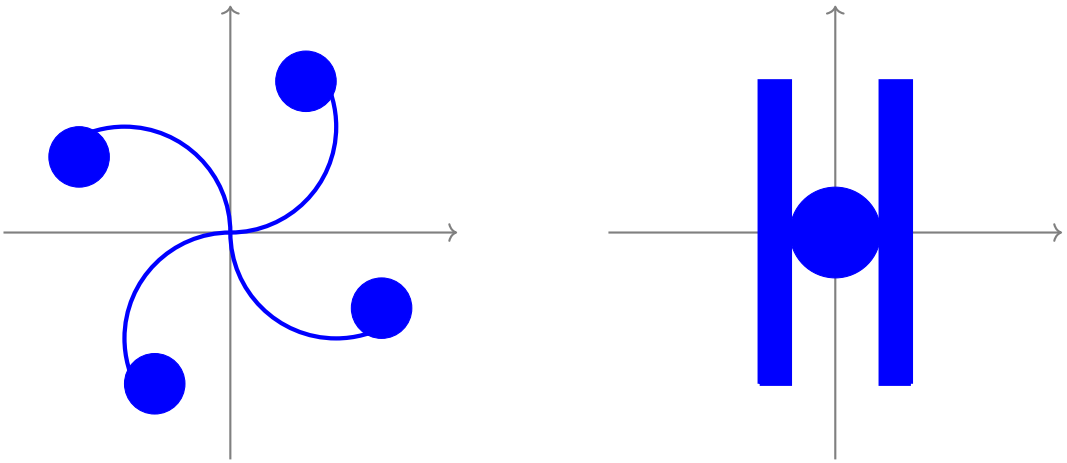
Zum Beispiel hat die Gruppe $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ genau zwei Elemente: die Identitätsabbildung und die komplexe Konjugation. (Warum gibt es keine weiteren?) ◊

BEISPIEL 2.4. Eine weitere Variante von Gruppen, die aus Bijektionen eines Objekts bestehen, sind *Symmetriegruppen* von Teilmengen von $\mathbb{R}^2$, $\mathbb{R}^3$ oder höherdimensionalen $\mathbb{R}$-Vektorräumen, oder allgemeiner von Teilmengen eines Vektorraums V über einem beliebigen Körper K. Für $M \subseteq V$ nennen wir den Stabilisator

$$\mathrm{Stab}(M) = \{f \in \mathrm{Aut}_K(V);\, f(M) = M\}$$

von M in der Automorphismengruppe von V die Symmetriegruppe von M. Im Fall des Standardvektorraums $V = K^n$ können wir die Symmetriegruppe von M auch als Untergruppe der allgemeinen linearen Gruppe $GL_n(K)$ betrachten.

Den Begriff der Gruppe kann man als den mathematischen Ansatz betrachten, Symmetrien zu beschreiben. Zum Beispiel hat die links abgebildete Teilmenge von $\mathbb{R}^2$ Symmetriegruppe $\mathbb{Z}/4$ (die »Symmetrien« sind die Drehungen um Vielfache von 90°), die rechts abgebildete Teilmenge hat Symmetriegruppe $\mathbb{Z}/2 \times \mathbb{Z}/2$ (die Symmetrien sind neben der identischen Abbildung die Spiegelungen an x- und y-Achse und ihre Verkettung, also die Punktspiegelung am Ursprung). In beiden Fällen gibt es 4 Symmetrien (einschließlich der Identität), und die Gruppenstruktur ermöglicht eine präzise Beschreibung. Gruppen, die nicht zu einer Untergruppe von $GL_2(\mathbb{R})$ isomorph sind, können nicht die Symmetriegruppe einer Teilmenge von $\mathbb{R}^2$ sein; ein Beispiel dafür ist die Quaternionengruppe (siehe Ergänzung 2.8).



Ein konkretes Beispiel, das wir in der Linearen Algebra (wenigstens am Rande, siehe Abschnitt LA1.8.1.6) gesehen haben, sind die Diedergruppen: D_{2n} ist die Untergruppe von $GL_2(\mathbb{R})$ aller derjenigen Automorphismen $\mathbb{R}^2 \xrightarrow{\sim} \mathbb{R}^2$, die ein fixiertes regelmäßiges n-Eck (das den Ursprung als Mittelpunkt hat) auf sich abbilden. Sie hat $2n$ Elemente, und zwar n Drehungen und n Spiegelungen.

Vergleiche auch Abschnitt 2.3. ◊

BEISPIEL 2.5 (Produkt von Gruppen). (1) Sind G und H Gruppen, so können wir das Produkt

$$G \times H = \{(g,h);\, g \in G,\, h \in H\}$$

bilden. Mit der komponentenweisen Verknüpfung

$$(g,h)(g',h') = (gg',hh')$$

bildet dieses wieder eine Gruppe. Die *Projektionen*

$$p_G\colon G \times H \to G,\ (g,h) \mapsto g, \quad \text{und} \quad p_H\colon G \times H \to H,\ (g,h) \mapsto h,$$

sind (surjektive) Gruppenhomomorphismen. Das Produkt erfüllt die universelle Eigenschaft des Produkts, d.h. die Abbildung

$$\mathrm{Hom}(T, G \times H) \to \mathrm{Hom}(T, G) \times \mathrm{Hom}(T, H), \quad \varphi \mapsto (p_G \circ \varphi, p_H \circ \varphi),$$

ist eine Bijektion. Siehe Abschnitt LA2.18.1.1.

(2) Allgemeiner können wir für jede Menge I und jede Familie $(G_i)_{i\in I}$ von Gruppen das Produkt $\prod_{i\in I} G_i$ bilden. Auch hier haben wir die Projektionen auf die einzelnen Faktoren des Produkts, und es ist eine universelle Eigenschaft erfüllt.

◊

In der Algebra-Vorlesung werden im Vergleich zur Linearen Algebra endliche Gruppen eine größere Rolle spielen. Wir sammeln daher einige Beispiele.

Beispiel 2.6 (Gruppen mit wenigen Elementen). Wir geben für $n \leq 7$ eine »vollständige Liste bis auf Isomorphie« der Gruppen mit n Elementen an, das bedeutet, eine Liste $G_1, G_2, \ldots, G_{r(n)}$ von Gruppen, so dass jede Gruppe mit n Elementen zu genau einer der Gruppen aus dieser Liste isomorph ist.

Die Beweise, dass die Listen jeweils vollständig sind, verschieben wir auf später (bzw. auf die Übungen).

Die Gruppe G schreiben wir in diesem Beispiel stets multiplikativ.

(1) $\#G = 1$. Die »einzige« Gruppe mit genau einem Element ist die sogenannte *triviale Gruppe* $\{1\}$ mit $1 \cdot 1 = 1$, d.h.: für jede Gruppe G, die genau ein Element a enthält, ist $G \to \{1\}$, $a \mapsto 1$ ein Isomorphismus von Gruppen.

(2) $\#G = 2$. Ist $G = \{a, b\}$ eine Gruppe mit genau zwei Elementen, wobei ohne Einschränkung a das neutrale Element bezeichne, so ist $G \to \mathbb{Z}/2$, $a \mapsto 0$, $b \mapsto 1$, ein Gruppenisomorphismus (wobei wir $\mathbb{Z}/2$ als Gruppe bezüglich der Addition verstehen).

(3) $\#G = p$, p Primzahl. Dann ist G isomorph zur (additiven) Gruppe $\mathbb{Z}/p$, insbesondere ist G also kommutativ. Sei $g \in G \setminus \{1\}$. Dann ist

$$\mathbb{Z}/p \to G, i \mapsto g^i$$

ein Isomorphismus von der (additiven) Gruppe $\mathbb{Z}/p$ auf die Gruppe G.

Es gibt also bis auf Isomorphie nur eine einzige Gruppe der Ordnung p. Siehe Beispiel 2.22.

(4) $\#G = 4$. In diesem Fall gibt es genau zwei nicht-isomorphe Gruppen, und zwar die Gruppen $\mathbb{Z}/4$ und $\mathbb{Z}/2 \times \mathbb{Z}/2$ (letztere nennt man auch die *Kleinsche Vierergruppe*). Dass die beiden Gruppen nicht isomorph sind, ist klar, weil $\mathbb{Z}/4$ ein Element der Ordnung 4 enthält, $\mathbb{Z}/2 \times \mathbb{Z}/2$ aber nur Elemente der Ordnung 1 und 2 (siehe 2.12).

(5) $\#G = 6$. Auch in diesem Fall gibt es zwei Gruppen auf der Liste, nämlich $\mathbb{Z}/6$ und die symmetrische Gruppe S_3. Weil S_3 nicht kommutativ ist, sind diese beiden Gruppen offenbar nicht zueinander isomorph.

◊

Beispiel 2.7 (Endliche abelsche Gruppen). (1) Für jedes $n \in \mathbb{N}_{>0}$ ist $\mathbb{Z}/n$ eine kommutative Gruppe mit n Elementen.

(2) Für $r \in \mathbb{N}$ und $n_1, \ldots, n_r \in \mathbb{N}_{>0}$ ist

$$\mathbb{Z}/n_1 \times \cdots \mathbb{Z}/n_r$$

eine abelsche Gruppe (mit $n_1 \cdots n_r$ Elementen). Im Allgemeinen ist diese nicht isomorph zu einer Gruppe der Form $\mathbb{Z}/n$, zum Beispiel ist $\mathbb{Z}/2 \times \mathbb{Z}/2$ nicht von dieser Form.

(Manchmal allerdings doch; der chinesische Restsatz, Satz LA2.15.61, liefert für *paarweise teilerfremde* Zahlen $n_1, \dots, n_r$ einen Isomorphismus $\mathbb{Z}/n_1 \times \cdots \mathbb{Z}/n_r \cong \mathbb{Z}/n_1 \cdots n_r$.)

(3) Der *Hauptsatz über endliche abelsche Gruppen* besagt, dass jede endliche abelsche Gruppe isomorph ist zu einer Gruppe der Form in (2). Genauer gilt: Ist G eine endliche abelsche Gruppe, dann existieren natürliche Zahlen $n_1, \dots, n_r > 1$ mit

$$G \cong \mathbb{Z}/n_1 \times \cdots \mathbb{Z}/n_r ,$$

und so dass $n_1 \mid n_2, n_2 \mid n_3, \dots, n_{r-1} \mid n_r$, und $n_1, \dots, n_r$ sind durch G eindeutig bestimmt. Siehe Korollar LA2.18.93 in den Ergänzungen des LA2-Skripts.

◊

ERGÄNZUNG 2.8 (Gruppen mit 8 Elementen). Für Gruppen mit 8 Elementen ist es schon ein bisschen komplizierter, eine »Klassifikation (bis auf Isomorphie)« wie in Beispiel 2.6 anzugeben.

Das Ergebnis ist die folgende Liste:

(1) $\mathbb{Z}/8$,

(2) $\mathbb{Z}/4 \times \mathbb{Z}/2$,

(3) $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$,

(4) die Diedergruppe D_8, siehe Beispiel 2.4, Abschnitt LA1.8.1.6.

(5) die *Quaternionengruppe* Q, d.h. die multiplikative Untergruppe der Einheitengruppe $\mathbb{H}^\times$ der Hamiltonschen Quaternionen (Ergänzung LA1.4.11), die von $1, i, j, k$ erzeugt wird. Es ist also

$$Q = \{1, i, j, k, -1, -i, -j, -k\}$$

mit neutralem Element 1 und

$$(-1)^2 = 1, \quad (-1)\cdot i = i\cdot(-1) = -i, \quad (-1)\cdot j = j\cdot(-1) = -j, \quad (-1)\cdot k = k\cdot(-1) = -k,$$
$$i^2 = j^2 = k^2 = -1, \quad ij = k.$$

Alle anderen Produkte ergeben sich daraus, zum Beispiel

$$kj = (ij)j = ij^2 = -i, \quad ji = (ij)^{-1} = k^{-1} = -k.$$

□ Ergänzung 2.8

BEISPIEL 2.9. Für eine Primzahl p und $n \in \mathbb{N}$ ist $GL_n(\mathbb{F}_p)$, die Gruppe der invertierbaren $(n \times n)$-Matrizen über $\mathbb{F}_p$, eine endliche Gruppe. Können Sie »ausrechnen« (d.h. eine geschlossene Formel dafür angeben), wie viele Elemente $GL_n(\mathbb{F}_p)$ hat? ◊

2.2. Der Quotient nach einem Normalteiler

2.2.1. Nebenklassen und der Satz von Lagrange. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Die Teilmengen von G der Form

$$gH = \{gh;\ h \in H\}, \quad g \in G,$$

nennen wir die *Linksnebenklassen* von H in G. Es handelt sich um die Äquivalenzklassen bezüglich der durch

$$g \sim g' \quad \Longleftrightarrow \quad g^{-1}g' \in H$$

gegebenen Äquivalenzrelation. Wir schreiben G/H für die Menge aller Linksnebenklassen von H in G und nennen gH die *(Links-)Nebenklasse* oder *Restklasse* von g.

Für $g \in G$ ist die Multiplikation mit g eine Bijektion $H \to gH$. Im Fall einer endlichen Gruppe ergibt sich daraus der folgende Satz.

SATZ 2.10 (Satz von Lagrange). *Sei G eine endliche Gruppe und $H \subseteq G$ eine Untergruppe. Dann gilt*

$$\#G = \#H \cdot \#(G/H).$$

In diesem Zusammenhang definieren wir die folgenden Begriffe.

DEFINITION 2.11. (1) Sei G eine (endliche) Gruppe. Die Anzahl $\#G$ der Elemente von G nennt man auch die *Ordnung* von G. (Manchmal schreibt man $\mathrm{ord}(G) = \#G$.) Ist G nicht endlich, so ist die Ordnung von G unendlich (in Zeichen: ∞).

(2) Sei G eine Gruppe und H eine Untergruppe. Die Anzahl der Elemente von G/H (in $\mathbb{N}_{>0} \cup \{\infty\}$) nennt man auch den *Index* der Untergruppe H in G. Wir schreiben auch $[G : H] = \#G/H$.

⊣

Analog kann man auch *Rechtsnebenklassen*, also Teilmengen der Form Hg betrachten. Wir bezeichnen mit $H\backslash G$ die Menge der Rechtsnebenklassen. Die Abbildung $gH \mapsto Hg^{-1}$ ist eine Bijektion $G/H \to H\backslash G$, insbesondere haben diese beiden Mengen dieselbe Mächtigkeit (so dass man den Index auch als die Anzahl der Rechtsnebenklassen definieren könnte). (Warum ist die Abbildung $gH \mapsto Hg^{-1}$ wohldefiniert und bijektiv? Wie ist es mit $gH \mapsto Hg$?)

DEFINITION 2.12. Sei G eine Gruppe und $g \in G$. Die *Ordnung* $\mathrm{ord}(g)$ von g ist die kleinste positive ganze Zahl n mit $g^n = 1$, oder ∞ wenn kein solches n existiert. ⊣

LEMMA 2.13. *Sei G eine Gruppe und $g \in G$. Dann gilt*

$$\mathrm{ord}(g) = \#\langle g \rangle.$$

BEWEIS. Es gilt $\langle g \rangle = \{g^i;\ i \in \mathbb{Z}\}$, denn die rechte Seite ist die kleinste Untergruppe von G, die g enthält. Wenn $\mathrm{ord}(g)$ unendlich ist, dann sind die Elemente g^i, $i \in \mathbb{Z}$ alle verschieden; denn aus $g^i = g^j$ folgt $g^{i-j} = 1$.

Sei nun $m = \mathrm{ord}(g)$ endlich. Es gilt also $g^m = 1$ und $g^d \neq 1$ für alle $1 \leq d < m$. Es folgt $g^{m-1} = g^{-1}$, und dass $\{1, g, \ldots, g^{m-1}\}$ eine *Untergruppe* von G mit m Elementen ist. Keine echte Teilmenge dieser Menge ist eine Untergruppe, die g enthält, deshalb ist $\langle g \rangle = \{1, g, \ldots, g^{m-1}\}$ und $\#\langle g \rangle = m = \mathrm{ord}(g)$. □

Aus dem Satz von Lagrange folgt damit:

KOROLLAR 2.14. *Sei G eine endliche Gruppe und $g \in G$. Dann gilt* $\mathrm{ord}(g) \mid \#G$.

Insbesondere gilt $g^{\mathrm{ord}(g)} = 1$.

Geben Sie ein Beispiel einer Gruppe G und eines Teilers der Gruppenordnung $\#G$, der nicht die Ordnung eines Gruppenelements ist. Immerhin gilt aber Lemma 2.23, siehe auch Ergänzung 2.83.

2.2.2. Normalteiler und der Quotient nach einem Normalteiler. Schon in der Linearen Algebra haben wir gelernt (Abschnitt LA2.18.3), dass nicht jede Untergruppe einer Gruppe der Kern irgendeines Gruppenhomomorphismus sein muss, und man demzufolge auch nicht den Quotienten nach beliebigen Untergruppen bilden kann, sondern nur nach sogenannten *Normalteilern*. Wir beginnen mit der Wiederholung der Definition dieses Begriffs.

DEFINITION 2.15. Sei G eine Gruppe. Eine Untergruppe $H \subseteq G$ heißt *Normalteiler*, wenn für alle $g \in G$ die Links- und Rechtsnebenklasse von g bezüglich H übereinstimmen, d.h.

$$gH = Hg.$$

⊣

Wir sammeln einige einfache Aussagen, die wir benutzen werden und in der Linearen Algebra noch nicht bewiesen haben. Wir schreiben für $g, g' \in G$ und eine Untergruppe H analog zur Nebenklassenschreibweise auch

$$gHg' = \{ghg';\ h \in H\}$$

und speziell

$$gHg^{-1} = \{ghg^{-1};\ h \in H\}.$$

Für jede Untergruppe H ist die Menge gHg^{-1} ebenfalls eine Untergruppe von G, die wir eine *zu H konjugierte* Untergruppe nennen. Sie ist das Bild unter der *Konjugation mit g*, d.h. unter dem Gruppenisomorphismus $G \to G, x \mapsto gxg^{-1}$. Siehe auch Beispiel 2.30.

Ist G eine abelsche Gruppe, dann ist jede Untergruppe von G ein Normalteiler. In jeder Gruppe G sind $\{1\}$ und G Normalteiler. Sind G und H Gruppen, so ist $G \times \{1\} \subseteq G \times H$ ein Normalteiler, und ebenso natürlich $\{1\} \times H \subseteq G \times H$; entsprechendes gilt für beliebige Produkte von Gruppen. Die Untergruppe $\{\mathrm{id}, (12)\} \subseteq S_3$ ist (warum?) kein Normalteiler. Ist $H \subseteq G$ der Kern irgendeines Gruppenhomomorphismus $G \to G'$, so ist H ein Normalteiler von G (wie aus Teil (2) des folgenden Lemmas folgt).

LEMMA 2.16. *Seien G eine Gruppe und H eine Untergruppe.*

(1) *Wenn $gH \subseteq Hg$ für alle $g \in G$ gilt, dann ist H ein Normalteiler.*
(2) *Wenn $gHg^{-1} \subseteq H$ für alle $g \in G$ gilt, dann ist H ein Normalteiler.*
(3) *Wenn $H \subseteq gHg^{-1}$ für alle $g \in G$ gilt, dann ist H ein Normalteiler.*
(4) *Das Bild eines Normalteilers unter einem surjektiven Gruppenhomomorphismus ist ein Normalteiler.*
(5) *Das Urbild eines Normalteilers unter einem Gruppenhomomorphismus ist ein Normalteiler.*
(6) *Ist $\pi\colon G \to G'$ ein surjektiver Gruppenhomomorphismus, dann sind die beiden Abbildungen $H \mapsto \pi(H)$ und $H' \mapsto \pi^{-1}(H')$ zueinander invers und induzieren eine inklusionserhaltende Bijektion zwischen der Menge der Normalteiler von G, die $\mathrm{Ker}(\pi)$ enthalten und der Menge der Normalteiler von G'.*

Die Bijektion in (6) nennen wir *inklusionserhaltend* weil für $H_1, H_2 \subseteq G$ genau dann $H \subseteq H'$ gilt, wenn $\pi(H_1) \subseteq \pi(H_2)$ gilt.

BEWEIS. Zu Teil (1): Es gelte $gH \subseteq Hg$ für alle $g \in G$. Wir müssen zeigen, dass stets auch die umgekehrte Inklusion gilt. Wenn wir die ursprüngliche Aussage auf g^{-1} anwenden, erhalten wir $g^{-1}H \subseteq Hg^{-1}$, und das impliziert, wenn wir »von links und rechts mit g multiplizieren«, dass $Hg \subseteq gH$ gilt, wie gewünscht.

Teile (2) und (3) kann man mit demselben Argument beweisen. Man beachte dazu, dass $gH \subseteq Hg$ äquivalent ist zu $gHg^{-1} \subseteq H$ und zu $H \subseteq g^{-1}Hg$, und entsprechend natürlich für die Gleichheit von Mengen anstelle der Inklusion.

Teile (4) und (5) sind nicht sehr schwierig; wir lassen den Beweis als Übung. Teil (6) folgt dann leicht aus (4) und (5). □

SATZ 2.17 (Quotient einer Gruppe nach einem Normalteiler). *Seien G eine Gruppe und $H \subseteq G$ ein Normalteiler. Dann ist die Abbildung*

$$G/H \times G/H \to G/H, \quad (gH, g'H) \mapsto gg'H,$$

wohldefiniert und definiert auf G/H die Struktur einer Gruppe, die wir den Quotienten der Gruppe G nach dem Normalteiler H *nennen.*

Die Abbildung $\pi\colon G \to G/H, g \mapsto gH$, ist ein surjektiver Gruppenhomomorphismus mit $\operatorname{Ker}(\pi) = H$, den wir die kanonische Projektion nennen.

Siehe auch Abschnitt LA2.18.3. Die folgenden beiden Lemmata geben noch einmal eine etwas andere Interpretation der Quotientenkonstruktion (und des Normalteilerbegriffs).

LEMMA 2.18. *Sei G eine Gruppe, X eine Menge und $f\colon G \to X$ eine surjektive Abbildung. Dann gibt es höchstens eine Verknüpfung $X \times X \to X$, die auf X die Struktur einer Gruppe definiert und so dass f ein Gruppenhomomorphismus ist.*

BEWEIS. Das ist klar, denn es muss $f(g) \cdot f(h) = f(gh)$ für alle $g, h \in G$ gelten, und wegen der Surjektivität von f hat jedes Element von X die Form $f(g)$ für ein geeignetes $g \in G$. □

LEMMA 2.19. *Sei G eine Gruppe, $H \subseteq G$ eine Untergruppe und $\pi\colon G \to G/H$ die (surjektive) Abbildung, die jedem $g \in G$ seine Nebenklasse gH zuordnet.*

Es gibt genau dann eine Gruppenstruktur auf G/H, so dass π ein Gruppenhomomorphismus ist, wenn H ein Normalteiler *in G ist (und diese ist nach dem vorherigen Lemma eindeutig bestimmt).*

BEWEIS. Dass für einen Normalteiler H eine Gruppenstruktur auf G/H existiert, zeigt man durch eine leichte Rechnung (die wir in der Linearen Algebra 2 durchgeführt haben). Wenn andererseits eine Gruppenstruktur existiert, für die π ein Homomorphismus ist, so sieht man leicht, dass $\operatorname{Ker}(\pi) = H$ gilt, und als Kern eines Gruppenhomomorphismus muss H ein Normalteiler sein. □

BEISPIEL 2.20. Sei $G = \mathbb{Z}$ die Gruppe der ganzen Zahlen. Ist $n \in \mathbb{N}$, so ist

$$n\mathbb{Z} = \{kn;\ k \in \mathbb{Z}\},$$

die Menge aller Vielfachen von $\mathbb{Z}$, eine Untergruppe von $\mathbb{Z}$. Ist umgekehrt $H \subseteq \mathbb{Z}$ eine Untergruppe, so existiert $n \in \mathbb{N}$ mit $H = n\mathbb{Z}$. (Definieren Sie, falls $H \neq 0$ gilt, n als ein Element $\neq 0$ von H, dessen Absolutbetrag unter allen Elementen von $H \setminus \{0\}$ minimal ist, und benutzen Sie Division mit Rest, um $H = n\mathbb{Z}$ zu zeigen. Oder benutzen Sie, dass jede Untergruppe von $\mathbb{Z}$ auch ein Ideal im Ring $\mathbb{Z}$ ist und dass $\mathbb{Z}$ ein Hauptidealring ist. In diesem »schnelleren« Beweis ist aber das direkte Argument auch (wo?) versteckt.)

Wenn $n = 0$ ist, so ist $n\mathbb{Z} = \{0\}$ und die kanonische Projektion $\mathbb{Z} \to \mathbb{Z}/n$ ist in diesem Fall ein Isomorphismus. Für $n \neq 0$ gilt $n\mathbb{Z} = (-n)\mathbb{Z}$ und der Quotient $\mathbb{Z}/n$ hat $|n|$ Elemente. ◊

Das wichtigste Werkzeug, um mit dem Quotienten zu arbeiten, ist der Homomorphiesatz (oder mit anderen Worten die »universelle Eigenschaft« des Quotienten).

SATZ 2.21 (Homomorphiesatz für Gruppen). *Sei G eine Gruppe und $H \subseteq G$ ein Normalteiler. Sei $\pi\colon G \to G/H$ die kanonische Projektion auf den Quotienten. Sei T eine Gruppe und $f\colon G \to T$ ein Gruppenhomomorphismus.*

(1) *Wenn $H \subseteq \operatorname{Ker} f$ gilt, dann existiert ein eindeutig bestimmter Homomorphismus $\varphi\colon G/H \to T$ mit $\varphi \circ \pi = f$.*

(2) *Existiert φ mit $\varphi \circ \pi = f$, so folgt $H \subseteq \operatorname{Ker} f$. Sind f mit $H \subseteq \operatorname{Ker} f$ und φ wie in (1), so gilt:* $\operatorname{Im}\varphi = \operatorname{Im} f$. *Die Abbildung φ ist genau dann injektiv wenn $H = \operatorname{Ker} f$ gilt, genauer gilt stets* $\operatorname{Ker}\varphi = \operatorname{Ker}(f)/H$.

BEISPIEL 2.22. Sei p eine Primzahl und G eine Gruppe der Ordnung p, also mit $\#G = p$. Dann sind $\{1\}$ und G die einzigen Untergruppen von G, denn nach dem Satz von Lagrange muss jede Untergruppe als Ordnung einen Teiler von $\#G$ haben, also 1 oder p. Insbesondere gilt für jedes $g \in G, g \neq 1$, dass $\langle g\rangle = G$ ist, denn die linke Seite ist jedenfalls eine nicht-triviale Untergruppe von G.

Man sieht dann leicht, dass die Abbildung $\mathbb{Z}/p \to G, i \mapsto g^i$, ein Gruppenisomorphismus ist. Bis auf Isomorphie ist also $\mathbb{Z}/p$ die einzige Gruppe mit p Elementen.

Es ist nicht sehr schwer zu sehen, dass eine Gruppe G, in der $\{1\}$ und G die einzigen Untergruppen sind, die Form $\mathbb{Z}/p$ für eine Primzahl p haben muss, siehe Beispiel 2.46. ◊

LEMMA 2.23. *Sei G eine endliche abelsche Gruppe und p eine Primzahl, die die Gruppenordnung $\#G$ teilt. Dann existiert ein Element $g \in G$ mit* $\operatorname{ord}(g) = p$.

BEWEIS. Ist $g \in G$ ein Element, dessen Ordnung $d := \operatorname{ord}(g)$ von p geteilt wird, so sieht man leicht, dass $g^{d/p}$ Ordnung p hat.

Wir führen nun Induktion nach $\#G$, um zu zeigen, dass für jeden Primteiler p der Gruppenordnung ein Element existiert, dessen Ordnung von p geteilt wird. Ist G die triviale Gruppe, so ist nichts zu zeigen. Sei also nun $G \neq 1$ und p eine Primzahl, die $\#G$ teilt. Sei $g \in G$ irgendein Element mit $\operatorname{ord}(g) > 1$. Gilt $p \mid \operatorname{ord}(g)$, so sind wir nach dem oben Gesagten fertig. Andernfalls bilden wir den Quotienten $G/\langle g\rangle$ nach dem Normalteiler $\langle g\rangle$. Wegen $\#G = \#(G/\langle g\rangle) \cdot \operatorname{ord}(g)$ gilt dann $p \mid \#(G/\langle g\rangle)$, nach Induktionsvoraussetzung existiert daher ein Element $\bar{h} \in G/\langle g\rangle$, dessen Ordnung von p geteilt wird. Sei nun $h \in G$ ein Element mit Restklasse $\bar{h}$. Dann ist $\langle \bar{h}\rangle$ ein Quotient von $\langle h\rangle$, und es folgt $\operatorname{ord}(\bar{h}) \mid \operatorname{ord}(h)$ und damit $p \mid \operatorname{ord}(h)$. □

Es ist wichtig, dass hier p eine Primzahl ist. Wo geht das obige Argument schief, wenn man diese Voraussetzung fallenlässt? Die Voraussetzung, dass G abelsch sei, ist aber nicht erforderlich für die Gültigkeit der Aussage (allerdings schon (warum?) für den hier gegebenen Beweis). Siehe Ergänzung 2.83.

KOROLLAR 2.24 (Isomorphiesatz). *Seien G eine Gruppe, $H \subseteq G$ eine Untergruppe und $N \subseteq G$ ein Normalteiler.*

(1) *Die Menge $HN = \{hn;\ h \in H,\ n \in N\}$ ist eine Untergruppe von G und zwar die von $H \cup N$ erzeugte Untergruppe von G.*

(2) *Es ist N ein Normalteiler von HN und $H \cap N$ ein Normalteiler von H und es gilt $HN/N \cong H/H\cap N$.*

BEWEIS. zu (1). Für alle $h \in H$ und $n \in N$ gilt $nh = h(h^{-1}nh) \in HN$, weil wegen der Normalteilereigenschaft von N mit n auch das Konjugierte $h^{-1}nh$ in N liegt. Insbesondere folgt die Abgeschlossenheit unter der Multiplikation: $hnh'n' = hh'((h')^{-1}nh')n' \in HN$ für $h, h' \in H$ und $n, n' \in N$ und die Abgeschlossenheit unter der Bildung des inversen Elements, denn $(hn)^{-1} = n^{-1}h^{-1}$. Offenbar liegt das neutrale Element von G in HN, und damit sind alle Bedingungen an eine Untergruppe erfüllt.

Es ist klar, dass H und N in HN enthalten sind, und dass jede Untergruppe von G, die H und N enthält, auch HN enthält.

zu (2). Weil N ein Normalteiler von G ist, ist N erst recht ein Normalteiler von HN. Ebenso folgt, dass $H \cap N$ ein Normalteiler von H ist. Die Abbildung

$$H \to HN/N, \quad h \mapsto hN,$$

ist surjektiv mit Kern $H \cap N$ und induziert daher nach dem Homomorphiesatz einen Isomorphismus $H/H \cap N \cong HN/N$. □

KOROLLAR 2.25 (Zweiter Isomorphiesatz). *Seien G Gruppe, $H, N \subseteq G$ Normalteiler in G mit $N \subseteq H$. Dann ist auch N ein Normalteiler in H, H/N kann in natürlicher Weise als Normalteiler von G/N aufgefasst werden, und es gilt*

$$(G/N)/(H/N) \cong G/H.$$

BEWEIS. Die Abbildung $H \to G \to G/N$ hat Kern N (insbesondere ist N ein Normalteiler von H) und induziert demnach einen injektiven Gruppenhomomorphismus $H/N \to G/N$, so dass wir H/N als Untergruppe von G/N betrachten können.

Die kanonische Projektion $G \to G/H$ faktorisiert über eine Surjektion

$$G/N \to G/H, \quad gN \mapsto gH,$$

deren Kern genau H/N ist, wie man unmittelbar überprüft. Daraus folgt einerseits, dass H/N ein Normalteiler von G/N ist (als Kern eines Gruppenhomomorphismus), und andererseits folgt mit dem Homomorphiesatz der behauptete Isomorphismus. □

2.3. Gruppenwirkungen

Wie oben bemerkt, sind »Gruppen von Bijektionen« bzw. allgemeiner *Automorphismengruppen* wichtige Beispiele von Gruppen. Ist G irgendeine Gruppe, so liefert uns »unsere« Definition von Gruppe, also der heutzutage übliche Gruppenbegriff, aber nur eine Verknüpfung auf G mit gewissen Eigenschaften und keine Anhaltspunkte für eine »konkrete Realisierung« der Elemente von G als Bijektionen einer Menge, als Automorphismen oder als »Symmetrien« einer Art. Allerdings ist es oft möglich (und nützlich) für eine gegebene Gruppe zu untersuchen, wie ein solcher Zusammenhang zu einer Gruppe der Form $\mathrm{Bij}(X)$ hergestellt werden kann. Ein offensichtlicher Ansatz ist es, Gruppenhomomorphismen $G \to \mathrm{Bij}(X)$ zu betrachten, mit anderen Worten Zuordnungen, die jedem Element von g eine Bijektion $X \to X$ zuordnen, so dass gewisse Eigenschaften erfüllt sein müssen. Schreibt man diese aus, erhält man den Begriff der *Wirkung* oder *Operation* einer Gruppe G auf einer Menge X wie in der folgenden Definition.

DEFINITION 2.26. Seien G eine Gruppe und X eine Menge. Eine *Wirkung* (oder: *Operation*) ist eine Abbildung

$$G \times X \to X, (g, x) \mapsto g \cdot x,$$

die die folgenden Eigenschaften hat:

(a) $(gh) \cdot x = g \cdot (h \cdot x)$ für alle $g, h \in G$ und alle $x \in X$,

(b) $1 \cdot x = x$ für alle $x \in X$ (wobei $1 \in G$ das neutrale Element bezeichne).

⊣

In äquivalenter Weise können wir eine Wirkung von G auf X als einen Gruppenhomomorphismus $\varphi\colon G \to \mathrm{Bij}(X)$ betrachten; die Beziehung zwischen den beiden Sichtweisen ist durch $\varphi(g)(x) = g \cdot x$ gegeben. Oft schreibt man statt $g \cdot x$ auch einfach gx (oder benutzt gegebenenfalls ein anderes Symbol).

Bevor wir Beispiele betrachten, führen wir noch die folgenden wichtigen Begriffe ein:

DEFINITION 2.27. Sei $G \times X \to X, (g, x) \mapsto gx$ eine Gruppenwirkung.

(1) Die *Bahn* (oder: der *Orbit*) *eines Elements $x \in X$ unter der Gruppe G* ist die Teilmenge

$$Gx := \{gx;\ g \in G\} \subseteq X.$$

(2) Der *Stabilisator* eines Elements x ist die Untergruppe
$$\mathrm{Stab}_G(x) := \{g \in G;\ gx = x\}$$
von G. Manchmal nennt man diese auch die *Standgruppe* oder die *Isotropiegruppe* von x in G.

(3) Allgemeiner kann man den *Stabilisator einer Teilmenge* $M \subseteq X$ definieren, dies ist die Untergruppe
$$\mathrm{Stab}_G(M) := \{g \in G;\ gM = M\}$$
von G. Hier schreiben wir $gM = \{gm;\ m \in M\} \subseteq X$.

⊣

Operiert die Gruppe G auf der Menge M und ist $H \subseteq G$ eine Untergruppe, so können wir die Operation »auf H einschränken«, d.h. die gegebene Abbildung $G \times M \to M$ einschränken zu einer Abbildung $H \times M \to M$ und erhalten so eine Operation von H auf M.

Beispiel 2.28. (1) Die symmetrische Gruppe S_n (und entsprechend jede Untergruppe von S_n) operiert auf der Menge $\{1, \dots, n\}$ durch $\sigma \cdot n = \sigma(n)$.

(2) Analog zu (1) operiert die Automorphismengruppe eines Objekts auf diesem Objekt, zum Beispiel haben wir für (Standard-)Vektorräume:

Sei K ein Körper und $n \in \mathbb{N}$. Die Gruppe $GL_n(K)$ operiert auf dem Vektorraum K^n durch Matrizenmultiplikation, d.h. die Operation ist gegeben durch
$$GL_n(K) \times K^n \to K^n, \quad (g, v) \mapsto gv.$$
Als Gruppenhomomorphismus $GL_n(K) \to \mathrm{Bij}(V)$ verstanden ist diese Operation (wenn wir invertierbare Matrizen als Automorphismen $K^n \xrightarrow{\sim} K^n$ verstehen) einfach die Inklusion der Gruppe aller *linearen* bijektiven Abbildungen in die Gruppe aller bijektiven Abbildungen.

Ist $M \subset K^n$ eine Teilmenge, so operiert die Gruppe $G := \mathrm{Stab}_{GL_n(K)}(M)$ auf M. (Dies ist ein allgemeines Prinzip, um die Wirkung einer Gruppe einzuschränken.) Siehe auch Abschnitt LA1.8.1.6.

(3) Ist K ein Körper, V ein K-Vektorraum und G eine Gruppe, so nennen wir eine Operation $\rho\colon G \to \mathrm{Bij}(V)$ von G auf V eine *Operation durch Vektorraumautomorphismen*, wenn das Bild von ρ in der Untergruppe $\mathrm{Aut}_K(V)$ aller Vektorraumautomorphismen von V liegt. Mit anderen Worten: Für jedes $g \in G$ ist die Bijektion $V \to V$, $v \mapsto gv$, eine lineare Abbildung.

Analog kann man Operationen von G auf einer Gruppe X durch Gruppenhomomorphismen oder auf einem Körper durch Körperautomorphismen, usw., betrachten.

(4) Die Gruppe $\mathbb{Z}/2$ operiert auf $\mathbb{C}$ durch komplexe Konjugation, d.h. wir definieren eine Gruppenoperation $\rho\colon \mathbb{Z}/2 \to \mathrm{Bij}(\mathbb{C})$ indem wir $\rho(0)$ als die Identitätsabbildung $\mathbb{C} \to \mathbb{C}$ und $\rho(1)$ als die komplexe Konjugation $\sigma\colon \mathbb{C} \to \mathbb{C}$ definieren. Weil $\sigma \circ \sigma = \mathrm{id}$ ist, ist dies ein Gruppenhomomorphismus.

(5) Die (additive) Gruppe $\mathbb{R}$ operiert auf $\mathbb{R}^2$ durch Drehungen, d.h. die Abbildung
$$\rho\colon \mathbb{R} \longrightarrow GL_2(\mathbb{R}), \quad \theta \mapsto \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta \end{pmatrix},$$
ist ein Gruppenhomomorphismus, und die Verkettung mit der Inklusion $GL_2(\mathbb{R}) = \mathrm{Aut}_{\mathbb{R}}(\mathbb{R}^2) \subset \mathrm{Bij}(\mathbb{R}^2)$ ist die oben genannte Wirkung. Alle Elemente der Untergruppe $2\pi\mathbb{Z} = \{2\pi k;\ k \in \mathbb{Z}\} \subset \mathbb{R}$ operieren »trivial«, also durch die Identitätsabbildung. Mit anderen Worten: $2\pi\mathbb{Z} \subseteq \mathrm{Ker}(\rho)$. Also erhalten wir nach dem Homomorphiesatz einen Homomorphismus
$$\bar{\rho}\colon \mathbb{R}/2\pi\mathbb{Z} \to GL_2(\mathbb{R}),$$

d.h. eine Wirkung der Gruppe $\mathbb{R}/2\pi\mathbb{Z}$ auch $\mathbb{R}^2$ durch Vektorraumautomorphismen. Die Bahnen dieser Operation sind einerseits die Teilmenge $\{0\}$, die nur aus dem Ursprung besteht, andererseits alle Kreise um den Ursprung (mit Radius > 0). Der Stabilisator von $0 \in \mathbb{R}^2$ ist die gesamte Gruppe, der Stabilisator eines Punktes $v \in \mathbb{R}^2 \setminus \{0\}$ ist die triviale Gruppe $\{0\}$.

$\Diamond$

Beispiel 2.29. Sei K ein Körper und seine $0 \leq r \leq n$ natürliche Zahlen. Sei $\mathscr{G}$ die Menge der r-dimensionalen Untervektorräume des K-Vektorraums K^n. Ist $f\colon K^n \to K^n$ ein Vektorraum-Automorphismus und $U \in \mathscr{G}$, so ist $f(U)$ ebenfalls ein Element von $\mathscr{G}$. Indem wir invertierbare Matrizen als Vektorraum-Automorphismen betrachten, erhalten wir so eine Operation der Gruppe $GL_n(K)$ auf der Menge $\mathscr{G}$. Was sind die Bahnen dieser Operation? Was ist der Stabilisator des Unterraums, der von den ersten r Standardbasisvektoren erzeugt wird? $\Diamond$

Beispiel 2.30. Sei G eine Gruppe. Dann ist $G \times G \to G, g \bullet h := ghg^{-1}$ eine Gruppenwirkung, die *Wirkung durch Konjugation* von G auf sich selbst. (An dieser Stelle ist es natürlich zwingend, die Operation nicht einfach als Multiplikation zu schreiben, weil sie sonst nicht von der Gruppenmultiplikation unterscheidbar wäre.)

Die Bahnen unter dieser Operation heißen die *Konjugationsklassen* der Gruppe G. Den Stabilisator eines Elements $h \in G$ unter der Konjugationswirkung nennen wir den *Zentralisator* von h und bezeichnen ihn mit Z_h. Es gilt also

$$Z_h = \{g \in G;\ ghg^{-1} = h\} = \{g \in G;\ gh = hg\}.$$

Allgemeiner sei für eine Teilmenge $S \in G$ der Zentralisator von S definiert als

$$Z_S = \bigcap_{h \in S} Z_h = \{g \in G;\ gh = hg \text{ für alle } h \in S\},$$

also als die Untergruppe von G derjenigen Elemente, die mit allen Elementen aus S kommutieren. Den Zentralisator Z_G der ganzen Gruppe G nennt man das *Zentrum* von G. Dies ist eine abelsche Gruppe und ein Normalteiler von G (allerdings besteht für manche Gruppen das Zentrum lediglich aus dem neutralen Element). Dass $Z_G = G$ gilt, ist dazu äquivalent, dass G abelsch ist.

Ist $H \subseteq G$ eine Untergruppe, so heißt der Stabilisator von H in G bezüglich der Konjugationswirkung der *Normalisator* der Untergruppe H. Dieser wird mit $N_G(H)$ bezeichnet und ist eine Untergruppe von G, die H enthält und in der H ein Normalteiler ist (und zwar die größte solche Untergruppe). Ausgeschrieben gilt also

$$N_G(H) = \{g \in G;\ gHg^{-1} = H\}.$$

Machen Sie sich den Unterschied zum Zentralisator Z_H klar! $\Diamond$

Beispiel 2.31. Sei K ein Körper. Die Gruppe $G = GL_n(K)$ operiert durch Konjugation auf dem Raum $M_n(K)$ der quadratischen Matrizen der Größe n, d.h. $g \in G$ operiert durch $A \mapsto gAg^{-1}$. Der Satz über die Jordansche Normalform beschreibt die Menge der Bahnen dieser Operation. $\Diamond$

Lemma 2.32. *Sei G eine Gruppe, die auf einer Menge X operiert. Sei $x \in X$. Dann induziert die Abbildung $G \to X, g \mapsto gx$, eine Bijektion $G/\operatorname{Stab}_G(x) \to Gx$.*

BEWEIS. Die angegebene Vorschrift ist wohldefiniert, denn für $g \in G$ und $h \in \mathrm{Stab}_G(x)$ gilt $(gh)x = g(hx) = gx$. Es ist klar, dass die Abbildung $G \to X$, $g \mapsto gx$, das Bild Gx hat, als Abbildung $G \to Gx$ verstanden also surjektiv ist. Elemente $g, g' \in G$ haben genau dann das gleiche Bild unter dieser Abbildung, wenn $gx = g'x$, also $g^{-1}g'x = x$ oder mit anderen Worten $g^{-1}g' \in \mathrm{Stab}_G(x)$ gilt. Das ist dazu äquivalent, dass g und g' dieselbe Restklasse in $G/\mathrm{Stab}_G(x)$ haben. Daraus folgt die Behauptung. □

Sei weiterhin G eine Gruppe, die auf einer Menge X operiert. Sind $x, y \in X$ mit $Gx \cap Gy \neq \emptyset$, etwa $z \in Gx \cap Gy$, so gilt können wir $z = gx = hy$ schreiben und erhalten $y = (h^{-1}g)x \in Gx$ und damit $Gy \subseteq Gx$. Aus Symmetriegründen folgt $Gy = Gx$. Zwei Bahnen sind also entweder disjunkt oder gleich. Mit anderen Worten: Die Menge X ist die disjunkte Vereinigung aller Bahnen.

Die Bahnen sind, wie man leicht überprüft, die Äquivalenzklassen bezüglich der Äquivalenzrelation

$$x \sim y \quad \Longleftrightarrow \quad \text{es existiert } g \in G \text{ mit } y = gx.$$

SATZ 2.33 (Bahnengleichung). *Sei G eine Gruppe, die auf einer endlichen Menge X operiert. Sei $x_1, \ldots, x_r$ ein Vertretersystem der Bahnen von X auf G, d.h. zu jeder Bahn $B \subseteq X$ in X unter G existiere ein eindeutig bestimmtes i mit $x_i \in B$. Dann gilt*

$$\#X = \sum_{i=1}^{r} \#Gx_i = \sum_{i=1}^{r} \#(G/\mathrm{Stab}_G(x_i)).$$

BEWEIS. Die erste Gleichheit folgt daraus, dass X die disjunkte Vereinigung aller Bahnen ist. Die zweite Gleichung ergibt sich aus Lemma 2.32. □

Wir wollen eine Folgerung aus der Bahnengleichung angeben, die dafür typisch ist, wie wir sie in Abschnitt 2.7 benutzen werden.

LEMMA 2.34. *Sei p eine Primzahl. Sei G eine endliche Gruppe, deren Ordnung eine Potenz von p ist. Sei X eine endliche Menge, auf der G operiert. Es sei*

$$X^G = \{x \in X; gx = x \text{ für alle } g \in G\}$$

die Menge der Fixpunkte *unter der G-Wirkung. Dann gilt*

$$\#X^G \equiv \#X \mod p.$$

BEWEIS. Dass ein Punkt $x \in X$ in X^G liegt, bedeutet gerade, dass er von allen Elementen von G fixiert wird, dass also $\mathrm{Stab}_G(x) = G$ gilt. Diese Elemente bilden jeweils eine eigene Bahn unter der Operation, und es gilt dann $G/\mathrm{Stab}_G(x) = 1$. In der Bahnengleichung

$$\#X = \sum_{i=1}^{r} \#Gx_i = \sum_{i=1}^{r} \#(G/\mathrm{Stab}_G(x_i))$$

sind alle Summanden $\#(G/\mathrm{Stab}_G(x_i))$, für die $\mathrm{Stab}_G(x_i) \neq G$ gilt, durch p teilbar. Diese können wir also vernachlässigen, wenn wir modulo p rechnen. Also ist

$$\#X \equiv \sum_{x \in X^G} \#(G/\mathrm{Stab}_G(x)) = \sum_{x \in X^G} 1 = \#X^G \mod p.$$

□

Im speziellen Fall der Wirkung einer endlichen Gruppe G auf sich selbst durch Konjugation erhalten wir:

SATZ 2.35 (Klassengleichung). *Sei G eine endliche Gruppe und sei $g_1, \ldots, g_r$ ein Vertretersystem derjenigen Konjugationsklassen in G, die aus mehr als einem Element bestehen. Dann gilt*

$$\#G = \#Z_G + \sum_{i=1}^{r} \#(G/Z_{x_i}).$$

BEWEIS. Dass die Konjugationsklasse eines Elements $g \in G$ aus einem einzigen Element besteht, also die Form $\{g\}$ hat, ist damit gleichbedeutend, dass g mit allen Elementen von G kommutiert, also im Zentrum Z_G der Gruppe G liegt. Die Elemente des Zentrums sind also diejenigen, die für sich genommen eine Bahn bilden. Daher ergibt sich die angegebene Gleichheit unmittelbar aus der Bahnengleichung für die Operation von G auf sich selbst durch Konjugation. □

Auch aus der Klassengleichung können wir eine interessante Folgerung über Gruppen ableiten, deren Ordnung eine Primzahlpotenz ist.

LEMMA 2.36. *Sei p eine Primzahl. Sei G eine endliche Gruppe, deren Ordnung eine Potenz p^r von p mit $r \geq 1$ ist. Dann ist das Zentrum von G nicht die triviale Gruppe.*

BEWEIS. Wir schreiben die Klassengleichung für G aus:

$$\#G = \#Z_G + \sum_{i=1}^{r} \#(G/Z_{x_i}).$$

Nach Definition der x_i gilt $Z_{x_i} \neq 1$ für alle i, so dass $\#(G/Z_{x_i}) > 1$ für alle i folgt. Diese Terme und damit auch die gesamte Summe sind folglich durch p teilbar. Weil $\#G$ auch durch p teilbar ist, folgt $p \mid \#Z_G$. Nun gilt $\#Z_G \geq 1$, weil das Zentrum jedenfalls das neutrale Element von G enthält. Insgesamt folgt $\#Z_G > 1$, wie behauptet. □

Oft ist die folgende Sprechweise nützlich:

DEFINITION 2.37. Eine Gruppenoperation heißt *transitiv*, wenn es genau eine Bahn gibt. ⊣

Operiert eine Gruppe G transitiv auf einer Menge X und ist x irgendein Element, so erhalten wir mit Lemma 2.32 eine Bijektion $G/\operatorname{Stab}_G(x) \to X, g \mapsto gx$, also eine Beschreibung von X in Termen von G und der Untergruppe $\operatorname{Stab}_G(x)$.

2.4. Zyklische Gruppen

DEFINITION 2.38. Eine Gruppe G heißt *zyklisch*, wenn ein Element $g \in G$ existiert, das die Gruppe G erzeugt, mit anderen Worten, so dass

$$G = \langle g \rangle = \{g^i;\ i \in \mathbb{Z}\}.$$

⊣

Offenbar ist jede zyklische Gruppe kommutativ. Die Umkehrung ist aber nicht richtig (überlegen Sie sich ein Beispiel!).

BEISPIEL 2.39. (1) Die (additiven) Gruppen $\mathbb{Z}$ und $\mathbb{Z}/n$, $n \in \mathbb{N}_{>0}$, sind zyklisch. (Und wir sehen unten, dass jede zyklische Gruppe zu einer dieser Gruppen isomorph ist.)

(2) Sei G irgendeine Gruppe und $g \in G$. Dann ist $\langle g \rangle = \{g^i;\ i \in \mathbb{Z}\}$ eine zyklische Untergruppe von G. Insbesondere besitzt jede nicht-triviale Gruppe eine nicht-triviale zyklische Untergruppe.

(3) Seien p eine Primzahl und G eine Gruppe mit p Elementen. Dann ist G zyklisch. (Jedes Element $g \neq 1$ ist ein Erzeuger von G, da $\operatorname{ord}(g)$ ein Teiler von p ist.)

$\Diamond$

SATZ 2.40. *Sei G eine Gruppe. Dann sind äquivalent:*

(i) *die Gruppe G ist zyklisch,*

(ii) *es gibt einen surjektiven Gruppenhomomorphismus $\mathbb{Z} \to G$,*

(iii) *G ist isomorph zu einer der Gruppen*

  (1) *$\mathbb{Z}$,*

  (2) *$\mathbb{Z}/n$ für $n \geq 1$.*

BEWEIS. Die Äquivalenz von (i) und (ii) ist einfach: Für $G = \{g^i;\ i \in \mathbb{Z}\}$ ist $\mathbb{Z} \to G$, $i \mapsto g^i$ ein surjektiver Gruppenhomomorphismus. Ist andererseits G eine Gruppe, für die ein surjektiver Gruppenhomomorphismus $\varphi\colon \mathbb{Z} \to G$ existiert, so gilt $G = \langle \varphi(1) \rangle$.

Aus (ii) folgt (iii), denn ist $f\colon \mathbb{Z} \to G$ ein surjektiver Gruppenhomomorphismus, so impliziert der Homomorphiesatz, dass $G \cong \mathbb{Z}/\operatorname{Ker}(f)$ ist, und die einzigen Untergruppen von $\mathbb{Z}$ sind die Mengen der Form $n\mathbb{Z}$ mit $n \in \mathbb{Z}$, und dabei können wir ohne Einschränkung $n \in \mathbb{N}$ wählen. (Siehe Beispiel 2.20.)

Andererseits sind offenbar die in (iii) genannten Gruppen sämtlich zyklisch, sie werden erzeugt von (der Restklasse von) 1. □

SATZ 2.41. *Untergruppen und Quotienten von zyklischen Gruppen sind zyklisch. Insbesondere gilt: Ist $\varphi\colon G \to H$ ein Gruppenhomomorphismus und ist G zyklisch, so sind $\operatorname{Ker}(\varphi)$ und $\operatorname{Im}(\varphi)$ zyklisch.*

BEWEIS. Mit Charakterisierung (ii) in Satz 2.40 ist klar, dass Quotienten zyklischer Gruppen zyklisch sind. Ist G zyklisch, $\varphi\colon \mathbb{Z} \to G$ ein surjektiver Gruppenhomomorphismus und $H \subseteq G$ eine Untergruppe, so ist $\varphi^{-1}(H) \to H$ ein surjektiver Gruppenhomomorphismus, und $\varphi^{-1}(H)$ ist entweder die triviale Gruppe oder isomorph zu $\mathbb{Z}$. In beiden Fällen folgt, dass H zyklisch ist. Der Zusatz folgt aus dem ersten Teil. □

SATZ 2.42. (1) *Die Elemente von $\mathbb{Z}$, die (jeweils) diese Gruppe erzeugen, sind 1 und -1.*

(2) *Sei nun $n \in \mathbb{N}_{>0}$ und $r \in \mathbb{Z}$. Dann sind äquivalent:*

  (i) *die Restklasse von r ist ein Erzeuger der Gruppe $\mathbb{Z}/n$,*

  (ii) *die Restklasse von r ist eine Einheit im Ring $\mathbb{Z}/n$,*

  (iii) *die Zahlen r und n sind teilerfremd (haben also größten gemeinsamen Teiler 1).*

BEWEIS. Teil (1) ist unmittelbar klar. Zu (2): Die Restklasse von r ist genau dann ein Erzeuger von $\mathbb{Z}/n$, wenn (die Restklasse von) 1 in ihrem Erzeugnis liegt, also wenn $a, b \in \mathbb{Z}$ existieren mit $ar + bn = 1$. Das ist dazu äquivalent, dass r eine Einheit in $\mathbb{Z}/n$ ist und auch dazu dass r und n teilerfremd sind (siehe auch Satz LA1.4.16). □

DEFINITION 2.43 (Eulersche φ-Funktion). Die *Eulersche φ-Funktion* ist die Abbildung

$$\varphi\colon \mathbb{N}_{>0} \to \mathbb{N}_{>0}, \quad n \mapsto \#(\mathbb{Z}/n)^\times,$$

mit anderen Worten die Abbildung, für die $\varphi(n)$ die Anzahl der zu n teilerfremden Zahlen zwischen 1 und n ist. ⊣

Wir geben einige leicht zu beweisende Eigenschaften der Eulerschen φ-Funktion an. Die Eigenschaften (1) und (2) erlauben es, die Werte von φ für jede (nicht allzu große) natürliche Zahl einigermaßen aufwandslos zu berechnen. Eigenschaft (3) werden wir im Beweis von Theorem 2.47 für ein trickreiches Abzählargument benutzen.

LEMMA 2.44 (Eigenschaften der Eulerschen φ-Funktion). (1) *Sind $m, n \in \mathbb{N}_{>0}$ teilerfremd, so gilt $\varphi(mn) = \varphi(m)\varphi(n)$.*

(2) *Ist p eine Primzahl und $r \in \mathbb{N}_{>0}$, so gilt $\varphi(p^r) = p^{r-1}(p-1)$.*

(3) *Für alle $n \in \mathbb{N}_{>0}$ gilt*

$$\sum_{1 \le d \le n,\, d \mid n} \varphi(d) = n.$$

BEWEIS. zu (1). Seien m und n teilerfremd. Der Chinesische Restsatz (Satz LA2.15.61, Satz LA2.18.36, siehe auch Satz 3.14 unten) liefert uns, dass der Ringhomomorphismus

$$\mathbb{Z}/mn \to \mathbb{Z}/m \times \mathbb{Z}/n\,, \quad a \mapsto (a, a),$$

wobei wir die Restklasse von $a \in \mathbb{Z}$ in $\mathbb{Z}/mn$, $\mathbb{Z}/m$ und $\mathbb{Z}/n$ jeweils einfach wieder mit a bezeichnen, ein Isomorphismus ist. Dieser induziert einen Isomorphismus

$$(\mathbb{Z}/mn)^\times \to (\mathbb{Z}/m)^\times \times (\mathbb{Z}/n)^\times,$$

und wegen $\varphi(n) = \#(\mathbb{Z}/n)^\times$ (und entsprechend für m und n) erhalten wir die Behauptung.

zu (2). Es ist klar, dass $\varphi(p) = p - 1$ für jede Primzahl p gilt. Auch für eine Primzahlpotenz p^r ist das Abzählen relativ leicht, weil eine Zahl a zwischen 1 und $p^r - 1$ genau dann zu p^r teilerfremd ist, wenn Sie nicht durch p teilbar ist. Die durch p teilbaren Zahlen sind $p, \ldots, p^r - p$, und dies sind genau $p^{r-1} - 1$ Zahlen, es folgt also

$$\varphi(p^r) = p^r - 1 - (p^{r-1} - 1) = p^{r-1}(p-1).$$

zu (3). Sei $n \in \mathbb{N}_{>0}$. Wir betrachten die zyklische Gruppe $\mathbb{Z}/n$.

Behauptung. Sei d ein Teiler von n. Dann haben genau $\varphi(d)$ Elemente von $\mathbb{Z}/n$ die Ordnung d.

Bevor wir die Behauptung zeigen, begründen wir, dass daraus die gewünschte Aussage folgt. Denn $\mathbb{Z}/n$ hat n Elemente, und jedes Element hat als Ordnung einen Teiler von n. Indem wir die Elemente von $\mathbb{Z}/n$ also »gemäß ihrer Ordnung als Gruppenelement sortiert« zählen, erhalten wir die Summendarstellung von n aus dem Lemma.

Begründung. Dass die Restklasse von $r \in \mathbb{Z}$ in $\mathbb{Z}/n$ eine Untergruppe mit d Elementen erzeugt, ist dazu äquivalent, dass rd durch n teilbar ist, aber rd' für jeden echten Teiler d' von d nicht durch n teilbar ist, oder mit anderen Worten, dass $r \equiv a\frac{n}{d} \mod n$ für ein $a \in \{1, \ldots, d-1\}$ ist, das zu d teilerfremd ist. Es gibt also genau $\varphi(d)$ solcher Elemente. □

KOROLLAR 2.45. *Sei G eine zyklische Gruppe der Ordnung n. Dann enthält G genau $\varphi(n)$ Elemente der Ordnung $= n$, mit anderen Worten: genau $\varphi(n)$ Elemente, die jeweils die Gruppe G erzeugen.*

BEISPIEL 2.46. Sei G eine Gruppe, die nicht die triviale Gruppe ist und derart dass $\{1\}$ und G die einzigen Untergruppen von G sind. Dann ist G zyklisch von Primzahlordnung.

In der Tat ist klar, dass G zyklisch ist, denn für $g \in G$, $g \neq 1$, ist $\langle g \rangle$ eine nichttriviale Untergruppe von G, nach Voraussetzung also $= G$. Wäre $\mathrm{ord}(g)$ keine Primzahl und etwa d ein echter Teiler von $\mathrm{ord}(g)$, so wäre $\langle g^d \rangle$ eine echte Untergruppe von G. ◊

THEOREM 2.47. *Sei G eine endliche Gruppe. Dann sind äquivalent:*

(i) *die Gruppe G ist zyklisch,*

(ii) *zu jedem Teiler d der Gruppenordnung $\#G$ existiert genau eine Untergruppe $H \subseteq G$ mit d Elementen,*

(iii) *zu jedem Teiler d der Gruppenordnung $\#G$ existiert höchstens eine Untergruppe $H \subseteq G$ mit d Elementen,*

(iv) *für jeden Teiler d der Gruppenordnung $\#G$ gilt*

$$\#\{x \in G;\ x^d = 1\} = d,$$

(v) *für jeden Teiler d der Gruppenordnung $\#G$ gilt*

$$\#\{x \in G;\ x^d = 1\} \leq d,$$

(vi) *für jeden Teiler d der Gruppenordnung $\#G$ gilt*

$$\#\{x \in G;\ \mathrm{ord}(x) = d\} = \varphi(d),$$

(vii) *für jeden Teiler d der Gruppenordnung $\#G$ gilt*

$$\#\{x \in G;\ \mathrm{ord}(x) = d\} \leq \varphi(d).$$

Beweis. (i) $\Rightarrow$ (ii). Ist G eine endliche zyklische Gruppe, die von einem Element $g \in G$ erzeugt wird und ist d ein Teiler von $n := \#G$, so ist $\langle g^{n/d} \rangle$ eine Untergruppe von G mit d Elementen.

Ist andererseits H eine Untergruppe von G mit d Elementen, so hat der Quotient G/H genau $\frac{n}{d}$ Elemente, und es folgt $g^{n/d} \in H$. Weil wir bereits wissen, dass $\#\langle g^{n/d} \rangle = d$ gilt, folgt die Gleichheit.

Die Implikationen (ii) $\Rightarrow$ (iii), (iv) $\Rightarrow$ (v) und (vi) $\Rightarrow$ (vii) sind klar.

(iii) $\Rightarrow$ (vii). Ist x ein Element mit $\mathrm{ord}(x) = d$, so gilt also $\#\langle x \rangle = d$, und die (zyklische) Gruppe $\langle x \rangle$ enthält $\varphi(d)$ Elemente der Ordnung $= d$ (die alle diese Gruppe erzeugen). Gäbe es mehr als $\varphi(d)$ Elemente der Ordnung d, so könnten diese nicht alle in der Untergruppe $\langle x \rangle$ liegen. Da es höchstens eine Untergruppe der Ordnung d gibt, ist das unmöglich. Dasselbe Argument zeigt auch die Implikation (v) $\Rightarrow$ (vii).

(vii) $\Rightarrow$ (vi) $\Rightarrow$ (i). Wir haben in Lemma 2.44 gesehen, dass $\sum_{d \mid n} \varphi(n) = n$ gilt (wobei über alle positiven Teiler von n summiert werde). Da jedes Element von G als Ordnung einen Teiler der Gruppenordnung hat, kann (vii) nur gelten, wenn für jedes d Gleichheit gilt (also (vi) gilt), und dann existieren insbesondere Elemente der Ordnung $n = \#G$, also Elemente die G erzeugen.

Für die Implikation (i) $\Rightarrow$ (iv) genügt es, die (additive) Gruppe $\mathbb{Z}/n$ zu betrachten, und hier sind genau die Restklassen von $0, \frac{n}{d}, \ldots, (d-1)\frac{n}{d}$ die Elemente x mit $dx = 0$. □

Aus dem Theorem erhalten wir leicht den folgenden interessanten Satz, der für uns später noch nützlich sein wird.

Satz 2.48. *Sei K ein Körper und sei $G \subseteq K^\times$ eine endliche Untergruppe. Dann ist G zyklisch.*

Beweis. Sei $n = \#G$ und sei d ein Teiler von n. Alle Elemente $x \in G$ mit $x^d = 1$ sind dann Nullstellen des Polynoms $X^d - 1$. Wir wissen, dass dieses Polynom in K höchstens d Nullstellen hat. Die Bedingung (v) in Theorem 2.47 ist also erfüllt und es folgt, dass G zyklisch ist. □

Korollar 2.49. *Sei K ein endlicher Körper. Dann ist die Gruppe $K^\times$ zyklisch.*

Für einen anderen, etwas direkteren Beweis des Satzes siehe Theorem LA1.8.60. Siehe auch die sich dort anschließende Bemerkung über die Vermutung von E. Artin, dass (zum Beispiel) die Restklasse von 2 für unendlich viele p ein Erzeuger der Gruppe $\mathbb{F}_p^\times$ ist.

Man beachte aber, dass für allgemeines n die Gruppe $(\mathbb{Z}/n)^\times$ nicht zyklisch ist, zum Beispiel ist $(\mathbb{Z}/8)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ (wobei natürlich links die Multiplikation und rechts die Addition die Gruppenstruktur geben).

ERGÄNZUNG 2.50 (Primitivwurzeln modulo n). Von Gauß wurde der folgende Satz bewiesen, der die Frage klärt, für welche $n > 1$ die Gruppe $(\mathbb{Z}/n)^\times$ zyklisch ist. (Einen Erzeuger dieser Gruppe nennt man eine *Primitivwurzel* modulo n.)

SATZ 2.51. *Sei $n \in \mathbb{N}_{>1}$. Die Gruppe $(\mathbb{Z}/n)^\times$ ist genau dann zyklisch, wenn n eine der Zahlen der folgenden Liste ist:*

(1) $n = 2$,
(2) $n = 4$,
(3) $n = p^r$ *für eine Primzahl* $p > 2$ *und* $r \geq 1$,
(4) $n = 2p^r$ *für eine Primzahl* $p > 2$ *und* $r \geq 1$.

Siehe zum Beispiel [**Bu**] Kap. 2 §5. □ Ergänzung 2.50

2.5. Die symmetrische Gruppe

Wir bezeichnen mit S_n die *symmetrische Gruppe* »auf n Buchstaben«, also die Gruppe der Bijektionen $\{1, \ldots, n\} \xrightarrow{\sim} \{1, \ldots, n\}$. Aus der Linearen Algebra kennen wir den Begriff des r-Zykels, Definition LA1.8.36.

SATZ 2.52 (Zerlegung in disjunkte Zykel). *Jede Permutation $\sigma \in S_n$ lässt sich als Produkt von Zykeln der Ordnung > 1 und mit paarweise disjunkten Trägern schreiben. Diese Darstellung ist bis auf die Reihenfolge der Faktoren eindeutig.*

BEWEIS. »Anschaulich« ist die Sache einigermaßen klar, siehe Ergänzung LA1.8.38. Überlegen Sie selbst einmal, wie Sie einen formalen Beweis organisieren würden. Dies ist auch ein gutes Beispiel eines Satzes, der in vielen (Algebra-)Büchern bewiesen wird, und wo der Beweis teils auf ziemlich unterschiedliche Weise aufgeschrieben wurde – vergleichen Sie einige Beweise (zum Beispiel [**Bo-A**] 5.3 Satz 1 (ii), [**JS**] Kap. I Satz 3.3 (a), [**Lo**] Kap. 15, [**Lö**] Prop. 1.3.6) und schreiben Sie am Ende »den für Sie selbst besten Beweis« auf.

Sei $G = \langle\sigma\rangle$ die von σ erzeugte zyklische Gruppe. Dann operiert G auf $\{1, \ldots, n\}$. Wir bezeichnen mit $B_1, \ldots, B_r$ diejenigen Bahnen von G auf $\{1, \ldots, n\}$, die mehr als ein Element haben. Sei $b_i \in B_i$ jeweils ein fixiertes Element und sei $n_i = \#B_i$. Für $1 \leq m < n_i$ gilt dann $\sigma^m(b_i) \neq b_i$, denn sonst hätte B_i höchstens m Elemente. Es folgt

$$B_i = \{b_i, \sigma(b_i), \sigma^2(b_i), \ldots, \sigma^{n_i-1}(b_i)\}$$

(die Inklusion $\supseteq$ ist klar, und mit dem vorher gegebenen Argument sieht man leicht, dass die Elemente auf der rechten Seite paarweise verschieden sind, so dass beide Seiten gleich viele Elemente haben), und dass $\sigma^{n_i}(b_i) = b_i$ gilt. Wenn wir mit π_i den Zykel $(b_i, \sigma(b_i), \sigma^2(b_i), \ldots, \sigma^{n_i-1}(b_i))$ bezeichnen, erhalten wir mit

$$\sigma = \pi_1 \cdots \pi_r$$

eine Zerlegung von σ als Produkt von Zykeln mit disjunkten Trägern.

Zur Eindeutigkeit beobachten wir zunächst, dass die in so einer Zerlegung auftretenden Zykel bijektiv den Bahnen von σ entsprechen müssen, die mehr als ein Element haben, weil die Träger dieser Zykel nach Voraussetzung disjunkt sind. Fixieren wir eine dieser Bahnen, etwa B, so stimmen die Einschränkung von σ und des der Bahn entsprechenden Zykel als Abbildungen $B \to B$ überein, und folglich sind die einzelnen Zykel in der Zerlegung eindeutig bestimmt. □

Bei der Eindeutigkeitsaussage ist zu beachten, dass sich die Eindeutigkeit eines Zykels auf die Eindeutigkeit als Permutation, nicht auf die Schreibweise bezieht, zum Beispiel gilt $(1234) = (2341) = (3412) = (4123)$.

Jeder Permutation σ können wir ihr *Signum* oder *Vorzeichen* $\operatorname{sgn}(\sigma) \in \{1, -1\}$ zuordnen. Die Signumabbildung $S_n \to \{1, -1\}$ ist ein Gruppenhomomorphismus.

DEFINITION 2.53. Wir schreiben $A_n = \operatorname{Ker}(\operatorname{sgn})$ und nennen diesen Normalteiler von S_n die *alternierende Gruppe*. ⊣

SATZ 2.54 (Satz von Cayley). *Sei G eine Gruppe, und sei $\operatorname{Bij}(G)$ die Gruppe der bijektiven Abbildungen $G \to G$ (mit der Verkettung von Abbildungen als Verknüpfung). Für $g \in G$ liegt die Abbildung $m_g \colon G \to G, x \mapsto gx$, in $\operatorname{Bij}(G)$ und die Abbildung*

$$G \to \operatorname{Bij}(G), \quad g \mapsto m_g,$$

ist ein injektiver Gruppenhomomorphismus.

Insbesondere gilt: Jede endliche Gruppe ist isomorph zu einer Untergruppe einer symmetrischen Gruppe.

BEWEIS. Für $g \in G$ definiert die Vorschrift $x \mapsto gx$ eine Abbildung $m_g \colon G \to G$ (dies ist kein Gruppenhomomorphismus, wenn g nicht das neutrale Element von G ist). Die Abbildung m_g ist bijektiv, denn ist $h \in G$ das inverse Element zu g, so ist m_h die Umkehrabbildung von m_g.

Wir erhalten eine Abbildung $G \to \operatorname{Bij}(G), g \mapsto m_g$. Diese Abbildung ist ein Gruppenhomomorphismus, denn für Elemente $g, h \in G$ gilt:

$$m_{h'}(x) = (gh)x = g(hx) = m_g(m_h(x)) = (m_g \circ m_h)(x).$$

(Dieser Gruppenhomomorphismus ist genau derjenige, der der Wirkung von G auf sich selbst durch Multiplikation von links entspricht.)

Zudem ist die Abbildung $g \to m_g$ injektiv. Es genügt dafür zu zeigen, dass nur das neutrale Element von G auf das neutrale Element von S_n abgebildet wird. Aber wenn $m_g = \mathrm{id}$ die Identitätsabbildung ist, dann folgt $gx = x$ für alle $x \in G$, und diese Eigenschaft charakterisiert das neutrale Element von G.

Der Zusatz folgt, weil für eine endliche Gruppe mit n Elementen jede Bijektion zwischen G und der Menge $\{1, \ldots, n\}$ einen Gruppenisomorphismus $\operatorname{Bij}(G) \xrightarrow{\sim} S_n$ induziert. □

ERGÄNZUNG 2.55 (Konjugationsklassen der symmetrischen Gruppe). Die Zykelzerlegung gibt auch Aufschluss über die *Konjugationsklassen* in der symmetrischen Gruppe S_n, also über die Bahnen unter der Konjugationsoperation von S_n auf sich selbst, oder noch anders gesagt über die Äquivalenzklassen in S_n bezüglich der Äquivalenzrelation

$$g \sim g' \quad \Longleftrightarrow \quad \text{es existiert } h \text{ mit } g' = hgh^{-1}.$$

Die Konjugationsklassen zu verstehen, gibt oft sehr interessante Informationen über die Struktur einer Gruppe und ist insbesondere in der Darstellungstheorie (siehe Ergänzungsabschnitt 2.8.4) von Bedeutung.

Für $\sigma \in S_n$ mit Zerlegung $\sigma = \pi_1 \cdots \pi_r$ in Zykel der Ordnung > 1 mit disjunkten Trägern nennen wir das absteigend geordnete Tupel der Ordnungen der Zykel π_i, ergänzt um Einsen (je eine 1 für jedes Element $\{1, \ldots, n\}$, das von σ auf sich selbst abgebildet wird) den *Zykeltyp* von σ. Zum Beispiel hat

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 8 & 2 & 5 & 9 & 3 & 6 & 7 \end{pmatrix} = (142)(38697)$$

den Zykeltyp $(5, 3, 1)$. Die Ergänzung um Einsen (sozusagen für die 1-Zykel, die wir in der Zykelzerlegung nicht hinschreiben) hat zur Folge, dass für jedes $\sigma \in S_n$ die Summe aller Einträge des Zykeltyps gleich n ist.

Dann gilt der folgende Satz:

SATZ 2.56. *Permutationen $\sigma, \tau \in S_n$ sind genau dann zueinander konjugiert, wenn sie denselben Zykeltyp haben.*

Siehe [**Soe**] Abschnitt 5.5. □ Ergänzung 2.55

2.6. Auflösbare Gruppen

Um die Struktur einer Gruppe zu untersuchen, liegt es nahe zu versuchen, sie »in kleinere Teile zu zerlegen«, die man dann unabhängig voneinander betrachten kann. Im einfachsten Fall eines Produkts von Gruppen $G \times H$ kann man tatsächlich alle interessanten Eigenschaften des Produkts beschreiben, wenn man die Faktoren G und H hinreichend genau versteht.

Allgemeiner kann man, gegeben eine Gruppe G, versuchen, einen Normalteiler $H \subseteq G$ zu finden und dann G zu verstehen, indem man H und den Quotienten G/H anschaut. Der Satz von Lagrange sagt zum Beispiel, dass man die Ordnung der Gruppe G aus den Ordnungen von H und G/H (nämlich als deren Produkt) berechnen kann. Für andere Eigenschaften ist es schwieriger (zum Beispiel sind für kommutatives G natürlich stets H und G/H kommutativ; die Umkehrung gilt aber nicht, wie Sie sich an einem Beispiel überlegen sollten). Dennoch ist der Ansatz grundsätzlich nützlich. Er lässt sich weiter verfeinern, indem man mit H und G/H genauso verfährt und dort nach echten Normalteilern sucht, usw. Äquivalent dazu ist es (vergleiche Lemma 2.16), in G eine Kette von Untergruppen zu suchen, so dass jede in der nächstgrößeren ein Normalteiler ist. Diesen Ketten geben wir den Namen *Normalreihe*.

DEFINITION 2.57. Sei G eine Gruppe. Eine *Normalreihe* in G ist eine Kette

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$$

von Untergruppen von G, so dass für alle i die Untergruppe G_{i+1} ein Normalteiler von G_i ist. Die Gruppenquotienten G_i/G_{i+1} nennt man auch die *Subquotienten* der Normalreihe. ⊣

Man beachte, dass die Untergruppen G_i (für $i > 1$) einer Normalreihe im allgemeinen keine Normalteiler von G sein werden (und suche ein Beispiel, wo das tatsächlich nicht der Fall ist – gegebenenfalls können Sie in Satz 2.65 fündig werden).

Auch wenn, wie gesagt, die Gruppe G durch die Subquotienten einer Normalreihe nicht eindeutig bestimmt ist, liefern diese doch eine gewisse Menge an Information über die Gruppe G. Wenn G außer $\{1\}$ und G gar keine Normalteiler besitzt, dann ist natürlich eine solche Zerlegung nicht möglich; diese Gruppen nennt man *einfache* Gruppen und solche Gruppen müssen mit anderen Methoden untersucht werden. Siehe Abschnitt 2.8 und speziell Ergänzung 2.70.

In diesem Abschnitt wollen wir uns mit dem verhältnismäßig einfachen Fall von Gruppen befassen, die eine Normalreihe besitzen, deren Subquotienten sämtlich kommutative Gruppen sind.

