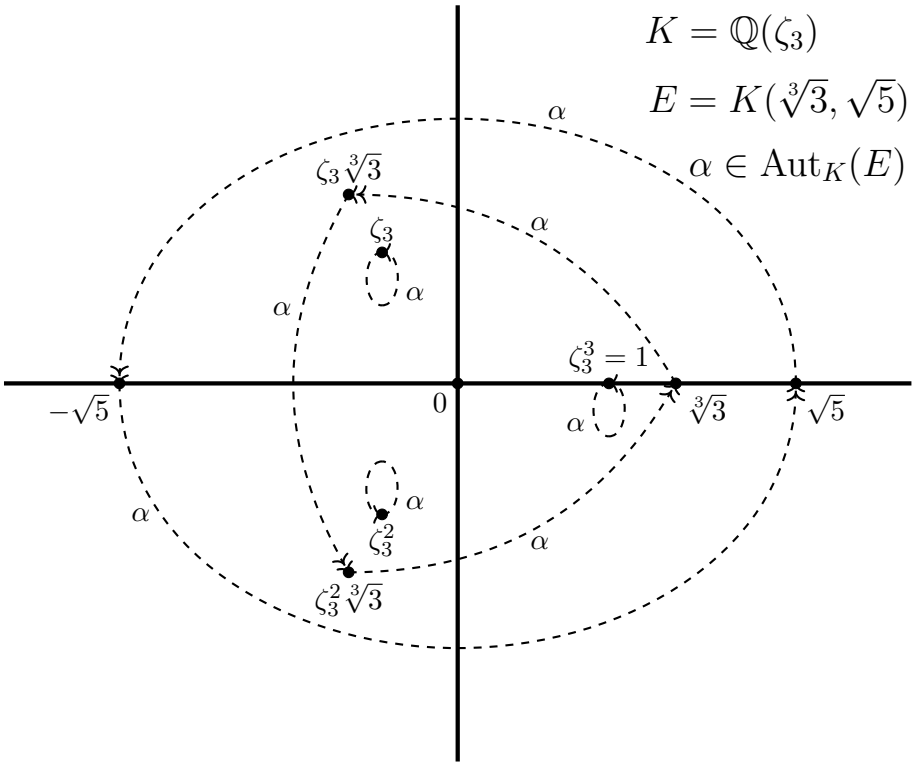


Algebra II

Eine vertiefende Vorlesung

Clemens Schindler Reinhard Winkler

Vorwort

Dieser Text setzt unser gemeinsam mit Martin Goldstern geschriebenes einführendes Buch *Algebra – eine grundlagenorientierte Einführungsvorlesung* fort, das (gemeinsam mit dem vorliegenden Text) unter `https://algebrabuch.github.io` zum Download verfügbar ist. Macht dort der begriffliche Aufbau einen wesentlichen Teil des Inhalts aus, so verlagern sich hier, da die meisten Begriffsbildungen bereits zur Verfügung stehen, die Gewichte hin zu subtileren Beweisen. Weiterhin ist unser Ziel, die Inhalte mit Blick auf die wesentlichen zugrundeliegenden Ideen möglichst organisch darzustellen und technische Komplikationen hintanzuhalten.
Inhaltlich konzentrieren wir uns auf klassische Algebra, wobei es sich an einigen Stellen als sinnvoll und – hoffentlich – klarheitschaffend herausstellt, zu einer allgemeineren Sichtweise zu wechseln und die Situation aus beispielsweise kategorientheoretischem Blickwinkel zu betrachten. In jedem Kapitel vertiefen wir das Wissen über eine bereits bekannte Klasse algebraischer Strukturen: Moduln in Kapitel 7 (mit dem wesentlichen Ziel des Klassifikationssatzes von endlich erzeugten Moduln über Hauptidealringen), Gruppen in Kapitel 8 (endliche und allgemeine), Körper in Kapitel 9 (mit der sogenannten Galoistheorie analysiert man Körpererweiterungen mithilfe ihrer Automorphismen) und kommutative Ringe in Kapitel 10 (mit dem wesentlichen Ziel des Hilbertschen Nullstellensatzes, der das Zusammenspiel zwischen Idealen des Polynomrings über einem Körper einerseits und gemeinsamen Nullstellen dieser Polynome andererseits untersucht).
Wir beziehen uns wiederholt auf Ergebnisse aus der *Einführungsvorlesung*; diese Referenzen sind an Kapitelnummern von 1 bis 6 zu erkennen. Gelegentlich greifen wir auch auf den dortigen Anhang A über mengentheoretische Grundlagen zurück. An einigen Stellen zeigen wir auf, welche weiterführenden Betrachtungen sich an die von uns behandelten Inhalte anschließen können. Dazu führen wir unseren Text ergänzende fundamentale Resultate an, deren Beweis uns aber zu weit führen würde und die stattdessen als Start für weitere Recherchen verwendet werden können.
Dieses Buch ist entstanden aus einem über die Jahre kontinuierlich verbesserten Skriptum von einem von uns (Reinhard Winkler) zu der regelmäßig angebotenen (Wahlpflicht-)Lehrveranstaltung *Algebra II* an der Technischen Universität Wien. Auf Reinhard Winklers Wunsch vor seinem Tod im Herbst 2021 nach kurzer schwerer Krankheit kam Clemens Schindler dazu, um das Projekt zu vollenden. Vereinzelte Fragmente stammen noch von anderen Autor:innen, die für uns nicht mehr alle identifizierbar sind, denen aber durchwegs unser Dank gilt. Insbesondere bedanken wir uns bei Thomas Baumhauer, Sophie Hotz, Christiane Schütz, Friedrich Urbanek und Sebastian Zivota sowie den unzähligen Studierenden, die uns auf Fehler, Ungereimtheiten und Verbesserungsmöglichkeiten aufmerksam gemacht haben und so zu einem wesentlich runderen Text beigetragen haben. Aus jüngerer Zeit möchten wir in diesem Zusammenhang Paul Winkler explizit nennen. Außerdem gilt ein großer Dank unserem Kollegen Michael Pinsker, der zahlreiche Verbesserungsvorschläge gemacht und Fehler aufgezeigt hat. Schließlich danken wir Martin Goldstern für viele Diskussionen. Wenn auch Sie Falsches oder Irreführendes entdecken, bitten wir um eine Nachricht an `algebrabuch@gmail.com` – herzlichen Dank!

Clemens Schindler, Reinhard Winkler † September 2023

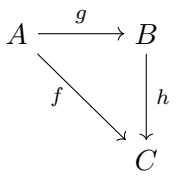
Notationelle Bemerkungen

Durch den gesamten Text hindurch verwenden wir einige notationelle Konventionen, die wir zum einfacheren Nachschlagen an dieser Stelle sammeln.

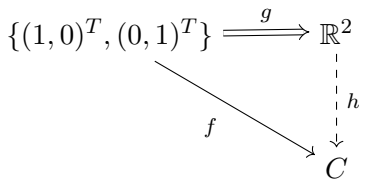
Die Verknüpfung von Funktionen schreiben wir „von rechts nach links“, also explizit $f \circ g(x) := f(g(x))$. Für Äquivalenzrelationen schreiben wir $\sim$, $\equiv$ etc. Für Ordnungsrelationen schreiben wir $\leq$, $\sqsubseteq$ etc., für die entsprechende strikte Ordnung $<$, $\sqsubset$ etc. Einzige Ausnahme davon bildet die Teilmengenrelation: Manche Autor:innen verwenden das Symbol $\subset$, wobei einige damit die strikte und andere die nicht-strikte Teilmenge meinen. Um hier keine Missverständnisse aufkommen zu lassen, schreiben wir $\subseteq$ für die nicht-strikte Teilmenge und $\subsetneq$ für die strikte Teilmenge.

Eines der zentralen Objekte, mit denen wir uns in diesem Text beschäftigen, ist die sogenannte algebraische Struktur. Das ist eine Trägermenge, sagen wir A, versehen mit gewissen Operationen, der Einfachheit halber betrachten wir exemplarisch Addition $+ : A \times A \to A$, $(a, b) \mapsto a + b$ und additive Inverse $- : A \to A$, $a \mapsto -a$. Die entstehende Struktur bezeichnen wir in diesem Beispiel mit $\mathfrak{A} = (A, +, -)$. Diese Namensgebung verfolgen wir durch den ganzen Text hindurch: Wenn die Trägermenge A, B, C, D etc. heißt, so heißt die entsprechende algebraische Struktur $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$ etc. Im Kontext der – den Großteil des Raums einnehmenden – klassischen algebraischen Strukturen, also Gruppen, Ringen, Körpern, Vektorräumen etc., und wenn aus dem Zusammenhang klar ist, von welchem Typus von Struktur gerade die Rede ist, werden wir auf die Unterscheidung zwischen A und $\mathfrak{A}$ zur einfacheren Notation verzichten. Beispielsweise werden wir zumeist von der Gruppe G sprechen, und nicht von der Gruppe $\mathfrak{G}$ auf der Trägermenge G.

An vielen Stellen werden sogenannte kommutative Diagramme eine wichtige Rolle spielen, wie zum Beispiel



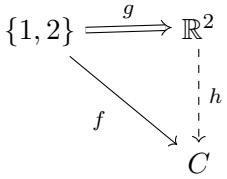
Das bedeutet, dass Abbildungen $f : A \to C$, $g : A \to B$ und $h : B \to C$ vorliegen, sodass $f = h \circ g$ gilt. Eine Erweiterung dieser Notation verdient eine spezielle Situation, auf die wir wiederholt stoßen werden und die sich am besten anhand eines Beispiels illustrieren lässt: Sei $\mathbb{R}^2$ der kanonische zweidimensionale Vektorraum über $\mathbb{R}$, sei $\{(1,0)^T, (0,1)^T\}$ die kanonische Basis und sei C irgendein Vektorraum über $\mathbb{R}$. Dann ist $\{(1,0)^T, (0,1)^T\}$ in $\mathbb{R}^2$ enthalten, also $g : \{(1,0)^T, (0,1)^T\} \to \mathbb{R}^2$ für die Inklusionsabbildung. Ist eine *beliebige* Abbildung $f : \{(1,0)^T, (0,1)^T\} \to C$ gegeben, so *existiert* eine *eindeutige* lineare Abbildung $h : \mathbb{R}^2 \to C$, sodass $f = h \circ g$, nämlich $h((x,y)^T) := xf((1,0)^T) + yf((0,1)^T)$ – dies ist eine Anwendung des Fortsetzungssatzes. Wir werden dafür



schreiben. Die unterschiedlichen Pfeiltypen sind also folgendermaßen zu verstehen: Die doppelt gezeichnete Inklusionsabbildung g ist fest mit dem betrachteten Objekt verbunden, hier mit der kanonischen Basis $\{(1,0)^T,(0,1)^T\}$ als Teilmenge von $\mathbb{R}^2$; vor der durchgezogenen Abbildung f sowie vor dem Objekt C ist ein Allquantor zu denken; und vor der strichliert gezeichneten Abbildung h ist ein Quantor der eindeutigen Existenz zu denken; kurz:

$$g \text{ fest} \rightsquigarrow \forall f, C\ \exists! h$$

Wenn wir uns später mit dieser Situation beschäftigen werden, wird g nicht notwendigerweise die Inklusionsabbildung sein. In unserem aktuellen Beispiel können wir zur Illustration die kanonische Basis $\{(1,0)^T,(0,1)^T\}$ durch $\{1,2\}$ ersetzen und die Abbildung $g : \{1,2\} \to \mathbb{R}^2$ betrachten, die durch $g(1) := (1,0)^T$ und $g(2) := (0,1)^T$ definiert ist[1]. Dann gilt



Explizit: Wenn g so wie eben beschrieben definiert ist (und damit fest gegeben ist), dann gibt es für jeden Vektorraum C und jede Funktion $f : \{1,2\} \to C$ eine eindeutige lineare Abbildung $h : \mathbb{R}^2 \to C$, die das Diagramm schließt (nämlich $h((x,y)^T) := xf(1)+yf(2)$).

[1] Dies ist die formale Entsprechung des üblichen Vorgehens, die kanonischen Basisvektoren mit Indizes zu definieren, also $e_1 := (1,0)^T$ und $e_2 := (0,1)^T$.

Klassifikation der UE-Aufgaben

Jede Übungsaufgabe wird zu einem von mehreren Typen (gelegentlich auch zu mehr als einem) durch jeweils einen der Buchstaben A, B, D, E, F, V, W zugeordnet. Dies soll Ihnen im Vorhinein darüber Information geben, welche Arbeit und welche Einsicht Sie erwartet:

(A) (Alternative Sichtweise): Für einen bereits bekannten Inhalt soll durch einen alternativen Zugang das Verständnis erweitert werden.

(B) (Beispiel): Damit wird ein explizites Beispiel behandelt, das charakteristisch ist für einen Begriff oder Sachverhalt aus der allgemeinen Theorie. Oder ein Gegenbeispiel, welches belegt, dass eine scheinbar harmlose Variante oder Umformulierung den Sinn einer Definition deutlich verändert, oder aus einem wahren und interessanten Satz einen falschen oder trivial gültigen Satz erzeugt.

(D) (Diskussion): Damit werden offene und möglicherweise vage Aufgabenstellungen markiert, die eher zur Diskussion anregen sollen als ein ganz bestimmtes Ergebnis einzufordern.

(E) (Erweiterung): Damit wird der eigentliche Inhalt des Textes verlassen. Der Lohn für den Aufwand, sich trotzdem mit der Aufgabe zu beschäftigen, besteht in einer Erweiterung des Horizonts und/oder Vertiefung des Verständnisses. Über diesen Umweg kann man davon eventuell auch in Hinblick auf den Kernstoff profitieren. Oft ergibt sich dieser Effekt schon allein dadurch, dass man sich die Aufgabenstellung klar macht.

(F) (Fingerübung): Solche Aufgaben dienen vor allem der Kontrolle des Verständnisses der wesentlichen Konzepte, sind abgesehen davon aber in der Regel für sich genommen von geringerem Interesse. Diese Aufgaben können sehr kurz oder auch länger sein. Substanzielle, d.h. für die Theorie wichtige neue Ideen sind für die Bearbeitung nicht erforderlich. Fingerübungen, die dennoch irgendwelche Einsichten von allgemeinerem Interesse zeitigen, sind mit (F+) gekennzeichnet.

(V) (Vervollständigung): Hier steht das Anliegen im Vordergrund, Beweislücken im Haupttext zu schließen. Häufig handelt es sich um kleine, eher technische Ergänzungen, die zunächst ausgespart wurden, damit in einem Beweis die wesentlichen Gedanken nicht durch ausufernde technische Details verschleiert werden. Außerdem werden gewisse Beweise, die aber weder sehr schwierig sind noch besondere Ideen beinhalten, in Übungsaufgaben von diesem Typ ausgelagert.

(W) (Wichtig, Wesentlich): In solchen Übungsaufgaben werden Aussagen bewiesen, die eine wichtige Rolle für das Verständnis der Hauptinhalte des Textes spielen.

Selbstverständlich sind die Grenzen zwischen diesen Typen nicht scharf, und die meisten Übungsaufgaben tragen viele Aspekte in sich. Wir haben den- oder diejenigen davon ausgewählt, den oder die wir im Vordergrund sehen.

Inhaltsverzeichnis

7 Vertiefung der Modultheorie

In diesem Kapitel greifen wir das Thema von Abschnitt 3.3 wieder auf. Zur Einstimmung beginnen wir zwecks Motivation mit einer Rekapitulation bekannter Tatsachen.
Die Theorie der Vektorräume und ihrer strukturverträglichen Abbildungen, nämlich der linearen, ist Gegenstand der Linearen Algebra. Von den wichtigen algebraischen Strukturen haben Vektorräume V über einem Körper K die einfachste Strukturtheorie: Ist K vorgegeben, so ist die Dimension nicht nur eine Invariante (je zwei isomorphe Vektorräume haben dieselbe Dimension), sondern auch umgekehrt: Je zwei Vektorräume derselben Dimension über K sind isomorph.
Im vorliegenden Kapitel beschäftigen wir uns mit der nächstallgemeineren Klasse algebraischer Strukturen. Sie entsteht im Wesentlichen dadurch, dass man die Forderung, K sei ein Körper, abschwächt. Verlangt man lediglich einen Ring R (mit oder ohne Einselement) bei sinngemäßer Beibehaltung aller anderen Forderungen, so erhält man die Klasse der Moduln A über R. Im Falle eines Einselementes $1_R \in R$ mit $1_R a = a$ für alle $a \in A$ spricht man von unitären Moduln über R. Die strukturverträglichen Abbildungen heißen R-Modulhomomorphismen. Man beachte, dass stets auch die abelschen Gruppen mit den Gruppenhomomorphismen sich in diesen Rahmen einfügen, nämlich als unitäre Moduln über dem Ring $\mathbb{Z}$; siehe Unterabschnitt 3.3.1. Um lästige Komplikationen zu vermeiden, werden wir uns, wenn nicht anders vermerkt, auf unitäre Moduln über Ringen mit 1 beschränken.
Wir beginnen mit wichtigen Beispielen, den Prüfergruppen und den p-adischen Zahlen samt einigem Drumherum zum Aufwärmen (7.1). Der darauf folgende Abschnitt 7.2 beschäftigt sich mit grundlegenden Themen der allgemeinen Strukturtheorie der Moduln wie der Frage, wie weit sich das Konzept der Dimension auf Moduln übertragen lässt. Als äußerst nützlich für die Strukturanalyse von Moduln erweisen sich exakte Sequenzen. Das zeigt sich bereits in Abschnitt 7.3 über projektive und injektive Moduln. Unter den abelschen Gruppen (aufgefasst als $\mathbb{Z}$-Moduln) sind die projektiven genau die freien, die injektiven genau die teilbaren. Der Struktursatz über endlich erzeugte Moduln über Hauptidealringen (bzw. endlich erzeugte abelsche Gruppen) ist Gegenstand von 7.4. Abschnitt 7.5 bildet den Abschluss des Kapitels und beschäftigt sich mit Verallgemeinerungen rund um das aus der Linearen Algebra bekannte Konzept des Dualraums. Ist R nicht kommutativ, erfordert das die Unterscheidung von Links-, Rechts- und Bimoduln, was einige technische Komplikationen zur Folge hat.

7.1 Wichtige Beispiele: Prüfergruppen und p-adische Zahlen

Die p-Prüfergruppe C_{p^∞}, $p \in \mathbb{P}$, lässt sich als multiplikative Untergruppe von $\mathbb{C}$ realisieren. Ihre Elemente sind sämtliche $z \in \mathbb{C}$ mit $z^{p^n} = 1$ für ein positives $n \in \mathbb{N}$. Offenbar

ist C_{p^∞} die Vereinigung zyklischer Gruppen C_{p^n} der Ordnung p^n. Gemeinsam erzeugen alle C_{p^∞}, $p \in \mathbb{P}$, die sogenannte universelle Prüfergruppe, die ihrerseits isomorph ist zur additiven Gruppe $\mathbb{Q}/\mathbb{Z}$. Nach einem Prolog über topologische Algebren (7.1.1) ist die Interpretation der Prüfergruppen als direkte Limiten Gegenstand von 7.1.2. In einem gewissen Sinn dual dazu sind die ganzen p-adischen Zahlen $\overline{\mathbb{Z}}_p$, die sich auch als Integritätsbereich mit Quotientenkörper $\overline{\mathbb{Q}}_p$ auffassen lassen, siehe 7.1.3. Das Wesen dieser Dualität wird in 7.1.4 genauer untersucht sowie in 7.1.5 kategorientheoretisch beleuchtet.

7.1.1 Prolog über topologische Algebren und insbesondere Gruppen

Viele Objekte in der Mathematik tragen sowohl eine algebraische als auch eine topologische Struktur. Von Interesse ist das insbesondere, wenn diese beiden Strukturen miteinander verträglich sind. Eine naheliegende Definition aus Sicht der Universellen Algebra lautet daher:

Definition 7.1.1.1. Sei $\mathfrak{A} = (A, \Omega)$ mit einer Familie $\Omega = (\omega_i)_{i\in I}$ von Operationen $\omega_i : A^{n_i} \to A$ der Stelligkeiten $n_i \in \mathbb{N}$ eine Algebra vom Typ $\tau = (n_i)_{i\in I}$. Außerdem sei eine Topologie $\mathcal{T}$ auf A gegeben und $\mathcal{T}_n$ die Produkttopologie auf A^n für alle $n \in \mathbb{N}$. Dann nennt man $\mathfrak{A}$ eine (universelle) *topologische Algebra*, wenn für alle $i \in I$ die Abbildung ω_i stetig ist bezüglich der Topologien $\mathcal{T}_{n_i}$ auf A^{n_i} und $\mathcal{T}$ auf A.

Üblicherweise spricht man bei einer topologischen Algebra, die gleichzeitig eine Halbgruppe, ein Monoid, eine Gruppe, ein Ring etc. ist, von einer *topologischen Halbgruppe*, einem *topologischen Monoid*, einer *topologischen Gruppe*, einem *topologischen Ring* etc. Doch ist Vorsicht geboten, weshalb wir keine allgemeine Definition dieser Art aussprechen. Denn nicht in allen Fällen, wo algebraische und topologische Struktur zusammentreffen, leistet Definition 7.1.1.1 das Gewünschte: In topologischen Körpern wird die Stetigkeit der multiplikativen Inversenbildung extra gefordert. In Definition 7.1.1.1 ist diese Eigenschaft nicht inkludiert.

UE 1 ► **Übungsaufgabe 7.1.1.2.** (B) Können Sie einen topologischen Ring finden, der algebraisch sogar ein Körper ist, nicht jedoch ein topologischer Körper? ◄ **UE 1**

Auch bei topologischen Moduln und Vektorräumen ist es üblich, Definition 7.1.1.1 zu verschärfen. Sei also A ein Modul über dem Ring R. Von einem topologischen R-Modul verlangt man nicht nur die Stetigkeit der einstelligen Abbildungen $a \mapsto ra$ für jedes $r \in R$. Man verlangt, dass neben A (als abelsche topologische Gruppe) auch der Ring R eine Topologie trägt, bezüglich der R ein topologischer Ring ist, und darüber hinaus die Abbildung $(r, a) \mapsto ra$ vom Produktraum $R \times A$ nach A stetig ist.

UE 2 ► **Übungsaufgabe 7.1.1.3.** (B) Können Sie einen topologischen Ring R und einen R-Modul A mit folgenden Eigenschaften finden? A soll eine abelsche topologische Gruppe sein und die Abbildungen $a \mapsto ra$ für jedes $r \in R$ stetig, nicht aber $(r, a) \mapsto ra$ als Abbildung $R \times A \to A$. ◄ **UE 2**

Die insgesamt wohl wichtigste Klasse algebraisch-topologischer Strukturen, die Klasse der *topologischen Gruppen* entspricht aber der Definition 7.1.1.1, explizit:
Eine Gruppe mit Trägermenge G, auf der zusätzlich eine Topologie $\mathcal{T}$ vorliegt, ist genau dann eine topologische Gruppe, wenn sowohl die binäre Operation $G\times G \to G$, $(g_1, g_2) \mapsto g_1g_2$, als auch die Inversenbildung $G \to G$, $g \mapsto g^{-1}$, stetig sind. Für das neutrale Element muss nichts extra gefordert werden: Die 0-stellige Funktion $G^0 = \{\emptyset\} \to G$, $\emptyset \mapsto e_G$, ist bezüglich der einzigen Topologie auf der einelementigen Menge G^0 jedenfalls stetig.
Hier soll die Theorie topologischer Gruppen nicht breit entwickelt werden. Wir begnügen uns mit einigen, teilweise durch Übungsaufgaben ergänzten Beobachtungen, die sich für unsere Zwecke immer wieder als nützlich erweisen. Elementare Begriffe aus der Topologie werden dabei als bekannt vorausgesetzt.
Aus der Stetigkeit der binären Operation auf einer topologischen Gruppe G folgt sehr leicht die Stetigkeit aller Links- und Rechtstranslationen $\lambda_g : G \to G$, $x \mapsto gx$, bzw. $\rho_g : G \to G$, $x \mapsto xg$. Weil auch ihre Umkehrabbildungen $\lambda_{g^{-1}}$ und $\rho_{g^{-1}}$ stetig sind, handelt es sich um Homöomorphismen. Sowohl durch λ_g als auch durch ρ_g wird daher der Umgebungsfilter der Eins (d.h. des neutralen Elements) in den Umgebungsfilter von g übergeführt. Man kann sagen: Eine topologische Gruppe sieht topologisch an jedem Punkt gleich aus. Liegt die algebraische Struktur von G vor, so genügt es für die Kenntnis der Topologie auf G, den Umgebungsfilter der 1 zu kennen, oder noch sparsamer: eine Umgebungsbasis der 1. In der Regel werden wir von dieser Einsicht Gebrauch machen und die Topologie einer topologischen Gruppe durch Angabe einer Umgebungsbasis der Eins definieren. Natürlich muss ein Mengensystem $\mathcal{U}$ auf G gewisse Bedingungen erfüllen, damit es eine (dann eindeutig bestimmte) Topologie $\mathcal{T}$ auf G gibt, sodass G bezüglich $\mathcal{T}$ eine topologische Gruppe und $\mathcal{U}$ eine Umgebungsbasis der Eins in G bezüglich $\mathcal{T}$ ist. Mit folgendem Kriterium werden wir bevorzugt arbeiten. Wir schreiben für $g \in G$ und für Teilmengen $U, V \subseteq G$ zur Abkürzung wie gewohnt $U^{-1} := \{u^{-1} : \ u \in U\}$, $UV := \{uv : \ u \in U, \ v \in V\}$, $gU := \{g\}U$, $Ug := U\{g\}$ etc.

Proposition 7.1.1.4. *Sei G eine Gruppe mit neutralem Element 1_G und $\mathcal{U}$ ein System von Teilmengen von G mit folgenden Eigenschaften:*

- *(Umgebung der Eins): $1_G \in U$ für alle $U \in \mathcal{U}$.*
- *(Filtereigenschaft): Zu allen $U, V \in \mathcal{U}$ gibt es ein $W \in \mathcal{U}$ mit $W \subseteq U \cap V$.*
- *(Stetigkeit der binären Operation): Zu allen $U \in \mathcal{U}$ gibt es ein $V \in \mathcal{U}$ mit $VV \subseteq U$.*
- *(Stetigkeit der Inversenbildung): Zu allen $U \in \mathcal{U}$ gibt es ein $V \in \mathcal{U}$ mit $V^{-1} \subseteq U$.*

Dann gilt:

1. *$\mathcal{T} := \{O \subseteq G : \ \forall g \in O \ \exists U \in \mathcal{U} : \ Ug \subseteq O\}$ ist eine Topologie auf G.*
2. *Für jedes $g \in G$ ist $\mathcal{U}_g := \{Ug : \ U \in \mathcal{U}\}$ eine Umgebungsbasis für g.*
3. *G ist bezüglich $\mathcal{T}$ eine topologische Gruppe.*

4. *Ist $\mathcal{U} \subseteq \mathcal{T}$, so auch $\mathcal{U}_g \subseteq \mathcal{T}$ für alle $g \in G$, und $\mathcal{B} := \bigcup_{g\in G} \mathcal{U}_g$ ist eine Basis für die Topologie $\mathcal{T}$.*

5. *Die Topologie $\mathcal{T}$ ist genau dann T2 (d.h. eine Hausdorff-Topologie, je zwei verschiedene Punkte besitzen disjunkte Umgebungen), wenn der Schnitt aller $U \in \mathcal{U}$ nur 1_G enthält.*

6. *(Stetigkeit der Konjugationen): Zu allen $U \in \mathcal{U}$ und $g \in G$ gibt es ein $V \in \mathcal{U}$ mit $gVg^{-1} \subseteq U$.*

UE 3 ▶ **Übungsaufgabe 7.1.1.5.** (V) Beweisen Sie Proposition 7.1.1.4. ◀ **UE 3**
Bemerkung: In der vorletzten Aussage von Proposition 7.1.1.4 kann das Trennungsaxiom T2 auch durch eines der Trennungsaxiome T0, T1, T3 oder T$3\frac{1}{2}$ ersetzt werden.

UE 4 ▶ **Übungsaufgabe 7.1.1.6.** (E) Rekapitulieren Sie aus der Topologie die Hierarchie der Trennungsaxiome. In topologischen Gruppen sind T0, T1, T2, T3 und T$3\frac{1}{2}$ äquivalent. Zeigen Sie möglichst viele der Implikationen, seien Sie aber nicht frustriert, wenn Ihnen nicht alle Beweise gelingen. ◀ **UE 4**

Wir werden uns mit zwei wichtigen Beispielklassen topologischer Gruppen befassen, den lokalkompakten abelschen Gruppen in 7.1.4 und in der (unendlichdimensionalen) Galoistheorie (siehe 9.3.4) mit gewissen Automorphismengruppen, also speziellen Permutationsgruppen. Als Vorbereitung auf die letzteren sind schon hier ein paar Überlegungen am Platze.
Jede Menge X trägt die diskrete Topologie, die Menge X^X aller Abbildungen von X nach X entsprechend die Produkttopologie, die wir in diesem Kontext auch die Topologie der punktweisen Topologie oder auch die schwache Topologie nennen. Als Rechtfertigung für diese Sprechweise dient die folgende etwas allgemeiner formulierte Tatsache:

Proposition 7.1.1.7. *Seien X_i, $i \in I$, topologische Räume. Auf dem kartesischen Produkt $X := \prod_{i\in I} X_i$ stimmen folgende drei Topologien überein:*

Produkttopologie: *Das ist jene Topologie auf X, für die alle Mengen $[O_{i_0}]$, O_{i_0} offen in X_{i_0}, $i_0 \in I$, eine Subbasis bilden. Dabei bezeichnet $[O_{i_0}]$ die Menge aller $(x_i)_{i\in I} \in X$ mit $x_{i_0} \in O_{i_0}$.*

schwache Topologie: *Das ist die schwächste Topologie auf X, bezüglich der alle Projektionen $\pi_j : X \to X_j$, $(x_i)_{i\in I} \mapsto x_j$, $j \in I$, stetig sind.*

Topologie der punktweisen Konvergenz: *Das ist jene Topologie auf X, bezüglich der ein Netz aus X genau dann gegen $(x_i)_{i\in I}$ konvergiert, wenn für jedes $j \in I$ das Netz der Bilder unter π_j gegen $x_j \in X_j$ konvergiert.*

UE 5 ► Übungsaufgabe 7.1.1.8. (V) Beweisen Sie Proposition 7.1.1.7. **◄ UE 5**

Im Spezialfall des Produktraumes $X^X = \prod_{i\in X} X$ aller Abbildungen $X \to X$ liegt zusätzlich die binäre Operation der Hintereinanderausführung und somit ein Monoid mit id_X als neutralem Element vor, das sogenannte symmetrische Monoid auf X, siehe auch Definition 3.1.2.4. Für diskretes X ist diese Verknüpfung stetig:

Proposition 7.1.1.9. *Sei X eine Menge mit diskreter Topologie. Dann bildet die Menge X^X aller Abbildungen von X nach X bezüglich der Hintereinanderausführung $\circ$ und bezüglich der Produkttopologie ein topologisches Monoid. Dieses erfüllt das Hausdorffsche Trennungsaxiom: Je zwei $f \neq g \in X^X$ haben disjunkte Umgebungen.*
Die symmetrische Gruppe $S(X)$ (bestehend aus allen bijektiven $f : X \to X$) bildet ein Untermonoid von X^X, das sogar eine topologische Gruppe ist.

Beweis. Wir müssen die Stetigkeit von $\circ$ an einer Stelle $(f, g) \in X^X \times X^X$ überprüfen. Sei dazu eine Umgebung U von $f \circ g$ gegeben. Nach Definition der Topologie gibt es eine endliche Menge $E \subseteq X$ derart, dass U sicher all jene $h \in X^X$ enthält, die $h(x) = (f\circ g)(x) = f(g(x))$ für alle $x \in E$ erfüllen. Wir haben Umgebungen U_f von f und U_g von g zu finden mit $f_1 \circ g_1 \in U$ für alle $f_1 \in U_f$ und $g_1 \in U_g$. Die Menge U_f, bestehend aus jenen $f_1 \in X^X$, die $f_1(g(x)) = f(g(x))$ für alle $x \in E$ erfüllen, ist eine offene Umgebung von f. Analog ist die Menge U_g, bestehend aus jenen $g_1 \in X^X$, die $g_1(x) = g(x)$ für alle $x \in E$ erfüllen, eine offene Umgebung von g. Für alle $x \in E$, $f_1 \in U_f$ und $g_1 \in U_g$ gilt $(f_1 \circ g_1)(x) = f_1(g_1(x)) = f_1(g(x)) = f(g(x))$, also liegt $f_1 \circ g_1$ für $f \in U_f$ und $g \in U_g$ tatsächlich in U.
Um zu zeigen, dass auf $S(X)$ auch die Inversenbildung stetig ist, sei $f \in S(X)$ und U eine Umgebung von f^{-1}. Wieder gibt es eine endliche Menge $E \subseteq X$ derart, dass U sicher all jene $h \in S(X)$ enthält, die $h(x) = f^{-1}(x)$ für alle $x \in E$ erfüllen. Wir betrachten die Menge E' aller $f^{-1}(x)$ mit $x \in E$. Weil mit f auch f^{-1} bijektiv, insbesondere also injektiv ist, sind diese Elemente paarweise verschieden. All jene $g \in S(X)$, die auf E' mit f übereinstimmen, bilden eine offene Umgebung V von f. Jedes solche g hat eine Umkehrabbildung, die auf E mit f^{-1} übereinstimmt, also liegt g^{-1} für $g \in V$ tatsächlich in U.
Zur Hausdorffschen Trennungseigenschaft: Sind $f, g \in X^X$ verschieden, so gibt es ein $x \in X$ mit $f(x) \neq g(x)$. Dann ist $U_f := \{f_1 \in X^X : \ f_1(x) = f(x)\}$ eine Umgebung von f und $U_g := \{g_1 \in X^X : \ g_1(x) = g(x)\}$ eine Umgebung von g, sodass $U_f \cap U_g = \emptyset$. □

UE 6 ► Übungsaufgabe 7.1.1.10. (F) Zeigen Sie in der Situation von Proposition 7.1.1.9, dass bei unendlichem X die Teilmenge $S(X)$ in X^X nicht abgeschlossen ist. **◄ UE 6**

Bei der Strukturanalyse topologischer Algebren, insbesondere topologischer Gruppen, ist ein Homomorphismus bzw. Isomorphismus der algebraischen Struktur besonders dann von Interesse, wenn es sich zugleich um eine stetige Abbildung bzw. um einen Homöomorphismus, einen sogenannten *topologischen Isomorphismus* handelt.

7.1.2 Beispiel Prüfergruppe

Wir erinnern an die Definition und eine wesentliche Eigenschaft der Prüfergruppen; siehe Satz 3.3.3.7. Bezeichne wieder C_n die zyklische Gruppe der Ordnung n. Wir können uns C_n als Untergruppe der multiplikativen Gruppe aller komplexen Zahlen z vom Betrag $|z| = 1$ vorstellen, nämlich als Gruppe der n-ten komplexen Einheitswurzeln.
Sei p eine feste natürliche Zahl.[1] Für eine beliebige natürliche Zahl n ist C_{p^n} somit eine Untergruppe von $C_{p^{n+1}}$. Wir bezeichnen die Inklusionsabbildung mit ι_n, außerdem die Vereinigung der aufsteigenden Folge

$$C_p \leq C_{p^2} \leq C_{p^3} \leq \dots$$

mit C_{p^∞}; diese Vereinigung ist offensichtlich eine Gruppe. Für p prim heißt C_{p^∞} auch *p-Prüfergruppe*. Die Inklusionsabbildung von C_{p^n} nach C_{p^∞} bezeichnen wir mit $\iota_{n,\infty}$. Als Vereinigung einer aufsteigenden Folge kann man die p-Prüfergruppe nach Satz 2.2.4.2 bzw. Unterabschnitt 2.3.3 auch als direkten Limes auffassen, genauer: Die Gruppe C_{p^∞} zusammen mit den Inklusionsabbildungen $\iota_{n,\infty}$ bildet einen direkten Limes der Gruppen C_{p_k}, $k \in \mathbb{N}$, zusammen mit den Homomorphismen ι_n, $n \in \mathbb{N}$. Die p-Prüfergruppe erfüllt somit die folgende universelle Eigenschaft:

> Für jede Gruppe G und jede Familie $(\psi_n : n \in \mathbb{N})$ von Homomorphismen $\psi_n \colon C_{p^n} \to G$, die $\psi_n = \psi_{n+1} \circ \iota_n$ für alle $n \in \mathbb{N}$ erfüllen, gibt es genau einen Homomorphismus $\theta \colon C_{p^\infty} \to G$ mit $\theta \circ \iota_{n,\infty} = \psi_n$ für alle $n \in \mathbb{N}$.

Die universelle Prüfergruppe C_∞ ist definiert als das gemeinsame Gruppenerzeugnis aller p-Prüfergruppen, p prim. In Satz 3.3.3.7 hat sich herausgestellt, dass die universelle Prüfergruppe die (innere) direkte Summe der p-Prüfergruppen ist, $C_\infty = \bigoplus_{p \in \mathbb{P}} C_{p^\infty}$.
An dieser Stelle wollen wir eine universelle Eigenschaft auch für die universelle Prüfergruppe herleiten (die in Unterabschnitt 7.1.5 Anlass geben wird zu einer verallgemeinerten Definition des direkten Limes). Dazu betrachten wir zunächst obige Situation unter einem etwas anderen Blickwinkel: Klarerweise existieren nicht nur die Inklusionen $C_{p^n} \to C_{p^{n+1}}$, sondern allgemeiner die Inklusionen $\iota_{m,n} \colon C_{p^m} \to C_{p^n}$ für natürliche Zahlen $m \leq n$. Dabei gilt $\iota_{n,n} = \mathrm{id}_{C_{p^n}}$ für alle $n \in \mathbb{N}$ und $\iota_{n,r} \circ \iota_{m,n} = \iota_{m,r}$ für alle $m \leq n \leq r$ – diese Eigenschaften werden bei der Abstraktion der Situation in Unterabschnitt 7.1.5 noch eine Rolle spielen. Die obige universelle Eigenschaft lässt sich also folgendermaßen umformulieren:

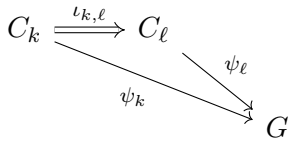
> Für jede Gruppe G und jede Familie $(\psi_n : n \in \mathbb{N})$ von Homomorphismen $\psi_n \colon C_{p^n} \to G$, die $\psi_m = \psi_n \circ \iota_{m,n}$ für alle $m \leq n$ erfüllen, gibt es genau einen Homomorphismus $\theta \colon C_{p^\infty} \to G$ mit $\theta \circ \iota_{n,\infty} = \psi_n$ für alle $n \in \mathbb{N}$.

Der Vorteil dieser Sichtweise liegt darin, dass wir nicht mehr darauf angewiesen sind, dass jedes Element der Indexmenge (hier: $n \in \mathbb{N}$) einen Nachfolger $n+1$ hat, und wir somit allgemeinere Indexmengen (samt allgemeineren Ordnungen auf diesen Indexmengen) zulassen können.

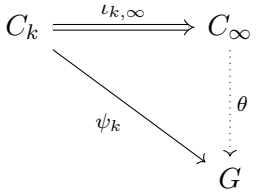
[1] Üblicherweise betrachtet man hier vor allem Primzahlen p, das ist an dieser Stelle aber nicht relevant.

Konkret beobachtet man, dass sogar $C_j \leq C_k$ für alle $j, k \in \mathbb{N} \setminus \{0\}$ mit $j|k$ gilt. Folglich betrachten wir die Inklusionen $\iota_{j,k} \colon C_j \to C_k$ für $j|k$ und bemerken wieder $\iota_{k,k} = \mathrm{id}_{C_{p^k}}$ für alle $k \in \mathbb{N}$ sowie $\iota_{k,\ell} \circ \iota_{j,k} = \iota_{j,\ell}$ für alle $j \leq k \leq \ell$. Damit können wir die universelle Eigenschaft der universellen Prüfergruppe angeben:

Proposition 7.1.2.1. *Sei G eine beliebige Gruppe, und sei $(\psi_k : k \in \mathbb{N} \setminus \{0\})$ eine Familie von Homomorphismen $\psi_k \colon C_k \to G$, sodass alle Diagramme*



für $k|\ell$ kommutieren. (Das heißt, für alle $k|l$ gilt $\psi_l \circ \iota_{k,l} = \psi_k$.)
Dann gibt es einen eindeutig bestimmten Homomorphismus $\theta \colon C_\infty \to G$, sodass alle Diagramme der Form



kommutieren. (Das heißt, für alle k gilt $\theta \circ \iota_{k,\infty} = \psi_k$.)

UE 7 ► Übungsaufgabe 7.1.2.2. (V) Zeigen Sie Proposition 7.1.2.1. **◄ UE 7**

Als Vorgriff auf Unterabschnitt 7.1.5 sei bereits jetzt angemerkt, dass wir die universelle Eigenschaft aus Proposition 7.1.2.1 verwenden werden, um C_∞ als direkten Limes aller zyklischen Gruppen C_k, $k \in \mathbb{N} \setminus \{0\}$, aufzufassen, wobei die Indexmenge $\mathbb{N} \setminus \{0\}$ durch Teilbarkeit geordnet sein soll.

7.1.3 Beispiel p-adische Zahlen

Dual zur eben besprochenen Situation einer unendlichen Folge injektiv ineinander eingebetteter Strukturen sind surjektiv aufeinander abgebildete. Auch hier eignen sich zur Illustration zyklische Gruppen als geradezu archetypische Beispiele. Wir halten eine Primzahl p fest und fassen jedes C_{p^n} als Restklassengruppe $\mathbb{Z}/p^n\mathbb{Z}$ auf, deren Elemente die Gestalt $k + p^n\mathbb{Z}$ haben. Dabei steht $p^n\mathbb{Z}$ für den Normalteiler in $\mathbb{Z}$, der aus allen Vielfachen von p^n besteht. Die ganze Zahl k wird eindeutig, wenn man $0 \leq k < p^n$ fordert.
Die zyklische Gruppe $C_{p^{n+1}}$ der Ordnung p^{n+1} lässt sich homomorph auf die zyklische Gruppe C_{p^n} abbilden, etwa indem man eine Restklasse $k + p^{n+1}\mathbb{Z}$ modulo p^{n+1} auf die Restklasse $k + p^n\mathbb{Z}$ modulo p^n abbildet. Es liegt also eine Serie von Epimorphismen $\varphi_n \colon C_{p^{n+1}} \to C_{p^n}$ vor. Im Gegensatz zur Prüfergruppe werden die Gruppen in Richtung

der Urbilder größer. Eine natürliche Möglichkeit, die gesamte Serie in ein Objekt zu fassen, besteht also darin, gewissermaßen alle unendlichen Rückwärtspfade als Elemente zu betrachten. Formal lässt sich ihre Gesamtheit als eine Untergruppe des unendlichen direkten Produktes $P = \prod_{n\in\mathbb{N}} C_{p^n}$ auffassen. Wir bezeichnen diese Untergruppe mit $\overline{\mathbb{Z}}_p$ (nicht mit $\mathbb{Z}_p$, dem endlichen Restklassenring modulo p verwechseln!). Man nennt sie die Gruppe der *ganzen p-adischen Zahlen*. Sie tragen auch eine multiplikative Struktur, der wir uns etwas später zuwenden werden. Explizit besteht $\overline{\mathbb{Z}}_p$ aus jenen Elementen $(x_n)_{n\in\mathbb{N}} \in P$, die $\varphi_n(x_{n+1}) = x_n$ für alle $n \in \mathbb{N}$ erfüllen.
Es gibt eine sehr ansprechende Darstellung von $\overline{\mathbb{Z}}_p$ bzw. seiner Elemente. Zu einem Element $k + p^n\mathbb{Z}$ sei $k = \sum_{i=0}^{n} a_i p^i$ mit $a_i \in \{0, \ldots, p-1\}$ die übliche Darstellung von k zur Basis p. Dann lässt sich die Wirkung von $\varphi_n \colon \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ beschreiben durch

$$\varphi_n : \quad \sum_{i=0}^{n} a_i p^i + p^{n+1}\mathbb{Z} \quad \mapsto \quad \sum_{i=0}^{n-1} a_i p^i + p^n\mathbb{Z}.$$

Der Epimorphismus φ_n vergisst also gewissermaßen den Koeffizienten a_n. Da alle Wahlen von Folgen $(a_n)_{n\in\mathbb{N}}$ mit $a_n \in \{0, \ldots, p-1\}$ sinnvoll sind, kann man die Elemente von $\overline{\mathbb{Z}}_p$ mit diesen Folgen $(a_n)_{n\in\mathbb{N}}$ identifizieren, oder, der arithmetischen Struktur noch besser angepasst, mit den entsprechenden, zunächst nur formalen, unendlichen Summen

$$\sum_{n=0}^{\infty} a_n p^n,$$

die man als Potenzreihen[2] in p bezeichnen kann. Die Bausteine C_{p^n} von $\overline{\mathbb{Z}}_p$ tragen wie schon angedeutet nicht nur Gruppen-, sondern, vermittels der Darstellung als $\mathbb{Z}/p^n\mathbb{Z}$ mit dem Ideal $p^n\mathbb{Z}$, sogar Ringstruktur. Überdies sind die φ_n auch mit der multiplikativen Struktur verträglich. Folglich trägt $\overline{\mathbb{Z}}_p$ ebenfalls eine Ringstruktur. Üblicherweise ist diese gemeint, wenn von den *ganzen p-adischen Zahlen* die Rede ist. Wie man sofort nachprüft, ist $\overline{\mathbb{Z}}_p$ sogar ein Integritätsbereich und besitzt daher einen Quotientenkörper $\overline{\mathbb{Q}}_p$, den *Körper der p-adischen Zahlen*. OBdA wollen wir $\overline{\mathbb{Z}}_p$ als Unterring von $\overline{\mathbb{Q}}_p$ auffassen. Das Element $p = 0p^0 + 1p^1 + 0p^2 + 0p^3 + \ldots \in \mathbb{Z}_p$ besitzt, wie man leicht einsieht, innerhalb $\overline{\mathbb{Z}}_p$ kein multiplikatives Inverses. Folglich liegt p^{-1} in $\overline{\mathbb{Q}}_p \setminus \overline{\mathbb{Z}}_p$, entsprechend auch p^{-2}, p^{-3} etc. Da in $\overline{\mathbb{Q}}_p$ beliebige endliche Produkte und Summen gebildet werden können, muss $\overline{\mathbb{Q}}_p$ also wenigstens alle Elemente der Gestalt

$$\sum_{n=-N}^{\infty} a_n p^n \quad (\textit{formale Laurentreihen} \text{ in } p, \text{ Operationen jedoch mit Übertrag})$$

mit $N \in \mathbb{N}$ und $a_n \in \{0, 1, \ldots, p-1\}$ enthalten. In der Tat kann man sich überzeugen, dass damit sogar ganz $\overline{\mathbb{Q}}_p$ beschrieben wird.
Wir beschränken uns nochmals kurz auf die ganzen p-adischen Zahlen und ihre Darstellung als Potenzreihen in p. Offenbar gibt es für alle $n \in \mathbb{N}$ natürliche Homomorphismen

[2] Die Bezeichnung als *Potenzreihe* ist hier mit Vorsicht zu genießen. Denn anders als beim Umgang mit Unbestimmten (die wir eher mit $x, y, \ldots$ bezeichnen) wird hier mit Übertrag gerechnet. Der einfacheren Sprechweise halber wollen wir aber an dieser Terminologie festhalten.

$\psi_n\colon \overline{\mathbb{Z}}_p \to \mathbb{Z}/p^n\mathbb{Z}$, nämlich

$$\psi_n : \quad \sum_{i=0}^{\infty} a_i p^i \quad \mapsto \quad \sum_{i=0}^{n-1} a_i p^i + p^n\mathbb{Z},$$

die den Bedingungen $\psi_n = \varphi_n \circ \psi_{n+1}$ für alle $n \in \mathbb{N}$ genügen. Diese Eigenschaft werden wir etwas später als Motivation für den kategorientheoretischen Begriff des indirekten, projektiven oder auch inversen Limes verwenden.
In den Überlegungen, die uns zu den p-adischen Zahlen geführt haben, wurden manche Schritte nicht vollständig ausgeführt. Diese, aber auch weitere interessante Eigenschaften und Aspekte der p-adischen Zahlen sind Gegenstand der folgenden mehrteiligen und relativ umfangreichen Übungsaufgabe. Teile davon involvieren auch topologische Begriffe, die aber weitgehend im Zuge der Aufgabenstellung erklärt werden.

UE 8 ► Übungsaufgabe 7.1.3.1. (V,E) In den topologischen Teilen dieser Aufgabe dürfen Sie sich, wenn Sie wollen, auch auf 7.1.1 beziehen. **◄ UE 8**

(1) Rekapitulieren Sie die Konstruktion des Ringes $\overline{\mathbb{Z}}_p$ der ganzen p-adischen Zahlen und beweisen Sie im Zuge dessen, dass die Elemente von $\overline{\mathbb{Z}}_p$ tatsächlich in einer bijektiven Beziehung zu den formalen Potenzreihen in p stehen. Verwenden Sie im Weiteren diese Potenzreihendarstellung als Normalform.

(2) Beschreiben Sie die Operationen im Ring $\overline{\mathbb{Z}}_p$ anhand der Normalform. (Rechnen mit Übertrag, im Gegensatz zum Rechnen mit Potenzreihen in einer Unbestimmten)

(3) Zeigen Sie, dass die im Text definierten Abbildungen ψ_n tatsächlich der Bedingung $\psi_n = \varphi_n \circ \psi_{n+1}$ genügen.

(4) Rekapitulieren Sie die Definition des Quotientenkörpers eines Integritätsbereiches und beweisen Sie, dass speziell die formalen Laurentreihen in p mit Übertrag wie oben angesprochen tatsächlich einen Quotientenkörper von $\overline{\mathbb{Z}}_p$ bilden. (Insbesondere erfordert dies die Beschreibung der Operationen auf $\overline{\mathbb{Q}}_p$ inklusive multiplikativer Inversenbildung.) Verwenden Sie im Weiteren diese Darstellung von Laurentreihen als Normalform.

(5) Die Menge $\overline{\mathbb{Q}}_p$ trägt eine natürliche Topologie τ. Eine topologische Basis ist gegeben durch alle Mengen $B(N, a_{-N}, a_{-N+1}, \ldots, a_0, \ldots, a_{k-1})$ mit $N, k \in \mathbb{N}$ und $a_i \in \{0, 1 \ldots, p-1\}$. Dabei bestehe $B(N, a_{-N}, a_{-N+1}, \ldots, a_0, \ldots, a_{k-1})$ definitionsgemäß aus allen formalen Laurentreihen der Form $\sum_{n=-N}^{\infty} b_n p^n$, $b_n \in \{0, \ldots, p-1\}$, mit $b_i = a_i$ für $i = -N, -N+1, \ldots, 0, 1, \ldots, k-1$. (Anmerkung: Insbesondere gilt $B(0) = \overline{\mathbb{Z}}_p$.)

Sei dazu τ die Menge aller beliebigen – endlichen oder unendlichen – Vereinigungen von Basismengen $B(N, a_{-N}, a_{-N+1}, \ldots, a_0, \ldots, a_k)$. Zeigen Sie, dass τ tatsächlich eine Topologie auf $\overline{\mathbb{Q}}_p$ ist. Das bedeutet wiederum nach Definition, dass τ abgeschlossen ist bezüglich endlicher Durchschnitte und beliebiger Vereinigungen. Insbesondere müssen $\emptyset$ und $\overline{\mathbb{Q}}_p$ in τ liegen.

(6) Zeigen Sie: Die Topologie τ aus Teil 5 wird durch eine Metrik d induziert, die sogar eine Ultrametrik ist, d.h. die der verschärften Dreiecksungleichung $d(x,z) \leq \max\{d(x,y), d(y,z)\}$ genügt. Anleitung: Wählen Sie als Abstand zweier verschiedener formaler Laurentreihen z.B. die positive Zahl p^{-k}, sofern k der kleinste Index mit unterschiedlichen Gliedern ist.

(7) Beweisen Sie, dass die Mengen $B(N, a_{-N}, a_{-N+1}, \ldots, a_0, \ldots, a_k)$ bezüglich τ abgeschlossen und sogar kompakt sind, und folgern Sie daraus, dass $\overline{\mathbb{Z}}_p$ kompakt und $\overline{\mathbb{Q}}_p$ lokalkompakt ist (d.h. jedes Element in $\overline{\mathbb{Q}}_p$ besitzt eine kompakte Umgebung).

Anleitung: Hier soll Kompaktheit auch das Hausdorffsche Trennungsaxiom inkludieren: Je zwei verschiedene Elemente besitzen disjunkte Umgebungen. Dieses folgt aber bereits aus der Metrisierbarkeit (Teil 6). Der interessante Teil ist die Überdeckungseigenschaft (jede offene Überdeckung hat eine offene Teilüberdeckung). Wenn bekannt, können Sie den Satz von Tychonoff (der Produktraum kompakter Räume ist wieder kompakt) einsetzen. Alternativ können Sie beweisen und dann verwenden, dass ein metrischer Raum (nach Teil 6 liegt ein solcher vor) dann (und nur dann) kompakt ist, wenn der Satz von Bolzano-Weierstraß gilt: Jede unendliche Teilmenge A hat einen Häufungspunkt. (Definitionsgemäß ist das ein solcher Punkt, zu dem jede Umgebung von diesem verschiedene Punkte von A enthält.)

(8) Zeigen Sie, dass τ sowohl $\overline{\mathbb{Z}}_p$ als auch $\overline{\mathbb{Q}}_p$ zu 0-dimensionalen und somit total unzusammenhängenden topologischen Räumen macht. (Ein topologischer Raum heißt 0-dimensional, wenn er eine topologische Basis hat, deren Elemente sowohl offen als auch abgeschlossen sind. Total unzusammenhängend bedeutet, dass die einelementigen Teilmengen die einzigen zusammenhängenden sind.)

(9) Zeigen Sie, dass in $\overline{\mathbb{Q}}_p$ Addition, Multiplikation und Inversenbildung (additiv wie multiplikativ) stetig sind. Anleitung: Weil es sich um einen metrischen Raum handelt, kann man mit Folgenstetigkeit arbeiten. Für die Addition beispielsweise genügt es daher zu beweisen: Konvergieren Elemente $q_n, r_n \in \mathbb{Q}_p$ gegen q bzw. r, so konvergieren ihre Summen $q_n + r_n$ gegen $q + r$. (Definitionsgemäß besagt die hier zu beweisende Stetigkeit der Operationen, dass $\overline{\mathbb{Q}}_p$ sogar ein topologischer Körper und $\overline{\mathbb{Z}}_p$ ein topologischer Ring ist.)

(10) Zeigen Sie: $\overline{\mathbb{Z}}_p$ ist als topologischer Raum homöomorph zur Cantormenge[3], insbesondere also überabzählbar. Anleitung: Zeigen Sie zunächst den für sich äußerst interessanten Satz, dass jeder nichtleere, total unzusammenhängende und kompakte metrische Raum ohne isolierte Punkte homöomorph zur Cantormenge ist. (Statt total unzusammenhängend dürfen Sie auch 0-dimensional voraussetzen.)

(11) Zeigen Sie: Eine unendliche Reihe $\sum_{n=0}^{\infty} q_n$ p-adischer Zahlen q_n ist konvergent (d.h. definitionsgemäß: die Folge der Partialsummen ist konvergent) genau dann, wenn die q_n eine Nullfolge in $\overline{\mathbb{Q}}_p$ bilden.

(12) Bei der Konstruktion von $\overline{\mathbb{Z}}_p$ ist es nur auf die Surjektivität der Homomorphismen

[3] Betrachten Sie die Cantormenge als die Menge aller reellen Zahlen x der Gestalt $x = \sum_{n=1}^{\infty} \frac{a_n}{3^n}$ mit $a_n \in \{0, 2\}$, ausgestattet mit jener Topologie, die diese Menge als Spurtopologie (Unterraumtopologie) von der natürlichen Topologie auf $\mathbb{R}$ erbt.

φ_n angekommen. Da zwischen zwei beliebigen zyklischen Gruppen bzw. Restklassenringen $\mathbb{Z}/(m_i)$ ein Epimorphismus $\varphi\colon \mathbb{Z}/(m_2) \to \mathbb{Z}/(m_1)$ genau dann existiert, wenn m_1 ein Teiler von m_2 ist, können wir statt der Teilerkette $p^0 \mid p^1 \mid p^2 \mid \ldots$ auch irgendeine andere aufsteigende Teilerkette $1 = m_0 \mid m_1 \mid m_2 \mid \ldots$ in $\mathbb{N}$ betrachten, wobei wir oBdA $m_i < m_{i+1}$ für alle $i \in \mathbb{N}$ voraussetzen wollen. Der anstelle von $\overline{\mathbb{Z}}_p$ entstehende Ring sei mit $\overline{\mathbb{Z}}_{(m_n)_{n\in\mathbb{N}}}$ bezeichnet.

Untersuchen Sie, welche Aussagen, die bisher über $\overline{\mathbb{Z}}_p$ gemacht wurden, entsprechend auch für $\overline{\mathbb{Z}}_{(m_n)_{n\in\mathbb{N}}}$ gelten und welche falsch werden.

(13) Zeigen Sie: Der Ring $\overline{\mathbb{Z}}_{(m_n)_{n\in\mathbb{N}}}$ lässt sich als direktes Produkt gewisser Ringe R_p darstellen, wobei p alle Primzahlen durchläuft. Dabei ist R_p entweder isomorph zu einem endlichen Restklassenring $\mathbb{Z}/p^n\mathbb{Z}$ oder zum Ring $\overline{\mathbb{Z}}_p$ der ganzen p-adischen Zahlen. Erklären Sie auch, wie diese Fälle von $(m_n)_{n\in\mathbb{N}}$ abhängen.

Ebenfalls einen lokalkompakten topologischen Ring bzw. Körper erhält man auf ganz ähnliche Weise, wenn man von formalen Potenz- bzw. Laurentreihen

$$\sum_{n=-N}^{\infty} a_n x^n$$

in einer *Unbestimmten* x (statt von Elementen p aus einem vorgegebenen endlichen Ring) ausgeht. Aus ziemlich offensichtlichen Gründen spricht man bei festem $N = 0$ vom Ring $\mathbb{Z}_p[[x]]$ der formalen Potenzreihen über dem Körper $\mathbb{Z}_p = \mathbb{Z}/(p)$ mit p Elementen (siehe auch 3.4.6). Bei variablem $N \in \mathbb{Z}$ lässt sich der resultierende Ring $\mathbb{Z}_p[[[x]]]$ der formalen Laurentreihen als dessen Quotientenkörper auffassen. Topologisch besteht kein Unterschied zu $\overline{\mathbb{Z}}_p$ bzw. $\overline{\mathbb{Q}}_p$, sehr wohl aber algebraisch. Denn mit den Koeffizienten $a_i \in \{0, 1, \ldots, p-1\}$ wird jetzt nicht mit Übertrag gerechnet, sondern modulo p. Man hat es also mit Potenz- bzw. Laurentreihen in einer Variablen x im eigentlichen Sinn zu tun. Statt des Primkörpers $\mathbb{Z}_p$ kann man genauso von einem beliebigen endlichen Körper ausgehen. Diese Aspekte wollen wir genauer in der nächsten Übungsaufgabe beleuchten.

UE 9 ► Übungsaufgabe 7.1.3.2. (A) **◄ UE 9**

(1) Welche der Teile von Übungsaufgabe 7.1.3.1 gelten identisch oder wenigstens sinngemäß auch mit $\mathbb{Z}_p[[x]]$ statt mit $\overline{\mathbb{Z}}_p$?

(2) Begründen Sie, warum $\overline{\mathbb{Z}}_p$ und $\mathbb{Z}_p[[x]]$ schon als additive Gruppen und somit erst recht als Ringe nicht isomorph sein können, analog für ihre Quotientenkörper.

(3) Wie verhält es sich mit der Isomorphie der vorkommenden Strukturen bei variierendem p?

(4) Wie steht es mit topologischen Homöomorphismen zwischen den betrachteten Strukturen?

Aus Übungsaufgabe 7.1.3.2 ergeben sich zwei unendliche Serien paarweise nicht isomorpher lokalkompakter topologischer Körper: jene der $\overline{\mathbb{Q}}_p$ und jene der $\mathbb{Z}_p[[[x]]]$ mit $p \in \mathbb{P}$. Auch endliche Erweiterungen dieser Körper (siehe Kapitel 6) sind lokalkompakt, ebenso

wie klarerweise $\mathbb{R}$ und $\mathbb{C}$. Schließlich sind diskrete Körper trivialerweise lokalkompakt. Denn in der diskreten Topologie sind alle Teilmengen offen, insbesondere ist $\{x\}$ eine kompakte Umgebung eines beliebigen Punktes x. Lässt man auch nichtkommutative Körper (Schiefkörper) zu, so kommen noch die Hamiltonschen Quaternionen $\mathbb{H}$ dazu (siehe Übungsaufgabe 1.2.4.10). Ein bemerkenswerter Satz (den wir nicht beweisen werden) besagt, dass es bis auf topologische Isomorphie keine weiteren Beispiele gibt.
Einige der obigen Erkenntnisse fassen wir knapp zusammen:

Satz 7.1.3.3. *Die ganzen p-adischen $\overline{\mathbb{Z}}_p$ bilden einen kompakten topologischen Ring, der sogar ein Integritätsbereich ist. Sein Quotientenkörper ist (zusammen mit der kanonischen Einbettung) der lokalkompakte Körper $\overline{\mathbb{Q}}_p$ der p-adischen Zahlen.*
Ganz analog gilt: Die formalen Potenzreihen $K[[x]]$ über einem endlichen Körper K bilden einen kompakten topologischen Ring, der sogar ein Integritätsbereich ist. Sein Quotientenkörper ist (zusammen mit der kanonischen Einbettung) der lokalkompakte Körper $K[[[x]]]$ der formalen Laurentreihen über K.

7.1.4 Pontrjaginsche Dualität

Als Motivation, Prüfergruppen und p-adische Zahlen unmittelbar hintereinander einzuführen, diente bisher eine gewisse Dualität zwischen injektiven Einbettungen und surjektiven Homomorphismen. Diese Dualität zwischen beiden Objekten lässt sich präzisieren und zeigt noch weitere reizvolle Aspekte. Betrachten wir dazu C_{p^∞} und $\overline{\mathbb{Z}}_p$ als abelsche Gruppen, die überdies mit Topologien ausgestattet sind, welche sie zu topologischen Gruppen machen. Bei C_{p^∞} ist das die diskrete Topologie, bei $\overline{\mathbb{Z}}_p$ die kompakte Topologie aus Übungsaufgabe 7.1.3.1. Insbesondere handelt es sich in beiden Fällen um lokalkompakte abelsche Gruppen, die sich als dual zueinander im Rahmen der Pontrjaginschen Dualitätstheorie erweisen. Weitgehend ohne Beweise soll nun erklärt werden, was dies bedeutet. Man beachte dabei die Analogie zu (stetigen) linearen Funktionalen auf (topologischen) Vektorräumen, auf die wir uns als Vergleich beziehen wollen.
In der Pontrjaginschen Dualität tritt an die Stelle des Skalarkörpers (des Wertebereichs der Funktionale) die kompakte Gruppe $\mathbb{T} = \mathbb{R}/\mathbb{Z}$. Die Topologie auf $\mathbb{T}$ ist die Quotiententopologie, in der genau jene Teilmengen O offen sind, deren Urbilder $\kappa^{-1}(O)$ unter der kanonischen Abbildung $\kappa\colon \mathbb{R} \to \mathbb{T}$, $r \mapsto r + \mathbb{Z}$, offen in $\mathbb{R}$ sind.
Oft ist es praktisch, die Elemente von $\mathbb{T}$ als komplexe Zahlen vom Betrag 1 aufzufassen und die Operation als Multiplikation. Entsprechend wird in diesem Zusammenhang oft die multiplikative Schreibweise bevorzugt. Es gilt:

Proposition 7.1.4.1. *Bezeichne C die multiplikative Gruppe aller $z \in \mathbb{C}$ mit $|z| = 1$ mit der als Unterraum von $\mathbb{C}$ ererbten Topologie. Dann ist durch $\varphi : r + \mathbb{Z} \mapsto e^{2\pi i r} = \cos(2\pi r) + i \sin(2\pi r)$ eine Abbildung $\varphi\colon \mathbb{T} \to C$ definiert ist, die sowohl Gruppenisomorphismus als auch Homöomorphismus topologischer Räume ist. Insbesondere ist $\mathbb{T}$ eine kompakte topologische Gruppe.*

UE 10 ▶ Übungsaufgabe 7.1.4.2. (V) Beweisen Sie Proposition 7.1.4.1. **◀ UE 10**

Trotz der Beziehung zur Multiplikation komplexer Zahlen wollen wir hier an der additiven Schreibweise festhalten.

Jeder lokalkompakten abelschen Gruppe G wird ihr sogenanntes *Pontrjaginsches Dual* G^* zugeordnet, das sich ebenfalls als lokalkompakte abelsche Gruppe erweist. Die Trägermenge von G^* enthält als Elemente sämtliche sogenannte *Charaktere* χ von G, das sind definitionsgemäß die stetigen Homomorphismen $\chi\colon G \to \mathbb{T}$. Die Operation auf G^* ist punktweise definiert, d.h. durch $(\chi_1+\chi_2)(g) := \chi_1(g)+\chi_2(g)$, analog $(-\chi)(g) := -\chi(g)$. Nullelement ist der konstante Charakter χ_0 mit Wert 0. Auf G^* ist die *kompakt-offene Topologie* $\mathcal{T}$ definiert, genannt auch die *Topologie der gleichmäßigen Konvergenz auf kompakten Teilmengen*. Nach Proposition 7.1.1.4 genügt es eine Umgebungsbasis $\mathcal{U}$ von χ_0 mit den dort vorausgesetzten Eigenschaften anzugeben. Und zwar bestehe $\mathcal{U}$ aus allen Mengen $B(K,U)$, $K \subseteq G$ kompakt, U Umgebung von 0 in $\mathbb{T}$, wobei $B(K,U)$ genau jene $\chi \in G^*$ mit $\chi(K) \subseteq U$ enthalte. Leicht prüft man nach, dass alle Bedingungen an $\mathcal{U}$ aus Proposition 7.1.1.4 mit G^* an der Stelle von G erfüllt sind.

UE 11 ► **Übungsaufgabe 7.1.4.3.** (V) Prüfen Sie diese Bedingungen aus Proposition 7.1.1.4 nach. ◄ **UE 11**

Also macht die dort definierte Topologie $\mathcal{T}$ die Gruppe G^* zu einer topologischen Gruppe, eben das *Pontrjaginsche Dual* von G. Tatsächlich gilt noch mehr:

Satz 7.1.4.4. *Ist G eine lokalkompakte abelsche Gruppe, so auch das Dual G^* von G.*

Der Beweis dieses Satzes ist anspruchsvoll und würde den Rahmen sprengen, und wir verzichten auf den Beweis bzw. lagern ihn in die folgende Übungsaufgabe für Ambitionierte aus.

UE 12 ► **Übungsaufgabe 7.1.4.5.** (E) Beweisen Sie Satz 7.1.4.4. (Achtung, anspruchsvoll!) ◄ **UE 12**

Viel einfacher sind die Beobachtungen der nächsten Übungsaufgabe.

UE 13 ► **Übungsaufgabe 7.1.4.6.** (F) Zeigen Sie für eine lokalkompakte Gruppe G und die kompakt-offene Topologie $\mathcal{T}$ auf dem Dual G^*: ◄ **UE 13**

1. Konvergenz von Charakteren (genauer: eines Netzes von Charakteren) in G^* bezüglich $\mathcal{T}$ ist äquivalent zu gleichmäßiger Konvergenz auf jeder kompakten Teilmenge von G.
2. Ist G kompakt, so beschreibt $\mathcal{T}$ die gleichmäßige Konvergenz auf G und ist diskret.
3. Ist G diskret, so beschreibt $\mathcal{T}$ die punktweise Konvergenz und ist kompakt.

Aus Satz 7.1.4.4 folgt, dass der Prozess des Dualisierens für jede lokalkompakte abelsche Gruppe G iteriert werden kann. Insbesondere besitzt jede lokalkompakte Gruppe G ein

sogenanntes *Bidual* $G^{**} := (G^*)^*$. Bevor wir dieses näher in Augenschein nehmen, interessieren wir uns in der nächsten Übungsaufgabe für die Duale von besonders einfachen und wichtigen Beispielen lokalkompakter abelscher Gruppen:

UE 14 ► **Übungsaufgabe 7.1.4.7.** (F,W) Zeigen Sie folgende Strukturaussagen über Pontrjagin- **◄ UE 14**
insche Duale. Isomorphien $\cong$ sind durchwegs sowohl algebraisch als auch topologisch zu verstehen. Beschreiben Sie auch den Isomorphismus.

1. $(\prod_{i\in I} G_i)^* \cong \bigoplus_{i\in I} G_i^*$ für kompakte abelsche Gruppen G_i.
2. $(\bigoplus_{i\in I} G_i)^* \cong \prod_{i\in I} G_i^*$ für diskrete abelsche Gruppen G_i.
3. $G^* \cong G$ für jede (diskrete) endliche abelsche Gruppe G. (Sie dürfen den Hauptsatz über endlich erzeugte abelsche Gruppen 3.3.4.2 verwenden. Er besagt insbesondere, dass jede endliche abelsche Gruppe eine direkte Summe (äquivalent: direktes Produkt) zyklischer Gruppen ist.)
4. $\mathbb{Z}^* \cong \mathbb{T}$.
5. $\mathbb{T}^* \cong \mathbb{Z}$.
6. $\mathbb{R}^* \cong \mathbb{R}$.
7. $C_{p^\infty}^* \cong \overline{\mathbb{Z}}_p$.
8. $\overline{\mathbb{Z}}_p^* \cong C_{p^\infty}$.

Es fällt auf, dass in allen behandelten Fällen $G \cong G^{**}$ gilt. Der verantwortliche Isomorphismus erweist sich stets als natürlich in einer Weise, die an den letzten Absatz in Abschnitt 2.3.4 erinnert. Es handelt sich nämlich um jene Abbildung $G \to G^{**}$, die jedem Element $g \in G$ die Auswertungsabbildung $\chi \mapsto \chi(g)$ zuordnet, welche ja tatsächlich ein Homomorphismus von G^* nach $\mathbb{T}$ ist, der sich auch als stetig (bezüglich der kompakt-offenen Topologie auf G^* und der natürlichen Topologie auf $\mathbb{T}$) erweist. Der tiefliegende Dualitätssatz von Pontrjagin besagt, dass dies nicht nur für die behandelten Beispiele gilt, sondern für jede lokalkompakte Gruppe.

Satz 7.1.4.8. (Dualitätssatz von Pontrjagin) *Ist G eine lokalkompakte abelsche Gruppe mit Dual G^* und Bidual G^{**}, dann ist die kanonische Abbildung*

$$\Phi\colon G \to G^{**}, \quad g \mapsto g^{**},$$

mit

$$g^{**}\colon G^* \to \mathbb{T}, \quad \chi \mapsto \chi(g),$$

ein sowohl algebraischer als auch topologischer Isomorphismus zwischen G und G^{**}.

Lokalkompakte Gruppen besitzen also die analoge Eigenschaft zu reflexiven (topologischen) Vektorräumen.

7.1.5 Der kategorientheoretische Aspekt

Wir kennen aus 2.2.4 bereits das Konzept des direkten Limes einer Folge von Algebren $\mathfrak{A}_n$, $n \in \mathbb{N}$, zusammen mit Homomorphismen $\iota_n : \mathfrak{A}_n \to \mathfrak{A}_{n+1}$. In diesem Unterabschnitt wollen wir diese Definition einerseits verallgemeinern, um auch die universelle Eigenschaft der universellen Prüfergruppe C_∞ aus Proposition 7.1.2.1 abzudecken, und andererseits eine „duale“ Definition finden, die die ganzen p-adischen Zahlen einfängt.
Im Falle der zyklischen Gruppen C_k existieren Einbettungen nur für gewisse Paare (k, ℓ), nämlich wenn k ein Teiler von ℓ ist. Diese Situation verallgemeinernd fassen wir die folgende Definition.

Definition 7.1.5.1. Unter einer *gerichteten Menge* versteht man eine Halbordnung $(N, \leq)$, in der es zu je zwei Elementen $\nu_1, \nu_2 \in N$ stets ein $\nu \in N$ gibt mit $\nu_1 \leq \nu$ und $\nu_2 \leq \nu$.

Gerichtete Mengen fungieren in der Topologie als Indexmengen für sogenannte Netze, die den Begriff der Folge dahingehend verallgemeinern, dass an die Stelle des Spezialfalles $(\mathbb{N}, \leq)$ eine beliebige gerichtete Menge $(N, \leq)$ tritt. So wie in metrischen Räumen die Topologie vollständig durch sämtliche konvergente Folgen samt ihrer Grenzwerte eindeutig bestimmt ist, kann mit Hilfe der Konvergenz von Netzen die Topologie auch von nicht metrisierbaren topologischen Räumen eingefangen werden. Das spielt für uns im Folgenden allerdings kaum eine Rolle. Wir verwenden gerichtete Mengen lediglich zur Definition von injektiven und projektiven Systemen sowie Limiten.

Definition 7.1.5.2. Sei $\mathcal{C}$ eine Kategorie und $(N, \leq)$ ein gerichtete Menge. Gegeben seien für jedes $\nu \in N$ ein Objekt A_ν in $\mathcal{C}$ und, für alle $\nu_1 \leq \nu_2 \in N$, Morphismen $\varphi_{\nu_1,\nu_2} \colon A_{\nu_1} \to A_{\nu_2}$ mit der Eigenschaft, dass für alle $\nu_1 \leq \nu_2 \leq \nu_3 \in N$ die Beziehung $\varphi_{\nu_2,\nu_3} \circ \varphi_{\nu_1,\nu_2} = \varphi_{\nu_1,\nu_3}$ gilt. Weiters verlangen wir $\varphi_{\nu,\nu} = \mathrm{id}_{A_\nu}$ für alle ν. Dann nennt man die A_ν zusammen mit den φ_{ν_1,ν_2} ein *injektives System* in $\mathcal{C}$.

Bilden die A_ν zusammen mit den φ_{ν_1,ν_2} ein injektives System in der Kategorie $\mathcal{C}$, so können wir die folgende Kategorie $\mathcal{C}^+$ betrachten. Ihre Objekte seien Tupel $(A, (\psi_\nu)_{\nu\in N})$ mit Objekten A und Morphismen $\psi_\nu \colon A_\nu \to A$ aus $\mathcal{C}$ derart, dass für alle $\nu_1 \leq \nu_2$ die Beziehung $\psi_{\nu_1} = \psi_{\nu_2} \circ \varphi_{\nu_1,\nu_2}$ gilt. Die Morphismen von $(A, (\psi_\nu)_{\nu\in N})$ nach $(A', (\psi'_\nu)_{\nu\in N})$ in $\mathcal{C}^+$ seien jene Morphismen $f \colon A \to A'$ in $\mathcal{C}$, die für alle $\nu \in N$ die Beziehung $\psi'_\nu = f \circ \psi_\nu$ erfüllen. Die Komposition von Morphismen in $\mathcal{C}^+$ ist die aus $\mathcal{C}$. Mit diesen Notationen lautet die Definition eines direkten Limes nun wie folgt.

Definition 7.1.5.3. Jedes initiale Objekt in der Kategorie $\mathcal{C}^+$ heißt *direkter* oder *injektiver Limes* (manchmal auch *Kolimes*) des vorgegebenen injektiven Systems. Für so ein initiales Objekt schreibt man (etwas ungenau, weil die Abhängigkeit vom injektiven System dabei nur sehr unvollständig zum Ausdruck kommt) auch $\lim_{\to} A_\nu$.

Als universelles Objekt in der Kategorie $\mathcal{C}^+$ ist ein direkter Limes bis auf Äquivalenz eindeutig bestimmt (siehe Satz 2.3.3.2), also – wie man sich sofort klar macht – auch in der ursprünglich vorgegebenen Kategorie $\mathcal{C}$.
Formulieren wir Proposition 7.1.2.1 um, so erhalten wir:

Proposition 7.1.5.4. *Die universelle Prüfergruppe C_∞ ist ein direkter Limes des folgenden injektiven Systems: Die gerichtete Menge sei $(\mathbb{N}\setminus\{0\},|)$, für $k\in\mathbb{N}\setminus\{0\}$ sei das Objekt A_k gegeben durch C_k und für $k|\ell$ sei der Homomorphismus $\varphi_{k,\ell}$ gegeben durch die Inklusionsabbildung $\iota_{k,\ell}: C_k\to C_\ell$.*

Wie in der spezielleren Situation aus Unterabschnitt 2.2.4, siehe insbesondere Satz 2.2.4.6, existiert auch im allgemeinen Fall in Varietäten der direkte Limes eines injektiven Systems:

UE 15 ► **Übungsaufgabe 7.1.5.5.** (W) Sei $\mathcal{V}$ eine Varietät, sei $(N,\leq)$ eine gerichtete Menge und sei $((\mathfrak{A}_\nu)_{\nu\in N},(\varphi_{\nu_1,\nu_2})_{\nu_1\leq\nu_2})$ ein injektives System in $\mathcal{V}$. Dann existiert in $\mathcal{V}$ ein direkter Limes des injektiven Systems. ◄ **UE 15**

Auch im Fall der p-adischen Zahlen $\overline{\mathbb{Z}}_p$ ist die Situation ähnlich, nur dass sich die Richtungen der Morphismen umdrehen und Epimorphismen an die Stelle der Monomorphismen treten. Fasst man den Begriff entsprechend allgemein, gelangt man zunächst zum Begriff eines projektiven Systems und anschließend zu einem zum direkten Limes dualen Begriff, dem des indirekten oder projektiven Limes.

Definition 7.1.5.6. Sei $\mathcal{C}$ eine Kategorie und $(N,\leq)$ ein gerichtete Menge. Gegeben seien für jedes $\nu\in N$ ein Objekt A_ν in $\mathcal{C}$ und, für alle $\nu_1\leq\nu_2\in N$, Morphismen $\varphi_{\nu_1,\nu_2}\colon A_{\nu_2}\to A_{\nu_1}$ mit der Eigenschaft, dass für alle $\nu_1\leq\nu_2\leq\nu_3\in N$ die Beziehung $\varphi_{\nu_1,\nu_2}\circ\varphi_{\nu_2,\nu_3}=\varphi_{\nu_1,\nu_3}$ gilt. Weiters verlangen wir $\varphi_{\nu,\nu}=\mathrm{id}_{A_\nu}$ für alle ν. Dann nennt man die A_ν zusammen mit den φ_{ν_1,ν_2} ein *projektives System* in $\mathcal{C}$.

Bilden die A_ν zusammen mit den φ_{ν_1,ν_2} ein projektives System in der Kategorie $\mathcal{C}$, so können wir die folgende Kategorie $\mathcal{C}_+$ betrachten. Ihre Objekte seien Tupel $(A,(\psi_\nu)_{\nu\in N})$ mit Objekten A und Morphismen $\psi_\nu\colon A\to A_\nu$ aus $\mathcal{C}$ derart, dass für alle $\nu_1\leq\nu_2$ die Beziehung $\psi_{\nu_1}=\varphi_{\nu_1,\nu_2}\circ\psi_{\nu_2}$ gilt. Die Morphismen von $(A,(\psi_\nu)_{\nu\in N})$ nach $(A',(\psi'_\nu)_{\nu\in N})$ in $\mathcal{C}_+$ seien jene Morphismen $f\colon A\to A'$ in $\mathcal{C}$, die für alle $\nu\in N$ die Beziehung $\psi'_\nu\circ f=\psi_\nu$ erfüllen. Die Komposition von Morphismen in $\mathcal{C}_+$ ist die aus $\mathcal{C}$. Mit diesen Notationen lautet die Definition eines projektiven Limes nun wie folgt.

Definition 7.1.5.7. Jedes terminale Objekt in der Kategorie $\mathcal{C}_+$ heißt *indirekter* oder *projektiver Limes* des vorgegebenen injektiven Systems. Für so ein terminales Objekt schreibt man (etwas ungenau, weil die Abhängigkeit vom projektiven System dabei nur sehr unvollständig zum Ausdruck kommt) auch $\lim_{\leftarrow} A_\nu$.

UE 16 ► **Übungsaufgabe 7.1.5.8.** (B) Zeigen Sie, dass die p-adischen Zahlen $\overline{\mathbb{Z}}_p$ als projektiver Limes aufgefasst werden können. ◄ **UE 16**

UE 17 ► **Übungsaufgabe 7.1.5.9.** (W) Sei $\mathcal{V}$ eine Varietät, sei $(N,\leq)$ eine gerichtete Menge und sei $((\mathfrak{A}_\nu)_{\nu\in N},(\varphi_{\nu_1,\nu_2})_{\nu_1\leq\nu_2})$ ein projektives System in $\mathcal{V}$. Dann existiert in $\mathcal{V}$ ein projektives Limes des projektiven Systems. ◄ **UE 17**

7.2 Grundbegriffe der Strukturtheorie der Moduln

Der Begriff der Dimension eines Vektorraums baut auf dem der Basis auf. Die dazu erforderlichen Begriffe *Erzeugnis* und *lineare (Un-)Abhängigkeit* lassen sich zwar problemlos auf Moduln übertragen. Im Gegensatz zu Vektorräumen hat aber nicht jeder Modul eine Basis, d.h. nicht alle Moduln sind frei. Zunächst haben wir uns mit den daraus resultierenden Komplikationen zu beschäftigen (7.2.1). Beschränkt man den Dimensionsbegriff auf freie Moduln, so nennt man Ringe, über denen je zwei Basen ein und desselben Moduls gleiche Kardinalität haben, dimensionsinvariant. Viele Ringe haben diese Eigenschaft, z.B. Divisionsringe und auch kommutative Ringe mit 1 (7.2.2). Für das Studium von Modulhomomorphismen und somit für die allgemeine Strukturtheorie von Moduln erweisen sich schließlich sogenannte exakte Sequenzen als sehr nützlich (7.2.3). Wenn es nicht ausdrücklich anders vermerkt ist, betrachten wir nur unitäre Moduln über einem Ring mit 1.

7.2.1 Freie Moduln, Basen und Dimension

Auf sehr einfache Weise lassen sich die Komplikationen, mit denen wir uns in der Theorie der Moduln oder auch abelschen Gruppen herumschlagen müssen, folgendermaßen illustrieren:
Ist K ein Körper, so hat jeder eindimensionale, d.h. von einem Element $\neq 0$ erzeugte, Vektorraum dieselbe Struktur, nämlich die von K, aufgefasst als Vektorraum über sich selbst. Nehmen wir statt K den Ring $\mathbb{Z}$ und die abelschen Gruppen als unitäre $\mathbb{Z}$-Moduln, so gilt dies nicht mehr. Denn es gibt unendlich viele von einem Element $\neq 0$ erzeugte abelsche Gruppen, nämlich neben $\mathbb{Z}$ selbst für jedes $n \geq 2$ die zyklische Gruppe C_n. Wir definieren etwas allgemeiner:

Definition 7.2.1.1. Ein R-Modul A heißt *zyklisch*, wenn er von einem Element erzeugt wird.

