Algebra

Marc Technau

Marc Technau, Institut für Analysis und Zahlentheorie, Technische Universität Graz, Kopernikusgasse 24, 8010 Graz
Email address: mtechnau@math.tugraz.at
URL: https://www.math.tugraz.at/~mtechnau

2024-01-20 @ 12:14.

Einleitung

Wir greifen inhaltlich des Öfteren auf Inhalte der von mir im Sommer 2021 gehaltenen Vorlesung *Einführung in die Algebra* [33] zurück, beginnen zur Einstimmung aber in Kapitel 1 mit Material, welches im Wesentlichen bekannt sein dürfte (vgl. insbesondere [33, Kapitel 11]). Die Vorlesung orientiert sich nicht konkret an einem Buch. Bei der Ausarbeitung dieser Vorlesung waren jedoch die Lehrbücher [1, 8, 23, 26, 36] hilfreich. Das Buch von Aluffi [1] sei als besonders inspirierend hervorgehoben. Eine hingegen sehr prägnante Darstellung findet man z.B. bei Wolfahrt [36].

Die erste Ausarbeitung dieser Notizen erfolgte zum Wintersemester 2019/20. Die Hörerinnen und Hörerinnen haben mich damals schon sehr fleißig auf einige Fehler hingewiesen. Namentlich sei diesbezüglich Konstantin Andritsch, Iris Holzmannhofer, Stefan Kreiner, Christoph Pratl und Martin Stoiber gedankt. Julian Zalla wies mich ebenfalls auf einige Fehler hin. Nach einer erneuten Abhaltung im Wintersemester 2021/22 ließ mir Christoph Raunjak ebenfalls eine Fehlerliste zukommen. Auch ihm sei gedankt!

Als *Motivation* für die erste Hälfte der Vorlesung betrachten wir folgende Frage: Gegeben ein Polynom $P \in \mathbb{Q}[X]$, kann man eine komplexe Nullstelle von P durch einen Ausdruck angeben, in dem nur rationale Zahlen, arithmetische Operationen (Addition, Subtraktion, Multiplikation, Division) und Ziehung k-ter Wurzeln vorkommen? — Solche Ausdrücke nennen wir ***Wurzelausdrücke***. Beispielsweise ist

$$\sqrt[113]{5-\sqrt{4+\frac{12}{17}}+\frac{11}{42}}$$

ein Wurzelausdruck, wobei wir die berechtigte Frage nach Mehrdeutigkeiten beim Wurzelziehen zunächst bewusst offen lassen. Die Details klären sich dann in § 5.6.)

Für die Nullstellen von Polynomen kleinen Grades lassen sich sehr wohl Wurzelausdrücke gewinnen. Die folgenden Überlegungen dienen primär zur Verschaffung eines Überblicks in die zugrundeliegende Methodik und sind dabei bewusst wenig rigoros.

Beispiele (Wurzelausdrücke für Nullstellen von Polynomen kleinen Grades)**.**

(1) Die Nullstelle des linearen Polynoms $X + a_0 \in \mathbb{Q}[X]$ ist $-a_0$.

(2) Zur Bestimmung der Nullstellen des quadratischen Polynoms $X^2+a_1X+a_0 \in \mathbb{Q}[X]$ benutzen wir quadratische Ergänzung. Es ist

$$X^2 + a_1X + a_0 = (X + a_1/2)^2 + (a_0 - a_1^2/4).$$

Schreibt man also $Y = X + a_1/2$, so gilt es Nullstellen von $Y^2 + (a_0 - a_1^2/4)$ zu finden. Das sind genau $\pm\sqrt{-(a_0 - a_1^2/4)}$ und Rücksubstitution liefert

$$-\frac{a_1}{2} \pm \sqrt{-(a_0 - a_1^2/4)} = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0}}{2}$$

als die Nullstellen des fraglichen Polynoms.

(3) Zur Bestimmung der Nullstellen des kubischen Polynoms $P = X^3 + a_2X^2 + a_1X + a_0 \in \mathbb{Q}[X]$ bedienen wir uns einer analogen Substitution, nämlich $Y = X + a_2/3$. Damit ergibt sich

$$P = Y^3 + \left(a_1 - \frac{a_2^2}{3}\right)Y + \left(\frac{2a_2^3}{27} + a_0 - \frac{1}{3}a_1a_2\right),$$

was wir als

$$P = Y^3 + pY + q \tag{0.1}$$

schreiben; Der Vorteil ist hier die erfolgreiche Elimination des zweithöchsten Terms. (Man vergleiche dies mit der in (2) durchgeführten Substitution!) Als Nächstes stellen wir

$$\begin{aligned}(V + W)^3 &= V^3 + 3V^2W + 3VW^2 + W^3\\ &= V^3 + 3VW(V + W) + W^3\end{aligned}$$

zu

$$(\underline{V + W})^3 - 3VW(\underline{V + W}) - (V^3 + W^3) = 0$$

um, und bemühen — nach einem Vergleich mit (0.1) — den Ansatz

$$Y = V + W, \quad p = -3VW \quad \text{und} \quad q = -(V^3 + W^3),$$

bzw. $Y = W - p/(3W)$ nach Umstellen der zweiten und Einsetzen in die erste Gleichung. Einsetzen in (0.1) liefert dann

$$P = W^3 + q - \frac{p^3}{27W^3}.$$

Nullstellen hiervon sind Nullstellen von $(W^3)^2 + qW^3 - p^3/27$ und diese lassen sich mit der quadratischen Lösungsformel durch Wurzelausdrücke angeben (siehe (2)). Invertiert man dann sämtliche Substitutionen, so gelangt man zu einem Wurzelausdruck für eine Nullstelle von P. Die entstehenden Formeln ganz in Abhängigkeit von a_0, a_1 und a_2 hinzuschreiben macht keine Freude ...

(4) Auch für Polynome vierten Grades kann man die Nullstellen noch durch Wurzelausdrücke angeben.

Bemerkung. Eine deutlich didaktisch hochwertigere Aufbereitung der obigen Beispiele findet man beispielsweise auf dem YouTube-Kanal von Burkhard Polster.[1] Dort werden die oben durchgeführten Substitutionen auch durch geometrische Überlegungen motiviert.

Für höhere Grade führen die obigen Überlegungen im Allgemeinen nicht mehr zu einer Lösung, wie der folgende Satz lehrt. Dieser wurde zuerst 1799 von Paolo Ruffini in lückenhafter Form publiziert. Der erste stichhaltige Beweis gelang Niels Henrik Abel im Jahr 1824. Ein konzeptionell einsichtigerer Beweis gelang Évariste Galois mittels der nach ihm benannten Theorie.

Satz (Abel–Ruffini)**.** *Die Nullstellen von Polynomen vom Grad* 5 *oder höher lassen sich im Allgemeinen nicht durch Wurzelausdrücke angeben.*

Der Beweis des Satzes von Abel–Ruffini benötigt etwas Vorarbeit. Wir führen diesen in § 5.6 im Kontext der noch zu entwickelnden allgemeinen Theorie. Zur Veranschaulichung stellen wir jedoch jetzt schon folgende Überlegung an:
Die Zahl $x = \sqrt[3]{1-\sqrt{2}} \in \mathbb{C}$ ist Nullstelle des (irreduziblen) Polynoms $P = X^6 - 2X^3 - 1 \in \mathbb{Q}[X]$. Beim Ausrechnen von x mittels obigen Wurzelausdrucks erhält man die Zwischenergebnisse

$$1, \quad 1-\sqrt{2}, \quad \sqrt[3]{1-\sqrt{2}} = x$$

und diese führen auf einen Turm von Körpererweiterungen

$$\mathbb{Q} = \mathbb{Q}(1) \subset \mathbb{Q}(1-\sqrt{2}) \subset \mathbb{Q}(x)$$

in dem jeder (nichttriviale) Schritt durch Hinzunahme einer k-ten Wurzel entsteht (hier: $k = 2, 3$). Auch ohne direkte Kenntnis von x kann man aus P einen zu $\mathbb{Q}(x)$ isomorphen Körper konstruieren. Nun stellt sich die Frage, ob wir anhand dessen auch schon „sehen“ können, dass zwischen diesem und $\mathbb{Q}$ ein passender Turm von Zwischenkörpern liegt, der auf einen Wurzelausdruck von x führen würde (auch wenn man x nicht schon als solchen gegeben hätte).

Eine Antwort hierauf liefert die *Galois-Theorie*, welche eine (umkehrbare!) 1:1-Korrespondenz zwischen Zwischenkörpern einer *Körpererweiterung* und Untergruppen von einer geeigneten Automorphismen*gruppe* herstellt. Die Existenz eines passenden Turms übersetzt sich dann in geeignete gruppentheoretische Eigenschaften, die man tatsächlich nachprüfen kann, auch ohne *a-priori* einen Wurzelausdruck für die gesuchten Nullstellen zu kennen.

Die oben angedeutete *Galois-Korrespondenz* hat auch weitere Anwendungen und es lohnt sich die Theorie auch (zumindest in Teilen) für im Wesentlichen beliebige Körpererweiterungen zu entwickeln. Wir beginnen die Vorlesung daher mit entsprechenden Überlegungen zur Körpertheorie …

[1] Siehe `https://youtu.be/N-KXStupwsc`.

Inhaltsverzeichnis

Teil 1

Körpertheorie

KAPITEL 1

Körpererweiterungen

1.1. Charakteristik eines Körpers

Mit ***Ring*** meinen wir stets einen Ring *mit Einselement*. Ein Ringhomomorphismus $f: R \to R'$ erfüllt definitionsgemäß stets $f(1_R) = 1_{R'}$; Eins- und Nullelemente eines Rings R notieren wir oft als 1_R und 0_R, um den Bezug auf R zu betonen, schreiben aber gelegentlich auch einfach nur 1 und 0 (insbesondere, wenn es sich bei dem Ring um einen der Ringe $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$ handelt). Unter „dem“ ***Nullring*** verstehen wir jeden Ring, der nur genau ein Element enthält. In diesem stimmen Eins- und Nullelement überein. Ein ***Integritätsbereich*** ist ein vom Nullring verschiedener kommutativer Ring, der keine Nullteiler enthält. (Ein Element $x \neq 0_R$ eines kommutativen Rings R heißt ***Nullteiler***, falls es ein Element $y \in R$ mit $xy = 0_R$ gibt.)

Wir beginnen unser Studium der Körpertheorie mit der folgenden grundlegenden Beobachtung:

Proposition 1.1. *Jeder Körperhomomorphismus ist injektiv.*

Beweis. Sei $\iota: K \to L$ ein Körperhomomorphismus, dann ist $\ker \iota$ ein Ideal in K. Da K als Körper nur die trivialen Ideale $\{0_K\}$ und K besitzt, folgt $\ker \iota = \{0_K\}$ (beachte $\iota(1_K) \neq 0_L$). Also ist ι injektiv. □

Gemäß der obigen Proposition gibt es in der Körpertheorie keine[1] Faktorbildung wie man sie aus der Ring- oder Gruppentheorie kennt; Es drängt sich die Untersuchung von Teilkörpern — oder umgekehrt — Oberkörpern/Körper*erweiterungen* ins Zentrum der Betrachtungen.

Einen Körperhomomorphismus $\iota: K \to L$ nennen wir ***Körpererweiterung*** oder einfach nur ***Erweiterung***, sofern der Bezug auf Körper klar ist. Speziell falls K ein Teilkörper von L ist (also insbesondere für die zugrundeliegenden *Mengen* $K \subseteq L$ gilt), so schreiben wir für die Körperweiterung $\mathrm{id}_L|_K: K \to L$ auch kurz L/K und sprechen dies als „L über K“. In der Literatur findet man oft auch die Notation $L \mid K$ oder seltener $L : K$ für L/K. Wir benutzen diese Notationen hier nicht, da der Bruchstrich besser zu der oben erwähnten Aussprache passt und eine Verwechslung mit der gleichartig notierten Faktorbildung nicht zu befürchten ist. (L/K als Faktorring

[1] Faktorringe kann man freilich auch bei Körpern bilden, aber Nutzen gewinnt man daraus keinen, da die einzigen Ideale eines Körpers das Nullideal und der Körper selbst sind. Die daraus konstruierten Körper sind damit entweder isomorph zum ursprünglichen Körper, oder zum Nullring.

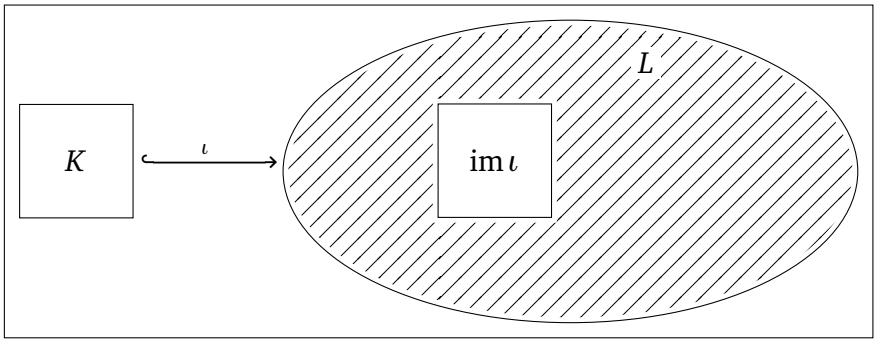


Abbildung 1. Zur Illustration von Proposition 1.1: ein Körperhomomorphismus $\iota\colon K \to L$ bildet K stets auf eine dazu isomorphe Kopie $\iota(K) \subseteq L$ ab.

verstehen zu wollen fiele uns ja allenfalls ein, wenn es sich bei K um ein Ideal von L handelte. Wegen $1_L = 1_K \in K$ tritt Letzteres aber nur im trivialen Fall $K = L$ ein.)

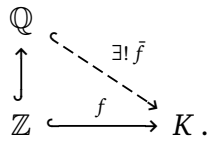
Später, in Kapitel 5, wenn die Theorie hinreichend weit entwickelt ist, werden wir unseren Blick vornehmlich auf Körpererweiterungen L/K richten. Das theoretische Fundament hierzu errichten wir allerdings bereits in § 2.3, wenn wir die Existenz algebraischer Abschlüsse sicherstellen. Grob gesprochen, verfolgen wir die Idee, zunächst für jeden Körper K eine hinreichend große Körpererweiterung $\iota_{\mathrm{a}}\colon K \to K^{\mathrm{a}}$ zu erschaffen, welche groß genug ist, um (bis auf Isomorphie) alle für uns interessanten Körpererweiterungen von K zu enthalten. Fasst man anschließend ι_{a} gedanklich durch Umbenennung von Elementen als Teilmengeninklusion auf, so darf man sich auf das Studium von Körpererweiterungen L/K mit $K \subseteq L \subseteq K^{\mathrm{a}}$ beschränken. Falls man nun im Rahmen dieser Untersuchungen auf Konstruktionsprobleme stößt, die über L hinaus führen, können diese immer noch einfach in K^{a} durchgeführt werden. — So jedenfalls die Hoffnung! Um uns jedoch der Aufgabe der Beschaffung von ι_{a} „aus dem Nichts“ stellen zu können, ist es bequem, sich allgemein mit Körperhomomorphismen $\iota\colon K \to L$ zu beschäftigen.

Eine erste grobe Einteilung von Körpern liefert die folgende Überlegung: Zu einem jeden Körper K gibt es genau einen Ringhomomorphismus $f\colon \mathbb{Z} \to K$. In der Tat erhält man die Eindeutigkeit direkt daraus, dass ein solcher Ringhomomorphismus die Eins in $\mathbb{Z}$ auf die Eins in K abbilden muss und damit schon völlig festgelegt ist, da $\mathbb{Z}$ von 1 additiv erzeugt wird. Für die Existenz rechnet man einfach nach, dass

$$f(0) = 0_K, \quad f(n) = \underbrace{1_K + 1_K + \ldots + 1_K}_{n \text{ mal}}, \quad f(-n) = -f(n) \quad (n \in \mathbb{N})$$

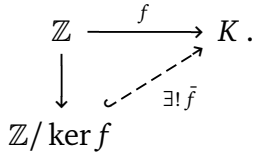
das Gewünschte leistet (vgl. [33, Proposition 6.3]). Wir unterscheiden nun zwei Fälle:

(1) *Ist f injektiv*, so setzt sich f auf genau eine Weise zu einem (injektiven) Körperhomomorphismus $\bar{f}\colon \mathbb{Q} \to K$ fort sodass folgendes Diagramm kommutiert:



($\bar{f}$ bildet einen Bruch $a/q \in \mathbb{Q}$ mit $a, q \in \mathbb{Z}$, $q \neq 0$, auf das Element $f(a)f(q)^{-1} \in K$ ab;[2] eleganter beschafft man sich $\bar{f}$, indem man sich erinnert, dass $\mathbb{Q}$ als Quotientenkörper von $\mathbb{Z}$ natürlich die Lokalisierung $S^{-1}\mathbb{Z}$ von $\mathbb{Z}$ nach dem multiplikativen System $S = \mathbb{Z} \setminus \{0\}$ ist und sich dann auf die universelle Eigenschaft von Lokalisierungen beruft [33, Satz 7.11].) Gemäß Proposition 1.1 ist $\bar{f}$ injektiv und $\mathbb{Q}$ daher via $\bar{f}$ als Teilkörper von K aufzufassen.

(2) *Ist hingegen f nicht injektiv*, also $\ker f \supsetneq \{0\}$, so betrachten wir den kanonischen Ringhomomorphismus $\bar{f}\colon \mathbb{Z}/\ker f \to K$:



($\bar{f}$ bildet eine Restklasse n mod $\ker f$ auf $f(n)$ ab.[3]) Bei $\bar{f}$ handelt es sich um einen injektiven Homomorphismus in einen nullteilerfreien Ring. Dementsprechend ist $\mathbb{Z}/\ker f$ notwendigerweise selbst nullteilerfrei und $\ker f$ also ein Primideal. In $\mathbb{Z}$ sind alle Primideale $\neq \{0\}$ maximale Ideale (da $\mathbb{Z}$ ein Hauptidealbereich ist; siehe [33, Proposition 8.8, Aufgabe 10.2 (c) oder Beispiel 6.11]). Also ist $\mathbb{Z}/\ker f$ ein Körper. Das maximale Ideal $\ker f$ schreibt sich als $\ker f = p\mathbb{Z}$ mit einer Primzahl $p \in \mathbb{N}$.

In der Situation von (2) sagen wir, der Körper K habe ***Charakteristik p***. In der Situation von (1) sagen wir, K habe ***Charakteristik 0***.

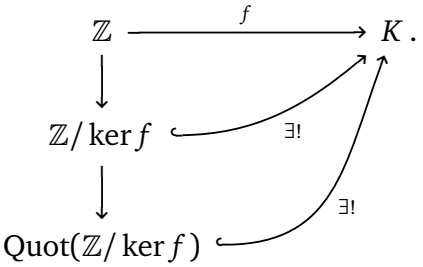
Der jeweils durch $\operatorname{im}\bar{f}$ gegebene Teilkörper von K heißt ***Primkörper von K***. Wegen der Eindeutigkeit von f ist keine Verwechslung zu befürchten, wenn wir etwas

[2] Man überlege sich weshalb $\bar{f}$ einerseits so abbilden *muss*, damit das fragliche Diagramm kommutiert, und andererseits überlege man sich alle weiteren Details: $f(a)f(q)^{-1} = f(a')f(q')^{-1}$ gilt für alle $a, a', q, q' \in \mathbb{Z}$ mit $q, q' \neq 0$ und $a/q = a'/q'$, und durch die Festlegung $\bar{f}(a/q) := f(a)f(q)^{-1}$ erhält man auch wirklich einen Körperhomomorphismus $\mathbb{Q} \to K$, der das fragliche Diagramm kommutativ macht.

[3] Auch hier sind natürlich wieder einige Details bezüglich Existenz und Eindeutigkeit zu klären. Diese sollten im Zusammenhang mit Faktorringen bekannt sein (siehe [33, Satz 6.7]).

unsauber den Definitionsbereich von $\bar{f}$ mit seinem Bild identifizieren und beispielsweise $\mathbb{Q}$ als *den* Primkörper von K bezeichnen, auch wenn $\mathbb{Q}$ streng genommen keine *Teilmenge* von K zu sein braucht.

Bemerkung. Die obige Fallunterscheidung suggeriert die Existenz eines fundamentalen Unterschieds zwischen Körpern der Charakteristik 0 und Körpern mit positiver Charakteristik. Dies ist in der Tat der Fall und wir werden im Verlauf der Vorlesung noch sehen, dass in Charakteristik p oft mehr Vorsicht geboten ist. Dennoch sei hier bemerkt, dass man unsere Argumente zur Einführung der Charakteristik auch leicht zusammenführen kann. Das zugehörige kommutative Diagramm nimmt die folgende Form an:



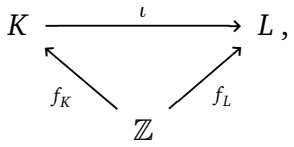
(Man überlege sich als freiwillige Übung, wie die gekrümmten Pfeile zustande kommen; beachte insbesondere $\mathbb{Z}/\{0\} \cong \mathbb{Z}$, $\mathrm{Quot}(\mathbb{Z}/\{0\}) \cong \mathbb{Q}$, sowie $\mathrm{Quot}(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$ für Primzahlen p.)

Bemerkung 1.2. Für jeden Körper K ist dessen Primkörper k durch den Schnitt aller Teilkörper von K gegeben (Aufgabe 1.1). Insbesondere ist der Primkörper von K der kleinste Teilkörper von K (bezüglich mengentheoretischer Inklusion).

Der nächste Satz besagt, dass Körper verschiedener Charakteristik nicht miteinander interagieren und somit gewissermaßen ihr eigenes Reich bilden (siehe auch Abbildung 2).

Satz 1.3. *Sind K, L zwei Körper mit verschiedener Charakteristik. Dann gibt es keinen Körperhomomorphismus $\iota\colon K \to L$.*

Beweis. Wir argumentieren via Kontraposition. Sei $\iota\colon K \to L$ ein Körperhomomorphismus. Wir betrachten dann das folgende Diagramm



wobei f_K und f_L die eindeutigen(!) Ringhomomorphismen von $\mathbb{Z}$ nach K bzw. L sind. Aus der Eindeutigkeit folgt die Kommutativität des Diagramms, d.h. $f_L = \iota \circ f_K$. Es folgt $\ker f_L = \ker(\iota \circ f_K)$. Mit der Injektivität von ι (siehe Proposition 1.1) ergibt sich hieraus $\ker f_L = \ker f_K$. Da diese Kerne aber bereits die Charakteristiken von K und L eindeutig bestimmen, folgt die Behauptung. □

Beispiele 1.4 (Beispiele für Primkörper)**.**

(1) Der Primkörper von $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}(\mathrm{i}) = \mathbb{Q} + \mathrm{i}\mathbb{Q}$, sowie $\mathbb{Q}(\sqrt{2}) = \mathbb{Q} + \sqrt{2}\mathbb{Q}$ ist jeweils $\mathbb{Q}$.
(2) Sei p eine Primzahl. Der Primkörper von $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ist $\mathbb{F}_p$ selbst.
(3) Der Primkörper von $\mathbb{F}_4 = \{0, 1, x, y\}$ mit $\#\mathbb{F}_4 = 4$, $1 + 1 = 0$, $x + 1 = y$ und $x^2 = y$ ist (isomorph zu) $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. (Den Körper $\mathbb{F}_4$ kann man auch konstruieren, indem man $(\mathbb{Z}/2\mathbb{Z})[X]$ nach dem durch das (irreduzible!) Polynom $X^2 + X + 1$ erzeugte maximale Ideal faktorisiert; vgl. [33, Aufgabe 14.2].)
(4) Es gibt auch Körper mit unendlich vielen Elementen, aber endlichem Primkörper; Beispielsweise der Quotientenkörper $\mathrm{Quot}(\mathbb{F}_4[X])$ von $\mathbb{F}_4[X]$ hat ebenfalls den Primkörper $\mathbb{F}_2$.

Zusammen mit den obigen Beispielen und Satz 1.3 erhalten wir einen ersten groben Überblick über Körpern und den Homomorphismen zwischen diesen. Wir illustrieren dies anhand von Abbildung 2.

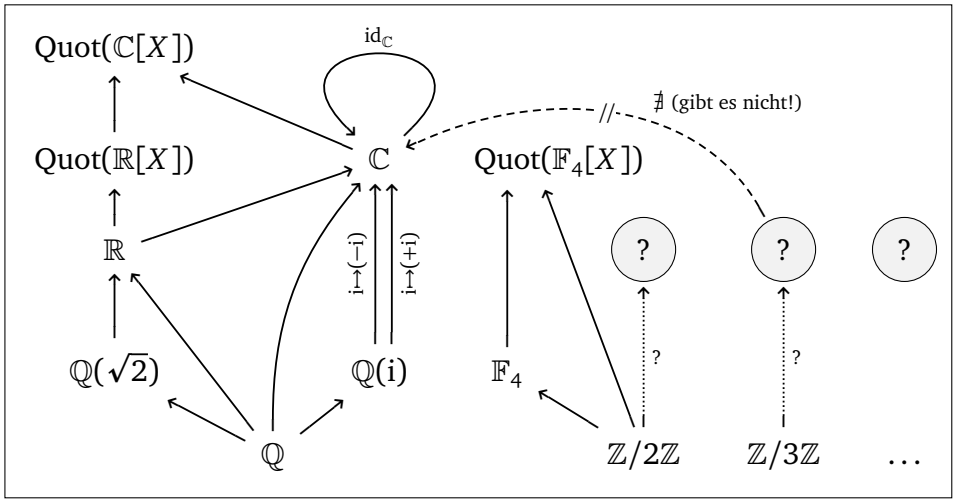


Abbildung 2. Einige Körper und Homomorphismen zwischen diesen. (Dieses Diagramm ist ausnahmsweise mal *nicht* kommutativ! — Weshalb?) Gemäß Satz 1.3 liegen (auch nach beliebiger Ergänzung von Körperhomomorphismen) die Körper $\mathbb{Q}$, $\mathbb{Z}/2$, $\mathbb{Z}/3\mathbb{Z}$, ... ($\mathbb{Z}/p\mathbb{Z}$, p prim) in verschiedenen Zusammenhangskomponenten. In Kapitel 4 werden wir verstehen, wie die Fragezeichen zu ergänzen sind, wenn man sich auf *endliche Körper* beschränkt.

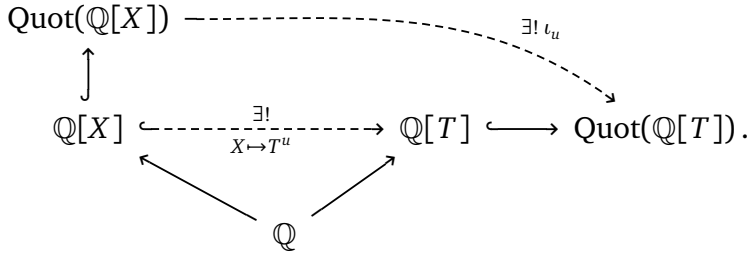
1.2. Grad einer Erweiterung

In diesem Abschnitt kombinieren wir Körpererweiterungen und lineare Algebra. Der hiesige Inhalt sollte bereits aus [33, Kapitel 11] bekannt sein. Jede Körpererweiterung $\iota\colon K \to L$ stattet L mit einer K-Vektorraumstruktur aus: Die Vektoraddition ist die übliche Körperaddition aus L und die Skalarmultiplikation von $x \in L$ mit einem Skalar $\lambda \in K$ sei gegeben durch $\lambda x := \iota(\lambda)x$, wobei auf der rechten Seite die Körpermultiplikation von L benutzt wird.
Wir schreiben $[L : K] = \dim_K L$ für die Dimension des K-Vektorraums L und nennen dies den ***Grad von L über K***.

Beispiele (Beispiele für den Grad einer Körpererweiterung)**.**

- Für jeden Körper K hat die triviale Körpererweiterung K/K Grad $[K : K] = 1$.
- Die Körpererweiterung $\mathbb{R}/\mathbb{Q}$ hat Grad $[\mathbb{R} : \mathbb{Q}] = \infty$.[4]
- Die Körpererweiterung $\mathbb{C}/\mathbb{R}$ hat Grad $[\mathbb{C} : \mathbb{R}] = 2$.
- Auch die Körpererweiterungen $\mathbb{Q}(\mathrm{i})/\mathbb{Q}$ und $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ haben jeweils Grad 2 (vgl. Beispiel 1.4 (1)).

Bemerkung 1.5. Der Bezug auf $\iota\colon K \to L$, welches erst die K-Vektorraumstruktur auf L liefert, wird in der Definition des Grades $[L : K]$ unterdrückt, aber dieser hängt sehr wohl von ι ab. Wählt man etwa $K = \mathrm{Quot}(\mathbb{Q}[X])$ und $L = \mathrm{Quot}(\mathbb{Q}[T])$ und fasst L via des durch $X \mapsto T$ erhaltenen Homomorphismus ι_1 als K-Vektorraum auf, so ist $\dim_K L = 1$. In der Situation mit dem durch $X \mapsto T^2$ erhaltenen Homomorphismus ι_2 gilt hingegen $\dim_K L > 1$. Die fraglichen Homomorphismen erhält man durch „Hochhangeln“ in dem folgenden kommutativen Diagramm, wobei man schrittweise die gestrichelten Pfeile mittels geeigneter universeller Eigenschaften konstruiere $(u = 1, 2)$:



(Siehe [33, Satz 7.4 und Satz 7.11].)

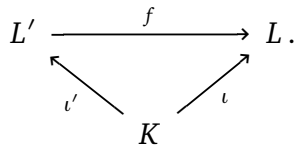
Bemerkung 1.5 lässt erahnen, dass der für Körper bekannte Homomorphiebegriff zu unrestriktiv ist, um Vektorraumstruktur bei Körpererweiterungen zu respektieren. Die nötige Strenge wird (natürlich) durch das zusätzliche Fordern von Linearität bewirkt! Ein Körperhomomorphismus $f\colon L' \to L$ zwischen zwei Körpererweiterungen $\iota'\colon K \to L'$ und $\iota\colon K \to L$ nennen wir einen ***K-Homomorphismus***, falls dieser K-

[4] Man beachte, dass die eines jeden endlich-dimensionalen $\mathbb{Q}$-Vektorraum jeweils zugrundeliegende Menge stets abzählbar ist. Die Menge der reellen Zahlen ist hingegen nicht abzählbar.

linear ist. Ein bijektiver K-Homomorphismus[5] heißt ***K-Isomorphismus***. Existiert ein K-Isomorphismus zwischen den Körpererweiterungen $K \to L'$ und $K \to L$, so nennen wir diese ***K-isomorph***.

Das folgende Resultat stellt ein nützliches Kriterium für K-Homomorphie bereit:

Lemma 1.6. *Ein Körperhomomorphismus $f\colon L' \to L$ zwischen zwei Körpererweiterungen $\iota'\colon K \to L'$ und $\iota\colon K \to L$ ist genau dann ein K-Homomorphismus, wenn das folgende Diagramm kommutiert:*



Beweis. Wir schreiben zwecks besserer Verständlichkeit in diesem Beweis „$*$“ für die K-Skalarmultiplikation auf L' und „$\star$“ für die K-Skalarmultiplikation auf L. Die übliche Multiplikation in den Körpern L' und L notieren wir hier ohne Symbol durch direktes nebeneinanderschreiben der zu multiplizierenden Elemente.

Kommutiert das fragliche Diagramm, so gilt für alle $x' \in L'$

$$f(\lambda * x') = f(\iota'(\lambda)x') = f(\iota'(\lambda))f(x') = (f \circ \iota')(\lambda)f(x') = \iota(\lambda)f(x') = \lambda \star f(x').$$

Also respektiert f die Skalarmultiplikation. Dass f ebenfalls die *Vektoraddition* (d.h. die *Addition in den Körpern L' und L*) respektiert, ist bereits dadurch sichergestellt, dass f als Körperhomomorphismus vorausgesetzt war. Also ist f K-linear und damit ein K-Homomorphismus.

Ist umgekehrt f ein K-Homomorphismus, so gilt für alle $\lambda \in K$

$$\begin{aligned}\iota(\lambda) &= \iota(\lambda)1_L = \iota(\lambda)f(1_{L'}) \\ &= \lambda \star f(1_{L'}) = f(\lambda * 1_{L'}) \\ &= f(\iota'(\lambda)1_{L'}) = f(\iota'(\lambda)) = (f \circ \iota')(\lambda).\end{aligned}$$

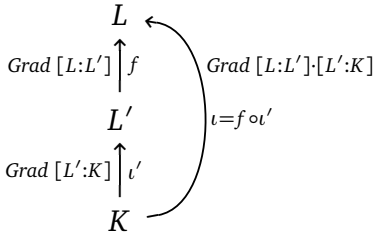
Es folgt $\iota = f \circ \iota'$ und das fragliche Diagramm kommutiert. □

Wir werden im Folgenden Lemma 1.6 zumeist stillschweigend benutzen; im Laufe der Vorlesung konstruieren wir oft Körperhomomorphismen mittels universeller Eigenschaften (häufig über Umwege mit Polynomringen, Faktorringen etc.) und es ergeben sich dann sehr schnell kommutative Diagramme in denen man kommutative Dreiecke wie in Lemma 1.6 ausmachen kann. Die Abbildungen, welche dort die Position von f in Lemma 1.6 einnehmen sind damit dann automatisch K-Homomorphismen und diese Tatsache bedarf keiner weiteren mühseligen Begründung, bei der man auf Ebene der abgebildeten Elemente Linearität nachzurechnen hätte.

[5] Gemäß Proposition 1.1 ist ein K-Homomorphismus ohnehin stets injektiv; Die Surjektivität ist der kritische Punkt.

Wie sich Körpergrade unter Verkettung von Körpererweiterungen verhalten, wird durch die sogenannte ***Gradformel*** beschrieben:

Satz 1.7 (Gradformel). *Seien $\iota' \colon K \to L'$ und $f \colon L' \to L$ zwei Körpererweiterungen. Dann gilt $[L : K] = [L : L'] \cdot [L' : K]$, wobei hier L vermöge des durch Verkettung $f \circ \iota' \colon K \to L'$ erhaltenen Homomorphismus als K-Vektorraum aufgefasst werde.*



Beweis. Seien zunächst $m = [L' : K]$ und $n = [L : L']$ beide endlich. Dann gibt es eine K-Basis $\{b'_1, \ldots, b'_m\}$ von L', sowie eine L'-Basis $\{b_1, \ldots, b_n\}$ von L. Man rechnet nun leicht nach, dass es sich bei

$$\{\, b'_j b_k : 1 \leq j \leq m,\, 1 \leq k \leq n \,\}$$

um eine K-Basis von L handelt; diese hat $[L : K] = mn$ Elemente.

Ist nun einer der Grade $[L' : K]$ oder $[L : L']$ unendlich, so sieht man durch Einschränkung auf endliche Unterräume aus dem Argument von eben auch, dass L als K-Vektorraum Unterräume beliebig großer Dimension enthält. Die Behauptete Formel gilt also im Sinne von „$\infty = \infty \cdot \infty$“ bzw. „$\infty = \infty \cdot k$“ ($k \in \mathbb{N}$) auch im unendlich-dimensionalen Fall. □

Die ernüchternde Beobachtung aus Bemerkung 1.5 löst sich nun mit dem stärkeren Begriff der K-Homo-/Isomorphie in Wohlgefallen auf:

Korollar 1.8. *Es sei $f \colon L' \to L$ ein K-Homomorphismus zwischen zwei Körpererweiterungen $\iota' \colon K \to L'$ und $\iota \colon K \to L$. Dann gelten die folgenden Aussagen:*

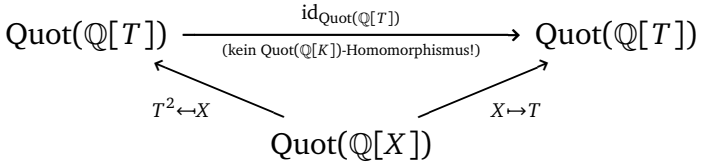
(1) $[L' : K] \leq [L : K]$.
(2) Ist f sogar surjektiv (also ein K-Isomorphismus), so gilt $[L' : K] = [L : K]$.
(3) Ist $[L : K] < \infty$ und gilt $[L' : K] = [L : K]$, so ist f ein K-Isomorphismus.

Beweis. Die Voraussetzungen nebst Lemma 1.6 liefern $\iota = f \circ \iota'$ und damit die Anwendbarkeit von Satz 1.7. Wir haben also

$$[L : K] = [L : L'] \cdot [L' : K] \geq [L' : K].$$

Ist f sogar surjektiv, so ist $[L : L'] = 1$ und die obige Ungleichung gilt dann also sogar mit Gleichheit. Ist alternativ $[L' : K] = [L : K] < \infty$ vorausgesetzt, so handelt es sich bei f dank Proposition 1.1 um eine injektive K-lineare Abbildung zwischen Vektorräumen derselben endlichen Dimension. Also ist f sogar surjektiv und somit ein K-Isomorphismus. □

Bemerkung. Bei der identischen Abbildung $\mathrm{Quot}(\mathbb{Q}[T]) \to \mathrm{Quot}(\mathbb{Q}[T])$ handelt es sich nicht um einen $\mathrm{Quot}(\mathbb{Q}[X])$-Homomorphismus, wenn man $\mathrm{Quot}(\mathbb{Q}[T])$ mittels der beiden in Bemerkung 1.5 erwähnten Homomorphismen ι_2 und ι_1 als Körpererweiterung von $\mathrm{Quot}(\mathbb{Q}[X])$ auffasst. In der Tat kommutiert auch das Diagramm



nicht. (Das sieht man unmittelbar, indem man verfolgt worauf X abgebildet wird.) Hier gilt

$$[\mathrm{Quot}(\mathbb{Q}[T]) : \mathrm{Quot}(\mathbb{Q}[X])]_{\iota_2} > 1 = [\mathrm{Quot}(\mathbb{Q}[T]) : \mathrm{Quot}(\mathbb{Q}[X])]_{\iota_1},$$

wobei wir die Körpergrade jeweils mit dem Homomorphismus als Index annotiert haben, welcher die Vektorraumstruktur stiften soll.

KAPITEL 2

Algebraische Erweiterungen

Zu einer Körpererweiterung $\iota\colon K \to L$ wollen wir nun diejenigen K-Untervektorräume von L untersuchen, die auch Teilkörper von L sind. Hierzu beschränken wir uns zunächst auf die von *einem* Element „erzeugten“ K-Unterräume. Der Begriff des „Erzeugens“ ist hier mit Vorsicht zu gebrauchen. Im Sinne der linearen Algebra wäre hier an 1-dimensionale K-Unterräume Kx zu denken, doch suchen wir hier Teilkörper oder jedenfalls Teilringe von L und jeder solcher enthält mit x auch automatisch x^2 und weitere Potenzen. (Man spricht hier auch von „einfach erzeugten K-Algebren“ anstatt von einfach erzeugten K-Vektorräumen.)
Sei also x ein beliebiges Element von L. Wir betrachten die Menge (wiederholt vorkommende Elemente sollen hier auch mit Vielfachheiten gezählt werden!)

$$\mathscr{M} = \{1_L, x, x^2, x^3, \ldots\} = \{\, x^k : k \in \mathbb{N}_0 \,\} \subseteq L. \tag{2.1}$$

Es gibt zwei Fälle: entweder $\mathscr{M}$ ist K-linear abhängig, oder $\mathscr{M}$ ist K-linear unabhängig. Im ersten Fall nennen wir x ***algebraisch über K*** und anderenfalls ***transzendent über K***. Falls alle Elemente $x \in L$ algebraisch über K sind, so nennen wir die Körperweiterung ι ***algebraisch***.

Teilkörper von L, welche $\operatorname{im}\iota$ enthalten, nennt man ***Zwischenkörper der Körpererweiterung $\iota\colon K \to L$***. Den kleinsten Zwischenkörper von L, der x enthält,[1] notieren wir als $K(x)$ (lies: „***K adjungiert x***“). Man beachte, dass es sich bei diesem insbesondere auch um einen K-Untervektorraum von L handelt (Aufgabe 1.3) und veranschauliche sich die Situation anhand von Abbildung 3.

2.1. Einfache Erweiterungen

Unser nächstes Ziel ist es, $K(x)$ bis auf K-Isomorphie zu bestimmen. Wir erreichen dies durch Satz 2.1 und Satz 2.5.

Satz 2.1. *Sei $\iota\colon K \to L$ eine Körpererweiterung und $x \in L$ algebraisch über K. Ferner sei $m_x = X^n + \mu_{n-1}X^{n-1} + \ldots + \mu_0 X^0 \in K[X] \setminus \{0\}$ das normierte Polynom kleinsten Grades mit*

$$x^n + \mu_{n-1}x^{n-1} + \ldots + \mu_0 x^0 = 0_L.$$

[1] D.h. der kleinste Teilkörper von L, der $(\operatorname{im}\iota) \cup \{x\}$ enthält.

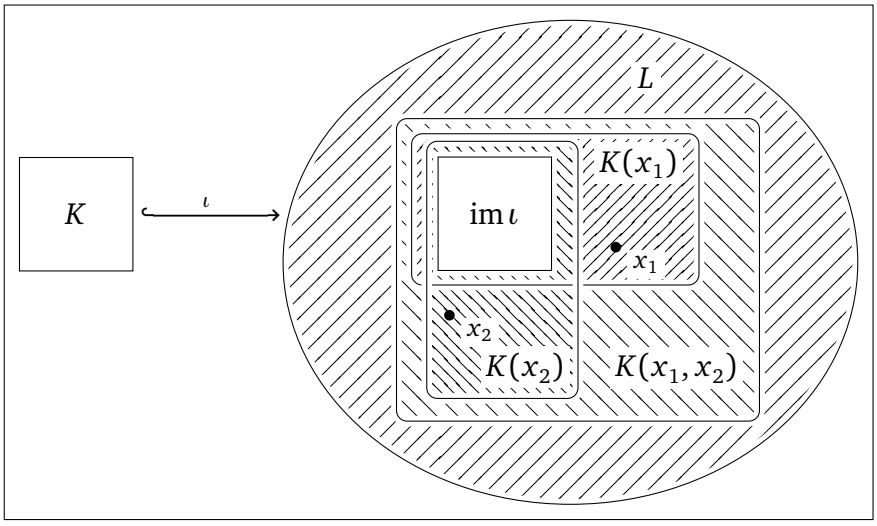


Abbildung 3. Schaubild zur Definition von Adjunktion von Elementen $x_1, x_2 \in L$ mit Bezug auf eine Körpererweiterung $\iota\colon K \to L$.

Dann ist $\mathfrak{m} = m_x K[X]$ *ein maximales Ideal und die Körpererweiterung*[2] $K \to K[X]/\mathfrak{m}$ *ist* K*-isomorph zu der von* ι *induzierten Körpererweiterung* $K \to K(x)$*. Des Weiteren ist*

$$[K(x) : K] = [K[X]/\mathfrak{m} : K] = \deg m_x. \tag{2.2}$$

Das Polynom m_x aus Satz 2.1 nennen wir das ***Minimalpolynom von*** x ***über*** K. Da $m_x K[X]$ ein maximales Ideal ist, handelt es sich bei m_x um ein irreduzibles Polynom. Man bezeichnet die Körpererweiterung $K \to K(x)$ als ***einfach***. (Die Körpererweiterung $K \to L$ heißt ***einfach***, falls $L = K(x)$ für ein $x \in L$ ist.)

Beweis von Satz 2.1. Es gibt genau einen Ringhomomorphismus $\rho\colon K[X] \to L$, der X auf x abbildet und das folgende Diagramm kommutativ macht:

$$\begin{array}{ccc} K[X] & \xrightarrow{\ \rho\ } & L\,. \\ \uparrow & \nearrow_{\iota} & \\ K & & \end{array}$$

Da x algebraisch ist, gibt es Skalare $\lambda_0, \lambda_1, \ldots, \lambda_n \in K$, nicht alle $= 0_L$, mit

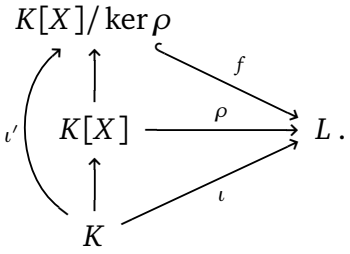
$$\lambda_0 1_L + \lambda_1 x + \ldots + \lambda_n x^n = 0_L,$$

aber letzteres heißt $\rho(\lambda_0 X^0 + \lambda_1 X + \ldots + \lambda_n X^n) = 0_L$. Da nicht alle Skalare gleich 0_L sind, hat ρ also einen nicht-trivialen Kern. Durch Faktorbildung erweitert sich das

[2] Die fragliche Abbildung ist gegeben durch $K \ni \lambda \longmapsto ((\lambda X^0) + \mathfrak{m}) \in K[X]/\mathfrak{m}$.

obige kommutative Diagramm wie folgt:

(2.3)



Mit Argumenten wie bei der Einführung der Charakteristik sieht man, dass es sich bei $K[X]/\ker\rho$ um einen Körper handelt. Insbesondere ist $\mathfrak{m} = \ker\rho$ maximal und der normierte Erzeuger von $\mathfrak{m}$ ist offenbar das im Satz beschriebene Polynom m_x. — Mehr noch: $\iota'\colon K \to K[X]/\ker\rho$ ist eine Körpererweiterung und f ein K-Homomorphismus. Durch Einschränken des Zielbereichs von f auf $\operatorname{im} f = \operatorname{im}\rho = K(x)$ erhält man einen K-Isomorphismus.