DEFINITION 2.58. Sei G eine Gruppe. Wir nennen G *auflösbar*, wenn eine Normalreihe

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$$

in G existiert, derart dass alle Quotienten G_i/G_{i+1} *abelsche* Gruppen sind. ⊣

Offenbar ist jede abelsche Gruppe auflösbar, aber zum Beispiel auch die Gruppen S_3 (das ist recht leicht zu sehen) und S_4 (siehe Satz 2.65).

Ein nützliches Werkzeug zum Studium dieser Eigenschaft ist die sogenannte Kommutatoruntergruppe, die wir als nächstes einführen.

DEFINITION 2.59. Sei G eine Gruppe.

(1) Für Elemente $g, h \in G$ heißt
$$[g,h] := ghg^{-1}h^{-1}$$
der *Kommutator* der Elemente g und h.

(2) Für Untergruppen $H, H' \subseteq G$ bezeichnen wir mit $[H,H']$ die von allen Elementen der Form $[h,h']$, $h \in H, h' \in H'$ erzeugte Untergruppe von G.

(3) Die Untergruppe $[G,G] \subseteq G$, also die von allen Elementen der Form $[g,h]$, $g,h \in G$, erzeugte Untergruppe von G, heißt die *Kommutatoruntergruppe* von G.

⊣

SATZ 2.60. *Sei G eine Gruppe. Dann ist $[G,G]$ ein Normalteiler von G und der Quotient $G_{ab} = G/[G,G]$ ist eine abelsche Gruppe und hat die folgende universelle Eigenschaft (und heißt deshalb der* maximale abelsche Quotient *der Gruppe G):*

Ist H eine abelsche Gruppe und $f\colon G \to H$ ein Gruppenhomomorphismus, so faktorisiert f eindeutig über G_{ab}, d.h. es existiert ein eindeutig bestimmter Gruppenhomomorphismus $\varphi\colon G_{ab} \to H$, so dass f mit der Verkettung von φ und der kanonischen Projektion $G \to G_{ab}$ übereinstimmt.

BEWEIS. Für $g,h,x \in G$ gilt
$$x[g,h]x^{-1} = xghg^{-1}h^{-1}x^{-1} = xgx^{-1}xhx^{-1}xg^{-1}x^{-1}xh^{-1}x^{-1} = [xgx^{-1}, xhx^{-1}] \in [G,G].$$
Es folgt $x[G,G]x^{-1} \subseteq [G,G]$ und (mit derselben Rechnung für x^{-1} anstelle von x) sogar $x[G,G]x^{-1} = [G,G]$. Weil das Argument für alle $x \in G$ gültig ist, sehen wir, dass $[G,G]$ ein Normalteiler in G ist. Ist $\pi\colon G \to G/[G,G]$ die kanonische Projektion, so gilt $\pi([g,h]) = 1$, also $\pi(g)\pi(h) = \pi(h)\pi(g)$ für alle $g,h \in G$. Weil π surjektiv ist, folgt, dass $G_{\mathrm{ab}} = G/[G,G]$ abelsch ist.

Ist H abelsch, so bildet jeder Gruppenhomomorphismus $f\colon G \to H$ Elemente der Form $[g,h]$ auf das neutrale Element in H ab. Nach dem Homomorphiesatz faktorisiert f über einen eindeutig bestimmten Gruppenhomomorphismus $G_{\mathrm{ab}} \to H$. □

BEISPIEL 2.61. (1) Die Kommutatoruntergruppe einer Gruppe G ist genau dann die triviale Gruppe, wenn G kommutativ ist.

(2) Sei K ein Körper und $n \in \mathbb{N}$. Weil der Quotient $GL_n(K)/SL_n(K) \cong K^\times$ abelsch ist, liegt die Kommutatoruntergruppe von $GL_n(K)$ in der speziellen linearen Gruppe $SL_n(K)$. Man kann zeigen (vergleiche LA1, WS20/21, Hausaufgabe 11.4), dass sogar $[GL_n(K), GL_n(K)] = SL_n(K)$ gilt, es sei denn es ist $K = \mathbb{F}_2$ und $n = 2$ (in diesem Fall ist $SL_2(\mathbb{F}_2) = GL_2(\mathbb{F}_2) \cong S_3$, und die Kommutatoruntergruppe hat 3 Elemente).

Man kann weiterhin zeigen, dass die Gruppe $GL_n(K)$ genau dann auflösbar ist, wenn $n = 1$ oder wenn $n = 2$ und $\#K \leq 3$ ist.

◊

LEMMA 2.62. *Sei G eine Gruppe. Sei $D^0G = G$, $D^1G := [G,G]$, und allgemein $D^iG = [D^{i-1}G, D^{i-1}G]$ für $i \geq 1$. Dann sind äquivalent:*

(i) *Die Gruppe G ist auflösbar.*

(ii) *Es existiert $n \in \mathbb{N}$, so dass $D^n G$ die triviale Gruppe ist.*

BEWEIS. Sei zunächst G auflösbar und

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$$

eine Normalreihe mit abelschen Subquotienten. Weil G_0 / G_1 abelsch ist, folgt $DG \subseteq G_1$. Induktiv sehen wir dann $D^i \subseteq G_i$ für alle i und insbesondere $D^r G = 1$.

Ist andererseits $D^n G = 1$, so ist

$$G \supset DG \supset D^2 G \supset \cdots \supset D^n G = \{1\}$$

eine Normalreihe mit abelschen Quotienten. □

LEMMA 2.63. (1) *Sei G eine auflösbare Gruppe. Dann ist jede Untergruppe $H \subseteq G$ auflösbar.*

(2) *Sei G eine Gruppe und sei $H \subseteq G$ ein Normalteiler. Sei $\pi\colon G \to G/H$ die kanonische Projektion auf den Quotienten. Dann sind äquivalent:*

  (i) *Die Gruppe G ist auflösbar.*

  (ii) *Die Gruppen H und G/H sind auflösbar.*

(3) *Seien $G_1, \ldots, G_n$ Gruppen. Das Produkt $\prod_{i=1}^n G_i$ ist genau dann auflösbar, wenn alle G_i, $i = 1, \ldots, n$, auflösbar sind.*

BEWEIS. Teil (1) folgt aus dem vorherigem Lemma, weil $D^i H \subseteq D^i G$ für alle i gilt.

In Teil (2) ist für die Implikation (i) $\Rightarrow$ (ii) nun nur noch die Auflösbarkeit von G/H zu zeigen. Das folgt daraus, dass $\pi(D^i G) = D^i(G/H)$ gilt, wie man leicht per Induktion nach i zeigt. (Alternativ kann man Lemma 2.16 (6) und Korollar 2.25 benutzen, um zu sehen, dass eine Normalreihe von G mit abelschen Subquotienten unter π auf eine Normalreihe von G/H mit abelschen Subquotienten abgebildet wird.)

Zur Umkehrung (ii) $\Rightarrow$ (i) betrachten wir Normalreihen

$$H = H_0 \supset H_1 \supset \cdots \supset H_r = \{1\}$$

und

$$G/H = \bar{G}_0 \supset \bar{G}_1 \supset \cdots \supset \bar{G}_s = \{1\}$$

mit abelschen Subquotienten. Dann ist

$$G = \pi^{-1}(\bar{G}_0) \supset \pi^{-1}(\bar{G}_1) \supset \cdots \supset \pi^{-1}(\bar{G}_s) = H = H_0 H_1 \supset \cdots \supset H_r = \{1\}$$

eine Normalreihe von G (Lemma 2.16 (6)) mit abelschen Subquotienten, denn aus dem Homomorphiesatz (oder alternativ aus Korollar 2.25, denn $\pi^{-1}(\bar{G}_i)/H = \bar{G}_i$) folgt

$$\pi^{-1}(\bar{G}_i)/\pi^{-1}(\bar{G}_{i+1}) \cong \bar{G}_i/\bar{G}_{i+1}$$

für alle i. (Alternativ kann man auch hier mit den iterierten Kommutatoruntergruppen argumentieren.)

Teil (3) folgt für ein Produkt mit zwei Faktoren aus Teil (2) (denn H ist ein Normalteiler von $H \times H'$) und im Allgemeinen dann per Induktion. □

LEMMA 2.64. *Sei G eine endliche Gruppe. Dann sind äquivalent:*

(i) *Die Gruppe G ist auflösbar.*

(ii) *Es existiert eine Kette*

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$$

von Untergruppen von G, so dass für alle i die Untergruppe G_i ein Normalteiler von G_{i+1} ist und der Quotient G_i / G_{i+1} eine zyklische Gruppe ist.

BEWEIS. Die Implikation (ii) $\Rightarrow$ (i) ist trivial und für die Richtung (i) $\Rightarrow$ (ii) können wir eine Normalreihe von G mit abelschen Subquotienten verfeinern, indem wir zusätzliche Untergruppen so hinzufügen, dass die Normalreiheneigenschaft erhalten bleibt und nach diesem Prozess alle Subquotienten zyklisch sind.

Das bedeutet, dass es genügt zu zeigen, dass jede abelsche Gruppe eine Normalreihe mit zyklischen Subquotienten besitzt. Das zeigen wir durch Induktion nach der Gruppenordnung. Der Induktionsanfang ist klar. Im allgemeinen betrachten wir für gegebenes $G \neq 1$ irgendein Element $g \in G$, das vom neutralen Element verschieden ist. Dann ist $\langle g \rangle \subseteq G$ ein Normalteiler und eine zyklische Gruppe. Nach Induktionsvoraussetzung existiert eine Normalreihe von $G / \langle g \rangle$ mit zyklischen Subquotienten, und durch Zusammensetzen wie im Beweis von Lemma 2.63 erhalten wir eine Normalreihe von G mit zyklischen Subquotienten. □

Der folgende Satz liefert uns einige nicht-triviale Beispiele für auflösbare und (vor allem) für nicht auflösbare Gruppen, und er wird am Ende der Vorlesung bei der Anwendung der Galois-Theorie auf die Frage der Auflösbarkeit von Gleichungen durch Radikale noch einmal nützlich sein.

SATZ 2.65. (1) *Für alle $n \geq 2$ gilt $[S_n, S_n] = A_n$.*

(2) *Für $n \leq 4$ sind S_n und A_n auflösbar.*

(3) *Für $n > 4$ sind weder S_n noch A_n auflösbar.*

BEWEIS. zu (1). Weil der Quotient $S_n / A_n \cong \{1, -1\}$ abelsch ist, faktorisiert die Signum-Abbildung über $(S_n)_{\mathrm{ab}}$, also ist $A_n \subseteq [S_n, S_n]$. Für $n = 2$ ist auch die Gleichheit klar. Sei nun $n \geq 3$ und $\sigma \in A_n$. Die Aussage in (1) folgt dann aus den folgenden beiden Behauptungen:

Behauptung 1. Jedes Element von A_n ist Produkt von 3-Zykeln.

Begründung. Es genügt zu zeigen, dass das Produkt von zwei verschiedenen Transpositionen stets ein Produkt von 3-Zykeln ist, weil sich jedes Element von A_n als ein Produkt einer geraden Anzahl von Transpositionen schreiben lässt. Nun können wir für paarweise verschiedene Elemente a, b, c bzw. a, b, c, d von $\{1, \ldots, n\}$ schreiben:

$$(a, b)(b, c) = (a, b, c), \qquad (a, b)(c, d) = (a, c, b)(a, c, d).$$

Behauptung 2. Jeder 3-Zykel ist ein Kommutator von Elementen von S_n.

Begründung. Seien $a, b, c \in \{1, \ldots, n\}$ paarweise verschieden. Dann gilt

$$(a, b, c) = (a, c)(b, c)(a, c)(b, c) = [(a, c), (b, c)].$$

zu (2). Es ist leicht zu sehen, dass S_1, S_2 und S_3 auflösbar sind. (Prüfen Sie das nach!) Wir betrachten nun die symmetrische Gruppe S_4, eine Gruppe mit 24 Elementen. Die Untergruppe A_4 hat also 12 Elemente, und nach Teil (1) genügt es zu zeigen, dass A_4 auflösbar ist.

Behauptung. $[A_4, A_4] = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.

Begründung. Wir schreiben $V = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. Dies ist offenbar eine Untergruppe von A_4, und isomorph zu $\mathbb{Z}/2 \times \mathbb{Z}/2$. Man rechnet nun direkt nach, dass V ein Normalteiler ist. Daraus folgt, dass $[A_4, A_4] \subseteq V$ ist, weil der Quotient A_4 / V als Gruppe mit 3 Elementen jedenfalls abelsch ist. Die Inklusion $V \subseteq [A_4, A_4]$ kann man wiederum direkt nachrechnen, zum Beispiel gilt, weil alle 3-Zykel in der alternierenden Gruppe liegen,

$$(12)(34) = [(123), (124)] \in [A_4, A_4].$$

Weil V abelsch ist, folgt aus der Behauptung sofort die Auflösbarkeit von A_4.

zu (3). Sei nun $n \geq 5$. Wir haben im Beweis von Teil (1) gesehen, dass jedes Element von A_n ein Produkt von 3-Zykeln ist. Es genügt also zu zeigen, dass jeder 3-Zykel sich als Kommutator von 3-Zykeln ausdrücken lässt. Seien $a, b, c \in \{1, \ldots, n\}$ paarweise verschieden. Weil $n \geq 5$ ist, können wir Elemente $d \neq e$ wählen, die von a, b und c verschieden sind und haben dann

$$(a, b, c) = [(a, b, d), (a, c, e)].$$

□

Mit ähnlichen Methoden (aber etwas mehr Arbeit ...) kann man die Verschärfung von Teil (3) dieses Satzes zeigen, dass für $n \geq 5$ die Gruppe A_n einfach ist, also überhaupt keine nicht-trivialen Normalteiler besitzt.

Wir geben zum Schluss als Ergänzungen noch einige Ergebnisse über nicht notwendig auflösbare Gruppen an, von denen der folgende Satz von Jordan-Hölder recht einfach, der Satz von Feit und Thompson und vor allem die Klassifikation der endlichen einfachen Gruppen aber extrem schwierig zu beweisen sind.

Ergänzung 2.66 (Kompositionsreihen und der Satz von Jordan-Hölder).

Definition 2.67. Eine Gruppe G heißt *einfach*, wenn G nicht die triviale Gruppe ist und $\{1\}$ und G die einzigen Normalteiler von G sind. ⊣

Definition 2.68. Sei G eine Gruppe. Eine Normalreihe von G heißt *Kompositionsreihe*, wenn alle Subquotienten einfache Gruppen sind. ⊣

Ist G eine endliche Gruppe, so kann man offenbar jede Normalreihe zu einer Kompositionsreihe verfeinern, indem man gegebenenfalls zusätzliche Untergruppen einfügt (vergleiche Lemma 2.16). Weil G endlich ist, muss dieser Prozess irgendwann abbrechen. Insbesondere besitzt jede endliche Gruppe eine Kompositionsreihe.

Satz 2.69 (Satz von Jordan-Hölder). *Sei G eine endliche Gruppe. Je zwei Kompositionsreihen einer endlichen Gruppe haben die gleiche Länge und die Subquotienten einer Kompositionsreihe sind bis auf Reihenfolge und Isomorphie eindeutig bestimmt.*

Beweis. Explizit ausgeschrieben bedeutet der Satz also, dass für Kompositionsreihen

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$$
$$G = G'_0 \supset G'_1 \supset \cdots \supset G'_r = \{1\}$$

von G gelten muss, dass $r = s$ ist, und dass es eine Permutation $\sigma \in S_r$ sowie Isomorphismen $G_{i-1}/G_i \cong G'_{\sigma(i)-1}/G'_{\sigma(i)}$ für alle $i = 1, \ldots, r$ gibt.

Wir führen zum Beweis Induktion nach $\#G$. Für die triviale Gruppe ist nichts zu zeigen.

Ist $G'_1 \subseteq G_1$, so muss sogar die Gleichheit gelten, denn sonst wäre das Bild von G_1 unter der kanonischen Projektion nach G/G'_1 ein nicht-trivialer Normalteiler. Wenn tatsächlich $G_1 = G'_1$ gilt, so folgt die Aussage direkt aus der Induktionsvoraussetzung.

Wir betrachten nun den Fall, dass $G_1 \not\subseteq G'_1$ und $G'_1 \not\subseteq G_1$ gilt. Dann ist das Bild H von G_1 unter der kanonischen Projektion $G \to G/G'_1$ ein Normalteiler der einfachen Gruppe G/G'_1, der nicht die triviale Gruppe ist, wegen der Einfachheit also gleich G/G'_1. Mit anderen Worten: Die Abbildung $G_1 \to G/G'_1$ ist surjektiv, und sie induziert nach dem Homomorphiesatz einen Isomorphismus $G_1/G_1 \cap G'_1 \cong G/G'_1$. Genauso erhalten wir einen Isomorphismus $G'_1/G_1 \cap G'_1 \cong G/G_1$.

Sei nun

$$H = H_0 \supset H_1 \supset \cdots \supset H_t = \{1\}$$

irgendeine Kompositionsreihe von $H := G_1 \cap G_1'$. Das oben Gesagte impliziert, dass die beiden Kompositionsreihen

$$G = G_0 \supset G_1 \supset G_1 \cap G_1' = H \supset H_1 \supset \cdots \supset H_t = \{1\},$$
$$G = G_0' \supset G_1' \supset G_1 \cap G_1' = H \supset H_1 \supset \cdots \supset H_t = \{1\}$$

bis auf Reihenfolge und Isomorphie dieselben Subquotienten haben. Offenbar haben sie auch dieselbe Länge. Andererseits haben auch die beiden Kompositionsreihen

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\},$$
$$G = G_0 \supset G_1 \supset G_1 \cap G_1' = H \supset H_1 \supset \cdots \supset H_t = \{1\}$$

einerseits (Induktionsvoraussetzung angewandt auf G_1) und

$$G = G_0' \supset G_1' \supset \cdots \supset G_r' = \{1\},$$
$$G = G_0' \supset G_1' \supset G_1 \cap G_1' = H \supset H_1 \supset \cdots \supset H_t = \{1\}$$

andererseits (Induktionsvoraussetzung angewandt auf G_1') dieselben Längen und bis auf Reihenfolge und Isomorphie dieselben Subquotienten. Indem wir alles zusammensetzen, erhalten wir die Behauptung. □

Wie man am Beweis sieht, lässt sich das Prinzip des Satzes von Jordan-Hölder auf andere Situationen übertragen, in denen ein ähnlicher Formalismus von Unterobjekten, Quotienten und dem Homomorphiesatz zur Verfügung steht. □ Ergänzung 2.66

ERGÄNZUNG 2.70 (Endliche einfache Gruppen). Wie oben bemerkt, können wir für jede endliche Gruppe eine Kompositionsreihe finden, also eine Normalreihe, die nicht weiter verfeinert werden kann. Nach dem Satz von Jordan-Hölder sind sogar die Länge einer solchen Kompositionsreihe und die einfachen Gruppen, die dort als Subquotienten auftreten, mit den jeweiligen Vielfachheiten bis auf Isomorphismus eindeutig bestimmt. Andererseits liefern diese Ergebnisse keinerlei Aussagen über einfache Gruppen selbst, also über Gruppen, die keine nicht-trivialen Normalteiler besitzen.

Es ist eine naheliegende Frage, ob man diese einfachen Gruppen besser verstehen kann, zum Beispiel ob man sie »auflisten« kann, genauer, ob man eine vollständige Liste der endlichen einfachen Gruppen bis auf Isomorphie angeben kann, also eine Liste, so dass jede endliche Gruppe zu genau einer der Gruppen auf der Liste isomorph ist (vergleiche Beispiel 2.6), wo wir entsprechende Listen für Gruppen der Ordnung ≤ 6 angegeben haben.

Das ist tatsächlich möglich (wenn auch nicht einfach). Der folgende Satz beantwortet die Frage im wesentlichen; in der dort angegebenen Liste gibt es einige Überschneidungen, d.h. einige der genannten Gruppen sind zueinander isomorph, aber diese sind gut verstanden. Wir werden aber die Gruppen unter (3), (4) und (5) hier nicht definieren.

THEOREM 2.71 (Klassifikation der endlichen einfachen Gruppen). *Sei G eine endliche einfache Gruppe, d.h. eine endliche Gruppe, die außer G und $\{1\}$ keine Normalteiler besitzt. Dann ist G isomorph zu einer der Gruppen der folgenden Liste:*

(1) *Zyklische Gruppen $\mathbb{Z}/p$ für eine Primzahl p,*
(2) *Alternierende Gruppen A_n für $n \geq 5$,*
(3) *Gruppen »vom Lie-Typ«,*
(4) *die Tits-Gruppe,*
(5) *eine der 26 sporadischen endlichen einfachen Gruppen.*

Von den Gruppen dieser Liste haben wir die zyklischen Gruppen von Primzahlordnung (dies sind genau die abelschen Gruppen auf der Liste) und die alternierenden Gruppen bereits kennengelernt.

Die (einfachen) endlichen Gruppen vom Lie-Typ (benannt nach Sophus Lie[1]) hängen eng mit Matrix-Gruppen zusammen. Zum Beispiel liefert die folgende Konstruktion eine unendliche Familie endlicher einfacher Gruppen. Wir betrachten einen endlichen Körper K und $n \in \mathbb{N}$, $n > 1$. Die Gruppe $SL_n(K)$ ist im Allgemeinen nicht einfach, denn ihr Zentrum

$$Z_{SL_n(K)} = \{\mathrm{diag}(\zeta, ..., \zeta);\ \zeta \in K,\ \zeta^n = 1\}$$

ist im Allgemeinen nicht-trivial. Der Quotient $PSL_n(K) := SL_n(K)/Z_{SL_n(K)}$ ist eine einfache Gruppe, es sei denn es ist $n = 2$ und $\#K \leq 3$. Die Gruppen $PSL_n(K)$ sind Gruppen vom Lie-Typ, und die anderen solchen Gruppen entstehen, grob gesprochen, durch ähnliche Matrix-Konstruktionen.

Die ersten drei Punkte auf der Liste umfassen jeweils unendlich viele Gruppen (jeweils mit »ähnlicher Struktur« bzw. ähnlichen Konstruktionsmethoden). Der vierte Punkt umfasst nur eine einzige Gruppe, die nach Jacques Tits[2] benannte Tits-Gruppe, die eng mit den endlichen Gruppen vom Lie-Typ verwandt ist (und daher manchmal auch zu diesen hinzugerechnet wird; von anderen Autoren wird sie zu den sporadischen Gruppen hinzugefügt, so dass diese von 27 sporadischen Gruppen sprechen).

Als die sporadischen Gruppen werden die endlich vielen verbleibenden Gruppen genannt, die nicht in natürlicher Weise in eine der unendlichen Familien aus den Punkten (1) bis (3) eingeordnet werden können und für die jeweils ad hoc eine Konstruktion angegeben werden muss. Die kleinste der sporadischen Gruppen ist die sogenannte Mathieu-Gruppe M_{11} mit 7920 Elementen, die größte ist die Monster-Gruppe[3] mit

$$808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000$$

Elementen. Das Problem dabei, mit dieser Gruppe zu arbeiten und sie zu verstehen ist dabei nicht einmal so sehr die Größe der Gruppe. Die Gruppe A_{50} hat beispielsweise noch mehr Elemente, aber wenn zwei Elemente (als Permutationen von $\{1, ..., 50\}$ mit Signum 1) gegeben sind, könnte man diese notfalls sogar per Hand multiplizieren. Für die Elemente der Monstergruppe gibt es aber, wie man weiß, keine derart einfache »Realisierung« durch Permutationen (oder durch Matrizen). Der Satz von Cayley besagt zwar, dass man auch diese Gruppe mit einer Untergruppe einer symmetrischen Gruppe S_n identifizieren kann. Aber hier muss n mindestens $97,239,461,142,009,186,000$ sein! Möchte man die Monstergruppe als Untergruppe einer Gruppe der Form $GL_n(K)$, K ein Körper, realisieren (also einen Isomorphismus mit so einer Untergruppe finden), muss $n \geq 196,882$ gelten.

[1] https://de.wikipedia.org/wiki/Sophus_Lie
[2] https://de.wikipedia.org/wiki/Jacques_Tits
[3] https://de.wikipedia.org/wiki/Monstergruppe

Übersichtsartikel zur Klassifikation der endlichen einfachen Gruppen:

M. Aschbacher, *The Status of the Classification of the Finite Simple Groups*, Notices of the A. M. S. **51**, no. 7 (2004), 736–740,
https://www.ams.org//notices/200407/fea-aschbacher.pdf

R. Solomon, *A brief history of the classification of the finite simple groups*, Bull. A. M. S. **38**, no. 3 (2001), 315–352,
https://www.ams.org/journals/bull/2001-38-03/S0273-0979-01-00909-0/

Ein spektakulärer Zusammenhang zwischen Monstergruppe und sogenannten Modulformen, die in der Zahlentheorie auftreten, wurde Ende der 1980er Jahre von Conway und Norton vermutet (monstrous moonshine conjecture[a]) und 1992 von Borcherd bewiesen, der unter anderem dafür mit der Fields-Medaille ausgezeichnet wurde.

R. Borcherds, *What is ... the Monster?*
http://www.ams.org/notices/200209/what-is.pdf

M. Ronan, *Symmetry and the Monster*, Oxford University Press 2006.

[a] https://en.wikipedia.org/wiki/Monstrous_moonshine

Der Beweis des Klassifikationstheorems ist *sehr lang* – von der Wikipedia[4]-Seite: »The proof of the theorem consists of tens of thousands of pages in several hundred journal articles written by about 100 authors, ...«

Eine konkrete Aussage, die man mithilfe der Klassifikation der einfachen endlichen Gruppen beweisen konnte, für die aber kein direkter Beweis bekannt ist, ist Teil (2) des folgenden Satzes[5]. Teil (1) wurde schon 1903 von Frobenius bewiesen, und Teil (2) wurde von ihm als Vermutung formuliert.

SATZ 2.72. *Sei G eine endliche Gruppe und sei n ein Teiler von $\#G$.*

(1) *Die Anzahl der Elemente $x \in G$ mit $x^n = 1$ ist ein Vielfaches von n.*

(2) *Wenn es genau n Elemente $x \in G$ mit $x^n = 1$ gibt, dann bilden diese Elemente einen Normalteiler von G.*

□ Ergänzung 2.70

ERGÄNZUNG 2.73 (Satz von Feit-Thompson[6]). Der Satz von Feit und Thompson ist der folgende einfach zu formulierende und zunächst überraschende Satz.

THEOREM 2.74. *Sei G eine endliche Gruppe, für die $\#G$ ungerade ist. Dann ist G auflösbar.*

Der Beweis von Feit und Thompson wurde 1963 veröffentlich und umfasst 250 Seiten. Nach wie vor sind keine wesentlich kürzeren Beweise bekannt. Der Beweis konnte 2012 (nach mehrjähriger Arbeit daran) soweit formalisiert werden, dass er von dem System Coq[7] verifiziert werden konnte.

Man kann den Satz in äquivalenter Weise so formulieren: Sei G eine endliche einfache Gruppe, die nicht abelsch ist. Dann ist $\#G$ eine gerade Zahl. Insofern ist (mehr oder weniger...)

[4] https://en.wikipedia.org/wiki/Classification_of_finite_simple_groups
[5] https://en.wikipedia.org/wiki/Frobenius%27s_theorem_(group_theory)
[6] https://de.wikipedia.org/wiki/Satz_von_Feit-Thompson
[7] https://de.wikipedia.org/wiki/Coq_(Software)

klar, dass man den Satz von Feit und Thompson auch als Korollar zur Klassifikation der endlichen einfachen Gruppen erhalten könnten – aber das wäre sozusagen mit Kanonen auf Spatzen geschossen. □ Ergänzung 2.73

2.7. Die Sylow-Sätze

Wir beginnen diesen Abschnitt mit der Beobachtung (Satz 2.76), dass jede Gruppe, deren Ordnung die Potenz einer Primzahl ist, auflösbar ist.

DEFINITION 2.75. Seien p eine Primzahl und G eine endliche Gruppe. Wir nennen G eine *p-Gruppe*, wenn die Ordnung von G eine Potenz von p ist. ⊣

(Wir lassen hier den Fall p^0, also den Fall der trivialen Gruppe auch zu, weil es im folgenden einige Formulierungen vereinfacht.)

SATZ 2.76. *Jede p-Gruppe ist auflösbar.*

BEWEIS. Wir führen Induktion nach der Gruppenordnung. Der Fall der trivialen Gruppe ist klar, sei also nun $\#G > 1$. Wir haben schon als Folgerung aus der Klassengleichung gezeigt (Lemma 2.36), dass dann das Zentrum Z_G nicht-trivial ist. Nun ist $Z_G \subseteq G$ ein Normalteiler und der Quotient G/Z_G ist ebenfalls eine p-Gruppe und damit nach Induktionsvoraussetzung auflösbar. Mit Lemma 2.63 folgt die Behauptung. □

Wir wollen nun untersuchen, was wir über Untergruppen H einer endlichen Gruppe G sagen können, für die $\#H$ eine Primzahlpotenz ist. Diejenigen dieser Untergruppen, für die die Potenz maximal ist, nennt man Sylow-Gruppen nach dem norwegischen Mathematiker Ludwig Sylow[8] (1832–1918), der 1872 die *Sylow-Sätze*, Satz 2.78, bewies.

DEFINITION 2.77. Sei G eine endliche Gruppe und sei p eine Primzahl. Sei $\#G = p^m q$ mit $p \nmid q$. Unter einer *p-Sylow-Untergruppe* von G verstehen wir eine Untergruppe $H \subseteq G$ mit $\#H = p^m$. ⊣

Mit anderen Worten ist eine p-Sylow-Untergruppe von G eine Untergruppe H von G, die eine p-Gruppe ist und so dass $\#G/H$ nicht durch p teilbar ist.

SATZ 2.78 (Sylow-Sätze). *Sei G eine endliche Gruppe und sei p eine Primzahl. Wir schreiben $\#G = p^m q$ mit $p \nmid q$.*

(1) *Für alle natürlichen Zahlen $k \leq m$, existiert eine Untergruppe $H \subseteq G$ mit $\#H = p^k$. Insbesondere besitzt G eine p-Sylow-Untergruppe.*
(2) *Ist $H \subseteq G$ eine Untergruppe, die eine p-Gruppe ist, und ist $S \subseteq G$ eine p-Sylow-Gruppe von G, so existiert $g \in G$ mit $H \subseteq gSg^{-1}$. Insbesondere gilt: Je zwei p-Sylow-Untergruppen von G sind zueinander konjugiert.*
(3) *Sei s_p die Anzahl der p-Sylow-Untergruppen von G. Dann gilt*

$$s_p \mid q \quad \text{und} \quad s_p \equiv 1 \mod p.$$

Man nennt manchmal auch die drei Teile des Satzes den ersten, zweiten bzw. dritten Sylow-Satz.

[8] https://de.wikipedia.org/wiki/Peter_Ludwig_Mejdell_Sylow

BEWEIS. Für den Fall $m = 0$, also $p \nmid \#G$ ist nichts zu zeigen, wir nehmen daher von vorneherein $m > 0$ an.

zu (1). Wir führen Induktion nach $\#G$ und betrachten die Klassengleichung (Satz 2.35) für G:

$$\#G = \#Z_G + \sum_{i=1}^{r} \#(G/Z_{x_i}).$$

Wie üblich sei hier $x_1, \ldots, x_r$ ein Vertretersystem der Konjugationsklassen von G, die mehr als ein Element enthalten.

1. Fall: $p \mid \#Z_G$. Nach Lemma 2.23 existiert dann ein Element $g \in Z_G$ mit $\operatorname{ord}(g) = p$. Weil g im Zentrum von G liegt, ist $\langle g \rangle \subseteq G$ ein Normalteiler, und der Quotient $G/\langle g \rangle$ hat Ordnung $p^{m-1}q$. Er besitzt nach Induktionsvoraussetzung eine Untergruppe $\bar{H}$ mit p^{k-1} Elementen. Sei $\pi\colon G \to G/\langle g \rangle$ die kanonische Projektion. Dann ist $H := \pi^{-1}(\bar{H})$ eine Untergruppe von G, die genau p^k Elemente hat, denn es gilt $H/\langle g \rangle \cong \bar{H}$, wie man leicht nachprüft.

2. Fall: $p \nmid \#Z_G$. In diesem Fall folgt aus der Klassengleichung, dass wenigstens einer der Summanden $\#(G/Z_{x_i})$ ebenfalls nicht durch p teilbar ist. Dann gilt aber $p^k \mid \#Z_{x_i}$, und nach Induktionsvoraussetzung hat Z_{x_i} und damit auch G eine Untergruppe mit p^k Elementen.

zu (2). Wir betrachten die Operation von H durch Linksmultiplikation auf der Menge G/S der Nebenklassen von G nach S (wir setzen nicht voraus, dass S ein Normalteiler in G ist!), d.h. $h \in H$ bildet gS auf hgS ab. Da $\#(G/S) = \frac{\#G}{\#S} = q$ nicht durch p teilbar ist, aber H eine p-Gruppe ist, folgt aus Lemma 2.34, dass $g \in G$ existiert, so dass $hgS = gS$ für alle $h \in H$ gilt. Das bedeutet aber gerade $g^{-1}hg \in S$ für alle $h \in H$ oder mit anderen Worten, dass $H \subseteq gSg^{-1}$ ist.

zu (3). Sei nun X die Menge aller p-Sylow-Gruppen von G. Nach Teil (1) wissen wir, dass $X \neq \emptyset$ ist. Es ist klar, dass für $g \in G$ und $S \in X$ auch gSg^{-1} eine p-Sylow-Gruppe in G ist, denn $\#(gSg^{-1}) = \#S$. Also operiert G durch Konjugation auf X. Aus Teil (2) folgt, dass diese Operation transitiv ist, das bedeutet, dass zu $S, S' \in X$ stets ein Element $g \in G$ mit $S' = gSg^{-1}$ existiert. Es gibt also nur eine einzige Bahn unter der G-Wirkung auf X, und das liefert uns, wenn wir ein Element $S \in X$ fixieren, eine Bijektion $G/N_G(S) \to X$, die durch $g \mapsto gSg^{-1}$ induziert wird. Hier ist $N_G(S)$ der Stabilisator von S unter der Operation durch Konjugation – es handelt sich gerade um den Normalisator von S in G,

$$N_G(S) = \{g \in G;\ gSg^{-1} = S\},$$

eine Untergruppe von G, die S enthält und in der S Normalteiler ist.

Weil S in $N_G(S)$ als Untergruppe enthalten ist, folgt

$$s_p = \#X = \#(G/N_G(S)) \mid q.$$

Um den Beweis abzuschließen, ist noch die Aussage $\#X \equiv 1 \mod p$ zu zeigen. Wir betrachten nun die Operation von S auf X durch Konjugation; also dieselbe Wirkung wie vorher, aber eingeschränkt auf die Untergruppe S. Weil S eine p-Gruppe ist, folgt aus Lemma 2.34, dass $\#X \equiv \#(X^S) \mod p$ gilt, wobei X^S die Menge der Fixpunkte unter S ist, also die Menge derjenigen p-Sylow-Gruppen S', für die $gS'g^{-1} = S'$ für alle $g \in S$ gilt, mit anderen Worten, für die $S \subseteq N_G(S')$ gilt.

Es genügt dann zu zeigen, dass X^S als einziges Element S selbst enthält. Aber wenn $S' \in X$ mit $S \subseteq N_G(S')$ ist, dann sind S und S' auch p-Sylow-Gruppen in $N_G(S')$, folglich nach Teil (2) in $N_G(S')$ zueinander konjugiert. Weil aber jedes Element des Normalisators $N_G(S')$ die Gruppe S' in sich selbst konjugiert, folgt $S = S'$. □

KOROLLAR 2.79. *Sei G eine endliche Gruppe und sei p eine Primzahl.*

(1) *Jede Untergruppe von G, die eine p-Gruppe ist, ist in einer p-Sylow-Untergruppe enthalten.*

(2) *Eine Untergruppe H ist genau dann eine p-Sylow-Untergruppe von G, wenn H eine p-Gruppe ist und es keine Untergruppe von G gibt, die eine p-Gruppe ist und H als echte Untergruppe enthält.*

(3) *Hat G genau eine p-Sylow-Untergruppe H, dann ist H ein Normalteiler von G.*

(4) *Ist G abelsch, so gibt es für jede Primzahl p genau eine p-Sylow-Gruppe in G.*

BEISPIEL 2.80. Wir geben einige typische Anwendungen der Sylow-Sätze.

(1) Jede Gruppe G der Ordnung 15 ist zyklisch (also isomorph zu $\mathbb{Z}/15$). Denn ist $g \in G$, so ist $\operatorname{ord}(g) \in \{1, 3, 5, 15\}$. Wir wollen zeigen, dass der Fall $\operatorname{ord}(g) = 15$ tatsächlich auftreten muss. Hat g Ordnung 3, so ist $\langle g \rangle$ eine 3-Sylow-Gruppe von G, und ist $\operatorname{ord}(g) = 5$, dann ist $\langle g \rangle$ eine 5-Sylow-Gruppe.

Weil die Anzahl s_3 der 3-Sylow-Gruppen ein Teiler von 5 und kongruent zu 1 modulo 3 ist, folgt $s_3 = 1$. Ebenso sehen wir $s_5 = 1$. Es gibt also jeweils genau eine 3-Sylow-Gruppe und 5-Sylow-Gruppe, und folglich genau 2 Elemente der Ordnung 3 und genau 4 Elemente der Ordnung 5. Zusammen mit dem neutralen Element sind das aber nur 7 Elemente, die anderen 8 ($= \varphi(15)$) Elemente haben also Ordnung 15.

(2) Ist G eine Gruppe mit 6 Elementen, so ist G isomorph zu $\mathbb{Z}/6$ oder zu S_3.

Es folgt aus den Sylow-Sätzen, dass G genau eine 3-Sylow-Untergruppe H hat. Diese muss die Form $\{1, \sigma, \sigma^2\}$ für ein Element $\sigma \in G$ der Ordnung 3 haben. Sei $H' = \{1, \tau\}$ eine 2-Sylow-Untergruppe, also $\tau \in G$ ein Element der Ordnung 2.

Wenn $\sigma\tau = \tau\sigma$ gilt, dann ist die Abbildung $f\colon H \times H' \to G, (h, h') \mapsto hh'$ ein Gruppenhomomorphismus. Der Kern von f besteht (warum?) aus den Elementen der Form (h, h^{-1}) mit $h \in H \cap H' = \{1\}$, ist also trivial. Folglich ist f ein Isomorphismus. Aus dem chinesischen Restsatz (oder einfach, indem man direkt begründet, dass $\sigma\tau$ ein Element der Ordnung 6 ist) folgt $G \cong \mathbb{Z}/6$.

Wir betrachten nun den Fall, dass $\sigma\tau \neq \tau\sigma$ ist. Weil H ein Normalteiler ist, muss dann (warum?) $\sigma\tau = \tau\sigma^2$ gelten. Es ist

$$G = H \cup \tau H = \{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$$

und mit ein wenig Rechnen ergibt sich, dass die Gruppenstruktur auf G durch die Gleichheiten $\sigma^3 = 1, \tau^2 = 1, \sigma\tau = \tau\sigma^2$ vollständig festgelegt ist. Mit anderen Worten: Sind G, G' nicht-zyklische Gruppen mit 6 Elementen und $\sigma, \tau \in G$ und $\sigma', \tau' \in G'$ jeweils wie oben beschrieben gewählt, so gibt es genau einen Gruppenisomorphismus $G \xrightarrow{\sim} G'$ mit $\sigma \mapsto \sigma', \tau \mapsto \tau'$.

Wenden wir das auf die symmetrische Gruppe $G' := S_3$ an, so sehen wir, dass jede nicht-zyklische Gruppe mit 6 Elementen isomorph ist zu S_3.

(Man kann an dieser Stelle die Benutzung der Sylow-Sätze recht leicht vermeiden, indem man direkt zeigt, dass es in G ein Element der Ordnung 3 und ein Element der Ordnung 2 geben muss und ausnutzt, dass jede Untergruppe vom Index 2 ein Normalteiler ist.)

◊

ERGÄNZUNG 2.81 (Eine p-Sylow-Gruppe in $GL_n(\mathbb{F}_p)$). Sei wieder p eine Primzahl und $n \in \mathbb{N}$. Die Gruppe $GL_n(\mathbb{F}_p)$ der invertierbaren $(n \times n)$-Matrizen über dem endlichen Körper $\mathbb{F}_p$ hat

$$(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$$

Elemente (denn für die erste Spalte einer invertierbaren Matrix kommt jeder Vektor aus $\mathbb{F}_p^n \setminus \{0\}$ in Betracht; für die zweite Spalte jeder Vektor auf $\mathbb{F}_p^n$, der nicht in der von der ersten Spalte erzeugten Gerade liegt, usw.). Die maximale p-Potenz, die diese Zahl teilt, ist

$$p \cdot p^2 \cdots p^{n-1} = p^{\frac{n(n-1)}{2}}.$$

Sei nun $U \subset GL_n(\mathbb{F}_p)$ die Menge der oberen Dreiecksmatrizen, deren Diagonaleinträge alle $= 1$ sind. Dies ist eine Untergruppe von $GL_n(\mathbb{F}_p)$, wie man leicht nachrechnet. Es ist klar, dass

$$\#U = p^{\frac{n(n-1)}{2}},$$

weil die $\frac{n(n-1)}{2}$ Einträge oberhalb der Diagonale frei wählbar sind, und alle anderen Einträge fest vorgegeben sind. Also ist U eine p-Sylow-Untergruppe von $GL_n(\mathbb{F}_p)$.

Weil jede endliche Gruppe in eine symmetrische Gruppe S_n eingebettet werden kann, die wiederum zur Untergruppe der Permutationsmatrizen in $GL_n(\mathbb{F}_p)$ isomorph ist, ist auch jede endliche Gruppe isomorph zu einer Untergruppe vom $GL_n(\mathbb{F}_p)$ (für geeignetes n). Das kann man benutzen, um einen anderen Beweis der Sylow-Sätze zu erhalten, siehe [**Lo**] Kapitel 10.
□ Ergänzung 2.81

Ergänzung 2.82 (Abelsche endliche Gruppen sind das Produkt ihrer Sylow-Untergruppen). Wie oben bemerkt gibt es in einer abelschen Gruppe G für jede Primzahl p genau eine p-Sylow-Untergruppe $G_p \subseteq G$. Nur für endlich viele p (nämlich diejenigen Primzahlen, die $\#G$ teilen) ist G_p nicht-trivial, und wir erhalten wegen der Kommutativität von G aus der Gruppenmultiplikation einen Gruppenhomomorphismus

$$\prod_p G_p \to G, \quad (g_p)_p \mapsto \prod_p g_p.$$

Es ist nicht schwer zu zeigen, dass dieser injektiv ist, und weil beide Seiten dieselbe Mächtigkeit haben, handelt es sich um einen Isomorphismus.

Diese Aussage kann man als Vorstufe zum Hauptsatz über endliche abelsche Gruppen betrachten. Siehe Beispiel 2.7 und [**JS**] Abschnitt II.5 für einen Beweis des Satzes, der von diesem Punkt ausgeht. (Die Begründung der Injektivität der obigen Abbildung finde ich dort allerdings etwas knapp.) □ Ergänzung 2.82

Ergänzung 2.83 (Der Satz von Cauchy).

Satz 2.84. *Sei G eine endliche Gruppe und p eine Primzahl, die die Gruppenordnung $\#G$ teilt. Dann existiert ein Element $g \in G$ mit* $\operatorname{ord}(g) = p$.

Beweis. Der Satz folgt leicht aus den Sylow-Sätzen. Denn es existiert in G eine p-Sylow-Gruppe H, die nicht die triviale Gruppe ist. Sei $g \in H \setminus \{1\}$. Dann ist $\operatorname{ord}(h) = p^r$ für ein $r \geq 1$ und demzufolge hat $h^{p^{r-1}}$ Ordnung p.

Für einen direkten Beweis mithilfe der Klassengleichung siehe [**JS**] Satz II.1.2. Ein Beweis, der die Struktur der Gruppe $GL_n(\mathbb{F}_p)$ ausnutzt, wird in [**Soe**] Übungsaufgabe 4.1.35 skizziert. □

Korollar 2.85. *Seien p eine Primzahl und G eine endliche Gruppe, so dass für alle $g \in G$ die Ordnung* $\operatorname{ord}(g)$ *eine Potenz von p ist. Dann ist G eine p-Gruppe.*

□ Ergänzung 2.83

2.8. Wie untersucht man eine Gruppe? *

In diesem Abschnitt sammele ich einige Ansätze, wie man eine Gruppe »verstehen« kann/könnte oder welche Fragen man üblicherweise stellt, um eine Gruppe zu untersuchen. Was *verstehen* genau bedeutet, kann dabei natürlich vom Kontext abhängen, und was ich hier schreibe, erhebt auch keinen Anspruch auf Vollständigkeit.

Ein erste Bemerkung ist, dass eine Gruppe G (jedenfalls im endlichen Fall) durch ihre Verknüpfungstabelle gegeben ist, oder mit anderen Worten (und auch ganz allgemein) durch die Angabe der Abbildung $G \times G \to G$. Nur diese Abbildung in der Hand zu haben, ist allerdings praktisch nutzlos, wenn man von den simpelsten Fällen absieht. (Genauso wie es schon »unmöglich« ist, in einfacher Weise anhand einer Verknüpfungstabelle nachzuprüfen, ob die gegebene Verknüpfung assoziativ ist.)

Stattdessen sollte man als erstes versuchen zu entscheiden, welche der *Eigenschaften von Gruppen*, die wir definiert haben, eine gegebene Gruppe G hat.

2.8.1. Endliche/unendliche Gruppen. Die Methoden, die wir in den vorherigen Abschnitten bereitgestellt haben, betreffen in erster Linie endliche Gruppen.

Für unendliche Gruppen ist es in vielen Fällen, in denen man die gegebene Gruppe gut verstehen kann, so, dass eine »zusätzliche Struktur« gegeben ist, zum Beispiel eine »Topologie«, die Struktur einer »Lie-Gruppe« oder einer »linearen algebraischen Gruppe«. Alle diese Gruppen spielen in der Algebra-Vorlesung keine Rolle und es ist auch nicht möglich, diesen Begriffen in ein paar Zeilen gerecht zu werden, daher belassen wir es bei dieser Bemerkung.

2.8.2. Eigenschaften von Gruppen. Die folgende Liste nennt einige der Eigenschaften von Gruppen, die wir kennengelernt haben. Jede der Eigenschaften impliziert alle darauf folgenden.

(1) zyklisch von Primzahlordnung (dies sind genau die Gruppen $G \neq 1$, die außer $\{1\}$ und G keine Untergruppen haben),
(2) zyklisch,
(3) abelsch,
(4) auflösbar.

Für eine beliebige endliche Gruppe G erhalten wir aus der Diskussion in Ergänzung 2.66, dass G eine Normalreihe besitzt, die nicht weiter verfeinert werden kann (eine sogenannte Kompositionsreihe), und dass die Länge sowie die Subquotienten einer solchen Kompositionsreihe (bis auf Reihenfolge und Isomorphie) eindeutig bestimmt sind. Die Subquotienten sind einfache Gruppen, und die endlichen einfachen Gruppen sind »im Prinzip« bekannt (Ergänzung 2.70).

2.8.3. Kleine Gruppen. Die Subquotienten einer Kompositionsreihe zu kennen, legt eine Gruppe allerdings nicht vollkommen fest, und daher bleibt es schwierig, auch für relativ kleine Zahlen n alle Gruppen der Ordnung n bis auf Isomorphie zu klassifizieren. Für $n = 2048$ weiß man zum Beispiel nicht, wie viele solche Isomorphieklassen es überhaupt gibt. Siehe Wikipedia[9] für »ganz kleine« n.

Die Folge der Anzahlen der Isomorphieklassen von Gruppen der Ordnung n ist die *erste* Folge A000001[10] in der OEIS, der *Online Encyclopedia of Integer Sequences*. Dort finden sich auch weitere Literaturverweise.

[9] https://en.wikipedia.org/wiki/List_of_small_groups
[10] https://oeis.org/A000001

2.8.4. Darstellungstheorie. Ein besonders mächtiger Ansatz, um eine Gruppe zu »verstehen«, ist es, ihre *Darstellungen* im Sinne der folgenden Definition zu betrachten.

DEFINITION 2.86. Sei K ein Körper. Sei G eine Gruppe. Eine *Darstellung* von G über K ist ein Gruppenhomomorphismus $G \to \mathrm{Aut}_K(V)$ von G in die Automorphismengruppe eines K-Vektorraums V. ⊣

Mit anderen Worten ist also eine Darstellung eine Gruppenwirkung auf einem K-Vektorraum durch Vektorraumautomorphismen. Es folgt (warum?) aus dem Satz von Cayley (Satz 2.54), dass zu jeder endlichen Gruppe G eine injektive Darstellung $G \to GL_n(K) \cong \mathrm{Aut}_K(K^n)$ existiert.

Andererseits ist zum Beispiel die Quaternionengruppe Q (Ergänzung 2.8) nicht isomorph zu einer Untergruppe von $GL_2(\mathbb{R})$. Das kann man mit Methoden der linearen Algebra zeigen, aber es ist nicht offensichtlich.

Für den Moment belasse ich es bei dieser kurzen Bemerkung zur Darstellung. Weitere Informationen finden Sie gegebenenfalls in den in der Box angegebenen Quellen.

Quellen zur Darstellungstheorie endlicher Gruppen:

J. P. Serre, *Linear representations of finite groups*, Springer 1977. Dieser Klassiker (ursprünglich auf französisch, und es gab auch eine deutsche Übersetzung) ist aus einer Vorlesung entstanden, die für Chemiker∗innen gehalten wurde. Die Verbindung zur Chemie wird im Buch selbst kaum thematisiert, aber Gruppendarstellungen spielen auch in der Chemie eine Rolle, zum Beispiel bei der Untersuchung gewisser Molekülstrukturen und ihrer Symmetrien, und bei der Untersuchung von Kristallen.

B. Steinberg, *Representation Theory of Finite Groups*, Springer 2012
https://doi.org/10.1007/978-1-4614-0776-8

G. James, M. Liebeck, *Representations and Characters of Groups*, Cambridge Univ. Press 2005.

KAPITEL 3

Ringe

Zur Terminologie: Anders als in der Linearen Algebra verstehen wir in dieser Vorlesung unter einem Ring immer einen *kommutativen* Ring.

3.1. Ringe, Ringhomomorphismen und Ideale

3.1.1. Vorkenntnisse. Wir haben in der Linearen Algebra 2 den Begriff des *Rings* eingeführt. Ein Ring heißt kommutativ, wenn die Ringmultiplikation kommutativ ist, und dies wollen wir wie gesagt stets voraussetzen, wenn nicht explizit etwas anderes gesagt wird. Ähnlich wie für Gruppen haben wir die Begriffe des Ringhomomorphismus und des Ringisomorphismus, sowie des Unterrings. Ist R ein Ring, so bezeichnen wir mit $R^\times$ die Teilmenge von R, die aus allen denjenigen Elementen besteht, die ein multiplikatives Inverses besitzen. Dies ist eine Gruppe bezüglich der Ringmultiplikation, die sogenannte *Einheitengruppe* $R^\times$ von R. Ihre Elemente nennt man die *Einheiten* von R. Ein Körper ist ein (kommutativer) Ring K, für den $K^\times = K \setminus \{0\}$ gilt. Der einzige Ring mit nur einem einzigen Element heißt der *Nullring* (genau genommen ist dieser natürlich nur bis auf eindeutigen Isomorphismus eindeutig bestimmt). Siehe Abschnitt LA2.15.1.

Sei R ein Ring. Ein Element $x \in R$ heißt *Nullteiler*, wenn $y \in R \setminus \{0\}$ mit $xy = 0$ existiert. Ist R ein Ring, der vom Nullring verschieden ist und in dem 0 der einzige Nullteiler ist, dann nennen wir R einen *Integritätsring*.

BEISPIEL 3.1. Einige Ringe, die in der Algebra wichtig sind

(1) Körper,

(2) der Polynomring $K[X]$ über einem Körper K in einer Unbestimmten,

(3) der Ring $\mathbb{Z}$ der ganzen Zahlen.

Alle diese Ringe sind Integritätsringe. ◊

BEISPIEL 3.2 (Beispiele von Ringhomomorphismen). (1) Sei R ein Ring. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus $f\colon \mathbb{Z} \to R$. Dabei wird für eine natürliche Zahl $n \in \mathbb{N}$ die Zahl n abgebildet auf $1 + \cdots + 1$ (n Summanden, Summe in R), und $-n$ auf $-f(n)$ abgebildet. Es ist leicht zu sehen, dass dies einen Ringhomomorphismus definiert. Weil per Definition jeder Ringhomomorphismus 1 auf 1 abbildet, kann es keine anderen Ringhomomorphismen $\mathbb{Z} \to R$ geben. Der so definierte Ringhomomorphismus ist im Allgemeinen *nicht injektiv*. Trotzdem schreiben wir oft n statt $f(n)$ und fassen so ganze Zahlen als Elemente des Rings R auf. Insbesondere im Fall von Ringen, für die f nicht injektiv ist, muss man dann aber genau unterscheiden, wo jeweils eine Gleichheit gilt – zum Beispiel gilt $2 = 0$ in $\mathbb{Z}/2$, aber natürlich sind 0 und 2 als ganze Zahlen nicht gleich.

(2) (Der *Frobenius-Homomorphismus*.) Sei R ein Ring, in dem (im Sinne von Teil (1)) $p = 0$ gilt. Dann ist die Abbildung

$$\mathrm{Frob}_p\colon R \to R, \quad x \mapsto x^p,$$

ein Ringhomomorphismus.

Es ist klar, dass $\mathrm{Frob}_p(1) = 1$ und $\mathrm{Frob}_p(xy) = \mathrm{Frob}_p(x)\,\mathrm{Frob}_p(y)$ gilt (hier wird die Voraussetzung, dass $p = 0$ in R gilt, gar nicht benötigt).

Zu zeigen bleibt die Additivität, also dass

$$(x+y)^p = x^p + y^p$$

für alle $x, y \in R$ gilt.

In jedem (kommutativen) Ring gilt der binomische Lehrsatz

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i\, y^{p-i}.$$

Dies ist als Gleichung in R zu interpretieren, indem die natürlichen Zahlen $\binom{p}{i}$ mit dem Ringhomomorphismus $\mathbb{Z} \to R$ nach R abgebildet werden. Weil dieser Ringhomomorphismus nach Voraussetzung p auf 0 abbildet, genügt es zu zeigen, dass für alle $i = 1, \ldots, p-1$ der Binomialkoeffizient $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ durch p teilbar ist. Nun ist der Zähler dieses Bruchs durch p teilbar, der Nenner (weil p eine Primzahl ist) aber nicht.

◊

3.1.2. Der Quotientenkörper eines Integritätsrings. Sei R ein Integritätsring. In der Linearen Algebra 2 haben wir zu R seinen *Quotientenkörper* $\mathrm{Quot}(R)$ konstruiert, Abschnitt LA2.15.5. Dies können wir in dem folgenden Satz zusammenfassen.

Satz 3.3. *Sei R ein Integritätsring. Dann existiert ein Körper K zusammen mit einem injektiven Ringhomomorphismus $\iota\colon R \to K$, so dass jedes Element von K sich in der Form $\iota(a)\iota(b)^{-1}$ mit $a, b \in R$, $b \neq 0$, schreiben lässt. Für $a, b \in R$, $b \neq 0$, schreiben wir auch $\frac{a}{b}$ statt $\iota(a)\iota(b)^{-1}$ und a statt $\frac{a}{1} = \iota(a)$.*

Der Körper K ist durch R im folgenden Sinne bis auf eindeutigen Isomorphismus eindeutig bestimmt: Seien K und K' mit injektiven Ringhomomorphismen $\iota\colon R \to K$, $\iota'\colon R \to K'$ wie im Satz. Dann existiert ein eindeutig bestimmter Isomorphismus $\varphi\colon K \to K'$ von Ringen mit $\iota' = \varphi \circ \iota$. Wir nennen einen Körper wie im Satz (zusammen mit der Einbettung von R) daher *den* Quotientenkörper von R.

Im Quotientenkörper eines Rings gelten die »üblichen Bruchrechenregeln« – das folgt aus den Körperaxiomen.

Um die Existenz des Quotientenkörpers zu zeigen, konstruiert man ihn als die Menge der Äquivalenzklassen der Menge $R \times (R \setminus \{0\})$ bezüglich der Äquivalenzrelation

$$(a,b) \sim (c,d) \quad \Longleftrightarrow \quad ad = bc,$$

die die übliche Gleichheit von Brüchen beschreibt, die durch Erweitern bzw. Kürzen auseinander hervorgehen. Es ist dann die Wohldefiniertheit der Addition und Multiplikation von Brüchen (die man durch die gewohnten Formeln definiert) zu prüfen.

3.1.3. Ideale. Sei R ein (wie immer: kommutativer) Ring. Wir haben in der Linearen Algebra 2 den Begriff des *Ideals* definiert, den wir hier wiederholen.

Definition 3.4. Sei R ein Ring. Eine Teilmenge $\mathfrak{a} \subseteq R$ heißt *Ideal*, wenn $\mathfrak{a}$ eine Untergruppe bezüglich der Addition ist und für alle $x \in R$, $a \in \mathfrak{a}$ gilt, dass $xa \in \mathfrak{a}$ ist. ⊣

In jedem Ring R sind $0 = \{0\}$ (das *Nullideal*) und R (das *Einsideal*) Ideale. Ist $\mathfrak{a} \subset R$ ein Ideal, das eine Einheit $u \in R^\times$ enthält, so ist auch $1 = u^{-1}u \in \mathfrak{a}$ und in diesem Fall folgt $\mathfrak{a} = R$. Insbesondere sind in einem Körper das Nullideal und das Einsideal die einzigen Ideale.

Der Kern eines Ringhomomorphismus ist stets ein Ideal. Als Folgerung dieser Bemerkungen sehen wir:

LEMMA 3.5. *Seien K ein Körper, $R \neq 0$ ein Ring und $\varphi\colon K \to R$ ein Ringhomomorphismus. Dann ist φ injektiv.*

BEWEIS. Der Kern von φ ist ein Ideal, das $\neq K$ ist, weil $1 \in K$ unter φ auf $1 \in R$ abgebildet wird. Ein Ringhomomorphismus mit trivialem Kern ist injektiv. □

3.1.4. Konstruktionen von Idealen. Wie man leicht sieht, ist der Durchschnitt von Idealen ein Ideal.

LEMMA 3.6. *Seien R ein Ring und I eine Menge. Sind $\mathfrak{a}_i$, $i \in I$, Ideale, so ist auch der Durchschnitt $\bigcap_{i\in I} \mathfrak{a}_i$ ein Ideal.*

DEFINITION 3.7 (Von einer Teilmenge erzeugtes Ideal). Sei R ein Ring.

(1) Sei $M \subseteq R$ eine Teilmenge. Der Durchschnitt aller Ideale von R, die M enthalten ist das kleinste Ideal von R, das M enthält und wird das *von M erzeugte Ideal* genannt und mit (M) bezeichnet.

Statt $(\{a_1, \ldots, a_n\})$ schreiben wir auch $(a_1, \ldots, a_n)$.

(2) Ein Ideal $\mathfrak{a}$ von R heißt *endlich erzeugt*, wenn eine endliche Teilmenge $M \subseteq R$ mit $\mathfrak{a} = (M)$ existiert.

(3) Ein Ideal der Form
$$(a) = \{xa;\ x \in R\}, \quad a \in R,$$
heißt *Hauptideal*.

⊣

Explizit gilt
$$(a_1, \ldots, a_n) = \left\{ \sum_{i=1}^{n} x_i a_i;\ x_i \in R \right\},$$
denn offenbar gilt $\supseteq$ und die rechte Seite ist ein Ideal, das alle a_i enthält.

Das Nullideal $\{0\} = (0)$ und das Einsideal $R = (1)$ sind in jedem Ring R Hauptideale. Das Ideal $(2, X)$ im Ring $\mathbb{Z}[X]$ ist kein Hauptideal.

Wir nennen Elemente x, y eines Integritätsrings zueinander *assoziiert*, wenn $(x) = (y)$ gilt, wenn also x und y dasselbe Hauptideal erzeugen. Das ist dazu äquivalent, dass eine Einheit $u \in R^\times$ mit $y = ux$ existiert. Assoziiertheit ist eine Äquivalenzrelation auf R.

DEFINITION 3.8. Ein *Hauptidealring* ist ein Integritätsring, in dem jedes Ideal ein Hauptideal ist. ⊣

BEISPIEL 3.9. Wir haben in der Linearen Algebra 2 gesehen, dass jeder euklidische Ring ein Hauptidealring ist. Insbesondere sind die Ringe $\mathbb{Z}$ und $K[X]$ (K ein Körper) Hauptidealringe. ◊

DEFINITION 3.10. Sei R ein Ring.

(1) Seien $\mathfrak{a}, \mathfrak{b} \subseteq R$ Ideale. Die *Summe* von $\mathfrak{a}$ und $\mathfrak{b}$ ist das Ideal
$$\mathfrak{a} + \mathfrak{b} = (\mathfrak{a} \cup \mathfrak{b}) = \{a + b;\ a \in \mathfrak{a},\ b \in \mathfrak{b}\},$$
d.h. das von $\mathfrak{a} \cup \mathfrak{b}$ erzeugte Ideal.

(2) Seien I eine Menge und $\mathfrak{a}_i$, $i \in I$, Ideale in R. Die *Summe* der Ideale ist das Ideal

$$\sum_{i\in I} \mathfrak{a}_i = \left(\bigcup_{i\in I} a_i\right) = \left\{\sum_{i\in I} a_i;\ a_i \in \mathfrak{a}_i,\ \text{nur endlich viele } a_i \neq 0\right\}.$$

⊣

DEFINITION 3.11. Sei R ein Ring. Seien $\mathfrak{a}, \mathfrak{b} \subseteq R$ Ideale. Das *Produkt* von $\mathfrak{a}$ und $\mathfrak{b}$ ist

$$\mathfrak{a}\mathfrak{b} = (\{ab;\ a \in \mathfrak{a},\ b \in \mathfrak{b}\}),$$

d.h. das von allen Produkten von Elementen aus $\mathfrak{a}$ und $\mathfrak{b}$ erzeugte Ideal.

Analog definiert man das Produkt einer endlichen Familie von Idealen. ⊣

Für Ideale $\mathfrak{a}$ und $\mathfrak{b}$ eines Rings R gilt

$$\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}.$$

Überlegen Sie sich ein Beispiel, in dem diese Inklusion echt ist.

3.1.5. Der Quotient eines Rings nach einem Ideal. Ähnlich wie den Quotienten einer Gruppe nach einem Normalteiler haben wir den Quotientenring eines Rings nach einem Ideal (siehe auch Abschnitt LA2.18.4). Ist R ein Ring und $\mathfrak{a}$ ein Ideal, so ist insbesondere $\mathfrak{a} \subseteq R$ eine Untergruppe bezüglich der Addition, und sogar ein Normalteiler, weil die Addition kommutativ ist. Wir haben daher den Gruppenquotienten $R/\mathfrak{a}$, eine additive Gruppe zusammen mit der kanonischen Projektion, einem surjektiven Gruppenhomomorphismus $\pi\colon R \to R/\mathfrak{a}$ mit Kern $\mathfrak{a}$. Aus der Idealeigenschaft folgt dann leicht, dass die Multiplikation von R auf $R/\mathfrak{a}$ eine Multiplikation induziert, so dass π ein Ringhomomorphismus ist.

Auch für diese Quotientenbildung gilt der Homomorphiesatz. Weil wir später viel mit Quotienten von Ringen (insbesondere vom Polynomring in einer Variablen über einem Körper K) arbeiten werden, geben wir ihn noch einmal explizit an.

SATZ 3.12 (Homomorphiesatz für Ringe). *Sei R ein Ring, $\mathfrak{a} \subseteq R$ ein Ideal und $\pi\colon R \to R/\mathfrak{a}$ die kanonische Projektion.*

Sei T ein Ring und sei $f\colon R \to T$ ein Ringhomomorphismus. Es existiert genau dann ein Ringhomomorphismus $\varphi\colon R/\mathfrak{a} \to T$ mit $\varphi \circ \pi = f$, wenn $\mathfrak{a} \subseteq \operatorname{Ker} f$ ist. In diesem Fall ist φ eindeutig bestimmt und es gilt: $\operatorname{Im}\varphi = \operatorname{Im} f$. *Die Abbildung φ ist genau dann injektiv wenn $\mathfrak{a} = \operatorname{Ker} f$ gilt.*

BEWEIS. Man kann auf die zugrundeliegenden additiven Gruppen den Homomorphiesatz für Gruppen anwenden. Es ist dann nur noch zu überprüfen, dass im Fall ihrer Existenz (als Gruppenhomomorphismus) die Abbildung φ automatisch ein Ringhomomorphismus ist. Das folgt leicht daraus, dass π surjektiv und f ein Ringhomomorphismus ist. □

Der folgende Satz gibt eine Beziehung zwischen den Idealen im Quotientenring $R/\mathfrak{a}$ und Idealen in R (nämlich denjenigen, die $\mathfrak{a}$ enthalten) an. Man vergleiche Lemma 2.16 (6).

SATZ 3.13. *Sei R ein Ring und sei $\mathfrak{a} \subseteq R$ ein Ideal. Sei $\pi\colon R \to R/\mathfrak{a}$ die kanonische Projektion. Dann sind die Abbildungen*

$$\begin{aligned} \{\mathfrak{b} \subseteq R \text{ Ideal};\ \mathfrak{a} \subseteq \mathfrak{b}\} &\xrightarrow{\sim} \{\mathfrak{c} \subseteq R/\mathfrak{a} \text{ Ideal}\} \\ \mathfrak{b} &\mapsto \pi(\mathfrak{b}), \\ \pi^{-1}(\mathfrak{c}) &\mapsfrom \mathfrak{c}, \end{aligned}$$

zueinander inverse, inklusionserhaltende Bijektionen.

BEWEIS. Es ist zu überprüfen, dass die beiden Abbildungen die angegebenen Mengen in sich abbilden und zueinander invers sind. Wir lassen die Details aus. □

SATZ 3.14 (Chinesischer Restsatz). *Seien R ein Ring und $\mathfrak{a}_1, \ldots, \mathfrak{a}_r \subseteq R$ Ideale, so dass $\mathfrak{a}_i + \mathfrak{a}_j = R$ für alle $i \neq j$ gilt. Sei $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{a}_i$. Dann ist der natürliche Ringhomomorphismus*

$$R \to R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_r\,, \quad x \mapsto (\overline{x}, \ldots, \overline{x}),$$

wobei $\overline{x}$ die Restklasse von x im jeweiligen Quotienten bezeichne, surjektiv mit Kern $\mathfrak{a}$ und induziert folglich einen Isomorphismus

$$R/\mathfrak{a} \xrightarrow{\sim} R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_r\,.$$

BEWEIS. Wir erhalten die gesuchte Abbildung aus dem Homomorphiesatz, und dieser zeigt auch die Injektivität. Die Surjektivität folgt aus der Surjektivität der ursprünglichen Abbildung. Um diese zu zeigen, genügt es, wie man leicht einsieht, zu zeigen, dass die »Standardbasisvektoren«, d.h. die Elemente $e_i := (0, \ldots, 0, 1, 0, \ldots, 0)$ (mit der 1 an der i-ten Stelle) im Bild liegen.

Um die Notation zu vereinfachen, zeigen wir, dass e_1 im Bild liegt. Für allgemeines i lässt sich dasselbe Argument verwenden. Wir schreiben $1 = b_j + a_j$ mit $b_j \in \mathfrak{a}_1, a_j \in \mathfrak{a}_j, j = 2, \ldots, r$. Es folgt

$$1 = \prod_{j=2}^{r} (b_j + a_j)$$

und durch Ausmultiplizieren erhalten wir einen Ausdruck der Form

$$1 = b + a$$

mit $b \in \mathfrak{a}_1$ (b ist die Summe aller Faktoren, in denen wenigstens ein b_j vorkommt) und $a := a_2 \cdot \cdots \cdot a_r \in \bigcap_{j=2}^{r} \mathfrak{a}_j$.

Das Bild von $a = 1 - b$ ist dann das oben definierte Element e_1. □

BEMERKUNG 3.15. (1) Sei K ein Körper und f ein Endomorphismus eines endlichdimensionalen K-Vektorraums V. Der Einsetzungshomomorphismus $K[X] \to \mathrm{End}_K(V)$ vom Polynomring in den (nicht-kommutativen) Endomorphismenring von V faktorisiert über den Quotienten $K[X]/(\mathrm{minpol}_f)$ (das ist mehr oder weniger die Definition des Minimalpolynoms von f) und liefert so einen Isomorphismus

$$K[X]/(\mathrm{minpol}_f) \cong K[f] := \left\{ \sum_{i=0}^{n} a_i f^i;\ n \in \mathbb{N},\ a_i \in K \right\} \subseteq \mathrm{End}_K(V).$$

(2) Sei L ein Körper und $K \subseteq L$ ein Teilkörper von L. Sei $\alpha \in L$. Wir betrachten nun den Einsetzungshomomorphismus $\Phi\colon K[X] \to L, X \mapsto \alpha$.

1. Fall: Φ ist nicht injektiv. Dann ist $\mathrm{Ker}(\Phi) \neq 0$, also von der Form $(f), f \neq 0$, und $K[X]/(f) \to L$ ist injektiv. Folglich ist $K[X]/(f)$ ein Integritätsring, der K als Unterring enthält, und gleichzeitig ein endlichdimensionaler K-Vektorraum, also ein Körper.

Es gilt dann $K[\alpha] := \mathrm{Im}(\Phi) \cong K[X]/(f)$, also ist $K[\alpha]$ ein Teilkörper von L.

2. Fall: Φ ist injektiv. In diesem Fall ist $K[\alpha] := \mathrm{Im}(\Phi)$ isomorph zum Polynomring $K[X]$ und insbesondere kein Körper.

Auf diese Überlegungen werden wir noch ausführlich zurückkommen, siehe Abschnitt 4.2, Definition 4.9.

◊

3.2. Primideale und maximale Ideale

In der Linearen Algebra 2 haben wir den Begriff des *Primelements* in einem Integritätsring R eingeführt. Und zwar heißt $p \in R$ ein Primelement, wenn p keine Einheit und $\neq 0$ ist und die folgende *Primeigenschaft* erfüllt: Für alle $x, y \in R$ mit $p \mid xy$ gilt $p \mid x$ oder $p \mid y$.

Wir wissen, dass wir Teilbarkeit von Ringelementen auch in Termen von Idealen ausdrücken können: $p \mid x$ ist äquivalent zu $x \in (p)$. Daher ist es naheliegend, die obige Primeigenschaft wie folgt auf Ideale zu übertragen.

Definition 3.16. Sei R ein Ring. Ein Ideal $\mathfrak{p} \subset R$ heißt *Primideal*, wenn $\mathfrak{p} \neq R$ gilt und wenn für alle $x, y \in R$ gilt: Falls $xy \in \mathfrak{p}$, dann ist $x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$. ⊣

Ist R ein Integritätsring und $p \in R$, $p \neq 0$, so ist das Hauptideal (p) genau dann ein Primideal, wenn p ein Primelement in R ist. Es gibt hier also eine kleine Diskrepanz in den Bezeichnungen: Während per Definition $0 \in R$ kein Primelement ist, kann das Nullideal ein Primideal sein. Genauer ist $(0) \subseteq R$ genau dann ein Primideal, wenn R ein Integritätsring ist. Etwas allgemeiner gilt das folgende Lemma.

Lemma 3.17. *Seien R ein kommutativer Ring und $\mathfrak{p} \subseteq R$ ein Ideal. Dann sind äquivalent:*

(i) *der Quotient $R/\mathfrak{p}$ ist ein Integritätsring,*

(ii) *das Ideal $\mathfrak{p}$ ist ein Primideal.*

Beweis. Der Beweis ist einfach wir und lassen ihn aus. Versuchen Sie es selbst und fragen Sie gegebenenfalls nach! □

Eine weitere wichtige Klasse von Idealen, die wir betrachten wollen, bilden die sogenannten *maximalen* Ideale. Die Maximalität bezieht sich hier auf die Inklusion von Teilmengen, allerdings wird dabei das Einsideal des Rings außen vor gelassen (sonst wäre der Begriff langweilig, weil dann immer das Einsideal das einzige maximale Ideal wäre).

Definition 3.18. Sei R ein Ring. Ein Ideal $\mathfrak{m} \subset R$ heißt *maximales Ideal*, wenn $\mathfrak{m} \neq R$ ist und $\mathfrak{m}$ maximal mit dieser Eigenschaft bezüglich der Inklusion von Idealen ist, d.h. wenn für jedes Ideal $\mathfrak{a} \subseteq R$ mit $\mathfrak{m} \subseteq \mathfrak{a} \subseteq R$ gilt: $\mathfrak{a} = \mathfrak{m}$ oder $\mathfrak{a} = R$. ⊣

Lemma 3.19. *Sei R ein kommutativer Ring und $\mathfrak{m} \subseteq R$ ein Ideal. Dann sind äquivalent:*

(i) *der Quotient $R/\mathfrak{m}$ ist ein Körper,*

(ii) *das Ideal $\mathfrak{m}$ ist ein maximales Ideal.*

Beweis. Ein kommutativer Ring $R \neq 0$ ist genau dann ein Körper, wenn (0) und R die einzigen Ideale in R sind. (Warum?) Daher folgt die Äquivalenz im Lemma aus Satz 3.13. □

Insbesondere ist jedes maximale Ideal ein Primideal.

Satz 3.20. *Sei R ein Hauptidealring und $\mathfrak{p} \subset R$ ein Primideal, das nicht das Nullideal ist. Dann ist $\mathfrak{p}$ ein maximales Ideal von R.*

Beweis. Weil R ein Hauptidealring ist, existiert $p \in R$ mit $\mathfrak{p} = (p)$. Da $\mathfrak{p}$ ein Primideal ist, ist p prim. Sei nun $\mathfrak{a} = (a)$ ein Ideal mit $\mathfrak{p} \subseteq \mathfrak{a} \subseteq R$. Dann ist $p \in \mathfrak{a}$, etwa $p = ad$, $d \in R$. Als Primelement ist p insbesondere irreduzibel und es folgt, dass entweder a oder d eine Einheit in R ist. Also ist entweder $\mathfrak{a} = R$ oder a und p sind assoziiert, und dann gilt $\mathfrak{a} = \mathfrak{p}$. □

BEISPIEL 3.21. (1) Die Primideale im Hauptidealring $\mathbb{Z}$ sind die Ideale (0) und (p) für Primzahlen p. Die maximalen Ideale sind die Ideale (p) für Primzahlen p. Wir sehen so erneut, dass $\mathbb{Z}/p$ für jede Primzahl p ein Körper ist.

(2) Das Ideal $(X) \subset \mathbb{Z}[X]$ ist ein Primideal, aber kein maximales Ideal.

$\Diamond$

Es ist manchmal wichtig zu wissen, dass jeder Ring $\neq 0$ ein maximales Ideal besitzt. (Konkret werden wir dies in Abschnitt 4.4 benötigen.) Das wollen wir als nächstes beweisen. Der Beweis beruht auf dem *Lemma von Zorn*, das wir hier kurz vorstellen; siehe auch Abschnitt LA1.B.1. Das Lemma von Zorn beweisen wir hier nicht; es folgt aus der »Tatsache«, dass für jede Menge I und Mengen $X_i \neq \emptyset, i \in I$ das kartesische Produkt $\prod_{i\in I} X_i$ nicht leer ist. Anschaulich halten das viele (die meisten?) Mathematiker*innen für »klar«, aber (und deshalb steht *Tatsache* in Anführungszeichen) es folgt nicht aus den heutzutage oft zugrunde gelegten Axiomen der Mengenlehre von Zermelo und Fraenkel, sondern ist ein zusätzliches Axiom, das sogenannte *Auswahlaxiom*, auf Englisch *Axiom of choice*; man spricht von ZFC als dem Axiomensystem von Zermelo und Fraenkel zusammen mit dem Auswahlaxiom. Man kann zeigen, dass die Aussage des Auswahlaxioms äquivalent ist (unter den Axiomen ZF von Zermelo und Fraenkel) zum Zornschen Lemma. Wir geben deshalb unten das Lemma von Zorn als Axiom an.