Ist der Ring R mit dem Einselement 1_R vorgegeben, so überblickt man die Struktur der zyklischen R-Moduln recht schnell. Denn wann immer $a \in A$ ein erzeugendes Element eines zyklischen R-Moduls A ist, gilt $A = Ra = \{ra \mid r \in R\}$. Folglich ist der R-Modul-Homomorphismus $f\colon R \to A$, $r \mapsto ra$, surjektiv, nach dem Homomorphiesatz daher $A \cong R/\ker f$. In dieser Faktorisierung ist $\ker f$ ein R-Untermodul des (selbst zyklischen, weil von 1_R erzeugten) R-Moduls R. Die R-Untermoduln von R sind genau die Linksideale von R. Also:

Proposition 7.2.1.2. *Die unitären zyklischen R-Moduln sind bis auf Isomorphie gegeben durch sämtliche Faktor-R-Moduln R/I nach Linksidealen I von R.*

Wir wollen uns nicht auf zyklische Moduln beschränken. Deshalb definieren wir in völliger Analogie zur Theorie der Vektorräume:

Definition 7.2.1.3. Sei I eine Menge, A ein (unitärer) R-Modul und $(a_i)_{i\in I} \in A^I$ eine mit I indizierte Familie von Elementen $a_i \in A$.

Die Familie $(a_i)_{i\in I} \in A^I$ heißt *linear abhängig*, wenn es paarweise verschiedene Indizes $i_1, \ldots, i_n \in I$ mit $n \geq 1$ und Elemente $r_1, \ldots, r_n \neq 0$ aus R gibt, sodass $\sum_{k=1}^{n} r_k a_{i_k} = 0$ gilt. Ist die Familie $(a_i)_{i\in I} \in A^I$ nicht linear abhängig, so nennt man sie, ebenso wie die Menge $\{a_i : i \in I\}$, *linear unabhängig*.
Die Familie $(a_i)_{i\in I} \in A^I$ heißt eine *Basis* von A, wenn sie linear unabhängig ist und $\{a_i : i \in I\}$ ein Erzeugendensystem von A ist, d.h. wenn es zu jedem $a \in A$ endlich viele Indizes $i_1, \ldots, i_n \in I$ und Elemente $r_1, \ldots, r_n \in R$ gibt mit $a = \sum_{k=1}^{n} r_k a_{i_k}$. Ist die Familie $(a_i)_{i\in I} \in A^I$ eine Basis von A, so nennt man auch die Menge $\{a_i : i \in I\}$ eine Basis von A.

In dieser Definition fällt auf, dass wir lineare Abhängigkeit nur für Familien definiert haben, lineare Unabhängigkeit hingegen auch für Mengen. Den Grund erkennt man aus folgenden Beobachtungen: Ist $(a_i)_{i\in I} \in A^I$ eine Basis von A, so gilt $a_{i_1} \neq a_{i_2}$ für alle $i_1 \neq i_2 \in I$, weil sonst $1a_{i_1} - 1a_{i_2} = 0$ eine nichttriviale Darstellung der 0 wäre. Folglich ist die Zuordnung $f\colon i \mapsto a_i$ bijektiv zwischen der Indexmenge I und $\{a_i : i \in I\}$. Es ist offensichtlich, dass die lineare Abhängigkeit bzw. Unabhängigkeit von $(a_i)_{i\in I} \in A^I$ weder von I noch von der speziellen Bijektion f abhängt. Das bedeutet umgekehrt: Ist irgendeine Teilmenge $B \subseteq A$ gegeben, so liefern alle bijektiven Indizierungen von B hinsichtlich linear abhängig/unabhängig denselben Befund. Lassen wir hingegen auch nicht bijektive Indizierungen zu, so können manche davon linear abhängige Familien definieren, obwohl B als Menge linear unabhängig ist. Einfachstes Beispiel: Für $a = a_1 = a_2$ und $I = \{1, 2\}$ ist die Familie $(a_i)_{i\in I}$ linear abhängig im Sinne von Definition 7.2.1.3, während die Menge $\{a_1, a_2\} = \{a, a\} = \{a\}$ als Singleton linear unabhängig sein kann (und sicher auch ist, sofern $a \neq 0$ und A ein Vektorraum ist). Doch nun zurück zu unserem Hauptthema.
Weil die unitären Moduln über einem Ring R mit 1 eine Varietät bilden, gibt es nach Satz 4.1.3.1 auch über jeder Menge X einen freien R-Modul. Seine Struktur wird durch folgenden Satz beschrieben:

Satz 7.2.1.4. *Für einen unitären R-(Links-)Modul F sind die folgenden Aussagen äquivalent:*

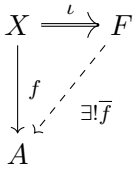
(i) *F hat eine Basis.*

(ii) *F ist die innere direkte Summe einer Familie zyklischer (d.h. von jeweils einem Element erzeugter) R-Moduln, wobei jeder davon als Links-Modul isomorph zu R ist, genauer: $F = \bigoplus_{i\in I} Ra_i$ und $R \cong Ra_i$ via $r \mapsto ra_i$.*

(iii) *F ist als R-Modul isomorph zu einer direkten Summe von Kopien von R.*

(iv) *Es existiert eine Menge X und eine Funktion $\iota\colon X \to F$ mit der folgenden Eigenschaft:*

Sind ein beliebiger unitärer R-Modul A und eine Funktion $f\colon X \to A$ gegeben, dann gibt es einen eindeutigen R-Modul-Homomorphismus $\overline{f}\colon F \to A$ mit $\overline{f}\iota = f$.



Mit anderen Worten: F ist zusammen mit ι ein freies Objekt in der konkreten Kategorie der unitären R-Moduln.

UE 18 ► Übungsaufgabe 7.2.1.5. (V) Zeigen Sie Satz 7.2.1.4. **◄ UE 18**

Aus Satz 7.2.1.4 kann man direkt, d.h. auch ohne den entsprechenden allgemeinen Satz 4.1.3.2 für Varietäten, folgern:

Folgerung 7.2.1.6. *Jeder unitäre Modul A über einem Ring R ist homomorphes Bild eines freien R-Moduls F. Hat A ein Erzeugendensystem X, so kann F als frei über X gewählt werden.*

Beweis. Sei F der freie Modul über X, wobei wir nach Satz 7.2.1.4 als $F = \bigoplus_{x\in X} R$ annehmen können. Definiert man $f\colon F \to A$, $(r_x)_{x\in X} \mapsto \sum_{x\in X} r_x x$, so sieht man unmittelbar, dass f ein wohldefinierter, surjektiver Homomorphismus ist. □

Weil jeder Vektorraum nach Satz 1.3.1.3 eine Basis hat, sehen wir auch:

Folgerung 7.2.1.7. *Jeder Vektorraum über einem Schiefkörper ist frei, und zwar über jeder beliebigen Basis.*

7.2.2 Dimensionsinvarianz

Definition 7.2.2.1. Sei R ein Ring mit 1 und F ein freier unitärer R-Modul. Wenn je zwei Basen X_1, X_2 von F gleichmächtig sind, dann heißt $\kappa := |X_1| = |X_2|$ die *Dimension* oder der *Rang* von F über R. Wenn sogar jeder freie unitäre R-Modul F eine Dimension hat, dann heißt R *dimensionsinvariant*.

Um den Fall unendlicher Dimension untersuchen zu können, werden wir folgende Tatsachen über unendliche Kardinalitäten brauchen.

Proposition 7.2.2.2. *Für die Kardinalitäten von Mengen A, B gelten folgende Beziehungen:*

1. *(Satz von Cantor-Schröder-Bernstein) Aus $|A| \leq |B|$ und $|B| \leq |A|$ folgt $|A| = |B|$.*
2. *Ist A unendlich, $B \neq \emptyset$ und $|B| \leq |A|$ (d.h. es gibt ein injektives $f\colon B \to A$), so gilt $|A \times B| = |A|$ (d.h. es gibt ein bijektives $f\colon A \times B \to A$). Insbesondere gilt das für abzählbares B.*

3. *Ist A eine unendliche Menge und $\mathfrak{P}_{\text{fin}}(A)$ die Menge aller endlichen Teilmengen von A, dann ist $|\mathfrak{P}_{\text{fin}}(A)| = |A|$.*

UE 19 ► **Übungsaufgabe 7.2.2.3.** (V) Beweisen Sie Proposition 7.2.2.2. Hinweis: Anhang, Unterabschnitte A.5.2 und A.5.6. ◄ **UE 19**

Die wichtigsten Resultate im Zusammenhang mit Dimensionsinvarianz sind in folgendem Satz zusammengefasst:

Satz 7.2.2.4.

1. *Sei R ein Ring mit 1 und F ein freier R-Modul mit einer unendlichen Basis. Dann haben je zwei Basen von F dieselbe Kardinalität. (Man beachte, dass die Kardinalität einer Basis $(b_i)_{i\in I}$ gleich der Kardinalität der Indexmenge I ist.)*
2. *Divisionsringe (also insbesondere Körper) sind dimensionsinvariant.*
3. *Seien R, S Ringe mit 1 und $f\colon R \to S$ ein Epimorphismus. Ist S dimensionsinvariant, so auch R.*
4. *Jeder kommutative Ring mit $1 \neq 0$ ist dimensionsinvariant.*

Beweis.

1. Sei X eine unendliche Basis und Y eine weitere Basis von F. Wir zeigen zuerst, dass Y unendlich ist, indem wir indirekt annehmen, $Y = \{y_1, \ldots, y_n\}$ wäre endlich. Jedes y_i lässt sich darstellen als Linearkombination von Elementen aus X:

$$y_i = \sum_{k=1}^{n_i} r_{i,k} x_{i,k}$$

Das würde aber bedeuten, dass die endlich vielen $x_{i,k}$ ($i = 1, \ldots, n$ und $k = 1, \ldots, n_i$) schon F erzeugen, Widerspruch. Also muss Y unendlich sein.

Wir definieren nun eine Funktion $f\colon X \to \mathfrak{P}_{\text{fin}}(Y)$ von X in die Menge $\mathfrak{P}_{\text{fin}}(Y)$ aller endlichen Teilmengen von Y durch $f(x) := \{y_1, \ldots, y_n\}$, wobei $x = \sum_{i=1}^{n} r_i y_i$ mit $r_i \neq 0$ und paarweise verschiedenen $y_i \in Y$. Ganz symmetrisch sei die Funktion $g : Y \to \mathfrak{P}_{\text{fin}}(X)$ definiert, indem $g(y) = \{x_1, \ldots, x_m\}$, sofern $y = \sum_{j=1}^{m} s_j x_j$ mit $s_j \neq 0$ und paarweise verschiedenen $x_j \in X$.

Das Bild $\operatorname{Im} f$ von f ist unendlich. Andernfalls erzeugte die endliche Menge $\bigcup \operatorname{Im} f = \bigcup_{x\in X} f(x)$ ganz F, Widerspruch.

Als nächstes wollen wir zeigen, dass auch $f^{-1}(T)$ endlich ist für alle $T \in \operatorname{Im} f$. Dazu definieren wir für ein beliebiges $T \in \operatorname{Im} f$ die endliche Menge

$$S_T := \bigcup_{y\in T} g(y) \subseteq X.$$

Weil jedes $y \in T$ in der linearen Hülle von $g(y) \subseteq S_T$ liegt, gilt $\langle T \rangle \subseteq \langle S_T \rangle$. Damit zeigen wir nun $f^{-1}(T) \subseteq S_T$: Aus $x \in f^{-1}(T)$ folgt $x \in \langle T \rangle \subseteq \langle S_T \rangle$. Weil X als Basis linear unabhängig ist, ist das nur für $x \in S_T$ möglich. Damit ist $f^{-1}(T)$ enthalten in der endlichen Menge S_T und daher selbst endlich.

Für jedes $T \in \operatorname{Im} f$ sei $f^{-1}(T) = \{x_{T,1}, x_{T,2}, \ldots, x_{T,n}\}$ mit paarweise verschiedenen $x_{T,i}$. Wir definieren eine injektive Funktion $\varphi_T \colon f^{-1}(T) \to \operatorname{Im} f \times \mathbb{N}$ durch

$$\varphi_T : x_{T,k} \mapsto (T, k).$$

Da die Mengen $f^{-1}(T)$, $T \in \operatorname{Im} f$, eine Partition von X bilden, ist die Funktion

$$\varphi := \left(\bigcup_{T \in \operatorname{Im} f} \varphi_T \right) : X \to \operatorname{Im} f \times \mathbb{N}$$

wohldefiniert und injektiv. Folglich gilt (siehe Proposition 7.2.2.2)

$$|X| \leq |\operatorname{Im} f \times \mathbb{N}| = |\operatorname{Im} f| \cdot \aleph_0 = |\operatorname{Im} f| \leq |\mathfrak{P}_{\text{fin}}(Y)| = |Y|.$$

Analog zeigt man $|Y| \leq |X|$, woraus (wieder nach Proposition 7.2.2.2, Satz von Schröder-Bernstein) $|X| = |Y|$ folgt.

2. Siehe Lineare Algebra (Austauschsatz von Steinitz) im Fall einer endlichen Basis, andernfalls Aussage 1.

3. Beweisskizze (genaue Ausarbeitung Übung): Es genügt Folgendes zu zeigen: Sei R ein Ring und $I \lhd R$ ein echtes Ideal von R, F ein freier R-Modul mit Basis X. Dann ist $IF \leq F$. Sei weiters $\pi \colon F \to F/IF$ der kanonische Epimorphismus von F nach F/IF. Dann ist F/IF ein freier R/I-Modul mit Basis $\pi(X)$ und $|\pi(X)| = |X|$.

4. Sei M ein maximales Ideal von R. (Ein solches existiert in jedem kommutativen Ring mit $1 \neq 0$ nach Satz 3.4.2.4). Es existiert ein Epimorphismus von R auf den Körper R/M (nochmals Satz 3.4.2.4), nämlich die kanonische Abbildung. Nach den Aussagen 2 und 3 ist damit auch R dimensionsinvariant. □

UE 20 ► **Übungsaufgabe 7.2.2.5.** (V) Arbeiten Sie die Beweisskizze für Aussage (3) in Satz 7.2.2.4 im Detail aus. ◄ **UE 20**

7.2.3 Exakte Sequenzen

Weiterhin betrachten wir, wenn nicht ausdrücklich anders vermerkt, nur unitäre R-Moduln über einem Ring R mit Einselement. Wir werden nun exzessiv von (kommutativen) Diagrammen in der Kategorie der (Links- oder Rechts-) Moduln über einem Ring R Gebrauch machen. Eine besondere Rolle spielen Sequenzen, nämlich Diagramme von der Form

$$\ldots \xrightarrow{f_{i-2}} A_{i-1} \xrightarrow{f_{i-1}} A_i \xrightarrow{f_i} A_{i+1} \xrightarrow{f_{i+1}} \ldots,$$

wobei die Folgen der R-Moduln A_i und Morphismen f_i nach links und rechts endlich oder unendlich sein dürfen. Man beachte, dass Diagramme dieser Art immer auf eindeutige Weise zu kommutativen ergänzt werden können. Diese Ergänzungen wollen wir bei Bedarf stillschweigend verwenden, sodass wir es also tatsächlich mit kommutativen Diagrammen im Sinne von Unterabschnitt 2.3.5 zu tun haben.
Der folgende Begriff lässt sich nicht in beliebigen Kategorien definieren, erweist sich im Fall der Moduln aber als äußerst fruchtbar.

Definition 7.2.3.1. Ein Paar von Modul-Homomorphismen $A \xrightarrow{f} B \xrightarrow{g} C$ heißt *exakt*, sofern $\operatorname{Im} f = \ker g$. Eine Folge von Modul-Homomorphismen

$$\ldots \xrightarrow{f_{i-2}} A_{i-1} \xrightarrow{f_{i-1}} A_i \xrightarrow{f_i} A_{i+1} \xrightarrow{f_{i+1}} \ldots$$

heißt *exakt bei* A_i, falls $\operatorname{Im} f_{i-1} = \ker f_i$, und *(schlechthin) exakt*, wenn dies für alle i, für die diese Beziehung definiert ist, gilt.
Exakte Sequenzen der Form $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ heißen *kurzexakt.* (Hierin sowie an entsprechenden Stellen in der Folge steht 0 für einen einelementigen Modul.) Explizit bedeutet das: f ist injektiv, g ist surjektiv, und es gilt $\operatorname{Im} f = \ker g$.

Beispiel 7.2.3.2.

(a) Jeder R-Modulhomomorphismus $f : A \to B$ induziert eine kurzexakte Sequenz, nämlich

$$0 \to \ker f \xrightarrow{\iota} A \xrightarrow{f} \operatorname{Im} f \to 0$$

mit der Einbettung ι.

(b) Sei $U \leq A$ ein Untermodul von A. Dann ist

$$0 \to U \xrightarrow{\iota} A \xrightarrow{\kappa} A/U \to 0$$

mit der Inklusionsabbildung ι und dem kanonischen Epimorphismus $\kappa : a \mapsto a + U$ kurzexakt.

(c) Von besonderem Interesse für das Weitere (siehe Satz 7.2.3.8) ist die folgende Situation. Seien A, B Moduln über R. Dann ist

$$0 \to A \xrightarrow{\iota_1} A \oplus B \xrightarrow{\pi_2} B \to 0$$

mit $\iota_1 : a \mapsto (a, 0)$ und $\pi_2 : (a, b) \mapsto b$ kurzexakt.

Wie in Unterabschnitt 2.3.5 beschrieben, fassen wir Sequenzen einer gegebenen Länge selbst wieder als Objekte einer Kategorie auf. Für uns ist der zugehörige Äquivalenzbegriff von besonderem Interesse. Ohne den kategorientheoretischen Hintergrund aufzurollen (den interessierten Leser:innen sei allerdings sehr wohl ans Herz gelegt, diese Zusammenhänge zu rekapitulieren, siehe auch Übungsaufgabe 7.2.3.4), sei der für uns relevante Kontext durch die folgende Definition explizit hervorgehoben.

Definition 7.2.3.3. Zwei kurzexakte Sequenzen

$$S:\ 0 \to A \to B \to C \to 0$$

und

$$S':\ 0 \to A' \to B' \to C' \to 0$$

heißen *isomorph*, falls es Modulisomorphismen $\alpha : A \to A', \beta : B \to B', \gamma : C \to C'$ gibt, sodass das Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

kommutativ ist.

UE 21 ► **Übungsaufgabe 7.2.3.4.** (A) Rekapitulieren Sie den kategorientheoretischen Rahmen, innerhalb dessen Definition 7.2.3.3 als Spezialfall des Begriffs der Äquivalenz in einer geeigneten Kategorie aufgefasst werden kann. ◄ **UE 21**

Die folgende Definition hat diese Situation in Verbindung mit Beispiel 7.2.3.2(c) im Visier.

Definition 7.2.3.5. S bezeichne die kurzexakte Sequenz

$$0 \to A_1 \xrightarrow{f} B \xrightarrow{g} A_2 \to 0.$$

Angenommen S kann zu einem kommutativen Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \xrightarrow{\iota_1} & A_1 \oplus A_2 & \xrightarrow{\pi_2} & A_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_{A_1}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}_{A_2}} & & \\ 0 & \longrightarrow & A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2 & \longrightarrow & 0 \end{array}$$

ergänzt werden, wobei id_{A_1} und id_{A_2} die identischen Abbildungen auf A_1 bzw. A_2 sind, $\iota_1 : a_1 \mapsto (a_1, 0)$ die Einbettung in die erste Komponente, $\pi_2 : (a_1, a_2) \mapsto a_2$ die Projektion auf die zweite Komponente und (das ist die interessanteste Bedingung) φ ein Isomorphismus ist. Dann sagt man, die Sequenz S *zerfällt* bzw. S ist eine *zerfallende Sequenz.*

An zerfallenden Sequenzen ist die Beobachtung von Interesse, dass im obigen Diagramm die Homomorphismen $\pi_1 \colon A_1 \oplus A_2 \to A_1$, $(a_1, a_2) \mapsto a_1$, mit $\pi_1\iota_1 = \mathrm{id}_{A_1}$ und $\iota_2 \colon A_2 \to A_1 \oplus A_2$, $a_2 \mapsto (0, a_2)$, mit $\pi_2\iota_2 = \mathrm{id}_{A_2}$ zusätzlich eingezeichnet werden können. Das wird etwas später in der Charakterisierung zerfallender Sequenzen zum Ausdruck kommen (7.2.3.8). Dabei treten zum Beispiel Diagramme wie im nachfolgenden Lemma 7.2.3.6 (oder genauer: wie im Spezialfall Folgerung 7.2.3.7) auf.

Lemma 7.2.3.6. *[Fünferlemma] Für $i = 1, 2, 3, 4, 5$ seien die R-Moduln A_i, B_i sowie die Homomorphismen $\alpha_i \colon A_i \to B_i$ gegeben. Im kommutativen Diagramm*

$$\begin{array}{ccccccccc} A_1 & \xrightarrow{f_1} & A_2 & \xrightarrow{f_2} & A_3 & \xrightarrow{f_3} & A_4 & \xrightarrow{f_4} & A_5 \\ \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} & & \downarrow{\scriptstyle \alpha_4} & & \downarrow{\scriptstyle \alpha_5} \\ B_1 & \xrightarrow{g_1} & B_2 & \xrightarrow{g_2} & B_3 & \xrightarrow{g_3} & B_4 & \xrightarrow{g_4} & B_5 \end{array}$$

mögen beide Zeilen exakte Sequenzen bilden. Dann gilt:

(a) Ist α_1 surjektiv, und sind α_2, α_4 injektiv, dann ist α_3 injektiv.

(b) Ist α_5 injektiv und sind α_2, α_4 surjektiv, dann ist α_3 surjektiv.

Beweis. Um Aussage (a) zu beweisen, setzen wir voraus, dass α_1 surjektiv ist, α_2 und α_4 injektiv und dass $\alpha_3(a_3) = 0$ gilt für ein $a_3 \in A_3$. Wir haben daraus $a_3 = 0$ zu folgern. Weil das Diagramm (drittes Quadrat) kommutiert, gilt $g_3\alpha_3 = \alpha_4 f_3$. Wegen $g_3\alpha_3(a_3) = 0$ bedeutet das $\alpha_4 f_3(a_3) = 0$, was wegen der Injektivität von α_4 nur für $f_3(a_3) = 0$ möglich ist. Folglich liegt a_3 im Kern von f_3, der wegen der Exaktheit der oberen Zeile bei A_3 mit dem Bild von f_2 übereinstimmt. Also gibt es ein $a_2 \in A_2$ mit $f_2(a_2) = a_3$. Es folgt mit der Kommutativität des Diagramms (zweites Quadrat) $g_2\alpha_2(a_2) = \alpha_3 f_2(a_2) = \alpha_3(a_3) = 0$. Also liegt $\alpha_2(a_2)$ im Kern von g_2, der wegen der Exaktheit der unteren Zeile bei B_2 mit dem Bild von g_1 übereinstimmt. Folglich gibt es ein $b_1 \in B_1$ mit $g_1(b_1) = \alpha(a_2)$ und somit, wegen der Surjektivität von α_1, ein $a_1 \in A_1$ mit (Kommutativität des ersten Quadrats) $\alpha_2 f_1(a_1) = g_1\alpha_1(a_1) = \alpha_2(a_2)$. Das wiederum zeigt, dass $f_1(a_1) - a_2$ im Kern von α_2 liegt. Weil α_2 injektiv ist, folgt daraus $f_1(a_1) = a_2$. Wir setzen das ein in $a_3 = f_2(a_2) = f_2 f_1(a_1)$. Wegen der Exaktheit der oberen Zeile bei A_2 ist $f_2 f_1$ aber die Nullabbildung. Somit ist $a_3 = 0$ bewiesen.
Für den Beweis von Aussage (b) seien α_2 und α_4 surjektiv, α_5 injektiv und $b_3 \in B_3$. Wir müssen ein $a_3 \in A_3$ finden mit $\alpha_3(a_3) = b_3$. Wegen der Surjektivität von α_4 gibt es ein $a_4 \in A_4$ mit $\alpha_4(a_4) = g_3(b_3)$. Die Exaktheit der unteren Zeile bei B_4 garantiert, dass das Bild $g_3(b_3)$ im Kern von g_4 liegt, also $0 = g_4 g_3(b_3) = g_4\alpha_4(a_4) = \alpha_5 f_4(a_4)$ (Kommutativität des vierten Quadrats). Weil α_5 injektiv ist, folgt daraus $f_4(a_4) = 0$. Somit liegt a_4 im Kern von f_4. Wegen der Exaktheit der oberen Zeile bei A_4 garantiert das die Existenz eines $a_3' \in A_3$ mit $f_3(a_3') = a_4$. Die Kommutativität des dritten Quadrats liefert $\alpha_4 f_3(a_3') = g_3\alpha_3(a_3')$. Wir würden gerne zeigen, dass die Differenz $d := b_3 - \alpha_3(a_3')$ gleich 0 ist, das gelingt aber nicht. Doch es gilt

$$g_3(d) = g_3(b_3) - g_3\alpha_3(a_3') = \alpha_4(a_4) - \alpha_4 f_3(a_3') = \alpha_4(a_4 - f_3(a_3')) = \alpha_4(0) = 0.$$

Folglich liegt d im Kern von g_3, der (Exaktheit der unteren Zeile) mit dem Bild von g_2 übereinstimmt. Beachten wir außerdem die Surjektivität von α_2, so gibt uns das ein $a_2 \in A_2$ in die Hand mit $d = g_2\alpha_2(a_2) = \alpha_3 f_2(a_2)$ (Kommutativität des zweiten Quadrats). Das Element $a_3 := a_3' + f_2(a_2)$ erfüllt nun tatsächlich $\alpha_3(a_3) = \alpha_3(a_3' + f_2(a_2)) = \alpha_3(a_3') + \alpha_3 f_2(a_2) = (b_3 - d) + d = b_3$. □

Etwas leichter einzuprägen und für unsere späteren Anwendungen völlig ausreichend ist der Spezialfall, dass A_1, A_5, B_1 und B_5 und folglich auch α_1 und α_5 trivial sind.

Folgerung 7.2.3.7 (Kurzes Fünferlemma)**.** *Sei R ein Ring und*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0 \end{array}$$

ein kommutatives Diagramm von R-Moduln und R-Modul-Homomorphismen, sodass beide Zeilen kurzexakte Sequenzen sind. Sind α, γ Mono-/ Epi-/ Isomorphismen, so ist auch β ein Mono-/ Epi-/ Isomorphismus.

Beweis. Unmittelbare Folgerung aus 7.2.3.6. □

Es folgt das für die weitere Strukturtheorie wichtigste Hilfsmittel im Zusammenhang mit kurzexakten Sequenzen.

Satz 7.2.3.8. *Für eine kurzexakte Sequenz S der Form $0 \to A_1 \xrightarrow{f} B \xrightarrow{g} A_2 \to 0$ sind äquivalent:*

(i) $\exists \sigma\colon A_2 \to B : g\sigma = \mathrm{id}_{A_2}$ *(Ein solches σ heißt Sektion.)*

$$0 \longrightarrow A_1 \xrightarrow{f} B \underset{\sigma}{\overset{g}{\rightleftarrows}} A_2 \longrightarrow 0$$

Achtung: Dieses Diagramm kommutiert im Allgemeinen nicht, da $\sigma g = \mathrm{id}_B$ nicht gelten muss!

(ii) $\exists \rho\colon B \to A_1 : \rho f = \mathrm{id}_{A_1}$ *(Ein solches ρ heißt Retraktion.)*

$$0 \longrightarrow A_1 \underset{\rho}{\overset{f}{\rightleftarrows}} B \xrightarrow{g} A_2 \longrightarrow 0$$

Achtung: Auch dieses Diagramm kommutiert im Allgemeinen nicht, da $f\rho = \mathrm{id}_B$ nicht gelten muss!

(iii) Die gegebene Sequenz S zerfällt. Insbesondere ist $B \cong A_1 \oplus A_2$.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \underset{\pi_1}{\overset{\iota_1}{\rightleftarrows}} & A_1 \oplus A_2 & \underset{\iota_2}{\overset{\pi_2}{\rightleftarrows}} & A_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_{A_1}} & & \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle \mathrm{id}_{A_2}} & & \\ 0 & \longrightarrow & A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2 & \longrightarrow & 0 \end{array}$$

Beweis. Wir zeigen die Implikationen (i)⇒(iii), (ii)⇒(iii) und (iii)⇒(i),(ii).
(i)⇒(iii): Wir definieren $\varphi\colon A_1 \oplus A_2 \to B$ durch $(a_1, a_2) \mapsto f(a_1) + \sigma(a_2)$. Klarerweise ist φ ein R-Modul-Homomorphismus. Wir zeigen nun, dass das Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \xrightarrow{\iota_1} & A_1 \oplus A_2 & \xrightarrow{\pi_2} & A_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_{A_1}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}_{A_2}} & & \\ 0 & \longrightarrow & A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2 & \longrightarrow & 0 \end{array}$$

kommutiert. Wegen

$$\varphi\iota_1(a_1) = f(a_1) + \sigma(0) = f(a_1)$$

für alle $a_1 \in A_1$ kommutiert das linke Quadrat im Diagramm. Wegen $\operatorname{Im} f = \ker g$ gilt weiters $gf = 0$ und somit $g\sigma = \mathrm{id}_{A_2}$. Folglich erhalten wir

$$g\varphi(a_1, a_2) = g(f(a_1) + \sigma(a_2)) = gf(a_1) + g\sigma(a_2) = 0 + a_2 = \pi_2(a_1, a_2)$$

für alle $(a_1, a_2) \in A_1 \oplus A_2$ und es kommutiert auch das rechte Quadrat. Nach dem kurzen Fünferlemma 7.2.3.7 ist φ daher ein Isomorphismus.

(ii)⇒(iii): Wir definieren einen R-Modul-Homomorphismus $\psi\colon B \to A_1 \oplus A_2$ durch $\psi : b \mapsto (\rho(b), g(b))$. Wir zeigen, dass das Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_{A_1}} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \mathrm{id}_{A_2}} & & \\ 0 & \longrightarrow & A_1 & \xrightarrow{\iota_1} & A_1 \oplus A_2 & \xrightarrow{\pi_2} & A_2 & \longrightarrow & 0 \end{array}$$

kommutiert. Wegen

$$\pi_2\psi(b) = \pi_2(\rho(b), g(b)) = g(b)$$

für alle $b \in B$ kommutiert das rechte Quadrat. Wegen $\operatorname{Im} f = \ker g$ gilt weiters $gf = 0$ und somit $\rho f = \mathrm{id}_{A_1}$. Folglich erhalten wir

$$\psi f(a_1) = (\rho f(a_1), gf(a_1)) = (a_1, 0) = \iota_1(a_1)$$

für alle $a_1 \in A_1$ und es kommutiert auch das linke Quadrat. Wieder nach dem kurzen Fünferlemma 7.2.3.7 ist ψ ein Isomorphismus.

(iii)⇒(i),(ii): Gegeben ist das kommutative Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \xrightarrow{\iota_1} & A_1 \oplus A_2 & \xrightarrow{\pi_2} & A_2 & \longrightarrow & 0 \\ & & {\scriptstyle \mathrm{id}_{A_1}}\downarrow & \nwarrow^{\pi_1} & \downarrow{\scriptstyle \varphi} & \nwarrow^{\iota_2} & \downarrow{\scriptstyle \mathrm{id}_{A_2}} & & \\ 0 & \longrightarrow & A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2 & \longrightarrow & 0 \end{array}$$

mit einem Isomorphismus φ. Definiere $\sigma := \varphi\iota_2 \colon A_2 \to B$ und $\rho := \pi_1\varphi^{-1} \colon B \to A_1$. Nun gilt wegen der Kommutativität des Diagramms

$$g\sigma(a_2) = g\varphi\iota_2(a_2) = \pi_2\iota_2(a_2) = a_2 \text{ und}$$
$$\rho f(a_1) = \pi_1\varphi^{-1}f(a_1) = \pi_1\varphi^{-1}\varphi\iota_1(a_1) = \pi_1\iota_1(a_1) = a_1$$

für alle $a_1 \in A_1$, $a_2 \in A_2$. Somit sind die gesuchte Sektion σ und Retraktion ρ gefunden. □

7.3 Injektive und projektive Moduln

In $\mathbb{Q}$ hat jede Gleichung der Form $nx = a$ für gegebenes $a \in \mathbb{Q}$ und $n \in \mathbb{N} \setminus \{0\}$ eine (in diesem Fall sogar eindeutige) Lösung, nämlich $x = \frac{a}{n}$. Für eine abelsche Gruppe G nimmt man diese Eigenschaft als Definition für die sogenannte *Teilbarkeit* von G (siehe 7.3.1). Eine sinnvolle Verallgemeinerung von abelschen Gruppen auf Moduln ist etwas komplizierter. Sie erfolgt mit Hilfe eines geeigneten kommutativen Diagramms und führt zum Begriff des *injektiven Moduls* (siehe 7.3.2). Durch Dualisierung dieses Konzeptes (d.h. durch Umkehrung von Pfeilrichtungen u.ä.) ergibt sich der Begriff des *projektiven Moduls*, der sich wiederum als eine Abschwächung der Eigenschaft *frei* auffassen lässt (siehe 7.3.3). Über Hauptidealringen sind die projektiven Moduln sogar genau die freien. Die Resultate aus 7.3.3 werden sich unter anderem beim Beweis des Hauptsatzes über endlich erzeugte Moduln über Hauptidealringen als sehr fruchtbar erweisen.

7.3.1 Teilbare Gruppen

Definition 7.3.1.1. Sei D eine abelsche Gruppe, $a \in D$ und $n \in \mathbb{Z} \setminus \{0\}$. Das Element a heißt *teilbar durch n* in D, wenn es ein $d \in D$ gibt mit $nd = a$; a heißt (schlechthin) *teilbar in D*, wenn a durch alle $n \in \mathbb{Z} \setminus \{0\}$ teilbar ist. D heißt *teilbar durch n*, wenn alle $a \in D$ durch n teilbar sind; D heißt (schlechthin) *teilbar*, wenn alle $a \in D$ teilbar sind.

Beispiele teilbarer Gruppen sind $\mathbb{Q}$ und $\mathbb{R}$, außerdem direkte Summen und Produkte teilbarer Gruppen sowie deren homomorphe Bilder. Die wichtigsten Beispiele teilbarer Torsionsgruppen sind die Prüfergruppen.

UE 22 ► **Übungsaufgabe 7.3.1.2.** (F) Beweisen Sie, dass tatsächlich $\mathbb{Q}$, $\mathbb{R}$ und die Prüfergruppen teilbar sind sowie dass sich Teilbarkeit sowohl auf direkte Summen und Produkte als auch auf homomorphe Bilder überträgt. ◄ **UE 22**

Als Ausgangspunkt für das Weitere dient die Beobachtung, dass jeder Homomorphismus von einer Untergruppe einer Gruppe G in eine teilbare Gruppe D stets auf ganz G fortgesetzt werden können.

Satz 7.3.1.3. *Ist D eine teilbare Gruppe, $U \leq A$ und $f_U \colon U \to D$ ein Homomorphismus, so gibt es eine homomorphe Fortsetzung von f_U auf ganz A, d.h. einen Homomorphismus $f \colon A \to D$ mit $f(u) = f_U(u)$ für alle $u \in U$.*

Beweis. Das System $\mathcal{S}$ aller Homomorphismen $f_B\colon B \to D$ mit $U \leq B \leq A$, die $f_B(u) = f_U(u)$ für alle $u \in U$ erfüllen, bildet bezüglich $\subseteq$ eine Halbordnung, in der jede Kette nach oben beschränkt ist (z.B. durch ihre Vereinigung). Also ist das Lemma von Zorn anwendbar und liefert ein maximales $f_0\colon A_0 \to D$ in $\mathcal{S}$. Wir zeigen, dass bereits $A_0 = A$ gilt und folglich $f := f_0$ das Gewünschte leistet.
Wir nehmen indirekt an, es gäbe ein $a \in A \setminus A_0$, und setzen $A_1 := A_0 + \langle a\rangle \leq A$. $H := \langle a\rangle \cap A_0$ ist als Untergruppe der zyklischen Gruppe $\langle a\rangle$ selbst zyklisch mit $H = \langle ma\rangle$ für ein $m \in \mathbb{N}$. Wir halten fest, dass ka für $k \in \mathbb{Z}$ genau dann in H liegt, wenn es ein $n \in \mathbb{Z}$ mit $k = nm$ gibt. Ist $m \neq 0$, so gibt es wegen der Teilbarkeit von D ein $d \in D$ mit $md = f_0(ma)$, für $m = 0$ nehmen wir $d = 0$. Wir behaupten, dass die Zuordnung $f_1 : a_0 + ka \mapsto f_0(a_0) + kd$ für $a_0 \in A_0$ und $k \in \mathbb{Z}$ einen wohldefinierten Homomorphismus $f_1\colon A_1 \to D$ definiert. Zu zeigen ist: Aus $a_0 + ka = a_0' + k'a$ mit $a_0, a_0' \in A_0$ und $k, k' \in \mathbb{Z}$ folgt $f_0(a_0) + kd = f_0(a_0') + k'd$; die Homomorphieeigenschaft ist dann offensichtlich. Zunächst gilt $f_0(a_0') + k'd = f_0(a_0 + a_0' - a_0) + (k + k' - k)d = f_0(a_0) + kd + r$ mit dem Rest $r = f_0(a_0' - a_0) - (k - k')d$, von dem wir $r = 0$ zu zeigen haben. Wegen $a_0 - a_0' = (k' - k)a \in A_0 \cap \langle a\rangle = H$ gibt es ein $n \in \mathbb{Z}$ mit $nm = k - k'$. Somit gilt $f_0(a_0' - a_0) = f_0((k - k')a) = f_0(nma) = nf_0(ma) = nmd$ und $(k - k')d = nmd$, folglich $r = f_0(a_0' - a_0) - (k - k')d = 0$. □

Die Fortsetzungseigenschaft aus Satz 7.3.1.3 lässt sich einprägsam mittels Diagrammen darstellen. Es gilt sogar:

Satz 7.3.1.4. *Eine abelsche Gruppe D ist genau dann teilbar, wenn zu jedem Diagramm abelscher Gruppen*

$$\begin{array}{ccccc} 0 & \longrightarrow & U & \overset{g}{\longrightarrow} & A \\ & & \big\downarrow{\scriptstyle f} & & \\ & & D & & \end{array}$$

mit injektivem g ein Homomorphismus h existiert, sodass das Diagramm

$$\begin{array}{ccccc} 0 & \longrightarrow & U & \overset{g}{\longrightarrow} & A \\ & & {\scriptstyle f}\big\downarrow & \swarrow{\scriptstyle h} & \\ & & D & & \end{array}$$

kommutiert.

Beweis. Wegen der Injektivität von g dürfen wir U oBdA als Untergruppe von A betrachten. Dass aus der Teilbarkeit von D die im Satz behauptete Diagrammeigenschaft folgt, ist daher nur eine Umformulierung von Satz 7.3.1.3.
Zu zeigen bleibt die Umkehrung. Gelte also für D die im Satz formulierte Diagrammeigenschaft, sei $a \in D$ und $n \in \mathbb{Z} \setminus \{0\}$. Ist a von unendlicher Ordnung (Fall 1), so wählen wir $A := \mathbb{Q}$, $U := \mathbb{Z} \leq \mathbb{Q} = A$, $f\colon k \mapsto ka$ und die Inklusionsabbildung

$g = \iota\colon \mathbb{Z} \to \mathbb{Q}$, $k \mapsto k$. Laut Voraussetzung gibt es einen Homomorphismus $h\colon \mathbb{Q} \to D$ mit $f = h \circ g$. Dann hat das Element $d := h(\frac{1}{n}) \in D$ die gewünschte Eigenschaft: $nd = nh(\frac{1}{n}) = h(n\frac{1}{n}) = h \circ g(1) = f(1) = a$. Hat a hingegen eine endliche Ordnung $m \in \mathbb{N}$ (Fall 2), so wählt man statt $\mathbb{Q}$ die Gruppe $A := \mathbb{Q}/m\mathbb{Z}$, ihre Untergruppe $U := \mathbb{Z}/m\mathbb{Z}$, den (wohldefinierten) Homomorphismus $f\colon k + m\mathbb{Z} \mapsto ka$ und die Inklusionsabbildung $g = \iota\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Q}/m\mathbb{Z}$, $k + m\mathbb{Z} \mapsto k + m\mathbb{Z}$. Die laut Voraussetzung existierende Fortsetzung h von f liefert wie im Fall 1 ein Element $d := h(\frac{1}{n} + m\mathbb{Z}) \in D$ mit

$$\begin{aligned} nd &= nh\left(\frac{1}{n} + m\mathbb{Z}\right) = h\left(n\left(\frac{1}{n} + m\mathbb{Z}\right)\right) = h(1 + m\mathbb{Z}) = (h \circ g)(1 + m\mathbb{Z}) \\ &= f(1 + m\mathbb{Z}) = 1a = a. \end{aligned}$$

□

Die Erweiterung der additiven Gruppe $\mathbb{Z}$ zur teilbaren Gruppe $\mathbb{Q}$ lässt sich auf beliebige abelsche Gruppen verallgemeinern:

Satz 7.3.1.5. *Jede abelsche Gruppe lässt sich in eine teilbare Gruppe einbetten.*

Beweis. Sei A eine beliebige abelsche Gruppe. Es gibt eine freie abelsche Gruppe F (zum Beispiel die von sämtlichen $a \in A$ frei erzeugte abelsche Gruppe) und einen surjektiven Homomorphismus $\varphi\colon F \to A$. Sei $K \leq F$ der Kern von φ. Als freie abelsche Gruppe ist F isomorph zur Gruppe $\bigoplus_{i\in I} \mathbb{Z}$, wobei eine Indexmenge I mit $|I| = \dim_{\mathbb{Z}} F$ zu wählen ist (siehe Satz 7.2.1.4). Diese Isomorphie werde durch den Isomorphismus $\psi\colon F \to \bigoplus_{i\in I} \mathbb{Z}$ vermittelt. Bezeichne ι die kanonische Einbettung $\iota\colon \bigoplus_{i\in I} \mathbb{Z} \to D_0 := \bigoplus_{i\in I} \mathbb{Q}$ (Inklusionsabbildung). D_0 ist teilbar, folglich auch die Faktorgruppe $D := D_0/\iota\psi(K)$. Offenbar gilt

$$A \cong F/K \cong \frac{\iota\psi(F)}{\iota\psi(K)} \leq \frac{D_0}{\iota\psi(K)} = D.$$

Also lässt sich A in die teilbare Gruppe D einbetten. □

Eine der wichtigsten Eigenschaften teilbarer Gruppen besteht darin, dass sie, eingebettet in eine umfassende abelsche Gruppe, stets direkte Summanden derselben sind.

Satz 7.3.1.6. *Jede teilbare Untergruppe D einer abelschen Gruppe A ist direkter Faktor, d.h. es gibt eine Untergruppe $U \leq A$ mit $A = D \oplus U$.*

Beweis. Der Beweis gelingt überraschend einfach mit Hilfe zerfallender Sequenzen: Zur kurzexakten Sequenz $0 \to D \to A \to A/D \to 0$ gibt es nach Satz 7.3.1.3 einen die Identität auf D fortsetzenden Homomorphismus $\rho\colon A \to D$, also eine Retraktion. Nach Satz 7.2.3.8 ist also $A = D \oplus U$ mit geeignetem U. □

Mit den nunmehr zur Verfügung stehenden Hilfsmitteln lässt sich ohne allzu große Schwierigkeiten ein vollständiger Überblick über die Struktur teilbarer Gruppen gewinnen:

Satz 7.3.1.7. *Jede teilbare Gruppe D ist isomorph zu einer direkten Summe von Kopien der additiven Gruppe $\mathbb{Q}$ der rationalen Zahlen sowie von Prüferschen Gruppen C_{p^∞}, $p \in \mathbb{P}$, also*

$$D \cong \bigoplus_{i \in I_0} \mathbb{Q} \oplus \bigoplus_{p \in \mathbb{P}} \bigoplus_{i \in I_p} C_{p^\infty},$$

wobei die Kardinalitäten der Indexmengen I_0 und I_p, $p \in \mathbb{P}$, durch D eindeutig bestimmt sind.

Der Beweis dieses Satzes ergibt sich aus der folgenden Übungsaufgabe, die mit einigen Anleitungen versehen ist.

UE 23 ► **Übungsaufgabe 7.3.1.8.** (V) Beweisen Sie Satz 7.3.1.7, indem Sie mit Hilfe der bisherigen Resultate folgende Aussagen beweisen. ◄ **UE 23**

1. Ist $p \in \mathbb{P}$ und D eine teilbare p-Gruppe (d.h. die Ordnungen sämtlicher Elemente sind p-Potenzen), so ist $D \cong \bigoplus_{i \in I} C_{p^\infty}$ eine direkte Summe von isomorphen Kopien der p-Prüfergruppe C_{p^∞}. Hinweis: Die Menge aller Elemente der Ordnung p bilden in natürlicher Weise einen Vektorraum über $\mathrm{GF}(p)$. Sei X eine Basis. Zu jedem $x \in X$ wähle man eine Folge von $x_n \in D$ mit $x_1 = x$ und $px_{n+1} = x_n$ für $n = 1, 2, \ldots$. Die von den x_n erzeugte Untergruppe $U_x \leq D$ ist isomorph zu C_{p^∞}. Damit gilt $D \cong \bigoplus_{x \in X} U_x$.

2. Jede Torsionsgruppe G (d.h. alle Elemente von G haben endliche Ordnung) ist nach Satz 3.3.3.6 die direkte Summe ihrer p-Komponenten G_p (= Mengen aller Elemente von p-Potenz-Ordnung), $p \in \mathbb{P}$. Ist G teilbar, so müssen die G_p ebenfalls teilbar sein.

3. Ist D torsionsfrei und $x \in D$, so gibt es zu jedem $n \in \mathbb{Z} \setminus \{0\}$ ein sogar eindeutiges Element $y \in D$ mit $ny = x$. Bezeichnet man dieses mit $\frac{1}{n}x$, so ist für alle $\frac{p}{q} \in \mathbb{Q}$, $p, q \in \mathbb{Z}$, das Element $\frac{p}{q}x := p(\frac{1}{q}x)$ wohldefiniert. Auf diese Weise wird D zu einem Vektorraum über $\mathbb{Q}$. Daraus folgt die Isomorphie $D \cong \bigoplus_{i \in I} \mathbb{Q}$ abelscher Gruppen, wenn I geeignet gewählt wird.

4. Die Torsionselemente (Elemente endlicher Ordnung) bilden eine teilbare Untergruppe D_t mit $D \cong D_0 \oplus D_t$ und torsionsfreiem, teilbarem $D_0 \cong D/D_t$.

5. Setzen Sie das Bisherige zu einem Beweis für die Existenz der behaupteten Darstellung zusammen.

6. Beweisen Sie die Eindeutigkeitsaussage in Satz 7.3.1.7, indem Sie geeignete Vektorräume und deren Dimension betrachten.

7.3.2 Injektive Moduln

Als natürliche Verallgemeinerung des Begriffs einer teilbaren Gruppe von abelschen Gruppen, d.h. von Moduln über dem Ring $\mathbb{Z}$, auf Moduln über beliebigen Ringen erweist

sich der Begriff des injektiven Moduls. Zunächst zur Definition von Injektivität, wie sie durch Satz 7.3.1.4 motiviert wird.

Definition 7.3.2.1. Ein R-Modul J heißt *injektiv*, wenn für alle Diagramme von R-Moduln

$$\begin{array}{ccc} 0 \longrightarrow A & \xrightarrow{g} & B \\ & \downarrow{\scriptstyle f} & \\ & J & \end{array}$$

mit injektivem g ein R-Modul-Homomorphismus h existiert, sodass das Diagramm

$$\begin{array}{ccc} 0 \longrightarrow A & \xrightarrow{g} & B \\ & {\scriptstyle f}\downarrow \swarrow {\scriptstyle h} & \\ & J & \end{array}$$

kommutiert.

Aus Satz 7.3.1.4 folgt unmittelbar:

Proposition 7.3.2.2. *Eine abelsche Gruppe ist teilbar genau dann, wenn sie als unitärer $\mathbb{Z}$-Modul injektiv ist.*

Viele Eigenschaften teilbarer Gruppen lassen sich auf den allgemeineren Fall injektiver Moduln übertragen, allerdings nicht immer auf triviale Weise. Die entsprechenden Resultate werden wir im Folgenden nicht mehr benötigen, weshalb wir uns mit Hinweisen, Beweisskizzen sowie Verweisen begnügen. Noch relativ einfach ist die folgende Übungsaufgabe:

UE 24 ► Übungsaufgabe 7.3.2.3. (F) Zeigen Sie: **◄ UE 24**

1. Vektorräume sind als Moduln injektiv.
2. Das direkte Produkt von R-Moduln $\prod_{i\in I} J_i$ ist genau dann injektiv, wenn alle J_i, $i \in I$, injektiv sind.

Deutlich mehr Aufwand erfordert der Beweis der Verallgemeinerung von Satz 7.3.1.5:

Satz 7.3.2.4. *Jeder unitäre R-Modul lässt sich in einen injektiven unitären R-Modul einbetten.*

UE 25 ► Übungsaufgabe 7.3.2.5. (E) **◄ UE 25**
(Achtung, Anspruchsvoll!) Beweisen Sie Satz 7.3.2.4, indem Sie folgende Aussagen zeigen:

1. Zeigen Sie: Sei R ein Ring mit 1 und J ein unitärer R-Modul. Dann ist J genau dann injektiv, wenn es zu jedem Linksideal L von R und jedem R-Modulhomomorphismus $f\colon L \to J$ eine Fortsetzung $h\colon R \to J$ gibt. (Hinweis: Schlagen Sie in der Literatur nach. Der Beweis dieser Aussage ist beispielsweise als Lemma 3.8 in Kapitel IV von Hungerfords Algebra-Buch enthalten.)

2. Ist J eine teilbare abelsche Gruppe und R ein Ring mit 1, dann ist der Raum $\mathrm{Hom}_{\mathbb{Z}}(R, J)$ der $\mathbb{Z}$-Modul-Homomorphismen $R \to J$ (äquivalent: Gruppenhomomorphismen zwischen den additiven Gruppen) auf natürliche Weise ein injektiver unitärer R-Modul. Hinweis: Verwenden Sie den ersten Teil und die entsprechende Eigenschaft teilbarer Gruppen.

3. Folgern Sie Satz 7.3.2.4, indem Sie den R-Modul zunächst als $\mathbb{Z}$-Modul auffassen und in $\mathrm{Hom}_{\mathbb{Z}}(R, J)$ einbetten.

Diese Hilfsmittel dienen auch beim Beweis der folgenden Charakterisierung injektiver Moduln, die an Satz 7.3.1.6 anschließt.

Satz 7.3.2.6. *Sei R ein Ring mit 1 und J ein unitärer R-Modul. Dann sind folgende Aussagen äquivalent:*

(i) J ist injektiv.

(ii) Jede kurzexakte Sequenz $0 \to J \xrightarrow{f} A \xrightarrow{g} B \to 0$ zerfällt. Insbesondere ist $A \cong J \oplus B$.

(iii) Sei $J \leq B$. Dann existiert ein R-Modul K, sodass $B = J \oplus K$.

UE 26 ► **Übungsaufgabe 7.3.2.7.** (V) Beweisen Sie Satz 7.3.2.6. Hinweis für die erste Implikation: Dualisieren Sie den späteren Beweis von Satz 7.3.3.4. ◄ **UE 26**

7.3.3 Projektive Moduln

Die Definition von Projektivität eines Moduls ergibt sich aus jener von Injektivität durch Dualisierung.

Definition 7.3.3.1. Ein R-Modul P heißt *projektiv*, wenn für alle Diagramme von R-Moduln

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle f} & & \\ A & \xrightarrow{g} & B & \longrightarrow & 0 \end{array}$$

mit surjektivem g ein R-Modul-Homomorphismus h existiert, sodass das Diagramm

$$\begin{array}{ccccc} & & & & P \\ & & & \overset{h}{\swarrow} & \downarrow f \\ A & \xrightarrow{g} & B & \longrightarrow & 0 \end{array}$$

kommutiert.

Die wichtigsten Beispiele projektiver Moduln sind die freien:

Satz 7.3.3.2. *Jeder freie R-Modul ist projektiv.*

Beweis. Sei F ein freier R-Modul mit Basis X. Für den Beweis des Satzes haben wir uns irgendwelche R-Moduln A und B sowie R-Modulhomomorphismen $g\colon A \to B$ und $f\colon F \to B$ vorzugeben, wobei g surjektiv sei. Wir müssen einen Homomorphismus $h\colon F \to A$ mit $f = g \circ h$ finden.

$$\begin{array}{ccccc} & & & & F \\ & & & \overset{h}{\swarrow} & \downarrow f \\ A & \xrightarrow{g} & B & \longrightarrow & 0 \end{array}$$

Wegen der Surjektivität von g gibt es zu jedem $x \in X$ ein $a_x \in A$ mit $g(a_x) = f(x)$. Da F frei über X ist, gibt es einen (eindeutigen) Homomorphismus $h\colon F \to A$ mit $h(x) = a_x$ für alle $x \in X$. Somit gilt $(g \circ h)(x) = g(a_x) = f(x)$ für alle x aus dem Erzeugendensystem X von F. Weil sowohl $g \circ h$ als auch f Homomorphismen sind, müssen sie sogar auf dem Erzeugnis von X, also auf ganz F, übereinstimmen, womit $f = g \circ h$ bewiesen ist. □

Später (siehe Folgerung 7.4.2.5) werden wir sehen, dass für Moduln über Hauptidealringen die Begriffe frei und projektiv sogar zusammenfallen. Im allgemeinen Fall müssen projektive Moduln aber nicht frei sein. Zur Illustration einfache Übungen:

UE 27 ► Übungsaufgabe 7.3.3.3. (F,B) Zeigen Sie: **◄ UE 27**

1. Der $\mathbb{Z}$-Modul $\mathbb{Q}$ ist nicht projektiv.
2. $\mathbb{Z}_2$ und $\mathbb{Z}_3$ sind projektive $\mathbb{Z}_6$-Moduln, aber nicht frei.
3. Die direkte Summe von R-Moduln $\bigoplus_{i\in I} P_i$ ist genau dann projektiv, wenn alle P_i, $i \in I$, projektiv sind.

Die für uns wichtigsten Strukturaussagen über projektive Moduln bilden den folgenden, zu 7.3.2.6 dualen Satz.

Satz 7.3.3.4. *Für einen R-Modul P sind folgende Bedingungen äquivalent:*

(i) P ist projektiv.

(ii) Jede kurzexakte Sequenz $0 \to A \xrightarrow{f} B \xrightarrow{g} P \to 0$ *zerfällt. Insbesondere ist* $B \cong A \oplus P$.

(iii) Es existiert ein freier R*-Modul* F *und ein* R*-Modul* K*, sodass* $F \cong K \oplus P$.

Beweis. Wir gehen zyklisch vor, indem wir die drei Implikationen (i)⇒(ii), (ii)⇒(iii) und (iii)⇒(i) beweisen.
(i)⇒(ii): Sei die kurzexakte Sequenz

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} P \longrightarrow 0$$

vorgegeben. Die Projektivität von P liefert ein h, sodass

$$\begin{array}{ccccc} & & & & P \\ & & \overset{h}{\swarrow} & \overset{\nearrow}{\downarrow}{\scriptstyle \mathrm{id}_P} & \\ B & \xrightarrow{g} & P & \longrightarrow & 0 \end{array}$$

kommutiert. So ein h ist eine Sektion:

$$0 \longrightarrow A \xrightarrow{f} B \underset{h}{\overset{g}{\rightleftarrows}} P \longrightarrow 0$$

Nach Satz 7.2.3.8 zerfällt dann die kurzexakte Sequenz, und $B \cong A \oplus P$.

(ii)⇒(iii): Nach Folgerung 7.2.1.6 ist P homomorphes Bild eines freien R-Moduls F unter einem Homomorphismus κ. Definiere $K := \ker \kappa$. Die Sequenz $0 \to K \xrightarrow{\iota} F \xrightarrow{\kappa} P \to 0$ ist kurzexakt. Nach (ii) ist damit $F \cong K \oplus P$.

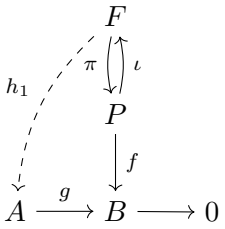
(iii)⇒(i): Sei oBdA $F = K \oplus P$ frei. Gegeben sei ein Diagramm

$$\begin{array}{ccccc} & & & & P \\ & & & & \downarrow{\scriptstyle f} \\ A & \xrightarrow{g} & B & \longrightarrow & 0 \end{array}$$

mit surjektivem g. Betrachte nun

$$\begin{array}{ccccc} & & & & F \\ & & & & \pi \big\downarrow \big\uparrow \iota \\ & & & & P \\ & & & & \downarrow{\scriptstyle f} \\ A & \xrightarrow{g} & B & \longrightarrow & 0 \end{array}$$

mit $\iota : p \mapsto (0, p)$ und $\pi : (k, p) \mapsto p$. Da F frei und somit nach Satz 7.3.3.2 projektiv ist, gibt es einen R-Modul-Homomorphismus h_1, sodass



kommutiert. Dann leistet $h := h_1\iota$ das Gewünschte. Somit ist P projektiv. □

7.4 Moduln über Hauptidealringen

Wir spezialisieren nun auf den Fall eines Hauptidealrings R (siehe auch Abschnitt 5.2, insbesondere 5.2.2). Definitionsgemäß ist das ein Integritätsbereich, in dem jedes Ideal I von der Form $I = rR$ mit einem Erzeugenden $r \in R$ ist. Insbesondere ist R also faktoriell, und die Primelemente in R sind genau die irreduziblen. Alle R-Moduln seien unitär. Speziell sind damit für $R = \mathbb{Z}$ auch weiterhin die abelschen Gruppen erfasst. Wir beginnen mit einigen Definitionen und Schreibweisen, die das Konzept der Ordnung eines Gruppenelementes verallgemeinern (7.4.1). Sodann wenden wir uns den freien Moduln zu und zeigen, dass deren Untermoduln wieder frei sind. Als Folgerung ergibt sich daraus, dass unter den Moduln über Hauptidealringen die freien genau die projektiven sind und weiters, dass endlich erzeugte torsionsfreie Moduln frei sind (7.4.2). Besonders gut versteht man die Struktur endlich erzeugter Moduln, die durch den Hauptsatz beschrieben wird. Ihm zufolge sind sie direkte Summen endlich vieler zyklischer Moduln. Die genaue Formulierung sowie ein Überblick über die Beweisstrategie sind Gegenstand von 7.4.3. Nach einer genaueren Untersuchung von Torsionsmoduln (7.4.4), kann der Beweis in 7.4.5 abgeschlossen werden. Als interessante Anwendung davon ergibt sich daraus die aus der Linearen Algebra bekannte Jordansche Normalform quadratischer Matrizen (7.4.6).

7.4.1 Notationen und Sprechweisen

Bevor wir den Hauptsatz formulieren, brauchen wir die Verallgemeinerungen einiger Begriffe, Schreib- und Sprechweisen für R-Moduln vom Fall abelscher Gruppen ($R = \mathbb{Z}$) auf einen beliebigen Hauptidealring R. (Manche der Begriffe lassen sich sogar für einen beliebigen Integritätsbereich R definieren.)
Sei also R ein Hauptidealring, $r \in R$, A ein unitärer R-Modul (geschrieben als Linksmodul) und $a \in A$. Die Assoziiertheitsrelation in R sei mit $\sim$ bezeichnet, d.h.: $r \sim s$ bedeutet $r = es$ für eine Einheit (ein multiplikativ invertierbares Element) $e \in R$. Die Assoziiertenklasse von r wird mit $[r]_\sim$ bezeichnet. Der einfacheren Notation halber werden wir nicht immer streng zwischen r und $[r]_\sim$ unterscheiden. Für das von r erzeugte Hauptideal $(r) \lhd R$ erweist es sich oft als zweckmäßig, $rR \lhd R$ zu schreiben, da dies

mit der Schreibweise $Ra = \{r \cdot a \mid r \in R\}$ für den von a erzeugten Untermodul harmoniert (siehe unten). Über diese Konventionen hinausgehend verwenden wir folgende Schreibweisen, die im Lichte der anschließenden Proposition 7.4.1.2 zu sehen sind:

Definition 7.4.1.1.

- $\mathbb{P}(R) := \{p \in R : p \text{ prim}\}$ und $\mathbb{P}_\sim(R) := \{[p]_\sim : \ p \in \mathbb{P}(R)\}$. Häufig wird es vorteilhaft sein, Vertretersysteme P der Assoziertenklassen sämtlicher Primelemente zu betrachten.

- $\mathcal{O}_a := \{r \in R : r \cdot a = 0\} \lhd R$ heißt *Ordnungsideal*[4] von $a \in A$. Ist $\mathcal{O}_a = rR$, so heißt r oder, genauer, $[r]_\sim$ auch die *Ordnung* von a.

- $A_t := \{a \in A : \mathcal{O}_a \neq \{0\}\} \leq A$ heißt der *Torsionsanteil* von A. Elemente $a \in A_t$ heißen *Torsionselemente*.

- A heißt *Torsionsmodul*, wenn $A = A_t$, und *torsionsfrei*, wenn $A_t = \{0\}$.

- Ein von einem Element a erzeugter Untermodul Ra heißt *zyklischer Untermodul*.

- A heißt *p-primär*, $p \in \mathbb{P}$, falls es zu jedem $a \in A$ ein $n \in \mathbb{N}$ mit $\mathcal{O}_a = p^n R$ gibt.

- Für $p \in \mathbb{P}(R)$ heißt $A(p) := \{a \in A : \exists n \in \mathbb{N} : \ p^n a = 0\} \leq A$ der *p-Anteil* von A. (Man beachte: $p_1 \sim p_2$ impliziert $A(p_1) = A(p_2)$. Deshalb ist auch $A([p]_\sim) := A(p)$ wohldefiniert.)

Sehr leicht überprüft man die impliziten Behauptungen in obigen Definitionen:

Proposition 7.4.1.2. *Mit obigen Bezeichnungen gilt:*

(1) *$\mathcal{O}_a$ ist tatsächlich ein Ideal von R.*
(2) *$A_t \leq A$.*
(3) *Der von a erzeugte Untermodul ist genau $Ra = \{r \cdot a \mid r \in R\}$.*
(4) *Für jedes $p \in \mathbb{P}(R)$ ist $A(p) \leq A_t$.*
(5) *Für $a \in A$ und $r \sim s \in R$ ist $ra = 0$ genau dann, wenn $sa = 0$.*
(6) *Aus $p_1 \sim p_2$ folgt $A(p_1) = A(p_2)$.*
(7) *Sind $p_1, p_2 \in \mathbb{P}(R)$ nicht assoziiert, so ist $A(p_1) \cap A(p_2) = \{0\}$.*

UE 28 ▶ Übungsaufgabe 7.4.1.3. Beweisen Sie Proposition 7.4.1.2. **◀ UE 28**

[4] Man unterscheide die so definierten Ordnungsideale im ringtheoretischen Sinn von Idealen in Halbordnungen, die manchmal gleichfalls Ordungsideale genannt werden.

7.4.2 Untermoduln freier Moduln

Fasst man abelsche Gruppen als $\mathbb{Z}$-Moduln auf, so sind die Torsionselemente offenbar genau jene mit endlicher Ordnung. Deshalb sind freie abelsche Gruppen auch torsionsfrei. Im endlich erzeugten Fall werden sich auch umgekehrt torsionsfreie Moduln als frei erweisen. Allgemein gilt das nicht, wie der torsionsfreie aber nicht freie $\mathbb{Z}$-Modul $\mathbb{Q}$ zeigt. Weiterhin bezeichnet R stets einen Hauptidealring.
Wir werden von der folgenden Beobachtung Gebrauch machen, die Proposition 7.2.1.2 erweitert.

Proposition 7.4.2.1. *Sei R ein Hauptidealring*

1. *Jedes $I \lhd R$ ist als R-Modul frei, wobei nur zwei Fälle auftreten können: $I \cong \{0\}$ (frei über der leeren Menge) oder $I \cong R$ (frei über dem Singleton seines Erzeugers).*

2. *Sei A zyklisch mit erzeugendem Element $a \in A$. Gilt $\mathcal{O}_a = \{0\}$, so ist $A \cong R$ und A frei über $\{a\}$. Gilt hingegen $\mathcal{O}_a = (p^n) = p^n R$ mit $p \in \mathbb{P}(R)$ und positivem $n \in \mathbb{N}$, so ist A p-primär und nicht frei; und es gilt $A \cong R/p^n R$.*

Der Beweis ist nicht schwierig und Gegenstand einer Übungsaufgabe:

UE 29 ► **Übungsaufgabe 7.4.2.2.** (V) Beweisen Sie Proposition 7.4.2.1. Hinweis: Betrachten Sie den Homomorphismus $f_a \colon R \to A$, $r \mapsto ra$. Überlegen Sie weiter, dass f_a surjektiv ist mit Kern $\mathcal{O}_a = rR$ für ein $r \in R$ und verwenden Sie den Homomorphiesatz. ◄ **UE 29**

Der berühmte Satz von Nielsen-Schreier besagt, dass jede Untergruppe einer freien Gruppe wieder frei ist. Ein Beweis (zum Beispiel unter Zuhilfenahme von Fundamentalgruppen und Überlagerungen aus der algebraischen Topologie) würde uns hier zu weit führen. Leichter zu beweisen ist das analoge Resultat für abelsche Gruppen, hier etwas allgemeiner ausgesprochen für Moduln über Hauptidealringen:

Satz 7.4.2.3. *Sei F ein freier R-Modul und $G \leq F$ ein Untermodul. Dann ist auch G ein freier R-Modul, und es gilt* $\operatorname{rang}(G) \leq \operatorname{rang}(F)$.

Beweis. Sei $X = \{x_i : i \in I\}$ eine Basis von F und $\leq$ eine Wohlordnung von I, also $|I| = \operatorname{rang}(F)$. Wir schreiben $i+1$ für den Nachfolger von $i \in I$ und definieren

$$F_i := \langle x_j : j \leq i \rangle$$
$$G_i := G \cap F_i.$$

Die F_i bilden eine aufsteigende transfinite Mengenfolge, was sich auch auf die G_i überträgt. Man beachte, dass auch $G_i = G \cap F_i = G_{i+1} \cap F_i$ gilt. Deshalb gilt nach dem ersten Isomorphiesatz 2.2.6.3:

$$G_{i+1}/G_i = G_{i+1}/(G_{i+1} \cap F_i) \cong (G_{i+1} + F_i)/F_i \leq F_{i+1}/F_i \cong R.$$

Also ist G_{i+1}/G_i isomorph zu einem Untermodul von R. Jeder Untermodul von R ist ein Ideal von R und nach Proposition 7.4.2.1 frei vom Rang 0 oder 1. Laut Satz 7.3.3.4 und Satz 7.3.3.2 zerfällt die Sequenz

$$0 \to G_i \to G_{i+1} \to G_{i+1}/G_i \to 0,$$

und es gilt $G_{i+1} \cong G_i \oplus (G_{i+1}/G_i) \cong G_i \oplus y_i R$. (Hier ist $y_i = 0$ genau dann, wann $G_i = G_{i+1}$.) Mittels transfiniter Induktion zeigt man (Übung) $G \cong \bigoplus_{i \in I} y_i R \cong \bigoplus_{i \in I_1} R$ mit $I_1 = \{i : y_i \neq 0\}$. Die Menge $B := \{y_i : i \in I_1\}$ ist dann eine Basis von G, folglich gilt $\operatorname{rang}(G) = |B| \leq |I| = \operatorname{rang}(F)$. □

UE 30 ► **Übungsaufgabe 7.4.2.4.** (V) Führen Sie jenen Schritt im Beweis von Satz 7.4.2.3 in Einzelnen aus, wo mittels transfiniter Induktion auf $G \cong \bigoplus_{i \in I_1} R$ geschlossen wird. ◄ **UE 30**

An dieser Stelle erinnern wir uns an Satz 7.3.3.4, wonach jeder projektive Modul P direkter Summand und daher Untermodul eines freien Moduls, über einem Hauptidealring laut Satz 7.4.2.3 also selbst frei ist. Umgekehrt sind freie Moduln nach Satz 7.3.3.2 immer projektiv, also:

Folgerung 7.4.2.5. *Ein Modul über einem Hauptidealring ist frei genau dann, wenn er projektiv ist.*

Eine weitere Konsequenz von Satz 7.4.2.3 bezieht sich auf die Kardinalität von Erzeugendensystemen beliebiger Moduln:

Folgerung 7.4.2.6. *Sei A ein R-Modul mit Erzeugendensystem $E \subseteq A$ und $B \leq A$ ein Untermodul. Dann hat B ein Erzeugendensystem $E_B \subseteq B$ mit $|E_B| \leq |E|$. Insbesondere ist jeder Untermodul eines endlich erzeugten Moduls endlich erzeugt.*

Beweis. Nach Folgerung 7.2.1.6 ist A homomorphes Bild eines über E freien R-Moduls F unter einem Epimorphismus $f : F \to A$. Sei $G := f^{-1}(B) \leq F$ das Urbild von B unter f. Nach Satz 7.4.2.3 ist G frei mit einem Erzeugendensystem $X \subseteq F$ mit $|X| \leq |E|$. Dann ist $E_B := f(X) \subseteq B$ ein Erzeugendensystem von B mit $|E_B| \leq |X| \leq |E|$. □

Im endlich erzeugten Fall gilt folgende bemerkenswerte Äquivalenz:

Satz 7.4.2.7. *Endlich erzeugte Moduln über Hauptidealringen sind genau dann frei, wenn sie torsionsfrei sind.*

Beweis. Dass jeder freie Modul torsionsfrei ist, werden wir im Weiteren nicht benötigen. Der Beweis ist nicht sehr schwierig und Inhalt einer Übungsaufgabe. Hier führen wir nur den Beweis, dass jeder endlich erzeugte torsionsfreie Modul A über einem Hauptidealring R frei ist.
Sei dazu E ein endliches Erzeugendensystem von A mit $0 \notin E$ und $S = \{x_1, \ldots, x_k\}$ eine maximale linear unabhängige Teilmenge von E. Wir betrachten den von S frei erzeugten R-Modul F. Für jedes $y \in E \setminus S$ gibt es wegen der Maximalität von S Koeffizienten

$r_y \in R$ und $r_i \in R$, $i = 1, \ldots, k$ (nicht alle gleich 0), sodass $r_y y + \sum_{i=1}^{k} r_i x_i = 0$. Dann gilt $r_y y = -\sum_{i=1}^{k} r_i x_i \in F$ und außerdem ist $r_y \neq 0$ für jedes $y \in E \setminus S$, da sonst auch alle $r_i = 0$ sein müssten. Wir setzen $r := \prod_{y \in E \setminus S} r_y$. Dann ist $rE \subseteq F$ und damit $rA = r\langle E \rangle \leq F$. Nach Satz 7.4.2.3 ist rA als Untermodul eines freien Moduls selbst frei. Die Abbildung $f\colon A \to rA,\ a \mapsto ra$ ist ein R-Modul-Epimorphismus, und wegen der Torsionsfreiheit von A gilt $\ker f = \{0\}$. Also ist $A \cong rA$ ebenfalls frei. □

UE 31 ► **Übungsaufgabe 7.4.2.8.** (V) Zeigen Sie, dass jeder freie Modul über einem Hauptidealring torsionsfrei ist. ◄ **UE 31**

Für die Strukturtheorie werden wir noch folgenden Satz benötigen, wonach endlich erzeugte Moduln in eine direkte Summe aus einem freien und einem Torsionsmodul zerfallen.

Satz 7.4.2.9. *Sei R ein Hauptidealring und A ein endlich erzeugter R-Modul. Dann gilt $A = A_t \oplus F$, wobei F ein freier R-Modul von endlichem Rang ist mit $F \cong A/A_t$.*

Beweis. Für jedes Erzeugendensystem $E \subseteq A$ von A bilden sämtliche $a + A_t$ ein Erzeugendensystem des Faktormoduls A/A_t. Folglich vererbt sich die endliche Erzeugtheit von A auf A/A_t. Der Modul A/A_t ist aber auch torsionsfrei: Sei $r(a + A_t) = 0$ in A/A_t mit $r \neq 0$ und $a \in A$. Zu zeigen ist $a \in A_t$. Zunächst folgt aus unserer Annahme $ra \in A_t$. Weil A_t der Torsionsanteil ist, gibt es in R ein $s \neq 0$ mit $sra = 0 \in A$. Aus der Nullteilerfreiheit von R folgt $rs \neq 0$ und somit $a \in A_t$. Also ist $F := A/A_t$ tatsächlich torsionsfrei und endlich erzeugt, nach Satz 7.4.2.7 daher frei und nach Satz 7.3.3.2 projektiv. Laut Satz 7.3.3.4 zerfällt dann die Sequenz

$$0 \to A_t \to A \to F \to 0,$$

und es gilt $A \cong A_t \oplus F$. □

7.4.3 Formulierung des Hauptsatzes und Beweisstrategie

Der Hauptsatz besagt, dass jeder endlich erzeugte R-Modul A die direkte Summe endlich vieler zyklischer Moduln ist. Diese zyklischen Summanden können so gewählt werden, dass eine gewisse Teilerkettenbedingung erfüllt ist, oder, alternativ, dass jeder der zyklischen Summanden entweder frei oder p-primär für ein geeignetes $p \in \mathbb{P}(R)$ ist. Die folgende Formulierung enthält beide Varianten:

Satz 7.4.3.1 (Hauptsatz über endlich erzeugte R-Moduln)**.** *Sei A ein endlich erzeugter Modul über dem Hauptidealring R. Dann folgt:*

(a) $A \cong R^n \oplus \bigoplus_{i=1}^{k} R/(p_i^{s_i} R)$ *mit $p_i \in \mathbb{P}(R)$. Dabei sind die Zahlen $k, n \in \mathbb{N}$ eindeutig bestimmt und die Ideale $p_i^{s_i} R$ (und somit die s_i sowie bis auf Assoziiertheit die p_i) sind bis auf die Reihenfolge eindeutig bestimmt. Die $p_i^{s_i}$ heißen auch die* Elementarteiler!eines Moduls *von A.*

(b) $A \cong R^n \oplus \bigoplus_{i=1}^{t} R/(r_i R)$ *mit* $n \in \mathbb{N}$ *und* $r_1 \mid r_2 \mid \ldots \mid r_t \in R$*, wobei die* r_i *weder* 0 *noch Einheiten sind. Dabei sind die Zahlen* $t, n \in \mathbb{N}$ *eindeutig bestimmt und die Ideale* $r_i R$ *(und somit bis auf Assoziiertheit die* r_i*) sind bis auf die Reihenfolge eindeutig bestimmt. Die Ideale* $r_i R$ *heißen auch die* invarianten Faktoren *von* A*.*

In beiden Formulierungen bezeichnet n *dieselbe natürliche Zahl, genannt der* Rang *von* A*, symbolisch* $n = \operatorname{rang}(A)$*.*

Durch Spezialisierung auf den Fall $r = \mathbb{Z}$ und abelsche Gruppen erhalten wir die folgende Verallgemeinerung von Satz 3.3.4.2:

Satz 7.4.3.2 (Hauptsatz über endlich erzeugte abelsche Gruppen)**.** *Sei* G *eine endlich erzeugte abelsche Gruppe. Dann folgt:*

(a) $G \cong \mathbb{Z}^n \oplus \bigoplus_{i=1}^{k} C_{p_i^{s_i}}$ *mit* $p_i \in \mathbb{P}$*. Dabei sind die Zahlen* $k, n \in \mathbb{N}$ *eindeutig bestimmt und die Primzahlpotenzen* $p_i^{s_i}$ *sind bis auf die Reihenfolge eindeutig bestimmt. Die* $p_i^{s_i}$ *heißen auch die* Elementarteiler!einer abelschen Gruppe *von* G*.*

(b) $G \cong \mathbb{Z}^n \oplus \bigoplus_{i=1}^{t} C_{m_i}$ *mit* $n, t \in \mathbb{N}$ *und* $1 < m_1 \mid m_2 \mid \ldots \mid m_t \in \mathbb{N}$*. Dabei sind die Zahlen* $t, n \in \mathbb{N}$ *eindeutig bestimmt und die Zahlen* $m_i \in \mathbb{N}$ *sind bis auf die Reihenfolge eindeutig bestimmt. Die Zahlen* $m_i \in \mathbb{N}$ *heißen auch die* invarianten Faktoren *von* G*.*

In beiden Formulierungen bezeichnet n *dieselbe natürliche Zahl, genannt der* Rang *von* G*, symbolisch* $n = \operatorname{rang}(G)$*.*

Der Rest dieses Abschnitts ist dem Beweis von Satz 7.4.3.1 und somit auch von Satz 7.4.3.2 gewidmet. Wir werden wie folgt vorgehen:
Nach Satz 7.4.2.9 lässt sich jeder endlich erzeugte Modul A als direkte Summe $A = A_t \oplus F$ eines Torsions- und eines freien Moduls schreiben. Dass der freie Summand F in eine direkte Summe zerfällt, wissen wir schon aus dem sehr allgemeinen Satz 7.2.1.4, in dem die Hauptidealeigenschaft von R gar keine Rolle spielt. Klarerweise können in einer direkten Zerlegung eines endlich erzeugten Moduls auch nur endlich viele nichttriviale Summanden auftreten. Somit bleibt der Torsionsmodul A_t zu untersuchen. Zunächst werden wir, ganz in Analogie zur Situation bei abelschen Gruppen, zeigen, dass jeder Torsionsmodul – endlich oder unendlich erzeugt – die direkte Summe seiner p-Anteile ($p \in \mathbb{P}(R)$) ist. Als letzter substantieller Beweisteil des Hauptsatzes bleibt dann die Zerlegung eines endlich erzeugten p-Moduls in zyklische Summanden. Auch hier kann man wie bei endlichen abelschen Gruppen vorgehen, indem man zunächst einen einzigen, in einem naheliegenden Sinn maximalen zyklischen Summanden abspaltet. Dieser Schritt kann dann iteriert werden und wird wegen der Endlichkeitsvoraussetzung schließlich zum Ziel führen.

7.4.4 Torsionsmoduln

Wir rekapitulieren: Für einen Hauptidealring R, einen R-Modul A besteht der *Torsionsanteil* A_t von A aus jenen $a \in A$, für die es ein $r \in R \setminus \{0\}$ gibt mit $ra = 0$. Für ein

Primelement $p \in R$ heißt $A(p) := \{a \in A : \exists n \in \mathbb{N} :\ p^n a = 0\} \leq A$ der p-Anteil von A. Jedes $a \in A_t$ heißt *Torsionselement* von A, jedes $a \in A(p)$ heißt p-Element.

Diese Begriffsbildungen sind unmittelbare Verallgemeinerungen entsprechender Konzepte für abelsche Gruppen aus Abschnitt 3.3. Das gilt auch für die folgenden Strukturaussagen. Für unser erstes Resultat beachte man die Analogie zu Satz 3.3.3.6.

Satz 7.4.4.1. *Ist A ein unitärer Torsionsmodul über dem Hauptidealring R, dann gilt*

$$A = \bigoplus_{p \in P} A(p),$$

wobei p ein Vertretersystem P sämtlicher Assoziiertenklassen primer Elemente von R durchläuft. Ist A endlich erzeugt, so sind nur endlich viele $A(p)$ nichttrivial.

Beweis. Im ersten Teil zeigen wir, dass jedes $a \in A$ als endliche Summe geeigneter p-Elemente dargestellt werden kann. Da R ein Hauptidealring ist, ist $\mathcal{O}_a = rR$ mit einem $r \in R$, insbesondere gilt $ra = 0$. Weil a ein Torsionselement ist, folgt $r \neq 0$. Ist r eine Einheit von R, so folgt $1 \in \mathcal{O}_a = (r) = R$. Daher ist $a = 1a = 0$ als leere Summe von p-Elementen darstellbar. Wir dürfen ab nun also annehmen, dass r weder 0 noch eine Einheit ist. In diesem Fall gibt es eine Primfaktorzerlegung $r = \prod_{i=1}^{k} p_i^{e_i}$ mit $k \geq 1$, paarweise nicht assoziierten $p_i \in \mathbb{P}(R)$ und $e_i > 0$. Definiere

$$r_i := \frac{r}{p_i^{e_i}} \in R$$

für jedes $i = 1, \ldots, k$. Dann ist $\mathrm{ggT}(r_1, \ldots, r_k) = 1$. Da R ein Hauptidealring ist, gibt es daher $s_i \in R$, sodass $1_R = \sum_{i=1}^{k} s_i r_i$. Es folgt

$$a = 1_R a = \sum_{i=1}^{k} s_i r_i a,$$

und $p_i^{e_i} s_i r_i a = s_i r a = 0$, das heißt $s_i r_i a \in A(p_i)$. Also wird A von den $A(p)$, p prim, erzeugt.
Im zweiten Teil des Beweises bleibt zu zeigen, dass die Zerlegung direkt ist, d.h.

$$A(p) \cap \sum_{q \in P \setminus \{p\}} A(q) = \{0\}.$$

Sei also $a \in A(p) \cap \sum_{q \in P \setminus \{p\}} A(q)$. Dann gibt es ein $m \in \mathbb{N}$ mit $p^m a = 0$ und paarweise verschiedene $q_i \in P \setminus \{p\}$ sowie $a_i \in A(q_i),\ q_i \neq p$, mit $a = \sum_{i=1}^{k} a_i$. Nun gibt es auch $m_i \in \mathbb{N}$ mit $q_i^{m_i} a_i = 0$. Definiere $d := \prod_{i=1}^{k} q_i^{m_i}$, dann ist d teilerfremd zu p^m, und es gibt $s, t \in R$ mit $1_R = sp^m + td$. Es folgt

$$a = 1_R a = sp^m a + tda = 0 + t \sum_{i=1}^{k} da_i = 0,$$

also ist die Summe direkt. Wenn A endlich erzeugt ist, sagen wir $A = \langle E \rangle$ für E endlich, dann kann man jedes $a \in E$ als endliche Summe geeigneter $a_p \in A(p)$ für $p \in P(a)$ schreiben. Setzen wir $P_0 := \bigcup_{a \in E} P(a)$, so folgt $A = \bigoplus_{p \in P_0} A(p)$, also $A(p) \neq \{0\}$ nur für p in der endlichen Menge P_0. □

Der wichtigste noch ausständige Schritt im Beweis des Hauptsatzes besteht darin, aus einem endlich erzeugten p-Modul einen zyklischen direkten Summanden abzuspalten. Auch hier kann man so vorgehen wie bei abelschen Gruppen, indem man zunächst folgendes Lemma beweist; siehe auch Lemma 3.3.4.1.

Lemma 7.4.4.2. *Sei A ein R-Modul und $p \in \mathbb{P}(R)$, sodass $p^n A = \{0\}$ aber $p^{n-1} A \neq \{0\}$ für ein $n \in \mathbb{N}$. Habe $a \in A$ die Ordnung p^n, d.h. $p^n a = 0 \neq p^{n-1} a$. Dann gilt:*

(a) Ist $A \neq Ra$, dann existiert ein $b \in A \setminus \{0\}$ mit $Ra \cap Rb = \{0\}$.

(b) Es gibt einen Untermodul C von A mit $A = Ra \oplus C$.