Es verbleibt noch (2.2) nachzuweisen. Die erste Gleichheit ist dabei eine direkte Konsequenz aus dem bereits Gezeigten und Korollar 1.8. Für die zweite Gleichheit beachte man, dass sich jedes Polynom aus $K[X]$ — vermöge Polynomdivision durch m_x — in eindeutiger Weise als die Summe eines Polynoms vom Grad $< \deg m_x$ und einem Element von $\mathfrak{m}$ schreibt. Daraus leitet man leicht ab, dass es sich bei den Elementen $X^{j-1} + \mathfrak{m}$ mit $j = 1, \ldots, \deg m_x$ um eine K-Basis von $K[X]/\mathfrak{m}$ handelt. □

Beispiel 2.2. Wir betrachten $x = \sqrt{2} + \sqrt{3}$ in der Körpererweiterung $\mathbb{R}/\mathbb{Q}$. Unter Berücksichtigung des Pascalschen Dreiecks

					1					
				1		1				
			1		2		1			
		1		3		3		1		
	1		4		6		4		1	
$\iddots$		$\vdots$		$\vdots$		$\vdots$		$\vdots$		$\ddots$

berechnet man leicht mittels des Binomischen Lehrsatzes die Potenzen

$$x^2 = 2 + 2\sqrt{2}\sqrt{3} + 3 = 5 + 2\sqrt{6},$$
$$x^3 = 2\sqrt{2} + 3\cdot 2\sqrt{3} + 3\sqrt{2}\cdot 3 + 3\sqrt{3} = 11\sqrt{2} + 9\sqrt{3},$$
$$x^4 = 4 + 4\cdot 2\sqrt{2}\sqrt{3} + 6\cdot 2\cdot 3 + 4\sqrt{2}\cdot 3\sqrt{3} + 9 = 49 + 20\sqrt{6}.$$

Die Menge $\mathscr{M} = \{1, x, x^2, x^3, x^4\}$ ist offenbar linear abhängig, denn wir haben

$$x^4 - 10x^2 + 1 = 0. \tag{2.4}$$

Also ist x algebraisch über $\mathbb{Q}$. Ferner ist $X^4 - 10X^2 + 1$ das Minimalpolynom m_x von x: in der Tat teilt m_x als Erzeuger des Ideals aller x-annulierenden Polynome über

$\mathbb{Q}[X]$ ja $X^4 - 10X^2 + 1$, doch handelt es sich bei $X^4 - 10X^2 + 1$ um ein normiertes, irreduzibles Polynom über $\mathbb{Q}$. Um dabei die Irreduzibilität einzusehen, beachte, dass es genügt die Irreduzibilität des verschobenen Polynoms

$$\tfrac{1}{8}P(2X+1) = 2X^4 + 4X^3 - 2X^2 - 4X - 1$$

über $\mathbb{Q}$ einzusehen. Tatsächlich ist die Irreduzibilität eines Polynoms $G \in \mathbb{Q}[X]$ äquivalent zur Irreduzibilität des reziproken Polynoms $X^{\deg G}G(1/X)$. (Denn jede nicht-triviale Faktorisierung übersetzt sich durch Reziprokenbildung zu einer nicht-trivialen Faktorisierung des reziproken Polynoms und umgekehrt.) Es genügt also die Irreduzibilität von

$$-X^4 - 4X^3 - 2X^2 + 4X + 2$$

nachzuweisen. Das funktioniert aber problemlos mit dem Irreduzibilitätskriterium von Eisenstein [33, Korollar 9.12]. Also ist x algebraisch über $\mathbb{Q}$. Aus Satz 2.1 folgt, dass $\mathbb{Q}(x)/\mathbb{Q}$ Grad 4 haben muss.

Bemerkung. Die Irreduzibilität von $P = X^4 - 10X^2 + 1 \in \mathbb{Q}[X]$ kann man auch einsehen indem man sich klar macht, dass P die vier Nullstellen $\pm\sqrt{2} \pm \sqrt{3}$ (mit unabhängiger Vorzeichenwahl) besitzt. Sei $x = \sqrt{2} + \sqrt{3}$. Wegen $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(x)$ und $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ (das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$ ist $X^2 - 2$) ist 2 ein Teiler von $[\mathbb{Q}(x) : \mathbb{Q}]$. Demnach hat das Minimalpolynom m_x von x mindestens Grad 2 und es teilt P. Aus Gradgründen ist P also irreduzibel, oder zerfällt in ein Produkt quadratischer irreduzibler Faktoren. Es gilt letzteres auszuschließen. Dies sieht man aber (mit etwas Rechenarbeit), indem man alle Produkte $(X - x_1)(X - x_2)$ mit verschiedenen Nullstellen $x_1, x_2 \in \{\pm\sqrt{2} \pm \sqrt{3}\}$ bildet und einsieht, dass diese nicht in $\mathbb{Q}[X]$ liegen; z.B.

$$(X - (\sqrt{2} + \sqrt{3}))(X - (-\sqrt{2} + \sqrt{3})) = X^2 - 2\sqrt{3}X + 1 \notin \mathbb{Q}[X].$$

Korollar 2.3. *Sei $\iota\colon K \to L$ eine Körpererweiterung. Dann ist $x \in L$ genau dann algebraisch über K, wenn $[K(x) : K]$ endlich ist. Ist x algebraisch, so gilt ferner $K(x) = K[x]$, wobei die rechte Seite den kleinsten Teilring von L bezeichne, der $(\operatorname{im}\iota) \cup \{x\}$ enthält.*

Beweis. Ist x transzendent, so enthält $K(x)$ die unendliche linear unabhängige Menge $\mathscr{M}$ aus (2.1) und hat somit unendlichen Grad über K. Ist x algebraisch, so liefert Satz 2.1 die Endlichkeit des Grades $[K(x) : K]$. Ist x nun algebraisch, so erhält man leicht $K[x] = \operatorname{im}\rho = \operatorname{im} f = K(x)$ mit den Abbildungen ρ und f aus (2.3).
(Alternativ verifiziert man leicht, dass es sich bei $K[x]$ um das K-Erzeugnis der Menge $\mathscr{M}$ aus (2.1) handelt. Wenn x algebraisch ist, so enthält $K[x] \subseteq K(x)$ auch alle benötigten inversen Elemente und ist daher gleich $K(x)$: In der Tat ist $K[x]$ ein Unterraum des endlich-dimensionalen(!) K-Vektorraums $K(x) \subseteq L$. Folglich ist der zu $y \in K[x] \setminus \{0_L\}$ durch $K[x] \to K[x]$, $a \mapsto ay$ gegebene injektive K-lineare Endomorphismus sogar auch surjektiv. Es gibt also ein $a \in K[x]$ mit $ay = 1_L \in K[x]$ und das heißt wir haben $y^{-1} \in K[x]$.) □

Bemerkung 2.4. Achtung: Korollar 2.3 trifft keine Endlichkeitsaussage über den Grad $[L : K]$ der gesamten Körpererweiterung $\iota\colon K \to L$, auch wenn L nur aus über K algebraischen Elementen besteht. So hat beispielsweise die Körpererweiterung $\mathbb{C}/\mathbb{Q}$ unendlichen Grad, enthält aber sehr wohl algebraische Elemente: Unter anderem ist $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ eine Körpererweiterung vom Grad zwei. Allerdings enthält $\mathbb{C}$ natürlich auch transzendente Elemente, nämlich sogar überabzählbare viele: Die Menge aller algebraischen Elemente (in $\mathbb{C}/\mathbb{Q}$)

$$\mathbb{A} = \{x \in \mathbb{C} \text{ algebraisch über } \mathbb{Q}\}$$

ist nämlich abzählbar. Tatsächlich handelt es sich bei $\mathbb{A}$ um einen Körper (man überlege sich weshalb!), den ***Körper der algebraischen Zahlen (über $\mathbb{Q}$)***, und damit bei $\mathbb{A}/\mathbb{Q}$ um eine Körpererweiterung. Diese enthält (nach Konstruktion!) nur algebraische Elemente, hat aber dennoch unendlichen Grad. (Man überlege sich z.B. $\mathbb{Q}(\sqrt[n]{2}) \subseteq \mathbb{A}$ und $n = [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] \leq [\mathbb{A} : \mathbb{Q}]$ für $n = 1, 2, 3, \ldots$)

Beispiel. Zur Illustration von Korollar 2.3 erinnere man sich an Beispiel 2.2. Dort hat sich das Minimalpolynom von $x = \sqrt{2} + \sqrt{3}$ bezüglich der Körpererweiterung $\mathbb{R}/\mathbb{Q}$ als $X^4 - 10X^2 + 1$ erwiesen. Demnach haben wir

$$(\sqrt{2} + \sqrt{3})^{-1} = -(\sqrt{2} + \sqrt{3})^3 + 10(\sqrt{2} + \sqrt{3}).$$

(Das erhält man durch Umstellen von $0 = x^4 - 10x^2 + 1 = x(x^3 - 10x) + 1$.)

Satz 2.5. *Sei $\iota\colon K \to L$ eine Körpererweiterung und $x \in L$ transzendent über K. Dann ist die Körpererweiterung $K \to \mathrm{Quot}(K[X])$ K-isomorph zu der von ι induzierten Körpererweiterung $K \to K(x)$.*

Beweis. Der Beweis sei den Leserinnen und Lesern zur Übung überlassen (Aufgabe 2.3).[3] □

2.2. Zerfällungskörper

Zu einem Polynom $P \in K[X]$ und einer Körpererweiterung $\iota\colon K \to L$ kann man P via ι auch als ein Polynom über L auffassen. — Dieses wollen wir mit $\iota^* P$ bezeichnen. Präziser gibt es genau einen Ringhomomorphismus der $X \in K[X]$ auf $X \in L[X]$ abbildet und folgendes Diagramm kommutativ macht:

$$\begin{array}{ccc} K[X] & \xrightarrow{\iota^*} & L[X] \\ \uparrow & & \uparrow \\ K & \xrightarrow[\iota]{} & L\,. \end{array}$$

[3] *Hinweis:* Der Beweis ähnelt in der Weise dem Beweis von Satz 2.1, wie unsere zur Überlegungen vor der Definition von Körpern der Charakteristik 0 denen zu Charakteristik p ähneln.

(Die vertikalen Pfeile bedeuten jeweils die kanonische Abbildung, also diejenige Abbildung, welche das Körperelement λ_0 auf das Polynom $\lambda_0 X^0$ abbildet.) Konkret sieht das so aus:

$$\iota^*(\lambda_0 X^0 + \lambda_1 X + \ldots + \lambda_n X^n) = \iota(\lambda_0)X^0 + \iota(\lambda_1)X + \ldots + \iota(\lambda_n)X^n.$$

Die folgenden Beispiele zeigen, dass man sich $\iota^* P$ einerseits als „P im größeren Ring $L[X]$“ vorstellen sollte, sich aber vor Augen führen muss, dass die Arithmetik in $L[X]$ nicht dieselbe zu sein braucht, wie in $K[X]$.

Beispiele 2.6.

(1) Wir betrachten die durch die Inklusion $\mathbb{Q} \subset \mathbb{C}$ gegebene Körpererweiterung $\iota\colon \mathbb{Q} \to \mathbb{C}$ und das Polynom $P = X^2 - 2 \in \mathbb{Q}[X]$. Dann ist

$$\iota^* P = X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2}) \in \mathbb{C}[X].$$

Man beachte, dass P irreduzibel ist, $\iota^* P$ hingegen aber nicht.

(2) Sei nun $\iota\colon \mathbb{Q} \to L$ die offensichtliche Körpererweiterung mit $L = \mathbb{Q}[T]/\mathfrak{m}$ und dem maximalen Ideal $\mathfrak{m} = (T^2 - 2)\mathbb{Q}[T]$ von $\mathbb{Q}[T]$. Wir betrachten nun erneut das Polynom $P = X^2 - 2 \in \mathbb{Q}[X]$. Dann ist (ganz ähnlich wie in (1))

$$\iota^* P = X^2 - (2 + \mathfrak{m}) = (X - (T + \mathfrak{m}))(X + (T + \mathfrak{m})) \in L[X],$$

wegen

$$(T + \mathfrak{m})^2 = T^2 + \mathfrak{m} = T^2 - (T^2 - 2) + \mathfrak{m} = 2 + \mathfrak{m}.$$

Wir sagen, dass P eine ***Nullstelle in L*** besitzt (oder eher: in der Körpererweiterung $\iota\colon K \to L$), wenn es ein $x \in L$ gibt derart, dass das Polynom $\iota^* P$ ausgewertet bei x Null ergibt: $(\iota^* P)(x) = 0_L$.

Beispiel. Das Polynom $P = X^2 - 2 \in \mathbb{Q}[X]$ hat keine Nullstelle (in $\mathbb{Q}$), aber sehr wohl Nullstellen in $\mathbb{C}$, nämlich $\pm\sqrt{2}$. Überdies hat P auch Nullstellen in $L = \mathbb{Q}[T]/\mathfrak{m}$ aus Beispiel 2.6 (2), nämlich $\pm(T + \mathfrak{m})$.

Wir wenden uns nun der Aufgabe zu, zu einem gegebenen Polynom $P \in K[X]$ eine Körpererweiterung $\iota\colon K \to L$ zu konstruieren in der P eine Nullstelle besitzt. Offensichtlich dürfen wir davon ausgehen, dass P irreduzibel ist (sonst betrachte statt P einen irreduziblen Faktor von P). Mit $P(T)$ bezeichnen wir das Polynom, welches das Bild von P unter dem Ringisomorphismus $K[X] \to K[T]$ ist, der X auf T abbildet. (Einfache Umbenennung der Variablen X in T)

Dann ist $\mathfrak{m} = P(T)K[T]$ ein maximales Ideal von $K[T]$ und $L = K[T]/\mathfrak{m}$ ein Körper und die offensichtliche Abbildung $\iota\colon K \to K[T]/\mathfrak{m}$ ist eine Körpererweiterung (siehe Satz 2.1). Ist $P = \sum_j \lambda_j X^j$, so ist

$$\begin{aligned}(\iota^* P)(T + \mathfrak{m}) &= \sum\nolimits_j \iota(\lambda_j)(T + \mathfrak{m})^j = \sum\nolimits_j (\lambda_j T^0 + \mathfrak{m})(T^j + \mathfrak{m}) \\ &= \sum\nolimits_j (\lambda_j T^j + \mathfrak{m}) = \sum\nolimits_j \lambda_j T^j + \mathfrak{m} = P(T) + \mathfrak{m} = 0_L.\end{aligned} \tag{2.5}$$

(Die eben durchgeführte Rechnung kennen wir letztlich bereits in einem Spezialfall aus Beispiel 2.6 (2).) Also hat P eine Nullstelle in L, nämlich $T + \mathfrak{m}$. Kombiniert man diese Erkenntnis mit Satz 2.1, so erhält man das folgende Resultat:

Satz 2.7 (Kronecker, Cauchy)**.** *Sei $P \in K[X]$ ein irreduzibles Polynom über einem Körper K. Dann hat die Körpererweiterung $\iota\colon K \to L$ mit $L = K[X]/PK[X]$ die folgenden Eigenschaften:*

(1) $[L : K] = \deg P$.
(2) $x = X + PK[X]$ *ist eine Nullstelle des Polynoms* $\iota^* P$.
(3) P *ist assoziiert zum Minimalpolynom* m_x *von* x *über* K.

Beweis. (1) hatten wir im Wesentlichen schon im Beweis von Satz 2.1 argumentiert und (2) haben wir schon in (2.5) nachgerechnet. Es verbleibt (3) zu zeigen. Hierfür beachte man, dass m_x das Ideal $\mathfrak{m} = \{ Q \in K[X] : (\iota^* Q)(x) = 0_L \}$ erzeugt und P wegen (2) in $\mathfrak{m}$ enthalten ist. Wegen (1) und Satz 2.1 (siehe (2.2)) haben aber m_x und $\deg P$ denselben Grad. Also folgt $P = \lambda m_x$ für ein $\lambda \in K \setminus \{0_K\}$. □

Sei $\iota\colon K \to L$ eine Körpererweiterung und $P \in K[X]$ ein Polynom vom Grad $n \geq 0$. Wir nennen L ***Zerfällungskörper von P***, wenn Folgendes gilt:

(1) Es gibt Elemente $c, x_1, \ldots, x_n \in L$ mit $\iota^* P = c \prod_{j=1}^{n} (X - x_j)$ und
(2) $K(x_1, \ldots, x_n) = L$, wobei der Ausdruck linker Hand den kleinsten Teilkörper von L bezeichne, der die Elemente $x_1, \ldots, x_n$ enthält.

Die erste Bedingung besagt, dass P „genug“ Nullstellen in L besitzt, um über L in Linearfaktoren zu zerfallen und die zweite Bedingung besagt, dass L nicht unnötig groß ist.

Da ein Zerfällungskörper $\iota\colon K \to L$ stets durch Adjunktion endlich vieler algebraischer Elemente entsteht, folgt mit Korollar 2.3 und Satz 1.7, dass der Grad $[L : K]$ endlich ist.

Wir beschäftigen uns nun mit der Frage nach Existenz und Eindeutigkeit von Zerfällungskörpern. Der nächste Satz klärt jedenfalls die Existenzfrage. Die Eindeutigkeitsfrage behandeln wir nach einiger Vorarbeit in Proposition 2.10. Für eine Diskussion der dabei auftretenden Körpergrade siehe Aufgabe 3.3.

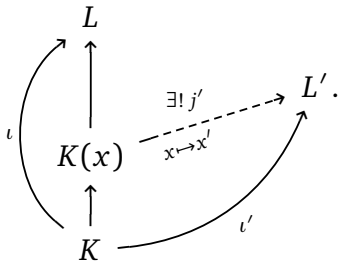
Satz 2.8. *Zerfällungskörper existieren immer. Präziser: Sei K ein Körper und P ein Polynom über K. Dann gibt es eine Körpererweiterung $\iota\colon K \to L$ derart, dass L Zerfällungskörper von P ist.*

Beweis. Das kann man via Satz 2.7 und einer Induktion zeigen. □

Das nächste Resultat erlaubt die Konstruktion von K-Homomorphismen (siehe insbesondere Beispiel 2.11). Die Leserinnen und Leser mögen sich bitte mit Blick auf dessen Beweis klar machen, dass es sich im Endeffekt nur um eine Umformulierung der universellen Eigenschaft von Polynomringen $K[X]$ handelt, welche mittels Faktorbildung auf Körper $K[X]/\mathfrak{m}$ hinübertransportiert wird. Dabei ist freilich darauf

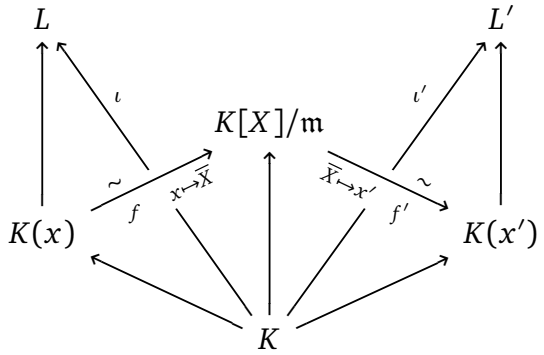
zu achten, dass sich die Ideale $\mathfrak{m}$ geeignet mit den zu transportierenden Homomorphismen vertragen, doch dies wird durch gewisse Annahmen an Minimalpolynome sichergestellt.

Lemma 2.9 (Fortsetzungslemma)**.** *Seien $\iota\colon K \to L$ und $\iota'\colon K \to L'$ zwei Körpererweiterungen, sowie $P \in K[X]$ ein irreduzibles Polynom, $x \in L$ eine Nullstelle von ι^*P und $x' \in L'$ eine Nullstelle von $(\iota')^*P$. Ist $K(x) \subseteq L$ der kleinste Zwischenkörper von $\iota\colon K \to L$, der x enthält,*[4] *so besitzt ι' genau eine Fortsetzung zu einem K-Homomorphismus $j'\colon K(x) \to L'$ mit $j'(x) = x'$:*



Beweis. Gemäß Korollar 2.3 wird der Körper $K(x)$ als K-Vektorraum von den Vektoren $1_L, x, x^2, \ldots$ erzeugt. Für einen K-Homomorphismus j' wie in der Aussage des Lemmas ist also das Bild $j'(1_L) = \iota'(1_K) = 1_{L'}$ bereits festgelegt, aber auch $j'(x) = x'$ und damit $j'(x^k) = (x')^k$ für $k = 1, 2, \ldots$; j' ist uns also bereits auf einer Basis bekannt und daher — sofern es überhaupt ein solches j' gibt — eindeutig.

Zum Beweis der *Existenz* von j' sei $K(x')$ der kleinste Zwischenkörper von $\iota'\colon K \to L'$, der x' enthält. Wir schreiben $\mathfrak{m} = PK[X]$ und $\overline{X} = X + \mathfrak{m}$. Zweimaliges Anwenden von Satz 2.1 liefert dann ein kommutatives Diagramm der Form



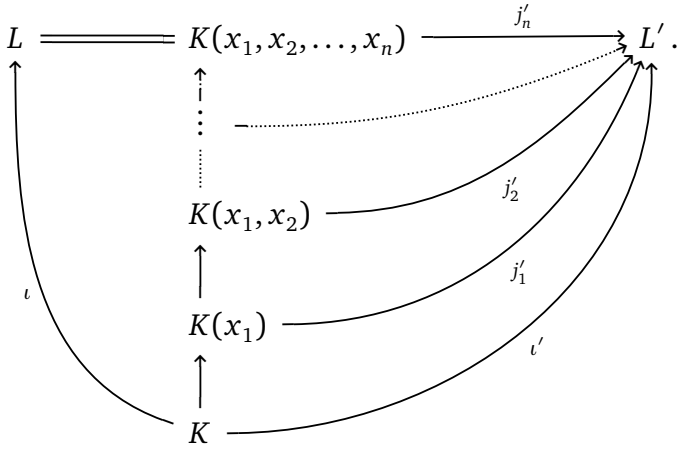
mit K-Isomorphismen f und f', welche $f(x) = \overline{X}$ und $f'(\overline{X}) = x'$ erfüllen. Die Inklusion $K(x') \hookrightarrow L'$ verkettet mit der Abbildung $f' \circ f$ ist offenbar der gesuchte K-Homomorphismus j'. □

[4] Wir betonen diesen Punkt hier, da die Notation $K(x)$ von der zugrundegelegten Körpererweiterung abhängt, diese aber nicht explizit kenntlich macht. Wegen der parallelen Betrachtung von ι und ι' könnte hier also ohne eine solche Klarstellung Verwirrung auftreten.

Bemerkung. Alternativ kann man die Eindeutigkeitsaussage in Lemma 2.9 auch über die universelle Eigenschaft von Polynomringen beweisen. (Tatsächlich ist das zuvor gebrachte Argument, mittels Korollar 2.3 und der Tatsache, dass der K-Homomorphismus j' durch $j'(x) = x'$ bereits eindeutig festgelegt wird, nur eine spezielle Instanz davon.) In der Tat, gäbe es zwei Möglichkeiten für den K-Homomorphismus j', so könnte man zwei verschiedene K-Homomorphismen $K[X]/\mathfrak{m} \to L$ mit $\overline{X} \mapsto x'$ konstruieren. Dann hätte man allerdings (mittels der bekannten Beschreibung von Homomorphismen von Faktorringen) auch zwei verschiedene „K-Homomorphismen“[5] $K[X] \to K(x')$ mit $X \mapsto x'$. Dies widerspricht allerdings der Eindeutigkeitsaussage in der universellen Eigenschaft von Polynomringen.

Proposition 2.10. *Sei $P \in K[X]$ vom Grad $n \geq 1$ (nicht notwendigerweise irreduzibel). Dann sind je zwei Körpererweiterungen $\iota\colon K \to L$ und $\iota'\colon K \to L'$, die beide Zerfällungskörper von P sind, zueinander K-isomorph.*

Beweis. Sei $L = K(x_1, x_2, \ldots, x_n)$ wie in der Definition des Begriffs *Zerfällungskörper*. Wir setzen ι' — vermöge Lemma 2.9 — zu einem K-Homomorphismus $j_1'\colon K(x_1) \to L'$ fort und erhalten induktiv für $k = 2, \ldots, n$ weiter $K(x_1, \ldots, x_{k-1})$-Homomorphismen $j_k'\colon K(x_1, \ldots, x_{k-1}, x_k) \to L'$:



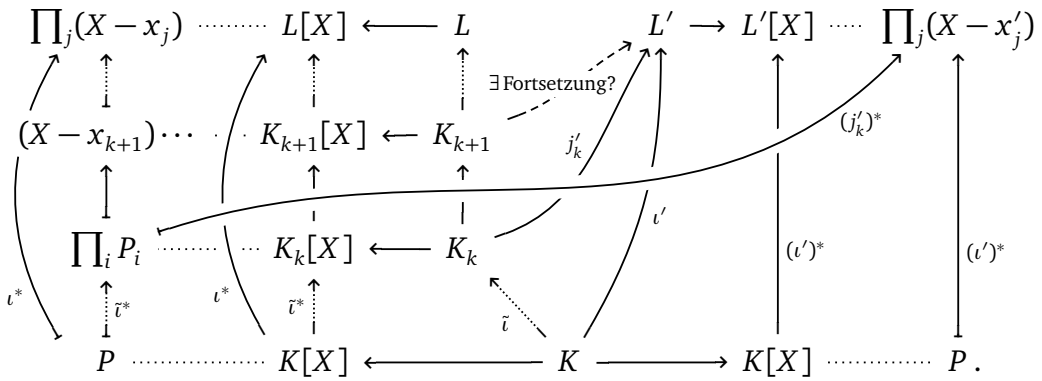
In der Tat sei $\tilde{\iota}\colon K \to K_k$ mit $K_k := K(x_1, x_2, \ldots, x_k)$ die von ι induzierte Körpererweiterung und $\tilde{\iota}^* P$ das Polynom P aufgefasst als Polynom über K_k. Dieses zerlegt sich in ein Produkt $\prod_i P_i$ von irreduziblen Faktoren $P_i \in K_k[X]$ (die natürlich nicht linear zu sein brauchen!) und einer von diesen — nennen wir ihn P_* — hat in $K_{k+1} := K(x_1, x_2, \ldots, x_k, x_{k+1})$ die Nullstelle x_{k+1}. Allerdings hat P_* auch in L' eine Nullstelle x'_{k+1} (denn $(\iota')^* P$ zerfällt in Linearfaktoren und $(j_k')^* P_*$ ist ein Teiler von $(\iota')^* P$), und Lemma 2.9 liefert einen K_k-Homomorphismus $j'_{k+1}\colon K_{k+1} \to L'$ mit

[5] Die kanonische Abbildung $K \to K[X]$ ist natürlich kein Körperhomomorphismus, da $K[X]$ kein Körper ist. Gemeint mit K-Homomorphismus ist hier dennoch, dass ein entsprechendes Diagramm wie in Lemma 1.6 kommutiert.

$j'_k(x_{k+1}) = x'_{k+1}$, wie gewünscht:

$$\begin{aligned}\prod_i (j'_k)^* P_i = (j'_k)^*\Big(\prod_i P_i\Big) = (j'_k)^*(\tilde{\iota}^* P) = (j'_k \circ \tilde{\iota})^* P \\ = (\iota')^* P = \text{Produkt von Linearfaktoren in } L'[X].\end{aligned}$$

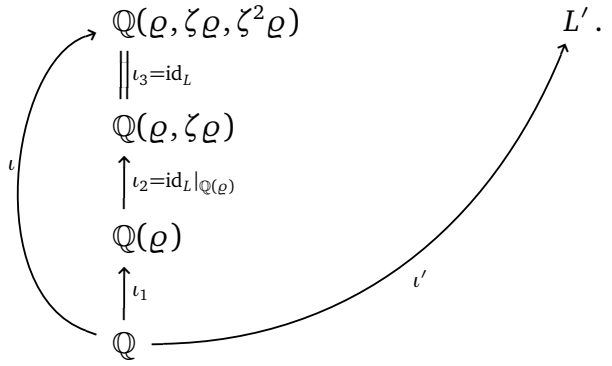
Man veranschaulicht sich diesen Sachverhalt vielleicht anhand des (zugegebenermaßen sehr unübersichtlichen) Diagramms, wobei wir hier P als normiert angenommen haben:



Bei j'_n handelt es sich um eine injektive (siehe Proposition 1.1) K-lineare Abbildung von dem endlichdimensionalen K-Vektorraum L in den ebenfalls endlichdimensionalen K-Vektorraum L'. Also ist $[L : K] \leq [L' : K]$. In analoger Art und Weise erhält man durch Fortsetzung von ι die Aussage $[L : K] \geq [L' : K]$. Also stimmen die Dimensionen von L und L' als K-Vektorräume überein; als injektive lineare Abbildung zwischen endlichdimensionalen Vektorräumen mit gleicher Dimension ist j'_n also sogar surjektiv (siehe Korollar 1.8). Folglich handelt es sich bei j'_n um einen K-Isomorphismus zwischen L und K'. □

Beispiel 2.11. Wir betrachten das Polynom $P = X^3 - 2 \in \mathbb{Q}[X]$ und exerzieren die Konstruktion aus Proposition 2.10 an P durch. Das Polynom P hat in $\mathbb{C}$ die drei Nullstellen $\varrho = \sqrt[3]{2} \in \mathbb{R} \subset \mathbb{C}$, $\zeta\varrho$ und $\zeta^2\varrho$ mit $\zeta = \exp(2\pi i/3)$. Daher handelt es sich bei der Körpererweiterung $L/\mathbb{Q}$ mit $L = \mathbb{Q}(\varrho, \zeta\varrho, \zeta^2\varrho) = \mathbb{Q}(\varrho, \zeta)$ um einen Zerfällungskörper von P. Wir schreiben im Folgenden auch $L' = L$ und betrachten

das kommutative Diagramm



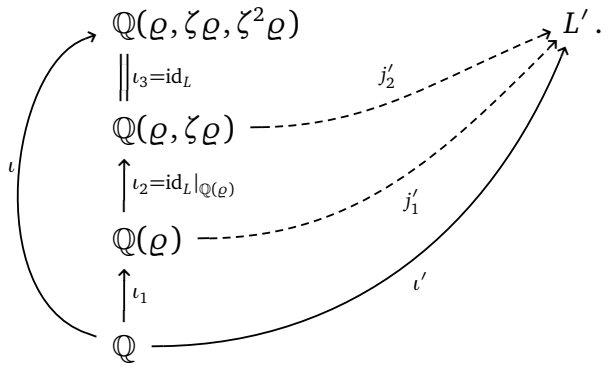
Es gibt nun einen $\mathbb{Q}$-Homomorphismus $j_1'\colon \mathbb{Q}(\varrho) \to L'$, der ϱ auf $\zeta\varrho$ abbildet (Lemma 2.9). Wir haben

$$\iota_1^* P = (X-\varrho)(X^2+\varrho X+\varrho^2) =: (X-\varrho)P_1.$$

Zudem ist $\zeta\varrho$ ist eine Nullstelle von P_1 in L und $\zeta^2\varrho$ ist eine Nullstelle von P_1 in L':

$$(j_1')^* P_1 = X^2 + j_1'(\varrho)X + j_1'(\varrho^2) = X^2 + \zeta\varrho X + (\zeta\varrho)^2 = (X-\varrho)(X-\zeta^2\varrho).$$

Lemma 2.9 liefert also einen $\mathbb{Q}(\varrho)$-Homomorphismus $j_2'\colon \mathbb{Q}(\varrho,\zeta\varrho) \to L'$, der j_1' fortsetzt und $\zeta\varrho \in L$ auf $\zeta^2\varrho \in L'$ abbildet:



Natürlich sind wir wegen $\mathbb{Q}(\varrho,\zeta\varrho) = L$ hier eigentlich schon fertig, wollen aber trotzdem noch den Schritt zu j_3' durchführen, obwohl sich selbstverständlich $j_3' = j_2'$ herausstellen wird. (Das Ziel ist hier zu sehen, dass die oben gegebene Konstruktion auch robust genug ist, um solche degenerierten Fälle zu behandeln.) Nun ist

$$\iota_2^*(\iota_1^* P) = (X-\varrho)(X-\zeta\varrho)(X-\zeta^2\varrho) =: (X-\varrho)(X-\zeta\varrho)P_2$$

und $P_2 \in \mathbb{Q}(\varrho, \zeta\varrho)[X]$ hat in L die Nullstelle $\zeta^2\varrho$ und in L' die Nullstelle ϱ, denn[6]

$$\begin{aligned}(j_2')^* P_2 &= X - j_2'(\zeta^2\varrho) = X - j_2'(\zeta^2\varrho^2\varrho^{-1}) \\ &= X - j_2'(\zeta\varrho)^2 j_2'(\varrho)^{-1} = X - (\zeta^2\varrho)^2(\zeta\varrho)^{-1} \\ &= X - \zeta^3\varrho = X - \varrho.\end{aligned}$$

Entsprechend setzt sich j_2' zu einem $\mathbb{Q}(\varrho, \zeta\varrho)$-Homomorphismus $j_3'\colon \mathbb{Q}(\varrho, \zeta\varrho, \zeta^2\varrho) \to L'$ mit $j_3'(\zeta^2\varrho) = \varrho$ fort.

2.3. Algebraischer Abschluss

Satz 2.12 (Steinitz, 1910). *Jeder Körper K besitzt einen **algebraischen Abschluss**, d.h. es gibt eine algebraische Körpererweiterung $\iota_{\mathrm{a}}\colon K \to K^{\mathrm{a}}$ derart, dass die über K^{a} irreduziblen Polynome genau die linearen Polynome sind.*

Es gibt diverse Beweise von Satz 2.12 — siehe etwa [22] oder [26, 1] (auch unter Berücksichtigung von [18]). Hier folgen wir einer Exposition von K. Conrad [12, „*Constructing algebraic closures, I*“], der den Beweis seinem Bruder B. Conrad (auf eine Konstruktion von E. Artin zurückgehend) zuschreibt.

Beweis von Satz 2.12. Zunächst wählen wir für jedes nichtkonstante,[7] normierte Polynom $P \in K[X]$ verschiedene Variablen $T_{P,1}, \dots, T_{P,\deg P}$, die auch verschieden zu allen anderen so gewählten Variablen seien mögen. Wir schreiben kurz $\boldsymbol{T}$ für die Gesamtheit dieser Variablen und betrachten den über K definierten Polynomring $R = K[\boldsymbol{T}]$ in diesen Variablen. Selbstverständlich sollen in dieser Konstruktion die zu P gewählten Variablen als Nullstellen von P fungieren. Zur Abkürzung schreiben wir im Folgenden

$$\prod\nolimits_k := \prod_{k=1}^{\deg P} \quad \text{und} \quad \sum\nolimits_j := \sum_{j=0}^{(\deg P)-1}.$$

Wir betrachten zunächst das kommutative Diagramm

$$\begin{array}{ccc} K[X] & \xrightarrow{\varrho^*} & R[X] \\ \uparrow & & \uparrow \\ K & \xrightarrow{\varrho} & R, \end{array}$$

[6] Die Aussage, dass das Polynom $X - \zeta^2\varrho \in \mathbb{Q}(\varrho, \zeta\varrho)[X]$ die Nullstelle ϱ in L' habe, mag paradox klingen, rührt aber daher, dass hier L' nicht via der Identität, sondern mittels j_2' als Körpererweiterung von $\mathbb{Q}(\varrho, \zeta\varrho)$ aufgefasst wird, und $X - \zeta^2\varrho \in \mathbb{Q}(\varrho, \zeta\varrho)[X]$ eben erst in das Polynom $(j_2')^*(X - \zeta^2\varrho)$ umgerechnet werden muss.

[7] Achtung: Gemeint sind Polynome P mit $P \neq \lambda X^0$ für alle $\lambda \in K$; Etwa $X^2 + X \in (\mathbb{Z}/2\mathbb{Z})[X]$ liefert bei Einsetzen eines Elements aus $\mathbb{Z}/2\mathbb{Z}$ stets den Wert 0, ist aber in dem von uns gemeinten Sinne dennoch nicht „konstant“.

wobei die unbeschrifteten Abbildungen und ϱ jeweils die offensichtlichen Ringhomomorphismen seien und $\varrho^*(X) = X$ gelte. Man ist also versucht die Relation

$$„\, \varrho^* P = \prod\nolimits_k (X - T_{P,k})\,“$$

gewissermaßen „gewaltsam“ herzustellen. Diese gilt selbstverständlich dann und nur dann, wenn die Koeffizienten $a_{P,j} \in K[\boldsymbol{T}]$ in der Darstellung

$$\varrho^* P - \prod\nolimits_k (X - T_{P,k}) =: \sum\nolimits_j a_{P,j} X^j \tag{2.6}$$

alle gleich Null sind. Das stimmt in R so natürlich nicht, gilt aber sicher, wenn man die fraglichen Koeffizienten (präziser: deren Bilder) im Faktorring $R/\mathfrak{a}$ anschaut, wobei hier $\mathfrak{a}$ das von

$$\{\, a_{P,j} \in K[\boldsymbol{T}] : P \in K[X] \text{ normiert}, \, 0 \le j < \deg P \,\}$$

erzeugte Ideal bezeichnet. Die gewünschten Relationen gelten damit auch in jedem *Körper* $R/\mathfrak{m}$, wenn $\mathfrak{m}$ ein maximales Ideal bezeichnet, welches $\mathfrak{a}$ enthält. Ein solches Ideal gibt es — wie aus [33, Korollar 6.13] bekannt — immer, sofern es sich bei $\mathfrak{a}$ nicht um das triviale Ideal $\mathfrak{a} = R$ handelt.

Wir wollen $1_R \notin \mathfrak{a}$ (und damit $\mathfrak{a} \neq R$) einsehen und gehen daher zwecks Erzeugung eines Widerspruchs gegenteilig von $1_R \in \mathfrak{a}$ aus. Dann gibt es nach Definition von $\mathfrak{a}$ eine Summendarstellung

$$1_R = \sum_{P \in \mathscr{P}} \sum_{j=1}^{\deg P - 1} r_{P,j} a_{P,j} =: \sum_{(P,j)} r_{P,j} a_{P,j}, \tag{2.7}$$

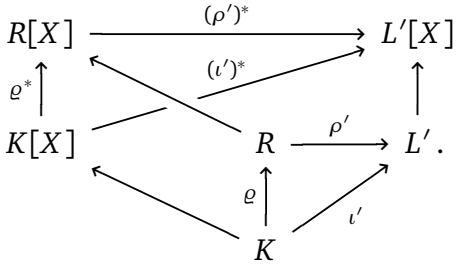
wobei $r_{P,j} \in R$ und $\mathscr{P}$ eine endliche(!) Menge normierter Polynome über $K[X]$ sei. Mit Satz 2.8 erhalten wir einen Zerfällungskörper $\iota' \colon K \to L'$ des Produkts $\prod_{P \in \mathscr{P}} P$. Wir haben also insbesondere für jedes $P \in \mathscr{P}$ eine Darstellung der Form

$$(\iota')^* P = \prod\nolimits_k (X - t_{P,k}) \quad (\text{mit } t_{P,1}, \ldots, t_{P,\deg P} \in L' \text{ geeignet}). \tag{2.8}$$

Man betrachte den Ringhomomorphismus ρ', welcher das Diagramm

$$\begin{array}{ccc} R = K[\boldsymbol{T}] & \xrightarrow{\rho'} & L', \\ \varrho \uparrow & \nearrow_{\iota'} & \\ K & & \end{array} \qquad \text{mit} \quad \rho'(T_{P,k}) = \begin{cases} t_{P,k} & \text{falls } P \in \mathscr{P}, \\ 0_{L'} & \text{falls } P \notin \mathscr{P} \end{cases}$$

kommutativ macht. Dann kommutiert auch das Diagramm

(2.9)


Damit, und in Kombination mit (2.6) und (2.8), sehen wir

$$\begin{aligned}\textstyle\sum_j \rho'(a_{P,j})X^j &= (\rho')^*\Big(\textstyle\sum_j a_{P,j}X^j\Big)\\ &= (\rho')^*\Big(\varrho^*P - \textstyle\prod_k (X - T_{P,k})\Big) && \text{(via (2.6))}\\ &= ((\rho')^* \circ \varrho^*)P - \textstyle\prod_k (X - \rho'(T_{P,k}))\\ &= (\iota')^*P - \textstyle\prod_k (X - t_{P,k}) && \text{(via (2.9) und (2.8))}\\ &= 0_{L'[X]}.\end{aligned}$$

Also ist $\rho'(a_{P,j}) = 0_{L'}$ für alle $P \in \mathscr{P}$ und $0 \le j < \deg P$. Wendet man nun ρ' auf die Gleichung (2.7) an, so erhält man

$$1_{L'} = \rho'(1_R) = \rho'\Big(\sum_{(P,j)} r_{P,j}a_{P,j}\Big) = \sum_{(P,j)} \rho'(r_{P,j})\rho'(a_{P,j}) = \sum_{(P,j)} r_{P,j}0_{L'} = 0_{L'},$$

im Widerspruch dazu, dass im Körper L' natürlich $1_{L'} \neq 0_{L'}$ gilt.

Sei nun $\mathfrak{m} \supseteq \mathfrak{a}$ ein beliebiges maximales Ideal von $R = K[\boldsymbol{T}]$; Dessen Existenz haben wir dank [33, Korollar 6.13] eben mit dem Nachweis von $1_R \notin \mathfrak{a} \neq R$ sichergestellt. Durch Verkettung der offensichtlichen Homomorphismen

$$K \xrightarrow{\ \rho\ } R = K[\boldsymbol{T}] \xrightarrow{\ \pi\ } K[\boldsymbol{T}]/\mathfrak{m} = K^{\mathrm{a}}$$
$$\iota_{\mathrm{a}}$$

erhält man eine Körpererweiterung $\iota_{\mathrm{a}}\colon K \to K^{\mathrm{a}}$. Diese Körpererweiterung hat nun die gewünschte Zerfällungseigenschaft: Wegen $\mathfrak{a} \subseteq \mathfrak{m}$ sieht man

$$\iota_{\mathrm{a}}^*P = \textstyle\prod_k (X - \pi(T_{P,k})) \tag{2.10}$$

für jedes normierte nicht-konstante Polynom $P \in K[X]$, denn

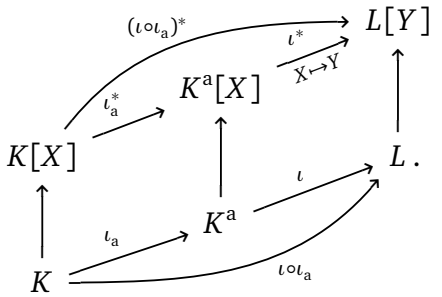
$$\begin{aligned}\iota_{\mathrm{a}}^*P - \textstyle\prod_k (X - \pi(T_{P,k})) &= \pi^*\rho^*P - \pi^*\Big(\textstyle\prod_k (X - T_{P,k})\Big) = \pi^*\Big(\rho^*P - \textstyle\prod_k (X - T_{P,k})\Big)\\ &= \pi^*\Big(\textstyle\sum_j a_{P,j}X^j\Big) = \textstyle\sum_j \pi(a_{P,j})X^j && \text{(via (2.6))}\\ &= \textstyle\sum_j 0_{K^{\mathrm{a}}}X^j = 0_{K^{\mathrm{a}}[X]}. && \text{(Weil } a_{P,j} \in \mathfrak{a} \subseteq \mathfrak{m}.\text{)}\end{aligned}$$

D.h. jedes nichtkonstante Polynom über K zerfällt über K^{a} in Linearfaktoren. Überdies ist die Erweiterung $\iota_{\mathrm{a}}\colon K \to K^{\mathrm{a}}$ algebraisch, denn da

$$\mathscr{B} = \{\, T_1^{\nu_1} \cdots T_k^{\nu_k} \in R : k, \nu_1, \ldots, \nu_k \in \mathbb{N}_0,\ T_1, \ldots, T_k \in \boldsymbol{T} \,\}$$

eine K-Basis von $R = K[\boldsymbol{T}]$ ist, ist $\pi(\mathscr{B})$ zumindest ein K-Erzeugendensystem von L. Für jedes $x \in K^{\mathrm{a}}$ ist also $K(x)$ in $K(\boldsymbol{t})$ enthalten, wobei $\boldsymbol{t}$ eine geeignete endliche Teilmenge von $\pi(\mathscr{B})$ bezeichne. Mit Blick auf (2.10) sieht man, dass alle Elemente von $\pi(T)$ $(T \in \boldsymbol{T})$ algebraisch über K sind und selbiges gilt für alle Elemente von $\boldsymbol{t}$. Mit Korollar 2.3 sieht man also, dass der Grad $[K(\boldsymbol{t}) : K]$ endlich ist; Dieser ist gemäß Korollar 1.8 jedenfalls nicht kleiner als $[K(x) : K]$ und daher ist $[K(x) : K]$ auch endlich. Unter erneuter Berufung auf Korollar 2.3 sieht man somit, dass x algebraisch über K ist.