SATZ 3.22. *Sei R ein Ring und sei $\mathfrak{a} \subsetneq R$ ein Ideal. Dann besitzt R ein maximales Ideal, das $\mathfrak{a}$ enthält. Insbesondere besitzt jeder Ring $R \neq 0$ ein maximales Ideal.*

Um das Lemma von Zorn zu formulieren, machen wir die folgenden Definitionen; siehe auch Abschnitt LA1.3.14.

DEFINITION 3.23. (1) Sei M eine Menge. Eine *partielle Ordnung* auf M ist eine Relation $\leq$ auf M (d.h. für je zwei Elemente $x, y \in M$ gilt entweder $x \leq y$, oder nicht $x \leq y$ – dann schreiben wir $x \not\leq y$), die reflexiv, transitiv und anti-symmetrisch ist. Es gilt also $x \leq x$ für alle $x \in M$, aus $x \leq y$ und $y \leq z$ folgt $x \leq z$ für alle $x, y, z \in M$, und aus $x \leq y$ und $y \leq x$ folgt $x = y$ für alle $x, y \in M$.

Wir nennen dann M zusammen mit $\leq$ eine *partiell geordnete Menge*. (Auf Englisch spricht man manchmal von *poset* (= *p. o. set* = *partially ordered set*.)

(2) Sei M eine partiell geordnete Menge. Ein Element $m \in M$ heißt *maximales Element*, wenn für alle $m' \in M$ mit $m \leq m'$ gilt, dass $m = m'$ ist.

(3) Sei M eine partiell geordnete Menge. Ein Element $m \in M$ heißt *größtes Element*, wenn für alle $m' \in M$ gilt, dass $m' \leq m$ ist.

(4) Sei T eine Menge. Eine *totale Ordnung* auf T ist eine partielle Ordnung $\leq$ auf T, so dass für alle $x, y \in M$ gilt, dass $x \leq y$ oder $y \leq x$ ist.

Ist M eine partiell geordnete Menge und $T \subseteq M$ eine Teilmenge, derart dass die Einschränkung der auf M gegebenen Ordnung auf T eine totale Ordnung ist, so nennt man T eine *Kette*.

(5) Sei M eine partiell geordnete Menge und $M' \subseteq M$ eine Teilmenge. Eine *obere Schranke* von M' in M ist ein Element $m \in M$, so dass $m' \leq m$ für alle $m' \in M'$ gilt.

$\dashv$

Ein typisches Beispiel für eine partiell geordnete Menge (die im Allgemeinen nicht total geordnet ist) ist die Potenzmenge einer Menge X, also die Menge aller Teilmengen von X, mit der Inklusion $\subseteq$ von Teilmengen als Relation. Anstatt aller Teilmengen von X kann man natürlich auch jede Teilmenge der Potenzmenge mit dieser partiellen Ordnung versehen.

Ist M eine partiell geordnete Menge, so muss M weder ein maximales noch ein größtes Element besitzen. Wenn ein größtes Element existiert, so ist es eindeutig bestimmt, und ist dann insbesondere das einzige maximale Element. Ein maximales Element (wenn es existiert) ist im Allgemeinen nicht eindeutig bestimmt. Wenn es mehr als ein maximales Element gibt, so gibt es kein größtes Element.

AXIOM 3.24 (Lemma von Zorn). *Jede nicht-leere partiell geordnete Menge, in der zu jeder total geordneten Teilmenge eine obere Schranke existiert, besitzt ein maximales Element.*

Eine Menge, die die Voraussetzungen des Lemmas von Zorn erfüllt, nennt man manchmal auch eine *induktiv geordnete Menge*. Die Voraussetzung, dass die gegebene Menge nicht-leer sei, folgt automatisch aus den anderen Bedingungen, denn die leere Menge ist eine Kette und muss eine obere Schranke haben.

BEWEIS VON SATZ 3.22. Sei $\mathscr{M}$ die Menge aller Ideale von R, die von R verschieden sind und $\mathfrak{a}$ enthalten. Weil $\mathfrak{a} \in \mathscr{M}$ ist, ist $\mathscr{M}$ nicht leer. Die Menge $\mathscr{M}$ ist durch die Inklusion partiell geordnet, und ein maximales Element von $\mathscr{M}$ ist gerade ein maximales Ideal von R, das $\mathfrak{a}$ enthält. Nach dem Lemma von Zorn genügt es nun, zu zeigen, dass jede Kette von Idealen in $\mathscr{M}$ eine obere Schranke in $\mathscr{M}$ besitzt.

Sei $\mathscr{T} \subseteq \mathscr{M}$ eine total geordnete Teilmenge von $\mathscr{M}$, mit anderen Worten eine Menge von echten Idealen von R, die das Ideal $\mathfrak{a}$ enthalten, und so dass für je zwei Ideale $\mathfrak{b}, \mathfrak{c} \in \mathscr{T}$ gilt, dass $\mathfrak{b} \subseteq \mathfrak{c}$ oder $\mathfrak{c} \subseteq \mathfrak{b}$ ist. Insbesondere ist daher $\mathfrak{b} \cup \mathfrak{c}$ ein Element von $\mathscr{T}$ (weil es sich bei der Vereinigung einfach um $\mathfrak{b}$ oder um $\mathfrak{c}$ handelt).

Wir zeigen, dass $\mathscr{T}$ eine obere Schranke in $\mathscr{M}$ besitzt. Ist $\mathscr{T} = \emptyset$, so ist $\mathfrak{a}$ eine obere Schranke. Sonst definieren wir $\mathfrak{t}$ als die Vereinigung von allen Idealen in $\mathscr{T}$ und zeigen, dass $\mathfrak{t}$ die gewünschte Eigenschaft hat.

Jedenfalls enthält die Menge $\mathfrak{t}$ das Ideal $\mathfrak{a}$. Um zu sehen, dass $\mathfrak{t}$ ein Ideal ist, seien $b, c \in \mathfrak{t}$. Dann liegen b und c in gewissen Elementen $\mathfrak{b}, \mathfrak{c} \in \mathscr{T}$. Die Vereinigung $\mathfrak{b} \cup \mathfrak{c}$ ist wie oben gezeigt ein Element von $\mathscr{T}$ und damit eine Teilmenge von $\mathfrak{t}$, die b und c und als Ideal auch die Summe $b + c$ enthält. Dass für $a \in \mathfrak{t}$ und $x \in R$ auch $xa \in \mathfrak{t}$ gilt, ist noch einfacher zu sehen.

Schließlich gilt $\mathfrak{t} \neq R$. Denn sonst wäre $1 \in \mathfrak{t}$, aber dann wäre 1 schon in einem der Ideale aus $\mathscr{T}$ enthalten, ein Widerspruch! □

BEMERKUNG 3.25. Eine weitere typische Anwendung des Lemmas von Zorn ist der Satz, dass jeder Vektorraum eine Basis besitzt. Sei nämlich K ein Körper und V ein K-Vektorraum. Nach Definition ist eine Basis von V eine Teilmenge von V, so dass sich jeder Vektor in V eindeutig als Linearkombination von Elementen dieser Teilmenge darstellen lässt. (Dabei sind Linearkombinationen immer *endliche* Summen.) Äquivalent ist, dass eine Basis eine maximale linear unabhängige Teilmenge von V ist. (Um diese Äquivalenz zu zeigen, wird nicht benötigt, dass V endlich erzeugt ist.)

Sei nun $\mathscr{M}$ die Menge aller linear unabhängigen Teilmengen von V, mit der Inklusion von Teilmengen als partieller Ordnung. Es gilt $\emptyset \in \mathscr{M}$, und ist $\mathscr{T}$ eine Kette in $\mathscr{M}$, so ist die Vereinigung aller Elemente von $\mathscr{T}$ eine linear unabhängige Teilmenge von V und damit eine obere Schranke von $\mathscr{T}$ in $\mathscr{M}$. Mit dem Lemma von Zorn folgt nun die Existenz einer maximalen linear unabhängigen Teilmenge in V.

Man kann darüber hinaus zeigen, dass zu je zwei Basen $\mathscr{B}, \mathscr{B}' \subset V$ eine Bijektion $\mathscr{B} \xrightarrow{\sim} \mathscr{B}'$ existiert. Das bedeutet, dass man (im Sinne der Kardinalität unendlicher Mengen) auch im allgemeinen Fall von der Dimension eines Vektorraums sprechen kann. Siehe Ergänzung LA1.6.48, [**Soe-AZT**] 5.3. ◊

ERGÄNZUNG 3.26 (Maximale echte Untergruppen von $\mathbb{Q}$). Dass hier verschiedene Existenzaussagen (eines maximalen Ideals, einer Basis) mit dem Lemma von Zorn auf eine Art und Weise bewiesen werden, die (fast) rein formal aussieht, sollte nicht zu dem Irrglauben verleiten, dass ein »maximales Objekt« immer existiert.

Zum Beispiel existiert keine *maximale echte Untergruppe* der additiven Gruppe $\mathbb{Q}$. (Das ist nicht ganz offensichtlich, aber auch nicht sehr schwer zu beweisen.)

Was ist an dem folgenden »Beweis« nicht korrekt?

Sei $\mathscr{M}$ die Menge aller echten Untergruppen von $\mathbb{Q}$. Offenbar ist $\mathscr{M}$ nicht leer. Für eine durch die Inklusion total geordnete nicht-leere Teilmenge $\mathscr{T} \subseteq \mathscr{M}$ ist die Vereinigung aller Elemente von $\mathscr{T}$ wieder eine Untergruppe von $\mathbb{Q}$, also eine obere Schranke von $\mathscr{T}$. Nach dem Lemma von Zorn besitzt $\mathscr{M}$ ein maximales Element. □ Ergänzung 3.26

ERGÄNZUNG 3.27 (Konstruktion der reellen Zahlen). Sei $\mathbb{Q}^{\mathbb{N}} = \prod_{i\in\mathbb{N}} \mathbb{Q}$, verstanden als Ring mit komponentenweiser Addition und Multiplikation. Wir betrachten die Elemente dieses Rings als *Folgen* (im Sinne der Analysis) von rationalen Zahlen. Sei $R \subset \mathbb{Q}^{\mathbb{N}}$ der Unterring aller Cauchy-Folgen. Dann ist die Teilmenge $\mathfrak{n}$ aller Nullfolgen ein Ideal in R, und zwar sogar ein maximales Ideal. Die Abbildung

$$R/\mathfrak{n} \to \mathbb{R}, \quad (a_n)_n \mapsto \lim_{n\to\infty} a_n,$$

die (die Restklasse) einer Cauchy-Folge auf ihren Grenzwert abbildet, ist ein Isomorphismus.

Diese Überlegung kann man benutzen, um die reellen Zahlen aus den rationalen Zahlen *zu konstruieren*, also die Existenz eines Körpers zu beweisen, der die »üblichen Eigenschaften« des Körpers $\mathbb{R}$ hat (also formaler ausgedrückt: ein System von Axiomen erfüllt, die den Körper $\mathbb{R}$ eindeutig charakterisieren). Dazu muss man »direkt nachrechnen«, dass $R/\mathfrak{n}$ tatsächlich diese Eigenschaften hat.

In Abschnitt LA2.18.8.3 finden Sie etwas mehr Details. □ Ergänzung 3.27

3.3. Polynomringe

DEFINITION 3.28. Sei R ein Ring.

(1) Eine *R-Algebra* ist ein Ring S zusammen mit einem Ringhomomorphismus $\varphi\colon R \to S$.

(2) Seien S, S' mit Ringhomomorphismen $\varphi\colon R \to S$, $\varphi'\colon R \to S'$ Algebren über R. Ein *Homomorphismus von R-Algebren* ist ein Ringhomomorphismus $\psi\colon S \to S'$, so dass $\varphi' = \psi \circ \varphi$ gilt.

Wir bezeichnen mit $\mathrm{Hom}_R(S, S')$ die Menge aller R-Algebren-Homomorphismen von S nach S'. Besonders dann, wenn R ein Körper ist, sprechen wir statt von einem R-Algebren-Homomorphismus auch einfach von einem K-Homomorphismus.

⊣

Man kann allgemeiner definieren, wann ein nicht-kommutativer Ring S eine Algebra über einem kommutativen Ring R ist, aber die Definition ist ein kleines bisschen komplizierter als oben und wir beschränken uns auf den Fall dass R *und* S kommutative Ringe sind.

Ist K ein Körper und A eine K-Algebra, gegeben durch einen Ringhomomorphismus $\varphi\colon K \to A$, so können wir A als K-Vektorraum mit der Skalarmultiplikation $x \cdot a := \varphi(x)a$ verstehen (für $x \in K$, $a \in A$, und wobei rechts die Ringmultiplikation von A verwendet wird). Es ist

leicht nachzurechnen, dass die Vektorraumaxiome erfüllt sind. Ist andererseits A ein Ring, der auch ein K-Vektorraum ist, stimmen Ring- und Vektorraumaddition überein, und gilt $x(ab) = (xa)b = a(xb)$ für alle $x \in K, a, b \in A$, so trägt A eine K-Algebrenstruktur, nämlich $K \to A, x \mapsto x \cdot 1$. Verwendet man den Begriff des R-Moduls (siehe Abschnitt LA2.18.7.1) so kann man den Begriff der R-Algebra auch für beliebige kommutative Ringe in analoger Weise betrachten.

Beispiel 3.29. Sei R ein Ring. Der Polynomring $R[X]$ ist eine R-Algebra (vermöge des Ringhomomorphismus $R \to R[X]$, der $a \in R$ abbildet auf das konstante Polynom a). Ist S eine R-Algebra, gegeben durch $\varphi\colon R \to S$, $\alpha \in S$ und $\Phi\colon R[X] \to S$ der zugehörige Einsetzungshomomorphismus mit $\Phi(X) = \alpha$, $\Phi(a) = \varphi(a)$ für $a \in R$, so ist Φ ein Homomorphismus von R-Algebren. ◊

Wir verallgemeinern die Konstruktion des Polynomrings über einem Ring in einer Variablen, indem wir auch mehrere Variablen zulassen (gegebenenfalls auch unendlich viele). Ist I die vorgegebene Indexmenge für die Variablen, so definieren wir einen kommutativen Ring $R[X_i; i \in I]$, den Polynomring in den Variablen X_i, $i \in I$. Seine Elemente sind Linearkombinationen (mit Koeffizienten in R) von Ausdrücken der Form $X_{i_1}^{n_1} \cdot \dots \cdot X_{i_r}^{n_r}$ für $r \in \mathbb{N}$, $i_s \in I$, $n_s \in \mathbb{N}_{>0}$. (In jedem einzelnen Polynom treten also immer nur endlich viele Variablen auf.) Diese Polynome werden in der offensichtlichen Weise addiert. Die Multiplikation ist durch die Regel

$$X_{i_1}^{m_1} \cdot \dots \cdot X_{i_r}^{m_r} \cdot X_{i_1}^{n_1} \cdot \dots \cdot X_{i_r}^{n_r} = X_{i_1}^{m_1+n_1} \cdot \dots \cdot X_{i_r}^{m_r+n_r}$$

und die Distributivgesetze eindeutig bestimmt (wobei wir hier auch $m_s = 0$ bzw. $n_s = 0$ zulassen und $X_i^0 = 1$ setzen).

Den Polynomring $R[X_1, \dots, X_n]$ in endlich vielen Variablen $X_1, \dots, X_n$ kann man identifizieren mit $(R[X_1, \dots, X_{n-1}])[X_n]$, so dass man diese Ringe auch induktiv konstruieren kann. Im Fall einer unendlichen Indexmenge I der Variablen kann man den Polynomring $R[X_i;\ i \in I]$ als die Vereinigung der Ringe $R[X_i;\ i \in I']$ über alle endlichen Teilmengen $I' \subset I$ definieren (allerdings vereinigt man hier Mengen, die nicht als Teilmengen einer gemeinsamen Obermenge gegeben sind).

Wir haben dann den Begriff des Einsetzungshomomorphismus.

Satz 3.30. *Seien R ein Ring, I eine Menge, S eine R-Algebra, gegeben durch einen Ringhomomorphismus $\varphi\colon R \to S$. Sind Elemente $x_i \in S$, $i \in I$ gegeben, dann gibt es einen eindeutig bestimmten R-Algebren-Homomorphismus $\Phi\colon R[X_i;\ i \in I] \to S$ mit $\Phi(X_i) = x_i$ für alle $i \in I$.*

Für $f \in R[X_i]$ schreiben wir meist $f(x_i)$ statt $\Phi(f)$.

Allgemeiner kann man hier auch Ringhomomorphismen $\varphi\colon R \to S$ in einen nicht notwendig kommutativen Ring S betrachten. Man erhält dann zu Elementen $x_i \in S$ wie oben einen eindeutig bestimmten Ringhomomorphismus Φ für den $\Phi(x) = \varphi(x)$ für $x \in R$ und $\Phi(X_i) = x_i$ für alle $i \in I$ gilt.

Beweis. Die Eindeutigkeit ist klar, ebenso ist ein Kandidat für Φ offensichtlich. Man muss dann nur überprüfen, dass es sich um einen R-Algebren-Homomorphismus handelt. Das ist unproblematisch; man benutzt, dass Polynome aus Elementen aus R und den Unbestimmten durch sukzessive Multiplikation und Addition aufgebaut sind und dass φ ein Ringhomomorphismus ist. □

Den Satz über den Einsetzungshomomorphismus kann man auch als universelle Eigenschaft des Polynomrings betrachten und folgendermaßen umformulieren.

SATZ 3.31. *Sei R ein kommutativer Ring und I eine Menge. Dann existiert eine R-Algebra P zusammen mit Elementen $X_i \in P$, $i \in I$, so dass für alle R-Algebren S die Abbildung*

$$\mathrm{Hom}_R(P,S) \to \mathrm{Abb}(I,S), \quad f \mapsto (i \mapsto f(X_i)),$$

bijektiv ist.

Die R-Algebra P ist eindeutig bestimmt bis auf eindeutigen Isomorphismus im folgenden Sinne: Ist P' zusammen mit Elementen $X_i' \in P'$ eine R-Algebra, die ebenfalls die obige Eigenschaft besitzt, so existiert ein eindeutig bestimmter R-Algebren-Isomorphismus $P \to P'$ mit $X_i \mapsto X_i'$ für alle i.

Wir schreiben auch $R[X_i,\ i \in I] := P$ und nennen diesen Ring den Polynomring über R in den Variablen X_i, $i \in I$.

BEWEIS. Wir definieren P als den oben konstruierten Polynomring. Die Umkehrabbildung der Abbildung $\mathrm{Hom}_R(P,S) \to \mathrm{Abb}(I,S)$ bildet eine Abbildung von I nach S, also eine durch I indizierte Familie von Elementen von S ab auf den zugehörigen Einsetzungshomomorphismus $P = R[X_i] \to S$.

Dass P durch die genannte »universelle« Eigenschaft eindeutig bestimmt ist bis auf eindeutigen Isomorphismus, zeigt man »wie üblich«, siehe zum Beispiel Abschnitt LA2.18.1.1. □

BEMERKUNG 3.32. Etwas formaler kann man wie folgt vorgehen. Wir hatten den Polynomring in einer Variablen definiert als die Menge $R^{(\mathbb{N})}$ aller Tupel von Elementen aus R, in denen höchstens endlich viele Einträge $\neq 0$ sind. Addiert werden Elemente von $R^{(\mathbb{N})}$ komponentenweise. Die Multiplikation zweier solcher Tupel $(a_n)_n$, $(b_n)_n$ ist das Tupel

$$(a_n)_n \cdot (b_n)_n = \left(\sum_{j+k=n} a_j b_k \right)_n .$$

Um dieses zu bilden, wird neben der Addition und Multiplikation in R nur die Addition auf $\mathbb{N}$ benötigt. Die Variable X wurde dann als das Element $(0,1,0,\dots)$ definiert. Damit kann man dann jedes Element aus $R[X] := R^{(\mathbb{N})}$ in der üblichen Form $\sum_{i=0}^{d} a_i X^i$ mit $d \in \mathbb{N}$, und eindeutig bestimmten $a_i \in R$ schreiben.

Den Polynomring in den Variablen X_i, $i \in I$, für eine beliebige Indexmenge können wir dann konstruieren, indem wir die Menge $\mathbb{N}$ oben ersetzen durch

$$\mathbb{N}^{(I)} := \{(n_i)_{i\in I};\ n_i \in \mathbb{N},\ \text{höchstens endlich viele } n_i \neq 0\}\,.$$

Es wird

$$R^{(\mathbb{N}^{(I)})} = \{(a_n)_{n\in\mathbb{N}^{(I)}};\ a_n \in R,\ \text{höchstens endlich viele } a_n \neq 0\}$$

zu einem Ring mit der komponentenweisen Addition und der Multiplikation

$$(a_n)_n \cdot (b_n)_n = \left(\sum_{j+k=n} a_j b_k \right)_n ,$$

wobei nun $n, j, k \in \mathbb{N}^{(I)}$ zu betrachten sind (und auf $\mathbb{N}^{(I)}$ die komponentenweise Addition verwendet wird).

Die Variablen definieren wir wie folgt. Zu $i \in I$ sei $e_i \in \mathbb{N}^{(I)}$ der »i-te Standardbasisvektor«, d.h. das Tupel mit einer 1 an der i-ten Stelle und sonst überall Nullen. Wir setzen dann $X_i := (\xi_{in})_n$ mit $\xi_{ie_i} = 1$ und $\xi_{in} = 0$ für alle $n \neq e_i$.

Noch etwas allgemeiner kann man in dieser Konstruktion $\mathbb{N}^{(I)}$ durch irgendeine Menge mit einer kommutativen und assoziativen Verknüpfung mit einem neutralen Element ersetzen (also durch ein kommutatives »Monoid«). Siehe auch [**Bo-A**] 2.5, [**JS**] IV.3. ◊

DEFINITION 3.33. Sei R ein Ring, $f \in R[X]$ ein Polynom und S eine R-Algebra. Sei $\alpha \in S$.

(1) Das Element α heißt *Nullstelle* von f (in S), wenn $f(\alpha) = 0$ gilt. (Um $f(\alpha)$ in S »auszurechnen«, wenden wir also auf alle Koeffizienten von f den zur R-Algebra S gehörigen Ringhomomorphismus $R \to S$ an und setzen dann für X das Element α ein.)

(2) Sei nun in der obigen Situation S ein Integritätsring und $f \neq 0$. Die eindeutig bestimmte natürliche Zahl m mit $(X-\alpha)^m \mid f$ und $(X-\alpha)^{m+1} \nmid f$ heißt die *Vielfachheit* (oder *Ordnung*) von α als Nullstelle von f; wir schreiben $\mathrm{mult}_\alpha(f) := m$.

⊣

Es ist also α genau dann eine Nullstelle von f, wenn $\mathrm{mult}_\alpha(f) \geq 1$ gilt. Im Fall $\mathrm{mult}_\alpha(f) = 1$ nennen wir α auch eine *einfache Nullstelle*, falls $\mathrm{mult}_\alpha(f) > 1$ ist, so heißt α eine *mehrfache Nullstelle*. Genauer sprechen wir im Fall $\mathrm{mult}_\alpha(f) = 2$ von einer *doppelten Nullstelle*, usw.

In der Analysis wird bewiesen, dass man für eine differenzierbare Funktion $\mathbb{R} \to \mathbb{R}$ an der Ableitung ablesen kann, ob es sich bei einer Nullstelle um eine mehrfache Nullstelle handelt. Eine Ableitung im Sinne der Analysis, die auf dem Grenzwertbegriff basiert, steht uns im Allgemeinen natürlich nicht zur Verfügung. Überraschender Weise ist aber die »formale Ableitung« eines Polynoms, die durch die Anwendung der üblichen Ableitungsregeln gebildet wird, für manche Eigenschaften ein nützlicher Ersatz.

DEFINITION 3.34. Sei R ein Ring. Die *(formale) Ableitung* eines Polynoms $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ ist das Polynom

$$f' := \sum_{i=1}^{n} i a_i X^{i-1} \in R[X].$$

⊣

LEMMA 3.35. *Sei R ein Ring. Die Bildung der Ableitung von Polynomen genügt den folgenden Rechenregeln. Hier seien $f, g \in R[X]$, $a \in R$.*

(1) $(af)' = a \cdot f'$,

(2) $(f+g)' = f' + g'$,

(3) $(fg)' = f'g + fg'$.

BEWEIS. Die Teile (1) und (2) sind leicht nachzurechnen. Für Teil (3) genügt es wegen (1) und (2) dann, den Fall $f = X^i$, $g = X^j$ zu betrachten (denn beide Seiten der Gleichung in (3) verhalten sich »R-bilinear« in f und g). In diesem Fall ist die Sache klar. □

LEMMA 3.36. *Seien R ein Integritätsring, $f \in R[X]$, $f \neq 0$, und $\alpha \in R$ eine Nullstelle von f. Dann sind äquivalent:*

(i) *α ist eine mehrfache Nullstelle von f,*

(ii) $f'(\alpha) = 0$.

BEWEIS. Wir schreiben $f = (X-\alpha)^r g$ mit $g(\alpha) \neq 0$, also $r = \mathrm{mult}_\alpha(f)$. Nach Voraussetzung ist $r \geq 1$. Es gilt dann, wie man leicht nachrechnet,

$$f' = r(X-\alpha)^{r-1} g + (X-\alpha)^r g',$$

und Einsetzen von α liefert

$$f'(\alpha) = \begin{cases} g(\alpha) \neq 0 & \text{wenn } r = 1 \\ 0 & \text{wenn } r > 1. \end{cases}$$

Daraus folgt die Behauptung. □

BEMERKUNG 3.37. Wir können also in der Situation des Lemmas sagen:

(1) $f(\alpha) = 0 \quad \Leftrightarrow \quad \mathrm{mult}_\alpha(f) > 0$,
(2) $f(\alpha) = f'(\alpha) = 0 \quad \Leftrightarrow \quad \mathrm{mult}_\alpha(f) > 1$,

Wo liegt das Problem, wenn man die Liste fortsetzen wollte, indem man höhere Ableitungen von f betrachtet und dementsprechende höhere Vielfachheiten als Nullstelle? ◊

3.4. Faktorielle Ringe

Im weiteren Verlauf der Vorlesung wird der Begriff des *irreduziblen Polynoms* eine wichtige Rolle spielen, also von Polynomen $f \in K[X]$ (K ein Körper), die sich nicht als Produkt $f = gh$ mit nicht-konstanten Polynomen g, h schreiben lassen.

Diese Polynome haben dann stets auch die *Primeigenschaft* als Elemente des Rings $K[X]$, d.h. ein Produkt wird genau dann von einem irreduziblen Polynom geteilt, wenn einer der Faktoren von dem Polynom geteilt wird. Das liegt daran, dass $K[X]$ ein *faktorieller* Ring ist. Siehe Definition 3.38, Definition LA2.15.49.

Um dann auch in konkreten Fällen entscheiden zu können, ob gegebene Polynome irreduzibel sind, sind die Irreduzibilitätskriterien aus Abschnitt 3.6 nützlich, die darauf beruhen, Polynome mit Koeffizienten in einem faktoriellen Ring zu betrachten, in dem es Primelemente gibt (der also kein Körper ist), zum Beispiel mit Koeffizienten im Ring $\mathbb{Z}$ der ganzen Zahlen. Die Kriterien geben dann auch Aufschluss über die Irreduzibilität der entsprechenden Polynome, wenn man sie als Elemente des Polynomrings über dem Quotientenkörper dieses faktoriellen Rings betrachtet.

Das grundlegende Ergebnis hierfür ist der Satz von Gauß, Satz 3.50.

Wir beginnen damit, einige Begriffe zu wiederholen, die wir schon in der Linearen Algebra 2 definiert haben, siehe auch Abschnitt LA2.15.4.3.

DEFINITION 3.38. Sei R ein Integritätsring.

(1) Ein Element $p \in R \setminus (R^\times \cup \{0\})$ heißt *irreduzibel*, wenn in jeder Darstellung $p = ab$ von p als Produkt von Elementen $a, b \in R$ gilt, dass $a \in R^\times$ oder $b \in R^\times$ ist.
(2) Ein Element $p \in R \setminus (R^\times \cup \{0\})$ heißt *prim* (oder: ein *Primelement*), wenn für alle $a, b \in R$ mit $p \mid ab$ gilt, dass $p \mid a$ oder $p \mid b$.
(3) Ein *faktorieller Ring* ist ein Integritätsring R, derart dass sich jedes Element von $R \setminus (R^\times \cup \{0\})$ als (endliches) Produkt von Primelementen schreiben lässt.

⊣

Ist p ein Primelement eines Integritätsrings, dann ist p irreduzibel. Ist R ein faktorieller Ring, so sind die Begriffe *irreduzibel* und *prim* für Elemente von R äquivalent.

In der Linearen Algebra 2 haben wir bewiesen (Satz LA2.15.47):

SATZ 3.39. *Sei R ein Hauptidealring. Dann ist R faktoriell.*

BEWEISSKIZZE. (Für einen vollständigen Beweis siehe das Skript zur Linearen Algebra 2 wie oben zitiert.) Weil R ein Hauptidealring ist, wird jede aufsteigende Kette von Idealen stationär. Daraus folgt, dass sich jedenfalls jedes Element von $R \setminus (R^\times \cup \{0\})$ als Produkt von irreduziblen Elementen schreiben lässt. (Sei $a \in R \setminus (R^\times \cup \{0\})$ gegeben. Ist a irreduzibel, so sind wir direkt fertig. Sonst gibt es eine Zerlegung $a = a_0 a_1$. Induktiv kann man a_0 und a_1 weiter zerlegen, bis man zu einem Produkt von irreduziblen Elementen kommt. Das

genannte Ergebnis über Idealketten impliziert, dass dieser Prozess nach endlich vielen Schritten zum Ende kommen muss.)

Es ist dann noch zu zeigen, dass jedes irreduzible Element in R auch prim ist. Ist $p \in R$ irreduzibel, so folgt aus $(p) \subseteq (a)$ für $a \in R$, dass $(a) = (p)$ oder $(a) = R$ gilt. Das Ideal (p) ist also maximal und daher insbesondere ein Primideal. Deshalb ist p tatsächlich ein Primelement. □

Sei R ein faktorieller Ring. Sind p, p' zueinander assoziiert, dann ist p genau dann prim, wenn p' prim ist. Unter einem Vertretersystem der Primelemente in R bis auf Assoziiertheit verstehen wir eine Teilmenge $P \subset R$, die aus Primelementen von R besteht und so dass jedes Primelement von R zu *genau einem* Element von P assoziiert ist. Zum Beispiel bilden die positiven Primzahlen ein Vertretersystem der Primelemente im Ring $\mathbb{Z}$ bis auf Assoziiertheit.

Satz 3.40. *Sei R ein faktorieller Ring, K sein Quotientenkörper und $P \subset R$ ein Vertretersystem der Primelemente von R bis auf Assoziiertheit.*

(1) *Jedes Element $x \in R \setminus \{0\}$ lässt sich in der Form*

$$x = u \prod_{p \in P} p^{v_p}$$

mit $u \in R^\times$ und mit $v_p \in \mathbb{N}$ schreiben, wobei höchstens endlich viele v_p von Null verschieden sind. Sowohl u als auch die Exponenten v_p sind durch x eindeutig bestimmt. Man schreibt auch $v_p(x) := v_p$ für die Vielfachheit, mit der p in der obigen Darstellung (der »Primfaktorzerlegung« von x) auftritt.

(2) *Jedes Element $x \neq 0$ des Quotientenkörpers von R lässt sich schreiben als*

$$x = u \prod_{p \in P} p^{v_p}$$

mit $u \in R^\times$ und mit $v_p \in \mathbb{Z}$, wobei wieder höchstens endlich viele v_p von Null verschieden sind und dieselbe Eindeutigkeitsaussage gilt. Wir erhalten so eine Abbildung $K^\times \to \mathbb{Z}, x \mapsto v_p(x)$.

Beweis. Jedenfalls lässt sich jedes x, das keine Einheit ist, als Produkt von Primelementen aus R schreiben. Indem wir diese gegebenenfalls um Einheiten abändern, können wir x als Produkt einer Einheit in R und von Elementen der Menge P schreiben. Das liefert die Existenzaussage in (1), und auch in (2), wenn wir das Ergebnis aus Teil (1) auf Zähler und Nenner einer Darstellung von $x \in K^\times$ anwenden.

Um die Eindeutigkeit in (1) zu zeigen, beweisen wir, dass für $p \in P$ die Gleichheit

$$v_p(x) = \max\{r;\ p^r \mid x\}$$

gilt. Jedenfalls ist $p^{v_p(x)} \mid x$ klar. Die Beziehung $p^{v_p(x)+1} \mid x$ wäre aber nur möglich, wenn p ein Teiler des Produkts $\prod_{q \in P \setminus \{p\}} q^{v_q}$ wäre. Induktiv folgte dann aber aus der Primeigenschaft von p, dass $p \mid q$ für ein $q \in P \setminus \{p\}$ gilt. Weil q prim (und damit irreduzibel) ist, wären dann p und q zueinander assoziiert, was der Definition von P widerspräche. □

In einem faktoriellen Ring R existiert zu je zwei Elementen x, y ein *größter gemeinsamer Teiler*, also ein Element $d \in R$, das sowohl x als auch y teilt, und so dass jeder gemeinsame Teiler von x und y ein Teiler von d ist. Ein solcher größter gemeinsamer Teiler ist eindeutig bestimmt bis auf Assoziiertheit. Ist P wie oben ein Vertretersystem der Primelemente von R bis auf Assoziiertheit, so ist mit der obigen Schreibweise $\prod_{p \in P} p^{\min(v_p(x), v_p(y))}$ ein größter gemeinsamer Teiler von $x, y \in R \setminus \{0\}$.

Beispiel 3.41. Wir skizzieren zwei Beispiele von Integritätsringen, die nicht faktoriell sind.

(1) Die Teilmenge
$$\mathbb{Z}[i\sqrt{5}] := \{a + ib\sqrt{5};\ a, b \in \mathbb{Z}\} \quad \subseteq \mathbb{C}$$
ist ein Unterring. Man kann zeigen, dass dieser Integritätsring nicht faktoriell ist. Das Element 2 ist in diesem Ring irreduzibel, jedoch kein Primelement, denn es teilt das Produkt
$$(1 - i\sqrt{5})(1 + i\sqrt{5}) = 6 = 2 \cdot 3,$$
aber teilt weder $1 - i\sqrt{5}$ noch $1 + i\sqrt{5}$.

Um diese Behauptungen zu beweisen, ist es nützlich, die sogenannte Normabbildung
$$N\colon \mathbb{Z}[i\sqrt{5}] \to \mathbb{Z}, \quad a + ib\sqrt{5} \mapsto |a + ib\sqrt{5}|^2 = a^2 + 5b^2,$$
wobei die Betragsstriche den üblichen Absolutbetrag der komplexen Zahl $a + ib\sqrt{5}$ bezeichnen. Weil es sich bis auf das Quadrat um die Einschränkung des komplexen Absolutbetrags handelt, ist dieser Abbildung multiplikativ. Insbesondere gilt $N(u) \in \mathbb{Z}^\times = \{1, -1\}$ für jedes $u \in \mathbb{Z}[i\sqrt{5}]^\times$, also sind 1 und -1 die einzigen Einheiten von $\mathbb{Z}[i\sqrt{5}]$.

(2) Sei K ein Körper. Die Teilmenge
$$K[T^2, T^3] := \left\{ \sum_{i=0}^{n} a_i T^i;\ n \in \mathbb{N},\ a_i \in K,\ a_1 = 0 \right\} \subseteq K[T]$$
ist ein Unterring. Dieser Ring ist ein weiteres Beispiel eines Integritätsrings, der nicht faktoriell ist, denn $T^6 = (T^2)^3 = (T^3)^2$ hat zwei verschiedene Zerlegungen in irreduzible Elemente.

Der surjektive K-Algebren-Homomorphismus $K[X, Y] \to K[T^2, T^3]$, $X \mapsto T^2$, $Y \mapsto T^3$, induziert einen Isomorphismus $K[X, Y]/(Y^2 - X^3)$. Wir sehen daran, dass der Quotient eines faktoriellen Rings nach einem Ideal im allgemeinen nicht faktoriell ist.

Siehe auch (Ergänzungs-)Abschnitt 3.8.

◊

3.5. Der Satz von Gauß

Um zu entscheiden, ob ein Polynom in $\mathbb{Q}[X]$ irreduzibel ist, ist es oft nützlich, die Frage als eine Frage über ein Polynom mit Koeffizienten in $\mathbb{Z}$ zu formulieren (indem man das gegebene Polynom mit einer geeigneten ganzen Zahl multipliziert, kann man eventuell auftretende Nenner »beseitigen«). Im faktoriellen Ring $\mathbb{Z}$ liefert dann die durch die Primzahlen gegebene Struktur zusätzliche Werkzeuge, zum Beispiel die Möglichkeit, die Koeffizienten »modulo einer Primzahl p zu reduzieren«, also das Polynom in $\mathbb{F}_p[X]$ zu betrachten, das entsteht, wenn jeder Koeffizient durch seine Restklasse modulo p ersetzt wird.

Eine wesentliche Grundlage dieser Methoden ist die Tatsache, dass auch der Ring $\mathbb{Z}[X]$ faktoriell ist (auch wenn es sich *nicht* um einen Hauptidealring handelt). Allgemeiner besagt der Satz von Gauß, dass der Polynomring über einem faktoriellen Ring R ebenfalls faktoriell ist, und er liefert darüberhinaus eine Beschreibung der irreduziblen Elemente in $R[X]$ in Termen des Polynomrings $\mathrm{Quot}(R)[X]$ über dem Quotientenkörper von R.

Ein konkretes Beispiel einer nützlichen Folgerung sehen wir in Beispiel 3.48.

Definition 3.42. Sei R ein faktorieller Ring und sei p ein Primelement von R. Sei K der Quotientenkörper von R.

Für $x \in K^\times$ schreiben wir $v_p(x)$ für die eindeutig bestimmte ganze Zahl m, so dass sich x in der Form $x = p^m y$ für ein $y \in K^\times$ schreiben lässt, in dessen Darstellung als gekürzter Bruch weder der Zähler noch der Nenner durch p teilbar sind.

Außerdem setzen wir $v_p(0) = \infty$. ⊣

Das ist (abgesehen von der neuen Konvention über das Nullelement) dieselbe Zahl $v_p(x)$ wie oben.

Sind in der Situation der Definition $p, p' \in R$ zueinander assoziierte Primelemente, so gilt $v_p(x) = v_{p'}(x)$ für alle $x \in K$. Es ist genau dann $x \in R$, wenn $v_p(x) \geq 0$ für alle Primelemente p von R gilt. Äquivalent genügt es, diese Bedingung für alle Elemente eines Vertretersystems der Primelemente bis auf Assoziiertheit nachzuprüfen.

Ist p ein Primelement von R und $\mathrm{red}_p \colon R \to R/(p)$ die kanonische Projektion, so gilt für $x \in R$ genau dann $\mathrm{red}_p(x) = 0$, wenn $v_p(x) > 0$ ist.

Entscheidend sind für das Folgende das Verhalten der Abbildungen v_p bei der Anwendung auf Produkte bzw. Summen, wie es im nächsten Lemma beschrieben wird. Machen Sie sich dessen Aussage insbesondere im Fall $R = \mathbb{Z}$ klar!

LEMMA 3.43. *Sei R ein faktorieller Ring und sei p ein Primelement von R. Sei K der Quotientenkörper von R und seien $x, y \in K$. Dann gilt:*

(1) $v_p(xy) = v_p(x) + v_p(y)$,
(2) $v_p(x+y) \geq \min(v_p(x), v_p(y))$.

BEWEIS. Ist $x = 0$ oder $y = 0$, dann sind die beiden Aussagen leicht nachzuprüfen (wenn in der offensichtlichen Weise mit ∞ gerechnet wird).

Sei nun $x \neq 0, y \neq 0$. Wir schreiben $x = p^{v_p(x)}x'$ und $y = p^{v_p(y)}y'$ mit $p \nmid x'$, $p \nmid y'$. Weil p ein Primelement ist, gilt dann auch $p \nmid x'y'$. Daraus folgt direkt Teil (1).

Für Teil (2) sei ohne Einschränkung $v_p(x) \leq v_p(y)$. Dann ist $x + y = p^{v_p(x)}(x' + p^{v_p(y)-v_p(x)}y')$, also $v_p(x+y) = v_p(x) + v_p(x' + p^{v_p(y)-v_p(x)}y') \geq v_p(x) = \min(v_p(x), v_p(y))$. □

Teil (2) des Lemmas kann man im Fall $v_p(x) \neq v_p(y)$ noch präzisieren – unter dieser stärkeren Voraussetzung gilt $v_p(x+y) = \min(v_p(x), v_p(y))$.

ERGÄNZUNG 3.44 (Bewertungen). Sei K ein Körper. Eine Funktion $v \colon K^\times \to \mathbb{Z}$ mit

(a) $v(xy) = v(x) + v(y)$,
(b) $v(x+y) \geq \min(v(x), v(y))$

für alle $x, y \in K^\times$ nennt man eine *Bewertung* auf K. (Auf Englisch: *valuation*, das erklärt auch die Verwendung des Buchstaben »v«.) Wir setzen stets $v(0) := \infty$.

Beispiele erhält man wie oben, wenn K der Quotientenkörper eines faktoriellen Rings R ist und $v = v_p$ für ein Primelement $p \in R$ ist. Zum Beispiel kann man $R = \mathbb{Z}$, $K = \mathbb{Q}$, p eine Primzahl betrachten; man spricht dann von der p-adischen Bewertung auf $\mathbb{Q}$.

Ist v eine Bewertung auf dem Körper K und $r \in \mathbb{R}$ mit $0 < r < 1$, so kann man durch

$$|x| := r^{v(x)}$$

einen *Absolutbetrag* auf K definieren (dabei verstehen wir die Definition so, dass $|0| := 0$ sei), also eine Funktion $K \to \mathbb{R}_{\geq 0}$ mit den folgenden drei Eigenschaften für alle $x, y, z \in K$:

(a) $x = 0 \quad \Leftrightarrow \quad |x| = 0$,
(b) $|xy| = |x| \cdot |y|$,
(c) (Dreiecksungleichung) $|x+y| \leq |x| + |y|$.

Diese Betragsfunktion liefert eine Abstandsfunktion (oder: Metrik) auf K durch $d(x,y) := |y-x|$, aus der man weitere geometrische Begriffe ableiten kann.

Ein Absolutbetrag, der wie oben von einer Bewertung herkommt, erfüllt sogar die sogenannte *starke Dreiecksungleichung*

$$|x+y| \leq \max(|x|,|y|),$$

wie unmittelbar aus dem Verhalten von Bewertungen folgt, wenn man Summen einsetzt. Diese starke Dreiecksungleichung widerspricht allerdings recht drastisch unserer üblichen geometrischen Anschauung. Für den gewöhnlichen Absolutbetrag auf $\mathbb{R}$ ist sie nicht richtig; dies zeigt, dass der gewöhnliche Absolutbetrag auf $\mathbb{R}$ nicht von einer Bewertung her stammt. Für einen Absolutbetrag, der von einer Bewertung kommt, gilt zum Beispiel $|n| \leq 1$ für alle $n \in \mathbb{Z}$. □ Ergänzung 3.44

Definition 3.45. Sei R ein faktorieller Ring und sei p ein Primelement von R. Sei K der Quotientenkörper von R.

Für $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ definieren wir

$$v_p(f) := \min\{v_p(a_i);\ i = 0,\dots,n\}.$$

(Für $f = 0$ setzen wir wieder $v_p(f) = \infty$.) ⊣

Es gilt dann also für $f \in K[X]$: Es ist $f \in R[X]$ genau dann, wenn $v_p(f) \geq 0$ ist für alle Primelemente p von R.

Für $p \in R$ induziert die kanonische Projektion $\mathrm{red}_p\colon R \to R/(p)$ einen Ringhomomorphismus $: R[X] \to (R/(p))[X]$, der dadurch gegeben ist, dass auf alle Koeffizienten eines Polynoms $f \in R[X]$ die Abbildung red_p angewendet wird. Wir können diese Abbildung als Einsetzungshomomorphismus verstehen, wenn wir $R/(p)$ vermöge red_p als R-Algebra auffassen und $X \in R[X]$ auf $X \in (R/(p))[X]$ abgebildet wird. Damit ist ohne weitere Rechnung klar, dass es sich um einen Ringhomomorphismus handelt, den wir die *Reduktion der Koeffizienten modulo p* nennen und wieder mit red_p bezeichnen.

Lemma 3.46 (Lemma von Gauß). *Sei R ein faktorieller Ring und sei p ein Primelement von R. Sei K der Quotientenkörper von R und seien $f, g \in K[X]$. Dann gilt: $v_p(fg) = v_p(f) + v_p(g)$.*

Beweis. Ist $f = 0$ oder $g = 0$, so sind beide Seiten per Definition gleich ∞. Daher nehmen wir im folgenden an, dass $fg \neq 0$ gilt. Es ist klar, dass die Formel richtig ist, wenn f konstant ist. Das bedeutet auch, dass es genügt, den Satz für $f, g \in R[X]$ mit $v_p(f) = v_p(g) = 0$ zu beweisen. (Denn daraus erhalten wir den allgemeinen Fall, indem wir mit geeigneten Elementen aus $K^\times$ multiplizieren.)

Für $f, g \in R[X]$ gilt natürlich $fg \in R[X]$, so dass wir bereits $v_p(fg) \geq 0 = v_p(f) + v_p(g)$ sehen. Die andere Abschätzung erhalten wir durch Reduktion der Koeffizienten modulo p: Aus $v_p(f) = v_p(g) = 0$ folgt $\mathrm{red}_p(f) \neq 0, \mathrm{red}_p(g) \neq 0$. Weil $(R/(p))[X]$ ein Integritätsring ist, folgt $\mathrm{red}_p(fg) \neq 0$ und sodann $v_p(fg) = 0$. □

Korollar 3.47. *Sei R ein faktorieller Ring und sei $h \in R[X]$ normiert. Ist dann $h = fg$ eine Zerlegung von h als Produkt von normierten Polynomen $f, g \in K[X]$ so gilt $f, g \in R[X]$.*

Beweis. Nach Voraussetzung gilt für alle Primelemente $p \in R$, dass $v_p(h) = 0$ (weil h in $R[X]$ liegt und normiert ist) und $v_p(f) \leq 0$, $v_p(g) \leq 0$ (weil f und g normiert sind). Mit dem Lemma von Gauß folgt $v_p(g) = v_p(h) = 0$, und damit $f, g \in R[X]$. □

Beispiel 3.48. Sei $f \in \mathbb{Z}[X]$ ein normiertes Polynom. Ist $a \in \mathbb{Q}$ eine Nullstelle von f, so gilt $a \in \mathbb{Z}$ und a ist ein Teiler des Absolutkoeffizienten von f. (Wende das Korollar an auf die Zerlegung $f = (X - a)g$ in $\mathbb{Q}[X]$, die man aus der Polynomdivision von f durch $X - a$ erhält.)

Insbesondere gilt: Hat ein normiertes Polynom $f \in \mathbb{Z}[X]$ keine Nullstellen in $\mathbb{Z}$, dann hat f auch keine Nullstellen in $\mathbb{Q}$. ◊

Definition 3.49. Sei R ein faktorieller Ring. Ein Polynom $f \in R[X]$ heißt *primitiv*, wenn $f \neq 0$ und wenn 1 ein größter gemeinsamer Teiler der Koeffizienten von f ist. ⊣

Mit anderen Worten: Ein Polynom $f \in R[X]$ ist genau dann primitiv, wenn $v_p(f) = 0$ für alle Primelemente $p \in R$ gilt.

Satz 3.50 (Satz von Gauß). *Sei R ein faktorieller Ring, und sei K der Quotientenkörper von R. Dann ist auch der Polynomring $R[X]$ faktoriell.*

Ein Element $f \in R[X]$ ist genau dann ein Primelement, wenn

(1) $\deg(f) = 0$ *und f als Element von R prim ist, oder*

(2) $\deg(f) > 0$, *f primitiv und f als Element von $K[X]$ prim ist.*

Beweis. Jedenfalls sind die angegebenen Elemente prim in $R[X]$. Für f wie in (1) ist nämlich der Ring $R/(f)$ und damit auch der Ring $(R/(f))[X] \cong R[X]/fR[X]$ ein Integritätsring. (Hier schreiben wir $fR[X]$ für das von f in $R[X]$ erzeugte Hauptideal.)

Für f wie in (2) argumentieren wir mit dem Lemma von Gauß. Gilt $f \mid gh$ für $g, h \in R[X]$, so teilt jedenfalls f in $K[X]$ einen der Faktoren. Wir betrachten ohne Einschränkung den Fall $f \mid g$ in $K[X]$, sagen wir $g = fr$ mit $r \in K[X]$. Nach dem Lemma von Gauß gilt dann $0 \leq v_p(g) = v_p(fr) = v_p(f) + v_p(r) = v_p(r)$ für alle Primelemente p von R, wobei wir ganz links ausgenutzt haben, dass $g \in R[X]$ ist, und ganz rechts, dass f primitiv ist. Aus $v_p(r) \geq 0$ für alle Primelemente p von R folgt, dass $r \in R[X]$ gilt, die Teilbarkeitsbeziehung $f \mid g$ gilt also sogar in $R[X]$.

Wir zeigen nun, dass sich jedes Element aus $R[X] \setminus (R^\times \cup \{0\})$ als Produkt von Elementen der Form (1) und (2) schreiben lässt. Daraus folgt der Satz, und zwar auch, dass es keine weiteren Primelemente geben kann, denn jedes solche lässt sich ja auch als ein Produkt von Elementen aus dieser Liste schreiben, und in diesem Fall kann das Produkt nur einen einzigen Faktor haben.

Sei also $f \in R[X]$ ein Polynom, das von 0 verschieden und keine Einheit in $R[X]$ (äquivalent: keine Einheit in R) ist. Wenn wir f als Element von $K[X]$ betrachten, können wir f in der Form $f = uf_1 \cdots f_r$ mit irreduziblen Polynomen $f_i \in K[X]$ und $u \in K^\times$ schreiben. Indem wir nötigenfalls u verändern, können wir alle in den f_i auftretenden Nenner und einen größten gemeinsamen Teiler der Koeffizienten jedes dieser Polynome »herausziehen« und daher annehmen, dass alle f_i sogar in R liegen und primitiv sind. Damit handelt es sich bei den f_i um Elemente der Form (2).

Wir zeigen nun, dass (im Fall, dass alle f_i primitiv sind) das Element $u \in K^\times$ in R liegen muss. Dies folgt direkt aus dem Lemma von Gauß, das uns $0 \leq v_p(f) = v_p(u) + \sum_i v_p(f_i) = v_p(u)$ für alle Primelemente p von R liefert. Weil u in R liegt, lässt es sich als Produkt von Elementen der Form (1) schreiben (oder ist eine Einheit in R, und dann können wir einfach f_1 durch uf_1 ersetzen). Insgesamt erhalten wir so die gesuchte Produktdarstellung für f. □

3.6. Irreduzibilitätskriterien

In der Regel ist es schwierig zu überprüfen, ob ein gegebenes Polynom mit Koeffizienten in einem Körper irreduzibel ist.

Für Polynome von kleinem Grad ist die Irreduzibilität an die (Nicht-)Existenz von Nullstellen geknüpft, genauer gilt:

BEMERKUNG 3.51 (Einfache Irreduzibilitätskriterien). Sei K ein Körper.

(1) Jedes Polynom in $K[X]$ vom Grad 1 ist irreduzibel. (Denn der Grad eines Produkts ist die Summe der Grade der Faktoren, also können Polynome vom Grad 1 keine Zerlegung als Produkt nicht-konstanter Polynome haben.)

(2) Ein Polynom $f \in K[X]$ mit $2 \leq \deg(f) \leq 3$ ist genau dann irreduzibel, wenn es keine Nullstelle in K besitzt. Denn in einer Zerlegung $f = gh$ mit $\deg(g) > 0$, $\deg(h) > 0$ muss (mindestens) einer der Faktoren g, h Grad 1 haben. Andererseits ist jedes Polynom vom Grad > 1, das eine Nullstelle $\alpha \in K$ besitzt, reduzibel, weil der zugehörige Linearfaktor $X - \alpha$ ein nicht-trivialer Teiler ist.

$\Diamond$

Ein weiteres Kriterium, das leicht zu begründen ist, ist, dass die Eigenschaft *irreduzibel* invariant ist unter Isomorphismen: Ist K ein Körper und $\varphi\colon K[X] \to K[X]$ ein K-Algebren-Automorphismus, dann ist $f \in K[X]$ genau dann irreduzibel, wenn $\varphi(f)$ irreduzibel ist. (Es ist nicht schwer zu zeigen, dass die Automorphismen φ genau die Abbildungen mit $X \mapsto aX + b$ für $a, b \in K$, $a \neq 0$, sind.) In Beispiel 3.55 kommt diese Überlegung zum Einsatz.

Mit dem folgenden Reduktionskriterium lässt sich die Irreduzibilität eines Polynoms $f \in R[X]$ mit Koeffizienten in einem faktoriellen Ring R zeigen, indem man die Reduktion von f modulo Primelementen p betrachtet. Ein typisches Beispiel, in dem wir das Kriterium später anwenden werden, ist $R = \mathbb{Z}$, p eine Primzahl. Man beachte, dass im allgemeinen der Ring $R/(p)$ nicht wieder faktoriell sein muss (vergleiche Beispiel 3.41 (2)), aber das wird auch nicht benötigt.

SATZ 3.52 (Reduktionskriterium). *Sei R ein faktorieller Ring mit Quotientenkörper K, sei $p \in R$ ein Primelement und sei $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ ein Polynom vom Grad $n > 0$, so dass a_n nicht von p geteilt wird. Wenn das Bild von f in $(R/(p))[X]$ irreduzibel ist, dann ist f irreduzibel in $K[X]$.*

Wird zusätzlich f als primitiv vorausgesetzt, so folgt, dass f in $R[X]$ irreduzibel ist.

BEWEIS. Wir betrachten zunächst den Fall, dass f primitiv ist und zeigen, dass dann f in $R[X]$ irreduzibel ist.

Angenommen, wir könnten f zerlegen als $f = gh$ mit $g, h \in R[X]$ Der Leitkoeffizient a_n von f ist das Produkt der Leitkoeffizienten von g und h. Die Voraussetzung impliziert also, dass diese beiden Leitkoeffizienten nicht durch p geteilt werden. Mit anderen Worten: Wenn wir mit $\mathrm{red}_p(f)$, $\mathrm{red}_p(g)$, $\mathrm{red}_p(h)$ die Polynome bezeichnen, die aus f, g bzw. h durch Reduktion der Koeffizienten mit der kanonischen Projektion $R \to R/(p)$ entstehen, dann haben diese jeweils denselben Grad wie das ursprüngliche Polynom. Weil die Reduktion der Koeffizienten ein Ringhomomorphismus ist, erhalten wir die Zerlegung $\mathrm{red}_p(f) = \mathrm{red}_p(g)\ \mathrm{red}_p(h)$. Weil $\mathrm{red}_p(f)$ nach Voraussetzung irreduzibel ist, muss einer der Faktoren in dieser Zerlegung eine Einheit sein und daher Grad 0 haben. Ohne Einschränkung können wir annehmen, dass $\deg(g) = \deg(\mathrm{red}_p(g)) = 0$ ist. Dann ist g ein konstantes Polynom, und das Element $g \in R$ ist ein gemeinsamer Teiler aller Koeffizienten von f. Weil f primitiv ist, folgt $g \in R^\times$. Wir haben gezeigt, dass in jeder Produktzerlegung von f einer der Faktoren eine Einheit ist. Also ist f irreduzibel.

Im allgemeinen Fall ist f ein Produkt eines Elements aus R mit einem primitiven Polynom $\tilde{f}$, das die Voraussetzungen des Satzes ebenfalls erfüllt. Mit dem obigen Argument sehen wir, dass $\tilde{f}$ in $R[X]$ und damit (nach dem Satz von Gauß) auch in $K[X]$ irreduzibel ist. In $K[X]$ sind aber f und $\tilde{f}$ assoziiert zueinander, so dass auch die Irreduzibilität von f als Element von $K[X]$ folgt. □

Das nächste Irreduzibilitätskriterium, das in den Fällen, in denen es anwendbar ist, noch einfacher ist als das Reduktionskriterium, ist benannt nach G. Eisenstein[I] und beruht ebenfalls auf der Betrachtung eines Primelements p in einem faktoriellen Ring.

Satz 3.53 (Irreduzibilitätskriterium von Eisenstein). *Seien R ein faktorieller Ring und K sein Quotientenkörper, sei $p \in R$ ein Primelement und sei $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ ein Polynom vom Grad $n > 0$. Es gelte*

$$p \nmid a_n, \qquad p \mid a_i,\ i = 0, \dots, n-1, \qquad p^2 \nmid a_0.$$

Dann ist f irreduzibel in $K[X]$. Ist das Polynom f zusätzlich primitiv, so ist es auch irreduzibel in $R[X]$.

Beweis. Sei zunächst f primitiv. Dann gibt es keine Zerlegung von f als Produkt in $R[X]$ mit einem Faktor in $R \setminus R^\times$.

Angenommen, $f = gh$ wäre eine Zerlegung von f in $R[X]$ mit $\deg(g) > 0$, $\deg(h) > 0$. Wir wenden wieder Reduktion der Koeffizienten modulo p an. Sei $\pi\colon R \to R/(p)$ die kanonische Projektion. Die Voraussetzung impliziert $\operatorname{red}_p(f) = \pi(a_n)X^{\deg(f)}$. Es gilt also

$$\operatorname{red}_p(g)\operatorname{red}_p(h) = \operatorname{red}_p(f) = \pi(a_n)X^{\deg(f)}.$$

Zwar ist $(R/(p))[X]$ nicht unbedingt faktoriell, aber jedenfalls ist X ein Primelement in diesem Ring (wegen Lemma 3.17, denn $(R/(p))[X]/(X) \cong R/(p)$ ist ein Integritätsring). Weil X das Produkt $\operatorname{red}_p(g)\operatorname{red}_p(h)$ teilt, teilt X einen der Faktoren. Indem wir X »ausklammern« und dann induktiv fortfahren, sehen wir, dass $\operatorname{red}_p(g) = cX^i$ und $\operatorname{red}_p(h) = dX^j$ mit $c, d \in R/(p)$, $i, j \in \mathbb{N}$, gilt. (Alternativ kann man die Zerlegung im Polynomring über dem Quotientenkörper von $R/(p)$ betrachten, der in jedem Fall faktoriell ist.)

Nun gilt $\deg(\operatorname{red}_p(g)) \leq \deg(g)$, entsprechend für h, und so folgt, dass $i = \deg(g) > 0$ und $j = \deg(h) > 0$ gilt.

Die Absolutkoeffizienten von g und h sind also beide durch p teilbar. Das ist aber ein Widerspruch zu der Voraussetzung $p^2 \nmid a_0$. Also ist f irreduzibel in $R[X]$ und in $K[X]$.

Im allgemeinen Fall können wir f durch das Polynom $d^{-1}f$ ersetzen, wo d ein größter gemeinsamer Teiler der Koeffizienten von f ist, um die Irreduzibilität in $K[X]$ zu zeigen. Weil $p \nmid a_n$ gilt, haben wir auch $p \nmid d$, so dass diese Ersetzung nichts an den Bedingungen bezüglich der Teilbarkeit der Koeffizienten durch p ändert. Wir können uns somit auf den Fall einschränken, dass f primitiv ist, den wir bereits behandelt haben. □

Beispiel 3.54. (1) Sei $a \in \mathbb{Z}$ eine ganze Zahl, so dass eine Primzahl p existiert, die a teilt, aber so dass p^2 kein Teiler von a ist. Dann ist für jedes $n \in \mathbb{N}_{>0}$ das Polynom $X^n - a$ irreduzibel in $\mathbb{Q}[X]$ (und sogar in $\mathbb{Z}[X]$). Dies folgt aus dem Eisenstein-Kriterium für den faktoriellen Ring $\mathbb{Z}$, angewandt auf das Primelement p.

(2) Sei k ein Körper und $R = k[T]$ der Polynomring über k in der Unbestimmten T. Sei K der Quotientenkörper von R. (Wir schreiben auch $K = k(T)$ und nennen K den Körper der rationalen Funktionen in T über k.) Dann ist das Polynom $X^n - T$ irreduzibel in $K[X]$ (und auch in $R[X]$). Dies folgt aus dem Eisenstein-Kriterium für den faktoriellen Ring R, angewandt auf das Primelement T.

◊

[I] https://de.wikipedia.org/wiki/Gotthold_Eisenstein

BEISPIEL 3.55. Sei p eine Primzahl. Dann ist das Polynom

$$f = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Q}[X] \quad \text{irreduzibel.}$$

Zwar ist hier das Eisenstein-Kriterium nicht direkt anwendbar, aber wir können uns mit dem folgenden Trick behelfen. Wir betrachten den K-Automorphismus $K[X] \to K[X], X \mapsto X + 1$. (Der Umkehrhomomorphismus ist gegeben durch $X \mapsto X - 1$.) Es genügt dann zu zeigen, dass $f(X + 1)$ irreduzibel ist. Nun haben wir (mit der »endlichen geometrischen Reihe«; die folgenden Rechnungen finden im Quotientenkörper von $K[X]$ statt)

$$f = \frac{X^p - 1}{X - 1},$$

also

$$f(X+1) = \frac{(X+1)^p - 1}{(X+1) - 1} = \frac{(X+1)^p - 1}{X} = \sum_{i=1}^{p} \binom{p}{i} X^{i-1},$$

wobei wir zum Schluss den binomischen Lehrsatz benutzt haben. Es gilt $\binom{p}{p} = 1$, $p \mid \binom{p}{i}$ für $i = 1, \ldots, p-1$ (vergleiche Beispiel 3.2 (2)), und $p^2 \nmid p = \binom{p}{1}$, so dass für das Polynom $f(X+1)$ die Voraussetzungen des Eisensteinschen Kriteriums über dem Ring $\mathbb{Z}$ und für das Primelement p erfüllt sind. ◊

BEISPIEL 3.56. Nicht in jedem Fall lässt sich die Irreduzibilität eines Polynoms (etwa in $\mathbb{Z}[X]$) durch Reduktion modulo geeigneter Primelemente zeigen. Zum Beispiel ist das Polynom $X^4 + 1$ zwar irreduzibel in $\mathbb{Z}[X]$ (das lässt sich leicht nachrechnen), aber seine Reduktion modulo p ist für jede Primzahl p reduzibel (das ist nicht ganz so leicht – siehe [**JS**] Beispiel IV.4.10). ◊

3.7. Wie untersucht man einen Ring? *

Wir haben (in der Algebra und zum Teil schon in der Linearen Algebra) unter anderem die folgenden Eigenschaften von Ringen kennengelernt; in dieser Liste impliziert jede genannte Eigenschaft alle darauf folgenden.

(1) Körper,
(2) Euklidischer Ring,
(3) Hauptidealring,
(4) Faktorieller Ring,
(5) Integritätsring.

Allerdings ist diese Einordnung sehr grob, denn es gibt viele faktorielle Ringe, die keine Hauptidealringe sind, sehr viele Integritätsringe die nicht faktoriell sind, und natürlich auch sehr viele Ringe, die keine Integritätsringe sind.

Eine »Klassifikation« von Ringen bis auf Isomorphie ist nur unter sehr restriktiven zusätzlichen Annahmen möglich.

Weitere Methoden zur Untersuchung von Ringen werden im Gebiet der *Kommutativen Algebra* bereitgestellt, zum Beispiel die *Lokalisierung nach einer multiplikativen Teilmenge* (das ist ein Bruchrechenkalkül, der die Konstruktion des Quotientenkörpers eines Integritätsrings verallgemeinert) und das *Tensorprodukt* (ähnlich wie das Tensorprodukt von Vektorräumen, das wir in der Linearen Algebra 2 angeschaut haben). Außerdem ist es nützlich, *Moduln* über Ringen zu studieren, das sind additive Gruppen mit einer Skalarmultiplikation (vergleiche Abschnitt LA2.18.7.1). Der Modulbegriff entspricht also genau dem Vektorraumbegriff, nur dass man auf die Voraussetzung verzichtet, dass die Skalare einen Körper bilden; stattdessen

kann man über jedem kommutativen Ring Moduln betrachten. Oft kann man einen Ring besser verstehen, wenn man die Moduln darüber gut versteht.

In der *Algebraischen Geometrie* ordnet man jedem Ring R ein »geometrisches Objekt« Spec R zu, das sogenannte *(Prim-)Spektrum* von R. Diese Verbindung zwischen (kommutativer) Algebra und Geometrie hat sich in den vergangenen Jahrzehnten als sehr nützlich und fruchtbar erwiesen. Siehe Ergänzungsabschnitt 3.8.

3.8. Das Primspektrum eines Rings *

An dieser Stelle könnte man noch wesentlich mehr schreiben, aber für den Moment belasse ich es bei einigen Andeutungen und Verweisen auf die Literatur...

In der Kommutativen Algebra ist ein wesentliches Hilfsmittel zum Studium eines Rings R die Untersuchung des sogenannten *Primspektrums* (oder: *Spektrums*) $\operatorname{Spec}(R)$ von R, das ist die Menge der Primideale von R.

Dabei wird diese Menge mit zusätzlicher Struktur versehen, zunächst mit der Struktur eines »topologischen Raums«, was man sich als Grundform einer »geometrischen Struktur« vorstellen sollte.

In der Algebraischen Geometrie wird dieser Standpunkt noch weiter auf die Spitze getrieben, in dem Sinne als das Spektrum $X = \operatorname{Spec}(R)$ als das Objekt des hauptsächlichen Interesses gesehen wird – denn hier handelt es sich um ein »geometrisches Objekt« – und der Ring dann als der Ring der »Funktionen auf X« aufgefasst wird.

Ein Prototyp dieser Korrespondenz ist am Beispiel des Polynomrings $K[X]$ über einem algebraisch abgeschossenen Körper K sichtbar. Die Primideale im Hauptidealring sind neben dem Nullideal die maximalen Ideale, und dies sind gerade die von irreduziblen Polynomen erzeugten Ideale. Über einem algebraisch abgeschlossenen Körper hat jedes irreduzible Polynom Grad 1, es gilt daher

$$\operatorname{Spec}(K[X]) = \{(0)\} \cup \{(X - a);\ a \in K\}.$$

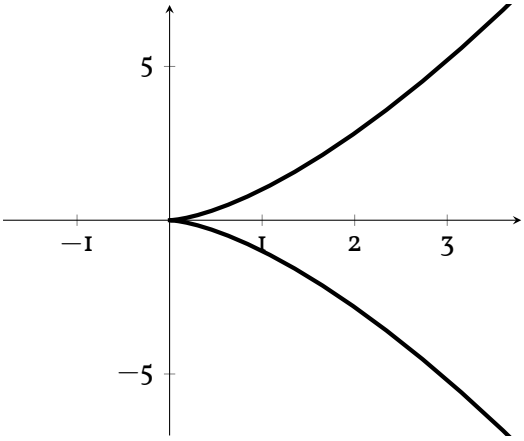
Bis auf das Nullideal, dessen Rolle wir an dieser Stelle nicht klären wollen, stehen also die Elemente des Spektrums in Bijektion zu den Elementen von K, also zum eindimensionalen Standardvektorraum. Der (nicht ganz einfache) *Hilbertsche Nullstellensatz* besagt, dass die maximalen Ideale im Polynomring $K[X_1, ..., X_n]$ über einem algebraisch abgeschlossenen Körper K genau die Ideale der Form $(X_1 - a_1, ..., X_n - a_n)$, $(a_i)_i \in K^n$, sind. Wir erhalten also eine Bijektion zwischen den maximalen Idealen in $K[X_1, ..., X_n]$ und dem n-dimensionalen Standardvektorraum K^n.

Sei weiter K algebraisch abgeschlossen. Ausgehend vom Hilbertschen Nullstellensatz ist es leicht zu sehen, dass für eine Polynomgleichung, wie zum Beispiel $y^2 = x^3$ eine Bijektion zwischen der Menge der maximalen Ideale im Quotienten $K[X, Y] / (Y^2 - X^3)$ und der Nullstellenmenge

$$V(Y^2 - X^3, K) = \{(x, y) \in K^2;\ y^2 = x^3\}$$

besteht. Siehe die Abbildung, in der wir aber nur ein Bild für den (nicht algebraisch abgeschlossenen) Körper $\mathbb{R}$ der reellen Zahlen angeben können.

Es ist faszinierend, dass sich dann geometrische Eigenschaften dieser Nullstellenmenge (wie die »Spitze« am Ursprung, wo die gezeichnete Kurve auch bei starker Vegrößerung nicht »wie eine Gerade aussieht«) in algebraischen Eigenschaften des Rings $K[X, Y] / (Y^2 - X^3)$ widerspiegeln (konkret: dass dieser Ring nicht faktoriell ist).



Die Menge $\{(x,y)^t \in \mathbb{R}^2;\ y^2 = x^3\}$

Der Zusammenhang zwischen dem Ring $K[T^2, T^3]$ und der Gleichung $y^2 - x^3 = 0$ kommt daher, dass die Abbildung $K[X,Y] \to K[T], X \mapsto T^3$, $Y \mapsto T^2$, ein Ringhomomorphismus mit Bild $K[T^2, T^3]$ und Kern $(Y^2 - X^3)$ ist.

Wie gesagt ist die Bedeutung der nicht-maximalen Primideale hier im Dunkeln geblieben. Sie ist aber wesentlich für den modernen Aufbau der algebraischen Geometrie, der auf Alexander Grothendieck zurückgeht und sowohl die »klassische« algebraische Geometrie beflügelt als auch eine enge Verbindung zwischen algebraischer Zahlentheorie und algebraischer Geometrie geführt hat, ohne die die meisten großen Durchbrüche in der algebraischen Zahlentheorie in den letzten Jahrzehnten (zum Beispiel der Beweis der Taniyama-Shimura-Weil-Vermutung durch Wiles und Taylor, aus der sich der Beweis der Fermatschen Vermutung ergibt) undenkbar gewesen wären.

Mehr Informationen finden Sie in [**Bo-A**], Abschnitt 3.9, und in meinem Übersichtsartikel Classics revisited: Éléments de géométrie algébrique[a], Jahresbericht der DMV **120**(4) (2018), 235–290.
Für einen systematischeren Einstieg können die Bücher von M. Reid, Undergraduate Algebraic Geometry[b], Cambrigde University Press oder K. Hulek, *Elementare Algebraische Geometrie*, Springer dienen, oder – schon etwas anspruchsvoller – der Klassiker von D. Mumford, *The Red Book of Varieties and Schemes*, Springer.
Ansonsten können Sie natürlich in entsprechenden umfangreicheren Lehrbüchern (R. Hartshorne, *Algebraic Geometry*; R. Vakil, Foundations of Algebraic Geometry[c]; U. Görtz, T. Wedhorn, *Algebraic Geometry I*, Springer) und in den Vorlesungen *Kommutative Algebra* und *Algebraische Geometrie* mehr über diese Theorie lernen.

[a] `https://www.uni-due.de/%7Ehx0050/pdf/classics_revisited_EGA-20180608.pdf`
[b] `https://homepages.warwick.ac.uk/staff/Miles.Reid/MA4A5/UAG.pdf`
[c] `http://math.stanford.edu/%7Evakil/216blog/FOAGnov1817public.pdf`

KAPITEL 4

Körper und Körpererweiterungen

4.1. Körper und die Charakteristik eines Körpers

Wir wollen uns nun detaillierter mit Körpern und insbesondere mit *Körpererweiterungen* beschäftigen, wie wir sie im nachfolgenden Abschnitt einführen werden. Ein Körper K ist ein (kommutativer) Ring, dessen Einheitengruppe aus allen Elementen $\neq 0$ besteht. (Insbesondere ist der Nullring kein Körper.)

Einen Ringhomomorphismus zwischen zwei Körpern nennen wir auch Körperhomomorphismus (oder einfach Homomorphismus, wenn klar ist, was gemeint ist).

Jeder Körper K ist ein Integritätsring. Der Kern des eindeutigen Ringhomomorphismus $\mathbb{Z} \to K$ (Beispiel 3.2 (1)) ist daher ein Primideal (Lemma 3.17).

DEFINITION 4.1. Sei K ein Körper. Wir sagen, K habe *Charakteristik 0*, wenn der eindeutig bestimmte Ringhomomorphismus $\mathbb{Z} \to K$ injektiv ist, und habe *Charakteristik p*, wenn sein Kern von der Primzahl p erzeugt wird. Die ⊣

In einem Körper der Charakteristik $p > 0$ gilt also $1 + \cdots + 1 = 0$ (mit p Summanden auf der linken Seite), und p ist die kleinste Zahl > 0, für die das richtig ist.

DEFINITION 4.2. Sei K ein Körper. Der kleinste Teilkörper von K, mit anderen Worten der Durchschnitt aller Teilkörper von K, heißt der *Primkörper* von K. ⊣

SATZ 4.3. *Sei K ein Körper.*

(1) *Es sind äquivalent:*
   (i) *Der Körper K hat Charakteristik 0.*
   (ii) *Der Primkörper von K ist isomorph zu $\mathbb{Q}$.*

(2) *Es sind äquivalent:*
   (i) *Der Körper K hat Charakteristik $p > 0$.*
   (ii) *Der Primkörper von K ist isomorph zu $\mathbb{F}_p$.*

BEWEIS. In beiden Fällen ist die Implikation (ii) $\Rightarrow$ (i) klar. (Diese Implikation folgt auch formal daraus, dass die in (i) betrachteten Fälle alle Möglichkeiten abdecken, sobald wir (i) $\Rightarrow$ (ii) in (1) und (2) gezeigt haben.)

Wenn K Charakteristik 0 hat, dann ist der Ringhomomorphismus $\varphi\colon \mathbb{Z} \to K$ injektiv und induziert durch $\frac{a}{b} \mapsto \varphi(a)\varphi(b)^{-1}$ einen Homomorphismus $\psi\colon \mathbb{Q} \to K$. Da das Bild von φ in jedem Teilkörper von K enthalten ist, gilt das auch für das Bild dieser Fortsetzung nach $\mathbb{Q}$. Also liegt $\psi(\mathbb{Q})$ im Primkörper von K. Andererseits handelt es sich bei $\psi(\mathbb{Q})$ um einen Teilkörper, so dass dies der Primkörper von K sein muss. Dann ist ψ der gesuchte Isomorphismus.

Im Fall positiver Charakteristik induziert der Ringhomomorphismus $\varphi\colon \mathbb{Z} \to K$ einen Körperhomomorphismus $\mathbb{F}_p \to K$, dessen Bild ein Körper ist, der in jedem Teilkörper von K enthalten ist. Wie vorher folgt auch in diesem Fall die Behauptung. □

BEMERKUNG 4.4. Sei K ein endlicher Körper der Charakteristik $p > 0$. Dann ist der Primkörper von K der Körper $\mathbb{F}_p$, und wir können K als $\mathbb{F}_p$-Algebra betrachten. Insbesondere ist K ein $\mathbb{F}_p$-Vektorraum und folglich $\#K$ eine Potenz von p.

Wir werden später sehen, dass es zu jeder Potenz $q = p^r, r \geq 1$, einen Körper mit q Elementen gibt, und dass je zwei solche Körper zueinander isomorph sind. ◊

4.2. Algebraische Körpererweiterungen

Ein wesentlicher Aspekt ist im Folgenden die Untersuchung von (Polynom-)Gleichungen in einer Variablen und deren Lösungen. Wir stellen hier zunächst einige Grundbegriffe zur Verfügung, die es erlauben, die folgenden Situationen zu beschreiben:

- Ist K ein Körper und $f \in K[X]$ ein Polynom, dann hat f möglicherweise keine Nullstellen in K. Es ist aber möglich, dass K Teilkörper eines Körpers L ist, in dem f eine Nullstelle hat. (Zum Beispiel $K = \mathbb{R}, f = X^2 + 1, L = \mathbb{C}$.)
  Wir werden später zeigen, dass es zu K und $f \in K[X]$ mit $\deg(f) > 0$ immer einen Körper L gibt, in dem K ein Teilkörper ist und in dem f eine Nullstelle besitzt.
- Andererseits kann es für einen Körper L und einen Teilkörper K Elemente von L geben, die nicht Nullstelle eines Polynoms mit Koeffizienten in K sind. (Natürlich ist jedes $\alpha \in L$ Nullstelle eines Polynoms in $L[X]$, nämlich zum Beispiel von $X - \alpha$.)