Beweis. Zu Punkt (a): Zwecks Konstruktion von b sei zunächst $c \in A \setminus Ra$ und $j \geq 1$ minimal mit $p^j c \in Ra$. Wir schreiben $p^j c = r_1 a$ und $r_1 = rp^k$ mit $k \in \mathbb{N}$ und $p \nmid r$. Daher gilt

$$0 = p^n c = p^{n-j}(p^j c) = p^{n-j} r_1 a = p^{n-j}(rp^k)a = p^{n-j+k} ra.$$

Da $p^{n-1} a \neq 0$ und $p \nmid r$, muss $n - j + k \geq n$ sein, also $1 \leq j \leq k$. Definiere

$$b := \underbrace{p^{j-1} c}_{\notin Ra} - \underbrace{rp^{k-1} a}_{\in Ra} \notin Ra.$$

Insbesondere ist $b \neq 0$, gleichzeitig $pb = p^j c - rp^k a = p^j c - r_1 a = 0$. Wir müssen $Ra \cap Rb = \{0\}$ zeigen. Wäre $Ra \cap Rb \neq \{0\}$, so gäbe es ein $s \in R$ mit $0 \neq sb \in Ra$. Da aber $pb = 0$, kann s kein Vielfaches von p sein. Daher sind s und p zueinander teilerfremd, und es gibt $x, y \in R$ mit $1_R = sx + py$. Damit erhält man

$$b = 1_R b = sxb + pyb = x(sb) \in Ra,$$

Widerspruch.

Zu Punkt (b): Sei $U \leq A$ maximal mit $U \cap Ra = \{0\}$. Die Existenz eines solchen U folgt in der üblichen Weise aus dem Lemma von Zorn. Nach Proposition 3.3.2.9 (oder alternativ Folgerung 3.3.2.10 bzw. Satz 3.3.2.11) ist $A_0 := U + Ra = U \oplus Ra$. Somit bleibt lediglich $A_0 = A$ zu zeigen. Dazu gehen wir indirekt vor:
Angenommen es wäre $A_0 \neq A$. Dann ist der von $a + U$ im Faktormodul A/U erzeugte zyklische Untermodul nicht ganz A/U. Außerdem hat $a + U$ in A/U die Ordnung p^n, was unter den p-Elementen in A/U sicher maximal ist. Nach Teil (a), angewendet auf A/U statt A und $a+U$ statt a, gibt es folglich ein $b \in A \setminus U$ mit $\langle a+U \rangle \cap \langle b+U \rangle = \{U\}$. Damit wäre der Untermodul $U' := U + Rb \leq A$ eine echte Obermenge von U, die außerdem $U' \cap Ra = \{0\}$ erfüllt (denn wenn $u + rb = r'a$ für $u \in U$ und $r, r' \in R$ ist, so folgt $rb + U = r'a + U \in \langle a + U \rangle \cap \langle b + U \rangle = U$, also $rb \in U$ und daher $u + rb = r'a \in U \cap Ra = \{0\}$). Dies ist ein Widerspruch zur Maximalität von U, sodass $A_0 = A$ gelten muss. □

Im endlich erzeugten Fall können wir damit die gewünschte direkte Zerlegung eines p-Moduls in zyklische Summanden herleiten:

Satz 7.4.4.3. *Ist A ein endlich erzeugter p-primärer R-Modul für ein $p \in \mathbb{P}$, dann gilt $A \cong \bigoplus_{i=1}^{k} R/p^{n_i}R$ mit $k \in \mathbb{N}$ und $n_1 \geq \ldots \geq n_k \geq 1$.*

Beweis. Wir führen den Beweis durch Induktion nach der Anzahl m der Erzeugenden $a_1, \ldots, a_m$ von A. Der Fall $m = 1$ ist trivial. Gelte nun die Aussage für $m-1$ und werde A von $a_1, \ldots, a_m \in A$ mit $\mathcal{O}_{a_i} = (p^{\tilde{n}_i})$ für $i = 1, \ldots, m$ erzeugt. OBdA sei $n_1 := \tilde{n}_1$ maximal unter den $\tilde{n}_i$. Dann ist $p^{n_1}A = \{0\} \neq p^{n_1-1}A$. Lemma 7.4.4.2 liefert daher einen Untermodul $C \leq A$ mit $A = Ra_1 \oplus C$. Sei $\pi : A \to C$, $ra_1 + c \mapsto c$ für $r \in R$ und $c \in C$ die dieser direkten Zerlegung entsprechende Projektion auf C. Dann wird C von den Bildern $\pi(a_1), \pi(a_2), \ldots, \pi(a_m)$ erzeugt, wobei wegen $\pi(a_1) = 0$ mit $\{\pi(a_2), \ldots, \pi(a_m)\}$ sogar ein $(m-1)$-elementiges Erzeugendensystem von C vorliegt. Laut Induktionsannahme gibt es folglich eine direkte Zerlegung von C, die wir aus notationellen Gründen in der Form

$$C \cong \bigoplus_{i=2}^{k} R/p^{n_i}R$$

anschreiben. Wegen $Ra_1 \cong R/p^{n_1}R$ erhalten wir also insgesamt die Behauptung

$$A = Ra_1 \oplus C \cong \bigoplus_{i=1}^{k} R/p^{n_i}R.$$

□

7.4.5 Abschluss des Beweises des Hauptsatzes

Der Beweis des Hauptsatzes 7.4.3.1 über endlich erzeugte R-Moduln über einem Hauptidealring R ist nun recht schnell vervollständigt, wie die folgende Beweisskizze zeigt:

Skizze der verbleibenden Beweisteile von Satz 7.4.3.1: Zuerst zur Existenz einer Zerlegung wie in Satz 7.4.3.1(a): Die Sätze 7.4.2.9, 7.4.4.1 und 7.4.4.3 liefern eine Darstellung wie in (a), wobei wegen „endlich erzeugt“ nur endlich viele Summanden $\neq 0$ auftreten können. Die Darstellung aus (b) erhält man durch geeignetes Zusammensetzen von Faktoren $R/p_j^{e_j}R$, $j = 1, \ldots, s$, zu $R/rR \cong \bigoplus_{j=1}^{s} R/p_j^{e_j}R$ mit $r = \prod_{j=1}^{s} p_j^{e_j}$ aus dem Chinesischen Restsatz 3.4.7.1, wenn man sich klar macht, dass die Ringisomorphie des Chinesischen Restsatzes auch die Modulisomorphie liefert.
Zur Eindeutigkeit einer Zerlegung wie in 7.4.3.1(a): A_t ist eindeutig bestimmt, somit muss der Rang von F gleich dem Rang von A/A_t sein (Dimensionsinvarianz, Satz 7.2.2.4). Innerhalb A_t sind die $A(p)$ als p-Anteile ebenfalls eindeutig bestimmt. Für (a) zu zeigen bleibt daher noch: Für p-primäre A sind die e_n in $A \cong \bigoplus_{n=1}^{N}(R/p^nR)^{e_n}$ eindeutig bestimmt. Setzen wir $A[l] := \{a \in A \mid l \cdot a = 0\}$ (siehe auch Beispiel 7.4.5.2), so ist die Dimension von $A[p^m]/A[p^{m-1}]$ über dem Körper R/pR genau $\sum_{k \geq m} e_k$. Daraus folgt die gesuchte Eindeutigkeit der e_n. Verwendet man die oben angedeutete Isomorphie $R/rR \cong \bigoplus_{j=1}^{s} R/(p_j^{e_j}R)$ mit $r = \prod_{j=1}^{s} p_j^{e_j}$, so erhält man auch die Eindeutigkeitsaussage für die Darstellung in 7.4.3.1(b). □

UE 32 ▶ **Übungsaufgabe 7.4.5.1.** (V) Arbeiten Sie obige Beweisskizze vollständig aus. Insbesondere sind die Anwendung des Chinesischen Restsatzes, die Übersetzung zwischen den Darstellungen aus (a) und (b) sowie die Eindeutigkeitsaussagen ausführlich zu begründen. ◀ **UE 32**

Beispiel 7.4.5.2. Zur näheren Erläuterung der $A[l]$ aus obigem Beweis.
Sei $A = \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8$, $R = \mathbb{Z}$ und $p = 2$. Dann ist $R/pR \cong \mathbb{Z}_2$ und

$$\begin{aligned} A[1] &= \{0\}, \\ A[2] &\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \\ A[4] &\cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \text{ und} \\ A[8] &= \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8 = A. \end{aligned}$$

Dabei ist $\dim_{\mathbb{Z}_2}(A[2]/A[1]) = 4 = e_1 + e_2 + e_3$, $\dim_{\mathbb{Z}_2}(A[4]/A[2]) = 3 = e_2 + e_3$ und $\dim_{\mathbb{Z}_2}(A[8]/A[4]) = 1$, also $e_1 = 1, e_2 = 2$ und $e_3 = 1$.

7.4.6 Eine Anwendung des Hauptsatzes: Jordansche Normalformen

Ein Beispiel für eine Anwendung des Hauptsatzes 7.4.3.1 auf Moduln über einem Hauptidealring $R \neq \mathbb{Z}$ (und damit nicht schlicht auf abelsche Gruppen) liefert ein Ergebnis, das aus der Linearen Algebra bekannt ist: die Jordansche Normalform eines Endomorphismus eines endlichdimensionalen Vektorraums. Wie diese beiden Themen in Zusammenhang gebracht werden können, soll nun sehr kurz und nur andeutungsweise skizziert werden.

Sei V ein n-dimensionaler Vektorraum über einem Körper K und $\varphi : V \to V$ linear, also ein Endomorphismus von V. Weil die Endomorphismen von V sogar eine Algebra bilden, induziert jedes Polynom $f \in K[x]$ über K die lineare Abbildung $f_\varphi := f(\varphi)$. Diese lässt sich auf Elemente $x \in V$ anwenden. Wir betrachten nun die Abbildung

$$\cdot_\varphi : K[x] \times V \to V, \quad (f, x) \mapsto f_\varphi(x).$$

Sie macht V zu einem endlich erzeugten $K[x]$-Modul. Da jeder Polynomring über einem Körper ein Hauptidealring ist (siehe Unterabschnitt 5.2.3), lässt sich der Hauptsatz 7.4.3.1 anwenden. Um zu verstehen, was seine Aussage im vorliegenden Kontext bedeutet, hat man sich zum Beispiel zu überlegen, was zyklische Unter-$K[x]$-Moduln von V sind etc. Führt man all diese Überlegungen durch, kommt man zu direkten Zerlegungen des Vektorraumes V in sogenannte φ-zyklische Unterräume, aus denen man sich Basen konstruieren kann, bezüglich derer man φ auf Normalform bringen kann.

UE 33 ▶ **Übungsaufgabe 7.4.6.1.** (V,E,D) Arbeiten Sie diese Ansätze aus. ◀ **UE 33**

7.5 Hom-Funktor und Dualität

Es überrascht nicht, dass das Konzept des Dualraums V^* eines Vektorraums V über einem Körper K, d.h. des Vektorraums aller linearen Funktionale $f\colon V \to K$ aus der Linearen Algebra bzw. Funktionalanalysis, auf Moduln über einem Ring R verallgemeinert werden kann. Allerdings müssen mancherlei Komplikationen beachtet werden, vor allem für den Fall, dass R nicht kommutativ ist. Dies sowie daran anschließende Konzepte sind Gegenstand des vorliegenden Abschnitts, des letzten zur Modultheorie.
In 7.5.1 wird ein hinreichend weiter begrifflicher Rahmen gesteckt. Insbesondere wird der Hom-Funktor eingeführt. Die Komplikationen bei Nichtkommutativität werden in 7.5.2 behandelt. Es folgen das Konzept des dualen Moduls in 7.5.3 und des Tensorproduktes in 7.5.4. Abschnitt und Kapitel schließen in 7.5.5 mit dem allgemeinen Begriff einer Algebra über einem Ring.

7.5.1 Die abelsche Gruppe $\mathrm{Hom}_R(A,B)$ und der Hom-Funktor

Wir beginnen mit einer sehr allgemeinen Situation, zunächst sogar unabhängig von jeglicher algebraischen Struktur.

Definition 7.5.1.1. Seien A, B, C, D beliebige Mengen. Gegeben seien zwei Abbildungen $\varphi\colon C \to A$ und $\psi\colon B \to D$. Für $f : A \to B$ sei $\theta(f) := \psi \circ f \circ \varphi : C \to D$.

$$C \xrightarrow{\varphi} A \xrightarrow{f} B \xrightarrow{\psi} D$$

Dadurch ist eine Abbildung $\theta\colon B^A \to D^C$ definiert. (Die Potenzschreibweise B^A steht wie üblich für die Menge aller Abbildungen von A nach B.)
Seien A, B, C, D Moduln über einem Ring R und φ, ψ entsprechend R-Modulhomomorphismen. Schränkt man θ auf die bezüglich der punktweisen Addition abelsche Gruppe $\mathrm{Hom}_R(A,B)$ aller R-Homomorphismen $f\colon A \to B$ ein, so nennt man diese Einschränkung

$$\mathrm{Hom}(\varphi,\psi) := \theta|_{\mathrm{Hom}(A,B)} : \mathrm{Hom}(A,B) \to \mathrm{Hom}(C,D), \quad f \mapsto \psi \circ f \circ \varphi$$

den von φ und ψ *induzierten Homomorphismus.*
Ist, noch spezieller, $B = D$ und $\psi = \mathrm{id}_B$, so ist $\theta : f \mapsto f \circ \varphi$, und wir schreiben für den Homomorphismus $\mathrm{Hom}(\varphi,\psi)$ auch $\bar{\varphi}$; im Fall $A = C$, $\varphi = \mathrm{id}_C$ und somit $\theta : f \mapsto \psi \circ f$ schreiben wir entsprechend $\bar{\psi}$.

Man beachte: $\mathrm{Hom}_R(A,B)$ ist eine Menge von R-Modulhomomorphismen. Hingegen ist $\mathrm{Hom}(\varphi,\psi)$ selbst ein Homomorphismus (zwischen abelschen Gruppen), der auf der Menge $\mathrm{Hom}_R(A,B)$ definiert ist.

Proposition 7.5.1.2. *Mit der Notation aus Definition 7.5.1.1 gilt:*

1. $\mathrm{Hom}_R(A,B)$ *ist (wie in Definition 7.5.1.1 implizit behauptet) eine abelsche Gruppe bezüglich der punktweisen Addition* $(f+g)(a) := f(a) + g(a)$.

2. $\mathrm{Hom}_R(A,B)$ *ist bezüglich der punktweisen Definition* $(rf)(a) := rf(a)$ *im Allgemeinen* kein *R-Linksmodul.*

3. *Bei geeigneter (natürlicher) Wahl der Definitions- und Zielmengen der involvierten Abbildungen gilt:* $\mathrm{Hom}(\varphi\varphi', \psi'\psi) = \mathrm{Hom}(\varphi', \psi')\,\mathrm{Hom}(\varphi, \psi)$

Beweis. Übungsaufgabe. □

UE 34 ► Übungsaufgabe 7.5.1.3. (V) Beweisen Sie Satz 7.5.1.2. Als Hinweis für die zweite Aussage sei lediglich die Möglichkeit **◄ UE 34**

$$(r_1 f)(r_2 a) = r_1 f(r_2 a) = r_1 r_2 f(a) \neq r_2 r_1 f(a) = r_2((r_1 f)(a))$$

hervorgehoben.

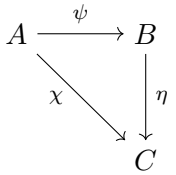
Mehr Klarheit schafft die kategorientheoretische Betrachtungsweise, siehe auch Abschnitt 2.3: Gegeben sei ein Ring R (mit oder ohne 1) und ein R-Modul D (unitär oder auch nicht). Im kovarianten Fall wird jedem R-Modul A die abelsche Gruppe $\mathrm{Hom}_R(D,A)$ und jedem R-Homomorphismus $\psi : A \to B$ der induzierte Homomorphismus

$$\bar{\psi} : \mathrm{Hom}_R(D,A) \to \mathrm{Hom}_R(D,B), \quad f \mapsto \psi \circ f$$

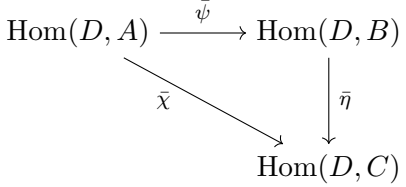
zugeordnet. Diese Zuordnung ist, wie man leicht nachprüft, ein Funktor, der von D induzierte *kovariante Hom-Funktor* $A \mapsto \mathrm{Hom}_R(D,A)$, $\psi \mapsto \bar{\psi}$.
Im kontravarianten Fall wird dem R-Modul A statt der abelschen Gruppe $\mathrm{Hom}_R(D,A)$ entsprechend die abelsche Gruppe $\mathrm{Hom}_R(A,D)$ zugeordnet, und ein Homomorphismus $\varphi : A \to B$ geht in den induzierten Homomorphismus

$$\bar{\varphi} : \mathrm{Hom}_R(A,D) \to \mathrm{Hom}_R(B,D), \quad f \mapsto f \circ \varphi$$

über. Man erhält so den *kontravarianten Hom-Funktor* $A \mapsto \mathrm{Hom}_R(A,D)$, $\varphi \mapsto \bar{\varphi}$.
Wie meist in der Kategorientheorie kann man das Spiel weitertreiben. Wir wollen auch kommutative Diagramme von R-Moduln und R-Modulhomomorphismen betrachten. Dazu gibt man sich einen Graphen Γ vor. Die Objekte einer neuen Kategorie sind dann kommutative Diagramme von R-Moduln über Γ. Als Morphismen zwischen zwei solchen Objekten dienen dann Familien von R-Modulhomomorphismen, die entsprechende Knoten verbinden und insgesamt wieder ein kommutatives Diagramm liefern. Bei gegebenem R-Modul D induzieren ko- wie auch kontravarianter Hom-Funktor auf Modulebene je einen entsprechenden Funktor auf Diagrammebene, zum Beispiel wird aus



im kovarianten Fall das Diagramm



Für die Modultheorie (und, darauf aufbauend, für die homologische Algebra, die wir aber nicht vertiefen werden) sind, wie wir wissen, Sequenzen S von besonderer Bedeutung, etwa von der Form $S:\ 0 \to A \to B \to C \to 0$. Weil in ihnen keine Kreise auftreten, lassen sie sich automatisch als kommutative Diagramme deuten, und alle Konstruktionen sind sinnvoll.

UE 35 ► **Übungsaufgabe 7.5.1.4.** (F) Rekapitulieren Sie die erforderlichen kategorientheoretischen Begriffe, um die angedeutete Konstruktion ausführlich zu beschreiben. Begründen Sie auch, warum man tatsächlich wieder Kategorien bzw. Funktoren erhält. ◄ **UE 35**

In den folgenden Untersuchungen werden wir uns auf sehr einfache Beispiele beschränken und nur einige wenige Tatsachen erwähnen, die einen ersten Eindruck von homologischer Algebra geben mögen.
Konzentrieren wir uns zunächst auf einen R-Modulhomomorphismus $\psi : A \to B$. Bei Vorgabe eines weiteren R-Moduls D induziert ψ gemäß Definition 7.5.1.1 einen Homomorphismus $\bar{\psi} : \mathrm{Hom}_R(D, A) \to \mathrm{Hom}_R(D, B)$, definiert durch $f \mapsto \psi \circ f$. Entsprechend geht die Sequenz $S : 0 \to A \to B \to D \to 0$ von R-Moduln in eine Sequenz

$$S_D :\ 0 \to \mathrm{Hom}_R(D, A) \to \mathrm{Hom}_R(D, B) \to \mathrm{Hom}_R(D, C) \to 0$$

abelscher Gruppen über, die wir die (von S durch D) *induzierte Sequenz* nennen.
Dual dazu kann man D statt als Definitions- auch als Zielbereich von Modulhomomorphismen einsetzen. Dann induziert jedes $\varphi : A \to B$ gemäß Definition 7.5.1.1 einen Homomorphismus $\bar{\varphi} : \mathrm{Hom}_R(B, D) \to \mathrm{Hom}_R(A, D)$, definiert durch $f \mapsto f \circ \varphi$. Entsprechend geht die Sequenz $S :\ 0 \to A \to B \to C \to 0$ von R-Moduln in eine Sequenz

$$S^*_D :\ 0 \to \mathrm{Hom}_R(C, D) \to \mathrm{Hom}_R(B, D) \to \mathrm{Hom}_R(A, D) \to 0$$

über. Zur Unterscheidung der beiden von D induzierten Sequenzen S_D und S^*_D könnte man S_D die *ko-* und S^*_D die *kontravariant* induzierte Sequenz nennen.

Wir begnügen uns mit den folgenden Aussagen über die Verträglichkeit der Hom-Funktoren mit diversen Konstruktionen und der Exaktheit von Sequenzen. Die Beweise sind mit Hilfe der bereits verfügbaren Theorie nicht sehr schwierig, erfordern insgesamt aber beträchtlichen Aufwand. Wir verlagern sie in Übungsaufgaben.

Proposition 7.5.1.5. *Alle nachfolgenden Aussagen beziehen sich, wenn nicht anders spezifiziert, auf die Kategorie der (unitären) Moduln über einem Ring R (mit 1).*

1. *Die Sequenz*
$$S: \ 0 \to A \to B \to C$$
von R-Moduln ist genau dann exakt, wenn die kovariant induzierte Sequenz
$$S_D: \ 0 \to \mathrm{Hom}_R(D, A) \to \mathrm{Hom}_R(D, B) \to \mathrm{Hom}_R(D, C)$$
abelscher Gruppen für alle R-Moduln D exakt ist.

2. *Die Sequenz*
$$S: \ A \to B \to C \to 0$$
von R-Moduln ist genau dann exakt, wenn die kontravariant induzierte Sequenz
$$S_D^*: \ 0 \to \mathrm{Hom}_R(C, D) \to \mathrm{Hom}_R(B, D) \to \mathrm{Hom}_R(A, D)$$
abelscher Gruppen für alle R-Moduln D exakt ist.

3. *Für die Sequenz*
$$S: \ 0 \to A \to B \to C \to 0$$
von R-Moduln sind die folgenden drei Bedingungen äquivalent:
   a) *S ist kurzexakt und zerfällt.*
   b) *Die kovariant induzierte Sequenz*
   $$S_D: \ 0 \to \mathrm{Hom}_R(D, A) \to \mathrm{Hom}_R(D, B) \to \mathrm{Hom}_R(D, C) \to 0$$
   ist kurzexakt und zerfällt für alle R-Moduln D.
   c) *Die kontravariant induzierte Sequenz*
   $$S_D^*: \ 0 \to \mathrm{Hom}_R(C, D) \to \mathrm{Hom}_R(B, D) \to \mathrm{Hom}_R(A, D) \to 0$$
   ist kurzexakt und zerfällt für alle R-Moduln D.

4. *Für einen R-Modul P sind äquivalent:*
   a) *P ist projektiv.*
   b) *Jeder surjektive Homomorphismus $\psi : B \to C$ induziert kovariant einen surjektiven Homomorphismus $\bar{\psi} : \mathrm{Hom}_R(P, B) \to \mathrm{Hom}_R(P, C)$ abelscher Gruppen.*
   c) *Jede kurzexakte Sequenz*
   $$S: \ 0 \to A \to B \to C \to 0$$
   von R-Moduln induziert kovariant eine gleichfalls kurzexakte Sequenz
   $$S_P: \ 0 \to \mathrm{Hom}_R(P, A) \to \mathrm{Hom}_R(P, B) \to \mathrm{Hom}_R(P, C) \to 0$$
   abelscher Gruppen.

5. *Für einen R-Modul J sind äquivalent:*
   a) *J ist injektiv.*
   b) *Jeder injektive Homorphismus $\varphi : A \to B$ induziert kontravariant einen surjektiven Homomorphismus $\bar{\varphi} : \mathrm{Hom}_R(B, J) \to \mathrm{Hom}_R(A, J)$ abelscher Gruppen.*
   c) *Jede kurzexakte Sequenz*

$$S : \ 0 \to A \to B \to C \to 0$$

   von R-Moduln induziert kontravariant eine gleichfalls kurzexakte Sequenz

$$S_J^* : \ 0 \to \mathrm{Hom}_R(C, J) \to \mathrm{Hom}_R(B, J) \to \mathrm{Hom}_R(A, J) \to 0$$

   abelscher Gruppen.

6. *Für R-Moduln A, B, A_i $(i \in I)$ und B_j $(j \in J)$ gelten folgende Isomorphien abelscher Gruppen:*
   a) $\mathrm{Hom}_R(\bigoplus_{i\in I} A_i, B) \cong \prod_{i\in I} \mathrm{Hom}_R(A_i, B)$
   b) $\mathrm{Hom}_R(A, \prod_{j\in J} B_j) \cong \prod_{j\in J} \mathrm{Hom}_R(A, B_j)$

UE 36 ▶ Übungsaufgabe 7.5.1.6. (V) Beweisen Sie Proposition 7.5.1.5. **◀ UE 36**

7.5.2 Rechts-, Links- und Bimoduln

Für R-Moduln A, B wollen wir die abelsche Gruppe $\mathrm{Hom}_R(A, B)$ strukturell anreichern und selbst zu einem R-Modul machen. Es überrascht kaum, dass dies möglich ist. Allerdings ist dabei Vorsicht nötig, um eine mögliche Nichtkommutativität von R und die daraus resultierende Unterscheidung zwischen Links- und Rechtsmoduln zu berücksichtigen (siehe beispielsweise Aussage 2 in Proposition 7.5.1.2).

Definition 7.5.2.1. Seien R und S Ringe und A eine abelsche Gruppe, die sowohl R-Links- als auch S-Rechtsmodul ist. Dann nennen wir A einen *R-S-Bimodul*, sofern

$$r(as) = (ra)s$$

für alle $r \in R$, $a \in A$ und $s \in S$ gilt. Wir verwenden die Schreibweisen ${}_RB$, ${}_RA_S$ und C_S, um anzudeuten, dass B ein R-Links-, A ein R-S-Bi- und C ein S-Rechtsmodul ist.

Klarerweise wird jeder Linksmodul A über einem kommutativen Ring R durch die Festsetzung $ar := ra$ für $r \in R$ und $a \in A$ zu einem R-R-Bimodul. Aus $r(as) = r(sa) = (rs)a$ und $(ra)s = s(ra) = (sr)a$ ersieht man allerdings, dass hier die Kommutativität essenziell ist. Allein wegen der Assoziativität der Multiplikation hingegen, also unabhängig von Kommutativität, ist jeder Ring R ein R-R-Bimodul.
Die angekündigte Modulstruktur auf $\mathrm{Hom}_R(A, B)$ lässt sich folgendermaßen beschreiben.

Proposition 7.5.2.2. *Über den Ringen R und S seien die Moduln ${}_RA$, ${}_RB_S$, ${}_RC_S$ und ${}_RD$ gegeben. Dann gilt:*

1. $\mathrm{Hom}_R(A,B)$ *wird zu einem S-Rechtsmodul, wenn man für $a \in A$, $s \in S$ und $f \in \mathrm{Hom}_R(A,B)$ definiert:* $(fs)(a) := (f(a))s$.
2. *Jeder Homomorphismus $\varphi\colon A \to A'$ von R-Links-Moduln induziert einen Homomorphismus $\bar{\varphi}\colon \mathrm{Hom}_R(A',B) \to \mathrm{Hom}_R(A,B)$ von S-Rechts-Moduln.*
3. $\mathrm{Hom}_R(C,D)$ *wird zu einem S-Linksmodul, wenn man für $c \in C$, $s \in S$ und $g \in \mathrm{Hom}_R(C,D)$ definiert:* $(sg)(c) := g(cs)$.
4. *Jeder Homomorphismus $\psi\colon D \to D'$ von R-Links-Moduln induziert einen Homomorphismus $\bar{\psi}\colon \mathrm{Hom}_R(C,D) \to \mathrm{Hom}_R(C,D')$ von S-Links-Moduln.*
5. *Ist R kommutativ und fassen wir A und B als R-R-Bimoduln auf, so ist auch $\mathrm{Hom}_R(A,B)$ ein R-R-Bimodul.*

UE 37 ► **Übungsaufgabe 7.5.2.3.** (V) Beweisen Sie Proposition 7.5.2.2 und geben Sie eine ◄ **UE 37** funktorielle Deutung.

Ein nützliche Beobachtung an einem R-Linksmodul A ist die Isomorphie

$$A \cong \mathrm{Hom}_R(R,A) \quad \text{via} \quad a \mapsto f_a \quad \text{mit} \quad f_a(r) := ra,$$

sofern R ein Einselement hat und A als R-Modul unitär ist. Betrachtet man $\mathrm{Hom}_R(A,R)$ statt $\mathrm{Hom}_R(R,A)$, so erhält man den zu A dualen R-Rechtsmodul. Ihm gilt nun unser Interesse.

7.5.3 Duale Moduln

Ist A ein Linksmodul über dem Ring R, so ist $A^* := \mathrm{Hom}_R(A,R)$ nach Proposition 7.5.2.2 ein R-Rechtsmodul über R. Etwas ausführlicher:

Definition 7.5.3.1. Sei A ein R-Linksmodul. Dann ist $\mathrm{Hom}_R(A,R)$ ein R-Rechtsmodul bzgl.

$$\begin{aligned}(f_1+f_2)(a) &= f_1(a) + f_2(a)\\ (fr)(a) &= f(a)\cdot r,\end{aligned}$$

genannt der *duale Modul,* in Zeichen A^*. Jedes $f \in A^*$ heißt auch *lineares Funktional.* Sei B ein weiterer R-Linksmodul. Für $\varphi \in \mathrm{Hom}_R(A,B)$ heißt

$$\begin{aligned}\varphi^*\colon B^* &\to A^*\\ f &\mapsto f\circ\varphi\end{aligned}$$

die *duale Abbildung.*

Geht man von einem R-Rechtsmodul aus, so werden die dualen Moduln in analoger Weise zu R-Linksmoduln. Somit führt Iteration der Konstruktion von einem R-Linksmodul A wieder zu einem R-Linksmodul A^{**}, von einem R-Rechtsmodul A wieder zu einem R-Rechtsmodul A^{**}. In beiden Fällen heißt A^{**} der *biduale Modul* zu A.
Die *natürliche Abbildung* Φ ist durch

$$\Phi : A \to A^{**},\ a \mapsto a^{**} \quad \text{mit} \quad a^{**} : A^* \to R,\ f \mapsto f(a)$$

definiert. Ist Φ ein Isomorphismus, so heißt A *reflexiv*.

Proposition 7.5.3.2. *Sei R ein Ring. Die Zuordnung $.^*$ führe einen R-Linksmodul A in sein Dual (den R-Rechtsmodul A^*) über sowie einen Homomorphismus $f\colon A \to B$ von R-Linksmoduln in den Homomorphismus $f^*\colon B^* \to A^*$ (die zu f duale Abbildung). Dann ist $.^*$ ein kontravarianter Funktor von der Kategorie der R-Linksmoduln in die Kategorie der R-Rechtsmoduln. Folglich ist die Iteration $A \mapsto A^{**}$, $f \mapsto f^{**}$ ein kovarianter Funktor von der Kategorie der R-Linksmoduln (bzw. der R-Rechtsmoduln) in sich selbst.*

UE 38 ► Übungsaufgabe 7.5.3.3. (V) Zeigen Sie Proposition 7.5.3.2. **◄ UE 38**

Von Interesse sind die in folgender Übungsaufgabe behandelten Gesichtspunkte und Sachverhalte.

UE 39 ► Übungsaufgabe 7.5.3.4. (F) **◄ UE 39**

(1) Zeigen Sie: $(A \oplus B)^* \cong A^* \oplus B^*$

(2) Zeigen Sie: Ist R ein Divisionsring, dann führt $.^*$ kurzexakte Sequenzen von Vektorräumen über R in kurzexakte Sequenzen über.

(3) Beschreiben Sie F^* für einen freien R-Linksmodul F. Ist F^* ebenfalls frei? (Hierzu wäre eine „duale“ Basis zu finden.)

(4) Zeigen Sie: Hat R ein Einselement, und ist der unitäre R-Linksmodul F frei, so ist die natürliche Abbildung von F nach F^{**} eine Einbettung.

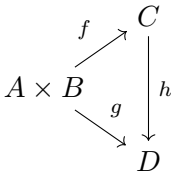
(5) Besitzt überdies F sogar eine endliche Basis, so ist F reflexiv.

7.5.4 Das Tensorprodukt

Sei A ein Rechts-R-Modul und B ein Links-R-Modul. Das *Tensorprodukt* $A \otimes_R B$ ist definiert als initiales Objekt in der folgenden Kategorie $\mathcal{M}(A, B)$:
Die Objekte von $\mathcal{M}(A, B)$ sind die sogenannten *mittellinearen Abbildungen*, genauer: Paare (f, C) mit Abbildungen $f\colon A \times B \to C$ in eine abelsche Gruppe C, die den Gleichungen

$$\begin{aligned} f(a_1 + a_2, b) &= f(a_1, b) + f(a_2, b) \\ f(a, b_1 + b_2) &= f(a, b_1) + f(a, b_2) \\ f(ar, b) &= f(a, rb) \end{aligned}$$

genügen. Ist R kommutativ, so lassen sich die mittellinearen Abbildungen durch *bilineare* Abbildungen ersetzen: $f(ar, b) = rf(a, b) = f(a, rb)$
Die Menge $\mathrm{Hom}_{\mathcal{M}(A,B)}(f, g)$ der Morphismen von f nach g in der Kategorie $\mathcal{M}(A, B)$ ist die Menge aller Gruppenhomomorphismen $h\colon C \to D$, für die das Diagramm



kommutiert. Komposition in $\mathcal{M}(A, B)$ ist die Abbildungskomposition.

Eine alternative Beschreibung des Tensorprodukts lautet wie folgt: Sei F die freie abelsche Gruppe über der Menge $A \times B$ und K die von allen Elemente

$$(a_1 + a_2, b) - (a_1, b) - (a_2, b),$$
$$(a, b_1 + b_2) - (a, b_1) - (a, b_2) \text{ und}$$
$$(ar, b) - (a, rb)$$

erzeugte Untergruppe. Dann ist $A \otimes_R B \cong F/K$.

UE 40 ► **Übungsaufgabe 7.5.4.1.** (V) Zeigen Sie, dass die abelsche Gruppe F/K tatsächlich als initiales Objekt in $\mathcal{M}(A, B)$ aufgefasst werden kann. ◄ **UE 40**

Elemente des so definierten Tensorproduktes schreiben wir als $a \otimes b := (a, b) + K$ an.

UE 41 ► **Übungsaufgabe 7.5.4.2.** (F) A, B seien (Links-) Moduln über dem Ring R. ◄ **UE 41**

1. Formulieren und beweisen Sie die folgenden Rechengesetze:
   $(a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \otimes b$, $a \otimes (b_1 + b_2) = a \otimes b_1 + a \otimes b_2$, $(ra) \otimes b = a \otimes (rb)$
2. Wir nehmen an, die Elemente $a_i, i \in I$, bilden ein Erzeugendensystem von A, die b_j, $j \in J$ ein Erzeugendensystem von B. Zeigen Sie, dass sich dann jedes Element von $A \otimes B$ als $\sum_{i,j} n_{i,j}(a_i \otimes b_i)$ mit $n_{i,j} \in \mathbb{Z}$ schreiben lässt, wobei nur endlich viele $n_{i,j}$ von 0 verschieden sind.
3. Unter welchen Bedingungen ist diese Darstellung eindeutig?

Ist R kommutativ, so können A und B als Bimoduln aufgefasst und auf dem Tesorprodukt $A \otimes B$ eine Operation $R \times (A \otimes B) \to A \otimes B$, $(r, a \otimes b) \mapsto ra \otimes b$ mit $r(a \otimes b) = (ra) \otimes b = a \otimes (rb)$ definiert werden, die das Tensorprodukt wieder zu einem R-Modul macht.

UE 42 ► **Übungsaufgabe 7.5.4.3.** (F) Führen Sie diesen Ansatz aus, insbesondere für den Fall, dass $R = K$ ein Körper ist. Dann sind A und B Vektorräume. Was kann über die Dimension von $A \otimes B$ ausgesagt werden? ◄ **UE 42**

7.5.5 Algebren

Definition 7.5.5.1. Sei A ein Ring, K ein Ring mit 1 zusammen mit einer Abbildung $\cdot : K \times A \to A$. A heißt eine *K-Algebra*, wenn gilt:

(i) $(A, +)$ ist bezüglich $\cdot$ ein unitärer (Links-) K-Modul und

(ii) $k \cdot (ab) = (k \cdot a)b = a(k \cdot b)$ für alle $k \in K$, $a, b \in A$.

Eine K-Algebra, die ein Divisionsring ist, nennt man *Divisionsalgebra.* Im klassischen Fall ist K ein Körper, also A ein Vektorraum.

Ohne die Theorie der Algebren zu vertiefen begnügen wir uns mit der Angabe einiger wichtiger Beispiele:

Beispiel 7.5.5.2. Folgende Strukturen sind Algebren:

(a) Jeder Ring ist auch eine $\mathbb{Z}$-Algebra.

(b) $K[x_1, \ldots, x_n]$ und $K[[x_1, \ldots, x_n]]$ über einem Körper K.

(c) $\mathrm{Hom}_K(V, V)$ für einen Vektorraum über einem Körper K.

(d) Ist A ein Ring mit 1 und K ein Unterring des Zentrums von A mit $1 \in K$, dann ist A eine K-Algebra, wobei die K-Modul-Struktur gegeben ist durch die Multiplikation in A.

(e) Der Divisionsring der Quaternionen $\mathbb{H}$ und auch der Körper der komplexen Zahlen $\mathbb{C}$ sind Divisionsalgebren über $\mathbb{R}$.

(f) Sei G eine Gruppe und K ein kommutativer Ring mit 1. Dann ist der Gruppenring $K(G)$ (siehe Unterabschnitt 4.2.4) eine K-Algebra, wobei die K-Modul-Struktur gegeben ist durch
$$k\left(\sum r_i g_i\right) = \sum (k r_i) g_i$$
für $k, r_i \in K$, $g_i \in G$. Diese Algebra $K(G)$ nennt man die *Gruppenalgebra* von G über K.

(g) Ist K ein kommutativer Ring mit 1, dann ist der Matrizenring $\mathrm{Mat}_n(K)$ aller $n \times n$-Matrizen eine K-Algebra.

8 Vertiefung der Gruppentheorie

In einführenden Kapiteln haben wir lediglich grundlegende Konzepte der Gruppentheorie kennengelernt, wobei als wichtigstes das des Normalteilers zu nennen ist. Unser Verständnis der Struktur von Gruppen geht noch kaum über den Cayleyschen Darstellungssatz (jede Gruppe G ist isomorph zu einer Permutationsgruppe auf der Trägermenge von G) und, für endliche Gruppen, den Satz von Lagrange (die Ordnung einer Untergruppe teilt die Gruppenordnung) hinaus. In Abschnitt 3.3 und Kapitel 7 haben wir die Struktur von abelschen Gruppen und, allgemeiner, von Moduln untersucht. Das vorliegende Kapitel bringt Vertiefungen insbesondere für den nichtabelschen Fall, wobei in den ersten beiden Abschnitten endliche Gruppen im Zentrum des Interesses stehen. Ziel in 8.1 sind vor allem die für die Strukturtheorie endlicher Gruppen grundlegenden Sylowsätze, wobei es sich als fruchtbar erweist, zunächst sogenannte Aktionen auch von beliebigen Gruppen in den Fokus zu nehmen. Abschnitt 8.2 versammelt einige Beispiele von Gruppen unter den vorangegangenen allgemeineren Gesichtspunkten. Für Gruppen der Ordnung ≤ 15 ergibt sich eine vollständige Klassifikation. In 8.3 geht es um Nilpotenz, Auflösbarkeit und Subnormalreihen. Das sind Begriffsbildungen, die um die Frage kreisen, wie weit und in welchem Sinn eine Gruppe davon entfernt ist, abelsch zu sein. Die beiden darauffolgenden Abschnitte konzentrieren sich auf die (bereits im Zusammenhang mit Normalreihen aufgetauchte) Frage, wie man sich komplizierte Gruppen eventuell aus einfacheren aufgebaut denken kann. In 8.4 ist das im Sinne von sogenannten Gruppenerweiterungen zu verstehen, in 8.5 über den Satz von Krull-Schmidt im Sinne von direkten Produkten.

8.1 Gruppenaktionen und Sylowsätze

Wir beginnen den Abschnitt in 8.1.1 mit dem weit über die Theorie endlicher Gruppen hinaus bedeutsamen Begriff der *Wirkung* oder *Aktion* einer Gruppe, stoßen dabei auf die Klassengleichung und spezialisieren in 8.1.2 auf den Spezialfall der Konjugation. Das erste darauf fußende bemerkenswerte Resultat ist der Satz von Cauchy in 8.1.3. Damit lassen sich als Kern der klassischen Theorie endlicher Gruppen in 8.1.4 die drei Sylowsätze beweisen. Wir schließen in 8.1.5 mit dem Satz von Wedderburn als Anwendung der Klassengleichung: Jeder endliche Schiefkörper ist sogar ein Körper.

8.1.1 Gruppenaktionen und allgemeine Klassengleichung

Mit jeder Transformation $T\colon S \to S$ einer Menge S ist vermittels der Iterationen von T durch $(n, x) \mapsto T^n(x)$ eine Aktion $\alpha\colon \mathbb{N} \times S \to S$ der (additiven) Halbgruppe $\mathbb{N}$ gegeben. Ist T bijektiv, ist diese Definition auch für beliebige $n \in \mathbb{Z}$ sinnvoll. Allgemeiner definiert man:

Definition 8.1.1.1. Eine *Halbgruppenaktion* (oder auch *Halbgruppenwirkung*) einer Halbgruppe G auf einer Menge S ist eine Abbildung $\alpha\colon G \times S \to S$, $(g,x) \mapsto \alpha(g,x) =: gx$, die

$$\alpha(g_1g_2,x) = (g_1g_2)x = g_1(g_2x) = \alpha(g_1,\alpha(g_2,x))$$

für alle $x \in S$ und $g_1, g_2 \in G$ erfüllt. In diesem Fall *agiert* (oder *wirkt*) G auf S. Für festes $g \in G$ bezeichnen wir die Abbildung $x \mapsto \alpha(g,x)$ mit $\alpha_g\colon S \to S$.
Ist G sogar eine Gruppe mit neutralem Element e, so spricht man von einer *Gruppenaktion* (oder *Gruppenwirkung*), wenn zusätzlich $ex = x$ für alle $x \in S$ gilt.

Wir wollen uns hier auf Gruppenaktionen $\alpha\colon G \times S \to S$ konzentrieren. Dann gelten die Beziehungen $\alpha_e = \mathrm{id}_S$ und wegen $\alpha_{g_1} \circ \alpha_{g_2} = \alpha_{g_1g_2}$ für $g_1 = g$ und $g_2 = g^{-1}$ auch $\alpha_g \circ \alpha_{g^{-1}} = \alpha_{g^{-1}} \circ \alpha_g = \mathrm{id}_S$. Also sind alle α_g Permutationen der Menge S, mit anderen Worten: Elemente von $\mathrm{Sym}(S)$. Wie üblich bezeichnet dabei $\mathrm{Sym}(S) := \{f\colon S \to S \text{ bijektiv}\}$ die symmetrische Gruppe auf der Menge S mit der Komposition von Abbildungen als Gruppenoperation.
Anders formuliert induziert jede Aktion α einer Gruppe G auf einer Menge S einen Gruppenhomomorphismus

$$\varphi_\alpha\colon G \to \mathrm{Sym}(S), g \mapsto \alpha_g, \quad \text{wobei } \alpha_g(x) := \alpha(g,x).$$

Umgekehrt induziert jeder Homomorphismus $\varphi\colon G \to \mathrm{Sym}(S)$, $g \mapsto \pi_g$ die Aktion $\alpha : (g,x) \mapsto \pi_g(x)$, denn es gilt

$$\alpha(g_1g_2,x) = \pi_{g_1g_2}(x) = (g_1g_2)x = g_1(g_2x) = \alpha(g_1,\alpha(g_2,x)).$$

Die beiden Zugänge über Aktionen bzw. Homomorphismen in eine Permutationsgruppe sind also äquivalent.

Der Satz von Cayley, wonach jede Gruppe G via $g \mapsto \pi_g$, $\pi_g(x) := gx$, isomorph ist zu einer Permutationsgruppe (d.h. definitionsgemäß zu einer Untergruppe einer symmetrischen Gruppe) auf ihrer eigenen Trägermenge, lässt sich also auch so formulieren:

Satz 8.1.1.2 (Cayley)**.** *Jede Gruppe G agiert auf ihrer Trägermenge vermittels der Aktion $\alpha\colon (g,x) \to g \cdot x$ (Linkstranslation), wobei die Abbildung $g \mapsto \alpha_g$, $\alpha_g : x \mapsto gx$, eine isomorphe Einbettung ist.*

Die Definition einer Gruppenaktion legt unmittelbar einige weitere Begriffe nahe.

Definition 8.1.1.3. Die Gruppe G agiere auf der Menge S. Für $x \in S$ sei $G_x := \{g \in G : gx = x\} \leq G$. der *Stabilisator* oder die *Isotropiegruppe* von x. (Offenbar handelt es sich tatsächlich um eine Untergruppe von G.) Wenn $gx = x$, dann heißt umgekehrt x ein Fixpunkt von g.
Die Klassen bzgl. der Äquivalenz (um eine solche handelt es sich offenbar) $x \sim x' :\Leftrightarrow \exists g \in G : gx = x'$ auf S heißen *Orbits*, die wir mit $\overline{x} := [x]_\sim$ oder auch $O(x)$ bezeichnen. Wenn es zu je zwei Elementen $x, y \in S$ ein $g \in G$ mit $gx = y$ gibt (wenn ganz S also der einzige Orbit der Gruppenaktion ist), heißt die Aktion *transitiv*.

Wir wollen uns noch kurz der in der Definition auftretenden Äquivalenzrelation $\sim$ zuwenden. Angenommen, aus den Orbits sei je ein Vertreter $x_i \in S$ ausgewählt. Darunter seien jene $x \in S$, die für sich bereits eine einelementige $\sim$-Äquivalenzklasse $O(x) = \overline{x} = \{x\} = [x]_\sim$ bilden, zur Menge $S_0 \subseteq S$ zusammengefasst und die anderen mit $i \in I$ indiziert. Mit dieser Notation gilt offenbar:

Proposition 8.1.1.4 (Klassengleichung für allgemeine Gruppenaktionen)**.** *Agiere G auf S, sei $S_0 := \{x \in S \mid O(x) = \{x\}\}$ und mögen die Elemente x_i, $i \in I$, ein vollständiges Vertretersystem für die Orbits mit mehr als einem Element bilden. Dann gilt:*

$$|S| = |S_0| + \sum_{i \in I} |O(x_i)|.$$

Für uns wird der Fall, dass S endlich ist, also $I = \{1, \ldots, n\}$ mit $n \in \mathbb{N}$, von besonderem Interesse sein. So werden wir sehen, dass im Falle der Aktion einer Gruppe durch Konjugation auf sich selbst diese an sich triviale Beziehung zu überraschend starken Einsichten in die Struktur endlicher Gruppen führt. Das hat auch mit der nächsten Beobachtung zu tun.

Proposition 8.1.1.5. *Sei G eine Gruppe, die auf S agiert, und $x \in S$. Dann gilt $|O(x)| = [G : G_x]$ (Index = Anzahl der Nebenklassen von G_x in G). Für endliches G ist insbesondere $|O(x)|$ ein Teiler von $|G|$.*

Beweis. Seien $g_1, g_2 \in G$. Dann gilt

$$g_1 x = g_2 x \iff g_1^{-1} g_2 x = x \iff g_1^{-1} g_2 \in G_x \iff g_1 G_x = g_2 G_x.$$

Also entsprechen den Elementen im Orbit von x die Linksnebenklassen von G_x in G in bijektiver Weise. □

Anwendung dieses Faktums auf Proposition 8.1.1.4 liefert:

Folgerung 8.1.1.6. *Ist die Ordnung der endlichen, auf der endlichen Menge S agierenden Gruppe G eine Primzahlpotenz $p^n = |G|$ ($p \in \mathbb{P}$, $n \in \mathbb{N}$), so ist $|S| \equiv |S_0| \mod p$.*

Beweis. In der Gleichung $|S| = |S_0| + \sum_{i=1}^{n} |O(x_i)|$ aus Proposition 8.1.1.4 sind nach Proposition 8.1.1.5 und dem Satz von Lagrange (3.2.1.4) alle Summanden $|O(x_i)|$ durch p teilbar (man beachte $|O(x_i)| > 1$). □

UE 43 ▶ Übungsaufgabe 8.1.1.7. (F) **◀ UE 43**

(a) Gibt es eine transitive Aktion von S_4 auf $\{1, 2, 3, 4, 5\}$?

(b) Geben Sie eine Aktion von S_4 auf $\{1, 2, 3, 4, 5\}$ an, die die kleinstmögliche Anzahl an Orbits hat.

8.1.2 Aktion durch Konjugation und spezielle Klassengleichung

Im Zentrum steht nun eine besondere Gruppenaktion, die mit jeder (auch abstrakten) Gruppe automatisch einhergeht.

Definition 8.1.2.1. Ist H eine Untergruppe von G, dann agiert H via $\alpha : (h, x) \mapsto hxh^{-1}$ auf G. Diese Gruppenaktion α heißt *Konjugation*. Dabei sind die $\alpha_h : x \mapsto hxh^{-1}$ sogar Automorphismen von G, die sogenannten *inneren Automorphismen*. Insbesondere agiert H auch auf $\mathrm{Sub}(G) := \{U : U \leq G\}$. (Dabei sind alle Normalteiler Fixpunkte; im Fall $H = G$ sind die Normalteiler genau die Fixpunkte.) Die Orbits bezüglich Konjugation heißen *Konjugiertenklassen* (sowohl auf $\mathrm{Sub}(G)$ als auch auf G).

Durch Spezialisierung der Konzepte aus Unterabschnitt 8.1.1 auf Konjugation stoßen wir auf weitere wichtige Begriffe.

Definition 8.1.2.2. Sei H eine Untergruppe von G.

- Der Stabilisator eines Elementes $x \in G$ bezüglich der Konjugation von H auf G, d.h. die Untergruppe

  $$Z_H(x) := H_x = \{h \in H \mid hxh^{-1} = x\} = \{h \in H \mid hx = xh\}$$

  von H, heißt *Zentralisator* von x in H.

- Der Schnitt aller $Z_G(x)$ (d.h. der Kern der Abbildung $g \mapsto \alpha_g$, der aus allen $x \in G$ mit $xg = gx$ für alle $g \in G$ besteht) wird mit $Z(G)$ bezeichnet und heißt *Zentrum* von G.

- Schließlich nennt man den Stabilisator einer Untergruppe $K \leq G$ bezüglich der Aktion von H durch Konjugation, also die Untergruppe $N_H(K) := \{h \in H \mid hKh^{-1} = K\}$ von H, den *Normalisator* von K in H.

Anmerkung 8.1.2.3. Offenbar ist $N_G(K)$, der Normalisator von K in G, die größte Untergruppe von G, in der K Normalteiler ist. Insbesondere gilt stets $K \lhd N_G(K)$.

Bezüglich der Aktion von G durch Konjugation auf sich selbst bildet ein Element x genau dann für sich eine einelementige Konjugiertenklasse $\overline{x} = \{x\}$, wenn $gxg^{-1} = x$, also $gx = xg$, für alle $g \in G$ gilt, wenn also $x \in Z(G)$. Sämtliche Konjugierten eines beliebigen $x \in G$ bilden den Orbit $O(x) = \overline{x}$, dessen Kardinalität nach Proposition 8.1.1.5 der Index des Stabilisators von x in G ist, hier also des Zentralisators $Z_G(x)$. Wir fassen zusammen:

Proposition 8.1.2.4. *Sei G eine endliche Gruppe. Dann gilt*

1. *Für jedes $x \in G$ ist die Anzahl $|\overline{x}|$ der Elemente in der Konjugiertenklasse von x gleich $[G : Z_G(x)]$ und teilt daher $|G|$.*

2. *Die Anzahl der zu $K \leq G$ konjugierten Untergruppen ist $[G : N_G(K)]$ und teilt daher $|G|$.*

3. Seien $\overline{x}_1, \ldots, \overline{x}_n$ sämtliche Konjugiertenklassen (jede genau einmal). Dann ist

$$|G| = \sum_{i=1}^{n} [G : Z_G(x_i)].$$

Die Klassengleichung aus 8.1.1.4 nimmt damit folgende Form an: Bilden die Elemente $x_1, \ldots, x_m \in G$ ein vollständiges Vertretersystem der Konjugiertenklassen außerhalb des Zentrums $Z(G)$, so gilt

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : Z_G(x_i)]. \tag{8.1}$$

Beweis. Alle Aussagen ergeben sich mit Hilfe des Vorangegangenen unmittelbar durch Spezialisierung der entsprechenden Aussagen aus Unterabschnitt 8.1.1. □

Bezeichne α die Aktion einer Gruppe G auf sich selbst vermittels Konjugation, d.h. $\alpha_g \colon G \to G$, $x \mapsto gxg^{-1}$ sei der durch $g \in G$ induzierte innere Automorphismus. Der Gruppenhomomorphismus $\varphi \colon G \to \mathrm{Aut}(G)$, $g \mapsto \alpha_g$ ist injektiv genau dann, wenn $|Z(G)| = 1$. Insbesondere ist dies der Fall, wenn $G = S_n$ eine symmetrische Gruppe mit $n \geq 3$ ist. In diesem Fall ist φ also sogar eine isomorphe Einbettung von G in seine Automorphismengruppe $\mathrm{Aut}(G)$, siehe auch Proposition 3.2.5.6.
Zum Abschluss noch zwei Übungsaufgaben zur Illustration der Resultate:

UE 44 ► **Übungsaufgabe 8.1.2.5.** (F) Sei G eine Gruppe mit $|G| = p^n$ für eine Primzahl p und $n \geq 1$ und sei $\mathrm{NT}(G)$ die Menge der Normalteiler von S.
Zeigen Sie $|\mathrm{Sub}(G)| \equiv |\mathrm{NT}(G)| \mod p$. ◄ **UE 44**

UE 45 ► **Übungsaufgabe 8.1.2.6.** (F) Sei G eine Gruppe, die ein Element $x \in G$ enthält, dessen Konjugiertenklasse genau zwei Elemente hat. Zeigen Sie, dass G nicht einfach ist, also einen nichttrivialen Normalteiler besitzt.
Hinweis: Proposition 3.2.2.17 kann nützlich sein. ◄ **UE 45**

8.1.3 Folgerungen aus der Klassengleichung und der Satz von Cauchy

Die erste von mehreren wichtigen Konsequenzen der Klassengleichung für Konjugation ist die folgende.

Folgerung 8.1.3.1. *Jede endliche Gruppe G von Primzahlpotenzordnung $p^n = |G|$ ($p \in \mathbb{P}$, $n \in \mathbb{N}$ mit $n \geq 1$) hat ein nichttriviales Zentrum $Z(G)$.*

Beweis. Nach der Klassengleichung aus 8.1.2.4 gilt

$$\underbrace{|G|}_{\equiv 0 \mod p} = |Z(G)| + \sum_{i=1}^{m} \underbrace{[G : Z_G(x_i)]}_{\equiv 0 \mod p}$$

Daher teilt p auch $|Z(G)|$. Nun ist aber sicher $e \in Z(G)$, also gibt es mindestens $p > 1$ verschiedene Elemente in $Z(G)$. □

Nach den bisherigen Beobachtungen verwundert es nicht, dass die Theorie endlicher Gruppen stark kombinatorischen Charakter hat und dass überdies Teilbarkeiten eine besonders wichtige Rolle spielen, folglich auch Primzahlen und Primzahlpotenzen.
Als ersten Schritt in Richtung einer entsprechenden Analyse endlicher Gruppen beweisen wir eine Art Umkehrung des Satzes von Lagrange.

Satz 8.1.3.2 (Cauchy)**.** *Sei G eine endliche Gruppe und $p \in \mathbb{P}$ ein Teiler der Gruppenordnung $|G|$. Dann gibt es ein $x \in G$ mit Ordnung p. Insbesondere existiert ein $H \leq G$ mit Ordnung $|H| = p$, nämlich $H = \langle x \rangle$ (die von x erzeugte Untergruppe).*

Beweis. Die p-elementige zyklische Gruppe C_p (aufgefasst als Addition modulo p) agiert auf der Menge $S := \{(a_1, \ldots, a_p) \in G^p : a_1 \ldots a_p = e\}$ mittels

$$\alpha(k, (a_1, \ldots, a_p)) := (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, \ldots, a_k) \in S.$$

Diese Aktion ist wohldefiniert, weil für $s \in S$ und $k \in C_p$ auch $\alpha(k, s) \in S$ gilt. Denn für $k \in C_p$ und $s = (a_1, \ldots, a_p) \in S$ folgt aus $a_1 \ldots a_p = e$ mit $x := a_1 \ldots a_k$ und $y := a_{k+1} \ldots a_p$ sofort $xy = e$, also $y = x^{-1}$ und somit auch $yx = a_{k+1} \ldots a_p a_1 \ldots a_k = e$, was

$$\alpha(k, s) = (a_{k+1}, \ldots, a_p, a_1, \ldots a_k) \in S$$

bedeutet, wie behauptet. Offensichtlich ist (Notation aus Proposition 8.1.1.4 $(a_1, \ldots, a_p) \in S_0$ genau dann, wenn $a_1 = \ldots = a_p$. Insbesondere gilt $(e, \ldots, e) \in S_0$, also $|S_0| \geq 1$. Weil sich jedes der p^{n-1} verschiedenen $n-1$-Tupel $(a_1, \ldots, a_{p-1}) \in G^{p-1}$ durch genau ein a_p zu einem p-Tupel $(a_1, \ldots, a_{p-1}, a_p) \in S$ ergänzen lässt, ist $|S| = |G|^{p-1} \equiv 0 \mod p$ (beachte $p \geq 2$). Folgerung 8.1.1.6 (die Rolle des dortigen G spielt hier C_p) zeigt $|S_0| \equiv |S| \equiv 0 \mod p$ und somit $|S_0| \geq p$. Das bedeutet aber gerade, dass es mindestens p Elemente x gibt mit $(x, \ldots, x) \in S_0 \subseteq S$, also mit $x^p = e$. Davon ist wegen $p \geq 2$ mindestens eines von e verschieden. So ein x hat die Ordnung p. □

Definition 8.1.3.3. Sei G eine beliebige Gruppe und $p \in \mathbb{P}$. Ist für alle $x \in G$ die Ordnung von x eine p-Potenz, so heißt G eine *p-Gruppe*, im Fall $|G| > 1$ eine *nichttriviale p-Gruppe*.
$H \leq G$ heißt *p-Untergruppe* von G, wenn H eine p-Gruppe ist. Maximale p-Untergruppen von G heißen *p-Sylowgruppen* von G (diese existieren nach dem Lemma von Zorn auch für unendliche Gruppen).

Folgerung 8.1.3.4. *Die Ordnung jeder endlichen p-Gruppe G ist eine p-Potenz.*

Beweis. Andernfalls hätte $|G|$ einen von p verschiedenen Primteiler q, nach dem Satz 8.1.3.2 von Cauchy also auch ein Element $x \in G$ der Ordnung q, was der Definition einer p-Gruppe widerspricht. □

UE 46 ► Übungsaufgabe 8.1.3.5. (F) Zeigen Sie die folgenden Tatsachen über p-Gruppen und p-Sylowgruppen: **◄ UE 46**

(1) In jeder Gruppe G gibt es für jedes $p \in \mathbb{P}$ eine p-Sylowgruppe.

(2) Eine endliche Gruppe G ist eine p-Gruppe genau dann, wenn $|G| = p^n$ für ein $n \in \mathbb{N}$.

Anmerkung: Man kann sich nach dieser Aufgabe fragen, ob man für endliche Gruppen eine p-Sylowgruppe alternativ als p-Untergruppe mit maximaler Ordnung definieren kann. Der erste Sylowsatz wird unter anderem besagen, dass diese Vermutung korrekt ist.

8.1.4 Die drei Sylowsätze

Die drei Sylowsätze, deren Beweis unser nächstes Ziel ist, geben Auskunft über die p-Sylowgruppen P einer endlichen Gruppe G. Grob gesprochen besagen sie: Erstens gibt es in jedem G und zu jedem $p \in \mathbb{P}$ ein P, dessen Ordnung die maximale Potenz von p ist, durch die $|G|$ teilbar ist (das also eine p-Sylowgruppe ist). Zweitens sind je zwei solcher P zueinander konjugiert. Und drittens ist ihre Anzahl n einerseits Teiler von $|G|$ und andererseits kongruent 1 modulo p.
Ein wesentliches Hilfsmittel im Beweis des ersten Sylowsatzes ist das nachfolgende Lemma. Gemeinsam mit dem Satz von Cauchy hat es zur Folge, dass man Untergruppen von p-Potenzordnung p^i zu solchen der Ordnung p^{i+1} erweitern kann, bis man bei der maximalen p-Potenz, welche die Gruppenordnung $|G|$ teilt, angelangt ist.

Lemma 8.1.4.1. *Sei G eine endliche Gruppe und H eine p-Untergruppe von G. Dann ist $[N_G(H) : H] \equiv [G : H] \mod p$. Gilt zusätzlich $p|[G : H]$, so ist insbesondere $H \subsetneq N_G(H)$.*

Beweis. Sei $S := \{aH : a \in G\}$. Dann agiert H auf S durch Linkstranslation mit $|S| = [G : H]$. Nach Folgerung 8.1.1.6 gilt $|S| \equiv |S_0| \mod p$. Die erste Behauptung des Lemmas folgt, sofern wir zeigen können, dass S_0 gerade aus jenen Nebenklassen xH mit $x \in N_G(H)$ besteht. Denn dann folgt

$$[N_G(H) : H] = |S_0| \equiv |S| = [G : H] \mod p.$$

Tatsächlich gilt folgende Kette von Äquivalenzen:

$$\begin{aligned} xH \in S_0 &\Leftrightarrow hxH = xH \quad \forall h \in H \\ &\Leftrightarrow x^{-1}hxH = H \quad \forall h \in H \\ &\Leftrightarrow x^{-1}hx \in H \quad \forall h \in H \\ &\Leftrightarrow xHx^{-1} = H \\ &\Leftrightarrow x \in N_G(H) \end{aligned}$$

Die zweite Behauptung folgt daraus unmittelbar. □

Satz 8.1.4.2 (Erster Sylowsatz)**.** *Sei G eine endliche Gruppe mit $|G| = p^n m$, $n \in \mathbb{N}$ und $p \in \mathbb{P}$, wobei m nicht durch p teilbar ist. Dann gibt es in G eine p-Sylowgruppe der (nach dem Satz von Lagrange maximal möglichen p-Potenz-) Ordnung p^n.*

Es gilt sogar stärker: Es gibt eine aufsteigende Kette von Untergruppen $H_i \leq G$ mit $|H_i| = p^i$ für $i = 0, \ldots, n$ und

$$H_0 = \{e\} \lhd H_1 \lhd \ldots \lhd H_i \lhd H_{i+1} \lhd \ldots \lhd H_n.$$

Beweis. Wir zeigen mit Induktion nach k, dass es für $k = 0, 1, \ldots, n$ eine aufsteigende Kette von Untergruppen $H_i \leq G$ gibt mit $|H_i| = p^i$ für $i = 0, \ldots, k$ und

$$H_0 = \{e\} \lhd H_1 \lhd \ldots \lhd H_i \lhd H_{i+1} \lhd \ldots \lhd H_k.$$

Für $k = 0$ ist nichts zu zeigen, und für $k = 1$ folgt die Behauptung unmittelbar aus dem Satz von Cauchy (8.1.3.2). Gelte also die Behauptung für ein k mit $1 \leq k < n$ und sei $H_k \leq G$ mit Ordnung $|H_k| = p^k$. Aus $k < n$ folgt $p|[G : H_k]$. Aus Lemma 8.1.4.1 schließen wir

$$1 \leq [N_G(H_k) : H_k] \equiv [G : H_k] \equiv 0 \mod p,$$

also $p|[N_G(H) : H_k]$. Wendet man nochmals den Satz von Cauchy an, diesmal auf $N_G(H_k)/H_k$, dann erhält man eine Untergruppe H' von $N_G(H_k)/H_k$ der Ordnung p. Nun ist $H' = H_{k+1}/H_k$ mit $H_k < H_{k+1} \leq N_G(H_k)$, daher $|H_{k+1}| = |H_k| \cdot [H_{k+1} : H_k] = p^k \cdot p = p^{k+1}$ und wegen $H_k \lhd N_G(H_k)$ auch $H_k \lhd H_{k+1}$. □

Satz 8.1.4.3 (Zweiter Sylowsatz)**.** *Sei G eine endliche Gruppe und $p \in \mathbb{P}$, $H \leq G$ eine p-Untergruppe und P eine p-Sylowgruppe von G. Dann existiert ein $x \in G$, sodass $H \leq xPx^{-1}$. Insbesondere sind je zwei p-Sylowgruppen konjugiert und somit auch isomorph.*

Beweis. H agiert auf der Menge $S := \{aP : a \in G\}$ via Linkstranslation. Aus Folgerung 8.1.1.6 und weil P eine p-Sylowgruppe ist, folgt $|S_0| \equiv |S| = [G : P] \not\equiv 0 \mod p$. Also ist $|S_0| > 0$, d.h. es gibt ein $xP \in S_0$. Das bedeutet $hxP = xP$ und somit $x^{-1}hx \in P$ für alle $h \in H$. Somit ist $x^{-1}Hx \leq P$ bzw. $H \leq xPx^{-1}$, die erste Behauptung. Ist speziell H eine weitere p-Sylowgruppe, so folgt aus Kardinalitätsgründen $H = xPx^{-1}$. □

Folgerung 8.1.4.4. *Sei P eine p-Sylowgruppe der endlichen Gruppe G. Dann ist P genau dann die einzige p-Sylowgruppe von G, wenn P Normalteiler in G ist.*

Beweis. Ist P die einzige p-Sylowgruppe, so muss P mit allen seinen Konjugierten $xPx^{-1} = P$ übereinstimmen, also $P \lhd G$. Die Umkehrung folgt aus dem zweiten Sylowsatz (8.1.4.3). □

Satz 8.1.4.5 (Dritter Sylowsatz)**.** *Sei G eine endliche Gruppe, $p \in \mathbb{P}$ und $n := |S|$ für die Menge S aller p-Sylowgruppen von G. Dann teilt n die Gruppenordnung $|G|$, und außerdem ist $n \equiv 1 \mod p$.*

Beweis. Für beide Behauptungen betrachten wir Aktionen auf S durch Konjugation – für die erste die Aktion von G, für die zweite die Aktion von P, einer p-Sylowgruppe, die nach dem ersten Sylowsatz 8.1.4.2 ja existiert.
Agiert G, so ist S nach dem zweiten Sylowsatz (8.1.4.3) gerade der Orbit von P. Seine Kardinalität n teilt nach Proposition 8.1.2.4(i) die Gruppenordnung $|G|$.

In Hinblick auf die zweite Behauptung $n \equiv 1 \mod p$ bemühen wir Folgerung 8.1.1.6, wonach ja $n = |S| \equiv |S_0| \mod p$ für die Menge S_0 aller gemeinsamen Fixpunkte der Aktion gilt. Bei der Aktion von P auf S sind das jene $Q \in S$ mit $xQx^{-1} = Q$ für alle $x \in P$, d.h. mit $P \subseteq N_G(Q)$. Wegen $Q \lhd N_G(Q)$ kann es innerhalb $N_G(Q)$ nach Folgerung 8.1.4.4 aber nur eine p-Sylowgruppe geben, also $P = Q$. Somit ist $S_0 = \{P\}$, folglich $n \equiv 1 \mod p$, wie behauptet. □

Folgerung 8.1.4.6. *Sei G eine endliche Gruppe, $p \in \mathbb{P}$ und P eine p-Sylowgruppe von G. Für $N := N_G(P)$ gilt dann $N_G(N) = N$.*

Beweis. Wir müssen die Inklusion $N_G(N) \subseteq N$ beweisen. Sei dazu $x \in N_G(N)$, d.h. $xNx^{-1} = N$. Folglich ist neben P auch $P' := xPx^{-1} \subseteq xNx^{-1} = N$ eine p-Sylowgruppe innerhalb von N. Wegen $P \lhd N = N_G(P)$ und Folgerung 8.1.4.4 ist P aber die einzige p-Sylowgruppe von N. Also ist $P = P' = xPx^{-1}$ und somit auch $x \in N_G(P) = N$. □

UE 47 ► **Übungsaufgabe 8.1.4.7.** (B) Beschreiben Sie für eine möglichst große Menge von Paaren $(n, p) \in \mathbb{N} \times \mathbb{P}$ alle p-Sylowgruppen der symmetrischen Gruppe S_n. ◄ **UE 47**

UE 48 ► **Übungsaufgabe 8.1.4.8.** (B) Sei A eine endliche abelsche Gruppe. Bestimmen Sie die p-Sylowgruppen von A und prüfen Sie die Gültigkeit der drei Sylowsätze nach. ◄ **UE 48**

8.1.5 Eine Anwendung der Klassengleichung: Der Satz von Wedderburn

In Abschnitt 6.3 wurden die endlichen Körper klassifiziert: Unter den natürlichen Zahlen sind es genau die Primzahlpotenzen p^n, $p \in \mathbb{P}$ und $n \in \mathbb{N}$ mit $n \geq 1$, zu denen es einen Körper K mit dieser Kardinalität gibt, und je zwei Körper der Kardinalität p^n sind isomorph zueinander. Es ist bemerkenswert, dass diese Aussage auch gilt, wenn man auch Schiefkörper (Divisionsringe) zulässt, also Ringe mit Einselement, wo die von 0 verschiedenen Elemente eine mutiplikative Gruppe bilden, die im Gegensatz zu den Körpern aber nicht kommutativ sein muss. Mit anderen Worten: Jeder endliche Schiefkörper ist sogar ein Körper. Nichtkommutative Schiefkörper müssen also unendlich sein, so wie die Hamiltonschen Quaternionen, das prominenteste Beispiel eines Schiefkörpers. Unser Ziel ist also der Beweis folgenden Satzes:

Satz 8.1.5.1 (Wedderburn)**.** *Jeder endliche Divisionsring (Schiefkörper) D ist ein Körper.*

Beweis. Für jedes $a \in D$ sei $Z(a) := \{d \in D : da = ad\}$. Wir behaupten zunächst, dass $Z(a)$ ein Unterdivisionsring von D ist, folglich auch der Schnitt K aller $Z(a)$, $a \in D$. Weil

$$K = \{a \in D : \forall d \in D : ad = da\}$$

selbst kommutativ ist, handelt es sich um einen endlichen Körper. Nach dem Klassifikationssatz 6.3.1.2 ist daher $q := |K| = p^m$ mit $p \in \mathbb{P}$ und positivem $m \in \mathbb{N}$.

Zum Beweis, dass $Z(a)$ ein Unterdivisionsring von D ist, stellen wir zunächst $0, 1 \in Z(a)$ fest. Außerdem beachte man, dass $Z(a)$ der Zentralisator von a innerhalb der multiplikativen Gruppe $D^* = D \setminus \{0\}$ erweitert um die 0 ist. Daraus folgt, dass $Z(a)^*$ eine Untergruppe von D^* ist. Klarerweise ist dann auch $Z(a) = Z(a)^* \cup \{0\}$ multiplikativ abgeschlossen. $Z(a)$ ist aber auch eine additive Untergruppe von D: Aus $d_1, d_2 \in Z(a)$ folgt $ad_1 = d_1a$ und $ad_2 = d_2a$, somit auch $a(d_1+d_2) = ad_1+ad_2 = d_1a+d_2a = (d_1+d_2)a$, also $d_1 + d_2 \in Z(a)$. Schließlich liegt mit $d \in Z(a)$ auch $-d$ in $Z(a)$, wie die Umformung $a(-d) = -(ad) = -(da) = (-d)a$ beweist.
Wir können D also auch als Vektorraum auffassen, sowohl über K als auch über $Z(a)$, überdies $Z(a)$ als Vektorraum über K. Seien $n := \dim_K D$, $d_a := \dim_{Z(a)} D$ und $n_a := \dim_K Z(a)$ die zugehörigen Dimensionen. Zu zeigen ist $n = 1$. Nach dem Gradsatz 6.1.2.2 gilt $n = n_a d_a$, insbesondere also $n_a | n$. Außerdem ist $|D| = |K|^n = q^n = p^{mn}$. Für die multiplikativen Gruppen $Z(a)^* \leq D^*$ gilt $|D^*| = q^n - 1$ und $|Z(a)^*| = q^{n_a} - 1$, nach dem Satz von Lagrange folglich $q^{n_a} - 1 | q^n - 1$ bzw., äquivalent, $\frac{q^n-1}{q^{n_a}-1} \in \mathbb{N}$.
Für D^* bringen wir nun die Klassengleichung aus 8.1.2.4 ins Spiel:

$$q^n - 1 = |D^*| = |K^*| + \sum_{a \in A} [D^* : Z(a)^*] = q - 1 + \sum_{a \in A} \frac{q^n - 1}{q^{n_a} - 1} \in \mathbb{N},$$

wobei a ein vollständiges Repräsentantensystem A für jene Konjugiertenklassen durchläuft, die aus mehr als einem Element bestehen.
Außerdem ziehen wir die Kreisteilungspolynome g_n aus Unterabschnitt 6.2.5 zu Rate. Zur Erinnerung: Diese Polynome haben ganzzahlige Koeffizienten mit konstantem Term ± 1 und zerfallen in das Produkt

$$g_n = \prod_{k \in \mathbb{Z}_n^*} (x - \zeta^k),$$

wobei ζ eine primitive n-te Einheitswurzel ist. Die Einheitengruppe $\mathbb{Z}_n^*$ besteht aus den zu n teilerfremden Restklassen modulo n. Weil ζ auf dem komplexen Einheitskreis liegt und q eine natürliche Zahl mit $q > 1$ ist, gilt in der komplexen Zahlenebene die später noch nützliche Abschätzung $|q - \zeta| > q - 1 \geq 1$. Das Polynom $x^n - 1$ lässt sich wie folgt zerlegen:

$$x^n - 1 = \prod_{d|n} g_d(x) = (x^{n_a} - 1) g_n(x) \prod_{\substack{d|n; d \nmid n_a \\ d \neq n}} g_d(x).$$

Wegen der Ganzzahligkeit der Koeffizienten der Kreisteilungspolynome zeigt Einsetzen von q für x die Teilbarkeiten $g_n(q) \mid q^n - 1$ und sogar $g_n(q) \mid \frac{q^n-1}{q^{n_a}-1}$. Weil letzteres für alle a gilt, lesen wir aus der Klassengleichung ab, dass auch der verbleibende Summand $q - 1$ durch $g_n(q)$ teilbar ist, also $g_n(q) | q - 1$. Daraus und aus der indirekten Annahme $n > 1$ werden wir nun einen Widerspruch ableiten können:
Sei $\zeta = a + ib$ mit $a^2 + b^2 = 1$, $a, b \in \mathbb{R}$, irgendeine der primitiven n-ten Einheitswurzeln mit Realteil a und Imaginärteil b. Für $n > 1$ ist $a < 1$. Daraus ergibt sich

$$|q-\zeta|^2 = |q-a-ib|^2 = (q-a)^2+b^2 = q^2-2aq+a^2+b^2 = q^2-2aq+1 > q^2-2q+1 = (q-1)^2,$$

folglich $|q-\zeta| > q-1 \geq 1$ und, weil das für alle primitiven Einheitswurzeln ζ gilt,

$$|g_n(q)| = \prod_{\zeta} |q-\zeta| > q-1.$$

Das verträgt sich aber nicht mit der zuvor hergeleiteten Teilbarkeit $g_d(q)|q-1$. Der Widerspruch zur Annahme $n > 1$ zeigt $n = 1$, also ist $D = K$ tatsächlich ein Körper. □

8.2 Einige konkrete Beispiele

In diesem Abschnitt nehmen wir uns ein paar konkrete Beispiele vorwiegend endlicher Gruppen vor. Der Fokus liegt auf den nichtabelschen Gruppen, weil wir die abelschen dank Hauptsatz 7.4.3.2 schon sehr gut verstehen. Für die nichtabelschen gelingt selbst unter Zuhilfenahme der bisher entwickelten allgemeinen Theorie ein vollständiger Überblick lediglich für kleine Ordnungen. Als nützlich erweist sich die (nicht auf endliche Gruppen beschränkte) Methode der Darstellung durch Erzeuger und Relationen (8.2.1). Mit ihrer Hilfe lassen sich auch die sogenannten Diedergruppen (sprich: Di-eder-gruppen) D_n der Ordnung $2n$ (8.2.2), die Alternierenden Gruppen A_n der Ordnung $\frac{n!}{2}$ (8.2.3), die achtelementige *Quaternionengruppe* Q_8 und eine verwandte 12-elementige Gruppe als Spezialfälle sogenannter dizyklischer Gruppen beschreiben (8.2.4). Zusammen mit zwei Struktursätzen (8.2.5) erweisen sich diese Gruppen in 8.2.6 für die Klassifikation aller Gruppen bis zur Ordnung 15 als zweckmäßig.

8.2.1 Die Beschreibung von Gruppen durch Erzeuger und Relationen

Eine wichtige Möglichkeit zur Beschreibung von Gruppen besteht vermöge *Erzeuger und Relationen*:

Definition 8.2.1.1. Sei X eine Menge, und $F(X)$ die von X frei erzeugte Gruppe, die wir als Menge (reduzierter) Gruppenwörter (siehe Unterabschnitt 4.1.4) auffassen. Für eine Teilmenge $Y \subseteq F(X)$ sei $N = N(Y) \lhd F(X)$ der von Y erzeugte Normalteiler in $F(X)$. Die Gruppe $G := F(X)/N$ heißt die durch X und die Relationen „$w = e$“, $w \in Y$, dargestellte Gruppe. Man schreibt für G auch $\langle X|Y\rangle$ und spricht dabei von einer *Darstellung durch Erzeuger und Relationen*.

Als Beispiel bestehe $X = \{x, y\}$ aus zwei Elementen $x \neq y$, $Y = \{w\}$ aus dem einzigen Wort $w = xyx^{-1}y^{-1}$. Die Gruppe $\langle X|Y\rangle$ ist dann isomorph zu $\mathbb{Z}^2$. Denn die Relation $w = xyx^{-1}y^{-1} = e$ ist äquivalent zu $xy = yx$, drückt also das Vertauschen der beiden Elemente x und y aus. Somit ist die von $X = \{x, y\}$ erzeugte Gruppe kommutativ. Weitere Einschränkungen gibt es nicht, also ist $\langle X|Y\rangle$ die von zwei Elementen frei erzeugte abelsche Gruppe, die isomorph ist zu $\mathbb{Z}^2$.

UE 49 ► Übungsaufgabe 8.2.1.2. (F,A) **◄ UE 49**

1. Geben Sie einen strengen Beweis für die oben behauptete Isomorphie $\langle X|Y\rangle \cong \mathbb{Z}^2$ für $X = \{x, y\}$ und $Y = \{xyx^{-1}y^{-1}\}$ unter Verwendung von Definition 8.2.1.1.

2. Zeigen Sie allgemein: Ist H eine beliebige von X erzeugte Gruppe, welche die Relationen $w = e, w \in Y$, erfüllt, so existiert ein eindeutiger Epimorphismus von $G := \langle X|Y\rangle$ nach H, der die Elemente $xN(Y) \in F(X)/N(Y)$, $x \in X$, auf $x \in H$ abbildet. Deuten Sie entsprechend G auch als universelles Objekt in einer geeigneten Kategorie.

8.2.2 Die Diedergruppen D_n

Die *Diedergruppe* (sprich: Di-eder-gruppe) D_n lässt sich am einfachsten beschreiben als Symmetriegruppe des regelmäßigen n-Ecks. Definitionsgemäß ist damit die Menge D_n aller Isometrien $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ gemeint (f soll also den Euklidischen Abstand zwischen zwei Punkten der Ebene unverändert lassen), welche die Menge E_n der Eckpunkte $\zeta_k = (\cos(\frac{2k\pi}{n}), \sin(\frac{2k\pi}{n}))$, $k = 0, 1, \ldots, n-1$, permutiert. Gruppenoperation ist die Komposition von Abbildungen. Klarerweise lassen sich isomorphe Kopien von D_n auch anders beschreiben. Zwei derartige Beschreibungen ergeben sich aus den folgenden Aufgaben.

UE 50 ► Übungsaufgabe 8.2.2.1. (B) Beschreiben Sie eine zu D_n isomorphe Gruppe G als Untergruppe der symmetrischen Gruppe S_n. **◄ UE 50**

In Hinblick auf die Klassifikation kleiner Gruppen in Unterabschnitt 8.2.6 wollen wir uns in der nächsten Aufgabe nicht mit einer Darstellung durch Erzeuger und Relationen zufriedengeben, sondern eine *Charakterisierung* der Diedergruppen durch strukturelle Eigenschaften in den Fokus nehmen. Man beachte, dass es nach Übungsaufgabe 8.2.1.2 für eine Gruppe $G = \langle X|Y\rangle$ und eine andere Gruppe H, die ebenfalls die durch Y gegebenen Relationen erfüllt, stets einen Epimorphismus $G \to H$ gibt – wir streben aber stärker einen Isomorphismus an.

UE 51 ► Übungsaufgabe 8.2.2.2. (B) **◄ UE 51**

(a) Geben Sie Isometrien $f, g \in D_n$ an mit

(i) $\mathrm{ord}(f) = n$, $\mathrm{ord}(g) = 2$

(ii) $D_n = \langle f, g\rangle$

(ii') $D_n = \{g^j f^i \mid 0 \le i \le n-1, 0 \le j \le 1\}$, wobei
$g^j f^i = g^{j'} f^{i'} \Rightarrow j = j', i = i'$ und daher $|D_n| = 2n$

(iii) $gf = f^{-1}g$

(b) Zeigen Sie: Wenn G eine Gruppe mit $|G| = 2n$ ist, sodass es $a, b \in G$ gibt, die die Bedingungen (i),(ii),(iii) aus (a) sinngemäß erfüllen ((ii') ist nicht vorausgesetzt!), dann gilt $G \cong D_n$.

Hinweis: Zeigen Sie $G = \langle a, b\rangle = \{b^j a^i \mid 0 \le i \le n-1, 0 \le j \le 1\}$ und geben Sie einen Isomorphismus $\varphi : G \to D_n$ an (wieso ist er wohldefiniert?).

8.2.3 Die alternierenden Gruppen A_n

Die *alternierende Gruppe* A_n ist jene Untergruppe der S_n, die aus den geraden Permutationen besteht.

UE 52 ▶ **Übungsaufgabe 8.2.3.1.** (F) Behandeln Sie im Zusammenhang mit der alternierenden Gruppe A_n folgende Aufgaben. ◀ **UE 52**

1. Rekapitulieren Sie die Schreibweise von Permutationen mittels paarweise elementfremder Zyklen und wie sich daraus ihre Ordnungen als Gruppenelemente ablesen lassen.
2. Wiederholen Sie aus Unterabschnitt 3.2.5, wie gerade und ungerade Permutationen definiert sind und warum für $n \geq 2$ die geraden innerhalb der symmetrischen Gruppe S_n einen Normalteiler der Ordnung $\frac{n!}{2}$ bilden.
3. Beschreiben Sie allgemein anhand der Zyklenschreibweise, welche Permutationen aus der symmetrischen Gruppe S_n zu A_n gehören.
4. Bestimmen Sie in A_4 die Ordnungen der Elemente, das Zentrum und sämtliche Untergruppen und Normalteiler.
5. Geben Sie eine Darstellung von A_4 durch Relationen und Erzeuger an.