Es bleibt noch einzusehen, dass es in $K^{\mathrm{a}}[X]$ keine irreduziblen Polynome mit Grad > 1 gibt. Sei daher $m \in K^{\mathrm{a}}[X]$ ein irreduzibles Polynom und $\mathfrak{m} = mK^{\mathrm{a}}[X]$. Dann hat m die Nullstelle $x = X + \mathfrak{m}$ in der Körpererweiterung $\iota\colon K^{\mathrm{a}} \to K^{\mathrm{a}}[X]/\mathfrak{m} =: L$. Der kleinste Zwischenkörper von $\iota_{\mathrm{a}}\colon K \to K^{\mathrm{a}}$, der sämtliche Koeffizienten von m enthält, hat endlichen Grad (benutze Satz 2.1 und Satz 1.7) und x ist algebraisch über diesem. Also folgt, dass x sogar algebraisch über K ist und wir können das Minimalpolynom $m_x \in K[X]$ von x über K betrachten. Wegen der Kommutativität des Diagramms[8]



haben wir

$$0_L = ((\iota \circ \iota_{\mathrm{a}})^* m_x)(x) = (\iota^*(\iota_{\mathrm{a}}^* m_x))(x),$$

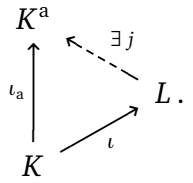
und der Ausdruck rechter Hand ist genau das Bild von $\iota_{\mathrm{a}}^* m_x$ unter der kanonischen Projektion $K^{\mathrm{a}}[X] \to K^{\mathrm{a}}[X]/\mathfrak{m}$. Also folgt $\iota_{\mathrm{a}}^* m_x \in \mathfrak{m}$, weswegen $\iota_{\mathrm{a}}^* m_x$ ein Vielfaches von m ist. Da m_x aber nach dem bereits Gezeigten über K^{a} in Linearfaktoren zerfällt, gilt dies auch für m. Weil m irreduzibel ist, muss m also Grad 1 haben. □

Bemerkung. Die hier verwendete Konstruktionsmethode für algebraische Abschlüsse lässt sich vielleicht kurz als „man nehme einen hinreichend großen Polynomring und faktorisiere diesen nach einem geeigneten Ideal, sodass die Variablen die gewünschten Relationen erfüllen“. Diese Strategie kennen wir schon aus der „Einführung in die Algebra“ [33, § 7.3] von der Konstruktion der Lokalisierung $S^{-1}R$ eines kommutativen Rings R nach einem multiplikativen System $S \subseteq R$.

[8] Man beachte die Einführung der neuen Variablen, da „X“ schon in $L = K^{\mathrm{a}}[X]/\mathfrak{m}$ vorkam.

Das nächste Lemma besagt, dass ein jeder algebraischer Abschluss eines Körpers K reichhaltig genug ist, um gewissermaßen jede algebraische Erweiterung von K „in sich aufzunehmen“.

Lemma 2.13 (Einbettungslemma). *Sei $\iota_a\colon K \to K^a$ ein algebraischer Abschluss von K, sowie $\iota\colon K \to L$ eine beliebige algebraische Erweiterung. Dann gibt es einen K-Homomorphismus $j\colon L \to K^a$:*



Achtung: Im Allgemeinen gibt es in der Situation von Lemma 2.13 sehr viele K-Homomorphismen j; Es wird hier also keinerlei Eindeutigkeitsaussage getroffen!

Für den Beweis von Lemma 2.13 benötigen wir das bereits aus der *Einführung in die Algebra* bekannte ***Lemma von Zorn*** (für mehr hierzu, siehe etwa [26, Appendix 2]). Man beachte auch Abbildung 4.

Lemma 2.14 (Zorn). *Sei $\mathscr{M}$ eine nichtleere Menge, die bezüglich einer binären Relation $\preceq$ **partiell geordnet** ist.*[9] *Ferner besitze jede **Kette***[10] *eine obere Schranke in $\mathscr{M}$. Dann enthält $\mathscr{M}$ mindestens ein maximales Element.*

Beweis von Lemma 2.13. Wir betrachten die Menge

$$\mathscr{J} = \{K\text{-Homomorphismen } f\colon L' \to K^a \text{ mit Zwischenkörper } L' \subseteq L \text{ von } \iota\}$$

und schreiben $\mathrm{dom}(f)$ für L', wenn L' der Definitionsbereich von f ist. Die Menge $\mathscr{J}$ ist nichtleer, denn sie enthält $\iota_a \circ \iota^{-1}\colon \iota(K) \to L$ (wobei ι^{-1} hier als die Umkehrabbildung von $\iota : K \to \iota(K)$ und *nicht* von $\iota : K \to L$ zu verstehen ist, was ja ggf. mangels Surjektivität gar nicht umkehrbar zu sein braucht). Überdies ist $\mathscr{J}$ bezüglich der durch

$$f \preceq \tilde{f} \quad :\Longleftrightarrow \quad \mathrm{dom}(f) \subseteq \mathrm{dom}(\tilde{f}) \text{ und } \tilde{f}|_{\mathrm{dom}(f)} = f$$

definierten Relation partiell geordnet. (Diese Behauptung nachzurechnen involviert mehrere triviale Verifikationen, die wir hier nicht näher ausführen.) Jede Kette $\mathscr{K}$ in $\mathscr{J}$ hat eine obere Schranke $\tilde{f}$ in $\mathscr{J}$, nämlich z.B. $\tilde{f}\colon L' \to K^a$ definiert durch

$$L' = \bigcup_{f \in \mathscr{K}} \mathrm{dom}(f), \quad \tilde{f}(x) = f(x)$$

[9] Zur Erinnerung: Das heißt, dass die Relation $\preceq$ reflexiv, antisymmetrisch und transitiv ist. Allerdings braucht $\preceq$ nicht notwendigerweise ***total*** zu sein, d.h. es kann durchaus Elemente $a, x \in \mathscr{M}$ geben, für die weder $a \preceq x$ noch $x \preceq a$ gilt. — Siehe auch Abbildung 4.

[10] Das ist eine bezüglich $\preceq$ total geordnete Teilmenge von $\mathscr{M}$

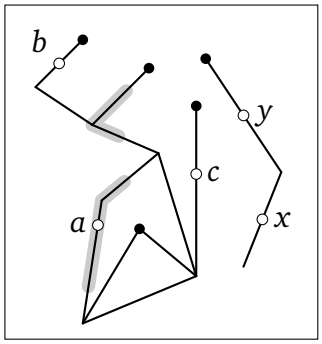


Abbildung 4. Veranschaulichung zum Lemma von Zorn: Die Menge $\mathscr{M}$ sei hier durch das schwarz gefärbte „Gebilde“ im $\mathbb{R}^2$ repräsentiert und ein Punkt darauf sei „kleiner“ als ein anderer Punkt, wenn man von dem Ausgangspunkt stetig und in der Vertikalen monoton steigend zum anderen Punkt „laufen“ kann. Beispielsweise ist a kleiner als b und x kleiner als y. Des Weiteren kann man keinen der Punkte a, b, oder x miteinander vergleichen. Alle maximalen Elemente sind als schwarze Punkte im Gebilde hervorgehoben. Grau hinterlegt sieht man eine Kette.

mit $f \in \mathscr{K}$ und $x \in \mathrm{dom}(f)$. (Auch hier hat man genau genommen wieder einiges nachzurechnen, z.B. dass L' ein Zwischenkörper ist und $\tilde{f}$ wirklich ein Homomorphismus ist.)

Nach dem Lemma von Zorn besitzt $\mathscr{J}$ also ein maximales Element j. Wäre nun nicht $\mathrm{dom}(j) = L$, so könnte man zu $x \in L \setminus \mathrm{dom}(j)$ mittels Lemma 2.9 j zu einem K-Homomorphismus von $\mathrm{dom}(j)(x) \supsetneq \mathrm{dom}(j)$ fortsetzen, was der Maximalität von j widerspräche. Also ist $\mathrm{dom}(j) = L$ und wir sind fertig. □

Der aus Satz 2.12 bereits bekannten Existenzaussage für algebraische Abschlüsse stellen wir nun die folgende wichtige Eindeutigkeitsaussage zur Seite. Deren Beweis schöpfen wir aus Lemma 2.13.

Proposition 2.15. *Je zwei algebraische Abschlüsse von K sind K-isomorph.*

Beweis. Sind $\iota\colon K \to L$ und $\iota'\colon K \to L'$ zwei algebraische Abschlüsse, so kann man zeigen, dass jeder aus Lemma 2.13 erhaltene K-Homomorphismus $j\colon L' \to L$ ein Isomorphismus ist. Die Klärung der zugehörigen Details seien den Leserinnen und Lesern überlassen (Aufgabe 4.3). □

Einen Körper K der K-isomorph zu einem (und dann jedem) algebraischen Abschluss von K ist, nennen wir ***algebraisch abgeschlossen***. Offensichtlich ist K genau dann algebraisch abgeschlossen, wenn jedes nicht-konstante Polynom $P \in K[X]$ in Linearfaktoren zerfällt.

Beispiel. Die Erweiterung $\mathbb{A}/\mathbb{Q}$ aus Bemerkung 2.4 ist ein algebraischer Abschluss von $\mathbb{Q}$. Um dies zu sehen, bemühen wir den Fundamentalsatz der Algebra (siehe später; Satz 5.9). Ist nämlich $P = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{A}[X]$ ein nicht-konstantes Polynom, so zerfällt dieses jedenfalls über $\mathbb{C}$ in Linearfaktoren. Sei $X - z_0 \in \mathbb{C}$ ein solcher Linearfaktor. Wenn wir $z_0 \in \mathbb{A}$ einsehen, folgt die algebraische Abgeschlossenheit von $\mathbb{A}$, da P dann ja schon über $\mathbb{A}$ in Linearfaktoren zerfällt. Sei $K = \mathbb{Q}(a_0, a_1, \ldots, a_n) \subseteq \mathbb{A}$. Dann ist die Erweiterung $K(z_0)/K$ endlich, da z_0 ja Nullstelle von $a_0 + a_1X + \ldots + a_nX^n \in K[X]$ ist. Also ist auch $K(z_0)/\mathbb{Q}$ endlich und somit auch $\mathbb{Q}(z_0)/\mathbb{Q}$. Daraus folgt aber schon $z_0 \in \mathbb{A}$.

Beispiel. Kein endlicher Körper ist algebraisch abgeschlossen. Ist $\mathbb{F}$ nämlich ein endlicher Körper, so ist $1_\mathbb{F} + \prod_{x\in\mathbb{F}}(X - x) \in \mathbb{F}[X]$ ein Polynom vom Grad $\#\mathbb{F} \geq 2$ ohne Nullstellen in $\mathbb{F}$. Insbesondere zerfällt dieses Polynom nicht in Linearfaktoren über $\mathbb{F}$.

2.4. Transzendenzbasen

In Satz 2.5 sind wir bereits mit transzendenten Elementen in Berührung gekommen. Allgemeiner sei $\iota\colon K \to L$ eine Körpererweiterung. Wir nennen Elemente $x_1, \ldots, x_n \in L$ ***algebraisch unabhängig K***, falls der (eindeutige) K-Homomorphismus $\rho\colon K[X_1, \ldots, X_n] \to L$ mit $\rho(X_j) = x_j$ für $j = 1, \ldots, n$, welcher das Diagramm

$$\begin{array}{ccc} K[X_1,\ldots,X_n] & \xrightarrow[\forall j\colon X_j \mapsto x_j]{\rho} & L \\ \uparrow & \nearrow_{\iota} & \\ K & & \end{array}$$

kommutativ macht, injektiv ist.

Beispiel. Sind $x_1, x_2, x_3 \in \mathbb{C}$ algebraisch unabhängig über $\mathbb{Q}$, so ist beispielsweise

$$x_2^{15} - \tfrac{9}{4}x_1x_2x_3^4 + 8 = \rho(X_2^{15} - \tfrac{9}{4}X_1X_2X_3^4 + 8) \neq \rho(0_{K[X_1,\ldots,X_n]}) = 0_L.$$

Algebraische Unabhängigkeit formalisiert die Vorstellung, dass es zwischen den Elementen x_1, x_2, x_3 keine nicht-trivialen algebraischen Relationen gibt. Man vergleiche dies etwa mit algebraischen Elementen: Für diese liefert schon das zugehörige Minimalpolynom eine nicht-triviale algebraische Relation.

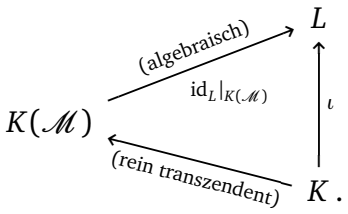
In Verallgemeinerung von Satz 2.5 erhält man durch Fortsetzung von ρ auf $L' = \mathrm{Quot}(K[X_1, \ldots, X_n])$ einen K-Homomorphismus $L' \to L$, der sich auf einen K-Isomorphismus $L' \to K(x_1, \ldots, x_n)$ einschränkt. Körpererweiterungen von K, die K-isomorph zu der Erweiterungen $K \to \mathrm{Quot}(K[X_1, \ldots, X_n])$ für ein $n \in \mathbb{N}_0$ sind, nennen wir ***rein transzendente Erweiterungen***.

Ist $\mathcal{M}$ eine Teilmenge von L mit der Eigenschaft, dass je endlich viele Elemente von $\mathcal{M}$ algebraisch unabhängig sind und $\mathcal{M}$ maximal in der Hinsicht ist, dass keine echte Obermenge von $\mathcal{M}$ diese Eigenschaft hat, so nennen wir $\mathcal{M}$ eine ***Transzendenzbasis*** von der Körpererweiterung $\iota\colon K \to L$.

Man kann sich überlegen, dass für jede Transzendenzbasis $\mathscr{M}$ die Körpererweiterung $L/K(\mathscr{M})$ algebraisch (aber nicht notwendigerweise endlich) ist. So erhält man eine Zerlegung der Erweiterung $\iota\colon K \to L$ in zwei Teilerweiterungen:

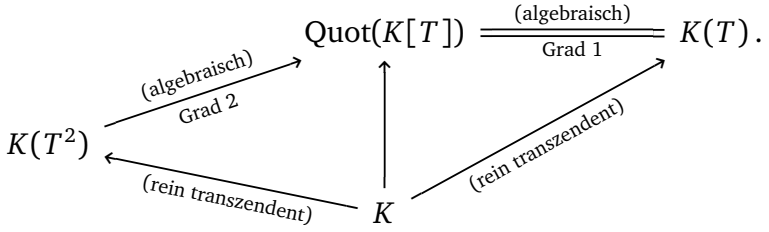
- Eine rein transzendente Erweiterung $K \to K(\mathscr{M})$, und
- eine algebraische Erweiterung $L/K(\mathscr{M})$.

Man veranschaulicht sich diese Situation anhand des folgenden kommutativen Diagramms:



Nach einem ***Satz von Lüroth*** ist für eine einelementige Transzendenzbasis $\mathscr{M}$ jeder echte Zwischenkörper von $K \to K(\mathscr{M})$ selbst eine rein transzendente Erweiterung. — Es sind also alle Elemente von $K(\mathscr{M}) \setminus \operatorname{im}\iota$ transzendent über K.

Man beachte des Weiteren, dass der Grad der obigen algebraischen Erweiterung $L/K(\mathscr{M})$ i.Allg. von der Wahl der Transzendenzbasis $\mathscr{M}$ abhängig ist:



Dennoch ist zumindest die Kardinalität einer Transzendenzbasis wohl-bestimmt und heißt ***Transzendenzgrad*** der betrachteten Körpererweiterung:

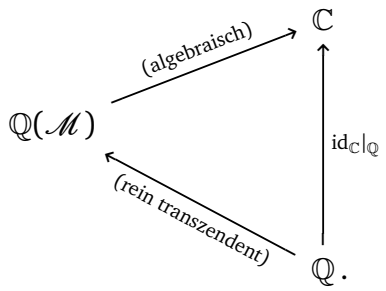
Satz 2.16. *Transzendenzbasen existieren immer. Überdies sind je zwei Transzendenzbasen von ein und derselben Körpererweiterung gleichmächtig.*

Für einen Beweis (eines Spezialfalles) des obigen Satzes, sowie für diverse Rechenregeln und Verträglichkeitseigenschaften von Transzendenzbasen konsultiere man etwa das Buch von Wolfahrt [36, §§ 6.5.1–6.5.2], oder die (fortgeschrittenere) Darstellung von Lang [26, Kapitel VIII, § 1]. Die Existenz von Transzendenzbasen ergibt sich mittels des Zornschen Lemmas (Lemma 2.14): man betrachte die Menge der algebraisch unabhängigen Teilmengen von L und die durch Teilmengeninklusion induzierte partielle Ordnung darauf. Anschließend wähle man ein maximales Element bezüglich dieser partiellen Ordnung mittels des Zornschen Lemmas. Ein solches maximales Element konstituiert dann automatisch eine Transzendenzbasis. Die Aussage über die Mächtigkeit ist aufwändiger zu beweisen (siehe die oben genannte Literatur).

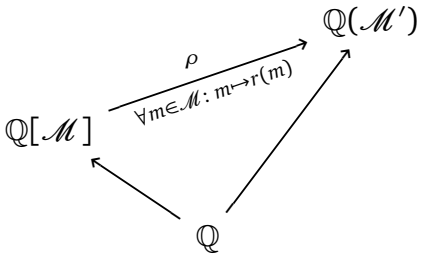
Wir schließen diesen Abschnitt mit einer *Anwendung von Transzendenzbasis-Techniken*: Transzendenzbasen können zur Konstruktion von Körperhomomorphismen benutzt werden. Das folgende Ergebnis findet keine Verwendung im weiteren Verlauf der Vorlesung, ist aber vielleicht hinreichend kontra-intuitiv, um für sich selbst genommen interessant zu sein.

Satz 2.17. *Es gibt echte Teilkörper von den komplexen Zahlen $\mathbb{C}$, welche wiederum zu $\mathbb{C}$ ($\mathbb{Q}$-)isomorph sind.*

Beweisskizze. Man wähle mittels Satz 2.16 eine Transzendenzbasis $\mathscr{M}$ von der Erweiterung $\mathbb{C}/\mathbb{Q}$:

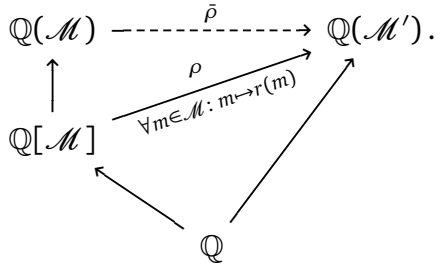


Mit den Ideen aus Aufgabe 3.1 (c) kann man sich überlegen, dass $\mathscr{M}$ überabzählbar (und insbesondere unendlich) ist. Darum gibt es eine Bijektion $r\colon \mathscr{M} \xrightarrow{\sim} \mathscr{M}'$ von $\mathscr{M}$ auf eine *echte* Teilmenge $\mathscr{M}' \subsetneq \mathscr{M}$. (Um die zuletzt gemachte Behauptung tatsächlich zu beweisen, benötigt man das Auswahlaxiom (bzw. eine schwache Form davon). Wir verzichten auf weitere Ausführungen hierzu.) Diese setzt sich (auf genau eine Weise) zu einen Ringhomomorphismus $\mathbb{Q}[\mathscr{M}]$ fort, der das offensichtliche Diagramm



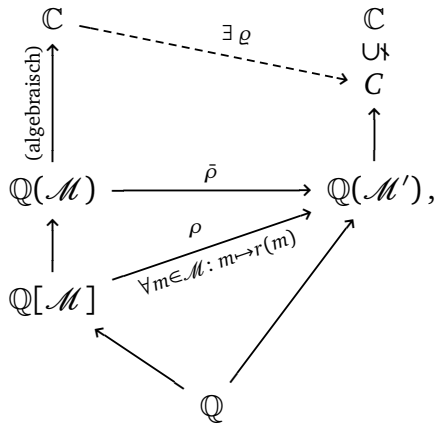
kommutativ macht. Wegen der algebraischen Unabhängigkeit der Elemente von $\mathscr{M}$ und dem injektiven Abbildungsverhalten auf $\mathscr{M}$ (beachte $\rho(m) = r(m)$ für $m \in \mathscr{M}$), ist ρ injektiv und setzt sich also zu einem $\mathbb{Q}$-Homomorphismus $\bar{\rho}\colon \mathbb{Q}(\mathscr{M}) \to \mathbb{Q}(\mathscr{M}')$

fort:



Man kann sich nun überlegen, dass die Menge C aller komplexen Zahlen, die über $\mathbb{Q}(\mathscr{M}')$ algebraisch sind, einen algebraischen Abschluss $\mathbb{Q}(\mathscr{M}') \to C$ von $\mathbb{Q}(\mathscr{M}')$ bilden. (Hierzu bemühe man den *Fundamentalsatz der Algebra*[11] und die Technik aus dem Beweis von Satz 2.12, welche zeigt, dass eine algebraische Erweiterung über der jedes Polynom mit Koeffizienten aus dem Grundkörper zerfällt, bereits ein algebraischer Abschluss ist.)

Da Elemente von $\mathscr{M} \setminus \mathscr{M}'$ transzendent über $\mathbb{Q}(\mathscr{M}')$ sind, ist $C \subsetneq \mathbb{C}$. Weil aber die Erweiterung $\mathbb{C}/\mathbb{Q}(\mathscr{M})$ (nach Wahl von $\mathscr{M}$) algebraisch ist, liefert[12] Lemma 2.13 eine Fortsetzung $\varrho\colon \mathbb{C} \to C$ von $\bar{\rho}$:



und die Einschränkung von ϱ zu $\varrho\colon \mathbb{C} \to \operatorname{im}\varrho$ ist nun ein $\mathbb{Q}$-Isomorphismus von $\mathbb{C}$ auf einen *echten* Teilkörper von $\mathbb{C}$. □

Dass Satz 2.17 tatsächlich überraschend sein sollte, wird durch den nächsten Satz bekräftigt. Dieser besagt, dass die Aussage von Satz 2.17 falsch ist, wenn man $\mathbb{C}$ durch $\mathbb{R}$ ersetzt:

Satz 2.18. *Der einzige ($\mathbb{Q}$-)Homomorphismus von $\mathbb{R}$ nach $\mathbb{R}$ ist* $\mathrm{id}_{\mathbb{R}}$.

[11] Das ist Satz 5.9; Der Beweis folgt später.

[12] Hierzu sollte man sich noch überlegen, dass es sich bei der Verkettung $\mathbb{Q}(\mathscr{M}) \to C$ von der Inklusion $\mathbb{Q}(\mathscr{M}') \to C$ mit $\bar{\rho}$ um einen algebraischen Abschluss von $\mathbb{Q}(\mathscr{M})$ handelt (man beachte, dass es sich hier nicht um $\mathrm{id}_C|_{\mathbb{Q}(\mathscr{M})}$ handelt — $\bar{\rho}$ „wirft“ die Elemente von $\mathbb{Q}(\mathscr{M})$ natürlich sehr wild in $\mathbb{C}$ herum). Das geht aber sehr einfach, weil $\bar{\rho}$ tatsächlich ein $\mathbb{Q}$-Isomorphismus von $\mathbb{Q}(\mathscr{M})$ auf $\mathbb{Q}(\mathscr{M}')$ ist, und $\mathbb{Q}(\mathscr{M}') \to C$ ein algebraischer Abschluss von $\mathbb{Q}(\mathscr{M}')$ ist.

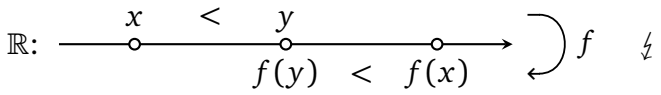
Beweis. Sei $f\colon \mathbb{R} \to \mathbb{R}$ ein $\mathbb{Q}$-Homomorphismus. Die bezüglich der auf $\mathbb{R}$ wohl-bekannten Ordnung positiven Elemente sind genau die Quadrate $\neq 0$ (hierbei geht das aus der *Analysis* bekannte Ergebnis ein, dass *jede* nicht-negative reelle Zahl eine reelle Quadratwurzel besitzt). Da f als Körperhomomorphismus Quadrate von Elementen wieder auf Quadrate abbildet ($\forall x \in \mathbb{R}\colon f(x^2) = f(x)^2$), respektiert f die Ordnung auf $\mathbb{R}$: für $x, y \in \mathbb{R}$ haben wir die Implikation

$$x < y \implies f(x) < f(y).$$

Nun sei $f \neq \mathrm{id}_{\mathbb{R}}$ angenommen und wir werden sehen, dass uns dies auf einen Widerspruch führt. Wegen $f \neq \mathrm{id}_{\mathbb{R}}$ gibt es ein $x \in \mathbb{R}$ mit $f(x) \neq x$ und es gilt also $x < f(x)$ oder $x > f(x)$. Wir betrachten nur den ersteren Fall; Der zweite geht analog. Aus der *Analysis* weiß man, dass $\mathbb{Q}$ dicht in $\mathbb{R}$ liegt. Es gibt also eine *rationale* Zahl y mit

$$x < y < f(x).$$

Wegen $f|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ widerspricht dies aber der Tatsache, dass f die Ordnung auf $\mathbb{R}$ respektiert:



□

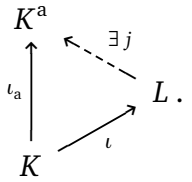
KAPITEL 3

Normale und separable Körpererweiterungen

Die noch zu entwickelnde *Galois-Theorie* ist bemüht Körpererweiterungen $\iota\colon K \to L$ durch die Betrachtung der Gruppe der K-Automorphismen von L zu verstehen. Dafür ist es wichtig, dass diese in zweierlei Hinsicht nicht „zu klein“ ausfällt. Der Ausschluss von dementsprechend degenerierten Fällen führt auf die Begriffe der *Separabilität* und *Normalität*, die Gegenstand des aktuellen Kapitels sind.

3.1. Separabilitätsgrad

Sei $\iota\colon K \to L$ eine algebraische Körpererweiterung und $\iota_{\mathrm{a}}\colon K \to K^{\mathrm{a}}$ ein algebraischer Abschluss von K. (Die nachfolgenden Betrachtungen hängen wegen Proposition 2.15 nicht von der Wahl von K^{a} ab.) In Lemma 2.13 haben wir gesehen, dass es *mindestens* einen K-Homomorphismus $j\colon L \to K^{\mathrm{a}}$ gibt:



Die *Anzahl* solcher K-Homomorphismen j bezeichnen wir als den ***Separabilitätsgrad von $\iota\colon K \to L$***; In Zeichen:

$$[L : K]_{\mathrm{s}} = \#\{K\text{-Homomorphismen } L \to K^{\mathrm{a}}\}.$$

Wie groß ist $[L : K]_{\mathrm{s}}$?

Lemma 3.1. *Sei $\iota\colon K \to K(x)$ eine einfache algebraische Erweiterung und m_x das Minimalpolynom von x. Für jeden algebraischen Abschluss $\iota_{\mathrm{a}}\colon K \to K^{\mathrm{a}}$ von K gilt dann*

$$[K(x) : K]_{\mathrm{s}} = \#\{\textit{verschiedene Nullstellen von } \iota_{\mathrm{a}}^* m_x\} \leq [K(x) : K].$$

Beweis. Die behauptete Ungleichung folgt sofort aus der Tatsache, dass $\iota_{\mathrm{a}}^* m_x$ höchstens so viele Nullstellen haben kann, wie der Grad von m_x angibt, und dieser Grad ist identisch mit $[K(x) : K]$ laut Satz 2.1.

Zur Bestimmung von $[K(x) : K]_{\mathrm{s}}$ sei $m_x = a_n X^n + \ldots + a_0 X^0$. Dann gilt für jeden K-Homomorphismus $j\colon K(x) \to K^{\mathrm{a}}$ die Gleichung $\iota_{\mathrm{a}}^* = (j \circ \iota)^*$ und somit

$$(\iota_{\mathrm{a}}^* m_x)(j(x)) = ((j \circ \iota)^* m_x)(j(x)) = j((\iota^* m_x)(x)) = j(0_{K(x)}) = 0_{K^{\mathrm{a}}}.$$

Also ist $j(x)$ eine Nullstelle des Polynoms $\iota_{\mathrm{a}}^* m_x \in K^{\mathrm{a}}[X]$. Weil $\{1_{K(x)}, x, x^2, \ldots\}$ ein K-Erzeugendensystem von $K(x)$ ist, ist j mittels Multiplikativität und K-Linearität allein durch die Kenntnis des Funktionswertes $j(x)$ bereits vollkommen festgelegt. Die Abbildung

$$\{K\text{-Homomorphismen } K(x) \to K^{\mathrm{a}}\} \longrightarrow \{\text{verschiedene Nullstellen von } \iota_{\mathrm{a}}^* m_x\},$$
$$j \longmapsto j(x)$$

ist also *injektiv* und es folgt

$$[K(x) : K]_{\mathrm{s}} \leq \#\{\text{verschiedene Nullstellen von } \iota_{\mathrm{a}}^* m_x\}.$$

Tatsächlich ist die fragliche Abbildung aber auch surjektiv (was erlaubt „$\leq$“ durch Gleichheit zu ersetzen), denn zu jeder Nullstelle $x^* \in K^{\mathrm{a}}$ von $\iota_{\mathrm{a}}^* m_x$ gibt es ein j wie oben mit $j(x) = x^*$. — Das wissen wir aus Lemma 2.9. □

Wir wollen ein Beispiel dafür geben, dass in der Ungleichung aus Lemma 3.1 im Allgemeinen nicht Gleichheit zu gelten braucht. Als Vorbereitung notieren wir ein wichtiges Lemma, welches auch noch später in Kapitel 4 eine Schlüsselrolle spielen wird.

Lemma 3.2 (Frobenius-Endomorphismus). *Für eine Primzahl p sei $\mathbb{Z}/p\mathbb{Z} \to R$ ein Homomorphismus in einen kommutativen Ring R. Betrachte die Abbildung $\phi\colon R \to R$, $r \mapsto r^p$. Dann gelten die folgenden Aussagen:*

*(1) ϕ ist ein Ringendomorphismus, der sogenannte **Frobenius-Endomorphismus** von R.*
(2) Ist R ein Integritätsbereich, so ist ϕ injektiv.
(3) Ist R ein endlicher Körper, so ist ϕ sogar bijektiv, also ein Automorphismus.

Beweis. Die Multiplikativität von ϕ ist offensichtlich. Nun zur Additivität. Wegen der Existenz eines Homomorphismus $f\colon \mathbb{Z}/p\mathbb{Z} \to R$ ist

$$0_R = f(0_{\mathbb{Z}/p\mathbb{Z}}) = f(p \bmod p) = \underbrace{f(1_{\mathbb{Z}/p\mathbb{Z}}) + \ldots + f(1_{\mathbb{Z}/p\mathbb{Z}})}_{p \text{ Summanden}} = 1_R + \ldots + 1_R.$$

Damit und mit dem Binomischen Lehrsatz erhalten wir für alle $x, y \in R$

$$\begin{aligned}\phi(x+y) = (x+y)^p &= \sum_{\ell=0}^{p} \binom{p}{\ell} x^\ell y^{p-\ell} = x^p + \underbrace{0_R + \ldots + 0_R}_{\text{von den Termen mit } 0<\ell<p} + y^p \\ &= \phi(x) + \phi(y),\end{aligned}$$

denn für $0 < k < p$ teilt p den Binomialkoeffizienten

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = p\frac{(p-1)!}{k!(p-k)!}.$$

Also ist ϕ ein Ringhomomorphismus von R nach R. Ist R ein Integritätsbereich, so $\phi(x) = x^p$ natürlich nur gleich 0_R, wenn schon $x = 0_R$ gilt. Also ist $\ker\phi$ trivial

und ϕ also injektiv. Ist R ein endlicher Körper, so ist ϕ als injektive Abbildung sogar bijektiv und also ein Automorphismus. □

Man beachte, dass die Voraussetzung aus Lemma 3.2, einen Homomorphismus $\mathbb{Z}/p\mathbb{Z} \to R$ zu haben insbesondere erfüllt ist, wenn R ein Körper mit Charakteristik p oder ein Polynomring über einem solchen Körper ist. In Kapitel 4 wird der zuerst genannte Fall von Interesse sein, im Folgenden Beispiel allerdings der zuletzt genannte.

Beispiel 3.3. Sei $\mathbb{F}$ ein beliebiger endlicher Körper der Charakteristik $p \neq 0$, z.B. $\mathbb{F} = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Wir betrachten den Körper $K = \mathrm{Quot}(\mathbb{F}[T])$. Das Polynom

$$P = X^p - T \in K[X]$$

ist irreduzibel.[1] Für einen beliebigen algebraischen Abschluss $\iota_a \colon K \to K^a$ von K und eine beliebige Nullstelle x von $\iota_a^* P$ gilt $x^p = \iota_a(T)$ und daher, dank Lemma 3.2,

$$(X - x)^p = X^p + (-1_K)^p \iota_a(T).$$

Nun ist $(-1_K)^p = -1_K$ (klar für ungerades p und für gerades p, also $p = 2$, ist ohnehin $1_K = -1_K$). Insgesamt haben wir also

$$(X - x)^p = \iota_a^* P.$$

Das irreduzible Polynom P zerfällt in K^a also (wie erwartet) in Linearfaktoren, aber überraschenderweise sind diese alle identisch! — $\iota_a^* P$ hat in K^a nur eine Nullstelle.

Beispiel 3.3 zeigt, dass die in Lemma 3.1 behauptete Ungleichung keine Gleichheit zu sein braucht. Das Ausschließen dieses Defekts führt auf den folgenden wichtigen Begriff: Eine algebraische Körpererweiterung $\iota \colon K \to L$ heißt ***separabel***, falls für *jedes* $x \in L$ die folgende Gleichheit gilt:

$$[K(x) : K]_s = [K(x) : K].$$

Proposition 3.4. *Sei $\iota \colon K \to L$ eine algebraische Erweiterung von endlichem Grad. Dann gilt*

$$[L : K]_s \leq [L : K].$$

Überdies ist $\iota \colon K \to L$ genau dann separabel wenn hierin Gleichheit gilt.

Beweisskizze. Für beliebige Elemente $x_1, x_2 \in L$ überlege man sich die *Multiplikationsformel*

$$[K(x_1, x_2) : K]_s = [K(x_1, x_2) : K(x_1)]_s \cdot [K(x_1) : K]_s$$

durch Identifikation von K-Homomorphismen $j \colon K(x_1, x_2) \to K^a$ in einen algebraischen Abschluss K^a von K mit Paaren (x_1^*, x_2^*), wobei x_1^* eine Nullstelle in K^a des Minimalpolynoms von x_1 über K und x_2^* eine Nullstelle in K^a des Minimalpolynoms

[1] Gemäß des Lemmas von Gauß genügt es die Irreduzibilität von P in $(\mathbb{F}[T])[X]$ nachzuweisen. Dies gelingt mit dem Eisenstein-Kriterium und dem von T erzeugten Primideal $T\mathbb{F}[T] \subset \mathbb{F}[T]$.

von x_2 über $K(x_1)$ bezeichne.[2] Schreibt man nun $L = K(x_1, \ldots, x_n)$ mit geeigneten Elementen $x_1, \ldots, x_n \in L$, so folgt die behauptete Ungleichung leicht mittels Induktion aus Lemma 3.1 und der Gradformel (Satz 1.7). Den Zusatz über Separabilität beweist man auch, indem man die Elemente $x_1, \ldots, x_n$ geeignet wählt. Die Details hierzu bilden Aufgabe 5.3. □

3.2. Separabilitätskriterien

Sei $\iota\colon K \to L$ eine Körpererweiterung. Wir nennen ein Element $x \in L$ ***separabel***, falls das Minimalpolynom von x über K in einem algebraischen Abschluss K^{a} von K genau so viele Nullstellen besitzt, wie sein Grad angibt. (Das ist offensichtlich äquivalent dazu, dass in der Situation von Lemma 3.1 $[K(x) : K]_{\mathrm{s}} = [K(x) : K]$ gilt.) Polynome mit dieser Nullstelleneigenschaft nennen wir ebenfalls ***separabel***.

Beispiele.

- Das Polynom $X^p - T$ aus Beispiel 3.3 ist nicht separabel, da es nur genau eine Nullstelle in K^{a} hat.
- Das Polynom X ist separabel, jedoch nicht das Polynom X^2 (über jedem beliebigen Körper).
- Das Polynom $X^2 - X = X(X-1)$ ist separabel, aber nicht das Polynom $X^3 - X^2 = X^2(X-1)$.

Bemerkung. Man sieht an den obigen Beispielen, dass Separabilität und Irreduzibilität im Allgemeinen nichts miteinander zu tun haben müssen. (Aufgabe: Welche der obigen Polynome sind irreduzibel; Welche sind es nicht?) Man kontrastiere dies jedoch mit Korollar 3.7, sowie Bemerkung 3.9.

Satz 3.5 (Separabilitätskriterium). *Sei $\iota\colon K \to L$ eine algebraische Körpererweiterung. Dann sind die folgenden Aussagen äquivalent:*

(1) $\iota\colon K \to L$ ist separabel.
(2) Es gilt $L = K(\{ x_r : r \in I \})$ mit separablen Erzeugern x_r und Indexmenge I.
(3) Für jeden Zwischenkörper F von $\iota\colon K \to L$ mit endlichem Grad $[F : K]$ gilt $[F : K]_{\mathrm{s}} = [F : K]$.

Beweis. Die Implikationen (3) $\Longrightarrow$ (1) $\Longrightarrow$ (2) sind trivial. Es verbleibt noch die Implikation (2) $\Longrightarrow$ (3) einzusehen. Sei hierzu F ein Teilkörper von L wie in (3). Wegen $[F : K] < \infty$ gibt es eine endliche Indexmenge $I_0 \subseteq I$ mit $F \subseteq L' = K(\{ x_r : r \in I_0 \})$. Mit Blick auf den Beweis von Proposition 3.4 und unter Ausnutzung der Separabilität der Erzeuger x_r sieht man

$$[L' : K]_{\mathrm{s}} = [L' : K].$$

[2] Im letzten Fall sollte man „Nullstelle in K^{a}“ bezüglich der von j induzierten Körpererweiterung $j|_{K(x_1)}\colon K(x_1) \to K^{\mathrm{a}}$ verstehen.

In der Tat sei etwa $L' = K(x_1, \ldots, x_n)$. Setze $K_0 := K$, $K_\nu = K(x_1, \ldots, x_\nu)$. Wegen Aufgabe 5.3 ist dann

$$[L' : K]_s = [K_n : K_{n-1}]_s \cdots [K_1 : K_0]_s.$$

Es genügt zu sehen, dass wir in jedem Faktor auf der rechten Seite Separabilitätsgrad durch Körpererweiterungsgrad ersetzen dürfen, da letztere sich zu $[L' : K]$ aufmultiplizieren. Wir wollen also

$$[K_\nu(x) : K_\nu]_s = [K_\nu(x) : K_\nu]$$

für $\nu = 0, 1, \ldots, n-1$ und $x = x_{\nu+1}$ einsehen. Hierzu beachte, dass wegen der Separabilität von x über K die Gleichung $[K(x) : K]_s = [K(x) : K]$ gilt. Nach Lemma 3.1 hat das Minimalpolynom $m_x \in K[X]$ von x über K also nur einfache Nullstellen in einem (und dann jedem) algebraischen Abschluss von K. Dann ist das Minimalpolynom von x über K_ν allerdings ein Teiler von $\iota^* m_x$ und hat demnach in einem algebraischen Abschluss von K_ν auch nur einfache Nullstellen. Die Multiplikationsformel für den Separabilitätsgrad wurde bereits für Adjunktion zweier algebraischer Elemente bestätigt (Aufgabe 5.3). Mit Induktion bestätigt man diese allgemein für algebraische Erweiterungen, die durch Adjunktion endlich vieler Elemente entstehen. Wegen dieser verallgemeinerten Multiplikationsformel für den Separabilitätsgrad und der üblichen Gradformel (Satz 1.7) ergibt sich aus der obigen Gleichung nun

$$[L' : F]_s \cdot [F : K]_s = [L' : F] \cdot [F : K].$$

Also haben wir $[F : K]_s = [F : K]$. □

Der eben bewiesene Satz liefert ein günstiges Kriterium zum Überprüfen von Separabilität einer Körpererweiterung, da man Separabilität von Elementen sehr einfach prüfen kann (siehe auch Abbildung 5):

Proposition 3.6. *Sei K ein Körper und*

$$P = \sum_{r=0}^{n} a_r X^r = a_n X^n + \ldots + a_2 X^2 + a_1 X + a_0 \in K[X]$$

ein beliebiges (nicht notwendigerweise irreduzibles) Polynom vom Grad $\deg P = n \geq 1$ *und*

$$P' = \sum_{r=1}^{n} r a_r X^{r-1} = n a_n X^{n-1} + \ldots + 2 a_2 X + a_1$$

bezeichne die ***formale Ableitung von P****. Dann ist P genau dann separabel, wenn P und P' teilerfremd sind.*

Beispiele. Wir illustrieren Proposition 3.6 anhand der Beispiele von Seite 38.

- Das Polynom $P_1 = X^p - T$ aus Beispiel 3.3 ist nicht separabel, denn wir haben $P_1' = pX^{p-1} = 0 = 0 \cdot P_1$ und dieses ist nicht teilerfremd zu P_1.

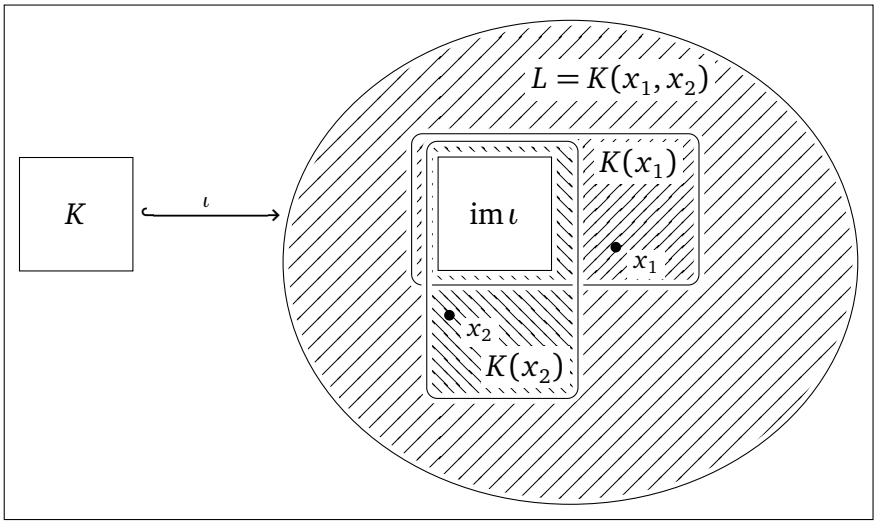


Abbildung 5. Zur Implikation „(2) $\Longrightarrow$ (1)“ in Satz 3.5: Falls man weiß, dass die einfachen Erweiterungen $K \to K(x_1)$ und $K \to K(x_2)$ separabel sind, und $L = K(x_1, x_2)$ gilt, so ist bereits die Erweiterung $\iota\colon K \to L$ separabel. Man braucht Separabilität einer Körpererweiterung also nur auf einigen geeignet ausgewählten einfachen Teilerweiterungen nachprüfen. Für Letzteres eignet sich oft Proposition 3.6.