DEFINITION 4.5. Ist K ein Teilkörper eines Körpers L, so nennen wir auch L einen *Erweiterungskörper* von K und sprechen von der *Körpererweiterung* L/K.

Ist E ein Teilkörper von L, der seinerseits K als Teilkörper enthält, $K \subseteq E \subseteq L$, so heißt E ein *Zwischenkörper* der Erweiterung L/K. ⊣

Manchmal betrachten wir nicht nur die Inklusion eines Teilkörpers in einem Erweiterungskörper sondern allgemeiner auch einen (notwendigerweise injektiven) Körperhomomorphismus als Körpererweiterung.

BEISPIEL 4.6. Beispiele für Körpererweiterungen, die wir bereits kennen, sind

(1) $\mathbb{C}/\mathbb{R}$.

(2) $\mathbb{C}/\mathbb{Q}$.

(3) $\mathbb{Q}[i]/\mathbb{Q}$, wobei $\mathbb{Q}[i] = \{a + ib;\ a, b \in \mathbb{Q}\}$ ist (dies ist ein Teilkörper von $\mathbb{C}$, auch $\mathbb{C}/\mathbb{Q}[i]$ ist also eine Körpererweiterung).

◊

DEFINITION 4.7. Sei L/K eine Körpererweiterung. Sei $M \subseteq L$ eine Teilmenge.

(1) Die von M erzeugte K-Algebra ist der kleinste Unterring von L, der K und M enthält. Äquivalent ist dies das Bild des Einsetzungshomomorphismus $K[X_m,\ m \in M] \to L$, $X_m \mapsto m$, also die Menge aller polynomialen Ausdrücke in den Elementen von M mit Koeffizienten in K. Wir bezeichnen diese K-Algebra mit $K[M]$.

(2) Der über K von M erzeugte Teilkörper von L ist der kleinste Teilkörper von L, der K und M enthält. Dieser kann mit dem Quotientenkörper von $K[M]$ identifiziert werden. Wir bezeichnen diesen Teilkörper von L mit $K(M)$.

⊣

In der Situation der Definition gilt stets $K[M] \subseteq K(M)$. Wir werden unten die Bedingung, dass hier Gleichheit besteht, genauer untersuchen.

Die Bezeichnung $K[M]$ steht im Konflikt mit der Bezeichnung für den Polynomring in einer Variablen – man muss hier also aufpassen, ob M der Name der einen Variablen ist, oder eine Teilmenge einer K-Algebra.

DEFINITION 4.8. (1) Eine Körpererweiterung L/K heißt *endlich erzeugt*, wenn eine endliche Teilmenge $M \subseteq L$ mit $L = K(M)$ existiert.

(2) Eine Körpererweiterung L/K heißt *einfach*, wenn ein Element $\alpha \in L$ mit $L = K(\alpha)$ existiert.

⊣

DEFINITION 4.9. Sei L/K eine Körpererweiterung.

(1) Ein Element $\alpha \in L$ heißt *algebraisch über K*, wenn ein Polynom $f \in K[X] \setminus \{0\}$ existiert mit $f(\alpha) = 0$. Das eindeutig bestimmte normierte Polynom kleinsten Grades in $K[X]$, das α als Nullstelle hat, heißt dann das *Minimalpolynom* von α über K.

Wir bezeichnen das Minimalpolynom von α über K mit $\operatorname{minpol}_{\alpha,K}$.

(2) Ein Element $\alpha \in L$, das nicht algebraisch über K ist, heißt *transzendent*.

(3) Die Körpererweiterung L/K heißt *algebraisch*, wenn jedes Element von L über K algebraisch ist. Andernfalls heißt die Erweiterung *transzendent*.

⊣

In der Situation von Teil (1) ist jedenfalls klar, dass es ein normiertes Polynom f kleinsten Grades gibt, das α als Nullstelle hat. Dies ist dann auch das normierte Polynom kleinsten Grades im Kern des Einsetzungshomomorphismus $K[X] \to L, X \mapsto \alpha$. Dieser Kern ist ein Hauptideal, und es folgt, dass f den Kern als Ideal erzeugt. Daraus folgt auch die Eindeutigkeit von f.

BEISPIEL 4.10. Wir betrachten die Körpererweiterung $\mathbb{C}/\mathbb{Q}$.

(1) Die Elemente $\sqrt{2}$ und i von $\mathbb{C}$ sind algebraisch über $\mathbb{Q}$, denn sie sind Nullstellen von $X^2 - 2$ bzw. $X^2 + 1$.

Allgemeiner sind die (positiven) n-ten Wurzeln $\sqrt[n]{a}$ von Zahlen $a \in \mathbb{R}_{>0}$ algebraisch über $\mathbb{Q}$. Natürlich ist überhaupt jede Zahl $\alpha \in \mathbb{C}$, für die es $n \in \mathbb{N}$ mit $\alpha^n \in \mathbb{Q}$ gibt, algebraisch über $\mathbb{Q}$, denn es handelt sich dann um eine Nullstelle von $X^n - a \in \mathbb{Q}[X]$ mit $a = \alpha^n$. Die Schreibweise $\sqrt[n]{a}$ sollte man dann aber nicht verwenden (jedenfalls nicht, ohne es explizit zu präzisieren), weil es verschiedene Elemente gibt, deren n-te Potenz gleich a ist (wenn nicht gerade $a = 0$ oder $n = 1$ ist).[1]

(2) Die Erweiterung $\mathbb{C}/\mathbb{Q}$ ist *nicht* algebraisch. Zum Beispiel ist die Kreiszahl π nicht algebraisch über $\mathbb{Q}$ – dies ist der Satz von Lindemann, der aber nicht einfach zu beweisen ist. Überhaupt ist es nicht ganz einfach, Elemente von $\mathbb{C}$ konkret anzugeben, die transzendent über $\mathbb{Q}$ ist. Das einfachste Argument, um zu begründen, dass $\mathbb{C}/\mathbb{Q}$ nicht algebraisch ist, ist ein Mächtigkeitsargument. Siehe Ergänzung 4.21.

◊

[1] Eine Ausnahme sieht man manchmal: Ist L/K eine Körpererweiterung und $n \in \mathbb{N}$ und $a \in K$ ein Element, für das das Polynom $X^n - a$ über L vollständig in Linearfaktoren zerfällt, so schreibt man manchmal $K(\sqrt[n]{a})$, wenn dieser Erweiterungskörper davon unabhängig ist, *welche* Nullstelle von $X^n - a$ mit $\sqrt[n]{a}$ bezeichnet wird. Konkretes Beispiel: $\mathbb{Q}(\sqrt{-5}) \subseteq \mathbb{C}$, denn der Körper ist derselbe, egal ob $i\sqrt{5}$ oder $-i\sqrt{5}$ zu $\mathbb{Q}$ adjungiert wird.

SATZ 4.11. *Sei L/K eine Körpererweiterung. Ist $\alpha \in L$ algebraisch über K, so ist $K[\alpha] \cong K[X]/(\mathrm{minpol}_{\alpha,K})$ ein Körper, und es gilt folglich $K[\alpha] = K(\alpha)$ und dass $\mathrm{minpol}_{\alpha,K}$ irreduzibel ist.*

BEWEIS. Nach Definition ist $K[\alpha]$ das Bild des Einsetzungshomomorphismus $K[X] \to L$, $X \mapsto \alpha$. Aus dem Homomorphiesatz (und der Definition des Minimalpolynoms von α) erhalten wir den Isomorphismus $K[\alpha] \cong K[X]/(\mathrm{minpol}_{\alpha,K})$. Als Unterring von L ist $K[\alpha]$ ein Integritätsring, also ist $\mathrm{minpol}_{\alpha,K}$ irreduzibel (Lemma 3.17). Aus Satz 3.20 folgt dann auch, dass $K[\alpha]$ sogar ein Körper ist, und daher auch die Gleichheit $K[\alpha] = K(\alpha)$. □

Unser nächstes Ziel ist zu beweisen, dass eine Körpererweiterung der Form $K(M)/K$ genau dann algebraisch ist, wenn alle Elemente des Erzeugendensystems M algebraisch über K sind. Das bedeutet, dass Summen, Produkte und Quotienten algebraischer Elemente wieder algebraisch sind. Es ist nicht offensichtlich, wie man das beweisen könnte! (Denken Sie einmal darüber nach.) Mit ähnlichen Methoden können wir dann auch zeigen, dass sich die Eigenschaft »algebraisch« transitiv in einem »Turm« von Körpererweiterungen verhält, das heißt: Sind E/K und L/E algebraische Erweiterungen, so ist auch L/K algebraisch.

Die entscheidende Zutat, mit der der Beweis dann letztlich nicht mehr schwierig ist, ist der Begriff der endlichen Körpererweiterung. Wir greifen hier auf (Grund-)Begriffe der Linearen Algebra zurück und verwenden, dass ein Erweiterungskörper L eines Körpers K insbesondere als K-Vektorraum betrachtet werden kann, wenn wir als Addition die Körperaddition und als Skalarmultiplikation die Einschränkung der Multiplikation $L \times L \to L$ von L auf den Definitionsbereich $K \times L$ verwenden.

DEFINITION 4.12. Sei L/K eine Körpererweiterung.

(1) Die Vektorraumdimension von L als K-Vektorraum heißt auch der *Grad* der Erweiterung L/K und wird mit $[L : K]$ bezeichnet.
(2) Die Erweiterung L/K heißt *endlich*, wenn ihr Grad endlich ist, andernfalls *unendlich*.

⊣

BEISPIEL 4.13. Sei L/K eine Körpererweiterung.

(1) Ein fundamentales Beispiel ist das folgende: Sei $\alpha \in L$ algebraisch über K mit Minimalpolynom f. Dann gilt $[K(\alpha) : K] = \deg(f)$.
Denn wie wir gesehen haben ist $K(\alpha) = K[\alpha] \cong K[X]/(f)$, und die Restklassen von $1, X, \ldots, X^{\deg(f)-1}$ bilden eine Basis dieses Quotienten als K-Vektorraum.
(2) Ist andererseits $\alpha \in L$ transzendent über K, dann ist der Einsetzungshomomorphismus $K[X] \to K(\alpha)$, $X \mapsto \alpha$, injektiv. Daraus folgt $[K(\alpha) : K] \geq \dim_K K[X] = \infty$.

◊

BEISPIEL 4.14. Weil $X^7 - 2$ irreduzibel über $\mathbb{Q}$ ist (Eisenstein-Kriterium für den faktoriellen Ring $\mathbb{Z}$ und das Primelement $p = 2$) und $\alpha := \sqrt[7]{2}$ als Nullstelle hat, ist $X^7 - 2 = \mathrm{minpol}_{\alpha,\mathbb{Q}}$.

Es gilt

$$\mathbb{Q}(\sqrt[7]{2}) = \{a_0 + a_1\sqrt[7]{2} + a_2(\sqrt[7]{2})^2 + \cdots + a_6(\sqrt[7]{2})^6;\ a_0, \ldots, a_6 \in \mathbb{Q}\}.$$

Es ist nämlich klar, dass die linke Seite in der rechten Seite enthalten ist. Die Gleichheit kann man auf verschiedene Arten begründen: Wir haben gesehen, dass $\mathbb{Q}(\sqrt[7]{2}) \cong \mathbb{Q}[X]/(X^7 - 2)$ ist, wobei hier die Restklasse von X genau dem Elemente $\sqrt[7]{2}$ entsprechen soll. Weil die Restklassen von $1, X, \ldots, X^6$ eine Basis des $\mathbb{Q}$-Vektorraums $\mathbb{Q}[X]/(X^7 - 2)$ bilden, bilden 1, $\sqrt[7]{2}, \ldots, (\sqrt[7]{2})^6$ eine Basis von $\mathbb{Q}(\sqrt[7]{2})$.

Alternativ kann man nachprüfen, dass die Menge auf der linken Seite der obigen Gleichung ein Unterring von $\mathbb{Q}(\sqrt[7]{2})$ ist. Weil dieser als $\mathbb{Q}$-Vektorraum endlichdimensional, und offenbar ein Integritätsring ist, handelt es sich um einen Körper (Übungsaufgabe). Daraus folgt die Gleichheit. ◊

SATZ 4.15 (Gradformel). *Seien M/L und L/K Körpererweiterungen. Dann sind äquivalent:*

(i) *Die Erweiterungen M/L und L/K sind endlich.*

(ii) *Die Erweiterung M/K ist endlich.*

In diesem Fall gilt

$$[M : K] = [M : L] \cdot [L : K].$$

BEWEIS. Sei $(b_i)_{i\in I}$ eine Basis von L als K-Vektorraum und $(c_j)_{j\in J}$ eine Basis von M als L-Vektorraum.

Behauptung. Die Familie $(b_i c_j)_{i\in I, j\in J}$ ist eine Basis von M als K-Vektorraum.

Begründung. Wir zeigen zuerst, dass die angegebene Familie ein Erzeugendensystem ist. Sei dazu $x \in M$. Wir können $x = \sum \gamma_j c_j$ schreiben, mit $\gamma_j \in L$, höchstens endlich viele γ_j sind $\neq 0$. Jedes γ_j können wir in der Form $\gamma_j = \sum_i \beta_{ij} b_i$ schreiben, $\beta_{ij} \in K$, höchstens endlich viele β_{ij} sind $\neq 0$. Damit erhalten wir insgesamt die Darstellung

$$x = \sum_j \left(\sum_i \beta_{ij} b_i \right) c_j = \sum_{i,j} \beta_{ij} (b_i c_j)$$

von x als endliche Linearkombination der Elemente $b_i c_j$ mit Koeffizienten in K.

Nun zeigen wir, dass die Familie $(b_i c_j)_{i\in I, j\in J}$ linear unabhängig über K ist. In der Tat, ist $\sum_{i,j} \beta_{ij} b_i c_j = 0$ eine Darstellung des Nullvektors mit $\beta_{ij} \in K$, so folgt $\sum_j \left(\sum_i \beta_{ij} b_i \right) c_j = 0$, wegen der linearen Unabhängigkeit der c_j über L also $\sum_i \beta_{ij} b_i = 0$ für alle j. Nun wenden wir an, dass die b_i linear unabhängig über K sind und erhalten $\beta_{ij} = 0$ für alle i und j, wie gewünscht.

Daraus folgt sowohl die Äquivalenz von (i) und (ii) als auch die Dimensionsformel.

Wenn man im nicht-endlichdimensionalen Fall nicht die Existenz von Basen benutzen möchte, kann man das Argument auch etwas modifizieren, um das zu vermeiden. □

BEMERKUNG 4.16. Die Gradformel hat viele nützliche einfache Anwendungen. Zum Beispiel:

(1) Eine Körpererweiterung, deren Grad eine Primzahl ist, hat keine echten Zwischenkörper.

(2) Es gilt $\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{2})$. (Und analog kann man ähnliche Aussagen dieser Form beweisen.)

◊

Das folgende Lemma fasst mehrere nützliche Charakterisierungen zusammen (die wir teilweise schon gesehen haben). Neu ist insbesondere die Implikation (iv) ⇒ (i), die zeigt, dass jede endliche Körpererweiterung algebraisch ist.

LEMMA 4.17. *Sei L/K eine Körpererweiterung, $\alpha \in L$. Dann sind äquivalent:*

(i) *Das Element α ist algebraisch über K.*

(ii) *Der Unterring $K[\alpha]$ von L ist ein Körper.*

(iii) *Es gilt* $K[\alpha] = K(\alpha)$.

(iv) *Die Erweiterung* $K(\alpha)/K$ *ist endlich.*

In diesem Fall ist $\mathrm{minpol}_{\alpha,K}$ *irreduzibel in* $K[X]$ *und* $[K(\alpha) : K] = \deg(\mathrm{minpol}_{\alpha,K})$.

BEWEIS. (i) $\Rightarrow$ (ii). Wir haben bereits gesehen, dass in der Situation von (i) $K[\alpha] = K(\alpha)$ ein Körper ist.

(ii) $\Leftrightarrow$ (iii). Dies ist klar.

(iii) $\Rightarrow$ (iv). Da $K[\alpha]$ ein Körper ist, kann der Homomorphismus $K[X] \to L$ nicht injektiv sein. (Denn sonst wäre $K[\alpha] \cong K[X]$, und der Polynomring $K[X]$ hat Einheitengruppe $K^\times$, ist also kein Körper.) Also ist $K(\alpha) = K[\alpha] \cong K[X]/(f)$ für ein Polynom $f \neq 0$, und der Quotient ist ein endlichdimensionaler K-Vektorraum (Beispiel 4.13).

(iv) $\Rightarrow$ (i). Die Elemente $1, \alpha, \ldots, \alpha^{[K(\alpha):K]}$ sind linear abhängig, und eine nicht-triviale Linearkombination liefert uns ein Polynom $\neq 0$ mit α als Nullstelle.

Die Aussagen im letzten Satz haben wir schon Satz 4.11 bewiesen. □

SATZ 4.18. *Sei* L/K *eine Körpererweiterung. Dann sind äquivalent:*

(i) *Die Erweiterung* L/K *ist endlich.*

(ii) *Die Erweiterung* L/K *ist algebraisch und endlich erzeugt.*

(iii) *Es existieren Elemente* $\alpha_1, \ldots, \alpha_r \in L$*, die über* K *algebraisch sind und die* L *als Erweiterungskörper von* K *erzeugen, also so dass* $L = K(\alpha_1, \ldots, \alpha_r)$ *gilt.*

BEWEIS. Die Implikation (i) $\Rightarrow$ (ii) ist nach dem oben Gesagten klar. Für $\alpha \in L$ ist mit L/K auch $K(\alpha)/K$ endlich, also α algebraisch über L. Zudem ist jede Vektorraumbasis von L über K erst recht ein Erzeugendensystem von L als Erweiterungskörper von K.

Dass (iii) aus (ii) folgt, ist offensichtlich. Ist andererseits $L = K(\alpha_1, \ldots, \alpha_r)$ für algebraische Elemente α_i, so sind die Erweiterungen $K(\alpha_1, \ldots, \alpha_i)/K(\alpha_1, \ldots, \alpha_{i-1})$ alle endlich, und damit wegen Satz 4.15 auch L/K. □

Insbesondere folgt also, dass für Elemente $\alpha_1, \ldots, \alpha_r$ eines Erweiterungskörpers eines Körpers K, die über K algebraisch sind, auch alle Elemente, die sich aus den α_i durch Summen, Produkte, Quotienten und Multiplikation mit Elementen von K bilden lassen, über K algebraisch sind. Konkret ist zum Beispiel $\frac{\sqrt{7}+\sqrt[3]{6}}{9+\sqrt[4]{3}}$ algebraisch über $\mathbb{Q}$. Es ist offensichtlich wesentlich bequemer, das aus dem obigen Satz folgern zu können, als ein normiertes Polynom mit Koeffizienten in $\mathbb{Q}$ finden zu müssen, das dieses Element als Nullstelle hat.

Entsprechend gilt für nicht notwendig endlich erzeugte Erweiterungen das folgende Korollar: Jede Erweiterung, die von algebraischen Element erzeugt wird, ist algebraisch.

KOROLLAR 4.19. *Sei* L/K *eine Körpererweiterung und sei* $M \subseteq L$ *eine Teilmenge, die* L *als Erweiterungskörper von* K *erzeugt, d.h. es gilt* $L = K(M)$*, und so dass alle Elemente von* M *algebraisch über* K *sind. Dann ist die Erweiterung* L/K *algebraisch.*

BEWEIS. Es ist

$$K(M) = \bigcup_{M' \subseteq M} K(M'),$$

wobei die Vereinigung über alle endlichen Teilmengen von M gebildet werde. Denn die rechte Seite ist (warum?) ein Teilkörper von L, der K und M enthält, und enthält daher $K(M)$. Die andere Inklusion ist klar. Die Behauptung folgt daher aus dem vorherigen Satz. □

SATZ 4.20. *Seien* L/K *und* M/L *Körpererweiterungen. Dann sind äquivalent:*

(i) *Die Erweiterungen M/L und L/K sind algebraisch.*

(ii) *Die Erweiterung M/K ist algebraisch.*

BEWEIS. Es ist klar, dass (i) aus (ii) folgt. Sei andererseits (i) gegeben und $\alpha \in M$. Dann existiert ein Polynom $f = \sum_{i=0}^{n} \beta_i X^i \neq 0$ mit $f(\alpha) = 0$ und $\beta_i \in L$. Sei $E = K(\beta_0, \ldots \beta_n)$. Dies ist nach Satz 4.18 eine endliche Körpererweiterung, denn die β_i sind als Elemente von L nach Voraussetzung algebraisch über K. Weil f in $E[X]$ liegt, ist aber α algebraisch über E, die Erweiterung $E(\alpha)/E$ ist mithin endlich. Wegen der Transitivität der Eigenschaft »endlich« ist auch $E(\alpha)/K$ endlich, und es folgt, dass α algebraisch ist über K. □

ERGÄNZUNG 4.21 (Transzendente Zahlen). Um zu begründen, dass es überhaupt Körpererweiterungen gibt, die nicht algebraisch sind, also transzendente Elemente enthalten, kann man einfach einen Körper K und als Erweiterungskörper den Quotientenkörper $K(X) = \mathrm{Quot}(K[X])$ des Polynomrings über K betrachten. Offenbar ist X nicht Nullstelle eines Polynoms $\neq 0$ mit Koeffizienten in K. Interessanter ist, dass die Erweiterungen $\mathbb{R}/\mathbb{Q}$ und $\mathbb{C}/\mathbb{Q}$ nicht algebraisch sind. Das kann man folgendermaßen begründen.

(1) Am einfachsten ist es, die Mächtigkeit von $\mathbb{C}$ (oder $\mathbb{R}$) mit der Mächtigkeit der Teilmenge aller über $\mathbb{Q}$ algebraischen Elemente zu vergleichen. Siehe Anhang B.1 für die nötigen Begriffe.

Der Polynomring $\mathbb{Q}[X]$ ist abzählbar, und es folgt, dass die Teilmenge von $\mathbb{C}$, die aus allen über $\mathbb{Q}$ algebraischen komplexen Zahlen besteht, ebenfalls abzählbar ist: Wir können sie darstellen als die Vereinigung der endlichen Nullstellenmengen aller nicht-konstanten Polynome in $\mathbb{Q}[X]$.

Andererseits ist $\mathbb{C}$ selbst überabzählbar. Es muss sich daher um eine echte Teilmenge handeln.

Dieses Argument beweist die Existenz transzendenter Zahlen, allerdings liefert es keine Möglichkeit, irgendeine transzendente Zahl anzugeben.

(2) Ein berühmtes Beispiel einer transzendenten Zahl ist die Zahl π, deren Transzendenz 1882 von Lindemann bewiesen wurde. Der Beweis ist nicht einfach und benötigt, wie angesichts der Definition von π zu erwarten ist, analytische Methoden. Siehe zum Beispiel [**Lo**] Kapitel 17, [**Po**] Anhang A oder [**Bu**] Kapitel 6. Siehe auch Abschnitt 4.5.1.

(3) Die Eulersche Zahl e ist transzendent, wie 1876 von Hermite gezeigt werden konnte. Auch dies ist nicht einfach (wenn auch etwas leichter als für π).

(4) Die ersten konkreten Beispiele transzendenter Zahlen wurden 1844 von J. Liouville gegeben, die sogenannten Liouville-Zahlen[2]. Die entscheidende Beobachtung (die auch in den meisten anderen Transzendenzbeweisen essenziell ist) ist, dass sich algebraische Zahlen nur »schlecht« durch rationale Zahlen annähern lassen (d.h. dass man große Nenner verwenden muss, um die Zahl gut anzunähern – natürlich ist es wichtig, dies dann genauer zu quantifizieren). Siehe zum Beispiel [**Bu**] Kapitel 6.

□ Ergänzung 4.21

4.3. Adjunktion von Nullstellen nach Kronecker

Die folgende Konstruktion, die auf Leopold Kronecker[3] (1823 – 1891) zurückgeht, ist von fundamentaler Bedeutung für das Studium von Körpererweiterungen.

[2] https://en.wikipedia.org/wiki/Liouville_number
[3] https://de.wikipedia.org/wiki/Leopold_Kronecker

SATZ 4.22. *Sei K ein Körper und sei $f \in K[X]$ ein irreduzibles Polynom. Dann ist $L := K[X]/(f)$ ein Erweiterungskörper von K, und die Restklasse von X ist eine Nullstelle von f in L.*

BEWEIS. Nach Voraussetzung ist f irreduzibel. Weil der Ring $K[X]$ als Hauptidealring faktoriell ist, ist f ein Primelement, also ist (f) ein maximales Ideal (Satz 3.20). Deshalb ist der Quotient $L = K[X]/(f)$ ein Körper. Sei $\pi\colon K[X] \to L$ die kanonische Projektion. Es gilt $f(\pi(X)) = \pi(f(X)) = 0$, weil π ein Ringhomomorphismus ist, also ist $\pi(X)$ eine Nullstelle von f in L. □

ERGÄNZUNG 4.23. Wenn Sie Lust haben, schauen Sie sich an, wie umständlich die Beschreibung dieser Konstruktion in dem Buch [**Ar**] von Artin ist (S. 26 ff.), der in der Vorlesung, aus der das Buch entstanden ist, den Begriff des Quotienten eines Rings nach einem Ideal vermeiden wollte. □ Ergänzung 4.23

KOROLLAR 4.24. *Sei K ein Körper und sei $f \in K[X]$ ein nicht-konstantes Polynom. Dann gibt es einen Erweiterungskörper von K, in dem f vollständig in Linearfaktoren zerfällt.*

BEWEIS. Wir zerlegen f als ein Produkt irreduzibler Polynome und adjungieren dann schrittweise mit dem vorherigen Satz Nullstellen von irreduziblen Faktoren hinzu, und zerlegen nach jedem Schritt das »verbleibende« Polynom erneut in irreduzible Polynome. Lineare Faktoren können wir dabei ignorieren, so dass in jedem Schritt der Grad des zu betrachtenden Polynoms sinkt. Das stellt sicher, dass dieser Prozess nach endlich vielen Schritten endet. □

Sei K ein Körper und $f \in K[X]$ ein Polynom. Für einen Erweiterungskörper L von K bezeichnen wir mit $V(f, L) \subseteq L$ die Menge der Nullstellen von f in L. Der folgende einfache Satz ist ein wichtiges Werkzeug, um Homomorphismen zwischen Körpern zu verstehen.

SATZ 4.25. *Seien K ein Körper, α ein Element eines Erweiterungskörpers von K, das über K algebraisch ist, und L/K eine Körpererweiterung. Die Abbildung*

$$\mathrm{Hom}_K(K[\alpha], L) \to L, \quad \varphi \mapsto \varphi(\alpha),$$

induziert eine Bijektion

$$\mathrm{Hom}_K(K[\alpha], L) \xrightarrow{\sim} V(\mathrm{minpol}_{\alpha,K}, L).$$

BEWEIS. Sei $\varphi\colon K[\alpha] \to L$ ein K-Homomorphismus und sei $f = \mathrm{minpol}_{K,\alpha}$. Es gilt dann $f(\varphi(\alpha)) = \varphi(f(\alpha)) = 0$, also liegt $\varphi(\alpha)$ in $V(f, L)$. Weil $K[\alpha]$ als K-Algebra von α erzeugt wird, ist jedes solche φ durch den Wert $\varphi(\alpha)$ eindeutig bestimmt, die angegebene Abbildung ist also injektiv.

Für den Beweis der Surjektivität benutzen wir den Homomorphiesatz. Ist $\beta \in V(f, L)$, so faktorisiert der Einsetzungshomomorphismus $K[X] \to L$, $X \mapsto \beta$ über den Quotienten $K[X]/(f)$, wir erhalten also einen K-Homomorphismus $K[\alpha] \cong K[X]/(f) \to L$, der α auf β abbildet. □

4.4. Die Existenz eines algebraischen Abschlusses

DEFINITION 4.26. Ein Körper K heißt *algebraisch abgeschlossen*, wenn die folgenden äquivalenten Bedingungen erfüllt sind:

(i) Jedes nicht-konstante Polynom $f \in K[X]$ besitzt eine Nullstelle in K.

(ii) Jedes nicht-konstante Polynom $f \in K[X]$ zerfällt über K vollständig in Linearfaktoren.

⊣

Es ist klar, dass (i) aus (ii) folgt. Um andersherum (ii) zu zeigen, wenn (i) gilt, führen wir Induktion nach dem Grad von f. Nach (i) besitzt jedes nicht-konstante f jedenfalls eine Nullstelle $\alpha \in K$. Wir schreiben $f = (X - \alpha)g$ für ein Polynom g und wenden dann auf g (sofern g nicht konstant ist) die Induktionsvoraussetzung an.

LEMMA 4.27. *Sei K ein Körper. Die folgenden Aussagen sind äquivalent:*

(i) *Der Körper K ist algebraisch abgeschlossen.*

(ii) *Die irreduziblen Polynome in $K[X]$ sind genau die Polynome vom Grad 1.*

(iii) *Für jede algebraische Körpererweiterung L/K gilt $L = K$. (Wir sagen, K habe keine echten algebraischen Erweiterungen.)*

(iv) *Für jede endliche Körpererweiterung L/K gilt $L = K$. (Wir sagen, K habe keine echten endlichen Erweiterungen.)*

BEWEIS. (i) $\Rightarrow$ (ii). In jedem Fall ist jedes Polynom vom Grad 1 irreduzibel. Ist K algebraisch abgeschlossen, so zerfällt jedes Polynom als Produkt von linearen Polynomen. Gibt es mehr als einen Faktor, so ist das Polynom natürlich nicht irreduzibel.

(ii) $\Rightarrow$ (iii). Sei K algebraisch abgeschlossen und L/K eine algebraische Erweiterung. Für $\alpha \in L$ ist dann das Minimalpolynom $\mathrm{minpol}_{K,\alpha}$ irreduzibel, hat also Grad 1, das bedeutet $\alpha \in K$.

(iii) $\Rightarrow$ (iv) ist klar, weil jede endliche Erweiterung algebraisch ist.

(iv) $\Rightarrow$ (i). Sei $f \in K[X]$ ein nicht-konstantes Polynom. Wir wollen zeigen, dass f eine Nullstelle in K besitzt. Indem wir gegebenenfalls f durch einen Teiler ersetzen, können wir annehmen, dass f irreduzibel ist. Dann ist $K[X]/(f)$ eine endliche Körpererweiterung von K vom Grad $\deg(f)$. Aus (iv) folgt also $\deg(f) = 1$. Also ist f linear und besitzt insbesondere eine Nullstelle in K. □

Wir wollen zeigen, dass jeder Körper einen algebraisch abgeschlossenen Erweiterungskörper besitzt, genauer: einen *algebraischen Abschluss* im Sinne der folgenden Definition.

DEFINITION 4.28. Sei K ein Körper. Unter einem *algebraischen Abschluss* von K verstehen wir einen algebraisch abgeschlossenen Erweiterungskörper $\overline{K}$ von K, derart dass die Erweiterung $\overline{K}/K$ algebraisch ist. ⊣

LEMMA 4.29. *Sei L/K eine algebraische Körpererweiterung, so dass jedes nicht-konstante Polynom $f \in K[X]$ über dem Körper L vollständig in Linearfaktoren zerfällt. Dann ist L ein algebraischer Abschluss von K.*

BEWEIS. Es ist zu zeigen, dass L algebraisch abgeschlossen ist. Wir zeigen, dass für jede algebraische Körpererweiterung M/L notwendigerweise $M = L$ gilt.

Sei also M ein algebraischer Erweiterungskörper von L und sei $\alpha \in M$. Dann ist α algebraisch über K, und das Minimalpolynom von α über K zerfällt in $L[X]$ nach unserer Voraussetzung vollständig in Linearfaktoren. Weil $\mathrm{minpol}_L(\alpha)$ ein irreduzibles Polynom in $L[X]$ ist, das $\mathrm{minpol}_K(\alpha)$ teilt, folgt $\deg(\mathrm{minpol}_L(\alpha)) = 1$, also $\alpha \in L$. □

BEMERKUNG 4.30. Es ist sogar die folgende stärkere Aussage richtig (aber schwieriger zu zeigen):

Sei L/K eine algebraische Körpererweiterung, derart dass jedes nicht-konstante Polynom $f \in K[X]$ eine Nullstelle in L besitzt. Dann ist L ein algebraischer Abschluss von K. ◊

THEOREM 4.31. *Sei K ein Körper. Dann existiert ein algebraischer Abschluss $\overline{K}$ von K.*

Wir werden später zeigen (Satz 4.33), dass zu zwei algebraischen Abschlüssen L_1 und L_2 eines Körpers K ein K-Isomorphismus $L_1 \to L_2$ existiert.

Um die Existenz eines algebraischen Abschlusses zu zeigen, benutzen wir dieselbe Idee wie bei der Adjunktion einzelner Nullstellen im vorherigen Abschnitt. Allerdings fügen wir jetzt zu *jedem* nicht-konstanten Polynom eine Nullstelle hinzu.

BEWEIS VON THEOREM 4.31 NACH E. ARTIN. Wir beschreiben zuerst, wie wir zu einem Körper K einen Erweiterungskörper $C(K)$ konstruieren, in dem jedes nicht-konstante Polynom mit Koeffizienten in K eine Nullstelle besitzt. Wir wenden dazu sozusagen das Kronecker-Verfahren simultan auf alle nicht-konstanten Polynome in $K[X]$ an, und zwar sei $K[X]_{\geq 1}$ die Menge aller Polynome in $K[X]$ vom Grad ≥ 1 und sei

$$R := K[X_f, f \in K[X]_{\geq 1}]$$

der Polynomring, in dem wir für jedes Polynom f über K vom Grad ≥ 1 eine Variable X_f haben.

Behauptung. Das Ideal $\mathfrak{a} := (f(X_f), f \in K[X]_{\geq 1}) \subseteq R$ ist ein echtes Ideal, also $\neq R$.

Begründung. Wenn $1 \in \mathfrak{a}$ wäre, dann ließe sich eine Darstellung von 1 von der Form

$$1 = \sum_{i=1}^{n} g_i f_i(X_{f_i})$$

mit Polynomen $g_i \in R$ finden. Indem wir gegebenenfalls Terme zusammenfassen, können wir annehmen, dass die f_i paarweise verschieden sind.

Sei L ein Erweiterungskörper, in dem die Polynome $f_1, \ldots, f_n$ eine Nullstelle haben (wir wenden Korollar 4.24 auf das Produkt dieser Polynome an). Sei jeweils $\alpha_i \in L$ eine Nullstelle von f_i.

Dann erhalten wir durch $X_{f_i} \mapsto \alpha_i$ und $X_f \mapsto 0$ für alle $f \in K[X]_{\geq 1}$, die nicht in $\{f_1, \ldots, f_n\}$ liegen, einen Homomorphismus $R \to L$ von K-Algebren, der $\sum_{i=1}^{n} g_i f_i(X_{f_i})$ auf 0 abbildet, im Widerspruch dazu, dass diese Summe $= 1$ ist. Es kann also eine solche Darstellung nicht geben.

Aus der Behauptung folgt mit Satz 3.22, dass ein maximales Ideal $\mathfrak{m} \subset R$ existiert, das $\mathfrak{a}$ enthält. Wir setzen $C(K) = R/\mathfrak{m}$. Dies ist eine K-Algebra, also ein Erweiterungskörper von K. Die Restklasse von X_f in $C(K)$ ist eine Nullstelle von f, also besitzt jedes nicht-konstante Polynom über K eine Nullstelle in $C(K)$.

Die Erweiterung $C(K)/K$ ist algebraisch, denn sie wird erzeugt von den Restklassen der Variablen X_f, und X_f ist eine Nullstelle von f.

Um die Konstruktion eines algebraischen Abschlusses von K abzuschließen, setzen wir nun

$$K_0 := K, \qquad K_i := C(K_{i-1}) \quad \text{für } i \geq 1,$$

so dass wir eine Kette

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots$$

von Körpererweiterungen erhalten. Wir definieren dann

$$\overline{K} := \bigcup_{i \geq 0} K_i.$$

Behauptung. Der Körper $\overline{K}$ ist ein algebraischer Abschluss von K.

Begründung. Sei $f \in \overline{K}[X]$ ein nicht-konstantes Polynom. Dann existiert $i \in \mathbb{N}$, so dass alle (endlich vielen) Koeffizienten von f in K_i liegen. Aber dann hat f in K_{i+1} und insbesondere in $\overline{K}$ eine Nullstelle. Es folgt, dass $\overline{K}$ algebraisch abgeschlossen ist. Weil die Erweiterungen K_i/K_{i-1} algebraisch sind, gilt das auch für die Erweiterung $\overline{K}/K$. □

ERGÄNZUNG 4.32 (Alternative Beweise zum algebraischen Abschluss). Es gibt verschiedene andere Möglichkeiten, die Existenz eines algebraischen Abschlusses zu beweisen, siehe [**Mi**] Ch. 6 für eine Liste und die Notiz https://kconrad.math.uconn.edu/blurbs/galoistheory/algclosureshorter.pdf von K. Conrad für einen weiteren Beweis (der auf Zorn zurückgeht). □ Ergänzung 4.32

Wir kommen nun zum Beweis der Eindeutigkeitsaussage, die immerhin sicherstellt, dass je zwei algebraische Abschlüsse eines Körpers K isomorph sind (als K-Algebren).

SATZ 4.33. *Seien K ein Körper, L/K eine algebraische Körpererweiterung und sei $\varphi\colon K \to E$ ein Körperhomomorphismus von K in einen algebraisch abgeschlossenen Körper E.*

(1) *Dann existiert eine Fortsetzung von φ zu einem Körperhomomorphismus $\psi\colon L \to E$ (d.h. ψ ist ein Homomorphismus und es gilt $\psi(x) = \varphi(x)$ für alle $x \in K$, oder äquivalent: ψ ist ein K-Algebra-Homomorphismus).*

(2) *Ist zusätzlich L algebraisch abgeschlossen und E algebraisch über K, so ist jede Fortsetzung wie in Teil (1) ein Isomorphismus.*

Auch wenn die Aussage des Satzes an die Sprechweise der universellen Eigenschaft erinnert, handelt es sich hier *nicht* um eine universelle Eigenschaft, weil die Eindeutigkeit des Homomorphismus ψ in Teil (1) nicht gegeben ist. Es folgt daher *nicht*, dass zwischen zwei algebraischen Abschlüssen von K ein *eindeutig bestimmter* K-Isomorphismus existiere (und das ist in aller Regel auch nicht der Fall), sondern nur, dass es (irgend-)einen solchen Isomorphismus gibt. In der Regel gibt es sehr viele, von denen keiner in besonderer Weise ausgezeichnet ist. Aus diesem Grund kann man die algebraischen Abschlüsse eines Körpers nicht »in natürlicher Weise« miteinander identifizieren. Daher sollte man auch nicht von *dem* algebraischen Abschluss eines Körpers sprechen (oder sich wenigstens dieser Problematik bewusst sein, wenn man es trotzdem tut …).

BEWEIS. Zu (1). Ist $L = K[\alpha]$ für ein Element $\alpha \in L$, so können wir den gegebenen Homomorphismus $\varphi\colon K \to E$ nach L fortsetzen, indem wir α auf irgendeine Nullstelle des Minimalpolynoms $\operatorname{minpol}_{\alpha,K}$ in E abbilden (Satz 4.25). (Ganz genau genommen betrachten wir hier $\operatorname{minpol}_{\alpha,K}$ mittels φ als Polynom in $E[X]$.)

(Induktiv folgt die Fortsetzbarkeit dann für jede endliche Erweiterung L/K, aber man kann auch ohne diese Bemerkung direkt zum allgemeinen Fall übergehen.)

Um den allgemeinen Fall zu erledigen, wenden wir nochmals das Lemma von Zorn an, und zwar betrachten wir die Menge

$$\mathscr{M} = \{(M, \psi);\ K \subseteq M \subseteq L \text{ Zwischenkörper}, \psi\colon M \to E \text{ eine Fortsetzung von } \varphi\}$$

aller Paar von Zwischenkörpern der Erweiterung L/K zusammen mit einer Fortsetzung der gegebenen Abbildung. Wir definieren auf $\mathscr{M}$ eine partielle Ordnung durch

$$(M, \psi) \leq (M', \psi') \quad \Longleftrightarrow \quad M \subseteq M' \text{ und } \psi'_{|M} = \psi.$$

Es ist leicht zu sehen, dass es sich hier tatsächlich um eine partielle Ordnung handelt. Die Voraussetzungen für das Lemma von Zorn sind erfüllt. Denn ist $(M_i, \psi_i)_i$ eine Kette in $\mathscr{M}$, dann ist $\bigcup_i M_i$ zusammen mit der Abbildung $\bigcup_i M_i \to E$, die $\alpha \in M_j$ auf $\psi_j(\alpha)$ abbildet, eine obere Schranke.

Es existiert also ein maximales Element (M, ψ) in $\mathscr{M}$. Dann muss aber $M = L$ gelten, denn gäbe es ein Element $\alpha \in L \setminus M$, dann könnten wir mit dem am Anfang gegebenen Argument die Abbildung $\psi\colon M \to E$ auch noch nach $M[\alpha]$ fortsetzen, im Widerspruch zur Maximalität von (M, ψ). Aber wenn $M = L$ gilt, ist $\psi\colon L = M \to E$ die gesuchte Fortsetzung von φ nach L.

Zu (2). Seien nun L algebraisch abgeschlossen und E algebraisch über K, und $\psi\colon L \to E$ eine Fortsetzung von φ. Weil jeder Körperhomomorphismus injektiv ist, ist ψ ein Isomorphismus $L \xrightarrow{\sim} \psi(L)$. Insbesondere ist $\psi(L)$ ebenfalls algebraisch abgeschlossen. Weil mit E/K auch die Erweiterung $E/\psi(L)$ algebraisch ist, folgt $\psi(L) = E$. □

BEMERKUNG 4.34. Sei K ein Körper und sei L ein Erweiterungskörper von K, der algebraisch abgeschlossen ist. Dann ist $\{x \in L;\ x \text{ ist algebraisch über } K\}$ ein algebraischer Abschluss von K (warum?). Für Teilkörper von $\mathbb{C}$ (zum Beispiel für $\mathbb{Q}$) kann man so einen »kanonischen« algebraischen Abschluss definieren. ◊

4.5. Konstruierbarkeit mit Zirkel und Lineal

Die Frage nach der *Konstruierbarkeit* gewisser Größen ist eine klassische Frage der Mathematik, die schon im antiken Griechenland vor mehr als 2000 Jahren betrachtet wurde. Ein Konstruktionsproblem ist gegeben durch eine Menge von Punkten in der Ebene sowie die Aufgabe, daraus weitere Punkte mit vorgegebenen Eigenschaften nur mit einem (unmarkierten) Lineal und einem Zirkel zu konstruieren. Das Lineal kann also (nur) dazu verwendet werden, bereits konstruierte Punkte durch eine Gerade zu verbinden. Mit dem Zirkel kann man einen Kreis zeichnen, dessen Mittelpunkt bereits konstruiert ist und dessen Radius der Abstand zweier bereits konstruierter Punkte ist. Die Schnittpunkte der auf diese Art entstehenden Geraden und Kreise sind dann weitere konstruierte Punkte.

Zu den klassischen Konstruktionsproblemen gehören insbesondere die folgenden.

(1) *Quadratur des Kreises.* Gegeben sind zwei verschiedene Punkte in der Ebene. Sei r ihr Abstand und A der Flächeninhalt des Kreises mit Radius r. Man konstruiere, ausgehend von den beiden gegebenen Punkten, zwei Punkte, deren Abstand genau die Seitenlänge des zum Kreis flächengleichen Quadrats ist, also deren Abstand genau $\sqrt{A} = r\sqrt{\pi}$ ist.

(2) *Verdoppelung des Würfels.* Gegeben sind zwei verschiedene Punkte in der Ebene. Sei d ihr Abstand und $V = d^3$ das Volumen des Würfels mit Seitenlänge d. Man konstruiere, ausgehend von den beiden gegebenen Punkten, zwei Punkte, deren Abstand genau die Seitenlänge des Würfels ist, der das doppelte Volumen hat, also deren Abstand gleich $d\sqrt[3]{2}$ ist.

(3) *Konstruktion des regelmäßigen n-Ecks.* Sei $n \in \mathbb{N}$, $n \geq 3$. Gegeben sind zwei verschiedene Punkte $P_0 \neq P_1$ in der Ebene. Sei K der Kreis mit Mittelpunkt P_0, deren Radius der Abstand zwischen P_1 und P_0 ist. Man konstruiere ausgehend von P_0 und P_1 mit Zirkel und Lineal n Punkte auf der Kreislinie K, die die Eckpunkte eines regelmäßigen n-Ecks sind, die also den Kreis in n gleiche Abschnitte unterteilen.

> Der Tag war der 29. März 1796, und der Zufall hatte gar keinen Anteil daran. [...] Durch angestrengtes Nachdenken über den Zusammenhang aller Wurzeln untereinander nach arithmetischen Gründen glückte es mir, bei einem Ferienaufenthalt in Braunschweig am Morgen des gedachten Tages (ehe ich aus dem Bette aufgestanden war) diesen Zusammenhang auf das klarste anzuschauen, so daß ich die spezielle Anwendung auf das 17-Eck und die numerische Bestätigung auf der Stelle machen konnte.
>
> aus einem Brief von Gauß an C. L. Gerling, 1819

Bemerkung 4.35. Die Relevanz dieser Fragestellung in der Algebra-Vorlesung ist natürlich nicht eine praktische Anwendung – niemand konstruiert »per Hand« mit Zirkel und Lineal ein regelmäßiges 17-Eck. Noch weniger anwendungsrelevant ist die Tatsache, dass man beispielsweise ein regelmäßiges 7-Eck *nicht* mit Zirkel und Lineal konstruieren kann.

Dennoch ist das Thema Standardstoff der Algebra-Vorlesung. Die Gründe, warum ich dem folge, sind diese:

- Insbesondere die Ergebnisse, dass gewisse Konstruktionsprobleme unlösbar sind, sind faszinierende Beispiele »mathematischer Kreativität«. Zu zeigen, dass man beispielsweise ein regelmäßiges 17-Eck konstruieren kann, ist vielleicht kompliziert, es ist aber klar, was am Ende des Beweises stehen wird: Eine Abfolge von einzelnen Konstruktionsschritten der oben beschriebenen Art, durch die man dann die gewünschte Konstruktion durchführen kann. Aber wie würde man zeigen, dass eine Konstruktionsaufgabe *nicht* lösbar ist?
- Es zeigt sich hier eine verblüffende Verbindung zwischen Algebra und Geometrie. Punkte in der Ebene durch ihre Koordinaten zu beschreiben und damit »zu rechnen« (sagen wir im Sinne der Linearen Algebra) ist uns vertraut. Um Konstruierbarkeit zu verstehen, ist es aber nötig, weitere Methoden hinzuzunehmen. Es ist nützlich, die Ebene als die *komplexe Zahlenebene* zu betrachten, also mit dem Körper $\mathbb{C}$ zu identifizieren. Wie wir sehen werden, bildet die Gesamtheit aller ausgehend von 0 und 1 konstruierbaren Punkte einen *Teilkörper* $\mathbb{K}$ von $\mathbb{C}$, auf den man die Theorie der Körpererweiterungen anwenden kann. Genauer handelt es sich bei $\mathbb{K}$ um eine algebraische Erweiterung von $\mathbb{Q}$. Eine über $\mathbb{Q}$ transzendente Zahl kann also nicht konstruierbar (beginnend mit 0 und 1) sein.
- Das Problem ist historisch bedeutsam für Entwicklung der Mathematik und illustriert auch, dass auch nach langer Zeit ohne nennenswerten Fortschritt Lösungen für mathematische Probleme gefunden werden können, die auf neuen Einsichten beruhen (die sich oft in einer Art und Weise ergeben haben, die durch ganz andere Fragen motiviert war).

◊

Nach dieser Vorbemerkung kommen wir zur formalen Definition. In allen drei oben genannten Problemen geht man von zwei gegebenen Punkten aus, und man überlegt sich leicht, dass es keine Rolle spielt, welche Punkte in der Ebene das sind. Wir können also ohne Einschränkung mit 0 und 1 beginnen.

Definition 4.36. (1) Sei M eine Teilmenge von $\mathbb{C}$. Wir bezeichnen mit M' dann die Menge aller komplexen Zahlen, die im folgenden Sinne in (höchstens) einem Schritt aus M mit Zirkel und Lineal konstruiert werden können, das heißt M' besteht aus

- allen Elementen von M,
- allen Schnittpunkten von zwei verschiedenen Geraden, die jeweils durch zwei verschiedene Punkte auf M gehen,
- allen Schnittpunkten einer Gerade und eines Kreises, wobei die Gerade durch zwei verschiedene Punkte von M verläuft und der Kreis als Mittelpunkt einen Punkte aus M und als Radius den Abstand zweier Punkte aus M hat und
- allen Schnittpunkten von zwei verschiedenen Kreisen, deren Mittelpunkte Punkte aus M und deren Radien Abstände zweier Punkte aus M sind.

(2) Sei nun M eine Teilmenge von $\mathbb{C}$ mit $0, 1 \in M$. Sei $K_0 = M$ und für $n \in \mathbb{N}_{>0}$ sei $K_n = K'_{n-1}$ (im Sinne von Teil (1)). Dann heißt

$$\mathbb{K}(M) := \bigcup_{n\in\mathbb{N}} K_n$$

die Menge der (ausgehend von M mit Zirkel und Lineal) *konstruierbaren* Zahlen.

(3) Im Fall $M = \{0, 1\}$ schreiben wir $\mathbb{K}$ statt $\mathbb{K}(\{0, 1\})$ und nennen $\mathbb{K}$ die Menge der mit Zirkel und Lineal konstruierbaren Zahlen.

⊣

Notationskonflikt: Man beachte, dass die Notation $\mathbb{K}(M)$ nicht den über $\mathbb{K}$ von M erzeugten Körper bezeichnet!

Mit anderen Worten ist $\mathbb{K}(M) \subseteq \mathbb{C}$ die kleinste Teilmenge von $\mathbb{C}$, die die folgenden Eigenschaften hat:

(a) $M \subseteq \mathbb{K}(M)$,

(b) für je zwei unterschiedliche Geraden, die jeweils durch (mindestens) zwei verschiedene Punkte von $\mathbb{K}(M)$ gehen, liegt auch deren Schnittpunkt in $\mathbb{K}(M)$,

(c) für jede Gerade, die durch (mindestens) zwei Punkte von $\mathbb{K}(M)$ geht, und jeden Kreis, dessen Mittelpunkt in $\mathbb{K}(M)$ liegt, und so dass der Radius gleich dem Abstand zweier Punkte in $\mathbb{K}(M)$ ist, liegen auch die Schnittpunkte der Geraden und des Kreises in $\mathbb{K}(M)$,

(d) für je zwei unterschiedliche Kreise, deren Mittelpunkte in $\mathbb{K}(M)$ liegen, und so dass die Radien jeweils gleich dem Abstand zweier Punkte in $\mathbb{K}(M)$ sind, liegen auch die Schnittpunkte der Kreise in $\mathbb{K}(M)$.

ERGÄNZUNG 4.37. Man kann zeigen, dass man dieselbe Menge konstruierbarer Zahlen erhält, wenn man als Kreise in den Konstruktionsschritten nur solche Kreise erlaubt, deren Mittelpunkt bereits konstruiert ist und so dass ein bereits konstruierter Punkt auf der Kreislinie liegt. Man braucht also nicht zwingend die Möglichkeit, die wir in unserer Definition vorgesehen haben, den Zirkel auf den Abstand zweier Punkte »einzustellen« und dann einen dritten Punkt als Mittelpunkt zu nehmen. Stattdessen könnte man mit einem kollabierenden Zirkel[4] arbeiten, der direkt »zusammenklappt«, wenn man ihn vom Zeichenblatt hochhebt. □ Ergänzung 4.37

Die Geraden und Kreise, die bei diesen Konstruktionsschritten auftreten, nennen wir auch *konstruierbare* Geraden bzw. Kreise. Sind $A \neq B$ Punkte in der Ebene und $r \in \mathbb{R}_{>0}$, so sei $d(A, B)$ ihr Abstand, AB die Strecke zwischen A und B, $g(A, B)$ die Gerade durch A und B und $K(A, r)$ der Kreis mit Mittelpunkt A und Radius r.

Einfache Beispiele für Konstruktionen mit Zirkel und Lineal sind:

[4] https://de.wikipedia.org/wiki/Kollabierender_Zirkel

- Konstruiere die Mittelsenkrechte einer Strecke und damit den Mittelpunkt der Strecke zwischen zwei Punkten $A \neq B$.

  ($K(A, d(A,B))$ und $K(B, d(A,B))$ schneiden sich in zwei Punkten C, D. Dann ist $g(C,D)$ die Mittelsenkrechte der Strecke AB und der Schnittpunkt von $g(A,B)$ und $g(C,D)$ der Mittelpunkt dieser Strecke.)
- Konstruiere die Senkrechte zu einer bereits konstruierten Gerade g durch einen Punkt P, der nicht auf dieser Geraden liegt.

  (Weil g schon konstruiert ist, gibt es einen konstruierten Punkt Q, der auf g liegt. Seien Q, Q' die Schnittpunkte von $K(P, d(P,Q))$ mit g und R der Mittelpunkt der Strecke QQ' (bzw. $R = Q$ in dem Spezialfall, dass $Q' = Q$, also Q der einzige Schnittpunkt von $K(P, d(P,Q))$ mit g ist). Dann ist $g(P,R)$ die gesuchte Gerade.)
- Konstruiere die Parallele zu einer bereits konstruierten Gerade g durch einen bereits konstruierten Punkt P.

  (Konstruiere zuerst wie oben die Senkrechte h auf g durch P. Sei R ihr Schnittpunkt mit g. Konstruiere dann eine zu h parallele Gerade h' als Mittelsenkrechte zwischen zwei anderen Punkten auf g. Sei R' der Schnittpunkt von g und h' und sei P' der Schnittpunkt von $K(R', d(R,P))$ mit h', der auf derselben Seite von g liegt wie P. Die Gerade, die P und P' verbindet, ist die gesuchte Parallele zu g.)
- Konstruiere zu einem bereits konstruierten Punkt P und einer Gerade g den Punkt P', der aus P durch Spiegelung an g entsteht.

  (Der Punkt P' ist der Schnittpunkt der Senkrechten h auf g durch P und des Kreises mit Mittelpunkt gleich dem Schnittpunkt R von h und g und Radius $d(P,R)$.)

LEMMA 4.38. *Sei $M \subseteq \mathbb{C}$ eine Teilmenge, die 0 und 1 enthält. Für $\alpha \in \mathbb{C}$ sind äquivalent:*

(i) $\alpha \in \mathbb{K}(M)$,

(ii) $\overline{\alpha} \in \mathbb{K}(M)$,

(iii) *Real- und Imaginärteil von α liegen in $\mathbb{K}(M)$.*

BEWEIS. Sei $\alpha \in \mathbb{K}(M)$. Ist $\alpha \in \mathbb{R}$, so ist für die Äquivalenz von (i) und (ii) nichts zu zeigen. Andernfalls können wir $\overline{\alpha}$ aus α durch Spiegelung an der Gerade $\mathbb{R} = g(0,1)$ konstruieren.

Ist $\alpha \in \mathbb{K}(M)$, so lassen sich Real- und Imaginärteil konstruieren, wenn man die Konstruktion der Senkrechten zur reellen bzw. imaginären Achse durch α benutzt. Sind andererseits $a, b \in \mathbb{R}$ konstruierbar, so ist ib einer der Schnittpunkte von $K(0, |b|)$ mit der imaginären Achse $g(0, i)$ (der Mittelsenkrechten der Strecke zwischen 1 und -1). Dann können wir die Parallele zur reellen Achse durch ib und die Parallele zur imaginären Achse durch a konstruieren. Ihr Schnittpunkt ist $a + ib$. □

SATZ 4.39. *Sei $M \subseteq \mathbb{C}$ eine Teilmenge, die 0 und 1 enthält.*

(1) *Die Menge $\mathbb{K}(M)$ ist ein Teilkörper des Körpers der komplexen Zahlen.*

(2) *Für alle $\alpha \in \mathbb{K}(M)$ gilt $\pm\sqrt{\alpha} \in \mathbb{K}(M)$.*

BEWEIS. Zu (1). Offenbar gilt $0, 1 \in \mathbb{K}(M)$. Es ist also zu zeigen, dass für Elemente $a, b \in \mathbb{K}(M)$ auch die komplexen Zahlen

$$a + b, \quad -a, \quad ab, \quad a^{-1} \text{ (falls } a \neq 0)$$

in $\mathbb{K}(M)$ liegen. Wir arbeiten das nacheinander ab.

Summe: $a + b \in \mathbb{K}(M)$. Seien zunächst a und b linear unabhängig über $\mathbb{R}$ (also nicht auf derselben Ursprungsgeraden). Dann ist $a + b$ einer der Schnittpunkte von $K(a, d(0,b))$ und $K(b, d(0,a))$.

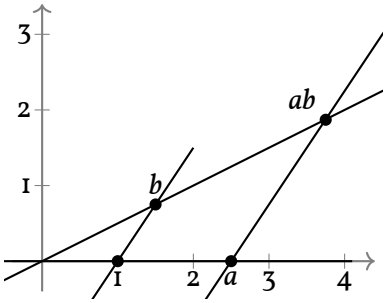
Sind $a \neq 0$ und b linear abhängig über $\mathbb{R}$, dann ist $a + b$ einer der Schnittpunkte von $g(0,a)$ mit $K(b, d(0,a))$.

Negatives: $-a \in \mathbb{K}(M)$. Für $a \neq 0$ ist $-a$ der zweite Schnittpunkt (neben a selbst) von $g(0,a)$ und $K(0,d(0,a))$.

Produkt: $ab \in \mathbb{K}(M)$. Vorbemerkung: Für $a \in \mathbb{K}(M)$ gilt $|a| \in \mathbb{K}(M)$. (Einer der Schnittpunkte von $K(0,d(0,a))$ und $g(0,1) = \mathbb{R}$.) Wir beweisen als nächstes die

Behauptung. Für $a \in \mathbb{K}(M) \cap \mathbb{R}_{>0}$, $b \in \mathbb{K}(M)$ gilt $ab \in \mathbb{K}(M)$ und $a^{-1} \in \mathbb{K}(M)$.

Begründung. Sei g die Gerade $g(0,b)$ und h irgendeine andere bereits konstruierte Ursprungsgerade. (Es ist leicht zu sehen, dass es eine solche gibt.) Sei P einer der Schnittpunkte von h mit dem Einheitskreis $K(0,1)$ und Q der Schnittpunkt von h mit dem Kreis $K(0,d(0,a))$, der auf h auf derselben Seite des Ursprungs liegt, wie P. Sei l die Parallele zu $g(b,P)$ durch Q. Dann ist nach dem ersten Strahlensatz[5] ab der Schnittpunkt von g mit l.



Für die Konstruktion von a^{-1} können wir ebenfalls den Strahlensatz anwenden. Sei $g = g(0,1) = \mathbb{R}$ die reelle Achse, sei h eine andere Ursprungsgerade, sei P einer der Schnittpunkte von $K(0,1)$ mit h und Q der Schnittpunkt von h mit dem Kreis $K(0,d(0,a))$, der auf h auf derselben Seite des Ursprungs liegt wie P. Dann ist a^{-1} nach dem ersten Strahlensatz der Schnittpunkt der Parallelen zu $g(Q,1)$ durch P mit g.

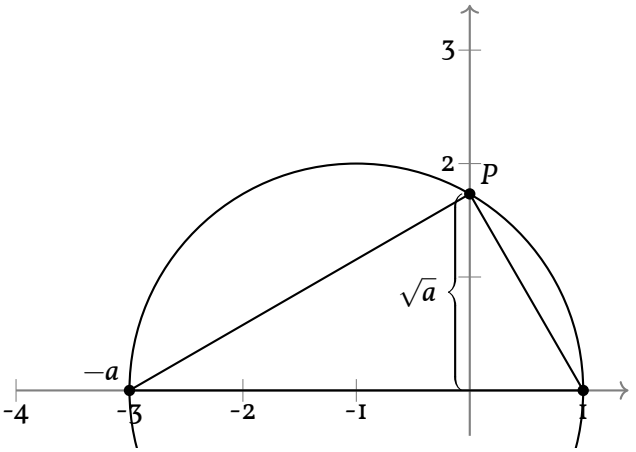
Für den allgemeinen Fall genügt es angesichts der Vorbemerkung und der soeben bewiesenen Behauptung, den Fall $|a| = |b| = 1$ zu betrachten. In diesem Fall liegen a, b und $a+b$ auf dem Einheitskreis und man kann $a+b$ aus a und b durch »Winkeladdition« konstruieren, was einfach ist. Alternativ kann man Real- und Imaginärteil des Produkts als Produkte/Summen/Differenzen in Termen der Real- und Imaginärteile der Faktoren ausdrücken.

Multiplikatives Inverses: $a^{-1} \in \mathbb{K}(M)$. Nach obigem ist ohne Einschränkung $|a| = 1$, also $a^{-1} = \bar{a}$, und die Konstruierbarkeit von $\bar{a}$ haben wir bereits gezeigt.

Zu (2). Zur Konstruktion der Quadratwurzel einer Zahl $a \in \mathbb{K}(M)$ können wir wieder die Fälle $|a| = 1$ und $a \in \mathbb{R}_{>0}$ separat behandeln. Für den ersten Fall genügt es zu bemerken, dass sich die Winkelhalbierende des Winkels zwischen der reellen Achse und der Ursprungsgerade durch a konstruieren lässt, was nicht schwierig ist.

Sei nun $a \in \mathbb{K}(M) \cap \mathbb{R}_{>0}$. Sei $M = \frac{1-a}{2}$ der Mittelpunkt der Strecke zwischen $-a$ und 1 und sei $K = K(M, \frac{a+1}{2})$ der Kreis um M, auf dem $-a$ und 1 liegen. Sei P ein Schnittpunkt von K mit der imaginären Achse $g(0,i)$. Nach dem Satz des Thales[6] ist das Dreieck mit den Eckpunkten $-a$, 1 und P rechtwinklig (mit dem rechten Winkel bei P). Nach dem Höhensatz für rechtwinklige Dreiecke[7] ist $d(0,P) = \sqrt{a}$, also ist $\sqrt{a}$ als einer der Schnittpunkte von $K(0,d(0,P))$ mit $\mathbb{R}$ in $\mathbb{K}(M)$.

[5] https://de.wikipedia.org/wiki/Strahlensatz
[6] https://de.wikipedia.org/wiki/Satz_des_Thales
[7] https://de.wikipedia.org/wiki/Höhensatz



□

Für den Fall $M = \{0, 1\}$ erhalten wir also:

KOROLLAR 4.40. (1) *Die Menge $\mathbb{K}$ ist ein Teilkörper des Körpers der komplexen Zahlen.*
(2) *Für alle $\alpha \in \mathbb{K}$ gilt $\pm\sqrt{\alpha} \in \mathbb{K}$.*

Um die Elemente von $\mathbb{K}$ zu charakterisieren, ist entscheidend, dass sich Schnittpunkte von Geraden und Kreisen durch das Lösen linearer oder quadratischer Gleichungen bestimmen lassen. Genauer gilt das folgende Lemma.

LEMMA 4.41. *Sei $K \subset \mathbb{C}$ ein Teilkörper, der unter der komplexen Konjugation auf sich selbst abgebildet wird und die Zahl i enthält. Sei $x \in \mathbb{C}$ eine ausgehend von K in einem Schritt konstruierbare komplexe Zahl (also $x \in K'$ mit der Schreibweise von Definition 4.36).*

Dann existiert eine Erweiterung L/K vom Grad ≤ 2 mit $x \in L$.

BEWEIS. Weil K unter der Konjugation auf sich selbst abgebildet wird und i enthält, sind mit jedem $\alpha \in K$ auch der Realteil $\frac{1}{2}(\alpha + \overline{\alpha})$ und der Imaginärteil $\frac{1}{2i}(\alpha - \overline{\alpha})$ Elemente von K. Außerdem ist auch $|\alpha|^2 = \alpha\overline{\alpha} \in K$.

Wenn x der Schnittpunkt von zwei Geraden ist, die jeweils durch zwei Punkte aus M verlaufen, dann ist $x \in \mathbb{C} = \mathbb{R}^2$ die eindeutig bestimmte Lösung eines linearen Gleichungssystems, dessen Koeffizienten durch Real- und Imaginärteil der Punkte auf diesen Geraden ausgedrückt werden können, liegt also sogar in K.

Ist x der Schnittpunkt einer konstruierbaren Geraden und eines konstruierbaren Kreises oder der Schnittpunkt zweier konstruierbarer Kreise, dann ist $x \in \mathbb{C} = \mathbb{R}^2$ eine der Lösungen eines Gleichungssystems in zwei Unbestimmten, das aus einer linearen und einer quadratischen Gleichung oder aus zwei quadratischen Gleichungen besteht. Die Koeffizienten dieser Gleichungen liegen dabei in K. Zum Beispiel ist der Kreis um $M = M_1 + iM_2$ mit Radius $r \in \mathbb{R}_{>0}$ (mit $r^2 \in K$) gegeben durch die Gleichung

$$(x_1 - M_1)^2 + (x_2 - M_2)^2 = r^2$$

mit Koeffizienten in K. In beiden Fällen sieht man (durch Einsetzen bzw. indem man die beiden Kreisgleichungen voneinander abzieht), dass sich Real- und Imaginärteil der Schnittpunkte durch Lösen einer quadratischen Gleichung »finden lassen«, genauer, dass sie in einem Erweiterungskörper L von K mit $[L : K] \leq 2$ liegen, und dann liegt auch x in L. □

SATZ 4.42. *Sei $M \subseteq \mathbb{C}$ eine Teilmenge, die 0 und 1 enthält, und sei $K_0 = \mathbb{Q}(M \cup \overline{M})$. Für $\alpha \in \mathbb{C}$ sind äquivalent:*

(i) *Die Zahl α ist ausgehend von M in endlich vielen Schritten konstruierbar mit Zirkel und Lineal.*

(ii) *Es gibt eine endliche Kette*

$$\mathbb{Q}(M \cup \overline{M}) = K_0 \subset K_1 \subset \cdots \subset K_r$$

von Körpererweiterungen, so dass $[K_i : K_{i-1}] = 2$ für alle $i = 1, \ldots, r$ gilt und $\alpha \in K_r$ ist.

BEWEIS. (i) $\Rightarrow$ (ii). Wir zeigen die folgende Behauptung, aus der (ii) dann durch Induktion folgt. (Weil die Erweiterung $K_0(i)/K_0$ Grad ≤ 2 hat, können wir $K_1 = K_0(i)$ setzen und von dort die Induktion beginnen.)

Behauptung. Sei $K \subseteq \mathbb{C}$ ein Teilkörper, der unter komplexer Konjugation stabil ist und die Zahl i enthält. Sei $x \in K'$, also x in einem einzigen Schritt aus K konstruierbar. Dann existiert eine Kette $K \subseteq L_1 \subseteq L_2$ von Erweiterungen vom Grad ≤ 2, so dass $x \in L_2$ und $\overline{L_2} = L_2$ gilt.

Begründung. Sei $L_1 = K(x)$. Dann gilt nach dem vorherigen Lemma $[L_1 : K] \leq 2$. Wir setzen nun $L_2 = L_1(\overline{x})$. Die Erweiterung $K(\overline{x})$ hat über K denselben Grad wie $K(x)$, denn aus dem Minimalpolynom von x über K erhalten wir die komplexe Konjugation der Koeffizienten das Minimalpolynom von $\overline{x}$ über K (denn dieses Polynom hat ja wieder Koeffizienten in K). Insbesondere gilt $[L_2 : L_1] \leq [K(\overline{x}) : K] \leq 2$. Außerdem ist $\overline{L_2} = \overline{K(x, \overline{x})} = L_2$.

(ii) $\Rightarrow$ (i). Weil alle Elemente von $\mathbb{Q}$ konstruierbar sind, genügt es zu zeigen, dass jede komplexe Zahl x, die eine Gleichung der Form $x^2 + px + q = 0$ mit konstruierbaren Zahlen p, q erfüllt, selbst konstruierbar ist. Aber das folgt angesichts von Satz 4.39 aus der Lösungsformel für diese quadratische Gleichung. □

Im Fall $M = \{0, 1\}$, der uns am meisten interessiert, erhalten wir also die folgende Beschreibung.

KOROLLAR 4.43. *Für $\alpha \in \mathbb{C}$ sind äquivalent:*

(i) *Es gilt $\alpha \in \mathbb{K}$, d.h. α ist ausgehend von 0 und 1 konstruierbar mit Zirkel und Lineal.*

(ii) *Es gibt eine endliche Kette*

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_r$$

von Körpererweiterungen, so dass $[K_i : K_{i-1}] = 2$ für alle $i = 1, \ldots, r$ gilt und $\alpha \in K_r$ ist.

Insbesondere erhalten wir direkt das folgende Korollar:

KOROLLAR 4.44. *Die Erweiterung $\mathbb{K}/\mathbb{Q}$ ist algebraisch. Ist $\alpha \in \mathbb{K}$, so ist $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ eine Potenz von 2.*

Die Umkehrung ist nicht richtig und wir werden den Sachverhalt zum Ende der Vorlesung noch genauer klären, siehe Abschnitt 6.6.

KOROLLAR 4.45. *Die »Verdoppelung des Würfels« mit Zirkel und Lineal ist unmöglich.*

BEWEIS. Ausgehend vom Würfel mit der Kantenlänge 1 ist als Kantenlänge des Würfels mit dem doppeltem Volumen, also mit Volumen 2 die Zahl $\sqrt[3]{2}$ zu konstruieren. Weil $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$ gilt, ist aber $\sqrt[3]{2}$ nicht in einem Erweiterungskörper von $\mathbb{Q}$ enthalten, dessen Grad eine Potenz von 2 ist, liegt also nicht in $\mathbb{K}$. □

”

Die Bewohner der Insel Delos befragten ein Orakel, um von Plagen befreit zu werden. Sie erhielten als Antwort, dass Sie im Apollo-Tempel einen neuen Altar bauen sollten, der wie der bisherige würfelförmig sei, aber genau das doppelte Volumen habe.

Theon von Smyrna in seiner Schrift *Das an mathematischem Wissen für die Lektüre Platons Nützliche*, ca. 100 n. Chr.

Diese Geschichte findet man auch bei Eratosthenes und bei Plutarch. Das Problem der Würfelverdoppelung mit Zirkel und Lineal heißt auch *Delisches Problem*.

BEISPIEL 4.46. Die folgenden Beispiele waren schon in der Antike bekannt. Teil (1) ist einfach, Teil (2) schon etwas kniffliger (Übung...).

(1) Das regelmäßige Sechseck (mit dem Einheitskreis als Umkreis) ist konstruierbar mit Zirkel und Lineal.

(2) Das regelmäßige Fünfeck (mit dem Einheitskreis als Umkreis) ist konstruierbar mit Zirkel und Lineal.

◊

4.5.1. Die Quadratur des Kreises. Dass die Quadratur des Kreises nicht möglich ist, beruht auf dem folgenden Satz, den Ferdinand Lindemann 1882 bewies.

THEOREM 4.47 (Satz von Lindemann). *Die Kreiszahl $\pi \in \mathbb{C}$ ist transzendent über $\mathbb{Q}$.*

Siehe zum Beispiel [**Lo**] Kapitel 17, [**Po**] Anhang A, [**Bu**] Kapitel 6 oder [**La**], Appendix 1.

Ein Klassiker in diesem Bereich ist das Buch *Transcendental Number Theory* von A. Baker (Cambridge University Press).

KOROLLAR 4.48. *Die »Quadratur des Kreises« mit Zirkel und Lineal ist nicht möglich.*

BEWEIS. Ein zum Einheitskreis flächengleiches Quadrat hat Kantenlänge $\sqrt{\pi}$. Weil π über $\mathbb{Q}$ transzendent ist, gilt das erst recht für $\sqrt{\pi}$. Die Erweiterung $\mathbb{K}/\mathbb{Q}$ ist aber algebraisch und kann daher die Zahl $\sqrt{\pi}$ nicht enthalten. □

KAPITEL 5

Galois-Theorie

Als nächstes werden wir zwei wichtige Eigenschaften von gewissen Körpererweiterungen studieren, nämlich *Normalität* und *Separabilität*. Für endliche Erweiterungen, die sowohl normal als auch separabel sind, werden wir mit dem Hauptsatz der Galois-Theorie (Theorem 5.49) ein Ergebnis beweisen, dass sehr genaue Auskunft über die Zwischenkörper der Erweiterung in Termen der Galois-Gruppe, also der Automorphismengruppe der gegebenen Körpererweiterung (siehe Bemerkung 2.3, Satz 5.44) liefert.

5.1. Normale Körpererweiterungen

DEFINITION 5.1. Sei K ein Körper und sei $(f_i)_{i\in I}$ eine Familie von Polynomen in $K[X]$.

Ein Erweiterungskörper L von K heißt *Zerfällungskörper* der Familie $(f_i)_i$, wenn die folgenden beiden Bedingungen erfüllt sind:

(a) Jedes f_i zerfällt über L vollständig in Linearfaktoren und

(b) die Körpererweiterung L/K wird von den Nullstellen der Polynome f_i erzeugt.

⊣

Für den Beweis der Eindeutigkeit eines Zerfällungskörpers bis auf Isomorphismus werden wir das folgende Lemma verwenden.

LEMMA 5.2. *Seien K ein Körper und seien E, E' Erweiterungskörper von K. Sei $f \in K[X]$ ein Polynom, das sowohl in E als auch in E' vollständig in Linearfaktoren zerfällt. Dann induziert jeder K-Homomorphismus $\sigma\colon E \to E'$ eine Bijektion $V(f,E) \xrightarrow{\sim} V(f,E')$ zwischen den Nullstellenmengen von f in E und in E'.*

BEWEIS. Wir schreiben $f = c(X-\alpha_1)\cdots(X-\alpha_d)$ mit $c \in K$, $\alpha_i \in E$, $d = \deg(f)$. Der Homomorphismus $\sigma\colon E \to E'$ induziert einen Ringhomomorphismus $E[X] \to E'[X]$, der dadurch gegeben ist, dass auf alle Koeffizienten eines gegebenen Polynoms in $E[X]$ der Homomorphismus σ angewendet wird. (Wir können das als Einsetzungshomomorphismus mit $X \mapsto X$ sehen, wenn wir E' mittels σ als E-Algebra betrachten.)

Unter dieser Abbildung wird f auf f abgebildet, weil $f \in K[X]$ ist und σ ein K-Homomorphismus ist. Andererseits wird das Produkt $c(X-\alpha_1)\cdots(X-\alpha_d)$, weil es sich hier um einen Ringhomomorphismus handelt, auf $c(X-\sigma(\alpha_1))\cdots(X-\sigma(\alpha_d)) \in E'[X]$ abgebildet. Das bedeutet aber genau, dass $\sigma(\alpha_1), \ldots, \sigma(\alpha_d)$ die Nullstellen von f in E' sind. Insbesondere schränkt sich σ zu einer Abbildung $V(f,E) \to V(f,E')$ ein und diese ist surjektiv. Als Einschränkung der injektiven Abbildung $\sigma\colon E \to E'$ ist sie auch injektiv. □

SATZ 5.3. *Sei K ein Körper und sei $(f_i)_{i\in I}$ eine Familie von Polynomen in $K[X]$.*

(1) *Es existiert ein Zerfällungskörper der gegebenen Familie von Polynomen.*

(2) *Sind L und L' Zerfällungskörper der Familie $(f_i)_i$, so existiert ein K-Isomorphismus $L \xrightarrow{\sim} L'$.*

BEWEIS. Zu (1). Für endlich viele Polynome haben wir das schon bewiesen (Korollar 4.24). Im allgemeinen Fall verwenden wir, dass K einen algebraischen Abschluss $\overline{K}$ besitzt (Theorem 4.31). Sei $L \subseteq \overline{K}$ dann der von den Nullstellen aller f_i erzeugte Erweiterungskörper von K. Es ist klar, dass L ein Zerfällungskörper der Familie $(f_i)_i$ ist.