Entscheidende Implikationen in der Galoistheorie hat der nächste Satz und seine Folgerung:

Satz 8.2.3.2. *A_n ist für alle $n \geq 5$ einfach.*

UE 53 ▶ **Übungsaufgabe 8.2.3.3.** (V) Beweisen Sie Satz 8.2.3.2, indem Sie für einen beliebigen Normalteiler $N \lhd A_n$ mit $|N| > 1$ zeigen, dass $N = A_n$ folgt. Das ergibt sich durch die unten vorgeschlagenen Schritte, wobei wir zunächst nur $n \geq 4$ annehmen. Wir beziehen uns auf Zyklenschreibweise, d.h. auf die Darstellung von Elementen in S_n als Produkte paarweise elementfremder Zyklen. ◀ **UE 53**

1. A_n wird von sämtlichen Dreierzyklen erzeugt.
2. Beliebige 3-Zyklen lassen sich durch spezielle erzeugen, nämlich für beliebig aber fest gewählte $a \neq b \in \{1, \ldots, n\}$ durch alle (abc), $c = 1, \ldots, n$.
3. Enthält N einen 3-Zyklus, so folgt $N = A_n$. Hinweis: Aussage 2 verwenden.
4. Enthält N ein Element, in dessen Zyklenschreibweise ein k-Zyklus mit $k \geq 4$ vorkommt, so folgt $N = A_n$.
5. Enthält N ein Element, in dessen Darstellung zwei 3-Zyklen vorkommen, so folgt $N = A_n$.

6. Enthält N ein Element, in dessen Darstellung ein 3-Zyklus und sonst lauter 2-Zyklen vorkommen, so folgt $N = A_n$.

7. Jetzt sei $n \geq 5$ angenommen. N enthalte ein Element σ mit disjunkter Zyklendarstellung $\sigma = (a_1a_2)(a_3a_4)\tau$, wobei sich τ ausschließlich aus (zueinander und zu $\{a_1, a_2, a_3, a_4\}$ disjunkten) 2-Zyklen zusammensetze. Sei b verschieden von a_1, a_2, a_3, a_4 (hier geht $n \geq 5$ ein), $\xi = (a_1a_2b) \in A_n$ und $\zeta = (a_1a_3)(a_2a_4)$. Zeigen Sie $\zeta \in N$ (Hinweis: $\zeta = \sigma^{-1}(\delta\sigma\delta^{-1})$ mit $\delta = (a_1a_2a_3)$) und $\zeta\xi\zeta\xi^{-1} = (a_1a_3a_4ba_2) \in N$, um auf $N = A_n$ zu schließen.

8. Schließen Sie den Beweis von Satz 8.2.3.2 ab.

Folgerung 8.2.3.4.

- *Für $n = 1, 2$ hat S_n nur die trivialen Normalteiler.*
- *Der einzige nichttriviale Normalteiler von S_3 ist die alternierende Gruppe A_3.*
- *Die einzigen nichttrivialen Normalteiler von S_4 sind die alternierende Gruppe A_4 und die Kleinsche Vierergruppe $V := \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$.*
- *Für $n \geq 5$ ist der einzige nichttriviale Normalteiler von S_n die alternierende Gruppe A_n.*

UE 54 ► Übungsaufgabe 8.2.3.5. (V) Zeigen Sie Folgerung 8.2.3.4. Hinweis: Betrachten Sie für einen Normalteiler $N \lhd S_n$ den Schnitt $N \cap A_n$. **◄ UE 54**

8.2.4 Die Quaternionengruppe Q_8 und dizyklische Gruppen

Die achtelementige *Quaternionengruppe* Q_8 lässt sich definieren als die (multiplikative) Gruppe komplexer 2×2-Matrizen, die von den Elementen $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ und $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ erzeugt wird. Leicht sieht man einige hilfreiche Eigenschaften ein.

UE 55 ► Übungsaufgabe 8.2.4.1. (B) Zeigen Sie für Q_8: **◄ UE 55**

(1) Die oben angegebenen Erzeugenden erfüllen $BA = A^3B$.

(2) $|Q_8| = 8$.

(3) Es gibt eine Darstellung von Q_8 mit Hilfe der oben angegebenen Erzeugenden A und B und geeigneten Relationen. Mit welchen?

(4) Eine zu Q_8 isomorphe Gruppe G besteht aus den Elementen $\pm 1, \pm i, \pm j, \pm k$ mit $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$ und $ik = -j$ etc. Führen Sie diesen Ansatz aus.

(5) Bestimmen Sie die Ordnungen der Elemente von Q_8 sowie sämtliche Untergruppen, Normalteiler und das Zentrum $Z(Q_8)$.

Die Darstellung von Q_8 mittels Erzeugern und Relationen, nach der in Teil (3) obiger Übungsaufgabe gefragt wurde, lässt sich verallgemeinern:

Satz 8.2.4.2. *Zu jeder positiven natürlichen Zahl n gibt es eine (bis auf Isomorphie eindeutig bestimmte) Gruppe, genannt die* dizyklische Gruppe *Dic_n der Ordnung $4n$ (für Zweierpotenzen auch:* verallgemeinerte Quaternionengruppe*), mit der Darstellung $Dic_n = \langle X|Y\rangle$, wobei X die beiden Erzeuger x, y enthält, und Y den Relationen $x^{2n} = e$, $x^n = y^2$ und $yxy^{-1} = x^{-1}$ entspricht. Für $n = 1$ ist diese Gruppe isomorph zu $C_2 \times C_2$, für $n = 2$ zu Q_8.*

UE 56 ▶ Übungsaufgabe 8.2.4.3. (V) Beweisen Sie Satz 8.2.4.2. **◀ UE 56**

Über die dizyklischen Gruppen $\mathrm{Dic}_2 \cong Q_8$ und Dic_3 der Ordnung 8 bzw. 12 lassen sich noch weitere interessante Aussagen machen, die Gegenstand der folgenden beiden Übungsaufgaben sind und sich bei der Klassifikation in Unterabschnitt 8.2.6 als nützlich erweisen werden.

UE 57 ▶ Übungsaufgabe 8.2.4.4. (B) Zeigen Sie die folgende Aussagen für die Gruppe $Q_8 \cong \mathrm{Dic}_2$. **◀ UE 57**

1. Q_8 wird von zwei Elementen a, b erzeugt. Dabei haben beide die Ordnung 4, und es gelten die Gleichungen $a^2 = b^2$ und $ba = a^{-1}b$.
2. Jede Gruppe der Ordnung 8 mit den Eigenschaften aus 1 ist zu Q_8 isomorph.

UE 58 ▶ Übungsaufgabe 8.2.4.5. (B) Zeigen Sie, dass es eine Gruppe $G \leq S_3 \times C_4$ mit folgenden Eigenschaften gibt. **◀ UE 58**

1. $|G| = 12$.
2. G wird von zwei Elementen a, b erzeugt. Dabei hat a die Ordnung 6, und es gelten die Gleichungen $a^3 = b^2$ und $ba = a^{-1}b$.
3. Jede Gruppe der Ordnung 12 mit den Eigenschaften aus 2 ist zu Dic_3 isomorph.

8.2.5 Zwei weitere Struktursätze

Wir erwähnen noch zwei weitere für die Strukturtheorie endlicher Gruppen typische Sätze. In Unterabschnitt 8.2.6 werden sie sich als hilfreich bei der Klassifikation aller Gruppen der Ordnung ≤ 15 erweisen.

Satz 8.2.5.1. *Jede Gruppe der Ordnung p^2, $p \in \mathbb{P}$, ist abelsch.*

UE 59 ► Übungsaufgabe 8.2.5.2. Beweisen Sie Satz 8.2.5.1. Anleitung: Zeigen Sie, dass jede Gruppe mit zyklischem $G/Z(G)$ abelsch ist. **◄ UE 59**

Satz 8.2.5.3. *Sei G eine Gruppe mit $|G| = pq$ für $p, q \in \mathbb{P}$, wobei $p > q$. Ist G nicht zyklisch (d.h. nicht isomorph zu C_{pq}), dann liegt folgende Situation vor: Es gilt $q|p-1$ und es gibt $a, b \in G$ mit*

(i) $\operatorname{ord}(a) = p$, $\operatorname{ord}(b) = q$

(ii) $G = \langle a, b\rangle$

(iii) Es existiert ein $s \in \mathbb{N}$, sodass $ba = a^s b$ sowie $s \not\equiv 1 \mod p$ und $s^q \equiv 1 \mod p$.

Beweis. Nach dem Satz 8.1.3.2 von Cauchy gibt es $a, b \in G$ mit $\operatorname{ord}(a) = p$, $\operatorname{ord}(b) = q$. Wir zeigen als Erstes, dass $U := \langle a\rangle$ ein Normalteiler von G ist. Klarerweise ist U eine p-Sylowgruppe. Nach Folgerung 8.1.4.4 müssen wir nur zeigen, dass U sogar die einzige p-Sylowgruppe ist. Die Anzahl n der p-Sylowgruppen ist nach dem dritten Sylowsatz (Satz 8.1.4.5) ein Teiler von $|G| = pq$ mit $n \equiv 1 \mod p$. Wegen $p > q$ ist das nur für $n = 1$ möglich.
Die Faktorgruppe G/U hat $|G|/|U| = q \in \mathbb{P}$ Elemente und ist daher zyklisch, wobei jedes vom neutralen Element verschiedene Element ein Erzeuger ist. Wäre $bU = eU$, d.h. $b \in U$, dann wäre $q = \operatorname{ord}(b) \mid |U| = p$, Widerspruch. Also gilt $G/U = \langle bU\rangle$.
Daraus folgt $G = \{b^j a^i \mid 0 \le j \le q-1, 0 \le i \le p-1\}$: Für $g \in G$ ist $gU = (bU)^j = b^j U$ für ein geeignetes $0 \le j \le q-1$, also $b^{-j} g = a^i$ für ein $0 \le i \le p-1$ und somit $g = b^j a^i$. Wir erhalten auch $G = \langle a, b\rangle$.
Sei m die Anzahl der q-Sylowgruppen von G. Wieder nach dem dritten Sylowsatz (Satz 8.1.4.5) gilt $m \mid pq$ und $m \equiv 1 \mod q$. Somit kommen nur $m = 1$ und $m = p$ infrage.
Wenn $m = 1$, dann ergibt sich erneut mit Folgerung 8.1.4.4 auch $V := \langle b\rangle \lhd G$. Aus der oben bewiesenen Darstellung $G = \{b^j a^i \mid 0 \le j \le q-1, 0 \le i \le p-1\}$ folgt $G = V \cdot U$; außerdem gilt $V \cap U = \{e\}$, da die Ordnung jedes Elements von $V \cap U$ sowohl $|V| = q$ als auch $|U| = p$ teilen muss. Nach Proposition 3.2.3.3 ist G das innere direkte Produkt von V und U, d.h. $G = V \odot U \cong V \times U$. Die Gruppen V bzw. U sind zyklische Gruppen der Ordnung q bzw. p, also folgt $G \cong C_q \times C_p \cong C_{pq}$, wobei wir die letzte Isomorphie aus Übungsaufgabe 3.3.2.13 erhalten. Dieser Fall ist nach Voraussetzung ausgeschlossen.
Wenn $m = p$, dann ergibt sich $q \mid p-1$. Um die Zahl s zu finden, sei bemerkt, dass $bab^{-1} \in U$ wegen $U \lhd G$. Daher existiert s mit $bab^{-1} = a^s$ bzw. $ba = a^s b$. Sei zunächst $s \equiv 1 \mod p$ angenommen. Dann gilt $a^s = a$ und daher $ba = ab$. Daraus folgt, dass G abelsch ist, womit $m = 1$ sein müsste, Widerspruch. Somit ist $s \not\equiv 1 \mod p$. Mit Induktion nach j zeigt man $b^j a b^{-j} = a^{s^j}$ für alle $j \ge 1$. Setzen wir speziell $j = q$, dann erhalten wir $a = b^q a b^{-q} = a^{s^q}$ und somit $s^q \equiv 1 \mod p$. □

Folgerung 8.2.5.4. *Ist $p \in \mathbb{P} \setminus \{2\}$ und $|G| = 2p$, dann ist entweder $G \cong C_{2p}$ oder $G \cong D_p$.*

UE 60 ► Übungsaufgabe 8.2.5.5. (V) Beweisen Sie Folgerung 8.2.5.4. **◄ UE 60**

8.2.6 Bemerkungen zur Klassifikation endlicher Gruppen

Die Klassifikation aller endlichen Gruppen scheint aus heutiger Sicht illusorisch. Immerhin gelang 1982 als Zusammenfassung fast unüberschaubar vieler Einzelresultate die Klassifikation aller endlichen einfachen Gruppen (also jener endlichen Gruppen, die nur die trivialen Normalteiler haben). Neben den zyklischen Gruppen C_p von Primzahlordnung p und den alternierenden Gruppen A_n mit $n \geq 5$ treten darin 16 unendliche Serien auf (man nennt sie *Gruppen vom Lie-Typ*) und darüber hinaus 26 sogenannte *sporadische Gruppen*. Doch schon eine genaue Formulierung des entsprechenden Klassifikationssatzes würde unseren Rahmen hier bei Weitem sprengen.
Im Lichte späterer Resultate – nämlich des Satzes von Jordan-Hölder (8.3.4.3) und der Erweiterungstheorie, siehe Abschnitt 8.4 – wird die Bedeutung der Klassifikation der endlichen einfachen Gruppen deutlicher. Denn mit den dort eingeführten Begriffen hat jede endliche Gruppe G eine Kompositionsreihe (siehe Unterabschnitt 8.3.3). Die Faktoren irgendeiner Kompositionsreihe sind nach Jordan-Hölder bis auf Isomorphie und Reihenfolge durch G eindeutig eindeutige bestimmt. Wenn man auch noch versteht, wie diese Faktoren zu verschiedenen Gruppen G zusammengesetzt werden können – und das ist der Gegenstand der Erweiterungstheorie – überblickt man alle endlichen Gruppen. Leider ist die Erweiterungstheorie nicht so mächtig. Erst recht müssen wir uns in dieser Vorlesung äußerst bescheiden mit einer Klassifikation der endlichen Gruppen G der Ordnung $n = |G| \leq 15$ begnügen. Die Tabelle in Abbildung 8.1 gibt darüber hinaus die Anzahl der abelschen und nichtabelschen Isomorphietypen bis zur Ordnung 20 an.
Ähnlich wie bei den meisten Klassifikationen besteht der schwierigste Teil auch hier darin zu beweisen, dass in der Tabelle keine Gruppe fehlt. Dass je zwei Gruppen daraus nicht isomorph sind, folgt relativ leicht mit ein paar bereits bekannten, typischen Eigenschaften der Gruppen. Dieses Programm soll nun etwas genauer besprochen werden, wobei wir die Details allerdings auf mehrere Übungsaufgaben auslagern.
Die in der Tabelle enthaltene Klassifikation der abelschen Gruppen folgt aus dem Hauptsatz 7.4.3.2 über endlich erzeugte abelsche Gruppen bzw. bereits aus Satz 3.3.4.2.

Proposition 8.2.6.1. *Jede abelsche Gruppe mit einer Ordnung $|G| \leq 15$ ist zu genau einer der Gruppen in der Tabelle aus Abbildung 8.1 isomorph.*

UE 61 ► Übungsaufgabe 8.2.6.2. (V) Beweisen Sie Proposition 8.2.6.1. **◄ UE 61**

Klarerweise kann eine derartige Klassifikation für abelsche Gruppen beliebiger Ordnung durchgeführt werden. Behandeln Sie als Test die folgende Frage über deren Anzahl.

UE 62 ► Übungsaufgabe 8.2.6.3. (F,E) Was können Sie über die Anzahl paarweise nichtisomorpher abelscher Gruppen G mit folgender Ordnung n aussagen? **◄ UE 62**

1. $n = p^e$, $p \in \mathbb{P}$, $e \in \mathbb{N}$
2. $n = \prod_{p \in \mathbb{P}} p^{e(p)}$

n	**abelsch** zyklisch / nicht zyklisch	**Anzahl**	**nichtabelsch**	**Anzahl**
1	C_1	1		
2	C_2	1		
3	C_3	1		
4	$C_4, C_2 \times C_2$	2		
5	C_5	1		
6	C_6	1	$S_3 \cong D_3$	1
7	C_7	1		
8	$C_8, C_4 \times C_2, C_2^3$	3	$D_4, Q_8 \cong \mathrm{Dic}_2$	2
9	$C_9, C_3 \times C_3$	2		
10	C_{10}	1	D_5	1
11	C_{11}	1		
12	$C_{12}, C_2 \times C_6$	2	$A_4, D_6 \cong S_3 \times C_2, \mathrm{Dic}_3$	3
13	C_{13}	1		
14	C_{14}	1	D_7	1
15	C_{15}	1		
16	$C_{16}, C_8 \times C_2, C_4^2, C_4 \times C_2^2, C_2^4$	5	...	9
17	C_{17}	1		
18	$C_{18}, C_6 \times C_3$	2	...	3
19	C_{19}	1		
20	$C_{20}, C_{10} \times C_2$	2	...	3

Abbildung 8.1: Klassifikation aller Gruppen G mit kleinem $n = |G|$

3. $n \leq 100$

4. $n \leq N$ für wachsendes N (Asymptotik in N?)

Wir wenden uns nun den nichtabelschen Gruppen in Abbildung 8.1 zu.

Proposition 8.2.6.4. *Die in der Tabelle von Abbildung 8.1 angegebenen nichtabelschen Gruppen G mit $n = |G| \leq 15$ sind paarweise nicht isomorph zueinander.*

UE 63 ► **Übungsaufgabe 8.2.6.5.** (V) Begründen Sie Proposition 8.2.6.4. (Offenbar sind lediglich die drei Gruppen A_4, D_6 und Dic_3 untereinander zu vergleichen sowie D_4 mit Q_8.) ◄ **UE 63**

UE 64 ► **Übungsaufgabe 8.2.6.6.** (V) Verwenden Sie die Ergebnisse aus Unterabschnitt 8.2.5, um zu zeigen, dass jede Gruppe G mit $|G| = n \in \{1, 2, 3, 4, 5, 7, 9, 11, 13, 15\}$ abelsch ist. ◄ **UE 64**

UE 65 ► **Übungsaufgabe 8.2.6.7.** (V) Zeigen Sie, dass jede nichtabelsche Gruppe G mit $|G| = 8$ entweder zu D_4 oder zu $Q_8 \cong \mathrm{Dic}_2$ isomorph ist.
Hinweis: Zeigen Sie zuerst, dass G ein Element a mit $\mathrm{ord}(a) = 4$ enthalten muss. Wählen Sie irgendein $b \notin U := \langle a \rangle$ und zeigen Sie $G = \langle a, b \rangle$, $U \lhd G$ sowie $b^2 \in U$ (zB: G/U betrachten). Welche Möglichkeiten gibt es für b^2? Welche Möglichkeiten gibt es für bab^{-1}? Verwenden Sie die Übungsaufgaben 8.2.2.2 und 8.2.4.4. ◄ **UE 65**

UE 66 ► **Übungsaufgabe 8.2.6.8.** (V) Zeigen Sie, dass jede nichtabelsche Gruppe G mit $|G| = 12$ entweder zu A_4 oder zu $D_6 \cong S_3 \times C_2$ oder zu Dic_3 isomorph ist.
Anleitung: Sei $c \in G$ mit $\mathrm{ord}(c) = 3$ (warum existiert so ein c?) und $P := \langle c \rangle$. Verwenden Sie die Aktion von G auf den Linksnebenklassen von P durch Linkstranslation, um einen Homomorphismus $f : G \to S_4$ mit $\ker f \subseteq P$ zu konstruieren. Entweder $\ker f = \{e\}$ und G ist isomorph zu einer Untergruppe von S_4 – verwenden Sie Folgerung 8.2.3.4. Oder $\ker f = P$ (warum gibt es keine weiteren Optionen?), also $P \lhd G$. Verwenden Sie den zweiten Sylowsatz 8.1.4.3, um zu zeigen, dass G nur zwei Elemente der Ordnung 3 haben kann. Zeigen Sie $[G : Z_G(c)] \in \{1, 2\}$ und leiten Sie daraus her, dass es $d \in Z_G(c)$ mit $\mathrm{ord}(d) = 2$ gibt. Setzen Sie $a := cd$. Welche Ordnung hat a? Wählen sie irgendein $b \notin U := \langle a \rangle$ und zeigen Sie $G = \langle a, b \rangle$, $U \lhd G$ sowie $b^2 \in U$ (zB: G/U betrachten). Welche Möglichkeiten gibt es für bab^{-1}? Welche Möglichkeiten gibt es für b^2? Verwenden Sie die Übungsaufgaben 8.2.2.2 und 8.2.4.5. ◄ **UE 66**

Damit sind alle Bestandteile für folgenden zusammenfassenden Satz gesammelt.

Satz 8.2.6.9. *Jede Gruppe mit einer Ordnung $|G| \leq 15$ ist zu genau einer der Gruppen in der Tabelle aus Abbildung 8.1 isomorph.*

8.3 Nilpotenz, Auflösbarkeit und Subnormalreihen

Die Struktur abelscher Gruppen ist, wie wir bereits gesehen haben, wesentlich überschaubarer als die beliebiger Gruppen. Es liegt daher nahe, nichtabelsche Gruppen unter dem Gesichtspunkt zu untersuchen, wie stark sie vom Abelschsein abweichen. Zwei wichtige Konzepte, die das zum Ausdruck bringen, sind Nilpotenz und Auflösbarkeit. Nilpotenz (8.3.1) kommt gewissermaßen von unten, indem sie vom Zentrum einer Gruppe ausgeht, also von der Untergruppe (sogar Normalteiler) jener Elemente, die mit allen anderen vertauschen. Iteration der Zentrumsbildung in einem geeigneten Sinn führt zur sogenannten aufsteigenden Zentralreihe. Bei Auflösbarkeit (8.3.2) geht es, sozusagen von oben kommend, darum, ob eine Gruppe durch Faktorisierung nach einem nicht zu großen Normalteiler abelsch gemacht werden kann. Iteriert man auch diesen Prozess, so stößt man in sehr natürlicher Weise auf die Konzepte Normal-, Subnormal- und Kompositionsreihe (8.3.3), über die der Satz von Jordan-Hölder, fußend auf dem Lemma von Zassenhaus und dem Satz von Schreier, eine sehr starke Aussage macht (8.3.4).

8.3.1 Nilpotente Gruppen

Wie bisher bezeichne $Z(G)$ das Zentrum einer Gruppe G.

Definition 8.3.1.1. Sei G eine Gruppe. Die *aufsteigende Zentralreihe* ist die Folge von Untergruppen $Z_i = Z_i(G) \leq G$ mit

$$Z_0 \leq Z_1 \leq Z_2 \leq \ldots,$$

die rekursiv definiert sind durch:

$$Z_0 := \{e\},\ Z_{i+1} := \kappa_i^{-1}(Z(G/Z_i))$$

mit den kanonischen Homomorphismen $\kappa_i \colon G \to G/Z_i,\ g \mapsto gZ_i$. Die Gruppe G heißt *nilpotent*, wenn es ein $n \in \mathbb{N}$ gibt mit $Z_n = G$.

Man beachte, dass wegen $Z(G/Z_i) \lhd G/Z_i$ die Faktorgruppe $\frac{G/Z_i}{Z(G/Z_i)} = (G/Z_i)/Z(G/Z_i)$ gebildet werden kann. Als Urbild des Normalteilers $Z(G/Z_i)$ unter dem kanonischen Homomorphismus κ_i ist auch Z_{i+1} ein Normalteiler von G, und nach dem Zweiten Isomorphiesatz 2.2.6.7 gilt $\frac{G/Z_i}{Z(G/Z_i)} \cong G/Z_{i+1}$.
Klarerweise ist jede abelsche Gruppe nilpotent. Doch das Konzept geht viel weiter, wie der folgende Satz zeigt:

Satz 8.3.1.2. *Jede endliche p-Gruppe ist nilpotent.*

UE 67 ► Übungsaufgabe 8.3.1.3. (V) Folgern Sie Satz 8.3.1.2 aus Folgerung 8.1.3.1. **◄ UE 67**

Wenig überraschend und nicht sehr schwer zu beweisen sind folgende Vererbungseigenschaften von Nilpotenz.

Proposition 8.3.1.4.

1. *Das direkte Produkt endlich vieler nilpotenter Gruppen ist nilpotent.*
2. *Jede Untergruppe einer nilpotenten Gruppe ist nilpotent.*
3. *Jede Faktorgruppe einer nilpotenten Gruppe ist nilpotent.*

UE 68 ► Übungsaufgabe 8.3.1.5. (V) Beweisen Sie Proposition 8.3.1.4. **◄ UE 68**

Unter den endlichen Gruppen lassen sich die nilpotenten auf sehr griffige Weise charakterisieren. Hilfreich ist dabei das folgende Lemma.

Lemma 8.3.1.6. *Sei G eine nilpotente Gruppe mit einer echten Untergruppe $H \lneqq G$. Dann ist $H \lneqq N_G(H)$, d.h. H ist eine echte Untergruppe auch seines Normalisators $N_G(H)$.*

Beweis. Sei n maximal mit $Z_n \leq H$. Dann gibt es ein $a \in Z_{n+1} \setminus H$. Es genügt zu zeigen, dass so ein a auch im Normalisator $N_G(H)$ liegt. Weil a in $Z_{n+1} = \kappa_n^{-1}(Z(G/Z_n))$ liegt, vertauscht es modulo Z_n mit allen $g \in G$. Insbesondere bedeutet das für ein beliebiges $h \in H$, dass $Z_n ah = (Z_n a)(Z_n h) = (Z_n h)(Z_n a) = Z_n ha$. Folglich gibt es ein $h' \in Z_n \leq H$, sodass $ah = h'ha$ bzw. $aha^{-1} = h'h \in H$, also tatsächlich $a \in N_G(H)$. □

Damit können wir die angekündigte Charakterisierung nilpotenter Gruppen beweisen – man beachte die partielle Analogie zu Satz 3.3.3.6.

Satz 8.3.1.7. *Sei G eine endliche Gruppe. Dann sind die folgenden Aussagen äquivalent:*

1. *G ist nilpotent.*
2. *Zu jedem $p \in \mathbb{P}$ hat G genau eine p-Sylowgruppe.*
3. *$G = \bigodot_{p\in\mathbb{P}} G_p$ (inneres direktes Produkt, siehe Definition 3.2.3.12) mit einer p-Sylowgruppe G_p von G zu jedem $p \in \mathbb{P}$.*
4. *Zu jedem $p \in \mathbb{P}$ gibt es eine nilpotente p-Gruppe H_p, wobei nur endlich viele H_p nichttrivial sind, sodass $G \cong \prod_{p\in\mathbb{P}} H_p$.*

Beweis. $1 \Rightarrow 2$: Sei G nilpotent und $G_p \lneqq G$ eine p-Sylowgruppe von G. Laut Folgerung 8.1.4.6 gilt $H := N_G(G_p) = N_G(N_G(G_p))$. Nach Lemma 8.3.1.6 ist das nur für $H = G$ möglich, also ist

$$G_p \lhd N_G(G_p) = H = G.$$

Daher ist G_p wegen Folgerung 8.1.4.4 die einzige p-Sylowgruppe von G.
$2 \Rightarrow 3$: Sei $|G| = \prod_{p\in\mathbb{P}} p^{n_p}$ (nur endlich viele n_p sind von 0 verschieden), und sei für jedes $p \in \mathbb{P}$ die (laut Voraussetzung eindeutige) p-Sylowgruppe von G mit G_p bezeichnet. Nach Satz 8.1.4.2 gilt $|G_p| = p^{n_p}$, und nach Folgerung 8.1.4.4 sind alle G_p Normalteiler. Für paarweise verschiedene Primzahlen $p, p_1, \ldots, p_n$ gilt $G_p \cap \prod_{j=1}^{n} G_{p_j} = \{e\}$, denn die

Ordnung jedes Elements in diesem Schnitt muss die teilerfremden Zahlen $|G_p| = p^{n_p}$ und $|\prod_{j=1}^{n} G_{p_j}| = \prod_{j=1}^{n} p_j^{n_{p_j}}$ teilen. Das Komplexprodukt von Normalteilern ist wieder ein Normalteiler (siehe Proposition 3.2.2.9). Nach Satz 3.2.3.15 bilden die G_p daher ein inneres direktes Produkt $P := \bigodot_{p\in\mathbb{P}} G_p \leq G$. Wegen

$$|P| = \prod_{p\in\mathbb{P}} |G_p| = \prod_{p\in\mathbb{P}} p^{n_p} = |G|$$

muss P bereits ganz G sein.
$3 \Rightarrow 4$: Nach Satz 8.3.1.2 sind die p-Sylowgruppen G_p als p-Gruppen nilpotent. Damit folgt die Aussage direkt aus Definition 3.2.3.12 kombiniert mit der Tatsache, dass wegen der Endlichkeit von G nur endlich viele p-Sylowgruppen G_p nichttrivial sein können.
$4 \Rightarrow 1$: Nach Proposition 8.3.1.4 ist G als de facto nur endliches direktes Produkt nilpotenter Gruppen selbst nilpotent. □

8.3.2 Auflösbare Gruppen

Zwei Gruppenelemente a, b vertauschen genau dann, wenn $ab = ba$ oder, äquivalent, wenn $aba^{-1}b^{-1} = e$ gilt. Von dieser Beobachtung gehen wir aus, wenn wir die Frage untersuchen, wie ein Normalteiler $N \lhd G$ beschaffen sein muss, damit G/N abelsch ist.

Definition 8.3.2.1. Für $a, b \in G$ heißt das Element $[a, b] := aba^{-1}b^{-1}$ *Kommutator* von a und b. Die von allen Kommutatoren erzeugte Gruppe $G' := \langle\{[a, b] \mid \ a, b \in G\}\rangle$ heißt die *Ableitung* oder auch *Kommutatorgruppe* von G.
Die (höheren) *abgeleiteten Untergruppen*

$$G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \ldots$$

sind rekursiv definiert durch:

$$G^{(0)} := G,\ G^{(i+1)} := (G^{(i)})'.$$

G heißt *auflösbar*, wenn es ein $n \in \mathbb{N}$ gibt mit $G^{(n)} = \{e\}$.

Jeder Endomorphismus $f\colon G \to G$ erfüllt $f([a, b]) = [f(a), f(b)]$, bildet also Kommutatoren auf Kommutatoren ab. Entsprechendes gilt für die erzeugten Untergruppen, also $f(G') \leq G'$. Insbesondere gilt diese Beziehung, wenn f ein innerer Automorphismus von G ist, also ist G' ein Normalteiler von G. Wir halten fest:

Proposition 8.3.2.2. *Für eine Gruppe G und ihre Ableitung G' gilt $G' \lhd G$.*

Für einen Homomorphismus $f\colon G \to H$ in eine abelsche Gruppe H liegt wegen $f([a, b]) = f(a)f(b)f(a)^{-1}f(b)^{-1} = e$ jeder Kommutator im Kern, also ist ganz G' im Kern von f enthalten. Sei $\kappa\colon G \to G/G'$ die kanonische Abbildung. Der Kern von κ ist genau G'. Folglich gibt es nach dem Homomorphiesatz genau einen Homomorphismus $g\colon G/G' \to H$ mit $f = g \circ \kappa$, nämlich $gG' \mapsto f(g)$. Ist speziell $N \lhd G$ und $f\colon G \to G/N$, $g \mapsto gN$, der kanonische Homomorphismus, lesen wir insbesondere ab:

Proposition 8.3.2.3. *Für einen Normalteiler $N \lhd G$ sind äquivalent:*

1. *G/N ist abelsch.*
2. *$G' \subseteq N$.*

Auflösbarkeit vererbt sich in ähnlicher Weise wie Nilpotenz:

Proposition 8.3.2.4.

1. *Das direkte Produkt endlich vieler auflösbarer Gruppen ist auflösbar.*
2. *Jede Untergruppe einer auflösbaren Gruppe ist auflösbar.*
3. *Jede Faktorgruppe einer auflösbaren Gruppe ist auflösbar.*
4. *Ist $N \lhd G$ und sind N und G/N auflösbar, dann ist auch G auflösbar.*

UE 69 ► Übungsaufgabe 8.3.2.5. (V) Beweisen Sie Proposition 8.3.2.4. **◄ UE 69**

Von großem Interesse ist der folgende Satz:

Satz 8.3.2.6. *Jede nilpotente Gruppe ist auflösbar.*

Beweis. Ist G nilpotent, so gibt es ein $n \in \mathbb{N}$ mit $Z_n = G$. Wir zeigen mittels Induktion nach i, dass $G^{(i)} \leq Z_{n-i}$ gilt, was für $i = n$ die Behauptung beweist.
Für $i = 0$ ist die Behauptung $G^{(0)} \leq Z_n = G$ trivialerweise wahr. Für den Schritt von i auf $i + 1$ dürfen wir von der Induktionsannahme $G^{(i)} \leq Z_{n-i}$ ausgehen. Laut Definition der aufsteigenden Zentralreihe ist $Z_{n-i}/Z_{n-(i+1)}$ abelsch und wir erhalten $Z'_{n-i} \leq Z_{n-(i+1)}$ nach Proposition 8.3.2.3. Daraus folgt aber bereits die Induktionsbehauptung $G^{(i+1)} = (G^{(i)})' \leq Z'_{n-i} \leq Z_{n-(i+1)}$. □

UE 70 ► Übungsaufgabe 8.3.2.7. (B,D) Man untersuche interessante Beispiele (endlicher und unendlicher) nichtabelscher Gruppen auf Nilpotenz und Auflösbarkeit, insbesondere alle Gruppen der Ordnung ≤ 15 oder Gruppen linearer Transformationen von Vektorräumen. **◄ UE 70**

8.3.3 Subnormalreihen

Definition 8.3.3.1. Sei G eine Gruppe. Eine absteigende Folge

$$G = G_0 \geq G_1 \geq \ldots \geq G_n = \{e\}$$

von Untergruppen heißt *Subnormalreihe*, sofern $G_{i+1} \lhd G_i$ für $i = 1, \ldots, n-1$ gilt. Die $F_i := G_i/G_{i+1}$ heißen die *Faktoren* der Subnormalreihe. Die Anzahl der F_i mit $|F_i| > 1$ heißt die *Länge* der Subnormalreihe.

Ist $G_{i+1} \lhd N \lhd G_i$, so nennt man

$$G = G_0 \geq G_1 \geq \ldots \geq G_i \geq N \geq G_{i+1} \geq \ldots \geq G_n = \{e\}$$

eine *Einschrittverfeinerung* der Subnormalreihe. Iteration von Einschrittverfeinerungen liefert beliebige *Verfeinerungen* der Subnormalreihe. Die Verfeinerung heißt *echt*, wenn sich durch sie die Länge der Subnormalreihe vergrößert (wenn also $G_{i+1} \neq N \neq G_i$).
Sind alle Faktoren einfach und nichttrivial (d.h. $|F_i| > 1$), so spricht man von einer *Kompositionsreihe*.
Ist $G_i \lhd G$ für alle $i = 1, \ldots, n$, sind also die G_i Normalteiler sogar in ganz G, so nennt man eine Subnormalreihe auch eine *Normalreihe*.
Eine Subnormalreihe heißt *auflösbar*, wenn alle Faktoren abelsch sind.
Zwei Subnormalreihen heißen *äquivalent*, wenn sie gleich lang sind und wenn es eine Bijektion zwischen den Faktoren gibt, sodass je zwei Partner zueinander isomorph sind.

Zur Einübung der Begriffe zwei leichte Übungsaufgaben:

UE 71 ► Übungsaufgabe 8.3.3.2. (F) Begründen Sie: **◄ UE 71**

(i) Sei N ein echter Normalteiler der Gruppe G. Dann ist G/N genau dann einfach, wenn N als echter Normalteiler maximal ist.

(ii) Eine Subnormalreihe mit Faktoren $|F_i| > 1$ ist genau dann Kompositionsreihe, wenn keine echte Verfeinerung existiert.

(iii) Jede Subnormalreihe einer endlichen Gruppe lässt sich zu einer Kompositionsreihe verfeinern. Insbesondere hat jede endliche Gruppe eine Kompositionsreihe.

Hinweis: Isomorphiesätze können nützlich sein.

UE 72 ► Übungsaufgabe 8.3.3.3. (F) Begründen Sie: **◄ UE 72**

(i) Jede Verfeinerung einer auflösbaren Subnormalreihe ist auflösbar.

(ii) Eine Gruppe ist genau dann auflösbar, wenn sie eine auflösbare Subnormalreihe besitzt. Hinweis: Zeigen Sie zu einer vorgegebenen auflösbaren Subnormalreihe $G = G_0 \geq G_1 \geq \ldots \geq G_n = \{e\}$ mittels Induktion nach i die Inklusion $G^{(i)} \leq G_i$.

(iii) Eine endliche Gruppe ist genau dann auflösbar, wenn sie eine Kompositionsreihe mit Faktoren $F_i \cong C_{p_i}$, $p_i \in \mathbb{P}$, besitzt.

(iv) Ist G eine endliche auflösbare Gruppe, dann gibt es einen Normalteiler $H \lhd G$ mit $[G : H] \in \mathbb{P}$.

Hinweis: Isomorphiesätze können nützlich sein.

8.3.4 Die Sätze von Zassenhaus, Schreier und Jordan-Hölder

Das Hauptergebnis dieses Unterabschnitts ist der Satz 8.3.4.3 von Jordan-Hölder, wonach je zwei Kompositionsreihen einer Gruppe G äquivalent sind. Somit stellt, sofern es überhaupt eine Kompositionsreihe von G gibt, die (ungeordnete) Familie der Faktoren eine Isomorphieinvariante für G dar.
Der Grundgedanke des Beweises besteht darin, zu je zwei Subnormalreihen Verfeinerungen zu finden, die äquivalent zueinander sind. Ist dies immer möglich – und das ist der Inhalt des Satzes 8.3.4.2 von Schreier –, so folgt der Satz von Jordan-Hölder sehr schnell. Für den Beweis des Satzes von Schreier besteht die Aufgabe also darin, zwei gegebene Subnormalreihen

$$\text{(I)} \quad G = G_0 \geq G_1 \geq \ldots \geq G_n = \{e\}$$

und

$$\text{(II)} \quad G = H_0 \geq H_1 \geq \ldots \geq H_m = \{e\}$$

von G geeignet zu verfeinern. Das gelingt, indem man zwischen aufeinanderfolgende Glieder $G_i \geq G_{i+1}$ in (I) jeweils eine die zweite Subnormalreihe (II) imitierende Folge von Gruppen $G(i,j)$ dazwischen schaltet, sodass

$$G_i = G(i,0) \geq G(i,1) \geq \ldots \geq G(i,j) \geq \ldots \geq G(i,m{-}1) \geq G(i,m) = G(i{+}1,0) = G_{i+1},$$

und vice versa mit vertauschten Rollen von (I) und (II). Naheliegenderweise soll $G(i,j)$ (monoton) von H_j abhängen. Rein verbandstheoretisch betrachtet bieten sich, um die Nebenbedingung $G_i \geq G(i,j) \geq G_{i+1}$ zu garantieren, an dieser Stelle zwei Definitionen für $G(i,j)$ an, nämlich $G_i \wedge (G_{i+1} \vee H_j)$ und $G_{i+1} \vee (G_i \wedge H_j)$. Die erste scheidet schnell aus, weil die von G_{i+1} und H_j erzeugte Untergruppe $G_{i+1} \vee H_j$ im allgemeinen Fall schwer zu handhaben ist. Im Gegensatz dazu lässt sich mit der Definition $G(i,j) := G_{i+1} \vee (G_i \wedge H_j) = G_{i+1}(G_i \cap H_j)$ (hier fließt $G_{i+1} \lhd G_i$ ein) bestens weiterarbeiten. Es zeigt sich nämlich $G(i,j+1) \lhd G(i,j)$ (siehe Lemma 8.3.4.1(a)), außerdem natürlich $G(i,m) = G(i+1,0)$. Also liegt eine Subnormalreihe mit Länge $\leq nm$ vor. Symmetrisches gilt, wenn man $H(i,j) := H_{j+1}(H_j \cap G_i)$ setzt.
Die beiden auf diese Weise erhaltenen Subnormalreihen sind äquivalent, sofern

$$G(i,j)/G(i,j+1) =: \frac{G(i,j)}{G(i,j+1)} \cong \frac{H(i,j)}{H(i+1,j)} := H(i,j)/H(i+1,j)$$

für $0 \leq i < n$ und $0 \leq j < m$ gezeigt werden kann. Denn dadurch wird offenbar eine bijektive Beziehung zwischen paarweise isomorphen Faktoren hergestellt. Der Nachweis dieser Isomorphie wiederum gelingt, indem man ein symmetrisches Zwischenglied identifiziert, welches zu beiden Gruppen isomorph ist. Dieses Zwischenglied ist die Gruppe

$$\frac{G_i \cap H_j}{(G_{i+1} \cap H_j)(G_i \cap H_{j+1})}.$$

Genau diese Situation wird im nun folgenden sogenannten *Lemma von Zassenhaus*, genannt auch *Schmetterlingslemma* (vgl. Abbildung 8.2), behandelt, wobei $G_i = A$, $G_{i+1} = A^*$, $H_j = B$ und $H_{j+1} = B^*$ zu setzen ist.

Lemma 8.3.4.1 (Zassenhaus, vgl. Abbildung 8.2)**.** *Sei G eine Gruppe, $A^* \lhd A \leq G$ und $B^* \lhd B \leq G$. Dann folgt*

(a) $A^*(A \cap B^*) \lhd A^*(A \cap B)$,

(b) $B^*(A^* \cap B) \lhd B^*(A \cap B)$ *und*

(c) $\frac{A^*(A\cap B)}{A^*(A\cap B^*)} \cong \frac{B^*(A\cap B)}{B^*(A^*\cap B)}$.

Beweis. Wegen $B^* \lhd B$ ist auch $A \cap B^* = (A \cap B) \cap B^* \lhd A \cap B$. Analog folgt $A^*\cap B \lhd A\cap B$. Daraus erhält man unmittelbar $D := (A^*\cap B)(A\cap B^*) \lhd A\cap B$. Außerdem gilt $A^*(A\cap B) \leq A$ und $B^*(A\cap B) \leq B$. Wir werden einen surjektiven Homomorphismus $f\colon A^*(A \cap B) \to (A \cap B)/D$ mit $\ker f = A^*(A \cap B^*)$ definieren. Dann folgt nämlich $A^*(A \cap B^*) \lhd A^*(A \cap B)$, also Aussage (a), analog (b). Nach dem Homomorphiesatz gilt dann aber auch $\frac{A^*(A\cap B)}{A^*(A\cap B^*)} \cong \frac{A\cap B}{D}$, womit, wieder aus Symmetriegründen, auch $\frac{A\cap B}{D} \cong \frac{B^*(A\cap B)}{B^*(A^*\cap B)}$ und somit die Behauptung (c) folgt.
Wir definieren f folgendermaßen: Für $a \in A^*, c \in A \cap B$ sei

$$f(ac) := Dc \in (A \cap B)/D.$$

Damit ist f wohldefiniert, denn sind $a_1, a_2 \in A^*, c_1, c_2 \in A \cap B$ mit $a_1c_1 = a_2c_2$, dann ist

$$a_2^{-1}a_1 = c_2c_1^{-1} \in A^* \cap (A \cap B) = A^* \cap B \subseteq D,$$

also $Dc_1 = Dc_2$. Offensichtlich ist f surjektiv. Wir zeigen nun die Homomorphiebedingung: Wegen $A^* \lhd A$ gibt es für beliebige $a_1, a_2 \in A^*$ und $c_1, c_2 \in A \cap B$ ein $a_3 \in A^*$ mit $c_1a_2 = a_3c_1$. Daraus folgt

$$f((a_1c_1)(a_2c_2)) = f(a_1a_3c_1c_2) = Dc_1c_2 = Dc_1Dc_2 = f(a_1c_1)f(a_2c_2).$$

Also ist f ein Homomorphismus.
Wir müssen nur noch zeigen, dass auch $\ker f = A^*(A \cap B^*)$ gilt. Für $a \in A^*$ und $c \in A \cap B$ ist $ac \in \ker f$ genau dann, wenn $c \in D$. Für den Beweis der ersten Inklusion $\ker f \subseteq A^*(A \cap B^*)$ nehmen wir also $a \in A$ und $c \in A \cap B$ mit $ac \in \ker f$, d.h. $c \in D$ an. Nach Definition von D gibt es dann Elemente $a_1 \in A^* \cap B$ und $c_1 \in A \cap B^*$ mit $c = a_1c_1$, folglich liegt $ac = (aa_1)c_1$ in $A^*(A \cap B^*)$. Für die umgekehrte Inklusion $A^*(A \cap B^*) \subseteq \ker f$ seien nun Elemente $a \in A^*$ und $c \in A \cap B^*$ gegeben. Dann gilt $c \in D$, also $ac \in \ker f$. □

In der oben (vor Lemma 8.3.4.1) beschriebenen Weise folgt hieraus der Satz von Schreier.

Satz 8.3.4.2 (Schreier)**.** *Je zwei Subnormalreihen ein und derselben Gruppe G haben äquivalente Verfeinerungen.*

Da zwei Kompositionsreihen nur sich selbst als Verfeinerung besitzen, ist damit auch unser Hauptresultat bewiesen:

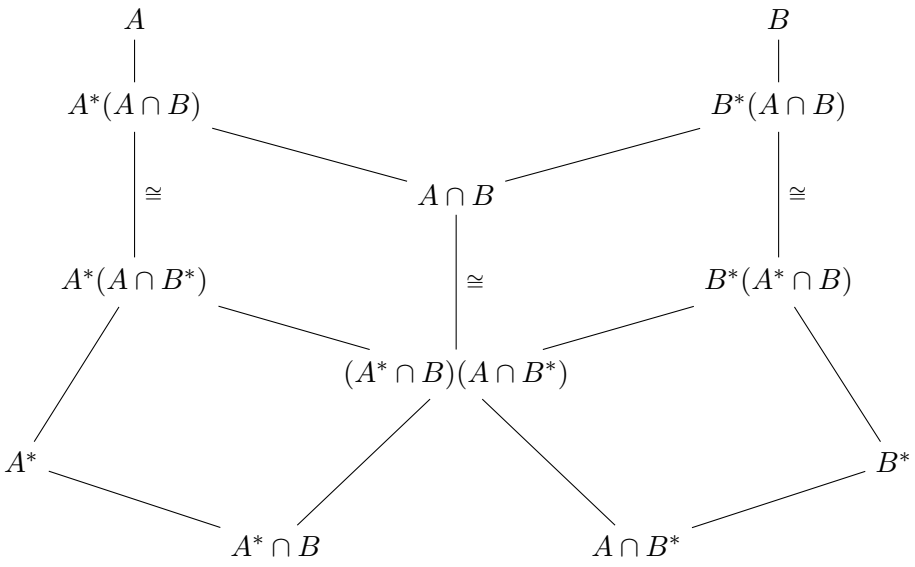


Abbildung 8.2: „Schmetterlingslemma“

Satz 8.3.4.3 (Jordan-Hölder)**.** *Je zwei Kompositionsreihen ein und derselben Gruppe G sind äquivalent.*

Man beachte, dass für zwei äquivalente Kompositionsreihen

$$G = G_0 \geq G_1 \geq \cdots \geq G_n = \{e\}$$
$$G = H_0 \geq H_1 \geq \cdots \geq H_n = \{e\}$$

nicht zwingend $G_i/G_{i+1} \cong H_i/H_{i+1}$ für alle i gelten muss, sondern eventuell eine Umordnung der Faktoren notwendig ist. Zur Illustration ein einfaches Beispiel:

Beispiel 8.3.4.4. Sei $G = C_6 = \{\bar{0}, \bar{1}, \ldots, \bar{5}\}$ und $G_1 := \{\bar{0}, \bar{2}, \bar{4}\} \cong C_3$ sowie $H_1 := \{\bar{0}, \bar{3}\} \cong C_2$. Dann sind

$$G = G_0 \geq G_1 \geq G_2 = \{\bar{0}\}$$
$$G = H_0 \geq H_1 \geq H_2 = \{\bar{0}\}$$

zwei Kompositionsreihen und es gilt $G_0/G_1 \cong H_1/H_2$ sowie $G_1/G_2 \cong H_0/H_1$.

Für die Galoistheorie von Bedeutung ist die aus dem Satz von Jordan-Hölder folgende Nichtauflösbarkeit der symmetrischen Gruppen großer Ordnung:

Folgerung 8.3.4.5. *Die symmetrische Gruppe S_n ist für $n \leq 4$ auflösbar, sonst nicht.*

UE 73 ► Übungsaufgabe 8.3.4.6. (V) Beweisen Sie Folgerung 8.3.4.5. Hinweis: Satz 8.2.3.2 bzw. Folgerung 8.2.3.4. **◄ UE 73**

Eines der spektakulärsten Resultate über die Auflösbarkeit von Gruppen ist der *Satz von Feit-Thompson*: Jede Gruppe ungerader Ordnung ist auflösbar. Die Aussage wurde schon im Jahr 1911 vom bedeutenden Gruppentheoretiker William Burnside (1852-1927) vermutet, aber erst im Jahr 1963 von Walter Feit (1930-2004) und John Griggs Thompson (geb. 1932) in einer 250 Seiten langen Arbeit bewiesen. Vielleicht erweisen sich die folgenden Übungsaufgaben als leichter:

UE 74 ► Übungsaufgabe 8.3.4.7. (F) Zeigen Sie: **◄ UE 74**

(1) Eine abelsche Gruppe besitzt genau dann eine endliche Kompositionsreihe, wenn sie endlich ist.

(2) Eine auflösbare Gruppe mit einer Kompositionsreihe ist endlich.

(3) Jede Gruppe G mit $|G| = p^2q$ für $p, q \in \mathbb{P}$ ist auflösbar. Hinweis: Satz 8.2.5.1.

UE 75 ► Übungsaufgabe 8.3.4.8. (B) Finden Sie (wenn möglich alle) Kompositionsreihen verschiedener Gruppen G: **◄ UE 75**

(1) G endlich und abelsch mit vorgegebener Ordnung $n = |G| = \prod_{p\in\mathbb{P}} p^{e(p)}$

(2) G nichtabelsch mit $|G| \leq 15$

(3) $G = S_4$

(4) $G = S_n$ mit $n \geq 5$

(5) Ein unendliches G Ihrer Wahl mit endlicher Kompositionsreihe.

Zum Abschluss dieses Themenkomplexes wollen wir vergleichen bzw. zusammenfassen, welche Eigenschaften betreffend Untergruppen/Normalteiler einer gewissen Größe allgemeine, auflösbare und nilpotente Gruppen haben. Zunächst zwei Übungsaufgaben:

UE 76 ► Übungsaufgabe 8.3.4.9. (F) Zeigen Sie: Sei G eine endliche nilpotente Gruppe. Dann gibt es zu jedem Teiler t von $n := |G|$ eine Untergruppe $U \leq G$ mit $|U| = t$.
Hinweis: Nehmen Sie zuerst an, dass G eine p-Gruppe ist. **◄ UE 76**

UE 77 ► Übungsaufgabe 8.3.4.10. (B) **◄ UE 77**

(1) Finden Sie eine endliche auflösbare Gruppe G und einen Teiler t von $n := |G|$, sodass es *keine* Untergruppe $U \leq G$ mit $|U| = t$ gibt.

(2) Finden Sie eine endliche auflösbare Gruppe G und einen Primteiler p von $n := |G|$, sodass es *keinen* Normalteiler $N \lhd G$ mit $[G : N] = p$ gibt.

Sei G eine endliche Gruppe mit $n := |G|$. Damit erhalten wir:

1. Allgemeine Gruppen:

   Für jede Primzahl $p \in \mathbb{P}$ mit $p \mid n$ gibt es eine Untergruppe $U \leq G$ mit $|U| = p$.
   (Satz von Cauchy, Satz 8.1.3.2)

   Stärker: Für jede Primpotenz p^k, $p \in \mathbb{P}, k \geq 1$ mit $p^k \mid n$ gibt es eine Untergruppe $U \leq G$ mit $|U| = p^k$.
   (1. Sylowsatz, Satz 8.1.4.2)

   Ist m maximal mit $p^m \mid n$, so gilt für $U \leq G$ mit $|U| = p^m$ genau dann $U \lhd G$, wenn U die einzige Untergruppe mit $|U| = p^m$ ist.
   (2. Sylowsatz, Satz 8.1.4.3)

   Ist m maximal mit $p^m \mid n$, so ist die Anzahl der Untergruppen U mit $|U| = p^m$ ein Teiler von n und kongruent zu 1 modulo p.
   (3. Sylowsatz, Satz 8.1.4.5)

   Im Allgemeinen muss es keinen Normalteiler $H \lhd G$ geben mit $[G : H] \in \mathbb{P}$.
   (Man betrachte zum Beispiel eine einfache Gruppe, die nicht von Primordnung ist, wie A_5.)

2. Auflösbare Gruppen:

   Es existiert eine Primzahl $p \in \mathbb{P}$ mit $p \mid n$, sodass es einen Normalteiler $H \lhd G$ mit $[G : H] = p$ gibt. Im Allgemeinen gilt das aber nicht für alle $p \in \mathbb{P}$ mit $p \mid n$. Im Allgemeinen gibt es nicht für alle Teiler $t \mid n$ eine Untergruppe $U \leq G$ mit $|U| = t$.
   (Übungsaufgaben 8.3.3.3(iv), 8.3.4.10)

3. Nilpotente Gruppen:

   Für alle Teiler $t \mid n$ gibt es eine Untergruppe $U \leq G$ mit $|U| = t$.
   (Übungsaufgabe 8.3.4.9)

8.4 Konstruktionen zur Erweiterung von Gruppen

Der Satz von Jordan-Hölder (8.3.4.3) besagt, dass jede Gruppe G, die eine Kompositionsreihe $\{e\} = G_0 \leq G_1 \leq \ldots \leq G_n = G$ besitzt, eine bis auf Isomorphie und Reihenfolge eindeutige Familie von einfachen Faktoren $F_i \cong G_i/G_{i-1}$, $i = 1, \ldots, n$, bestimmt. Umgekehrt kann man fragen, welche Struktur für G möglich ist, wenn man die Faktoren F_i vorgibt. Sicher ist das direkte Produkt $P = \prod_{i=1}^{n} F_i$ eine Möglichkeit. Im Allgemeinen gibt es aber viele andere, zu P nicht isomorphe Gruppen G mit Faktoren, die zu den F_i isomorph sind.
Schon der Fall mit $n = 2$ und vorgegebenem $F_1 \cong G_1 = N \lhd G$ und $F_2 = K \cong G/N$ ist von Interesse und keineswegs trivial. Man spricht von Erweiterungen von N mit K (8.4.1). Einen wichtigen Spezialfall davon bilden semidirekte Produkte (8.4.2). Er

ist dadurch gekennzeichnet, dass der Faktor K auch als Untergruppe in G realisiert werden kann, sodass die Einbettung von K in G mit der Faktorisierung nach N in einem natürlichen Sinn verträglich ist. In Analogie zu direkten Produkten, die den einfachsten Spezialfall darstellen und wo man gleichfalls innere und äußere unterscheidet, spricht man in dieser Situation auch von einem *inneren semidirekten Produkt*. Dabei erweist sich die Aktion von K durch Konjugation auf N vermittels innerer Automorphismen als interessant. Wenn man nämlich umgekehrt diese drei Daten – Struktur von N, Struktur von K und Aktion von K mittels Automorphismen auf N – vorgibt, kann daraus G als sogenanntes *äußeres semidirektes Produkt* (8.4.2) rekonstruiert werden. Universell nicht nur für sämtliche Aktionen von K auf N, sondern überhaupt für alle Erweiterungen von N mit K ist schließlich das *Kranzprodukt* (8.4.3), das selbst wieder in geeigneter Weise als semidirektes Produkt, allerdings größerer Gruppen, definiert ist.

8.4.1 Allgemeine Gruppenerweiterungen

Die Ausgangssituation lässt sich durch eine *kurzexakte Sequenz* (vgl. Unterabschnitt 7.2.3) von (diesmal im Allgemeinen nichtkommutativen) Gruppen beschreiben:

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\kappa} K \to 1$$

Am Anfang und Ende der Sequenz steht jeweils die mit 1 (bei additiver Notation mit 0) bezeichnete einelementige Gruppe. Zur Erinnerung: Wie schon bei Sequenzen von Moduln bedeutet Exaktheit der Sequenz in einem bestimmten Glied (nicht am Anfang oder Ende der Sequenz), dass das Bild der Abbildung, die durch den Pfeil von links symbolisiert wird, übereinstimmt mit dem Kern der Abbildung, die zum Pfeil nach rechts gehört. Konkret im Beispiel: Bei N bedeutet die Exaktheit die Injektivität von ι, bei K die Surjektivität von κ und bei G, dass das Bild von ι gerade mit dem Kern von κ übereinstimmt. In diesem Fall ist nach dem Homomorphiesatz $N \cong \iota(N) \lhd G$ und $K \cong G/\iota(N)$. Ist umgekehrt ein Normalteiler $N \lhd G$ einer Gruppe vorgegeben, so können wir $K := G/N$ setzen, und es liegt eine kurzexakte Sequenz obiger Gestalt mit der Einbettung $\iota\colon N \to G$, $n \mapsto n$ und der kanonischen Abbildung $\kappa\colon G \to K = G/N$, $g \mapsto gN$ vor.
Wir werden uns beispielsweise für die Frage interessieren, inwiefern sich G mittels N und K beschreiben lässt, und fassen die allgemeine Situation in folgende Definition.

Definition 8.4.1.1. $\mathcal{E} = (G, \iota, \kappa)$ heißt *Erweiterung* der Gruppe N durch die Gruppe K[1], wenn $\iota\colon N \to G$ injektiv, $\kappa\colon G \to K$ surjektiv und $\iota(N) = \ker \kappa$ ist, d.h. wenn die Sequenz

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\kappa} K \to 1$$

(kurz)exakt ist.

Dabei ist die Struktur von G durch jene von N und K allein nicht eindeutig bestimmt. Ein einfaches Beispiel dafür ist gegeben durch die Gruppen $G_1 := C_6$ und $G_2 := S_3$. Beide

[1] In der englischen Version von Bourbaki wird G (mit vertauschten Präpositionen) *extension of K by N* genannt.

haben einen Normalteiler $N \cong C_3$ mit Quotienten $K \cong C_2$. Somit hat die kurzexakte Sequenz

$$1 \to C_3 \xrightarrow{\iota} G \xrightarrow{\kappa} C_2 \to 1$$

für G die beiden zueinander nicht isomorphen Lösungen $G = C_6$ und $G = S_3$.
Will man G aus N und K rekonstruieren, reichen die Isomorphietypen von N und K alleine also nicht aus. Man braucht zusätzliche Information darüber, wie K und N in G zusammenwirken. Das lässt sich wie folgt besser verstehen.
Wie auch schon in der Theorie der Moduln kann man die Situation näher untersuchen, wenn es ρ und/oder σ der Form

$$0 \longrightarrow N \underset{\rho}{\overset{\iota}{\rightleftarrows}} G \underset{\sigma}{\overset{\kappa}{\rightleftarrows}} K \longrightarrow 0$$

gibt, wobei $\rho\colon G \to N$ die Relation $\rho \circ \iota = \mathrm{id}_N$ und $\sigma\colon K \to G$ die Relation $\kappa \circ \sigma = \mathrm{id}_K$ erfüllt[2]. Wieder nennt man dann ρ eine *Retraktion* und σ eine *Sektion* von $\mathcal{E}$.

Beispiel 8.4.1.2. Die *triviale Erweiterung*: $G = N \times K$, $\iota(n) = (n, 1)$, $\kappa(n, k) = k$. Hier gibt es die Sektion $\sigma : k \mapsto (1, k)$ und die Retraktion $\rho : (n, k) \mapsto n$.

Das einfache Beispiel der kurzexakten Sequenz

$$0 \to 2\mathbb{Z} \xrightarrow{\iota} \mathbb{Z} \xrightarrow{\kappa} \mathbb{Z}/(2\mathbb{Z}) \to 0$$

zeigt, dass Sektionen und Retraktionen nicht immer existieren. Von besonderem Interesse ist der Fall, dass es eine Sektion σ gibt. Er führt uns zu den semidirekten Produkten.

8.4.2 Semidirekte Produkte

Wir gehen davon aus, dass für die kurzexakte Sequenz

$$1 \longrightarrow N \xrightarrow{\iota} G \underset{\sigma}{\overset{\kappa}{\rightleftarrows}} K \longrightarrow 1$$

eine Sektion σ vorliegt, d.h. ein Homomorphismus $\sigma\colon K \to G$ mit $\kappa \circ \sigma = \mathrm{id}_K$. So ein σ ist notwendig injektiv, also können wir K oBdA mit $\sigma(K) \leq G$ in G identifizieren, d.h. als Untergruppe von G auffassen. Aus der Exaktheit der Sequenz folgt leicht sowohl $N \cap K = \{e\}$ als auch $NK = G$.

Definition 8.4.2.1. Die Gruppe G heißt *inneres semidirektes Produkt* von $N \lhd G$ und $K \leq G$, sofern $N \cap K = 1$ und $NK = G$.

Diese Überlegungen lassen sich umkehren, sodass man zusammenfassend erhält:

[2] Achtung: Wie schon in Unterabschnitt 7.2.3 kommutiert dieses erweiterte Diagramm im Allgemeinen nicht!

Proposition 8.4.2.2. *Sei G eine Gruppe, $N \lhd G$ und $K \leq G$ sowie $\sigma : K \to G$ die Inklusionsabbildung. Dann sind folgende Aussagen äquivalent:*

1. *G ist das innere semidirekte Produkt von $N \lhd G$ und $K \leq G$, d.h. es gilt $N \cap K = 1$ und $NK = G$.*
2. *Bezeichne $\pi \colon G \to G/N$ die kanonische Abbildung. Dann ist $\pi \circ \sigma \colon K \to G/N$ ein Isomorphismus.*
3. *Für die Inklusionsabbildung $\iota : N \to G$ gibt es ein κ, sodass eine kurzexakte Sequenz vorliegt, für die σ eine Sektion ist:*

$$1 \longrightarrow N \xrightarrow{\iota} G \underset{\sigma}{\overset{\kappa}{\rightleftarrows}} K \longrightarrow 1$$

Insbesondere entspricht jedes semidirekte Produkt einer Gruppenerweiterung.

Man beachte die partielle Analogie zu Satz 7.2.3.8 über das Zerfallen von Sequenzen von Moduln.

UE 78 ▶ Übungsaufgabe 8.4.2.3. (V) Beweisen Sie Proposition 8.4.2.2 in allen Details. **◀ UE 78**

UE 79 ▶ Übungsaufgabe 8.4.2.4. (B) Zeigen Sie anhand eines Beispiels, dass in der dritten äquivalenten Bedingung in Proposition 8.4.2.2 nicht auf die Sektionsbedingung an σ verzichtet werden kann. **◀ UE 79**

Das einfachste Beispiel eines semidirekten Produktes liegt offenbar vor, wenn $G = N \times K$ das direkte Produkt zweier Untergruppen ist, die dann notwendig beide sogar Normalteiler sind. Denkt man sich N und K vorgegeben, so liefert die Konstruktion des äußeren direkten Produktes eine Gruppe G, in die N und K in natürlicher Weise eingebettet sind. Klarerweise ist jedes direkte Produkt auch ein semidirektes. Für ein semidirektes Produkt bestehen aber noch andere Möglichkeiten, weil ja nur N, aber nicht unbedingt K Normalteiler sein muss.
Zum besseren Verständnis des Beziehung von N und K gehen wir von der Situation beim inneren semidirekten Produkt aus. Sei also $N \lhd G$, $K \leq G$ mit $N \cap K = \{e\}$ und $NK = G$. Dann besitzt jedes $g \in G$ eine eindeutige Darstellung als $g = nk$ mit $n \in N$ und $k \in K$. Außerdem sei $\tau \colon K \to \mathrm{Aut}(N)$ mit $\tau(k) = \alpha_k$, wobei $\alpha_k(n) = knk^{-1}$, d.h. K agiert vermittels Konjugation auf N. Es gilt $\alpha_{k_1} \circ \alpha_{k_2} = \alpha_{k_1 k_2}$, d.h. τ ist Homomorphismus. Außerdem gilt

$$(n_1 k_1)(n_2 k_2) = n_1 k_1 n_2 k_1^{-1} k_1 k_2 = n_1 \alpha_{k_1}(n_2) k_1 k_2.$$

Wir gehen nun umgekehrt von folgender Situation aus:

Vorgegeben seien N und K sowie ein Homomorphismus $\tau\colon K \to \mathrm{Aut}(N)$, d.h. eine Aktion $\alpha : (k,n) \mapsto \tau(k)(n)$ von K auf N vermittels Automorphismen. Wir schreiben

$$^k n := \tau(k)(n)$$

und definieren auf der Trägermenge $G := N \times K$ die Operation $\cdot_\tau$ durch

$$(n_1,k_1) \cdot_\tau (n_2,k_2) := (n_1\, {}^{k_1}n_2, k_1k_2).$$

Die Operation $\cdot_\tau$ ist eine Gruppenoperation auf G mit neutralem Element $e_G = (e_N, e_K)$ und Inversen $(n,k)^{-1} = ({}^{k^{-1}}n^{-1}, k^{-1})$.
Diese Gruppe wird *(äußeres) semidirektes Produkt* von N und K genannt, i.Z. $G = N \rtimes K$ oder (präziser, weil dadurch die Abhängigkeit von τ zum Ausdruck kommt, aber weniger verbreitet) $N \rtimes_\tau K$.
Offenbar ist

$$1 \to N \xrightarrow{\iota} G = N \rtimes K \xrightarrow{\kappa} K \to 1$$

mit $\iota(n) = (n, e_K)$ und $\kappa(n,k) = k$ kurzexakt, also ist $G = N \rtimes K$ eine Erweiterung von N durch K. Außerdem gilt

$$(e_N,k) \cdot_\tau (n,e_K) \cdot_\tau (e_N,k)^{-1} = ({}^k n, k) \cdot_\tau (e_N, k^{-1}) = ({}^k n, e_K),$$

d.h. K agiert auf N via Konjugation, wie beim inneren semidirekten Produkt weiter oben beschrieben.
Wir haben bereits in Proposition 8.4.2.2 gesehen, dass jedes semidirekte Produkt einer Gruppenerweiterung entspricht. Die Umkehrung gilt nicht. Das ergibt sich aus dem letzten Teil der folgenden Übungsaufgabe.

UE 80 ► Übungsaufgabe 8.4.2.5. (V) **◄ UE 80**

(1) Ergänzen Sie bei der Konstruktion des äußeren semidirekten Produktes die nicht explizit ausgeführten Rechnungen.

(2) Sei die Gruppe G inneres semidirektes Produkt von $N \lhd G$ und $K \leq G$. Zeigen Sie, dass G isomorph zum äußeren direkten Produkt $G = N \rtimes K$ (bezüglich der Aktion von K auf N vermittels Konjugation) ist.

(3) Zeigen Sie umgekehrt explizit, dass sich jedes äußere semidirekte Produkt auch als inneres deuten lässt.

Bildet τ immer auf id_N ab (d.h.: ist τ die triviale Aktion von K auf N), so erhält man das direkte Produkt mit $(n_1k_1)(n_2k_2) = n_1n_2k_1k_2$. Die Rolle der trivialen Aktion τ wird noch deutlicher durch folgende, nicht schwer zu beweisende Aussage:

Proposition 8.4.2.6. *Sei τ eine Aktion der Gruppe K vermittels Automorphismen auf der Gruppe N. Dann ist das semidirekte Produkt $G := N \rtimes_\tau K$ genau dann abelsch, wenn folgende drei Bedingungen erfüllt sind:*

1. *Die Gruppe N ist abelsch.*

2. Die Gruppe K ist abelsch.

3. Die Aktion τ ist trivial, d.h. $\tau(k) = \mathrm{id}_N$ für alle $k \in K$.

UE 81 ▶ **Übungsaufgabe 8.4.2.7.** (V) Beweisen Sie Proposition 8.4.2.6. ◀ **UE 81**

Die Abhängigkeit der Konstruktion des semidirekten Produktes $G := N \rtimes_\tau K$ von der Aktion τ schlägt sich auch in der Struktur der resultierenden Gruppe G nieder. Zum Beispiel lassen sich sowohl C_6 als auch S_3 als semidirektes Produkt $C_3 \rtimes C_2$ erhalten.

UE 82 ▶ **Übungsaufgabe 8.4.2.8.** (V) Führen Sie das aus, indem Sie die entsprechenden Aktionen von C_2 als Automorphismen von C_3 angeben. ◀ **UE 82**

Etwas anspruchsvoller:

UE 83 ▶ **Übungsaufgabe 8.4.2.9.** (B) Beschreiben Sie sämtliche Aktionen τ von $K := C_2$ auf $N := C_8$ vermittels Automorphismen und die zugehörigen semidirekten Produkte $G_\tau := C_8 \rtimes_\tau C_2$. Wieviele davon sind paarweise nichtisomorph?
Hinweis: Es kann nützlich sein, die Ordnungen der Elemente von G_τ zu bestimmen (wenn man richtig anfängt, kann man sich dabei viel Arbeit ersparen). ◀ **UE 83**

8.4.3 Das Kranzprodukt

Wie wir gesehen haben, ist ein semidirektes Produkt und erst recht eine Erweiterung G von N durch K durch die Isomorphietypen von N und K nicht eindeutig bestimmt. Deshalb entsteht der Wunsch, einen Überblick über alle Möglichkeiten zu bekommen. Als Schritt in diese Richtung lässt sich das auch für sich interessante Kranzprodukt deuten, welches *alle* Erweiterungen von N mit K enthält.
Um die Konstruktion besser zu verstehen, denken wir an Permutationsgruppen. N können wir gemäß Cayley mittels linkskürzbarer Aktion auf sich selbst realisieren. Im Fall eines semidirekten Produktes agiert auch K auf N. Für beliebige Erweiterungen, noch dazu für alle auf einmal, kommen wir damit aber nicht aus. Um Platz zu schaffen, denken wir uns für jedes $k \in K$ eine isomorphe Kopie N_k von N, in der sich alle Möglichkeiten für Produkte nk mit $n \in N$ realisieren lassen. Die Aktion von K spiegelt sich wider in Permutationen der Kopien N_k gemäß der Gruppenoperation in K. Es lohnt sich, noch etwas weiter auszuholen.
Sei Σ eine Partition der Menge Ω in gleich große Klassen C (sie werden den Kopien N_k entsprechen). Wir definieren die sogenannte *Automorphismengruppe*

$$G = \mathrm{Aut}(\Sigma) := \{f \in \mathrm{Sym}(\Omega) : f(\Sigma) = \Sigma\} = \{f \in \mathrm{Sym}(\Omega) : \ f(C) \in \Sigma \ \text{ für alle } C \in \Sigma\}$$

der Partition Σ. Diese Definition garantiert, dass alle $C \in \Sigma$ sogenannte Blöcke unter der Aktion von G sind.) Dann wird durch $\rho(g, C) := g(C)$ eine Aktion von G auf Σ

definiert. Bezeichne

$$B := \{g \in G : g(C) = C \text{ für alle } C \in \Sigma\} \cong \prod_{C\in\Sigma} \mathrm{Sym}(C) \cong \mathrm{Sym}(C)^\Sigma$$

(die letzte Isomorphie gilt für jedes $C \in \Sigma$, da die Klassen C gleich groß sind) die sogenannte *Basisgruppe*. B besteht also aus jenen Permutationen, die Elemente nur innerhalb der Klassen $C \in \Sigma$ vertauschen. Dann ist $G \cong B \rtimes \mathrm{Sym}(\Sigma)$ bezüglich der Aktion ρ.

UE 84 ► **Übungsaufgabe 8.4.3.1.** (F) Prüfen Sie nach, dass G tatsächlich semidirektes Produkt der angegebenen Form ist. ◄ **UE 84**

Wir untersuchen nun den Fall, dass jede Klasse $C \in \Sigma$ eine isomorphe Kopie einer vorgegebenen Gruppe N ist. Sei N^Σ das direkte Produkt von mit $\sigma \in \Sigma$ indizierten Kopien von N. Agiert K auf Σ, dann agiert K auch auf N^Σ durch Automorphismen, nämlich vermittels

$${}^k(n_\sigma)_{\sigma\in\Sigma} := (n_{k(\sigma)})_{\sigma\in\Sigma}, \quad n_\sigma \in N, k \in K.$$

Das semidirekte Produkt $N^\Sigma \rtimes K$ bezüglich dieser Aktion heißt dann *Kranzprodukt*[3], bezeichnet mit $N \operatorname{wr}_\Sigma K$. Als *Basisgruppe* des Kranzproduktes bezeichnet man $B := \{(n, 1) : n \in N^\Sigma\}$.
Als Standardfall betrachten wir den Spezialfall $\Sigma = K$ mit linkskürzbarer Aktion auf sich selbst, also ${}^k k' = kk'$. Entsprechend heißt $N \operatorname{wr} K := N \operatorname{wr}_K K = N^K \rtimes K$ auch das *Standardkranzprodukt*.

UE 85 ► **Übungsaufgabe 8.4.3.2.** (F) Beschreiben Sie explizit Elemente und Operationen im Kranzprodukt $N \operatorname{wr}_\Sigma K$ und im Standardkranzprodukt $N \operatorname{wr} K$. ◄ **UE 85**

Wie bereits angekündigt ist die wichtigste Eigenschaft des Kranzproduktes die folgende.

Satz 8.4.3.3 (Universelle Eigenschaft des Kranzproduktes bzgl. Erweiterung)**.** *Sind N und K Gruppen, so lässt sich jede Erweiterung von N durch K isomorph in das Standardkranzprodukt N wr K einbetten.*

UE 86 ► **Übungsaufgabe 8.4.3.4.** (V) Beweisen Sie Satz 8.4.3.3. ◄ **UE 86**

UE 87 ► **Übungsaufgabe 8.4.3.5.** (D) Besprechen Sie interessante Beispiele von Kranzprodukten. ◄ **UE 87**

[3] englisch: *wreath product*

8.5 Direkte Zerlegung: Der Satz von Krull-Schmidt

Durch den Satz von Jordan-Hölder wird jeder Gruppe mit einer Kompositionsreihe als Isomorphieinvariante die (ungeordnete) Liste der Isomorphietypen der (dann notwendig einfachen) Faktoren zugeordnet. Damit verwandt ist die Frage nach Darstellungen als direktes Produkt von Faktoren, die selbst nicht mehr echt in ein direktes Produkt zerlegt werden können. Klar ist einerseits, dass endliche Gruppen solche Zerlegungen haben, andererseits aber sicher nicht alle Gruppen. Man denke an ein direktes Produkt unendlich vieler isomorpher Kopien ein und derselben Gruppe. Relativ schnell kann man erkennen, dass jede der sogenannten Kettenbedingungen für Normalteiler, aufsteigend (ACC) wie absteigend (DCC), hinreicht für eine Zerlegung in endlich viele selbst unzerlegbare direkte Faktoren. Diese Kettenbedingungen besagen, dass es keine unendlichen, echt aufsteigenden bzw. absteigenden Folgen von Normalteilern gibt. Die Argumente dafür sind durchaus verwandt mit jenen für die Existenz der Primfaktorzerlegung einer natürlichen Zahl. Keineswegs leicht einzusehen ist die bemerkenswerte Aussage des Satzes von Krull-Schmidt: Sind beide Kettenbedingungen erfüllt, gilt für direkte Zerlegungen sogar Eindeutigkeit bis auf Isomorphie und Reihenfolge der Faktoren. Der Beweis des Satzes von Krull-Schmidt ist das Ziel dieses Abschnitts.
In 8.5.1 werden die beiden Kettenbedingungen definiert und der Satz von Krull-Schmidt präzise formuliert. Wie schon erwähnt, reicht bereits jede der beiden für sich hin, um die Existenz einer direkten Zerlegung zu zeigen. Zum Beweis der viel schwieriger zu beweisenden Eindeutigkeitsaussage des Satzes von Krull-Schmidt kann an dieser Stelle nur eine Andeutung der Methoden gegeben werden. Die Beweisarbeit im Detail beginnt in 8.5.2 mit der Einführung des Begriffs des normalen Endomorphismus und dem Beweis eines ersten wichtigen Lemmas, das eine Beziehung zu den Kettenbedingungen herstellt. Diese Stoßrichtung wird in 8.5.3 mit dem Fitting-Lemma vertieft, wonach für eine Gruppe G mit ACC und DCC und jeden normalen Endomorphismus f von G ein $n \in \mathbb{N}$ mit $G = \ker f^n \odot \operatorname{Im} f^n$ existiert – eine erste interessante direkte Zerlegung. Der Abschluss des Beweises des Satzes von Krull-Schmidt gelingt schließlich in 8.5.4.

8.5.1 Kettenbedingungen und Formulierung des Satzes

Definition 8.5.1.1.

- Eine Gruppe G heißt *direkt zerlegbar*, wenn es nichttriviale Untergruppen $A, B \leq G$ mit $G = A \odot B$ (inneres direktes Produkt, siehe Definition 3.2.3.5) gibt. Andernfalls heißt G *direkt unzerlegbar*.

- G erfüllt die *aufsteigende Kettenbedingung (ACC)* für Normalteiler, falls

$$G_1 \leq G_2 \leq G_3 \leq \ldots, \quad G_i \lhd G \Longrightarrow \exists n \in \mathbb{N}\, \forall i \geq n : G_i = G_n.$$

- G erfüllt die *absteigende Kettenbedingung (DCC)* für Normalteiler, falls

$$G_1 \geq G_2 \geq G_3 \geq \ldots, \quad G_i \lhd G \Longrightarrow \exists n \in \mathbb{N}\, \forall i \geq n : G_i = G_n.$$

Man beachte, dass wir die auf- bzw. absteigende Kettenbedingung für Halbordnungen bereits in Definition 2.1.2.6 eingeführt haben – eine Gruppe erfüllt ACC (DCC) im obigen Sinne genau dann, wenn ihr Normalteilerverband ACC (DCC) in Sinne von Definition 2.1.2.6 erfüllt.

Satz 8.5.1.2. *Erfüllt eine Gruppe G wenigstens eine der beiden Bedingungen ACC oder DCC, dann existieren direkt unzerlegbare $G_1, G_2, \ldots, G_s$, sodass $G = G_1 \odot G_2 \odot \ldots \odot G_s$.*

UE 88 ► Übungsaufgabe 8.5.1.3. (V) Beweisen Sie Satz 8.5.1.2: **◄ UE 88**

1. Unter der Voraussetzung von ACC.
2. Unter der Voraussetzung von DCC.

Man beachte die Analogie zur Rolle der Teilerkettenbedingung im Zusammenhang mit der Faktorisierung in $\mathbb{Z}$.

UE 89 ► Übungsaufgabe 8.5.1.4. (B) Zeigen Sie, dass die Gruppe $(\mathbb{Z}, +)$ ACC erfüllt, DCC nicht erfüllt und direkt unzerlegbar ist. **◄ UE 89**
Hinweis: Betrachten Sie den Schnitt von nichttrivialen Normalteilern.

UE 90 ► Übungsaufgabe 8.5.1.5. (B) Sei p eine Primzahl und C_{p^∞} die p-Prüfergruppe. Zeigen Sie, dass C_{p^∞} ACC nicht erfüllt, DCC erfüllt und direkt unzerlegbar ist. **◄ UE 90**
Hinweis: Satz 3.3.3.7.

UE 91 ► Übungsaufgabe 8.5.1.6. (B) Sei C_∞ die universelle Prüfergruppe. Zeigen Sie, dass C_∞ *keine* endliche direkte Zerlegung $C_\infty = H_1 \odot \cdots \odot H_s$ mit direkt unzerlegbaren H_i hat. **◄ UE 91**
Hinweis: Satz 3.3.3.7.

UE 92 ► Übungsaufgabe 8.5.1.7. (F) Die Gruppe $G = G_1 \times G_2 \times \ldots \times G_s$ erfülle ACC bzw. DCC. Zeigen Sie, dass dann auch alle G_i ACC bzw. DCC erfüllen. **◄ UE 92**

Man könnte vermuten, dass die Übertragung der Kettenbedingungen in der letzten Aufgabe nur an der Existenz der kanonischen Projektionen $\pi_i : G_1 \times G_2 \times \ldots \times G_s \to G_i$ liegt. Tatsächlich ist die Situation aber komplizierter:

UE 93 ► Übungsaufgabe 8.5.1.8. (B) Zeigen Sie anhand eines Beispiels, dass direkte Unzerlegbarkeit durch Epimorphismen nicht übertragen werden muss. **◄ UE 93**

Das Ziel dieses Abschnitts ist der Beweis des folgenden Satzes.

Satz 8.5.1.9 (Krull-Schmidt)**.** *Sei G eine Gruppe, die ACC und DCC erfüllt, und gelte $G = G_1 \odot G_2 \odot \ldots \odot G_s$ sowie $G = H_1 \odot H_2 \odot \ldots \odot H_t$ für direkt unzerlegbare G_i, H_j. Dann folgt:*
Es gilt $s = t$ und es existiert eine Permutation π der Indizes 1 bis s derart, dass $G_i \cong H_{\pi(i)}$ für $i = 1, \ldots, s$ und für jedes $r \leq s$ gilt:

$$G = G_1 \odot G_2 \odot \ldots \odot G_r \odot H_{\pi(r+1)} \odot \ldots \odot H_{\pi(s)}.$$

UE 94 ► **Übungsaufgabe 8.5.1.10.** (B) Finden Sie eine Gruppe G mit ACC und DCC (der Satz von Krull-Schmidt soll also anwendbar sein) sowie zwei direkte Zerlegungen $G = G_1 \odot G_2 \odot \cdots \odot G_s$ und $G = H_1 \odot H_2 \odot \cdots \odot H_s$, sodass nur auf Isomorphie der G_i mit den $H_{\pi(i)}$ geschlossen werden kann, nicht aber auf Gleichheit. ◄ **UE 94**

Der Beweis der Eindeutigkeitsaussage ist einigermaßen anspruchsvoll und wird uns für den Rest des Abschnitts beschäftigen, selbst wenn zahlreiche Beweisschritte in Übungsaufgaben ausgelagert werden. Bevor wir ins technische Detail gehen, seien hier ein paar Andeutungen zur Beweisidee vorangestellt.
Der Einfachheit halber wollen wir dazu von zwei Zerlegungen $G = G_1 \odot G_2 = H_1 \odot H_2$ in jeweils nur zwei unzerlegbare Bestandteile ausgehen. Mit jeder direkten Zerlegung gehen Einbettungs- und Projektionsabbildungen für die Komponenten einher. Solche Endomorphismen haben eine interessante Eigenschaft, die man *normal* nennt. Eine Konsequenz von Normalität besteht darin, dass nicht nur Urbilder, sondern auch Bilder von Normalteilern wieder Normalteiler sind. Damit lässt sich unter Verwendung von ACC und DCC für jeden normalen Endomorphismus f eine Zerlegung der Gestalt $G = \ker f^n \odot \operatorname{Im} f^n$ konstruieren (Fitting-Lemma 8.5.3.1). Für unzerlegbare Faktoren in einer Zerlegung heißt dies, dass f entweder nilpotent ist ($\operatorname{Im} f^n$ trivial) oder injektiv ($\ker f^n$ trivial). Der zweite Fall lässt sich bei Anwendung auf geeignete f, die sich aus Einbettungen und Projektionen zusammensetzen, so weit ausbeuten, dass schlussendlich Isomorphismen $G_1 \cong H_1$ und $G_2 \cong H_2$ (oder umgekehrt) gefunden werden können.