- Das Polynom $P_2 = X$ ist separabel, denn wir haben $P_2' = 1$. Hingegen das Polynom $P_3 = X^2$ ist nicht separabel, denn wir haben $P_3' = 2X$ und $P_3 = \frac{1}{2}XP_3'$ sofern $2 \neq 0$ im zugrundeliegenden Körper ist, und $P_3' = 0 \cdot P_3$ anderenfalls.
- Das Polynom $P_4 = X^2 - X = X(X-1)$ ist separabel (denn $P_4' = 2X-1$ und eine Fallunterscheidung je nachdem ob die Charakteristik des zugrundeliegenden Körpers gleich 2 ist, oder nicht, liefert die Behauptung), aber nicht das Polynom $P_5 = X^3 - X^2 = X^2(X-1)$, denn

  $$P_5' = 3X^2 - 2X = X(3X-2) \quad \text{und} \quad P_5 = X(X^2 - X)$$

  haben den gemeinsamen Teiler X. (Aufgabe an die Leserin oder den Leser: Ist X auch stets ein größter gemeinsamer Teiler von P_5 und P_5'?)

Beweis von Proposition 3.6. Im Folgenden sei stets $\iota_{\mathrm{a}}\colon K \to K^{\mathrm{a}}$ ein algebraischer Abschluss von K. Wir betrachten zunächst die Situation, wenn P nicht separabel ist. Dann gilt $\iota_{\mathrm{a}}^* P = (X-x)^k Q$ für ein geeignetes Element $x \in K^{\mathrm{a}}$, $k \geq 2$ und $Q \in K^{\mathrm{a}}[X]$ mit $Q(x) \neq 0_{K^{\mathrm{a}}}$. Man bestätigt leicht durch Nachrechnen

$$\begin{aligned}\iota_{\mathrm{a}}^*(P') = (\iota_{\mathrm{a}}^* P)' &= ((X-x)^k Q)' \\ &= ((X-x)^k)' Q + (X-x)^k Q' \\ &= k(X-x)^{k-1} Q + (X-x)^k Q'.\end{aligned}$$

Einsetzen von x zeigt $\iota_{\mathrm{a}}^*(P')(x) = 0_{K^{\mathrm{a}}} = (\iota_{\mathrm{a}}^* P)(x)$. Demnach liegen sowohl P' wie auch P, in dem Ideal

$$\{\text{Polynome aus } K[X] \text{ mit Nullstelle } x \text{ in } K^{\mathrm{a}}\} \subset K[X],$$

welches vom Minimalpolynom von x über K erzeugt wird. Insbesondere ist dieses Minimalpolynom ein gemeinsamer Teiler von P' und P.

Sei nun umgekehrt G ein nichtkonstanter gemeinsamer Teiler von P' und P. Wir schreiben $x_1, \dots, x_n$ für alle Nullstellen von P in K^{a} (Wiederholungen erlaubt!) und gehen o.E. davon aus, dass P und G normiert sind und $x_1, \dots, x_s$ (mit $s < n$) die Nullstellen von G in K^{a} sind. Dann ist

$$\begin{aligned}\iota_{\mathrm{a}}^*(P') = (\iota_{\mathrm{a}}^* P)' &= \Big(\prod_{r=1}^{n}(X - x_r)\Big)' = \sum_{\ell=1}^{n}\prod_{r\neq\ell}(X - x_r) \\ &= \underbrace{\Big(\prod_{r=1}^{s}(X - x_r)\Big)}_{=\iota_{\mathrm{a}}^* G}\sum_{\ell=s+1}^{n}\prod_{\substack{r=s+1\\ r\neq\ell}}^{n}(X - x_r) + \underbrace{\sum_{\ell=1}^{s}\prod_{r\neq\ell}(X - x_r)}_{=:H}.\end{aligned}$$

Allerdings ist $\iota_{\mathrm{a}}^*(P')$ aber auch ein Vielfaches von $\iota_{\mathrm{a}}^* G$. Darum ist auch H ein Vielfaches von $\iota_{\mathrm{a}}^* G$. Einsetzen von x_1 (eine Nullstelle von $\iota_{\mathrm{a}}^* G$!) zeigt

$$0_{K^{\mathrm{a}}} = H(x_1) = \sum_{\ell=2}^{s}\underbrace{(x_1 - x_1)}_{=0_{K^{\mathrm{a}}}}\prod_{\substack{r\neq\ell\\ r\neq 1}}(x_1 - x_r) + \prod_{r\neq 1}(x_1 - x_r) = \prod_{r\neq 1}(x_1 - x_r)$$

und also $x_1 = x_r$ für ein $r \neq 1$. Insbesondere hat P eine doppelte Nullstelle und ist daher nicht separabel. □

Die nächsten beiden Korollare lassen sich unter dem Merkspruch „*Inseparabilität ist selten*“ zusammenfassen.

Korollar 3.7. *Sei K ein Körper und $P \in K[X]$ irreduzibel und inseparabel. Dann hat K Charakteristik $p \neq 0$ und P ist von der Form $P = g(X^p)$ mit einem Polynom $g \in K[X]$.*

Beweis. Da P als inseparabel angenommen wurde, haben P und P' gemäß Proposition 3.6 einen nichtkonstanten gemeinsamen Teiler. Aus der Irreduzibilität von P folgt, dass es sich bei diesem Teiler um ein zu P assoziiertes Polynom handelt. D.h. P teilt P'. Wegen $\deg P' < \deg P$ ist dies nur möglich wenn P' das Nullpolynom ist. In der Notation von Proposition 3.6 ergibt sich für die Koeffizienten von P daraus $a_r = 0$ für alle nicht durch p teilbaren r. Daraus ergibt sich die Behauptung. □

Korollar 3.8. *Alle algebraischen Körpererweiterungen von Körpern mit Charakteristik 0 sind separabel.*

Beweis. Sei $\iota\colon K \to L$ eine algebraische Körpererweiterung eines Körpers K mit Charakteristik 0. Gemäß Satz 3.5 genügt es die Separabilität von allen Elementen $x \in L$ nachzuprüfen. Diese folgt aber sofort aus Korollar 3.7, da das Minimalpolynom von x

über K als irreduzibles Polynom über einem Körper mit Charakteristik 0 automatisch separabel ist. □

Bemerkung 3.9. Man kann sich auch überlegen, dass jedes irreduzible Polynom über einem endlichen Körper automatisch separabel ist (siehe Aufgabe 6.1 (b)). Daraus folgt auch, dass man um solchen Inseparabilitätsphänomenen zu begegnen tatsächlich einen Körper mit positiver Charakteristik und positivem Transzendenzgrad über seinem Primkörper betrachten muss. Beispiel 3.3 ist also in gewisser Weise das einfachste Beispiel eines Körpers, über dem irreduzible, inseparable Polynome existieren. Wenn man also nicht solche Körper betrachtet, braucht man sich über Inseparabilität keine Sorgen machen.

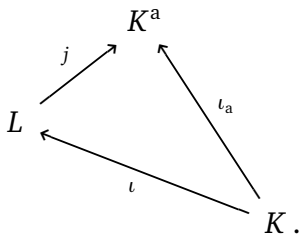
3.3. Normale Körpererweiterungen

Für eine Körpererweiterung $\iota\colon K \to L$ definieren wir die ***relative Automorphismengruppe von L über K*** durch

$$\mathrm{Aut}_K(L) = \{K\text{-Isomorphismen von } L \text{ nach } L\}.$$

(Achtung: Wie so häufig hängt diese Definition von ι ab, obgleich wir dies nicht in der Notation kenntlich machen.) Die Menge $\mathrm{Aut}_K(L)$ bildet zusammen mit der Verkettung von Abbildungen als Verknüpfung eine Gruppe. Wir wollen im Folgenden untersuchen, wann diese Gruppe besonders viele Elemente enthält.

Sei nun $\iota\colon K \to L$ algebraisch und $\iota_{\mathrm{a}}\colon K \to K^{\mathrm{a}}$ ein algebraischer Abschluss von K und $j\colon L \to K^{\mathrm{a}}$ ein beliebiger K-Homomorphismus (die Existenz eines solchen j wird durch Lemma 2.13 gewährleistet):



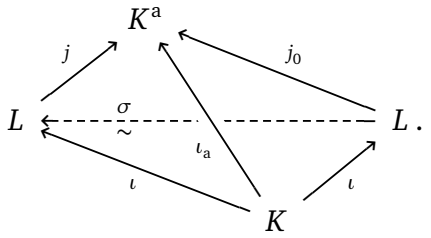
Für jedes $\sigma \in \mathrm{Aut}_K(L)$ ist dann auch $j \circ \sigma$ ein K-Homomorphismus von L nach K^{a}. Diese Zuordnung stiftet eine *injektive* Abbildung

$$\begin{aligned} \mathrm{Aut}_K(L) &\longrightarrow \{K\text{-Homomorphismen } L \to K^{\mathrm{a}}\}, \\ \sigma &\longmapsto j \circ \sigma. \end{aligned}$$

Bekommt man auf diese Weise alle K-Homomorphismen von L nach K^{a}? Nicht immer, wie wir noch sehen werden. Wir nennen die Körpererweiterung $\iota\colon K \to L$ ***normal***, falls die obige Abbildung surjektiv ist, also

$$\{\, j \circ \sigma : \sigma \in \mathrm{Aut}_K(L) \,\} = \{K\text{-Homomorphismen } L \to K^{\mathrm{a}}\}$$

gilt. Das besagt, dass es für jeden K-Homomorphismus $j_0\colon L \to K^{\mathrm{a}}$ einen K-Automorphismus $\sigma\colon L \to L$ gibt, der das folgende Diagramm kommutativ macht:



Man überlegt sich leicht, dass zwar die Menge auf der linken Seite von der Wahl von j abhängen kann, aber die Frage, ob Gleichheit zur rechten Seite besteht oder nicht, unabhängig von der Wahl von j ist.

Für eine (algebraische) normale Körpererweiterung $\iota\colon K \to L$ gilt

$$\#\mathrm{Aut}_K(L) = \#\{\, j \circ \sigma : \sigma \in \mathrm{Aut}_K(L) \,\} = [L : K]_{\mathrm{s}}.$$

Ist $\iota\colon K \to L$ zusätzlich noch separabel und habe endlichen Grad, so folgt mittels Proposition 3.4 sogar

$$\#\mathrm{Aut}_K(L) = [L : K].$$

Falls hingegen $\iota\colon K \to L$ nicht normal oder nicht separabel ist (aber nach wie vor von endlichem Grad), so ist

$$\#\mathrm{Aut}_K(L) < [L : K].$$

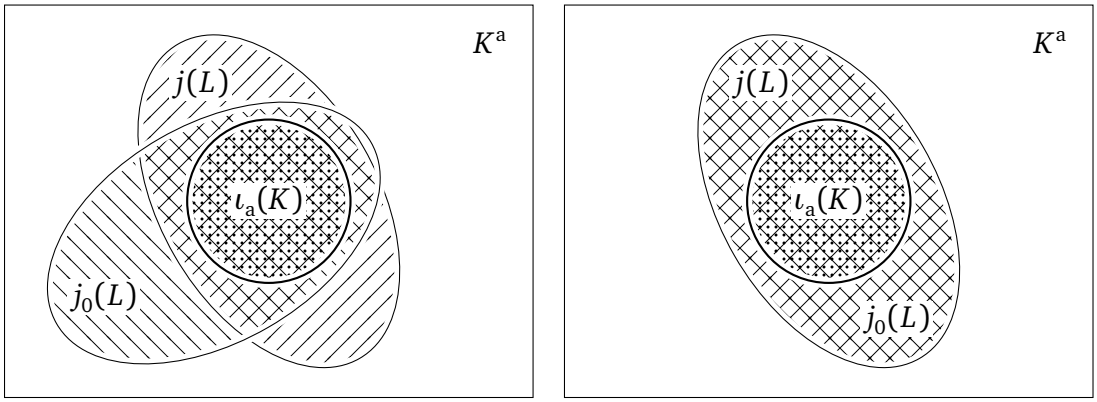
Diese Charakterisierung besagt, dass genau das Zusammenspiel von Normalität und Separabilität eine besonders reichhaltige K-Automorphismengruppe gewährleistet.

Es verbleibt noch die Aufgabe, den soeben eingeführten Normalitätsbegriff durch ein Kriterium brauchbar zu machen, welches den praktischen Nachweis von Normalität einer gegebenen Körpererweiterung ermöglicht.

Satz 3.10 (Normalitätskriterium). *Sei $\iota\colon K \to L$ eine algebraische Körpererweiterung. Dann sind die folgenden Aussagen äquivalent:*

(1) $\iota\colon K \to L$ ist normal.
(2) Je zwei beliebige K-Homomorphismen $j, j_0\colon L \to K^{\mathrm{a}}$ in einen algebraischen Abschluss von $K \to K^{\mathrm{a}}$ haben dasselbe Bild.
(3) L ist Zerfällungskörper von einer Menge[3] von Polynomen aus $K[X]$.
(4) Jedes irreduzible Polynom aus $K[X]$ mit einer Nullstelle in L zerfällt in L bereits gänzlich in Linearfaktoren.

[3]Natürlich kann eine solche Menge genau dann als endliche Menge gewählt werden, wenn die Erweiterung $\iota\colon K \to L$ selbst endlich ist. Mit ***Zerfällungskörper einer Menge $\mathscr{P}$ von Polynomen aus $K[X]$*** ist eine Körpererweiterung $\iota\colon K \to L$ gemeint derart, dass $\iota^* P$ für jedes $P \in \mathscr{P}$ in Linearfaktoren zerfällt, und $L = K(\mathscr{V})$ mit der Nullstellenmenge $\mathscr{V}$ eben dieser Linearfaktoren gilt.



(a) Nicht normal, **(b)** normal.

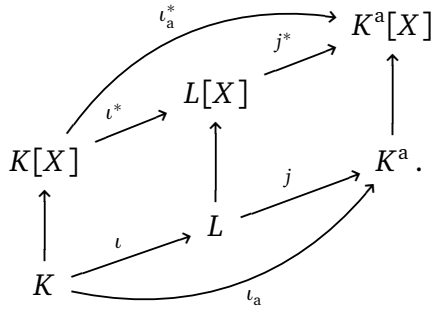
Abbildung 6. Veranschaulichung der Äquivalenz „(1) $\Longleftrightarrow$ (2)“ im Normalitätskriterium (Satz 3.10).

Beweis. Die Implikation (4) $\Longrightarrow$ (3) ist trivial.

Zum Beweis der Implikation (3) $\Longrightarrow$ (2) seien $j, j_0 \colon L \to K^{\mathrm{a}}$ zwei beliebige K-Homomorphismen. Ferner sei (gemäß (3)) $L = K(\mathscr{X})$ für eine Menge $\mathscr{X} \subseteq L$ von Elementen, deren Minimalpolynome über K in L vollständig in Linearfaktoren zerfallen. Wir betrachten ein beliebiges $x \in \mathscr{X}$. Das Minimalpolynom m_x von x über K zerfällt laut Annahme in L vollständig:

$$\iota^* m_x = \prod\nolimits_k (X - x_k).$$

Unter Ausnutzung der Kommutativität des Diagramms (und desselben Diagramms wobei j durch j_0 zu ersetzen ist)



sehen wir

$$\prod\nolimits_\ell (X - j(x_\ell)) = j^*(\iota^* m_x) = \iota_{\mathrm{a}}^* m_x = j_0^*(\iota^* m_x) = \prod\nolimits_k (X - j_0(x_k)).$$

Daher ist $j(x) = j(x_\ell) = j_0(x_k)$ für ein geeignetes Paar (ℓ, k). Da $x \in \mathscr{X}$ beliebig war und $L = K(\mathscr{X})$ gilt, folgt hieraus $\operatorname{im} j \subseteq \operatorname{im} j_0$, sowie die umgekehrte Inklusion (indem man in unserem Argument die Rollen von j und j_0 vertauscht).

Für die Implikation (2) $\Longrightarrow$ (1) seien $j, j_0 \colon L \to K^{\mathrm{a}}$ zwei beliebige K-Homomorphismen. Schränkt man den Bildbereich von j auf $\operatorname{im} j$ ein, so ist j als Abbildung von L nach $\operatorname{im} j$ natürlich ein K-Isomorphismus. Wir schreiben $j^{-1} \colon \operatorname{im} j \to L$ für dessen Umkehrabbildung. Da wegen (2) j und j_0 dasselbe Bild haben, ist $\sigma = j^{-1} \circ j_0 \colon L \to L$ wohl-definiert und ein K-Automorphismus von L mit $j \circ \sigma = j_0$; Daraus folgt (1).

Für den Beweis von (1) $\Longrightarrow$ (4) sei $P \in K[X]$ ein irreduzibles Polynom mit einer Nullstelle in $x \in L$. Wir dürfen o.E. annehmen, dass P normiert ist. Zunächst beachte man, dass jedenfalls $\iota_{\mathrm{a}}^* P$ zerfällt, etwa

$$\iota_{\mathrm{a}}^* P = \prod\nolimits_k (X - \alpha_k).$$

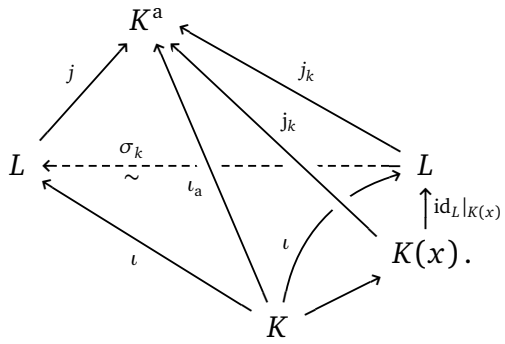
Sei $j \colon L \to K^{\mathrm{a}}$ wie zuvor ein beliebiger K-Homomorphismus. Sofern wir nun die Existenz von Elementen $x_k \in L$ mit $\alpha_k = j(x_k)$ nachweisen können, folgt (4), denn das obige kommutative Diagramm zeigt dann

$$\begin{aligned} j^*(\iota^* P) = (j^* \circ \iota^*)P = \iota_{\mathrm{a}}^* P = \prod\nolimits_k (X - \alpha_k) = \prod\nolimits_k (X - j(x_k)) \\ = j^*\Big(\prod\nolimits_k (X - x_k)\Big), \end{aligned}$$

woraus wir mittels der Injektivität von j^*, wie gewünscht, auf

$$\iota^* P = \prod\nolimits_k (X - x_k)$$

schließen können. Zum Nachweis der Existenz der fraglichen Elemente x_k beachte man, dass es gemäß Lemma 2.9 einen K-Homomorphismus $\mathrm{j}_k \colon K(x) \to K^{\mathrm{a}}$ mit $\mathrm{j}_k(x) = \alpha_k$ gibt. Diesen kann man mittels Lemma 2.13 zu einem $K(x)$-Homomorphismus $j_k \colon L \to K^{\mathrm{a}}$ fortsetzen. Wegen (1) ist $j_k = j \circ \sigma_k$ für einen geeigneten Automorphismus $\sigma_k \in \operatorname{Aut}_K(L)$. Man veranschaulicht sich die gesamte Situation vielleicht anhand des folgenden kommutativen Diagramms:



Für $x_k = \sigma_k(x)$ ist dann

$$j(x_k) = (j \circ \sigma_k)(x) = j_k(x) = (j_k \circ \mathrm{id}_L|_{K(x)})(x) = \mathrm{j}_k(x) = \alpha_k. \qquad \square$$

Beispiele 3.11.

(1) Für jeden Körper K ist die triviale Körpererweiterung K/K normal.

(2) Jede quadratische Körpererweiterung L/K ist normal, denn für $x \in L \setminus K$ ist $L = K(x)$ Zerfällungskörper vom Minimalpolynom von x. (Denn jedes quadratische Polynom mit einer Nullstelle in einem Körper zerfällt über diesem aus Gradgründen schon in Linearfaktoren.)
(3) Jeder algebraische Abschluss $\iota_a\colon K \to K^a$ ist normal.
(4) Keine der Erweiterungen $\mathbb{R}/\mathbb{Q}$ oder $\mathbb{C}/\mathbb{Q}$ ist normal, denn diese sind nicht algebraisch (siehe Aufgabe 3.1 (c)).
(5) Wir betrachten das irreduzible Polynom $P = X^3 - 2$ über $\mathbb{Q}$. In $\mathbb{R}$ hat P genau eine Nullstelle, nämlich $\sqrt[3]{2}$ und zerlegt sich über $\mathbb{Q}(\sqrt[3]{2})$ wie folgt:

$$X^3 - 2 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4}).$$

Offensichtlich zerfällt $X^3 - 2$ also nicht über $\mathbb{Q}(\sqrt[3]{2})$, weswegen die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ nicht normal ist.
Ist nun $\zeta = \exp(2\pi i/3)$, so verifiziert man $|\zeta| = 1$ und $\zeta \neq \zeta^2 \neq \zeta^3 = 1$. Über den komplexen Zahlen ist daher

$$X^3 - 2 = (X - \sqrt[3]{2})(X - \zeta\sqrt[3]{2})(X - \zeta^2\sqrt[3]{2}).$$

Der Körper $\mathbb{Q}(\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ ist Zerfällungskörper von $X^3 - 2$ und daher normal.
Mittels Lemma 2.9 kann man sich des Übrigen auch überlegen, dass die Körper $\mathbb{Q}(\sqrt[3]{2})$ und $\mathbb{Q}(\zeta^k\sqrt[3]{2})$ (mit $k = 1, 2$) jeweils verschiedene $\mathbb{Q}$-isomorphe Körper sind. Man vergleiche dies mit Abbildung 8.

KAPITEL 4

Endliche Körper

Endliche Körper haben vielerlei Anwendungen. Einfache Beispiele kennt man schon in Form der Faktorringe $\mathbb{Z}/p\mathbb{Z}$ für Primzahlen p. Weitere endliche Körper — bedingt durch die binären Beschaffenheiten moderner Computerhardware oftmals mit Charakteristik 2 — werden häufig für Kryptographie und Codierungstheorie herangezogen, da diese sehr angenehme algebraische Eigenschaften aufweisen und bestens verstanden sind.

In diesem Kapitel wollen wir endliche Körper verstehen; Dieses Ziel erreichen wir in erstaunlich umfassender Weise: Wir lernen (bis auf Isomorphie) alle endlichen Körper kennen und bekommen eine vollständige Übersicht über ihren gesamten Teilkörperverband, sowie deren Einheitengruppen.

4.1. Existenz und Eindeutigkeit bis auf Isomorphie

Für eine Primzahl p schreiben wir $\mathbb{F}_p$ für den Körper $\mathbb{Z}/p\mathbb{Z}$. Einen endlichen Körper mit $q = p^n$ Elementen notieren wir im Folgenden stets als $\mathbb{F}_q$. Dass zumindest strukturelle Aussagen über diesen nur von q abhängen ist Gegenstand des nächsten wichtigen Satzes. Große Teile des Beweises davon sind bereits aus Aufgabe 1.2 und Aufgabe 4.2 bekannt. Wir wiederholen die relevanten Schritte dennoch.

Satz 4.1 (E. H. Moore, 1893)**.**

(1) Sei K ein endlicher Körper. Dann ist $\#K$ eine Primzahlpotenz ≥ 2.

(2) Sei $q = p^n \geq 2$ eine Primzahlpotenz. Dann existiert bis auf $\mathbb{F}_p$-Isomorphie nur genau ein endlicher Körper $\mathbb{F}_q$ mit q Elementen, nämlich der[1] Zerfällungskörper von $X^q - X \in \mathbb{F}_p[X]$ über $\mathbb{F}_p$. Überdies ist die Erweiterung $\mathbb{F}_p \to \mathbb{F}_q$ separabel.

Beweis. Zum Beweis von (1) sei K ein endlicher Körper und $F \subseteq K$ sein Primkörper. Dann ist K als F-Vektorraum isomorph zu $F^{[K:F]}$ und dieser Vektorraum hat genau $p^{[K:F]} \geq 2$ Elemente, wobei $p = \#F$ die Charakteristik von K bezeichne. Das beweist die erste Aussage. (Man erinnere sich auch an Aufgabe 1.2.)

Zum Beweis von (2) sei $q = p^n$ eine Primzahlpotenz und $\mathbb{F}_q$ ein Zerfällungskörper von $X^q - X$. Wir haben also $X^q - X = (X - x_1) \cdots (X - x_q)$ mit $x_1, \ldots, x_q \in \mathbb{F}_q$. Man rechnet leicht nach, dass es sich bei der Menge $\{x_1, \ldots, x_q\} \subseteq \mathbb{F}_q$ tatsächlich schon

[1] Es wäre hier wohl angemessener den unbestimmten Artikel zu benutzen, aber laut Proposition 2.10 sind je zwei Zerfällungskörper desselben Polynoms über $\mathbb{F}_p$ automatisch $\mathbb{F}_p$-isomorph.

um einen Körper handelt.[2] Tatsächlich ist $\{x_1, \dots, x_q\}$ auch schon Zerfällungskörper von $X^q - X$. Mit Proposition 2.10 schließt man nun $\{x_1, \dots, x_q\} = \mathbb{F}_q$. Da $X^q - X$ keine doppelten Nullstellen besitzt (siehe Proposition 3.6) sind die Elemente $x_1, \dots, x_q$ paarweise verschieden und wir haben $\#\mathbb{F}_q = q$. Das klärt die Existenz eines Körpers mit q Elementen und die Separabilität der zugehörigen Körpererweiterung von $\mathbb{F}_p$. (Letzteres hätte man sich alternativ auch mittels Aufgabe 6.1 (b) überlegen können).

Sei nun K ein beliebiger Körper mit q Elementen. Wir zeigen nun, dass in diesem das Polynom $X^q - X$ zerfällt. Mit Proposition 2.10 folgt dann, dass K und $\mathbb{F}_q$ zueinander $\mathbb{F}_p$-isomorph sind. Die Einheitengruppe $K^\times = K \setminus \{0\}$ von K hat $q-1$ Elemente. Dementsprechend folgt mit dem Satz von Lagrange $x^{q-1} = 1_{K^\times} = 1_K$ für jedes $x \in K^\times$. Demnach gilt $x^q = x$ für jedes $x \in K$ und wir sehen $X^q - X = \prod_{x \in K}(X - x)$. □

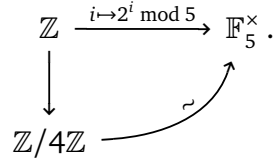
Vor allem in älterer Literatur wird der Körper $\mathbb{F}_q$ auch mit $\mathrm{GF}(q)$ bezeichnet, wobei „GF“ als Abkürzung für „***Galois field***“ steht[3] und an den französischen Mathematiker Évariste Galois erinnern soll.

4.2. Struktur der Einheitengruppe

Ziel dieses Abschnittes ist das Studium der Einheitengruppe endlicher Körper und der Ziehung einiger wichtiger Konsequenzen daraus. Da das anvisierte Hauptresultat (Satz 4.4) bereits als Konsequenz von [33, Korollar 7.7] bekannt ist, wurde in der Vorlesung deutlich abgekürzt. Das soeben zitierte Resultat wurde damals als Konsequenz einer Nullstellenabschätzung für Polynome über Integritätsbereichen (Anzahl der Nullstellen $\leq$ Grad) und dem Hauptsatz über endliche abelsche Gruppen ([33, Satz 5.3]) gewonnen. (Den Bezug zu Polynomen motivieren wir abermals in Beispiel 4.2.) Es stellt sich heraus, dass jener Hauptsatz im Beweis vermeidbar ist; dies führen wir im Folgenden aus.

Wir beginnen mit einer einführenden *ad-hoc* Überlegung:

Beispiel 4.2. Die Einheitengruppe $\mathbb{F}_5^\times$ des Körpers $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ ist zyklisch. Ja, tatsächlich rechnet man leicht nach, dass 2 mod 5 die Gruppe $(\mathbb{F}_5^\times, \cdot)$ erzeugt und $\mathbb{Z} \to \mathbb{F}_5^\times$, $i \mapsto (2^i \bmod 5)$ einen Isomorphismus zwischen den Gruppen $(\mathbb{Z}/4\mathbb{Z}, +)$ und $(\mathbb{F}_5^\times, \cdot)$ induziert:



Hätte man die Zyklizität von $(\mathbb{F}_5^\times, \cdot)$ auch anders einsehen können? — Ja! Wäre nämlich $(\mathbb{F}_5^\times, \cdot)$ nicht zyklisch, so hätte man zwangsweise $\mathbb{F}_5^\times \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) =: G$, denn andere Isomorphietypen von Gruppen mit genau vier Elementen gibt es nicht! In

[2] Das folgt leicht mit Lemma 3.2 und ein wenig Rechenarbeit.

[3] „Field“ ist der englische Begriff für „Körper“ (im Sinne der Algebra).

G erfüllt jedoch jedes Element $g \in G$ die Gleichung $2g = 0_G$ (additive Schreibweise!); Zöge man dies auf $\mathbb{F}_5^\times$ zurück (multiplikative Schreibweise!) käme $x^2 = 1_{\mathbb{F}_5^\times}$ für jedes $x \in \mathbb{F}_5^\times$ und das Polynom $X^2 - 1_{\mathbb{F}_5} \in \mathbb{F}_5[X]$ hätte damit mindestens vier Nullstellen, was aber unmöglich ist.

Wenn man die Strukturtheorie endlicher abelscher Gruppen bemüht, kann man die obige Überlegung leicht zu einem Beweis dessen ausbauen, dass die Einheitengruppe eines jeden endlichen Körpers stets zyklisch ist (Korollar 4.5). Hier wollen wir allerdings einen Beweis geben, der etwas weniger Vorwissen verlangt (aber schlussendlich auf derselben Idee fußt). Die Notation $\sum_{d|n}$ bezeichne die Summation über alle positiven Teiler d von n.

Lemma 4.3. *Sei G eine endliche Gruppe mit $n = \#G$ und für jeden positiven Teiler d von n gelte $N_d(G) := \#\{\, x \in G : x^d = 1_G \,\} \leq d$. Dann ist G zyklisch. Die Umkehrung gilt auch.*

Beweis. Ist G zyklisch, also $G = \langle g \rangle$ für ein $g \in G$, so haben wir für jeden positiven Teiler d von n[4]

$$\{\, x \in G : x^d = 1_G \,\} = \{\, g^{kn/d} : 1 \leq k \leq d \,\}$$

und diese Menge hat höchstens (tatsächlich genau gleich) d Elemente, wie vom Lemma behauptet wird.

Sei G nun umgekehrt eine beliebige endliche Gruppe mit $N_d(G) \leq d$ für alle Teiler $d \geq 1$ von $n = \#G$. Falls es in G überhaupt ein Element g der Ordnung d gibt, so ist $\langle g \rangle \subseteq \{\, x \in G : x^d = 1_G \,\}$ und aus Ordnungsgründen gilt Gleichheit. Dann sind also automatisch *alle* Elemente von G mit Ordnung d in der zyklischen Gruppe $\langle g \rangle$ enthalten und wir haben $N_d(G) = \varphi(d)$ mit der ***Eulerschen φ-Funktion***

$$\varphi\colon \mathbb{N} \longrightarrow \mathbb{N}, \quad d \longmapsto \#\{\, 1 \leq k \leq d : k \text{ teilerfremd zu } d \,\}$$

Insgesamt ist also stets $N_d(G) \in \{0, \varphi(d)\}$. Sei nun C_n eine zyklische Gruppe mit genau n Elementen (z.B. $(\mathbb{Z}/n\mathbb{Z}, +)$). Dann ist

$$n = \#G = \sum_{d|n} N_d(G) \leq \sum_{d|n} \varphi(d) = \sum_{d|n} N_d(C_n) = \#C_n = n.$$

Daraus folgt $N_d(G) = \varphi(d)$ für alle positiven Teiler d von n. Insbesondere haben wir somit $N_n(G) > 0$ und G ist zyklisch. □

Satz 4.4. *Sei K ein beliebiger (nicht notwendigerweise endlicher) Körper und $G \subseteq K^\times$ eine endliche Untergruppe der multiplikativen Gruppe von K. Dann ist G zyklisch.*

Beweis. Da jedes Polynom $X^d - 1_K \in K[X]$ höchstens d Nullstellen in K besitzt, erfüllt jede endliche Untergruppe G von $K^\times$ die Voraussetzungen von Lemma 4.3 und ist also zyklisch. □

[4] Das folgert man leicht aus dem üblichen *Ordnungskalkül*: Schreibt man $\operatorname{ord}(\cdot)$ für die Ordnung eines Gruppenelements, so ist $\operatorname{ord}(g^{kn/d}) = n/\operatorname{ggT}(k,d)$ für $n = \operatorname{ord}(g)$ und jeden Teiler d von n.

Korollar 4.5. *Die Einheitengruppe eines endlichen Körpers ist stets zyklisch.*

Satz 4.4 hat eine weitere bemerkenswerte Konsequenz: jede endliche Erweiterung eines endlichen Körpers ist *einfach* im Sinne von § 2.1. Dies ist ein Spezialfall vom sogenannten ***Satz vom primitiven Element***, den wir in § 5.2 noch näher betrachten werden.

Korollar 4.6 (Satz vom primitiven Element, Teil I)**.** *Sei $\iota\colon \mathbb{F} \to \mathbb{F}'$ eine Körpererweiterung zwischen endlichen Körpern. Dann ist $\mathbb{F}' = \mathbb{F}(x')$ für ein $x' \in \mathbb{F}'$.*

Beweis. Es genügt x' als einen Erzeuger der multiplikativen Gruppe von $\mathbb{F}'$ zu wählen; Ein solcher Erzeuger existiert gemäß Korollar 4.5 stets. □

Laut Satz 4.1 gibt es für jede Primzahl p und jede natürliche Zahl n eine Körpererweiterung $\mathbb{F}_{p^n}/\mathbb{F}_p$. Diese hat natürlich Grad n und laut Korollar 4.6 ist diese einfach: $\mathbb{F}_{p^n} = \mathbb{F}_p(x)$ für ein geeignetes $x \in \mathbb{F}_{p^n}$. Das Minimalpolynom von x über $\mathbb{F}_p$ ist dann also ein irreduzibles Polynom über $\mathbb{F}_p$ vom Grad n (vgl. Satz 2.1). Insbesondere *gibt es* über $\mathbb{F}_p$ mindestens ein irreduzibles Polynom vom Grad n. In Satz 4.11 zeigen wir noch eine deutlich stärkere, quantitative Form dieser Aussage.

4.3. Verband der Teilkörper

In diesem Abschnitt beschaffen wir uns einen *vollständigen* Überblick über sämtliche Zwischenkörper einer Erweiterung von endlichen Körpern (Satz 4.7; vgl. Aufgabe 7.2) und bestimmen in sehr konkreter Art und Weise deren relative Automorphismengruppe (Satz 4.9). Mit dem in Kapitel 5 zu besprechenden *Hauptsatz der Galois-Theorie* (Satz 5.3) ließe sich Satz 4.7 tatsächlich aus Satz 4.9 gewinnen, doch an dieser Stelle geben wir ein *ad-hoc*-Argument.

Satz 4.7. *Seien p eine Primzahl und n, k natürliche Zahlen. Genau dann hat $\mathbb{F}_{p^n}$ einen — und dann auch nur einen — zu $\mathbb{F}_{p^k}$ isomorphen Teilkörper, wenn k ein Teiler von n ist. Die Aussage bleibt auch dann gültig, wenn man p durch eine Primzahlpotenz q ersetzt und den Isomorphiebegriff zu $\mathbb{F}_q$-Isomorphie spezialisiert.*[5]

Beweis. Sei $\iota\colon \mathbb{F}_{p^k} \to \mathbb{F}_{p^n}$ eine Körpererweiterung. Dann hat $\mathbb{F}_{p^n}$ als $[\mathbb{F}_{p^n} : \mathbb{F}_{p^k}]$-dimensionaler Vektorraum offenbar

$$(p^k)^{[\mathbb{F}_{p^n}:\mathbb{F}_{p^k}]} = p^{k[\mathbb{F}_{p^n}:\mathbb{F}_{p^k}]}$$

viele Elemente. Wegen $\#\mathbb{F}_{p^n} = p^n$ folgt dann, dass k ein Teiler von n ist. Überdies kann $\mathbb{F}_{p^n}$ keinen zweiten, zu $\iota(\mathbb{F}_{p^k})$ isomorphen Teilkörper enthalten, da die (laut Korollar 4.5) zyklische Gruppe $\mathbb{F}_{p^n}^\times$ höchstens eine zu $\mathbb{F}_{p^k}^\times$ isomorphe Untergruppe enthalten kann.

[5] *Achtung:* Der letzte Teil zur $\mathbb{F}_q$-Isomorphie ist etwas unachtsam formuliert. Man beachte insbesondere die weiteren Ausführungen in den Lösungshinweisen zu Aufgabe 7.2

Sei nun umgekehrt k ein Teiler von n, also etwa $n = kt$. Dann hat $\mathbb{F}_{p^n}^\times$ als zyklische Gruppe der Ordnung[6]

$$p^n - 1 = p^{kt} - 1 = (p^k - 1)(p^{k(t-1)} + p^{k(t-2)} + \ldots + p^k + 1)$$

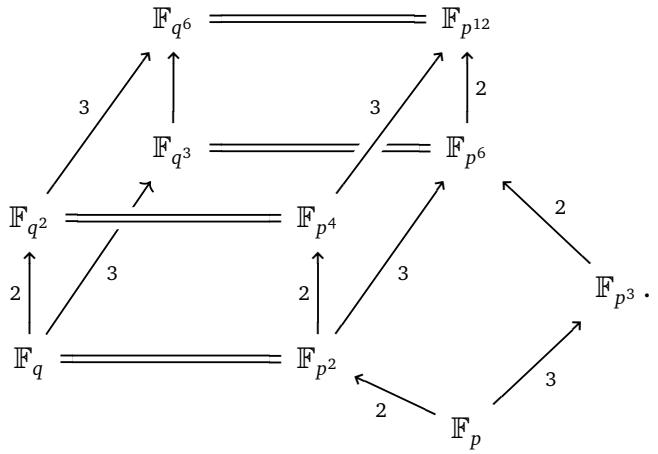
eine Untergruppe U der Ordnung $p^k - 1$ (siehe Lemma 4.3). Insbesondere zerfällt in $\mathbb{F}_{p^n}$ also das Polynom

$$X^{p^k} - X = X \prod_{u \in U} (X - u)$$

und $\mathbb{F}_{p^n}$ enthält daher laut Proposition 2.10 einen Zerfällungskörper von $X^{p^k} - X$ als Teilkörper. In Satz 4.1 hatten wir gesehen, dass dieser Zerfällungskörper aus genau p^k vielen Elementen besteht.

Der Zusatz über Primzahlpotenzen q sei den Leserinnen und Lesern zur Übung überlassen (Aufgabe 7.2). □

Beispiel 4.8. Die Zahl $12 = 2^2 3$ hat die positiven Teiler 1, 2, 3, 4, 6 und 12. Die positiven Teiler von 6 sind 1, 2, 3 und 6. Sei nun p eine beliebige Primzahl und $q = p^2$. Im Folgenden fassen wir $\mathbb{F}_{p^d}$ mit $d \mid 12$ jeweils als Teilkörper von $\mathbb{F}_{p^{12}}$ auf. Das folgende Diagramm zeigt dann alle Teilkörper von $\mathbb{F}_{p^{12}}$:



(Die Pfeile sind jeweils die Inklusionsabbildungen und sind mit den Graden der resultierenden Körpererweiterung annotiert.)

Bemerkung. Man beachte (vielleicht mit Blick auf das Diagramm in Beispiel 4.8), dass es durchaus mehr Abbildungen von z.B. $\mathbb{F}_{p^2}$ nach $\mathbb{F}_{p^4}$ gibt, als hier gezeichnet wurden. In der Tat erhält man eine solche, indem man die[7] Inklusion $\mathbb{F}_{p^2} \hookrightarrow \mathbb{F}_{p^4}$

[6] Die letzte Gleichung bestätigt man durch Ausmultiplikation der rechten Seite; Es entsteht eine Teleskopsumme, bei der nur die Randterme, also p^{kt} und -1 übrig bleiben.

[7] Der bestimmte Artikel ist hier gerechtfertigt, weil man in der Situation von Beispiel 4.8 den Körper $\mathbb{F}_{p^2}$ als Teilkörper von $\mathbb{F}_{p^4}$ aufzufassen beschlossen hat. Das korrespondiert dazu *eine* solche Inklusion als *bestimmt* auszuzeichnen.

mit den Frobenius-Automorphismus auf $\mathbb{F}_{p^2}$ verkettet. Das erhaltene Bild in $\mathbb{F}_{p^4}$ ist natürlich dasselbe (denn sonst hätte $\mathbb{F}_{p^4}$ mindestens zwei zu $\mathbb{F}_{p^2}$ isomorphe Teilkörper, was Satz 4.7 widerspräche), aber die erhaltenen Abbildungen sind verschieden.

Satz 4.9. *Sei $q = p^n$ eine Primzahlpotenz. Dann ist die Gruppe* $\mathrm{Aut}(\mathbb{F}_q)$ *der Körperautomorphismen von $\mathbb{F}_q$ zyklisch von der Ordnung n und wird vom Frobenius-Automorphismus erzeugt.*

Beweis. Sei $\phi\colon \mathbb{F}_q \to \mathbb{F}_q$ der Frobenius-Automorphismus. Mit dem Satz von Lagrange folgt

$$\phi^n(x) = (\underbrace{\phi \circ \ldots \circ \phi}_{n \text{ mal}})(x) = x^{p^n} = x \quad \text{und also} \quad \phi^n = \mathrm{id}_{\mathbb{F}_q}.$$

Andererseits ist $\phi^k \neq \mathrm{id}_{\mathbb{F}_q}$ für $k < n$, denn das Polynom $X^{p^k} - X \in \mathbb{F}_q$ hat höchstens $p^k < \#\mathbb{F}_q$ viele Nullstellen. Demnach hat ϕ die Ordnung n.
Allerdings haben wir gemäß Proposition 3.4

$$\#\mathrm{Aut}(\mathbb{F}_q) = \#\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q) \leq [\mathbb{F}_q : \mathbb{F}_p]_s \leq [\mathbb{F}_q : \mathbb{F}_p] = n,$$

also insgesamt $\mathrm{Aut}(\mathbb{F}_q) = \{\, \phi^k : 1 \leq k \leq n \,\}$, wie behauptet. □

Der Hauptgegenstand des nächsten Kapitels ist eine Korrespondenz zwischen Teilkörpern einer Körpererweiterung und Untergruppen der zugehörigen relativen Automorphismengruppe. Im Fall endlicher Körper ist diese Automorphismengruppe gemäß Satz 4.9 sehr überschaubar und wir illustrieren die noch zu beweisende Korrespondenz darum hier schon einmal an einem Beispiel; Wir bemühen uns an dieser Stelle nicht, die dabei gemachten Aussagen stichhaltig zu begründen, da deren Richtigkeit einen einfachen Spezialfall der später entwickelten Theorie darstellt.

Beispiel 4.10. In Fortführung von Beispiel 4.8 betrachten wir die zyklische Gruppe $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^{12}}) = \mathrm{Aut}(\mathbb{F}_{p^{12}})$, die vom Frobenius-Automorphismus ϕ erzeugt wird. Die Untergruppen von G sind genau $U_d = \{\, \phi^{kd} : k \in \mathbb{Z} \,\}$ für Teiler $d \geq 1$ von n, wobei Potenzierung von ϕ als Verkettung zu lesen ist. Fassen wir die Körperhomomorphismen in Beispiel 4.8 als Inklusionen auf (man ersetze die Elemente von $\mathbb{F}_{p^k}$ mit ihren Bildern unter der jeweiligen Abbildung $\mathbb{F}_{p^k} \to \mathbb{F}_{p^{12}}$), und definieren wir

$$\mathrm{Gal}(\mathbb{F}_{p^{12}}/\mathbb{F}_{p^k}) = \mathrm{Aut}_{\mathbb{F}_{p^k}}(\mathbb{F}_{p^{12}}),$$

sowie

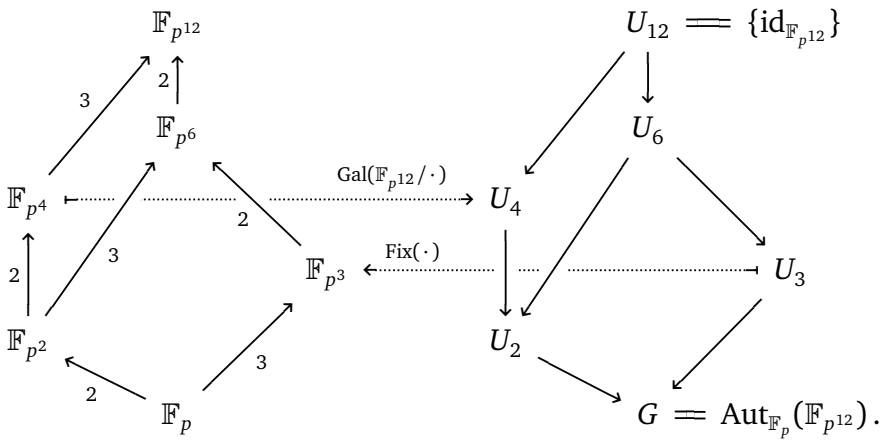
$$\mathrm{Fix}(U) = \{\, x \in \mathbb{F}_{p^{12}} : \forall \psi \in U\,.\, \psi(x) = x \,\}$$

für jede Untergruppe U von G, so erhalten wir dadurch inklusionsumkehrende, zueinander inverse Abbildungen

$$\{\text{Zwischenkörper von } \mathbb{F}_{p^{12}}/\mathbb{F}_p\} \underset{\mathrm{Fix}(\,\cdot\,)}{\overset{\mathrm{Gal}(\mathbb{F}_{p^{12}}/\,\cdot\,)}{\rightleftarrows}} \{\text{Untergruppen von } \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^{12}})\}.$$

(Die Aussage zum zueinander Invers sein könnte man an diesem konkreten Beispiel natürlich in aufwändiger Art und Weise per Hand verifizieren, allerdings beweisen

wir die fragliche Aussage später in Satz 5.3 (1) noch in allgemeinerem Rahmen.) Man veranschaulicht sich dies auch in folgendem Diagramm:



Bemerkung. Sei $\mathbb{F}$ ein beliebiger endlicher Körper. Ein Blick auf die Beweise der Hauptergebnisse dieses Kapitels zeigt die fundamentale Rolle, welche die Endlichkeit der Einheitengruppe endlicher Körper in unseren Untersuchungen eingenommen hat. Die Tatsache, dass alle(!) Elemente von $\mathbb{F}^\times$ dem Satz von Lagrange unterworfen sind, und die — aus der Körpertheorie gezogene — Einsicht, dass wir die Anzahl der Elemente in $\mathbb{F}^\times$ mit gegebener (multiplikativer) Ordnung beschränken können,[8] war Dreh- und Angelpunkt unserer Argumente. (Geneigte Lesende mögen diese Behauptungen verifizieren!)