Zu (2). Sei $\overline{L'}$ ein algebraischer Abschluss von L'. Weil die Erweiterung L'/K algebraisch ist, ist dann $\overline{L'}$ auch ein algebraischer Abschluss von K. Nach Satz 4.33 gibt es einen K-Homomorphismus $\sigma\colon L \to \overline{L'}$. Für jedes Polynom f_i sind nach dem vorherigen Lemma die Bilder der Nullstellen von f_i die Nullstellen von f_i in L'. Weil diese Nullstellen die Erweiterung L/K erzeugen, liegt das Bild von σ in L'. Weil L' von den Nullstellen der f_i erzeugt wird und das Bild von σ ein Teilkörper von L' ist, der alle diese Nullstellen enthält, ist $\operatorname{Im}(\sigma) = L'$. Also induziert σ einen Isomorphismus $L \to L'$. □

Man beachte, dass der Isomorphismus in Teil (2) des Satzes in aller Regel nicht eindeutig bestimmt ist. In der Tat werden wir die Gesamtheit der Isomorphismen $L \xrightarrow{\sim} L'$ in dieser Situation im folgenden noch genauer studieren, jedenfalls in der Situation, dass L/K endlich ist (Abschnitt 5.5).

Ist andererseits $(f_i)_i$ eine Familie von Polynomen über einem Körper K und M ein Erweiterungskörper von K, in dem alle f_i vollständig in Linearfaktoren zerfallen, dann gibt es genau einen Teilkörper von M, der ein Zerfällungskörper dieser Familie ist, nämlich den Teilkörper, der über K von allen Nullstellen aller f_i erzeugt wird. In dieser Situation sprechen wir auch von *dem* Zerfällungskörper der gegebenen Familie von Polynomen *in* M.

SATZ 5.4. *Sei L/K eine algebraische Körpererweiterung und $\overline{L}$ ein algebraischer Abschluss von L. Dann sind die folgenden Aussagen äquivalent.*

(i) *Es gibt eine Familie von Polynomen in $K[X]$, derart dass L ein Zerfällungskörper dieser Familie ist.*

(ii) *Für jeden K-Homomorphismus $\varphi\colon L \to \overline{L}$ gilt* $\operatorname{Im}(\varphi) \subseteq L$.

(iii) *Ist $f \in K[X]$ ein irreduzibles Polynom, das in L eine Nullstelle besitzt, so zerfällt f über L vollständig in Linearfaktoren.*

Die Erweiterung L/K heißt normal, *wenn diese Bedingungen erfüllt sind.*

BEWEIS. (i) ⇒ (ii). Sei $(f_i)_i$ eine Familie von Polynomen, für die L ein Zerfällungskörper ist, und sei σ wie in (ii). Nach Lemma 5.2 liegen die Bilder aller Nullstellen der f_i unter σ in L. Weil diese Nullstellen L über K erzeugen, gilt $\operatorname{Im}(\varphi) \subseteq L$. (Genauer gilt sogar $\operatorname{Im}(\varphi) = L$, denn alle Nullstellen der f_i in $\overline{L}$ liegen ja in $\operatorname{Im}(\varphi)$.)

(ii) ⇒ (iii). Sei $f \in K[X]$ irreduzibel. Sind $\alpha \in L$ und $\beta \in \overline{L}$ Nullstellen von f, dann gibt es nach Satz 4.25 (genau) einen K-Homomorphismus $K[\alpha] \to \overline{L}$ mit $\alpha \mapsto \beta$. Diesen können wir nach Satz 4.33 zu einem K-Homomorphismus $\varphi\colon L \to \overline{L}$ fortsetzen, der nach (ii) Bild in L hat. Da $\beta = \sigma(\alpha)$ im Bild liegt, folgt $\beta \in L$.

(iii) ⇒ (i). Unter Voraussetzung (iii) ist L der Zerfällungskörper aller irreduziblen Polynome auf $K[X]$, die in L eine Nullstelle besitzen: Nach Voraussetzung zerfallen alle diese Polynome über L vollständig in Linearfaktoren. Dass ihre Nullstellen L erzeugen ist klar, denn *jedes* Element von L ist Nullstelle eines irreduziblen Polynoms über K, nämlich seines Minimalpolynoms. □

BEISPIEL 5.5. (1) Quadratische Erweiterungen (also Erweiterungen vom Grad 2) sind normal. (Warum? – Eine beliebte Prüfungsfrage…)

(2) Die Erweiterung $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist nicht normal. Die Nullstellen des irreduziblen Polynoms $X^3 - 2$ in $\mathbb{C}$ sind $\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}$, wobei $\zeta = e^{\frac{2\pi i}{3}}$ ist, also $\zeta^3 = 1$. Weil $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ gilt, kann der Körper $\mathbb{Q}(\sqrt[3]{2})$ die beiden nicht-reellen Nullstellen nicht enthalten.

(3) Ist $\overline{K}$ ein algebraischer Abschluss von K, so ist die Erweiterung $\overline{K}/K$ normal.

$\Diamond$

LEMMA 5.6. *Seien E/K und L/E Körpererweiterungen. Ist die Erweiterung L/K normal, so ist auch die Erweiterung L/E normal.*

BEWEIS. Ist L ein Zerfällungskörper einer Familie von Polynomen mit Koeffizienten in K, so ist L auch Zerfällungskörper *derselben* Familie von Polynomen, nun aufgefasst als Polynome mit Koeffizienten in E. □

Allerdings – und das ist im Grunde die interessantere Tatsache – ist in der Situation des Lemmas die Erweiterung E/K nicht unbedingt normal. Und wenn E/K und L/E normale Körpererweiterungen sind, ist die Erweiterung L/K nicht unbedingt normal. (Suchen Sie sich Beispiele für diese beiden Situationen!)

SATZ 5.7. *Sei L/K eine algebraische Körpererweiterung.*

(1) *Es existiert ein Erweiterungskörper L' von L, so dass die Erweiterung L'/K normal ist, und so dass kein echter Teilkörper von L', der L enthält, normal über K ist. Der Körper L' ist bis auf K-Isomorphismus eindeutig bestimmt.*

(2) *Ist die Erweiterung L/K endlich, so ist auch L'/K endlich.*

(3) *Ist M/K eine normale Erweiterung, so dass L in M enthalten ist, so ist der von allen $\sigma(L)$, $\sigma \in \mathrm{Hom}_K(L, M)$, über K erzeugte Teilkörper $L' \subseteq M$ der eindeutig bestimmte Zwischenkörper von M/K, der die Eigenschaft in Teil (1) hat.*

Wir nennen L' eine normale Hülle *der Erweiterung L/K (bzw. in der Situation von Teil (3)* die normale Hülle von L/K in M*). Manchmal spricht man auch vom* normalen Abschluss.

BEWEIS. Wir beginnen mit Teil (3) und beweisen zunächst:

Behauptung. Der in (3) beschriebene Körper L' ist der Teilkörper L'' von M, der von den Nullstellen aller Minimalpolynome von Elementen von L (über K) erzeugt wird.

Begründung. Weil alle Minimalpolynome von Elementen von L über K irreduzibel sind und eine Nullstelle in $L \subseteq M$ besitzen, zerfallen sie über dem normalen Erweiterungskörper M von K vollständig in Linearfaktoren.

Die Inklusion $L' \subseteq L''$ gilt, weil jeder K-Homomorphismus σ Nullstellen von Polynomen in $K[X]$ auf Nullstellen desselben Polynoms abbildet. Die Inklusion $L'' \subseteq L'$ folgt, weil es zu jeder Nullstelle $\beta \in M$ von $\mathrm{minpol}_{\alpha,K}$, $\alpha \in L$, einen K-Homomorphismus $L \to M$ mit $\sigma(\alpha) = \beta$ gibt (Satz 4.25, Satz 4.33, Satz 5.4).

Damit ist klar, dass L' über K normal ist. Weil die Minimalpolynome aller Elemente von L in jedem Erweiterungskörper von L, der über K normal ist, zerfallen müssen, kann es keinen kleineren Erweiterungskörper von L mit dieser Eigenschaft geben als L'.

Zu (1). Nachdem wir Teil (3) bereits bewiesen haben, ist nur noch die Eindeutigkeit zu zeigen. Jedes L' wie in (1) ist der Zerfällungskörper aller Minimalpolynome (über K) von Elementen von L. Daher folgt die Eindeutigkeitsaussage aus der entsprechenden Eindeutigkeitsaussage für den Zerfällungskörper einer Familie von Polynomen (Satz 5.3 (2)).

Zu (2). Wird L über K erzeugt von $\alpha_1, \ldots, \alpha_n$, so ist der Teilkörper eines algebraischen Abschlusses von L, der von allen Nullstellen der Minimalpolynome der α_i erzeugt wird, als Zerfällungskörper einer Familie von Polynomen normal über K und daher eine normale Hülle von L/K. Da es sich hier nur um endlich viele Polynome handelt, ist dieser Erweiterungskörper endlich erzeugt über K, also auch endlich, weil die Erweiterung algebraisch ist. □

In der *Behauptung* im Beweis könnte man äquivalent L'' als den Zerfällungskörper aller Minimalpolynome der Elemente irgendeines Erzeugendensystems von L als Erweiterungskörper von K definieren. Noch einmal konkret ausgeschrieben bedeutet das: Die normale Hülle von $L = K(\alpha_i,\ i \in I)$ in einem algebraischen Abschluss $\overline{L}$ über einem Körper K ist der Zerfällungskörper aller Polynome $\operatorname{minpol}_{\alpha_i,K}$, $i \in I$.

Frage/Übung (im Moment noch schwierig): Gibt es eine normale Erweiterung $K/\mathbb{Q}$ von Grad 3?

5.2. Separable Körpererweiterungen

Die zweite Eigenschaft (neben der Normalität), die eine Galois-Erweiterung (Satz 5.44) haben muss, ist die *Separabilität*. Wie wir sehen werden, ist diese für Körper der Charakteristik 0 immer gegeben; es handelt sich also um eine Eigenschaft, die nur in positiver Charakteristik relevant bzw. interessant ist.

DEFINITION 5.8. Sei K ein Körper und $\overline{K}$ ein algebraischer Abschluss von K. Ein Polynom $f \in K[X]$ heißt *separabel*, wenn f in $\overline{K}$ nur einfache Nullstellen hat. ⊣

Die Nullstellen eines separablen Polynoms sind also alle voneinander verschieden, oder »getrennt«, lateinisch: »separiert«. Der Begriff *separabel* (für Polynome) wird in der Literatur nicht ganz einheitlich gehandhabt; im wichtigsten Fall, dass das betrachtete Polynom irreduzibel ist, stimmen aber alle Definitionen überein. Die Eigenschaft, separabel zu sein, ist unabhängig von der Wahl eines algebraischen Abschlusses von K.

SATZ 5.9. *Sei K ein Körper und $f \in K[X]$ ein irreduzibles Polynom. Dann sind äquivalent:*

(i) *f ist separabel,*

(ii) $f' \neq 0$.

Insbesondere gilt: Über einem Körper der Charakteristik 0 ist jedes irreduzible Polynom separabel. Über einem Körper der Charakteristik $p > 0$ ist jedes irreduzible Polynom, dessen Grad nicht von p geteilt wird, separabel. (Siehe den folgenden Satz für eine genauere Beschreibung.)

BEWEIS. Das Polynom f hat genau dann eine mehrfache Nullstelle, etwa α, in einem algebraischen Abschluss $\overline{K}$ von K, wenn f und f' eine gemeinsame Nullstelle haben, oder mit anderen Worten: Wenn es einen Linearfaktor $X - \alpha$ gibt, der f und f' teilt. Das ist genau dann der Fall, wenn der größte gemeinsame Teiler von f und f' nicht-konstant ist. Diese Eigenschaft können wir aber genausogut in $K[X]$ überprüfen wie in $\overline{K}[X]$, denn der größte gemeinsame Teiler ist in beiden Ringen derselbe. Das kann man damit begründen, dass der größte gemeinsame Teiler mit dem euklidische Algorithmus (siehe Bemerkung LA2.15.43) berechnet werden kann, und diese Berechnung findet vollständig im Ring $K[X]$ statt, wenn die beiden betrachteten Polynom in $K[X]$ liegen, wie es hier der Fall ist. Weil f irreduzibel ist, folgt dann, dass sich f und der ggT von f und f' nur durch Multiplikation mit einer Konstanten in $K^\times$ unterscheiden. Andererseits gilt $\deg(f') < \deg(f)$. Weil der ggT von f und f' auch ein Teiler von f' ist, muss $f' = 0$ gelten. Ist andererseits $f' = 0$, dann ist jede Nullstelle von f eine mehrfache Nullstelle.

Wenn man vermeiden möchte, auf den euklidischen Algorithmus zurückzugreifen, den wir in der Algebra-Vorlesung nicht wiederholt haben, kann man wie folgt argumentieren: Wenn α eine gemeinsame Nullstelle von f und f' ist, dann ist $\operatorname{minpol}_{\alpha,K}$ ein gemeinsamer Teiler von f und f' in $K[X]$. Aus der Irreduzibilität von f folgt dann, dass sich f und $\operatorname{minpol}_{\alpha,K}$ höchstens um ein Skalar in $K^\times$ unterscheiden. Damit sehen wir, wie im vorherigen Argument, dass f ein Teiler von f' ist, was aus Gradgründen nur möglich ist, wenn $f' = 0$ gilt. □

Überlegen Sie sich, dass man auf die Voraussetzung, dass f irreduzibel sei, im obigen Satz nicht verzichten kann.

Ist K ein Körper der Charakteristik $p > 0$, so ist das Polynom $X^p - a$ (mit $a \in K$) nicht separabel, denn seine Ableitung verschwindet, so dass jede Nullstelle eine mehrfache Nullstelle ist. Ist c eine Nullstelle dieses Polynoms (in einem geeigneten Erweiterungskörper von K), so gilt dort $X^p - a = X^p - c^p = (X - c)^p$, also ist c eine p-fache Nullstelle von $X^p - a$. Es gibt also, wenn überhaupt eine p-te Wurzel von a existiert, *genau eine* p-te Wurzel! Entsprechend verhält es sich mit p^r-ten Wurzeln für $r > 1$, und allgemeiner haben wir den folgenden Satz.

SATZ 5.10. *Sei K ein Körper der Charakteristik $p > 0$ und sei $f \in K[X]$ irreduzibel. Sei $r \in \mathbb{N}$ maximal mit der Eigenschaft, dass f die Form $g(X^{p^r})$ für ein Polynom $g \in K[X]$ hat. Dann ist g durch f eindeutig bestimmt, separabel und irreduzibel.*

Jede Nullstelle von f hat die Vielfachheit p^r, und die Nullstellen von f (in einem algebraischen Abschluss $\overline{K}$ von K) sind gerade die p^r-ten Wurzeln der Nullstellen von g.

In der Situation des Satzes ist also f genau dann separabel, wenn $f = g$ oder äquivalent $r = 0$ gilt.

BEWEIS. Es ist klar, dass g durch die angegebene Beschreibung eindeutig bestimmt ist. Hätte g eine Zerlegung als Produkt von nicht-konstanten Polynomen, so würden wir durch Einsetzen von X^{p^r} für X eine nicht-triviale Zerlegung von f erhalten, im Widerspruch zur Irreduzibilität von f. Wegen der Maximalität von r ist nicht jede Potenz von X, die in g mit Koeffizient $\neq 0$ auftritt, durch p teilbar. Daher ist g' nicht das Nullpolynom. Weil g irreduzibel ist, ist g nach Satz 5.9 separabel.

Offenbar gilt $f(\alpha) = 0$ genau dann, wenn $g(\alpha^{p^r}) = 0$ ist. Wir schreiben $g = \gamma(X-\beta_1)\cdots(X-\beta_s)$ mit $\gamma, \beta_i \in \overline{K}$. Sei $\alpha_i \in \overline{K}$ das eindeutig bestimmte Element mit $\alpha_i^{p^r} = \beta_i$. Es folgt

$$f = \gamma \prod_i (X^{p^r} - \alpha_i^{p^r}) = \gamma \prod_i (X - \alpha_i)^{p^r}$$

und wir sehen, dass jede Nullstelle von f (in $\overline{K}$) Vielfachheit p^r hat. (Diese Aussage gilt auch, wenn diese Nullstellen von f in Teilkörpern von $\overline{K}$ betrachtet werden.) □

DEFINITION 5.11. Sei L/K eine algebraische Körpererweiterung.

(1) Ein Element $a \in L$ heißt *separabel über K*, wenn ein separables Polynom $p \in K[X] \setminus \{0\}$ existiert mit $p(a) = 0$. Es ist äquivalent zu fordern, dass das Minimalpolynom von a über K separabel sei.

(2) Ein Element $a \in L$, das nicht separabel über K ist, heißt *inseparabel*.

(3) Die Körpererweiterung L/K heißt *separabel*, wenn jedes Element von L über K separabel ist.

(4) Ist die Erweiterung L/K nicht separabel, so heißt sie *inseparabel*. Ist sogar jedes Element von L, das nicht in K liegt, inseparabel über K, dann nennt man die Erweiterung L/K *rein inseparabel*.

⊣

Aus dem oben Gesagten folgt, dass jede algebraische Erweiterung von Körpern der Charakteristik 0 separabel ist. Ist K ein Körper der Charakteristik $p > 0$ und L/K eine Erweiterung, deren Grad nicht von p geteilt wird, dann ist die Erweiterung (warum?) separabel.

BEISPIEL 5.12. Sei p eine Primzahl. Sei $K = \mathbb{F}_p(T) = \mathrm{Quot}(\mathbb{F}_p[T])$ der Körper der rationalen Funktionen in T über $\mathbb{F}_p$. Das Polynom $X^p - T$ ist irreduzibel nach dem Eisenstein-Kriterium (Satz 3.53). Sei $\sqrt[p]{T}$ die eindeutig bestimmte Nullstelle des Polynoms $X^p - T$ in einem fixierten algebraischen Abschluss von K. Dann ist $L := K[\sqrt[p]{T}]$ ein Erweiterungskörper von K (vom Grad p), derart dass die Erweiterung L/K nicht separabel ist, denn das Element $\sqrt[p]{T}$ ist nicht separabel über K. ◊

DEFINITION 5.13. Ein Körper K heißt *perfekt* (oder: *vollkommen*), wenn jede algebraische Erweiterung von K separabel ist. ⊣

Aus dem oben Gesagten folgt, dass ein irreduzibles Polynom f über einem Körper K (zum Beispiel das Minimalpolynom eines algebraischen Elements eines Erweiterungskörpers) höchstens dann nicht separabel sein kann, wenn K positive Charakteristik p hat und p den Grad von f teilt. Damit erhalten wir:

KOROLLAR 5.14. (1) *Jeder Körper der Charakteristik* 0 *ist ein perfekter Körper.*

(2) *Ist K ein Körper der Charakteristik $p > 0$ und ist L/K eine endliche Erweiterung, deren Grad nicht von p geteilt wird, dann ist die Erweiterung L/K separabel.*

In positiver Charakteristik haben wir die folgende Charakterisierung perfekter Körper. Dabei benutzen wir den Frobenius-Homomorphismus aus Beispiel 3.2.

SATZ 5.15. *Sei K ein Körper der Charakteristik $p > 0$. Dann sind äquivalent:*

(i) *Der Körper K ist perfekt.*

(ii) *Jede endliche Erweiterung von K ist separabel.*

(iii) *Der Frobenius-Homomorphismus $K \to K, x \mapsto x^p$, ist surjektiv (und folglich ein Isomorphismus).*

BEWEIS. Trivialerweise folgt (ii) aus (i). Nun gelte (ii). Um (iii) zu zeigen, betrachten wir $y \in K$. Das Polynom $X^p - y$ hat in einem endlichen Erweiterungskörper L eine Nullstelle x. Es gilt dann $\mathrm{minpol}_{x,K} \mid (X^p - y)$ und andererseits $X^p - y = X^p - x^p = (X - x)^p$. Weil die Erweiterung L/K separabel ist, hat $\mathrm{minpol}_{x,K}$ nur einfache Nullstellen. Insgesamt folgt $\mathrm{minpol}_{x,K} = X - x$, also $x \in K$. Somit liegt y im Bild des Frobenius-Homomorphismus.

Nun gelte (iii). Wir zeigen, dass jede Erweiterung L/K separabel ist. Sei $\alpha \in L$ und $f = \mathrm{minpol}_{\alpha,K}$. Seien r und g wie in Satz 5.10 definiert, also $f = g(X^{p^r})$ und g hat nur einfache Nullstellen. Wir wollen zeigen, dass $r = 0$ (also $g = f$) gilt. Wir schreiben $g = \sum_{i=0}^{n} b_i X^i$ und wählen $a_i \in K$ mit $a_i^{p^r} = b_i$. (Weil die Abbildung $x \mapsto x^p$ und damit auch die Abbildung $x \mapsto x^{p^r}$ surjektiv ist, ist das möglich.) Dann ist

$$f = \sum_{i=0}^{n} b_i X^{ip^r} = \left(\sum_{i=0}^{n} a_i X^i \right)^{p^r}.$$

Weil f irreduzibel ist, impliziert das $p^r = 1$, also $r = 0$, wie gewünscht. □

KOROLLAR 5.16. *Jeder endliche Körper ist perfekt.*

BEWEIS. Weil der Frobenius-Homomorphismus wie jeder Homomorphismus zwischen Körpern injektiv ist und ein endlicher Körper gegeben ist, ist der Frobenius-Homomorphismus auch surjektiv. Aus der Charakterisierung perfekter Körper im vorherigen Satz folgt die Behauptung. □

Wir wollen nun zeigen, dass jede Körpererweiterung L/K, die erzeugt wird durch Elemente von L, die über K separabel sind, eine separable Erweiterung ist. (Mit anderen Worten: Summen, Differenzen, Produkte und Quotienten von separablen Elementen sind wieder separabel.) Ähnlich wie beim analogen Ergebnis für den Begriff »algebraisch« (wo wir zum Beweis den *Grad* einer Körpererweiterung eingeführt haben), brauchen wir auch an dieser Stelle einen neuen Begriff, den sogenannten *Separabilitätsgrad* einer Körpererweiterung, der uns erlaubt zu messen, »wie nah« die Erweiterung an einer separablen Erweiterung ist.

DEFINITION 5.17. Sei L/K eine endliche Körpererweiterung und sei $\overline{K}$ ein algebraischer Abschluss von K. Dann heißt

$$[L : K]_s := \#\operatorname{Hom}_K(L, \overline{K}) \quad \in \mathbb{N} \cup \{\infty\}$$

der *Separabilitätsgrad* der Erweiterung L/K. ⊣

LEMMA 5.18. *Ist L/K eine einfache Erweiterung, etwa $L = K(\alpha)$, dann ist $[L : K]_s \leq [L : K]$ und Gleichheit gilt genau dann, wenn α separabel über K ist.*

BEWEIS. Nach Satz 4.25 ist $[L : K]_s$ gerade die Anzahl der Nullstellen von $\operatorname{minpol}_{\alpha,K}$. Nach Lemma 4.17 ist $\deg(\operatorname{minpol}_{\alpha,K}) = [L : K]$. Daraus folgt die Behauptung. □

Um allgemeinere Erweiterungen zu betrachten, beweisen wir zuerst, dass sich der Separabilitätsgrad, ebenso wie der Grad, multiplikativ in einem Turm von Erweiterungen verhält.

LEMMA 5.19. *Seien E/K und L/E endliche Körpererweiterungen. Dann gilt*

$$[L : K]_s = [L : E]_s\,[E : K]_s.$$

(Für den Fall, dass nicht alle Separabilitätsgrade hier endlich sind, ist die Aussage so zu interpretieren, dass die linke Seite genau dann unendlich ist, wenn (mindestens) einer der Faktoren auf der rechten Seite unendlich ist.)

BEWEIS. Sei $\overline{K}$ ein algebraischer Abschluss von K. Durch Einschränkung von K-Homomorphismen erhalten wir eine Abbildung

$$R\colon \operatorname{Hom}_K(L, \overline{K}) \to \operatorname{Hom}_K(E, \overline{K}), \quad \sigma \mapsto \sigma_{|E}.$$

Wir untersuchen die Fasern dieser Abbildung. Für $\tau \in \operatorname{Hom}_K(E, \overline{K})$ lässt sich τ nach Satz 4.33 zu einem K-Homomorphismus $L \to \overline{K}$ fortsetzen, also ist die Faser $R^{-1}(\tau)$ nicht-leer. Ist $\sigma_0 \in R^{-1}(\tau)$ ein fixiertes Element, das wir fortsetzen zu $\tilde{\sigma}_0\colon \overline{K} \to \overline{K}$ (wieder mit Satz 4.33, dessen zweiter Teil zeigt, dass $\tilde{sigma}_0$ ein Isomorphismus ist), dann ist die Abbildung

$$R^{-1}(\tau) \to \operatorname{Hom}_E(L, \overline{K}), \quad \sigma \mapsto \tilde{\sigma}_0^{-1} \circ \sigma$$

bijektiv. Jedenfalls ist $\tilde{\sigma}_0^{-1} \circ \sigma$ ein E-Homomorphismus, denn für $\alpha \in E$ gilt

$$(\tilde{\sigma}_0^{-1} \circ \sigma)(\alpha) = \tilde{\sigma}_0^{-1}(\tau(\alpha)) = \tilde{\sigma}_0^{-1}(\sigma_0(\alpha)) = \alpha.$$

Die Bijektivität folgt, weil die Abbildung eine Umkehrabbildung hat, nämlich $\sigma \mapsto \tilde{\sigma}_0 \circ \sigma$.) Jede Faser $R^{-1}(\tau)$ von R hat also $[L : E]_s$ Elemente. Weil $\operatorname{Hom}_K(L, \overline{K})$ die disjunkte Vereinigung der Fasern von R ist und es $\#\operatorname{Hom}_K(E, \overline{K}) = [E : K]_s$ Fasern gibt, folgt die behauptete Gleichheit. □

LEMMA 5.20. *Für jede endliche Körpererweiterung L/K gilt $[L : K]_s \leq [L : K]$.*

BEWEIS. Wegen der Multiplikativät des Separabilitätsgrades in einem Turm von Erweiterungen genügt es, die Behauptung für einfache Erweiterungen zu zeigen. In diesem Fall haben wir die Aussage aber bereits in Lemma 5.18 notiert. □

Man kann auch zeigen (siehe Satz 5.33), dass für eine endliche Körpererweiterung L/K der Separabilitätsgrad immer ein Teiler des Grads ist und dass der Quotient $[L : K]/[L : K]_s$ gleich 1 oder sonst eine Potenz der (notwendigerweise positiven) Charakteristik p von K ist.

SATZ 5.21. *Sei L/K eine endliche Körpererweiterung. Es sind äquivalent:*

(i) *Die Erweiterung L/K ist separabel.*

(ii) *Es gibt separable Elemente $\alpha_1, \ldots, \alpha_r \in L$ mit $L = K(\alpha_1, \ldots, \alpha_r)$.*

(iii) *Es gilt $[L : K]_s = [L : K]$.*

BEWEIS. Wenn (i) gilt, dann folgt (ii) – wir können ein beliebiges endliches Erzeugendensystem der Erweiterung L/K hernehmen. Ist (ii) gegeben, so erhalten wir (iii) aus Lemma 5.18, indem wir die Multiplikativität des Separabilitätsgrades ausnutzen für die Kette

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq \cdots \subseteq K(\alpha_1, \ldots, \alpha_r) = L.$$

(Nach Voraussetzung ist α_i separabel über K, also erst recht über jedem Erweiterungskörper E von K, denn $\operatorname{minpol}_{\alpha,E} \mid \operatorname{minpol}_{\alpha,K}$.)

Schließlich zeigen wir die Implikation (iii) $\Rightarrow$ (i). Sei $\alpha \in L$. Aus

$$[L : K]_s = [L : K], \quad [L : K(\alpha)]_s \leq [L : K(\alpha)], \quad [K(\alpha) : K]_s \leq [K(\alpha) : K]$$

und der Multiplikativität von Separabilitätsgrad und gewöhnlichem Grad folgt mit der Voraussetzung (iii), dass $[K(\alpha) : K]_s = [K(\alpha) : K]$ gilt. Also ist das Element α separabel über K (Lemma 5.18). □

BEMERKUNG 5.22. Ist L/K separabel, dann gilt immer $[L : K]_s = [L : K]$, mit anderen Worten: Es ist dann L/K genau dann endlich, wenn $[L : K]_s$ endlich ist. Es ist nämlich $[E : K]_s \leq [L : K]_s$ für jeden Zwischenkörper E von L/K, und eine unendliche Erweiterung besitzt Zwischenkörper beliebig hohen endlichen Grades über dem Grundkörper. ◊

Entsprechendes gilt dann auch für nicht notwendig endlich erzeugte Erweiterungen:

KOROLLAR 5.23. *Sei L/K eine algebraische Körpererweiterung und $M \subseteq L$ eine Teilmenge mit $L = K(M)$. Sind alle Elemente aus M separabel über K, dann ist die Erweiterung L/K separabel.*

BEWEIS. Das folgt aus den vorherigen Ergebnissen, weil jedes Element von $K(M)$ in einem Teilkörper von $K(M)$ enthalten ist, der von einer geeignet gewählten endlichen Teilmenge von M erzeugt wird. Vergleiche den Beweis von Korollar 4.19. □

KOROLLAR 5.24. *Seien L/E und E/K algebraische Körpererweiterungen. Dann ist äquivalent:*

(i) *Die Erweiterung L/K ist separabel.*

(ii) *Die Erweiterungen L/E und E/K sind separabel.*

BEWEIS. Wenn L/K endlich ist, folgt die Behauptung direkt aus dem oben Gesagten, indem wir Grad und Separabilitätsgrad dieser Erweiterungen betrachten. Den allgemeinen Fall können wir wie folgt darauf zurückführen. Dass (ii) aus (i) folgt, ist einfach. Sei nun (ii) gegeben und $\alpha \in L$. Sei $\operatorname{minpol}_{\alpha,E} = \sum_{i=0}^{d} a_i X^i$, $a_i \in E$ und $E' = K(a_1, \ldots, a_d)$. Weil α über E separabel ist, hat $\operatorname{minpol}_{\alpha,E}$ nur einfache Nullstellen. Deshalb ist α auch separabel über E', denn das Minimalpolynom von α über E' ist dasselbe Polynom. Weil E über K separabel ist, ist auch E' separabel über K. Weil die Erweiterungen $E'(\alpha)/E'$ und E'/K endlich und separabel sind, ist auch $E'(\alpha)/K$ separabel, insbesondere ist α separabel über K. □

Wir schließen diesen Abschnitt ab mit dem *Satz vom primitiven Element*, der sowohl ein für sich genommen interessantes Ergebnis darstellt, als auch später für uns beim Studium von »Galois-Erweiterungen« nützlich sein wird.

SATZ 5.25 (Satz vom primitiven Element). *Sei L/K eine endliche separable Körpererweiterung. Dann existiert $\alpha \in L$ mit $L = K(\alpha)$. Wir nennen α ein* primitives Element *der Erweiterung L/K.*

BEWEIS. Wenn K und damit auch L endlich ist, können wir für α irgendeinen Erzeuger der multiplikativen Gruppe $L^\times$ wählen (nach Korollar 2.49 ist diese Gruppe zyklisch). Sei nun K unendlich und sei $\overline{K}$ ein algebraischer Abschluss von K.

Jedenfalls ist L über K endlich erzeugt, und per Induktion können wir uns auf den Fall beschränken, dass $L = K(\beta, \gamma)$ von zwei Elementen erzeugt wird.

Es genügt nun, ein Element α mit $[K(\alpha) : K]_s = [L : K]_s = [L : K]$ zu finden, oder mit anderen Worten ein Element $\alpha \in L$, für das die Einschränkungsabbildung $\mathrm{Hom}_K(L, \overline{K}) \to \mathrm{Hom}_K(K(\alpha), \overline{K})$ injektiv ist. (Wir wissen ja bereits, dass diese Abbildung immer surjektiv ist.) Die Injektivität ist dazu äquivalent, dass die Bilder $\sigma(\alpha)$ von α für $\sigma \in \mathrm{Hom}_K(L, \overline{K})$ paarweise verschieden sind.

Wir machen den Ansatz $\alpha = b\beta + \gamma$ für ein Element $b \in K$, das noch geeignet zu wählen ist. Die Bedingung, die b erfüllen muss, ist

$$b\sigma(\beta) + \sigma(\gamma) \neq b\tau(\beta) + \tau(\gamma) \quad \text{für } \sigma \neq \tau \in \mathrm{Hom}_K(L, \overline{K}),$$

oder mit anderen Worten

$$\prod_{\sigma \neq \tau} (b(\sigma(\beta) - \tau(\beta)) + (\sigma(\gamma) - \tau(\gamma))) \neq 0.$$

(Das Produkt wird hier und im Folgenden über alle $\sigma \neq \tau \in \mathrm{Hom}_K(L, \overline{K})$ gebildet.) Das heißt, dass b *keine* Nullstelle des Polynoms

$$f = \prod_{\sigma \neq \tau} ((\sigma(\beta) - \tau(\beta))X + (\sigma(\gamma) - \tau(\gamma))) \in \overline{K}[X]$$

ist. Wenn $\sigma(\beta) = \tau(\beta)$ und $\sigma(\gamma) = \tau(\gamma)$ gilt, dann folgt $\sigma = \tau$, weil L von β und γ erzeugt wird. Faktoren mit $\sigma = \tau$ treten im Produkt nicht auf; also ist $f \neq 0$. Daher hat f höchstens endlich viele Nullstellen in K. Weil K unendlich ist, existiert also $b \in K$ mit $f(b) \neq 0$ und dann ist $b\beta + \gamma$ ein Element von L, das L über K erzeugt. □

”

Lieber Herr Hasse!
Ich möchte Ihnen doch auch noch den Galoisschen Beweis für die Existenz des primitiven Elements zur eventuellen Aufnahme in Ihr Buch angeben.1) Bei Galois (in seiner großen Abhandlung über die Auflösung durch Radikale) steht er für den Fall, daß es sich...

So beginnt eine Postkarte[a] von Emmy Noether[b] an Helmut Hasse[c]. (Aus dem von Lemmermeyer und Roquette herausgegebenen Buch über die Korrespondenz Noether–Hasse[d], PDF kostenlos verfügbar.)

»Sehen« Sie, dass es sich um »denselben« Beweis handelt, wie wir ihn gegeben haben?

[a] https://www.mathi.uni-heidelberg.de/%7Eroquette/hasse-noether/hano_003_10-11-192_.html
[b] https://de.wikipedia.org/wiki/Emmy_Noether
[c] https://de.wikipedia.org/wiki/Helmut_Hasse
[d] https://univerlag.uni-goettingen.de/handle/3/isbn-3-938616-35-0

ERGÄNZUNG 5.26. Es gilt der folgende Satz:

SATZ 5.27. *Sei L/K eine algebraische Körpererweiterung. Dann sind äquivalent:*

(i) *Die Erweiterung L/K besitzt ein primitives Element, d.h. es existiert $\alpha \in L$ mit $L = K(\alpha)$.*
(ii) *Die Erweiterung L/K hat nur endlich viele Zwischenkörper.*

BEWEIS. Vielleicht als Übung... □

□ Ergänzung 5.26

5.3. Rein inseparable Körpererweiterungen *

Wir hatten definiert:

DEFINITION 5.28. Eine algebraische Körpererweiterung L/K heißt *rein inseparabel*, wenn jedes Element $\alpha \in L \setminus K$ über K inseparabel ist. ⊣

Wir hatten auch schon gesehen (vergleiche Satz 5.9), dass es nicht-triviale rein inseparable Erweiterungen eines Körpers K nur geben kann, wenn K positive Charakteristik hat.

SATZ 5.29. *Sei K ein Körper von positiver Charakteristik p und sei L/K eine rein inseparable Körpererweiterung. Dann gibt es für jedes $\alpha \in L$ eine Zahl $r \in \mathbb{N}$ mit $\alpha^{p^r} \in K$. Ist r mit dieser Eigenschaft minimal gewählt, so gilt $[K(\alpha) : K] = p^r$ und $\operatorname{minpol}_{\alpha,K} = X^{p^r} - \alpha^{p^r}$.*

BEWEIS. Sei $\alpha \in L$, $f = \operatorname{minpol}_{\alpha,K}$ und g das im Sinne von Satz 5.10 zu f gehörige Polynom, etwa $f = g(X^{p^r})$. Dann ist $\alpha^{p^r} \in L$ eine Nullstelle des separablen Polynoms $g \in K[X]$, ist also separabel über K und liegt demnach angesichts unserer Voraussetzung in K. Es folgt $\alpha^{p^r} \in K$ und auch $\deg(g) = 1$, also ist $[K(\alpha) : K] = \deg(f) = p^r$ und $f = X^{p^r} - \alpha^{p^r}$. Weil kein normiertes Polynom in $K[X]$ vom Grad $< p^r$ existiert, das α als Nullstelle hat, ist klar, dass r minimal ist mit der Eigenschaft $\alpha^{p^r} \in K$. □

SATZ 5.30. *Sei K ein Körper von positiver Charakteristik p. Sei L/K eine algebraische Körpererweiterung. Dann sind äquivalent:*

(i) *Die Erweiterung L/K ist rein inseparabel.*

(ii) *Für jedes $\alpha \in L$ existiert $r \geq 0$ mit $\alpha^{p^r} \in K$.*

(iii) *Es gilt $[L : K]_s = 1$.*

BEWEIS. Die Implikation (i) $\Rightarrow$ (ii) haben wir bereits gezeigt. Nun gelte (ii) und sei $\sigma\colon L \to \overline{K}$ ein K-Homomorphismus von L in einen algebraischen Abschluss von K. Sei $\alpha \in L$ und r so gewählt, dass $\alpha^{p^r} \in K$ gilt. Dann teilt $\operatorname{minpol}_{\alpha,K}$ das Polynom $X^{p^r} - \alpha^{p^r} = (X-\alpha)^{p^r}$, das nur eine einzige Nullstelle hat. Unter σ muss daher α auf die eindeutig bestimmte Nullstelle dieses Polynoms in $\overline{K}$ abgebildet werden, oder mit anderen Worten: auf die eindeutig bestimmte p^r-te Wurzel von α^{p^r} in $\overline{K}$. Da für jedes $\alpha \in L$ das Bild unter σ eindeutig bestimmt ist, gibt es nur genau einen K-Homomorphismus von L nach $\overline{K}$. Das bedeutet genau, dass $[L : K]_s = 1$ ist.

Gilt schließlich (iii) und ist $\alpha \in L$ separabel über K, dann folgt aus der Multiplikativität des Separabilitätsgrads, dass $[K(\alpha) : K]_s = 1$ ist. Weil α separabel über K ist, gilt andererseits $[K(\alpha) : K]_s = [K(\alpha) : K]$. Es folgt $\alpha \in K$. □

KOROLLAR 5.31. *Seien M/L und L/K algebraische Körpererweiterungen. Dann ist äquivalent:*

(i) *Die Erweiterungen M/L und L/K sind rein inseparabel.*

(ii) *Die Erweiterung M/K ist rein inseparabel.*

BEWEIS. Das folgt aus dem vorherigen Satz und der Multiplikativität des Separabilitätsgrads (Lemma 5.19). □

KOROLLAR 5.32. *Sei K ein Körper der Charakteristik $p > 0$ und sei L/K eine endliche rein inseparable Körpererweiterung. Dann ist $[L : K]$ eine Potenz von p.*

BEWEIS. Wir führen Induktion nach dem Grad $[L : K]$. Im Fall $[L : K] = 1$ ist nichts zu zeigen. Andernfalls sei $\alpha \in L \setminus K$. In Satz 5.29 haben wir bereits gesehen, dass $[K(\alpha) : K]$ eine Potenz von p ist. Nach Korollar 5.32 ist die Erweiterung $L/K(\alpha)$ rein inseparabel. Nach Induktionsvoraussetzung ist ihr Grad eine Potenz von p. Aus der Gradformel folgt nun die Behauptung. □

SATZ 5.33. *Sei L/K eine algebraische Körpererweiterung. Dann heißt*

$$E := \{\alpha \in L;\ \alpha \text{ ist separabel über } K\}$$

der separable Abschluss von K in L. *Es ist E ein Teilkörper von L, die Erweiterung E/K ist separabel, die Erweiterung L/E ist rein inseparabel und es gilt (wenn $[L : K]$ endlich ist):*

$$[L : K] = [L : K]_s \cdot [L : E].$$

BEWEIS. Der Teilkörper $K(E)$ von L, der von E über K erzeugt wird, ist separabel über K, weil er von separablen Elementen erzeugt wird (vergleiche Satz 5.21). Das bedeutet aber $K(E) = E$, also ist E tatsächlich ein Körper. Es ist dann klar, dass E/K separabel ist.

Es ist auch klar, dass L/E rein inseparabel ist, denn ist $\alpha \in L$ separabel über E, dann ist α auch separabel über K (nach Korollar 5.24), liegt also in E.

Für die Behauptung am Schluss genügt es, $[L : K]_s = [E : K]$ zu zeigen, oder äquivalent $[L : K]_s = [E : K]_s$. Aber L ist, wie gerade bemerkt, rein inseparabel über E, also zeigt Satz 5.30, dass $[L : E]_s = 1$ gilt. Die Gleichheit $[L : K]_s = [E : K]_s$ folgt daher aus der Multiplikativität des Separabilitätsgrads (Lemma 5.19). □

Man kann auch zeigen, dass der im obigen Satz beschriebene separable Abschluss von K in L der eindeutig bestimmte Zwischenkörper E von L/K ist, so dass E/K separabel und L/K rein inseparabel ist. Wenn L über K normal ist, dann ist auch der separable Abschluss von K in L normal über K.

BEMERKUNG 5.34. Für eine *normale* Erweiterung L/K existiert andererseits ein (eindeutig bestimmter) Zwischenkörper E', so dass E'/K rein inseparabel und L/E' separabel ist. Und zwar besteht E' genau aus denjenigen Elementen von L, die unter jedem K-Homomorphismus $L \to L$ auf sich selbst abgebildet werden. Es ist nicht schwer zu zeigen, dass der so definierte Körper E' über K rein inseparabel ist. Um zu zeigen, dass L/E' separabel ist, kann man Satz 5.44 aus dem nächsten Kapitel benutzen. Es ist E' normal über K. ◊

DEFINITION 5.35. Man nennt einen Körper K *separabel abgeschlossen*, wenn jede algebraische Erweiterung von K rein inseparabel ist. ⊣

Sei K ein Körper. Wir können nun zeigen, dass der im Beweis von Theorem 4.31 konstruierte Erweiterungskörper $C(K)$ algebraisch abgeschlossen ist. Das heißt, dass man bei der Konstruktion eines algebraischen Abschlusses von K darauf verzichten kann, diese Konstruktion zu iterieren und dann die Vereinigung zu bilden. Es gilt nämlich:

SATZ 5.36. *Sei L/K eine algebraische Körpererweiterung, so dass jedes Polynom in $K[X]$ eine Nullstelle in L hat. Dann ist L algebraisch abgeschlossen.*

BEWEISSKIZZE. Es genügt zu zeigen, dass L perfekt und separabel abgeschlossen ist, denn dann ist jede algebraische Körpererweiterung von L sowohl separabel als auch rein inseparabel, also trivial. Ist E ein perfekter Körper und E'/E eine algebraische Erweiterung, dann ist auch E' perfekt (Übung). Die entsprechende Aussage gilt auch für die Eigenschaft *separabel abgeschlossen*. Es genügt also zu zeigen, dass die Erweiterung L/K einerseits einen perfekten und andererseits einen separabel abgeschlossenen Zwischenkörper enthält. Das folgt aus den folgenden beiden Behauptungen. (Im Fall, dass K und damit auch L Charakteristik 0 hat, ist L »automatisch« perfekt, und es genügt, die erste Behauptung zu zeigen.)

Behauptung. Sei $K_s \subseteq L$ der separable Abschluss von K in L. Dann ist K_s separabel abgeschlossen.

Begründung. Es genügt zu zeigen, dass K_s keine nicht-trivialen einfachen separablen Erweiterungen hat. Sei eine einfache separable Erweiterung $K_s(\alpha)/K$ gegeben. Dann ist α auch separabel über K (weil K_s/K separabel ist, folgt das aus Korollar 5.24). Ist E ein Zerfällungskörper von $\mathrm{minpol}_{\alpha,K}$ über K, dann ist E ebenfalls endlich und separabel über K. Nach dem Satz vom primitiven Element (Satz 5.25) handelt es sich also um eine einfache Erweiterung, etwa $E = K(\gamma)$, $\gamma \in E$. Nach Voraussetzung hat $\mathrm{minpol}_{\gamma,K}$ eine Nullstelle β in L. Die Zuordnung $\gamma \mapsto \beta$ gibt uns dann einen K-Homomorphismus $K(\gamma) \to L$ (vergleiche Satz 4.25), also zerfällt $\mathrm{minpol}_{\alpha,K}$ über L vollständig in Linearfaktoren. Dies gilt sogar über K_s, weil $\mathrm{minpol}_{\alpha,K}$ separabel ist. Weil $\mathrm{minpol}_{\alpha,K_s}$ ein irreduzibler Teiler von $\mathrm{minpol}_{\alpha,K}$ in $K_s[X]$ ist, folgt $\deg(\mathrm{minpol}_{\alpha,K_s}) = 1$, also $\alpha \in K_s$.

Behauptung. Wir betrachten nun den Fall positiver Charakteristik p. Sei $K_i \subseteq L$ definiert durch

$$K_i = \{\alpha \in L; \text{ es existiert } r \geq 0 \text{ mit } \alpha^{p^r} \in K\}.$$

Dann ist K_i ein perfekter Teilkörper von K.

Begründung. Man rechnet leicht direkt nach, dass K_i ein Teilkörper von L ist. Angenommen, K_i wäre nicht perfekt. Nach Satz 5.15 ist die Abbildung $K_i \to K_i, x \mapsto x^p$ nicht surjektiv. Sei

$\alpha \in K_i$ ein Element, das nicht im Bild liegt. Nach Definition von K_i existiert dann $r \geq 0$ mit $\alpha^{p^r} \in K$. Sei nun $\beta \in L$ eine Nullstelle des Polynoms $X^{p^{r+1}} - \alpha^{p^r} \in K[X]$, es gilt also $\beta^{p^{r+1}} = \alpha^{p^r}$. Insbesondere ist β ein Element von K_i. Darüber hinaus folgt $\beta^p = \alpha \in K_i$. Dann besitzt aber α in K_i die p-te Wurzel β, im Widerspruch dazu, dass wir α als ein Element gewählt hatten, dass nicht im Bild des Frobenius-Homomorphismus liegt. □

5.4. Endliche Körper

SATZ 5.37. *Sei K ein endlicher Körper. Dann hat K positive Charakteristik p und die Anzahl q der Elemente von K ist eine Potenz von p. Für alle $x \in K$ gilt $x^q = x$.*

BEWEIS. Der Ringhomomorphismus $\mathbb{Z} \to K$ kann nicht injektiv sein, weil K endlich ist. Folglich hat K positive Charakteristik p. Dann ist der Primkörper von K (isomorph zu) $\mathbb{F}_p$ und damit ist K ein $\mathbb{F}_p$-Vektorraum. Weil K endlich ist, ist K als $\mathbb{F}_p$-Vektorraum endlichdimensional und hat folglich $p^{\dim_{\mathbb{F}_p} K}$ Elemente.

Ist $x \in K^\times$, so teilt die Ordnung von x als Element der Gruppe $K^\times$ die Ordnung dieser Gruppe, also $q - 1$. Das bedeutet $x^{q-1} = 1$. Also gilt $x^q = x$, und diese Gleichheit gilt natürlich auch für $x = 0$. □

SATZ 5.38. *Sei p eine Primzahl. Zu jedem $r \in \mathbb{N}_{>0}$ gibt es einen Körper mit $q := p^r$ Elementen. Dieser Körper ist ein Zerfällungskörper des Polynoms $X^q - X \in \mathbb{F}_p[X]$.*

Sind K, K' endliche Körper mit $\#K = \#K'$, dann existiert ein Körperisomorphismus $K \cong K'$.

BEWEIS. Sei $\overline{\mathbb{F}}_p$ ein algebraischer Abschluss von $\mathbb{F}_p$. Die Menge

$$K := V(X^q - X, \overline{\mathbb{F}}_p) = \{x \in \overline{\mathbb{F}}_p;\ x^q = x\}$$

bildet einen Teilkörper von $\overline{\mathbb{F}}_p$, wie man leicht nachprüft. Es handelt sich nämlich genau um die Menge der Elemente von $\overline{\mathbb{F}}_p$, die unter dem q-Frobenius-Homomorphismus $x \mapsto x^q$ (Beispiel 3.2) auf sich selbst abgebildet werden. Vergleiche Satz 5.43.

Die Ableitung des Polynoms $X^q - X$ ist -1, also hat $X^q - X$ nur einfache Nullstellen, und es folgt $\#K = q$. Aus der Definition folgt auch direkt, dass K der Zerfällungskörper von $X^q - X$ in $\overline{\mathbb{F}}_p$ ist. Aus dieser Charakterisierung folgt auch die Eindeutigkeit bis auf Isomorphismus (siehe Satz 5.3). □

SATZ 5.39. *Sei $\overline{\mathbb{F}}_p$ ein algebraischer Abschluss des Körpers $\mathbb{F}_p$. Für jedes $r \in \mathbb{N}$ enthält $\overline{\mathbb{F}}_p$ genau einen Teilkörper $\mathbb{F}_{p^r}$ mit p^r Elementen und es gilt*

$$\overline{\mathbb{F}}_p = \bigcup_{r \geq 1} \mathbb{F}_{p^r}.$$

Für $r, s \in \mathbb{N}$ gilt genau dann $\mathbb{F}_{p^r} \subseteq \mathbb{F}_{p^s}$, wenn $r \mid s$ gilt.

BEWEIS. Sei $q = p^r$. Die Nullstellenmenge von $X^q - X$ in $\overline{\mathbb{F}}_p$ bildet einen Teilkörper mit q Elementen. Andererseits gilt für jedes Element x eines (Teil-)Körpers mit q Elementen, dass $x^q = x$, also dass x eine Nullstelle von $X^q - X$ ist. Das zeigt die Eindeutigkeit.

Wenn $\mathbb{F}_{p^r} \subseteq \mathbb{F}_{p^s}$, dann ist $\mathbb{F}_{p^s}$ ein endlichdimensionaler $\mathbb{F}_{p^r}$-Vektorraum, hat also Kardinalität $p^s = p^{rd}$, wobei d die Dimension bezeichne. Ist andererseits r ein Teiler von s, etwa $s = rd$ und daher $p^s = (p^r)^d$, und $x \in \mathbb{F}_{p^r}$, dann gilt $x^{p^s} = x^{(p^r)^d} = (\cdots(x^{p^r})^{p^r})\cdots)^{p^r} = x$, also $x \in \mathbb{F}_{p^s}$. Es folgt $\mathbb{F}_{p^r} \subseteq \mathbb{F}_{p^s}$. □

SATZ 5.40. *Jede Erweiterung L/K endlicher Körper ist normal und separabel.*

BEWEIS. Weil L endlich ist, ist L als K-Vektorraum endlich erzeugt, die Erweiterung L/K also notwendigerweise endlich. Wir haben bereits gesehen (Korollar 5.16), dass endliche Körper vollkommen sind. Ist schließlich $\#L = q$ und p die Charakteristik von K und L, dann ist L der Zerfällungskörper von $X^q - X \in \mathbb{F}_p[X] \subseteq K[X]$, also ist L normal über K. □

ERGÄNZUNG 5.41 (Anwendungen endlicher Körper). Endliche Körper sind nicht nur von theoretischem Interesse (besonders zum Beispiel in der Zahlentheorie, aber auch in der Kombinatorik), sondern spielen auch in Anwendungen eine Rolle, inbesondere in der Informatik. Einige Stichpunkte dazu sind

- Kryptographie, zum Beispiel RSA (siehe Bemerkung LA1.4.22, Bemerkung LA1.8.58), Kryptographie mit elliptischen Kurven, siehe [**We**],
- Kodierungstheorie, siehe Kapitel LA1.12 und die dort gegebenen Verweise,
- Linear rückgekoppelte Schieberegister[1] (englisch: Linear Feedback Shift Register, LFSR), Pseudozufallszahlengeneratoren, siehe auch [**Lö**], Beispiel 3.3.9.

□ Ergänzung 5.41

5.5. Galois-Erweiterungen

5.5.1. Definition des Begriffs *Galois-Erweiterung*. Ist L ein Körper, so bezeichnen wir mit $\mathrm{Aut}(L)$ die Gruppe (bezüglich der Verkettung von Abbildungen) aller Körperautomorphismen $L \xrightarrow{\sim} L$.

Sei L/K eine Körpererweiterung. Wir bezeichnen mit $\mathrm{Aut}_K(L)$ die Gruppe aller K-Automorphismen von L, also aller Isomorphismen $L \xrightarrow{\sim} L$ von K-Algebren. Konkret ausgeschrieben bedeutet das:

$$\mathrm{Aut}_K(L) = \{\sigma\colon L \to L \text{ Körperautomorphismus};\ \sigma(x) = x \text{ für alle } x \in K\}.$$

BEMERKUNG 5.42. Ist L/K algebraisch – und das ist der Fall, für den wir uns interessieren, dann ist $\mathrm{Aut}_K(L) = \mathrm{Hom}_K(L, L)$, denn jeder K-Homomorphismus $\sigma\colon L \to L$ ist bijektiv. Die Injektivität ist klar. Die Surjektivität zeigen wir wie folgt: Sei $\alpha \in L$. Die Menge $V(\mathrm{minpol}_{\alpha,K}, L)$ der Nullstellen des Minimalpolynoms von α in L ist eine endliche Teilmenge, die von σ nach Satz 4.25 in sich abgebildet wird. Weil σ injektiv ist, impliziert die Endlichkeit, dass σ eine Bijektion dieser Menge mit sich selbst induziert. Insbesondere liegt α im Bild von σ. ◊

SATZ 5.43. (1) *Sei L ein Körper und sei G eine Gruppe, die auf L durch Körperautomorphismen operiert. (Es ist also eine Operation $G \times L \to L$ gegeben, derart dass das Bild des zugehörige Gruppenhomomorphismus $G \to \mathrm{Bij}(L)$ in $\mathrm{Aut}(L)$ liegt.)*

Dann ist

$$L^G := \{x \in L;\ \sigma(x) = x \text{ für alle } \sigma \in G\}$$

ein Teilkörper von L, der sogenannte Fixkörper *unter der Operation von G.*

(2) *Ist L/K eine Körpererweiterung und operiert die Gruppe G auf L durch K-Automorphismen, so ist L^G ein Zwischenkörper der Erweiterung L/K.*

BEWEIS. Zum Beweis ist im Grunde nichts zu sagen: Alle Aussagen kann man leicht direkt nachprüfen. □

[1] https://de.wikipedia.org/wiki/Linear_rückgekoppeltes_Schieberegister

In den meisten Fällen, in denen wir den Fixkörper unter einer Gruppe G betrachten, ist G einfach eine Untergruppe von $\mathrm{Aut}(L)$.

Wir definieren nun den Begriff der Galois-Erweiterung, der für den weiteren Verlauf zentral ist.

SATZ 5.44. *Sei L/K eine algebraische Körpererweiterung.*

(1) *Es sind äquivalent:*

(i) *Es gilt*
$$K = L^{\mathrm{Aut}_K(L)}.$$

(ii) *Es gibt eine Untergruppe $G \subseteq \mathrm{Aut}(L)$, so dass*
$$K = L^G$$
gilt.

(iii) *Die Erweiterung L/K ist normal und separabel.*

Wenn diese Bedingungen erfüllt sind, dann heißt die Erweiterung L/K galoissch *oder eine* Galois-Erweiterung. *In diesem Fall nennen wir* $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$ *die* Galois-Gruppe *der Erweiterung L/K.*

(2) *Sei L/K galoissch und G wie in (ii). Die Erweiterung ist genau dann endlich, wenn $\#G$ endlich ist. In diesem Fall gilt $G = \mathrm{Gal}(L/K)$ und $\#\mathrm{Gal}(L/K) = [L : K]$.*

BEWEIS. Zu (1). Die Implikation (i) $\Rightarrow$ (ii) ist offensichtlich.

(ii) $\Rightarrow$ (iii). Die Bedingung $K = L^G$ impliziert, dass $G \subseteq \mathrm{Aut}_K(L) = \mathrm{Hom}_K(L, L)$ ist. Wir betrachten die Bahn von α unter G, also die Teilmenge $\{\sigma(\alpha);\ \sigma \in G\}$ von L. Dies ist eine Teilmenge der Menge der Nullstellen von $\mathrm{minpol}_{\alpha,K}$ in L, also eine endliche Menge.

Es sei
$$f = \prod_{\beta \in G\alpha} (X - \beta) \in L[X].$$

Behauptung. Es gilt $f \in K[X]$, d.h. alle Koeffizienten von f werden von den Elementen von G fixiert.

Begründung. Ist $\sigma \in G$, dann ist die Abbildung $\beta \mapsto \sigma(\beta)$ eine Bijektion $G\alpha \to G\alpha$. Also gilt $f = \prod_{\beta \in G\alpha}(X - \sigma(\beta))$, und weil σ durch einen Homomorphismus $L \to L$ wirkt, ist die rechte Seite genau das Polynom, das aus f durch Anwenden von σ auf alle Koeffizienten entsteht.

Wir haben damit ein separables Polynom in $K[X]$ gefunden, das α als Nullstelle hat und das über L vollständig in Linearfaktoren zerfällt. Der Körper L ist der Zerfällungskörper aller dieser separablen Polynome über K und ist folglich normal und separabel über K.

Als nächstes zeigen wir die Implikation (iii) $\Rightarrow$ (i). Dass $K \subseteq L^{\mathrm{Aut}_K(L)}$ gilt, ist klar. Ist andererseits $\alpha \in L$, $\alpha \notin K$, dann hat das Minimalpolynom von α über K Grad > 1. Weil L/K normal ist, zerfällt es über L vollständig in Linearfaktoren und wegen der Separabilität hat es eine von α verschiedene Nullstelle β. Wir erhalten einen K-Homomorphismus $K[\alpha] \to L$, $\alpha \mapsto \beta$, den wir zu einem K-Automorphismus von L fortsetzen können (hier benutzen wir noch einmal die Normalität der Erweiterung L/K). Weil dieser Automorphismus α nicht auf sich selbst abbildet, ist $\alpha \notin L^{\mathrm{Aut}_K(L)}$. Damit ist auch die andere Inklusion bewiesen.

Zu (2). Sei L/K galoissch. Dann ist $\#\mathrm{Gal}(L/K) = [L : K]_s = [L : K]$ (für die erste Gleichheit benutzen wir die Normalität der Erweiterung, für die zweite die Separabilität, vergleiche Bemerkung 5.22). Es bleibt noch zu zeigen, dass L/K endlich ist, wenn die Untergruppe G von $\mathrm{Gal}(L/K)$ endlich ist, und dass dann $G = \mathrm{Gal}(L/K)$ gilt. Dazu genügt es nun zu

zeigen, dass $[L : K] \leq \#G$ gilt. Aus dem obigen Beweis der Implikation (ii) $\Rightarrow$ (iii) folgt, dass $\deg(\mathrm{minpol}_{\alpha,K}) \leq \#G$ für alle $\alpha \in L$ gilt. Ist L/K endlich, so besitzt die Erweiterung wegen der Separabilität ein primitives Element und es folgt $[L : K] \leq \#G$. Ist L/K unendlich, so enthält L Elemente mit Minimalpolynom beliebig hohen Grades, und es folgt, dass G unendlich sein muss. □

Évariste Galois

Ein wesentlicher Durchbruch beim Verständnis von algebraischen Körpererweiterungen (im Sinne des heutigen Sprachgebrauchs, Begriffe wie *Körper*, *Körpererweiterung* und auch *Gruppe* gab es damals noch nicht) gelang dem französischen Mathematiker Évariste Galois[a] (1811-1832), nach dem die hier behandelte Theorie heute benannt ist. Galois starb schon im Alter von 20 Jahren, und zwar bei einem Duell. Seine mathematische Karriere verlief nicht geradlinig, und seine Manuskripte wurden teils erst lange nach seinem Tod als relevant wahrgenommen und veröffentlicht.
Für weitere Informationen können Sie zum Beispiel die folgenden Quellen konsultieren:

Die Einführung des Buchs von Bosch [**Bo-A**], die die geschichtliche Entwicklung der Theorie der Lösbarkeit algebraischer Gleichungen zusammenfasst. (Oder wesentlich ausführlicher zu diesem Thema: Jean-Pierre Tignol, *Galois' Theory of Algebraic Equations*, 2nd ed., World Scientific 2016.)

In seinem Buch *Galois Theory*, Springer Graduate Texts in Mathematics **101**, stellt H. Edwards die Galois-Theorie in heutiger Sprache aber mathematisch gesehen sehr nah an den Arbeiten von Galois vor.

Speziell zum Leben von Galois:

T. Rothman, *The Short Life of Évariste Galois*, Scientific American **246**, No. 4 (April 1982), 136–149, https://www.jstor.org/stable/24966575

T. Rothman, *Genius and Biographers: The Fictionalization of Evariste Galois*, The Amer. Math. Monthly **89**, No. 2 (Feb. 1982), 84–106, https://www.jstor.org/stable/2320923

[a] https://de.wikipedia.org/wiki/Évariste_Galois

BEMERKUNG 5.45. Ist L/K eine nicht notwendig algebraische Erweiterung und G eine *endliche* Gruppe, die auf L durch K-Homomorphismen operiert, dann zeigt der Beweis des Satzes, dass L/L^G algebraisch, also eine endliche Galois-Erweiterung ist. ◊

BEISPIEL 5.46. Sei p eine Primzahl, q eine Potenz von p, K ein Körper mit q Elementen und L/K eine endliche Körpererweiterung vom Grad d. Nach Satz 5.40 ist die Erweiterung L/K galoissch. Der q-Frobenius-Homomorphismus $\mathrm{Frob}_q : L \to L, x \mapsto x^q$, ist ein Element der Galois-Gruppe $\mathrm{Gal}(L/K)$. Da L genau q^d Elemente hat und $L^\times$ zyklisch ist, gilt $\mathrm{Frob}_q^r = \mathrm{id}_L$ dann und nur dann, wenn $d \mid r$. Es folgt, dass die von Frob_q in $\mathrm{Gal}(L/K)$ erzeugte Untergruppe d Elemente hat. Weil $\#\mathrm{Gal}(L/K) = [L : K] = d$ gilt, sehen wir, dass $\mathrm{Gal}(L/K)$ zyklisch ist und von Frob_q erzeugt wird. ◊

ERGÄNZUNG 5.47. Ist L/K in der Situation des obigen Satzes unendlich, dann kann $\mathrm{Gal}(L/K)$ (unendliche) echte Untergruppen haben, die K als Fixkörper haben. Sei zum Beispiel p eine Primzahl, $K = \mathbb{F}_p$ und $L = \overline{\mathbb{F}}_p$ ein algebraischer Abschluss von $\mathbb{F}_p$. Sei $\mathrm{Frob}_p : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ der Frobenius-Automorphismus von $\overline{\mathbb{F}}_p$ und $G = \langle \mathrm{Frob}_p \rangle \subseteq \mathrm{Gal}(\overline{\mathbb{F}}_p / \mathbb{F}_p)$ die von Frob_p erzeugte

Untergruppe. Dann gilt $\overline{\mathbb{F}}_p^G = \mathbb{F}_p$, aber man kann zeigen, dass G eine echte Untergruppe von $\mathrm{Gal}(\overline{\mathbb{F}}_p \big/ \mathbb{F}_p)$ ist. Siehe zum Beispiel [**Bo-A**], Abschnitt 4.2. □ Ergänzung 5.47

Im weiteren Verlauf werden wir uns auf das Studium *endlicher* Galois-Erweiterungen beschränken. Man kann zwar die Theorie auch auf den Fall unendlicher Erweiterungen verallgemeinern, das macht die Sache aber etwas komplizierter. Gleichwohl ist es eine schöne Theorie, die auch in weiten Teilen analog zum endlichen Fall entwickelt werden kann, wenn man die Galois-Gruppe als »topologische Gruppe« betrachtet und anstelle aller Untergruppen nur solche hernimmt, die »abgeschlossen« im Sinne der gegebenen Topologie sind. Aus Zeitgründen müssen wir es aber bei dieser Werbung belassen, siehe zum Beispiel [**Bo-A**], Abschnitt 4.2 für weitere Details.

LEMMA 5.48. *Sei L/K eine endliche Körpererweiterung.*

(1) *Sei E ein Zwischenkörper der Körpererweiterung L/K. Ist L/K galoissch, dann ist auch L/E galoissch.*

(2) *Sei E ein Zwischenkörper der Körpererweiterung L/K. Sind L/K und E/K galoissch, dann ist die Einschränkung von Homomorphismen ein surjektiver Gruppenhomomorphismus* $\mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$ *mit Kern* $\mathrm{Gal}(L/E)$.

BEWEIS. Teil (1) folgt direkt aus Lemma 5.6 und Korollar 5.24.

Wir kommen zu Teil (2). Ist $\sigma\colon L \to L$ ein K-Homomorphismus, so hat $\sigma_{|E}\colon E \to L$ Bild in E, weil E normal ist über K. Wir können also $\sigma_{|E}$ als K-Homomorphismus $E \to E$ betrachten. In diesem Sinne ist die Einschränkungsabbildung in Teil (2) zu verstehen. Es handelt sich offenbar um einen Gruppenhomomorphismus mit Kern $\mathrm{Gal}(L/E)$. Ist ein K-Automorphismus $E \to E$ gegeben, so können wir ihn mit Satz 4.33 zu einem K-Automorphismus $L \to L$ fortsetzen. □

5.5.2. Der Hauptsatz der Galois-Theorie. Für eine Gruppe G bezeichnen wir mit $\mathrm{UG}(G)$ die Menge aller Untergruppen von G. Für eine Körpererweiterung L/K bezeichnen wir mit $\mathrm{ZK}(L/K)$ die Menge aller Zwischenkörper dieser Erweiterung.

THEOREM 5.49 (Hauptsatz der Galois-Theorie). *Sei L/K eine endliche Galois-Erweiterung mit Galois-Gruppe G.*

(1) *Dann sind die Abbildungen*

$$\mathrm{UG}(G) \to \mathrm{ZK}(L/K), \quad H \mapsto L^H, \qquad \textit{und} \quad \mathrm{ZK}(L/K) \to \mathrm{UG}(G), E \mapsto \mathrm{Gal}(L/E),$$

zueinander inverse inklusionsumkehrende Bijektionen zwischen der Menge der Untergruppen der Galois-Gruppe G und der Menge der Zwischenkörper der gegebenen Körpererweiterung.

(2) *Für einen Zwischenkörper E der Erweiterung L/K sind äquivalent:*

(i) *Die Erweiterung E/K ist normal.*

(ii) *Die Erweiterung E/K ist galoissch.*

(iii) *Die Untergruppe $H := \mathrm{Gal}(L/E) \subseteq \mathrm{Gal}(L/K)$ ist ein Normalteiler.*

Sind diese äquivalenten Bedingungen erfüllt, so induziert die Abbildung $\sigma \mapsto \sigma_{|E}$ einen Isomorphismus $\mathrm{Gal}(L/K) \,/\, \mathrm{Gal}(L/E) \to \mathrm{Gal}(E/K)$.

BEWEIS. Zu (1). Die angegebenen Zuordnungsvorschriften definieren Abbildungen $\mathrm{UG}(G) \to \mathrm{ZK}(L/K)$ (offensichtlich) und $\mathrm{ZK}(L/K) \to \mathrm{UG}(G)$ (nach Lemma 5.48 ist für einen Zwischenkörper E von L/K die Erweiterung L/E galoissch, so dass wir von der Galois-Gruppe sprechen können, und im selben Lemma haben wir festgestellt, dass es sich um eine Untergruppe von $\mathrm{Gal}(L/K)$ handelt).

Es ist auch leicht zu sehen, dass diese inklusionsumkehrend sind: Sind $H \subseteq H' \subseteq G$ Untergruppen, so ist $L^{H'} \subseteq L^H$. Sind $E \subseteq E' \subseteq L$ Zwischenkörper, so ist $\mathrm{Gal}(L/E') \subseteq \mathrm{Gal}(L/E)$.

Wir zeigen nun, dass die beiden Abbildungen zueinander invers sind. Die wesentliche Arbeit dafür haben wir bereits im Beweis von Satz 5.44 geleistet. Sei zunächst E ein Zwischenkörper und $H = \mathrm{Gal}(L/E)$. Wir müssen zeigen, dass $L^H = E$ gilt. Dies folgt aus Satz 5.44, denn wir wissen ja, dass L/E eine Galois-Erweiterung ist.

Sei nun H eine Untergruppe von $\mathrm{Gal}(L/K)$ und $E = L^H$. Dann liefert uns Satz 5.44 (2), dass $\mathrm{Gal}(L/E) = H$ gilt, weil mit L/K auch L/E endlich ist.

Zu (2). Die äquivalenten Charakterisierungen dafür, dass ein Zwischenkörper E normal über K ist, können wir folgendermaßen begründen. Die Implikation (i) $\Rightarrow$ (ii) ist klar. Gilt (ii), dann zeigt Lemma 5.48, dass $H := \mathrm{Gal}(L/E)$ der Kern eines Gruppenhomomorphismus ist, es handelt sich somit um einen Normalteiler.

Nun gelte (iii), es sei also H ein Normalteiler in $G = \mathrm{Gal}(L/K)$. Sei $\overline{K}$ ein algebraischer Abschluss von L und $\sigma\colon E \to \overline{K}$ ein K-Homomorphismus. Wir möchten zeigen, dass σ Bild in E hat. Wir können σ zu einem Homomorphismus $L \to \overline{K}$ fortsetzen und weil L/K normal ist, ist das Bild dieses Homomorphismus in L enthalten. Deshalb genügt es zu zeigen, dass für jedes $\sigma \in \mathrm{Gal}(L/K)$ gilt, dass $\sigma(E) \subseteq E$ ist.

Nun ist $E = L^H$, es ist also zu zeigen, dass $\tau(\sigma(x)) = \sigma(x)$ für alle $x \in L^H$. Aber weil H ein Normalteiler ist, liegt mit τ auch $\sigma^{-1}\tau\sigma$ in H und fixiert das Element x. Daraus folgt $\tau(\sigma(x)) = \sigma(x)$, wie gewünscht.

Wenn diese äquivalenten Bedingungen erfüllt sind, folgt wieder mit Lemma 5.48, dass die Einschränkung von Homomorphismen einen Isomorphismus $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/L^H) \to \mathrm{Gal}(L^H/K)$ liefert. □

BEMERKUNG 5.50. Alternativ kann man für den Beweis der Implikation (iii) $\Rightarrow$ (i) in Teil (2) des Hauptsatzes wie folgt argumentieren: Ist G irgendeine Gruppe, die auf einer Menge X operiert, ist H ein Normalteiler und ist X^H die Menge der Fixpunkte unter H, also $X^H = \{x \in X;\ \text{für alle } h \in H : hx = x\}$, dann operiert der Quotient G/H auf X^H, und zwar durch

$$G/H \times X^H \to X^H, \quad (gH, x) \mapsto gx.$$

Dass $gx \in X^H$ ist, zeigt man mit derselben Rechnung wie oben.

In unserem Fall sehen wir, dass G/H auf dem Fixkörper L^H von L unter H operiert. Es ist klar, dass dann $(L^H)^{G/H} = L^G = K$ gilt, und aus Satz 5.44 folgt, dass L^H/K eine Galois-Erweiterung ist. ◊

BEISPIEL 5.51. (1) Sei $a \in \mathbb{Q}$ ein Element, das in $\mathbb{Q}$ keine dritte Wurzel besitzt, also derart dass das Polynom $f = X^3 - a$ irreduzibel ist. Sei $K \subset \mathbb{C}$ der Zerfällungskörper von f. Sei $\alpha \in \mathbb{C}$ ein Element mit $\alpha^3 = a$ und sei $\zeta = e^{\frac{2\pi i}{3}} \in \mathbb{C}$. Es gilt dann

$$f = (X - \alpha)(X - \zeta\alpha)(X - \zeta^2\alpha) \quad \in \mathbb{C}[X]$$

und daher $K = \mathbb{Q}(\alpha, \zeta)$.

Weil die Grade $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ und $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$ teilerfremd sind, folgt aus der Gradformel, dass $[K : \mathbb{Q}] = 6$ gilt. Es folgt auch $\zeta\alpha \notin \mathbb{Q}(\alpha)$ (sonst wäre $\mathbb{Q}(\alpha) = K$) und

damit $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\zeta\alpha)$ und analog $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\zeta^2\alpha)$, $\mathbb{Q}(\zeta\alpha) \neq \mathbb{Q}(\zeta^2\alpha)$. Die Erweiterung $K/\mathbb{Q}$ hat also (mindestens) 3 Zwischenkörper, die über $\mathbb{Q}$ Grad 3 haben.

Die Galoisgruppe $\mathrm{Gal}(K/\mathbb{Q})$ hat 6 Elemente, ist also isomorph zu einer der Gruppen S_3 und $\mathbb{Z}/6$. Die zyklische Gruppe $\mathbb{Z}/6$ hat aber nur genau eine Untergruppe mit 2 Elementen. Angesichts des Hauptsatzes der Galois-Theorie kann daher $\mathrm{Gal}(K/\mathbb{Q})$ nicht zu $\mathbb{Z}/6$ isomorph sein.

Es folgt $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$. Daran sehen wir zum Beispiel auch, dass K genau einen Teilkörper E besitzt, der über $\mathbb{Q}$ Grad 2 hat. Denn S_3 besitzt genau eine Untergruppe mit 3 elementen, nämlich die alternierende Gruppe A_3. Es ist $E = \mathbb{Q}(\zeta)$, denn $\mathrm{minpol}_{\zeta,\mathbb{Q}} = X^2 + X + 1$.

(2) Sei $K \subset \mathbb{C}$ der Zerfällungskörper des Polynoms $f = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$. Es gilt $(X-1)\cdot f = X^7 - 1$ und daher mit $\zeta := e^{\frac{2\pi i}{7}}$, dass

$$f = \prod_{i=1}^{6} (X - \zeta^i) \quad \in \mathbb{C}[X].$$

Das Polynom f zerfällt also schon über $\mathbb{Q}(\zeta)$ vollständig in Linearfaktoren und es folgt $K = \mathbb{Q}(\zeta)$. Das Polynom f ist nach Beispiel 3.55 irreduzibel, also gilt $[K : \mathbb{Q}] = 6$.

Die $\mathbb{Q}$-Automorphismen $\mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ entsprechen bijektiv den Nullstellen von $f = \mathrm{minpol}_{\zeta,\mathbb{Q}}$ in $\mathbb{Q}(\zeta)$, also den möglichen Bildern von ζ, also den Nullstellen von f, d.h. den Elementen ζ^i für $i = 1, \ldots, 6$. Wir schreiben σ_i für den eindeutig bestimmten Automorphismus $\mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ mit $\zeta \mapsto \zeta^i$. Dann gilt

$$\sigma_i(\sigma_j(\zeta)) = \sigma_i(\zeta^j) = \sigma_i(\zeta)^j = \zeta^{ij} = \sigma_j(\sigma_i(\zeta)),$$

die Gruppe $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ ist also kommutativ. Weil sie 6 Elemente hat, folgt $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \mathbb{Z}/6$. (Eine bessere Sichtweise ist eigentlich, die Galois-Gruppe mit der Gruppe $(\mathbb{Z}/7)^\times$ zu identifizieren, denn eine ähnliche Rechnung wie die obige zeigt, dass die Abbildung $(\mathbb{Z}/7)^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, $i \mapsto \sigma_i$, ein Gruppenhomomorphismus ist. Vergleiche Abschnitt 6.3 für eine ausführliche allgemeinere Analyse.)