8.5.2 Normale Endomorphismen

In unserer Strukturanalyse direkter Zerlegungen $G = G_1 \times G_2 \times \ldots G_n$ werden die natürlichen Projektionen $\pi_i \colon G \to G_i$, $a = a_1 a_2 \ldots a_n \mapsto a_i$ (wohldefiniert, da ein inneres direktes Produkt vorliegt), die Einbettungen $\iota_i \colon G_i \to G$ sowie deren Kompositionen, die Endomorphismen $\varphi_i := \iota_i \pi_i \colon G \to G$, eine wichtige Rolle spielen, außerdem die Möglichkeit, aus den φ_i, $i = 1, 2, \ldots, n$, wieder die Identität auf G zusammenzusetzen. Vor allem auf derartige Situationen werden wir die nachfolgende Definition anwenden.

Definition 8.5.2.1. Sei G eine Gruppe. Mit $\operatorname{End}(G)$ bezeichnen wir die Menge aller Endomorphismen $f \colon G \to G$. Ein $f \in \operatorname{End}(G)$ heißt *normal*, wenn f mit allen inneren Automorphismen $\varphi_a : x \mapsto axa^{-1}$ vertauscht, d.h. wenn für alle $a, b \in G$ gilt:

$$af(b)a^{-1} = \varphi_a(f(b)) \overset{(!)}{=} f(\varphi_a(b)) = f(aba^{-1}).$$

Wir bezeichnen die Menge aller normalen Endomorphismen mit $\mathrm{End}_{\lhd}(G)$.
f heißt *nilpotent*, wenn ein $n \in \mathbb{N}$ existiert, sodass $f^n \equiv e$ konstant ist.
Für beliebige $f, g \in \mathrm{End}(G)$ definieren wir außerdem eine (im Allgemeinen nicht kommutative) Summe $f + g$ durch $(f + g)(a) := f(a)g(a)$.

Proposition 8.5.2.2. *Sei G eine Gruppe und $f, g \in \mathrm{End}(G)$. Dann gilt:*

(i) Genau dann ist $f + g \in \mathrm{End}(G)$, wenn für alle $c \in \mathrm{Im}\, f$ und alle $d \in \mathrm{Im}\, g$ gilt $cd = dc$. In diesem Fall gilt $f + g = g + f$.

(ii) Aus $f, g \in \mathrm{End}_{\lhd}(G)$ folgt auch $fg := f \circ g \in \mathrm{End}_{\lhd}(G)$.

(iii) Normale Endomorphismen $f \in \mathrm{End}_{\lhd}(G)$ bilden Normalteiler auf Normalteiler ab: $H \lhd G \Rightarrow f(H) \lhd G$

(iv) Ist für $f, g \in \mathrm{End}_{\lhd}(G)$ die Summe $f + g$ ein Endomorphismus, dann sogar ein normaler, d.h. $f + g \in \mathrm{End}_{\lhd}(G)$.

(v) Für $G = G_1 \odot \ldots \odot G_n$ und $j = 1, \ldots, n$ seien

$$\iota_j \colon G_j \to G, \quad a_j \mapsto a_j,$$

die kanonischen Einbettungen,

$$\pi_j : G \to G_j, \quad a = a_1 \ldots a_n \mapsto a_j$$

die kanonischen Projektionen und

$$\varphi_j := \iota_j \pi_j \in \mathrm{End}(G).$$

Dann sind für alle Auswahlen von Indizes $1 \leq j_1 < \ldots < j_k \leq n$ die Summen $\varphi_{j_1} + \ldots + \varphi_{j_k}$ normale Endomorphismen von G.

UE 95 ▶ Übungsaufgabe 8.5.2.3. (V) Beweisen Sie Proposition 8.5.2.2. **◀ UE 95**

Lemma 8.5.2.4. *Sei G eine Gruppe.*

(a) G erfülle ACC und sei $f \in \mathrm{End}(G)$. Dann folgt aus der Surjektivität von f bereits Bijektivität, also $f \in \mathrm{Aut}(G)$.

(b) G erfülle DCC und sei sogar $f \in \mathrm{End}_{\lhd}(G)$. Dann folgt auch aus der Injektivität von f bereits Bijektivität, also $f \in \mathrm{Aut}(G)$.

Beweis. Zu Punkt (a): Wir betrachten die folgende aufsteigende Kette von Normalteilern von G:

$$\{e\} \leq \ker f \leq \ker f^2 \leq \ldots.$$

Wegen ACC gibt es ein n, sodass $\ker f^n = \ker f^{n+1}$. Sei $a \in \ker f$. Da mit f auch f^n surjektiv ist, gibt es ein $b \in G$ mit $f^n(b) = a$ und es folgt $e = f(a) = f^{n+1}(b)$. Also ist $b \in \ker f^{n+1} = \ker f^n$, d.h. $a = f^n(b) = e$. Also ist f auch injektiv und somit bijektiv.
Zu Punkt (b): Da f ein normaler Endomorphismus ist, gilt $\operatorname{Im} f^k \lhd G$ für alle $k \geq 1$. Wir betrachten also die absteigende Kette

$$G \geq \operatorname{Im} f \geq \operatorname{Im} f^2 \geq \dots.$$

Wegen DCC gibt es ein n, sodass $\operatorname{Im} f^n = \operatorname{Im} f^{n+1}$, das heißt für jedes $a \in G$ gibt es ein $b \in G$, sodass $f^n(a) = f^{n+1}(b) = f^n(f(b))$. Mit f ist auch f^n injektiv, und es folgt $a = f(b)$. Also ist f auch surjektiv und somit bijektiv. □

UE 96 ► **Übungsaufgabe 8.5.2.5.** (B,D) Versuchen Sie, die Endomorphismenmonoide $\operatorname{End}(G)$ und $\operatorname{End}_{\lhd}(G)$ für einige Gruppen G zu beschreiben. Welche der Endomorphismen von G sind sogar Automorphismen? Unverbindliche Vorschläge für G: ◄ **UE 96**

1. zyklisches G
2. endlich erzeugtes abelsches G (Hauptsatz verwenden)
3. $G = S_3$ als die kleinste nichtabelsche Gruppe
4. $G = S_4$ oder eine andere endliche nichtabelsche Gruppe
5. ein davon verschiedenes G, insbesondere ein unendliches und nichtabelsches

8.5.3 Normale Endomorphismen induzieren direkte Zerlegungen

Lemma 8.5.3.1 (Fittings Lemma)**.** *Sei G eine Gruppe, die ACC und DCC erfüllt, und sei $f \in \operatorname{End}_{\lhd}(G)$. Dann gibt es ein $n \in \mathbb{N} \setminus \{0\}$, sodass $G = \ker f^n \odot \operatorname{Im} f^n$.*

Beweis. Da f ein normaler Endomorphismus ist, gilt $\operatorname{Im} f^k \lhd G$ für alle $k \geq 1$. Betrachte also die Ketten

$$G \geq \operatorname{Im} f \geq \operatorname{Im} f^2 \geq \dots \quad \text{und} \quad \{e\} \leq \ker f \leq \ker f^2 \leq \dots.$$

Wegen ACC und DCC gibt es ein $n \in \mathbb{N}$, sodass $\operatorname{Im} f^k = \operatorname{Im} f^n$ und $\ker f^k = \ker f^n$ für alle $k \geq n$. Für den Nachweis von $\ker f^n \cap \operatorname{Im} f^n = \{e\}$ sei $a \in \ker f^n \cap \operatorname{Im} f^n$. Dann gibt es ein b mit $f^n(b) = a$. Wir schließen daraus $f^{2n}(b) = f^n(a) = e$, also $b \in \ker f^{2n} = \ker f^n$, folglich tatsächlich $a = f^n(b) = e$. Gelingt auch der Nachweis von $G = \ker f^n \cdot \operatorname{Im} f^n$, so folgt die Behauptung aus Proposition 3.2.3.3 (oder alternativ Satz 3.2.3.8 bzw. Satz 3.2.3.15). Sei also $c \in G$, dann ist $f^n(c) \in \operatorname{Im} f^n = \operatorname{Im} f^{2n}$, also gibt es ein $d \in G$, sodass $f^n(c) = f^{2n}(d)$. Nun gilt

$$f^n(cf^n(d^{-1})) = f^n(c)f^{2n}(d^{-1}) = f^n(c)f^{2n}(d)^{-1} = f^n(c)f^n(c)^{-1} = e.$$

Also ist $cf^n(d^{-1}) \in \ker f^n$. Es folgt $c = (cf^n(d^{-1}))f^n(d) \in \ker f^n \cdot \operatorname{Im} f^n$. □

Folgerung 8.5.3.2. *Sei G eine direkt unzerlegbare Gruppe, die ACC und DCC erfüllt, und sei $f \in \mathrm{End}_{\lhd}(G)$. Dann ist f nilpotent oder ein Automorphismus von G.*

Beweis. Aus Fittings Lemma 8.5.3.1 folgt, dass $G = \ker f^n \odot \operatorname{Im} f^n$ für ein $n \geq 1$. Da G direkt unzerlegbar ist, ist entweder $\ker f^n = \{e\}$ oder $\operatorname{Im} f^n = \{e\}$. Gilt $\operatorname{Im} f^n = \{e\}$, so ist f nilpotent. Gilt $\ker f^n = \{e\}$, dann auch $\ker f = \{e\}$, also ist f injektiv und daher nach Lemma 8.5.2.4(b) ein Automorphismus auf G. □

Folgerung 8.5.3.3. *Sei G eine direkt unzerlegbare Gruppe, die ACC und DCC erfüllt, und seien $f_1, \ldots, f_n \in \mathrm{End}_{\lhd}(G)$ nilpotent mit $f_{i_1} + \ldots + f_{i_r} \in \mathrm{End}(G)$ für alle $1 \leq i_1 < \ldots < i_r \leq n$. Dann ist $f_1 + \ldots + f_n \in \mathrm{End}_{\lhd}(G)$ nilpotent.*

Beweisskizze. Wegen Proposition 8.5.2.2iv genügt es, die Aussage für $n = 2$ zu zeigen, der allgemeine Fall folgt dann mit Induktion. Angenommen, $f_1 + f_2$ ist nicht nilpotent, dann ergibt sich aus Folgerung 8.5.3.2, dass $f_1 + f_2 \in \mathrm{Aut}(G)$. Definiere $g := (f_1 + f_2)^{-1}$, $g_1 := f_1 g$ und $g_2 := f_2 g$. Nach Proposition 8.5.2.2i gilt $cd = dc$ für alle $c \in \operatorname{Im} f_1$ und $d \in \operatorname{Im} f_2$, insbesondere für alle $c \in \operatorname{Im} g_1 \leq \operatorname{Im} f_1$ und $d \in \operatorname{Im} g_2 \leq \operatorname{Im} f_2$. Wir folgern (abermals mit Proposition 8.5.2.2i), dass $g_1 + g_2 \in \mathrm{End}(G)$ und $g_1 + g_2 = g_2 + g_1$.
Weiters rechnen wir

$$(g_1 + g_2)(x) = g_1(x)g_2(x) = (f_1 g)(x)(f_2 g)(x) = (f_1 + f_2)(g(x)) = x,$$

also $g_1 + g_2 = \mathrm{id}_G$. Es ergibt sich

$$g_1 g_1 + g_1 g_2 = g_1(g_1 + g_2) = g_1 \,\mathrm{id}_G = \mathrm{id}_G \, g_1 = (g_1 + g_2)g_1 = g_1 g_1 + g_2 g_1.$$

Daraus erhält man $g_1 g_2 = g_2 g_1$. Mittels Induktion folgt daraus (hier sind einige technische Details zu beachten, siehe Übungsaufgabe 8.5.3.4)

$$(g_1 + g_2)^m = \sum_{i=0}^{m} \binom{m}{i} g_1^i g_2^{m-i}$$

für alle $m \geq 1$. Da g surjektiv ist und f_1, f_2 nicht injektiv (da nilpotent) sind, können die $g_i = f_i g$, $i = 1, 2$ nicht injektiv sein. Also folgt wieder aus Folgerung 8.5.3.2, dass g_1, g_2 beide nilpotent sind. Das heißt aber

$$\mathrm{id}_G = (g_1 + g_2)^m = \sum_{i=0}^{m} \binom{m}{i} g_1^i g_2^{m-i} \equiv e$$

für hinreichend großes m. Widerspruch. □

UE 97 ► Übungsaufgabe 8.5.3.4. (V) Schließen Sie den Beweis von Folgerung 8.5.3.3 ab, **◄ UE 97** indem Sie Folgendes zeigen:

(1) Seien $\alpha_1, \alpha_2 \in \mathbb{N} \setminus \{0\}$ und $(i_1, j_1), (i_2, j_2) \in \mathbb{N} \times \mathbb{N}$, wobei weder $i_1 = 0 = i_2$ noch $j_1 = 0 = j_2$. Dann gilt (Achtung, im Allgemeinen sind diese Summen *keine* Endomorphismen, sondern einfach Funktionen $G \to G$):

$$\alpha_1 g_1^{i_1} g_2^{j_1} + \alpha_2 g_1^{i_2} g_2^{j_2} = \alpha_2 g_1^{i_2} g_2^{j_2} + \alpha_1 g_1^{i_1} g_2^{j_1}.$$

(2) Es gilt die im Beweis verwendete Version des binomischen Lehrsatzes:

$$(g_1 + g_2)^m = \sum_{i=0}^{m} \binom{m}{i} g_1^i g_2^{m-i}$$

für alle $m \geq 1$.

8.5.4 Beweis der Eindeutigkeit

Nach diesen Vorarbeiten können wir den Satz von Krull-Schmidt beweisen:

Beweis (von Satz 8.5.1.9). Für G mit ACC und DCC folgt aus 8.5.1.2 die Existenz einer Zerlegung in direkt unzerlegbare Untergruppen. Zu beweisen ist daher nur noch die Eindeutigkeitsaussage von Satz 8.5.1.9.
Sei also $G = G_1 \odot \ldots \odot G_s = H_1 \odot \ldots \odot H_t$ mit G_i, H_j direkt unzerlegbar. Zu zeigen ist $s = t$ und nach geeigneter Umnummerierung $G_i \cong H_i$ für $i = 1, \ldots, s = t$ und $G = G_1 \odot \ldots \odot G_r \odot H_{r+1} \odot \ldots \odot H_t$ für $0 \leq r \leq t$.
Im Folgenden bedeute die Aussage $A(r)$ für $r \leq \min(s,t)$: Es existiert eine Umnummerierung der H_j mit $G_i \cong H_i$ für $i = 1, \ldots, r$ und $G = G_1 \odot \ldots \odot G_r \odot H_{r+1} \odot \ldots \odot H_t$.
Der Beweis erfolgt durch Induktion nach r.
$A(0)$ bedeutet $G = H_1 \odot \ldots \odot H_t$, gilt also nach Voraussetzung.
Sei also $A(r-1)$, $1 \leq r \leq \min(s,t)$ vorausgesetzt, d.h.

$$G = G_1 \odot \ldots \odot G_{r-1} \odot H_r \odot \ldots \odot H_t$$

nach geeigneter Umnummerierung der H_j, wobei $G_i \cong H_i$ für $i = 1, \ldots, r-1$. Seien $\pi_1, \ldots, \pi_s$ bzw. $\pi'_1, \ldots, \pi'_t$ die Projektionen für die Darstellungen $G = G_1 \odot \ldots \odot G_s$ und $G = G_1 \odot \ldots \odot G_{r-1} \odot H_r \odot \ldots \odot H_t$ sowie $\iota_1, \ldots, \iota_s$ bzw. $\iota'_1, \ldots, \iota'_t$ die zugehörigen Einbettungen. Wir definieren $\varphi_i := \iota_i \pi_i$ bzw. $\psi_j := \iota'_j \pi'_j$ und halten fest, dass es sich dabei laut Proposition 8.5.2.2 um normale Endomorphismen handelt. Dann gilt:

$\varphi_i\|_{G_i} = \mathrm{id}_{G_i}$	$\varphi_i \varphi_i = \varphi_i$	$\varphi_{i_1} \varphi_{i_2} \equiv e \ (i_1 \neq i_2)$
$\psi_1 + \ldots + \psi_t = \mathrm{id}_G$	$\psi_j \psi_j = \psi_j$	$\psi_{j_1} \psi_{j_2} \equiv e \ (j_1 \neq j_2)$
$\mathrm{Im}\, \varphi_i = G_i$	$\mathrm{Im}\, \psi_j = G_j \ (j < r)$	$\mathrm{Im}\, \psi_j = H_j \ (j \geq r)$

Es folgt, dass $\varphi_r \psi_j \equiv e$ für $j < r$, denn

$$\varphi_r \psi_j(x) = \varphi_r \,\mathrm{id}_{G_j}\, \psi_j(x) = \varphi_r \varphi_j \psi_j(x) = e.$$

Daher gilt

$$\varphi_r = \varphi_r \,\mathrm{id}_G = \varphi_r(\psi_1 + \ldots + \psi_t) = \varphi_r \psi_1 + \ldots + \varphi_r \psi_t. = \varphi_r \psi_r + \ldots + \varphi_r \psi_t.$$

Aus Proposition 8.5.2.2 folgt, dass alle „Partialsummen“ normale Endomorphismen sind. Da $\varphi_r|_{G_r}$ nicht nilpotent sein kann (es gilt $\varphi_r^2 = \varphi_r$) und mit G nach Übungsaufgabe 8.5.1.7 auch G_r ACC und DCC erfüllt, muss es nach Folgerung 8.5.3.2 und 8.5.3.3

zumindest einen Summanden $\varphi_r\psi_j$ in $\varphi_r\psi_r + \ldots + \varphi_r\psi_t$ geben, dessen Einschränkung auf G_r in $\mathrm{Aut}(G_r)$ liegt. Also ist auch

$$(\varphi_r\psi_j)^{n+1}|_{G_r} = \varphi_r(\psi_j\varphi_r)^n\psi_j|_{G_r} \in \mathrm{Aut}(G_r)$$

und $\psi_j\varphi_r|_{H_j} \in \mathrm{End}_{\triangleleft}(H_j)$ nicht nilpotent. Weil auch H_j sowohl ACC als auch DCC erfüllt, folgt aus Folgerung 8.5.3.2, dass $\psi_j\varphi_r|_{H_j}$ ein Automorphismus auf H_j ist. Daher sind $\psi_j|_{G_r}\colon G_r \to H_j$ und $\varphi_r|_{H_j}\colon H_j \to G_r$ Isomorphismen. Es folgt nach geeigneter Umnummerierung $G_r \cong H_r$.
Zu zeigen bleibt $G = G_1 \odot \ldots \odot G_r \odot H_{r+1} \odot \ldots \odot H_t$. Sei zu diesem Zwecke

$$G^* := G_1 \cdot \ldots \cdot G_r \cdot H_{r+1} \cdot \ldots \cdot H_t = \{g_1 \cdot \ldots \cdot g_r \cdot h_{r+1} \cdot \ldots \cdot h_t : g_i \in G_i, h_j \in H_j\}.$$

Nach der Induktionsannahme können wir

$$G_* := G_1 \cdot \ldots \cdot G_{r-1} \cdot H_{r+1} \cdot \ldots \cdot H_t = G_1 \odot \ldots \odot G_{r-1} \odot H_{r+1} \odot \ldots \odot H_t$$

betrachten. Für $j < r$ ist $\psi_r(G_j) = \psi_r\psi_j(G) = \{e\}$, für $j > r$ ist $\psi_r(H_j) = \psi_r\psi_j(G) = \{e\}$, also $\psi_r(G_*) = \{e\}$. Da $\psi_r|_{G_r}$ ein Isomorphismus ist, folgt $G_r \cap G_* = \{e\}$. Außerdem sind alle Faktoren in der nachfolgenden Zerlegung Normalteiler, weshalb wirklich eine direkte Zerlegung vorliegt:

$$G^* = G_* \odot G_r = G_1 \odot \ldots \odot G_r \odot H_{r+1} \odot \ldots \odot H_t \leq G.$$

Wir definieren $\theta\colon G = G_* \odot H_r \to G_* \odot G_r = G^*$ durch

$$g = g_1 \cdot \ldots \cdot g_{r-1} \cdot h_r \cdot \ldots \cdot h_t \in G \mapsto g_1 \cdot \ldots \cdot g_{r-1} \cdot \varphi_r(h_r) \cdot h_{r+1} \cdot \ldots \cdot h_t,$$

wobei $g_i \in G_i, h_j \in H_j$. Anhand der Darstellung $G = G_1 \odot \ldots \odot G_{r-1} \odot H_r \odot \ldots \odot H_t$ (Induktionsannahme) sieht man, dass θ auf G wohldefiniert ist, wegen der Injektivität von φ_r auf H_r auch injektiv. Auch die Normalität von φ_r vererbt sich auf θ (nachrechnen, siehe Übungsaufgabe 8.5.4.1). Wegen Lemma 8.5.2.4 ist daher $\theta \in \mathrm{Aut}(G)$, also $G = \mathrm{Im}\,\theta = G^*$. Damit ist $A(r)$ gezeigt und der Induktionsbeweis erbracht. Insbesondere gilt $A(\min(s,t))$.
Nach Umnummerierung gilt also $G_i \cong H_i$ für $0 \leq i \leq \min(s,t)$. Ist $\min(s,t) = s$, dann gilt

$$G_1 \odot \ldots \odot G_s = G = G_1 \odot \ldots \odot G_s \odot H_{s+1} \odot \ldots \odot H_t.$$

Ist $\min(s,t) = t$, dann gilt

$$G_1 \odot \ldots \odot G_s = G = G_1 \odot \ldots \odot G_t.$$

Da aber alle $G_i, H_j \neq \{e\}$ sind, muss in jedem Fall $s = t$ gelten. □

UE 98 ► Übungsaufgabe 8.5.4.1. (V) Überprüfen Sie, dass der in obigem Beweis auftretende Endomorphismus θ tatsächlich ein normaler ist. **◄ UE 98**

9 Galoistheorie

Die Galoistheorie ist eine Vertiefung der Körpertheorie mit vorwiegend gruppentheoretischen Methoden. Das vorliegende Kapitel kann daher als eine Fortsetzung von Kapitel 6 unter essenzieller Verwendung von Ergebnissen aus Kapitel 8 betrachtet werden.
Die Galoistheorie erfreut sich innerhalb der Algebra – um nicht zu sagen innerhalb der gesamten Mathematik – eines besonderen Status. Sie entsprang historisch einem klassischen Anliegen der Mathematik, nämlich dem Lösen von Gleichungen. Indem die Galoistheorie auf geniale Weise Automorphismengruppen von Körpern nutzbar macht, sind gleichzeitig ihre Methoden und Sichtweisen darüber hinaus von einer Originalität, von der im Laufe der Geschichte auch viele andere Gebiete der Mathematik außerhalb der Algebra profitiert haben.
Um diese Besonderheiten ins rechte Licht zu stellen, ist dem Kapitel ein eigener Abschnitt über das sehr allgemeine Konzept der Galoiskorrespondenz vorangestellt – von einer beliebigen zweistelligen Relation induziert wie auch der abstrakten (9.1). Sodann wenden wir uns der klassischen Galoiskorrespondenz zu, die durch Körpererweiterungen $K \leq E$ über die Fixpunktrelation von K-Automorphismen von E induziert wird. Dabei stößt man auf sehr natürliche Weise auf den Begriff der Galoisschen Erweiterung, dem Abschnitt 9.2 gewidmet ist. Der Hauptsatz der Galoistheorie ist Gegenstand von 9.3. Er beschreibt die Galois-abgeschlossenen Elemente bei Galoisschen Erweiterungen. Konkret geht es um die bijektive Beziehung zwischen den Körpern Z mit $K \leq Z \leq E$ einerseits und den (bezüglich einer natürlichen Topologie abgeschlossenen) Untergruppen der sogenannten Galoisgruppe $\mathrm{Aut}_K(E)$ andererseits. Dabei besteht $\mathrm{Aut}_K(E)$ definitionsgemäß aus den K-Automorphismen von E, d.h. aus jenen Automorphismen von E, die K punktweise fest lassen. Der Spezialfall, dass E der Zerfällungskörper eines Polynoms über K ist, wird in 9.4 ausführlich untersucht. Der letzte Abschnitt der Kapitels (9.5) widmet sich schließlich dem historischen Ursprung der Galoistheorie, der sogenannten Auflösbarkeit von Gleichungen durch Radikale.

9.1 Historie und allgemeine Grundkonzepte

Ein wenn auch kurzer, so doch eigener einleitender Abschnitt zum Kapitel über Galoistheorie ist dem bereits in der Kapiteleinleitung hervorgehobenen Umstand geschuldet, dass die Galoistheorie in vielerlei Hinsicht paradigmatisch für zahlreiche wichtige Teile der Mathematik ist. In 9.1.1 wird das unter historischem Blickpunkt relativ ausführlich besprochen – ausführlicher jedenfalls als Historisches in anderen Kapiteln zur Sprache kommt. Auf mathematischer Ebene spiegelt sich die paradigmatische Rolle der Galoistheorie wider im sehr allgemeinen und von der Theorie der Körper an sich unabhängigen Begriff der Galoiskorrespondenz. Meist treten Galoiskorrespondenzen als durch eine Re-

lation induziert auf. Das ist Gegenstand von 9.1.2. Man kann aber auch von der Relation abstrahieren und den Begriff der abstrakten Galoiskorrespondenz prägen. Das geschieht in 9.1.3. Abschließend werden noch einige andere prominente Beispiele aus unterschiedlichen Gebieten des Mathematik erwähnt (9.1.4).

9.1.1 Historisches

Ihren historischen Ausgangspunkt nahm die Galoistheorie bei der Suche nach Lösungsformeln für algebraische Gleichungen in einer Variablen, also Gleichungen der Form $f(x) = 0$ mit einem Polynom f. Klarerweise wird diese Aufgabe mit wachsendem Grad n von f zunehmend schwieriger. Die Lösungen für $n = 1$ und teilweise auch $n = 2$ waren schon Mathematikern antiker Hochkulturen vertraut. Nach Europa gelangten diese Einsichten aber erst im Mittelalter. Die Lösung für $n = 3, 4$ geht auf italienische Mathematiker des 16. Jahrhunderts zurück, dann stand man an. Erst um 1800 gelang Carl Friedrich Gauß (1777-1855) der erste Beweis des sogenannten Fundamentalsatzes der Algebra, dass jedes nichtkonstante Polynom eine komplexe Nullstelle hat. Allgemeine Lösungsformeln für $n \geq 5$ wurden aber keine gefunden. Langsam kam man zur Überzeugung, dass dies gar nicht möglich ist. Die wichtigsten Namen in diesem Zusammenhang sind Niels Henrik Abel (1802–1829) und Évariste Galois (1811–1832). Abel konnte zeigen, dass es keine allgemeine Lösungsformel für algebraische Gleichungen vom Grad ≥ 5 gibt, und Galois schuf eine Theorie, die sehr genau erklärt, woran das liegt und welche speziellen Gleichungen sehr wohl durch solche Formeln gelöst werden können. Berühmt ist die Geschichte von dem Duell, in dem der nicht einmal 21-jährige Galois umkam. In der Nacht davor hatte er seine Ideen in einem Brief an einen Freund hastig zu Papier gebracht. Hermann Weyl (1885-1955) schreibt darüber in seinem Buch über Symmetrie: „Ich wage die Behauptung, daß dieser Brief, auf die Originalität und die Tiefe der darin niedergelegten Ideen hin beurteilt, das inhaltreichste Stück Literatur ist, das wir besitzen.“ Wir werden in Abschnitt 9.5 ausführlich auf das Hauptresultat von Galois zurückkommen.

Aus heutiger Perspektive ist die Lösung des ursprünglichen Problems vergleichsweise eine Randerscheinung. Von ungeheurer Tragweite hingegen ist die Methode, mit der die Einsichten gewonnen wurden. Und zwar stellt sich heraus, dass für die Auflösbarkeit einer algebraischen Gleichung die Symmetrien zwischen den verschiedenen Lösungen entscheidend sind, technisch gesprochen: Die sogenannte Galoisgruppe des Polynoms f muss auflösbar im Sinne der Gruppentheorie sein.

Natürlich ist die Chronologie der Terminologie umgekehrt. Denn Galois führte erst im Zuge seiner Problemlösung den Begriff der Gruppe ein, und die Bezeichnung „auflösbar“ in Bezug auf eine Gruppe ergab sich erst im Anschluss daran in Hinblick auf die Auflösbarkeit von Gleichungen durch Lösungsformeln. Damit wurde eine Abstraktionsebene ganz neuer Art geschaffen – in ähnlicher Weise wie etwa zur gleichen Zeit János Bolyai (1802–1860), Nikolai Iwanowitsch Lobatschewski (1792–1856) und Gauß gleichfalls Unmöglichkeitsbeweise führten. Indem sie Beispiele nichteuklidischer Geometrien angaben, zeigten sie, dass das legendäre Parallelenpostulat, das für die euklidische Geometrie typisch ist, in diesen Modellen aber verletzt ist, aus den anderen Grundannahmen, die

in ihren Geometrien sehr wohl erfüllt sind, also nicht denknotwendig folgt. Derartige Gedankengänge waren damals von einer revolutionären Abstraktheit und führten die Mathematik in eine neue Epoche.
Revolutionär an der Galoistheorie war es, den unmittelbar gegebenen Objekten – in diesem Fall algebraische Gleichungen bzw. Polynome – abstrakte Strukturen zuzuordnen: einerseits Erweiterungs- und Zwischenkörper, andererseits die Gruppen von Automorphismen – eben die Galoisgruppen. Die neugeschaffenen Gebilde können ihrerseits unter völlig neuen Gesichtspunkten betrachtet werden, wodurch wiederum neue Phänomene – gefasst im Begriff der Galoiskorrespondenz – sichtbar werden. Das führt zu Einsichten, die auf der ursprünglichen, elementaren Ebene von einem Dickicht technischer Details überwuchert werden, in dem sie anders wahrscheinlich nie entdeckt worden wären.
Es ist sehr bemerkenswert, dass der Gesichtspunkt der Galoistheorie, mathematische Objekte durch ihre (eventuell auch sehr abstrakten) Symmetrien besser zu verstehen, auch dort, wo Symmetrie scheinbar ihren Ursprung hat, nämlich in der Geometrie, erst später zum Paradigma wurde. Berühmt ist in diesem Zusammenhang das sogenannte Erlangener Programm von Felix Klein (1849–1925) aus dem Jahr 1872. Darin werden Eigenschaften geometrischer Objekte dadurch als interessant und untersuchenswürdig ausgezeichnet, dass sie unter Transformationen unterschiedlicher Art invariant bleiben. Im Vergleich mit der Galoistheorie wird die Rolle der Galoisgruppe nun von geometrisch motivierten Transformationsgruppen übernommen.
Im 20. Jahrhundert erfuhr diese Herangehensweise auf nochmals gesteigertem Abstraktionsniveau eine Fortsetzung in der Modelltheorie, einem der mittlerweile als klassisch etablierten Teilgebiete der mathematischen Logik, das gleichzeitig eine sehr lebendige und fruchtbare Verbindung wieder zurück zur Algebra darstellt. Im Vergleich mit der Galoistheorie treten in der Modelltheorie an die Stelle von Körpern allgemeinere Klassen von Strukturen, wie wir sie in Abschnitt 2.1 und insbesondere in Unterabschnitt 2.1.4 behandelt haben. Auch in der Modelltheorie spielen Erweiterungen und Automorphismengruppen eine große Rolle. Dabei wird auch die eminente Bedeutung der zugrunde liegenden formalen Sprache deutlich, was auch der Grund dafür ist, dass die Modelltheorie traditionell der Logik und nicht mehr der Algebra zugeordnet wird.

Abgesehen von der prägenden Rolle der Galoistheorie in der Ideengeschichte der gesamten Mathematik empfinden viele Mathematiker:innen an ihr auch einen ganz außergewöhnlichen ästhetischen Reiz. Um diesen zu genießen, wollen wir nach unserem historischen Exkurs zurückkehren zum mathematisch konkret Fassbaren. Es beginnt mit einem der Galoistheorie zugrundeliegenden sehr allgemeinen Konzept, das in vielen Teilen der Mathematik wirksam ist.

9.1.2 Die von einer Relation induzierte Galoiskorrespondenz

Wir wollen unsere Überlegungen mit einer einfachen Beobachtung beginnen. Seien X und Y Mengen (oder gar Klassen, die keine Mengen sind) und $R \subseteq X \times Y$ eine Relation, sei $f_R \colon \mathcal{P}(X) \to \mathcal{P}(Y)$ definiert als

$$f_R : A \mapsto A^{(R)} := \{y \in Y \mid \forall x \in A : xRy\}$$

und $g_R\colon \mathcal{P}(Y) \to \mathcal{P}(X)$ als

$$g_R : B \mapsto {}^{(R)}B := \{x \in X \mid \forall y \in B : xRy\}.$$

Dann sind

(a) f_R, g_R *antiton*, d.h.

$$A_1 \subseteq A_2 \Rightarrow f_R(A_1) \supseteq f_R(A_2)$$
$$B_1 \subseteq B_2 \Rightarrow g_R(B_1) \supseteq g_R(B_2)$$

und

(b) $g_R f_R, f_R g_R$ *extensiv*, d.h.

$$\overline{A} = \overline{A}^{(R)} := g_R f_R(A) \supseteq A$$
$$\overline{B} = \overline{B}^{(R)} := f_R g_R(B) \supseteq B.$$

Mit dieser Notation definieren wir:

Definition 9.1.2.1. Das Paar (f_R, g_R) heißt die *von der Relation R induzierte Galoiskorrespondenz* oder auch *Galoisverbindung*. Die Mengen $A \in \mathrm{Im}(g_R)$ und $B \in \mathrm{Im}(f_R)$ (die also als Bilder unter g_R bzw. f_R auftreten), heißen *Galois-abgeschlossen*.

In diesem Kapitel wird das folgende klassische Beispiel einer Galoiskorrespondenz im Zentrum stehen:

Beispiel 9.1.2.2. Sei $K \leq E$ eine Körpererweiterung,

$$X := \mathrm{Aut}_K(E) := \{\sigma \in \mathrm{Aut}(E) \mid \forall \alpha \in K : \sigma(\alpha) = \alpha\}$$

die Menge aller K-*Automorphismen* des Erweiterungskörpers E, also jener $\sigma \in \mathrm{Aut}(E)$, die jedes Element α des Grundkörpers K auf sich selbst abbilden, weiters $Y := E$ und

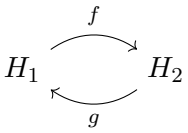
$$R := \{(\sigma, \alpha) \in X \times Y \mid \sigma(\alpha) = \alpha\}.$$

Für $A \subseteq X$ ist $A^{(R)}$ offenbar stets ein K umfassender Unterkörper von E, für $B \subseteq Y$ ist ${}^{(R)}B$ stets eine Untergruppe von $\mathrm{Aut}_K(E)$. Die von R induzierte Galoiskorrespondenz ist die klassische, die der Galoistheorie zugrunde liegt.

Man kann das Konzept der Galoiskorrespondenz aber auch von einer Relation loslösen und eine abstrakte Definition geben.

9.1.3 Abstrakte Galoiskorrespondenzen

Definition 9.1.3.1. Seien die Halbordnungen $(H_1, \leq_1), (H_2, \leq_2)$ gegeben zusammen mit Abbildungen $f : H_1 \to H_2$, $g : H_2 \to H_1$.



Dann heißt (f, g) *(abstrakte) Galoisverbindung* oder *Galoiskorrespondenz* auf den Halbordnungen $(H_1, \leq_1)$ und $(H_2, \leq_2)$, falls f, g *antiton* sind (d.h. explizit: $h_1 \leq h_1'$ impliziert $f(h_1) \geq f(h_1')$ und $h_2 \leq h_2'$ impliziert $g(h_2) \geq g(h_2')$ für alle $h_i, h_i' \in H_i$) und die Verkettungen gf, fg *extensiv* sind (d.h. explizit: $h_1 \leq g(f(h_1))$ und $h_2 \leq f(g(h_2))$ für alle $h_i \in H_i$). Elemente von H_1 und H_2, die als Bilder unter g bzw. f auftreten, heißen *Galois-abgeschlossen*.

Nach Unterabschnitt 9.1.2 ist jede von einer Relation $R \subseteq X \times Y$ induzierte Galoiskorrespondenz auch eine abstrakte Galoiskorrespondenz auf den Halbordnungen $(\mathcal{P}(X), \subseteq)$ und $(\mathcal{P}(Y), \subseteq)$.
Es zeigt sich, dass sogar eine Art Umkehrung gilt: Jede abstrakte Galoiskorrespondenz (f, g) hängt sehr eng mit einer Galoiskorrespondenz zusammen, die von einer Relation R induziert wird.
Um das zu sehen, wählen wir mit der Notation aus Definition 9.1.3.1 die Mengen $X := H_1$ und $Y := H_2$ sowie die Relation

$$R := \{(x, y) : f(x) \geq_2 y\} \subseteq X \times Y.$$

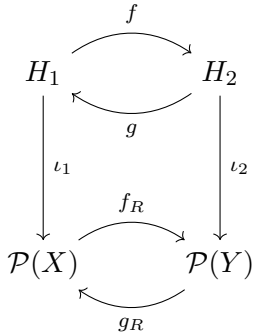
Nach Unterabschnitt 9.1.2 induziert R auf den Halbordnungen $(\mathcal{P}(X), \subseteq)$ und $(\mathcal{P}(Y), \subseteq)$ eine Galoiskorrespondenz (f_R, g_R). Vermittels der injektiven Abbildungen

$$\iota_1 : X \to \mathcal{P}(X), \quad \iota_1(h_1) := \{x \in X : x \leq_1 h_1\}$$

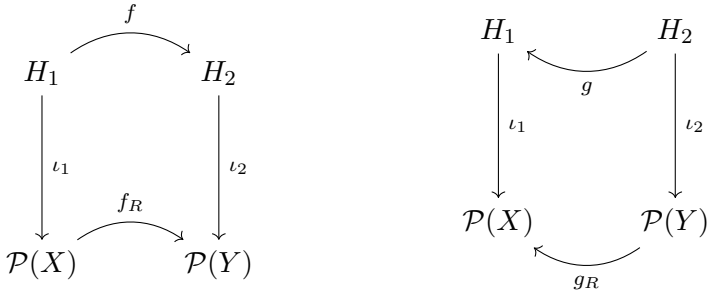
und

$$\iota_2 : Y \to \mathcal{P}(Y), \quad \iota_2(h_2) := \{y \in Y : y \leq_2 h_2\}$$

wird die ursprüngliche Galoiskorrespondenz (f, g) in die von R induzierte Galoiskorrespondenz (f_R, g_R) eingebettet. Die Situation wird durch das Diagramm



veranschaulicht. Als ganzes ist es zwar *nicht* kommutativ, weil die Abbildungen f und g sowie f_R und g_R nicht auf ihrem gesamten Definitionbereich invers zueinander sind. Zerlegt man das ursprüngliche Diagramm in einen f- und einen g-Teil, so erhält man aber zwei Diagramme, von denen jedes für sich sehr wohl kommutiert:



Da also $f_R\iota_1 = \iota_2 f$ und $g_R\iota_2 = \iota_1 g$ gilt, ist es durchaus suggestiv und nicht abwegig, von einer Einbettung von (f, g) in (f_R, g_R) zu sprechen.

UE 99 ► **Übungsaufgabe 9.1.3.2.** (V) Verifizieren Sie alle die Einbettung von (f, g) in (f_R, g_R) betreffenden Behauptungen. ◄ **UE 99**

Wir fassen die wichtigsten Eigenschaften abstrakter Galoiskorrespondenzen zusammen:

Satz 9.1.3.3. *Für eine (abstrakte) Galoiskorrespondenz (f, g) auf den Halbordnungen $(H_1, \leq_1)$ und $(H_2, \leq_2)$ gilt*

(a) Idempotenz: $f = fgf$ und $g = gfg$.

(b) $\operatorname{Im} f = \operatorname{Im} fg$ *und* $\operatorname{Im} g = \operatorname{Im} gf$ *(die Mengen der Galois-abgeschlossenen Elemente).*

(c) $f|_{\operatorname{Im} g}$ und $g|_{\operatorname{Im} f}$ sind zueinander inverse antitone Bijektionen, insbesondere gilt:

$$(\operatorname{Im} g, \leq_1) \cong (\operatorname{Im} f, \geq_2)$$

Beweis. (a): Da fg und gf extensiv sind, gilt $h_1 \leq gf(h_1)$ und $f(h_1) \leq fg(f(h_1))$ für alle $h_1 \in H_1$. Da f antiton ist, folgt aus der ersten Ungleichung auch $f(h_1) \geq f(gf(h_1))$, zusammen mit der zweiten daher insgesamt $f = fgf$. Analog erhält man $g = gfg$.
(b): Es gilt

$$\operatorname{Im} f \supseteq \operatorname{Im} fg \supseteq \operatorname{Im} fgf \overset{(a)}{=} \operatorname{Im} f,$$

also $\operatorname{Im} f = \operatorname{Im} fg$. Analog folgt $\operatorname{Im} g = \operatorname{Im} gf$.
(c): Aus (a) ergibt sich $fg|_{\operatorname{Im} f} = \mathrm{id}_{\operatorname{Im} f}$ und $gf|_{\operatorname{Im} g} = \mathrm{id}_{\operatorname{Im} g}$, woraus direkt die Behauptung folgt. □

9.1.4 Beispiele von Galoiskorrespondenzen

Anhand einiger typischer Beispiele von Galoiskorrespondenzen aus verschiedenen Teilgebieten der Mathematik (teils nicht zwischen Mengen, sondern zwischen echten Klassen X, Y definiert) soll nun illustriert werden, dass in solchen Situationen immer wieder die Galois-abgeschlossenen Mengen von besonderem Interesse sind. Vieles wird im Rahmen von Übungsaufgaben abgehandelt.
Auf relativ elementarem Niveau gilt das für $X := V$ (Vektorraum über einem Körper K), $Y := V^*$ (Dualraum von V) und die Relation $R := \{(x, y) : \ y(x) = 0\} \subseteq X \times Y$ (Annihilatorrelation). Ist V endlichdimensional, so sind genau die Unterräume von V bzw. V^* die Galois-abgeschlossenen Mengen. Bei unendlichdimensionalem V ist die Situation jedoch komplizierter. Eine genauere Analyse ist Gegenstand der folgenden Übungsaufgabe, die in vielerlei Hinsicht schon einen Vorgeschmack auf den Hauptsatz der Galoistheorie liefert.

UE 100 ► **Übungsaufgabe 9.1.4.1.** (B,E) Sei V ein Vektorraum über einem Körper K und V^* sein Dualraum, d.h. der Vektorraum aller linearen Funktionale $f : V \to K$. Die Relation $R := \{(f, v) \in V^* \times V : \ f(v) = 0\}$ induziert eine Galoisverbindung, von der im Folgenden die Rede ist. Sei B eine Basis von V und B^* die Menge aller $f_b \in V^*$, $b \in B$, die durch die Forderung $f_b(b') = \delta_{b,b'}$ (Kronecker-δ), $b' \in B$, eindeutig definiert sind. Rekapitulieren Sie aus der Linearen Algebra und/oder Funktionalanalysis bzw. beweisen Sie: ◄ **UE 100**

1. Die bezüglich R Galois-abgeschlossenen Teilmengen von V sind genau die Unterräume von V.

2. Die bezüglich R Galois-abgeschlossenen Teilmengen von V^* sind durchwegs Unterräume von V^*.

3. Ist V endlichdimensional, so ist umgekehrt jeder Unterraum von V^* auch Galois-abgeschlossen.

4. Sei $K = \mathbb{Q}$, $V := \bigoplus_{n\in\mathbb{N}} \mathbb{Q}$ und $b_n := (\delta_{n,k})_{k\in\mathbb{N}}$ für alle $n \in \mathbb{N}$. Dann gibt es Unterräume von V^*, die nicht Galois-abgeschlossen sind. Beweisen Sie das zunächst in dieser Teilaufgabe mit einem Kardinalitätsargument. Hinweis: $B := \{b_n : \ n \in \mathbb{N}\}$ ist eine abzählbare Basis von V, V selbst ist abzählbar, und die Menge $\mathrm{Sub}(V) := \{U : \ U \leq V\}$ aller Unterräume von V hat die Kardinalität c des Kontinuums. Hingegen ist V^* überabzählbar von der Kardinalität c. Daraus folgt, dass $\mathrm{Sub}(V^*)$ von der Kardinalität 2^c ist. Nach Cantor kann es also keine Bijektion zwischen $\mathrm{Sub}(V)$ und $\mathrm{Sub}(V^*)$ geben.

5. Bezeichne τ die schwach-$*$-Topologie. Das ist per definitionem die schwächste Topologie auf V^*, bezüglich der alle Auswertungsfunktionale $v^* : V^* \to K$, $f \mapsto f(v)$, $v \in V$, stetig sind. Wenn K mit der diskreten Topologie versehen ist, ist eine Umgebungsbasis des Nullfunktionals $0_{V^*} \equiv 0_K$ bezüglich τ gegeben durch das System sämtlicher Mengen $O_E := \{f \in V^* : \ f(v) = 0 \text{ für alle } v \in E\}$, wobei E alle

endlichen Teilmengen (oder äquivalent: alle endlich erzeugten Unterräume) von V durchläuft.

6. Die schwach-$*$-Topologie τ macht V^* zu einem topologischen Vektorraum.

7. Alle Galois-abgeschlossenen Unterräume von V^* sind auch bezüglich der schwach-$*$-Topologie τ abgeschlossen.

8. Es gilt auch die Umkehrung: Jeder schwach-$*$-abgeschlossene Unterraum von V^* ist Galois-abgeschlossen. Die ordnungsumkehrenden Bijektionen der Galoiskorrespondenz bestehen also zwischen sämtlichen Unterräumen von V und den schwach-$*$-abgeschlossenen Unterräumen von V^*.

Eine ganz ähnliche Situation wird uns in der eigentlichen Galoistheorie begegnen. Der Hauptsatz in seiner allgemeinen Fassung (9.3.4.2) wird in ganz ähnlicher Weise eine mit einer zur schwach-$*$ Topologie analogen Topologie angereicherte Verallgemeinerung des endlichdimensionalen Falles sein.
Der Übergang von den Sichtweisen der Linearen Algebra zu jenen der Funktionalanalysis wird in der folgenden Übungsaufgabe vollzogen:

UE 101 ► **Übungsaufgabe 9.1.4.2.** (B,E) Versuchen Sie Übungsaufgabe 9.1.4.1 so weit wie möglich von diskreten auf lokalkonvexe Vektorräume V zu verallgemeinern. Der Dualraum V^* besteht dann lediglich aus den stetigen Funktionalen. Aus welchem berühmten Satz der Funktionalanalysis ergibt sich sehr schnell eine Beschreibung der Galois-abgeschlossenen Teilmengen von V? Was können Sie über jene in V^* aussagen? ◄ **UE 101**

Sehr ähnlich verhält es sich, wenn man lokalkonvexe Vektorräume durch lokalkompakte abelsche Gruppen, den Skalarkörper $\mathbb{R}$ durch die Gruppe $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ und lineare Funktionale durch stetige Homomorphismen ersetzt.

UE 102 ► **Übungsaufgabe 9.1.4.3.** (B,E,D) Rekapitulieren Sie die Pontrjagin-Dualität aus Unterabschnitt 7.1.4 so weit wie nötig, um analoge Fragen für eine lokalkompakte abelsche Gruppe G, ihr Pontrjagin-Dual G^* und die Annihilatorrelation $\chi(g) = 0$ für $g \in G$ und $\chi \in G^*$ zu behandeln. Es wird nicht erwartet, dass Sie alle Beweise für die hier interessanten Aussagen führen. Es genügt, wenn Sie die Ergebnisse recherchieren. ◄ **UE 102**

Als weiteres Beispiel für die Beschreibung von Galois-Abgeschlossenheit ist der Satz von Birkhoff 4.1.7.1 zu nennen. Er lässt sich als Beschreibung der Galois-abgeschlossenen Elemente (nämlich der Varietäten) bezüglich einer geeigneten Galoiskorrespondenz interpretieren. Diese wird induziert von der Relation der Gültigkeit einer Gleichung in einer bestimmten Algebra. Allerdings muss man hier den Rahmen von Mengen verlassen und auch Klassen (nämlich von Algebren) zulassen.

UE 103 ▶ **Übungsaufgabe 9.1.4.4.** (B,E,D) Präzisieren Sie diese Andeutungen. Beschreiben Sie insbesondere genauer die Relation, bezüglich derer laut dem Satz von Birkhoff 4.1.7.1 auf der einen Seite genau die Varietäten Galois-abgeschlossen sind. Wie könnte eine Beschreibung der Galois-abgeschlossenen Mengen auf der anderen Seite dieser Galoiskorrespondenz aussehen? ◀ **UE 103**

Man kann die Betrachtung auf der einen Seite von rein algebraischen Strukturen auf beliebige algebraisch-relational gemischte Strukturen eines bestimmten Typs (einer bestimmten Signatur) (τ, σ) ausweiten, siehe Unterabschnitt 2.1.4. Auf der anderen Seite entspricht dem eine Anreicherung der formalen Sprache von Gleichungen für algebraische Operationen und Variablen (um die es im Satz von Birkhoff geht) zu einer vollen prädikatenlogischen Sprache für (τ, σ). Die Relation ist wieder die Gültigkeit einer Formel in einer Struktur. Die Frage nach den Galois-abgeschlossenen Elementen führt direkt in das Zentrum der mathematischen Logik. Wer sich dafür interessiert, sollte an der folgenden Übungsaufgabe Freude finden.

UE 104 ▶ **Übungsaufgabe 9.1.4.5.** (B,E,D) Untersuchen Sie die angedeutete Galoiskorrespondenz, die von jener Relation R induziert wird, die aus gewissen Paaren $(\mathfrak{A}, \varphi)$ besteht mit folgenden Eigenschaften: $\mathfrak{A}$ ist eine relationale Struktur mit der (als vorgegeben zu denkenden) Signatur (τ, σ) und φ ein Satz (d.h. eine Formel ohne freie Variable, der somit in jedem Modell ein eindeutig bestimmter Wahrheitswert zukommt) einer zugehörigen formalen Sprache. Zu R gehört das Paar $(\mathfrak{A}, \varphi)$ genau dann, wenn φ in $\mathfrak{A}$ wahr ist. ◀ **UE 104**

Die bisher angedeuteten Galoiskorrespondenzen wurden hier nur als illustrierende Beispiel erwähnt. Genauer untersuchen werden wir in dieser Vorlesung zwei Beispiele: in diesem Kapitel die klassische Galoiskorrespondenz (siehe Unterabschnitt 9.2.1) sowie im letzten Kapitel den Hilbertschen Nullstellensatz (siehe Abschnitt 10.3).

UE 105 ▶ **Übungsaufgabe 9.1.4.6.** (D) Fallen Ihnen noch weitere interessante Beispiele von Galoiskorrespondenzen ein? Wenn ja erklären Sie solche. Geben Sie insbesondere jeweils X, Y und R an und beschreiben Sie nach Möglichkeit die Galois-abgeschlossenen Elemente $\subseteq X$ und/oder $\subseteq Y$. ◀ **UE 105**

9.2 Galoissche Körpererweiterungen

Nach dem Studium allgemeiner Galoiskorrespondenzen in Abschnitt 9.1 wenden wir uns nun der klassischen Galoiskorrespondenz zu (siehe 9.2.1). Diese wird bei gegebener Körpererweiterung $K \leq E$ durch die Fixpunktrelation zwischen K-Automorphismen und Körperelementen von E induziert. Die Erweiterung heißt Galoissch, wenn der Grundkörper K bezüglich dieser Galoiskorrespondenz Galois-abgeschlossen ist. Ist dies der Fall, so lassen sich für algebraische Erweiterungen sehr schnell zwei Eigenschaften herleiten: normal und separabel (siehe 9.2.2). Beiden ist jeweils ein Unterabschnitt gewidmet (9.2.3

bzw. 9.2.4), bevor wir schließlich zeigen, dass für algebraische Erweiterungen die Eigenschaften normal und separabel auch hinreichend dafür sind, eine Galoissche Erweiterung zu bilden (9.2.5). Nur einzelne Ergebnisse von Abschnitt 9.2 sind für den Beweis des Hauptsatzes der Galoistheorie in Abschnitt 9.3 erforderlich. Trotzdem wurde dieser Abschnitt als der weniger technische und stärker konzeptionell geprägte vorgezogen.

9.2.1 Die klassische Galoiskorrespondenz

Wie schon in der Einleitung erwähnt, geht es in der klassischen Galoistheorie um die Untersuchung von Körpererweiterungen $K \leq E$ mit gruppentheoretischen Methoden. Und zwar geht es um die Galoisgruppe, deren Elemente sogenannte K-Automorphismen von E sind, die definitionsgemäß K punktweise fest lassen. Die Galoiskorrespondenz wird von der Fixpunktrelation induziert. Es folgt eine Zusammenfassung dieser sowie unmittelbar daran anschließender Definitionen.

Definition 9.2.1.1. Sei $K \leq E$ eine Körpererweiterung. Unter einem *K-Automorphismus* von E versteht man einen Automorphismus $\sigma \in \mathrm{Aut}(E)$ mit $\sigma(\alpha) = \alpha$ für alle $\alpha \in K$. Die Menge

$$G_K(E) = \mathrm{Aut}_K(E) := \{\sigma \in \mathrm{Aut}(E) \mid \forall \alpha \in K\ \sigma(\alpha) = \alpha\}$$

aller K-Automorphismen von E heißt die *Galoisgruppe* von E über K.
Die von der Relation (*Fixpunktrelation*)

$$R := \{(\sigma, \alpha) \in \mathrm{Aut}_K(E) \times E \mid \sigma(\alpha) = \alpha\}$$

auf $\mathrm{Aut}_K(E) \times E$ induzierte Galoiskorrespondenz (f_R, g_R) heißt die von der Erweiterung $K \leq E$ induzierte *(klassische) Galoiskorrespondenz*. Für die Wirkung von f_R und g_R auf Teilmengen $H \subseteq \mathrm{Aut}_K(E)$ bzw. $Z \subseteq E$ schreiben wir vorzugsweise auch

$$f_R: \quad \mathrm{Aut}_K(E) \supseteq H \quad \mapsto \quad H' := \{\alpha \in E \mid \sigma(\alpha) = \alpha \text{ für alle } \sigma \in H\} \leq E$$

bzw.

$$g_R: \quad E \supseteq Z \quad \mapsto \quad Z' := \{\sigma \in \mathrm{Aut}_K(E) \mid \sigma(\alpha) = \alpha \text{ für alle } \alpha \in Z\} \leq \mathrm{Aut}_K(E).$$

Für $K \leq Z \leq E$ ist Z' die *Galoisgruppe* von E über Z, für $H \subseteq \mathrm{Aut}_K(E)$ ist H' der *Fixpunktkörper* von H (siehe auch Proposition 9.2.1.2).
Ein Körper Z mit $K \leq Z \leq E$ heißt *Zwischenkörper* (bezüglich der Erweiterung $K \leq E$).
Die Körpererweiterung $K \leq E$ heißt *Galoissche Erweiterung*, und E heißt *Galoissch* über K, wenn K bezüglich der klassischen Galois-Korrespondenz Galois-abgeschlossen ist, d.h. wenn es zu jedem $\alpha \in E \setminus K$ ein $\sigma \in \mathrm{Aut}_K(E)$ mit $\sigma(\alpha) \neq \alpha$ gibt.[1]

Folgende einfache aber wichtige Beobachtungen halten wir fest:

[1] Man erinnere sich an die Rolle der Punktetrennung zum Beispiel von Funktionen im Approximationssatz von Weierstraß oder von linearen Funktionalen in der Funktionalanalysis.

Proposition 9.2.1.2. *Sei $K \leq E$ eine beliebige Körpererweiterung. Dann gilt mit den Notationen aus Definition 9.2.1.1:*

1. *Die Galoisgruppe $\mathrm{Aut}_K(E)$ ist bezüglich der Komposition $\circ$ tatsächlich eine Gruppe.*
2. *Für eine Teilmenge $Z \subseteq E$ ist $Z' \leq \mathrm{Aut}_K(E)$.*
3. *Für eine Teilmenge $H \subseteq \mathrm{Aut}_K(E)$ ist H' ein Zwischenkörper bezüglich der Erweiterung $K \leq E$, d.h. $K \leq H' \leq E$.*
4. *Bezeichne $K_1 := \mathrm{Aut}_K(E)'$ den Fixpunktkörper der Galoisgruppe $\mathrm{Aut}_K(E)$. Dann ist $K \leq K_1 \leq E$ und die Erweiterung $K_1 \leq E$ Galoissch mit Galoisgruppe $\mathrm{Aut}_{K_1}(E) = \mathrm{Aut}_K(E)$.*

UE 106 ▶ Übungsaufgabe 9.2.1.3. (V) Beweisen Sie Proposition 9.2.1.2. **◀ UE 106**

Ein vertrautes Beispiel für die Begriffe aus Definition 9.2.1.1 ist die Körpererweiterung $K = \mathbb{R} \leq \mathbb{C} = E$. Aus Satz 1.2.4.3 folgt, dass die Galoisgruppe von $\mathbb{C}$ über $\mathbb{R}$ zwei Elemente hat, die Identität und die komplexe Konjugation. Die komplexe Konjugation lässt nur die Elemente des Grundkörpers $\mathbb{R}$ fest. Also ist $\mathbb{R} \leq \mathbb{C}$ eine Galoissche Erweiterung. Als zweielementige Gruppe hat die Galoisgruppe $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ genau zwei Untergruppen, nämlich die einelementige Gruppe $\{\mathrm{id}_{\mathbb{C}}\}$ mit Fixpunktkörper $\mathbb{C}$ und sich selbst mit Fixpunktkörper $\mathbb{R}$. Bezüglich dieser Erweiterung gibt es auch genau zwei Zwischenkörper, nämlich die zugehörigen Fixpunktkörper $\{\mathrm{id}_{\mathbb{C}}\}' = \mathbb{C}$ und $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})' = \mathbb{R}$. Offenbar gilt auch $\mathbb{C}' = \{\mathrm{id}_{\mathbb{C}}\}$ und $\mathbb{R}' = \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$.
Nicht Galoissch ist hingegen die Erweiterung $\mathbb{Q} \leq \mathbb{R}$. Laut Folgerung 3.5.3.14 ist nämlich die Identität der einzige Automorphismus des Körpers $\mathbb{R}$, die Galoisgruppe $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R})$ also einelementig.
Dass eine durch die Fixpunktrelation induzierte bijektive Galoiskorrespondenz zwischen den (abgeschlossenen) Untergruppen und den Zwischenkörpern wie im Beispiel $\mathbb{R} \leq \mathbb{C}$ ganz allgemein für jede algebraische Galoissche Erweiterung besteht, ist die wichtigste Aussage des Hauptsatzes der Galoistheorie 9.3.1.1 bzw. 9.3.4.2.

Wir wollen noch ein wichtiges Resultat über die Veträglichkeit von K-Automorphismen mit Polynomen über K herleiten, die wir sehr häufig verwenden werden. Es lässt sich als Verallgemeinerung der bekannten Tatsache interpretieren, dass für jede komplexe Nullstelle α eines reellen Polynoms auch die konjugiert komplexe Zahl eine Nullstelle desselben Polynoms ist.

Proposition 9.2.1.4. *Sei $K \leq E$ eine Körpererweiterung mit Galoisgruppe $\mathrm{Aut}_K(E)$, $f \in K[x]$ ein Polynom über K und N die Menge aller Nullstellen von f in E. Dann ist die Einschränkung $\sigma|_N$ jedes Automorphismus $\sigma \in \mathrm{Aut}_K(E)$ auf N eine Permutation von N.*

Beweis. Sei $f(x) = \sum_{i=0}^{n} a_i x^i$. Wegen $f \in K[x]$ ist $a_i \in K$ für alle $i = 0, \ldots, n$. Ist $\alpha \in N$, also $f(\alpha) = 0$, so folgt aus der K-Linearität von σ (siehe auch Proposition 9.2.1.2, Aussage 2):

$$f(\sigma(\alpha)) = \sum_{i=1}^{n} a_i \sigma(\alpha) = \sigma\left(\sum_{i=1}^{n} a_i \alpha\right) = \sigma(f(\alpha)) = \sigma(0) = 0.$$

Also ist $\sigma(\alpha) \in N$ und somit, weil $\alpha \in N$ beliebig war, $\sigma(N) \subseteq N$. Als Automorphismus ist σ injektiv. Erst recht gilt das für die Einschränkung $\sigma|_N : N \to N$. Auf der endlichen Menge N zieht die Injektivität dieser Abbildung sogar Bijektivität nach sich. Insgesamt ist $\sigma|_N$ also eine Permutation von N. □

Somit liegt es in vielen Situationen nahe, Galoisgruppen als Permutationsgruppen auf endlichen Mengen zu interpretieren, was die Analyse vor allem bei endlichdimensionalen Erweiterungen in mancherlei Hinsicht einfacher machen kann. In Abschnitt 9.4 wird das der vorherrschende Standpunkt sein. Vorerst bevorzugen wir aber die allgemeine, abstrakte Sichtweise.

Wie bereits erwähnt, gilt der Hauptsatz der Galoistheorie nur für algebraische Galoissche Erweiterungen. Zwar ist es wegen der vierten Aussage aus Proposition 9.2.1.2 bei einer beliebig vorgegebenen Körpererweiterung $K \leq E$ stets möglich, zu einer Galoisschen überzugehen, indem man den Grundkörper K durch den Fixpunktkörper $K_1 := \mathrm{Aut}_K(E)'$ ersetzt. Auch führt dieser Schritt wieder zu einer algebraischen Erweiterung $K_1 \leq E$, sofern $K \leq E$ algebraisch ist. Trotzdem ist es von Interesse, Bedingungen dafür zu kennen, dass bereits $K \leq E$ Galoissch ist, also $K = K_1$ gilt.

9.2.2 Galoissch und algebraisch impliziert normal und separabel

Fragt man sich, ob eine Körpererweiterung $K \leq E$ Galoissch ist, hat man zu überlegen, ob es zu jedem $u \in E$ ein $\sigma \in \mathrm{Aut}_K(E)$ gibt mit $\sigma(u) \neq u$. Ist u algebraisch über K mit Minimalpolynom f, so kommen für $\sigma(u)$ laut Proposition 9.2.1.4 nur Nullstellen von f in Frage. Enthält E nur u als einzige Nullstelle von E, so werden wir also sicher kein $\sigma(u) \neq u$ finden, und die Erweiterung ist sicher nicht Galoissch.
Auf den ersten Blick fallen zweierlei mögliche Gründe für diese Situation ins Auge: Es kann erstens sein, dass E nicht sämtliche Nullstellen von f enthält, oder dass u in seinem Zerfällungskörper die einzige, also eine mehrfache Nullstelle von f ist. Das folgende Resultat zeigt, dass diese beiden Probleme bei Galoisschen Erweiterungen tatsächlich nicht auftreten können.

Proposition 9.2.2.1. *Sei $K \leq E$ eine Galoissche Erweiterung, $u \in E$ algebraisch über K und $f \in K[x]$ das Minimalpolynom von $u = u_1 \in E$. Dann zerfällt*

$$f(x) = \prod_{i=1}^{r} (x - u_i)$$

über E mit lauter verschiedenen Nullstellen $u_i \in E$.

Beweis. Seien $u = u_1, u_2, \ldots, u_r$ sämtliche paarweise verschiedene Wurzeln von f in E. Insbesondere ist $\operatorname{grad}(f) \geq r$. (A priori muss E keinen Zerfällungskörper von f enthalten!) Wir definieren

$$g(x) := \prod_{i=1}^{r}(x - u_i) = \sum_{j=0}^{r} a_j x^j$$

Die a_j sind bis auf das Vorzeichen die elementarsymmetrischen Polynome in den u_i. Alle $\tau \in \operatorname{Aut}_K(E)$ permutieren die u_i (Proposition 9.2.1.4), lassen also die a_j und somit g invariant. Somit gilt $a_i \in (\operatorname{Aut}_K(E))' = K$, weil $K \leq E$ Galoissch ist und es folgt $g \in K[x]$. Nach Voraussetzung ist f das Minimalpolynom von u über K. Wegen $g(u) = 0$ bedeutet das $f \mid g$. Da außerdem $\operatorname{grad}(g) = r \leq \operatorname{grad}(f)$ und f wie auch g normiert sind, folgt $f = g$. □

Proposition 9.2.2.1 motiviert zu den folgenden Definitionen 9.2.2.2 und 9.2.2.4:

Definition 9.2.2.2. Eine algebraische Körpererweiterung $K \leq E$ heißt *normal*, falls jedes irreduzible $f \in K[x]$ mit einer Nullstelle in E sogar in Linearfaktoren über E zerfällt.

Aus Proposition 9.2.2.1 folgt daher unmittelbar:

Proposition 9.2.2.3. *Ist die algebraische Körpererweiterung $K \leq E$ Galoissch, so ist sie auch normal.*

Definition 9.2.2.4. Ein Polynom $f \in K[x]$ heißt *separabel* über K, falls alle Nullstellen von f im Zerfällungskörper von f über K einfach sind. Ist E eine beliebige Körpererweiterung von K, so heißt ein Element $u \in E$ *separabel* über K, falls u algebraisch ist über K mit separablem Minimalpolynom. Die Körpererweiterung $K \leq E$ selbst heißt *separable Erweiterung*, falls alle $u \in E$ separabel über K sind.
Ein Polynom $f \in K[x]$ heißt *(rein) inseparabel*, falls es im Zerfällungskörper Z von der Form $f(x) = a(x-u)^n$ mit $a, u \in Z$ und $n \in \mathbb{N}$ ist. Ist E eine beliebige Körpererweiterung von K, so heißt ein Element $u \in E$ *inseparabel* über K, falls u algebraisch ist über K mit inseparablem Minimalpolynom. Die Körpererweiterung $K \leq E$ selbst heißt *inseparable Erweiterung*, falls alle $u \in E$ inseparabel über K sind.

Man beachte: Elemente des Grundkörpers K sind sowohl separabel als auch inseparabel über K, während es für Elemente aus $E \setminus K$ auch möglich ist, keine der beiden Eigenschaften zu haben. „Inseparabel“ ist also nicht die Negation von „separabel“.

Separabilität betreffend entnehmen wir Proposition 9.2.2.1 ebenfalls unmittelbar:

Proposition 9.2.2.5. *Ist die algebraische Körpererweiterung $K \leq E$ Galoissch, so ist sie auch separabel.*

Wir fassen das Wichtigste zusammen: Für algebraische Körpererweiterungen $K \leq E$ folgen aus „Galoissch“ die Eigenschaften „normal“ und „separabel“. Es wird sich zeigen, dass auch umgekehrt für algebraische Körpererweiterungen „normal und separabel“ stets „Galoissch“ nach sich zieht. Um das zu sehen, wollen wir zunächst die beiden Eigenschaften „normal“ und „separabel“ besser verstehen.

9.2.3 Normale Erweiterungen

Als Erstes zeigen wir eine Hilfsaussage, die wir mehrmals einsetzen werden und die das technische Rückgrat für viele Überlegungen betreffend Zerfällungskörper und Automorphismen bildet.

Lemma 9.2.3.1. *Sei $K \leq E$ eine Körpererweiterung, wobei E der Zerfällungskörper einer Menge $S \subseteq K[x]$ über K sei. Seien weiters $u, v \in E$ und sei $f \in K[x]$ ein irreduzibles Polynom mit $f(u) = f(v) = 0$. Dann gibt es einen Automorphismus $\sigma \in \mathrm{Aut}_K(E)$ mit $\sigma(u) = v$.*
Insbesondere gilt diese Aussage für $E = \overline{K}$, den algebraischen Abschluss von K.

Beweis. Da f irreduzibel ist, ist es das Minimalpolynom von u und v über K. Nach Satz 6.1.3.4 gibt es einen (eindeutigen) Isomorphismus $\varphi : K(u) \to K(v)$ mit $\varphi(c) = c$ für alle $c \in K$ und $\varphi(u) = v$. Ist $\varphi_x : K(u)[x] \to K(v)[x]$ der (eindeutige) Isomorphismus, der φ fortsetzt und $x \in K(u)[x]$ auf $x \in K(v)[x]$ abbildet, so gilt $\varphi_x(S) = S$. Wenden wir Satz 6.2.3.1 auf $K_1 = K(u)$, $K_2 = K(v)$, $P_1 = S = P_2$ und $Z_1 = E = Z_2$ an, so erhalten wir einen Automorphismus σ von E, der φ fortsetzt. Also gilt $\sigma \in \mathrm{Aut}_K(E)$ und $\sigma(u) = v$.
Für die zweite Aussage ist nur zu bemerken, dass $\overline{K}$ als Zerfällungskörper über K auftritt, nämlich von $S = K[x]$. □

Genauere Beschreibungen normaler Erweiterungen ergeben sich aus der folgenden Äquivalenz.

Satz 9.2.3.2. *Sei $K \leq E$ eine algebraische Körpererweiterung. Dann sind äquivalent:*

(i) *$K \leq E$ ist normal.*

(ii) *E ist Zerfällungskörper einer Menge $S \subseteq K[x]$ von Polynomen über K.*

(iii) *Bezeichne $\overline{K}$ einen algebraischen Abschluss von K mit $K \leq E \leq \overline{K}$ (oder äquivalent: einen algebraischen Abschluss von E) und sei $\sigma\colon E \to \overline{K}$ irgendeine isomorphe Einbettung von E in $\overline{K}$, die K punktweise fest lässt. Dann ist $\mathrm{Im}\,\sigma = E$, d.h. $\sigma \in \mathrm{Aut}_K(E)$.*

Beweis. (i) ⇒ (ii): Sei S die Menge aller irreduziblen Polynome über K, die in E wenigstens eine Nullstelle haben. Wir behaupten, dass E ein Zerfällungskörper von S über K ist. Weil E nach Voraussetzung (i) normal über K ist, enthält E sogar die Menge N sämtlicher Nullstellen von Polynomen aus $f \in S$. Der von K und N erzeugte Unterkörper $Z \leq E$ ist also ein Zerfällungskörper von S über K. Zu zeigen bleibt die umgekehrte Inklusion $E \leq Z$. Sei dazu $u \in E$ beliebig. Weil E laut Generalvoraussetzung algebraisch über K ist, gibt es ein Minimalpolynom $f \in K[x]$ von u. Wegen $f(u) = 0$ und weil f als Minimalpolynom irreduzibel ist, liegt f in S. Somit liegt u auch im Zerfällungskörper Z von S.

(ii) ⇒ (iii): Sei E Zerfällungskörper einer Menge $S \subseteq K[x]$, wobei wir oBdA alle $f \in S$ als irreduzibel voraussetzen dürfen. (Andernfalls ersetzen wir reduzible f in S durch ihre

irreduziblen Faktoren.) Zum Beweis von (iii) haben wir uns eine isomorphe Einbettung $\sigma\colon E \to \overline{K}$ mit $\sigma|_K = \mathrm{id}_K$ vorzugeben. Für den Nachweis von $\operatorname{Im}\sigma = E$ zeigen wir die beiden Mengeninklusionen.
$\operatorname{Im}\sigma \subseteq E$: Sei $u \in \operatorname{Im}\sigma$. Dann gibt es ein $v \in E$ mit $\sigma(v) = u$. Als Zerfällungskörper von S wird E von den Wurzeln aller $f \in S$ erzeugt. Es gibt also endlich viele $f_i \in S$ und $v_i \in E$ mit $f_i(v_i) = 0$, $i = 1, \ldots, n$, sodass $v \in K(v_1, \ldots, v_n)$. Somit existiert eine gebrochen rationale Funktion $g \in K(x_1, \ldots, x_n)$ über K in n Variablen mit $v = g(v_1, \ldots, v_n)$. Nach Proposition 9.2.1.4 sind auch die $\sigma(v_i)$ Wurzeln der $f_i \in S$, liegen also im Zerfällungskörper von S, der ja E ist, also $\sigma(v_i) \in E$. Daraus folgt schließlich

$$u = \sigma(v) = \sigma(g(v_1, \ldots, v_n)) \overset{(*)}{=} g(\sigma(v_1), \ldots, \sigma(v_n)) \in E,$$

wobei in der Gleichheit $\overset{(*)}{=}$ verwendet wurde, dass σ den Grundkörper K elementweise fest lässt.
$E \subseteq \operatorname{Im}\sigma$: Der Beweis verläuft ähnlich zu dem der ersten Inklusion. Sei $u \in E$, dann gibt es endlich viele $f_i \in S$ und $u_i \in E$ mit $f_i(u_i) = 0$, $i = 1, \ldots, n$, sodass $u \in K(u_1, \ldots, u_n)$, d.h. $u = g(u_1, \ldots, u_n)$ mit einer gebrochen rationalen Funktion $g \in K(x_1, \ldots, x_n)$. Weil E Zerfällungskörper von S ist, liegen alle Wurzeln der $f_i \in S$ in E, und der Automorphismus σ kann diese für jedes i nur untereinander permutieren. Das bedeutet, dass es $v_i \in E$ gibt mit $\sigma(v_i) = u_i$. Auch das Element $v := g(v_1, \ldots, v_n)$ liegt in E. Folglich ist

$$u = g(u_1, \ldots, u_n) = g(\sigma(v_1), \ldots, \sigma(v_n)) \overset{(*)}{=} \sigma(g(v_1, \ldots, v_n)) = \sigma(v) \in \operatorname{Im}\sigma.$$

(iii) $\Rightarrow$ (i): Sei $f \in K[x]$ irreduzibel, $f(u) = 0$ mit $u \in E$, und sei $v \in \overline{K}$ eine weitere Wurzel von f, d.h. $f(v) = 0$. Zu zeigen ist $v \in E$. Nach Lemma 9.2.3.1 angewandt auf $\overline{K}$ gibt es einen Automorphismus $\sigma \in \mathrm{Aut}_K(\overline{K})$ mit $\sigma(u) = v$. Die Einschränkung von σ auf E ist eine isomorphe Einbettung $\sigma|_E : E \to \overline{K}$, die K punktweise fest lässt. Nach Voraussetzung (iii) ist daher tatsächlich $v = \sigma(u) \in \operatorname{Im}\sigma|_E = E$. □

UE 107 ► Übungsaufgabe 9.2.3.3. (F) Zeigen Sie: Jede Körpererweiterung $K \leq E$ mit Erweiterungsgrad $[E : K] = 2$ ist normal. **◄ UE 107**

UE 108 ► Übungsaufgabe 9.2.3.4. (B) Zeigen Sie: **◄ UE 108**

(a) Normalität ist *nicht* transitiv, d.h. es gibt Körper $K \leq Z \leq E$ so, dass $K \leq Z$ und $Z \leq E$ normal sind, aber $K \leq E$ nicht normal ist.

(b) Es gibt eine Körpererweiterung $K \leq E$ mit $[E : K] = 3$, die nicht normal ist.

Hinweis: Man kann jeweils $K = \mathbb{Q}$ wählen.

Immer wieder hilfreich ist auch die Beobachtung, dass sich für eine Körpererweiterung $K \leq E$ die Eigenschaften normal und separabel auch auf $Z \leq E$ für Zwischenkörper Z übertragen. Hier halten wir das für Normalität fest:

Proposition 9.2.3.5. *Sei $K \leq E$ eine algebraische Körpererweiterung und Z ein Zwischenkörper, also $K \leq Z \leq E$. Ist $K \leq E$ normal, so auch $Z \leq E$.*

Beweis. Mit zweimaliger Hilfe von Satz 9.2.3.2 schließt man sehr schnell: Ist $K \leq E$ normal, so gibt es eine Menge $S \subseteq K[x] \subseteq Z[x]$, sodass E Zerfällungskörper von S über K ist. Dann ist E Zerfällungskörper von S auch über Z und somit normal über Z. □

Der Begriff der normalen Erweiterung legt den des normalen Abschluss nahe:

Definition 9.2.3.6. Seien $K \leq E \leq N$ Körpererweiterungen. N heißt *normaler Abschluss* von E über K, wenn N normal über K ist und minimal mit dieser Eigenschaft ist, d.h.: Für jede normale Erweiterung $E \leq N'$ mit $E \leq N' \leq N$ gilt $N' = N$.

Die folgenden Eigenschaften des normalen Abschluss sind mit Hilfe des Bisherigen, insbesondere mit Satz 9.2.3.2, leicht einzusehen:

Proposition 9.2.3.7. *Sei die Körpererweiterung $K \leq E$ algebraisch, $S \subseteq K[x] \subseteq E[x]$ die Menge aller irreduziblen Polynome über K, welche in E wenigstens eine Nullstelle haben und $N := Z_S$ ein Zerfällungskörper von S über E mit $K \leq E \leq N$. Dann gilt:*

(i) N ist ein normaler Abschluss von E über K.

(ii) Jeder normale Abschluss N' von E über K ist E-isomorph zu N.

(iii) Bezeichne $\overline{K}$ einen algebraischen Abschluss von K mit $K \leq E \leq \overline{K}$ (oder äquivalent: einen algebraischen Abschluss von E). Dann ist das Erzeugnis $\langle \bigcup_\sigma \sigma(E) \rangle$ in $\overline{K}$ ein normaler Abschluss, wobei σ alle isomorphen Einbettungen $E \to \overline{K}$ durchläuft, die K punktweise festlassen.

(iv) $[N : K]$ ist genau dann endlich, wenn $[E : K]$ endlich ist.

Insbesondere gibt es also stets einen normalen Abschluss.

UE 109 ▶ **Übungsaufgabe 9.2.3.8.** (V) Beweisen Sie Proposition 9.2.3.7. Hinweis: Verwenden Sie Satz 9.2.3.2. ◀ **UE 109**

9.2.4 Separable Erweiterungen

Wir erinnern an die Rolle der formalen Ableitung $f'(x) := \sum_{k=1}^{n} k a_k x^{k-1}$ eines Polynoms $f(x) = \sum_{k=0}^{n} a_k x^k$ im Zusammenhang mit der Mehrfachheit von Nullstellen aus Unterabschnitt 6.2.4:

Proposition 9.2.4.1. *Sei K ein Körper und $f \in K[x]$. Dann gilt:*

1. *Ist $K \leq E$ eine Körpererweiterung und $u \in E$, so ist u genau dann eine mehrfache Nullstelle von f, wenn $f(u) = f'(u) = 0$.*

2. *Ein Polynom $f \in K[x]$ ist genau dann separabel, wenn f und seine formale Ableitung f' teilerfremd sind.*

3. *Ist $f \in K[x]$ irreduzibel, so ist f genau dann separabel, wenn die Ableitung f' nicht das Nullpolynom ist.*

4. *Hat K die Charakteristik $\operatorname{char} K = 0$, so ist jedes irreduzible Polynom $f \in K[x]$ separabel.*

5. *Jede Körpererweiterung mit $\operatorname{char} K = \operatorname{char} E = 0$ ist separabel.*

6. *Hat K die Primzahlcharakteristik $\operatorname{char} K = p \in \mathbb{P}$, so ist f genau dann separabel, wenn es nicht von der Gestalt $f(x) = g(x^p)$ mit einem $g \in K[x]$ ist (also genau dann, wenn f mindestens einen Koeffizienten $a_k \neq 0$ mit einem nicht durch p teilbaren k hat).*

UE 110 ► **Übungsaufgabe 9.2.4.2.** (V) Beweisen Sie Proposition 9.2.4.1. Hinweis: Rekapitulieren Sie Unterabschnitt 6.2.4. ◄ **UE 110**

Proposition 9.2.4.3. *Sei $K \leq E$ eine algebraische Körpererweiterung und Z ein Zwischenkörper, also $K \leq Z \leq E$. Ist $K \leq E$ separabel, so auch $Z \leq E$.*

Beweis. Sei $K \leq E$ separabel und $u \in E$ beliebig. Weil $K \leq E$ algebraisch ist, gibt es ein Minimalpolynom f_K von u über K. Nach Voraussetzung ist f_K separabel. Das Minimalpolynom f_Z von u über Z ist im Polynomring $Z[x]$ ein Teiler von f_K, also ebenfalls separabel. Somit ist u auch separabel über Z. □

Als Nächstes wollen wir zeigen, dass Körpererweiterungen, in denen beide Körper endlich sind, separabel sind. Tatsächlich gilt noch mehr; es genügt nämlich, dass der Grundkörper endlich ist, wenn wir voraussetzen, dass die Erweiterung algebraisch ist.

Proposition 9.2.4.4. *Ist $K \leq E$ eine algebraische Körpererweiterung mit endlichem K, so ist die Erweiterung separabel.*

UE 111 ► **Übungsaufgabe 9.2.4.5.** (V) Beweisen Sie Proposition 9.2.4.4. Hinweis: Nehmen Sie zunächst an, dass E ebenfalls endlich und $K = \mathrm{GF}(p) = \mathbb{Z}_p$ der Primkörper ist, und rekapitulieren Sie Unterabschnitt 6.3.1. Betrachten Sie anschließend den Fall, dass $K = \mathrm{GF}(p) = \mathbb{Z}_p$ weiterhin der Primkörper ist und $E = \overline{\mathbb{Z}_p} = \mathrm{GF}(p^\infty)$ (siehe Unterabschnitt 6.3.5). ◄ **UE 111**

Nach den letzten Propositionen sind also algebraische Körpererweiterungen bei Charakteristik 0 stets separabel, genauso wie Erweiterungen, für die der Grundkörper endlich ist. Ist eine Körpererweiterung $K \leq E$ nicht separabel, so muss K also erstens unendlich sein und zweitens von Primzahlcharakteristik.