4.4. Primzahlsatz in $\mathbb{F}_q[X]$

4.4.1. Motivation: Der Primzahlsatz in $\mathbb{N}$. Wir beginnen mit der folgenden klassischen Frage: *Wie viele Primzahlen gibt es?* Nach einem wohl-bekannten Euklid zugeschriebenen Argument gibt es unendlich viele Primzahlen: Zu jeder endlichen Menge $\mathscr{P}$ von Primzahlen ist $n_{\mathscr{P}} = 1 + \prod_{p\in\mathscr{P}} p$ eine ganze Zahl, die von keiner Primzahl aus $\mathscr{P}$ geteilt wird, weswegen man in der Primfaktorzerlegung von $n_{\mathscr{P}}$ eine neue Primzahl findet, die nicht in $\mathscr{P}$ enthalten ist. Also kann die Menge aller Primzahlen nicht endlich sein!

Man kann sich nun fragen *wie häufig* Primzahlen unter den natürlichen Zahlen $\leq x$ auftreten. Unter diesem Betrachtungswinkel ist es naheliegend die ***Primzahlzählfunktion*** $\pi\colon \mathbb{R} \to \mathbb{N}_0$, gegeben durch

$$\pi(x) = \#\{p \in \mathbb{N} \text{ prim} : p \leq x\},$$

zu untersuchen. Mit etwas mehr Arbeit kann man das obige Argument von Euklid quantitativ machen, indem man ausgehend von $\mathscr{P}_1 = \{2\}$ einen Primfaktor p_2 von $n_{\mathscr{P}_1}$ wählt, $\mathscr{P}_2 := \mathscr{P}_1 \cup \{p_2\}$ betrachtet, induktiv fortfährt, und sich überlegt wie schnell die Folge $(p_n)_n$ wachsen kann. Das folgende Argument von Paul Erdős führt einfacher auf

[8] Für Letzteres wird die Endlichkeit von $\mathbb{F}$ aber nicht benötigt.

eine quantitative Aussage: Man schreibe jede natürliche Zahl $n \leq x \in \mathbb{N}$ als Produkt einer ***quadratfreien Zahl*** (das ist eine Zahl, die von keinem Quadrat einer Primzahl geteilt wird) und dem Quadrat einer natürlichen Zahl: $n = rs^2$. Diese Darstellung ist eindeutig, für s gibt es höchstens $\sqrt{x}$ verschiedene Möglichkeiten, und für r gibt es höchstens $2^{\pi(x)}$ verschiedene Möglichkeiten (denn für jede Primzahl $p \leq x$ gilt entweder, dass p die Zahl r teilt, oder nicht, und die Zahl r ist durch diese Information bereits eindeutig bestimmt). Also hat man $2^{\pi(x)}\sqrt{x} \geq \#\{\text{Zahlen} \leq x\} = x$. Durch Umstellen sieht man nun $\pi(x) \geq \frac{1}{2\log 2}\log x$.

Es geht aber deutlich besser! Zur Formulierung der nächsten Ergebnisse erweist sich die sogenannte ***Landau-Notation*** als zweckmäßig: Der Ausdruck „$o(f(x))$ für $x \to \infty$“ stehe als Platzhalter für eine Funktion g mit $\lim_{x\to\infty} g(x)/f(x) = 0$. In ähnlicher Weise schreiben wir $O(f(x))$ als Platzhalter für eine Funktion g, für die es eine von x unabhängige Konstante $c > 0$ gibt, sodass $|g(x)| \leq cf(x)$ für alle x gilt.

Der unabhängig von Adrien-Marie Legendre und Carl Friedrich Gauß kurz vor dem 19. Jahrhundert vermutete, und — unabhängig von einander — von Hadamard und de la Valée Poussin bewiesene ***Primzahlsatz*** proklamiert die Asymptotik[9]

$$\pi(x) = \mathrm{Li}(x)(1 + o(1)) \quad (\text{für } x \to \infty), \quad \text{mit} \quad \mathrm{Li}(x) = \int_2^x \frac{\mathrm{d}t}{\log t}.$$

Mittels partieller Integration gewinnt man leicht die asymptotische Formel

$$\mathrm{Li}(x) = \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right) \quad (\text{für } x \to \infty).$$

Die bisher unbewiesene *Riemannsche Vermutung* würde einen in gewissem Sinne optimalen Fehlerterm im Primzahlsatz liefern (und würde auch umgekehrt aus der Richtigkeit dieser Asymptotik folgen):

$$\pi(x) = \mathrm{Li}(x) + O(\sqrt{x}\log x) \quad (\text{für } x \to \infty).$$

Bisher ist es (leicht vereinfacht dargestellt) lediglich gelungen

$$\pi(x) = \mathrm{Li}(x) + O(x(\log x)^{-k}) \quad (\text{für } x \to \infty)$$

für beliebige $k \geq 1$ zu zeigen (wobei die in der $O(\ldots)$-Notation versteckte implizite Konstante von k abhängen mag), aber den $O(\ldots)$-Term durch $O(x^{1-\epsilon})$ für irgendein auch noch so kleines, aber konstantes $\epsilon > 0$ zu ersetzen, scheint weit abseits von dem zu liegen, was mit aktuell bekannten Methoden erreichbar ist.

[9] Hier und für die weiteren Betrachtungen sei stets $x \geq 2$ angenommen um Probleme mit $\log x \to 0$ für $x \to 1$ zu vermeiden.

4.4.2. Mehr zum analytischen Beweis des Primzahlsatzes. Der übliche Zugang zu den obigen Ergebnissen benutzt *komplexe Analysis*, um eine gewisse komplexwertige Funktion näher zu verstehen, die man als eine Art „multiplikative erzeugende Funktion“ der charakteristischen Funktion der Menge der Primzahlen auffassen kann. In jedem Fall sind diese Untersuchungen sehr subtil und gehen mit einigem technischen Aufwand einher. Darum beschränken wir uns hier darauf, lediglich ein paar Eckpunkte der Beweisstrategie zu skizzieren und verweisen für Details auf entsprechende Standardliteratur, wie etwa [34, 31, 5]. Besonders empfehlenswert ist [27], oder (für Fortgeschrittene!) [21].

Konkret startet man mit der mittels einer sogenannten ***Dirichlet-Reihe*** definierten ***Riemannschen Zeta-Funktion***

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}.$$

Diese Reihe konvergiert für alle s mit Realteil > 1 kompakt und stellt daher eine auf der Halbebene $\{ s \in \mathbb{C} : \operatorname{Re} s > 1 \}$ holomorphe Funktion dar. Riemann zeigte 1859, dass sich eben jene Funktion zu einer auf ganz $\mathbb{C} \setminus \{1\}$ holomorphen Funktion fortsetzt und an der Stelle 1 einen einfachen Pol mit Residuum 1 besitzt. Ferner zeigte Riemann, dass ζ einer gewissen Funktionalgleichung genügt, welche ihre Werte bei s und bei $1-s$ miteinander in Bezug setzt. Ausgangspunkt des zahlentheoretischen Interesses an der Zeta-Funktion ist die schon Euler bekannte Produktdarstellung

$$\zeta(s) = \prod_{p \text{ prim}} (1 - p^{-s})^{-1} \quad (\operatorname{Re} s > 1).$$

Diese gewinnt man, indem man das fragliche Produkt zunächst auf die Primzahlen $p < x$ einschränkt, die Faktoren als geometrische Reihen entwickelt und die so entstehenden Reihenprodukte (Cauchy-Produkt!) ausmultipliziert, um die Formel

$$\prod_{\substack{p \text{ prim} \\ p<x}} (1 - p^{-s})^{-1} = \sum_{\substack{n=1 \\ p \mid n \Rightarrow p < x}}^{\infty} n^{-s}$$

aus der eindeutigen Primfaktorzerlegung in $\mathbb{Z}$ zu erhalten. (Die untere Summationsbedingung soll bedeuten, dass man sich auf diejenigen n einschränkt, deren Primfaktoren alle samt kleiner als x sind.)

Aus der *komplexen Analysis* kennen die Leserinnen und Leser möglicherweise das ***logarithmische Differenzieren***. Dieses hat den Vorteil, dass es Produkte in Summen verwandelt und letztere sind den Methoden der Analysis oft einfacher zugänglich. Dabei ist die logarithmische Ableitung von $(1 - p^{-s})^{-1}$ (nach s) gleich

$$-\frac{p^{-s} \log p}{1 - p^{-s}} = -(\log p) \sum_{\nu=1}^{\infty} p^{-\nu s}$$

Mit Blick auf die obige Produktdarstellung erhält man für die logarithmische Ableitung der Zeta-Funktion also

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{p \text{ prim}} (\log p) \sum_{\nu=1}^{\infty} p^{-\nu s} = \sum_{n=1}^{\infty} \Lambda(n) n^{-s} \quad (\operatorname{Re} s > 1)$$

mit der ***von Mangoldtschen Lambda-Funktion***

$$\Lambda(n) := \begin{cases} \log p & \text{falls } n = p^{\nu} \text{ eine Primzahlpotenz ist,} \\ 0 & \text{sonst.} \end{cases}$$

Mit Hilfe des Residuensatzes lässt sich die sogenannte ***Perronsche Formel*** beweisen, welche die Koeffizientensummen von Dirichletreihen zu extrahieren vermag. Im vorliegenden Fall erhält man für jedes $c > 1$ und $x > 1$ mit $x \notin \mathbb{N}$

$$\sum_{n \le x} \Lambda(n) = \int_{c-\mathrm{i}\infty}^{c+\mathrm{i}\infty} \left(-\frac{\zeta'(s)}{\zeta(s)} \right) x^s \frac{\mathrm{d}s}{s}.$$

Die linke Seite zählt Primzahlpotenzen $\le x$ mit logarithmischem Gewicht. Dabei lässt sich der Beitrag der gezählten Primzahlpotenzen p^{ν} mit $\nu > 1$ leicht abschätzen und das Gewicht vor den gezählten Primzahlen lässt sich ebenfalls leicht (mit einer als ***partielle Summation*** bekannten Technik) entfernen. Das Ergebnis dieser Manipulationen ist, dass sich ein gutes Verständnis der linken Seite der obigen Gleichung direkt in ein Verständnis der Primzahlzählfunktion π übersetzt. Um nun die linke Seite zu verstehen, wenden sich Analytikerinnen und Analytiker furchtlos zur rechten Seite. Die Idee besteht nun darin, den Integrationsweg weiter nach links ($c < 1$) zu verschieben, da dort der Faktor x^s im Integranden kleiner wird und man darum vielleicht hoffen darf, die Integration durch grobe Abschätzungen zu behandeln.

Man beachte, dass hierfür die analytische Fortsetzung der Zeta-Funktion von ausgezeichneter Wichtigkeit ist, da erst dank dieser der Integrand tatsächlich meromorph auf einem Gebiet von geeigneter Größe ist. Gleichwohl wird man auch vor das schwierige Problem gestellt, die Zeta-Funktion links der 1 zu verstehen. Derartiges Verständnis scheint zwar bis heute schwer fassbar, aber dennoch gelang der Mathematik schon der ein oder andere Blick, wenngleich unter erheblichem Kraftaufwand.

Nutzt man nun den Residuenkalkül für die erwähnte Verschiebung, so handelt man sich dabei natürlich Korrekturterme bedingt durch Polstellen der logarithmischen Ableitung von ζ ein. Diese Polstellen kommen einzig von dem Pol von ζ bei 1 und den etwaigen *Nullstellen von* ζ in der Halbebene $\{ s \in \mathbb{C} : \operatorname{Re} s > c \}$.[10] Die berühmte ***Riemannsche Vermutung*** proklamiert, dass es für $c = 1/2$ keine solchen Nullstellen gibt. Bisher sind jedoch nur Ergebnisse bekannt, welche die Nullstellenfreiheit von ζ in Gebieten der Form

$$\{ s \in \mathbb{C} : \operatorname{Re} s > 1 - f(|\operatorname{Im} s|) \}$$

[10] Genau genommen muss man auch sicherstellen, dass die Spur des gewählten Integrationsweges frei von Polstellen ist, aber wir ignorieren derartige technische Details hier.

liefern, wo $f\colon \mathbb{R}_{\geq 0} \to (0,1/2)$ eine gewisse monoton gegen 0 fallende Funktion ist. Bereits diese Ergebnisse erforderten geniale Ideen und erheblichen technischen Aufwand; Wir besprechen hier allerdings nichts davon und wenden uns stattdessen sogleich wieder der *Algebra* zu.

4.4.3. Zurück in die Algebra. Die Frage nach dem Zählen von Primzahlen in $\mathbb{Z}$ liegt im Umfeld der hier entwickelten Theorie also zu tief, um diese im Rahmen eines kurzen Abstechers behandeln zu können. Umso überraschender mag es erscheinen, dass wir hier — mit vergleichsweise sehr bescheidenem Aufwand — eine sehr präzise Antwort auf die analoge Frage für $\mathbb{F}_q[X]$ geben können: Wir betrachten den Polynomring $\mathbb{F}_q[X]$ über einem endlichen Körper $\mathbb{F}_q$ mit Primzahlpotenz q. Dieser Polynomring ist faktoriell; Irreduzible Elemente und Primelemente stimmen also überein. — *Wie viele gibt es davon?*
Konkret sei

$$\mathscr{P}_n = \{\text{normierte, irreduzible Polynome in } \mathbb{F}_q[X] \text{ mit Grad } n\}.$$

Wir sind daran interessiert $\pi_=(n;q) = \#\mathscr{P}_n$ zu bestimmen. (Man beachte, dass unsere Einschränkung auf *normierte* irreduzible Polynome analog zu unserer obigen Einschränkung auf *positive* Primzahlen/Primelemente in $\mathbb{Z}$ entspricht: Es geht in beiden Fällen darum, zu vermeiden, dass man assoziierte Elemente mehrfach zählt.)

Wir fixieren einen algebraischen Abschluss $\mathbb{F}_q \to \mathbb{F}_q^{\mathrm{a}}$ von $\mathbb{F}_q$. Aus Satz 4.7 folgt, dass $\mathbb{F}_q^{\mathrm{a}}$ für jede natürliche Zahl n genau einen zu $\mathbb{F}_{q^n}$ $\mathbb{F}_q$-isomorphen Teilkörper enthält. Wir identifizieren alle diese Körper mit ihren Bildern in $\mathbb{F}_q^{\mathrm{a}}$. Im Sinne von Satz 4.7 haben wir dann also $\mathbb{F}_{q^k} \subseteq \mathbb{F}_{q^n}$ genau dann wenn k ein Teiler von n ist.

Die Nullstellen (in $\mathbb{F}_q^{\mathrm{a}}$) aller Polynome aus $\mathscr{P}_n$ erzeugen nun eine *endliche* Körpererweiterung $\mathbb{F}_q \to F$ und jede der betrachteten Nullstellen x erzeugt darin einen Teilkörper $\mathbb{F}_q(x)$ mit Grad $[\mathbb{F}_q(x) : \mathbb{F}_q] = n$, also $\mathbb{F}_q(x) = \mathbb{F}_{q^n} \subseteq \mathbb{F}_q^{\mathrm{a}}$. Zusammen mit der Separabilität von $\mathbb{F}_q \to \mathbb{F}_{q^n}$ (siehe Satz 4.1) ergibt sich also

$$\begin{aligned} n\pi_=(n;q) &= \#\{\, x \in \mathbb{F}_{q^n} : [\mathbb{F}_q(x) : \mathbb{F}_q] = n \,\} \\ &= \#\{\, x \in \mathbb{F}_{q^n} : x \notin \bigcup \{\text{Zwischenkörper } F \subsetneq \mathbb{F}_{q^n} \text{ von } \mathbb{F}_{q^n}/\mathbb{F}_q\} \,\} \\ &= \#\{\, x \in \mathbb{F}_{q^n} : x \notin \bigcup \{\text{maximale Körper } F \text{ mit } \mathbb{F}_q \subseteq F \subsetneq \mathbb{F}_{q^n}\} \,\}. \end{aligned}$$

Ist nun $n = p_1^{\nu_1} \cdots p_t^{\nu_t}$ die Primfaktorzerlegung von n, so folgt aus Satz 4.7, dass die maximal großen Körper F mit $\mathbb{F}_q \subseteq F \subsetneq \mathbb{F}_{q^n}$ genau durch $F_i := \mathbb{F}_{q^{n/p_i}}$ mit $1 \leq i \leq t$ gegeben sind. Ferner ist für jede Indexmenge $\mathscr{I} \subseteq \{1,\dots,t\}$

$$\bigcap_{i\in\mathscr{I}} F_i = \mathbb{F}_{q^{n/p(\mathscr{I})}} \quad \text{mit} \quad p(\mathscr{I}) = \prod_{i\in\mathscr{I}} p_i.$$

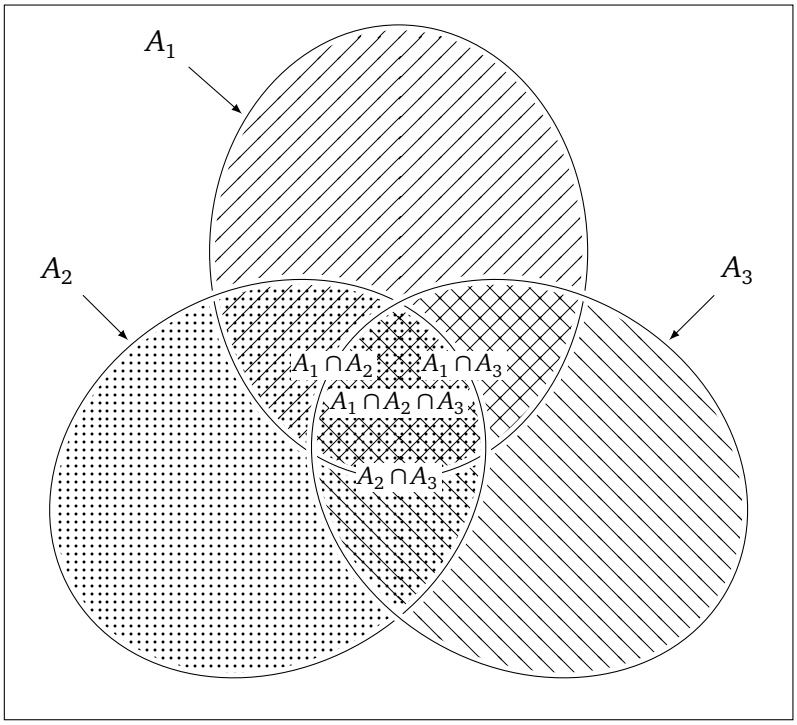


Abbildung 7. Das Prinzip der Inklusion–Exklusion für die Vereinigung von drei Mengen: $\#(A_1 \cup A_2 \cup A_3) = \#A_1 + \#A_2 + \#A_3 - \#(A_1 \cap A_2) - \#(A_1 \cap A_3) - \#(A_2 \cap A_3) + \#(A_1 \cap A_2 \cap A_3)$.

Wir erinnern an das kombinatorische ***Prinzip der Inklusion–Exklusion***: Für beliebige endliche Mengen $\mathscr{A}_1, \ldots, \mathscr{A}_t$ ist

$$\begin{aligned}\#\bigcup_{1\le i\le t}\mathscr{A}_i &= \sum_{1\le i\le t}\#\mathscr{A}_i - \sum_{1\le i_1<i_2\le t}\sum\#(\mathscr{A}_{i_1}\cap\mathscr{A}_{i_2}) + \sum_{1\le i_1<i_2<i_3\le t}\sum\sum\#(\mathscr{A}_{i_1}\cap\mathscr{A}_{i_2}\cap\mathscr{A}_{i_3}) \mp \ldots \\ &= \sum_{1\le m\le t}(-1)^{m+1}\sum_{1\le i_1<\ldots<i_m\le t}\ldots\sum\#(\mathscr{A}_{i_1}\cap\ldots\cap\mathscr{A}_{i_m}).\end{aligned}$$

Wir haben also

$$\begin{aligned}n\pi_=(n;q) &= \#\Big(\mathbb{F}_{q^n}\setminus\bigcup\nolimits_{i=1}^{t}\mathbb{F}_{q^{n/p_i}}\Big) \\ &= q^n + \sum_{1\le m\le t}(-1)^m\sum_{1\le i_1<\ldots<i_m\le t}\ldots\sum\#(F_{i_1}\cap\ldots\cap F_{i_k}) \\ &= q^n + \sum_{1\le m\le t}(-1)^m\sum_{1\le i_1<\ldots<i_m\le t}\ldots\sum q^{n/(p_{i_1}\cdots p_{i_m})}.\end{aligned} \tag{4.1}$$

Wir führen kurz die ***Möbiussche μ-Funktion*** ein, die eine Zahl n, welche durch kein Primzahlquadrat teilbar ist, auf $\mu(n) = (-1)^{\omega(n)}$ abbildet, wobei $\omega(n)$ die Anzahl der verschiedenen Primteiler von n bezeichne, und alle anderen n (teilbar durch ein

Primzahlquadrat) auf 0 abbildet. Damit schreibt sich (4.1) auch kurz in der Form

$$\pi_=(n;q) = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d} = \frac{q^n}{n} + \frac{1}{n}\sum_{\substack{d|n\\ d>1}}\mu(d)q^{n/d}.$$

Schreibt man in (4.1) $d = p_{i_1}\cdots p_{i_m}$, so durchläuft die dortige Summation genau die *quadratfreien* Teiler $d > 1$ von n. Davon gibt es genau $2^t - 1$ viele, wie man sich kombinatorisch überlegen kann: Für jeden der t Primteiler von n kann man sich aussuchen, ob diese das zu konstruierende d teilen soll, oder nicht. Es gibt also 2^t Möglichkeiten quadratfreie Teiler $d \geq 1$ von n zu konstruieren, von denen wir aber den Teiler $d = 1$ nicht zählen. Wir erhalten also

$$\left|\pi_=(n;q) - \frac{q^n}{n}\right| < \frac{1}{n}\sum_{\substack{d|n\\ d \text{ quadratfrei}}} q^{n/2} = \frac{2^t}{n}\,q^{n/2}.$$

Mit $2 \leq p_i$ folgt dann weiter

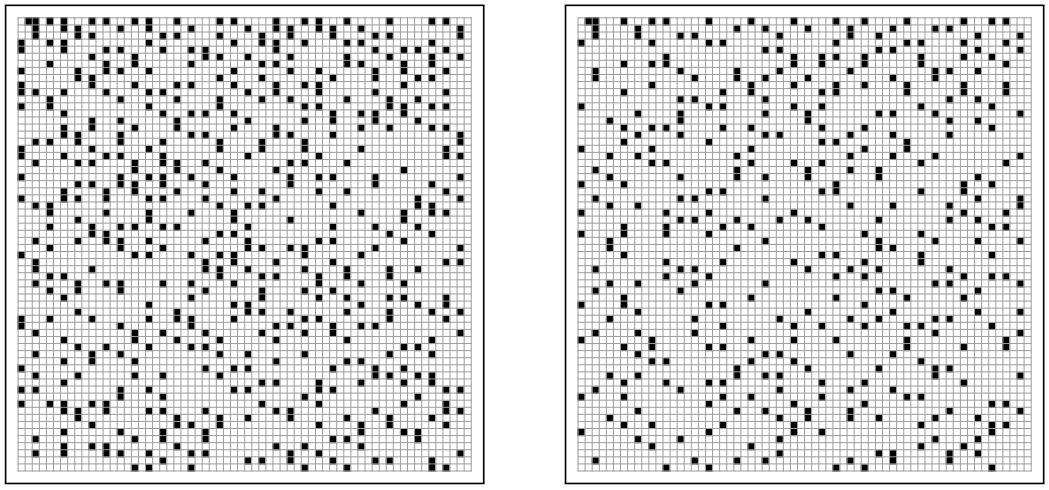
$$\left|\pi_=(n;q) - \frac{q^n}{n}\right| < \frac{p_1\cdots p_t}{n}\,q^{n/2} \leq q^{n/2}.$$

Zusammenfassend haben wir also Folgendes bewiesen:

Satz 4.11 (Primzahlsatz in $\mathbb{F}_q[X]$)**.** *Sei q eine Primzahlpotenz. Für die Anzahl $\pi_=(n;q)$ der normierten irreduziblen Polynome in $\mathbb{F}_q[X]$ vom Grad n gilt dann*

$$\left|\pi_=(n;q) - \frac{q^n}{n}\right| < q^{n/2}.$$

Bemerkung. Der hier geführte Beweis von Satz 4.11 folgt Chebulo und Mináč [10] und gibt den einzelnen Termen in (4.1) eine kombinatorische Bedeutung. Der Satz selbst war schon Gauß bekannt (siehe [17, S. 606–612]). In seinem Beweis zählt Gauß die irreduziblen Polynome und auf wie viele Arten sich reduzible Polynome durch Produktbildung aus diesen ergeben. Für einen Zeta-funktionentheoretischen Beweis von Satz 4.11 siehe [29].



(a) Primzahlen. **(b)** Irreduzible Polynome in $\mathbb{F}_2[X]$.

Abbildung 8. Veranschaulichung zu den Primzahlsätzen: die Kästchen korrespondieren, reihenweise von oben nach unten gelesen, den Zahlen $1, 2, 3, 4, \ldots, 4096$ bzw. Polynomen in $\mathbb{F}_2[X]$ mittels $\sum_i a_i 2^i \mapsto \sum_i (a_i + 2\mathbb{Z})X^i$ (in Binärdarstellung). Kästchen zu Primzahlen bzw. irreduziblen Polynomen sind schwarz hervorgehoben.

KAPITEL 5

Galois-Theorie und ihre Anwendungen

Wir betrachten im Folgenden stets Körpererweiterungen L/K, also solche Körpererweiterungen $\iota\colon K \to L$, bei denen K eine Teilmenge von L ist und ι mit der Inklusion $\mathrm{id}_L|_K : K \to L$ übereinstimmt.
Für jede Untergruppe $U \subseteq \mathrm{Aut}(L)$ von Automorphismen von L betrachten wir den zugehörigen ***Fixkörper***:

$$\mathrm{Fix}(U) = \{\, x \in L : \forall f \in U\colon f(x) = x \,\}.$$

Wir bezeichnen L/K als eine ***Galois-Erweiterung***, falls diese endlich, normal und separabel ist. In diesem Fall schreiben wir

$$\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$$

und nennen dies die ***Galois-Gruppe von L/K***. Für jeden Zwischenkörper M von L/K ist auch L/M eine Galois-Erweiterung[1] und es ist $\mathrm{Gal}(L/M) \subseteq \mathrm{Gal}(L/K)$.

Wie in Beispiel 4.10 erhalten wir inklusionsumkehrende Abbildungen

$$\{\text{Zwischenkörper von } L/K\} \underset{\mathrm{Fix}(\,\cdot\,)}{\overset{\mathrm{Gal}(L/\,\cdot\,)}{\rightleftarrows}} \{\text{Untergruppen von } \mathrm{Gal}(L/K)\}\,. \tag{5.1}$$

Die Beziehung beider Abbildungen zueinander ist Thema des Hauptsatzes der Galois-Theorie (siehe Satz 5.3) und dieser bietet ein Hilfsmittel zum Studium einer Körpererweiterung L/K und ihres Zwischenkörperverbandes durch den (oft auch wiederholten) Wechsel zur Gruppentheorie.

Bemerkung. Unsere Definition von Galois-Erweiterungen fordert endlichen Grad. Man kann auch auf diese Forderung verzichten und somit Galois-Theorie für Körpererweiterungen mit potentiell unendlichem Grad studieren, muss hier allerdings die relative Automorphismengruppe der fraglichen Körpererweiterung zusätzlich mit der Struktur einer topologischen Gruppe ausstatten. In der Situation von (5.1) muss man dann von abgeschlossenen Untergruppen sprechen. (Dies wirkt gewissermaßen dem Umstand entgegen, dass $\mathrm{Gal}(L/K)$ sonst viel reichhaltiger an Untergruppen ist, als die Erweiterung L/K an Zwischenkörpern.)

[1] Benutze Satz 1.7, Satz 3.10, sowie Satz 3.5.

5.1. Hauptsatz der Galois-Theorie

Ziel dieses Abschnittes ist Satz 5.3. Bevor wir jedoch zu diesem Satz kommen, sammeln wir zwei Hilfsresultate über die Körperautomorphismen. Das Erste davon kennen wir im Prinzip schon:

Proposition 5.1. *Eine endliche Körpererweiterung L/K ist genau dann eine Galois-Erweiterung, wenn* $\mathrm{Aut}_K(L)$ *aus genau* $[L:K]$ *Elementen besteht.*

Beweis. Das folgt direkt aus unseren Definitionen von Normalität und Separabilität. (Siehe auch die Diskussion auf Seite 43.) □

Das nächste Resultat — welches als ***Lemma von Artin*** bekannt ist — besagt, grob gesprochen, dass Körperautomorphismen *viele* Elemente fixieren und also stets einen großen Fixkörper produzieren.

Lemma 5.2 (Artin)**.** *Sei L ein Körper und U eine endliche Gruppe von Automorphismen von L. Dann gilt $[L:\mathrm{Fix}(U)] \leq \#U$. Insbesondere ist $\#\mathrm{Aut}_{\mathrm{Fix}(U)}(L) \leq \#U$.*

Beweis. Zwecks Erzeugung eines Widerspruchs sei $[L:\mathrm{Fix}(U)] > \#U =: k$ angenommen. Dann gibt es $k+1$ viele $\mathrm{Fix}(U)$-linear unabhängige Elemente $v_0, v_1, \ldots, v_k \in L$. Wir schreiben $U = \{f_1, \ldots, f_k\}$ und bemerken, dass das (unterbesetzte!) lineare Gleichungssystem

$$\begin{pmatrix} f_1(v_0) & f_1(v_1) & \ldots & f_1(v_k) \\ \vdots & \vdots & \ddots & \vdots \\ f_k(v_0) & f_k(v_1) & \ldots & f_k(v_k) \end{pmatrix} \begin{pmatrix} X_0 \\ X_1 \\ \vdots \\ X_k \end{pmatrix} \overset{!}{=} \begin{pmatrix} 0_L \\ \vdots \\ 0_L \end{pmatrix}$$

eine nichttriviale Lösung $\boldsymbol{x} = (x_0, x_1, \ldots, x_k) \in L^{k+1} \setminus \{\mathbf{0}\}$ besitzt. Wir wählen eine solche Lösung mit *maximal* vielen Null-Einträgen und nehmen ohne Einschränkung (durch etwaige Umnummerierung der $v_0, v_1, \ldots, v_k$ und Normierung) $x_0 = 1_L$ an.

Die zu $\mathrm{id}_L \in U$ gehörige Gleichung im obigen System liefert

$$v_0 + v_1 x_1 + \ldots + v_k x_k = 0_L.$$

Wegen der $\mathrm{Fix}(U)$-linearen Unabhängigkeit von $v_0, v_1, \ldots, v_k$ können nicht alle Elemente $x_1, \ldots, x_k$ in $\mathrm{Fix}(U)$ liegen. — Ohne Einschränkung sei $x_1 \notin \mathrm{Fix}(U)$ und entsprechend $g \in U$ derart, dass $g(x_1) \neq x_1$. Nun ist aber auch

$$g(\boldsymbol{x}) \coloneqq (g(x_0), g(x_1), \ldots, g(x_k)) \neq \boldsymbol{x}$$

eine Lösung vom obigen Gleichungssystem (hier geht ein, dass U als Untergruppe multiplikativ[2] abgeschlossen ist und das Vorschalten von g somit nur Permutation der Zeilen des obigen Gleichungssystems bewirkt). Dann ist aber auch die Differenz

$$g(\boldsymbol{x}) - \boldsymbol{x} = (0_L, g(x_1) - x_1, \ldots, g(x_k) - x_k) \neq \mathbf{0}$$

eine solche Lösung, hat aber mehr Null-Einträge als $\boldsymbol{x}$, ein Widerspruch! □

[2] Die Verknüpfung in der Gruppe $\mathrm{Aut}(L) \geq U$ ist natürlich die *Verknüpfung von Abbildungen*.

Bemerkung. Die Voraussetzung an U in Lemma 5.2 eine Untergruppe zu sein ist wichtig, wie das folgende Beispiel lehrt: wir betrachten den Körper $\mathbb{C}$ der komplexen Zahlen und die komplexe Konjugation $\tau\colon \mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{z}$. Natürlich ist $\mathbb{R} = \mathrm{Fix}(\{\tau\}) = \mathrm{Fix}(U)$ mit $U = \langle\tau\rangle = \{\mathrm{id}_{\mathbb{C}}, \tau\}$. Nun ist $2 = [\mathbb{C} : \mathrm{Fix}(U)] \leq \#U = 2$, aber $[\mathbb{C} : \mathrm{Fix}(\{\tau\})] = 2 \not\leq 1 = \#\{\tau\}$. Im Beweis von Lemma 5.2 wird die Untergruppeneigenschaft von U bei der Überlegung gebraucht, welche $g(\boldsymbol{x})$ als weitere Lösung des oben betrachteten Gleichungssystems identifiziert.

Nun kommen wir zum Schlüsselergebnis dieses Kapitels, dem ***Hauptsatz der (endlichen) Galois-Theorie***. Der Rest dieses Kapitels wird anschließend bemüht sein, interessante Konsequenzen aus dem Hauptsatz zu ziehen. Wir verzichten im Folgenden stets auf das zusätzliche Attribut „endlich“, behalten jedoch die Bemerkung von Seite 61 im Hinterkopf, dass es auch eine *unendliche* Galois-Theorie gibt, für deren Studium hier allerdings die Zeit fehlt.

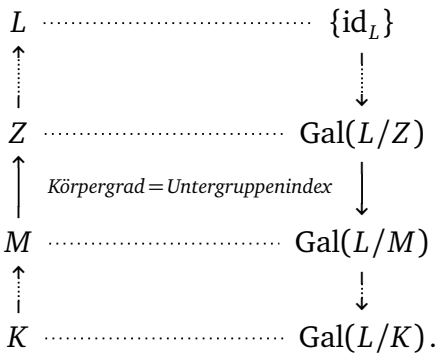
Satz 5.3 (Hauptsatz der Galois-Theorie)**.** *Sei L/K eine Galois-Erweiterung mit Galois-Gruppe $G = \mathrm{Gal}(L/K)$ und M ein Zwischenkörper von L/K. Dann gilt:*

*(1) (**Galois-Korrespondenz**.) Bei den beiden Abbildungen $\mathrm{Gal}(L/\cdot)$ und $\mathrm{Fix}(\cdot)$ aus (5.1) handelt es sich um zueinander inverse, inklusionsumkehrende Bijektionen. (Insbesondere ist $K = \mathrm{Fix}(\mathrm{Gal}(L/K))$.)*

(2) Ist Z ein Zwischenkörper von L/M, so ist

$$[Z : M] = [\mathrm{Gal}(L/M) : \mathrm{Gal}(L/Z)].$$

Man illustriert sich diese Situation wie folgt:



(3) Die Erweiterung M/K ist genau dann Galois, wenn $\mathrm{Gal}(L/M)$ ein Normalteiler von G ist. In diesem Fall induziert die Einschränkungsabbildung

$$G \longrightarrow \mathrm{Gal}(M/K), \quad f \longmapsto (f|_M)$$

einen Isomorphismus $G/\mathrm{Gal}(L/M) \cong \mathrm{Gal}(M/K)$.

Beweis. Die Aussage über das Umkehren von Inklusionen in (1) ist offensichtlich. Zum Beweis der gegenseitigen Inversionseigenschaft sei zunächst Z ein beliebiger

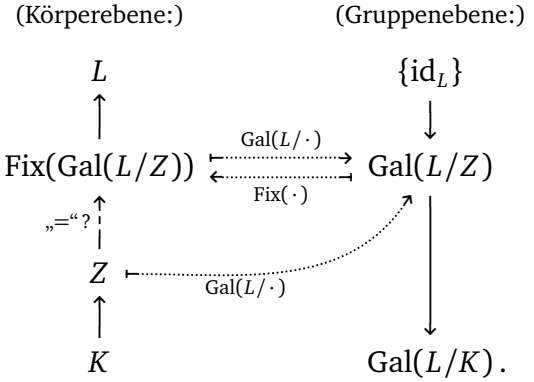
Zwischenkörper von L/K. Wir betrachten den Körper $\mathrm{Fix}(\mathrm{Gal}(L/Z)) \supseteq Z$. Wir haben (man beachte $\mathrm{Fix}(\mathrm{Gal}(L/Z)) \supseteq Z$)

$$\begin{aligned}\mathrm{Gal}(L/\mathrm{Fix}(\mathrm{Gal}(L/Z))) &= \{\mathrm{Fix}(\mathrm{Gal}(L/Z))\text{-Automorphismen von } L\}\\ &= \{Z\text{-Automorphismen von } L, \text{ die } \mathrm{Fix}(\mathrm{Gal}(L/Z)) \text{ fixieren}\}\\ &= \{f \in \mathrm{Gal}(L/Z) : \underbrace{f \text{ fixiert } \mathrm{Fix}(\mathrm{Gal}(L/Z))}_{\text{tautologisch}}\}\\ &= \mathrm{Gal}(L/Z),\end{aligned}$$

wobei wir für die letzte Gleichung benutzt haben, dass *jedes* $f \in \mathrm{Gal}(L/Z)$ trivialerweise $\mathrm{Fix}(\mathrm{Gal}(L/Z))$ fixiert, da ja für diese Fixkörper-Bildung genau die Elemente ausgewählt werden, die von *allen* Elementen von $\mathrm{Gal}(L/Z)$ (also insbesondere von f) fixiert werden. Mit Proposition 5.1 folgt die Gleichheit der Grade

$$[L : \mathrm{Fix}(\mathrm{Gal}(L/Z))] = [L : Z],$$

und somit $\mathrm{Fix}(\mathrm{Gal}(L/Z)) = Z$ gemäß Satz 1.7. Man veranschaulicht sich das soeben geführte Argument vielleicht anhand der folgenden Abbildung:



Sei nun umgekehrt U eine Untergruppe von G. Zunächst ist

$$\mathrm{Gal}(L/\mathrm{Fix}(U)) = \{\mathrm{Fix}(U)\text{-Automorphismen von } L\} \supseteq U,$$

da ja jedes Element von U die Elemente von $\mathrm{Fix}(U)$ fixiert und somit ein $\mathrm{Fix}(U)$-Automorphismen von L ist. Wegen Lemma 5.2 besteht $\mathrm{Gal}(L/\mathrm{Fix}(U))$ aus höchstens $\#U$ vielen Elementen. Das zeigt auch schon $\mathrm{Gal}(L/\mathrm{Fix}(U)) = U$.

Teil (2) erhält man unmittelbar aus Satz 1.7 und Proposition 5.1:

$$[Z : M] = \frac{[L : M]}{[L : Z]} = \frac{\#\mathrm{Gal}(L/M)}{\#\mathrm{Gal}(L/Z)} = [\mathrm{Gal}(L/M) : \mathrm{Gal}(L/Z)].$$

Zum Beweis von (3) bemerken wir zunächst die Gültigkeit der folgenden Identität:

$$\begin{aligned} f(\mathrm{Fix}(U)) &= \{\, x \in L : f^{-1}(x) \in \mathrm{Fix}(U) \,\} \\ &= \{\, x \in L : \forall g \in U\colon g(f^{-1}(x)) = f^{-1}(x) \,\} \\ &= \{\, x \in L : \forall g \in U\colon (f \circ g \circ f^{-1})(x) = f(g(f^{-1}(x))) = x \,\} \\ &= \mathrm{Fix}(f \circ U \circ f^{-1}). \end{aligned}$$

Durch Anwenden der Galois-Korrespondenz folgt hieraus

$$f \circ \mathrm{Gal}(L/M) \circ f^{-1} = \mathrm{Gal}(L/f(M))$$

für jeden Zwischenkörper M von L/K und jedes $f \in G$. Zusammen der Galois-Korrespondenz und Satz 3.10 (beachte Teil (2) davon) erhält man damit nun

$$\begin{aligned} &\mathrm{Gal}(L/M) \text{ ist eine normale Untergruppe von } \mathrm{Gal}(L/K) \\ &\quad\Longleftrightarrow (\forall f \in G\colon\ \mathrm{Gal}(L/f(M)) = \mathrm{Gal}(L/M)) \\ &\quad\Longleftrightarrow (\forall f \in G\colon f(M) = M) \\ &\quad\Longleftrightarrow M/K \text{ ist eine normale Körpererweiterung.} \end{aligned}$$

Ist nun $\mathrm{Gal}(L/M)$ normal in $\mathrm{Gal}(L/K)$, so liefert die Gültigkeit der mittleren Aussage in obiger Äquivalenz unmittelbar, dass es sich bei der Einschränkungsabbildung

$$\Psi\colon G \longrightarrow \mathrm{Gal}(M/K), \quad f \longmapsto f|_M$$

wirklich um eine wohl-definierte Abbildung handelt. Selbstverständlich ist diese sogar ein Gruppenhomomorphismus. Da sich jedes Element von $\mathrm{Gal}(L/M)$ zu id_M einschränkt, ist $\mathrm{Gal}(L/M) \subseteq \ker\Psi$. Wegen $M = \mathrm{Fix}(\mathrm{Gal}(L/M)) \supseteq \mathrm{Fix}(\ker\Psi) \supseteq M$ folgt $\mathrm{Fix}(\mathrm{Gal}(L/M)) = \mathrm{Fix}(\ker\Psi)$ und die Injektivität von $\mathrm{Fix}(\,\cdot\,)$ liefert $\mathrm{Gal}(L/M) = \ker\Psi$. Es verbleibt noch zu sehen, dass Ψ surjektiv ist. Wir wählen nun eine Einbettung von L/K in einen algebraischen Abschluss K^{a} von K und gehen o.B.d.A. durch Umbenennung von Elementen davon aus, dass es sich bei der Einbettung um eine Teilmengeninklusion handelt. Jedes $\tilde{f} \in \mathrm{Gal}(M/K)$ setzt sich zu einem K-Homomorphismus $f\colon L \to K^{\mathrm{a}}$ fort. Da L normal ist, hat f dasselbe Bild wie die Inklusion $L \hookrightarrow K^{\mathrm{a}}$, nämlich L. Also ist $f \in \mathrm{Gal}(L/K)$ und nach Konstruktion ist $\Psi(f) = f|_M = \tilde{f}$. Insgesamt ist Ψ also ein surjektiver Gruppenhomomorphismus mit Kern $\mathrm{Gal}(L/M)$. □

5.2. Satz vom primitiven Element

Ziel dieses Abschnittes ist es zu verstehen, wann eine endliche Körpererweiterung L/K einfach ist, also $L = K(x)$ für ein $x \in L$ erfüllt. — Ein solches x bezeichnet man dann als ***primitives Element*** und daher rührt der Name des Satzes. Das Hauptresultat hierzu ist der Satz vom primitiven Element in seiner allgemeinen Form (siehe Satz 5.5).