◊

Für Galois-Erweiterungen mit abelscher bzw. zyklischer Galois-Gruppe (wie im Beispiel, Teil (2)) verwendet man die folgende Sprechweise:

DEFINITION 5.52. Eine Körpererweiterung L/K heißt *abelsch* (bzw. *zyklisch*), wenn sie galoissch mit abelscher (bzw. zyklischer) Galois-Gruppe ist. ⊣

KOROLLAR 5.53. *Jede endliche separable Körpererweiterung besitzt nur endlich viele Zwischenkörper.*

BEWEIS. Sei L/K endlich und separabel. Sei M/K eine normale Hülle von L/K (konkret: ein Zerfällungskörper des Minimalpolynoms eines primitiven Elements von L/K, oder der Minimalpolynome von endlich vielen Erzeugern dieser Körpererweiterung, wenn man an dieser Stelle den Satz vom primitiven Element vermeiden möchte). Dann ist M/K wieder endlich und separabel und zudem normal, also eine Galois-Erweiterung. Die Menge der Zwischenkörper von M/K steht in Bijektion zur Menge der Untergruppen der Galois-Gruppe dieser Erweiterung. Eine endliche Gruppe hat aber offensichtlich nur endlich viele Untergruppen. Weil jeder Zwischenkörper von L/K auch ein Zwischenkörper von M/K ist, folgt die Behauptung. □

DEFINITION 5.54. Sei L/K eine Körpererweiterung mit Zwischenkörpern E und E'. Das *Kompositum* von E und E' ist der kleinste Teilkörper von L, der E und E' enthält und wird mit $E \cdot E'$ oder einfach mit EE' bezeichnet. ⊣

Ist L/K eine Körpererweiterung und sind $E = K(\alpha_1, ..., \alpha_r), E' = K(\beta_1, ..., \beta_s)$ Zwischenkörper ($\alpha_i, \beta_j \in L$), so ist das Kompositum EE' der Körper $K(\alpha_1, ..., \alpha_r, \beta_1, ..., \beta_s)$.

Man beachte, dass die Menge EE' nicht einfach die Menge aller Produkte xx', $x \in E, x' \in E'$ ist, sondern (in der Regel) noch andere Elemente enthält.

SATZ 5.55. *Sei L/K eine endliche Galois-Erweiterung mit Zwischenkörpern E und E'. Sei $H = \mathrm{Gal}(L/E)$ und $H' = \mathrm{Gal}(L/E')$.*

(1) *Es gilt $EE' = L^{H \cap H'}$.*

(2) *Es gilt $E \cap E' = L^{\tilde{H}}$, wobei $\tilde{H}$ die von H und H' in $\mathrm{Gal}(L/K)$ erzeugte Untergruppe bezeichne.*

(3) *Seien nun die Erweiterungen E/K und E'/K galoissch. Dann ist EE'/K eine Galois-Erweiterung und der Homomorphismus*

$$\mathrm{Gal}(EE'/E) \to \mathrm{Gal}(E'/E \cap E'), \quad \sigma \mapsto \sigma_{|E'},$$

ist bijektiv. Insbesondere ist $[EE' : E]$ ein Teiler von $[E' : K]$.

(4) *Seien wie in Teil (3) die Erweiterungen E/K und E'/K galoissch. Dann ist die Abbildung*

$$\mathrm{Gal}(EE'/K) \to \mathrm{Gal}(E/K) \times \mathrm{Gal}(E'/K), \quad \sigma \mapsto (\sigma_{|E}, \sigma_{|E'})$$

ein injektiver Gruppenhomomorphismus. Ist $E \cap E' = K$, so handelt es sich sogar um einen Isomorphismus.

BEWEIS. Zu (1) und (2). Beide Aussagen folgen direkt daraus, dass es sich bei der Bijektion im Hauptsatz der Galois-Theorie (für die Erweiterung L/K) um eine *inklusionsumkehrende* Bijektion handelt. Es ist nämlich EE' der *kleinste* Zwischenkörper, der E und E' enthält, und $H \cap H'$ die *größte* Untergruppe von $\mathrm{Gal}(L/K)$, die in H und in H' enthalten ist. Für Teil (2) bemerken wir, dass $E \cap E'$ der größte Zwischenkörper ist, der in E und in E' enthalten ist, und dass $\tilde{H}$ die kleinste Untergruppe ist, die H und H' enthält.

Zu (3). Ist E der Zerfällungskörper einer Familie $(f_i)_i$ und E' der Zerfällungskörper einer Familie $(g_j)_j$ von separablen Polynomen aus $K[X]$, dann ist EE' der Zerfällungskörper aller dieser Polynome f_i, g_j. Also ist EE'/K galoissch.

Die Vorschrift $\sigma \mapsto \sigma_{|E'}$ definiert jedenfalls eine Abbildung $\mathrm{Gal}(EE'/E) \to \mathrm{Gal}(E'/E \cap E')$, da E' sogar über K, also erst recht über $E \cap E'$ normal ist. Da EE' als Erweiterungskörper von E von den Elementen von E' erzeugt wird, ist sie injektiv.

Sei H das Bild der Abbildung. Um $H = \mathrm{Gal}(E'/E \cap E')$ und damit die Surjektivität zu zeigen, genügt es zu zeigen, dass $(E')^H = E \cap E'$ gilt. Aber für $x \in (E')^H$ gilt trivialerweise $x \in E'$ und außerdem $\sigma(x) = x$ für alle $\sigma \in \mathrm{Gal}(EE'/E)$, also $x \in E$.

Zu (4). Die Injektivität ist leicht zu sehen. Die Surjektivität im Fall $E \cap E' = K$ folgt daraus, dass in diesem Fall wegen Teil (3) und der Gradformel beide Seiten gleich viele Elemente haben. □

BEMERKUNG 5.56. Ohne die Bedingung, dass die Erweiterungen E/K und E'/K *galoissch* seien, gilt die Teilbarkeitsaussage in (3) im allgemeinen nicht, wie das Beispiel $K = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt[3]{2}), E' = \mathbb{Q}(e^{\frac{2\pi i}{3}}\sqrt[3]{2})$, zeigt. ◊

BEISPIEL 5.57. Sei K ein endlicher Körper mit $q = p^r$ Elementen, $p = \mathrm{char}(K)$, und L/K eine Körpererweiterung vom Grad d. Wir haben gesehen, dass die Erweiterung L/K dann galoissch ist (Satz 5.40). Dass die Galois-Gruppe $\mathrm{Gal}(L/K)$ zyklisch ist und vom q-Frobenius-Homomorphismus Frob_q erzeugt wird, können wir mit dem Hauptsatz der Galois-Theorie (alternativ zu Beispiel 5.46) auch dadurch begründen, dass für die von Frob_q erzeugte Untergruppe H von $\mathrm{Gal}(L/K)$ gilt, dass $L^H = K$ ist. ◊

5.5.3. Der Fundamentalsatz der Algebra. Aus dem Hauptsatz der Galois-Theorie erhalten wir (mit den Sätzen aus der Gruppentheorie, die wir zu Beginn der Vorlesung bewiesen haben) einen Beweis des Fundamentalsatzes der Algebra.

THEOREM 5.58. *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

BEWEIS. Wir benutzen im Beweis die folgenden »analytischen« Tatsachen über den Körper der reellen Zahlen.

(a) Ist $p \in \mathbb{R}[X]$ ein Polynom von ungeradem Grad, so hat p eine Nullstelle in $\mathbb{R}$.

(b) Jedes Polynom $p \in \mathbb{C}[X]$ vom Grad 2 hat eine Nullstelle in $\mathbb{C}$.

Punkt (a) folgt aus dem Zwischenwertsatz, weil für ein Polynom ungeraden Gerades sowohl positive als auch negative Werte annimmt (man betrachte die Grenzwerte $\lim_{x\to\infty} p(x)$ und $\lim_{x\to-\infty} p(x)$. Für Punkt (b) genügt es angesichts der Lösungsformel für quadratische Gleichungen zu wissen, dass man aus jeder komplexen Zahl in $\mathbb{C}$ eine Quadratwurzel ziehen kann. Dazu kann man am einfachsten mit Polarkoordinaten argumentieren: Für $r \in \mathbb{R}_{\geq 0}$, $t \in \mathbb{R}$ gilt $(\sqrt{r}e^{\frac{it}{2}})^2 = re^{it}$.

Um zu zeigen, dass $\mathbb{C}$ algebraisch abgeschlossen ist, genügt es zu zeigen, dass $\mathbb{C}$ selbst der einzige endliche Erweiterungskörper von $\mathbb{C}$ ist. Sei also $K/\mathbb{C}$ endlich. Indem wir gegebenenfalls zur normalen Hülle übergehen, können wir annehmen, dass die Erweiterung $K/\mathbb{R}$ normal und damit galoissch ist.

Behauptung. Der Grad $[K : \mathbb{R}]$ ist eine Potenz von 2.

Begründung. Wir schreiben $[K : \mathbb{R}] = 2^m d$ für eine ungerade Zahl d und werden zeigen, dass $d = 1$ gilt. Sei $H \subseteq \mathrm{Gal}(L/\mathbb{R})$ eine 2-Sylow-Untergruppe. Dann hat die Erweiterung $K^H/\mathbb{R}$ Grad d. Ist $\alpha \in K^H$, so ist $[K(\alpha) : \mathbb{R}] = \deg(\mathrm{minpol}_{\alpha,\mathbb{R}})$ ebenfalls ungerade, aus Eigenschaft (a) oben folgt also $\alpha \in \mathbb{R}$, und insgesamt sehen wir $K^H = \mathbb{R}$, also $d = 1$. (Alternativ könnte man, statt alle $\alpha \in K^H$ zu betrachten, ein primitives Element der Erweiterung $K^H/\mathbb{R}$ hernehmen.)

Es folgt, dass $K/\mathbb{C}$ eine Galois-Erweiterung ist, deren Grad eine Potenz von 2 ist. Also ist ihre Galois-Gruppe auflösbar (Satz 2.76), und es gibt eine Untergruppe vom Index 2 (Lemma 2.64). Diese entspricht einer quadratischen Erweiterung von $\mathbb{C}$, aber wir wissen wegen Eigenschaft (b), dass es eine solche Erweiterung nicht gibt. □

5.6. Die Galois-Gruppe einer Gleichung

In diesem Abschnitt definieren wir den Begriff der *Galois-Gruppe einer Gleichung* (bzw. *eines Polynoms*), und zwar ist dies einfach die Galois-Gruppe eines Zerfällungskörpers des gegebenen Polynoms. Speziell, wenn man sich für die Nullstellen eines bestimmten Polynoms interessiert, dann ist dies eine nützliche Sprechweise. Historisch gesehen ist sie wesentlich näher an der Sichtweise, die in den Arbeiten von Galois verwendet wird. Für den allgemeinen Aufbau und die Flexibilität der Theorie hat sich aber bewährt, den Begriff des Körperautomorphismus in den Vordergrund zu stellen, wie es als Erster Richard Dedekind[2] (1831–1916) getan hat.

DEFINITION 5.59. Sei K ein Körper und $f \in K[X]$ ein separables Polynom. Sei L ein Zerfällungskörper von f über K. Dann ist die Erweiterung L/K galoissch, ihre Galois-Gruppe hängt nicht von der Wahl von L ab und heißt auch die *Galois-Gruppe der Gleichung* $f(x) = 0$. ⊣

[2] https://de.wikipedia.org/wiki/Richard_Dedekind

Die Unabhängigkeit von der Wahl des Zerfällungskörpers folgt daraus, dass je zwei Zerfällungskörper über K isomorph sind, wie wir in Satz 5.3 gezeigt haben.

SATZ 5.60. *Sei K ein Körper, $\overline{K}$ ein algebraischer Abschluss und $f \in K[X]$ ein separables Polynom vom Grad $n \in \mathbb{N}$ mit Zerfällungskörper $L \subseteq \overline{K}$. Sei $G = \mathrm{Gal}(L/K)$ die Galois-Gruppe der Gleichung $f(x) = 0$. Seien $\alpha_1, \ldots, \alpha_n \in L$ die (nach Voraussetzung paarweise verschiedenen) Nullstellen von f in $\overline{K}$.*

Jedes Element von G induziert dann eine Permutation der α_i, und wir erhalten so einen injektiven Gruppenhomomorphismus $G \to S_n$. Insbesondere gilt $\#G \mid n!$.

Das Polynom ist genau dann irreduzibel in $K[X]$, wenn G transitiv auf der Menge $\{\alpha_1, \ldots, \alpha_n\}$ operiert.

BEWEIS. Dass jedes Element von G die Nullstellen von f permutiert, ist klar, denn für $\sigma \in G$ und jede Nullstelle α von f gilt $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$, wobei wir hier wieder σ für den Ringautomorphismus $L[X] \to L[X]$ schreiben, der dadurch gegeben ist, σ auf alle Koeffizienten anzuwenden. Vergleiche Satz 4.25, wo dasselbe Argument verwendet wird.

Wenn f irreduzibel ist, dann ist es das Minimalpolynom der Elemente α_i (insbesondere haben diese alle dasselbe Minimalpolynom). Aus dem schon zitierten Satz 4.25 folgt, dass es für alle i, j einen K-Homomorphismus $K(\alpha_i) \to L$ mit $\alpha_i \mapsto \alpha_j$ gibt, und diesen können wir wegen der Normalität von L über K fortsetzen zu einem K-Homomorphismus $L \to L$, also einem Element von $\mathrm{Gal}(L/K)$.

Ist andererseits f nicht irreduzibel in $K[X]$ und sind α_i und α_j Nullstellen von zwei verschiedenen Teilern von f in $K[X]$, dann kann es keinen K-Homomorphismus geben, der α_i auf α_j abbildet, weil α_i nur auf eine Nullstelle von $\mathrm{minpol}_{\alpha_i, K}$ abgebildet werden kann. □

> L'algèbre est généreuse, elle donne souvent plus qu'on lui demande.
>
> J. d'Alembert
>
> Auf Deutsch etwa: Die Algebra ist großzügig, sie gibt oft mehr, als man von ihr verlangt.

Wir wollen noch die *Diskriminante* eines Polynoms definieren.

DEFINITION 5.61. Seien K ein Körper, $f \in K[X]$ ein normiertes Polynom, L/K ein Zerfällungskörper von f und $f = \prod_{i=1}^{n}(X - \alpha_i)$ mit $\alpha_i \in L$ die Zerlegung von f in Linearfaktoren in $L[X]$. Dann nennt man

$$\Delta(f) = \prod_{i<j}(\alpha_j - \alpha_i)^2$$

die *Diskriminante* des Polynoms f. ⊣

Man findet in der Literatur teilweise auch die Definition $\prod_{i \neq j}(\alpha_j - \alpha_i)$, die aber mit unserer bis auf das Vorzeichen (also gegebenenfalls einen Faktor -1) übereinstimmt. Es gilt dann der folgende Satz.

SATZ 5.62. *Sei f wie in der Definition.*

(1) *Es gilt genau dann $\Delta(f) = 0$, wenn f in L eine mehrfache Nullstelle hat.*
(2) *Es gilt $\Delta(f) \in K$.*

BEWEIS. Teil (1) ist offensichtlich, und wenn f eine mehrfache Nullstelle hat, dann ist natürlich $\Delta(f) = 0 \in K$. Sonst ist f separabel und damit L/K eine Galois-Erweiterung. Dann folgt $\Delta(f) \in K$, weil jeder K-Automorphismus $L \to L$ die Nullstellenmenge von f auf sich abbildet (Lemma 5.2), und daher das Element $\Delta(f)$ fixiert. Also liegt $\Delta(f)$ im Fixkörper K von L unter $\mathrm{Gal}(L/K)$. □

BEISPIEL 5.63. (1) Hat f Grad 0 oder 1, so ist $\Delta(f) = 1$.

(2) Hat $f = X^2 + pX + q$ Grad 2, so sind die Nullstellen von f die Elemente

$$\alpha_1 = \frac{-p + \sqrt{p^2 - 4q}}{2}, \quad \alpha_2 = \frac{-p - \sqrt{p^2 - 4q}}{2}$$

wobei wir hier eine der beiden Quadratwurzeln von $p^2 - 4q$ in L willkürlich wählen und mit $\sqrt{p^2 - 4q}$ bezeichnen. Die folgende Berechnung ist von dieser Wahl unabhängig. Wir sehen, dass

$$\Delta(f) = (\alpha_1 - \alpha_2)^2 = p^2 - 4q$$

gilt.

(3) Ist f ein Polynom vom Grad 3 von der speziellen Form $f = X^3 + aX + b$, $a, b \in K$, so gilt

$$\Delta(f) = -4a^3 - 27b^2.$$

Dies kann man (wenn man die Formel erstmal hat) leicht nachrechnen, indem man a und b in Termen der Nullstellen von f ausdrückt.

◊

Man kann zeigen, dass sich wie in den obigen Beispielen für jedes Polynom die Diskriminante durch einen Polynomausdruck in den Koeffizienten von f ausdrücken lässt, der nur vom Grad von f abhängt. Wenn man diese Formel kennt, wie zum Beispiel die Formel $\Delta(f) = -4a^3 - 27b^2$ im obigen Beispiel, Teil (3), kann man also überprüfen, ob f (in irgendeinem Erweiterungskörper) *mehrfache* Nullstellen hat, ohne diese Nullstellen zu kennen.

Sei in der Situation und mit der Notation von Definition 5.61 nun f separabel und

$$\delta = \prod_{i<j} (\alpha_j - \alpha_i).$$

Offenbar gilt $\delta^2 = \Delta(f)$, also ist δ eine Quadratwurzel von $\Delta(f)$ (in L). Jedes Element $\sigma \in \mathrm{Gal}(L/K)$ induziert eine Permutation der Nullstellenmenge $V(f, L)$, die wir wieder mit σ bezeichnen, vergleiche Satz 5.60. Wir erhalten so einen injektiven Gruppenhomomorphismus $\mathrm{Gal}(L/K) \to S_n$, $n = \deg(f)$. Es gilt dann $\sigma(\delta) = \mathrm{sgn}(\sigma)\delta$, wie man an der Interpretation des Signums einer Permutation an der Anzahl ihrer Fehlstände sieht. Damit erhalten wir den folgenden Satz.

SATZ 5.64. *Seien K ein Körper, $f \in K[X]$ ein separables normiertes Polynom vom Grad n, L/K ein Zerfällungskörper von f und* $\mathrm{sgn}\colon \mathrm{Gal}(L/K) \to \{1, -1\}$ *der Gruppenhomomorphismus, der als Verkettung des oben beschriebenen Homomorphismus* $\mathrm{Gal}(L/K) \to S_n$ *und des Signumshomomorphismus besteht. (Die Abbildung* sgn *ist unabhängig von der Nummerierung der Nullstellen von f.)*

Sei $H \subseteq \mathrm{Gal}(L/K)$ die Untergruppe aller Elemente $\sigma \in \mathrm{Gal}(L/K)$ mit $\mathrm{sgn}(\sigma) = 1$.

Dann gilt $L^H = K(\sqrt{\Delta(f)})$, wobei $\sqrt{\Delta(f)}$ eine Quadratwurzel der Diskriminante von f in L ist.

BEWEIS. Im Grunde ist schon fast alles gesagt: Wir können mit der obigen Situation $\sqrt{\Delta(f)} = \delta$ wählen, und dann sind die Elemente von H genau die Automorphismen von $\mathrm{Gal}(L/K)$, die δ festhalten. Weil entweder $H = \mathrm{Gal}(L/K)$ gilt, oder H Index 2 in $\mathrm{Gal}(L/K)$ hat, ist L^H gleich K oder hat Grad 2 über K (und wird dann von irgendeinem beliebigen Element aus $L^H \setminus K$ erzeugt). □

5.7. Wie untersucht man einen Körper? *

Im Grunde lässt sich auf die Frage in der Überschrift keine sinnvolle umfassende Antwort geben, aber es gibt einige Klassen von Körpern, die besonders wichtig bzw. interessant sind, und für deren Untersuchung entsprechende Methoden entwickelt wurden.

Eine wichtige und ganz grundlegende Eigenschaft eines Körpers ist seine *Charakteristik*, bzw. äquivalent die Isomorphieklasse seines Primkörpers. In vielerlei Hinsicht verhalten sich Körper von Charakteristik 0 anders als solche von positiver Charakteristik.

Eine »Klassifikation« von Körpern ist nur in sehr speziellen Fällen möglich.

Oft interessiert man sich für die Lösbarkeit von Polynomgleichungen (auch in mehreren Variablen) in Körpern, ein Stichwort ist der Begriff des C_k-Körpers[3].

In der *Algebraischen Zahlentheorie* werden *Zahlkörper* untersucht, d.h. endliche Erweiterungskörper K des Körpers $\mathbb{Q}$ der rationalen Zahlen. Zum Beispiel möchte man die Struktur der (unendlichen) Galois-Gruppe $\mathrm{Gal}(\overline{K}/K)$ verstehen, wobei $\overline{K}$ ein algebraischer Abschluss von K ist. Auch für $K = \mathbb{Q}$ ist dies ein schwieriges Problem, das Gegenstand aktueller Forschung ist. Natürlich muss man hier geeignet präzisieren, das man darunter versteht, die »Struktur dieser Gruppe zu verstehen«. Eine solche Präzisierung erfolgt (im Prinzip) im Rahmen des Langlands-Programms[4].

Ein wichtiges Hilfsmittel für das Studium eines Zahlkörpers K ist die Betrachtung des sogenannten *Rings der ganzen Zahlen* von K, das heißt des Rings

$$\mathcal{O}_K = \{x \in K;\ \mathrm{minpol}_{x,\mathbb{Q}} \in \mathbb{Z}[X]\}.$$

(Es ist nicht trivial, dass dies ein Unterring von K ist.) Zum Beispiel ist eine interessante Eigenschaft des Körpers K, ob dieser Ring faktoriell ist.

ERGÄNZUNG 5.65 (Galois-Theorie in anderen Kontexten). Die Grundidee der Galois-Theorie (in der heutigen Formulierung), gewisse Strukturen durch ihre Automorphismengruppen zu beschreiben, ist ein wichtiges Prinzip, das auch in anderen Bereichen der Mathematik eine Rolle spielt. Speziell zum Beispiel in der »Überlagerungstheorie« von Riemannschen Flächen, algebraischen Kurven oder höherdimensionalen komplexen Mannigfaltigkeiten oder algebraischen Varietäten. Siehe [**Soe**] 8.2 für weitere Bemerkungen in diese Richtung.

Eine andere analoge Theorie ist die sogenannte differentielle Galois-Theorie, eine algebraische Theorie zur Untersuchung gewisser Differentialgleichungen, in der statt Körpern und Körpererweiterungen wie in der klassischen Theorie Körper (von gewissen Funktionen) zusammen mit einer Ableitungsfunktion und Erweiterungen von solchen untersucht werden.

□ Ergänzung 5.65

[3] https://en.wikipedia.org/wiki/Quasi-algebraically_closed_field#Ck_fields
[4] https://de.wikipedia.org/wiki/Langlands-Programm

KAPITEL 6

Anwendungen der Galois-Theorie

6.1. Lineare Unabhängigkeit von Charakteren *

Ist G eine Gruppe und K ein Körper, so nennt man einen Gruppenhomomorphismus $G \to K^\times$ auch einen *(multiplikativen) Charakter von G mit Werten in K* (auch wenn die Werte in der Einheitengruppe $K^\times$ liegen!).

SATZ 6.1. *Sei G eine Gruppe, sei K ein Körper und seien $\sigma_1, \dots, \sigma_r \colon G \to K^\times$ paarweise verschiedene Charaktere.*

Dann sind $\sigma_1, \dots, \sigma_r$ als Elemente des K-Vektorraums $\mathrm{Abb}(G, K)$ *linear unabhängig, das heißt: Sind $a_1, \dots, a_r \in K$ mit*

$$\sum_{i=1}^{r} a_i \sigma_i(g) = 0 \in K \quad \textit{für alle } g \in G,$$

so gilt $a_1 = \cdots = a_r = 0$.

BEWEIS. Angenommen, der Satz wäre falsch. Wir betrachten eine Gleichung $\sum_{i=1}^{r} a_i \sigma_i = 0$ mit $a_i \in K^\times$ mit minimalem r. Weil ein Charakter Werte in $K^\times$ hat, kann ein Charakter nicht die Nullabbildung sein, also gilt $r > 1$.

Es gilt also

$$\sum_{i=1}^{r} a_i \sigma_i(g) = 0$$

für alle $g \in G$. Wir können auch statt eines Elements g ein Produkt gh einsetzen. Aus der Multiplikativität der σ_i folgt dann

$$\sum_{i=1}^{r} a_i \sigma_i(g) \sigma_i(h) = 0$$

für alle $g, h \in G$. Weil $\sigma_1 \neq \sigma_2$ gilt, gibt es ein Element $h \in G$ mit $\sigma_1(h) \neq \sigma_2(h)$, das wir nun fixieren wollen.

Damit haben wir

$$\sum_{i=1}^{r} a_i \sigma_i(h) \sigma_i = 0$$

und andererseits, wenn wir die ursprüngliche Relation mit $\sigma_1(h)$ multiplizieren,

$$\sum_{i=1}^{r} a_i \sigma_1(h) \sigma_i = 0.$$

Ziehen wir diese Gleichungen voneinander ab, erhalten wir mit

$$\sum_{i=2}^{r} a_i (\sigma_i(h) - \sigma_1(h)) \sigma_i = 0$$

eine Relation, die weniger als r Summanden hat, aber wegen $\sigma_2(h) \neq \sigma_1(h)$ nicht trivial ist. Das ist ein Widerspruch zur Wahl von r als der Länge einer minimalen solchen Relation. □

Ist L ein Körper, so erhalten wir daraus, indem wir $G = L^\times$ setzen und ausnutzen, dass jeder Körperhomomorphismus $L \to L$ sich zu einem Gruppenhomomorphismus $L^\times \to L^\times$ einschränkt, das folgende Korollar. Denn aus der linearen Unabhängigkeit in $\mathrm{Abb}(L^\times, L)$ folgt erst recht die in $\mathrm{Abb}(L, L)$.

KOROLLAR 6.2. *Sei L ein Körper und seien $\sigma_1, \dots, \sigma_r \in \mathrm{Aut}(L)$ paarweise verschiedene Automorphismen von L. Dann sind $\sigma_1, \dots, \sigma_r$ als Elemente des L-Vektorraums $\mathrm{Abb}(L, L)$ linear unabhängig.*

Eine relative einfache Folgerung daraus ist das folgende wichtige Ergebnis der »fortgeschrittenen« Galois-Theorie. Eine Basis der dort angegebenen Form nennt man eine *Normalbasis* der Galois-Erweiterung L/K.

SATZ 6.3. *Sei L/K eine Galois-Erweiterung vom Grad n mit Galois-Gruppe $G = \{\sigma_1, \dots, \sigma_n\}$. Dann existiert ein Element $\alpha \in L$, derart dass die Elemente $\sigma_1(\alpha), \dots, \sigma_n(\alpha)$ eine Basis des K-Vektorraums L bilden.*

Für einen Beweis und eine ausführlichere Diskussion siehe [**Lo**] 12.3 oder [**JS**] Satz VI.3.5.

BEMERKUNG 6.4. (1) (Die Gruppenalgebra) Sei G eine endliche Gruppe und sei K ein Körper. Wir bezeichnen mit $K[G]$ die *Gruppenalgebra* von G über K. Dies ist eine Algebra über K in dem Sinne, dass $K[G]$ ein K-Vektorraum ist, der mit der Vektorraumaddition und einer Multiplikation $K[G] \times K[G] \to K[G]$ ein Ring ist, und so dass die Multiplikation mit Skalaren aus K mit der Ringmultiplikation kompatibel ist. Im allgemeinen ist dabei $K[G]$ ein nicht-kommutativer Ring (so dass diese Situation durch den von uns früher eingeführten Begriff einer K-Algebra nicht abgedeckt wird). Wir können diese Struktur auch so beschreiben, dass $K[G]$ ein Ring ist und die Abbildung $K \to K[G], \alpha \mapsto \alpha \cdot 1$ ein Ringhomomorphismus ist, so dass die Elemente im Bild mit allen Elementen aus $K[G]$ kommutieren.

Wir konstruieren $K[G]$ wie folgt: Die Elemente von G bilden eine K-Vektorraumbasis von $K[G]$, wir können also jedes Element von $K[G]$ in der Form $\sum_{g\in G} \alpha_g [g]$ mit eindeutig bestimmten Koeffizienten $\alpha_g \in K$ schreiben. (Wir schreiben hier $[g]$ statt g für das durch $g \in G$ gegebene Basiselement, um den Unterschied in der Notation sichtbar zu machen, ob g als Element von G oder als Element von $K[G]$ aufgefasst wird. Hier sind auch andere Schreibweisen üblich; oft schreibt man einfach in beiden Situationen g.) Die Ringstruktur ist durch die folgende Multiplikation gegeben. Wir setzen

$$[g] \cdot [h] := [gh]$$

und setzen dies bilinear fort, das heißt

$$\left(\sum_{g\in G} \alpha_g [g]\right) \cdot \left(\sum_{g\in G} \beta_g [g]\right) = \sum_{g\in G} \left(\sum_{h,h'\in G,\, hh'=g} \alpha_h \beta_{h'}\right) [g].$$

Es ist nicht schwer zu überprüfen, dass es sich hierbei um einen (im allgemeinen nicht-kommutativen) Ring handelt. Wenn G kommutativ ist, dann ist auch $K[G]$ kommutativ (und umgekehrt); vergleiche Bemerkung 3.32.

(2) Sei nun L/K eine endliche Galois-Erweiterung mit Galois-Gruppe G. Wir können dann L als »(Links-)Modul« über der Algebra $K[G]$ betrachten (vergleiche Abschnitt LA2.18.7.1), d.h. wir haben eine Skalarmultiplikation

$$K[G] \times L \longrightarrow L, \quad \left(\sum_{\sigma\in G} a_\sigma [\sigma]\right) \cdot \alpha = \sum_{\sigma\in G} a_\sigma \sigma(\alpha).$$

Ist $\alpha \in L$ wie im Satz von der Existenz einer Normalbasis, dann ist die Abbildung

$$\Phi\colon K[G] \longrightarrow L, \quad \left(\sum_{\sigma\in G} a_\sigma [\sigma]\right) \mapsto \sum_{\sigma\in G} a_\sigma \sigma(\alpha),$$

ein Isomorphismus von $K[G]$-Moduln. Umgekehrt gilt: Ist für $\alpha \in L$ die durch die obige Vorschrift gegebene Abbildung bijektiv, dann bildet die Familie $(\sigma(\alpha))_{\sigma\in G}$ eine K-Basis von L.

$\Diamond$

6.2. Norm und Spur, Hilbert 90 *

Sei L/K eine endliche Körpererweiterung und sei $\alpha \in L$. Das Minimalpolynom $\operatorname{minpol}_{\alpha,K}$ ist, wie man leicht sieht, genau das Minimalpolynom des K-Vektorraum-Endomorphismus $m_\alpha\colon L \to L, x \mapsto \alpha x$. Entsprechend kann man andere Begriffe aus der Linearen Algebra »in die Algebra übertragen« und speziell im Kontext von Körpererweiterungen untersuchen. In diesem Abschnitt wollen wir das mit der Spur und der Determinante eines Endomorphismus tun. Natürlich gelten die Eigenschaften aus der Linearen Algebra insbesondere in dieser speziellen Situation, aber man kann noch etwas mehr sagen (für das Minimalpolynom haben wir beispielsweise gesehen, dass ein Minimalpolynom im Sinne der Algebra immer irreduzibel ist).

Wir definieren unten die *Spur* $\operatorname{Spur}_{L/K}(\alpha)$ von α als die Spur des Endomorphismus m_α und die *Norm* $N_{L/K}(\alpha)$ als die Determinante von m_α. Der Begriff »Determinante« wird also durch dem Term »Norm« ersetzt (im speziellen Fall der Erweiterung $\mathbb{C}/\mathbb{R}$ gilt $N_{\mathbb{C}/\mathbb{R}}(z) = z\bar{z} = |z|^2$, es gibt also einen (schwachen) Zusammenhang zur Norm des Vektors $z \in \mathbb{C} = \mathbb{R}^2$), aber darüberhinaus haben diese beiden mathematischen Bedeutungen des Worts *Norm* nicht viel miteinander zu tun.

Einfache konkrete Anwendungen von Spur und Norm sind (Beispiel 6.12), dass man die Spur manchmal benutzen kann, um zu zeigen, dass gewisse Elemente (eines algebraischen Abschlusses von K) nicht in einem gegebenen Erweiterungkörper L eines Körpers K liegen, und mit der Normabbildung manchmal zeigen kann, dass ein Element $\alpha \in L$ keine n-te Potenz in L ist. Vor allem sind Norm und Spur aber nützliche technische Hilfsmittel für strukturelle Untersuchungen von endlichen Körpererweiterungen. Siehe die Sätze am Ende dieses Abschnitts.

Definition 6.5. Sei L/K eine endliche Körpererweiterung. Wir betrachten L als K-Vektorraum und für jedes Element $\alpha \in L$ die Multiplikation mit α als Element $m_\alpha \in \operatorname{End}_K(L)$. Dann heißt $N_{L/K}(\alpha) := \det(\alpha)$ die *Norm* und $\operatorname{Spur}_{L/K}(\alpha) := \operatorname{Spur}(m_\alpha)$ die Spur von α.

Die *Normabbildung* $N_{L/K}\colon L \to K$ ist multiplikativ, d.h. es gilt $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta)$ für alle $\alpha, \beta \in L$. Insbesondere erhalten wir einen Gruppenhomomorphismus

$$N_{L/K}\colon L^\times \to K^\times.$$

Die Spur ist ein K-Vektorraumhomomorphismus

$$\operatorname{Spur}_{L/K}\colon L \to K,$$

die sogenannte *Spurabbildung* der Erweiterung L/K. $\dashv$

Beispiel 6.6. (1) Sei L/K eine endliche Körpererweiterung, $n = [L : K]$. Für $a \in K$ gilt dann $\operatorname{Spur}_{L/K}(a) = na$, $N_{L/K}(a) = a^n$.

(2) Sei L/K eine endliche Körpererweiterung, $n = [L : K]$, und sei $\alpha \in L$ mit $L = K(\alpha)$. Dann das Minimalpolynom der linearen Abbildung M_α stimmt mit dem charakteristischen Polynom von m_α überein und ist gleich $\operatorname{minpol}_{\alpha,K}$. Schreiben wir $\operatorname{minpol}_{\alpha,K} = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, so folgt $\operatorname{Spur}_{K(\alpha)/K}(\alpha) = -a_{n-1}$ und $N_{K(\alpha)/K}(\alpha) = (-1)^n a_0$.

Die Elemente $1, \alpha, \ldots, \alpha^{n-1}$ bilden eine Basis von L als K-Vektorraum, und die Matrix, die den Endomorphismus m_α bezüglich dieser Basis beschreibt, ist die Begleitmatrix von $\operatorname{minpol}_{\alpha,K}$, Definition LA2.16.18.

◊

SATZ 6.7 (Transitivität von Norm und Spur). *Seien L/E und E/K endliche Körpererweiterungen.*

(1) *Es gilt* $\operatorname{Spur}_{L/K} = \operatorname{Spur}_{E/K} \circ \operatorname{Spur}_{L/E}$.

(2) *Es gilt* $N_{L/K} = N_{E/K} \circ N_{L/E}$.

BEWEIS. Dies kann man mit Methoden der linearen Algebra »nachrechnen« (aber es empfiehlt sich, die Sache »geschickt« anzugehen). Siehe [**Sch**] oder [**St**] 0BIE[1] für zwei etwas unterschiedliche Möglichkeiten. □

In [**Bo-A**], Abschnitt 4.7, wird der obige Satz mit noch einer anderen Methode bewiesen.

SATZ 6.8. *Sei L/K eine endliche separable Körpererweiterung. Sei $\overline{K}$ ein algebraischer Abschluss von K. Für alle $\alpha \in L$ gilt*

$$N_{L/K}(\alpha) = \prod_{\sigma \in \operatorname{Hom}_K(L,\overline{K})} \sigma(\alpha).$$

BEWEISSKIZZE. Sei $d = [K(\alpha) : K]$ und $\operatorname{minpol}_{\alpha,K} = \sum_{i=0}^{d} a_i X^i$. Nach Satz 6.7 und Beispiel 6.6 (2) ist $N_{L/K}(\alpha) = N_{L/K(\alpha)}(N_{K(\alpha)/K}(\alpha) = ((-1)^d a_0)^{\frac{n}{d}}$. Andererseits ist wegen der Separabilität $(-1)^d a_0$ genau das Produkt aller $\sigma(\alpha)$ für $\sigma \in \operatorname{Hom}_K(K(\alpha), \overline{K})$. Jeden dieser Homomorphismen können wir auf $\frac{n}{d}$ verschiedene Arten zu einem Homomorphismus $L \to \overline{K}$ fortsetzen (vergleiche den Beweis von Lemma 5.19), die natürlich α jeweils auf dasselbe Element abbilden. Daraus folgt die Behauptung. □

SATZ 6.9. *Sei L/K eine endliche Körpererweiterung. Sei $\overline{K}$ ein algebraischer Abschluss von K. Für alle $\alpha \in L$ gilt*

$$\operatorname{Spur}_{L/K}(\alpha) = \sum_{\sigma \in \operatorname{Hom}_K(L,\overline{K})} \sigma(\alpha).$$

BEWEIS. Man kann ganz analog zum vorherigen Satz argumentieren. □

BEMERKUNG 6.10. Man kann diese Beschreibungen auch (mit nur wenig Mehraufwand) auf den Fall nicht notwendig separabler Körpererweiterungen verallgemeinern, siehe zum Beispiel [**Bo-A**] Abschnitt 4.7. ◊

Als direkte Folgerung der Beschreibung von Spur und Norm in Termen der K-Homomorphismen $L \to \overline{K}$ erhalten wir, dass Spur und Norm einer Galois-Erweiterung »Galois-invariant« sind, das heißt:

KOROLLAR 6.11. *Sei L/K eine endliche Galois-Erweiterung. Für alle $\alpha \in L$ und $\sigma \in \operatorname{Gal}(L/K)$ gilt* $\operatorname{Spur}_{L/K}(\alpha) = \operatorname{Spur}_{L/K}(\sigma(\alpha))$ *und* $N_{L/K}(\alpha) = N_{L/K}(\sigma(\alpha))$.

BEISPIEL 6.12. Norm und Spur kann man manchmal benutzen, um konkrete Aussagen der folgenden Form zu beweisen.

[1] https://stacks.math.columbia.edu/tag/0BIE

(1) Es gilt $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2}) =: K$. Denn nehmen wir an, es gäbe $a, b, c \in \mathbb{Q}$ mit

$$\sqrt[3]{3} = a + b\sqrt[3]{2} + c\sqrt[3]{4}.$$

Man könnte versuchen, direkt vorzugehen, indem man beide Seiten zur dritten Potenz erhebt und einen Koeffizientenvergleich durchführt. Es ist aber nicht offensichtlich, dass dadurch gegebene (nicht-lineare!) Gleichungssystem für a, b, b keine Lösung besitzt.

Einfacher geht es wie folgt: Aus Gradgründen wäre $\mathbb{Q}(\sqrt[3]{3}) = \mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{4})$. An den jeweiligen Minimalpolynomen lesen wir ab, dass

$$\mathrm{Spur}_{K/\mathbb{Q}}(\sqrt[3]{3}) = \mathrm{Spur}_{K/\mathbb{Q}}(\sqrt[3]{2}) = \mathrm{Spur}_{K/\mathbb{Q}}(\sqrt[3]{4}) = 0.$$

Damit folg aus der obigen Gleichung wegen der Linearität der Spur, dass $a = 0$ ist.

Durch Multiplikation der Gleichung mit $\sqrt[3]{2}$ erhalten wir

$$\sqrt[3]{6} = b\sqrt[3]{4} + 2c.$$

Wie oben sehen wir, dass $\mathrm{Spur}_{K/\mathbb{Q}}(\sqrt[3]{6}) = 0$ ist, und wir erhalten $c = 0$.

Dann wäre aber $\sqrt[3]{3} = b\sqrt[3]{2}$ für ein $b \in \mathbb{Q}$, und es ist offensichtlich, dass es eine solche Zahl b nicht gibt.

(2) Das Element $\alpha = 1 - 5\sqrt[3]{2} + (\sqrt[3]{2})^2$ ist kein Quadrat in $\mathbb{Q}(\sqrt[3]{2})$. Indem man für die Basis $1, \sqrt[3]{2}, \sqrt[3]{4}$ die Matrix der Abbildung m_α aufstellt und deren Determinante ausrechnet, sieht man, dass $N_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(\alpha) = 277$ gilt. Weil dieses Element kein Quadrat in $\mathbb{Q}^\times$ ist, folgt die Behauptung.

◊

SATZ 6.13. *Sei L/K eine endliche Körpererweiterung. Die Spurabbildung $\mathrm{Spur}_{L/K}$ ist genau dann die Nullabbildung, wenn die Erweiterung L/K inseparabel ist.*

BEWEIS. Es ist leicht zu sehen, dass die Spurabbildung einer rein inseparablen Erweiterung die Nullabbildung ist. Mit Satz 6.7 und Satz 5.33 folgt daraus, dass dies für jede inseparable Erweiterung gilt.

Ist die Erweiterung separabel, so ist $\mathrm{Spur}_{L/K} = \sigma_1 + \cdots + \sigma_n$ nach Satz 6.9, wobei wir mit σ_i die K-Homomorphismen $L \to \overline{K}$ bezeichnen, $i = 1, \ldots, n = [L : K]$. Satz 6.1 über die lineare Unabhängigkeit von Charakteren impliziert, dass diese Summe (gebildet in $\mathrm{Abb}(L, \overline{K})$) nicht verschwindet. □

Genauer gilt im separablen Fall der folgende Satz.

SATZ 6.14. *Sei L/K eine separable endliche Körpererweiterung. Dann ist die Abbildung*

$$L \times L \to K, \quad (x, y) \mapsto \mathrm{Spur}_{L/K}(xy),$$

eine nicht-ausgeartete symmetrische Bilinearform auf dem K-Vektorraum L.

BEWEIS. Es ist klar, dass es sich hier um eine symmetrische Bilinearform handelt. Um zu zeigen, dass sie nicht ausgeartet ist, müssen wir zeigen, dass für jedes $x \in L^\times$ die Abbildung $y \mapsto \mathrm{Spur}_{L/K}(xy)$ (ein Element des Dualraums $L^\vee$ von L als K-Vektorraum) nicht die Nullabbildung ist.

Die ist aber klar, denn sonst wäre offensichtlich die Abbildung $\mathrm{Spur}_{L/K}$ selbst die Nullabbildung, und das haben wir im vorherigen Satz bereits ausgeschlossen. □

BEMERKUNG 6.15 (Die Diskriminante einer separablen Erweiterung). Sei L/K eine separable endliche Körpererweiterung vom Grad n, sei $\overline{K}$ ein algebraischer Abschluss von K, sei $\mathrm{Hom}_K(L,\overline{K}) = \{\sigma_1, \ldots, \sigma_n\}$ und sei $\alpha_1, \ldots, \alpha_n$ eine K-Vektorraum-Basis von L.

Das Element

$$D_{L/K} = \det((\mathrm{Spur}_{L/K}(\alpha_i\alpha_j)_{i,j})) \in K^\times$$

heißt die *Diskriminante* der Erweiterung L/K. Es handelt sich also genau um die Diskriminante der Strukturmatrix der durch die Spur gegebenen Bilinearform bezüglich der Basis $(\alpha_1, \ldots, \alpha_n)$. Aus der Basiswechselformel für die Strukturmatrix einer Bilinearform folgt, dass sich diese Determinante bei einem Wechsel der Basis um ein Quadrat in $K^\times$ ändert. Das oben definierte Element $D_{L/K}$ ist also abhängig von der Wahl der Basis, seine Restklasse in $K^\times/(K^\times)^2$ ist aber davon unabhängig und heißt auch oft die Diskriminante von L/K.

Schreiben wir $A = (\sigma_i(\alpha_j))_{i,j}$ so ist A^tA genau die Matrix in der obigen Definition und daher $D_{L/K} = \det(A)^2$.

Betrachten wir speziell den Fall $L = K(\alpha)$. Wir können als K-Basis von L dann die Elemente $1, \alpha, \ldots, \alpha^{n-1}$ wählen und die Matrix A hat dann die Form einer Vandermonde-Matrix. Weil die Elemente $\sigma_i(\alpha)$ gerade die Nullstellen des Minimalpolynoms $f := \mathrm{minpol}_{\alpha,K}$ von α über K sind, ist $D_{K(\alpha)/K}$ dann genau die Diskriminante von f (Definition 5.61).

Wenn wir mit $\alpha_1, \ldots, \alpha_n$ die Nullstellen von f und mit f' wie üblich die formale Ableitung von f bezeichnen, gilt in dieser Situation die folgende Formel, wie man unschwer nachrechnet:

$$D_{K(\alpha)/K} = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} f'(\alpha_i) = N_{K(\alpha/K}(f'(\alpha)).$$

Ist zum Beispiel $K = \mathbb{Q}$, p eine ungerade Primzahl und ζ eine primitive p-te Einheitswurzel, so ist $f = X^{p-1} + \cdots + X + 1$ und $D_{\mathbb{Q}(\zeta)/\mathbb{Q}} = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{p-1} f'(\zeta^i) = (-1)^{\frac{p(p-1)}{2}} p^{p-2}$. (Vergleiche die Hausaufgaben.)

Ein anderer Fall, in dem man leicht konkrete Formeln angeben kann, ist der Fall, dass das Minimalpolynom von α die spezielle Form $\mathrm{minpol}_{\alpha,K} = X^n + aX + b$ hat. ◊

Der folgende Satz beschreibt im Fall einer zyklischen Erweiterung L/K, welche Elemente $\alpha \in L$ die Norm $N_{L/K}(\alpha) = 1$ haben. Genauer sagt der Satz, dass dies nur in dem »offensichtlichen« Fall $\alpha = \beta/\sigma(\beta)$ für ein $\beta \in L$ und $\sigma \in \mathrm{Gal}(L/K)$ gilt. Dass diese Elemente tatsächlich Norm 1 haben, folgt direkt aus Korollar 6.11 und aus der Multiplikativität der Norm. Es genügt dann sogar, für σ einen Erzeuger der Galois-Gruppe zu fixieren. Der Satz wird meistens als »Hilberts Satz 90« bezeichnet, weil er in dem berühmten Zahlbericht [**Hi**] von D. Hilbert die Nummer 90 trägt. Es gibt verschiedene Verallgemeinerungen des Satzes, siehe zum Beispiel [**Bo-A**] Abschnitt 4.8.

THEOREM 6.16 (Satz 90 von Hilbert). *Sei L/K eine endliche zyklische Galois-Erweiterung, sei σ ein Erzeuger der Galois-Gruppe $\mathrm{Gal}(L/K)$ und sei $\alpha \in L$. Dann sind äquivalent:*

(i) $N_{L/K}(\alpha) = 1$,

(ii) *es gibt $\beta \in L$ mit $\alpha = \frac{\beta}{\sigma(\beta)}$.*

BEWEIS. Dass (i) aus (ii) folgt, ist einfach und haben wir oben bereits begründet. Sei nun $\alpha \in L$ mit $N_{L/K}(\alpha) = 1$. Wir schreiben $n = [L : K]$. Wegen der linearen Unabhängigkeit der Charaktere $\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ existiert für alle $\alpha_0, \ldots, \alpha_{n-1} \in L$ ein Element $\gamma \in L$ mit

$$\beta := \alpha_0\gamma + \alpha_1\sigma(\gamma) + \cdots + \alpha_{n-1}\sigma^{n-1}(\gamma) \neq 0.$$

Satz 90. Jede ganze oder gebrochene Zahl A in K, deren Relativnorm in Bezug auf k gleich 1 ist, wird die symbolische $(1-S)$te Potenz einer gewissen ganzen Zahl B des Körpers K.

Beweis. Es sei x eine Veränderliche und Θ eine den Körper K bestimmende Zahl; dann setze man:

$$A_x = \frac{x+\Theta}{x+S\Theta} A = (x+\Theta)^{1-S} A$$

und

$$B_x = 1 + A_x^1 + A_x^{1+S} + A_x^{1+S+S^2} + \cdots + A_x^{1+S+S^2+\cdots+S^{l-2}}.$$

Berücksichtigt man, dass nach Voraussetzung $A^{1+S+\cdots+S^{l-1}} = 1$ ist und folglich auch $A_x^{1+S+\cdots+S^{l-1}} = 1$ wird, so ergiebt sich $B_x^{1-S} = A_x$. Da B_x eine rationale Function von x ist, welche, wie leicht ersichtlich, nicht identisch für alle x verschwindet, so kann man eine ganze rationale Zahl $x = a$ so wählen, dass B_a eine von 0 verschiedene Zahl in K wird. Die Zahl $B^* = \frac{B_a}{a+\Theta}$ genügt dann der Gleichung $A = B^{*1-S}$. Setzen wir $B^* = \frac{B}{b}$, wo B eine ganze algebraische Zahl in K und b eine ganze rationale Zahl bedeutet, so ist auch $A = B^{1-S}$.

ABBILDUNG 1. Satz 90 aus Hilberts Zahlbericht [Hi]. Der 125 Jahre alte Text ist auch heute noch gut lesbar. Jedenfalls hat sich seitdem die »mathematische Ausdrucksweise« seitdem weit weniger geändert als die Orthographie (»Hülfssatz«, »in der That«, »ergiebt sich«, ...).

Wir wenden diese Überlegung an mit

$$\alpha_0 = 1, \quad \alpha_i = \alpha\sigma(\alpha_{i-1}),\ i > 0,$$

und erhalten dann für ein entsprechendes Element β, dass

$$\alpha\sigma(\beta) = \alpha\sigma(\gamma) + \alpha\sigma(\alpha)\sigma^2(\gamma) + \cdots + \alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha)\sigma^n(\gamma) = \beta,$$

denn $\sigma^n = \mathrm{id}$ und $\alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha) = N_{L/K}(\alpha) = 1$. Weil $\beta \neq 0$ ist, folgt $\alpha = \beta / \sigma(\beta)$. □

ERGÄNZUNG 6.17 (Additive Version des Satzes 90 von Hilbert). Zum Satz 90 von Hilbert gibt es die folgende additive Variante:

SATZ 6.18. *Sei L/K eine endliche zyklische Galois-Erweiterung und σ ein Erzeuger der Galois-Gruppe* $\mathrm{Gal}(L/K)$. *Für jedes $\alpha \in L$ sind dann äquivalent:*

(i) $\mathrm{Spur}_{L/K}(\alpha) = 0$,

(ii) *es gibt $\beta \in L$ mit $\alpha = \beta - \sigma(\beta)$.*

Siehe [JS] Satz VI.6.8 oder [Bo-A] Theorem 4.8/4. □ Ergänzung 6.17

6.3. Einheitswurzeln und zyklische Erweiterungen

DEFINITION 6.19. Sei K ein Körper. Sei $n \in \mathbb{N}_{>0}$.

(1) Ein Element $\zeta \in K^\times$ heißt eine *n-te Einheitswurzel*, wenn $\zeta^n = 1$ gilt. Wir bezeichnen mit $\mu_n(K)$ die Menge der n-ten Einheitswurzeln in K. Dies ist eine Untergruppe von $K^\times$.

(2) Ein Element $\zeta \in K^\times$ heißt *primitive n-te Einheitswurzel*, wenn ζ als Element der Gruppe $K^\times$ Ordnung n hat, wenn also $\zeta^n = 1$, aber $\zeta^m \neq 1$ für alle $1 \leq m < n$ gilt. Wir bezeichnen mit $\mu_n^{\text{prim}}(K)$ die Menge der primitiven n-ten Einheitswurzeln in K.

⊣

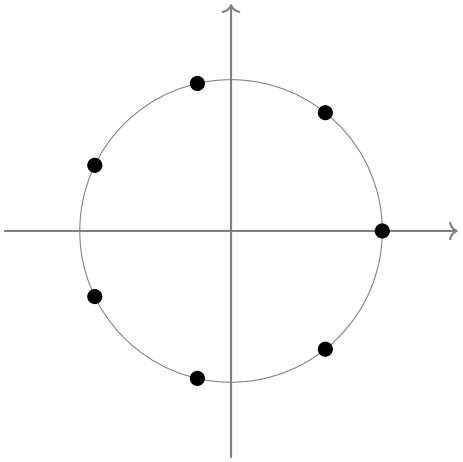
Die n-ten Einheitswurzeln in einem Körper K sind gerade die Nullstellen des Polynoms $X^n - 1$ in K. Es gilt also $\#\mu_n(K) \leq n$, und Gleichheit gilt genau dann, wenn es eine primitive n-te Einheitswurzel gibt. In diesem Fall zerfällt das Polynom $X^n - 1$ in n verschiedene Linearfaktoren. Insbesondere kann es in einem Körper positiver Charakteristik p für $p \mid n$ niemals eine primitive n-te Einheitswurzel geben (denn die Ableitung von $X^n - 1$ ist in dieser Situation gleich Null).

Die Gruppe $\mu_n(K)$ ist zyklisch (Satz 2.48). Gibt es in K eine primitive n-te Einheitswurzel ζ, so ist die Abbildung

$$\mathbb{Z}/n \to \mu_n(K), \quad i \mapsto \zeta^i,$$

ein Isomorphismus. (Weil $\zeta^n = 1$ gilt, ist der Ausdruck ζ^i wohldefiniert, also unabhängig von der Zahl eines Repräsentanten von $\mathbb{Z}$ von $i \in \mathbb{Z}/n$.) Dieser Isomorphismus schränkt sich ein zu einer Bijektion zwischen $(\mathbb{Z}/n)^\times$ und $\mu_n^{\text{prim}}(K)$, denn diese beiden Teilmengen sind jeweils die Teilmengen derjenigen Elemente, die die gegebene Gruppe erzeugen. Diese Eigenschaft wird unter jedem Gruppenisomorphismus erhalten.

BEISPIEL 6.20. Es gilt $\mu_n(\mathbb{C}) = \{\exp(\frac{2k\pi i}{n});\ k = 1, \ldots, n\}$. Insbesondere ist $\exp(\frac{2\pi i}{n})$ eine primitive n-te Einheitswurzel in $\mathbb{C}$.
In der Abbildung sind die siebten Einheitswurzen in $\mathbb{C}$ dargestellt. ◊



Körpererweiterungen, die durch Adjunktion einer Einheitswurzel entstehen, nennt man auch *zyklotomische Erweiterungen* (das Wort »zyklotomisch« kommt aus dem Griechischen und bedeutet »den (Einheits-)Kreis zerteilend«).

SATZ 6.21. *Sei K ein Körper, $\overline{K}$ ein algebraischer Abschluss von K und $\zeta \in \overline{K}$ eine primitive n-te Einheitswurzel. Dann gilt: Die Erweiterung $K(\zeta)/K$ ist eine abelsche Galois-Erweiterung. Die Galois-Gruppe ist isomorph zu einer Untergruppe von $(\mathbb{Z}/n)^\times$.*

BEWEIS. Nach Voraussetzung ist n die Ordnung von ζ in $K^\times$, also die kleinste natürliche Zahl > 0 mit $\zeta^n = 1$. Dann sind $1, \zeta, \ldots, \zeta^{n-1}$ paarweise verschieden, und daher ist $X^n - 1 = \prod_{i=0}^{n-1}(X - \zeta^i)$ ein separables Polynom. Offenbar ist $K(\zeta)$ der Zerfällungskörper dieses Polynoms über K (in $\overline{K}$), also ist $K(\zeta)/K$ eine Galois-Erweiterung. Für $\sigma \in \mathrm{Gal}(K(\zeta)/K)$ gilt

$\sigma(\zeta)^n = \sigma(\zeta^n) = 1$, und $\sigma(\zeta)^m \neq 1$, falls $0 < m < n$ gilt. Also ist $\sigma(\zeta)$ ebenfalls eine primitive n-te Einheitswurzel und somit von der Form $\sigma(\zeta) = \zeta^i$ für ein eindeutig bestimmtes $i \in (\mathbb{Z}/n)^\times$. Wir betrachten die Abbildung

$$\Phi\colon \mathrm{Gal}(K(\zeta)/K) \to (\mathbb{Z}/n)^\times, \qquad \sigma \mapsto i, \text{ s.d. } \sigma(\zeta) = \zeta^i.$$

Weil σ durch das Bild von ζ unter σ festgelegt ist, ist diese Abbildung injektiv.

Außerdem handelt es sich bei dieser Abbildung, wie man unmittelbar nachrechnet, um einen Gruppenhomomorphismus. Denn gilt etwa $\sigma(\zeta) = \zeta^i$, $\tau(\zeta) = \zeta^j$, so haben wir

$$(\sigma\tau)(\zeta) = \sigma(\tau(\zeta)) = \sigma(\zeta^j) = \sigma(\zeta)^j = \zeta^{ij},$$

also $\Phi(\sigma\tau) = ij = \Phi(\sigma)\Phi(\tau)$. Die Galois-Gruppe $\mathrm{Gal}(K(\zeta)/K)$ ist also isomorph zu einer Untergruppe der abelschen Gruppe $(\mathbb{Z}/n)^\times$, und insbesondere selbst abelsch. □

Im allgemeinen ist natürlich die Abbildung Φ aus dem Beweis des vorherigen Satzes kein Isomorphismus (zum Beispiel ist es ja möglich, dass $\zeta \in K$ ist). Aber im Fall des Grundkörpers $\mathbb{Q}$ ist Φ immer ein Isomorphismus, wie der nächste Satz zeigt.

Satz 6.22. *Sei $K = \mathbb{Q}$ und ζ eine primitive n-te Einheitswurzel (in einem algebraischen Abschluss von $\mathbb{Q}$). Dann gilt $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \#(\mathbb{Z}/n)^\times$ und $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n)^\times$.*

Beweis. Es genügt, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \#(\mathbb{Z}/n)^\times$ zu zeigen, denn wir wissen ja bereits, dass $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ zu einer Untergruppe von $(\mathbb{Z}/n)^\times$ isomorph ist.

Sei $f = \mathrm{minpol}_{\zeta,\mathbb{Q}}$. Jede Nullstelle von f ist (als Bild von ζ unter einem geeigneten Automorphismus von $\mathbb{Q}(\zeta)$) eine primitive n-te Einheitswurzel. Die Behauptung $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \#(\mathbb{Z}/n)^\times$ ist dazu äquivalent, dass *jede* primitive n-te Einheitswurzel eine Nullstelle von f ist. Wir beginnen mit der folgenden

Behauptung. Ist p eine zu n teilerfremde Primzahl, so gilt $f(\zeta^p) = 0$.

Begründung. Wir schreiben $X^n - 1 = fg$ mit einem Polynom g, das normiert ist und nach dem Lemma von Gauß (Korollar 3.47) in $\mathbb{Z}[X]$ liegt. Angenommen, es wäre $f(\zeta^p) \neq 0$. Dann ist also ζ^p eine Nullstelle von g, oder mit anderen Worten ζ eine Nullstelle von $g(X^p)$, und es folgt $f \mid g(X^p)$, weil f ja gerade das Minimalpolynom von ζ ist. Wir können also

$$g(X^p) = f \cdot h$$

für ein Polynom $h \in \mathbb{Q}[X]$ schreiben. Mit g und f ist dann auch h normiert und aus Korollar 3.47 folgt, dass auch h in $\mathbb{Z}[X]$ liegt.

Wir wenden nun den Ringhomomorphismus $\mathrm{red}_p\colon \mathbb{Z}[X] \to \mathbb{F}_p[X]$ an, der die Koeffizienten auf ihre Restklasse in $\mathbb{F}_p$ abbildet (siehe Abschnitt 3.5). Weil das Bilden der p-ten Potenz ein Ringhomomorphismus $\mathbb{F}_p[X] \to \mathbb{F}_p[X]$ ist (siehe Beispiel 3.2) und $a^p = a$ für alle $a \in \mathbb{F}_p$ gilt (siehe Satz 5.37), gilt $\mathrm{red}_p(g(X^p)) = \mathrm{red}_p(g)^p$, wir erhalten also

$$\mathrm{red}_p(g)^p = \mathrm{red}_p(f) \cdot \mathrm{red}_p(h) \quad \text{und} \quad X^n - 1 = \mathrm{red}_p(f)\,\mathrm{red}_p(g)$$

Aus der ersten Gleichung folgt, dass jede Nullstelle von f (in einem algebraischen Abschluss von $\mathbb{F}_p$) auch eine Nullstelle von $\mathrm{red}_p(g)^p$, also auch von $\mathrm{red}_p(g)$ ist. Aus der zweiten Gleichung folgt damit aber, dass jede Nullstelle von $\mathrm{red}_p(f)$ eine *mehrfache* Nullstelle von $X^n - 1$ ist. Aber die Ableitung nX^{n-1} von $X^n - 1$ hat wegen $n \neq 0 \in \mathbb{F}_p$ nur 0 als Nullstelle, folglich hat das Polynom $X^n - 1$ keine mehrfachen Nullstellen – ein Widerspruch!

Es bleibt nun noch, aus der obigen Behauptung zu folgern, dass jede primitive n-te Einheitswurzel ξ eine Nullstelle von f ist. Aber es gibt dann eine zu n teilerfremde Zahl m mit $\xi = \zeta^m$, und indem wir m als Produkt von Primzahlen schreiben, sehen wir, dass wir durch mehrfache Anwendung der Behauptung (auf ζ und auf Potenzen von ζ) schließlich $f(\xi) = 0$ folgern können. □

Mit einem Gradargument (und der Multiplikativität der Eulerschen φ-Funktion, Lemma 2.44) erhält man das folgende Korollar über das Kompositum von Erweiterungskörpern von $\mathbb{Q}$, die durch Adjunktion von Einheitswurzeln zu teilerfremden Ordnungen entstehen.

KOROLLAR 6.23. *Seien $m, n \in \mathbb{N}$ teilerfremde natürliche Zahlen und seien ζ_m, ζ_n bzw. ζ_{mn} eine m-te, n-te bzw. eine mn-te primitive Einheitswurzel in einem Erweiterungskörper von $\mathbb{Q}$ (zum Beispiel in $\mathbb{C}$). Dann gilt $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$.*

Wenn man dieses Korollar unabhängig vom Satz zeigen kann (und die algebraische Zahlentheorie liefert mit der sogenannten Verzweigungtheorie eine Methode dafür), kann man daraus einen Beweis des obigen Satzes erhalten, indem man zunächst den Fall abhandelt, dass n eine Primzahlpotenz ist (das geht so ähnlich wie der Fall einer Primzahl, für den wir Beispiel 3.55 heranziehen können), und dann die Aussage aus dem Korollar benutzt.

DEFINITION 6.24. Sei $n \in \mathbb{N}_{>0}$. Das n-te *Kreisteilungspolynom* Φ_n ist das Minimalpolynom einer primitiven n-ten Einheitswurzel ζ über $\mathbb{Q}$. ⊣

Der Beweis von Satz 6.22 zeigt, dass $\Phi = \prod_\xi (X - \xi)$ ist, wobei das Produkt über alle primitiven n-ten Einheitswurzeln ξ (in einem algebraischen Abschluss von $\mathbb{Q}$) gebildet wird. Insbesondere gilt $\deg(\Phi_n) = \#(\mathbb{Z}/n)^\times$.

SATZ 6.25. (1) *Für alle $n \in \mathbb{N}_{>0}$ gilt $\Phi_n \in \mathbb{Z}[X]$.*

(2) *Es gilt*

$$X^n - 1 = \prod_{d \mid n} \Phi_d,$$

wobei das Produkt über alle positiven Teiler d von n gebildet wird.

(3) *Sei K ein Körper, in dem n eine Einheit ist, und $z \in K$ eine Nullstelle von Φ_n. Dann ist z eine primitive n-te Einheitswurzel in K.*

BEWEIS. zu (1). Das Polynom Φ_n ist ein Teiler von $X^n - 1$ und ist normiert, daher folgt die Behauptung aus Korollar 3.47.

zu (2). Das Polynom $X^n - 1$ ist (in $\mathbb{C}$) das Produkt über alle Linearfaktoren $X - \xi$, $\xi \in \mu_n(\mathbb{C})$. Jedes solche ξ ist eine primitive $\operatorname{ord}(\xi)$-te Einheitswurzel, und $\operatorname{ord}(\xi) \mid n$. Daraus folgt die Behauptung.

zu (3). Ist z eine Nullstelle von Φ_n, so wegen Teil (2) auch von $X^n - 1$, es gilt also $z^n = 1$. Sei d die Ordnung von z in $K^\times$. Wir wollen zeigen, dass $d = n$ gilt. Jedenfalls ist d ein Teiler von n. Weil z eine Nullstelle von $X^d - 1$ ist, folgt mit Teil (2), nun auf $X^d - 1$ angewandt, dass z Nullstelle eines Polynoms $\Phi_{d'}$ mit $d' \mid d$ ist. Weil $X^n - 1$ wegen der Voraussetzung $n \in K^\times$ separabel ist, kann z aber keine mehrfache Nullstelle von $X^n - 1$ sein, es muss also $d' = n$ und damit insbesondere $d = n$ gelten. □

BEISPIEL 6.26. Für eine Primzahl p gilt $\Phi_p = X^{p-1} + \cdots + X + 1$, denn dieses Polynom ist irreduzibel (Beispiel 3.55) und ist gleich $(X^p - 1)/(X - 1)$.

Mit Teil (2) des vorherigen Satzes kann man die Kreisteilungspolynome induktiv durch Polynomdivision berechnen. Zum Beispiel:

$$\Phi_1 = X - 1, \quad \Phi_2 = X + 1, \quad \Phi_3 = X^2 + X + 1,$$
$$\Phi_4 = X^2 + 1, \quad \Phi_6 = X^2 - X + 1, \quad \Phi_8 = X^4 + 1.$$

Übungen: Ist p eine Primzahl und $r \geq 1$, so gilt $\Phi_{p^r} = (X^{p^r} - 1)/(X^{p^{r-1}} - 1) = \Phi_p(X^{p^{r-1}})$. Ist $n > 1$ ungerade, so gilt $\Phi_{2n}(-X) = \Phi_n(X)$.

Die kleinste Zahl n, für die Φ_n Koeffizienten mit Absolutbetrag > 1 hat, ist $n = 105$. (Diese Eigenschaft über den Betrag der Koeffizienten ist dazu äquivalent, dass n mindestens drei verschiedene ungerade Primfaktoren hat, siehe T. Y. Lam, K. H. Cheung, *On the cyclotomic polynomial* $\Phi_{pq}(T)$, Amer. Math. Monthly **103** (1996), 562–564. ◊

Wir können nun zyklische Erweiterungen L/K vom Grad n beschreiben, sofern K eine primitive n-te Einheitswurzel enthält.

SATZ 6.27. *Seien $n \in \mathbb{N}_{>1}$ und K ein Körper, der eine primitive n-te Einheitswurzel ζ enthält. Sei L/K eine Körpererweiterung.*

(1) *Wenn $L = K(\alpha)$ gilt für ein Element $\alpha \in L$, das Nullstelle eines Polynoms der Form $X^n - c$ mit $c \in K$ ist, dann ist L/K eine zyklische Galois-Erweiterung. Der Grad $d := [L : K]$ ist ein Teiler von n, es gilt $\alpha^d \in K$ und $X^d - \alpha^d$ ist das Minimalpolynom von α über K.*

(2) *Wenn die Erweiterung L/K zyklisch vom Grad n ist, dann existiert $\alpha \in L$, so dass $L = K(\alpha)$ ist und das Minimalpolynom von α über K die Form $\operatorname{minpol}_{\alpha,K} = X^n - c$ für ein $c \in K$ hat.*

BEWEIS. zu (1). Es gilt $X^n - c = \prod_{i=0}^{n}(X - \zeta^i\alpha)$, denn mit α ist offenbar auch $\zeta^i\alpha$ für alle i eine Nullstelle von $X^n - c$. Also ist $K(\alpha)$ der Zerfällungskörper des separablen Polynoms $X^n - c$ und daher eine Galois-Erweiterung.

Für jedes Element $\sigma \in \operatorname{Gal}(L/K)$ ist $\sigma(\alpha)$ eine Nullstelle von $X^n - c$, also von der Form $\zeta^i\alpha$ für ein eindeutig bestimmtes $i \in \mathbb{Z}/n$. Wir können also die Abbildung

$$\Phi\colon \operatorname{Gal}(L/K) \to \mathbb{Z}/n\,, \quad \sigma \mapsto i \text{ so dass } \sigma(\alpha) = \zeta^i\alpha,$$

betrachten. Diese ist ein Gruppenhomomorphismus, denn

$$(\sigma\tau)(\alpha) = \sigma(\tau(\alpha)) = \sigma(\zeta^{\Phi(\tau)}\alpha) = \zeta^{\Phi(\tau)}\sigma(\alpha) = \zeta^{\Phi(\sigma)+\Phi(\tau)}\alpha,$$

wobei wir benutzt haben, dass $\zeta \in K$ ist und ζ deshalb von allen Galois-Automorphismen fixiert wird. Weil ein K-Homomorphismus $K(\alpha) \to K(\alpha)$ durch das Bild von α eindeutig festgelegt ist, ist Φ injektiv. Es folgt, dass $\operatorname{Gal}(L/K)$ zu einer Untergruppe von $\mathbb{Z}/n$ isomorph ist, und insbesondere folgt, dass $\operatorname{Gal}(L/K)$ zyklisch ist (Satz 2.41) und dass $d = [K(\alpha) : K] \mid n$ gilt.

Weil für alle $\sigma \in \operatorname{Gal}(L/K)$ gilt, dass $\sigma(\alpha^d) = \sigma(\alpha)^d = \zeta^{d\Phi(\sigma)}\alpha^d = \alpha^d$ ist (denn $\Phi(\sigma)$ liegt ja in der d-elementigen Untergruppe von $\mathbb{Z}/n$ und wird daher von d annuliert), gilt $\alpha^d \in K$.

Es ist also α eine Nullstelle des Polynoms $X^d - \alpha^d \in K[X]$. Weil dieses Grad $d = [K(\alpha) : K]$ hat, handelt es sich um das Minimalpolynom von α.

zu (2). Sei σ ein Erzeuger von $\operatorname{Gal}(L/K)$. Wir betrachten σ als K-Vektorraum-Isomorphismus $L \xrightarrow{\sim} L$. Aus $\sigma^n = \mathrm{id}$ folgt $\operatorname{minpol}_\sigma \mid (X^n - 1)$ (hier ist $\operatorname{minpol}_\sigma$ das Minimalpolynom von σ im Sinne der Linearen Algebra). Weil $X^n - 1$ in $K[X]$ in n verschiedene Linearfaktoren zerfällt, ist σ über K diagonalisierbar (Korollar LA2.16.29).

Behauptung. Es gilt $\operatorname{minpol}_\sigma = X^n - 1$.

Begründung. Die Abbildung σ ist als Ringhomomorphismus verträglich mit der Multiplikation von L. Deshalb ist die Menge der Eigenwerte von σ eine *Untergruppe* von $K^\times$. Denn sind $\lambda, \mu \in K$ Eigenwerte mit zugehörigen Eigenvektoren $v, w \in L$, dann gilt

$$\sigma(vw) = \sigma(v)\sigma(w) = \lambda\mu vw,$$

also ist auch $\lambda\mu$ ein Eigenwert von σ. Außerdem gilt

$$\sigma(v^{-1}) = \sigma(v)^{-1} = \lambda^{-1}v^{-1}$$

und wir sehen so, dass auch λ^{-1} ein Eigenwert von σ ist. Weil σ diagonalisierbar ist, ist die Menge der Eigenwerte nicht leer.

Genauer ist die Menge der Eigenwerte von σ eine Untergruppe der zyklischen Gruppe $\mu_n(K)$, also von der Form $\mu_d(K)$ für einen Teiler d von n. Es folgt dann (weil σ diagonalisierbar ist), dass $\sigma^d = \mathrm{id}$ gilt. Weil σ die Gruppe $\mathrm{Gal}(L/K)$ mit n Elementen erzeugt, folgt $d = n$. Die Behauptung ist damit bewiesen.

Daher ist insbesondere die primitive n-te Einheitswurzel ζ ein Eigenwert von σ, es existiert also $\alpha \in L$ mit $\sigma(\alpha) = \zeta\alpha$ und allgemeiner $\sigma^i(\alpha) = \zeta^i\alpha$. Wir sehen damit, dass alle Elemente $\zeta^i\alpha$, $i = 0, \ldots, n-1$, Nullstellen von $\mathrm{minpol}_{\alpha,K}$ sind. Es folgt $\deg(\mathrm{minpol}_{\alpha,K}) = n$ und damit $L = K(\alpha)$. Außerdem ist $c := \alpha^n \in K$, denn $\sigma(\alpha^n) = \zeta^n\alpha^n = \alpha^n$. Weil das Polynom $X^n - c \in K[X]$ Grad $n = [K(\alpha) : K]$ und α als Nullstelle hat, handelt es sich hierbei um das Minimalpolynom von α. □

Ergänzung 6.28 (Alternative Ansätze zur Charakterisierung zyklischer Erweiterungen). Es gibt mehrere andere Möglichkeiten, im Beweis von Teil (2) des obigen Satzes zu zeigen, dass ζ ein Eigenwert von σ ist.

(1) Aus dem Satz über die lineare Unabhängigkeit von Charakteren folgt, dass die (paarweise verschiedenen) Abbildungen $\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ linear unabhängig sind. Also muss das Minimalpolynom von σ mindestens Grad n haben. Weil $\sigma^n = \mathrm{id}$ ist, folgt $\mathrm{minpol}_\sigma = X^n - 1$, also ist ζ eine Nullstelle von minpol_σ und daher ein Eigenwert von σ.

(2) Mit Hilberts Satz 90 (Satz 6.16) kann man folgendermaßen argumentieren: Es gilt $N_{L/K}(\zeta) = \zeta^n = 1$, also existiert $\alpha \in L$ mit $\zeta = \alpha/\sigma(\alpha)$.

□ Ergänzung 6.28

Ergänzung 6.29 (Artin-Schreier-Erweiterungen). Aufbauend auf der additiven Version des Satzes 90 von Hilbert (Ergänzung 6.17) kann man den Satz von Artin-Schreier über die Charakterisierung zyklischer Erweiterungen vom Grad p eines Körpers der Charakteristik $p > 0$ beweisen. Siehe [**JS**] Satz VI.6.9 oder [**Bo-A**] Theorem 4.8/5. □ Ergänzung 6.29

Ergänzung 6.30 (Der Satz von Kronecker-Weber). Der Satz von Kronecker und Weber ist das folgende Theorem über abelsche Galois-Erweiterungen von $\mathbb{Q}$. Der Beweis ist nicht leicht, so dass wir ihn hier auslassen. Der Satz gehört in den Kontext der (globalen) Klassenkörpertheorie[2], die noch präziser die abelschen Erweiterungen von $\mathbb{Q}$ und von endlichen Erweiterungskörpern von $\mathbb{Q}$ beschreibt. (Für $E \neq \mathbb{Q}$ ist es allerdings nicht ausreichend, Einheiswurzeln zu adjungieren, um alle abelschen Erweiterungen von E als Zwischenkörper zu erhalten.)

Theorem 6.31. *Sei $K/\mathbb{Q}$ eine abelsche endliche Galois-Erweiterung (die Zwischenkörper von einem fixierten algebraischen Abschluss $\overline{K}$ von K ist). Dann existiert eine Einheitswurzel $\zeta \in \overline{K}$ mit $K \subseteq \mathbb{Q}(\zeta)$.*

Den Satz kann man sehr konkret interpretieren: Ist $K/\mathbb{Q}$ abelsch und $\alpha \in K$, dann existieren $n \in \mathbb{N}$, eine n-te Einheitswurzel ζ und rationale Zahlen a_i, $i = 0, \ldots, n-1$ mit $\alpha = \sum_{i=0}^{n-1} a_i\zeta^i$.
□ Ergänzung 6.30

Ergänzung 6.32 (Einheitswurzeln über endlichen Körpern).

[2] https://de.wikipedia.org/wiki/Klassenkörpertheorie

SATZ 6.33. *Sei p eine Primzahl und $n \in \mathbb{N}$ eine natürliche Zahl, die nicht von p geteilt wird. Sei ζ eine primitive n-te Einheitswurzel in einem algebraischen Abschluss von $\mathbb{F}_p$. Sei $\Phi\colon \mathrm{Gal}(\mathbb{F}_p(\zeta)\big/\mathbb{F}_p) \to (\mathbb{Z}/n)^\times$ der injektive Gruppenhomomorphismus aus Satz 6.21.*

Dann ist $\mathrm{Im}(\Phi)$ die Untergruppe von $(\mathbb{Z}/n)^\times$, die von der Restklasse von p in $(\mathbb{Z}/n)^\times$ erzeugt wird.

BEWEIS. Sei $q = \#\mathbb{F}_p(\zeta) = p^r, r \in \mathbb{N}_{>0}$. Wir wissen bereits (Satz 5.40, Beispiel 5.46), dass $\mathbb{F}_p(\zeta)\big/\mathbb{F}_p$ als Erweiterung endlicher Körper eine zyklische endliche Galois-Erweiterung ist.