UE 112 ► **Übungsaufgabe 9.2.4.6.** (B) Finden Sie ein Beispiel einer algebraischen Körpererweiterung $K \leq E$, die nicht separabel ist. Geben Sie dazu ein Element von E an, dessen Minimalpolynom über K nicht separabel ist. Was ist die formale Ableitung dieses Minimalpolynoms?
Hinweis: Man kann $E = \mathbb{Z}_p(x)$ wählen (der Körper der gebrochen rationalen Funktionen über $\mathbb{Z}_p$ in einer Variablen). ◄ **UE 112**

9.2.5 Algebraisch, normal und separabel impliziert Galoissch

Nach diesen Vorarbeiten können wir die angekündigte Umkehrung beweisen:

Satz 9.2.5.1. *Sei $K \leq E$ algebraisch. Dann ist E genau dann Galoissch über K, wenn E separabel und normal über K ist.*

Beweis. Dass jede algebraische Galoissche Erweiterung normal und separabel ist, war Inhalt der Propositionen 9.2.2.3 bzw. 9.2.2.5 (beides unmittelbare Folgerungen aus Proposition 9.2.2.1).
Wir nehmen nun umgekehrt an, dass die algebraische Erweiterung $K \leq E$ sowohl separabel als auch normal ist. Um zu zeigen, dass sie Galoissch ist, müssen wir für ein beliebiges $u \in E \setminus K$ ein $\sigma \in \mathrm{Aut}_K(E)$ finden mit $\sigma(u) \neq u$. Weil E algebraisch über K ist, hat u ein Minimalpolynom $f \in K[x]$. Wegen $u \notin K$ hat f Grad ≥ 2. Weil E normal über K ist, enthält E einen Zerfällungskörper Z von f mit $K \leq Z \leq E$, insbesondere sämtliche Nullstellen von f. Weil $K \leq E$ separabel ist, sind diese Nullstellen paarweise verschieden. Es gibt also ein $v \in E \setminus K$, $v \neq u$, mit $f(v) = 0 = f(u)$. Nach Lemma 9.2.3.1 gibt es einen Automorphismus $\sigma \in \mathrm{Aut}_K(E)$ mit $\sigma(u) = v \neq u$, womit der Satz bewiesen ist. □

Für Körper der Charakteristik 0 erhalten wir die einfache Folgerung:

Folgerung 9.2.5.2. *Ist K ein Körper mit* $\mathrm{char}\, K = 0$*, so ist eine algebraische Erweiterung $K \leq E$ genau dann Galoissch, wenn sie normal ist.*

Beweis. Nach Satz 9.2.5.1 folgt normal aus Galoissch. Ist umgekehrt $K \leq E$ algebraisch und normal, so wegen $\mathrm{char}\, K = 0$ nach Proposition 9.2.4.1, Aussage 5, separabel, also nach Satz 9.2.5.1 auch Galoissch. □

UE 113 ► **Übungsaufgabe 9.2.5.3.** (F) Zeigen Sie, dass die Erweiterung $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ Galoissch ist und bestimmen Sie die Galoisgruppe $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3}))$. ◄ **UE 113**

Jeder endliche Körper $E = \mathrm{GF}(p^n)$, $p \in \mathbb{P}$, $n \in \mathbb{N}^+$, ist als Zerfällungskörper des Polynoms $f(x) = x^{p^n} - x$ über dem Primkörper $\mathrm{GF}(p)$ gemäß Satz 9.2.3.2 normal, somit nach Satz 9.2.3.5 auch über jedem Unterkörper $K \leq E$. Mit Proposition 9.2.4.4 schließen wir auf die Separabilität der Erweiterung $K \leq E$. Also folgt aus Satz 9.2.5.1:

Satz 9.2.5.4. *Ist $K \leq E$ eine Körpererweiterung mit endlichem E, so ist die Erweiterung Galoissch.*

Folgende Frage (die für sich genommen nichts mit Galoisschen Erweiterungen zu tun hat) ist noch offen: Erzeugt die Adjunktion separabler Elemente auch separable Körpererweiterungen? Die Antwort lautet „ja“. Das wird sich als Folgerung 9.2.5.6 aus der folgenden für sich sehr interessanten Charakterisierung Galoisscher Erweiterungen ergeben, die als Pendant des entsprechenden Satzes 9.2.3.2 über normale Erweiterungen aufgefasst werden kann:

Satz 9.2.5.5. *Eine algebraische Körpererweiterung $K \leq E$ ist Galoissch genau dann, wenn E der Zerfällungskörper einer Menge $S \subseteq K[x]$ separabler Polynome ist.*

Beweis. Ist die algebraische Erweiterung $K \leq E$ Galoissch, so nach Satz 9.2.5.1 normal, woraus nach Satz 9.2.3.2 folgt, dass E Zerfällungskörper einer Menge $S_0 \subseteq K[x]$ von Polynomen über K ist. Sei S die Menge aller irreduziblen Faktoren von Polynomen aus S_0. Dann ist E auch Zerfällungskörper von S. Nochmals wegen Satz 9.2.5.1 ist $K \leq E$ als algebraische und Galoissche Erweiterung auch separabel, was nur möglich ist, wenn alle $f \in S$ separabel sind.

Sei nun umgekehrt vorausgesetzt, dass E Zerfällungskörper einer Menge S separabler Polynome ist, die wir oBdA als irreduzibel (Argument wie im ersten Teil des Beweises; man beachte, dass die irreduziblen Faktoren separabler Polynome ebenfalls separabel sind), normiert und vom Grad ≥ 2 annehmen dürfen. Der Beweis des Satzes ist erbracht, wenn wir für ein beliebiges $u \in E \setminus K$ ein $\sigma \in \mathrm{Aut}_K(E)$ mit $\sigma(u) \neq u$ konstruieren können. Zunächst gehen wir ähnlich vor wie an der entsprechenden Stelle im Beweis von Satz 9.2.3.2: Als Zerfällungskörper wird E von den Wurzeln sämtlicher $f \in S$ erzeugt, wobei für jedes Element von E nur endlich viele nötig sind. Sei $I(n)$, $n \in \mathbb{N}$, die folgende Aussage:

> Für alle $u \in E \setminus K$, für die es $v_1, \ldots, v_n \in E$ und $f_1, \ldots, f_n \in S$ gibt mit $u \in K(u_1, \ldots, u_n)$ und $f_i(v_i) = 0$, existiert ein $\sigma \in \mathrm{Aut}_K(E)$ mit $\sigma(u) \neq u$.

Wir zeigen mit Induktion, dass $I(n)$ für alle $n \in \mathbb{N}$ wahr ist – nach den bisherigen Überlegungen ist damit der Beweis erbracht.
Für $n = 0$ wäre $u \in K$, Widerspruch. In diesem Fall ist also nichts zu zeigen.
Sei $n = 1$, also $u \in K(v)$ mit $v = v_1$ und $f \in S$ das Minimalpolynom von v. Weil E Zerfällungskörper von S ist und $f \in S$ separabel ist, zerfällt f über E in paarweise verschiedene Linearfaktoren

$$f(x) = \prod_{j=1}^{m} (x - \alpha_j),$$

$\alpha_j \in E$, $\alpha_1 = v$, wobei $m \geq 2$ der Grad von f ist. Nach Aussage (4) in Satz 6.1.3.4 ist jedes Element aus $K(v)$ darstellbar als Polynom in v mit Koeffizienten aus K und einem Grad $< m$. Speziell sei

$$u = p_u(v) \quad \text{mit} \quad p_u(x) = \sum_{j=0}^{m-1} b_j x^j, \quad b_j \in K.$$

Wieder wie im Beweis von Satz 9.2.5.1 schließen wir mittels Lemma 9.2.3.1: Für jedes $j = 1, \ldots, m$ gibt es ein $\sigma_j \in \mathrm{Aut}_K(E)$ mit $\sigma_j(v) = \alpha_j$. Wir wollen zeigen, dass wenigstens eines der σ_j das Element u nicht auf sich selbst abbildet. Wir gehen indirekt vor, indem wir $\sigma_j(u) = u$ für alle $j = 1, \ldots, m$ annehmen. Wir betrachten das Polynom $g(x) := p_u(x) - u \in E[x]$. Wegen $p_u \in K[x]$ und $u \notin K$ ist g nicht das Nullpolynom und hat einen Grad $< m$. Für $j = 1, \ldots, m$ gilt

$$g(\alpha_j) = p_u(\alpha_j) - u = p_u(\sigma_j(v)) - u = \sigma_j(p_u(v)) - u = \sigma_j(u) - u = u - u = 0.$$

Also hat das Polynom $g \neq 0$ mehr Nullstellen als sein Grad beträgt, Widerspruch. Folglich gibt es ein $\sigma \in \mathrm{Aut}_K(E)$ mit $\sigma(u) \neq u$.
Induktionsschritt von n auf $n+1$: Sei $u \in K(v_1, \ldots, v_{n+1}) \setminus K$ für Nullstellen v_i von Polynomen $f_i \in S$. Wir haben $\sigma \in \mathrm{Aut}_K(E)$ zu finden mit $\sigma(u) \neq u$. Dazu unterscheiden wir zwei Fälle: Wenn $u \in K(v_1, \ldots, v_n)$, dann liefert die Induktionsvoraussetzung $I(n)$ den gesuchten Automorphismus σ. Wenn andererseits $u \notin K(v_1, \ldots, v_n) =: K_0$, dann bemerken wir, dass $u \in K_0(v_{n+1})$ und dass E auch der Zerfällungskörper über K_0 von S (oder von den in $K_0[x]$ irreduziblen Faktoren der Polynome in S) ist. Somit liefert der oben abgehandelte Fall $n = 1$ einen Automorphismus $\sigma \in \mathrm{Aut}_{K_0}(E) \subseteq \mathrm{Aut}_K(E)$ mit $\sigma(u) \neq u$. □

Hieraus schließen wir:

Folgerung 9.2.5.6. *Sei $K \leq E$ eine Körpererweiterung, und enthalte $T \subseteq E$ ausschließlich über K separable Elemente. Dann ist auch die von T erzeugte Erweiterung $K(T)$ von K separabel über K.*

Beweis. Jedes $t \in T$ ist separabel über K, folglich algebraisch und hat deshalb ein separables Minimalpolynom $f_t \in K[x]$. Wir erweitern E zu einem algebraischen Abschluss $\overline{E}$. Dieser enthält einen Zerfällungskörper Z der Menge S aller f_t, $t \in T$. Es gilt $K \leq K(T) \leq Z$. Nach Satz 9.2.5.5 ist Z Galoissch, insbesondere separabel, und damit erst recht $K(T)$ separabel über K. □

Durch Kombination der Propositionen 9.2.3.5 und 9.2.4.3 über Normalität und Separabilität erhalten wir die entsprechende Aussage für Galoissche Erweiterungen:

Proposition 9.2.5.7. *Sei $K \leq E$ eine algebraische Körpererweiterung und Z ein Zwischenkörper, also $K \leq Z \leq E$. Ist $K \leq E$ Galoissch, so ist auch $Z \leq E$ Galoissch.*

Beweis. Ist $K \leq E$ Galoissch, so nach Satz 9.2.5.1 sowohl separabel als auch normal. Daher ist nach Proposition 9.2.4.3 auch $Z \leq E$ separabel, nach Proposition 9.2.3.5 normal, wieder nach Satz 9.2.5.1 also Galoissch. □

Zum Abschluss dieses Abschnitts erweitern wir den Satz vom primitiven Element aus Algebra I.

UE 114 ► **Übungsaufgabe 9.2.5.8.** (F+) Rekapitulieren Sie den Beweis des Satzes vom primitiven Element 6.2.6.1 und zeigen Sie den Satz für beliebige Charakteristik, jedoch unter der Voraussetzung, dass die Erweiterung separabel ist: Jede endlichdimensionale und separable Körpererweiterung $K \leq E$ ist einfach, d.h. es gibt ein $u \in E$ mit $E = K(u)$. ◄ **UE 114**

9.3 Der Hauptsatz der Galoistheorie

Der Hauptsatz der Galoistheorie besagt im Fall endlichdimensionaler Galoisscher Körpererweiterungen, dass die Galois-abgeschlossenen Elemente genau die Untergruppen bzw. die Zwischenkörper sind. Darüber hinaus macht er noch interessante Aussagen über Dimension und Index sowie darüber, welche Untergruppen sogar Normalteiler sind. Die genaue Formulierung ist Gegenstand von 9.3.1. Die wichtigste technische Hürde wird mit dem Beweis zweier Ungleichungen über Dimension und Index in 9.3.2 genommen. Zusammen mit einigen weiteren Überlegungen über stabile Zwischenkörper gelingt damit in 9.3.3 der Beweis des Hauptsatzes für den endlichdimensionalen Fall. Verzichtet man auf Endlichdimensionalität, so sind bei Galoisschen Erweiterungen zwar weiterhin alle Zwischenkörper Galois-abgeschlossen, jedoch nicht mehr alle Untergruppen, sondern nur mehr jene, die abgeschlossen bezüglich einer natürlich auftretenden Topologie sind. Das ist Gegenstand von 9.3.4. Zwei interessante Folgerungen aus dem Hauptsatz, nämlich die Charakterisierung der Galoisgruppe von $\mathrm{GF}(p^\infty)$ über $\mathrm{GF}(p^m)$ sowie ein galoistheoretischer Beweis des Fundamentalsatzes der Algebra, bilden in 9.3.5 den Abschluss von Abschnitt 9.3.

9.3.1 Formulierung des Hauptsatzes für endlichdimensionale Erweiterungen

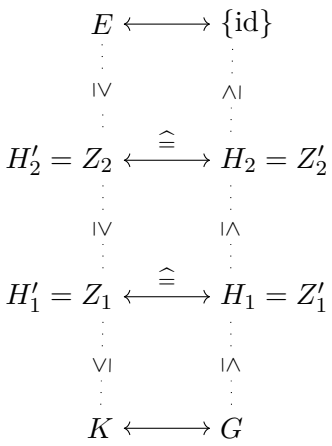
Die wichtigste Aussage des Hauptsatzes der Galoistheorie besteht in der Beschreibung der Galois-abgeschlossenen Elemente auf beiden Seiten der klassischen Galoiskorrespondenz. Sei dazu $K \leq E$ eine Körpererweiterung. Bei den in Definition 9.2.1.1 auftretenden Teilmengen $H' \subseteq E$ handelt es sich stets um Zwischenkörper, bei den $Z' \subseteq G$ um Untergruppen von $\mathrm{Aut}_K(E)$ (siehe Proposition 9.2.1.2, Aussage 5 bzw. 4).

Die naheliegende Frage lautet, ob *alle* $H \leq \mathrm{Aut}_K(E)$ bzw. *alle* Zwischenkörper Z Galois-abgeschlossen sind, d.h. ob sie $H'' = H$ und $Z'' = Z$ erfüllen.

Eine trivialerweise notwendige Bedingung dafür ist die Galois-Abgeschlossenheit wenigstens von K selbst. Nach Definition 9.2.1.1 ist das gerade die definierende Bedingung dafür, dass man die Erweiterung $K \leq E$ Galoissch nennt.

Das wichtigste Ziel dieses Abschnitts ist der Beweis des Hauptsatzes der Galoistheorie. Für endlichdimensionale Erweiterungen besagt er, dass in diesem Fall die notwendige Bedingung auch hinreichend ist: In der Galoiskorrespondenz für eine endlichdimensionale und Galoissche Erweiterung sind alle Untergruppen und alle Zwischenkörper Galois-abgeschlossen. Darüber hinaus charakterisiert der Hauptsatz unter den Untergruppen die Normalteiler dadurch, dass sie selbst Galoisschen Erweiterungen des Grundkörpers entsprechen.

Zur Illustration für eine Situation mit $K \leq Z_1 \leq Z_2 \leq E$ (im allgemeinen Fall muss die Halbordnung der Zwischenkörper keine Kette bilden, immerhin aber einen Verband):



Die qualitativen Aussagen des Hauptsatzes über die Galois-abgeschlossenen Elemente folgen aus quantitativen, nämlich aus den Identitäten zwischen einander entsprechenden Erweiterungsgraden und Gruppenindizes. In seiner ganzen Pracht lautet der Hauptsatz für endlichdimensionale Erweiterungen wie folgt.

Satz 9.3.1.1 (Hauptsatz der Galoistheorie für endlichdimensionale Erweiterungen)**.** *Sei $K \leq E$ eine endlichdimensionale Galoissche Körpererweiterung und $G := \mathrm{Aut}_K(E)$ die Galoisgruppe von E über K. Sei weiters*

$$\mathcal{Z} = \mathcal{Z}(K \leq E) := \{Z \mid \ K \leq Z \leq E\}$$

die Menge aller Zwischenkörper von K und E sowie

$$\mathrm{Sub}(G) := \{H \mid \ H \leq G\}$$

die Menge aller Untergruppen von G. Dann gilt:

(a) Die Galois-abgeschlossenen Teilmengen von E sind genau die Zwischenkörper $Z \in \mathcal{Z}$. Die Galois-abgeschlossenen Teilmengen von G sind genau die Untergruppen $H \in \mathrm{Sub}(G)$. Insbesondere sind $Z \mapsto Z'$ und $H \mapsto H'$ zueinander inverse antitone Bijektionen zwischen $\mathcal{Z}$ und $\mathrm{Sub}(G)$. Es gilt daher die Isomorphie

$$(\mathcal{Z}, \subseteq) \cong (\mathrm{Sub}(G), \supseteq)$$

von Halbordnungen.

(b) Ist $Z_1 \leq Z_2 \in \mathcal{Z}$, dann gilt

$$\underbrace{[Z_2 : Z_1]}_{Grad} = \underbrace{[Z_1' : Z_2']}_{Index}.$$

Ist $H_1 \leq H_2 \leq G$, dann gilt

$$\underbrace{[H_2 : H_1]}_{Index} = \underbrace{[H_1' : H_2']}_{Grad}.$$

(c) Für jedes $Z \in \mathcal{Z}$ ist $Z \leq E$ eine Galoissche Erweiterung.

(d) Für $Z \in \mathcal{Z}$ ist $K \leq Z$ genau dann eine Galoissche Erweiterung, wenn Z' ein Normalteiler von G ist. In diesem Fall ist $G/Z' \cong \mathrm{Aut}_K(Z)$, wobei die Einschränkungsabbildung $\varphi : \sigma \mapsto \sigma|_Z$ ein surjektiver Homomorphismus $\varphi : \mathrm{Aut}_K(E) \to \mathrm{Aut}_K(Z)$ mit $\ker \varphi = \mathrm{Aut}_Z(E) = Z'$ ist. Folglich gilt dann $\mathrm{Aut}_K(Z) \cong \mathrm{Aut}_K(E)/\mathrm{Aut}_Z(E)$.

In Hinblick auf Aussage (b) des Hauptsatzes 9.3.1.1 erweist sich die Arbeit mit Erweiterungsgraden und Gruppenindizes als zielführend. Zwei Ungleichungen in Verbindung miteinander ermöglichen den entscheidenden Durchbruch.

9.3.2 Zwei Ungleichungen

Der technisch wesentliche Schritt im Beweis des Hauptsatzes der Galoistheorie besteht darin, die Dimension von Körpererweiterungen mit dem Index von Untergruppen in Beziehung zu setzen. Das ist in zwei Richtungen möglich, was sich in zwei Ungleichungen zwischen diesen beiden Größen manifestiert, die für beliebige Körpererweiterungen (Galoissch oder auch nicht) gelten. Aus beiden Ungleichungen gemeinsam folgen dann sehr rasch die ersten beiden Aussagen des Hauptsatzes. Zunächst zur Abschätzung von Erweiterungsdimension durch Gruppenindex:

Lemma 9.3.2.1. *Seien $K \leq Z_1 \leq Z_2 \leq E$ Körper und $[Z_2 : Z_1] < \infty$. Dann gilt*

$$[Z_1' : Z_2'] \leq [Z_2 : Z_1].$$

Ist $K \leq E$ eine endlichdimensionale Erweiterung, so gilt $|\mathrm{Aut}_K(E)| \leq [E : K]$.

Beweis. Der Beweis erfolgt durch Induktion nach $n := [Z_2 : Z_1]$. Der Fall $n = 1$ ist trivial. Sei also $n > 1$ und gelte als Induktionsvoraussetzung (IV) die Behauptung für alle $i < n$. Sei $u \in Z_2 \setminus Z_1$ mit Minimalpolynom $f \in Z_1[x]$ vom Grad $k > 1$. Dann ist nach dem Gradsatz

$$[Z_1(u) : Z_1] = k \text{ und } [Z_2 : Z_1(u)] = \frac{n}{k}.$$

Ist $k < n$, so folgt nach dem Indexsatz (Satz 3.2.1.9)

$$[Z_1' : Z_2'] = [Z_1' : Z_1(u)'] \cdot [Z_1(u)' : Z_2'] \overset{\text{IV}}{\leq} [Z_1(u) : Z_1] \cdot [Z_2 : Z_1(u)] = k \cdot \frac{n}{k} = n = [Z_2 : Z_1].$$

Im Fall $k = n$ ist $Z_1(u) = Z_2$. Wir konstruieren eine injektive Funktion $\varphi : S \to T$ von der Menge S aller Linksnebenklassen von Z_2' in Z_1' in die Menge T aller (verschiedenen) Wurzeln von f in E wie folgt:

$$\varphi : \tau Z_2' \mapsto \tau(u)$$

Wegen $\tau\sigma(u) = \tau(u)$ für alle $\sigma \in Z_2'$ hängt $\tau(u)$ nicht vom speziellen Repräsentanten τ der Linksnebenklasse $\tau Z_2'$ ab. Also ist φ wohldefiniert. Wegen

$$\begin{aligned} \tau_1(u) = \tau_2(u) &\Rightarrow \tau_2^{-1}\tau_1(u) = u \\ &\Rightarrow \tau_2^{-1}\tau_1 \in Z_1(u)' = Z_2' \\ &\Rightarrow \tau_1 Z_2' = \tau_2 Z_2' \end{aligned}$$

ist φ auch injektiv, und es folgt $[Z_1' : Z_2'] = |S| \leq |T| \leq n = [Z_2 : Z_1]$.

Für den Beweis der letzten Aussage des Lemmas ist lediglich speziell $Z_1 := K$ und $Z_2 := E$ zu setzen. Ist nämlich $K \leq E$ endlichdimensional, so ist die Voraussetzung $[Z_2 : Z_1] = [E : K] < \infty$ erfüllt. Somit liefert das bisher Bewiesene die Behauptung

$$|\operatorname{Aut}_K(E)| = [K' : E'] = [Z_1' : Z_2'] \leq [Z_2 : Z_1] = [E : K].$$

□

Und nun eine analoge Ungleichung in die umgekehrte Richtung:

Lemma 9.3.2.2. *Für die Körpererweiterung $K \leq E$ seien $H_1 \leq H_2 \leq \operatorname{Aut}_K(E)$ Untergruppen mit endlichem Index $[H_2 : H_1] < \infty$. Dann gilt*

$$[H_1' : H_2'] \leq [H_2 : H_1].$$

Ist die Erweiterung Galoissch und $\operatorname{Aut}_K(E)$ endlich, so gilt $[E : K] \leq |\operatorname{Aut}_K(E)|$.

Beweis. Sei indirekt $[H_1' : H_2'] > [H_2 : H_1] =: n$. Dann existieren $u_1, \ldots, u_{n+1} \in H_1'$, die linear unabhängig über H_2' sind. Sei $\{\tau_1, \ldots, \tau_n\}$ ein vollständiges Vertretersystem für die Linksnebenklassen von H_1 in H_2, von denen es definitionsgemäß $[H_2 : H_1] = n$ Stück gibt. Das homogene System

$$\sum_{j=1}^{n+1} \tau_i(u_j) x_j = 0,\ i = 1, \ldots, n \tag{9.1}$$

aus n linearen Gleichungen mit den Koeffizienten $\tau_i(u_j) \in E$ in $n+1$ Unbekannten hat nichttriviale Lösungen. Sei $a = (a_1, \ldots, a_{n+1}) \in E^{n+1}$ eine solche und oBdA (d.h. nach eventueller Permutation der j)

$$a_1 = 1,\ a_2 \neq 0,\ a_3 \neq 0, \ldots, a_r \neq 0, a_{r+1} = 0, \ldots, a_{n+1} = 0$$

mit minimalem r. Wir werden ein $\sigma \in H_2$ konstruieren mit $\sigma(a_2) \neq a_2$, für welches $b := (b_1, \ldots, b_{n+1})$ mit $b_j := \sigma(a_j)$ ebenfalls Lösung von (9.1) ist. Das liefert eine weitere nichttriviale Lösung $c = (c_1, \ldots, c_{n+1}) := a - b$, $c_j := a_j - b_j$, mit

$$c_1 = 0,\ c_2 \neq 0,\ c_{r+1} = 0, \ldots, c_{n+1} = 0,$$

was einen Widerspruch zur Minimalität von r ergibt.
Zur Konstruktion von σ:
Sei oBdA $\tau_1 \in H_1$, also $\tau_1(u_j) = u_j$ für $j = 1, \ldots, n+1$. Setzt man die Lösung $a = (a_1, \ldots, a_{n+1})$ im System (9.1) in die Gleichung für $i = 1$ ein, erhält man

$$u_1 a_1 + \ldots + u_{n+1} a_{n+1} = 0.$$

Da die u_j linear unabhängig über H_2' sind, muss es ein i geben mit $a_i \notin H_2'$. Sei oBdA $i = 2$. Daher existiert ein $\sigma \in H_2$ mit $\sigma(a_2) \neq a_2$. Wenden wir nun σ auf (9.1) an, erhalten wir das System

$$\sum_{j=1}^{n+1} \sigma\tau_i(u_j)x_j = 0,\ i = 1, \ldots, n, \tag{9.2}$$

das klarerweise von $b_j := \sigma(a_j),\ j = 1, \ldots, n+1$ gelöst wird. Weil $\sigma \in H_2$ die Nebenklassen von H_1 permutiert, folgt

$$\{\sigma\tau_1 H_1, \ldots, \sigma\tau_n H_1\} = \{\tau_1 H_1, \ldots, \tau_n H_1\}$$

und wegen der Implikationskette

$$\rho_1 H_1 = \rho_2 H_1 \Rightarrow \rho_2^{-1}\rho_1 \in H_1 \overset{u_j \in H_1'}{\Rightarrow} \rho_2^{-1}\rho_1(u_j) = u_j \Rightarrow \rho_1(u_j) = \rho_2(u_j)$$

sind die beiden Systeme (9.1) und (9.2) bis auf die Reihenfolge der Gleichungen identisch. Daher bilden die b_j auch eine Lösung für (9.1) und σ erfüllt das Gewünschte.

Für die letzte Aussage ist speziell $H_1 := \{\mathrm{id}_E\}$ und $H_2 := \mathrm{Aut}_K(E)$ zu setzen. Für eine Galoissche Erweiterung gilt dann $H_2' = \mathrm{Aut}_K(E)' = K$, außerdem in jedem Fall $H_1' = E$. Ist die Galoisgruppe $\mathrm{Aut}_K(E)$ endlich, so liefert das bisher Bewiesene daher die Behauptung

$$[E : K] = [H_1' : H_2'] \leq [H_2 : H_1] = [\mathrm{Aut}_K(E) : \{\mathrm{id}_E\}] = |\,\mathrm{Aut}_K(E)|. \quad \square$$

9.3.3 Beweis des Hauptsatzes für endlichdimensionale Erweiterungen

Wir wollen nun die Voraussetzungen des Hauptsatzes 9.3.1.1 annehmen und die dortigen Bezeichnungen verwenden. Dann folgt, wie wir gleich sehen werden, die Behauptung (b) und damit auch (a) durch geschicktes Zusammensetzen der beiden Ungleichungen aus Lemma 9.3.2.1 und Lemma 9.3.2.2.
Zunächst ergibt sich für eine Galois-abgeschlossene Untergruppe $H_1 = H_1'' \leq G$ und $[H_2 : H_1] < \infty$ sofort

$$[H_2 : H_1] \leq [H_2'' : H_1] = [H_2'' : H_1''] \overset{9.3.2.1}{\leq} [H_1' : H_2'] \overset{9.3.2.2}{\leq} [H_2 : H_1].$$

Wegen $[H_2 : H_1] < \infty$ lassen sich die Ungleichungen zu Gleichungen zwischen Mengen verschärfen. Insbesondere folgt $H_2'' = H_2$, also ist mit H_1 auch H_2 Galois-abgeschlossen. Speziell ist $H_1 = \{\mathrm{id}\}$ aus trivialen Gründen Galois-abgeschlossen, folglich sind alle $H_2 \leq G$ Galois-abgeschlossen, außerdem $[H_2 : H_1] = [H_1' : H_2']$.
Analog schließt man für einen Galois-abgeschlossenen Zwischenkörper Z_1 mit $Z_1 \leq Z_2 \leq E$ auf die Galois-Abgeschlossenheit von Z_2 und auf $[Z_2 : Z_1] = [Z_1' : Z_2']$. Für eine Galoissche Erweiterung $K \leq E$ ist neben $H_1 = \{\mathrm{id}\}$ auch $Z_1 = K$ Galois-abgeschlossen, also tatsächlich sogar alle Zwischenkörper $Z \geq Z_1 = K$ und alle $H = H_2 \leq G$. Zusammen

mit dem allgemeinen Satz 9.1.3.3 über allgemeine Galoiskorrespondenzen sind damit die Aussagen (a) und (b) aus dem Hauptsatz 9.3.1.1 bewiesen.
Aussage (c) ist genau der Inhalt von Proposition 9.2.5.7.
Zu beweisen bleibt noch Aussage (d) im Hauptsatz, wonach für einen Zwischenkörper Z einer Galoisschen Erweiterung $K \leq E$ die Erweiterung $K \leq Z$ genau dann Galoissch ist, wenn $Z' = \mathrm{Aut}_Z(E)$ ein Normalteiler der Galoisgruppe $\mathrm{Aut}_K(E)$ ist. Außerdem wird behauptet, dass in diesem Fall die Einschränkung $\varphi : \mathrm{Aut}_K(E) \to \mathrm{Aut}_K(Z), \sigma \mapsto \sigma|_Z$ ein surjektiver Homomorphismus ist. Ist letzteres der Fall, so ist offenbar $\ker \varphi = \mathrm{Aut}_Z(E)$, und es folgt die Normalteilereigenschaft. Damit die Einschränkung wohldefiniert ist, müssen alle $\sigma \in \mathrm{Aut}_K(E)$ den Zwischenkörper Z zwar nicht punktweise aber als Menge invariant lassen. Diese Eigenschaft wollen wir nun näher untersuchen.

Definition 9.3.3.1. Sei $K \leq E$ eine Körpererweiterung. Ein Zwischenkörper Z, $K \leq Z \leq E$, heißt *stabil* bezüglich K und E, wenn $\sigma(Z) \subseteq Z$ für alle $\sigma \in \mathrm{Aut}_K(E)$ gilt.

Die Nützlichkeit dieses Begriffs wird an den folgenden Aussagen deutlich:

Lemma 9.3.3.2. *Für eine Körpererweiterung $K \leq E$ und einen Zwischenkörper Z, $K \leq Z \leq E$, gilt:*

(i) Ist Z stabil bzgl. K und E, so ist

$$\varphi : \mathrm{Aut}_K(E) \to \mathrm{Aut}_K(Z)$$
$$\varphi : \sigma \mapsto \sigma|_Z$$

wohldefiniert und ein Gruppenhomomorphismus mit $\ker \varphi = Z' \lhd \mathrm{Aut}_K(E)$. Ist zusätzlich $K \leq E$ Galoissch, so ist auch $K \leq Z$ Galoissch.

(ii) Ist $H \lhd \mathrm{Aut}_K(E)$, so ist H' stabil bzgl. K und E.

(iii) Ist $K \leq Z$ algebraisch und Galoissch, so ist Z stabil bzgl. K und E. Der Homomorphismus φ aus Aussage (i) ist in diesem Fall surjektiv.

Beweis. (i): Wohldefiniertheit: Bei der Einschränkung von σ von E auf Z bleiben Injektivität und Homomorphiebedingung von σ erhalten. Für die Wohldefiniertheit von φ haben wir $\sigma(Z) = Z$ zu zeigen. Dann ist nämlich $\varphi(\sigma) = \sigma|_Z$ bijektiv auf Z, folglich ein Element von $\mathrm{Aut}_K(Z)$. Tatsächlich, die Stabilität von Z zeigt, angewandt auf $\sigma \in \mathrm{Aut}_K(E)$, die Inklusion $\sigma(Z) \subseteq Z$ und, angewandt auf den inversen Automorphismus $\sigma^{-1} \in \mathrm{Aut}_K(E)$, auch $\sigma^{-1}(Z) \subseteq Z$. Somit ist auch $Z = \sigma(\sigma^{-1}(Z)) \subseteq \sigma(Z)$, insgesamt also $\sigma(Z) = Z$ bewiesen.
Homomorphieeigenschaft und Kern: Klarerweise gilt die Homomorphiebedingung

$$\varphi(\sigma\tau) = (\sigma\tau)|_Z = \sigma|_Z \ \tau|_Z = \varphi(\sigma)\varphi(\tau),$$

also ist φ ein Gruppenhomomorphismus. Der Kern von φ besteht offenbar genau aus jenen $\sigma \in \mathrm{Aut}_K(E)$, die Z punktweise fest lassen, stimmt folglich mit Z' überein.
Ist $K \leq E$ Galoissch, so auch $K \leq Z$: Unter der Voraussetzung, dass $K \leq E$ Galoissch ist, müssen wir für ein beliebiges $u \in Z \setminus K$ ein $\sigma_Z \in \mathrm{Aut}_K(Z)$ mit $\sigma(u) \neq u$ finden. Laut

Voraussetzung gibt es ein $\sigma \in \mathrm{Aut}_K(E)$ mit dieser Eigenschaft. Wegen der Stabilität von Z und dem Bisherigen ist $\sigma_Z := \sigma|_Z \in \mathrm{Aut}_K(Z)$ und hat die gewünschte Eigenschaft.

(ii): Sei $H \lhd \mathrm{Aut}_K(E)$, $\sigma \in \mathrm{Aut}_K(E)$ und $u \in H'$. Zun zeigen ist dann $\sigma(u) \in H'$, d.h. $\tau(\sigma(u)) = \sigma(u)$ für alle $\tau \in H$. Wegen $H \lhd \mathrm{Aut}_K(E)$ ist $\sigma^{-1}\tau\sigma \in \sigma^{-1}H\sigma \subseteq H$, wegen $u \in H'$ also $\sigma^{-1}\tau\sigma(u) = u$, d.h. tatsächlich $\tau\sigma(u) = \sigma(u)$.

(iii): Stabilität von Z: Sei $u \in Z$. Nach Proposition 9.2.2.1 zerfällt das Minimalpolynom $f(x) = \prod_{i=1}^{r}(x - u_i)$ von $u = u_1$ über K in Linearfaktoren mit paarweise verschiedenen $u_i \in Z$. Ist nun $\sigma \in \mathrm{Aut}_K(E)$, dann ist $\sigma(u)$ eine Wurzel von f, also $\sigma(u) = u_i$ für ein i und somit $\sigma(u) \in Z$.
Surjektivität von φ: Mit $K \leq E$ ist nach Proposition 9.2.5.7 auch $Z \leq E$ Galoissch, nach Proposition 9.2.2.3 also normal. Somit ist E Zerfällungskörper über Z (siehe Satz 9.2.3.2), und jeder Isomorphismus $Z \to Z$ lässt sich nach Satz 6.2.3.1 zu einem Isomorphismus $E \to E$ fortsetzen. Das bedeutet insbesondere: Jedes Element aus $\mathrm{Aut}_K(Z)$ tritt als Bild $\varphi(\sigma)$ eines $\sigma \in \mathrm{Aut}_K(E)$ unter φ auf. □

Lemma 9.3.3.2 enthält offenbar auch Aussage (d) im Hauptsatz 9.3.1.1. Damit ist der Hauptsatz der Galoistheorie für den Fall einer endlichdimensionalen Körpererweiterung vollständig bewiesen.

9.3.4 Der allgemeine Hauptsatz

Ist die algebraische Erweiterung $K \leq E$ unendlichdimensional, so gilt der Hauptsatz nicht mehr in seiner ursprünglichen Form, sehr wohl jedoch in einer geeigneten Modifikation. Wieder treten alle Zwischenkörper als Galois-abgeschlossene Mengen auf, aber nicht alle Untergruppen. Und zwar erweisen sich nur jene Untergruppen als Galois-abgeschlossen, die auch abgeschlossen sind bezüglich jener Topologie, die $\mathrm{Aut}_K(E)$ als Spurtopologie von der punktweisen Topologie (schwachen Topologie, Produkttopologie) auf E^E erbt, siehe Proposition 7.1.1.9.

Satz 9.3.4.1. *Ist $K \leq E$ eine algebraische Körpererweiterung, so ist die Galoisgruppe $\mathrm{Aut}_K(E)$ bezüglich der schwachen Topologie eine kompakte Hausdorffgruppe.*

Beweis. Nach Proposition 7.1.1.9 ist die symmetrische Gruppe $\mathrm{Sym}(E)$ aller Permutationen von E eine topologische Hausdorffgruppe. Klarerweise vererben sich diese Eigenschaften auf Untergruppen. Also ist auch $\mathrm{Aut}_K(E) \leq \mathrm{Sym}(E)$ eine topologische Hausdorffgruppe. Zu zeigen bleibt die Kompaktheit.
Für jedes $u \in E$ bezeichne C_u die endliche Menge aller Konjugierten von u, d.h. die Menge aller Nullstellen des Minimalpolynoms von u über K. Jeder K-Automorphismus $\sigma \in \mathrm{Aut}_K(E)$ bildet u auf ein Element aus C_u ab, ist daher ein Element des Produktes $P := \prod_{u \in E} C_u \subseteq E^E$. Weil sämtliche C_u endlich sind, ist dieses Produkt P nach dem Satz von Tychonow kompakt. Wir sind fertig, wenn wir zeigen können, dass $\mathrm{Aut}_K(E)$ als Teilmenge von P abgeschlossen ist. Wir beweisen das, indem wir für jedes $f \in P \setminus \mathrm{Aut}_K(E)$ eine Umgebung $U \subseteq P$ finden, die disjunkt ist zu $\mathrm{Aut}_K(E)$. Man beachte

zunächst, dass für alle $u \in K$ die Menge $C_u = \{u\}$ einelementig ist, also jedes $f \in P$ den Grundkörper K punktweise fest lässt. Damit bleiben nur drei Möglichkeiten, die alle denkbaren Fälle für ein $f \in P$, das kein K-Automorphismus ist, abdecken: nicht bijektiv, nicht mit der Addition verträglich, nicht mit der Multiplikation verträglich. Wir untersuchen diese drei Fälle.
Sei f nicht bijektiv. Jedes Element von P nimmt auf jeder der Mengen C_u ausschließlich Werte aus C_u an. Ist f insgesamt nicht bijektiv, so ist die Bijektivität auf wenigstens einem der C_u verletzt. Weil C_u endlich ist, gibt es $u_1 \neq u_2 \in C_u$ mit $f(u_1) = f(u_2) =: v$. Die Menge U aller $g \in P$ mit $g(u_1) = g(u_2) = v$ ist eine zu $\mathrm{Aut}_K(E)$ disjunkte Umgebung von f.
Sei f nicht verträglich mit der Addition, d.h. es gebe Elemente u_1, u_2 mit $f(u_1 + u_2) \neq f(u_1) + f(u_2)$. Die Menge U aller $g \in P$ mit $g(u) = f(u)$ für $u = u_1, u_2, u_1 + u_2$ ist eine zu $\mathrm{Aut}_K(E)$ disjunkte Umgebung von f.
Ist f nicht verträglich mit der Multiplikation, so verläuft das Argument völlig analog wie bei der Addition. □

Der allgemeine Hauptsatz der Galoistheorie lautet:

Satz 9.3.4.2 (Hauptsatz der Galoistheorie für algebraische Erweiterungen)**.** *Die (nicht notwendig endlichdimensionale) Körpererweiterung $K \leq E$ sei algebraisch und Galoissch. Dann gilt:*

1. *E ist Galoissch über jedem Zwischenkörper Z mit $K \leq Z \leq E$.*
2. *Die Galois-abgeschlossenen Teilmengen von E sind genau die Zwischenkörper Z mit $K \leq Z \leq E$.*
3. *Die Galois-abgeschlossenen Teilmengen der Galoisgruppe $\mathrm{Aut}_K(E)$ sind genau die topologisch abgeschlossenen Untergruppen von $\mathrm{Aut}_K(E)$.*
4. *Ein Zwischenkörper Z ist genau dann Galoissch über K, wenn $Z' \lhd \mathrm{Aut}_K(E)$ ein Normalteiler der Galoisgruppe ist. In diesem Fall ist $\mathrm{Aut}_K(Z) \cong K'/Z' = \mathrm{Aut}_K(E)/\mathrm{Aut}_Z(E)$.*

Beweis. Wir halten fest, dass E über K wegen Satz 9.2.5.1 normal und separabel ist.

1. Die erste Behauptung des Satzes ist gerade die Aussage von Proposition 9.2.5.7.
2. Nach Aussage 5 in Proposition 9.2.1.2 kommen nur Zwischenkörper als Galois-abgeschlossene Mengen in Frage. Somit bleibt zu zeigen, dass jeder Zwischenkörper Z mit $K \leq Z \leq E$ auch Galois-abgeschlossen ist. Das ist aber gerade die bereits bewiesene erste Behauptung.
3. Wir zeigen zunächst, dass jede Galois-abgeschlossene Menge $H \subseteq \mathrm{Aut}_K(E)$ eine topologisch abgeschlossene Untergruppe ist. Für jedes u aus dem Fixpunktkörper sei $H_u = \{u\}'$ die Menge aller $\sigma \in \mathrm{Aut}_K(E)$ mit $\sigma(u) = u$. Klarerweise ist H_u eine Untergruppe von $\mathrm{Aut}_K(E)$. Nach der Definition der Topologie auf $\mathrm{Aut}_K(E)$ ist H_u

aber auch topologisch abgeschlossen. Damit ist jeder Durchschnitt von gewissen H_u eine abgeschlossene Untergruppe von $\mathrm{Aut}_K(E)$. Als Galois-abgeschlossene Menge ist H aber gerade der Durchschnitt all jener H_u mit $u \in H'$, dem Fixpunktkörper von H.

Sei nun umgekehrt vorausgesetzt, dass $H \leq \mathrm{Aut}_K(E)$ topologisch abgeschlossen ist. Wir haben die Galois-Abgeschlossenheit von H zu beweisen. Dazu müssen wir von einem beliebigen $\sigma \in H''$ ausgehen und zeigen, dass es in H liegt. Weil H nach Voraussetzung topologisch abgeschlossen ist, genügt der Nachweis, dass σ im topologischen Abschluss $\overline{H}$ von H liegt. Dazu ist die endliche Interpolationseigenschaft zu beweisen: Für jede endliche Teilmenge $T = \{u_1, \ldots, u_n\} \subseteq E$ gibt es ein $\sigma_T \in H$ mit $\sigma_T(u_i) = \sigma(u_i)$ für $i = 1, \ldots, n$. So ein T sei nun vorgegeben. Weil E algebraisch über K ist, hat jedes u_i ein Minimalpolynom $f_i \in K[x]$. Als Galoissche Erweiterung ist E sogar normal und separabel über K, enthält mit den u_i also einen (innerhalb E eindeutigen) Zerfällungskörper Z_S von $S := \{f_1, \ldots, f_n\}$, wobei die f_i separabel sind. Auch Z_S ist normal (nach Satz 9.2.3.2) und separabel (nach Satz 9.2.5.5) über K, nach Satz 9.2.5.1 also Galoissch über K. Nach Lemma 9.3.3.2 ist Z_S stabil bezüglich K und E, und die Einschränkung $\sigma_{Z_S} := \sigma|_{Z_S}$ eines jeden $\sigma \in \mathrm{Aut}_K(E)$ ist ein Element von $\mathrm{Aut}_K(Z_S)$. Die Einschränkungen der Elemente von H bilden eine Untergruppe H_{Z_S} von $\mathrm{Aut}_K(Z_S)$. Der Körper $K_1 := H' \cap Z_S$ enthält jedenfalls K, die Erweiterung $K_1 \leq Z_S$ ist Galoissch (nach Proposition 9.2.5.7), außerdem endlichdimensional, erfüllt also den Hauptsatz 9.3.1.1 für endlichdimensionale Erweiterungen. Aus diesem folgt, dass der Fixpunktkörper K_1 *nur* von den Elementen in H_{Z_S} punktweise fest gelassen wird. Wegen $\sigma \in H''$ folgt daraus $\sigma_{Z_S} \in H_{Z_S}$. Also stimmt σ auf ganz Z_S mit einem Element σ_T von H überein, insbesondere also auf den Elementen $u_1, \ldots, u_n \in Z_S$. Damit ist der Beweis der dritten Behauptung erbracht.

4. Die vierte Behauptung folgt wie im endlichdimensionalen Fall aus Lemma 9.3.3.2. □

Es stellt sich die Frage, inwieweit sich der Hauptsatz auch auf nichtalgebraische Galoissche Erweiterungen ausdehnen lässt. Es stellt sich heraus, dass viele Aussagen in diesem Fall nicht mehr gelten; siehe Übungsaufgabe 9.3.4.5. Wir starten mit Beispielen (nicht-)Galoisscher transzendenter Erweiterungen.

UE 115 ► **Übungsaufgabe 9.3.4.3.** (F) Sei K ein Körper und bezeichne $K(x)$ den Körper der gebrochen rationalen Funktionen in einer Variablen über K. ◄ **UE 115**

(a) Sei $\alpha = \frac{f(x)}{g(x)} \in K(x) \setminus K$ mit $f, g \in K[x]$, wobei diese Darstellung gekürzt sei. Zeigen Sie, dass $[K(x) : K(\alpha)] = \max(\operatorname{grad} f, \operatorname{grad} g)$.

Anleitung: Es gibt ein kanonisches Polynom $m(t) \in K(\alpha)[t]$ mit $m(x) = 0$ vom Grad $\max(\operatorname{grad} f, \operatorname{grad} g)$; dabei gilt sogar $m(t) \in K[\alpha][t]$. Um zu zeigen, dass m über $K(\alpha)[t]$ irreduzibel ist, reicht es zu zeigen, dass m über $K[\alpha][t]$ irreduzibel ist (Lemma 5.3.2.5). Da α transzendent über K ist (warum?), ist $K[\alpha]$ kanonisch isomorph zu $K[z]$ für ein neues Variablensymbol z, sodass man m als Element von

$K[z][t]$ auffassen kann. Argumentieren Sie zunächst, dass m als Element von $K[t][z]$ irreduzibel ist.

(b) Schließen Sie aus (a): Für jeden Körper Z mit $K \lneq Z \leq K(x)$ gilt $[K(x) : Z] < \infty$.

(c) Zeigen Sie: Wenn K unendlich ist, dann ist die Gruppe $\mathrm{Aut}_K(K(x))$ unendlich.

(d) Zeigen Sie: Wenn K endlich ist, dann ist die Gruppe $\mathrm{Aut}_K(K(x))$ endlich.
Hinweis: Nochmal (a)

UE 116 ► Übungsaufgabe 9.3.4.4. (F) Sei K ein Körper. Zeigen Sie: **◄ UE 116**

(a) Wenn K unendlich ist, dann ist die (nichtalgebraische) Erweiterung $K \leq K(x)$ (der Körper der gebrochen rationalen Funktionen über K in einer Variablen) Galoissch.

Hinweis: Sei $Z := \mathrm{Aut}_K(K(x))' \ldots$

(b) Wenn K endlich ist, dann ist die (nichtalgebraische) Erweiterung $K \leq K(x)$ niemals Galoissch.

(c) Wenn K unendlich ist, dann ist die (nichtalgebraische) Erweiterung $K \leq K(x, y)$ (der Körper der gebrochen rationalen Funktionen über K in zwei Variablen) Galoissch.

Damit kommen wir zu den angekündigten Beispielen:

UE 117 ► Übungsaufgabe 9.3.4.5. (B) Zeigen Sie: **◄ UE 117**

(a) In der Galoisschen, nichtalgebraischen Erweiterung $\mathbb{Q} \leq \mathbb{Q}(x)$ ist der Zwischenkörper $\mathbb{Q}(x^2)$ Galois-abgeschlossen, der Zwischenkörper $\mathbb{Q}(x^3)$ aber nicht.

Hinweis: Ein Zwischenkörper Z ist genau dann Galois-abgeschlossen, wenn die Erweiterung $? \leq ?$ Galoissch ist.

(b) In der Galoisschen, nichtalgebraischen Erweiterung $\mathbb{Q} \leq \mathbb{Q}(x, y)$ ist der Zwischenkörper $\mathbb{Q}(x)$ Galoissch über $\mathbb{Q}$, aber nicht stabil.

Reizvoll ist auch die folgende Sichtweise auf algebraische Galoissche Körpererweiterungen $K \leq E$. Bezeichne $\mathcal{Z}_0$ das System aller Zwischenkörper Z, die gleichzeitig Zerfällungskörper Z_S einer endlichen Menge $S \subseteq K[x]$ von Polynomen sind. Solche Z sind normal über K und stabil bezüglich aller K-Automorphismen von Erweiterungen. Umgekehrt lässt sich für $Z_1, Z_2 \in \mathcal{Z}_0$ mit $Z_1 \leq Z_2$ jedes $\sigma_1 \in \mathrm{Aut}_K(Z_1)$ zu einem $\sigma_2 \in \mathrm{Aut}_K(Z_2)$ fortsetzen. Somit liegt ein projektives System vor. Trägermenge ist $\mathcal{Z}_0$, und für $Z_1 \leq Z_2$ ist die Einschränkungsabbildung $\varphi_{Z_2,Z_1} : \mathrm{Aut}_K(Z_2) \to \mathrm{Aut}_K(Z_1)$, $\sigma_2 \mapsto \sigma_2|_{Z_1}$ ein wohldefinierter Epimorphismus. Zusammen mit den $\psi_Z : \mathrm{Aut}_K(E) \to \mathrm{Aut}_K(Z)$, $\sigma \mapsto \sigma|_Z$, $Z \in \mathcal{Z}_0$, ist $\mathrm{Aut}_K(E)$ ein projektiver Limes dieses Systems. Weil alle $Z \in \mathcal{Z}_0$ endlichdimensional über K sind, sind auch alle $\mathrm{Aut}_K(Z)$ endlich. Eine Gruppe, die projektiver Limes endlicher Gruppen ist, nennt man *proendlich*[2]. Wir haben also im Wesentlichen bewiesen:

[2]Sprich: pro-endlich

Satz 9.3.4.6. *Ist E eine algebraische und Galoissche Erweiterung von K, so ist* $\mathrm{Aut}_K(E)$ *proendlich.*

UE 118 ▶ **Übungsaufgabe 9.3.4.7.** (V,D) Skizzenhaft wurde der Beweis von Satz 9.3.4.6 bereits erbracht. Führen Sie alle Argumente sorgfältig aus. Diskutieren Sie auch, was sich ändert, wenn für die algebraische Erweiterung $K \leq E$ nur Normalität vorausgesetzt wird, möglicherweise aber Inseparabilitäten auftreten. ◀ **UE 118**

Die bereits in Satz 9.3.4.1 bewiesene Kompaktheit von Galoisgruppen algebraischer Erweiterungen ließe sich auch aus der Proendlichkeit schließen. Es gilt nämlich:

Satz 9.3.4.8. *Jede proendliche Gruppe ist kompakt. (Der projektive Limes ist dabei auch im Sinne der Topologie zu verstehen.)*

UE 119 ▶ **Übungsaufgabe 9.3.4.9.** (V,E) Beweisen Sie Satz 9.3.4.8. ◀ **UE 119**

Von besonderem Interesse sind maximale algebraische Erweiterungen $K \leq E$. Dann ist E ein algebraischer Abschluss von K. In diesem Fall heißt $\mathrm{Aut}_K(E)$ die *absolute Galoisgruppe* des Körpers K. Die absolute Galoisgruppe eines algebraisch abgeschlossenen Körpers K ist trivial, die des Körpers $\mathbb{R}$ ist zweielementig, die von $\mathbb{Q}$ ist ziemlich schwer zu überschauen. Ein interessantes Beispiel zwischen uninteressant und undurchschaubar sind die endlichen Körper, die wir im nächsten Unterabschnitt betrachten wollen.

9.3.5 Zwei Folgerungen aus dem Hauptsatz

Wir wollen nun aus dem Hauptsatz der Galoistheorie die Gestalt der absoluten Galoisgruppe von endlichen Körpern ableiten. Danach präsentieren wir einen galoistheoretischen Beweis des Fundamentalsatzes der Algebra.
Zunächst zu den endlichen Körpern. Aus Satz 9.2.5.4 wissen wir bereits, dass eine Erweiterung $K \leq E$ von endlichen Körpern stets eine Galoissche Erweiterung ist. Erinnern wir uns an Satz 6.3.3.6, so erhalten wir darüber hinaus mit wenig Aufwand, dass die Galoisgruppe die einfachst denkbare Struktur hat:

Satz 9.3.5.1. *Die Galoisgruppe* $\mathrm{Aut}_K(E)$ *einer Erweiterung $K \leq E$ endlicher Körper ist zyklisch. Gilt $|K| = p^m$, so wird* $\mathrm{Aut}_K(E)$ *erzeugt vom Automorphismus $a \mapsto a^{p^m}$.*

Beweis. Sei $|E| = p^n$ mit $p \in \mathbb{P}$ und positivem $n \in \mathbb{N}$ und $P \leq K \leq E$ der Primkörper. Nach Satz 6.3.3.6 ist die Galoisgruppe der Erweiterung $P \leq E$ zyklisch, nämlich $\mathrm{Aut}_P(E) = \langle a \mapsto a^p \rangle = \{a \mapsto a^{p^i} \mid i = 0, \ldots, n-1\}$ für den Frobeniusautomorphismus $a \mapsto a^p$. Wegen $\mathrm{Aut}_K(E) \leq \mathrm{Aut}_P(E)$ und Aussage 4 in Satz 3.2.4.4 folgt daraus, dass auch $\mathrm{Aut}_K(E)$ zyklisch ist.
Die Galoisgruppe $\mathrm{Aut}_K(E)$ besteht definitionsgemäß genau aus jenen Automorphismen in $\mathrm{Aut}_P(E)$, die alle Elemente von K punktweise fixieren. Da K nach Satz 6.3.1.2 genau aus den Nullstellen von $x^{p^m} - x$ besteht, fixiert $a \mapsto a^{p^i}$ ganz K genau für $m \mid i$. Daraus folgt $\mathrm{Aut}_K(E) = \langle a \mapsto a^{p^m} \rangle$. □

Damit lässt sich nunmehr auch die absolute Galoisgruppe eines endlichen Körpers recht gut verstehen. Das zu erklären ist Gegenstand der folgenden Übungsaufgabe.

UE 120 ▶ **Übungsaufgabe 9.3.5.2.** Sei K ein endlicher Körper mit p^m Elementen, $p \in \mathbb{P}$, $m \in \mathbb{N}$, $m \geq 1$. Geben Sie eine möglichst transparente Beschreibung der absoluten Galoisgruppe von K.
Hinweis: Verwenden Sie Satz 9.3.5.1, außerdem die Ergebnisse aus den Unterabschnitten 6.3.5 und 9.3.4. Behandeln Sie zunächst den Fall $n = 1$. ◀ **UE 120**

Nun kommen wir zum Fundamentalsatz der Algebra. Dieser lautet bekanntlich:

Satz 9.3.5.3. *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

In Unterabschnitt 1.2.4 haben wir bereits einen analytischen Beweis skizziert, siehe auch Übungsaufgabe 1.2.4.9. An dieser Stelle wollen wir einen galoistheoretischen Beweis angeben, der den algebraischen Anteil stärker betont, aber trotzdem nicht ganz ohne analytisches (Basis-)Wissen auskommt.

Beweis. Es genügt zu zeigen, dass $\mathbb{C}$ keine echte endlichdimensionale Körpererweiterung E_1 besitzt. Wir gehen also von $\mathbb{C} \leq E_1$ mit $[E_1 : \mathbb{C}] < \infty$ aus. Es gibt eine Galoissche Erweiterung F von $\mathbb{R}$ mit $\mathbb{R} \leq \mathbb{C} \leq E_1 \leq F$ mit $d := [F : \mathbb{R}] < \infty$ (zum Beispiel den normalen Abschluss von E_1 über $\mathbb{R}$ (siehe Proposition 9.2.3.7). Wir wollen $F = \mathbb{C}$ zeigen. Sei dazu G die Galoisgruppe von F über $\mathbb{R}$. Nach dem Hauptsatz 9.3.1.1 ist G endlich, und alle Untergruppen und Zwischenkörper sind Galois-abgeschlossen. Sei $|G| = 2^n k$ mit k ungerade und $n \in \mathbb{N}$. Wir zeigen als Erstes $k = 1$. Nach dem ersten Sylowsatz (Satz 8.1.4.2) gibt es eine 2-Sylowgruppe $H \leq G$, d.h. eine Untergruppe der Ordnung $|H| = 2^n$. Sei $E := H'$. Die Gruppe H hat in G ungeraden Index k mit $[E : \mathbb{R}] = [H' : G'] = [G : H] = k$. Wir wollen $E = \mathbb{R}$ und $G = H$ zeigen. Sei dazu $u \in E = H'$, $f \in \mathbb{R}[x]$ das Minimalpolynom von u über $\mathbb{R}$ und $l := \operatorname{grad}(f)$. Dann ist $k = [H' : \mathbb{R}] = [H' : \mathbb{R}(u)] \cdot [\mathbb{R}(u) : \mathbb{R}] = [H' : \mathbb{R}(u)] \cdot l$. Also ist $l = \operatorname{grad}(f)$ als Teiler von k ebenfalls ungerade. Als reelles Polynom dieses ungeraden Grades l hat f eine Nullstelle in $\mathbb{R}$. Weil f überdies irreduzibel ist, folgt daraus $l = 1$, $u \in \mathbb{R}$ und somit tatsächlich $E = \mathbb{R}$ und $G = H$, also $|G| = 2^n$. Somit hat auch die Galoisgruppe $G_1 := \mathbb{C}'$ von F über $\mathbb{C}$ als Untergruppe von G eine Ordnung der Gestalt 2^m mit $m \in \mathbb{N}$. Wäre $m > 0$, so gäbe es entweder nach dem ersten Sylowsatz (Satz 8.1.4.2) oder alternativ nach Übungsaufgabe 8.3.4.9 eine Untergruppe $U \leq G_1$ der Ordnung 2^{m-1}, also $[G_1 : U] = 2$. Für $E_0 := U'$ hätten wir $[E_0 : \mathbb{C}] = [\mathbb{C}' : E_0'] = [G_1 : U] = 2$. Das jedoch widerspricht der Tatsache, dass in $\mathbb{C}$ quadratische Gleichungen stets lösbar sind. Daraus folgt $m = 0$ und somit $[F : \mathbb{C}] = [\mathbb{C}' : F'] = [G_1 : \{\mathrm{id}_F\}] = 1$, also $F = \mathbb{C}$. □

9.4 Die Galoisgruppe eines Polynoms

Die historisch ersten Körpererweiterungen $K \leq E$, an denen Galoisgruppen untersucht wurden, waren (in moderner Terminologie) Zerfällungskörper E eines Polynoms

$f \in K[x]$. Man spricht in dieser Situation auch von der Galoisgruppe $G(f)$ des Polynoms f. Die Elemente von $G(f)$ lassen sich mit den auf der Menge der Wurzeln von f induzierten Permutationen identifizieren. Galoisgruppen von Polynomen stehen im Zentrum des vorliegenden Abschnitts. Nach der Beobachtung einfacher allgemeiner Sachverhalte in 9.4.1 führt uns in 9.4.2 die bekannte Lösungsformel für die quadratische Gleichung zum Begriff der Diskriminante einer algebraischen Gleichung (siehe 9.4.3). Für Gleichungen vom Grad 3 (siehe 9.4.4) und 4 (siehe 9.4.5) steigt die Komplexität der Lösungstheorie schon beträchtlich, ist aber noch überschaubar. Für Grad 5 begnügen wir uns in Hinblick auf Abschnitt 9.5 im Wesentlichen mit einem Beispiel, in dem die Galoisgruppe die volle symmetrische Gruppe S_5 ist (siehe 9.4.6) sowie mit kurzen Bemerkungen zur sogenannten allgemeinen Gleichung n-ten Grades.

9.4.1 Galoisgruppen als endliche Permutationsgruppen

Definition 9.4.1.1. Ist K ein Körper, $f \in K[x]$ und $Z = Z_f$ ein Zerfällungskörper von f über K, so heißt $G(f) := \mathrm{Aut}_K(Z)$ die *Galoisgruppe* von f über K.

Ist f separabel, so hat f in Z genau $n := \operatorname{grad} f$ verschiedene Nullstellen $u_1, \ldots, u_n$. Es sei an Proposition 9.2.1.4 erinnert: Jedes $\sigma \in G(f)$ permutiert die Nullstellen von f. Da $Z = K(u_1, \ldots, u_n)$ von K und den u_i erzeugt wird, ist jedes $\sigma \in G(f)$ durch $\sigma|_{\{u_1,\ldots,u_n\}}$ eindeutig bestimmt. Daher kann jedes $\sigma \in G(f)$ mit jenem $\pi \in S_n$ identifiziert werden, welches $\sigma(u_i) = u_{\pi(i)}$ erfüllt, d.h. $G(f) \leq S_n$. Wenn f nicht separabel ist, dann gibt es $m < n$ verschiedene Nullstellen, womit wir $\sigma \in G(f)$ mit $\pi \in S_m$ identifizieren können. Da sich aber die Gruppe S_m mit einer Untergruppe von S_n identifizieren lässt, werden wir im Folgenden $G(f)$ für ein Polynom f vom Grad n unabhängig davon, ob f separabel ist oder nicht, sehr häufig stillschweigend als Untergruppe von S_n auffassen. Insbesondere denken wir uns eine Nummerierung der Nullstellen von f vorgegeben.

Proposition 9.4.1.2. *Die Ordnung $|G(f)|$ der Galoisgruppe eines Polynoms vom Grad n ist stets ein Teiler von $n! = |S_n|$. Ist $f \in K[x]$ außerdem separabel und irreduzibel, so ist $|G(f)|$ ein Vielfaches von n.*

Beweis. Die erste Aussage folgt aus unserer Identifizierung $G(f) \leq S_n$.
Für die zweite Aussage sei bemerkt, dass f genau n Nullstellen $u_1, \ldots, u_n$ hat. Wegen der Irreduzibilität können je zwei Nullstellen durch ein $\sigma \in G(f)$ aufeinander abgebildet werden (siehe Satz 6.1.3.4). Das bedeutet, dass $G(f)$ auf $\{u_1, \ldots, u_n\}$ transitiv agiert. Nach Proposition 8.1.1.5 folgt daraus, dass n ein Teiler von $|G(f)|$ ist. □

Wir wollen die Situation für aufsteigenden Grad $n = 1, 2, 3, 4, \ldots$ von

$$f(x) = \sum_{k=0}^{n} a_k x^k$$

mit $a_n \neq 0$ eingehender studieren. Wir werden bei dieser Gelegenheit auch die berühmten Lösungsformeln behandeln, die gleichzeitig als die wichtigste historische Motivation der Galoistheorie gelten können. Weil sich durch Division der Gleichung durch eine Konstante $\neq 0$ die Nullstellen nicht ändern und somit auch die Galoisgruppe dieselbe bleibt,

dürfen wir, wann immer es praktisch ist, zum normierten Polynom übergehen, das nach Division durch a_n aus f entsteht. Wir dürfen also oBdA $a_n = 1$ setzen.
Für $n = 1$ ist nichts weiter zu tun, weil Polynome vom Grad 1 ihre Nullstelle immer schon im Grundkörper haben, also $K = Z_f$ gilt und die Galoisgruppe $G(f) = \mathrm{Aut}_K(Z_f) = \mathrm{Aut}_K(K) = \{\mathrm{id}_K\}$ trivial ist. Für $n = 2$ ist die Situation ebenfalls noch sehr einfach, führt uns aber schon in natürlicher Weise zum verallgemeinerbaren Begriff der Diskriminante und verdient eine ausführlichere Diskussion.

9.4.2 Die quadratische Gleichung

Sei $f(x) = a_2x^2 + a_1x + a_0$ ein Polynom über dem Körper K vom Grad $n = 2$, also $a_2 \neq 0$. Die symmetrische Gruppe S_2 hat nur die beiden trivialen zwei Untergruppen, die einelementige und $S_2 \cong C_2$ selbst, in Zyklenschreibweise $S_2 = \{e, (12)\} \cong C_2$. Wir wollen uns überlegen, wann für ein quadratisches Polynom $f \in K[x]$ die Galoisgruppe $G(f)$ einelementig und wann $G(f) \cong C_2$ ist.
Ein quadratisches Polynom ist genau dann reduzibel, wenn es in zwei Linearfaktoren zerfällt, von denen jeder einer Nullstelle entspricht, die schon in K liegt. Die beiden Nullstellen können auch gleich sein (Doppelnullstelle). Für reduzibles f ist jedenfalls $Z_f = K$ und die Galoisgruppe $G(f) = \mathrm{Aut}_K(Z_f) = \mathrm{Aut}_K(K) = \{\mathrm{id}_K\}$ trivial (einelementig).
Ist f hingegen irreduzibel, dann liegt keine Nullstelle von f in K. Liegt im Zerfällungskörper Z_f eine doppelte Nullstelle u von f, so muss diese durch jeden K-Automorphismus σ von Z_f auf sich selbst abgebildet werden. Da $Z_f = K(u)$ über K von u erzeugt wird, muss σ auf ganz Z_f die Identität sein. Also ist bei inseparablem f die Galoisgruppe $G(f) = \{\mathrm{id}_{Z_f}\}$ ebenfalls trivial. Dieser Fall ist allerdings ziemlich speziell. Aus Proposition 9.2.4.1 wissen wir, dass er nur eintreten kann, wenn die Ableitung $f'(x) = 2a_2x + a_1$ das Nullpolynom ist. Wegen $a_2 \neq 0$ ist das nur der Fall, wenn $\mathrm{char}\, K = 2$ und $a_1 = 0$. Nach Normierung kommen also nur Polynome der Gestalt $x^2 - a$ über Charakteristik 2 in Frage. Ist u eine Nullstelle von $f(x) = x^2 - a$, so gilt $u^2 = a$, also $f(x) = x^2 - a = x^2 - u^2 = (x - u)^2$. Es liegt also wirklich eine doppelte Nullstelle vor.
In allen anderen Fällen, d.h. wenn f irreduzibel und separabel ist mit zwei verschiedenen Nullstellen $u_1 \neq u_2 \in Z_f$, so gibt es einen K-Isomorphismus σ, der u_1 und u_2 vertauscht. In diesem Fall ist $G(f)$, aufgefasst als Permutationsgruppe, ganz $S_2 \cong C_2$. Wir fassen zusammen:

Satz 9.4.2.1. *Ist K ein Körper und $f(x) = a_2x^2 + a_1x + a_0$, $a_2 \neq 0$, ein quadratisches Polynom über K mit Zerfällungskörper Z_f, so ist die Galoisgruppe $G(f)$ ein- oder zweielementig entsprechend der folgenden (vollständigen) Fallunterscheidung:*

1. *Hat f eine Nullstelle in K, so ist $G(f) = \{\mathrm{id}_K\}$ einelementig.*
2. *Ist $\mathrm{char}\, K = 2$ und $a_1 = 0$, so ist $G(f) = \{\mathrm{id}_{Z_f}\}$ einelementig.*
3. *Habe f keine Nullstelle in K, außerdem sei $\mathrm{char}\, K \neq 2$ oder $a_1 \neq 0$. Dann hat f zwei verschiedene Nullstellen $u_1, u_2 \in Z_f$, und $G(f) = \{\mathrm{id}_{Z_f}, \sigma\} \cong S_2 \cong C_2$*

ist zweielementig. Dabei bezeichnet σ den eindeutigen K-Automorphismus von Z_f, der u_1 mit u_2 vertauscht.

Dieser Satz beantwortet noch nicht die Frage, wie man entscheidet, ob $f(x) = a_2x^2 + a_1x + a_0$ eine Nullstelle in K hat und wie man die Nullstelle(n) von f ermittelt. In endlichen Körpern ist das ein finitäres Problem, weil man nur endlich viele Elemente durchzuprobieren hat. Man kann aber anspruchsvoller sein und nach Formeln für die Nullstellen fragen.
Lässt man Quadratwurzelsymbole in gewohnter Weise zu (d.h. $\sqrt{a}$ bezeichnet eines von im Allgemeinen zwei Elementen, deren Quadrat a ist), so kann man für $\operatorname{char} K \neq 2$ die Nullstellen eines quadratischen Polynoms $f(x) = a_2x^2 + a_1x + a_0$, $a_i \in K$, $a_2 \neq 0$, mit Hilfe der bekannten Lösungsformel für quadratische Gleichungen darstellen. Zunächst ändert sich die Lösungsmenge nicht, wenn man durch a_2 dividiert, also statt dem ursprünglichen Polynom nun $f(x) = x^2 + px + q$ mit $p = \frac{a_1}{a_2}$ und $q = \frac{a_0}{a_2}$ betrachtet und in bekannter Weise „auf ein vollständiges Quadrat ergänzt“:

$$f(x) = x^2 + px + q = \left(x + \frac{p}{2}\right)^2 - \frac{p^2}{4} + q.$$

Für eine Nullstelle u von f muss daher $(u + \frac{p}{2})^2 = \frac{p^2}{4} - q$ gelten. Kürzen wir $D := p^2 - 4q$ ab, so ergeben sich zwei Nullstellen u_1 und u_2 von f:

$$u_1 = \frac{1}{2}(-p + \sqrt{D}), \quad \text{und} \quad u_2 = \frac{1}{2}(-p - \sqrt{D})$$

Aus

$$f(x) = x^2 + px + q = (x - u_1)(x - u_2) = x^2 - (u_1 + u_2)x + u_1u_2$$

können wir als Spezialfall des Satzes von Vieta für $n = 2$ die Beziehungen $-p = u_1 + u_2$ und $u_1u_2 = q$ ablesen. Damit gilt

$$D = p^2 - 4q = (u_1 + u_2)^2 - 4u_1u_2 = u_1^2 - 2u_1u_2 + u_2^2 = (u_1 - u_2)^2.$$

Dieser Wert D heißt *Diskriminante* von f und ist offenbar genau dann 0, wenn $u_1 = u_2$ eine Doppelnullstelle von f ist. Wir fassen zusammen:

Satz 9.4.2.2. *Sei K ein Körper mit* $\operatorname{char} K \neq 2$ *und $f(x) = x^2 + px + q \in K[x]$. Dann zerfällt f über K (bzw. über einem Erweiterungskörper E von K) genau dann, wenn es ein $w \in K$ (bzw. $w \in E$) gibt mit $w^2 = D = p^2 - 4q$. Die Nullstellen von f sind dann gegeben durch*

$$u_1 = \frac{1}{2}(-p + w), \quad \textit{und} \quad u_2 = \frac{1}{2}(-p - w)$$

und stimmen genau dann überein, wenn $D = p^2 - 4q = 0$.

Die Definition der Diskriminante lässt sich auf Polynome beliebigen Grades verallgemeinern.

9.4.3 Die Diskriminante

Sei $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ ein normiertes Polynom n-ten Grades über einem Körper K und $f(x) = \prod_{i=1}^{n}(x - u_i)$ mit den Nullstellen u_i von f in einem Erweiterungskörper E von K. Dann gilt nach dem Satz 5.3.4.12 von Vieta $s_{n,i}(u_1, \ldots, u_n) = (-1)^i a_{n-i}$, $i = 1, \ldots, n$, mit den elementarsymmetrischen Polynomen $s_{n,i} \in K[x_1, \ldots, x_n]$ aus Unterabschnitt 5.3.4. Wir betrachten das Polynom

$$\Delta_n(x_1, \ldots, x_n) := \prod_{1 \le i < j \le n} (x_i - x_j).$$

Für $n = 1$ ist das Produkt leer und der allgemeinen Konvention entsprechend $\Delta_1 := 1$ zu setzen. Durch eine Permutation $\pi \in S_n$ der Indizes kann sich lediglich die Reihenfolge der Faktoren und das Vorzeichen ändern, letzteres je nachdem, ob π gerade ($\operatorname{sgn}(\pi) = 1$) oder ungerade ($\operatorname{sgn}(\pi) = -1$) ist. Folglich gilt

$$\Delta_n(x_{\pi(1)}, \ldots, x_{\pi(n)}) = \operatorname{sgn}(\pi)\Delta_n(x_1, \ldots, x_n).$$

Wegen $\operatorname{sgn}(\pi)^2 = (\pm 1)^2 = 1$ gilt für $D_n(x_1, \ldots, x_n) := \Delta_n(x_1, \ldots, x_n)^2$ daher

$$D_n(x_{\pi(1)}, \ldots, x_{\pi(n)}) = (\Delta_n(x_{\pi(1)}, \ldots, x_{\pi(n)}))^2 = \Delta_n(x_1, \ldots, x_n)^2 = D_n(x_1, \ldots, x_n).$$

Folglich ist D_n ein symmetrisches Polynom in den Variablen $x_1, \ldots, x_n$ und somit, nach dem Hauptsatz 5.3.4.4, selbst darstellbar als

$$D_n(x_1, \ldots, x_n) = g_n(s_{n,1}(x_1, \ldots, x_n), \ldots, s_{n,n}(x_1, \ldots, x_n))$$

mit einem eindeutig bestimmten Polynom g_n über K in n Variablen. Man beachte, dass g_n nur von n, nicht aber von K abhängt. Motiviert durch die oben erwähnte Vieta-Beziehung $s_{n,i}(u_1, \ldots, u_n) = (-1)^i a_{n-i}$, $i = 1, \ldots, n$ definieren wir nun:

Definition 9.4.3.1. Mit den obigen Bezeichnungen heißt

$$D = D(f) := g_n(-a_{n-1}, a_{n-2}, \ldots, (-1)^{n-1}a_1, (-1)^n a_0) \in K$$

die *Diskriminante* eines normierten Polynoms f vom Grad n. Ist $f(x) = \sum_{i=0}^{n} a_i x^i$ nicht normiert, so wird $D(f) := D(a_n^{-1}f)$ gesetzt.

UE 121 ► **Übungsaufgabe 9.4.3.2.** (F) Zeigen Sie, dass ein normiertes Polynom f in seinem Zerfällungskörper genau dann eine mehrfache Nullstelle hat, wenn $D(f) = 0$. ◄ **UE 121**

UE 122 ► **Übungsaufgabe 9.4.3.3.** (F) Für drei Polynome $f, g, h \in K[x]$ gelte $f(x) = g(x+c) = ch(x)$ mit $c \in K \setminus \{0\}$. Dann stimmen die Diskriminanten $D(f) = D(g) = D(h)$ überein. ◄ **UE 122**

Wir wollen nun kontrollieren, ob die in 9.4.3.1 definierte Diskriminante für $n = 2$ denselben Wert liefert wie in Satz 9.4.2.2. Wir erhalten

$$\begin{aligned} D_2(x_1, x_2) = (x_1 - x_2)^2 = x_1^2 - 2x_1x_2 + x_2^2 = (x_1 + x_2)^2 - 4x_1x_2 = \\ = s_{2,1}(x_1, x_2)^2 - 4s_{2,2}(x_1, x_2), \end{aligned}$$

also ist $g_2(y_1, y_2) = y_1^2 - 4y_2$. Um $D(f)$ für $f(x) = x^2 + a_1x + a_0 = x^2 + px + q$ zu berechnen, müssen wir Definition 9.4.3.1 folgend $y_1 = -a_1 = -p$ und $y_2 = a_0 = q$ einsetzen. Damit erhalten wir tatsächlich

$$D(f) = g_2(-p, q) = p^2 - 4q,$$

so wie in Satz 9.4.2.2.

Motiviert durch den Satz von Vieta 5.3.4.12, der den Zusammenhang zwischen Nullstellen und Koeffizienten eines Polynoms beschreibt, haben wir die Diskriminante eines Polynoms über den Umweg symmetrischer Polynome und unter Verwendung des Hauptsatzes 5.3.4.4 definiert. Wir hätten $D(f)$ auch direkt als das Produkt

$$D(f) := \prod_{1 \le i < j \le n} (u_i - u_j)^2$$

über alle $(u_i - u_j)^2$ definieren können, wenn $u_1, \ldots, u_n$ die Nullstellen von f in einem Zerfällungskörper Z sind, wobei jede entsprechend ihrer Vielfachheit vorkommt. Diese Größe ist tatsächlich unabhängig von der speziellen Wahl des Zerfällungskörpers und der Nummerierung u_i und liegt bereits im Grundkörper K:
Hat f eine doppelte Nullstelle, also $u_i = u_j$ für $i \neq j$, dann ist trivialerweise $D(f) = 0$. Sind hingegen alle u_i paarweise verschieden, so ist jeder der über K irreduziblen Faktoren von f separabel. Z ist also der Zerfällungskörper einer Menge separabler Polynome. Nach Satz 9.2.5.5 (den wir bei der obigen Vorgangsweise nicht bemühen mussten) ist daher die Erweiterung $K \le Z$ Galoissch. Wir wenden einen beliebigen K-Automorphismus σ von Z auf $D(f)$ an. Weil σ die u_i permutiert, liefert das ein Produkt mit denselben Faktoren, also $\sigma(D(f)) = D(f)$. Das Element $D(f)$ liegt also im Fixpunktkörper der vollen Galoisgruppe $\mathrm{Aut}_K(Z)$, daher – die Erweiterung $K \le Z$ ist Galoissch – in K.
Wenn wir hingegen

$$\Delta(f) := \prod_{1 \le i < j \le n} (u_i - u_j)$$

definieren, so erhalten wir eine Größe, die nicht in K liegen muss, somit vom speziellen Zerfällungskörper abhängt und auch dort nur bis auf das Vorzeichen eindeutig bestimmt ist, je nach der Nummerierung der u_i. Zum Beispiel kommen für das Polynom $f(x) := x^2 + 1$ über $K = \mathbb{Q}$ mit den Nullstellen i und $-i$ im Zerfällungskörper $Z := \mathbb{Q}[i] \le \mathbb{C}$ für $\Delta(f)$ die beiden Werte $i - (-i) = 2i$ und $-i - i = -2i$ in Frage, die nicht im Grundkörper $K = \mathbb{Q}$ liegen, weil dort $D(f) = p^2 - 4q = -4$ keine Quadratwurzel hat. In Hinblick auf die folgende Unterscheidung erweist sich diese Doppeldeutigkeit aber als unproblematisch, weil es nur darauf ankommt, ob Δ und somit auch $-\Delta$ im Grundkörper K liegt.

Satz 9.4.3.4. *Sei* $\operatorname{char} K \neq 2$ *und habe das Polynom* $f \in K[x]$ *Grad* $n \geq 1$ *und in seinem Zerfällungskörper* Z_f *nur einfache Nullstellen* $u_1, \ldots, u_n$*. Dann ist die Galoisgruppe* $G(f)$*, aufgefasst als Untergruppe von* S_n*, genau dann in der alternierenden Gruppe* $A_n \leq S_n$ *enthalten, wenn es in* K *ein Element* Δ *gibt mit* $\Delta^2 = D(f)$*.*

Beweis. Sei Z_f irgendein Zerfällungskörper von f. Es gilt $\Delta(f)^2 = D(f)$. Für ein beliebiges $\sigma \in G(f)$ sind zwei Fälle zu unterscheiden. Ist σ als Permutation der u_i gerade, so ist $\sigma(\Delta) = \Delta$, andernfalls $\sigma(\Delta) = -\Delta \neq \Delta$, letzteres wegen $\Delta \neq 0$ (weil die u_i paarweise verschieden sind) und wegen $\operatorname{char} K \neq 2$. Also liegt Δ genau dann im Fixpunktkörper K_0 der Galoisgruppe $G(f)$, wenn diese nur gerade Permutationen enthält, also in A_n enthalten ist. Zu zeigen bleibt $K_0 = K$, dass also die Erweiterung Galoissch ist. Nach Satz 9.2.5.5 ist das tatsächlich der Fall, weil Z_f der Zerfällungskörper der Menge S aller irreduziblen Faktoren von f ist, die wegen der Einfachheit der Nullstellen u_i separabel sind. □

9.4.4 Die kubische Gleichung

Ein Polynom $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0 \in K[x]$ dritten Grades, also mit $a_3 \neq 0$, ist genau dann reduzibel, wenn es einen Linearfaktor hat, d.h. eine Nullstelle in K. Ist eine Nullstelle gefunden, so ist f das Produkt von Polynomen kleineren Grades und die Nullstellensuche auf die bereits behandelten Fälle $n = 1, 2$ zurückgeführt. Wenn K ein Primkörper ist, dann ist die Suche nach einer Nullstelle von f in K ein finitäres Problem: Im Fall $\operatorname{char} K = p \in \mathbb{P}$, also $K \cong \mathbb{Z}_p$, muss man nur die endlich vielen Restklassen modulo p in f einsetzen. Ist $\operatorname{char} K = 0$, also $K \cong \mathbb{Q}$, so schränkt Proposition 5.3.2.9 (nach Multiplikation mit einer geeigneten ganzen Zahl, damit alle Koeffizienten ganzzahlig werden) die Möglichkeiten ebenfalls auf eine endliche Menge ein. Auch die Bestimmung der Galoisgruppe $G(f)$ lässt sich (egal ob K ein Primkörper ist oder nicht) für reduzibles f auf die Fälle $n = 1, 2$ zurückführen. Denn entweder zerfällt $f = f_1f_2f_3$ in drei Linearfaktoren, in welchem Fall $Z_f = K$ und somit $G(f) = \{\mathrm{id}_K\}$ trivial ist; oder $f = f_1f_2$ mit linearem f_1 und quadratischem f_2, in welchem Fall $G(f) \cong G(f_2)$ gilt.

UE 123 ► **Übungsaufgabe 9.4.4.1.** (F) Geben Sie den Isomorphismus $G(f) \cong G(f_2)$ explizit an. ◄ **UE 123**

Zur Bestimmung von $G(f)$ dürfen wir uns daher auf irreduzible f konzentrieren. Nach Satz 9.4.1.2 muss die Gruppenordnung $|G(f)|$ ein Vielfaches von 3 und ein Teiler von $3! = 6$ sein. Als Untergruppe von S_n kann es sich bei $G(f)$ also nur um die alternierende Gruppe $A_3 = \{\mathrm{id}, (123), (132)\}$ oder um die ganze symmetrische Gruppe S_3 handeln. Nach Satz 9.4.3.4 hängt das davon ab, ob die Diskriminante $D(f)$ Quadrat eines Elementes $\Delta \in K$ ist. Wegen Übungsaufgabe 9.4.3.3 ändert sich die Diskriminante nicht, wenn wir $f(x) = a_3x^3+a_2x^2+a_1x+a_0 \in K[x]$ durch $a_3 \neq 0$ dividieren. Wir setzen daher oBdA $a_3 = 1$ voraus. Ebenso wegen 9.4.3.3 dürfen wir anschließend (sofern $\operatorname{char} K \neq 3$) x durch $x - \frac{a_2}{3}$ ersetzen, wodurch das quadratische Glied wegfällt. Wir beschränken uns daher auf Polynome dritten Grades der Bauart $f(x) = x^3+px+q$. Nach etwas mühsamer Rechnung erhält man:

Satz 9.4.4.2. *Sei* $\operatorname{char} K \neq 2,3$. *Die Diskriminante eines Polynoms* $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0 \in K[x]$ *dritten Grades ist gegeben durch*

$$D(f) = -4p^3 - 27q^2.$$

Dabei sind p *und* q *so zu wählen, dass* $a_3^{-1}f(x - \frac{a_2}{3a_3}) = x^3 + px + q$ *gilt.*
Ist f *irreduzibel und* $D(f) = \Delta^2$ *mit einem* $\Delta \in K$, *so ist* $G(f) \cong A_3 \cong C_3$; *gibt es kein solches* $\Delta \in K$, *so ist* $G(f) \cong S_3$.

UE 124 ► Übungsaufgabe 9.4.4.3. Beweisen Sie Satz 9.4.4.2. Bedenken Sie weiterhin Übungsaufgabe 9.4.3.3. **◄ UE 124**

Wir wollen weiterhin $\operatorname{char} K \neq 2,3$ voraussetzen und unter dieser Bedingung die Lösungsformel von Cardano (siehe Satz 9.4.4.4 weiter unten) herleiten.
Wir gehen aus vom Polynom $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0 \in K[x]$ mit $a_3 \neq 0$, dessen Nullstellen gesucht sind. Wie schon in Satz 9.4.4.2 gehen wir über zum normierten Polynom $f_0 := a_3^{-1}f$ mit denselben Nullstellen wie f und sodann zum Polynom $f_0(x - \frac{a_2}{3a_3})$, dessen Nullstellen gegenüber jenen von f nur um $\frac{a_2}{3a_3}$ verschoben sind. Also genügt es weiterhin, von vornherein nur kubische Polynome der speziellen Bauart $f(x) = x^3 + px + q$ zu untersuchen. Seien also $u = u_1, u_2, u_3$ die Nullstellen im Zerfällungskörper Z_f von f. Der Rechentrick besteht darin, $u = a + b$ als Summe anzusetzen und nachträglich a und somit b geeignet zu wählen. Die dritte Potenz von u ist

$$u^3 = (a+b)^3 = a^3 + 3ab(a+b) + b^3,$$

was wir unter nochmaliger Verwendung von $a + b = u$ zu

$$u^3 - 3abu - (a^3 + b^3) = 0$$

umschreiben. Sind a und b so gewählt, dass $-3ab = p$ gilt, so folgt daraus $-(a^3 + b^3) = -u^3 + 3abu = -u^3 - pu = -f(u) + q = q$. Nach Vieta sind dann a^3 und b^3 die beiden Lösungen der sogenannten *quadratischen Resolvente*

$$r(x) := x^2 + qx - \frac{p^3}{27} = x^2 - (a^3 + b^3)x + a^3b^3$$

von f. Wegen $\operatorname{char} K \neq 2$ dürfen wir die Lösungsformel 9.4.2.2 für die quadratische Gleichung verwenden und erhalten

$$a^3, b^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Für $u = a + b$ gilt folglich die sogenannte *Cardanosche Formel*:

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Zu beachten ist, dass es im Allgemeinen drei dritte Wurzeln gibt und nicht alle 9 Kombinationen zugelassen sind, sondern nur solche Paare aus a und b, die $a^3b^3 = -\frac{p^3}{27}$ erfüllen. Somit lässt sich die Formel korrekter in folgende Aussage kleiden.