Ist $\#L$ endlich, so ist die Situation besonders einfach und mit Korollar 4.6 bereits bestens verstanden. Für das weitere Vorgehen benötigen wir ein Lemma aus der *linearen Algebra* (siehe auch Abbildung 9):

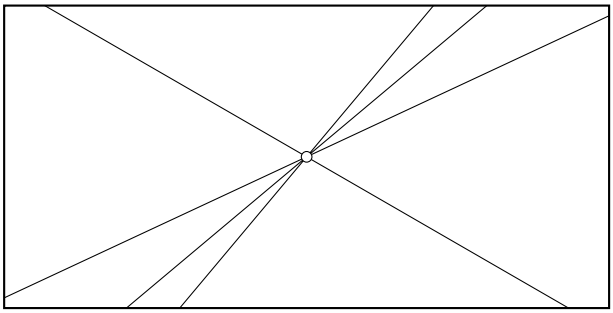


Abbildung 9. Illustration zu Lemma 5.4: Gezeichnet ist ein zweidimensionaler reeller Vektorraum (als Ebene) und endlich viele (vier) darin enthaltene Unterräume der Dimension Eins (Geraden). Offensichtlich gelingt es *nicht* die Ebene durch *endlich viele* solcher Unterräume auszuschöpfen. Auch im Dreidimensionalen (schwieriger zu zeichnen) scheint es anschaulich unmöglich, den Raum durch eine endliche Vereinigung von Ebenen und Geraden (und dem Nullraum) auszuschöpfen. Dass diese anschauliche Vorstellung auch nicht irreführend ist, sondern tatsächlich stimmt, ist die Aussage von Lemma 5.4.

Lemma 5.4. *Sei V ein Vektorraum über einem Körper K mit unendlich vielen Elementen. Dann ist V nicht die Vereinigung endlich vieler echter Unterräume.*

Beweis. Angenommen dies wäre falsch und es gäbe ein minimales $t \geq 2$ mit Unterräumen $U_1, U_2, \ldots, U_t \subsetneq V$ und $V = U_1 \cup U_2 \cup \ldots \cup U_t$. Wegen $U_1 \subsetneq V$ gibt es $v \in V \setminus U_1$. Wegen der Minimalität von t ist $U_1 \nsubseteq U_2 \cup \ldots \cup U_t$; Es gibt also $u_1 \in U_1$ mit $u_1 \notin U_2 \cup \ldots \cup U_t$.

Für jedes $\lambda \in K$ gibt es nun auch einen Index j mit $\lambda u_1 + v \in U_j$ und, da K unendlich viele Elemente enthält, gibt es auch $\lambda \neq \lambda'$ und ein j mit $\lambda u_1 + v, \lambda' u_1 + v \in U_j$. Also ist auch

$$u_1 = \frac{(\lambda u_1 + v) - (\lambda' u_1 + v)}{\lambda - \lambda'} \in U_j$$

und somit $j = 1$ nach Wahl von u_1. Dann ist aber auch $v = (\lambda u_1 + v) - \lambda u_1 \in U_1$, im Widerspruch zur Wahl von v. □

Satz 5.5 (Satz vom primitiven Element, II)**.** *Sei L/K eine endliche Körpererweiterung. Genau dann gibt es ein $x \in L$ mit $L = K(x)$, wenn die Erweiterung L/K nur endlich viele Zwischenkörper besitzt.*

Beweis. Sei zunächst $L = K(x)$ und m_x das Minimalpolynom von x über K. Sei L' ein beliebiger Zwischenkörper von L/K und m'_x das Minimalpolynom von x über L'. Dann ist m'_x ein Teiler von m_x in $L[X]$.[3] Tatsächlich ist die so konstruierte Abbildung

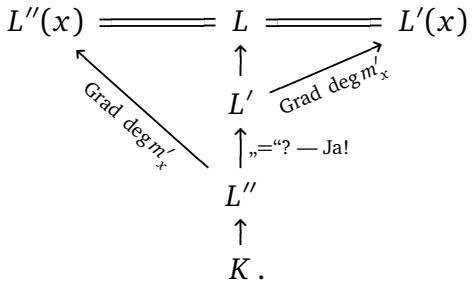
$$\{\text{Zwischenkörper von } L/K\} \longrightarrow \{\text{normierte Teiler von } m_x \text{ in } L[X]\}$$

[3]Die schmutzigen Details hierzu hatten wir uns bereits im Beweis von Satz 2.12 überlegt.

injektiv: Ist nämlich L'' der Zwischenkörper von L'/K, der von den Koeffizienten von m'_x erzeugt wird, so ist m'_x auch in $L''[X]$ irreduzibel und wir haben

$$[L : L''] = [L''(x) : L''] = \deg m'_x = [L'(x) : L'] = [L : L']$$

und somit $L' = L''$. Da nun m_x in $L[X]$ nur endlich viele normierte Teiler besitzt, folgt die Endlichkeit der Anzahl aller Zwischenkörper von L/K. Analog zum einen Teil unseres Beweises von Satz 5.3 (1) kann man sich das eben geführte Argument vielleicht an folgender Abbildung verdeutlichen:



Zum Beweis der umgekehrten Richtung dürfen wir auf Grund von Korollar 4.6 davon ausgehen, dass L unendlich viele Elemente besitzt. Da jeder Zwischenkörper von L/K ein K-Vektorraum ist, zeigt Lemma 5.4, dass es ein $x \in L$ gibt, welches in *keinem* echten Zwischenkörper von L/K enthalten ist. Für dieses x gilt dann notwendigerweise $L = K(x)$. □

Proposition 5.6. *Sei L/K eine endliche separable Erweiterung. Dann existiert eine Galois-Erweiterung L^g/K, welche L als Zwischenkörper enthält.*

Beweis. Das ist Aufgabe 6.3. □

Die Körpererweiterung L^g/K aus Proposition 5.6 bezeichnet man auch als die ***Galois-Hülle von L/K***, sofern diese minimal in dem Sinne ist, dass es keinen Zwischenkörper Z von L^g/L gibt derart, dass Z normal ist. Unter Benutzung von L^g/K und dem Hauptsatz der Galois-Theorie lässt sich ein besonders brauchbarer Spezialfall von Satz 5.5 isolieren, der auch als Satz vom primitiven Element bekannt ist:

Korollar 5.7 (Satz vom primitiven Element, III)**.** *Sei L/K eine endliche separable Erweiterung. Dann besitzt L/K nur endlich viele Zwischenkörper. Insbesondere ist $L = K(x)$ für ein $x \in L$.*

Beweis. Gemäß Proposition 5.6 dürfen wir L als Zwischenkörper in einer Galois-Erweiterung L^g/K annehmen. Deren Zwischenkörper korrespondieren laut Satz 5.3 nun aber zu den Untergruppen der (endlichen!) Gruppe $\mathrm{Gal}(L^g/K)$; Hiervon gibt es nur endlich viele. Da jeder Zwischenkörper von L/K auch ein Zwischenkörper von L^g/K ist, folgt hieraus der erste Teil der Aussage des Korollars. Der zweite Teil folgt aus dem ersten zusammen mit Satz 5.5. □

Korollar 5.8. *Sei L/K eine endliche Körpererweiterung und K habe entweder Charakteristik 0, oder sei ein endlicher Körper. Dann gibt es ein $x \in L$ mit $L = K(x)$.*

Beweis. Hat K Charakteristik 0, so ist L/K automatisch separabel nach Korollar 3.7 und Korollar 5.7 liefert die Behauptung. (Der Fall wenn K endlich ist, ist nur eine Wiederholung von Korollar 4.6.) □

5.3. Fundamentalsatz der Algebra

In diesem Abschnitt beweisen wir den berühmten Fundamentalsatz der Algebra auf — im Wesentlichen — rein algebraische Art und Weise.

Satz 5.9 (Fundamentalsatz der Algebra)**.** *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen. Insbesondere ist $\mathbb{C}/\mathbb{R}$ ein algebraischer Abschluss von $\mathbb{R}$.*

Der gleich folgende Beweis von Satz 5.9 illustriert in beeindruckender Weise die Kernidee des Hauptsatzes der Galois-Theorie: *der stete Wechsel von Zwischenkörpern zu Gruppen und umgekehrt*. Wir benötigen zweierlei Information, deren Herleitung letztlich auf Methoden der *Analysis* beruht:

Lemma 5.10.

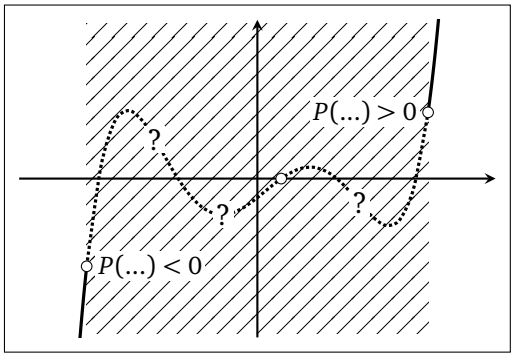
(1) Jedes Polynom über $\mathbb{R}$ mit ungeradem Grad besitzt eine reelle Nullstelle.

(2) Jedes quadratische Polynom über $\mathbb{C}$ besitzt eine komplexe Nullstelle.

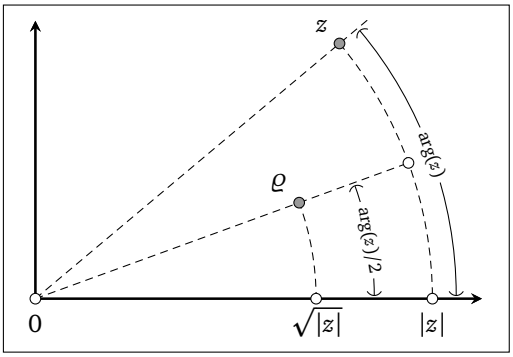
Beweis. (1): Ein reelles Polynom ungeraden Grades nimmt sowohl positive, wie auch negative Werte an. Der aus der Analysis bekannte *Zwischenwertsatz* liefert daher die Existenz einer reellen Nullstelle (vgl. Abbildung 10).

(2) folgt aus der bekannten Lösungsformel für quadratische Gleichungen und der Tatsache, dass man in $\mathbb{C}$ beliebige Quadratwurzeln ziehen kann; Letzteres verifiziert man leicht anhand der wohl-bekannten *Polarkoordinatendarstellung* komplexer Zahlen (vgl. abermals Abbildung 10). Man beachte, dass man die angedeutete Überlegung auch als eine Konsequenz der Tatsache ansehen kann, dass es einen *surjektiven* Gruppenhomomorphismus $(\mathbb{C}, +) \to (\mathbb{C}^\times, \cdot)$ gibt (nämlich die Exponentialfunktion). Dieser reduziert nämlich das Quadratwurzelziehen in $(\mathbb{C}^\times, \cdot)$ auf das Halbieren in $(\mathbb{C}, +)$, was natürlich stets möglich ist. Man vergleiche dies mit der Situation in $\mathbb{R}$: es gibt keinen surjektiven Gruppenhomomorphismus $f\colon (\mathbb{R}, +) \to (\mathbb{R}^\times, \cdot)$. (Denn gäbe es ein solches f mit $f(a) = -1$, so wäre $-1 = f(a/2)^2 \geq 0$, im Widerspruch zur Anordnung von $\mathbb{R}$.) □

Algebraisch interpretiert besagt obiges Lemma, dass Polynome in $\mathbb{R}[X]$ mit ungeradem Grad > 1 stets *reduzibel* sind und auch quadratische Polynome in $\mathbb{C}[X]$ stets reduzibel sind. Mittels des Bezugs von Körpergraden zu Graden von Minimalpolynomen schließt dies die Existenz gewisser Körpererweiterungen von $\mathbb{R}$ bzw. $\mathbb{C}$



(a) Plot einer Polynomfunktion $\mathbb{R} \to \mathbb{R}$, $x \mapsto P(x)$ mit ungeradem Grad. Man hat bei $P(x) \to \pm\infty$ für $x \to \pm\infty$ und also sowohl positive, wie auch negative Funktionswerte. Der Zwischenwertsatz liefert die Existenz einer reellen Nullstelle (hier z.B. der mittlere markierte Punkt), auch ohne den Verlauf des Funktionsgraphen im schraffierten Bereich konkret zu kennen (natürlich vorausgesetzt, man weiß, dass die Funktion dort stetig ist).



(b) Schreibt man eine beliebige komplexe Zahl $z \neq 0$ in der Form

$$z = |z| \exp(\mathrm{i} \arg(z))$$

(*Polarkoordinaten*!), so ist

$$\varrho = \sqrt{|z|} \exp(\mathrm{i} \arg(z)/2)$$

eine Quadratwurzel von z, denn es gilt ja $z = \varrho^2$.
(Die zweite Quadratwurzel von z ist selbstverständlich $-\varrho$.)

Abbildung 10. Zum Beweis von Lemma 5.10.

aus:

$$\begin{array}{ccc} \mathbb{R}(x) & & \mathbb{C}(x) \\ \Big\uparrow \mathrm{Grad} \in (2\mathbb{N}+1) & & \Big\uparrow \mathrm{Grad}\ 2 \\ \mathbb{R} & & \mathbb{C}\,. \end{array}$$

Ferner erinnern wir an das folgende Resultat aus der Gruppentheorie über Existenz von p-Untergruppen (siehe etwa [33, Satz 3.1] für einen Beweis):

Lemma 5.11 (Sylow). *Sei G eine endliche Gruppe und p^ν eine Primzahlpotenz, die $\#G$ teilt. Dann besitzt G eine Untergruppe mit genau p^ν Elementen.*[4]

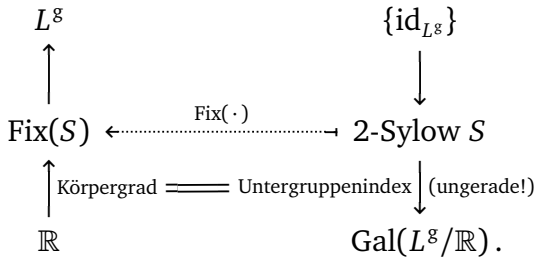
Wir führen nun den Beweis von Satz 5.9. Leserinnen und Leser seien dazu angehalten, speziell auf die Anwendung von Lemma 5.10, welche körpertheoretische Information bereitstellt, und die Anwendung von Lemma 5.11, welche hingegen gruppentheoretische Information bereitstellt, zu achten. Insbesondere das wechselseitige Ausnutzen dieser Informationen stellt ein Paradebeispiel für Galois-Theorie dar.

[4]Falls $p^{\nu+1}$ kein Teiler von $\#G$ ist, so bezeichnet man eine Untergruppe wie aus dem Lemma als eine ***p*-Sylowgruppe von *G***.

Beweis von Satz 5.9 (nach E. Artin). Sei $L/\mathbb{C}$ eine algebraische Erweiterung. Wir zeigen im Folgenden $L = \mathbb{C}$. Hierzu betrachten wir die Galois-Hülle $L^g/\mathbb{R}$ zu $L/\mathbb{R}$ und eine 2-Sylowgruppe S von $\mathrm{Gal}(L^g/\mathbb{R})$ (siehe Proposition 5.6 und Lemma 5.11). Dann ist (siehe Satz 5.3)

$$[\mathrm{Fix}(S) : \mathbb{R}] = \frac{[L^g : \mathbb{R}]}{[L^g : \mathrm{Fix}(S)]} = \frac{\#\mathrm{Gal}(L^g/\mathbb{R})}{\#S} = \frac{\#\mathrm{Gal}(L^g/\mathbb{R})}{\max\{\, 2^\nu : 2^\nu \text{ teilt } \#\mathrm{Gal}(L^g/\mathbb{R})\,\}}$$

eine ungerade Zahl:



Laut Korollar 5.7 ist $\mathrm{Fix}(S) = \mathbb{R}(x)$ für ein $x \in L^g$ und das Minimalpolynom von x hat Grad $[\mathrm{Fix}(S) : \mathbb{R}]$. Dieser ist wegen Lemma 5.10 (1) also gleich 1. Wir haben also $\mathrm{Fix}(S) = \mathbb{R}$ und damit $S = \mathrm{Gal}(L^g/\mathbb{R})$ (siehe wieder Satz 5.3).

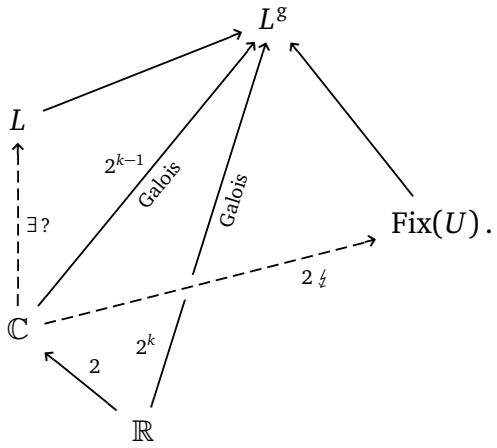
Da nach dem eben Gezeigten $\#\mathrm{Gal}(L^g/\mathbb{R})$ eine Zweierpotenz ist, gilt dies auch für $\#\mathrm{Gal}(L^g/\mathbb{C})$ (wegen $\mathrm{Gal}(L^g/\mathbb{C}) \leq \mathrm{Gal}(L^g/\mathbb{R})$). Ist $\#\mathrm{Gal}(L^g/\mathbb{C}) = 1$, so sind wir fertig. Anderenfalls besitzt die Gruppe $\mathrm{Gal}(L^g/\mathbb{C})$ wegen Lemma 5.11 eine Untergruppe U vom Index 2 und wir haben

$$[\mathrm{Fix}(U) : \mathbb{C}] = \frac{[L^g : \mathbb{C}]}{[L^g : \mathrm{Fix}(U)]} = 2.$$

Also ist $\mathrm{Fix}(U)/\mathbb{C}$ eine quadratische Erweiterung von $\mathbb{C}$. — So etwas gibt es laut Lemma 5.10 (2) nicht! □

Man veranschaulicht sich die im zweiten Teil vom Beweis von Satz 5.9 angestellten Überlegungen vielleicht anhand von folgendem mit Körpergraden annotierten Diagramm (je weiter rechts hier ein Körper auftritt, desto später kam dieser im Beweis

vor):



5.4. Galois-Gruppen als Permutationsgruppen

5.4.1. Operation auf Nullstellen. Sei K ein Körper und $P \in K[X]$ ein beliebiges nichtverschwindendes Polynom. Für eine Körpererweiterung $\iota\colon K \to L$ erinnern wir an die Notation $\iota^* P$ aus § 2.2, wollen hier aber nur Körpererweiterungen der Form L/K betrachten. In diesem Spezialfall schreiben wir der Einfachheit halber nur P statt $(\mathrm{id}_L|_K)^* P$.

Sei L/K nun ein Zerfällungskörper von P. Wir setzen $\mathrm{Aut}(P) \coloneqq \mathrm{Aut}_K(L)$. Die Erweiterung L/K ist normal; Falls diese auch separabel ist, schreiben wir $\mathrm{Gal}(P)$ für $\mathrm{Aut}(P)$ und nennen dies die ***Galois-Gruppe von P***. Die Notation $\mathrm{Aut}(P)$ nimmt offenbar keinen Bezug mehr auf den gewählten Zerfällungskörper L. Wir werden im Folgenden jedoch oft stillschweigend voraussetzen, dass dieser konstruiert wurde und L heißt, sobald wir von $\mathrm{Aut}(P)$ sprechen.

Bemerkung 5.12. Gemäß des Satzes vom primitiven Element in der Form von Korollar 5.7 ist die Galois-Gruppe $\mathrm{Gal}(L'/K)$ einer jeden Körpererweiterung L'/K (bis auf Isomorphie) stets von der Form $\mathrm{Gal}(P)$ mit einem geeigneten irreduziblen, separablen Polynom P.

Man kann die Gruppe $\mathrm{Aut}(P)$ wie folgt „sehen“ (vgl. Abbildung 12): Sei

$$V(P) = \{\, x \in L : P(x) = 0_L \,\}$$

die Menge der Nullstellen von P in L („Verschwindungsmenge“ von P in L) und $f \in \mathrm{Aut}(P)$ beliebig. Wegen $f|_K = \mathrm{id}_L|_K$ folgt für $x \in L$

$$P(f(x)) = f(P(x))$$

und daher

$$P(f(x)) = 0_L \iff P(x) = 0_L.$$

Da f injektiv und $V(P)$ endlich ist, erhält man so eine Abbildung

$$\mathrm{Aut}(P) \longrightarrow \mathrm{Sym}(V(P)), \quad f \longmapsto (x \mapsto f(x)),$$

welche man leicht als einen Gruppenhomomorphismus erkennt. In der Sprache der Gruppentheorie ***operiert*** $\mathrm{Aut}(P)$ auf $V(P)$. (Die aufmerksame Leserin oder der aufmerksame Leser kennt diese Überlegung bereits aus dem Beweis von Lemma 3.1 in etwas allgemeinerer Notation.)

Satz 5.13. *Sei P ein nichtverschwindendes Polynom über einem Körper K, L/K ein Zerfällungskörper von P und $\mathrm{Aut}(P) = \mathrm{Aut}_K(L)$. Dann gilt:*

*(1) Die soeben eingeführte Operation von $\mathrm{Aut}(P)$ auf der Nullstellenmenge $V(P)$ von P in L ist **treu**, d.h. der der Operation zugrundeliegende Gruppenhomomorphismus $\mathrm{Aut}(P) \to \mathrm{Sym}(V(P))$ ist injektiv und identifiziert $\mathrm{Aut}(P)$ mit einer Untergruppe von $\mathrm{Sym}(V(P))$.*

*(2) Ist P überdies irreduzibel, so operiert $\mathrm{Aut}(P)$ **transitiv** auf $V(P)$, d.h. für je zwei Elemente $x, x' \in V(P)$ gibt es ein $j' \in \mathrm{Aut}(P)$ mit $j'(x) = x'$.*

Beweis. Da L/K ein Zerfällungskörper von P ist, haben wir $L = K(V(P))$; Der einzige K-Homomorphismus $f \in \mathrm{Aut}(P) = \mathrm{Aut}_K(L)$, der $V(P)$ elementweise fixiert, ist daher die Identität $f = \mathrm{id}_L$. Also ist der Kern von $\mathrm{Aut}(P) \to \mathrm{Sym}(V(P))$ trivial und die fragliche Operation somit treu.

Ist P nun irreduzibel und sind $x, x' \in V(P)$ zwei Nullstellen von P in L, so kann man $\mathrm{id}_L|_K \colon K \to L$ vermöge Lemma 2.9 zu einem K-Homomorphismus $j' \colon K(x) \to L$ mit $j'(x) = x'$ fortsetzen, und dieser lässt sich weiter (auf i.Allg. mehrere Arten) zu einem K-Homomorphismus $L \to L$ fortsetzen, der als injektive Abbildung zwischen endlich-dimensionalen Vektorräumen sogar ein K-Isomorphismus ist, also ein Element von $\mathrm{Aut}(P)$, welches x auf x' abbildet. □

Bemerkung. Oft ist man bei der konkreten Berechnung einer Galois-Gruppe $\mathrm{Gal}(L/K)$ nicht unbedingt primär daran interessiert die Elemente von $\mathrm{Gal}(L/K)$ als K-Automorphismen von L zu kennen, sondern begnügt sich damit, $\mathrm{Gal}(L/K)$ bis auf Isomorphie zu bestimmen. Das genügt im Sinne von Satz 5.3 dann auch schon, um qualitativ zu sehen, wie sich die Zwischenkörper der Erweiterung L/K untereinander verhalten, auch wenn man diese damit vielleicht noch nicht unbedingt explizit berechnet hat.

Bemerkung 5.14. Mit Blick auf Bemerkung 5.12 und Satz 5.13 (2) geben wir hier eine Liste der Isomorphietypen sämtlicher transitiver Untergruppen der symmetrischen Gruppen $\mathfrak{S}_n = \mathrm{Sym}(\{1, \dots, n\})$ für $n = 3, 4, 5$:

$\mathfrak{S}_n$	…und Isomorphietypen transitiver, echter Untergruppen von $\mathfrak{S}_n$			
$\mathfrak{S}_3$	A_3			
$\mathfrak{S}_4$	A_4	$D_{2\cdot 4}$	$C_2 \times C_2 \cong V$	C_4
$\mathfrak{S}_5$	A_5	$D_{2\cdot 5}$	$C_5 \rtimes C_4 \cong \left(\begin{smallmatrix} \mathbb{F}_5^\times & \mathbb{F}_5 \\ 0 & 1 \end{smallmatrix}\right)$	C_5

Die hierin benutzten Abkürzungen haben die folgenden Bedeutungen:

- $A_n = \{\, \sigma \in \mathfrak{S}_n : \mathrm{sgn}\,\sigma = 1 \,\}$: die alternierende Gruppe,
- C_n: zyklische Gruppe mit genau n Elementen,

- $V \cong C_2 \times C_2$: Kleinsche Vierergruppe,
- D_{2n}: Diedergruppe mit genau $2n$ Elementen.

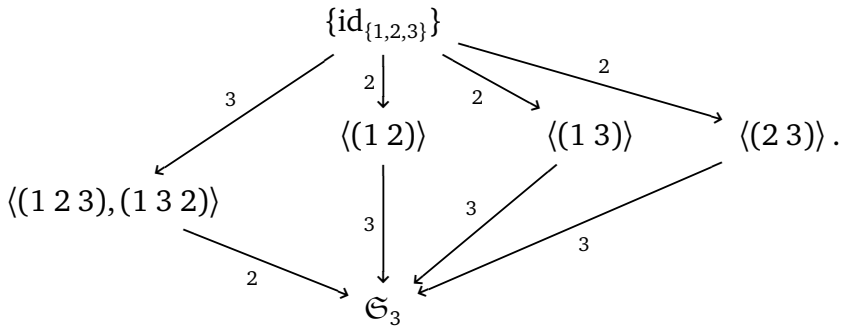
(Für einen Beweis siehe [13, § 2.9].) Im Hinblick auf Satz 5.13 kann obige Liste benutzt werden, um Galois-Gruppen mittels eines Ausschlussverfahrens zu berechnen.

Bemerkung (Semidirekte Produkte)**.** Die in Bemerkung 5.14 benutzte Notation $C_5 \rtimes C_4$ ist ein sogenanntes ***semidirektes Produkt***. Seien $(N, \star)$ und $(H, *)$ zwei Gruppen und $\psi\colon H \to \mathrm{Aut}(N)$ ein Gruppenhomomorphismus ($\mathrm{Aut}(N)$ bezeichnet hier die Gruppe der Gruppenautomorphismen von N mit Komposition von Abbildungen als Verknüpfung). Dann ist $N \rtimes_\psi H$ definiert als das (mengentheoretische) kartesische Produkt $N \times H$, zusammen mit der Verknüpfung

$$(n,h) \cdot (n',h') := (n \star \psi(h)(n'), h * h').$$

Für unseren konkreten Fall „$C_5 \rtimes C_4$“ braucht man also einen Gruppenhomomorphismus $C_4 \to \mathrm{Aut}(C_5) \cong C_4$. Es gibt genau zwei Gruppenautomorphismen von C_4, nämlich die Identität, und der Gruppenendomorphismus der die beiden Erzeuger von C_4 vertauscht. Man erhält also zwei Gruppenhomomorphismen $C_4 \to \mathrm{Aut}(C_5)$: den trivialen (triv: $x \mapsto \mathrm{id}_{C_5}$) und einen nicht-trivialen, den wir ψ nennen wollen. Mit $C_5 \rtimes C_4$ sei hier dann $C_5 \rtimes_\psi C_4$ gemeint. (Man beachte: $C_5 \rtimes_{\mathrm{triv}} C_4 = C_5 \times C_4$; Wäre also $C_5 \rtimes_{\mathrm{triv}} C_4$ gemeint gewesen, so hätten wir von Anfang an einfach $C_5 \times C_4$ geschrieben.) Hätte man als ψ den Gruppenhomomorphismus $C_4 \to \mathrm{Aut}(C_5)$ gewählt, der bezüglich der obigen Überlegung zu dem Gruppenendomorphismus $C_4 \to C_4$ gehört, welcher beide Erzeuger auf das (eindeutig bestimmte) Element mit Ordnung 2 abbildet, so ist das zugehörige semidirekte Produkt eine sogenannte ***dizyklische Gruppe***.

Bemerkung (Untergruppenverband von $\mathfrak{S}_3$)**.** Der Untergruppenverband von $\mathfrak{S}_3 \cong D_{2\cdot 3}$ sieht wie folgt aus:



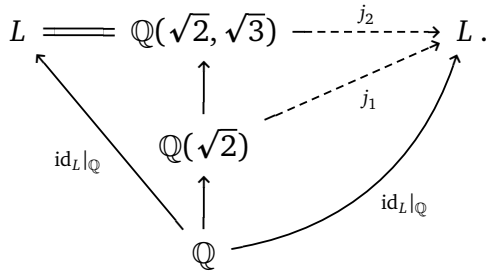
(Für einen Beweis, siehe die Lösung zu Aufgabe 8.3.) Man bestätigt hier leicht die in Bemerkung 5.14 aufgeworfene Behauptung über transitive Untergruppen von $\mathfrak{S}_3$.

5.4.2. Beispiele für Galois-Gruppen. Wir widmen uns nun der Aufgabe, einige Galois-Gruppen (mehr oder minder) explizit zu bestimmen. Wir betrachten hierzu drei Beispiele.

Beispiel 5.15 (Ein Polynom mit Galois-Gruppe $\cong V$)**.** Aus Beispiel 2.2 wissen wir $L = \mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(x)$ mit $x = \sqrt{2}+\sqrt{3}$, wobei sich das Minimalpolynom $P = X^4 - 10X^2 + 1$ von x über $\mathbb{Q}(x)$ wie folgt zerlegt:

$$X^4 - 10X^2 + 1 = \prod_{x_0 \in V(P)} (X - x_0),$$

mit $V(P) = \{\, \epsilon_1\sqrt{2} - \epsilon_2\sqrt{3} : \epsilon_1, \epsilon_2 \in \{\pm 1\}\,\}$; es handelt sich bei L also um den Zerfällungskörper von P. Wir haben $[L:\mathbb{Q}] = 4$ und laut Proposition 5.1 dann $\#\mathrm{Gal}(L/\mathbb{Q}) = 4$. Wir können auch leicht vier (und somit alle) Elemente von $G = \mathrm{Gal}(L/\mathbb{Q})$ konstruieren: Mittels Lemma 2.13 lassen sich Abbildungen j_1 und j_2 konstruieren, die das folgende Diagramm kommutativ machen, wobei die nicht-gestrichenen Pfeile jeweils die Inklusionen sind:



Dabei lassen sich zwei verschiedene j_1 konstruieren: Nämlich j_1 mit $j_1(\sqrt{2}) = \sqrt{2}$ (das führt auf $j_1 = \mathrm{id}_L|_{\mathbb{Q}(\sqrt{2})}$) und j_1 mit $j_1(\sqrt{2}) = -\sqrt{2}$. Die so erhaltenen Abbildungen j_1 kann man dann je durch $j_2(\sqrt{3}) = \pm\sqrt{3}$ fortsetzen. Dies liefert die behaupteten vier $\mathbb{Q}$-Automorphismen von L. Wir haben also

$$G = \{\, j_{\epsilon_2,\epsilon_3} : \epsilon_2, \epsilon_3 \in \{+,-\}\,\}$$

mit den $\mathbb{Q}$-Automorphismen $j_{\epsilon_2,\epsilon_3} \colon L \to L$ gegeben durch

$$j_{\epsilon_2,\epsilon_3}(\sqrt{2}) = \epsilon_2\sqrt{2}, \quad j_{\epsilon_2,\epsilon_3}(\sqrt{3}) = \epsilon_3\sqrt{3}$$

(diese zwei Bedingungen legen $j_{\epsilon_2,\epsilon_3}$ schon eindeutig fest).
Nummerieren wir die Elemente von $V(P)$ wie folgt, so erhalten wir einen expliziten Isomorphismus $\mathrm{Sym}(V(P)) \cong \mathfrak{S}_4$:

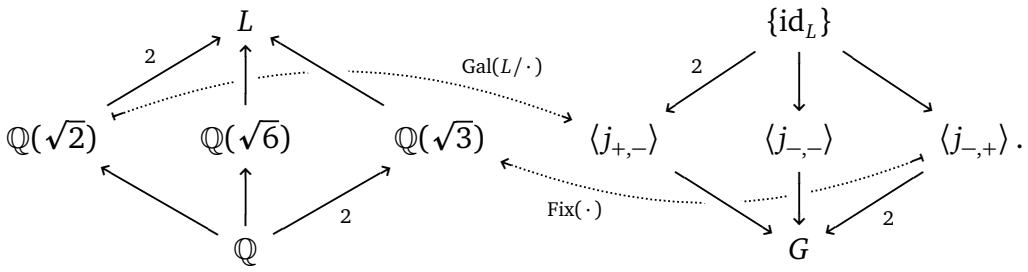
$$1\colon +\sqrt{2}+\sqrt{3}, \quad 2\colon -\sqrt{2}+\sqrt{3}, \quad 3\colon +\sqrt{2}-\sqrt{3}, \quad 4\colon -\sqrt{2}-\sqrt{3}.$$

Die oben beschriebene (treue!) Operation von G auf $V(P)$ lässt sich vermöge der eben gewählten Nummerierung durch eine Untergruppe von $\mathfrak{S}_4$ beschreiben. Elementweise haben wir die folgenden Entsprechungen zu Zyklen:

$$j_{+,+} \mapsto \mathrm{id}_{\{1,2,3,4\}}, \quad j_{-,+} \mapsto (1\,2)(3\,4), \quad j_{+,-} \mapsto (1\,3)(2\,4), \quad j_{-,-} \mapsto (1\,4)(2\,3).$$

(Siehe auch Abbildung 11.) Man sieht auch leicht, dass G isomorph zur kleinschen Vierergruppe ist: $G \cong V \cong C_2 \times C_2$. Die Galois-Korrespondenz aus Satz 5.3 nimmt

hier die folgende Gestalt an:



Achtung: Wir haben

$$G = \mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(P) = \mathrm{Gal}(\tilde{P}) \quad \text{mit} \quad \tilde{P} = (X^2-2)(X^2-3) \in \mathbb{Q}[X]$$

und G operiert treu und transitiv auf $V(P)$. Allerdings operiert G treu, jedoch nicht transitiv auf

$$V(\tilde{P}) = \{\pm\sqrt{2}, \pm\sqrt{3}\}\,!$$

Wir bemerken noch kurz, wie die jeweiligen Fixkörper berechnet werden können: Jedes Element x von L schreibt sich auf eindeutige Art und Weise in der Form

$$x = \lambda_1 1_L + \lambda_2\sqrt{2} + \lambda_3\sqrt{3} + \lambda_4\sqrt{6},$$

mit geeigneten Skalaren $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in \mathbb{Q}$. Nun gilt $x \in \mathrm{Fix}(\langle j_{-,-}\rangle)$ genau dann wenn x von $j_{-,-}$ fixiert wird. Anwenden von $j_{-,-}$ liefert

$$\begin{aligned} x \in \mathrm{Fix}(\langle j_{-,-}\rangle) &\iff x = \lambda_1 1_L - \lambda_2\sqrt{2} - \lambda_3\sqrt{3} + \lambda_4\sqrt{6} \\ &\iff 2\lambda_2\sqrt{2} + 2\lambda_3\sqrt{3} = 0_L \\ &\iff \lambda_2 = \lambda_3 = 0_{\mathbb{Q}} \\ &\iff x \in \mathrm{span}_{\mathbb{Q}}\{1_L, \sqrt{6}\} = \mathbb{Q}(\sqrt{6}). \end{aligned}$$

Also ist $\mathrm{Fix}(\langle j_{-,-}\rangle) = \mathbb{Q}(\sqrt{6})$, wie schon oben im Diagramm angezeichnet.

Bemerkung. Man sieht auch leicht, dass sich die im obigen Beispiel zur Fixkörper-Berechnung benutzte Methode ohne Probleme auf Untergruppen von Galois-Gruppen anwenden lässt, die von mehreren Elementen erzeugt werden: Man setzt allgemein ein Element als Linearkombination einer Basis der fraglichen Körpererweiterung an, und wendet die Erzeuger darauf an. (Dabei macht man sich zu nutze, dass man das Abbildungsverhalten der benutzen Erzeuger auf den gewählten Basiselementen bereits kennt.) Gleichsetzen mit eben diesem Element liefert dann ein lineares Gleichungssystem, das es zu lösen gilt. Die Lösungen sind dann genau die Elemente des gesuchten Fixkörpers.

Wir betrachten nun ein etwas interessanteres Beispiel, schreiten dabei jedoch etwas zügiger voran.

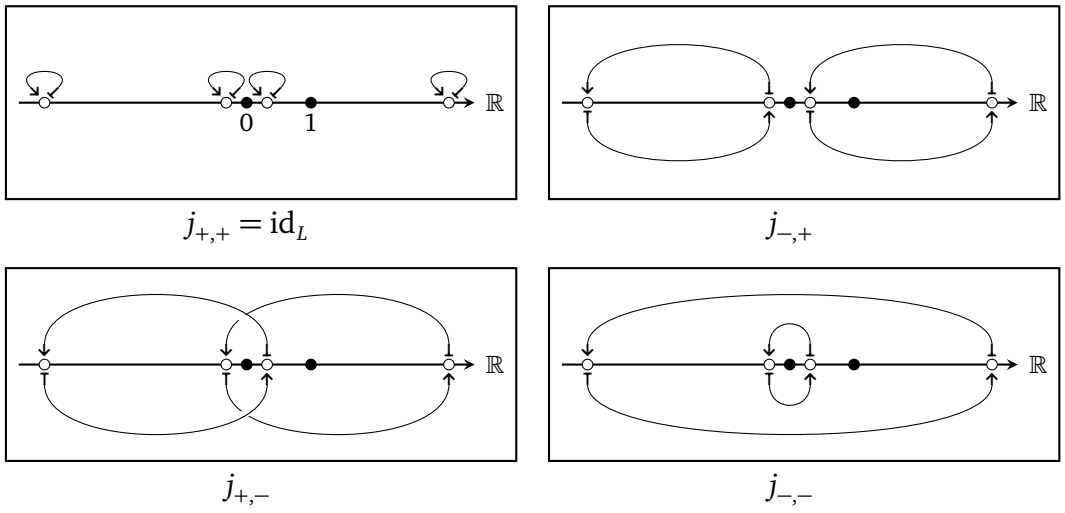
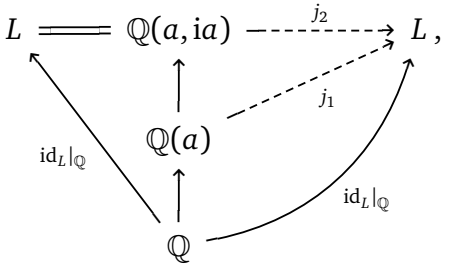


Abbildung 11. Veranschaulichung der Operation der Galois-Gruppe $\mathrm{Gal}(P) = \{ j_{\epsilon_2,\epsilon_3} : \epsilon_2, \epsilon_3 \in \{+,-\} \} \cong V$ auf den Nullstellen von $P = X^4 - 10X^2 + 1$ (weiße Punkte). (Siehe Beispiel 5.15.)

Beispiel 5.16 (Ein Polynom mit Galois-Gruppe $\cong D_{2\cdot 4}$)**.** Wir betrachten das Polynom $P = X^4 - 2$ über $\mathbb{Q}$. Dieses ist laut dem Eisenstein-Kriterium irreduzibel. Sei $a = \sqrt[4]{2}$. In $\mathbb{C}$ hat P die Nullstellenmenge $V(P) = \{ \mathrm{i}^\nu a : 1 \leq \nu \leq 4 \}$. Ein Zerfällungskörper $L = \mathbb{Q}(V(P)) = \mathbb{Q}(a, \mathrm{i})$ von P hat über $\mathbb{Q}$ Grad 8 und dies ist nach Proposition 5.1 dann auch die Ordnung der Galois-Gruppe $G = \mathrm{Gal}(L/\mathbb{Q})$. (Achtung: Man beachte, dass P Grad 4 hat, aber die Galois-Gruppe $G = \mathrm{Gal}(P)$ eine echt größere Ordnung besitzt.) Mit Bemerkung 5.14 sieht man, dass G isomorph zur Diedergruppe $D_{2\cdot 4}$ ist. (Siehe auch Abbildung 12.)
Wir wollen nun abermals die Elemente der Galois-Gruppe G explizit konstruieren. Wir verfahren analog zu Beispiel 2.11. Hierzu betrachten wir das kommutative Diagramm



wobei wir j_1 durch Fortsetzung von $\mathrm{id}_L|_{\mathbb{Q}}$, und j_2 durch Fortsetzung von j_1 erhalten (jeweils mittels Lemma 2.9). Dabei gibt es für j_1 genau vier Möglichkeiten, denn man kann sich für den Wert $j_1(a)$ ein beliebiges Element in $V(P)$ aussuchen, sagen wir $j_1(a) = \mathrm{i}^\nu a$, und das legt den $\mathbb{Q}$-Homomorphismus j_1 schon eindeutig fest. Nun hat

$ia \in \mathbb{Q}(a, \mathrm{i}a)$ über $\mathbb{Q}(a)$ das Minimalpolynom $X^2 + a^2$. Bei der Konstruktion von j_2 kann man sich den Wert $j_2(\mathrm{i}a)$ beliebig als eine der beiden Nullstellen von

$$j_1^*(X^2 + a^2) = X^2 + (\mathrm{i}^\nu a)^2 = (X - \mathrm{i}^{\nu+1}a)(X + \mathrm{i}^{\nu+1}a)$$

aussuchen. Damit erhalten wir die $\mathbb{Q}$-Automorphismen[5] von L

$$\sigma\colon \begin{cases} a \mapsto \mathrm{i}a \\ \mathrm{i}a \mapsto \mathrm{i}^2 a = -a \end{cases} \quad \text{und} \quad \tau\colon \begin{cases} a \mapsto \mathrm{i}^3 a \\ \mathrm{i}a \mapsto -\mathrm{i}^{3+1}a = -a \end{cases}$$

aus Abbildung 12, sowie deren Verknüpfungen; Insgesamt erhalten wir $4 \cdot 2 = 8$ Elemente, was auch zu $\#G = [L : \mathbb{Q}] = 8$ passt.
Nummeriert man die Elemente in $V(P)$ in der Form $\nu\colon \mathrm{i}^\nu a$, so erhält man wieder einen expliziten Gruppenisomorphismus $\mathrm{Sym}(V(P)) \cong \mathfrak{S}_4$ und also einen Gruppenmonomorphismus $\Psi\colon G \hookrightarrow \mathfrak{S}_4$. Nach einigen weiteren saloppen Identifikationen (man überlege sich die Details!) nimmt die Galois-Korrespondenz aus Satz 5.3 die in Abbildung 13 gezeigte Form an. (Die Bezeichner V und $D_{2\cdot 4}$ sollen hier stets nur den Isomorphietyp der jeweiligen Untergruppe von $\mathfrak{S}_4$ angeben. Welche Zyklen aus $\mathfrak{S}_4$ konkret enthalten sind, entnimmt man den darüberliegenden Zeilen.)

Beispiel 5.17 (Ein Polynom mit Galois-Gruppe $\cong \mathfrak{S}_5$)**.** Man betrachte das Polynom $P = X^5 - 4X + 2$ über $\mathbb{Q}$. Dieses ist nach Eisenstein irreduzibel. Anhand von $P(-2) < 0 < P(0) < P(-1)$ und $P(1) < 0 < P(2)$, sowie der Tatsache, dass $P' = 5X^4 - 4$ genau zwei reelle Nullstellen hat, schließt man leicht, dass P genau drei reelle und zwei komplexe, nichtreelle Nullstellen hat (siehe Abbildung 15). Sei $L \subseteq \mathbb{C}$ der von diesen Nullstellen erzeugte Zerfällungskörper. Da die Galois-Gruppe $G = \mathrm{Gal}(L/\mathbb{Q})$ laut Satz 5.13 transitiv auf der fünfelementigen Menge $V(P)$ operiert, liefert die Bahnengleichung (siehe [33, Satz 2.16] oder [16, Satz 1.12.10]), dass $\#G$ durch 5 teilbar ist („Bahnlänge = Stabilisatorindex“). Laut Lemma 5.11 hat G daher ein Element der Ordnung 5. Die Untergruppe von $\mathfrak{S}_5$, der G gemäß Satz 5.13 bei entsprechender Nummerierung der Elemente von $V(P)$ entspricht, enthält also einen 5-Zyklus σ. (Das sieht man, indem man das fragliche Element der Ordnung 5 in disjunkte Zyklen zerlegt. Dann ist 5 nämlich das kleinste gemeinsame Vielfache der darin auftretenden Zyklenlängen. Da 5 prim ist, müssen alle diese Zyklen Länge 5 haben, und da wir uns in $\mathfrak{S}_5$ befinden, kann es auch nicht zwei disjunkte solche Zyklen geben.)
Die komplexe Konjugation eingeschränkt auf L liefert ein Element von G. Dessen Operation auf der Nullstellenmenge von P bewirkt genau das Vertauschen der beiden komplexen Nullstellen und entspricht also einer Transposition $(a\ b)$ in $\mathfrak{S}_5$.[6] Ersetzt

[5] Diese sind *a-priori* natürlich erst mal nur $\mathbb{Q}$-Endomorphismen, aber als Körperhomomorphismen ja injektiv und also als injektive $\mathbb{Q}$-lineare Endomorphismen des endlich-dimensionalen $\mathbb{Q}$-Vektorraums L sogar auch surjektiv, also insgesamt bijektiv.