Die Galois-Gruppe $\mathrm{Gal}(\mathbb{F}_p(\zeta)\big/\mathbb{F}_p)$ wird erzeugt vom Frobenius-Automorphismus $\mathrm{Frob}\colon \mathbb{F}_p(\zeta) \to \mathbb{F}_p(\zeta), x \mapsto x^p$. Dieser wird unter Φ auf die Restklasse von p in $(\mathbb{Z}/n)^\times$ abgebildet. □

Insbesondere ist also in der Situation des Satzes der Grad $[\mathbb{F}_p(\zeta) : \mathbb{F}_p]$ gleich der Ordnung von p in $(\mathbb{Z}/n)^\times$.

Ein analoges Ergebnis gilt, wenn man $\mathbb{F}_p$ durch einen beliebigen endlichen Körper (und die Restklasse von p durch die Restklasse von $\#K$) ersetzt.

Wenn in der obigen Situation $\zeta \in \mathbb{F}_p$ liegt, wenn also der Körper $\mathbb{F}_p$ selbst eine primitive n-te Einheitswurzel enthält, gilt $p \equiv 1 \mod n$. Die Aussage dieses Spezialfalls folgt auch direkt daraus, dass für $\zeta \in \mathbb{F}_p$ gelten muss, dass $\zeta^{p-1} = 1$ ist, also dass $n \mid p - 1$. Aus dieser Beobachtung erhalten wir das folgende Korollar.

KOROLLAR 6.34. *Sei $n \in \mathbb{N}_{>0}$. Es gibt unendlich viele Primzahlen p, für die $p \equiv 1 \mod n$ gilt.*

BEWEIS. Nach dem vorherigen Satz ist es äquivalent zu zeigen, dass unendlich viele Primzahlen p existieren, für die $\mathbb{F}_p$ eine primitive n-te Einheitswurzel enthält. Wegen Satz 6.25 folgt die Aussage aus dem folgenden Lemma, angewandt auf das n-te Kreisteilungspolynom Φ_n. (Die endlich vielen Primteiler von n können wir ohne Einschränkung von der Betrachtung ausnehmen.) □

LEMMA 6.35. *Sei $f \in \mathbb{Z}[X]$ ein nicht-konstantes Polynom. Dann existieren unendlich viele Primzahlen p, für die f in $\mathbb{F}_p$ eine Nullstelle hat.*

Im Beweis argumentieren wir analog zur folgenden Variante von Euklids Beweis, dass es unendlich viele Primzahlen gibt (Satz LA1.3.6): Für $k \in \mathbb{N}$, $k > 1$, wird $k! + 1$ von einer Primzahl p geteilt, und diese muss größer als k sein (sonst gälte auch $p \mid k!$ und damit $p \mid 1$). Also gibt es zu jeder natürlichen Zahl Primzahlen, die größer als k sind.

BEWEIS. Sei $a = f(0)$ der konstante Term von f. Falls $a = 0$ gilt, ist 0 eine Nullstelle von f in jedem Körper. Sei nun $a \neq 0$. Wir schreiben $f = Xg + a$ mit $g \in \mathbb{Z}[X]$. Sei $k \in \mathbb{N}$ so groß, dass $|f(ak!)| > |a|$ gilt. (Weil f nicht konstant ist, gilt das für alle hinreichend großen k.) Es gilt

$$f(ak!) = ak!g(ak!) + a = a(k!g(ak!) + 1).$$

Weil $|f(ak!)| > |a|$ ist, ist $|k!g(ak!) + 1| > 1$, und jeder Primteiler p von $k!g(ak!) + 1$ ist ein Teiler von $f(ak!)$ (also ist die Restklasse von $ak!$ eine Nullstelle von f in $\mathbb{F}_p$), der zu $k!$ teilerfremd und daher größer als k ist. □

Es ist ein berühmter Satz von Dirichlet, dass für jedes Paar teilerfremde natürlicher Zahlen m, n unendlich viele Primzahlen p mit $p \equiv m \mod n$ existieren. Das Korollar ist der Spezialfall $m = 1$. Der allgemeine Fall ist schwieriger zu beweisen. (Siehe zum Beispiel [**Se**].)

Übung. Folgern Sie aus dem Korollar, dass es für jedes $n \in \mathbb{N}_{>0}$ eine Galois-Erweiterung $L/\mathbb{Q}$ gibt, deren Galois-Gruppe isomorph ist zur Gruppe $\mathbb{Z}/n$. □ Ergänzung 6.32

6.4. Auflösbarkeit von Gleichungen durch Radikale

Wir wollen jetzt die Galois-Theorie auf die Frage anwenden, für welche Polynome sich die Nullstellen als ein Ausdruck hinschreiben lassen, in dem neben den Grundrechenarten (plus, minus, mal, geteilt) nur n-te Wurzeln gezogen werden. Dass es typischerweise mehrere verschiedene n-te Wurzeln eines Elements gibt, berücksichtigen wir dadurch, dass wir auch Einheitswurzeln in dem Ausdruck erlauben. (Man darf also sozusagen immer eine »geeignete« n-te Wurzel verwenden.)

Um die Diskussion etwas zu vereinfachen, betrachten wir in diesem Abschnitt nur Körper der Charakteristik 0. Um die Ergebnisse in der »richtigen« Art und Weise auf Körper positiver Charakteristik zu übertragen, ist zu berücksichtigen, dass es über diesen im Allgemeinen auch zyklische Erweiterungen gibt, für die kein primitives Element mit Minimalpolynom der Form $X^n - c$ existiert (vergleiche Satz 6.27, der diese Fälle nicht abdeckt, weil es niemals eine primitive n-te Einheitswurzel gibt, wenn n ein Vielfaches der Charakteristik ist).

Für die Charakterisierung solcher Erweiterungen müssen wir im Grunde nur noch zusammensetzen, was wir bereits wissen:

- Körpererweiterungen, die durch Adjunktion von Einheitswurzel entstehen, sind abelsch, Satz 6.21,
- Körpererweiterungen der Form $K(\sqrt[n]{a})/K$, wo K eine primitive n-te Einheiswurzel enthält sind zyklisch, und (in geeignetem Sinne, in Charakteristik 0) umgekehrt, Satz 6.27,
- Sei L/K eine endliche Galois-Erweiterung. Die Galois-Gruppe $\mathrm{Gal}(L/K)$ ist genau dann auflösbar, wenn es eine Kette

  $$K = K_0 \subset K_1 \subset \cdots \subset K_r = L$$

  von Zwischenkörpern gibt, so dass alle Erweiterungen K_i/K_{i-1} zyklisch sind. (Theorem 5.49, Lemma 2.64).

Um das weiter auszuarbeiten, machen wir zunächst die folgenden Definitionen. Wir fixieren hier einen algebraischen Abschluss $\overline{K}$ von K und setzen ohne Einschränkung voraus, dass alle im Folgenden betrachteten Erweiterungskörper von K Teilkörper von $\overline{K}$ sind.

Definition 6.36. Sei L/K eine endliche Körpererweiterung.

(1) Wir sagen, die Körpererweiterung L/K sei *auflösbar durch Radikale*, wenn eine Kette

$$K = K_0 \subset K_1 \subset \cdots \subset K_r$$

endlicher Körpererweiterungen mit $L \subseteq K_r$ existiert, so dass jede der Erweiterungen K_{i+1}/K_i von einer der folgenden Formen ist:
- K_{i+1} entsteht aus K_i durch Adjunktion einer Einheitswurzel,
- $K_{i+1} = K_i(\alpha)$ für ein Element α aus K_{i+1}, so dass eine positive Potenz von α in K_i liegt.

(2) Wir sagen, die Körpererweiterung L/K sei *auflösbar*, wenn ein Erweiterungskörper E von L existiert, so dass E/K eine endliche Galois-Erweiterung mit auflösbarer Galois-Gruppe ist.

(3) Ist $f \in K[X]$, so sagen wir die Gleichung $f(x) = 0$ (oder: das Polynom f) sei *auflösbar durch Radikale* bzw. *auflösbar*, wenn der Zerfällungskörper von f die entsprechende Eigenschaft hat.

⊣

In Teil (1) ist der erste Typ der erlaubten Erweiterungen ein Spezialfall des zweiten Typs, aber es ist nützlich, die Adjunktion von Einheitswurzeln separat zu betrachten.

Wir werden sehen, dass es (beispielsweise über $K = \mathbb{Q}$) Polynome mit der Eigenschaft gibt, dass für jede Nullstelle α des Polynoms die Erweiterung $K(\alpha)/K$ nicht durch Radikale auflösbar ist. Das bedeutet, dass sich α nicht durch Elemente aus K, die Grundrechenarten, Einheitswurzeln und n-te Wurzeln ausdrücken lässt, denn sonst könnte man eine Kette wie oben mit $\alpha \in K_r$ und damit $K(\alpha) \subseteq K_r$ finden.

LEMMA 6.37. (1) *Eine Erweiterung L/K ist genau dann auflösbar durch Radikale, wenn die normale Hülle von L über K diese Eigenschaft hat.*

(2) *Eine Erweiterung L/K ist genau dann auflösbar, wenn die normale Hülle von L über K eine Galois-Erweiterung mit auflösbarer Galois-Gruppe ist.*

(3) *Sind L/K und E/K algebraische Körpererweiterungen (in $\overline{K}$) und ist L/K auflösbar durch Radikale bzw. auflösbar, so hat auch die Erweiterung LE/E diese Eigenschaft.*

(4) *Die Eigenschaften* auflösbar durch Radikale *und* auflösbar *verhalten sich transitiv in einem Turm $K \subset L \subset M$ von Körpererweiterungen, d.h. es gilt: M/K hat die entsprechende Eigenschaft genau dann, wenn sowohl M/L als auf L/K sie haben.*

BEWEIS. Zu (1). Dies ist nicht schwierig und wird im Folgenden nicht benötigt, daher lassen wir den Beweis aus.

Zu (2). Wenn die normale Hülle von L über K galoissch mit auflösbarer Galois-Gruppe ist, dann ist L/K nach Definition auflösbar. Ist andererseits L/K auflösbar, und etwa E ein Erweiterungskörper von K, so dass E/K eine endliche Galois-Erweiterung mit auflösbarer Galois-Gruppe ist, dann ist die normale Hülle L' von L über K in E enthalten und die Gruppe $\mathrm{Gal}(L'/K)$ als Quotient der auflösbaren Gruppe $\mathrm{Gal}(E/K)$ auch selbst auflösbar (Lemma 2.63).

Zu (3). Sei zunächst L/K durch Radikale auflösbar. Indem wir gegebenenfalls L vergrößern können wir annehmen, dass eine Kette von Teilkörpern der Erweiterung L/K besteht, so dass die einzelnen Schritte die oben genannten Typen haben. Indem wir für jeden dieser Schritte das Kompositum mit E bilden, erhalten wir eine entsprechende Kette von Teilkörpern der Erweiterung LE/E.

Ist L/K auflösbar, so können wir, indem wir L durch seine normale Hülle über K ersetzen, annehmen, dass die Erweiterung eine Galois-Erweiterung mit auflösbarer Galois-Gruppe ist. Insbesondere ist L Zerfällungskörper einer Familie von separablen Polynomen, und wir erhalten LE als Zerfällungskörper derselben Familie über E. Also ist auch LE/E eine Galois-Erweiterung. Wir erhalten durch Einschränkung einen Homomorphismus

$$\mathrm{Gal}(LE/E) \longrightarrow \mathrm{Gal}(L/K), \quad \sigma \mapsto \sigma_{|L},$$

der injektiv ist, weil LE über E von den Elementen von L erzeugt wird. Da nach Voraussetzung $\mathrm{Gal}(L/K)$ auflösbar ist, gilt das nach Lemma 2.63 auch für $\mathrm{Gal}(LE/E)$.

Zu (4). Es ist leicht zu sehen, dass M/L und L/K auflösbar durch Radikale (bzw. auflösbar) sind, wenn dies für M/K gilt.

Seien nun M/L und L/K auflösbar durch Radikale. Wir finden dann L'/L, so dass die Erweiterung L'/K eine Kette von Zwischenkörpern besitzt, deren einzelne Schritte Erweiterungen der oben genannten Typen sind. Nach Teil (3) ist auch ML'/L' auflösbar durch Radikale. Dann ist aber auch ML'/K und erst recht M/K durch Radikale auflösbar.

Seien schließlich die Erweiterungen M/L und L/K auflösbar. Durch Übergang zu den normalen Hüllen und mit Teil (3) können wir annehmen, dass beide Erweiterungen galoissch mit auflösbarer Galois-Gruppe sind. Ist dann die Erweiterung M/K galoissch, dann folgt

direkt, dass ihre Galois-Gruppe auflösbar ist, und wir sind fertig; im allgemeinen wird das aber nicht der Fall sein.

Sei M' die normale Hülle von M über K. Dann ist M'/K eine Galois-Erweiterung, denn M/K ist separabel (Satz 5.24) und M' ist der Zerfällungskörper der Minimalpolynome $\operatorname{minpol}_{\alpha,K}$ für $\alpha \in M$. Wir müssen zeigen, dass $\operatorname{Gal}(M'/K)$ auflösbar ist. Die Einschränkungsabbildung $R\colon \operatorname{Gal}(M'/K) \to \operatorname{Gal}(L/K)$ ist surjektiv, und $\operatorname{Gal}(L/K)$ ist auflösbar. Nach Lemma 2.63 genügt es daher zu zeigen, dass $\operatorname{Ker}(R) = \operatorname{Gal}(M'/L)$ auflösbar ist. Aber M' ist das Kompositum der Erweiterungskörper $\sigma(M)$ für $\sigma \in \operatorname{Hom}_K(M, \overline{K})$ (vergleiche Satz 5.7 über die normale Hülle). Alle Erweiterungen $\sigma(M)/\sigma(L)$ sind Galois-Erweiterungen, weil das für L/K gilt: Ist etwas $M = L(\alpha)$, so ist $\sigma(M) = \sigma(L)(\sigma(\alpha)) \subseteq \overline{K}$, und $\operatorname{minpol}_{\sigma(\alpha),\sigma(L)} = \sigma(\operatorname{minpol}_{\alpha,L})$; also ist $\operatorname{minpol}_{\sigma(\alpha),\sigma(L)}$ separabel und zerfällt über $\sigma(M)$ vollständig in Linearfaktoren. Die Abbildung $\tau \mapsto \sigma \circ \tau \circ \sigma^{-1}$ ist ein Isomorphismus $\operatorname{Gal}(L/K) \xrightarrow{\sim} \operatorname{Gal}(\sigma(M)/\sigma(L))$. Weil L/K eine Galois-Erweiterung ist, gilt zudem $\sigma(L) = L$ für alle σ.

Wir erhalten damit einen injektiven Gruppenhomomorphismus

$$\operatorname{Gal}(M'/L) \longrightarrow \prod_{\sigma \in \operatorname{Hom}_K(M,\overline{K})} \operatorname{Gal}(\sigma(M)/L), \quad \tau \mapsto (\tau_{|\sigma(M)})_\sigma.$$

Mit Lemma 2.63 sehen wir zunächst, dass der Wertebereich auflösbar ist und sodann, dass das auch für den Definitionsbereich gilt. □

Satz 6.38. *Eine Körpererweiterung ist genau dann auflösbar durch Radikale, wenn sie auflösbar ist.*

Beweis. Sei zunächst L/K auflösbar. Wir können wegen Lemma 6.37 (2) L durch seine normale Hülle ersetzen und daher annehmen, dass die Erweiterung galoissch mit auflösbarer Galois-Gruppe ist. Ist $\zeta \in \overline{K}$ irgendeine Einheitswurzel, so ist $L(\zeta) = LK(\zeta)$ und daher nach Satz 5.55 und Lemma 6.37 (3) die Erweiterung $L(\zeta)/K(\zeta)$ ebenfalls galoissch mit auflösbarer Galois-Gruppe. Weil die Erweiterung $K(\zeta)/K$ nach Definition durch Radikale auflösbar ist, genügt es (nun wegen Lemma 6.37 (4)) zu zeigen, dass $L(\zeta)/K(\zeta)$ durch Radikale auflösbar ist. Indem wir K durch $K(\zeta)$ ersetzen für eine $[L : K]!$-te Einheitswurzel ζ, können wir also voraussetzen, dass K alle d-ten Einheitswurzeln für alle Teiler d von $[L : K]$ enthält. Wir können (mit Lemma 2.64 und Theorem 5.49) eine Kette

$$K = K_0 \subset K_1 \subset \cdots \subset K_r = L$$

finden, so dass jede der Erweiterungen K_i/K_{-1} zyklisch ist. Nach Satz 6.27 hat dann jede dieser Erweiterungen die Form $K_i = K_{i-1}(\sqrt[n]{a})$ für $n \in \mathbb{N}$, $a \in K_{i-1}$. Also ist L/K auflösbar durch Radikale.

Sei nun L/K eine Körpererweiterung, die durch Radikale auflösbar ist. Sei

$$K = K_0 \subset K_1 \subset \cdots \subset K_r$$

eine Kette von Körpererweiterungen wie in Definition 6.36 (1) mit $L \subseteq K_r$. Wir können L durch einen Erweiterungskörper ersetzen und daher $L = K_r$ annehmen. Dann genügt es (wegen Lemma 6.37 (4)) zu zeigen, dass jede der Erweiterungen K_i/K_{i-1} auflösbar ist. Das aber ist klar für Erweiterungen vom Typ (1) (Adjunktion einer Einheitswurzel), denn es handelt sich ja sogar um abelsche Galois-Erweiterungen. Ist L/K eine Erweiterung vom Typ (2), d.h. $L = K(\alpha)$ und etwas $\alpha^n \in K$, so ist die Erweiterung ebenfalls auflösbar. Denn ist ζ eine n-te Einheitswurzel, dann ist die Erweiterung $L(\zeta)/K(\zeta)$ nach Satz 5.55 zyklisch, die Kette $K \subset K(\zeta) \subset L(\zeta)$ besteht also aus abelschen Galois-Erweiterungen und wir sehen, dass $L(\zeta)/K$ galoisch ist (denn L ist der Zerfällungskörper von $\operatorname{minpol}_{\alpha,K}$ und $X^n - 1$) und zwar mit auflösbarer Galois-Gruppe. □

Korollar 6.39. *Es gibt Gleichungen (zum Beispiel vom Grad 5 über $\mathbb{Q}$), die nicht durch Radikale auflösbar sind.*

BEWEIS. Wir haben gesehen (Satz 2.65), dass die Gruppe S_5 nicht auflösbar ist, es genügt also, ein Polynom $f \in \mathbb{Q}[X]$ vom Grad 5 mit Galois-Gruppe S_5 zu finden. Wenn f irreduzibel vom Grad 5 ist und L der Zerfällungskörper von f (in $\overline{\mathbb{Q}} \subset \mathbb{C}$) ist, dann operiert $G := \mathrm{Gal}(L/K)$ transitiv auf der Menge der Nullstellen von f in $\overline{\mathbb{Q}}$ und wir erhalten so einen injektiven Gruppenhomomorphismus $G \to S_5$, so dass wir G im folgenden als Untergruppe von S_5 betrachten können.

Wir wollen nun Polynome f finden, für die sogar die Gleichheit $G = S_5$ gilt. Dafür gibt es viele Möglichkeiten (siehe auch [**Bo-A**] Abschnitt 6.1). Man kann auch zeigen, dass in einem geeigneten Sinne »die meisten« Polynome vom Grad ≥ 5 eine nicht-auflösbare Galois-Gruppe haben. Eine Möglichkeit, um konkrete Beispiele angeben zu können, ist, die folgenden drei Aussagen zu zeigen. (Man könnte hier auch allgemeiner irgendeine Primzahl ≥ 5 betrachten.)

(1) Weil G transitiv auf der Menge der Nullstellen operiert, enthält G einen 5-Zykel.

(2) Wenn f so gewählt ist, dass G eine Transposition enthält, dann ist $G = S_5$.

(3) Wenn f genau zwei nicht-reelle Nullstellen hat, dann enthält G eine Transposition, also ist die Gleichung f nicht durch Radikale auflösbar.

Zu (1). Weil G eine Bahn mit 5 Elementen hat, folgt aus Lemma 2.32, dass 5 ein Teiler von $\#G$ ist. Weil 5^2 aber nicht $\#S_5$ teilt, hat jede 5-Sylow-Untergruppe von G genau 5 Elemente, ist also zyklisch von Ordnung 5. Also enthält G ein Element der Ordnung 5, d.h. einen 5-Zykel.

Zu (2). Nach Umnummerieren können wir annehmen, dass $(12) \in G$. Indem wir von dem in G enthaltenen 5-Zykel gegebenenfalls zu einer Potenz übergehen, können wir annehmen, dass dieser Zykel 1 auf 2 abbildet, und nach einer weiteren Umnummerierung annehmen, dass $(12345) \in G$ ist. Dann sehen wir, dass G auch die Transpositionen (23), (34) und (45) enthält, und diese erzeugen die Gruppe S_5.

Zu (3). Wenn f genau zwei Nullstellen in $\mathbb{C} \setminus \mathbb{R}$ enthält, dann sind diese zueinander konjugiert, die Einschränkung der komplexen Konjugation auf L ist daher ein Automorphismus von L, der auf der Nullstellenmenge von f durch eine Transposition operiert.

Ein konkretes Beispiel für ein irreduzibles Polynom in $\mathbb{Q}[X]$, das genau zwei nicht-reelle Nullstellen hat, ist $X^5 - 6X + 3$ (irreduzibel nach dem Eisenstein-Kriterium), wie man leicht mittels »Kurvendiskussion« beweist. □

Insbesondere bedeutet das natürlich, dass es für Polynome von Grad ≥ 5 keine allgemeine Lösungsformel für die Nullstellen in Termen der hier betrachteten Rechenoperationen geben kann.

Andererseits erhalten wir wegen der Auflösbarkeit der Gruppen S_n für $n \leq 4$ (und demzufolge aller ihrer Untergruppen) das folgende Ergebnis.

KOROLLAR 6.40. *Jede Gleichung vom Grad ≤ 4 ist durch Radikale auflösbar.*

Die Methoden der Galois-Theorie ermöglichen es auch, für Gleichungen vom Grad 3 und 4 konkrete Lösungsformeln aufzustellen, ähnlich der bekannten Lösungsformel für quadratische Gleichungen. Naturgemäß ist die Sache in Grad 3 und 4 etwas komplizierter, auch deshalb, weil man dabei auch dritte (und gegebenenfalls vierte) Einheitswurzeln verwenden muss. Siehe [**Bo-A**] Abschnitt 6.2.

ERGÄNZUNG 6.41 (Der Satz von Rost über den Radikalabschluss von $\mathbb{Q}$ in $\mathbb{R}$). Die reelle Zahl $\cos(\frac{2\pi}{7})$ ist ein Element von $\mathbb{Q}(\zeta)$ für $\zeta = e^{\frac{2\pi i}{7}}$, denn $\cos(\frac{2\pi}{7}) = \mathrm{Re}(\zeta) = \frac{1}{2}(\zeta + \zeta^{-1})$. Insbesondere ist diese reelle Zahl »durch Radikale darstellbar« in dem Sinne, dass die Erweiterung $\mathbb{Q}(\cos(\frac{2\pi}{7}))\big/\mathbb{Q}$ durch Radikale auflösbar ist. Die hier gegebene Darstellung

verwendet aber nicht-reelle komplexe Zahlen. Interessanterweise kann man zeigen, dass das auch nicht vermeidbar ist, das heißt, man kann $\cos(\frac{2\pi}{7})$ nicht durch die Grundrechenarten und das Ziehen von n-ten Wurzeln aus positiven reellen Zahlen darstellen (etwas formaler: $\cos(\frac{2\pi}{7})$ liegt nicht in dem kleinsten Teilkörper K von $\mathbb{R}$ mit der Eigenschaft, dass für alle $x \in \mathbb{R}$, $n \in \mathbb{N}_{>0}$ mit $x^n \in K$ auch x in K liegt). Der Beweis ist (mit dem, was wir schon wissen) nicht schwer zu verstehen, siehe [**Soe-AZT**] Abschnitt 4.8. □ Ergänzung 6.41

ERGÄNZUNG 6.42 (Arnolds Beweis, dass die allgemeine Gleichung vom Grad 5 nicht durch Radikale auflösbar ist). Der russische Mathematiker V. Arnold[3] (1937–2010) hat einen ganz anderen Beweis gegeben, dass es keine Lösungsformel für Gleichungen fünften Grades gibt, der keine Galois-Theorie verwendet, sondern auf topologischen Argumenten beruht. Damit erhält man sogar die noch stärkere Aussage, dass es keine Lösungsformel gibt, die nur die Grundrechenarten, die trigonometrischen Funktionen sin und cos und die Exponentialfunktion exp verwendet. (Das Wurzelziehen kann man dann mit der Exponentialfunktion ausdrücken.) Andererseits erhält man nicht die genauen Informationen über die Struktur der Körpererweiterung (zum Beispiel ihre Zwischenkörper), die die Galois-Theorie liefert. Siehe https://web.williams.edu/Mathematics/lg5/394/ArnoldQuintic.pdf für eine gut lesbare Darstellung des Beweises von Arnold. □ Ergänzung 6.42

6.5. Der Hauptsatz über symmetrische Polynome *

Für den Moment nur ein Platzhalter … Siehe zum Beispiel [**Bo-A**] *Abschnitte 4.3, 4.4;* [**Lo**] *Kapitel 15.*

6.6. Konstruierbarkeit mit Zirkel und Lineal

Mithilfe der Galois-Theorie können wir das Kriterium für Konstruierbarkeit mit Zirkel und Lineal, das wir in Satz 4.42 bewiesen haben, noch konkreter fassen. Wir verwenden die Notation aus Abschnitt 4.5.

SATZ 6.43. *Für $\alpha \in \mathbb{C}$ sind äquivalent:*

(i) *Es gilt $\alpha \in \mathbb{K}$, d.h. α ist ausgehend von 0 und 1 konstruierbar mit Zirkel und Lineal.*

(ii) *Es gibt eine endliche Kette*
$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_r$$
von Körpererweiterungen, so dass $[K_i : K_{i-1}] = 2$ für alle $i = 1, \ldots, r$ gilt und $\alpha \in K_r$ ist.

(iii) *Es gibt eine Galois-Erweiterung $K/\mathbb{Q}$ mit $\alpha \in K$, deren Grad eine Potenz von 2 ist.*

(iv) *Die normale Hülle von $\mathbb{Q}(\alpha)$ über $\mathbb{Q}$ hat als Grad über $\mathbb{Q}$ eine Potenz von 2.*

BEWEIS. Die Äquivalenz von (i) und (ii) haben wir bereits in Satz 4.42 bewiesen. Wenn (ii) gilt, dann erhalten wir für jeden Homomorphismus $\sigma\colon K_r \to \overline{\mathbb{Q}}$ in den algebraischen Abschluss von $\mathbb{Q}$ in $\mathbb{C}$ durch Anwenden von σ auf alle K_i eine Kette von Zwischenkörpern der Erweiterung $\sigma(K_r)/\mathbb{Q}$, deren einzelne Schritte alle Grad 2 haben. Damit folgt, dass für das Kompositum aller $\sigma(K_r)$, also den kleinsten Teilkörper von $\overline{\mathbb{Q}}$, der alle $\sigma(K_r)$ enthält, eine ebensolche Kette existiert. Aber dieses Kompositum ist genau die normale Hülle von K_r über $\mathbb{Q}$, also galoissch über $\mathbb{Q}$. Mit der Gradformel folgt die Aussage in (iii).

Ist andererseits (iii) gegeben, so können wir eine Kette von Untergruppen in der Galoisgruppe $\mathrm{Gal}(K/\mathbb{Q})$ finden, so dass die Indizes zwischen aufeinanderfolgenden Untergruppem alle gleich 2 sind. Denn nach Voraussetzung ist die Galois-Gruppe eine 2-Gruppe, so dass

[3] https://de.wikipedia.org/wiki/Wladimir_Igorewitsch_Arnold

wir Satz 2.76 und Lemma 2.64 anwenden können. Nach dem Hauptsatz der Galois-Theorie entspricht dieser Kette von Untergruppen eine Kette von Zwischenkörpern wie in Aussage (ii).

Schließlich sind (iii) und (iv) äquivalent. Dass (iii) aus (iv) folgt, ist trivial. Gilt andererseits (iii), dann ist die normale Hülle von $\mathbb{Q}(\alpha)$ über $\mathbb{Q}$ ein Teilkörper von K, und die Aussage folgt aus der Gradformel. □

Es folgt auch, dass eine komplexe Zahl $\alpha \in \mathbb{C}$, für die $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ eine Potenz von 2 ist, nicht notwendig konstruierbar ist. Ist nämlich das Minimalpolynom von α vom Grad 4 und mit Galois-Gruppe S_4, dann ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, aber die normale Hülle hat Grad 24 über $\mathbb{Q}$.

Mit diesem allgemeinen Ergebnis können wir insbesondere das Problem lösen, für welche n das (im Einheitskreis einbeschriebene) regelmäßige n-Eck ausgehend von 0 und 1 konstruierbar ist.

THEOREM 6.44. *Sei $n \geq 3$ eine natürliche Zahl. Dann sind äquivalent:*

(i) *Das regelmäßige n-Eck ist konstruierbar mit Zirkel und Lineal (d.h. $\exp(\frac{2\pi i}{n}) \in \mathbb{K}$).*

(ii) *Die Zahl $\varphi(n)$ ist eine Potenz von 2 (wobei φ die Eulersche φ-Funktion bezeichnet, d.h. $\varphi(n)$ ist die Anzahl der zu n teilerfremden Zahlen zwischen 1 und n).*

BEWEIS. Wir schreiben $\zeta := \exp(\frac{2\pi i}{n})$. Aus dem vorherigen Satz folgt, dass Aussage (i) äquivalent dazu ist, dass $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ eine Potenz von 2 ist. Wir haben in Satz 6.22 berechnet, dass dieser Grad gleich $\varphi(n)$ ist. □

Mit dem Begriff der Fermatschen Primzahl können wir das Kriterium noch etwas griffiger formulieren.

DEFINITION 6.45. Eine Primzahl der Form $2^k + 1$ mit $k \in \mathbb{N}_{>0}$ heißt *Fermatsche Primzahl*. Es ist dann notwendigerweise k selbst eine Potenz von 2. Wir schreiben $F_r = 2^{2^r} + 1$. ⊣

Zur Begründung der in der Definition gemachten Behauptung: Ist d ungerade, dann ist -1 eine Nullstelle von $X^d + 1$, also $X + 1$ ein Teiler von $X^d + 1$ (in $\mathbb{Z}[X]$). Ist $m \in \mathbb{N}_{>0}$, so folgt, dass $2^m + 1$ ein Teiler von $(2^m)^d + 1$ ist. Ist $d > 1$, so handelt es sich um einen echten Teiler.

Die einzigen bekannten Fermatschen Primzahlen sind $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257$ und $F_4 = 65537$. Euler zeigte, dass $2^{2^5} + 1$ durch 641 teilbar und mithin keine Primzahl ist. Es ist ein offenes Problem, ob es weitere solche Primzahlen gibt, und ist auch nicht bekannt, ob es möglicherweise sogar unendlich viele Fermatsche Primzahlen gibt. Von F_{33} ist zurzeit nicht bekannt, ob es sich um eine Primzahl handelt; diese Zahl hat über zweieinhalb Milliarden Stellen. Weitere Informationen: Wikipedia[4]

KOROLLAR 6.46. *Sei $n \geq 3$ eine natürliche Zahl. Dann sind äquivalent:*

(i) *Das regelmäßige n-Eck ist konstruierbar mit Zirkel und Lineal (d.h. $\exp(\frac{2\pi i}{n}) \in \mathbb{K}$).*

(ii) *Die Zahl n hat die Form $2^r p_1 \cdot \cdots \cdot p_l$ mit $r, l \geq 0$ und mit paarweise verschiedenen Fermatschen Primzahlen p_i.*

BEWEIS. Die φ-Funktion ist multiplikativ für teilerfremde Zahlen, d.h. für teilerfremde m, m' gilt $\varphi(mm') = \varphi(m)\varphi(m')$. Für eine Primzahlpotenz p^r gilt $\varphi(p^r) = (p-1)p^r$ (Lemma 2.44). Daraus folgt die Behauptung, indem wir n als Produkt von Potenzen paarweise verschiedener Primzahlen schreiben und das vorherige Ergebnis anwenden. □

Wir sehen also, dass das regelmäßige 5-Eck und das regelmäßige 17-Eck konstruierbar sind, nicht jedoch das regelmäßige 7-Eck.

[4] `https://de.wikipedia.org/wiki/Fermat-Zahl`

6.7. Das quadratische Reziprozitätsgesetz *

Das quadratische Reziprozitätsgesetz ist ein berühmter Satz aus der Zahlentheorie, der eine verblüffende Gesetzmäßigkeit über die Frage aussagt, welche quadratischen Gleichungen über endlichen Körpern der Form $\mathbb{F}_p$, p eine Primzahl, lösbar sind, oder genauer: Welche Elemente von $\mathbb{F}_p$ »Quadratzahlen«, also von der Form a^2 für ein $a \in \mathbb{F}_p$ sind.

6.7.1. Das Legendre-Symbol und das quadratische Reziprozitätsgesetz. Um zu untersuchen, welche Elemente eines endlichen Körpers Quadrate sind, bemerken wir zunächst, dass das für das Element $0 = 0^2$ offenbar stets der Fall ist, so dass wir nur Elemente von $\mathbb{F}_p^\times$ betrachten müssen. Der Fall $p = 2$ ist auch klar (sowohl 0 als auch 1 sind Quadrate) und unterscheidet sich ein bisschen von den anderen Fällen, so dass wir nun $p > 2$ voraussetzen. Die Abbildung

$$\mathbb{F}_p^\times \to \mathbb{F}_p^\times, \quad x \mapsto x^2,$$

ist ein Gruppenhomomorphismus mit Kern $\{1, -1\}$, und wir sehen, dass genau die Hälfte der Elemente von $\mathbb{F}_p^\times$ im Bild $(\mathbb{F}_p^\times)^2$ dieser Abbildung liegt, also das Quadrat eines Elements ist. Da $x^{p-1} = 1$ für alle $x \in \mathbb{F}_p^\times$ gilt, folgt für $x \in (\mathbb{F}_p^\times)^2$, etwa $x = a^2$, dass

$$x^{\frac{p-1}{2}} = a^{p-1} = 1.$$

Das Polynom $X^{\frac{p-1}{2}} - 1$ hat aber höchstens $\frac{p-1}{2}$ Nullstellen, daher haben nur die Quadrate x in $\mathbb{F}_p^\times$ die Eigenschaft $x^{\frac{p-1}{2}} = 1$; ist $x \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2}$, so muss $x^{\frac{p-1}{2}} = -1$ gelten (denn das Quadrat von $x^{\frac{p-1}{2}}$ ist ja $= 1$). Damit haben wir bewiesen:

LEMMA 6.47. *Sei p eine ungerade Primzahl. Ein Element $x \in \mathbb{F}_p^\times$ ist genau dann ein Quadrat in $\mathbb{F}_p^\times$, wenn $x^{\frac{p-1}{2}} = 1$ gilt.*

Dieses Lemma motiviert die folgende Definition.

DEFINITION 6.48. Sei p eine ungerade Primzahl und $x \in \mathbb{F}_p^\times$. Wir definieren das *Legendre-Symbol* durch

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{wenn } x \in (\mathbb{F}_p^\times)^2, \\ -1 & \text{wenn } x \in \mathbb{F}_p^\times \setminus (\mathbb{F}_p^\times)^2. \end{cases}$$

(Der Wert des Legendre-Symbols soll per Definition in $\mathbb{Z}$ oder einfach in der multiplikativen Gruppe $\{1, -1\}$ liegen, d.h. 1 und -1 werden hier nicht als Elemente eines endlichen Körpers betrachtet, weil wir später darüber sprechen wollen, wann Legendre-Symbole zu unterschiedlichen Primzahlen gleich sind.)

Für ganze Zahlen x, die zu p teilerfremd sind, definieren wir das Legendre-Symbol, indem wir die obigen Definition auf die Restklasse von x in $\mathbb{F}_p$ anwenden. ⊣

Hier ist also das Symbol $\left(\frac{x}{p}\right)$ als Gesamtpaket zu lesen – zwischen den Klammern steht keine Bruchzahl! Und deswegen kann man die Klammern natürlich auch nicht weglassen, weil sonst Verwirrung vorprogrammiert wäre. Weil wir das Legendre-Symbol als ganze Zahl betrachten, ist für $x \in \mathbb{F}_p^\times$ der Ausdruck $x^{\frac{p-1}{2}}$ (ein Element in $\mathbb{F}_p$) nicht *gleich* dem Legendre-Symbol, aber kongruent modulo p und daher eindeutig durcheinander bestimmt (weil p ungerade ist, gilt ja $1 \neq -1$ in $\mathbb{F}_p$).

Man kann die Definition des Legendre-Symbols auf den Fall ausdehnen, dass x ein Vielfaches von p ist (dann definiert man den Wert des Symbols als 0), aber für uns spielt das keine Rolle. Weitere Verallgemeinerungen, die nützlich sind, wenn man Legendre-Symbole mit Hilfe des quadratischen Reziprozitätsgesetzes tatsächlich ausrechnen möchte, sind das Jacobi- und das Kronecker-Symbol.

Aus der Definition und der vorherigen Diskussion erhalten wir sofort die folgenden einfachen Eigenschaften des Legendre-Symbols.

LEMMA 6.49 (Eigenschaften des Legendre-Symbols). *Sei p eine ungerade Primzahl. Seien $a, b \in \mathbb{Z}$ zu p teilerfremd.*

(1) *Das Legendre-Symbol ist multiplikativ, d.h. es gilt* $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

(2) *Es gilt* $\left(\frac{1}{p}\right) = 1$.

Das schon angekündigte quadratische Reziprozitätsgesetz stellt eine a priori völlig überraschende Beziehung zwischen den Legendre-Symbolen zu *verschiedenen* ungeraden Primzahlen her.

THEOREM 6.50 (Quadratisches Reziprozitätsgesetz). *Seien $p \neq q$ ungerade Primzahlen. Dann gilt*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)$$

Den Beweis geben wir weiter unten (genauer: einen von sehr vielen, und zwar einen, der Methoden der Galois-Theorie benutzt und dadurch »erhellender« ist als zum Beispiel der rein gruppentheoretische Beweis, den Sie in Ergänzung LA1.8.62 finden).

Zusammen mit den »Ergänzungssätzen« (Theorem 6.52) und der Multiplikativität des Legendre-Symbols kann man damit Legendre-Symbole mit geringem Aufwand ausrechnen (siehe Beispiel 6.54). Hauptsächlich liegt aber die Bedeutung des quadratischen Reziprozitätsgesetzes darin, dass hier eine zahlentheoretische Struktur sichtbar wird, deren besseres Verständnis und geeignete Verallgemeinerungen seit seiner Entdeckung (Euler hat diesen Satz um 1750 vermutet, Gauß konnte ihn als erster um 1800 beweisen) ein Antriebsmotor für die Entwicklung der Zahlentheorie gewesen ist und weiterhin ist.

6.7.2. Der quadratische Zwischenkörper von $\mathbb{Q}(\zeta_p)\big/\mathbb{Q}$.

SATZ 6.51. *Sei $p > 2$ eine Primzahl und sei $\zeta_p \in \overline{\mathbb{Q}}$ eine primitive p-te Einheitswurzel. Die Körpererweiterung $\mathbb{Q}(\zeta_p)\big/\mathbb{Q}$ besitzt einen eindeutig bestimmten Zwischenkörper E mit $[E:\mathbb{Q}] = 2$, und zwar ist dies der Körper $\mathbb{Q}(\sqrt{p^*})$ mit*

$$p^* = \left(\frac{-1}{p}\right)p = \begin{cases} p & \text{wenn } p \equiv 1 \mod 4, \\ -p & \text{wenn } p \equiv 3 \mod 4. \end{cases}$$

BEWEIS. Sei ζ eine primitive p-te Einheitswurzel über $\mathbb{Q}$. Es gilt $\operatorname{minpol}_{\zeta,\mathbb{Q}} = X^{p-1} + \cdots + 1$ (siehe Beispiel 3.55). Wir haben gesehen, dass $G := \operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/p)^\times$ gilt (Satz 6.22), und dies ist eine zyklische Gruppe (Korollar 2.49). Insbesondere gibt es in G genau eine Untergruppe vom Index 2. Dies übersetzt sich mit dem Hauptsatz der Galois-Theorie in die Tatsache, dass die Erweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$ einen eindeutig bestimmten Zwischenkörper E mit $[E:\mathbb{Q}] = 2$ besitzt.

Um E zu bestimmen, versuchen wir, ein Element $\alpha \in E$ »explizit« anzugeben, das nicht in $\mathbb{Q}$ liegt, aber so dass das Quadrat α^2 eine rationale Zahl ist. Offenbar gilt dann $E = \mathbb{Q}(\alpha)$. Statt das Ergebnis »vom Himmel fallen zu lassen«, wollen wir uns an dieser Stelle etwas mehr Zeit nehmen und illustrieren, wie man (mit genügend Ausdauer und den richtige Ideen …) darauf kommen könnte.

Wir bezeichnen mit $H \subseteq G$ die eindeutig bestimmte Untergruppe von G vom Index 2 (unter dem Isomorphismus $G \cong (\mathbb{Z}/p)^\times$ entspricht H der Untergruppe $\mathbb{F}_p^{\times 2}$ der Quadrate in $\mathbb{F}_p^\times$);

hier sehen wir einen ersten Hinweis, dass die folgenden Untersuchungen einen Zugang zum Reziprozitätsgesetz geben könnten. Zuerst bemerken wir, dass wir die Elemente von E etwas expliziter angeben können als

$$E = \mathbb{Q}(\zeta)^H = \left\{ \sum_{\sigma\in H} \sigma(x);\ x \in \mathbb{Q}(\zeta) \right\}.$$

Denn dass die rechte Seite in $\mathbb{Q}(\zeta)^H$ liegt, ist klar, und ist $z \in E$, so gilt $z = \frac{1}{\#H} \sum_{\sigma\in H} \sigma(z)$. (Vergleiche Satz 6.13, aus dem die Inklusion $\subseteq$, und damit die Gleichheit, für jede separable Körpererweiterung folgt, auch dann, wenn die Charakteristik die Ordnung $\#H$ teilt.)

Sei $\gamma \in G$ ein Erzeuger dieser zyklischen Gruppe. Die Galois-Gruppe $\mathrm{Gal}(E/\mathbb{Q})$ hat zwei Elemente und wird vom Bild von γ erzeugt. Wir bezeichnen dieses Bild (das ja einfach die Einschränkung von γ auf E ist) ebenfalls mit γ.

Wir wollen ein Element α mit $E = \mathbb{Q}(\alpha)$ und $\alpha^2 \in \mathbb{Q}$ angeben. Diese beiden Bedingungen sind zusammengenommen dazu äquivalent, dass $\alpha \neq 0$ und $\gamma(\alpha) = -\alpha$ gilt, also dass α ein Eigenvektor zum Eigenwert -1 von γ ist, wenn wir diese Abbildung als $\mathbb{Q}$-Vektorraum-Homomorphismus auffassen. Nun gilt $\gamma \neq \mathrm{id}$ und $\gamma^2 = \mathrm{id}$. Der Homomorphismus γ hat also Minimalpolynom $X^2 - 1$ und ist diagonalisierbar mit den Eigenwerten 1 und -1. Der Eigenraum zum Eigenwert 1 ist genau der Fixkörper von γ, also $\mathbb{Q}$. Der Eigenraum zum Eigenwert -1 ist ein eindimensionaler Komplementärraum dazu. Insbesondere ist α wie oben eindeutig bestimmt bis auf ein Skalar aus $\mathbb{Q}^\times$. Konkret können wir den Eigenraum zum Eigenwert -1 angeben als

$$\{z - \gamma(z);\ z \in E\}.$$

Dies ist ein sehr spezieller Fall von Satz LA2.17.13. In der speziellen Situation hier genügt es auch zu bemerken, dass Elemente der Form $z - \gamma(z)$ von γ auf ihr Negatives abgebildet werden und die Menge aller dieser Elemente ein Untervektorraum von E ist, der wegen $\gamma \neq \mathrm{id}$ nicht 0 sein kann.

Um $\alpha \in E$ mit $E = \mathbb{Q}(\alpha)$ und $\alpha^2 \in \mathbb{Q}$ anzugeben, genügt es also, irgendein $z \in E$ zu finden, für das $\alpha := z - \gamma(z) \neq 0$ ist. Wir machen dazu, vergleiche die vorhergehende Überlegung, den Ansatz $z = \sum_{\sigma\in H} \sigma(\zeta)$. Wenn wir das direkt mit dem Isomorphismus $G \cong \mathbb{F}_p^\times$ übersetzen (unter dem H der Untergruppe $\mathbb{F}_p^{\times 2}$ und daher die Nebenklasse γH der Menge $\mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2}$ der Nicht-Quadrate entspricht), gelangen wir zu der Definition

$$\alpha := \sum_{a\in\mathbb{F}_p^\times} \left(\frac{a}{p}\right) \zeta^a.$$

Weil die Elemente $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\zeta)$ bilden, ist klar, dass $\alpha \neq 0$ gilt, also $E = \mathbb{Q}(\alpha)$ und $\alpha^2 \in \mathbb{Q}$.

Wir wollen nun noch α^2 ausrechnen. Wir werden sehen, dass $\alpha^2 = p^*$ gilt; damit ist dann der Satz bewiesen. Wir müssen also

$$\alpha^2 = \sum_{a,b\in\mathbb{F}_p^\times} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \zeta^{a+b}$$

berechnen. Wir benutzen dazu, dass das Legendre-Symbol multiplikativ ist und dass für fixiertes $b \in \mathbb{F}_p^\times$ mit a auch ab die Menge $\mathbb{F}_p^\times$ durchläuft (wir also per »Indexverschiebung« in jedem Summanden a durch ab ersetzen können) und dass trivialerweise $\left(\frac{b^2}{p}\right) = 1$ ist. Also erhalten wir

$$\alpha^2 = \sum_{a,b\in\mathbb{F}_p^\times} \left(\frac{ab}{p}\right)\left(\frac{b}{p}\right) \zeta^{ab+b} = \sum_{a\in\mathbb{F}_p^\times} \left(\frac{a}{p}\right) \sum_{b\in\mathbb{F}_p^\times} (\zeta^{a+1})^b.$$

Für $a \neq -1$ ist ζ^{a+1} wieder eine primitive p-te Einheitswurzel, also eine Nullstelle von $X^{p-1} + \cdots + X + 1$; das bedeutet $\sum_{b \in \mathbb{F}_p^\times} (\zeta^{a+1})^b = -1$. Wir erhalten also

$$\alpha^2 = \left(\frac{-1}{p}\right)(p-1) - \sum_{a \in \mathbb{F}_p^\times,\, a \neq -1} \left(\frac{a}{p}\right).$$

Schließlich benutzen wir noch, dass $\sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) = 0$ gilt, weil $\mathbb{F}_p^\times$ ebenso viele Quadrate wie Nicht-Quadrate enthält. Damit folgt die Behauptung $\alpha^2 = \left(\frac{-1}{p}\right) p$. □

6.7.3. Beweis des quadratischen Reziprozitätsgesetz. Wir benutzen dieselbe Notation wie im vorherigen Abschnitt. Seien jetzt $p \neq q$ verschiedene ungerade Primzahlen. (Achtung: Hier ist also, anders als in Abschnitt 5.4, q nicht eine Potenz von p!) Sei wieder $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, $E = \mathbb{Q}(\sqrt{p^*})$ der eindeutig bestimmte quadratische Zwischenkörper von $\mathbb{Q}(\zeta)/\mathbb{Q}$ und $H \subset G$ die Galois-Gruppe von $\mathbb{Q}(\zeta)/E$.

Um das quadratische Reziprozitätsgesetz zu beweisen, müssen wir eine Beziehung zwischen Quadraten in $\mathbb{F}_p^\times$ und in $\mathbb{F}_q^\times$ herstellen. Unser Zugang beruht darauf, die Gruppe $\mathbb{F}_p^\times$ als die Galois-Gruppe G zu betrachen, und die Menge der Quadrate in $\mathbb{F}_p^\times$ dementsprechend mit H zu identifizieren.

Die Aussage, dass $\left(\frac{q}{p}\right) = 1$ ist, ist angesichts dieser Interpretation dazu äquivalent, dass der Homomorphismus $\sigma_q \colon \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ mit $\sigma_q(\zeta) = \zeta^q$ in H liegt. Weil $\mathbb{Q}(\zeta)^H = \mathbb{Q}(\alpha)$ ist, ist das wiederum dazu äquivalent, dass $\sigma_q(\alpha) = \alpha$ gilt:

$$\left(\frac{q}{p}\right) = 1 \quad \Longleftrightarrow \quad \sigma_q(\alpha) = \alpha.$$

Um den Körper $\mathbb{F}_q$ ins Spiel zu bringen, betrachten wir die Einschränkung von σ_q auf den Ring $\mathbb{Z}[\zeta] = \{\sum_{i=0}^{p-2} a_i \zeta^i;\ a_i \in \mathbb{Z}\} \cong \mathbb{Z}[X]/(X^{p-1} + \cdots + X + 1)$. Weil $\sigma_q(\zeta) \in \{\zeta, \zeta^2, \ldots, \zeta^{p-1}\}$ gilt, erhalten wir tatsächlich einen Ringhomomorphismus $\sigma_q \colon \mathbb{Z}[\zeta] \to \mathbb{Z}[\zeta]$. Durch Übergang zum Quotienten nach dem von q erzeugten Ideal erhalten wir

$$\mathbb{Z}[\zeta]/(q) \cong \mathbb{F}_q[\overline{\zeta}] \cong \mathbb{F}_q[X]/(X^{p-1} + \cdots + X + 1),$$

wobei $\overline{\zeta}$ das Bild von ζ in $\mathbb{Z}[\zeta]/(q)$, oder im Sinne des Isomorphimus mit der rechten Seite die Restklasse von X bezeichne. Entsprechend induziert σ_q einen Ringhomomorphismus

$$\mathbb{F}_q[\overline{\zeta}] \to \mathbb{F}_q[\overline{\zeta}], \quad \overline{\zeta} \mapsto \overline{\zeta}^q.$$

Weil $a^q = a$ für alle $a \in \mathbb{F}_q$ gilt, ist diese Abbildung einfach der q-Frobenius-Homomorphismus des Rings $\mathbb{F}_q[\overline{\zeta}]$ (Beispiel 3.2), der jedes Element aus $\mathbb{F}_q[\overline{\zeta}]$ auf seine q-te Potenz abbildet.

Sei $\overline{\alpha}$ das Bild von $\alpha \in \mathbb{Z}[\zeta]$ in $\mathbb{F}_q[\overline{\zeta}]$. Weil q ungerade ist und $\overline{\alpha}^2$ die Restklasse von p^* in $\mathbb{F}_q$, also von Null verschieden, ist, ist $\overline{\alpha} \neq -\overline{\alpha}$. Deshalb gilt $\sigma_q(\alpha) = \alpha$ genau dann, wenn $\overline{\alpha}^q = \sigma_q(\overline{\alpha}) = \overline{\alpha}$ ist.

Aber die Gleichheit $\overline{\alpha}^q = \overline{\alpha}$ ist äquivalent zu

$$(p^*)^{\frac{q-1}{2}} = (\overline{\alpha^2})^{\frac{q-1}{2}} = \overline{\alpha}^{q-1} = 1$$

in $\mathbb{F}_q[\overline{\zeta}]$.

Nun wissen wir, dass $(p^*)^{\frac{q-1}{2}} \equiv \left(\frac{p^*}{q}\right) \mod q$ gilt. Insgesamt haben wir damit

$$\left(\frac{q}{p}\right) = 1 \quad \Longleftrightarrow \quad \sigma_q(\alpha) = \alpha \quad \Longleftrightarrow \quad \left(\frac{p^*}{q}\right) = 1,$$

und das ist genau die Behauptung des quadratischen Reziprozitätsgesetzes.

> ... that it was only on reading it [Hermann Weyls Buch *Algebraic Theory of Numbers*] that I began to appreciate the beauty of the law of quadratic reciprocity to which I had earlier attached no importance.
>
> R. Langlands[a], https://publications.ias.edu/rpl/paper/2664.

Langlands hat seit Ende der 1960er Jahre das nunmehr sogenannte *Langlands-Programm* entwickelt, eine umfangreiche Theorie aus Vermutungen und Ergebnissen, von denen ein Kernpunkt die Verallgemeinerung des quadratischen Reziprozitätsgesetzes ist. Er wurde dafür 2018 mit dem Abel-Preis ausgezeichnet. Schon davor wurden unter anderem im Rahmen der *Klassenkörpertheorie* erste Verallgemeinerungen dieses Resultats bewiesen.

[a] `https://de.wikipedia.org/wiki/Robert_Langlands`

6.7.4. Die Ergänzungssätze. Um für beliebige $a \in \mathbb{F}_p^\times$ das Legendre-Symbol $\left(\frac{a}{p}\right)$ zu berechnen, betrachten wir die Primfaktorzerlegung eines Repräsentanten von $a \in \mathbb{Z}$. Damit ist die Berechnung reduziert auf die Berechnung von Legendre-Symbolen der Form $\left(\frac{q}{p}\right)$ für ungerade Primzahlen $q \neq p$ und der Form $\left(\frac{2}{p}\right)$ und Form $\left(\frac{-1}{p}\right)$.

Zur Berechnung von $\left(\frac{q}{p}\right)$ können wir q durch seine Restklasse in $\{1, \ldots, p-1\}$ modulo p ersetzen (und gegebenenfalls diese in Primfaktoren zerlegen) bzw., falls $q < p$ ist, das quadratische Reziprozitätsgesetz anwenden und dann zur Berechnung von $\left(\frac{p}{q}\right)$ die Zahl p durch ihre Restklasse in $\{1, \ldots, q-1\}$ modulo q ersetzen. So führt man die Berechnung schrittweise auf die Berechnung von Legendre-Symbolen mit immer kleineren Zahlen zurück.

Die Fälle $\left(\frac{2}{p}\right)$ und $\left(\frac{-1}{p}\right)$ schließlich werden durch die sogenannten Ergänzungssätze behandelt.

THEOREM 6.52 (Ergänzungssätze zum quadratischen Reziprozitätsgesetz). *Sei q eine ungerade Primzahl.*

(1) *Es gilt*
$$\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}.$$

(2) *Es gilt*
$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}.$$

Wir könnten in diesem Satz natürlich die betrachtete Primzahl ebenso gut mit p statt mit q benennen (und so wird er auch meistens formuliert, weil eben nur eine Primzahl vorkommt und man dann standardmäßig zuerst den Buchstaben p benutzt), aber wir wählen hier das Symbol q, damit die Analogie des Beweises von Teil (2) mit dem obigen Beweis des quadratischen Reziprozitätsgesetz selbst besser sichtbar wird.

BEWEIS. Die Aussage von Teil (1) haben wir schon gesehen, sie ist hier nur noch einmal aufgelistet, weil diese Aussage traditionell als der erste Ergänzungssatz zum quadratischen Reziprozitätsgesetz bezeichnet wird.

Teil (2). Wir argumentieren ähnlich wie im Beweis des quadratischen Reziprozitätsgesetzes selbst. Statt einer p-ten Einheitswurzel betrachten wir nun die primitive 8-te Einheitswurzel $\zeta = e^{\frac{2\pi i}{8}} \in \mathbb{C}$ und den Körper $\mathbb{Q}(\zeta)$. (Gewissermaßen ist einer der Knackpunkte des Beweises, dass man an dieser Stelle mit einer »zweiten Einheitswurzel« nichts ausrichten kann und eine geeignet größere, aber analoge, Erweiterung betrachten sollte, um »etwas sehen« zu können.) Die Körpererweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$ ist galoissch vom Grad 4 mit Galois-Gruppe $\cong (\mathbb{Z}/8)^\times$. (Die Gruppe $(\mathbb{Z}/8)^\times$ ist nicht zyklisch, sondern isomorph zu $\mathbb{Z}/2 \times \mathbb{Z}/2$, denn alle Elemente $\neq 1$ haben Ordnung 2.)

Es gilt $\zeta = \frac{1+i}{\sqrt{2}}$, also $\alpha := \zeta + \zeta^{-1} = \frac{1+i}{\sqrt{2}} + \frac{1-i}{\sqrt{2}} = \sqrt{2}$. Es ist also $\mathbb{Q}(\sqrt{2})$ ein Zwischenkörper der Erweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$. Wir betrachten den Körperhomomorphismus $\sigma_q \colon \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ mit $\zeta \mapsto \zeta^q$ bzw. ähnlich wie vorher seine Einschränkung $\sigma_q \colon \mathbb{Z}[\zeta] \longrightarrow \mathbb{Z}[\zeta]$. Sei außerdem $\mathbb{F}_q[\overline{\zeta}]$ analog wie vorher der Quotient von $\mathbb{Z}[\zeta]$ nach dem von q erzeugten Ideal. Auf diesem Quotienten induziert σ_q den q-Frobenius-Homomorphismus $x \mapsto x^q$. Sei $\overline{\alpha}$ das Bild von $\alpha = \sqrt{2}$ in $\mathbb{F}_q[\overline{\zeta}]$.

Es ist also 2 ein Quadrat in $\mathbb{F}_q^\times$ genau dann, wenn $\overline{\alpha}^q = \overline{\alpha}$, oder äquivalent, wenn $\sigma_q(\alpha) = \alpha$ gilt. Das wiederum entspricht der Bedingung $\sigma_q \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\alpha))$, und diese Untergruppe entspricht unter dem Isomorphismus $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q} \cong (\mathbb{Z}/8)^\times$ der Untergruppe $\{1, -1\}$. Damit erhalten wir, dass $\left(\frac{2}{q}\right) = 1$ äquivalent ist zu der Bedingung, dass $q \equiv 1 \mod 8$ oder $q \equiv -1 \mod 8$. Das bedeutet aber genau, dass $q+1$ oder $q-1$ durch 8 teilbar ist, oder anders gesagt, dass $\frac{q^2-1}{8}$ gerade ist. □

KOROLLAR 6.53. *Seien $a, b, c \in \mathbb{Z}$, $a \neq 0$. Dann existieren natürliche Zahlen $p_0, n \in \mathbb{N}_{>0}$, so dass die Lösbarkeit der quadratischen Gleichung $ax^2 + bx + c$ für Primzahlen $p \geq p_0$ nur von der Restklasse von p modulo n abhängt. Die Frage der Lösbarkeit ist also sozusagen »periodisch in p«.*

BEWEIS. Ist K ein Körper mit Charakteristik $\neq 2$ und $\alpha x^2 + \beta x + \gamma = 0$ eine quadratische Gleichung mit Koeffizienten in K ($\alpha \neq 0$), dann ist die Gleichung lösbar genau dann, wenn das Element $\beta - 4\alpha\gamma$ in K eine Quadratwurzel besitzt.

Wir wählen nun p_0 so groß, dass $p_0 > 2$ und alle Primteiler von $b - 4ac$ kleiner als p_0 sind. Die gegebene Gleichung hat dann für $p \geq p_0$ eine Lösung in $\mathbb{F}_p$ genau dann, wenn $\left(\frac{b-4ac}{p}\right) = 1$ gilt. Zerlegen wir $b - 4ac$ als Produkt von Primzahlen, so können wir dieses Legendre-Symbol mithilfe des quadratischen Reziprozitätsgesetzes schreiben als Produkt von Faktoren der folgenden Form (nicht alle müssen auftreten): -1, $\left(\frac{2}{p}\right)$, $\left(\frac{p}{q}\right)$ für Primzahlen q, die $b - 4ac$ teilen und daher $\leq p_0$ sind.

Weil $\left(\frac{p}{q}\right)$ nur von der Restklasse von p modulo q und $\left(\frac{2}{p}\right)$ nur von der Restklasse von p modulo 8 abhängt (letzteres nach dem zweiten Ergänzungssatz), folgt die Behauptung. □

BEISPIEL 6.54. Als konkretes Beispiel berechnen wir, ob 23 ein Quadrat modulo 127 ist. Man könnte natürlich die Restklassen von $1^2, 2^2, 3^2, \ldots$ in $\mathbb{F}_{127}$ berechnen und mit 23 vergleichen. Mit dem quadratischen Reziprozitätsgesetz geht es aber leichter. Mit der Rechnung

$$\left(\frac{23}{127}\right) = -\left(\frac{127}{23}\right) = -\left(\frac{12}{23}\right) = -\left(\frac{4}{23}\right)\left(\frac{3}{23}\right) = \left(\frac{23}{3}\right) = \left(\frac{-1}{3}\right) = -1$$

sehen wir, dass 23 kein Quadrat in $\mathbb{F}_{127}$ ist. Mit der direkten Methode hätten wir *alle* Quadrate in $\mathbb{F}_{127}$ berechnen müssen, um auszuschließen, dass 23 dabei ist. ◊

Weitere Quellen zum quadratischen Reziprozitätsgesetz sind Ergänzung LA1.8.62, [**Lo**] Kapitel 11, [**Se**] §I.3.

6.8. Ergänzungen *

Das einzige Beispiel einer nicht-trivialen *endlichen* Körpererweiterung L/K, in der L algebraisch abgeschlossen ist, das wir kennengelernt haben, ist die Erweiterung $\mathbb{C}/\mathbb{R}$. Es gibt zwar noch andere solche Erweiterungen (zum Beispiel $\overline{\mathbb{Q}}/\overline{\mathbb{Q}} \cap \mathbb{R}$ – Übung!), aber der folgende Satz von Artin zeigt, dass sie der vorgenannten sehr ähnlich sind, insbesondere muss eine solche Erweiterung Grad 2 haben.

Satz 6.55 (E. Artin). *Sei L/K eine endliche Körpererweiterung vom Grad > 1. Wenn L algebraisch abgeschlossen ist, dann ist $[L : K] = 2$ und es existiert ein Element $i \in L$ mit $i^2 = -1$ und $L = K(i)$.*

Für einen Beweis siehe zum Beispiel [**Bo-A**] Satz 6.3/2.

ANHANG A

Zusammenfassung *

Die Definitionen und Ergebnisse, die wir aus der Linearen Algebra wiederholt haben, sind in der Zusammenfassung nicht noch einmal aufgeführt.

A.1. Gruppen

A.1.1. Gruppenwirkungen.

DEFINITION A.1. Seien G eine Gruppe und X eine Menge. Eine *Wirkung* (oder: *Operation*) ist eine Abbildung

$$G \times X \to X, (g, x) \mapsto g \cdot x,$$

die die folgenden Eigenschaften hat:

(a) $(gh) \cdot x = g \cdot (h \cdot x)$ für alle $g, h \in G$ und alle $x \in X$,

(b) $1 \cdot x = x$ für alle $x \in X$ (wobei $1 \in G$ das neutrale Element bezeichne).

⊣

In äquivalenter Weise können wir eine Wirkung von G auf X als einen Gruppenhomomorphismus $\varphi\colon G \to \mathrm{Bij}(X)$ betrachten; die Beziehung zwischen den beiden Sichtweisen ist durch $\varphi(g)(x) = g \cdot x$ gegeben. Oft schreibt man statt $g \cdot x$ auch einfach gx (oder benutzt gegebenenfalls ein anderes Symbol).

DEFINITION A.2. Sei $G \times X \to X, (g, x) \mapsto gx$ eine Gruppenwirkung.

(1) Die *Bahn* (oder: der *Orbit*) *eines Elements $x \in X$ unter der Gruppe G* ist die Teilmenge

$$Gx := \{gx;\ g \in G\} \subseteq X.$$

(2) Der *Stabilisator* eines Elements x ist die Untergruppe

$$\mathrm{Stab}_G(x) := \{g \in G;\ gx = x\}$$

von G.

⊣

BEISPIEL A.3. Sei G eine Gruppe. Dann ist $G \times G \to G, g \bullet h := ghg^{-1}$ eine Gruppenwirkung, die *Wirkung durch Konjugation* von G auf sich selbst.

Die Bahnen unter dieser Operation heißen die *Konjugationsklassen* der Gruppe G. Den Stabilisator eines Elements $h \in G$ unter der Konjugationswirkung nennen wir den *Zentralisator* von h und bezeichnen ihn mit Z_h. Es gilt also

$$Z_h = \{g \in G;\ ghg^{-1} = h\} = \{g \in G;\ gh = hg\}.$$

Allgemeiner sei für eine Teilmenge $S \in G$ der Zentralisator von S definiert als

$$Z_S = \bigcap_{h \in S} Z_h = \{g \in G;\ gh = hg \text{ für alle } h \in S\},$$

also als die Untergruppe von G derjenigen Elemente, die mit allen Elementen aus S kommutieren. Den Zentralisator der ganzen Gruppe G nennt man das *Zentrum* von G; dies ist ein abelscher Normalteiler in G. ◊

In der Situation der obigen Definition induziert für jedes $x \in X$ die Abbildung $g \mapsto gx$ eine Bijektion $G/\operatorname{Stab}_G(x) \to Gx$. Da X die disjunkte Vereinigung aller Bahnen unter G ist, folgt insbesondere:

SATZ A.4 (Bahnengleichung). *Sei G eine Gruppe, die auf eine endlichen Menge X operiert. Sei $x_1, \ldots, x_r$ ein Vertretersystem der Bahnen von X auf G, d.h. zu jeder Bahn $B \subset X$ in X unter G existiere ein eindeutig bestimmtes i mit $x_i \in B$. Dann gilt*

$$\#X = \sum_{i=1}^{r} \#Gx_i = \sum_{i=1}^{r} \#(G/\operatorname{Stab}_G(x_i)).$$

Im speziellen Fall der Wirkung einer endlichen Gruppe G auf sich selbst durch Konjugation erhalten wir:

SATZ A.5 (Klassengleichung). *Sei G eine endliche Gruppe und sei $g_1, \ldots, g_r$ ein Vertretersystem derjenigen Konjugationsklassen in G, die aus mehr als einem Element bestehen. Dann gilt*

$$\#G = \#Z_G + \sum_{i=1}^{r} \#(G/Z_{x_i}).$$

DEFINITION A.6. Eine Gruppenoperation heißt *transitiv*, wenn es nur eine einzige Bahn gibt. ⊣

A.1.2. Zyklische Gruppen.

DEFINITION A.7. Eine Gruppe G heißt *zyklisch*, wenn $g \in G$ existiert mit

$$G = \langle g \rangle = \{g^i;\ i \in \mathbb{Z}\}.$$

⊣

SATZ A.8. *Sei G eine Gruppe. Dann sind äquivalent:*

(i) *die Gruppe G ist zyklisch,*

(ii) *es gibt einen surjektiven Gruppenhomomorphismus $\mathbb{Z} \to G$,*

(iii) *G ist isomorph zu einer der Gruppen*

  (1) $\mathbb{Z}$,

  (2) $\mathbb{Z}/n$ *für* $n \geq 1$.

(iv) *zu jedem Teiler d der Gruppenordnung $\#G$ existiert genau eine Untergruppe $H \subseteq G$ mit d Elementen.*

Die Erzeuger von $\mathbb{Z}$ sind 1 und -1. Die Erzeuger von $\mathbb{Z}/n$ sind (für $n > 0$) die Restklassen von zu n teilerfremden Zahlen, also die Elemente von $(\mathbb{Z}/n)^\times$.

SATZ A.9. *Untergruppen und Quotienten von zyklischen Gruppen sind zyklisch. Insbesondere gilt: Ist $\varphi\colon G \to H$ ein Gruppenhomomorphismus und ist G zyklisch, so sind $\operatorname{Ker}(\varphi)$ und $\operatorname{Im}(\varphi)$ zyklisch.*

THEOREM A.10. *Sei G eine endliche Gruppe. Dann sind äquivalent:*

(i) *die Gruppe G ist zyklisch,*

(ii) *zu jedem Teiler d der Gruppenordnung $\#G$ existiert genau eine Untergruppe $H \subseteq G$ mit d Elementen,*

(iii) *zu jedem Teiler d der Gruppenordnung $\#G$ existiert höchstens eine Untergruppe $H \subseteq G$ mit d Elementen.*

SATZ A.11. *Sei K ein Körper und sei $G \subseteq K^\times$ eine endliche Untergruppe. Dann ist G zyklisch.*

A.1.3. Die symmetrische Gruppe. Wir bezeichnen mit S_n die *symmetrische Gruppe* »auf n Buchstaben«, also die Gruppe der Bijektionen $\{1, \dots, n\} \xrightarrow{\sim} \{1, \dots, n\}$. Aus der Linearen Algebra kennen wir den Begriff des r-Zykels, Definition LA1.8.36.

SATZ A.12 (Zerlegung in disjunkte Zykel). *Jede Permutation $\sigma \in S_n$ lässt sich als Produkt von Zykeln mit paarweise disjunkten Trägern schreiben. Diese Darstellung ist bis auf die Reihenfolge der Faktoren eindeutig.*

Jeder Permutation σ können wir ihr *Signum* oder *Vorzeichen* $\operatorname{sgn}(\sigma) \in \{1, -1\}$ zuordnen. Die Signumsabbildung $S_n \to \{1, -1\}$ ist ein Gruppenhomomorphismus.

DEFINITION A.13. Wir schreiben $A_n = \operatorname{Ker}(\operatorname{sgn})$ und nennen diesen Normalteiler von S_n die *alternierende Gruppe*. ⊣

A.1.4. Auflösbare Gruppen.

DEFINITION A.14. Sei G eine Gruppe.

(1) Für Elemente $g, h \in G$ heißt
$$[g, h] := ghg^{-1}h^{-1}$$
der *Kommutator* der Elemente g und h.

(2) Für Untergruppen $H, H' \subseteq G$ bezeichnen wir mit $[H, H']$ die von allen Elementen der Form $[h, h']$, $h \in H$, $h' \in H'$ erzeugte Untergruppe von G.

(3) Die Untergruppe $[G, G] \subseteq G$, also die von allen Elementen der Form $[g, h]$, $g, h \in G$, erzeugte Untergruppe von G, heißt die *Kommutatoruntergruppe* von G.

⊣

SATZ A.15. *Sei G eine Untergruppe. Dann ist $[G, G]$ ein Normalteiler von G und der Quotient $G_{ab} = G/[G, G]$ ist eine abelsche Gruppe und hat die folgende universelle Eigenschaft (und heißt deshalb der* maximale abelsche Quotient *der Gruppe G):*

Ist H eine abelsche Gruppe und $f\colon G \to H$ ein Gruppenhomomorphismus, so faktorisiert f eindeutig über G_{ab}.

DEFINITION A.16. Sei G eine Gruppe. Wir nennen G *auflösbar*, wenn eine Kette
$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$$
von Untergruppen von G existiert, so dass für alle i die Untergruppe G_{i+1} ein Normalteiler von G_i ist und der Quotient G_i / G_{i+1} eine abelsche Gruppe ist. ⊣

LEMMA A.17. *Sei G eine Gruppe. Sei $D^0G = G$, $D^1G := [G, G]$, und allgemein $D^iG = [D^{i-1}G, D^{i-1}G]$ für $i \geq 1$. Dann sind äquivalent:*

(i) *Die Gruppe G ist auflösbar.*

(ii) *Es existiert $n \in \mathbb{N}$, so dass D^nG die triviale Gruppe ist.*

LEMMA A.18. (1) *Sei G eine auflösbare Gruppe. Dann ist jede Untergruppe von G auflösbar.*

(2) *Sei G eine Gruppe und sei $H \subseteq G$ ein Normalteiler. Dann sind äquivalent:*

  (i) *Die Gruppe G ist auflösbar.*

  (ii) *Die Gruppen H und G/H sind auflösbar.*

(3) *Seien $G_1, \dots, G_n$ Gruppen. Das Produkt $\prod_{i=1}^n G_i$ ist genau dann auflösbar, wenn alle G_i, $i = 1, \dots, n$, auflösbar sind.*

LEMMA A.19. *Sei G eine endliche Gruppe. Dann sind äquivalent:*

(i) *Die Gruppe G ist auflösbar.*

(ii) *Es existiert eine Kette*

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_r = G$$

von Untergruppen von G, so dass für alle i die Untergruppe G_i ein Normalteiler von G_{i+1} ist und der Quotient G_{i+1} / G_i eine zyklische Gruppe ist.

SATZ A.20. (1) *Für $n \leq 4$ sind S_n und A_n auflösbar.*

(2) *Für $n > 4$ sind weder S_n noch A_n auflösbar.*

A.1.5. Die Sylow-Sätze.

DEFINITION A.21. Seien p eine Primzahl und G eine endliche Gruppe. Wir nennen G eine *p-Gruppe*, wenn die Ordnung von G eine Potenz von p ist. ⊣

SATZ A.22. *Jede p-Gruppe ist auflösbar.*

DEFINITION A.23. Sei G eine endliche Gruppe und sei p eine Primzahl. Sei $\#G = p^r m$ mit $p \nmid m$. Unter einer *p-Sylow-Untergruppe* von G verstehen wir eine Untergruppe $H \subseteq G$ mit $\#H = p^r$. ⊣

Mit anderen Worten ist also eine p-Sylow-Untergruppe von G eine Untergruppe H von G, die eine p-Gruppe ist und so dass $\#G / H$ nicht durch p teilbar ist.

BEISPIEL A.24. Seien $n \in \mathbb{N}$, p eine Primzahl und $G = GL_n(\mathbb{F}_p)$. Die Untergruppe U der oberen Dreiecksmatrizen, deren Diagonaleinträge alle $= 1$ sind, ist eine p-Sylow-Untergruppe von G. ◊

SATZ A.25 (Sylow-Sätze). *Sei G eine endliche Gruppe und sei p eine Primzahl.*

(1) *Die Gruppe G besitzt eine p-Sylow-Untergruppe.*

(2) *Je zwei p-Sylow-Untergruppen von G sind zueinander konjugiert.*

(3) *Sei s_p die Anzahl der p-Sylow-Untergruppen von G. Dann gilt*

$$s_p \mid \#G \quad \textit{und} \quad s_p \equiv 1 \mod p.$$

KOROLLAR A.26. *Sei G eine endliche Gruppe und sei p eine Primzahl.*

(1) *Jede Untergruppe von G, die eine p-Gruppe ist, ist in einer p-Sylow-Untergruppe enthalten.*

(2) *Eine Untergruppe H ist genau dann eine p-Sylow-Untergruppe von G, wenn H eine p-Gruppe ist und es keine Untergruppe von G gibt, die eine p-Gruppe ist und H als echte Untergruppe enthält.*

A.2. Ringe

Wenn nicht ausdrücklich etwas anderes gesagt wird, verstehen wir in dieser Vorlesung unter einem Ring stets einen *kommutativen Ring*.

A.2.1. Ideale, Primideale, maximale Ideale.

LEMMA A.27. *Seien K ein Körper, $R \neq 0$ ein Ring und $\varphi\colon K \to R$ ein Ringhomomorphismus. Dann ist φ injektiv.*

SATZ A.28. *Sei R ein Ring und sei $\mathfrak{a} \subseteq R$ ein Ideal. Sei $\pi\colon R \to R/\mathfrak{a}$ die kanonische Projektion. Dann sind die Abbildungen*

$$\begin{aligned} \{\mathfrak{b} \subseteq R \text{ Ideal};\ \mathfrak{a} \subseteq \mathfrak{b}\} &\xrightarrow{\sim} \{\mathfrak{c} \subseteq R/\mathfrak{a} \text{ Ideal}\} \\ \mathfrak{b} &\mapsto \pi(\mathfrak{b}), \\ \pi^{-1}(\mathfrak{c}) &\mapsfrom \mathfrak{c}, \end{aligned}$$

zueinander inverse, inklusionserhaltende Bijektionen.