Satz 9.4.4.4. *Sei $f(x) = x^3+px+q \in K[x]$ ein normiertes Polynom dritten Grades über einem Körper K mit* $\operatorname{char} K \neq 2, 3$. *Die Elemente $w, a, b \in K$ mögen die Beziehungen $w^2 = \frac{q^2}{4} + \frac{p^3}{27}$, $a^3 = -\frac{q}{2} + w$ und $b^3 = -\frac{q}{2} - w$ erfüllen. Außerdem sei $\zeta \in K$ eine primitive dritte Einheitswurzel, d.h. $\zeta^3 = 1$ aber $\zeta \neq 1$. Dann liegen sämtliche drei (nicht notwendig paarweise verschiedenen) Nullstellen u_1, u_2, u_3 von f in K, und können als*

$$u_1 = a + b, \quad u_2 = \zeta a + \zeta^2 b, \quad u_3 = \zeta^2 a + \zeta b.$$

erhalten werden.

UE 125 ▶ **Übungsaufgabe 9.4.4.5.** (B) Sei $f \in K[x]$ ein separables kubisches Polynom mit Galoisgruppe S_3 und Wurzeln $u_1, u_2, u_3 \in E$. Zeigen Sie: Die Zwischenkörper dieser Erweiterung sind E, $K(\Delta)$, $K(u_1)$, $K(u_2)$, $K(u_3)$ und K. Die entsprechenden Untergruppen der Galoisgruppe sind $\{1\}$, A_3, $T_1 = \{\mathrm{id}, (23)\}$, $T_2 = \{\mathrm{id}, (13)\}$, $T_3 = \{\mathrm{id}, (12)\}$ und S_3. ◀ **UE 125**

UE 126 ▶ **Übungsaufgabe 9.4.4.6.** (B) ◀ **UE 126**

1. Für $f(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$ ist $G(f) \cong A_3$.
2. Für $g(x) = x^3 - 3x^2 - x - 1 \in \mathbb{Q}[x]$ ist $G(g) \cong S_3$.

9.4.5 Die Gleichung vierten Grades

Es überrascht wenig, dass sich die Dinge für Polynome vierten Grades komplizierter verhalten als bei kubischen. Immerhin lassen sich Galoisgruppe und Lösungen, wenn auch mit teilweise wesentlich mehr Aufwand, so doch grundsätzlich noch auf ähnliche Weise bestimmen. Das soll im Folgenden, teils nur skizzenhaft, ausgeführt werden.

Beginnen wir mit der Lösungsformel für Polynome vierten Grades über einem Körper K, von dem wir wie schon bei der kubischen Gleichung $\operatorname{char} K \neq 2, 3$ voraussetzen. Sei also

$$f(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

mit $a_4 \neq 0$ ein Polynom vierten Grades über dem Körper K. Bei Bedarf dürfen wir uns von diesem allgemeinen Fall auf den vereinfachten Fall $a_4 = 1$ (nach Division der Gleichung durch a_4) und $a_3 = 0$ (nach der „Ergänzung auf ein vollständiges Biquadrat“) $f(x) = (x + \frac{a_3}{4})^4 + p(x + \frac{a_3}{4})^2 + q(x + \frac{a_3}{4}) + r$, also auf Polynome der Bauart

$$f(x) = x^4 + px^2 + qy + r$$

mit geeigneten Koeffizienten $p, q, r \in K$ beschränken. Wir gehen von der Faktorisierung

$$f(x) = (x - u_1)(x - u_2)(x - u_3)(x - u_4),$$

aus. Gemäß Vieta multiplizieren wir aus zu

$$f(x) = x^4 - (u_1+u_2+u_3+u_4)x^3 + \left(\sum_{1\le i<j\le 4} u_iu_j\right)x^2 - \left(\sum_{1\le i<j<k\le 4} u_iu_ju_k\right)x + u_1u_2u_3u_4.$$

Nach Koeffizientenvergleich mit $f(x) = x^4 + px^2 + qy + r$ lesen wir für die vier elementarsymmetrischen Funktionen von u_1, u_2, u_3, u_4 ab:

$$u_1 + u_2 + u_3 + u_4 = 0, \quad \sum_{1\le i<j\le 4} u_iu_j = p, \quad \sum_{1\le i<j<k\le 4} u_iu_ju_k = -q, \quad u_1u_2u_3u_4 = r$$

Die entscheidende Idee besteht darin, die symmetrisch aufgebauten Elemente

$$v_1 := -(u_1+u_2)(u_3+u_4), \quad v_2 := -(u_1+u_3)(u_2+u_4), \quad v_3 := -(u_1+u_4)(u_2+u_3)$$

zu betrachten. Wegen $u_1+u_2+u_3+u_4 = 0$ sind in den Definitionen für die v_i die beiden Faktoren bis auf das Vorzeichen gleich, also kann man auch schreiben

$$v_1 = (u_1+u_2)^2 = (u_3+u_4)^2, \quad v_2 = (u_1+u_3)^2 = (u_2+u_4)^2, \quad v_3 = (u_1+u_4)^2 = (u_2+u_3)^2.$$

Mit den anderen oben genannten Bedingungen kann man die elementarsymmetrischen Funktionen auch von v_1, v_2, v_3 auf die Koeffizienten der Gleichung zurückführen. Und zwar rechnet man nach:

$$v_1 + v_2 + v_3 = -2p, \quad v_1v_2 + v_1v_3 + v_2v_3 = p^2 - 4r, \quad v_1v_2v_3 = q^2$$

Mit v_1, v_2, v_3 liegen folglich die drei Nullstellen der sogenannten *kubischen Resolvente*

$$R(x) = x^3 + 2px^2 + (p^2 - 4r)x - q^2$$

von f vor, die mit Hilfe der Cardanoschen Formel (siehe auch Satz 9.4.4.4) gefunden werden können. Wir werden nun die u_i auf die v_j zurückführen. Und zwar wählt man Quadratwurzeln w_i der v_i, wobei nur noch auf das Vorzeichen der zusätzlichen Bedingung $w_1w_2w_3 = -q$ zu achten ist. Dann kann man

$$u_1 + u_2 = -(u_3+u_4) = w_1, \quad u_1 + u_3 = -(u_2+u_4) = w_2, \quad u_1 + u_4 = -(u_2+u_3) = w_3$$

ablesen. Hieraus lassen sich die u_i zurückrechnen:

$$u_1 := \frac{w_1+w_2+w_3}{2},\ u_2 := \frac{w_1-w_2-w_3}{2},\ u_3 := \frac{-w_1+w_2-w_3}{2},\ u_4 := \frac{-w_1-w_2+w_3}{2}$$

Wir fassen zusammen:

Satz 9.4.5.1. *Sei K ein Körper der Charakteristik* $\operatorname{char} K \neq 2, 3$ *und $f(x) = x^4 + px^2 + qx + r \in K[x]$. Seien v_1, v_2, v_3 die Nullstellen der sogenannten kubischen Resolvente $R(x) := x^3 + 2px^2 + (p^2 - 4r)x - q^2$ (wie sie nach Elimination des quadratischen Gliedes mit Hilfe der Cardanoschen Formel, siehe Satz 9.4.4.4, gefunden werden können), weiters $w_1, w_2, w_3 \in K$ mit $w_1^2 = v_1$, $w^2 = v_2$ und $w_3^2 = v_3$ sowie $w_1w_2w_3 = -q$. Dann sind*

$$u_1 := \frac{w_1+w_2+w_3}{2},\ u_2 := \frac{w_1-w_2-w_3}{2},\ u_3 := \frac{-w_1+w_2-w_3}{2},\ u_4 := \frac{-w_1-w_2+w_3}{2}$$

die vier Nullstellen von f.

UE 127 ► **Übungsaufgabe 9.4.5.2.** (V) Vervollständigen Sie die ausgelassenen Schritte in obiger Ableitung der Lösungsformel für die Gleichung vierten Grades und damit im Beweis von Satz 9.4.5.1. ◄ **UE 127**

Wir wollen uns auch noch der Bestimmung der Galoisgruppe eines Polynoms $f(x) = a_4x^4+a_3x^3+a_2x^2+a_1x+a_0$ mit $a_4 \neq 0$ über einem Körper K zuwenden. Eingangs wollen wir den Fall behandeln, dass sich das Polynom in irreduzible Faktoren kleineren Grades zerlegen lässt. Ist einer dieser Faktoren linear, so liegt die zugehörige Nullstelle in K, und es geht nur mehr um die Permutation der übrigen drei Nullstellen eines Polynoms dritten Grades. Damit ist die Bestimmung der Galoisgruppe auf früher bereits behandelte Fälle zurückgeführt. Zerfällt $f = f_1f_2$ hingegen in zwei quadratische irreduzible Faktoren f_1 und f_2, so sind zwei Fälle zu unterscheiden. Stimmen die Zerfällungskörper Z_{f_1} und Z_{f_2} von f_1 und f_2 überein, so ist $G(f) = G(f_1) = G(f_2)$, und diese Fälle wurden bereits behandelt. Andernfalls ergibt sich der Zerfällungskörper Z_f als Iteration zweier quadratischer Erweiterungen. Das führt hier zu einer Erweiterung vierten Grades.

UE 128 ► **Übungsaufgabe 9.4.5.3.** (F) Welche Struktur kann die Galoisgruppe $G(f)$ eines Polynoms f vom Grad 4 haben, das in zwei irreduzible quadratische Faktoren zerfällt? ◄ **UE 128**

Ebenso Gegenstand einer Übungsaufgabe sei die Frage, wie entschieden werden kann, ob ein Polynom vierten Grades irreduzibel ist.

UE 129 ► **Übungsaufgabe 9.4.5.4.** (E,D) Beschreiben Sie, wie für jedes Polynom f vierten Grades über $\mathbb{Q}$ nach endlich vielen Schritten entschieden werden kann, ob es irreduzibel ist. Lässt sich Ihre Methode auf Polynome höheren Grades verallgemeinern? Wie sieht es mit Polynomen über endlichen Körpern (statt über $\mathbb{Q}$) aus? ◄ **UE 129**

Zu untersuchen bleibt als interessantester Fall der eines irreduziblen Polynoms f vierten Grades über einem Körper K. Wir beschränken uns auf den separablen Fall. Zunächst überlegen wir uns, welche Gruppen überhaupt in Frage kommen, und zwar aufgefasst als Untergruppen der symmetrischen Gruppe S_4. Aus Proposition 9.4.1.2 folgt, dass als Gruppenordnung $n := |G(f)|$ nur Teiler von $24 = 4! = |S_4|$ in Frage kommen, die (wegen irreduzibel) gleichzeitig ein Vielfaches von 4 sind, also $n = 4, 8, 12, 24$. Außerdem muss $G(f)$ als Permutationsgruppe auf $\{1, 2, 3, 4\}$ transitiv sein. Für $n = 4$ sind das einerseits die von einem Viererzyklus erzeugten zyklischen Untergruppen $\cong C_4$ von S_4 (davon gibt es drei Stück) sowie die Kleinsche Vierergruppe $V := \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \cong C_2 \times C_2$. Zur Ordnung $n = 8$: Die Diedergruppe D_4 (Symmetriegruppe des Quadrats, erzeugt z.B. von einem Viererzyklus (1234) und einer Transposition (13)) ist eine Gruppe der Ordnung 8, die sich in die S_4 einbetten lässt. Umgekehrt ist jede 8-elementige Untergruppe eine 2-Sylowgruppe von S_4. Nach dem zweiten Sylowsatz 8.1.4.3 diese zueinander konjugiert. Innerhalb S_4 bedeutet Konjugation lediglich Umnummerierung der Symbole $1, 2, 3, 4$. Also kennen wir im Wesentlichen mit der gegebenen D_4 bereits alle. (Insgesamt gibt es in S_4 drei Kopien. Denn nach dem dritten Sylowsatz 8.1.4.5 ist ihre

Anzahl ungerade und ein Teiler von 24, wobei die Anzahl 1 nicht in Frage kommt, weil D_4 kein Normalteiler von S_4 ist. Damit bleibt nur 3 als mögliche Anzahl.) Zu $n = 12$ gibt es nur eine Untergruppe, nämlich A_4: Jede 12-elementige Untergruppe von S_4 hat Index 2 und ist daher ein Normalteiler. Nach Folgerung 8.2.3.4 ist A_4 der einzige 12-elementige Normalteiler. Schließlich gibt es zu $n = 24$ klarerweise nur die volle Gruppe S_4.
Welcher dieser Fälle eintritt, lässt sich entscheiden, wenn man gewisse Hilfsgrößen kennt. Der folgende Satz beschreibt die Situation präzise:

Satz 9.4.5.5. *Sei f ein irreduzibles separables Polynom über dem Körper K mit Galoisgruppe $G(f)$ und mit paarweise verschiedenen Nullstellen u_1, u_2, u_3, u_4 in einem Zerfällungskörper Z_f von f. Wir definieren in Z_f die Elemente*

$$\alpha := u_1u_2 + u_3u_4, \quad \beta := u_1u_3 + u_2u_4, \quad \gamma := u_1u_4 + u_2u_3,$$

das Polynom $\overline{R}(x) := (x - \alpha)(x - \beta)(x - \gamma)$, sowie $m := [K(\alpha, \beta, \gamma) : K]$, den Erweiterungsgrad des Zerfällungskörpers von $\overline{R}$ in Z_f. Dann gilt die folgende (vollständige) Fallunterscheidung:

1. *$G(f) \cong S_4$ genau dann, wenn $m = 6$.*
2. *$G(f) \cong A_4$ genau dann, wenn $m = 3$.*
3. *$G(f) \cong V \cong C_2 \times C_2$ genau dann, wenn $m = 1$.*
4. *$G(f) \cong D_4$ genau dann, wenn $m = 2$ und f irreduzibel ist über $K(\alpha, \beta, \gamma)$.*
5. *$G(f) \cong C_4$ genau dann, wenn $m = 2$ und f reduzibel ist über $K(\alpha, \beta, \gamma)$.*

Das Polynom $\overline{R}$ nennt man, so wie R weiter oben, ebenfalls *kubische Resolvente* von f. Im Unterschied zu R muss $\overline{R}$ aber nicht in $K[x]$ liegen.
Nach unseren Vorüberlegungen kommen genau die fünf genannten (paarweise nichtisomorphen) Gruppen C_4, V, D_4, A_4, S_4 für $G(f)$ in Frage. Somit genügt der Nachweis, dass für jeden dieser Fälle m den in Satz 9.4.5.5 behaupteten Wert hat und, lediglich zur Unterscheidung der letzten beiden Fälle, f die behauptete (Ir-)Reduzibilität aufweist. Das soll im Rahmen der folgenden Übungsaufgabe ausgeführt werden.

UE 130 ► **Übungsaufgabe 9.4.5.6.** (V) Beweisen Sie Satz 9.4.5.5. Hinweis: Zeigen Sie zunächst, dass in der Galoiskorrespondenz der Galoisschen Erweiterung $K \leq Z_f$ dem Körper $K(\alpha, \beta, \gamma)$ die Gruppe $G(f) \cap V$ entspricht. Eine der beiden dafür zu beweisenden Inklusionen ist offensichtlich, für die andere ist zu zeigen, dass jedes $\sigma \in G(f) \notin V$ wenigstens eines der Elemente α, β, γ nicht fest lässt. A priori kommen $24 - 4 = 20$ verschiedene σ in Frage, man kann sich die Arbeit aber etwas erleichtern. ◄ **UE 130**

9.4.6 Die symmetrische Gruppe S_5 als Galoisgruppe

UE 131 ► **Übungsaufgabe 9.4.6.1.** Sei p eine Primzahl. Zeigen Sie, dass die beiden Permutationen (12) und $(12 \dots p)$ (Zyklenschreibweise) die S_p erzeugen. ◄ **UE 131**

Satz 9.4.6.2. *Sei $p \in \mathbb{P}$ und $f \in \mathbb{Q}[x]$ ein irreduzibles Polynom vom Grad p mit genau zwei Wurzeln in $\mathbb{C} \setminus \mathbb{R}$. Dann ist $G(f) \cong S_p$.*

Beweisskizze. Wir betrachten $G(f)$ als Untergruppe von S_p. Nach Proposition 9.4.1.2 teilt p die Gruppenordnung $|G(f)|$. Nach dem Satz von Cauchy 8.1.3.2 gibt es daher ein $\sigma \in G(f)$ mit Ordnung p. Wegen $p \in \mathbb{P}$ muss $\sigma = (1 j_2 \dots j_p)$ als Permutation ein p-Zyklus sein. Die komplexe Konjugation $a + bi \mapsto a - bi$ ist ein $\mathbb{R}$-Automorphismus von $\mathbb{C}$. Daher vertauscht diese Abbildung die beiden komplexen Wurzeln von f und hält alle anderen fest. Daraus folgt, dass $G(f)$ eine Transposition τ enthält, oBdA $\tau = (12)$. Für ein geeignetes k gilt $\sigma^k = (12 i_3 \dots i_p) \in G(f)$. Nach Übungsaufgabe 9.4.6.1 erzeugen (12) und $(123 \dots p)$ schon ganz S_p, also muss $G(f) = S_p$ gelten. □

UE 132 ► Übungsaufgabe 9.4.6.3. Zeigen Sie, dass das Polynom $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ die Eigenschaften aus Satz 9.4.6.2 und somit eine Galoisgruppe $G(f) \cong S_5$ hat. Hinweis: Eisensteinsches Kriterium, Kurvendiskussion. **◄ UE 132**

Das Polynom $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ hat also eine nicht auflösbare Galoisgruppe $G(f) \cong S_5$, siehe Folgerung 8.3.4.5. Mit den Ergebnissen aus Abschnitt 9.5, insbesondere Unterabschnitt 9.5.3, wird daraus folgen, dass es keine Lösungsformel für die Gleichung $x^5 - 4x + 2 = 0$ gibt. Erst recht kann es daher keine allgemeine Lösungsformel für beliebige Polynome vom Grad 5 geben. Trotzdem ist es lehrreich, die Frage nach solch einer allgemeinen Formel begrifflich zu fassen. Das soll nun skizziert werden.
Für ein normiertes Polynom

$$f_n(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$$

wollen wir zu diesem Zweck nun neben x auch die Koeffizienten a_i als Unbestimmte auffassen. Wir betrachten also die rein transzendente Erweiterung $E_n := K(a_0, \dots, a_{n-1})$ von K und f_n als ein Element von $E_n[x]$. Es bietet sich folgende Sprechweise an: Man sagt, dass es eine *allgemeine Lösungsformel* für Gleichungen über K vom Grad n gibt, wenn es eine Lösungsformel für $f_n \in E_n[x]$ gibt – denn aus einer solchen lässt sich bei gegebenem, „konkretem“ und oBdA normiertem Polynom $g(x) = x^n + c_{n-1}x^{n-1} + \dots + c_1 x + c_0 \in K[x]$ durch Einsetzen der Werte c_i für die a_i eine Lösungsformel für $g(x)$ gewinnen; so, wie man es beispielsweise von der quadratischen Lösungsformel gewöhnt ist. Ist Z_n der Zerfällungskörper von f_n über E_n, so heißt $\mathrm{Aut}_{E_n}(Z_n)$ die *Galoisgruppe der allgemeinen Gleichung n-ten Grades*. Es stellt sich heraus, dass $\mathrm{Aut}_{E_n}(Z_n)$ zur vollen symmetrischen Gruppe S_n isomorph ist und somit genau für $n \leq 4$ eine auflösbare Gruppe ist; siehe Übungsaufgabe 8.3.4.5. Mit den Ergebnissen aus Abschnitt 9.5 wird sich daraus ergeben, dass es genau für $n \leq 4$ allgemeine Lösungsformeln gibt.

UE 133 ► Übungsaufgabe 9.4.6.4. (V) Zeigen Sie, dass $\mathrm{Aut}_{E_n}(Z_n) \cong S_n$. **◄ UE 133**
Anleitung: Seien $u_1, \dots, u_n \in Z_n$ die Nullstellen von f_n. Zeigen Sie $Z_n = E_n(u_1, \dots, u_n) = K(u_1, \dots, u_n)$. Verwenden Sie Unterabschnitt 6.1.5, um zu zeigen, dass die u_i paarweise verschieden sind und dass $\{u_1, \dots, u_n\}$ algebraisch unabhängig über K ist sowie um eine isomorphe Einbettung $S_n \to \mathrm{Aut}_{E_n}(Z_n)$ herzuleiten.

9.5 Auflösung von Gleichungen durch Radikale

Dieser Abschnitt befasst sich mit jener Frage, aus der die Galoistheorie historisch ihren Ursprung nahm. Und zwar geht es um Lösungsformeln für algebraische Gleichungen in einer Variablen – das sind Gleichungen der Form $f(x) = 0$ für ein Polynom f – durch Radikale. Das bedeutet, dass die gesuchte Formel die Koeffizienten von f ausschließlich mit Hilfe der vier Körperoperationen sowie Wurzelsymbolen verbindet. Die Schwierigkeit, eine solche Formel zu finden, hängt sehr stark vom Grad n des Polynoms f ab. Für $n = 1$ sind gar keine Wurzelsymbole nötig, und Lösungen der gesuchten Art – wenn auch natürlich nicht in moderner Symbolik – waren schon in der Antike bekannt. Die allgemeine Lösung für $n = 2$ stammt aus der frühmittelalterlichen Blüte des orientalischen Bagdad um das Jahr 800. Für $n = 3, 4$ waren italienische Mathematiker des 16. Jahrhunderts erfolgreich. Für $n \geq 5$ stand man dann etwa 300 Jahre lang an, bis Abel und Galois in der ersten Hälfte des 19. Jahrhunderts zeigten, dass und warum genau es für Gleichungen vom Grad ≥ 5 keine allgemeine Formel der gesuchten Art geben kann. Wir beginnen in 9.5.1 mit der Präzisierung des Problems und der Definition der dafür hilfreichen Begriffe, insbesondere des Begriffs der radikalen Erweiterung. Eine besondere Rolle spielt bei Radikalen die Adjunktion sogenannter reiner Wurzeln, d.h. Lösungen von Gleichungen der Gestalt $x^n - a = 0$. Einige wichtige Aussagen dazu werden in 9.5.2 hergeleitet. Auf ihnen basiert der Beweis, dass radikale Erweiterungen stets auflösbare Galoisgruppen haben, siehe 9.5.3. Der Rest des Kapitels zielt auf den Beweis des Satzes von Galois ab, der auch die Umkehrung enthält: Ist die Galoisgruppe einer Gleichung auflösbar, so ist auch die Gleichung durch Radikale auflösbar. In 9.5.4 betrachten wir mit Norm und Spur zwei wesentliche Hilfsmittel, ehe wir in 9.5.5 die Ergebnisse aus 9.5.2 erweitern. Damit wird der Beweis der gerade angeführten Umkehrung möglich, siehe 9.5.6. In 9.5.7 fassen wir die Ergebnisse schließlich zusammen und formulieren den Satz von Galois.

9.5.1 Problemanalyse

Gesucht ist eine Darstellung der Lösungen von

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 = 0$$

als Funktionen der Koeffizienten unter Einbeziehung von Grundrechnungsarten und „Radikalen“ $\sqrt[k]{c}$, d.h. von Lösungen von Gleichungen der Form $x^k - c = 0$. Derart dargestellte Elemente liegen also in einem Erweiterungskörper E von K mit $K = Z_0 \leq \ldots \leq Z_m = E$ wobei $Z_{i+1} = Z_i(u_i)$ und $u_i^{k_i} - c_i = 0$, $c_i \in Z_i$. Für $\operatorname{char} K = 0$ erweist sich die „Auflösbarkeit“ in diesem Sinn als äquivalent zur Auflösbarkeit der Galoisgruppe von f im gruppentheoretischen Sinn (Satz von Galois 9.5.7.1).

Definition 9.5.1.1. E heißt *radikale Erweiterung* von K, falls Elemente $u_1, \ldots, u_m \in E$ existieren, sodass $E = K(u_1, \ldots, u_m)$ und es für jedes $i = 1, \ldots, m$ eine natürliche Zahl $k_i > 0$ gibt mit $\operatorname{char} K \nmid k_i$ und $u_i^{k_i} \in K(u_1, \ldots, u_{i-1})$.
(Für $\operatorname{char} K = 0$ ist die Bedingung $\operatorname{char} K \nmid k_i$ trivialerweise erfüllt!)

Für $f \in K[x]$ heißt die Gleichung $f(x) = 0$ *auflösbar durch Radikale*, falls eine radikale Erweiterung E existiert mit $K \leq Z_f \leq E$, wobei Z_f der Zerfällungskörper von f über K ist.

Die Bedingung $\operatorname{char} K \nmid k_i$ hat folgenden Hintergrund: Wir werden benötigen, dass – zumindest unter einer Zusatzvoraussetzung an K – die Erweiterungen $K(u_1, \ldots, u_{i-1}) \leq K(u_1, \ldots, u_i)$ Galoissch (insbesondere separabel) sind, um galoistheoretische Methoden anwenden zu können. Das ist für $\operatorname{char} K \mid k_i$ problematisch; umgekehrt zeigt die folgende Aufgabe, dass wir unter der *Annahme* separabler Erweiterungen stets auf $\operatorname{char} K \nmid k_i$ reduzieren können.

UE 134 ► **Übungsaufgabe 9.5.1.2.** (F) Sei K ein Körper mit Charakteristik $p := \operatorname{char} K > 0$. Sei weiters $K \leq E$ eine separable Erweiterung und sei $u \in E$ mit $u^{mp^j} \in K$, wobei $p \nmid m$ und $j \geq 1$. Zeigen Sie, dass $u^m \in K$.
Hinweis: Betrachten Sie das Minimalpolynom von u^m über K. ◄ **UE 134**

Unmittelbar aus der Definition folgt:

Lemma 9.5.1.3. *Jede radikale Erweiterung ist endlichdimensional.*

UE 135 ► **Übungsaufgabe 9.5.1.4.** (V) Beweisen Sie Lemma 9.5.1.3. ◄ **UE 135**

Wir werden später benötigen, dass Radikalität mit dem Bilden des normalen Abschlusses verträglich ist.

Lemma 9.5.1.5. *Sei $K \leq E$ eine radikale Erweiterung und sei N der normale Abschluss von E. Dann ist auch $K \leq N$ eine radikale Erweiterung.*

UE 136 ► **Übungsaufgabe 9.5.1.6.** (V) Beweisen Sie Lemma 9.5.1.5. ◄ **UE 136**
Hinweis: Verwenden Sie Proposition 9.2.3.7.

Um zu zeigen, dass jede radikale Erweiterung eine auflösbare Galoisgruppe hat, werden wir uns zunächst überlegen, dass bei der Adjunktion einer einzigen reinen n-ten Wurzel, das heißt einer Nullstelle eines Polynoms f der Bauart $f(x) = x^n - a$, stets abelsche Galoisgruppen entstehen. Nach Definition setzen sich radikale Erweiterungen ausschließlich aus Adjunktionen reiner Wurzeln zusammen. Denken wir an die Galoiskorrespondenz aus dem Hauptsatz und an die Definition der Auflösbarkeit einer Gruppe über Subnormalreihen mit abelschen Faktoren, so scheint damit der Beweis im Wesentlichen schon erbracht. Obwohl bei genauerer Analyse der Situation noch einige weitere Komplikationen zu bedenken sind, kann man in diesen Überlegungen die wichtigsten Ideen für den gesuchten Beweis sehen. Es folgt nun die Ausführung des angedeuteten Programms.

9.5.2 Die Adjunktion reiner Wurzeln

Wir beginnen mit dem Spezialfall von Einheitswurzeln. Zur Erinnerung (siehe Unterabschnitt 6.2.5): Eine n-te Einheitswurzel ist eine Nullstelle des Polynoms $x^n - 1$. Im Zerfällungskörper von $x^n - 1$ bilden die Einheitswurzeln eine zyklische Untergruppe der multiplikativen Gruppe; jedes erzeugende Element nennt man eine *primitive* n-te Einheitswurzel. Außerdem wissen wir, dass die Zahl der n-ten Einheitswurzeln in $\mathbb{C}$ genau n ist. Dasselbe Argument lässt sich auf den Fall von positiver Charakteristik ausdehnen, solange n kein Vielfaches der Charakteristik ist:

Lemma 9.5.2.1. *Sei K ein Körper und sei $n \geq 1$ mit $\operatorname{char} K \nmid n$ (für $\operatorname{char} K = 0$ ist diese Bedingung trivialerweise erfüllt). Dann hat das Polynom $x^n - 1$ in seinem Zerfällungskörper Z über K genau n Nullstellen. Ist $\zeta \in Z$ eine primitive n-te Einheitswurzel, so sind $1 = \zeta^0, \zeta = \zeta^1, \zeta^2, \ldots, \zeta^{n-1}$ paarweise verschieden.*

UE 137 ▶ **Übungsaufgabe 9.5.2.2.** (V) Rekapitulieren Sie Unterabschnitt 6.2.5 und zeigen Sie Lemma 9.5.2.1. ◀ **UE 137**

Anmerkung 9.5.2.3. In der Literatur wird eine primitive n-te Einheitswurzel auch definiert als n-te Einheitswurzel der multiplikativen Ordnung n (und nicht wie bei uns als multiplikativer Erzeuger der n-ten Einheitswurzeln bzw. äquivalent als n-te Einheitswurzel von maximaler multiplikativer Ordnung). Lemma 9.5.2.1 besagt, dass es für $\operatorname{char} K \nmid n$ primitive n-te Einheitswurzeln gemäß der alternativen Definition *gibt* und dass dann die beiden Definitionen zusammenfallen.

Proposition 9.5.2.4. *Sei $K \leq E$ eine Körpererweiterung mit $\operatorname{char} K \nmid n$ und $\zeta \in E$ eine primitive n-te Einheitswurzel. Dann ist $Z := K(\zeta)$ ein Zerfällungskörper für das Polynom $f(x) := x^n - 1$. Die Erweiterung $K \leq Z = K(\zeta)$ ist Galoissch mit abelscher Galoisgruppe $\operatorname{Aut}_K(Z)$.*

Beweis. In jedem Zerfällungskörper Z_f des Polynoms $f(x) := x^n - 1$ bilden die n-ten Einheitswurzeln nach dem Obigen und Lemma 9.5.2.1 multiplikativ eine zyklische Untergruppe der Ordnung n, deren Erzeugende genau die primitiven n-ten Einheitswurzeln sind. Folglich ist $Z := K(\zeta)$ ein Zerfällungskörper von f innerhalb E, auf den wir uns nun beziehen wollen. Da nach Lemma 9.5.2.1 alle ζ^i, $i = 0, \ldots, n-1$, paarweise verschieden sind, ist $x^n - 1$ ein separables Polynom, sodass die Erweiterung $K \leq K(\zeta) = Z$ wegen Satz 9.2.5.5 Galoissch ist.
Jedes $\sigma \in \operatorname{Aut}_Z(K)$ bildet ζ wieder auf eine primitive Einheitswurzel ab, also auf ein ζ^i mit $i \in \mathbb{Z}_n^*$. Wegen $Z = K(\zeta)$ ist σ durch den Wert $\sigma(\zeta)$ eindeutig bestimmt, also durch die Angabe von i. Wir schreiben für dieses σ daher $\sigma = \sigma_i$. Entscheidend ist die Beziehung

$$\sigma_i \sigma_j(\zeta) = \sigma_i(\zeta^j) = \sigma_i(\zeta)^j = (\zeta^i)^j = \zeta^{ij} = \sigma_{ij}(\zeta),$$

aus der wir $\sigma_i \sigma_j = \sigma_{ij}$ ablesen. Weil ζ die multiplikative Ordnung n hat, dürfen wir das Produkt ij modulo n interpretieren. Somit ist die Abbildung

$$\iota : \operatorname{Aut}_K(Z) \to \mathbb{Z}_n^*, \quad \sigma_i \mapsto i,$$

eine isomorphe Einbettung der Galoisgruppe $\mathrm{Aut}_K(Z)$ in die prime Restklassengruppe $\mathbb{Z}_n^*$ (das ist die Einheitengruppe des multiplikativen Monoids von $\mathbb{Z}/n\mathbb{Z}$). Diese ist abelsch, also ist auch $\mathrm{Aut}_K(Z)$ abelsch. □

Bemerkung zum obigen Beweis: Jede primitive n-te Einheitswurzel ist Nullstelle des n-ten Kreisteilungspolynoms g_n über K (siehe Unterabschnitt 6.2.5). Dieses hat den Grad $\varphi(n) = |\mathbb{Z}_n^*|$ (Eulersche φ-Funktion). Über $K = \mathbb{Q}$ stellen sich sämtliche Kreisteilungspolynome als irreduzibel heraus – siehe Proposition 9.5.2.5. Da wir diese (nichttriviale) Aussage im Haupttext nicht benötigen, lagern wir den Beweis in eine Übungsaufgabe mit Anleitung aus. In diesem Fall sind also genau die n-ten primitiven Einheitswurzeln die Konjugierten von ζ. Folglich gibt es zu jedem $i \in \mathbb{Z}_n^*$ auch ein σ_i, d.h. die Einbettung ι ist sogar surjektiv und somit ein Isomorphismus $\mathrm{Aut}_{\mathbb{Q}}(Z) \cong \mathbb{Z}_n^*$.

Proposition 9.5.2.5. *Die Kreisteilungspolynome g_n über $\mathbb{Q}$ sind in $\mathbb{Q}[x]$ irreduzibel. Ist $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel und $Z = \mathbb{Q}(\zeta)$, so gilt $[Z : \mathbb{Q}] = \varphi(n)$ und $\mathrm{Aut}_{\mathbb{Q}}(Z) \cong \mathbb{Z}_n^*$.*

UE 138 ► Übungsaufgabe 9.5.2.6. (V) Beweisen Sie Proposition 9.5.2.5. **◄ UE 138**
Anleitung: Es genügt zu zeigen, dass das gemäß Satz 6.2.5.2 normierte und ganzzahlige Polynom g_n in $\mathbb{Z}[x]$ irreduzibel ist (siehe Lemma 5.3.2.5). Sei also $h \in \mathbb{Z}[x]$ ein normierter und irreduzibler Faktor von g_n, d.h. $g_n = fh$ für ein $f \in \mathbb{Z}[x]$. Zeigen Sie $h = g_n$ durch die folgenden Schritte:

- Sei p eine Primzahl, die n nicht teilt. Wenn ζ eine primitive n-te Einheitswurzel ist, die eine Nullstelle von h ist, dann ist ζ^p ebenfalls eine Nullstelle von h: Angenommen nicht. Zeigen Sie, dass $f(x^p) = h(x)k(x)$ für ein $k \in \mathbb{Z}[x]$. Seien $\bar{f}, \bar{h}, \bar{k}$ die von f, h, k durch Reduzieren der Koeffizienten modulo p induzierten Polynome in $\mathbb{Z}_p[x]$. Folgern Sie $\bar{f}(x)^p = \bar{h}(x)\bar{k}(x)$, schließen Sie, dass $\bar{g}_n$ und somit $x^n - 1 \in \mathbb{Z}_p[x]$ eine mehrfache Nullstelle hat, und leiten Sie einen Widerspruch her.
- Iterieren Sie den vorherigen Punkt, um zu zeigen, dass nicht nur ζ sondern alle primitiven n-ten Einheitswurzeln Nullstellen von h sind, und schließen Sie $g_n = h$.

Ist eine primitive n-te Einheitswurzel ζ (und damit alle n-ten Einheitswurzeln) im Grundkörper vorhanden, so haben Erweiterungen um weitere reine n-te Wurzeln aus galoistheoretischer Sicht eine besonders einfache Struktur:

Proposition 9.5.2.7. *Sei K ein Körper, sei* $\mathrm{char}\, K \nmid n$ *und sei $\zeta \in K$ eine primitive n-te Einheitswurzel. Weiters sei $K \leq E$ eine Körpererweiterung und $u \in E$ mit $u^n = a \in K$. Dann ist $Z = Z_f := K(u)$ ein Zerfällungskörper des Polynoms $f(x) := x^n - a$ über K und die Erweiterung $K \leq Z = K(u)$ ist Galoissch. Die Galoisgruppe $G(f) = \mathrm{Aut}_K(Z)$ von f ist zyklisch von einer Ordnung, die n teilt, insbesondere also abelsch.*

Beweis. Für i sind die Elemente $u_i := \zeta^i u$ nach Lemma 9.5.2.1 paarweise verschieden. Wegen $u_i^n = (\zeta^n)^i u^n = u^n = a$ sind die u_i allesamt n Nullstellen von f; aus Gradgründen

bilden sie bereits alle Nullstellen von f. Sie liegen alle in $K(\zeta, u) = K(\zeta)(u) = K(u)$, folglich ist $K(u) = Z$ bereits der Zerfällungskörper von $f(x) = x^n - a$. Da die Nullstellen paarweise verschieden sind, ist f separabel und $K \leq Z = K(u)$ nach Satz 9.2.5.5 Galoissch.
Nach Proposition 9.2.1.4 permutiert jedes $\sigma \in \mathrm{Aut}_K(Z) = \mathrm{Aut}_K(K(u))$ die u_i und ist durch den Wert $\sigma(u)$ beim Erzeuger u bereits eindeutig festgelegt. Folglich gibt es eine injektive Abbildung

$$\iota : \mathrm{Aut}_K(E) \to \{0, 1, \ldots, n-1\}, \quad \sigma \mapsto i_\sigma = \iota(\sigma) \quad \text{mit} \quad \sigma(u) = u_{i_\sigma} = \zeta^{i_\sigma} u.$$

Identifizieren wir die $i \in \{0, 1, \ldots n-1\}$ mit den additiven Restklassen modulo n, so ist $\iota : \mathrm{Aut}_K(E) \to C_n$ also eine Abbildung in die zyklische Gruppe der Ordnung n. Wegen

$$\sigma_1\sigma_2(u) = \sigma_1(\zeta^{i_{\sigma_2}} u) = \zeta^{i_{\sigma_2}} \sigma_1(u) = \zeta^{i_{\sigma_2}} \zeta^{i_{\sigma_1}} u = \zeta^{i_{\sigma_1} + i_{\sigma_2}} u,$$

also $\iota(\sigma_1\sigma_2) = \iota(\sigma_1) + \iota(\sigma_2) \mod n$, ist ι ein Homomorphismus, aufgrund der Injektivität daher sogar eine isomorphe Einbettung in die zyklische Gruppe C_n. $\mathrm{Aut}_K(E)$ ist daher isomorph zu einer Untergruppe von C_n, also eine zyklische Gruppe (Proposition 3.2.4.4) mit einer Ordnung, die n teilt. □

Die Propositionen 9.5.2.4 und 9.5.2.7 motivieren die folgende Definition:

Definition 9.5.2.8. Ist $K \leq E$ algebraisch und Galoissch, so heißt die Erweiterung *zyklisch* bzw. *abelsch*, falls die Automorphismengruppe $\mathrm{Aut}_K(E)$ zyklisch bzw. abelsch ist.

Wir haben also gezeigt:

1. Ist ζ eine primitive n-te Einheitswurzel mit $\mathrm{char}\, K \nmid n$, so ist $K \leq K(\zeta)$ eine abelsche Erweiterung.
2. Ist andererseits eine primitive n-te Einheitswurzel ζ bereits in K enthalten und $u^n = a \in K$, so ist $K \leq K(u)$ eine zyklische Erweiterung.

9.5.3 Radikale Erweiterungen haben auflösbare Galoisgruppen

Wir wollen nun zeigen: Die Galoisgruppe eines Polynoms f über $\mathbb{Q}$, dessen Nullstellen sich durch Radikale ausdrücken lassen, ist stets auflösbar im Sinn von Definition 8.3.2.1. Umgekehrt formuliert: Die Lösungen von Gleichungen $f(x) = 0$ mit einem Polynom $f \in \mathbb{Q}[x]$ mit nicht auflösbarer Galoisgruppe – wie etwa $f(x) = x^5 - 4x + 2$ über $K = \mathbb{Q}$ (siehe Übungsaufgabe 9.4.6.3) – lassen sich nicht durch Radikale im Sinn von Definition 9.5.1.1 darstellen. Diese Behauptung ist in folgendem Satz enthalten:

Satz 9.5.3.1. *Ist $K \leq E$ eine radikale Erweiterung, dann ist $\mathrm{Aut}_K(Z)$ für jeden Zwischenkörper Z, $K \leq Z \leq E$, auflösbar. Insbesondere ist eine algebraische Gleichung $f(x) = 0$ mit einem Polynom $f \in K[x]$ nur dann durch Radikale auflösbar, wenn die Galoisgruppe von f (= die Galoisgruppe des Zerfällungskörpers von f über K) auflösbar ist.*

Bevor wir zum Beweis kommen, betrachten wir zwei Spezialfälle, die einerseits die Beweisidee sehr transparent zeigen, und auf die wir andererseits die allgemeine Aussage zurückführen werden.

Lemma 9.5.3.2. *Sei $K \leq E$ eine Galoissche und radikale Erweiterung, bezeugt durch Elemente $u_1, \ldots, u_m$, sodass $E = K(u_1, \ldots, u_m)$ und $u_i^{k_i} \in K(u_1, \ldots, u_{i-1})$ für natürliche Zahlen k_i, die keine Vielfache von* $\operatorname{char} K$ *sind. Außerdem enthalte K primitive k_i-te Einheitswurzeln für alle $i = 1, \ldots, m$. Dann ist die Galoisgruppe* $\operatorname{Aut}_K(E)$ *auflösbar.*

Beweis. Wir setzen $Z_0 := K$ und $Z_i := Z_{i-1}(u_i)$ für $i = 1, \ldots, m$. Weil E Galoissch und endlichdimensional über K ist (siehe Lemma 9.5.1.3), liefert der Hauptsatz 9.3.1.1 gemäß $H_i := Z_i' = \operatorname{Aut}_{Z_i}(E)$ eine Zuordnung folgender Art:

$$\begin{array}{ccccccccccccc} K & = & Z_0 & \leq & \ldots & \leq & Z_{i-1} & \leq & Z_i & \leq & \ldots & \leq & Z_m & = & E \\ & & \updownarrow & & & & \updownarrow & & \updownarrow & & & & \updownarrow & & \\ \operatorname{Aut}_K(E) & = & H_0 & \geq & \ldots & \geq & H_{i-1} & \geq & H_i & \geq & \ldots & \geq & H_m & = & \{\mathrm{id}\} \end{array}$$

Laut Proposition 9.5.2.7 sind auch die Erweiterungen $Z_{i-1} \leq Z_i$ Galoissch, wobei die Gruppe $\operatorname{Aut}_{Z_{i-1}}(Z_i)$ zyklisch ist, insbesondere abelsch. Durch eine weitere Anwendung des Hauptsatzes 9.3.1.1 (für $K = Z_{i-1}$ und $Z = Z_i$) folgt daraus $H_i \lhd H_{i-1}$ und

$$H_{i-1}/H_i = \operatorname{Aut}_{Z_{i-1}}(E)/\operatorname{Aut}_{Z_i}(E) \cong \operatorname{Aut}_{Z_{i-1}}(Z_i)$$

Somit ist

$$\operatorname{Aut}_K(E) = H_0 \geq \ldots \geq H_{i-1} \geq H_i \geq \ldots \geq H_m = \{\mathrm{id}\}$$

eine auflösbare Subnormalreihe und $\operatorname{Aut}_K(E)$ nach Übungsaufgabe 8.3.3.3 auflösbar. □

Mit derselben Idee behandeln wir Erweiterungen um primitive Einheitswurzeln.

Lemma 9.5.3.3. *Sei $K \leq E$ eine Körpererweiterung, wobei $E = K(\zeta_1, \ldots, \zeta_m)$ für primitive k_i-te Einheitswurzeln ζ_i mit* $\operatorname{char} K \nmid k_i$. *Dann ist die Erweiterung $K \leq E$ Galoissch und die Galoisgruppe* $\operatorname{Aut}_K(E)$ *ist auflösbar.*

Beweis. Wegen Lemma 9.5.2.1 sind einerseits die Polynome $x^{k_i} - 1$ separabel und andererseits E der Zerfällungskörper von $\{x^{k_i} - 1 \mid i = 1, \ldots, m\}$ über K. Nach Satz 9.2.5.5 folgt daraus, dass $K \leq E$ Galoissch ist.
Für die Auflösbarkeit von $\operatorname{Aut}_K(E)$ gehen wir genauso vor wie in Lemma 9.5.3.2: Sei $Z_0 := K$ und $Z_i := Z_{i-1}(\zeta_i)$ für $i = 1, \ldots, m$. Der Hauptsatz 9.3.1.1 liefert gemäß $H_i := Z_i' = \operatorname{Aut}_{Z_i}(E)$ die folgende Zuordnung:

$$\begin{array}{ccccccccccccc} K & = & Z_0 & \leq & \ldots & \leq & Z_{i-1} & \leq & Z_i & \leq & \ldots & \leq & Z_m & = & E \\ & & \updownarrow & & & & \updownarrow & & \updownarrow & & & & \updownarrow & & \\ \operatorname{Aut}_K(E) & = & H_0 & \geq & \ldots & \geq & H_{i-1} & \geq & H_i & \geq & \ldots & \geq & H_m & = & \{\mathrm{id}\} \end{array}$$

Laut Proposition 9.5.2.4 sind auch die Erweiterungen $Z_{i-1} \leq Z_i$ Galoissch, wobei die Gruppe $\mathrm{Aut}_{Z_{i-1}}(Z_i)$ abelsch ist. Daraus folgt $H_i \lhd H_{i-1}$ und

$$H_{i-1}/H_i = \mathrm{Aut}_{Z_{i-1}}(E)/\mathrm{Aut}_{Z_i}(E) \cong \mathrm{Aut}_{Z_{i-1}}(Z_i)$$

Wir erhalten die auflösbare Subnormalreihe

$$\mathrm{Aut}_K(E) = H_0 \geq \ldots \geq H_{i-1} \geq H_i \geq \ldots \geq H_m = \{\mathrm{id}\},$$

womit $\mathrm{Aut}_K(E)$ nach Übungsaufgabe 8.3.3.3 auflösbar ist. □

Um Satz 9.5.3.1 zu beweisen, werden wir eine gegebene radikale Erweiterung $K \leq E$ durch Vergrößern des Grundkörpers in eine Galoissche und radikale Erweiterung $K_1 \leq E$ verwandeln und zeigen, dass diese Konstruktion mit der Auflösbarkeit verträglich ist. Anschließend haben wir dieses Resultat auf Zwischenkörper Z, $K \leq Z \leq E$ auszudehnen.

Lemma 9.5.3.4. *Ist $K \leq E$ eine radikale Erweiterung, dann gibt es einen Körper K_1 mit $K \leq K_1 \leq E$, sodass $K_1 \leq E$ eine Galoissche und radikale Erweiterung ist und sodass $\mathrm{Aut}_{K_1}(E) = \mathrm{Aut}_K(E)$.*

Beweis. Wir setzen $K_1 := K'' = \mathrm{Aut}_K(E)'$, den Fixpunktkörper von $\mathrm{Aut}_K(E)$. Nach Proposition 9.2.1.2 ist $K_1 \leq E$ eine Galoissche Erweiterung mit $\mathrm{Aut}_{K_1}(E) = \mathrm{Aut}_K(E)$. Nach Voraussetzung ist $K \leq E$ eine radikale Erweiterung, bezeugt durch $u_1, \ldots, u_m$. Offensichtlich bezeugen dieselben Elemente, dass auch $K_1 \leq E$ eine radikale Erweiterung ist. □

Lemma 9.5.3.5. *Sei $K \leq E$ eine algebraische und normale Erweiterung, sodass $\mathrm{Aut}_K(E)$ auflösbar ist. Dann ist für jeden Zwischenkörper Z, $K \leq Z \leq E$, auch die Gruppe $\mathrm{Aut}_K(Z)$ auflösbar.*

Beweis. Wegen der Normalität von $K \leq E$ ist E ein Zerfällungskörper über K und somit auch über Z. Daher lässt sich jedes $\sigma_0 \in \mathrm{Aut}_K(Z)$ zu einem K-Automorphismus $\sigma \in \mathrm{Aut}_K(E)$ fortsetzen (siehe Satz 6.2.3.1), der notwendig Z als Menge fest lässt. Derartige σ bilden eine Untergruppe $H_Z \leq \mathrm{Aut}_K(E)$. Somit ist die Einschränkungsabbildung $\varphi : H_Z \to \mathrm{Aut}_K(Z)$, $\sigma \mapsto \sigma|_Z$ ein surjektiver Homomorphismus. Mit anderen Worten: $\mathrm{Aut}_K(Z)$ ist das homomorphe Bild einer Untergruppe der auflösbaren Gruppe $\mathrm{Aut}_K(E)$, nach Proposition 8.3.2.4 also selbst auflösbar. □

Mit diesen Vorarbeiten können wir jetzt Satz 9.5.3.1 zeigen. Die wesentliche noch zu überwindende Hürde ist das Hinzufügen von passenden primitiven Einheitswurzeln.

Beweis (von Satz 9.5.3.1). Bezeichnen wir den normalen Abschluss von E mit N, so ist $K \leq N$ wegen Lemma 9.5.1.5 ebenfalls eine radikale Erweiterung. Nach Lemma 9.5.3.4 existiert ein K_1 mit $K \leq K_1 \leq N$, sodass $K_1 \leq N$ Galoissch und radikal ist und sodass $\mathrm{Aut}_{K_1}(N) = \mathrm{Aut}_K(N)$. Gemäß Satz 9.2.5.5 gibt es eine Menge $S \subseteq K_1[x]$ separabler Polynome, sodass N der Zerfällungskörper von S über K_1 ist. Wegen der Radikalität existieren $u_1, \ldots, u_m \in N$ mit $N = K_1(u_1, \ldots, u_m)$ und $u_i^{k_i} \in K_1(u_1, \ldots, u_{i-1})$ für

$i = 1, \ldots, m$, wobei $\operatorname{char} K_1 \nmid k_i$. Nach Lemma 9.5.2.1 sind die Polynome $x^{k_i} - 1$ separabel, womit umgekehrt jeder Zerfällungskörper L von $S \cup \{x^{k_i} - 1 \mid i = 1, \ldots, m\}$ über K_1 erneut wegen Satz 9.2.5.5 Galoissch über K_1 ist; man beachte, dass es einen solchen Zerfällungskörper gibt, der N erweitert. Bezeichne $\zeta_i \in L$ eine primitive k_i-te Einheitswurzel. Nach dem Hauptsatz 9.3.1.1 ist auch $K_{adj} := K_1(\zeta_1, \ldots, \zeta_m) \leq L$ eine Galoissche Erweiterung. Dabei gilt $L = K_{adj}(u_1, \ldots, u_m)$, wobei $u_i^{k_i} \in K_{adj}(u_1, \ldots, u_{i-1})$. Aus dem Spezialfall in Lemma 9.5.3.2 folgt somit, dass $\operatorname{Aut}_{K_{adj}}(L)$ eine auflösbare Gruppe ist. Andererseits erhalten wir aus Lemma 9.5.3.3, dass $K_{adj} = K_1(\zeta_1, \ldots, \zeta_m)$ über K_1 Galoissch ist mit auflösbarer Galoisgruppe $\operatorname{Aut}_{K_1}(K_{adj})$. Erstere Tatsache liefert wieder nach dem Hauptsatz 9.3.1.1, dass $\operatorname{Aut}_{K_{adj}}(L)$ ein Normalteiler in $\operatorname{Aut}_{K_1}(L)$ ist, wobei

$$\operatorname{Aut}_{K_1}(L)/\operatorname{Aut}_{K_{adj}}(L) \cong \operatorname{Aut}_{K_1}(K_{adj}).$$

Folglich haben wir in $\operatorname{Aut}_{K_1}(L)$ einen Normalteiler gefunden, der einerseits auflösbar ist und sodass andererseits die Faktorgruppe nach diesem Normalteiler ebenfalls auflösbar ist. Nach Proposition 8.3.2.4 ist damit $\operatorname{Aut}_{K_1}(L)$ auflösbar. Gemäß Lemma 9.5.3.5 ist auch $\operatorname{Aut}_{K_1}(Z_1)$ für jeden Zwischenkörper $K_1 \leq Z_1 \leq L$ auflösbar, insbesondere $\operatorname{Aut}_{K_1}(N) = \operatorname{Aut}_K(N)$. Eine weitere Anwendung von Lemma 9.5.3.5 (diesmal auf $K \leq N$) liefert, dass auch $\operatorname{Aut}_K(Z)$ für jeden Zwischenkörper $K \leq Z \leq N$, insbesondere $K \leq Z \leq E$, auflösbar ist.

□

Anmerkung 9.5.3.6. Tatsächlich gilt im letzten Beweis $K_1 = K$, mit anderen Worten ist $K \leq N$ bereits Galoissch und radikal. Das folgt daraus, dass eine radikale Erweiterung stets separabel ist, wie man mit der folgenden Aussage (die sich als Verallgemeinerung von Folgerung 9.2.5.6 auffassen lässt) beweisen kann: Sind $K \leq L$ und $L \leq M$ separable Erweiterungen, so ist auch $K \leq M$ eine separable Erweiterung. Ihr Beweis erfordert aber einigen Aufwand; da wir die Aussage nicht mehr benötigen werden, begnügen wir uns mit dieser Andeutung sowie der folgenden Übungsaufgabe.

Wenn wir mit einer radikalen und zusätzlich Galoisschen Erweiterung starten können, lohnt sich ein weiterer Blick auf den letzten Beweis – in diesem Fall kann man das Resultat nämlich etwas direkter und ohne Rückgriff auf Proposition 8.3.2.4 erhalten.

UE 139 ► **Übungsaufgabe 9.5.3.7.** (A) Sei $K \leq E$ eine Galoissche und radikale Erweiterung, bezeugt durch Elemente $u_1, \ldots, u_m$, sodass $E = K(u_1, \ldots, u_m)$ und $u_i^{k_i} \in K(u_1, \ldots, u_{i-1})$ für natürliche Zahlen k_i, die keine Vielfache von $\operatorname{char} K$ sind. Sei L der Zerfällungskörper der Polynome $x^{k_i} - 1$, $i = 1, \ldots, m$, über E. Rekapitulieren Sie den Beweis von Satz 9.5.3.1 und geben Sie eine auflösbare Subnormalreihe von $\operatorname{Aut}_K(L)$ an. ◄ **UE 139**

Wir erinnern uns nochmals an Übungsaufgabe 9.4.6.4 (wonach die allgemeine Gleichung n-ten Grades eine zu S_n isomorphe Galoisgruppe hat) sowie die der Aufgabe vorangehende Diskussion und resümieren:

Folgerung 9.5.3.8 (Satz von Abel)**.** *Es gibt keine allgemeine Lösungsformel für algebraische Gleichungen vom Grad* ≥ 5.

In Umgekehrung von Satz 9.5.3.1 kann man unter geeigneten Bedingungen von der Auflösbarkeit der Galoisgruppe auf die Auflösbarkeit der entsprechenden Gleichung durch Radikale schließen (siehe Satz 9.5.7.1 von Galois). Das wesentliche Instrument ist eine Umkehrung von Proposition 9.5.2.7, die uns erlauben wird, von zyklischen Galoisgruppen auf Erweiterungen um Wurzeln zu schließen. Der Beweis dafür ist aber aufwendiger und erfordert einige weitere Begriffsbildungen, denen wir uns nun zuwenden.

9.5.4 Norm und Spur

Definition 9.5.4.1. Sei $K \leq E$ eine endlichdimensionale und separable Erweiterung und sei $\overline{K}^{\text{alg}}$ ein algebraischer Abschluss von K mit $E \leq \overline{K}^{\text{alg}}$. Seien $\sigma_1, \ldots, \sigma_r$ sämtliche K-Monomorphismen von E nach $\overline{K}^{\text{alg}}$ (es gibt nur endlich viele, da ein K-Monomorphismus durch seine Bilder auf der endlichen Basis bestimmt ist und für jedes Element nur endlich viele Bilder infrage kommen, nämlich seine Konjugierten). Für $u \in E$ heißt

$$N(u) = N_K^E(u) := \prod_{j=1}^{r} \sigma_j(u)$$

die *Norm* von u über K und

$$T(u) = T_K^E(u) := \sum_{j=1}^{r} \sigma_j(u)$$

die *Spur* von u.

Wir wollen uns auf Galoissche Erweiterungen konzentrieren. Sei also $K \leq E$ Galoissch und $\text{Aut}_K(E) = \{\sigma_1, \ldots, \sigma_r\}$. Man beachte, dass nach Satz 9.2.3.2(iii) die Monomorphismen von E nach $\overline{K}^{alg}$ genau die Elemente von $\text{Aut}_K(E)$ sind. Für alle $\sigma \in \text{Aut}_K(E)$ gilt

$$\sigma(N_K^E(u)) = \prod_{j=1}^{r} \sigma(\sigma_j(u)) = \prod_{j=1}^{r} \sigma_j(u) = N_K^E(u)$$

und analog $\sigma(T_K^E(u)) = T_K^E(u)$. Es folgt:

Lemma 9.5.4.2. *Sei $K \leq E$ eine endlichdimensionale und Galoissche Erweiterung. Dann gilt*

(a) $N_K^E(u) \in (\text{Aut}_K(E))' = K$. Analog folgt $T_K^E(u) \in K$.

(b) $N_K^E(u \cdot v) = N_K^E(u) \cdot N_K^E(v)$, $T_K^E(u + v) = T_K^E(u) + T_K^E(v)$.

(c) Ist $u \in K$, so folgt $N_K^E(u) = u^{[E:K]}$ und $T_K^E(u) = [E : K] \cdot u$.

Beispiel 9.5.4.3. Ist $K = \mathbb{R}$ und $E = \mathbb{C}$, so sind Norm und Spur gegeben durch

$$N(u) = u \cdot \overline{u} = |u|^2 \text{ und } T(u) = u + \overline{u} = 2 \cdot \text{Re}(u).$$

Bevor wir zum Hauptresultat dieses Abschnitts kommen, benötigen wir noch eine Hilfsaussage.

Lemma 9.5.4.4 (Artin-Lemma)**.** *Jede Menge paarweise verschiedener Automorphismen eines Körpers K, betrachtet als Elemente des K-Vektorraumes K^K, ist linear unabhängig.*

Beweis. Angenommen, die Aussage ist falsch. Sei n die minimale Anzahl, sodass es linear abhängige Automorphismen $\sigma_1, \ldots, \sigma_n$ gilt und sei

$$\sum_{i=1}^{n} a_i \sigma_i = 0 \tag{9.3}$$

mit $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$. Wegen der Minimalität von n gilt $a_1, \ldots, a_n \neq 0$. Dann gibt es ein v mit $\sigma_1(v) \neq \sigma_2(v)$. Aus (9.3) angewendet auf $u \cdot v$ für ein beliebiges $u \in K$ folgt

$$0 = \sum_{i=1}^{n} a_i \sigma_i(u \cdot v) = \sum_{i=1}^{n} a_i (\sigma_i(u) \cdot \sigma_i(v)).$$

Wenden wir andererseits (9.3) auf u an und multiplizieren mit $\sigma_1(v)$, so erhalten wir

$$0 = \sum_{i=1}^{n} a_i \sigma_i(u) \sigma_1(v).$$

Zieht man diese beiden Gleichungen voneinander ab, ergibt sich

$$0 = \sum_{i=2}^{n} a_i \underbrace{(\sigma_i(v) - \sigma_1(v))}_{=:b_i} \cdot \sigma_i(u)$$

für alle $u \in K$. Das heißt aber

$$\sum_{i=2}^{n} a_i b_i \sigma_i = 0$$

mit $a_2 b_2 \neq 0$, was ein Widerspruch zur Minimalität von n ist. □

Anmerkung 9.5.4.5. Man beachte die Ähnlichkeiten des letzten Beweises mit dem Beweis von Lemma 9.3.2.2.

Satz 9.5.4.6 (Hilbert 90[3])**.** *Sei $K \leq E$ Galoissch und $\mathrm{Aut}_K(E) \cong C_n$ zyklisch mit Erzeuger σ. Für $u \in E$ gilt*

$$\textit{(multiplikative Fassung)} \quad N_K^E(u) = 1 \iff \exists v \in E^* = E \setminus \{0\} : u = v\sigma(v)^{-1}$$
$$\textit{(additive Fassung)} \quad T_K^E(u) = 0 \iff \exists v \in E : u = v - \sigma(v).$$

[3]Der Name dieses Satzes bezieht sich auf die Nummerierung in Hilberts berühmtem *Zahlbericht* aus dem Jahre 1897.

Beweis. Wir beweisen hier nur die erste Aussage; der ähnliche Beweis der zweiten Aussage bleibt einer Übungsaufgabe vorbehalten.
Da σ ein Erzeuger der Automorphismengruppe ist, gilt

$$N_K^E(u) = \prod_{j=0}^{n-1} \sigma^j(u) = u\sigma(u)\sigma^2(u) \cdot \ldots \cdot \sigma^{n-1}(u).$$

Angenommen, es existiert ein $v \in E^*$ mit $u = v\sigma(v)^{-1}$. Dann ist (Teleskopprodukt)

$$\begin{aligned} N_K^E(u) &= \prod_{j=0}^{n-1} \sigma^j(v\sigma(v)^{-1}) = \\ &= (v\sigma(v)^{-1})(\sigma(v)\sigma^2(v)^{-1})(\sigma^2(v)\sigma^3(v)^{-1}) \ldots (\sigma^{n-1}(v)\sigma^n(v)^{-1}) = \\ &= v \underbrace{\sigma(v)^{-1}\sigma(v)}_{=1} \sigma^2(v)^{-1} \cdot \ldots \cdot \sigma^{n-2}(v) \underbrace{\sigma^{n-1}(v)^{-1}\sigma^{n-1}(v)}_{=1} \underbrace{\sigma^n(v)^{-1}}_{=v^{-1}} \\ &= 1 \end{aligned}$$

Sei nun umgekehrt $N_K^E(u) = 1$. Dann ist $u \neq 0$, folglich $a_j := \prod_{i=0}^{j} \sigma^i(u) \neq 0$ für $j = 0, \ldots, n-1$. Nach dem Artin-Lemma 9.5.4.4 gibt es ein $y \in E$, sodass

$$v := \sum_{j=0}^{n-1} a_j \sigma^j(y) = \sum_{j=0}^{n-1} \left(\prod_{i=0}^{j} \sigma^i(u) \right) \sigma^j(y) \neq 0.$$

Man rechnet nach, dass $\sigma(a_j) = \prod_{i=1}^{j+1} \sigma^i(u) = u^{-1}a_{j+1}$ für $j = 1, \ldots, n-2$ und

$$\sigma(a_{n-1}) = \prod_{i=1}^{n} \sigma^i(u) = \prod_{i=0}^{n-1} \sigma^i(u) = N_K^E(u) = 1 = u^{-1}u = u^{-1}a_0$$

gilt. Daraus folgt $\sigma(v) = u^{-1}v$, mit anderen Worten $u = v\sigma(v)^{-1}$. □

UE 140 ► **Übungsaufgabe 9.5.4.7.** (V) Beweisen Sie die additive Fassung von Satz 9.5.4.6 ◄ **UE 140**
(Hilbert 90).
Hinweis: Zeigen Sie zunächst, dass es ein $y \in E$ gibt mit $T_K^E(y) \neq 0$. Definieren Sie geeignete a_j, $j = 0, \ldots, n-1$, und betrachten Sie v mit $v \cdot T_K^E(y) = \sum_{j=0}^{n-1} a_j \sigma^j(y)$.

9.5.5 Nochmal reine Wurzeln

Wir kommen zur angekündigten Erweiterung von Proposition 9.5.2.7; die Implikation von (ii) auf (iii) ist dabei die entscheidende Aussage, wenn wir zeigen wollen, dass eine auflösbare Galoisgruppe eine radikale Erweiterung nach sich zieht.

Satz 9.5.5.1. *Sei $\zeta \in K$ eine primitive n-te Einheitswurzel, wobei* $\operatorname{char} K \nmid n$*, und $K \leq E$ eine Körpererweiterung. Dann sind die folgenden Aussagen äquivalent:*

(i) *E ist Zerfällungskörper von $f(x) = x^n - a \in K[x]$. (In diesem Fall ist $E = K(u)$ für jedes u mit $f(u) = 0$.)*

(ii) *$K \leq E$ ist zyklisch von einem Grad d mit $d \mid n$.*

(iii) *E ist Zerfällungskörper eines irreduziblen Polynoms der Gestalt $f(x) = x^d - b \in K[x]$ mit $d \mid n$. (In diesem Fall ist $E = K(v)$ für jedes v mit $f(v) = 0$.)*

Beweis. (i) $\Rightarrow$ (ii): Das ist genau Proposition 9.5.2.7.
(ii) $\Rightarrow$ (iii): Sei σ ein Erzeuger von $\mathrm{Aut}_K(E)$ der Ordnung d. Offenbar ist $\eta := \zeta^{\frac{n}{d}}$ eine primitive d-te Einheitswurzel. Da ζ ein Element von K ist, gilt $\sigma(\eta) = \eta$ für alle $\sigma \in \mathrm{Aut}_K(E)$. Daher ist

$$N_K^E(\eta) = \eta^{[E:K]} = \eta^d = 1.$$

Nach Satz 9.5.4.6 (Hilbert 90) in der multiplikativen Fassung (man beachte, dass $K \leq E$ als zyklische Erweiterung per definitionem Galoissch ist) gibt es ein $u \in E \setminus \{0\}$ mit $\eta = u\sigma(u)^{-1}$. Sei $v := u^{-1}$, dann ist

$$\sigma(v) = \sigma(u)^{-1} = \eta u^{-1} = \eta v,$$

und deshalb für $b := v^d$

$$\sigma(b) = (\eta v)^d = \eta^d v^d = v^d = b.$$

Somit erhalten wir $b \in \langle\sigma\rangle' = \mathrm{Aut}_K(E)' = K$. Es folgt, dass v eine Wurzel des Polynoms $f(x) := x^d - b \in K[x]$ ist. Wir wollen noch zeigen, dass f irreduzibel ist, oder äquivalent dass f das Minimalpolynom von v ist. Klarerweise ist f ein Vielfaches des Minimalpolynoms. Andererseits sind die paarweise verschiedenen Elemente $\eta^i v$, $i = 0, \ldots, d-1$, Nullstellen des Minimalpolynoms von v über K, da sie Bilder von v unter K-Automorphismen sind. Somit kann der Grad des Minimalpolynoms nicht kleiner als $d = \operatorname{grad} f$ sein, woraus unsere Behauptung folgt.
Schließlich folgt

$$[E : K] = |\,\mathrm{Aut}_K(E)| = d = \operatorname{grad} f = [K(v) : K]$$

und daraus $K(v) = E$.
(iii) $\Rightarrow$ (i): Ist v eine Wurzel von $x^d - b \in K[x]$, dann gilt $E = K(v)$ nach Proposition 9.5.2.7 (bzw. (i)), weil K die primitive d-te Einheitswurzel $\zeta^{\frac{n}{d}}$ enthält. Nun ist

$$v^n = v^{d\frac{n}{d}} = b^{\frac{n}{d}} \in K,$$

daher ist v eine Wurzel von $x^n - a \in K[x]$, wobei $a := b^{\frac{n}{d}}$. Wegen $\zeta \in K$ ist $E = K(v)$ nach Proposition 9.5.2.7 (bzw. (i)) der Zerfällungskörper von $x^n - a$. □

9.5.6 Auflösbare Galoisgruppen erzwingen Auflösbarkeit durch Radikale

Unser Ziel in diesem Unterabschnitt ist der folgende Satz:

Satz 9.5.6.1. *Sei $K \leq Z$ eine endlichdimensionale und Galoissche Erweiterung mit auflösbarer Galoisgruppe* $\mathrm{Aut}_K(Z)$ *und sei* $\mathrm{char}(K) \nmid [Z : K]$.
Dann existiert ein Erweiterungskörper $E \geq Z$, sodass $K \leq E$ eine radikale Erweiterung ist.

Wie schon in Unterabschnitt 9.5.3 beginnen wir mit einem Spezialfall, in dem die Beweisidee sehr transparent zum Ausdruck kommt, und leiten daraus dann die allgemeine Aussage her.

Lemma 9.5.6.2. *Sei $K \leq E$ eine endlichdimensionale und Galoissche Erweiterung mit auflösbarer Galoisgruppe* $\mathrm{Aut}_K(E)$ *und sei* $\mathrm{char}(K) \nmid [E : K] =: n$. *Außerdem enthalte K eine primitive n-te Einheitswurzel.*
Dann ist $K \leq E$ eine radikale Erweiterung.

Beweis. Da $\mathrm{Aut}_K(E)$ auflösbar ist, gibt es nach Übungsaufgabe 8.3.3.3 eine Kompositionsreihe von $\mathrm{Aut}_K(E)$, deren Faktoren zyklische Gruppen von Primordnung sind, also

$$\mathrm{Aut}_K(E) = H_0 \rhd \ldots \rhd H_{i-1} \rhd H_i \rhd \ldots \rhd H_m = \{\mathrm{id}\},$$

wobei $H_{i-1}/H_i \cong C_{p_i}$ mit $p_i \in \mathbb{P}$ für alle $i = 1, \ldots, m$. Dabei gilt $p_i \mid n$, insbesondere $p_i \neq \mathrm{char}(K)$. Der Hauptsatz 9.3.1.1 liefert gemäß $Z_i := H_i'$ die folgende Zuordnung:

$$\begin{array}{ccccccccccccccc}
\mathrm{Aut}_K(E) & = & H_0 & \rhd & \ldots & \rhd & H_{i-1} & \rhd & H_i & \rhd & \ldots & \rhd & H_m & = & \{\mathrm{id}\} \\
 & & \updownarrow & & & & \updownarrow & & \updownarrow & & & & \updownarrow & & \\
K & = & Z_0 & \leq & \ldots & \leq & Z_{i-1} & \leq & Z_i & \leq & \ldots & \leq & Z_m & = & E
\end{array}$$

Somit ist $H_i = Z_i' = \mathrm{Aut}_{Z_i}(E)$ ein Normalteiler in $H_{i-1} = Z_{i-1}' = \mathrm{Aut}_{Z_{i-1}}(E)$. Durch eine weitere Anwendung des Hauptsatzes 9.3.1.1 (für $K = Z_{i-1}$ und $Z = Z_i$) folgt daraus, dass die Erweiterung $Z_{i-1} \leq Z_i$ Galoissch ist mit Galoisgruppe

$$\mathrm{Aut}_{Z_{i-1}}(Z_i) \cong \mathrm{Aut}_{Z_{i-1}}(E)/\mathrm{Aut}_{Z_i}(E) = H_{i-1}/H_i \cong C_{p_i}.$$

Anders formuliert ist $Z_{i-1} \leq Z_i$ eine zyklische Erweiterung vom Grad p_i. Wegen $p_i \mid n$ enthält K und insbesondere Z_{i-1} auch eine primitive p_i-te Einheitswurzel (nämlich $\zeta^{\frac{n}{p_i}}$, wenn $\zeta \in K$ eine primitive n-te Einheitswurzel bezeichnet). Nach Satz 9.5.5.1 (für $K = Z_{i-1}$ und $E = Z_i$) ist Z_i der Zerfällungskörper eines irreduziblen Polynoms der Gestalt $x^{p_i} - b_i \in Z_{i-1}[x]$, wobei $Z_i = Z_{i-1}(u_i)$ für irgendein u_i mit $u_i^{p_i} = b_i \in Z_{i-1}$ gilt. Da $\mathrm{char}(K) \nmid p_i$, bezeugen die Elemente $u_1, \ldots, u_m$, dass $E = Z_m = K(u_1, \ldots, u_m)$ eine radikale Erweiterung ist. □

Damit können wir jetzt Satz 9.5.6.1 zeigen. Im Wesentlichen müssen wir dazu nur eine passende primitive Einheitswurzel hinzufügen und nachprüfen, dass wir Lemma 9.5.6.2 anwenden können.

Beweis (von Satz 9.5.6.1). Wir setzen $n := [Z : K]$. Nach Satz 9.2.5.5 gibt es eine Menge $S \subseteq K[x]$ separabler Polynome, sodass Z der Zerfällungskörper von S über K ist. Wegen der Voraussetzung $\mathrm{char}(K) \nmid n$ ist das Polynom $x^n - 1$ separabel, womit umgekehrt jeder Zerfällungskörper E von $S \cup \{x^n - 1\}$ über K erneut wegen Satz 9.2.5.5 Galoissch über K ist; man beachte, dass es einen solchen Zerfällungskörper gibt, der Z erweitert. Sei $\zeta \in E$ eine primitive n-te Einheitswurzel und setze $K_{adj} := K(\zeta)$. Nach dem Hauptsatz 9.3.1.1 ist auch $K_{adj} \leq E$ eine Galoissche Erweiterung.
Wir behaupten, dass Lemma 9.5.6.2 auf die Erweiterung $K_{adj} \leq E$ anwendbar ist. Aus Lemma 9.3.3.2 folgt, dass Z stabil bzgl. K und E ist und dass die Abbildung $\varphi\colon \mathrm{Aut}_K(E) \to \mathrm{Aut}_K(Z)$, $\varphi(\sigma) := \sigma|_Z$, ein wohldefinierter Homomorphismus ist, somit auch die Einschränkung

$$\theta := \varphi|_{\mathrm{Aut}_{K_{adj}}(E)}\colon \mathrm{Aut}_{K_{adj}}(E) \to \mathrm{Aut}_K(Z), \qquad \theta(\sigma) := \sigma|_Z.$$

Dabei ist θ injektiv, denn aus $\sigma|_Z = \theta(\sigma) = \mathrm{id}_Z$ für ein $\sigma \in \mathrm{Aut}_{K_{adj}}(E)$ folgt $\sigma|_{Z\cup\{\zeta\}} = \mathrm{id}_{Z\cup\{\zeta\}}$ und somit wegen $E = Z(\zeta)$ bereits $\sigma = \mathrm{id}_E$. Wir erhalten, dass $\mathrm{Aut}_{K_{adj}}(E)$ zu einer Untergruppe von $\mathrm{Aut}_K(Z)$ isomorph ist. Daraus schließen wir zweierlei: Einerseits ist $\mathrm{Aut}_{K_{adj}}(E)$ nach Proposition 8.3.2.4 auflösbar, andererseits ist $n_{adj} := [E : K_{adj}] = |\mathrm{Aut}_{K_{adj}}(E)|$ nach dem Satz von Lagrange ein Teiler von $|\mathrm{Aut}_K(Z)| = [Z : K] = n$. Insbesondere enthält K_{adj} eine primitive n_{adj}-te Einheitswurzel.
Aus dem Spezialfall in Lemma 9.5.6.2 folgt somit, dass $K_{adj} \leq E$ eine radikale Erweiterung ist, bezeugt durch Elemente $u_1, \ldots, u_m$. Da $K \leq K_{adj} = K(\zeta)$ ebenfalls eine radikale Erweiterung ist (hier geht nochmal $\mathrm{char}(K) \nmid n$ ein), erhalten wir, dass $K \leq E$ eine radikale Erweiterung ist, bezeugt durch die Elemente $\zeta, u_1, \ldots, u_m$. □

9.5.7 Zusammenfassung: Der Satz von Galois

Satz 9.5.7.1 (Satz von Galois)**.** *Sei K ein Körper und $f \in K[x]$ so, dass der Zerfällungskörper Z_f von f über K separabel ist (dies ist insbesondere dann der Fall, wenn entweder* $\mathrm{char}(K) = 0$ *oder K endlich ist). Wenn* $\mathrm{char}\, K > 0$*, so sei außerdem* $\mathrm{grad}\, f < \mathrm{char}\, K$*. Dann gilt: Die Gleichung $f(x) = 0$ lässt sich genau dann durch Radikale auflösen, wenn die Galoisgruppe $G(f)$ von f auflösbar ist.*

Beweis. Der Schluss von Auflösbarkeit durch Radikale auf Auflösbarkeit der Galoisgruppe ist genau der Inhalt von Satz 9.5.3.1.
Sei umgekehrt $G(f)$ auflösbar. Als Zerfällungskörper ist Z_f automatisch normal (siehe Satz 9.2.3.2) und wegen der angenommenen Separabilität somit Galoissch (siehe Satz 9.2.5.1). Setzen wir $n := \mathrm{grad}\, f$, so gilt daher $[Z_f : K] = |\mathrm{Aut}_K(Z_f)| = |G(f)|$ nach dem Hauptsatz 9.3.1.1, sodass wir $[Z_f : K] \mid n!$ aus Proposition 9.4.1.2 erhalten. Wegen $n < \mathrm{char}\, K$ folgt $\mathrm{char}\, K \nmid [Z_f : K]$. Nach Satz 9.5.6.1 existiert ein Körper $E \geq Z_f$, sodass $K \leq E$ radikal ist – mit anderen Worten ist die Gleichung $f(x) = 0$ durch Radikale auflösbar.
Dass Z_f automatisch separabel ist, wenn $\mathrm{char}\, K = 0$ oder $|K| < \infty$, folgt aus den Propositionen 9.2.4.1 bzw. 9.2.4.4 (für den zweiten Fall beachte man, dass Z_f endlichdimensional über K und daher endlich ist). □

Für Charakteristik 0 erhalten wir unmittelbar das klassische Resultat von Galois als einfachere Version:

Folgerung 9.5.7.2. *Sei K ein Körper mit* $\operatorname{char} K = 0$ *und $f \in K[x]$.*
Dann gilt: Die Gleichung $f(x) = 0$ lässt sich genau dann durch Radikale auflösen, wenn die Galoisgruppe $G(f)$ von f auflösbar ist.

Für positive Charakteristik ist Satz 9.5.7.1 insofern etwas unbefriedigend, als er eine obere Schranke für den Polynomgrad enthält. Verfolgt man die Beweise zurück, so wird klar, dass dies der folgenden Tatsache geschuldet ist: Die Erweiterung um reine Wurzeln (d.h. Elemente u mit $u^k \in K$) ist nur dann in unserem Rahmen handhabbar, wenn $\operatorname{char} K \nmid k$; siehe Proposition 9.5.2.4, Proposition 9.5.2.7, Satz 9.5.5.1 und Satz 9.5.6.1. Im Beweis von Satz 9.5.6.1 garantiert die Voraussetzung $\operatorname{char} K \nmid [Z : K]$, dass wir es nicht mit Erweiterungen vom Grad $\operatorname{char} K$ zu tun haben können. Wollen wir Satz 9.5.7.1 erweitern, so müssen wir zur Definition radikaler Erweiterungen diese Möglichkeit somit hinzufügen. Als Motivation führen wir uns vor Augen, dass diese Definition im Wesentlichen die Idee einfängt, eine Körpererweiterung aus „möglichst einfachen“ Erweiterungen zusammenzusetzen, nämlich durch Erweiterungen von Wurzeln, also Lösungen von $x^k = a$. Es stellt sich heraus, dass wir für $k = p$ nur ein etwas anderes (und immer noch sehr einfaches) Polynom verwenden müssen, nämlich $x^k - x = a$.

Definition 9.5.7.3. E heißt *RADIKALE Erweiterung* von K, falls Elemente $u_1, \ldots, u_m \in E$ existieren, sodass $E = K(u_1, \ldots, u_m)$ und für jedes $i = 1, \ldots, m$ eine der folgenden beiden Aussagen zutrifft:

(i) es gibt eine natürliche Zahl $k_i > 0$ mit $\operatorname{char} K \nmid k_i$ und $u_i^{k_i} \in K(u_1, \ldots, u_{i-1})$
ODER

(ii) $\operatorname{char}(K) = p$ und $u_i^p - u_i \in K(u_1, \ldots, u_{i-1})$.

Für $f \in K[x]$ heißt die Gleichung $f(x) = 0$ *auflösbar durch RADIKALE*, falls eine RADIKALE Erweiterung E existiert mit $K \leq Z_f \leq E$, wobei Z_f der Zerfällungskörper von f über K ist.

Mit dieser Definition lässt sich Satz 9.5.7.1 zum folgenden Resultat verbessern, dessen Beweis wir durch eine Serie von Übungsaufgaben erbringen:

Satz 9.5.7.4 (Satz von Galois, Fassung 2)**.** *Sei K ein Körper und $f \in K[x]$ so, dass der Zerfällungskörper Z_f von f über K separabel ist (dies ist insbesondere dann der Fall, wenn entweder* $\operatorname{char}(K) = 0$ *oder K endlich ist).*
Dann gilt: Die Gleichung $f(x) = 0$ lässt sich genau dann durch RADIKALE auflösen, wenn die Galoisgruppe $G(f)$ von f auflösbar ist.

UE 141 ▶ **Übungsaufgabe 9.5.7.5.** (E) Zeigen Sie die folgende Variante von Proposition 9.5.2.7: ◀ **UE 141**
Sei $K \leq E$ eine Körpererweiterung mit $p := \operatorname{char} K > 0$. Sei weiters $u \in E$ mit $u^p - u = a \in K$. Dann ist $Z = Z_f = K(u)$ ein Zerfällungskörper des Polynoms $f(x) := x^p - x - a$

über K und die Erweiterung $K \leq Z = K(u)$ ist Galoissch. Wenn $u \notin K$, dann ist die Galoisgruppe $G(f) = \mathrm{Aut}_K(Z)$ von f zyklisch mit Ordnung p, insbesondere also abelsch. Hinweis: Wenn u eine Nullstelle von f ist, dann ist auch $u + 1$ eine Nullstelle.

UE 142 ▶ **Übungsaufgabe 9.5.7.6.** (E) Zeigen Sie die folgende Variante von Lemma 9.5.1.5: Sei $K \leq E$ eine RADIKALE Erweiterung und sei N der normale Abschluss von E. Dann ist auch $K \leq N$ eine RADIKALE Erweiterung. ◀ **UE 142**

UE 143 ▶ **Übungsaufgabe 9.5.7.7.** (E) Zeigen Sie die folgende Variante von Satz 9.5.3.1: Ist $K \leq E$ eine RADIKALE Erweiterung, dann ist $\mathrm{Aut}_K(Z)$ für jeden Zwischenkörper Z, $K \leq Z \leq E$, auflösbar. Insbesondere ist eine algebraische Gleichung $f(x) = 0$ mit einem Polynom $f \in K[x]$ nur dann durch RADIKALE auflösbar, wenn die Galoisgruppe von f (= die Galoisgruppe des Zerfällungskörpers von f über K) auflösbar ist. ◀ **UE 143**

UE 144 ▶ **Übungsaufgabe 9.5.7.8.** (E) Zeigen Sie die folgende Variante von Satz 9.5.5.1: Sei $K \leq E$ eine Körpererweiterung mit $p := \mathrm{char}\, K > 0$. Dann sind die folgenden Aussagen äquivalent: ◀ **UE 144**

(i) $K \leq E$ ist zyklisch vom Grad p.

(ii) E ist Zerfällungskörper eines irreduziblen Polynoms der Gestalt $f(x) = x^p - x - a \in K[x]$. (In diesem Fall ist $E = K(v)$ für jedes v mit $f(v) = 0$.)