[6] Zusammen mit der Liste transitiver Untergruppen von $\mathfrak{S}_5$ aus Bemerkung 5.14 würde allein die Existenz einer solchen Permutation bereits genügen, um $G \cong \mathfrak{S}_5$ zu folgern, aber wir sind hier bemüht, uns nicht zu sehr auf die (hier unbewiesenen) Aussagen von Bemerkung 5.14 zu stützen.

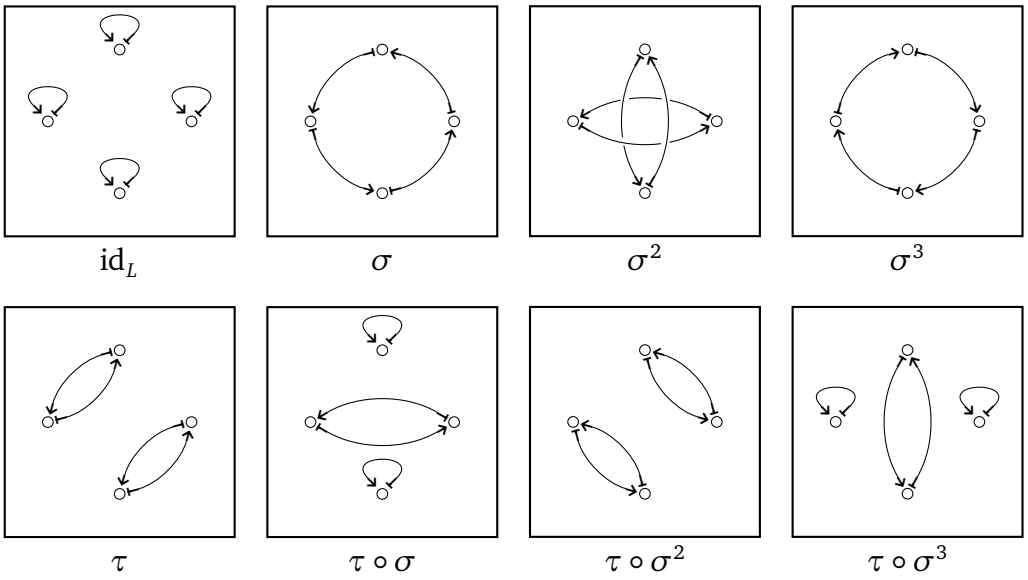


Abbildung 12. Veranschaulichung der Operation der Galois-Gruppe $\mathrm{Gal}(P) = \langle\sigma,\tau\rangle \cong D_8$ (mit $\sigma^4 = \tau^2 = (\tau\circ\sigma)^2 = \mathrm{id}_L$) von $P = X^4 - 2 \in \mathbb{Q}[X]$ auf den komplexen Nullstellen $\mathrm{i}^k\sqrt[4]{2}$ (mit $k = 1,2,3,4$), wobei wir uns hier den Zerfällungskörper $L/\mathbb{Q}$ von P als in die komplexen Zahlen eingebettet vorstellen. (Für detailliertere Rechnungen hierzu, siehe Beispiel 5.16.) Der $\mathbb{Q}$-Automorphismus $\sigma\colon L \to L$ operiert durch Multiplikation mit i, und der $\mathbb{Q}$-Automorphismus $\tau\colon L \to L$ operiert durch $\tau(\pm\sqrt[4]{2}) = \mp\mathrm{i}\sqrt[4]{2}$. Man beachte, dass $\mathrm{Gal}(P)$ in diesem Beispiel transitiv auf der Nullstellenmenge von P operiert (siehe insbesondere Satz 5.13 (2)), aber *nicht* jede Permutation dieser Nullstellen durch ein Element von $\mathrm{Gal}(P)$ bewirkt werden kann: z.B. gibt es kein $f \in \mathrm{Gal}(P)$ mit $f(\sqrt[4]{2}) = -\sqrt[4]{2}$ und $f(\mathrm{i}\sqrt[4]{2}) = \sqrt[4]{2}$, wie man anhand der obigen Bilder sieht. (Alternativ kann man auch bemerken, dass ein solches f auch $f(1) = -f(\mathrm{i})^2 = -(f(\mathrm{i}\sqrt[4]{2})/f(\sqrt[4]{2}))^2 = -(-1)^2 = -1$ erfüllen müsste, was absurd ist.)

man σ durch eine geeignete Potenz von σ, so darf man $\sigma = (a\ b\ \ldots)$ annehmen. ($\langle\sigma\rangle$ ist zyklisch mit Primzahlordnung 5; alle Elemente in $\langle\sigma\rangle \setminus \{\mathrm{id}_{\{1,2,3,4,5\}}\}$ haben darum Ordnung 5 und können in ihrer Zyklendarstellung darum nur aus einen 5-Zyklus bestehen.)
Durch geeignete Nummerierung der Nullstellenmenge von P dürfen wir also $\tau = (1\ 2)$ und $\sigma = (1\ 2\ 3\ 4\ 5)$ annehmen. Wegen $\langle(1\ 2),(1\ 2\ 3\ 4\ 5)\rangle = \mathfrak{S}_5$ ist also $G \cong \mathfrak{S}_5$ [33, Aufgabe 7.2]. Wir verzichten hier auf den Versuch die Untergruppen der $\mathfrak{S}_5$ (oder gar die Zwischenkörper von $L/\mathbb{Q}$) aufzulisten. — Davon gibt es 156 Stück! Siehe auch Abbildung 14.

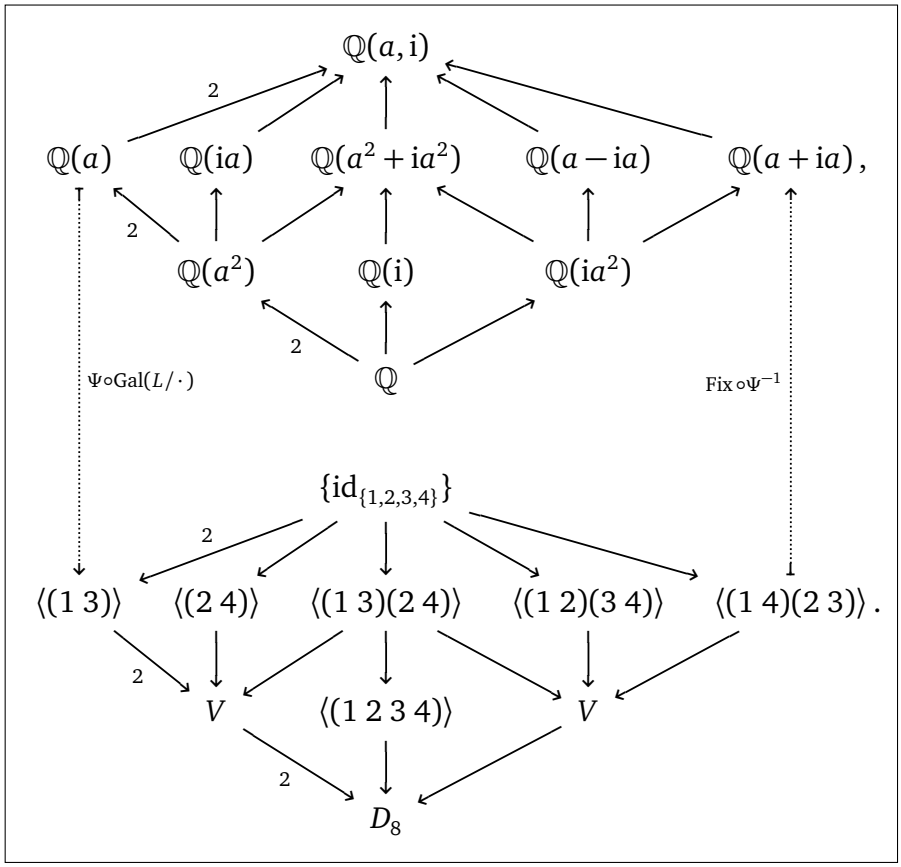


Abbildung 13. Die Galois-Korrespondenz zum Zerfällungskörper des Polynoms X^4-2 über $\mathbb{Q}$. (Siehe Beispiel 5.16.) Auf der Gruppenebene sind wir hier etwas unpräzise und schreiben zwei mal V, sowie D_8; Welche Zykel jeweils enthalten seien sollen, ist aber anhand der zweiten Zeile auf der Gruppenebene leicht rekonstruierbar.

5.4.3. Probabilistische Galois-Theorie. Die in Übungsaufgaben und Beispielen zur Galois-Theorie vorkommenden Galois-Gruppen von Polynomen P tendieren oft dazu isomorph zu einer echten Untergruppe der symmetrischen Gruppe $\mathfrak{S}_{\deg P}$ zu sein. Tatsächlich entspricht dies nicht dem „typischen“ Stand der Dinge; van der Waerden [35] zeigte Folgendes: Sei $\mathscr{P}_n(H)$ die Menger aller Polynome über $\mathbb{Z}$ vom Grad $n \geq 1$, deren Koeffizienten alle betragsmäßig durch H beschränkt sind. Dann gilt

$$\lim_{H\to\infty} \frac{\#\{\, P \in \mathscr{P}_n(H) : \mathrm{Aut}(P) \cong \mathfrak{S}_n \,\}}{\#\mathscr{P}_n(H)} = 1.$$

In diesem Sinne haben also „fast alle“ Polynome (über $\mathbb{Z}$) n-ten Grades eine zu $\mathfrak{S}_n$ isomorphe Automorphismen-Gruppe! Die ursprüngliche Vermutung von van der Waerden wurde kürzlich vom Fields-Medallisten Manjul Bhargava [6] bewiesen.

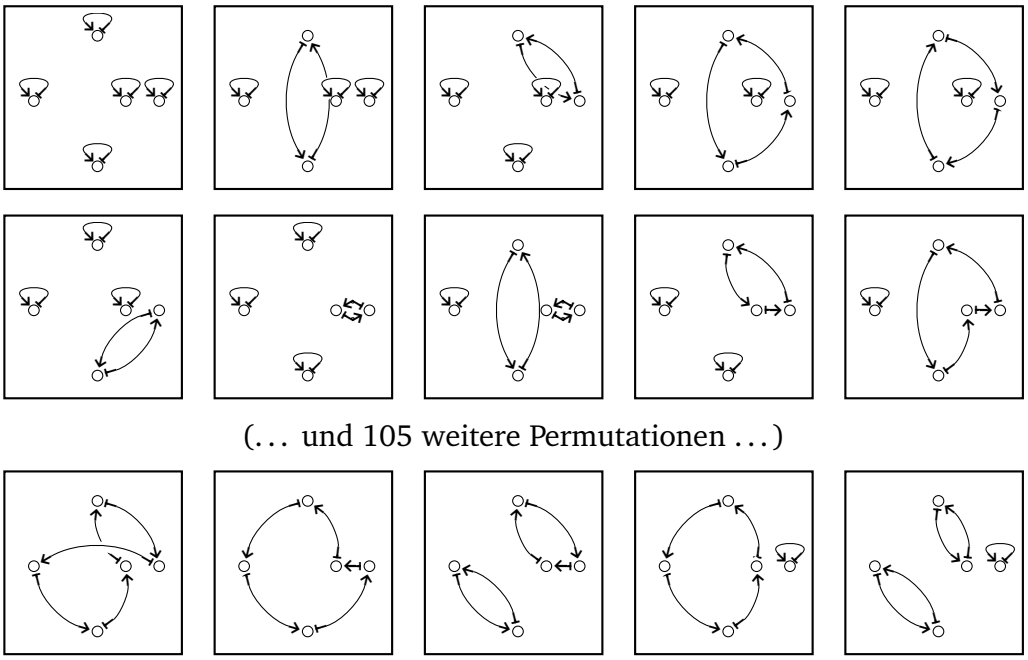


Abbildung 14. Veranschaulichung der Operation der Galois-Gruppe $\mathrm{Gal}(P) \cong \mathfrak{S}_5$ auf den Nullstellen von $P = X^5 - 4X + 2$ (weiße Punkte). (Siehe Beispiel 5.17.) Diese Galois-Gruppe enthält insgesamt $5! = 120$ Elemente; Hier ist lediglich das Abbildungsverhalten von 15 solcher Elemente gezeichnet.

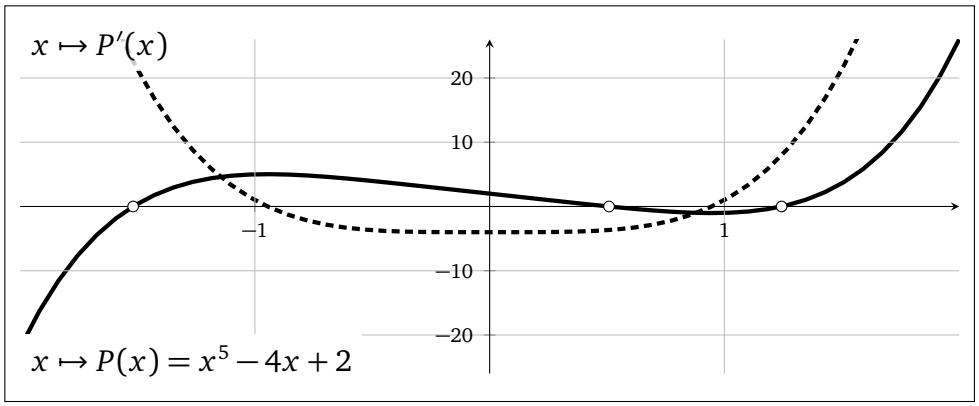


Abbildung 15. Plot der Polynomfunktion $\mathbb{R} \to \mathbb{R}$, $x \mapsto x^5 - 4x + 2$, sowie ihrer Ableitung. Man sieht, dass die fragliche Funktion genau drei reelle Nullstellen besitzt. Diese liegen ungefähr bei $-1{,}52$, $0{,}51$ und $1{,}24$. Siehe Beispiel 5.17.

5.5. Einheitswurzeln und Kreisteilungskörper

5.5.1. Kreisteilungspolynome und Struktur ihrer Galois-Gruppe. Sei K ein Körper. Elemente $\zeta \in K^\times$ von endlicher (multiplikativer) ***Ordnung*** $\operatorname{ord}(\zeta) < \infty$ heißen ***Einheitswurzeln***. Wir nennen ζ eine ***n-te Einheitswurzel***, falls $\operatorname{ord}(\zeta)$ ein Teiler von n ist. (Äquivalent: $\zeta^n = 1_K$.)

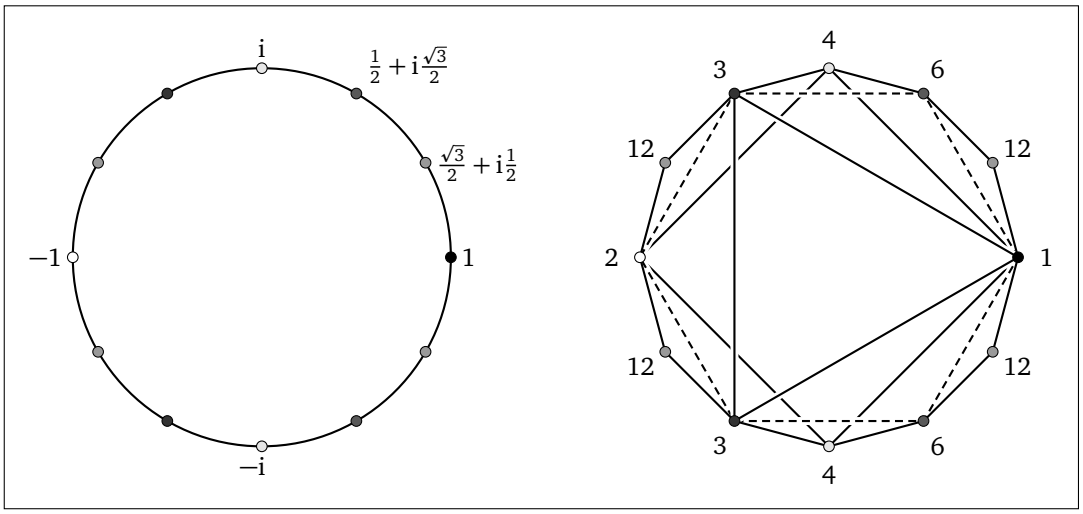


Abbildung 16. Alle 12-ten Einheitswurzeln in der komplexen Zahlenebene (linke Seite), annotiert mit ihren multiplikativen Ordnungen (rechte Seite).

Alle n-ten Einheitswurzeln von K sind Nullstellen von $X^n - 1 \in K[X]$ und umgekehrt ist jede Nullstelle von $X^n - 1$ eine d-te Einheitswurzel für einen Teiler d von n. Ist die Charakteristik von K kein Teiler von n, so ist $X^n - 1$ separabel und zerfällt also in einem algebraischen Abschluss $\iota_{\mathrm{a}}\colon K \to K^{\mathrm{a}}$ von K in n paarweise verschiedene Linearfaktoren. Wir schreiben dann

$$K^{\mathrm{a}}[X] \ni X^n - 1 = \prod_{\substack{\zeta \in (K^{\mathrm{a}})^\times \\ \zeta^n = 1}} (X - \zeta) = \prod_{d \text{ teilt } n} \Phi_d$$

mit dem ***d-ten Kreisteilungspolynom***

$$\Phi_d = \prod_{\substack{\zeta \in (K^{\mathrm{a}})^\times \\ \operatorname{ord}(\zeta) = d}} (X - \zeta) \in K^{\mathrm{a}}[X].$$

(In mancher Literatur heißen diese Polynome auch ***Zyklotomische Polynome***) Aus der obigen Formel ergibt sich unmittelbar das folgende Resultat:

Lemma 5.18. $\Phi_n = (X^n - 1) \Big/ \prod_{\substack{d \text{ teilt } n \\ d \neq n}} \Phi_d$, *falls die Charakteristik von K nicht n teilt.*

Mit Lemma 5.18 kann man die Kreisteilungspolynome induktiv berechnen; Zum Beispiel

$$\Phi_1 = X-1, \quad \Phi_2 = \frac{X^2-1}{\Phi_1} = X+1, \quad \Phi_4 = \frac{X^4-1}{\Phi_1\Phi_2} = \frac{X^4-1}{X^2-1} = X^2+1, \quad \ldots;$$

Anhand der Formel sieht man überdies induktiv, dass alle Kreisteilungspolynome Φ_n normiert sind und ganzzahlige[7] Koeffizienten besitzen (Division mit Rest in $\mathbb{Z}[X]$). In diesem Zusammenhang betrachte man auch Tabelle 1 und Abbildung 17.

n	$\deg \Phi_n = \varphi(n)$	Φ_n
1	1	$X-1$
2	1	$X+1$
3	2	X^2+X+1
4	2	X^2+1
5	4	$X^4+X^3+X^2+X+1$
6	2	X^2-X+1
7	6	$X^6+X^5+X^4+X^3+X^2+X+1$
8	4	X^4+1
9	6	X^6+X^3+1
10	4	$X^4-X^3+X^2-X+1$
11	10	$X^{10}+X^9+\ldots+X^2+X+1$
12	4	X^4-X^2+1
13	12	$X^{12}+X^{11}+\ldots+X^2+X+1$
14	6	$X^6-X^5+X^4-X^3+X^2-X+1$
15	8	$X^8-X^7+X^5-X^4+X^3-X+1$
16	8	X^8+1

Tabelle 1. Die ersten 16 Kreisteilungspolynome $\Phi_1, \ldots, \Phi_{16}$.

Sei weiterhin die Charakteristik von K kein Teiler von n, sodass X^n-1 in K^{a} genau n paarweise verschiedene Nullstellen besitzt. Die Menge $\{\zeta \in (K^{\mathrm{a}})^\times : \mathrm{ord}(\zeta) \text{ teilt } n\}$ bildet zusammen mit der Körpermultiplikation von K^{a} eine endliche Gruppe und ist darum laut Satz 4.4 zyklisch. Die Erzeuger dieser Gruppe nennen wir ***primitive n-te Einheitswurzeln***. Eine primitive n-te Einheitswurzel ist also ein Element von K^{a} mit multiplikativer Ordnung n.

Lemma 5.19. *Sei L/K eine Körpererweiterung und $\zeta \in L$ eine primitive n-te Einheitswurzel, wobei die Charakteristik von K kein Teiler von n sei. Dann ist $K(\zeta)/K$ eine Galois-Erweiterung und* $\mathrm{Gal}(K(\zeta)/K)$ *ist isomorph zu einer Untergruppe von* $(\mathbb{Z}/n\mathbb{Z})^\times$. *Insbesondere ist* $\mathrm{Gal}(K(\zeta)/K)$ *abelsch.*

[7] Gemeint ist natürlich, dass man jedes Φ_n als $f_*(\Phi)$ mit einem normierten Polynom $\Phi \in \mathbb{Z}[X]$ und dem kanonischen Ringhomomorphismus $f\colon \mathbb{Z} \to K^{\mathrm{a}}$ erhält.

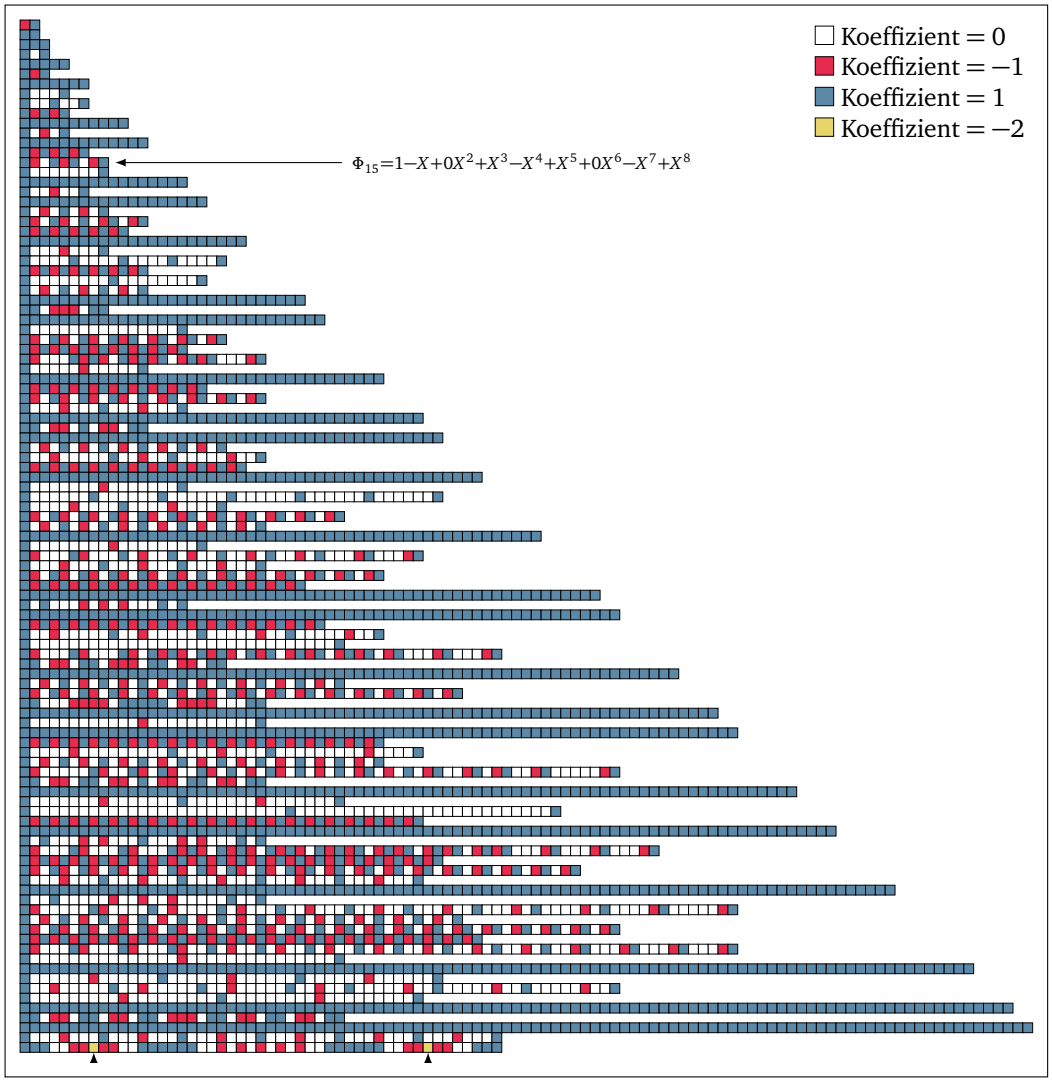
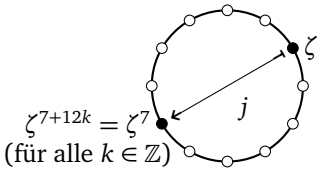


Abbildung 17. Visualisierung der ersten 105 Kreisteilungspolynome $\Phi_1, \ldots, \Phi_{105}$. Das Diagramm ist jeweils zeilenweise als Polynom $c_0 + c_1X + c_2X^2 + \ldots \in \mathbb{Z}[X]$ zu lesen, wobei die Koeffizienten $c_0, c_1, c_2, \ldots$ farbcodiert sind. Die erste Zeile zeigt $\Phi_1 = -1 + X$ und die letzte Zeile zeigt $\Phi_{105} = 1 + X + X^2 + 0X^3 + 0X^4 - X^5 - X^6 - 2X^7 - X^8 - \ldots + X^{48}$. Man beachte, dass Φ_{105} das erste Kreisteilungspolynom ist, welches einen Koeffizienten $\notin \{0, \pm 1\}$ besitzt.

Beweis. Wir dürfen o.B.d.A. davon ausgehen, dass L/K in einen algebraischen Abschluss K^{a}/K eingebettet ist. Sei $j\colon K(\zeta) \to K^{\mathrm{a}}$ ein beliebiger K-Homomorphismus. Offensichtlich ist mit ζ auch $j(\zeta)$ ein Element der Ordnung n in L und daher von der Form $j(\zeta) = \zeta^{\nu(j)} \in K(\zeta)$ mit einem Exponenten $\nu(j) \in \mathbb{N}$, der modulo n eindeutig

bestimmt ist und teilerfremd zu n ist (denn sonst hätte $\zeta^{\nu(j)}$ kleinere Ordnung als ζ). Zum Beispiel:



$$\Longrightarrow\ j \longmapsto (7 \bmod 12).$$

Wir sehen mit Satz 3.10, dass $K(\zeta)$ normal ist. Ferner ist $K(\zeta)$ auch separabel (denn das Minimalpolynom von ζ teilt das nach Voraussetzung separable Polynom $X^n - 1$). Die eben konstruierte Abbildung

$$\mathrm{Gal}(K(\zeta)/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \quad j \longmapsto (\nu(j) \bmod n)$$

erweist sich leicht als Gruppenhomomorphismus, ja sogar ein Gruppenmonomorphismus (denn $j \in \mathrm{Gal}(K(\zeta)/K)$ ist durch sein Bild auf ζ eindeutig festgelegt). Daraus ergibt sich die Behauptung. □

Selbstverständlich ist in der Situation von Lemma 5.19 $\mathrm{Gal}(K(\zeta)/K)$ im Allgemeinen eine *echte* Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$. (Man denke beispielsweise an den trivialen Fall, wenn ζ bereits in K enthalten ist. Dann ist $\mathrm{Gal}(K(\zeta)/K) = \{\mathrm{id}_{K(\zeta)}\}$ die triviale Gruppe. Alternativ beachte man $K(\exp(2\pi\mathrm{i}/4))/K$ mit $K = \mathbb{Q}(\mathrm{i}) \subset \mathbb{C}$.)

Da eine zyklische Gruppe der Ordnung n genau $\varphi(n)$ Erzeuger hat (hier ist φ die Eulersche φ-Funktion, siehe Lemma 4.3) folgt, dass Φ_n Grad $\varphi(n)$ hat. *Falls* wir wüssten, dass Φ_n irreduzibel ist, dann hätte $K(\zeta)/K$ in Lemma 5.19 mindestens Grad $\varphi(n)$ und wegen $\#((\mathbb{Z}/n\mathbb{Z})^\times) = \varphi(n)$ und Proposition 5.1 wäre dann $\mathrm{Gal}(K(\zeta)/K) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Das ist natürlich nicht immer der Fall.[8] Über den rationalen Zahlen löst sich aber alles in Wohlgefallen auf:

Satz 5.20 (Kronecker 1854)**.** *Sei $n \in \mathbb{N}$. Dann ist das n-te Kreisteilungspolynom Φ_n irreduzibel über $\mathbb{Q}$.*

Beweis (Dedekind, van der Waerden). Da Φ_n normiert ist, genügt es Irreduzibilität über $\mathbb{Z}$ zu zeigen. Sei also $\Phi_n = FG$ mit normierten Polynomen $F, G \in \mathbb{Z}[X]$ und F sei irreduzibel. Ferner sei ζ eine Nullstelle von F in $\mathbb{C}$. Wir behaupten, dass für jede Primzahl p die n nicht teilt auch ζ^p eine Nullstelle von F in $\mathbb{C}$ ist. Dies zeigen wir gleich, doch zunächst überlegen wir uns, weshalb daraus schon die Irreduzibilität von Φ_n folgt. In der Tat ist jede Nullstelle von Φ_n eine primitive n-te Einheitswurzel und schreibt sich als ζ^ν für ein geeignetes ν, welches teilerfremd zu n ist. Schreibt man $\nu = p_1 \cdots p_r$ als Produkt von (nicht notwendigerweise verschiedenen) Primzahlen, so sind all diese natürlich teilerfremd zu n und unsere Behauptung zeigt, dass auch

$$\zeta^\nu = \zeta^{p_1 \cdots p_r} = \left((\zeta^{p_1})^{\cdots}\right)^{p_r}$$

[8] Man betrachte z.B. $K = \mathbb{R}$: Dort sind alle Polynome vom Grad > 2 reduzibel, aber $\deg \Phi_n > 2$ für $n > 6$. Alternativ kann man auch den Fall $K = \mathbb{C}$ betrachten (beachte Satz 5.9).

eine Nullstelle von F ist. Dann hat aber F mindestens Grad $\varphi(n)$ und aus Grad- und Normiertheitsgründen ist dann $\Phi_n = F$.

Nun zur obigen Behauptung. Wir nehmen an, diese sei falsch. Sei also p prim und ζ^p keine Nullstelle von F. Da ζ^p aber eine Nullstelle von $\Phi_n = FG$ ist, muss ζ^p eine Nullstelle von G in $\mathbb{C}$ sein. Dann ist ζ aber eine Nullstelle von $G(X^p)$ und da F Minimalpolynom von ζ ist, handelt es sich bei F um einen Teiler von $G(X^p)$. Es ist also $G(X^p) = FH$ für ein Polynom $H \in \mathbb{Q}[X]$. Da $G(X^p)$ und F beide normierte Polynome mit Koeffizienten aus $\mathbb{Z}$ sind, liefert das Lemma von Gauß, dass H ebenfalls ganzzahlige Koeffizienten besitzt. Der Reduktionshomomorphismus $\overline{\cdot}\colon \mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]$, welcher die Koeffizienten von ganzzahligen Polynomen modulo p reduziert, führt dann zu

$$\overline{F}\,\overline{H} = \overline{G(X^p)} = \overline{G}(\overline{X}^p) = (\overline{G}(\overline{X}))^p = \overline{G}^p,$$

wobei wir für die letzte Gleichung den Frobenius-Endomorphismus von $(\mathbb{Z}/p\mathbb{Z})[X]$ benutzt haben. Zerlegt man die linke und die rechte Seite der obigen Gleichung über einem algebraischen Abschluss von $\mathbb{Z}/p\mathbb{Z}$ in Linearfaktoren, so sieht man, dass $\overline{F}$ und $\overline{G}$ gemeinsame Nullstellen haben. Dann hat das Polynom $\overline{X^n - 1}$, welches ja von $\overline{\Phi_d} = \overline{F}\,\overline{G}$ geteilt wird, aber eine doppelte Nullstelle in eben jenem algebraischen Abschluss und ist somit nicht separabel. Das ist aber widersprüchlich, da $\overline{X^n - 1}$ wegen $p \nmid n$ separabel ist. □

Korollar 5.21. *Sei $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel. Dann ist* $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Der Körper $\mathbb{Q}(\zeta)$ aus Korollar 5.21 mit primitiver n-ter Einheitswurzel ζ heißt ***n-ter Kreisteilungskörper***.

5.5.2. Anwendung auf Konstruierbarkeit mit Zirkel und Lineal. In diesem Abschnitt setzen wir Vertrautheit mit der Charakterisierung von mit Zirkel und Lineal konstruierbaren Zahlen voraus. Diese sollte aus [33, Satz 11.7] oder [16, Satz 4.5.9] bekannt sein.

Korollar 5.22. *Das regelmäßige* 5*-Eck ist mit Zirkel und Lineal konstruierbar.*

Wir merken an, dass unser Hauptziel hier *nicht* die Aussage von Korollar 5.22 selbst ist, sondern viel mehr in der im Zuge des Beweises gewonnenen Einsicht begründet liegt. In der Tat kann man Korollar 5.22 auch schlicht dadurch beweisen, indem man anmerkt, dass

$$\mathrm{Re}(\exp(\mathrm{i}\alpha)) = \cos(\alpha) = \tfrac{1}{4}(-1+\sqrt{5}) \quad (\alpha = 2\pi/5) \tag{5.2}$$

jedenfalls konstruierbar ist und durch Fällung eines Lotes und Schneiden mit dem Einheitskreis dann auch $\mathrm{Im}(\exp(\mathrm{i}\alpha))$, womit sich $\exp(\mathrm{i}\alpha)$ schon als konstruierbar erweist. Der Beweis der letzten Gleichheit in (5.2) ist damit eine Standard-Übungsaufgabe in Trigonometrie: Wegen $2\pi = 2\alpha + 3\alpha$ haben wir

$$\cos(3\alpha) = \cos(2\pi - 2\alpha) = \cos(-2\alpha) = \cos(2\alpha).$$

Andererseits liefern das Additionstheorem für den Kosinus und der „Trigonometrische Pythagoras“

$$\cos(2\alpha) = \cos(\alpha)^2 - \sin(\alpha)^2 = 2\cos(\alpha)^2 - 1.$$

Abermalige Anwendung von Additionstheorem, Pythagoras und der soeben gewonnenen Identität liefern

$$\begin{aligned}\cos(3\alpha) &= \cos(2\alpha)\cos(\alpha) - \sin(2\alpha)\sin(\alpha)\\ &= (2\cos(\alpha)^2 - 1)\cos(\alpha) - (2\cos(\alpha)\sin(\alpha))\sin(\alpha)\\ &= 2\cos(\alpha)^3 - \cos(\alpha) - 2\cos(\alpha)\sin(\alpha)^2\\ &= 2\cos(\alpha)^3 - \cos(\alpha) - 2\cos(\alpha)(1 - \cos(\alpha)^2)\\ &= 4\cos(\alpha)^3 - 3\cos(\alpha).\end{aligned}$$

Zusammen mit der eingangs erhaltenen Identität sehen wir

$$2\cos(\alpha)^2 - 1 = \cos(3\alpha) = \cos(2\alpha) = 4\cos(\alpha)^3 - 3\cos(\alpha).$$

Umstellen liefert

$$0 = 4\cos(\alpha)^3 - 2\cos(\alpha)^2 - 3\cos(\alpha) + 1 = (\cos(\alpha) - 1)(4\cos(\alpha)^2 + 2\cos(\alpha) - 1).$$

Wegen $\cos(\alpha) \neq 1$ folgt, dass $\cos(\alpha)$ Nullstelle des Polynoms $4X^2 + 2X - 1$ ist. Auflösen und Berücksichtigen von $\cos(\alpha) > 0$ liefert (5.2).

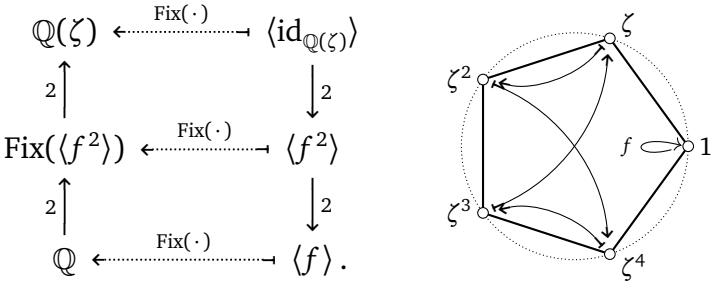
Die obige Rechnung *bestätigt* (5.2) und beweist (wie oben begründet) auch Korollar 5.22. Man lernt allerdings nicht viel daraus und es ist vollkommen unklar, wie man beispielsweise die Konstruierbarkeit des regelmäßigen 17-Ecks beweisen kann; der Ausdruck (5.2) fällt ja vom Himmel und sofern einem nicht auch für $\mathrm{Re}(\exp(2\pi\mathrm{i}/17))$ ein solcher Ausdruck vorgegeben wird, scheint es hoffnungslos, diesen mit den obigen Methoden zu *erraten*. Hier schafft Galois-Theorie Abhilfe und liefert eine transparente *Methode*, um sich Ausdrücke wie (5.2) zu beschaffen.

Beweis von Korollar 5.22. Das fragliche Problem läuft darauf hinaus die primitive 5-te Einheitswurzel $\zeta = \exp(2\pi\mathrm{i}/5) \in \mathbb{C}$ zu konstruieren. Gemäß Korollar 5.21 (siehe auch Beispiel 4.2) haben wir

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times \cong C_4.$$

Also ist $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ zyklisch! Ein Erzeuger von $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ ist z.B. der K-Homomorphismus f, welcher ζ auf ζ^2 abbildet. Wir haben dann folgende absteigende Kette von Automorphismengruppen und zugehörigen aufsteigenden Körperturm von

Fixkörpern:



Jede Erweiterung $\mathrm{Fix}(\langle f^{2k} \rangle)/\mathrm{Fix}(\langle f^k \rangle)$ mit $k = 1, 2$ ist quadratisch und alle Elemente in solchen Erweiterungen sind mit Zirkel und Lineal konstruierbar (siehe [33, Satz 11.7] oder [16, Satz 4.5.9]). Das zeigt auch schon die Aussage des Satzes. □

Wir wollen uns nun aber auch noch überlegen, wie man explizit Erzeuger der fraglichen Fixkörper aus dem obigem Beweis bestimmen kann (siehe hierzu insbesondere die Bemerkung auf Seite 75). Führt man dies bis zum Ende aus, so gewinnt man eine Formel für $\zeta = \exp(2\pi \mathrm{i}/5)$ als Wurzelausdruck, aus der man mit etwas Geduld eine explizite Konstruktionsanleitung herleiten kann. Wir behalten hierzu die Notation aus Korollar 5.22 bei. Jedes Element x von $\mathbb{Q}(\zeta)$ schreibt sich in der Form[9]

$$x = \lambda_1 \zeta + \lambda_2 \zeta^2 + \lambda_3 \zeta^3 + \lambda_4 \zeta^4.$$

Wegen

$$f^2(x) = \lambda_1 \zeta^4 + \lambda_2 \zeta^3 + \lambda_3 \zeta^2 + \lambda_4 \zeta$$

zeigt ein Koeffizientenvergleich, dass x genau dann in $\mathrm{Fix}(\langle f^2 \rangle)$ enthalten ist, wenn

$$\lambda_1 = \lambda_4 \quad \text{und} \quad \lambda_2 = \lambda_3.$$

Jedes $x \in \mathrm{Fix}(\langle f^2 \rangle)$ schreibt sich also in der Form

$$x = \lambda_1 \zeta + \lambda_2 \zeta^2 + \lambda_2 \zeta^3 + \lambda_1 \zeta^4 = \lambda_1(\zeta + \zeta^4) + \lambda_2(\zeta^2 + \zeta^3).$$

Daher ist eine Basis von $\mathrm{Fix}(\langle f^2 \rangle)$ gegeben durch die zwei Elemente

$$y := \zeta + \zeta^4 \quad \text{und} \quad \zeta^2 + \zeta^3 = \underbrace{1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4}_{=\Phi_5(\zeta)=0} - 1 - y = -1 - y.$$

Aus Galois-theoretischen Gründen wissen wir, dass y in einer quadratischen Erweiterung von $\mathbb{Q}$ liegt und also 1, y und y^2 $\mathbb{Q}$-linear abhängig sind. Es liegt also nahe, y^2 berechnen zu wollen, um schließlich ein quadratisches Polynom mit y als Nullstelle zu

[9] Vielleicht schiene der Ansatz $x = \mu_1 + \mu_2 \zeta + \mu_3 \zeta^2 + \mu_4 \zeta^3$ natürlicher, jedoch bildet f^2 das Element ζ auf ζ^4 ab, welches wir dann zunächst bezüglich der $\mathbb{Q}$-Basis $\{1, \zeta, \zeta^2, \zeta^3\}$ darstellen müssten, bevor wir einen Koeffizientenvergleich durchführen können. Das ist zwar auch nicht wirklich schwierig (da ζ Nullstelle von $\Phi_5 = X^4 + X^3 + X^2 + X + 1$ ist, sieht man $\zeta^4 = -\zeta^3 - \zeta^2 - \zeta - 1$), aber insgesamt doch etwas umständlicher.

bestimmen und sodann y als geeigneten Wurzelausdruck zu erhalten. Man verifiziert mühelos

$$y^2 = \zeta^2 + 2\zeta^5 + \zeta^3 = 1 - y.$$

Durch Auflösen sieht man $y \in \{(-1 \pm \sqrt{5})/2\}$. Man kann sich wegen $\operatorname{Re} y > 0$ auch $y = (-1 + \sqrt{5})/2$ überlegen, aber auch ohne dies ist nun klar, dass

$$\operatorname{Fix}(\langle f^2 \rangle) = \mathbb{Q}((-1 + \sqrt{5})/2).$$

Die Erweiterung $\mathbb{Q}(\zeta)/\operatorname{Fix}(\langle f^2 \rangle)$ hat Grad 2. Darum ist $\{1, \zeta\}$ eine $\operatorname{Fix}(\langle f^2 \rangle)$-Basis von $\mathbb{Q}(\zeta)$. Man berechnet leicht

$$\zeta^2 = y\zeta - 1.$$

Es folgt $\zeta \in \{(y \pm \sqrt{y^2 - 4})/2\}$ und also (beachte $\operatorname{Im} \zeta > 0$)

$$\zeta = \frac{y + \mathrm{i}\sqrt{4 - y^2}}{2} = \frac{\frac{-1+\sqrt{5}}{2} + \mathrm{i}\sqrt{4 - \frac{(-1+\sqrt{5})^2}{4}}}{2} = \frac{-1 + \sqrt{5}}{4} + \mathrm{i}\frac{\sqrt{5 + \sqrt{5}}}{2\sqrt{2}}.$$

Bemerkung. Bei Aluffi [1, Seite 470f.] findet man die zu Korollar 5.22 und unserer darauffolgenden Betrachtung analogen Überlegungen für das regelmäßige 17-Eck. Man sollte hier primär die Einsicht haben, dass die Überlegungen zum regelmäßigen 17-Eck rechenintensiver sind, aber eigentlich keine Ideen benötigen, die wir nicht auch schon bei unserer Diskussion des regelmäßgen 5-Ecks aufgeworfen haben.