DEFINITION A.29. Sei R ein Ring. Ein Ideal $\mathfrak{p} \subset R$ heißt *Primideal*, wenn $\mathfrak{p} \neq R$ gilt und wenn für alle $x, y \in R$ gilt: Falls $xy \in \mathfrak{p}$, dann ist $x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$. ⊣

LEMMA A.30. *Seien R ein kommutativer Ring und $\mathfrak{p} \subseteq R$ ein Ideal. Dann sind äquivalent:*

(i) *der Quotient $R/\mathfrak{p}$ ist ein Integritätsring,*

(ii) *das Ideal $\mathfrak{p}$ ist ein Primideal.*

DEFINITION A.31. Sei K ein Körper. Wir sagen, K habe *Charakteristik* 0, wenn der eindeutig bestimmte Ringhomomorphismus $\mathbb{Z} \to K$ injektiv ist, und habe *Charakteristik p*, wenn sein Kern von der Primzahl p erzeugt wird. ⊣

SATZ A.32. *Sei K ein Körper der Charakteristik $p > 0$. Dann ist die Abbildung*

$$K \to K, \quad x \mapsto x^p,$$

ein Körperhomomorphismus, der sogenannte Frobenius-Homomorphismus *von K.*

DEFINITION A.33. Sei R ein Ring. Ein Ideal $\mathfrak{m} \subset R$ heißt *maximales Ideal*, wenn $\mathfrak{m} \neq R$ ist und $\mathfrak{m}$ maximal mit dieser Eigenschaft bezüglich der Inklusion von Idealen ist, d.h. wenn für jedes Ideal $\mathfrak{a} \subseteq R$ mit $\mathfrak{m} \subseteq \mathfrak{a} \subseteq R$ gilt: $\mathfrak{a} = \mathfrak{m}$ oder $\mathfrak{a} = R$. ⊣

LEMMA A.34. *Sei R ein kommutativer Ring und $\mathfrak{m} \subseteq R$ ein Ideal. Dann sind äquivalent:*

(i) *der Quotient $R/\mathfrak{m}$ ist ein Körper,*

(ii) *das Ideal $\mathfrak{m}$ ist ein maximales Ideal.*

Insbesondere ist jedes maximale Ideal ein Primideal.

SATZ A.35. *Sei R ein Hauptidealring und $\mathfrak{p} \subset R$ ein Primideal, das nicht das Nullideal ist. Dann ist $\mathfrak{p}$ ein maximales Ideal von R.*

SATZ A.36. *Sei R ein Ring und sei $\mathfrak{a} \subsetneq R$ ein Ideal. Dann besitzt R ein maximales Ideal, das $\mathfrak{a}$ enthält. Insbesondere besitzt jeder Ring $R \neq 0$ ein maximales Ideal.*

Der Beweis beruht auf dem *Lemma von Zorn*, siehe Abschnitt LA1.B.1.

A.2.2. Polynomringe.

DEFINITION A.37. Sei R ein (kommutativer) Ring.

(1) Eine *R-Algebra* ist ein (kommutativer) Ring S zusammen mit einem Ringhomomorphismus $\varphi\colon R \to S$.

(2) Seien S, S' mit Ringhomomorphismen $\varphi\colon R \to S$, $\varphi'\colon R \to S'$ Algebren über R. Ein *Homomorphismus von R-Algebren* ist ein Ringhomomorphismus $\psi\colon S \to S'$, so dass $\varphi = \varphi' \circ \psi$ gilt.

   Wir bezeichnen mit $\mathrm{Hom}_R(S, S')$ die Menge aller R-Algebren-Homomorphismen von S nach S'. Besonders dann, wenn R ein Körper ist, sprechen wir statt von einem R-Algebren-Homomorphismus auch einfach von einem K-Homomorphismus.

⊣

Ist K ein Körper und A eine K-Algebra, gegeben durch einen Ringhomomorphismus $\varphi\colon K \to A$, so können wir A als K-Vektorraum mit der Skalarmultiplikation $x \cdot a := \varphi(x)a$ verstehen (für $x \in K$, $a \in A$, und wobei rechts die Ringmultiplikation von A verwendet wird). Es ist leicht nachzurechnen, dass die Vektorraumaxiome erfüllt sind. Ist andererseits A ein Ring, der auch ein K-Vektorraum ist, stimmen Ring- und Vektorraumaddition überein und gilt $x(ab) = (xa)b = a(xb)$ für alle $x \in K$, $a, b \in A$, so trägt A eine K-Algebrenstruktur, nämlich $K \to A$, $x \mapsto x \cdot 1$. Verwendet man den Begriff des R-Moduls (siehe Abschnitt LA2.18.7.1) so kann man den Begriff der R-Algebra auch für beliebige kommutative Ringe in analoger Weise betrachten.

Wir verallgemeinern die Konstruktion des Polynomrings über einem Ring in einer Variablen, indem wir auch mehrere Variablen zulassen (gegebenenfalls auch unendlich viele). Ist I die vorgegebene Indexmenge für die Variablen, so sind die Elemente des Polynomrings $R[X_i,\ i \in I]$ »Linearkombinationen« von Ausdrücken der Form $X_{i_1}^{n_1} \cdot \dots \cdot X_{i_r}^{n_r}$ für $r \in \mathbb{N}$, $i_s \in I$, $n_s \in \mathbb{N}_{>0}$. (In jedem einzelnen Polynom treten also immer nur endlich viele Variablen auf. Der Ring ist kommutativ, d.h. die Variablen kommutieren miteinander und mit Skalaren aus R.) Polynome werden in der offensichtlichen Weise addiert. Die Multiplikation ist durch die Regel

$$X_{i_1}^{m_1} \cdot \dots \cdot X_{i_r}^{m_r} \cdot X_{i_1}^{n_1} \cdot \dots \cdot X_{i_r}^{n_r} = X_{i_1}^{m_1+n_1} \cdot \dots \cdot X_{i_r}^{m_r+n_r}$$

und die Distributivgesetze eindeutig bestimmt (wobei wir hier auch 0 als Exponenten zulassen und $X_i^0 = 1$ setzen).

Den Polynomring $R[X_1, \dots, X_n]$ in endlich vielen Variablen $X_1, \dots, X_n$ kann man identifizieren mit $(R[X_1, \dots, X_{n-1}])[X_n]$, so dass man diese Ringe auch induktiv konstruieren kann. Im Fall unendlich vieler Variablen ist dies allerdings nicht ohne weiteres möglich. In jedem Fall haben wir den Begriff des Einsetzungshomomorphismus, der auch als universelle Eigenschaft des Polynomrings betrachtet werden kann:

DEFINITION A.38. Sei R ein kommutativer Ring und I eine Menge. Dann existiert eine R-Algebra P zusammen mit Elementen $X_i \in P$, $i \in I$, so dass für alle R-Algebren S die Abbildung

$$\mathrm{Hom}_R(P, S) \to \mathrm{Abb}(I, S), \quad f \mapsto (i \mapsto f(X_i)),$$

bijektiv ist.

Die R-Algebra P ist eindeutig bestimmt bis auf eindeutigen Isomorphismus im folgenden Sinne: Ist P' zusammen mit Elementen $X_i' \in P'$ eine R-Algebra, die ebenfalls die obige Eigenschaft besitzt, so existiert ein eindeutig bestimmter R-Algebren-Isomorphismus $P \to P'$ mit $X_i \mapsto X_i'$ für alle i.

Wir schreiben auch $R[X_i,\ i \in I] := P$ und nennen diesen Ring den *Polynomring über R in den Variablen $X_i, i \in I$.* ⊣

Definition A.39. Sei R ein Ring, $f \in R[X]$ ein Polynom und $\varphi\colon R \to S$ ein Ringhomomorphismus. Sei $\alpha \in S$.

(1) Das Element α heißt *Nullstelle* von f (in S), wenn $f(\alpha) = 0$ gilt. Wir fassen hierbei f vermöge φ als Element von $S[X]$ auf, wenden also auf alle Koeffizienten von f den Homomorphismus φ an.

(2) Sei nun in der obigen Situation S ein Integritätsring und $f \neq 0$. Die eindeutig bestimmte natürliche Zahl m mit $(X-\alpha)^m \mid f$ und $(X-\alpha)^{m+1} \nmid f$ heißt die *Vielfachheit* (oder *Ordnung*) von α als Nullstelle von f; wir schreiben $\mathrm{mult}_\alpha(f) := m$.

⊣

Es ist also α genau dann eine Nullstelle von f, wenn $\mathrm{mult}_\alpha(f) \geq 1$ gilt. Im Fall $\mathrm{mult}_\alpha(f) = 1$ nennen wir α auch eine *einfache Nullstelle*, falls $\mathrm{mult}_\alpha(f) > 1$ ist, so heißt α eine *mehrfache Nullstelle*. Genauer sprechen wir im Fall $\mathrm{mult}_\alpha(f) = 2$ von einer *doppelten Nullstelle*, usw.

Definition A.40. Sei R ein Ring. Die *(formale) Ableitung* eines Polynoms $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ ist das Polynom

$$f' := \sum_{i=1}^{n} i a_i X^{i-1} \in R[X].$$

⊣

Lemma A.41. *Sei R ein Ring. Die Bildung der Ableitung von Polynomen genügt den folgenden Rechenregeln. Hier seien $f, g \in R[X]$, $a \in R$.*

(1) $(af)' = a \cdot f'$,

(2) $(f+g)' = f' + g'$,

(3) $(fg)' = f'g + fg'$.

Lemma A.42. *Sei R ein Ring, $f \in R[X]$, $f \neq 0$, und $\alpha \in R$ eine Nullstelle von f. Dann sind äquivalent:*

(i) *α ist eine mehrfache Nullstelle von f,*

(ii) $f'(\alpha) = 0$.

A.2.3. Der Satz von Gauß.

Definition A.43. Sei R ein faktorieller Ring und sei p ein Primelement von R. Sei K der Quotientenkörper von R.

Für $x \in K^\times$ schreiben wir $v_p(x)$ für die eindeutig bestimmte ganze Zahl m, so dass sich x in der Form $x = p^m y$ für ein $y \in K^\times$ schreiben lässt, in dessen Darstellung als gekürzter Bruch weder der Zähler noch der Nenner durch p teilbar sind. Außerdem setzen wir $v_p(0) = \infty$. ⊣

Sind in der Situation der Definition $p, p' \in R$ zueinander assoziierte Primelemente, so gilt $v_p(x) = v_{p'}(x)$ für alle $x \in K$. Es ist genau dann $x \in R$, wenn $v_p(x) \geq 0$ für alle Primelemente p von R gilt. Äquivalent genügt es, diese Bedingung für alle Elemente eines Vertretersystems der Primelemente bis auf Assoziiertheit nachzuprüfen.

Lemma A.44. *Sei R ein faktorieller Ring und sei p ein Primelement von R. Sei K der Quotientenkörper von R und seien $x, y \in K$. Dann gilt:*

(1) $v_p(xy) = v_p(x) + v_p(y)$,

(2) $v_p(x+y) \geq \min(v_p(x), v_p(y))$.

DEFINITION A.45. Sei R ein faktorieller Ring und sei p ein Primelement von R. Sei K der Quotientenkörper von R.

Für $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ definieren wir

$$v_p(f) := \min\{v_p(a_i);\ i = 0, \ldots, n\}.$$

⊣

Es gilt dann also für $f \in K[X]$: $f \in R[X]$ genau dann, wenn $v_p(f) \geq 0$ für alle Primelemente p von R.

LEMMA A.46 (Lemma von Gauß). *Sei R ein faktorieller Ring und sei p ein Primelement von R. Sei K der Quotientenkörper von R und seien $f, g \in K[X]$. Dann gilt: $v_p(fg) = v_p(f) + v_p(g)$.*

KOROLLAR A.47. *Sei R ein faktorieller Ring und sei $h \in R[X]$ normiert. Ist dann $h = fg$ eine Zerlegung von h als Produkt von normierten Polynomen $f, g \in K[X]$ so gilt $f, g \in R[X]$.*

DEFINITION A.48. Sei R ein faktorieller Ring. Ein Polynom $f \in R[X]$ heißt *primitiv*, wenn $f \neq 0$ und wenn 1 ein größter gemeinsamer Teiler der Koeffizienten von f ist. ⊣

SATZ A.49 (Satz von Gauß). *Sei R ein faktorieller Ring, und sei K der Quotientenkörper von R. Dann ist auch der Polynomring $R[X]$ faktoriell.*

Ein Element $f \in R[X]$ ist genau dann irreduzibel, wenn

(a) $\deg(f) = 0$ *und f als Element von R irreduzibel ist, oder*

(b) $\deg(f) > 0$, *f primitiv und f als Element von $K[X]$ irreduzibel ist.*

A.2.4. Irreduzibilitätskriterien.

SATZ A.50 (Reduktionskriterium). *Sei R ein faktorieller Ring mit Quotientenkörper K, sei $p \in R$ ein Primelement und sei $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ ein Polynom vom Grad $n > 0$, so dass a_n nicht von p geteilt wird. Wenn das Bild von f in $(R/p)[X]$ irreduzibel ist, dann ist f irreduzibel in $K[X]$.*

Wird zusätzlich f als primitiv vorausgesetzt, so folgt, dass f in $R[X]$ irreduzibel ist.

SATZ A.51 (Irreduzibilitätskriterium von Eisenstein). *Seien R ein faktorieller Ring und K sein Quotientenkörper, sei $p \in R$ ein Primelement und sei $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ ein primitives Polynom vom Grad $n > 0$. Es gelte*

$$p \mid a_i,\ i = 0, \ldots, n-1, \qquad p^2 \nmid a_0.$$

Dann ist f irreduzibel in $R[X]$ und folglich auch irreduzibel in $K[X]$.

A.3. Algebraische Körpererweiterungen

A.3.1. Algebraische und endliche Körpererweiterungen.

DEFINITION A.52. Ist K ein Teilkörper eines Körpers L, so nennen wir auch L einen *Erweiterungskörper* von K und sprechen von der *Körpererweiterung* L/K.

Ist E ein Teilkörper von L, der seinerseits K als Teilkörper enthält, $K \subseteq E \subseteq L$, so heißt E ein *Zwischenkörper* der Erweiterung L/K. ⊣

Manchmal betrachten wir nicht nur die Inklusion eines Teilkörpers in einem Erweiterungskörper sondern allgemeiner auch einen (notwendigerweise injektiven) Körperhomomorphismus als Körpererweiterung.

DEFINITION A.53. Sei L/K eine Körpererweiterung. Sei $M \subseteq L$ eine Teilmenge.

(1) Die von M erzeugte K-Algebra ist der kleinste Unterring von L, der K und M enthält. Äquivalent ist dies das Bild des Einsetzungshomomorphismus $K[X_m,\ m \in M] \to L$, $X_m \mapsto m$, also die Menge aller polynomialen Ausdrücke in den Elementen von M mit Koeffizienten in K. Wir bezeichnen diese K-Algebra mit $K[M]$.

(2) Der über K von M erzeugte Teilkörper von L ist der kleinste Teilkörper von L, der K und L enthält. Dieser kann mit dem Quotientenkörper von $K[M]$ identifiziert werden. Wir bezeichnen diesen Teilkörper von L mit $K(M)$.

⊣

Es gilt also stets $K[M] \subseteq K(M)$. Wir werden unten die Bedingung, dass hier Gleichheit besteht, genauer untersuchen.

DEFINITION A.54. Eine Körpererweiterung L/K heißt *endlich erzeugt*, wenn eine endliche Teilmenge $M \subseteq L$ mit $L = K(M)$ existiert. ⊣

DEFINITION A.55. Sei L/K eine Körpererweiterung.

(1) Ein Element $\alpha \in L$ heißt *algebraisch über* K, wenn ein Polynom $p \in K[X] \setminus \{0\}$ existiert mit $p(\alpha) = 0$. Das eindeutig bestimmte normierte Polynom kleinsten Grades in $K[X]$, das α als Nullstelle hat, heißt dann das *Minimalpolynom* von α über K.

Wir bezeichnen das Minimalpolynom von α über K mit $\operatorname{minpol}_{\alpha,K}$.

(2) Ein Element $\alpha \in L$, das nicht algebraisch über K ist, heißt *transzendent*.

(3) Die Körpererweiterung L/K heißt *algebraisch*, wenn jedes Element von L über K algebraisch ist. Andernfalls heißt die Erweiterung *transzendent*.

⊣

Ist $\alpha \in L$ algebraisch über K, so ist $K[\alpha] \cong K[X] / (\operatorname{minpol}_{\alpha,K})$ ein Körper, und es gilt folglich $K[\alpha] = K(\alpha)$.

DEFINITION A.56. Sei L/K eine Körpererweiterung.

(1) Die Vektorraumdimension von L als K-Vektorraum heißt auch der *Grad* der Erweiterung L/K und wird mit $[L : K]$ bezeichnet.

(2) Die Erweiterung L/K heißt *endlich*, wenn ihr Grad endlich ist, andernfalls *unendlich*.

⊣

SATZ A.57 (Gradformel). *Seien L/K und M/L Körpererweiterungen. Dann sind äquivalent:*

(i) *Die Erweiterungen M/L und L/K sind endlich.*

(ii) *Die Erweiterung M/K ist endlich.*

In diesem Fall gilt

$$[M : K] = [M : L] \cdot [L : K].$$

LEMMA A.58. *Sei L/K eine Körpererweiterung, $a \in L$. Dann sind äquivalent:*

(i) *Das Element a ist algebraisch über K.*

(ii) *Die Erweiterung $K(a)/K$ ist endlich.*

(iii) *Es gilt $K[a] = K(a)$.*

(iv) *Der Unterring $K[a]$ von L ist ein Körper.*

SATZ A.59. *Sei L/K eine Körpererweiterung. Dann sind äquivalent:*

(i) *Die Erweiterung L/K ist endlich.*

(ii) *Die Erweiterung L/K ist algebraisch und endlich erzeugt.*

SATZ A.60. *Seien L/K und M/L Körpererweiterungen. Dann sind äquivalent:*

(i) *Die Erweiterungen M/L und L/K sind algebraisch.*

(ii) *Die Erweiterung M/K ist algebraisch.*

A.3.2. Die Existenz eines algebraischen Abschlusses.

SATZ A.61. *Sei K ein Körper und sei $f \in K[X]$ ein Polynom vom Grad > 0. Dann gibt es einen Erweiterungskörper L von K, in dem f eine Nullstelle besitzt.*

Ist f irreduzibel, so können wir $L := K[X]/(f)$ setzen.

Sei K ein Körper und $f \in K[X]$ ein Polynom. Für einen Erweiterungskörper L von K bezeichnen wir mit $V(f, L) \subseteq L$ die Menge der Nullstellen von f in L.

SATZ A.62. *Die Abbildung*

$$\mathrm{Hom}_K(K[\alpha], L) \to L, \quad \varphi \mapsto \varphi(\alpha),$$

induziert eine Bijektion

$$\mathrm{Hom}_K(K[\alpha], L) \xrightarrow{\sim} V(\mathrm{minpol}_{\alpha,K}, L).$$

DEFINITION A.63. Ein Körper K heißt *algebraisch abgeschlossen*, wenn die folgenden äquivalenten Bedingungen erfüllt sind:

(i) Jedes nicht-konstante Polynom $f \in K[X]$ besitzt eine Nullstelle in K.

(ii) Jedes nicht-konstante Polynom $f \in K[X]$ zerfällt über K vollständig in Linearfaktoren.

⊣

THEOREM A.64. *Sei K ein Körper. Dann existiert ein algebraisch abgeschlossener Erweiterungskörper L von K. Man kann zudem erreichen, dass die Erweiterung L/K algebraisch ist. In diesem Fall nennt man L einen* algebraischen Abschluss *von K.*

SATZ A.65. *Seien K ein Körper, L/K eine algebraische Körpererweiterung und sei $\varphi\colon K \to E$ ein Körperhomomorphismus von K in einen algebraisch abgeschlossenen Körper E.*

(1) *Dann existiert eine Fortsetzung von φ zu einem Körperhomomorphismus $\psi\colon L \to E$ (d.h. es gilt $\psi(x) = \varphi(x)$ für alle $x \in K$).*

(2) *Ist zusätzlich L algebraisch abgeschlossen und E algebraisch über K, so ist jede Fortsetzung wie in Teil (1) ein Isomorphismus.*

Auch wenn die Aussage des Satzes an die Sprechweise der universellen Eigenschaft erinnert, handelt es sich hier *nicht* um eine universelle Eigenschaft, weil die Eindeutigkeit des Homomorphismus ψ in Teil (1) nicht gegeben ist. Es folgt daher *nicht*, dass zwischen zwei algebraischen Abschlüssen von K ein eindeutig bestimmter K-Isomorphismus existiere (und das ist in aller Regel auch nicht der Fall), sondern nur, dass es (irgend-)einen solchen Isomorphismus gibt.

A.4. Galois-Theorie

A.4.1. Normale Körpererweiterungen.

DEFINITION A.66. Sei K ein Körper und sei $(f_i)_{i\in I}$ eine Familie von Polynomen in $K[X]$.

Ein Erweiterungskörper L von K heißt *Zerfällungskörper* der Familie $(f_i)_i$, wenn die folgenden beiden Bedingungen erfüllt sind:

(a) Jedes f_i zerfällt über L vollständig in Linearfaktoren und
(b) die Körpererweiterung L/K wird von den Nullstellen der Polynome f_i erzeugt.

⊣

SATZ A.67. *Sei K ein Körper und sei $(f_i)_{i\in I}$ eine Familie von Polynomen in $K[X]$.*

(1) *Es existiert ein Zerfällungskörper der gegebenen Familie von Polynomen.*
(2) *Sind L und L' Zerfällungskörper der Familie $(f_i)_i$, so existiert ein K-Isomorphismus $L \xrightarrow{\sim} L'$.*

Man beachte, dass der Isomorphismus in Teil (2) des Satzes in aller Regel nicht eindeutig bestimmt ist.

DEFINITION A.68. Eine Körpererweiterung L/K heißt *normal*, wenn die folgenden äquivalenten Bedingungen erfüllt sind. Hier bezeichne $\overline{L}$ einen fixierten algebraischen Abschluss von L.

(i) Es gibt eine Familie von Polynomen in $K[X]$, derart dass L ein Zerfällungskörper dieser Familie ist.
(ii) Für jeden K-Homomorphismus $\varphi\colon L \to \overline{L}$ gilt $\mathrm{Im}(\varphi) \subseteq L$.
(iii) Ist $f \in K[X]$ ein irreduzibles Polynom, das in L eine Nullstelle besitzt, so zerfällt f über L vollständig in Linearfaktoren.

⊣

BEISPIEL A.69. (1) Quadratische Erweiterungen (also Erweiterungen vom Grad 2) sind normal.
(2) Die Erweiterung $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist nicht normal.
(3) Ist $\overline{K}$ ein algebraischer Abschluss von K, so ist die Erweiterung $\overline{K}/K$ normal.

◊

LEMMA A.70. *Seien E/K und L/E Körpererweiterungen. Ist die Erweiterung L/K normal, so ist auch die Erweiterung L/E normal.*

SATZ A.71. *Sei L/K eine algebraische Körpererweiterung.*

(1) *Dann existiert ein Erweiterungskörper L' von L, so dass die Erweiterung L'/K normal ist, und so dass kein echter Teilkörper von L', der K enthält, normal über K ist. Der Körper L' ist bis auf K-Isomorphismus eindeutig bestimmt.*
(2) *Ist die Erweiterung L/K endlich, so ist auch L'/K endlich.*
(3) *Ist M/K eine normale Erweiterung, so dass L in M enthalten ist, so ist der von allen $\sigma(L)$, $\sigma \in \mathrm{Hom}_K(L, M)$, über K erzeugte Teilkörper von M der eindeutig bestimmte Zwischenkörper von M/K, der die Eigenschaft in Teil (1) hat.*

Wir nennen L' eine normale Hülle *der Erweiterung L/K (bzw. in der Situation von Teil (3)* die normale Hülle von L/K in M.

A.4.2. Separable Körpererweiterungen.

DEFINITION A.72. Sei K ein Körper und $\overline{K}$ ein algebraischer Abschluss von K. Ein Polynom $f \in K[X]$ heißt *separabel*, wenn f in $\overline{K}$ nur einfache Nullstellen hat. ⊣

Die Eigenschaft, separabel zu sein, ist unabhängig von der Wahl eines algebraischen Abschlusses von K.

SATZ A.73. *Sei K ein Körper und $f \in K[X]$ ein irreduzibles Polynom. Dann sind äquivalent:*

(i) *f ist separabel,*

(ii) $f' \neq 0$.

Insbesondere gilt: Über einem Körper der Charakteristik 0 ist jedes irreduzible Polynom separabel.

SATZ A.74. *Sei K ein Körper der Charakteristik $p > 0$ und sei $f \in K[X]$ irreduzibel. Sei $r \in \mathbb{N}$ maximal mit der Eigenschaft, dass f die Form $g(X^{p^r})$ für ein Polynom $g \in K[X]$ hat. Dann ist g durch f eindeutig bestimmt, separabel und irreduzibel.*

Jede Nullstelle von f hat die Vielfachheit p^r, und die Nullstellen von f (in einem algebraischen Abschluss $\overline{K}$ von K) sind gerade die p^r-ten Wurzeln der Nullstellen von g.

DEFINITION A.75. Sei L/K eine algebraische Körpererweiterung.

(1) Ein Element $a \in L$ heißt *separabel über K*, wenn ein separables Polynom $p \in K[X] \setminus \{0\}$ existiert mit $p(a) = 0$. Es ist äquivalent zu fordern, dass das Minimalpolynom von a über K separabel sei.

(2) Ein Element $a \in L$, das nicht algebraisch über K ist, heißt auch *inseparabel*.

(3) Die Körpererweiterung L/K heißt *separabel*, wenn jedes Element von L über K separabel ist.

(4) Ist die Erweiterung L/K nicht separabel, so heißt sie *inseparabel*. Ist sogar jedes Element von L, das nicht in K liegt, inseparabel über K, dann nennt man die Erweiterung L/K *rein inseparabel*.

⊣

DEFINITION A.76. Ein Körper K heißt *perfekt* (oder: *vollkommen*), wenn jede algebraische Erweiterung von K separabel ist. ⊣

Nach dem oben gesagten ist jeder Körper von Charakteristik 0 ein perfekter Körper. In positiver Charakteristik haben wir die folgende Charakterisierung.

SATZ A.77. *Sei K ein Körper der Charakteristik $p > 0$. Dann sind äquivalent:*

(i) *Der Körper K ist perfekt.*

(ii) *Jede endliche Erweiterung von K ist separabel.*

(iii) *Der Frobenius-Homomorphismus $K \to K$, $x \mapsto x^p$, ist surjektiv (und folglich ein Isomorphismus).*

KOROLLAR A.78. *Jeder endliche Körper ist perfekt.*

DEFINITION A.79. Sei L/K eine endliche Körpererweiterung und sei $\overline{K}$ ein algebraischer Abschluss von K. Dann heißt

$$[L : K]_s := \#\operatorname{Hom}_K(L, \overline{K})$$

der *Separabilitätsgrad* der Erweiterung L/K. ⊣

LEMMA A.80. *Seien E/K und L/E endliche Körpererweiterungen. Dann gilt*

$$[L : K]_s = [L : E]_s \, [E : K]_s.$$

Für jede endliche Körpererweiterung L/K gilt $[L : K]_s \leq [L : K]$.

SATZ A.81. *Sei L/K eine endliche Körpererweiterung. Es sind äquivalent:*

(i) *Die Erweiterung L/K ist separabel.*

(ii) *Es gilt $[L : K]_s = [L : K]$.*

(iii) *Es gibt separable Elemente $\alpha_1, \ldots, \alpha_r \in L$ mit $L = K(\alpha_1, \ldots, \alpha_r)$.*

KOROLLAR A.82. *Seien E/K und L/E algebraische Körpererweiterungen. Dann ist äquivalent:*

(i) *Die Erweiterung L/K ist separabel.*

(ii) *Die Erweiterungen E/K und L/E sind separabel.*

SATZ A.83 (Satz vom primitiven Element). *Sei L/K eine endliche separable Körpererweiterung. Dann existiert $\alpha \in L$ mit $L = K(\alpha)$. Wir nennen α ein* primitives Element *der Erweiterung L/K.*

A.4.3. Endliche Körper.

SATZ A.84. *Sei K ein endlicher Körper. Dann hat K positive Charakteristik p und die Anzahl der Elemente von K ist eine Potenz von p.*

SATZ A.85. *Sei p eine Primzahl. Zu jedem $r \in \mathbb{N}_{>0}$ gibt es einen Körper mit $q := p^r$ Elementen. Dieser Körper ist ein Zerfällungskörper des Polynoms $X^q - X$.*

Sind K, K' endliche Körper mit $\#K = \#K'$, dann existiert ein Körperisomorphismus $K \cong K'$.

SATZ A.86. *Sei $\overline{\mathbb{F}}_p$ ein algebraischer Abschluss des Körpers $\mathbb{F}_p$. Für jedes $r \in \mathbb{N}$ enthält $\overline{\mathbb{F}}_p$ genau einen Teilkörper $\mathbb{F}_{p^r}$ mit p^r Elementen und es gilt*

$$\overline{\mathbb{F}}_p = \bigcup_{r \geq 1} \mathbb{F}_{p^r}.$$

Für $r, s \in \mathbb{N}$ gilt genau dann $\mathbb{F}_{p^r} \subseteq \mathbb{F}_{p^s}$, wenn $r \mid s$ gilt.

SATZ A.87. *Jede Erweiterung L/K endlicher Körper ist normal und separabel.*

A.4.4. Galois-Erweiterungen. Ist L ein Körper, so bezeichnen wir mit $\mathrm{Aut}(L)$ die Gruppe (bezüglich der Verkettung von Abbildungen) aller Körperautomorphismen $L \xrightarrow{\sim} L$. Sei L/K eine Körpererweiterung. Wir bezeichnen mit $\mathrm{Aut}_K(L)$ die Gruppe aller K-Automorphismen von L, also aller Isomorphismen $L \xrightarrow{\sim} L$ von K-Algebren.

DEFINITION A.88. Sei L ein Körper und sei G eine Gruppe, die auf L durch Körperautomorphismen operiert. (Es ist also eine Operation $G \times L \to L$ gegeben, derart dass das Bild des zugehörige Gruppenhomomorphismus $G \to \mathrm{Bij}(L)$ in $\mathrm{Aut}(L)$ liegt.)

Dann ist

$$L^G := \{x \in L;\ gx = x \text{ für alle } g \in G\}$$

ein Teilkörper von L, der sogenannte *Fixkörper* unter der Operation von G. ⊣

Ist L/K eine Körpererweiterung und operiert die Gruppe G auf L durch K-Automorphismen, so ist L^G ein Zwischenkörper der Erweiterung L/K.

Wir definieren nun den Begriff der Galois-Erweiterung, der für den weiteren Verlauf zentral ist. Man kann die Theorie auch auf den Fall unendlicher Erweiterungen verallgemeinern, wir begnügen und aber in dieser Vorlesung mit dem endlichen Fall und verstehen daher *unter einer Galois-Erweiterung stets eine endliche Körpererweiterung* (mit den zusätzlichen Eigenschaften, die in der folgenden Definition genannt werden).

SATZ A.89. *Sei L/K eine endliche Körpererweiterung. Die folgenden Aussagen sind äquivalent.*

(i) *Es gilt*
$$K = L^{\mathrm{Aut}_K(L)}.$$

(ii) *Es gibt eine Untergruppe $G \subseteq \mathrm{Aut}(L)$, so dass*
$$K = L^G$$
gilt.

(iii) *Die Erweiterung L/K ist normal und separabel.*

Sind die Bedingungen erfüllt, so heißt die Erweiterung L/K galoissch *oder eine* Galois-Erweiterung. *Wir nennen dann* $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$ *die* Galois-Gruppe *der Erweiterung L/K.*

Es gilt dann $[L : K] = \#\,\mathrm{Gal}(L/K)$.

LEMMA A.90. (1) *Sei E ein Zwischenkörper der Körpererweiterung L/K. Ist L/K galoisch, dann ist auch L/E galoisch.*

(2) *Sei E ein Zwischenkörper der Körpererweiterung L/K. Sind L/K und E/K galoisch, dann ist die Einschränkung von Homomorphismen ein surjektiver Gruppenhomomorphismus* $\mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$ *mit Kern* $\mathrm{Gal}(L/E)$.

Für eine Gruppe G bezeichnen wir mit $\mathrm{UG}(G)$ die Menge aller Untergruppen von G. Für eine Körpererweiterung L/K bezeichnen wir mit $\mathrm{ZK}(L/K)$ die Menge aller Zwischenkörper dieser Erweiterung.

THEOREM A.91 (Hauptsatz der Galois-Theorie). *Sei L/K eine Galois-Erweiterung mit Galois-Gruppe G. Dann sind die Abbildungen*
$$\mathrm{UG}(G) \to \mathrm{ZK}(L/K), \quad H \mapsto L^H, \qquad \textit{und} \qquad \mathrm{ZK}(L/K) \to \mathrm{UG}(G), \quad E \mapsto \mathrm{Gal}(L/E),$$
zueinander inverse inklusionsumkehrende Bijektionen.

Für einen Zwischenkörper E der Erweiterung L/K sind äquivalent:

(i) *Die Erweiterung E/K ist normal.*

(ii) *Die Erweiterung E/K ist galoissch.*

(iii) *Die Untergruppe $H := \mathrm{Gal}(L/E) \subseteq \mathrm{Gal}(L/K)$ ist ein Normalteiler.*

Sind diese äquivalenten Bedingungen erfüllt, so induziert die Abbildung $\sigma \mapsto \sigma_{|L^H}$ einen Isomorphismus $G/H \xrightarrow{\sim} \mathrm{Gal}(L^H/K)$.

KOROLLAR A.92. *Jede endliche separable Körpererweiterung besitzt nur endlich viele Zwischenkörper.*

DEFINITION A.93. Eine Körpererweiterung L/K heißt *abelsch* (bzw. *zyklisch*), wenn sie galoissch mit abelscher (bzw. zyklischer) Galois-Gruppe ist. ⊣

DEFINITION A.94. Sei L/K eine Körpererweiterung mit Zwischenkörpern E und E'. Das *Kompositum* von E und E' ist der kleinste Teilkörper von L, der E und E' enthält und wird mit $E \cdot E'$ oder einfach mit EE' bezeichnet. ⊣

SATZ A.95. *Sei L/K eine Galois-Erweiterung mit Zwischenkörpern E und E'. Sei $H = \mathrm{Gal}(L/E)$ und $H' = \mathrm{Gal}(L/E')$.*

(1) *Es gilt $EE' = L^{H \cap H'}$.*

(2) *Es gilt $E \cap E' = L^{\tilde{H}}$, wobei $\tilde{H}$ die von H und H' in* $\mathrm{Gal}(L/K)$ *erzeugte Untergruppe bezeichne.*

(3) *Seien nun die Erweiterungen E/K und E'/K galoissch. Dann ist EE'/K eine Galois-Erweiterung und der Homomorphismus*

$$\mathrm{Gal}(EE'/E) \to \mathrm{Gal}(E'/E \cap E'), \quad \sigma \mapsto \sigma_{|E'},$$

ist bijektiv. Insbesondere ist $[EE' : E]$ ein Teiler von $[E' : K]$.

Aus dem Hauptsatz der Galois-Theorie erhalten wir (mit den Sätzen aus der Gruppentheorie, die wir zu Beginn der Vorlesung bewiesen haben) einen Beweis des Fundamentalsatzes der Algebra.

THEOREM A.96. *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

A.4.5. Die Galois-Gruppe einer Gleichung.

DEFINITION A.97. Sei K ein Körper und $f \in K[X]$ ein separables Polynom. Sei L ein Zerfällungskörper von f über K. Dann ist die Erweiterung L/K galoissch, ihre Galois-Gruppe hängt nicht von der Wahl von L ab und heißt auch die *Galois-Gruppe der Gleichung $f(x) = 0$* (oder die *Galois-Gruppe von f*). ⊣

SATZ A.98. *Sei K ein Körper, $\overline{K}$ ein algebraischer Abschluss und $f \in K[X]$ ein separables Polynom vom Grad $n \in \mathbb{N}$ mit Zerfällungskörper L. Sei $G = \mathrm{Gal}(L/K)$ die Galois-Gruppe der Gleichung $f(x) = 0$. Seien $\alpha_1, \ldots, \alpha_n \in L$ die (nach Voraussetzung paarweise verschiedenen) Nullstellen von f in $\overline{K}$.*

Jedes Element von G induziert dann eine Permutation der α_i, und wir erhalten so einen injektiven Gruppenhomomorphismus $G \to S_n$. Insbesondere gilt $\#G \mid n!$.

Das Polynom ist genau dann irreduzibel in $K[X]$, wenn G transitiv auf der Menge $\{\alpha_1, \ldots, \alpha_n\}$ operiert.

A.5. Anwendungen der Galois-Theorie

A.5.1. Einheitswurzeln und zyklische Erweiterungen.

DEFINITION A.99. Sei K ein Körper. Sei $n \in \mathbb{N}_{>0}$.

(1) Ein Element $\zeta \in K^\times$ heißt eine *n-te Einheitswurzel*, wenn $\zeta^n = 1$ gilt. Wir bezeichnen mit $\mu_n(K)$ die Menge der n-ten Einheitswurzeln. Dies ist eine Untergruppe von $K^\times$.

(2) Ein Element $\zeta \in K^\times$ heißt *primitive n-te Einheitswurzel*, wenn ζ als Element der Gruppe $K^\times$ Ordnung n hat, wenn also $\zeta^n = 1$, aber $\zeta^m \neq 1$ für alle $1 \leq m < n$ gilt. Wir bezeichnen mit $\mu_n^{\mathrm{prim}}(K)$ die Menge der primitiven n-ten Einheitswurzeln.

⊣

Wir nennen ein Element der multiplikativen Gruppe eines Körpers K eine *Einheitswurzel*, wenn es eine n-te Einheitswurzel für irgendein n ist, oder mit anderen Worten, wenn es endliche Ordnung in der Gruppe $K^\times$ hat.

Die n-ten Einheitswurzeln in einem Körper K sind gerade die Nullstellen des Polynoms $X^n - 1$. Es gilt also $\#\mu_n(K) \leq n$, und Gleichheit gilt genau dann, wenn es eine primitive n-te Einheitswurzel gibt. In diesem Fall zerfällt das Polynom $X^n - 1$ in n verschiedene Linearfaktoren. Insbesondere kann es in einem Körper positiver Charakteristik p für $p \mid n$ niemals eine primitive n-te Einheitswurzel geben (denn die Ableitung von $X^n - 1$ ist in dieser Situation gleich Null).

Die Gruppe $\mu_n(K)$ ist zyklisch. Gibt es in K eine primitive n-te Einheitswurzel ζ, so ist die Abbildung

$$\mathbb{Z}/n \to \mu_n(K), \quad i \mapsto \zeta^i,$$

ein Isomorphismus, der sich ein zu einer Bijektion zwischen $(\mathbb{Z}/n)^\times$ und $\mu_n^{\text{prim}}(K)$ einschränkt.

Es gilt $\mu_n(\mathbb{C}) = \{\exp(\frac{2k\pi i}{n});\ k = 0, ..., n-1\}$. Insbesondere ist $\exp(\frac{2\pi i}{n})$ eine primitive n-te Einheitswurzel.

SATZ A.100. *Sei K ein Körper, $\overline{K}$ ein algebraischer Abschluss von K und $\zeta \in \overline{K}$ eine Einheitswurzel. Dann gilt: Die Erweiterung $K(\zeta)/K$ ist eine Galois-Erweiterung.*

Sei in der Situation des Satzes ζ eine primitive n-te Einheitswurzel in $\overline{K}$. Wir betrachten die Abbildung $\psi' \colon \mathrm{Gal}(K(\zeta) \,/\, K) \to \mu_n^{\text{prim}}$, $\psi'(\sigma) = \sigma(\zeta)$. Dies ist eine injektive Abbildung, und durch Verkettung mit der Bijektion $\mu_n^{\text{prim}}(K(\zeta)) \cong (\mathbb{Z}/n)^\times$ erhalten wir einen injektiven Gruppenhomomorphismus $\psi \colon \mathrm{Gal}(K(\zeta) \,/\, K) \to (\mathbb{Z}/n)^\times$.

SATZ A.101. *Sei K ein Körper, $\overline{K}$ ein algebraischer Abschluss von K und $\zeta \in \overline{K}$ eine primitive n-te Einheitswurzel. Dann gilt: Die Erweiterung $K(\zeta)/K$ ist eine abelsche Galois-Erweiterung. Die Galois-Gruppe ist isomorph zu einer Untergruppe von $(\mathbb{Z}/n)^\times$.*

SATZ A.102. *Sei $K = \mathbb{Q}$ und ζ eine primitive n-te Einheitswurzel (in einem algebraischen Abschluss von $\mathbb{Q}$). Dann gilt $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \#(\mathbb{Z}/n)^\times$ und $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n)^\times$.*

SATZ A.103. *Seien $n \in \mathbb{N}_{>1}$ und K ein Körper, der eine primitive n-te Einheitswurzel enthält. Sei L/K eine Körpererweiterung.*

(1) *Wenn $L = K(\alpha)$ gilt für ein Element $\alpha \in L$, das Nullstelle eines Polynoms der Form $X^n - c$ mit $c \in K$ ist, dann ist L/K eine zyklische Galois-Erweiterung. Der Grad $d := [L : K]$ ist ein Teiler von n, es gilt $\alpha^d \in K$ und $X^d - \alpha^d$ ist das Minimalpolynom von α über K.*
(2) *Wenn die Erweiterung L/K zyklisch vom Grad n ist, dann existiert $\alpha \in L$, so dass $L = K(\alpha)$ ist und das Minimalpolynom von α über K die Form $\mathrm{minpol}_{\alpha,K} = X^n - c$ für ein $c \in K$ hat.*

A.5.2. Auflösbarkeit von Gleichungen durch Radikale. Um die Diskussion etwas zu vereinfachen, betrachten wir in diesem Abschnitt nur Körper der Charakteristik 0. Um die Ergebnisse in der »richtigen« Art und Weise auf Körper positiver Charakteristik zu übertragen, ist zu berücksichtigen, dass es über diesen im Allgemeinen auch zyklische Erweiterungen gibt, für die kein primitives Element mit Minimalpolynom der Form $X^n - c$ existiert (vergleiche Satz A.103, der diese Fälle nicht abdeckt, weil es niemals eine primitive n-te Einheitswurzel gibt, wenn n ein Vielfaches der Charakteristik ist).

DEFINITION A.104. Sei L/K eine endliche Körpererweiterung.

(1) Wir sagen, die Körpererweiterung L/K sei *auflösbar durch Radikale*, wenn eine Kette
$$K = K_0 \subset K_1 \subset \cdots \subset K_r$$
endlicher Körpererweiterungen mit $L \subseteq K_r$ existiert, so dass jede der Erweiterungen K_{i+1}/K_i von einer der folgenden Formen ist:
   - K_{i+1} entsteht aus K_i durch Adjunktion einer Einheitswurzel,
   - $K_{i+1} = K_i(\alpha)$ für ein Element α aus K_{i+1}, so dass eine positive Potenz von α in K_i liegt.
(2) Wir sagen, die Körpererweiterung L/K sei *auflösbar*, wenn ein Erweiterungskörper E von L existiert, so dass E/K eine Galois-Erweiterung mit auflösbarer Galois-Gruppe ist.
(3) Ist $f \in K[X]$, so sagen wir die Gleichung $f(x) = 0$ (oder: das Polynom f) sei *auflösbar durch Radikale* bzw. *auflösbar*, wenn der Zerfüllungskörper von f die entsprechende Eigenschaft hat.

⊣

LEMMA A.105. (1) *Eine Erweiterung L/K ist genau dann auflösbar durch Radikale, wenn die normale Hülle von L über K diese Eigenschaft hat.*

(2) *Eine Erweiterung L/K ist genau dann auflösbar, wenn die normale Hülle von L über K eine Galois-Erweiterung mit auflösbarer Galois-Gruppe ist.*

(3) *Die Eigenschaften* auflösbar durch Radikale *und* auflösbar *verhalten sich transitiv in einem Turm $K \subset L \subset M$ von Körpererweiterungen.*

SATZ A.106. *Eine Körpererweiterung ist genau dann auflösbar durch Radikale, wenn sie auflösbar ist.*

KOROLLAR A.107. *Es gibt Gleichungen (zum Beispiel vom Grad 5 über $\mathbb{Q}$), die nicht durch Radikale auflösbar sind.*

KOROLLAR A.108. *Jede Gleichung vom Grad ≤ 4 ist durch Radikale auflösbar.*

A.5.3. Konstruierbarkeit mit Zirkel und Lineal.

DEFINITION A.109. Die Teilmenge $\mathbb{K} \subseteq \mathbb{C}$ der (mit Zirkel und Lineal) *konstruierbaren* komplexen Zahlen ist die kleinste Teilmenge von $\mathbb{C}$, die die folgenden Eigenschaften hat:

(a) $0, 1 \in \mathbb{K}$,

(b) für je zwei unterschiedliche Geraden, die durch (mindestens) zwei Punkte von $\mathbb{K}$ gehen, liegt auch deren Schnittpunkt in $\mathbb{K}$,

(c) für jede Gerade, die durch (mindestens) zwei Punkte von $\mathbb{K}$ geht, und jeden Kreis, dessen Mittelpunkt in $\mathbb{K}$ liegt, und so dass der Radius gleich dem Abstand zweier Punkte in $\mathbb{K}$ ist, liegen auch die Schnittpunkte der Geraden und des Kreises in $\mathbb{K}$,

(d) für je zwei unterschiedliche Kreise, deren Mittelpunkte in $\mathbb{K}$ liegen, und so dass die Radien jeweils gleich dem Abstand zweier Punkte in $\mathbb{K}$ sind, liegen auch die Schnittpunkte der Kreise in $\mathbb{K}$.

⊣

SATZ A.110. (1) *Die Menge $\mathbb{K}$ ist ein Teilkörper des Körpers der komplexen Zahlen.*

(2) *Die Erweiterung $\mathbb{K}/\mathbb{Q}$ ist algebraisch.*

(3) *Für alle $\alpha \in \mathbb{K}$ gilt $\pm\sqrt{\alpha} \in \mathbb{K}$.*

SATZ A.111. *Für $\alpha \in \mathbb{C}$ sind äquivalent:*

(i) *Es gilt $\alpha \in \mathbb{K}$, d.h. α ist ausgehend von 0 und 1 konstruierbar mit Zirkel und Lineal.*

(ii) *Es gibt eine endliche Kette*
$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_r$$
von Körpererweiterungen, so dass $[K_i : K_{i-1}] = 2$ für alle $i = 1, \ldots, r$ gilt und $\alpha \in K_r$ ist.

(iii) *Es gibt eine Galois-Erweiterung $K/\mathbb{Q}$ mit $\alpha \in K$, deren Grad eine Potenz von 2 ist.*

KOROLLAR A.112. (1) *Es gilt $\sqrt[3]{2} \notin \mathbb{K}$, d.h. die »Verdoppelung des Würfels« ist nicht möglich.*

(2) *Aus dem Satz von Lindemann, dass π transzendent über $\mathbb{Q}$ ist, folgt, dass $\pi \notin \mathbb{K}$ gilt, also dass die »Quadratur des Kreises« nicht möglich ist.*

THEOREM A.113. *Sei $n \geq 3$ eine natürliche Zahl. Dann sind äquivalent:*

(i) *Das regelmäßige n-Eck ist konstruierbar mit Zirkel und Lineal (d.h. $\exp(\frac{2\pi i}{n}) \in \mathbb{K}$).*

(ii) *Die Zahl $\varphi(n)$ ist eine Potenz von 2 (wobei φ die Eulersche φ-Funktion bezeichnet, d.h. $\varphi(n)$ ist die Anzahl der zu n teilerfremden Zahlen zwischen 1 und $n-1$).*

DEFINITION A.114. Eine Primzahl der Form $2^k + 1$ heißt *Fermatsche Primzahl*. Es ist dann notwendigerweise k selbst eine Potenz von 2. Wir schreiben $F_r = 2^{2^r} + 1$. ⊣

KOROLLAR A.115. *Sei $n \geq 3$ eine natürliche Zahl. Dann sind äquivalent:*

(i) *Das regelmäßige n-Eck ist konstruierbar mit Zirkel und Lineal (d.h. $\exp(\frac{2\pi i}{n}) \in \mathbb{K}$).*

(ii) *Die Zahl n hat die Form $2^r p_1 \cdot \cdots \cdot p_l$ mit $r, l \geq 0$ und mit paarweise verschiedenen Fermatschen Primzahlen p_i.*

A.5.4. Das quadratische Reziprozitätsgesetz.

SATZ A.116. *Sei $p > 2$ eine Primzahl und sei $\zeta_p \in \overline{\mathbb{Q}}$ eine primitive p-te Einheitswurzel. Die Körpererweiterung $\mathbb{Q}(\zeta_p) \Big/ \mathbb{Q}$ besitzt einen eindeutig bestimmten Zwischenkörper E mit $[E : \mathbb{Q}] = 2$, und zwar ist dies der Körper $\mathbb{Q}(\sqrt{p^*})$ mit*

$$p^* = \begin{cases} p & \text{wenn } p \equiv 1 \mod 4, \\ -p & \text{wenn } p \equiv 3 \mod 4. \end{cases}$$

LEMMA A.117. *Sei p eine ungerade Primzahl. Ein Element $x \in \mathbb{F}_p^\times$ ist genau dann ein Quadrat in $\mathbb{F}_p^\times$, wenn $x^{\frac{p-1}{2}} = 1$ gilt.*

Dieses Lemma motiviert die folgende Definition.

DEFINITION A.118. Sei p eine ungerade Primzahl und $x \in \mathbb{F}_p^\times$. Wir definieren das *Legendre-Symbol* durch

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{wenn } x \in (\mathbb{F}_p^\times)^2, \\ -1 & \text{wenn } x \in \mathbb{F}_p^\times \setminus (\mathbb{F}_p^\times)^2. \end{cases}$$

(Der Wert des Legendre-Symbols soll per Definition in $\mathbb{Z}$ liegen, d.h. 1 und -1 werden hier als ganze Zahlen, nicht als Elemente eines endlichen Körpers, betrachtet.)

Für ganze Zahlen x, die zu p teilerfremd sind, definieren wir das Legendre-Symbol, indem wir die obigen Definition auf die Restklasse von x in $\mathbb{F}_p$ anwenden. ⊣

THEOREM A.119 (Quadratisches Reziprozitätsgesetz). *Seien $p \neq q$ ungerade Primzahlen. Dann gilt*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$$

THEOREM A.120 (Ergänzungssätze zum quadratischen Reziprozitätsgesetz). *Sei p eine ungerade Primzahl. Dann gilt*

(1) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$,

(2) $\left(\frac{2}{q}\right) = (-1)^{\frac{p^2-1}{8}}$.

ANHANG B

Mathematische Ergänzungen *

B.1. Kardinalzahlen

Wir stellen hier einige Tatsachen über Mächtigkeiten unendlicher Mengen zusammen (siehe auch Abschnitt LA1.3.15).

DEFINITION B.1. Wir nennen zwei Mengen M, M' *gleichmächtig*, wenn eine bijektive Abbildung $M \to M'$ existiert. ⊣

Der entscheidende Punkt an dieser Definition ist, dass zwei unendliche Mengen nicht unbedingt gleichmächtig sind, zum Beispiel sind $\mathbb{Q}$ und $\mathbb{R}$ nicht gleichmächtig (siehe unten). Es ist klar, dass Gleichmächtigkeit eine Äquivalenzrelation ist.

DEFINITION B.2. Eine *Kardinalzahl* ist eine Äquivalenzklasse von Mengen bezüglich der Äquivalenzrelation der Gleichmächtigkeit.

Für eine Menge M bezeichnen wir mit $\#M$ ihre Äquivalenzklasse im obigen Sinne und nennen $\#M$ auch die *Mächtigkeit* (oder: *Kardinalität*) von M. ⊣

DEFINITION B.3. Eine Menge M heißt *abzählbar* (oder genauer *abzählbar unendlich*), wenn M gleichmächtig ist zur Menge $\mathbb{N}$ der natürlichen Zahlen. Man schreibt dann auch $\#M = \aleph_0$, wir bezeichnen also mit $\aleph_0$ die Mächtigkeits-Äquivalenzklasse von $\mathbb{N}$. ⊣

($\aleph$, ausgesprochen Aleph, ist der erste Buchstabe des hebräischen Alphabets.)

Wenn man von einer Menge M sagt, sie sei *höchstens abzählbar*, so meint man, dass M endlich oder abzählbar unendlich sei. Eine unendliche Menge, die nicht abzählbar ist, heißt *überabzählbar*.

Es gelten dann die folgenden Aussagen:

SATZ B.4. (1) *Ist X eine Menge, so dass eine injektive Abbildung von X in eine abzählbar unendliche Menge existiert, dann ist X selbst höchstens abzählbar.*

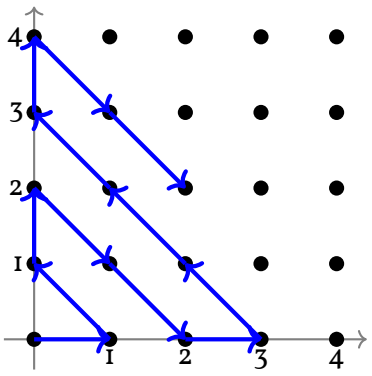
(2) *Jedes kartesische Produkt von abzählbar unendlichen Mengen über eine endliche Indexmenge ist abzählbar.*

(3) *Jede Vereinigung von abzählbar unendlichen Mengen über eine endliche oder abzählbar unendliche Indexmenge ist abzählbar.*

BEWEISSKIZZE. zu (1). Wir können annehmen, dass X unendlich ist und dass eine Injektion $f\colon X \to \mathbb{N}$ existiert. Wir konstruieren eine Bijektion $g\colon \mathbb{N} \to X$ indem wir induktiv $g(n)$ folgendermaßen definieren: Es sei $g(0)$ das Element x, für das $f(x)$ minimal ist. Für $n > 0$ sei $g(n)$ das eindeutig bestimmte x, für das $f(x)$ minimal ist unter allen Werten $f(y)$, $y \in X \setminus \{g(0), \ldots, g(n-1)\}$. Man zeigt dann, dass g bijektiv ist. (Dies ist auch ein Spezialfall des Satzes von Schröder-Bernstein, Theorem B.7.)

zu (2). Per Induktion können wir uns auf den Fall eines Produkts mit 2 Faktoren zurückziehen. Es genügt dann, die Abzählbarkeit von $\mathbb{N} \times \mathbb{N}$ zu beweisen. Dafür denken wir uns die

Elemente von $\mathbb{N} \times \mathbb{N}$ als die Punkte mit nicht-negativen ganzzahligen Koordinaten in $\mathbb{R}^2$, und »schreiben diese in eine Liste« (stellen also eine Bijektion mit $\mathbb{N}$) her, indem wir sie nach dem folgenden Schema anordnen:



Wir definieren also $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$ durch

$$0 \mapsto (0,0), \quad 1 \mapsto (1,0), \quad 2 \mapsto (0,1), \quad 3 \mapsto (0,2), \quad 4 \mapsto (1,1), \quad \text{usw.}$$

Jedenfalls von der Zeichnung her ist klar, dass es sich um eine Bijektion handelt, und mit etwas mehr Mühe kann man das auch formal hinschreiben.

zu (3). Wir betrachten eine Vereinigung $X = \bigcup_{i \in I} X_i$, wo alle X_i und die Indexmenge höchstens abzählbar seien. Wegen Teil (1) können wir diese Menge ohne Einschränkung vergrößern, wir können daher die Vereinigung durch eine disjunkte Vereinigung ersetzen und annehmen, dass sowohl I als auch alle X_i abzählbar unendlich sind. Durch Wahl geeigneter Bijektionen können wir diese Vereinigung mit $\bigcup_{i \in \mathbb{N}} \{i\} \times \mathbb{N} = \mathbb{N} \times \mathbb{N}$ identifizieren und die Frage so auf Teil (2) zurückführen. □

Siehe auch Ergänzung LA1.3.65 (das »Hilbertsche Hotel«).

KOROLLAR B.5. (1) *Die Menge $\mathbb{Q}$ der rationalen Zahlen ist abzählbar.*

(2) *Jeder endlichdimensionale $\mathbb{Q}$-Vektorraum ist höchstens abzählbar.*

(3) *Der Polynomring $\mathbb{Q}[X]$ ist abzählbar.*

Andererseits gilt:

SATZ B.6. (1) *Die Menge $\mathbb{R}$ der reellen Zahlen ist überabzählbar.*

(2) *Die Menge $\{0,1\}^{\mathbb{N}} = \prod_{i \in \mathbb{N}} \{0,1\}$ ist überabzählbar.*

BEWEIS. Dies folgt aus dem sogenannten *Diagonalargument* von Georg Cantor. Wir erklären den Beweis von Teil (1), für Teil (2) kann man ähnlich vorgehen.

Wir zeigen, dass sogar das Einheitsintervall $[0,1]$ nicht abzählbar ist. Sei $f\colon \mathbb{N} \to [0,1]$ eine Abbildung. Wir zeigen, dass f nicht surjektiv ist. Insbesondere kann es keine Bijektion zwischen $\mathbb{N}$ und $[0,1]$ geben. Jedes Element von $[0,1]$ hat eine Darstellung als Dezimalzahl (zum Beispiel $0,1234\ldots$). Diese Darstellung ist im allgemeinen nicht eindeutig (zum Beispiel ist $1 = 0,999\ldots$), sie ist aber eindeutig, wenn wir zusätzlich verlangen, dass die Darstellung nicht mit »Periode 9« endet, also nicht irgendwann nur noch Neunen folgen. (Alternativ könnte man die Eindeutigkeit auch erreichen, indem man verlangt, dass nicht irgendwann nur noch Nullen folgen.)

Wir schreiben nun die eindeutigen Dezimalzahldarstellungen von $f(0), f(1), f(2), \ldots$ untereinander und konstruieren die Dezimalzahldarstellung einer Zahl in $x \in [0,1] \setminus \mathrm{Im}(f)$ wie folgt: Die n-te Nachkommastelle von x sei

$$\begin{cases} 4 & \text{wenn die } n\text{-te Stelle nach dem Komma von } f(n-1) \text{ nicht gleich 4 ist,} \\ 5 & \text{wenn die } n\text{-te Stelle nach dem Komma von } f(n-1) \text{ gleich 4 ist.} \end{cases}$$

Dann ist $x \notin \mathrm{Im}(f)$, denn x und $f(n-1)$ unterscheiden sich (mindestens) an der n-ten Stelle hinter dem Komma. Wegen der Eindeutigkeit der Darstellung impliziert das $x \neq f(n-1)$. □

Weil der Körper $\mathbb{C}$ der komplexen Zahlen die Menge $\mathbb{R}$ als Teilmenge enthält, folgt insbesondere, dass $\mathbb{C}$ nicht abzählbar ist.

Auf den Kardinalzahlen lässt sich folgendermaßen eine totale Ordnung definieren: Für Mengen M, M' schreiben wir $\#M \leq \#M'$, wenn es eine injektive Abbildung $M \to M'$ gibt. Wir schreiben $\#M < \#M'$, wenn $\#M \leq \#M'$ und nicht $\#M = \#M'$ gilt, d.h. wenn es eine Injektion $M \to M'$, aber keine Bijektion zwischen M und M' gibt. Diese Definition für $\leq$ erfüllt die Eigenschaften einer totalen Ordnung: Offenbar folgt aus $\#M \leq \#M'$ und $\#M' \leq \#M''$, dass $\#M \leq \#M''$, weil die Verkettung injektiver Abbildungen wieder injektiv ist. Es ist auch klar, dass $\#M \leq \#M$ für alle M gilt, da die Identität eine injektive Abbildung ist.

Etwas schwieriger sind die folgenden beiden Ergebnisse, die die Antisymmetrie und Totalität zeigen:

THEOREM B.7 (Satz von Schröder-Bernstein). *Seien M, M' Mengen. Wenn es injektive Abbildungen $M \to M'$ und $M' \to M$ gibt, dann gibt es eine Bijektion $M \to M'$, d.h. M und M' sind gleichmächtig.*

THEOREM B.8. *Seien M, M' Mengen. Dann gilt genau eine der folgenden drei Aussagen:*

$$\#M < \#M', \quad \#M = \#M', \quad \#M > \#M'.$$

Für die Beweise der Theoreme und des folgenden Satzes siehe zum Beispiel [**Hu**] Kapitel 0, Abschnitt 8.

Die Kardinalzahl $\aleph_0$ ist die kleinste unendliche Kardinalzahl:

SATZ B.9. *Sei M eine unendliche Menge. Dann gilt $\#M \geq \#\mathbb{N}$.*

Mit dem Auswahlaxiom kann man aus der Existenz einer surjektiven Abbildung eine Abschätzung über die Kardinalitäten herleiten:

SATZ B.10. *Seien M, M' Mengen, so dass eine surjektive Abbildung $f: M \to M'$ existiert. Dann gilt $\#M' \leq \#M$.*

BEWEIS. Wir wählen für jedes Element $m' \in M'$ ein Element $g(m')$ aus der (nicht-leeren) Menge $f^{-1}(\{m'\})$ aus. Dies definiert eine Abbildung $g: M' \to M$ mit der Eigenschaft $f \circ g = \mathrm{id}_{M'}$. Insbesondere ist g injektiv. □

BEISPIEL B.11. Sei M eine Menge und $P(M)$ ihre Potenzmenge, d.h. die Menge alle Teilmengen von M. Dann gilt $\#M < \#P(M)$.

Es ist klar, dass es eine Injektion $M \to P(M)$ gibt, zum Beispiel die Abbildung $m \mapsto \{m\}$. Wir müssen daher zeigen, dass es keine Surjektion $M \to P(M)$ gibt. Sei $\varphi: M \to P(M)$ eine Abbildung. Wir behaupten, dass $X := \{m \in M;\ m \notin \varphi(m)\}$ nicht im Bild von φ liegt (insbesondere ist φ nicht surjektiv). In der Tat, nehmen wir an, dass $X = \varphi(m)$ für ein $m \in M$. Wenn $m \in X$, dann folgt $m \notin \varphi(m) = X$, ein Widerspruch. Wenn $m \notin X$, dann folgt $m \notin \varphi(m)$, also $m \in X$, auch ein Widerspruch. Weil weder $m \in X$ noch $m \notin X$ richtig sein kann, kann die Teilmenge X von M nicht im Bild von φ liegen. ◊

BEISPIEL B.12. (1) Es gilt $\#P(\mathbb{N}) = \#\{0,1\}^{\mathbb{N}}$. In der Tat können wir eine Bijektion zwischen $P(\mathbb{N})$ und $\{0,1\}^{\mathbb{N}} = \mathrm{Abb}(\mathbb{N},\{0,1\})$ definieren, indem wir einer Teilmenge $M \subseteq \mathbb{N}$ ihre *charakteristische Funktion*

$$\chi_M\colon \mathbb{N} \to \{0,1\}, \quad n \mapsto \begin{cases} 1 & n \in M, \\ 0 & n \notin M, \end{cases}$$

zuordnen, und umgekehrt einer Abbildung $\chi\colon \mathbb{N} \to \{0,1\}$ die Menge $\chi^{-1}(1)$.

(2) Es gilt $\#P(\mathbb{N}) = \#\mathbb{R}$. (Skizze: Nach Teil (1) genügt es zu zeigen, dass $\mathbb{R}$ und $\{0,1\}^{\mathbb{N}}$ dieselbe Mächtigkeit haben. Es ist nicht schwer, eine Bijektion zwischen $\mathbb{R}$ und dem offenen Einheitsintervall $(0,1)$ anzugeben. Also genügt es, $\#(0,1) = \#\{0,1\}^{\mathbb{N}}$ zu beweisen.

Eine Idee dafür ist, Elemente von $\{0,1\}^{\mathbb{N}}$, also abzählbar unendliche Tupel von Nullen und Einsen als Binärdarstellung (»nach dem Komma«) einer reellen Zahl zwischen 0 und 1 zu betrachten. Mit anderen Worten betrachten wir die Abbildung

$$\{0,1\}^{\mathbb{N}} \to [0,1], \quad (a_i)_{i\in\mathbb{N}} \mapsto \sum_{i=0}^{\infty} \frac{a_i}{2^{i+1}}.$$

Diese Abbildung ist surjektiv, allerdings auf das abgeschlossene Einheitsintervall. Sie ist außerdem nicht injektiv (vergleiche die Diskussion im Zusammenhang mit Cantors Diagonalargument oben). Immerhin sehen wir so aber $\#\{0,1\}^{\mathbb{N}} \geq \#[0,1] \geq \#(0,1) = \#\mathbb{R}$.

Statt diese Abbildung zu einer Bijektion $\{0,1\}^{\mathbb{N}} \to (0,1)$ abzuändern (was ziemlich lästig wäre), benutzen wir, dass es nach dem Satz von Schröder-Bernstein genügt, nun noch die andere Abschätzung, also $\#\{0,1\}^{\mathbb{N}} \leq \#\mathbb{R}$ zu zeigen. Eine Möglichkeit dafür ist, die injektive (warum?) Abbildung

$$\{0,1\}^{\mathbb{N}} \to \mathbb{R}, \quad (a_i)_{i\in\mathbb{N}} \mapsto \sum_{i=0}^{\infty} \frac{a_i}{3^{i+1}}$$

herzunehmen.

Wenn man Satz B.10 (für dessen Beweis wir das Auswahlaxiom benutzt haben) nicht einsetzen möchte, kann man die Abschätzung $\mathbb{R} \leq \#\{0,1\}^{\mathbb{N}} = \#P(\mathbb{N})$ auch folgendermaßen zeigen. Aus einer Bijektion $\mathbb{N} \cong \mathbb{Q}$ erhalten wir eine Bijektion $P(\mathbb{N}) \cong P(\mathbb{Q})$. Die Abbildung $\mathbb{R} \to P(\mathbb{Q}), x \mapsto \{r \in \mathbb{Q};\ r < x\}$, ist injektiv (denn x ist das Supremum in $\mathbb{R}$ seines Bildes unter dieser Abbildung). Also gilt $\#\mathbb{R} \leq \#P(\mathbb{Q}) = \#P(\mathbb{N})$.

◊

ERGÄNZUNG B.13 (Die Kontinuumshypothese). Unter der *Kontinuumshypothese* versteht man die Aussage, dass jede Menge M mit $\#\mathbb{N} \leq \#M \leq \#P(\mathbb{N})$ entweder abzählbar ist (also $\#\mathbb{N} = \#M$ gilt), oder die Mächtigkeit von $P(\mathbb{N})$ hat, also $\#M = \#P(\mathbb{N})(= \#\mathbb{R})$. Mit anderen Worten: Jede überabzählbare Teilmenge von $\mathbb{R}$ hat dieselbe Mächtigkeit wie $\mathbb{R}$.

Es wurde von Kurt Gödel[1] und Paul Cohen[2] bewiesen, dass die Kontinuumshypothese unabhängig von dem üblichen Axiomensystem ZFC ist – sie lässt sich weder widerlegen (Gödel, 1938), noch beweisen (Cohen, 1960). Man könnte also entweder die Kontinuumshypothese zu den anderen Axiomen hinzunehmen, oder ihre Negation. Cohen erhielt für seine Arbeiten 1966 die Fields-Medaille. □ Ergänzung B.13

[1] https://de.wikipedia.org/wiki/Kurt_Gödel
[2] https://de.wikipedia.org/wiki/Paul_Cohen_(Mathematiker)

ANHANG C

Bemerkungen zur Literatur *

C.1. Deutsche Lehrbücher und Vorlesungsskripte

Es gibt *sehr viele* Bücher und Skripte zur Algebra-Vorlesung. Hier eine kleine Auswahl von Texten, die ich alle empfehlen kann. Der Standardstoff (Gruppen, Ringe, Körper und Körpererweiterungen und Galois-Theorie) wird in allen dieser Bücher und Skripte behandelt, und meist noch einiges mehr. Jedes hat einen eigenen Ansatz oder jedenfalls eigene Schwerpunkte und und seinen eigenen Stil – am besten, Sie schauen selbst einmal, womit Sie am besten zurechtkommen.

S. Bosch, *Algebra*, 9. Aufl., Springer 2020.
https://doi.org/10.1007/978-3-662-61649-9

> Das Buch von Bosch ist inzwischen ein Standardwerk. Es ist gut organisiert, enthält im Haupttext alles Wesentliche, aber nicht viel »Drumherum«. Dafür gibt es mehrere Ergänzungsabschnitte sowie Einführungen zum Buch und den einzelnen Kapiteln.

J. C. Jantzen, J. Schwermer, *Algebra*, 2. Aufl., Springer 2014.
https://doi.org/10.1007/978-3-642-40533-4

> Jantzen und Schwermer behandeln neben den Themen der Vorlesung auch noch einiges andere, insbesondere aus der Theorie der Moduln über (nicht notwendig kommutativen) Ringen.

C. Löh, *Algebra*, Vorlesungsskript Univ. Regensburg, WS 2017/18.
http://www.mathematik.uni-regensburg.de/loeh/teaching/algebra_ws1718/lecture_notes.pdf

> In diesem Skript finden Sie insbesondere auch viele Anregungen und motivierende Bemerkungen, die Verbindungen zu anderen Bereichen der Mathematik und anderen Disziplinen herstellen.

F. Lorenz, *Algebra I*, 4. Aufl., Springer Spektrum 2007.

> Im Buch von Lorenz wird der Stoff in etwas anderer Reihenfolge präsentiert als es oft üblich ist (und als wir es in der Vorlesung machen). Statt zunächst die Gruppentheorie zu entwickeln, stellt Lorenz als Motivation eine Diskussion der Konstruierbarkeitsprobleme an den Anfang und entwickelt daran anknüpfend den Begriff der algebraischen Körpererweiterung.

W. Soergel, *Algebra und Zahlentheorie mit grundlegenden Abschnitten aus der Linearen Algebra*, Vorlesungsskript Univ. Freiburg,
http://home.mathematik.uni-freiburg.de/soergel/Skripten/XXALMG.pdf

Ein weiteres Vorlesungsskript, das mir sehr gut gefällt. Hier werden an vielen Stellen interessante Hintergrundinformationen gegeben, zum Beispiel, wie eine Begriffswahl zu erklären ist (oder warum sie vielleicht ungünstig ist und nur aus historischen Gründen beibehalten wird), aber auch, wie man über gewisse Definitionen denken sollte, usw.

C.2. Englische Lehrbücher und Vorlesungsskripte

Noch viel mehr Bücher (und Skripte) zur Algebra gibt es natürlich auf Englisch. Gehen Sie einmal in die Bibliothek und schauen in ein oder zwei davon herein – und sei es nur, um sich zu überzeugen, dass man mathematische Texte auf Englisch genauso leicht (oder oft: so schwer) verstehen kann, wie auf Deutsch.

M. Artin, *Algebra*, Prentice Hall 1991.

D. Dummit, R. Foote, *Abstract Algebra*, 3rd ed., Wiley 2003.

T. Hungerford, *Algebra*, Springer Graduate Texts in Math. **73**, 1974.

J. Milne, *Fields and Galois Theory*, 2021
https://www.jmilne.org/math/CourseNotes/FT.pdf

S. Lang, *Algebra*, Revised Third Ed., Springer Graduate Texts in Math. **211**, 2002. (Oder eine frühere Auflage.)

H. W. Lenstra jr., *Groups, rings, and fields*,
http://websites.math.leidenuniv.nl/algebra/topics.pdf

E. Vinberg, *A Course in Algebra*, Graduate Studies in Math. **56**, AMS 2003.

C.3. Klassiker, Sonstige

B. L. van der Waerden, *Algebra*, Springer, verschiedene Auflagen seit 1930 (zunächst unter dem Titel *Moderne Algebra*)

Ein einflussreiches Lehrbuch der Algebra, das schon sehr nahe an der Darstellung ist, die zum Beispiel in dieser Vorlesung gegeben wird. Im Vergleich zu älteren Lehrbüchern (zum Beispiel dem von H. Weber) tritt der Begriff der Gleichung gegenüber dem der Körpererweiterung in den Hintergrund.

E. Artin, *Galois theory*, Dover
https://projecteuclid.org/ebooks/notre-dame-mathematical-lectures/Galois-Theory/toc/ndml/1175197041

Ein kurzes Büchlein, in dem die Galois-Theorie dargestellt wird, und zwar werden hier besonders Methoden der Linearen Algebra verwendet. Insbesondere kann Artin damit den Hauptsatz der Algebra beweisen, ohne den Satz vom primitiven Element verwenden zu müssen. Der Begriff des Quotienten eines Rings nach einem Ideal wird nicht benutzt; was man dadurch spart, ihn nicht einführen zu müssen, verliert man aber zum Beispiel bei der Diskussion der Kronecker-Konstruktion (die dort mehrere Seiten in Anspruch nimmt, S. 26 ff.)
Achtung: Was bei Artin *normal* heißt, heißt bei uns *galoissch*.

N. Bourbaki, *Algèbre* und *Algébre commutative*.

> Nicolas Bourbaki[1] ist das Pseudonym einer Gruppe französischer Mathematiker, die mit den unter diesem Namen veröffentlichten Büchern einen großen Teil der Grundlagen Mathematik, insbesondere im Bereich der Algebra, im berühmt-berüchtigten »Bourbaki-Stil« – extrem rigoros und formal(istisch) – neu aufgeschrieben hat. Die Texte wurden üblicherweise in vielen Durchgängen intensiv und kontrovers diskutiert, bis schließlich eine endgültige Fassung erreicht wurde.

Stacks Project[2] [**St**]

> Das Stacks-Projekt ist eine Online-Enzyklopädie, in der die Theorie der algebraischen Stacks (ein Begriff aus der algebraischen Geometrie) einschließlich aller Voraussetzungen dargestellt werden soll. Momentaner Zwischenstand der pdf-Datei (Ende September 2021): 7310 Seiten. Das Projekt wurde initiiert und wird betreut von Johan de Jong[3]. Das Kapitel über Körper und Körpererweiterungen befindet sich hier: `https://stacks.math.columbia.edu/tag/09FA`

[1] `https://de.wikipedia.org/wiki/Nicolas_Bourbaki`
[2] `https://stacks.math.columbia.edu/`
[3] `https://de.wikipedia.org/wiki/Aise_Johan_de_Jong`

Literaturverzeichnis

[Ar] E. Artin, *Galois theory*, Dover
https://projecteuclid.org/ebooks/notre-dame-mathematical-lectures/Galois-Theory/toc/ndml/1175197041

[Bo-A] S. Bosch, *Algebra*, 9. Aufl., Springer 2020.
https://doi.org/10.1007/978-3-662-61649-9

[Bu] P. Bundschuh, *Einführung in die Zahlentheorie*, 6. Aufl., Springer 2008.
https://doi.org/10.1007/978-3-540-76491-5

[Hi] D. Hilbert, *Die Theorie der algebraischen Zahlkörper*, Jahresber. der DMV **4** (1897), 175–546.
http://www.digizeitschriften.de/dms/img/?PID=GDZPPN002115344

[Hu] T. Hungerford, *Algebra*, Springer Graduate Texts in Math. **73**, 1974.

[JS] J. C. Jantzen, J. Schwermer, *Algebra*, 2. Aufl., Springer 2014.
https://doi.org/10.1007/978-3-642-40533-4

[La] S. Lang, *Algebra*, Revised Third Ed., Springer Graduate Texts in Math. **211**, 2002. (Oder eine frühere Auflage.)

[Lö] C. Löh, *Algebra*, Vorlesungsskript Univ. Regensburg, WS 2017/18.
http://www.mathematik.uni-regensburg.de/loeh/teaching/algebra_ws1718/lecture_notes.pdf

[Lo] F. Lorenz, *Algebra I*, 4. Aufl., Springer Spektrum 2007.

[Mi] J. Milne, *Fields and Galois Theory*, 2021
https://www.jmilne.org/math/CourseNotes/FT.pdf

[Po] L. Pottmeyer, *Algebra*, Vorlesungsskript,
https://www.uni-due.de/~adg350u/Skripte/Algebra.pdf

[Sch] A. Scholl, *Transitivity of trave and norm*, 2005
https://www.dpmms.cam.ac.uk/study/II/Galois/handout-3.pdf

[Se] J.-P. Serre, *A course in arithmetic*, Springer Grad. Texts in Math. **7**, Springer 1973 (oder das französische Original *Cours d'arithmétique*, Presses Univ. de France, 1970).

[Soe-AZT] W. Soergel, *Algebra und Zahlentheorie*,
http://home.mathematik.uni-freiburg.de/soergel/Skripten/XXAL.pdf

[Soe] W. Soergel, *Algebra und Zahlentheorie mit grundlegenden Abschnitten aus der Linearen Algebra*,
http://home.mathematik.uni-freiburg.de/soergel/Skripten/XXALMG.pdf

[St] *The Stacks project*, https://stacks.math.columbia.edu, 2022.

[We] A. Werner, *Elliptische Kurven in der Kryptographie*, Springer 2002.

Index