Hinweis: Verwenden sie die additive Fassung von Hilbert 90 (Satz 9.5.4.6).
Anmerkung: Dieses Resultat wird auch als *Satz von Artin-Schreier* bezeichnet.

UE 145 ▶ **Übungsaufgabe 9.5.7.9.** (E) Zeigen Sie die folgende Variante von Satz 9.5.6.1: Sei $K \leq Z$ eine endlichdimensionale und Galoissche Erweiterung, und sei $\mathrm{Aut}_K(Z)$ auflösbar. Dann existiert ein Erweiterungskörper $E \geq Z$, sodass $K \leq E$ eine RADIKALE Erweiterung ist. ◀ **UE 145**

Durch Kombination der Übungsaufgaben 9.5.7.7 und 9.5.7.9 erhalten wir einen Beweis von Satz 9.5.7.4.

UE 146 ▶ **Übungsaufgabe 9.5.7.10.** (F+) ◀ **UE 146**

(1) Rekapitulieren Sie die klassischen Unmöglichkeitsbeweise folgender Konstruktionsaufgaben mit Zirkel und Lineal: Würfelverdoppelung, Winkeldreiteilung, Quadratur des Kreises.

(2) Zeigen Sie: Die Konstruktion des regelmäßigen n-Ecks mit Zirkel und Lineal ist genau dann möglich, wenn $n = 2^k \prod_{i=1}^{m} p_i$ mit $k \in \mathbb{N}$ und paarweise verschiedenen Primzahlen p_i der Gestalt $p_i = 2^{2^{e_i}} + 1$ mit $e_i \in \mathbb{N}$ (Fermatsche Primzahlen).

Hinweis: Verwenden Sie Proposition 9.5.2.5. Welche Primzahlen haben die Gestalt $2^m + 1$?

10 Kommutative Ringe und Nullstellensatz

In diesem Kapitel stehen kommutative Ringe R im Mittelpunkt, meist mit 1. Weil Ideale $I \lhd R$ auch als R-Moduln aufgefasst werden können, treten immer wieder auch Moduln in den Vordergrund. Ähnlich wie wir das schon an früheren Stellen gesehen haben, ermöglichen Kettenbedingungen interessante Ergebnisse. Noethersche Moduln und Ringe, die im Zentrum des ersten Abschnitts 10.1 stehen, sind explizit über die Kettenbedingung ACC an den Untermodul- bzw. an den Idealverband definiert. Auch der Begriff der Ganzheit von Ringerweiterungen und deren Elementen (siehe 10.2) hängt eng mit Kettenbedingungen zusammen. Mit seiner Hilfe lassen sich wichtige Hilfsresultate herleiten, die schließlich im Beweis des Hilbertschen Nullstellensatzes in 10.3 eine wichtige Rolle spielen. Dabei geht es um algebraische Gleichungssysteme in mehreren Variablen.

10.1 Noethersche Moduln und Ringe

In Hauptidealringen wird definitionsgemäß jedes Ideal von einem einzigen Element erzeugt. Schwächt man diese Eigenschaft etwas ab, so stößt man auf den Begriff eines Noetherschen Ringes, in dem jedes Ideal endlich erzeugt sein soll. Wie schon aus allgemeinerem Kontext bekannt, hängen derartige Eigenschaften eng mit Ketten- und Maximalbedingungen an den Idealverband eines Ringes zusammen. Etwas allgemeiner ist der Gesichtspunkt, statt der Ideale in einem Ring R Untermoduln von R-Moduln zu betrachten. Entsprechend beginnt der vorliegende Abschnitt in 10.1.1 mit Kettenbedingungen für Moduln, die in 10.1.2 auf Ringe übertragen werden und die Begriffe des Noetherschen sowie Artinschen Rings liefern. Eine der fundamentalen Tatsachen in diesem Zusammenhang ist der Hilbertsche Basissatz (10.1.3): Der Polynomring in einer und folglich auch in endlich vielen Variablen über einem Noetherschen Ring ist wieder Noethersch. Nach einem kurzen Einschub über Primideale (10.1.4) bietet 10.1.5 zum Abschluss und weitgehend ohne Beweise einen Überblick über die wichtigsten Konzepte und Ergebnisse der Idealtheorie über Noetherschen Ringen.

10.1.1 Kettenbedingungen für Moduln

Die folgende Definition ist eine Spezialisierung allgemeiner ordnungstheoretischer Konzepte, die wir schon in Unterabschnitt 2.1.2 kennengelernt haben. Man beachte auch die Analogie zu Unterabschnitt 8.5.1.

Definition 10.1.1.1. Sei A ein Modul.

- A erfüllt die *aufsteigende Kettenbedingung ACC* für Untermoduln (oder ist *Noethersch*), falls
$$A_1 \leq A_2 \leq A_3 \leq \ldots \leq A \Longrightarrow \exists n \in \mathbb{N}\, \forall i \geq n : A_i = A_n.$$

- A erfüllt die *absteigende Kettenbedingung DCC* für Untermoduln (oder ist *Artinsch*), falls

$$A \geq A_1 \geq A_2 \geq A_3 \geq \ldots \Longrightarrow \exists n \in \mathbb{N}\, \forall i \geq n : A_i = A_n.$$

Von folgender Charakterisierung werden wir wiederholt Gebrauch machen:

Proposition 10.1.1.2. *Für einen Modul A sind folgende Bedingungen äquivalent:*

(a) A ist Noethersch, d.h. definitionsgemäß: A erfüllt die aufsteigende Kettenbedingung ACC für Untermoduln.

(b) A erfüllt die Maximalbedingung für Untermoduln: Jede nichtleere Menge von Untermoduln von A enthält ein bezüglich $\subseteq$ maximales Element.

(c) Jeder Untermodul von A ist endlich erzeugt.

Beweis. Ergibt sich unmittelbar aus den Sätzen 2.1.2.12 und 2.2.1.26. □

Bei Moduln sind überdies folgende Aussagen über die Vererbung der Kettenbedingungen ACC und DCC nützlich:

Proposition 10.1.1.3. *Seien A, B, C Moduln über einem Ring R. Dann gilt:*

1. *Sei $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ eine kurzexakte Sequenz von Moduln. Dann gilt ACC bzw. DCC in B genau dann, wenn ACC bzw. DCC sowohl in A als auch in C gilt.*

2. *Sei A Untermodul eines Moduls B. Dann gilt ACC bzw. DCC in B genau dann, wenn ACC bzw. DCC sowohl in B als auch in A/B gilt.*

3. *Seien $A_1, \ldots, A_n$ Moduln und $A = A_1 \oplus A_2 \oplus \ldots \oplus A_n$. Dann gilt ACC bzw. DCC in A genau dann, wenn ACC bzw. DCC in allen A_i, $i = 1, \ldots, n$, gilt.*

Beweis. Die Beweise aller drei Aussagen verlaufen für aufsteigende und absteigende Kettenbedingung ACC und DCC völlig analog. Außerdem werden wir in diesem Kapitel nur die Versionen für ACC verwenden. Deshalb begnügen wir uns mit den Beweisen für ACC.

1. Wenn ACC für B gilt, so folgt ACC für A fast unmittelbar: Jede unendliche aufsteigende Kette von Untermoduln $A_i \leq A$ induziert eine unendliche Kette von Untermoduln $B_i := f(A_i)$ von B. Wäre sogar $A_i < A_{i+1}$ für alle n, so wegen der Injektivität von f auch $B_i < B_{i+1}$, Widerspruch. Ein ähnliches Argument zeigt, dass auch C die Bedingung ACC erfüllt: Liegt eine unendliche Kette aus $C_i \leq C$ mit $C_i \leq C_{i+1}$ vor, so bilden die $B_i := g^{-1}(C_i)$ eine gleichfalls unendlich aufsteigende Kette von Untermoduln von B. Weil g surjektiv ist, gilt $C_i = g(B_i)$ für alle n. Nach Voraussetzung gibt es ein n mit $B_i = B_n$, also $C_i = g(B_i) = g(B_n) = C_n$ für alle $i \geq n$. Damit ist die erste der beiden Implikationen gezeigt.

   Für die umgekehrte Implikation setzen wir ACC für A und C voraus und gehen von einer unendlich aufsteigenden Kette von Untermoduln $B_i \leq B$, $i \in \mathbb{N}$, von B

aus. Eine solche induziert die gleichfalls aufsteigenden Ketten der Untermoduln $A_i := f^{-1}(f(A) \cap B_i)$ von A und $C_i := g(B_i)$ von C. Laut Voraussetzung gibt es ein $n \in \mathbb{N}$ mit $A_i = A_n$ und $C_i = C_n$ für alle $i \geq n$. Man überlegt sich unmittelbar, dass für jedes $i \in \mathbb{N}$ die Sequenz $0 \to A_i \xrightarrow{f_i} B_i \xrightarrow{g_i} C_i \to 0$ mit den Einschränkungen f_i und g_i auf A_i bzw. B_i exakt ist, außerdem für $i \geq n$ das Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_n & \xrightarrow{f_n} & B_n & \xrightarrow{g_n} & C_n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_{A_n}} & & \downarrow{\scriptstyle \iota_{B_n,B_i}} & & \downarrow{\scriptstyle \mathrm{id}_{C_n}} & & \\ 0 & \longrightarrow & A_n & \xrightarrow{f_i} & B_i & \xrightarrow{g_i} & C_n & \longrightarrow & 0 \end{array}$$

kommutiert, wobei $\iota_{B_n,B_i} : B_n \to B_i$, $b \mapsto b$ die Inklusionsabbildung bezeichne (siehe Übungsaufgabe 10.1.1.4). Aus dem Kurzen Fünferlemma 7.2.3.7 folgt, dass mit id_{A_n} und id_{C_n} auch die Inklusionsabbildung ι_{B_n,B_i} surjektiv ist, also $B_i = B_n$.

2. Die erste Aussage angewandt auf die Sequenz $0 \to A \xrightarrow{\subseteq} B \to B/A \to 0$ liefert das Gewünschte.

3. Induktion nach n. Für den Induktionsschritt wendet man die erste Aussage auf die Sequenz $0 \to A_1 \oplus \cdots \oplus A_n \xrightarrow{\iota_1} A_1 \oplus \cdots \oplus A_n \oplus A_{n+1} \xrightarrow{\pi_2} A_{n+1} \to 0$ an. □

UE 147 ▶ **Übungsaufgabe 10.1.1.4.** (V) Überprüfen Sie die Exaktheit und Kommutativität der im Beweis der ersten Aussage von Proposition 10.1.1.3 auftretenden Sequenzen bzw. Diagramme. ◀ **UE 147**

So wie in Gruppen kann man auch in R-Moduln von Normalreihen und Subnormalreihen sprechen, wobei diese Begriffe offenbar zusammenfallen und schlicht endliche aufsteigende Ketten von Untermoduln bezeichnen. Ganz ähnlich den Sätzen von Jordan-Hölder und Schreier über Gruppen lässt sich dafür zeigen:

Satz 10.1.1.5. *Sei R ein Ring und A ein R-Modul. Dann gilt:*

1. *Je zwei Normalreihen von A haben äquivalente Verfeinerungen.*
2. *Je zwei Kompositionsreihen von A sind äquivalent.*

UE 148 ▶ **Übungsaufgabe 10.1.1.6.** (V) Beweisen Sie Satz 10.1.1.5. ◀ **UE 148**

Außerdem gilt:

Folgerung 10.1.1.7. *Sei R ein Ring und A ein R-Modul. Dann hat A genau dann eine Kompositionsreihe, wenn A sowohl ACC als auch DCC für Untermoduln erfüllt.*

UE 149 ▶ **Übungsaufgabe 10.1.1.8.** (V) Beweisen Sie Folgerung 10.1.1.7. ◀ **UE 149**

10.1.2 Kettenbedingungen für Ringe

Betrachtet man einen Ring als Links- oder Rechts-Modul über sich selbst, so sind die Untermoduln gerade die Links- bzw. Rechtsideale, im kommutativen Fall die Ideale. Das legt die folgende Definition nahe.

Definition 10.1.2.1. Ein Ring R heißt *links-* (bzw. *rechts-*) *Noethersch*, falls R die aufsteigende Kettenbedingung ACC bezüglich Links- (bzw. Rechts-) Idealen erfüllt. R heißt *Noethersch*, falls R sowohl links- als auch rechts-Noethersch ist.
Ein Ring R heißt *links-* (bzw. *rechts-*) *Artinsch*, falls R die absteigende Kettenbedingung DCC bezüglich links- (bzw. rechts-) Idealen erfüllt. R heißt *Artinsch*, falls R sowohl links- als auch rechts-Artinsch ist.

Damit ergibt sich aus Proposition 10.1.1.2 unmittelbar:

Folgerung 10.1.2.2. *Ein kommutativer Ring R mit 1 ist genau dann Noethersch, wenn jedes Ideal $I \lhd R$ endlich erzeugt ist. Insbesondere ist jeder Hauptidealring Noethersch.*

Wenig überraschend übertragen sich die Kettenbedingungen ACC und DCC von einem Ring R auch auf endlich erzeugte R-Moduln:

Satz 10.1.2.3. *Ist R ein links-Noetherscher bzw. links-Artinscher Ring und A ein endlich erzeugter R-Linksmodul, so ist A Noethersch bzw. Artinsch.*

Beweis. Sei R Noethersch, der Beweis für Artinsch verläuft völlig analog. Werde A von den Elementen $a_1, \ldots, a_n \in A$ erzeugt, und sei $F := \bigoplus_{i=1}^{n} Ra_i$ ein von $a_1, \ldots, a_n$ frei erzeugter R-Modul. Für jeden der Summanden gilt $Ra_i \cong R$ vermittels $ra_i \mapsto r$, also sind alle Ra_i Noethersch bzw. Artinsch. In Proposition 10.1.1.3 garantiert die dritte Aussage, dass folglich auch F ein Noetherscher R-Modul ist, die zweite, dass dies auch für das homomorphe Bild $A = f(F)$ unter dem (eindeutig bestimmten) Homomorphismus $f : F \to A$ mit $a_i \mapsto a_i$ für $i = 1, \ldots, n$ gilt. □

Es folgen zwei Beispiele in Form von Übungsaufgaben.

UE 150 ► Übungsaufgabe 10.1.2.4. (B) Zeigen Sie, dass **◄ UE 150**

$$R := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| \, a \in \mathbb{Z}, b, c \in \mathbb{Q} \right\}$$

ein Unterring von $\mathbb{Q}^{2\times 2}$ ist, der rechts-Noethersch aber nicht links-Noethersch ist.

UE 151 ► Übungsaufgabe 10.1.2.5. (B) Finden Sie einen faktoriellen Ring, der nicht Noethersch ist. **◄ UE 151**
Hinweis: Betrachten Sie Polynomringe über einem Körper.

10.1.3 Der Basissatz

Satz 10.1.3.1 (Hilbertscher Basissatz)**.** *Sei R ein kommutativer Ring mit 1. Ist R Noethersch, so ist auch $R[x_1, \ldots, x_n]$ Noethersch.*

Beweisskizze. Klarerweise reicht es, die Noethersche Eigenschaft für $n = 1$, d.h. für $R[x]$ zu beweisen, weil der Rest mittels Induktion nach n folgt. Sei also $J \lhd R[x]$. Wegen Satz 10.1.2.3 genügt der Nachweis, dass J endlich erzeugt ist. Sei

$$I_n := \{a_n \in R \mid \exists f \in R[x] : \ f(x) = a_n x^n + \ldots + a_1 x + a_0 \in J\}.$$

Offenbar ist $I_n \lhd R$ für alle n.
Wegen der Idealeigenschaft von J liegt mit jedem $f \in J$ auch xf in J, wobei der höchste Koeffizient $a_n \in I_n$ von f zum höchsten Koeffizienten von xf wird, also $a_n \in I_{n+1}$. Es liegt also eine aufsteigende Folge

$$I_1 \leq I_2 \leq I_3 \leq \ldots \lhd R$$

von Idealen in R vor. Folglich gibt es ein $n_0 \in \mathbb{N}$ mit $I_{n_0} = I_{n_0+1} = I_{n_0+2} = \ldots$. Jedes Ideal im Noetherschen Ring R ist endlich erzeugt, insbesondere die I_n, z.B. $I_n = \langle a_{n,i} \mid i = 1, \ldots, k_n \rangle$. Nach Wahl der I_n existieren Polynome $f_{n,i} \in J$ mit $f_{n,i}(x) = a_{n,i}x^n + \ldots + a_0 \in J$. Man zeigt leicht (siehe Übungsaufgabe 10.1.3.2), dass dann

$$J = \langle f_{n,i} \mid n = 1, \ldots, n_0, i = 1, \ldots, k_n \rangle$$

gilt, womit ein endliches Erzeugendensystem von J gefunden ist. □

UE 152 ► **Übungsaufgabe 10.1.3.2.** (V) Ergänzen Sie das im Beweis von Satz 10.1.3.1 nicht ausgeführte Argument, dass J tatsächlich von den $f_{n,i}$ für $n = 1, \ldots, n_0$ und $i = 1, \ldots, k_n$ erzeugt wird. ◄ **UE 152**

Die Möglichkeit, ein beliebiges Polynomideal in mehreren Variablen durch endlich viele Erzeugende anzugeben, findet weitreichende praktische Anwendungen in der vom österreichischen Mathematiker Bruno Buchberger (geb. 1942) Mitte der 60er Jahre begründeten Theorie der *Gröbnerbasen*, die er nach seinem akademischen Lehrer Wolfgang Gröbner (1899-1980) benannte. Berühmt ist dabei der sogenannte *Buchberger-Agorithmus* zur Berechnung einer Gröbnerbasis eines gegebenen Ideals. Der Nutzen einer Gröbnerbasis zeigt sich im Kontext der allgemeinen Idealtheorie Noetherscher Ringe, siehe Unterabschnitt 10.1.5.

Der Hilbertsche Basissatz gilt analog auch für den Ring $R[[x]]$ der formalen Potenzreihen anstelle des Polynomrings:

Satz 10.1.3.3. *Ist R ein kommutativer Noetherscher Ring, so auch der Ring $R[[x]]$ der formalen Potenzreihen über R.*

UE 153 ► **Übungsaufgabe 10.1.3.4.** (V,E) Beweisen Sie Satz 10.1.3.3. (Hinweis: Grundsätzlich führt eine ähnliche Vorgangsweise zum Ziel wie in Satz 10.1.3.1, Vorsicht ist aber geboten.) Gilt der entsprechende Satz auch für den Ring der formalen Laurentreihen über R? ◄ **UE 153**

10.1.4 Ein kurzer Einschub über Primideale

Folgender Satz erweist sich immer wieder als nützlich:

Satz 10.1.4.1. *Sei R ein kommutativer Ring mit 1 und $T \subseteq R$ multiplikativ abgeschlossen (d.h. $t_1, t_2 \in T \Rightarrow t_1 \cdot t_2 \in T$) sowie $I \lhd R$ mit $T \cap I = \emptyset$. Dann existiert ein Ideal $P \lhd R$ mit $I \subseteq P$ und $T \cap P = \emptyset$, das mit diesem Eigenschaften maximal[1] ist. Jedes solche Ideal P ist prim.*
Für $T = \emptyset$ bedeutet das, dass jedes Ideal in einem maximalen Ideal enthalten ist.

Beweis. Eine Standardanwendung des Lemmas von Zorn liefert ein maximales Ideal P mit den gewünschten Eigenschaften. Es bleibt zu beweisen, dass jedes derartige Ideal P prim ist. Wir gehen dazu von Elementen $a, b \in R$ mit $ab \in P$ aus und wollen zeigen, dass wenigstens eines der beiden in P enthalten ist. Wir nehmen indirekt an, das wäre nicht der Fall. Dann wären $P + Ra$ und $P + Rb$ Ideale, die P echt umfassen. Wegen der Maximalitätseigenschaft von P folgt daraus $(P + Ra) \cap T \neq \emptyset \neq (P + Rb) \cap T$. Es gibt also Elemente $p_i \in P$ und $r_a, r_b \in R$ mit $t_1 := p_1 + r_a a \in T$ und $t_2 := p_2 + r_b b \in T$. Weil T multiplikativ und R kommutativ ist, folgt einerseits $t_1 t_2 \in T$, andererseits

$$t_1 t_2 = p_1 p_2 + p_1 r_b b + r_a a p_2 + r_a r_b ab \in P,$$

im Widerspruch zu $T \cap P = \emptyset$. □

Jedem Ideal I in einem kommutativen Ring mit 1 wird das sogenannte Radikal $\mathrm{Rad}(I)$ zugeordnet. Die Definition lautet wie folgt.

Definition 10.1.4.2. Sei R ein kommutativer Ring mit 1. Für $I \lhd R$ heißt

$$\mathrm{Rad}(I) := \bigcap \{P \mid I \subseteq P, P \lhd R \text{ prim}\}$$

das *Radikal* von I.

Wichtig ist die folgende alternative Beschreibung, die zeigt, dass es sich beim Radikal $\mathrm{Rad}(I)$ gewissermaßen um den Abschluss von I bezüglich des Wurzelziehens handelt.

Proposition 10.1.4.3. *Sei R ein kommutativer Ring mit 1 und $I \lhd R$. Dann gilt*

$$\mathrm{Rad}(I) = \{r \in R \mid \exists n \geq 1 : \ r^n \in I\}.$$

[1] Achtung! Im Allgemeinen ist P kein maximales Ideal im Sinne von Definition 3.4.2.3.

Beweis. Wir kürzen $M := \{r \in R \mid \exists n \geq 1 : \ r^n \in I\}$ ab und haben die beiden Inklusionen $M \subseteq \mathrm{Rad}(I)$ und $\mathrm{Rad}(I) \subseteq M$ zu zeigen.
$M \subseteq \mathrm{Rad}\, I$: Sei $r \in M$, dann ist $r^n \in I$ für ein $n \geq 1$. Für alle Primideale $P \lhd R$ mit $I \subseteq P$ folgt $r^n \in P$, also auch $r \in P$ und damit $r \in \mathrm{Rad}(I)$. Also ist $M \subseteq \mathrm{Rad}(I)$.
$\mathrm{Rad}(I) \subseteq M$: Sei $s \notin M$. Die Menge $S := \{s^n + r : n \geq 1, r \in I\}$ ist multiplikativ abgeschlossen, $S \cap I = \emptyset$ und $s \in S$. Nach Satz 10.1.4.1 existiert ein primes $P \lhd R$ mit $P \cap S = \emptyset$ und $I \subseteq P$. Also ist $s \notin P$ und damit auch $s \notin \mathrm{Rad}\, I$. □

10.1.5 Idealtheorie in Noetherschen Ringen

Die Idealtheorie für Noethersche Ringe (insbesondere also für Polynomringe in den Variablen $x_1, \ldots, x_n$ über einem Körper) ermöglicht die Darstellung eines beliebigen Ideals $I \lhd R$ in einem Noetherschen Ring als mengentheoretischer Schnitt von sogenannten Primäridealen. Für derartige *Primärzerlegungen* gelten auch gewisse Eindeutigkeitsaussagen. Noch etwas allgemeiner sind die entsprechenden Resultate für Moduln. Weitgehend ohne Beweise seien hier lediglich die Hauptergebnisse samt den für deren Würdigung notwendigen Begriffsbildungen und Hilfsresultaten wiedergegeben. Zunächst definieren wir Primärideale und primäre Moduln:

Definition 10.1.5.1. Sei R ein kommutativer Ring mit 1. Ein Ideal $Q \lhd R$ mit $Q \neq R$ heißt *Primärideal* von R, wenn für alle $a, b \in R$ mit $ab \in Q$ und $a \notin Q$ folgt, dass $b^n \in Q$ für ein geeignetes positives $n \in \mathbb{N}$ gilt.
Sei nun A ein R-Modul. Ein Untermodul $U \leq A$ heißt *primär*, wenn aus $r \in R$, $a \in A \setminus U$ und $ra \in U$ stets $r^n A \subseteq U$ für ein geeignetes positives $n \in \mathbb{N}$ folgt.

Ein wichtiger Zusammenhang zwischen Primär- und Primidealen ist der folgende:

Proposition 10.1.5.2. *Ist R ein kommutativer Ring mit* 1 *und $Q \lhd R$ ein Primärideal in R, so ist* $\mathrm{Rad}(Q) \lhd R$ *ein Primideal.*

UE 154 ► Übungsaufgabe 10.1.5.3. (V) Beweisen Sie Proposition 10.1.5.2. **◄ UE 154**

Man zeigt sehr leicht:

Proposition 10.1.5.4. *Ist R ein kommutativer Ring mit* 1 *und $U \leq A$ ein primärer Untermodul eines R-Moduls A, dann ist $Q_U := \{r \in R : \ rA \subseteq U\}$ ein primäres Ideal, somit* $\mathrm{Rad}(Q_U)$ *ein Primideal.*

UE 155 ► Übungsaufgabe 10.1.5.5. (V) Beweisen Sie Proposition 10.1.5.4. **◄ UE 155**

Definition 10.1.5.6. In der Konstellation aus Proposition 10.1.5.4 sei $P := \mathrm{Rad}\, Q_U$. Dann sagt man, *U gehöre* zum Primideal P, und U heißt dann *P-primärer Untermodul* oder auch nur *primärer Untermodul* von A.

Ziel ist es, beliebige Ideale als Schnitte von endlich vielen Primäridealen darzustellen und möglichst auch Eindeutigkeitsaussagen herzuleiten. Wenn man will, kann man darin eine Verallgemeinerung der eindeutigen Primfaktorzerlegung in Hauptidealringen sehen.
Für Noethersche Ringe erweist sich die folgende Definition als zweckmäßig:

Definition 10.1.5.7. Sei R ein kommutativer Ring mit 1, A ein R-Modul und $U \leq A$. Gilt $U = Q_1 \cap \ldots \cap Q_n$ mit primären Untermoduln $Q_i \leq A$, so nennt man diese Darstellung von U als Schnitt eine *Primärzerlegung* von U. Wenn keines der Q_i im Schnitt der übrigen enthalten ist (wenn also keines der Q_i aus der Darstellung von A als Schnitt gestrichen werden kann) und alle zugehörigen Primideale $P_i := \operatorname{Rad} Q_i$ paarweise verschieden sind, so heißt die Darstellung *reduziert*. Ein Primideal P_i heißt in Bezug auf die Primärzerlegung *isoliert*, wenn es keines der übrigen P_j enthält, andernfalls *eingebettet*.

Nicht sehr schwierig ist der Nachweis, dass Primärzerlegungen stets in reduzierte übergeführt werden können:

Proposition 10.1.5.8. *Sei R ein kommutativer Ring mit 1, A ein R-Modul. Hat der Untermodul $U \leq A$ eine Primärzerlegung, so auch eine reduzierte.*

UE 156 ► **Übungsaufgabe 10.1.5.9.** (V) Beweisen Sie Proposition 10.1.5.8. Hinweis: Zeigen Sie zunächst, dass der Schnitt von P-primären Untermoduln wieder P-primär zum selben Primideal ist. ◄ **UE 156**

Das angestrebte Hauptergebnis lautet nun:

Satz 10.1.5.10. *Für reduzierte Primärzerlegungen von Moduln und von Idealen gelten folgende Existenz- bzw. Eindeutigkeitsaussagen. Dabei sei R ein kommutativer Ring mit 1, A ein R-Modul und $U \leq A$ ein Untermodul.*

1. *Ist A Noethersch, dann hat U eine reduzierte Primärzerlegung. Insbesondere haben jeder Untermodul eines endlich erzeugten Moduls über einem Noetherschen Ring sowie jedes Ideal in einem Noetherschen Ring eine reduzierte Primärzerlegung.*

2. *Seien*
$$Q_1 \cap \ldots \cap Q_n = U = Q'_1 \cap \ldots \cap Q'_{n'}$$
zwei reduzierte Primärzerlegungen von U und P_i sowie P'_j Primideale von R derart, dass die Q_i alle P_i-primär und die Q'_j alle P'_j-primär sind. Dann gilt $n = n'$ und, nach geeigneter Permutation der Indizes, $P_i = P'_i$ für $i = 1, \ldots, n$. Ist P_i in Bezug auf die Primärzerlegung isoliert, so gilt sogar $Q_i = Q'_i$.

UE 157 ► **Übungsaufgabe 10.1.5.11.** (E) Beweisen Sie Satz 10.1.5.10. (Achtung, anspruchsvoll!) ◄ **UE 157**

UE 158 ► **Übungsaufgabe 10.1.5.12.** (B,E) Finden Sie ein Beispiel einer Primärzerlegung, die nicht eindeutig ist. ◄ **UE 158**

10.2 Ganzheit in kommutativen Ringen

In diesem Abschnitt werden alle Ringe als kommutativ mit 1 vorausgesetzt.

In der Theorie der Ringerweiterungen spielt der Begriff der Ganzheit eine ähnliche Rolle wie jener der Algebraizität bei Körpererweiterungen. Im Fall von Körpern fallen die beiden Begriffe zusammen. Die Grundbegriffe werden in 10.2.1 bereitgestellt. Der ganze Abschluss eines Ringes R ist Gegenstand von 10.2.2. Im Gegensatz zum algebraischen Abschluss eines Körpers wird der ganze Abschluss eines Ringes R innerhalb einer gegebenen Ringerweiterung $R \leq S$ definiert. In 10.2.3 untersuchen wir für eine gegebene ganze Erweiterung $R \leq S$ das Zusammenspiel zwischen Idealen von R und Idealen von S. Dedekindsche Ringe sind spezielle Noethersche Ringe, die besonders in der algebraischen Zahlentheorie eine wichtige Rolle spielen und auf sehr vielfältige Weise charakterisiert werden können, u.a. durch Ganzheitseigenschaften, wie wir in 10.2.4 ohne Beweise andeuten. Ebenfalls in den Kontext ganzer Ringerweiterungen fügt sich das Beispiel aus 10.2.5 eines Hauptidealringes ein, der nicht Euklidisch ist. Damit wird ein bis dato offenes Desideratum aus 5.2.3 eingelöst.

10.2.1 Ganze Elemente und Ringerweiterungen

Definition 10.2.1.1. Ist R ein kommutativer Ring mit 1 und $R \leq S$, so heißt S eine *Ringerweiterung* von R. Für $X \subseteq S$ sei

$$R[X] := \{f(s_1, \ldots, s_n) \mid s_i \in X, f \in R[x_1, \ldots, x_n], n \in \mathbb{N}\}$$

der von $R \cup X$ erzeugte Unterring von S. Ein Element $s \in S$ heißt *ganz über* R, falls es ein monisches (d.h. normiertes, der führende Koeffizient ist 1) Polynom $f \in R[x]$ gibt mit $f(s) = 0$. Der Ring S heißt *ganz über* R, falls alle Elemente von S ganz über R sind.

Sind R und S Körper, so stimmt „ganz“ offenbar mit „algebraisch“ überein.

Satz 10.2.1.2. *Sei $R \leq S$ eine Ringerweiterung.*

(a) Für $s \in S$ sind folgende Aussagen äquivalent.

- *(i) s ist ganz über R.*
- *(ii) $R[s]$ ist ein endlich erzeugter R-Modul.*
- *(iii) Es existiert ein $T \leq S$, sodass $R[s] \subseteq T$ und T ein endlich erzeugter R-Modul ist.*

(b) Ist S ein endlich erzeugter R-Modul, so ist S ganz über R.

(c) Ist S ein endlich erzeugter R-Modul und T ein endlich erzeugter S-Modul, so ist T auch als R-Modul endlich erzeugt.

(d) Sind $s_1, \ldots, s_n \in S$ ganz über R, so ist $R[s_1, \ldots, s_n]$ ein endlich erzeugter R-Modul und damit ganz über R.

(e) In den Ringerweiterungen $R \leq S \leq T$ sei S ganz über R und T ganz über S. Dann ist T ganz über R.

Beweis. Wir zeigen nur die drei zyklischen Implikationen für (a). Der Rest folgt ähnlich wie die entsprechenden Aussagen über algebraische Körpererweiterungen in Unterabschnitt 6.1.4 und ist Inhalt einer Übungsaufgabe.
(i) $\Rightarrow$ (ii): Nach Voraussetzung gibt es ein normiertes Polynom $f(x) = x^n + r_{n-1}x^{n-1} + \ldots + r_1 x + r_0$ mit $r_i \in R$ und $f(s) = 0$. Wir behaupten, dass der von den Potenzen $s^0 = 1, s^1 = s, s^2, \ldots, s^{n-1}$ erzeugte R-Modul $A := \langle s^0 = 1, s, \ldots, s^{n-1}\rangle \subseteq R[s]$ bereits ganz $R[s]$ ist. Dazu müssen wir $s^m \in A$ für alle $m \in \mathbb{N}$ nachweisen (und nicht bloß für $m = 0, \ldots, n-1$), was wir mittels Induktion nach m bewerkstelligen. Aus der Nullstellengleichung für s lesen wir $s^n = -r_{n-1}s^{n-1} - \ldots - r_1 s^1 - r_0 s^0 \in A$ ab. Sei $m \geq n$ und $s^{m-1} \in A$. Wir wollen $s^m \in A$ zeigen. Dazu schreiben wir $s^{m-1} = r'_{n-1}s^{n-1} + \ldots + r'_1 s^1 + r'_0 s^0$ und folgern

$$s^m = ss^{m-1} = s(r'_{n-1}s^{n-1} + \ldots + r'_1 s^1 + r'_0 s^0) = r'_{n-1}s^n + \ldots + r'_1 s^2 + r'_0 s^1 \in A,$$

da jeder der Summanden in A enthalten ist. Somit ist insgesamt $R[s] = \{g(s) \mid g \in R[x]\} \subseteq A$, also $R[s] = A$, wie behauptet.
(ii) $\Rightarrow$ (iii): Offenbar hat $T := R[s]$ die behauptete Eigenschaft.
(iii) $\Rightarrow$ (i): Werde T von den Elementen $b_1, \ldots, b_n$ als R-Modul erzeugt. Dann gibt es Elemente $r_{i,j} \in R$ mit

$$sb_i = \sum_{j=1}^{n} r_{i,j} b_j \quad \text{für } i = 1, \ldots, n.$$

Wir setzen $r'_{i,j} := -r_{i,j}$ für $i \neq j$ und $r'_{i,i} := s - r_{i,i}$. Folglich gilt

$$\sum_{j=1}^{n} r'_{i,j} b_j = 0 \quad \text{für } i = 1, \ldots, n.$$

Daraus folgt $b_i \det(A') = 0$ für alle $i = 1, \ldots, n$ und die Matrix $A' := (r'_{i,j})_{1 \leq i,j \leq n}$ (Übungsaufgabe 10.2.1.3). Weil die b_i ganz T erzeugen, heißt das $t \det(A') = 0$ für alle $t \in T$. Setzen wir speziell $t = 1$ (man beachte, dass $1 \in R[s] \subseteq T$), so folgt $\det(A') = 0$. Wir betrachten nun für die Matrix $A := (r_{i,j})_{1 \leq i,j \leq n}$ das monische Polynom $f(x) := \det(xI_n - A) \in R[x]$ (mit der n-dimensionalen Einheitsmatrix I_n). Wegen $f(s) = \det(sI_n - A) = \det A' = 0$ ist s Nullstelle von f und somit ganz über R. □

UE 159 ► Übungsaufgabe 10.2.1.3. (V) Zeigen Sie die im Beweis von Satz 10.2.1.2(a), Implikation (iii) $\Rightarrow$ (i), verwendete Beziehung $b_i \det(A') = 0$ für $i = 1, \ldots, n$ unter den dort vorliegenden Bedingungen. **◄ UE 159**
Hinweis: $b_i \det(A') = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot r'_{\sigma(1),1} \cdot \ldots \cdot (r'_{\sigma(i),i} b_i) \cdot \ldots \cdot r'_{\sigma(n),n}$

UE 160 ► **Übungsaufgabe 10.2.1.4.** (V) Beweisen Sie die noch offenen Behauptungen (b) bis (e) aus Satz 10.2.1.2. Hinweis: Ist (a) einmal bewiesen, folgen die verbleibenden Aussagen sehr ähnlich wie die entsprechenden Zusammenhänge zwischen „algebraisch“ und „endlichdimensional“ bei Körpererweiterungen. ◄ **UE 160**

UE 161 ► **Übungsaufgabe 10.2.1.5.** (F) Sei $\alpha \in \mathbb{C}$ ganz über $\mathbb{Z}$ (man sagt auch, α ist *ganz algebraisch*). Klarerweise ist α dann algebraisch über $\mathbb{Q}$. Zeigen Sie, dass das (normierte) Minimalpolynom von α über $\mathbb{Q}$ ganzzahlige Koeffizienten hat.
Hinweis: Weisen Sie nach, dass die Koeffizienten des Minimalpolynoms selber ganz über $\mathbb{Z}$ sind.
Anmerkung: Diese Aufgabe zeigt, dass es für ein ganz algebraisches α keinen Sinn hat, ein Konzept des „ganz-minimalen Polynoms“ von α zu definieren, also des normierten *und ganzzahligen* Polynoms kleinsten Grades, das α annulliert. Denn das ganz-minimale Polynom in diesem Sinne stimmt genau mit dem gewöhnlichen Minimalpolynom überein. ◄ **UE 161**

10.2.2 Ganzer Abschluss

Definition 10.2.2.1. Sei $R \leq S$ eine Ringerweiterung. Der *ganze Abschluss von R in S* ist definiert als

$$\widehat{R} := \{s \in S : s \text{ ganz über } R\} \geq R.$$

Ist $\widehat{R} = R$, so heißt R *ganz abgeschlossen in S*. Ist R ein Integritätsbereich und ganz abgeschlossen in seinem Quotientenkörper S, so heißt R (schlechthin) *ganz abgeschlossen*.

Proposition 10.2.2.2. *Für eine Ringerweiterung $R \leq S$ gilt:*

(a) Der ganze Abschluss $\widehat{R}$ von R ist ein Unterring von S.

(b) $\widehat{R}$ ist ganz über R.

(c) Die Bildung des ganzen Abschlusses ist idempotent, d.h.: $\widehat{\widehat{R}} = \widehat{R}$.

(d) Ist R ein faktorieller Ring, so ist R ganz abgeschlossen (im Quotientenkörper S). Insbesondere ist $K[x_1, \ldots, x_n]$ für jeden Körper K und alle $n \in \mathbb{N}$ ganz abgeschlossen.

(e) Der Ring der ganzen Zahlen $\mathbb{Z}$ ist ganz abgeschlossen (im Quotientenkörper $\mathbb{Q}$), aber nicht ganz abgeschlossen in $\mathbb{C}$.

UE 162 ► **Übungsaufgabe 10.2.2.3.** (V) Beweisen Sie Proposition 10.2.2.2.
Hinweis: Proposition 5.3.2.9. ◄ **UE 162**

10.2.3 Ganze Erweiterungen und Ideale

Ist $R \leq S$ eine ganze Erweiterung, so besteht ein enger Zusammenhang zwischen Primidealen von R und Primidealen von S, der sich auch auf maximale Ideale übertragen lässt.

Lemma 10.2.3.1. *Sei $R \leq S$ ganz.*

1. *(Lying-over-Theorem): Sei $P \lhd R$ prim. Dann existiert ein $Q \lhd S$ prim mit $Q \cap R = P$.*

$$\begin{array}{ccc} \exists Q & \lhd_{prim} & S \\ \downarrow \cap R & & \vdots \\ P & \lhd_{prim} & R \end{array}$$

2. *(Going-up-Theorem): Seien P_1, P Primideale von R mit $P_1 \subseteq P$ und $Q_1 \lhd S$ prim mit $Q_1 \cap R = P_1$. Dann existiert ein $Q \lhd S$ prim mit $Q_1 \subseteq Q$ und $Q \cap R = P$.*

$$\begin{array}{ccccc} & & \lhd_{prim} & & \\ Q_1 & \subseteq & \exists Q & \lhd_{prim} & S \\ \downarrow \cap R & & \downarrow \cap R & & \vdots \\ P_1 & \subseteq & P & \lhd_{prim} & R \\ & & \lhd_{prim} & & \end{array}$$

3. *(Eindeutigkeitsaussage für lying-over-Ideale, vgl. 1.): Sei $P \lhd R$ prim, seien $Q, Q_1 \lhd S$ beide prim mit $Q \supseteq Q_1$ und $Q \cap R = P = Q_1 \cap R$. Dann ist $Q = Q_1$.*

Beweis.

1. $T := R \setminus P$ ist multiplikativ abgeschlossen, daher folgt aus Satz 10.1.4.1 die Existenz eines Primideals $Q \lhd S$, das als Ideal maximal ist mit der Eigenschaft $Q \cap (R \setminus P) = \emptyset$, also mit $Q \cap R \subseteq P$. Es bleibt zu zeigen, dass $P \subseteq Q$ und somit $P \subseteq Q \cap R$, insgesamt also $Q \cap R = P$.

   Angenommen, es gäbe ein $u \in P \setminus Q$. Dann umfasst $Q + Su$ echt Q. Da Q maximal mit $Q \cap (R \setminus P) = \emptyset$ ist, muss es ein $c \in (Q + Su) \cap (R \setminus P)$ geben. Dieses Element lässt sich schreiben als $c = q + su$ mit $q \in Q, s \in S$. Weil s ganz über R ist, existieren $r_i \in R$ mit

$$s^n + r_{n-1}s^{n-1} + \ldots + r_1 s + r_0 = 0.$$

   Multiplikation mit u^n liefert

$$(su)^n + r_{n-1}u(su)^{n-1} + \ldots + r_1 u^{n-1}(su) + r_0 u^n = 0.$$

In dieser Gleichung verwenden wir nun $su = c - q$ und wenden darauf den binomischen Lehrsatz an. Alle Terme, in denen q vorkommt, liegen in Q, also auch die Summe der verbleibenden:

$$v := c^n + r_{n-1}uc^{n-1} + \ldots + r_1u^{n-1}c + r_0u^n \in Q.$$

Aus $c, u, r_i \in R$ folgt $v \in R$, also sogar $v \in R \cap Q \subseteq P$. Wegen $u \in P$ bedeutet das auch $c^n \in P$ und, da P prim ist, $c \in P$ – Widerspruch.

2. Ähnlich wie 1.: Suche mittels $Q_1 \cap (R \setminus P) = \emptyset$ ein maximales Ideal Q mit $Q_1 \subseteq Q$ und $Q \cap R = P$.

3. Es genügt zu zeigen, dass jedes Primideal $Q \lhd S$ mit $Q \cap R = P$ maximal ist unter allen Idealen $I \lhd S$ mit $I \cap (R \setminus P) = \emptyset$. Wir nehmen indirekt an, es gäbe ein $I \lhd S$, das Q echt umfasst, d.h. mit einem $u \in I \setminus Q$. Zunächst gilt $I \cap R \subseteq P$. Weil S eine ganze Erweiterung von R ist, ist u Nullstelle eines monischen Polynoms über R, folglich gibt es auch ein monisches Polynom $f \in R[x]$ minimalen Grades mit $f(u) \in Q$. Sei $f(x) = \sum_{i=0}^{n} r_i x$ mit $r_n = 1$. Dann haben wir

$$u^n + r_{n-1}u^{n-1} + \ldots + r_1u + r_0 = f(u) \in Q \subseteq I.$$

Es folgt $r_0 \in I \cap R \subseteq P = Q \cap R$, also

$$u(u^{n-1} + r_{n-1}u^{n-2} + \ldots + r_2u + r_1) \in Q.$$

Weil Q ein Primideal ist, muss einer der beiden Faktoren in Q liegen. Der Klammerausdruck kann es wegen der minimalen Wahl von n nicht sein, also folgt $u \in Q$, was aber im Widerspruch zu unserer Wahl von u steht.

□

UE 163 ▶ Übungsaufgabe 10.2.3.2. (V) Beweisen Sie die zweite Aussage in Lemma 10.2.3.1. **◀ UE 163**

Proposition 10.2.3.3. *Sei $R \leq S$ eine ganze Ringerweiterung mit Primidealen $Q \lhd S$ und $P \lhd R$, die $Q \cap R = P$ erfüllen. Dann ist Q ist genau dann maximal in S, wenn P maximal in R ist.*

Beweis. Sei zunächst Q maximal in S. Wir erweitern P zu einem in R maximalen (und somit auch primen) Ideal M, d.h. $P \subseteq M \lhd R$. Laut der zweiten Aussage in Lemma 10.2.3.1 (Going-up-Theorem) gibt es ein Primideal Q' in S mit $Q \subseteq Q'$ und $Q' \cap R = M$. Wegen $Q' \neq S$ und der Maximalität von Q folgt $Q = Q'$, also ist $P = Q \cap R = Q' \cap R = M$ maximal.
Sei jetzt P maximal in R. Wir erweitern Q zu einem maximalen Ideal N in S. Als echtes Ideal enthält N sicher nicht das Einselement, folglich ist $R \neq R \cap N \lhd R$. Wegen $P = R \cap Q \subseteq R \cap N$ und der Maximalität von P folgt $P = R \cap N$. Nach der dritten Aussage in Lemma 10.2.3.1 folgt daraus $Q = N$. Also ist auch Q maximal. □

UE 164 ► **Übungsaufgabe 10.2.3.4.** (B,E,D) Illustrieren Sie anhand geeigneter Beispiele, was sich verändert, wenn man in Proposition 10.2.3.3 gewisse Voraussetzungen ($R \leq S$ ganz, P prim etc.) abschwächt. ◄ **UE 164**

10.2.4 Dedekindsche Ringe

Dedekindsche Ringe sind spezielle Integritätsbereiche und treten vor allem in der algebraischen Zahlentheorie auf. Sie bilden eine Teilklasse der Noetherschen Ringe und umfassen die Hauptidealringe. Dedekindsche Ringe lassen sich auf vielfältige Weise charakterisieren. Ohne Beweis werden wir einige Möglichkeiten angeben.
In der Idealtheorie Dedekindscher Ringe kann der mengentheoretische Schnitt durch das Produkt ersetzt werden. Es geht also um die Darstellung beliebiger Ideale als Produkt von Primär- und, sogar noch stärker, von Primidealen. Die Definition lautet:

Definition 10.2.4.1. Ein Integritätsbereich R heißt *Dedekindscher Ring*, wenn jedes Ideal $I \lhd R$ mit $I \neq R$ das Produkt endlich vieler Primideale ist. Dabei ist das Produkt zweier Ideale $I, J \lhd R$ definiert als das von allen Produkten ab mit $a \in I$ und $b \in J$ erzeugte Ideal, also die Menge aller endlichen Summen $\sum_{k=1}^{n} a_k b_k$ mit $n \in \mathbb{N}$, $a_k \in I$ und $b_k \in J$.

Für den Charakterisierungssatz 10.2.4.3 brauchen wir einige Begriffe.

Definition 10.2.4.2. Sei R ein Integritätsbereich und K sein Quotientenkörper. Ein R-Modul $I \subseteq K$ heißt ein *gebrochenes Ideal* von R, wenn es ein $r \in R$ mit $rI \subseteq R$ gibt. Unter dem *Produkt* IJ zweier gebrochener Ideale versteht man den von den Produkten ab mit $a \in I$ und $b \in J$ erzeugten R-Modul, also die Menge aller endlichen Summen $\sum_{k=1}^{n} a_k b_k$ mit $n \in \mathbb{N}$, $a_k \in I$ und $b_k \in J$. (Im Fall von Idealen $I, J \lhd R$ stimmt diese Definition also mit jener aus Definition 10.2.4.1 überein.)
Ein gebrochenes Ideal I heißt *invertierbar*, wenn es ein gebrochenes Ideal J mit $IJ = R$ gibt.

Es ist offensichtlich, dass die gebrochenen Ideale von R ein kommutatives Monoid mit Einselement R bilden, das sämtliche Ideale von R enthält.
In der letzten der Charakterisierungen Dedekindscher Ringe, die wir bringen wollen, verwenden wir auch noch den Begriff der *Lokalisierung* R_P eines Ringes R bei einem Primideal P. Darunter versteht man den Quotientenring (Bruchring, siehe Definition 3.4.5.1) von R bezüglich $S := R \setminus P$.
Damit können wir den angekündigten Charakterisierungssatz für Dedekindsche Ringe formulieren:

Satz 10.2.4.3. *Für einen Integritätsbereich R sind die folgenden Bedingungen äquivalent:*

1. *R ist ein Dedekindscher Ring, d.h. (definitionsgemäß) jedes Ideal $I \lhd R$, $I \neq R$, ist das Produkt endlich vieler Primideale.*

2. *Jedes Ideal $I \lhd R$, $I \neq R$, ist in eindeutiger Weise (bis auf die Reihenfolge der Faktoren) das Produkt endlich vieler Primideale.*
3. *Jedes Ideal $I \lhd R$ mit $I \neq \{0\}$ ist invertierbar.*
4. *Jedes gebrochene Ideal I von R mit $I \neq \{0\}$ ist invertierbar.*
5. *Die gebrochenen Ideale von R bilden bezüglich der Multiplikation eine Gruppe.*
6. *Jedes Ideal ist als R-Modul projektiv.*
7. *Jedes gebrochene Ideal von R ist als R-Modul projektiv.*
8. *R ist Noethersch, ganz abgeschlossen und jedes Primideal $P \neq \{0\}$ ist maximal.*
9. *R ist Noethersch und für jedes Primideal $P \neq \{0\}$ ist die Lokalisierung R_P von R bei P ein Hauptidealring mit einem Primideal $P \neq \{0\}$, wobei aus $P \neq P'$ stets $R_P \neq R_{P'}$ folgt.*

UE 165 ▶ **Übungsaufgabe 10.2.4.4.** (E,D) Beweisen Sie möglichst viele Implikationen zwischen den neun äquivalenten Bedingungen in Satz 10.2.4.3. (Achtung, anspruchsvoll!) ◀ **UE 165**

UE 166 ▶ **Übungsaufgabe 10.2.4.5.** (F,B) Zeigen Sie: Jeder Hauptidealring, aber nicht jeder faktorielle Ring ist Dedekindsch. ◀ **UE 166**

10.2.5 Ein Hauptidealring, der nicht Euklidisch ist

In der algebraischen Zahlentheorie sind Zahlenringe der Form $\mathbb{Z}[\alpha] = \{f(\alpha) : \ f \in \mathbb{Z}[x]\}$ mit gewissen algebraischen Zahlen $\alpha \in \mathbb{C} \setminus \mathbb{Q}$ von besonderem Interesse. Wir haben schon gesehen, dass man für $\alpha = i$ einen Euklidischen Ring erhält (den Ring der Gaußschen Zahlen), siehe Proposition 5.2.3.9, für $\alpha = \sqrt{-5}$ hingegen einen Integritätsbereich, der nicht einmal faktoriell ist, siehe Übungsaufgabe 5.1.4.9. Die Vielfalt der Möglichkeiten soll hier am Beispiel $\alpha := \frac{1+i\sqrt{19}}{2}$ weiter illustriert werden.

Satz 10.2.5.1. *Der Ring $\mathbb{Z}[\alpha]$ ist für $\alpha := \frac{1+i\sqrt{19}}{2}$ ein Hauptidealring aber nicht Euklidisch.*

Einer Anleitung von H. W. Lenstra Jr. und G. Bergman folgend soll ein Beweis dieser Behauptung im Wesentlichen im Rahmen von zwei Übungsaufgaben mit Anleitung skizziert werden.

UE 167 ▶ **Übungsaufgabe 10.2.5.2.** (B) Zeigen Sie, dass der Ring $\mathbb{Z}[\alpha]$ für $\alpha = \frac{1+i\sqrt{19}}{2}$ kein Euklidischer Ring ist. Anleitung: Gehen Sie schrittweise vor, indem Sie die folgenden Behauptungen beweisen: ◀ **UE 167**

1. Die Zahl α ist Nullstelle des Polynoms $f(x) = x^2 - x + 5$.
2. $\mathbb{Z}[\alpha] = \{a + b\alpha : \ a, b \in \mathbb{Z}\} = \{a + b\overline{\alpha} : \ a, b \in \mathbb{Z}\}$.
3. Die Normfunktion $N : x \mapsto |x|^2 = x\overline{x}$ ist ein Homomorphismus bezüglich der Multiplikation, der auf $\mathbb{Z}[\alpha]$ nur nichtnegative ganzzahlige Werte annimmt.
4. Alle Einheiten e von $\mathbb{Z}[\alpha]$ erfüllen $|e|^2 = 1$.
5. 1 und -1 sind die einzigen Einheiten in $\mathbb{Z}[\alpha]$. Anleitung: Man leite eine untere Abschätzung für den Betrag des Imaginärteils nicht reeller Elemente ab.
6. Die Annahme, $\mathbb{Z}[\alpha]$ sei Euklidisch, führt zu einem Widerspruch. Anleitung: Gehen Sie indirekt von einer Euklidischen Bewertung H und einem $x \neq 0$, das keine Einheit ist, mit minimalem $H(x)$ aus. Zeigen Sie, dass 0 und die Einheiten alle Nebenklassen des von x erzeugten Hauptideals repräsentieren. Also enthält der Faktorring $\mathbb{Z}[\alpha]/x\mathbb{Z}[\alpha]$ höchstens 3 Elemente. Prüfen Sie nach, dass in keinem dreielementigen Ring das Polynom f eine Nullstelle hat. Leiten Sie daraus den gesuchten Widerspruch ab.

$\mathbb{Z}[\alpha]$ ist für $\alpha := \frac{1+i\sqrt{19}}{2}$ also nicht Euklidisch. Um zu zeigen, dass $\mathbb{Z}[\alpha]$ aber sehr wohl ein Hauptidealring ist, sei ein beliebiges Ideal $I \lhd \mathbb{Z}[\alpha]$ vorgegeben, von dem nachzuweisen ist, dass es ein Hauptideal ist. Wir dürfen annehmen, dass I nicht das Nullideal ist und somit ein Element x mit minimalem positiven Betrag enthält. Der Absolutbetrag ist, wie aus Übungsaufgabe 10.2.5.2 hervorgeht, keine Euklidische Bewertung, wird aber ähnliche Dienste leisten, um $I = x\mathbb{Z}[\alpha]$ zu zeigen, also die Hauptidealeigenschaft. Das wird den Beweis von Satz 10.2.5.1 vervollständigen. Nützlich wird dabei die Menge $J := x^{-1}I = \{x^{-1}r : \ r \in I\} \subseteq \mathbb{C}$ sein. Können wir $J \subseteq \mathbb{Z}[\alpha]$ zeigen, folgt $I = x\mathbb{Z}[\alpha]$. Dies wird gelingen, indem aus der Annahme $y_0 \in J \setminus \mathbb{Z}[\alpha]$ ein Widerspruch abgeleitet wird.

UE 168 ► **Übungsaufgabe 10.2.5.3.** (B) Vervollständigen Sie den Beweis, dass der Ring $\mathbb{Z}[\alpha]$ für $\alpha = \frac{1+i\sqrt{19}}{2}$ ein Hauptidealring ist. Anleitung: Gehen Sie in folgenden Schritten vor, wobei die oben eingeführten Notationen weiter verwendet werden: ◄ **UE 168**

1. J ist ein $\mathbb{Z}[\alpha]$-Untermodul von $\mathbb{C}$, der $\mathbb{Z}[\alpha]$ enthält und in dem es außer 0 kein Element mit Absolutbetrag < 1 gibt.
2. Zeigen Sie: Aus $y \in J$ und $|y - r| < 1$ für ein $r \in \mathbb{Z}[\alpha]$ folgt $y \in \mathbb{Z}[\alpha]$.
3. Lassen Sie sich durch eine Skizze, die die geometrischen Verhältnisse in der komplexen Ebene wiedergibt, zu einem Beweis folgender Tatsache inspirieren: Ist $y \in J \setminus \mathbb{Z}[\alpha]$, d der Imaginärteil von y und $b \in \mathbb{Z}$, so folgt $|d - b\frac{\sqrt{19}}{2}| \geq \frac{\sqrt{3}}{2}$.
4. Wäre $J \setminus \mathbb{Z}[\alpha]$ nicht leer, so gäbe es darin ein Element y_0 mit Realteil im Intervall $(-\frac{1}{2}, \frac{1}{2}]$ und Imaginärteil im Intervall $[\frac{\sqrt{3}}{2}, \frac{\sqrt{19}}{2} - \frac{\sqrt{3}}{2}]$.

5. Für so ein y_0 läge der Imaginärteil von $2y_0$ zu nahe bei $\frac{\sqrt{19}}{2}$, als dass $2y_0$ zu $J \setminus \mathbb{Z}[\alpha]$ gehören kann.
6. Zeigen Sie, dass nur mehr die Möglichkeiten $y_0 = \frac{\alpha}{2}$ und $y_0 = -\frac{\overline{\alpha}}{2}$ verbleiben.
7. Schließen Sie daraus, dass $\frac{\alpha\overline{\alpha}}{2} \in J$, berechnen Sie diese Zahl und leiten Sie daraus einen Widerspruch ab.
8. Wir wissen nun, dass $J \setminus \mathbb{Z}[\alpha]$ leer ist, mit anderen Worten $\mathbb{Z}[\alpha] \supseteq J$. Schließen Sie daraus $I = x\mathbb{Z}[\alpha]$.

Um besser zu verstehen, worauf es bei der Wahl von α ankommt, kann man sich auch noch die folgende Aufgabe vornehmen.

UE 169 ► **Übungsaufgabe 10.2.5.4.** (B) Untersuchen Sie, was schief geht, wenn man in den Übungsaufgaben 10.2.5.2 und 10.2.5.3 die Zahl 19 durch 17 oder durch 23 ersetzt. ◄ **UE 169**

10.3 Der Hilbertsche Nullstellensatz

Der Hilbertsche Nullstellensatz (HNS) befasst sich mit der Lösungsmenge von Systemen von algebraischen (d.h. von Polynom-) Gleichungen in endlich vielen Variablen $x_1, \ldots, x_n$ über einem Körper K. In seiner einfacheren Form (kleiner HNS) besagt der HNS grob gesprochen: Ist ein algebraisches Gleichungssystem in endlich vielen Variablen über einem Körper K nicht widersprüchlich (d.h. kann daraus nicht durch die Bildung von Linearkombinationen die Gleichung $0 = 1$ abgeleitet werden), so gibt es auch Lösungen, die algebraisch über K sind, also im algebraischen Abschluss von K liegen. Die Vollversion des HNS nimmt zu einer gegebenen Menge $M \subseteq K[x_1, \ldots, x_n]$ von Polynomen mit gemeinsamer Lösungsmenge L die (jedenfalls M umfassende) Menge I *aller* $f \in K[x_1, \ldots, x_n]$ in den Blick, die von ganz L gelöst werden. Es ist fast trivial, dass I ein Ideal ist. Der volle HNS besagt nun, dass unter sämtlichen Idealen $I \lhd K[x_1, \ldots, x_n]$ genau jene tatsächlich in der beschriebenen Weise auftreten, die $\mathrm{Rad}(I) = I$ erfüllen.
Der Beweis des vollen HNS ist das Ziel in diesem Abschnitt. Erreichen werden wir es in 10.3.4. Der Beweis baut auf dem kleinen HNS aus 10.3.3 auf, für den wiederum das sogenannte Noethersche Normalisierungslemma aus 10.3.2 das entscheidende Hilfsmittel ist. Eingeleitet wird der Abschnitt in 10.3.1 mit einführenden Bemerkungen zur algebraischen Geometrie, einem wichtigen Teilgebiet der Mathematik, als dessen Ausgangspunkt der HNS gelten kann. Den Anfang macht die Galoiskorrespondenz zwischen K^n und $K[x_1, \ldots, x_n]$, die für $(a_1, \ldots, a_n) \in K^n$ und $f \in K[x_1, \ldots, x_n]$ durch die Relation $f(a_1, \ldots, a_n) = 0$ induziert wird.

10.3.1 Die Ausgangssituation in der algebraischen Geometrie

In der algebraischen Geometrie untersucht man Lösungsmengen algebraischer Gleichungssysteme in mehreren Variablen. Gegenstand ist daher die Relation $\perp$, definiert durch

$$f \perp (a_1, \ldots, a_n) \Leftrightarrow f(a_1, \ldots, a_n) = 0,$$

wobei K ein Körper, $a_1, \ldots, a_n \in K$ und $f \in K[x_1, \ldots, x_n]$. Die Relation $\perp$ induziert eine Galoisverbindung zwischen K^n und $K[x_1, \ldots, x_n]$. Die Galois-abgeschlossenen Mengen in K^n heißen *Varietäten* (= Lösungsmengen algebraischer Gleichungssysteme), jene in $K[x_1, \ldots, x_n]$ sind offensichtlich einmal Ideale. Unser Ziel ist zu verstehen, wie die Galois-abgeschlossenen Mengen in $K[x_1, \ldots, x_n]$ genau aussehen.
Für Polynome in einer einzigen Variablen über einem algebraisch abgeschlossenen Körper K ist eine Gleichung $f(x) = 0$ genau dann lösbar, wenn f kein konstantes Polynom $\neq 0$ ist, die Gleichung also nicht schon auf offensichtliche Weise widersprüchlich ist. Ähnliches wird sich auch für Gleichungssysteme in mehreren Variablen herausstellen. Dabei betrachten wir ein System

$$(*) \begin{cases} f_1(x_1, \ldots, x_n) &= 0 \\ & \vdots \\ f_k(x_1, \ldots, x_n) &= 0 \end{cases}$$

als offensichtlich widersprüchlich, falls eine geeignete Linearkombination der f_j ein konstantes Polynom $c \neq 0$ darstellt:

$$\sum_{j=1}^{k} \lambda_j f_j \equiv c \neq 0$$

Das ist äquivalent dazu, dass das von den f_j erzeugte Ideal ganz $K[x_1, \ldots, x_n]$ ist. Der Hilbertsche Nullstellensatz in seiner schwachen Form (kleiner Nullstellensatz 10.3.3.2) besagt, dass im Falle eines algebraisch abgeschlossenen Körpers diese offensichtliche Art von Widerspruch die einzige Möglichkeit ist, Lösungen des Gleichungssystems zu verhindern. Anders formuliert: Ein Ideal, das außer 0 keine Konstanten enthält, das also nicht bereits der ganze Polynomring $K[x_1, \ldots, x_n]$ ist, hat im algebraischen Abschluss gemeinsame Nullstellen. (Man beachte die Analogie zum Fall eines einzigen Polynoms in nur einer Variablen.) Oder, in der Sprache der Galoiskorrespondenzen: Ist $I \lhd K[x_1, \ldots, x_n]$ nicht der gesamte Polynomring, dann auch sein Galois-Abschluss. Der volle Nullstellensatz 10.3.4.1 verschärft diese Aussage, indem er den Galois-Abschluss von I sehr explizit beschreibt als Radikal $\mathrm{Rad}(I)$ von I.
Zur Rechtfertigung des Schlagwortes *algebraische Geometrie* ist noch eine kurze Bemerkung angebracht. Zunächst induzieren Polynome $f \in K[x_1, \ldots, x_n]$ Polynomfunktionen, also K-wertige Funktionen auf K^n. Sei nun V eine Varietät, d.h. die Nullstellenmenge eines Ideals I. Interessiert man sich für die Einschränkung von Polynomfunktionen auf V, so sind $f, g \in K[x_1, \ldots, x_n]$ genau dann zu identifizieren, wenn die zugehörigen Polynomfunktionen f, g auf V übereinstimmen. Offenbar ist das genau dann der Fall, wenn ihre Differenz $f - g$ im Ideal J liegt, das V durch die von der Nullstellenrelation $\perp$ induzierten Galoiskorrespondenz zugeordnet wird. Das ist aber gerade der Galois-Abschluss von I. Die Einschränkung der Polynomfunktionen auf V entspricht algebraisch also dem Übergang zum Faktorring $K[x_1, \ldots, x_n]/J$ mit dem Galois-abgeschlossenen Ideal J. Erinnert man sich an den Fall $K = \mathbb{R}$, die über $\mathbb{R}$ definierten euklidischen Vektorräume und an die dort auf der Hand liegende geometrische Interpretation von Lösungsmengen von Gleichungssystemen, so verwundert es nicht mehr, dass sich für jenes große

Teilgebiet der Mathematik, das die hier angedeuteten Ansätze vertieft, die Bezeichnung „algebraische Geometrie“ eingebürgert hat. Wir werden diesen geometrisch orientierten Pfad allerdings nicht weiter verfolgen.

10.3.2 Parametrisierung in Ringerweiterungen

Zur Motivation des folgenden Lemmas der großen Algebraikerin Emmy Noether (1882–1935) erinnern wir uns an Satz 6.1.5.6: Jede Körpererweiterung $K \leq E$ lässt sich interpretieren als eine Verkettung zweier Erweiterungen: einer rein transzendenten $K \leq Z = K(T)$ mit einer Transzendenzbasis T von E, gefolgt von der rein algebraischen Erweiterung $Z \leq E$. Ersetzen wir die Körpererweiterung $K \leq E$ durch eine endlich erzeugte Ringerweiterung $K \leq R$ des Körpers K und „algebraisch“ durch „ganz“, so erhalten wir die Aussage des Normalisierungslemmas.

Satz 10.3.2.1 (Noethersches Normalisierungslemma)**.** *Sei R ein Integritätsbereich und eine endlich erzeugte Ringerweiterung des Körpers K. Dann existieren algebraisch unabhängige $t_1, \ldots, t_r \in R$, sodass R ganz ist über $K[t_1, \ldots, t_r]$. Dabei ist r der Transzendenzgrad des Quotientenkörpers E von R über K.*

Beweis. Sei $R = K[u_1, \ldots, u_n]$, also $E = K(u_1, \ldots, u_n)$. Sind $u_1, \ldots, u_n$ algebraisch unabhängig über K, so ist $\{u_1, \ldots, u_n\}$ eine Transzendenzbasis von E über K. Also folgt die Behauptung mit $r = n$ und $t_i = u_i$. Seien daher $u_1, \ldots, u_n$ algebraisch abhängig, also $r \leq n - 1$. Dann gilt eine Beziehung der Form

$$\sum_{(i_1,\ldots,i_n)\in I} k_{i_1\ldots i_n} u_1^{i_1} \ldots u_n^{i_n} = 0 \tag{10.1}$$

mit $\emptyset \neq I \subseteq \mathbb{N}^n$ endlich und $k_{i_1\ldots i_n} \in K \setminus \{0\}$ für alle $(i_1, \ldots, i_n) \in I$. Wählen wir $c \in \mathbb{N}$ mit $c > \max\limits_{(i_1,\ldots,i_n)\in I} \max(i_1, \ldots, i_n)$, dann sind die ganzen Zahlen

$$i_1 + ci_2 + \ldots + c^{n-1} i_n$$

für $(i_1, \ldots, i_n) \in I$ paarweise verschieden (Darstellung zur Basis c). Daher gibt es ein eindeutiges Tupel $(j_1, \ldots, j_n) \in I$, sodass

$$e := j_1 + cj_2 + \ldots + c^{n-1} j_n$$

maximal ist. Wir definieren nun

$$\begin{aligned} v_2 &:= u_2 - u_1^c \\ v_3 &:= u_3 - u_1^{c^2} \\ &\vdots \\ v_n &:= u_n - u_1^{c^{n-1}}, \end{aligned}$$

also $u_i = v_i + u_1^{c^{i-1}}$ für $2 \leq i \leq n$. Durch Ausmultiplizieren mithilfe des binomischen Lehrsatzes ergibt sich

$$u_1^{i_1} u_2^{i_2} \dots u_n^{i_n} = u_1^{i_1} (v_2 + u_1^c)^{i_2} \dots (v_n + u_1^{c^{n-1}})^{i_n} = u_1^{i_1 + ci_2 + \dots + c^{n-1} i_n} + h(u_1, v_2, \dots, v_n)$$

für ein Polynom $h \in K[x_1, \dots, x_n]$, wobei der Grad von x_1 in h kleiner ist als die Summe $i_1 + ci_2 + \dots + c^{n-1} i_n$. Wenden wir dies auf jeden Summanden von (10.1) an und beachten, dass $(j_1, \dots, j_n)$ eindeutig (!) so gewählt war, dass diese Summe maximiert wird, so können wir die Terme $k_{i_1 \dots i_n} u_1^{i_1 + ci_2 + \dots + c^{n-1} i_n}$ für $(i_1, \dots, i_n) \neq (j_1, \dots, j_n)$ sowie sämtliche Terme der Form $k_{i_1 \dots i_n} h(u_1, v_2, \dots, v_n)$ zu einem gemeinsamen polynomiellen Ausdruck zusammenfassen und erhalten

$$k_{j_1 \dots j_n} u_1^e + f(u_1, v_2, \dots, v_n) = 0$$

für ein Polynom $f \in K[x_1, \dots, x_n]$, wobei der Grad von x_1 in f kleiner ist als $e = j_1 + cj_2 + \dots + c^{n-1} j_n$. Das Polynom

$$g(x) := x^e + k_{j_1 \dots j_n}^{-1} f(x, v_2, \dots, v_n) \in K[v_2, \dots, v_n][x]$$

ist monisch und hat u_1 als Nullstelle. Also ist u_1 ganz über $K[v_2, \dots, v_n]$, und damit ist $K[u_1, v_2, \dots, v_n] = K[v_2, \dots, v_n][u_1]$ wegen Satz 10.2.1.2(d) ganz über $K[v_2, \dots, v_n]$. Wegen $v_i = u_i - u_1^{c^{i-1}}$ sind außerdem $u_2, \dots, u_n$ auf triviale Weise ganz über $K[u_1, v_2, \dots, v_n]$. Nochmals nach Satz 10.2.1.2(d) ist daher auch $K[u_1, u_2, \dots, u_n]$ ganz über $K[v_2, \dots, v_n]$. Sind nun die $v_2, \dots, v_n$ algebraisch unabhängig, so ist $\{v_2, \dots, v_n\}$ eine Transzendenzbasis von E über K und die Behauptung ist mit $r = n - 1$ sowie $t_i := v_{i+1}$ gezeigt. Sind die $v_2, \dots, v_n$ algebraisch abhängig, so wiederholt man die obige Vorgangsweise und erhält, dass $K[v_2, \dots, v_n]$ ganz ist über $K[w_3, \dots, w_n]$, etc. Nach endlich vielen Schritten bricht dieser Prozess ab, und die Behauptung folgt. □

10.3.3 Der kleine Nullstellensatz

Eine „kleine“ (oder auch „schwache“) Version des Hilbertschen Nullstellensatzes besagt im Wesentlichen, dass jedes System aus polynomialen Gleichungen $f_i(x_1, \dots, x_n) = 0$ über einem Körper K in den Variablen $x_1, \dots, x_n$, aus dem sich nicht durch die Bildung von Linearkombinationen der Widerspruch $1 = 0$ ableiten lässt, eine Lösung $(x_1, \dots, x_n) = (a_1, \dots, a_n)$ mit Komponenten a_i aus dem algebraischen Abschluss $\overline{K}$ von K hat. Bevor wir den Beweis in allen Details führen, folgt eine Skizze der Argumentation.

Denkt man an die Methoden der algebraischen Körpererweiterung und insbesondere den Satz von Kronecker 6.2.1.1 zur Nullstellensuche von Polynomen in einer Variablen, so liegt folgende Konstruktion nahe: Die Voraussetzung an das Gleichungssystem besagt, dass das von den f_i erzeugte Ideal I nicht der gesamte Polynomring $K[x_1, \dots, x_n]$ ist. Erweitert man I zu einem maximalen Ideal $J \lhd K[x_1, \dots, x_n]$, so ist der Faktorring $L := K[x_1, \dots, x_n]/J$ ein Körper, den wir vermittels $k \mapsto k + J$ als Körpererweiterung von K auffassen. Die Elemente $a_i' := x_i + J$ bilden (analog zum Satz von Kronecker

für Polynome in einer Variablen) eine Lösung $(a'_1, \ldots, a'_n)$ des ursprünglich gegebenen Gleichungssystems. Wir wollen Lösungen aber in $\overline{K}$ finden und nicht in L. Wenn wir zeigen können, dass L algebraisch über K ist, dann gibt es eine Einbettung $\iota : L \to \overline{K}$, sodass sich die gesuchte Lösung aus den Komponenten $a_i := \iota(a'_i)$ zusammensetzt. Im Beweis des Satzes von Kronecker (d.h. wenn $n = 1$ und wenn J das von einem irreduziblen und oBdA normierten Polynom f erzeugte Hauptideal ist) ist dies sehr leicht: Denn für $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$ bildet $1 + J, x + J \ldots, x^{m-1} + J$ eine endliche Basis von L über K, da $x^m + J = -\sum_{j=0}^{m-1} a_j(x^j + J)$, und analog für höhere Potenzen von x. Im mehrdimensionalen Fall haben wir die Schwierigkeit, dass wir uns nicht so einfach auf endlich viele Potenzen (und endlich viele Produkte von Potenzen verschiedener Variablen) beschränken können.
Auf den ersten Blick klar ist, dass L über K von endlich vielen Elementen erzeugt wird, nämlich von $x_1+J, \ldots, x_n+J$. Wie der Gedanke an beispielsweise einfache transzendente Körpererweiterungen zeigt, hat das aber nur begrenzte Aussagekraft. Auf den zweiten Blick zeigt sich allerdings, dass der Körper L sogar als *Ring* von $x_1 + J, \ldots, x_n + J$ über K erzeugt wird, dass wir die Elemente $x_1 + J, \ldots, x_n + J$ beim Erzeugungsprozess also nicht invertieren müssen. Diese Beobachtung ermöglicht mithilfe des Noetherschen Normalisierungslemmas den entscheidenden Durchbruch, nämlich in Form des sogenannten *Lemmas von Zariski*:

Folgerung 10.3.3.1 (Lemma von Zariski)**.** *Sei $K \leq L$ eine Körpererweiterung, wobei L eine endlich erzeugte Ringerweiterung von K sei. Dann ist $K \leq L$ eine endlichdimensionale und insbesondere algebraische Körpererweiterung.*

Beweis. Nach dem Noetherschen Normalisierungslemma 10.3.2.1 gibt es algebraisch unabhängige $t_1, \ldots, t_r \in L$, sodass L als Ring ganz über $R := K[t_1, \ldots, t_r]$ ist. Wenn wir $r = 0$ zeigen können, dann ist L ganz über K, insbesondere algebraisch, womit L als Erweiterung von K um endlich viele algebraische Elemente nach dem Gradsatz endlichdimensional über K ist.
Sei also $r \geq 1$ angenommen. Dann ist das von t_1 erzeugte Hauptideal $P := Rt_1 \lhd R$ ein Primideal, da $t_1, \ldots, t_r$ algebraisch unabhängig sind und somit R zum Polynomring $K[z_1, \ldots, z_r]$ isomorph ist, wobei das Element t_1 dem Monom z_1 entspricht. Nach der ersten Aussage von Lemma 10.2.3.1 (Lying-over-Theorem) gibt es ein Primideal $Q \lhd L$ mit $Q \cap R = P$. Als Körper hat L aber nur die trivialen Ideale, insbesondere kein Primideal, womit wir einen Widerspruch erhalten. □

Satz 10.3.3.2 (Kleiner Hilbertscher Nullstellensatz)**.** *Sei E ein algebraisch abgeschlossener Körper mit $K \leq E$ als Unterkörper, außerdem $I \lhd K[x_1, \ldots, x_n]$ ein echtes Ideal (also $I \neq K[x_1, \ldots, x_n]$). Dann ist*

$$I^{(\perp)} := \{(a_1, \ldots, a_n) \in E^n : f(a_1, \ldots, a_n) = 0 \text{ für alle } f \in I\} \neq \emptyset.$$

Beweis. Nach Satz 3.4.2.4 ist I in einem maximalen Ideal $J \lhd K[x_1, \ldots, x_n]$ enthalten. Wegen $J^{(\perp)} \subseteq I^{(\perp)}$ reicht es zu zeigen, dass $J^{(\perp)} \neq \emptyset$. Aufgrund der Maximalität ist $L := K[x_1, \ldots, x_n]/J$ ein Körper, den wir durch die isomorphe Einbettung $k \mapsto k +$

J als Körpererweiterung von K auffassen können[2] – man beachte, dass $k \mapsto k + J$ injektiv ist, da sonst $J \cap K \neq \{0\}$ und somit $J = K[x_1, \ldots, x_n]$ wäre. Wegen $L = K[x_1 + J, \ldots, x_n + J]$ ist L eine endlich erzeugte Ringerweiterung von K. Aus dem Lemma 10.3.3.1 von Zariski folgt, dass $K \leq L$ eine algebraische Körpererweiterung ist. Somit ist ein algebraischer Abschluss $\overline{L}$ von L auch ein algebraischer Abschluss von K, siehe Proposition 6.2.2.4. Als algebraisch abgeschlossener Oberkörper von K enthält E einen weiteren algebraischen Abschluss $\overline{K}$ von K. Wegen der Eindeutigkeit von Zerfällungkörpern und somit algebraischen Abschlüssen modulo Äquivalenz (siehe Satz 6.2.3.1) gibt es einen Isomorphismus $\varphi\colon \overline{L} \to \overline{K}\,(\leq E)$ mit $\varphi|_K = \mathrm{id}_K$. Daraus folgt

$$f(\varphi(x_1 + J), \ldots, \varphi(x_n + J)) = \varphi(f(x_1 + J, \ldots, x_n + J)) = \varphi(0) = 0$$

für alle $f \in J$, sodass die gesuchte Nullstelle $(\varphi(x_1 + J), \ldots, \varphi(x_n + J)) \in J^{(\perp)} \neq \emptyset$ wegen $\varphi(x_i + J) \in E$ gefunden ist. □

10.3.4 Der volle Nullstellensatz

Wir erinnern an die Definition 10.1.4.2 des Radikals $\mathrm{Rad}(I)$ eines Ideals $I \lhd R$ in einem kommutativen Ring R mit 1 als Schnitt aller I umfassenden Primideale sowie an die Darstellung aus Proposition 10.1.4.3 als Menge aller $r \in R$ mit $r^n \in I$ für ein $n > 0$.
Der Hilbertsche Nullstellensatz besagt, dass $I \mapsto \mathrm{Rad}(I)$ der Abschlussoperator der von $\perp$ induzierten Galoiskorrespondenz auf der Polynomseite ist. Daraus folgt sehr unmittelbar der Kleine Nullstellensatz 10.3.3.2: Ist nämlich I ein echtes Ideal in $K[x_1, \ldots, x_n]$, so bedeutet das insbesondere $1 \notin I$. Weil es Primideale P mit $I \subseteq P \neq K[x_1, \ldots, x_n]$ gibt, also $1 \notin P$, folgt daraus nach Definition des Radikals auch $1 \notin \operatorname{Rad} I = \left(I^{(\perp)}\right)^{(\perp)}$, woraus sich $I^{(\perp)} \neq \emptyset$ ergibt.
Es ist bemerkenswert, dass auch umgekehrt der volle Nullstellensatz aus dem Kleinen Nullstellensatz hergeleitet werden kann, allerdings, wie wir gleich sehen werden, unter Verwendung eines sehr originellen Tricks, bei dem man an entscheidender Stelle den kleinen Nullstellensatz für $n + 1$ statt für n verwendet.

Satz 10.3.4.1 (Hilbertscher Nullstellensatz)**.** *Sei E ein algebraisch abgeschlossener Körper, $K \leq E$ und I ein Ideal von $K[x_1, \ldots, x_n]$. Dann ist* $\mathrm{Rad}(I)$ *der Galois-Abschluss von I bezüglich $\perp$, explizit: Die einzigen Polynome, die auf sämtlichen gemeinsamen Nullstellen von I verschwinden, sind jene $f \in K[x_1, \ldots, x_n]$, für die eine Potenz f^n mit positivem n in I liegt.*

Beweis. Für $I = K[x_1, \ldots, x_n]$ ist $\mathrm{Rad}(I)$ als Schnitt über die leere Menge wieder der ganze Polynomring, also gilt der Satz auf triviale Weise. Ab nun sei also I ein echtes Ideal mit Galois-Abschluss $\overline{I}$. Wir haben die beiden Inklusionen $\mathrm{Rad}(I) \subseteq \overline{I}$ und $\overline{I} \subseteq \mathrm{Rad}(I)$ zu zeigen.

$\mathrm{Rad}(I) \subseteq \overline{I}$: Ist $f \in \operatorname{Rad} I$, dann ist $f^m \in I$ für ein $m \geq 1$. Ist $(a_1, \ldots, a_n) \in I^{(\perp)}$, dann ist $0 = f^m(a_1, \ldots, a_n) = (f(a_1, \ldots, a_n))^m$. Also ist $f(a_1, \ldots, a_n) = 0$ und wir schließen

[2] Formal: Wir benennen das Element $k + J \in L$ in k um.

$f \in \left(I^{(\perp)}\right)^{(\perp)} = \overline{I}$.

$\overline{I} \subseteq \mathrm{Rad}(I)$: Sei nun umgekehrt $f \in \overline{I}$, d.h. im Galois-Abschluss von I. Wegen $0 \in \mathrm{Rad}(I)$ dürfen wir $f \neq 0$ annehmen. Betrachte $K[x_1, \ldots, x_n] \leq K[x_1, \ldots, x_n, y]$. Sei L das von I und $y \cdot f - 1$ in $K[x_1, \ldots, x_n, y]$ erzeugte Ideal.
Wir behaupten, dass $L^{(\perp)} = \emptyset$. Denn wäre $(a_1, \ldots, a_n, b) \in L^{(\perp)} \subseteq E^{n+1}$, so auch $(a_1, \ldots, a_n) \in I^{(\perp)} \subseteq E^n$. Es gilt jedoch für alle $(a_1, \ldots, a_n) \in I^{(\perp)}$

$$(yf - 1)(a_1, \ldots, a_n, b) = bf(a_1, \ldots, a_n) - 1 = -1 \neq 0,$$

Widerspruch. Also gilt die Behauptung $L^{(\perp)} = \emptyset$.
Nach dem „Kleinen Nullstellensatz“ 10.3.3.2 kann daher L kein echtes Ideal des Rings $K[x_1, \ldots, x_n, y]$ sein, also $L = K[x_1, \ldots, x_n, y]$. Insbesondere muss $1 \in L$ sein, also

$$1 = \sum_{i=1}^{t-1} g_i \cdot f_i + g_t \cdot (yf - 1),$$

wobei $f_1, \ldots, f_{t-1} \in I$, $g_1, \ldots, g_t \in K[x_1, \ldots, x_n, y]$. Wir definieren einen Einsetzungshomomorphismus $\varphi\colon K[x_1, \ldots, x_n, y] \to K(x_1, \ldots, x_n)$, der K punktweise fest lässt, durch

$$x_j \mapsto x_j \text{ und } y \mapsto \frac{1}{f(x_1, \ldots, x_n)} = f^{-1} \in K(x_1, \ldots, x_n).$$

In obiger Darstellung des konstanten Polynoms 1 fällt bei dieser Ersetzung der letzte Summand weg:

$$1 = \sum_{i=1}^{t-1} g_i(x_1, \ldots, x_n, f^{-1}) \cdot f_i(x_1, \ldots, x_n).$$

Ist $m \in \mathbb{N}$ größer als alle Grade von y in den g_i, dann ist

$$f^m(x_1, \ldots, x_n) \cdot g_i(x_1, \ldots, x_n, f^{-1}) \in K[x_1, \ldots, x_n]$$

für $i = 1, \ldots, t-1$, also

$$f^m = f^m \cdot 1 = \sum_{i=1}^{t-1} \underbrace{f^m(x_1, \ldots, x_n) g_i(x_1, \ldots, x_n, f^{-1})}_{\in K[x_1, \ldots, x_n]} \cdot \underbrace{f_i(x_1, \ldots, x_n)}_{\in I} \in I.$$

Damit ist $f \in \mathrm{Rad}(I)$, was zu zeigen war. □

Index