In der Vorlesung *Einführung in die Algebra* wurde im Anschluss an [33, Satz 11.7] bemerkt, dass nicht alle algebraischen Zahlen $x \in$ mit $[\mathbb{Q}(x) : \mathbb{Q}] =$ Zweierpotenz konstruierbar sind. Als Beispiel wurden hier die Nullstellen von $X^4 + X + 1$ angeführt und für Details wurde auf diese Vorlesung *Algebra* verwiesen. Wir skizzieren daher kurz, was zu tun ist. Sei x daher eine beliebige Nullstelle von $P = X^4 + X + 1$ in $\mathbb{C}$ und $L \subset \mathbb{C}$ Zerfällungskörper von P. Dank [33, Satz 11.7] genügt es jedenfalls zu sehen, dass es keinen quadratischen Zwischenkörper in der Erweiterung $\mathbb{Q}(x)/\mathbb{Q}$ gibt. Hierzu überlegt man sich, dass P irreduzibel ist und Galois-Gruppe $\operatorname{Gal}(P) = \operatorname{Gal}(L/\mathbb{Q}) \cong \mathfrak{S}_4$ besitzt; das mag mit den hier entwickelten Methoden vielleicht etwas zu schwierig sein, kann aber mit etwas mehr Theorie durch Betrachtung von P modulo einiger Primzahlen erfolgen. Für mehr Details hierzu verweisen wir auf [26, Chapter VI, § 2, Example 7, sowie Theorem 2.9 in Chapter VII, § 2]. Gäbe es nun einen Turm von quadratischen Erweiterungen

$$\mathbb{Q} \underset{\text{(Grad 2)}}{\subset} K \underset{\text{(Grad 2)}}{\subset} \mathbb{Q}(x),$$

so erhielte man mittels der Galois-Korrespondenz eine absteigende Folge von Untergruppen

$$\mathfrak{S}_4 \cong \operatorname{Gal}(L/\mathbb{Q}) \underset{\text{(Index 2)}}{\supset} \operatorname{Gal}(L/K) \underset{\text{(Index 2)}}{\supset} \operatorname{Gal}(L/\mathbb{Q}(x)).$$

Man kann sich nun durch Betrachtung der $\mathfrak{S}_4$ überlegen, dass es so etwas nicht gibt. (Man überlege sich zunächst, dass A_4 die einzige Index 2-Untergruppe von $\mathfrak{S}_4$ ist und A_4 selbst keine Index 2-Untergruppe besitzt.)

5.6. Auflösbarkeit durch Radikale

5.6.1. Radikalerweiterungen. Ein Höhepunkt der Galois-Theorie ist die Verneinende Beantwortung der Frage, ob es zu vorgegebenem Polynomgrad $n \geq 5$ eine allgemeine Formel geben könne, welche ausgehend von dessen Koeffizienten und den rationalen Zahlen nur unter Ausnutzung von Addition, Subtraktion, Multiplikation, Division und Ziehung k-ter Wurzeln eine Nullstelle des fraglichen Polynoms gewinnt.

Satz 5.23 (Abel–Ruffini)**.** *Die Nullstellen von Polynomen vom Grad* 5 *oder höher lassen sich im Allgemeinen nicht durch Wurzelausdrücke angeben.*

Wir verweisen hierzu auf Seite v und die dort besprochenen Beispiele. Da wir nun die Galois-Korrespondenz auch tatsächlich kennengelernt haben, wiederholen wir erneut die folgende Überlegung vom Beginn der Vorlesung:
Die Zahl $x = \sqrt[3]{1-\sqrt{2}} \in \mathbb{C}$ ist Nullstelle des (irreduziblen) Polynoms $P = X^6 - 2X^3 - 1 \in \mathbb{Q}[X]$. Beim Ausrechnen von x mittels obigen Wurzelausdrucks erhält man die Zwischenergebnisse

$$1, \quad 1-\sqrt{2}, \quad x$$

und diese führen auf einen Turm von Körpererweiterungen

$$\mathbb{Q} = \mathbb{Q}(1) \subset \mathbb{Q}(1-\sqrt{2}) \subset \mathbb{Q}(x).$$

Bemüht man nun die Galois-Korrespondenz die zum Zerfällungskörper $L \subseteq \mathbb{C}$ von P gehört, so übersetzt sich dieser Turm in eine absteigende Reihe von Untergruppen

$$\mathrm{Gal}(L/\mathbb{Q}) \supset \mathrm{Gal}(L/\mathbb{Q}(x)) \supset \mathrm{Gal}(L/\mathbb{Q}(1-\sqrt{2})) \supset \{\mathrm{id}_L\}.$$

Für den rigorosen Beweis ist es aus technischen Gründen (zur Gewährleistung von Normalität der Teilerweiterungen) günstig, den obigen Erweiterungen noch eine geeignete Einheitswurzel hinzuzufügen und kleinschrittiger vorzugehen. Dann liefert einem das Verständnis der Adjunktion in den Teilschritten ein Verständnis der zugehörigen Faktorgruppen auf der Ebene der Galois-Gruppen. Solche gruppentheoretischen Eigenschaften lassen sich nun gegebenenfalls nachprüfen (oder auch ausschließen), *ohne* die Nullstellen des gegebenen Polynoms a-priori als Wurzelausdrücke zu kennen! (Man erinnere sich etwa an Beispiel 5.17, wo uns die Bestimmung der Galois-Gruppe des Polynoms $X^5 - 4X + 2$ über $\mathbb{Q}$ gelang, *ohne* dessen Nullstellen zu berechnen.)

Mit Blick auf die obigen Überlegungen, sei $\iota\colon K \to L$ eine Körpererweiterung. Wir nennen diese eine ***Radikalerweiterung***, falls es Elemente $x_0, x_1, \ldots, x_t \in L$ und Exponenten $\nu_0, \nu_1, \ldots, \nu_t \in \mathbb{N}$ gibt mit $L = K(x_0, x_1, \ldots, x_t)$, $x_0^{\nu_0} \in K$ und

$$x_j^{\nu_j} \in K(x_0, \ldots, x_{j-1})$$

für $j = 1, \ldots, t$. (Mittels $\nu = \nu_0 \nu_1 \cdots \nu_t$ kann man die Exponenten alle identisch wählen.) Um auch in Charakteristik $p > 0$ eine zufrieden stellende Theorie zu erhalten, müsste man den obigen Begriff einer Radikalerweiterung noch geringfügig modifizieren und Adjunktion von Nullstellen von sogenannten Artin–Schreier-Polynomen

$X^p - X - a$ zulassen (siehe etwa [26, Chapter VI, § 7] und beachte auch [33, Aufgabe 14.4]). Wir blenden diese Details einfach aus, indem wir uns weiter unten an geeigneter Stelle auf Charakteristik 0 beschränken.

Lemma 5.24 (Adjunktion n-ter Wurzeln)**.** *Sei K ein Körper und $\zeta \in K$ eine primitive n-te Einheitswurzel, im Sinne von* $\operatorname{ord}(\zeta) = n$*. Ferner sei $a \in K^\times$ beliebig. Dann ist $P = X^n - a \in K[X]$ separabel, und* $\operatorname{Aut}(P) = \operatorname{Gal}(P)$ *ist eine zyklische Gruppe; Ihre Ordnung teilt n und ist gleich n, falls P irreduzibel ist.*

Bemerkung. Man beachte die wichtige Voraussetzung in Lemma 5.24, dass der Körper K bereits eine primitive n-te Einheitswurzel enthält. So wissen wir beispielsweise aus Beispiel 5.16, dass das Polynom $X^4 - 2 \in \mathbb{Q}[X]$ eine zu $D_{2\cdot 4}$ isomorphe Galois-Gruppe besitzt, und diese darum insbesondere nicht zyklisch ist. Betrachtet man stattdessen $X^4 - 2$ über dem Körper $\mathbb{Q}(\mathrm{i}) \subseteq \mathbb{C}$, der ja eine primitive 4-te Einheitswurzel (nämlich $\pm\mathrm{i}$) enthält, so erhält man als Galois-Gruppe eine zyklische Gruppe mit genau vier Elementen.

Beweis von Lemma 5.24. Wir denken uns K in einen algebraischen Abschluss eingebettet. Sei x dann eine (beliebige) Nullstelle von P in diesem. Dann sind $\zeta^j x$ mit $j = 1, \ldots, n$ sämtliche Nullstellen von P und diese sind alle verschieden. Also ist P separabel. Ferner ist $K(x) = K(\{\zeta^j x : j = 1, \ldots, n\}) = L$ ein Zerfällungskörper von K.

Wir betrachten nun die Abbildung

$$\Psi\colon \operatorname{Gal}(P) \longrightarrow \langle\zeta\rangle \subseteq K^\times, \quad f \longmapsto f(x)/x.$$

Sein $f, g \in \operatorname{Gal}(P)$ beliebig. Wegen $\Psi(g) \in K^\times \subset \operatorname{Fix}(\langle f\rangle)$ ist $\Psi(g) = f(\Psi(g))$ und also

$$\Psi(f)\Psi(g) = \Psi(f)f(\Psi(g)) = \frac{f(x)}{x} f\left(\frac{g(x)}{x}\right) = \frac{(f \circ g)(x)}{x} = \Psi(f \circ g).$$

Also ist Ψ ein Gruppenhomomorphismus. Überdies ist Ψ injektiv, denn $\Psi(f) = 1_{K^\times}$ impliziert $f(x) = x$ und wegen $K(x) = L$ dann $f = \mathrm{id}_L$. Es folgt also, dass $\operatorname{Gal}(P)$ isomorph zu einer Untergruppe der zyklischen Gruppe $\langle\zeta\rangle \cong C_n$ ist. Ist P zudem irreduzibel, so hat $\operatorname{Gal}(P)$ mindestens n Elemente und daher dann genau n Elemente. □

5.6.2. Auflösbare Gruppen. Wir schicken den nächsten Untersuchungen einen kurzen Ausflug in die Gruppentheorie vorweg. Eine Gruppe G heißt ***auflösbar***, wenn es eine aufsteigende Folge von normalen Untergruppen

$$\{1_G\} = U_0 \lhd U_1 \lhd \ldots \lhd U_{t-1} \lhd U_t = G.$$

mit abelschen Faktorgruppen gibt. Es sei hier noch explizit betont, dass hier zwar jedes U_{i-1} normal in U_i zu sein hat, aber U_{i-1} nicht normal in U_j für $j > i$ zu sein braucht. (Gelegentlich ist es notationsbedingt günstig die Indizierung umzudrehen und also *absteigende* Folgen zu betrachten. Offensichtlich führt dies auf denselben Auflösbarkeitsbegriff.)

Beispiele. Wir geben hier einige Beispiele; Die Details hierzu sind in Aufgabe 10.3 auszuführen.

(1) Die Diedergruppe $D_{2\cdot 4}$ mit 8 Elementen entsteht als Symmetriegruppe eines regelmäßigen 4-Ecks (ein Quadrat). Sie enthält eine 90°-Drehung σ. Man kann nun die nachstehenden Folgen von normalen Untergruppen (mit abelschen Faktorgruppen) bilden:

$$D_{2\cdot 4} \rhd \langle\sigma\rangle \rhd \{1_{D_{2\cdot 4}}\}, \quad D_{2\cdot 4} \rhd \langle\sigma^2\rangle \rhd \{1_{D_{2\cdot 4}}\},$$
$$D_{2\cdot 4} \rhd \langle\sigma\rangle \rhd \langle\sigma^2\rangle \rhd \{1_{D_{2\cdot 4}}\}.$$

(2) $\mathfrak{S}_4 \rhd A_4 \rhd \langle(1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\rangle \rhd \{\mathrm{id}_{\{1,2,3,4\}}\}$.

Der Zusammenhang zwischen Auflösbarkeit einer Galois-Gruppe und Auflösbarkeit durch Radikale wird später durch Lemma 5.28 hergestellt. Wir schicken diesem jedoch zunächst eine nähere gruppentheoretische Betrachtung des Auflösbarkeitsbegriffs voraus.

Sei G nun eine beliebige Gruppe. Die ***Kommutatoruntergruppe G' von G*** ist diejenige Untergruppe von G, die von allen Elementen der Form $[a,b] = aba^{-1}b^{-1}$ mit $a, b \in G$ erzeugt wird. (Elemente der Form $[a,b]$ nennt man ***Kommutatoren***.) Wegen

$$ab = (baa^{-1}b^{-1})ab = ba(a^{-1}b^{-1}ab) = ba[a^{-1}, b^{-1}] \tag{5.3}$$

misst die Kommutatorgruppe G' die Abweichung von G davon abelsch zu sein.

Lemma 5.25 (Eigenschaften von Kommutatoruntergruppen)**.** *Gegeben sei ein Gruppenhomomorphismus $f\colon G \to H$ zwischen zwei Gruppen G und H. Dann gelten die folgenden Aussagen:*

(1) Es ist $f(G') \subseteq H'$. Ist f surjektiv, so gilt hierin sogar Gleichheit.
(2) Ist N ein Normalteiler von G, so ist auch N' normal in G.
(3) G' ist normal in G und die Faktorgruppe G/G' ist abelsch.
(4) Ist N ein Normalteiler von G und G/N abelsch, dann ist $N \supseteq G'$.

Beweis. Zum Beweis von (1) beachte man

$$f([a,b]) = f(aba^{-1}b^{-1}) = f(a)f(b)f(a)^{-1}f(b)^{-1} = [f(a), f(b)].$$

Insbesondere gilt $f(G') \subseteq H'$. Ist f surjektiv, so gilt, wie behauptet, sogar $f(G') = H'$, wie man direkt mit Blick die obige Gleichung sieht.

Zum Beweis von (2) sei N normal in G. Jeder innere Automorphismus $i_a\colon x \mapsto axa^{-1}$ von G induziert (durch Einschränkung) einen Endomorphismus von N. Zusammen mit (1) folgt nun $i_a(N') \subseteq N'$ für jedes $a \in G$. Also ist N' normal in G.

Da G normal in sich selbst ist, folgt die Normalität von G' in G sofort aus (2). Dass G/G' abelsch ist folgt leicht mittels (5.3):

$$(aN)(bN) = (ab)N = (ba[a^{-1}, b^{-1}])N = (ba)N = (bN)(aN).$$

Das beweist (3).

Zum Beweis von (4) beachte man

$$(aN)(bN) = (bN)(aN) \iff 1_G N = [aN, bN] = [a,b]N \iff [a,b] \in N.$$

Ist also G/N abelsch, so enthält N sämtliche Kommutatoren $[a,b]$. Also ist dann $N \supseteq G'$. □

Durch $G^{(0)} := G$ und sukzessives Bilden von Kommutatoruntergruppen

$$G^{(k)} = (G^{(k-1)})' \quad (k = 1, 2, 3, \ldots)$$

erhalten wir also eine absteigende Reihe

$$G \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq \ldots \trianglerighteq G^{(k)} \trianglerighteq \ldots;$$

Diese ist „allgemein genug“, um Auflösbarkeit von G zu erkennen:

Proposition 5.26 (Auflösbarkeitskriterium)**.** *Eine Gruppe G ist genau dann auflösbar, wenn $G^{(t)} = \{1_G\}$ für ein $t \in \mathbb{N}$ gilt.*

Beweis. Ist $G^{(t)} = \{1_G\}$ für ein $t \in \mathbb{N}$, so zeigt die oben notierte absteigende Folge offensichtlich die Auflösbarkeit von G. Ist nun umgekehrt G auflösbar, so wollen wir $G^{(t)} = \{1_G\}$ für ein $t \in \mathbb{N}$ nachweisen. Sei hierzu

$$G = U_0 \rhd U_1 \rhd U_2 \rhd \ldots \rhd U_{t-1} \rhd U_t = \{1_G\}.$$

eine absteigende Folge mit abelschen Faktorgruppen. Gemäß Lemma 5.25 (4) haben wir stets $U_i \supseteq U_{i-1}'$, da die Faktorgruppe U_{i-1}/U_i ja abelsch ist. Nun ist $U_1 \supseteq U_0' = G' = G^{(1)}$ und dann induktiv $U_i \supseteq U_{i-1}' \supseteq (G^{(i-1)})' = G^{(i)}$, wie man sich auch anhand des folgenden Diagramms verdeutlichen mag:

$$\begin{array}{ccccccccccccc}
G & = & U_0 & \rhd & U_1 & \rhd & \ldots & \rhd & U_{i-1} & \rhd & U_i & \rhd & \ldots & \rhd & U_t & = & \{1_G\} \\
 & & & & \cup| & & & & \cup| & & \cup| & & & & \cup| & & || \\
 & & & & U_0' & & \ddots & & U_{i-2}' & & U_{i-1}' & & \ddots & & U_{t-1}' & = & \{1_G\} \\
 & & & & \cup| & & & & \cup| & & \cup| & & & & \cup| & & || \\
 & & G & \trianglerighteq & G^{(1)} & \trianglerighteq & \ldots & \trianglerighteq & G^{(i-1)} & \trianglerighteq & G^{(i)} & \trianglerighteq & \ldots & \trianglerighteq & G^{(t)} & = & \{1_G\}.
\end{array}$$

Induktionsanfang — Induktionsschritt

Für $i = t$ erhält man $\{1_G\} = U_t \supseteq G^{(t)} \supseteq \{1_G\}$, also $G^{(t)} = \{1_G\}$, wie gewünscht. □

Korollar 5.27. *Untergruppen auflösbarer Gruppen sind auflösbar und homomorphe Bilder von auflösbaren Gruppen sind auflösbar. Ist G eine Gruppe mit auflösbarem Normalteiler N und auflösbarer Faktorgruppe G/N, so ist auch G auflösbar.*

Beweis. Das ist Aufgabe 11.1. □

5.6.3. Radikalerweiterungen und Auflösbarkeit. Nach dem vorangegangen Exkurs in die Gruppentheorie schlagen wir nun wieder den Bogen zur Körpertheorie und verknüpfen die Begriffe der Auflösbarkeit von Gruppen und Auflösbarkeit von Polynomgleichungen durch Radikale.

Lemma 5.28. *Sei K ein Körper mit Charakteristik 0 und R/K eine Radikalerweiterung. Dann ist R ein Zwischenkörper in einer Galois-Erweiterung L/K mit auflösbarer Galois-Gruppe.*

Beweis. Sei R/K eine Radikalerweiterung. Es gibt also Elemente $x_0, x_1, \ldots, x_t \in R$ und einen Exponenten $\nu \in \mathbb{N}$ mit $R = K(x_0, x_1, \ldots, x_t)$ und $x_0^\nu \in K$, sowie

$$x_j^\nu \in K(x_0, \ldots, x_{j-1})$$

für $j = 1, \ldots, t$. Nun ist die Erweiterung R/K im Allgemeinen nicht normal und enthält auch nicht notwendigerweise eine primitive ν-te Einheitswurzel. Um diesen Defekt zu beheben, sei m_j das Minimalpolynom von x_j und L/K der Zerfällungskörper (in einem fixierten algebraischen Abschluss, der auch R/K enthält) des Polynoms $(X^\nu - 1)m_0 m_1 \cdots m_t$. Mit Korollar 3.7 folgt nun, dass L/K eine Galois-Erweiterung ist, welche R als Zwischenkörper enthält. Wir schreiben $n = [L : K]$.

Ferner enthält $L^\times$ genau ν Elemente deren Ordnung ν teilt, nämlich die Nullstellen von $X^\nu - 1$ (erneut ist hier Separabilität wichtig). Diese Elemente bilden eine Gruppe und jene ist laut Satz 4.4 zyklisch. Also enthält L eine primitive ν-te Einheitswurzel $\zeta \in L$.

Mittels Satz 5.13 und Satz 5.3 (3) sieht man (via eines Zwischenschrittes über die Galois-Gruppe von m_j), dass $\mathrm{Gal}(L/K)$ transitiv auf den Nullstellen von m_j in L operiert. Demnach ist also

$$L = K(\{\zeta\} \cup \{f(x_j) : 0 \leq j \leq t,\, f \in \mathrm{Gal}(L/K)\}).$$

Zu $0 \leq j \leq t$ seien nun $x_{j,1}, x_{j,2}, \ldots, x_{j,n}$ die Elemente $\{f(x_j) : f \in \mathrm{Gal}(L/K)\}$ in irgendeiner Reihenfolge (zur Vereinfachung der Notation erlauben wir hier die mehrfache Nennung von solchen Elementen). Wir betrachten nun den Körperturm

$$\begin{aligned}
K \subseteq K(\zeta) &= K_0 \\
&\subseteq K_0(x_{0,1}) \subseteq K_0(x_{0,1}, x_{0,2}) \subseteq \ldots \subseteq K_0(x_{0,1}, x_{0,2}, \ldots, x_{0,n}) = K_1 \\
&\subseteq K_1(x_{1,1}) \subseteq K_1(x_{1,1}, x_{1,2}) \subseteq \ldots \subseteq K_1(x_{1,1}, x_{1,2}, \ldots, x_{1,n}) = K_2 \\
&\vdots \\
&\subseteq K_t(x_{t,1}) \subseteq K_t(x_{t,1}, x_{t,2}) \subseteq \ldots \subseteq K_t(x_{t,1}, x_{t,2}, \ldots, x_{t,n}) = L\,.
\end{aligned}$$

Nach Lemma 5.19 ist K_0/K eine Galois-Erweiterung mit abelscher Galois-Gruppe

$$\mathrm{Gal}(K_0/K) \cong \frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/K_0)}.$$

Jeder weitere Schritt ist von der Form $K' \subseteq K'(x)$, mit $x = f(x_j)$ für ein $f \in \mathrm{Gal}(L/K)$ und ein $j \leq t$. Nach Voraussetzung ist $x_j^\nu \in K(x_0, \ldots, x_{j-1})$ und daher auch

$$a := x^\nu = f(x_j^\nu) \in f(K(x_0, \ldots, x_{j-1})) = K(f(x_0), \ldots, f(x_{j-1})) \subseteq K'.$$

Also ist das Minimalpolynom von x ein Teiler des Polynoms $X^\nu - a \in K'[X]$. Ist $K'' \supseteq K'(x)$ ein Zerfällungskörper von $X^\nu - a$ über K', so haben wir also laut Satz 5.3 (1) ein Diagramm der Form

$$\begin{array}{ccc} K'' & \overset{\mathrm{Gal}(K''/\,\cdot\,)}{\longmapsto} & \{\mathrm{id}_{K''}\} \\ \uparrow & & \downarrow \\ K'(x) & \longmapsto & \mathrm{Gal}(K''/K'(x)) \\ \uparrow & & \downarrow \\ K' & \longmapsto & \mathrm{Gal}(K''/K'), \end{array}$$

wobei $\mathrm{Gal}(K''/K')$ laut Lemma 5.24 zyklisch ist. Da $\mathrm{Gal}(K''/K')$ also insbesondere abelsch ist, ist die Untergruppe $\mathrm{Gal}(K''/K'(x)) \leq \mathrm{Gal}(K''/K')$ automatisch normal. Mittels Satz 5.3 (3) erkennen wir dann aber auch die Faktorgruppe

$$\frac{\mathrm{Gal}(L/K')}{\mathrm{Gal}(L/K'(x))} \cong \mathrm{Gal}(K'(x)/K') \cong \frac{\mathrm{Gal}(K''/K')}{\mathrm{Gal}(K''/K'(x))}$$

als zyklisch; Diese so auftretenden Faktorgruppen sind genau die Faktorgruppen, die zu der absteigenden Folge gehören, die man nach Anwenden von $\mathrm{Fix}(\,\cdot\,)$ auf den obigen Körperturm erhält. Das zeigt die Behauptung. □

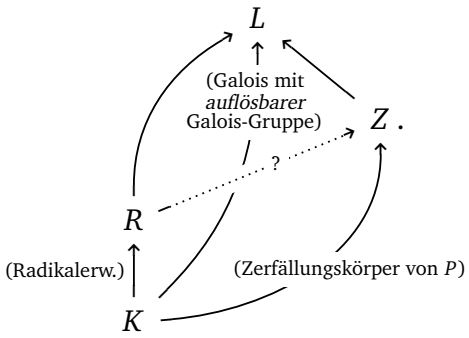
Bemerkung. Man mag sich fragen, ob man im obigen Beweis nicht auch L als R adjungiert eine geeignete Einheitswurzel setzen könnte und so schneller ans Ziel käme. Dies ist allerdings nicht so einfach, wie das folgende Beispiel zeigt: Betrachte die Radikalerweiterung $\mathbb{Q}(x_0, x_1)/\mathbb{Q}$ mit $x_0 = \sqrt{2}$ und $x_1 = \sqrt[4]{2}$. Die Hinzunahme von $x_0 = x_1^2$ ist in Gegenwart von x_1 offensichtlich redundant, doch wir haben damit einen Körpertum

$$\mathbb{Q} \subset \mathbb{Q}(x_0) \subset \mathbb{Q}(x_0, x_1)$$

mit $x_0^2 \in \mathbb{Q}$ und $x_1^2 \in \mathbb{Q}(x_0)$. In der Situation vom Beweis von Lemma 5.28 kann man also $\nu = 2$ und die primitive ν-te Einheitswurzel -1 ist freilich schon in $\mathbb{Q}(x_0, x_1)$ enthalten. Dennoch ist $\mathbb{Q}(x_0, x_1)/\mathbb{Q}$ nicht normal, denn $\sqrt[4]{2}$ hat über $\mathbb{Q}$ das Minimalpolynom $X^4 - 2$, dessen Nullstellen in $\mathbb{C}$ durch $\pm\sqrt[4]{2}$ und $\pm\mathrm{i}\sqrt[4]{2}$ gegeben sind. Die letztgenannten beiden sind allerdings nicht in $\mathbb{Q}(x_0, x_1)$ enthalten. Man beachte jedoch, dass beide Erweiterungen $\mathbb{Q}(x_0, x_1)/\mathbb{Q}(x_0)$ und $\mathbb{Q}(x_0)/\mathbb{Q}$ als quadratische Erweiterungen normal sind, ihre Verkettung ist allerdings nicht.

Korollar 5.29 (Galois)**.** *Sei K ein Körper mit Charakteristik 0 und $P \in K[X]$ ein irreduzibles Polynom. Hat P eine Nullstelle in einer Radikalerweiterung von K, so ist* $\mathrm{Gal}(P)$ *auflösbar.*

Beweis. Ist R/K eine Radikalerweiterung, welche eine Nullstelle von P enthält, und L/K wie aus Lemma 5.28, dann zerfällt P in L, da L/K normal ist. Insbesondere enthält L/K einen Zerfällungskörper Z von P als Zwischenkörper. Man veranschaulicht sich die vorliegende Situation vielleicht anhand des folgenden Diagramms:[10]



Die Galois-Gruppe von P ist also nach Satz 5.3 (3) isomorph zu einer Faktorgruppe der auflösbaren Gruppe $\mathrm{Gal}(L/K)$:

$$\mathrm{Gal}(P) = \mathrm{Gal}(Z/K) \cong \frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/Z)}.$$

Daher ist $\mathrm{Gal}(P)$ selbst auflösbar gemäß Korollar 5.27. □

Satz 5.30. *Für $n \geq 5$ ist die symmetrische Gruppe $\mathfrak{S}_n$ nicht auflösbar.*

Beweis. Für $n \geq 5$ kann man sich überlegen, dass die Kommutatoruntergruppe $\mathfrak{S}_n'$ von $\mathfrak{S}_n$ mit A_n übereinstimmt. Da A_n allerdings einfach und nicht abelsch ist, folgt weiter $\mathfrak{S}_n'' = A_n$ und also $\mathfrak{S}_n^{(t)} = A_n$ für alle $t \in \mathbb{N}$. Nun lässt sich Proposition 5.26 anwenden. Die Details hierzu sind Aufgabe 10.3 (b). □

Nun gelingt auch endlich der Beweis des Satzes von Abel–Ruffini:

Beweis von Satz 5.23. Man beachte, dass Beispiel 5.17 ein Polynom mit der gemäß Satz 5.30 nicht-auflösbaren Gruppe $\mathfrak{S}_5$ als Galois-Gruppe liefert. Mit Satz 5.30 folgt dann auch schon die Behauptung aus Korollar 5.29. □

[10] Man möchte hier vielleicht behaupten, dass R in Z liegt, da R ja laut Annahme eine Nullstelle von P enthält. Allerdings könnte R noch weitere Elemente enthalten, die nichts mit Z zu tun haben. Zum Glück ist die Frage, ob $R \subseteq Z$ gilt, aber egal für den Fortschritt des hiesigen Beweises.

Teil 2

Modultheorie

KAPITEL 6

Grundzüge der Modultheorie

„Much in the theory of modules over a ring is arrow-theoretic." —Serge Lang [26]

Moduln[1] sind „Vektorräume über Ringen." Bevor wir uns formal mit diesen beschäftigen, denken wir uns diese als nichts anderes als einen Ring R zusammen mit einer abelschen Gruppe M und einer „Skalarmultiplikation" $R \times M \to M$, die alle Eigenschaften erfüllt, die man von der Skalarmultiplikation von Vektorräumen kennt.

6.1. Motivation durch Beispiele

Neben den Vektorräumen kennen wir bereits andere Moduln sehr gut: Abelsche Gruppen.

Beispiel 6.1 (Abelsche Gruppen $=$ $\mathbb{Z}$-Moduln)**.** Jede abelsche Gruppe G lässt sich in natürlicher Weise als Modul über $\mathbb{Z}$ auffassen. Die Skalarmultiplikation ist hier durch

$$\mathbb{Z} \times G \longrightarrow G, \quad (n, g) \longmapsto \begin{cases} g + \ldots + g & \text{falls } n > 0, \\ 0_G & \text{falls } n = 0, \\ (-g) + \ldots + (-g) & \text{falls } n < 0 \end{cases}$$

gegeben, wobei die angedeutete Addition jeweils aus $|n|$ Summanden bestehe. Die Struktur von endlich erzeugten abelschen Gruppen hat man gut verstanden. Jede solche ist isomorph zu einem (und nur einem) Isomorphietyp der Form

$$\mathbb{Z}^n \times C_{k_1} \times C_{k_2} \times \ldots \times C_{k_d} \quad \text{(kart. Produkt von Gruppen)}$$

mit nichtnegativen ganzen Zahlen $n, d, k_1, \ldots, k_d$ und k_1 teilt k_2, k_2 teilt k_3, etc. (Siehe auch Beispiel 8.5.)

Auch Vektorräume hat man sehr gut verstanden:

Beispiel 6.2 (K-Vektorräume und Dimension)**.** Jeder endlich erzeugte (d.h. endlichdimensionale) K-Vektorraum V ist isomorph zu $K^n = \bigoplus_{j=1}^{n} K$ für ein (und nur ein) $n \in \mathbb{N}_0$: Für geeignete Elemente $v_1, \ldots, v_n \in V$ ist

$$V = \bigoplus_{j=1}^{n} Kv_j \cong \bigoplus_{j=1}^{n} K. \tag{6.1}$$

[1] Singular: Der Modul; Plural: Die Moduln.

Beispiel 6.3 (Darstellung eines Endomorphismus)**.** Fixiert man zusätzlich zu einem endlich-dimensionalen K-Vektorraum V auch einen Endomorphismus $f\colon V \to V$, so ist man erneut bemüht V — wie in Beispiel 6.2 — in „kleinere Bausteine“ zu zerlegen, auf denen man f getrennt untersuchen kann. Man zerlegt den Vektorraum V hierbei nicht bloß in eine Summe von eindimensionalen K-Vektorräumen K, sondern in eine Summe von f-invarianten Unterräumen:

$$V = \bigoplus_{j=1}^{d} W_j \quad \text{mit} \quad f(W_j) \subseteq W_j. \tag{6.2}$$

Dabei ist man besonders an maximal feinen Zerlegungen interessiert, also denjenigen, bei denen man kein W_j weiter in eine direkte Summe nicht-trivialer f-invarianter Unterräume zerlegen kann. Im bekannten Kalkül der linearen Algebra korrespondiert dies zu einer Darstellung von f durch eine Matrix A, welche diagonal ist, oder zumindest „fast“ diagonal ist.

$$\begin{array}{ccc} V & \xrightarrow{\quad f \quad} & V \\ \downarrow \wr & & \downarrow \wr \\ K^n & \xrightarrow{x \mapsto Ax} & K^n\,. \end{array}$$

(Wenn man eine Basis von V durch Aneinanderreihung von Basen der Unterräume W_j generiert, so nimmt die zugehörige Darstellungsmatrix von f eine Blockdiagonalgestalt an, deren Blöcke die Darstellungsmatrizen der eingeschränkten Abbildung $f|_{W_j}\colon W_j \to W_j$ bezüglich der Basen von W_j gegeben sind.)

Selbst bei diesem Standardproblem der linearen Algebra stößt man auf Moduln, die selbst keine Vektorräume sind: Durch

$$K[X] \times V \longrightarrow V, \quad (P, v) \longmapsto (P(f))(v)$$

wird eine Skalarmultiplikation definiert, wobei für ein Polynom $P = \sum_{k=1}^{r} a_k X^k$ der Endomorphismus $P(f)\colon V \to V$ durch $P(f) = \sum_{k=1}^{r} a_k f^{(k)}$ definiert sei und $f^{(k)}$ die k-fache Hintereinanderausführung von f bezeichne:

$$f^{(0)} = \mathrm{id}_V, \quad f^{(1)} = f, \quad f^{(2)} = f \circ f, \quad \ldots;$$

Die Untermoduln bezüglich dieser Modulstruktur sind nun genau diejenigen Unterräume von V (bezüglich der K-Vektorraumstruktur von V), welche f-invariant sind.

Unter diesem Gesichtspunkt entpuppt sich die Zerlegung (6.1) aus Beispiel 6.2 als Analogon zu der Zerlegung (6.2), sofern man sich diese auch hinreichend fein denkt. Eine sehr feine Zerlegung der Art (6.2) kennt man wohl aus der linearen Algebra schon als Jordan-Normalform für die Körper $\mathbb{R}$ und $\mathbb{C}$.

Beispiel. Wir führen die Idee aus Beispiel 6.3 exemplarisch für $V = \mathbb{R}^2$ und $f(v) = \left(\begin{smallmatrix} 1 & \\ & 2 \end{smallmatrix}\right) \cdot v$ aus. Bezüglich der durch f auf V gestifteten $K[X]$-Modulstruktur ist dann

$$V = \mathbb{R}[X]\begin{pmatrix}1\\1\end{pmatrix} = \mathbb{R}[X]\begin{pmatrix}1\\0\end{pmatrix} \oplus \mathbb{R}[X]\begin{pmatrix}0\\1\end{pmatrix}. \tag{6.3}$$

Man beachte, dass V hier von einem Element erzeugt werden kann, aber auch direkte Summe der Erzeugnisse von zwei anderen Elementen ist. Dies ist ein fundamentaler Unterschied zur bekannten Theorie der Vektorräume! Übrigens beachte man

$$X^0\begin{pmatrix}1\\0\end{pmatrix} = \mathrm{id}_V\left(\begin{pmatrix}1\\0\end{pmatrix}\right) = \begin{pmatrix}1\\0\end{pmatrix} = f\left(\begin{pmatrix}1\\0\end{pmatrix}\right) = X^1\begin{pmatrix}1\\0\end{pmatrix},$$

also

$$(X^0 - X^1)\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix} = 0_M.$$

Eine Darstellung eines Elements von V als

$$P_1\begin{pmatrix}1\\0\end{pmatrix} + P_2\begin{pmatrix}0\\1\end{pmatrix}$$

mit Polynomen (Skalaren!) $P_1, P_2 \in \mathbb{R}[X]$ ist also nicht eindeutig. Dennoch ist die Summe in (6.3) direkt. Wenn man nur lineare Algebra kennt, scheint dies vielleicht paradox, klärt sich aber später noch durch Proposition 6.9.

In diesem Kapitel untersuchen wir Moduln zunächst allgemein. Dem wichtigen Spezialfall von endlich erzeugten Moduln über Hauptidealbereichen wenden wir uns später in Kapitel 8 zu. Deren Strukturtheorie, die wir dort entwickeln, schließt insbesondere die hier besprochenen Beispiele als Spezialfälle mit ein.

6.2. Definitionen und einfache Eigenschaften

Sei $(R, +, \cdot)$ ein Ring und $(M, \dot{+})$ eine abelsche Gruppe zusammen mit einer Abbildung $*\colon R \times M \to M$, welche für alle $\lambda, \mu \in R$ und $v, w \in M$ die folgenden Axiome erfüllt:

- $\lambda * (v \dot{+} w) = (\lambda * v) \dot{+} (\lambda * w)$,
- $(\lambda + \mu) * v = (\lambda * v) \dot{+} (\mu * v)$,
- $(\lambda \cdot \mu) * v = \lambda * (\mu * v)$,
- $1_R * v = v$.

Dann bezeichnen wir $(M, \dot{+}, *)$ als einen ***Links-R-Modul***. Ist $*$ hingegen eine Abbildung der Form $M \times R \to M$ und gelten die in offensichtlicher Weise modifizierten Axiome, so bezeichnet man $(M, \dot{+}, *)$ als einen ***Rechts-R-Modul***. Wie üblich schreibt man häufig nur $+$ und $\cdot$ für alle auftretenden Abbildungen und spricht auch nur von einem Links(-/Rechts)-R-Modul M. Die Skalarmultiplikation wird auch gerne vollständig unterdrückt und man schreibt bloß λv für $\lambda * v$ bzw. $\lambda \cdot v$.

Wir sprechen abkürzend oft nur von einem ***R-Modul*** und meinen stets einen *Links-R*-Modul. (Diese Festlegung ist üblich, aber letztlich selbstverständlich willkürlich.) Im Zusammenhang mit R-Moduln nennen wir die Elemente von R auch ***Skalare***.

Ein ***R-Modulhomomorphismus*** ist eine Abbildung $f\colon M \to N$ zwischen zwei R-Moduln M und N, welche ein Homomorphismus der zugehörigen additiven Gruppen ist, und im folgenden Sinne mit den Skalarmultiplikationen $*_M$, $*_N$ auf M bzw. N verträglich ist:

$$f(\lambda *_M m) = \lambda *_N f(m)$$

für alle $\lambda \in R$ und alle $m \in M$. Wir bezeichnen R-Modulhomomorphismen auch als ***R-lineare Abbildungen***.

Ein ***Untermodul*** eines R-Moduls $(M, \dot{+}, *)$ ist eine Untergruppe U von $(M, \dot{+})$, welche stabil unter Skalarmultiplikation ist: Für alle $\lambda \in R$ und $u \in U$ gelte $\lambda * u \in U$. Wie üblich definiert man ***Kern*** und ***Bild*** von R-Modulhomomorphismen $f\colon M \to N$ und stellt fest, dass es sich bei $\ker f$ um einen Untermodul von M und bei $\operatorname{im} f$ um einen Untermodul von N handelt. Wie in der linearen Algebra beweist man, dass ein R-Modulhomomorphismus $f\colon M \to N$ genau dann injektiv ist, wenn $\ker f = \{0\}$ ist.

Beispiel 6.4. Jeder Ring R wird durch die Ringmultiplikation als Skalarmultiplikation zu einem Modul über sich selbst. Die (Links/Rechts-)Untermoduln von R sind dann genau die (Links/Rechts-)Ideale von R.

Ein injektiver/surjektiver/bijektiver R-Modulhomomorphismus heißt ***R-Modul-mono/epi/iso-morphismus***. Sind Quell- und Zielbereich identisch, handelt es sich also um einen R-Modulhomomorphismus $M \to M$, so nennen wir diesen einen ***R-Modulendomorphismus***. Die Menge aller R-Modulhomomorphismen von M nach N bezeichnen wir mit

$$\operatorname{Hom}_R(M, N).$$

Diese bildet zusammen mit der durch

$$+\colon \operatorname{Hom}_R(M,N) \times \operatorname{Hom}_R(M,N) \longrightarrow \operatorname{Hom}_R(M,N), \quad (f,g) \longmapsto (x \mapsto f(x) + g(x))$$

definierten Addition eine abelsche Gruppe. Ist der Ring R überdies kommutativ, so wird $\operatorname{Hom}_R(M,N)$ mittels der Skalarmultiplikation

$$R \times \operatorname{Hom}_R(M,N) \longrightarrow \operatorname{Hom}_R(M,N), \quad (\lambda, f) \longmapsto \lambda f := (x \mapsto \lambda f(x))$$

sogar zu einem R-Modul. Die Kommutativität von R ist hierbei wichtig, um sicherzustellen, dass es sich bei λf wieder um eine R-lineare Abbildung handelt:

$$\begin{aligned}(\lambda\mu)f(x) &= \lambda(\mu f(x)) = \lambda f(\mu x)\\ &= (\lambda f)(\mu x) \overset{!}{=} \mu(\lambda f)(x) = \mu(\lambda f(x)) = (\mu\lambda)f(x).\end{aligned}$$

Bemerkung 6.5. Sei K ein Körper. Dann stimmen die Begriffe „K-Modul“ und „K-Vektorraum“ überein (denn die jeweiligen Axiome sind dieselben). Insbesondere ist für jedes fixierte Element v eines K-Moduls V die Abbildung $K \to V$, $\lambda \mapsto \lambda v$ (via Skalarmultiplikation) injektiv.

Bemerkung 6.6. Ist M ein R-Modul über einem Ring R und R' ein zweiter Ring mit einem Ringhomomorphismus $f: R' \to R$, so wird M durch

$$R' \times M \longrightarrow M, \quad (r', x) \mapsto f(r')x \quad \text{(mittels } R\text{-Skalarmultiplikation)}$$

zu einem R'-Modul. Dieser Operation haben wir uns bereits in der Körpertheorie extensiv bedient, als wir mittels einer Körpererweiterung $\iota: K \to L$ (den eindimensionalen L-Vektorraum) L als K-Vektorraum aufgefasst haben. Man bezeichnet die eben eingeführte Operation als ***Einschränkung der Skalare*** (auch wenn der Ringhomomorphismus f nicht injektiv ist).

6.3. Summen und Produkte

Ein zentrales Konzept der Linearen Algebra ist es, eine lineare Abbildung zwischen Vektorräumen dadurch zu verstehen, dass man sowohl die zugrundeliegenden Räume, als auch die Abbildung selbst, in niedriger-dimensionale Bestandteile zerlegt (siehe Beispiel 6.2 und Beispiel 6.3).

Sei $(M_i)_i$ eine Familie von R-Moduln, wobei die Indizes i eine (nicht notwendigerweise endliche) Indexmenge durchlaufen. Das (mengentheoretische) kartesische ***Produkt***

$$\prod_i M_i$$

wird durch komponentenweise definierte Addition und Skalarmultiplikation selbst zu einem R-Modul. Für jeden fixierten Index j ist die ***Projektion***

$$\pi_j: \prod_i M_i \longrightarrow M_j, \quad (x_i)_i \longmapsto x_j$$

linear. Ferner definieren wir die ***direkte Summe***

$$\bigoplus_i M_i = \left\{ (x_i)_i \in \prod_i M_i : x_i \neq 0 \text{ für höchstens endlich viele } i \right\}. \tag{6.4}$$

Für jeden fixierten Index j haben wir hier die ***Inklusion***

$$\iota_j: M_j \longrightarrow \bigoplus_i M_i, \quad x \longmapsto (x_i)_i$$

mit $x_i = 0$ für $i \neq j$ und $x_j = x$. Diese ist ebenfalls linear.

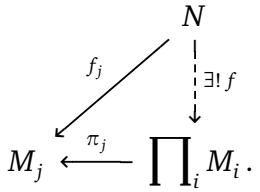
Handelt es sich bei $(M_i)_i$ um eine *endliche* Familie $M_1, \ldots, M_r$, so stimmen die beiden R-Moduln $\prod_i M_i$ und $\bigoplus_i M_i$ überein. Wir schreiben dann auch

$$M_1 \times \ldots \times M_r \quad \text{für} \quad \prod_i M_i, \quad \text{sowie} \quad M_1 \oplus \ldots \oplus M_r \quad \text{für} \quad \bigoplus_i M_i,$$

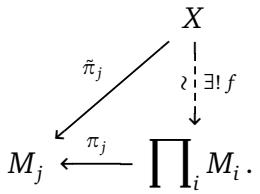
bevorzugen aber in solchen Fällen die Notation mit „$\oplus$“ bzw. „$\bigoplus$“. In diesem Zusammenhang (und in der Kategorientheorie) spricht man hier auch von ***Biprodukten***. Leserinnen und Leser sollten im Hinterkopf behalten, dass die oben definierten Projektionen π_j und Inklusionen ι_j *Teil der Struktur* von Produkten bzw. direkten Summen (bzw. Biprodukten im Übereinstimmungsfall) sind, genau so, wie man auch schon immer von *einer Gruppe* G spricht, aber formal eigentlich das Tupel $(G, \circ)$ aus zugrunde liegender Menge G und Gruppenverknüpfung $\circ: G \times G \to G$ meint.

Satz 6.7. *Sei $(M_i)_i$ eine Familie von R-Moduln und N ein R-Modul.*

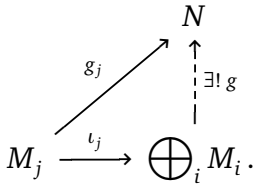
(1) Für jede Familie $(f_i)_i$ von R-Modulhomomorphismen $f_i\colon N \to M_i$ gibt es genau einen R-Modulhomomorphismus $f\colon N \to \prod_i M_i$, der für jeden Index j das folgende Diagramm kommutativ macht:



(2) Ist X ein R-Modul zusammen mit R-Modulhomomorphismen $\tilde{\pi}_j\colon X \to M_j$ derart, dass die Aussage in (1) auch für X statt $\prod_i M_i$ und $\tilde{\pi}_j$ statt π_j gilt, so gibt es genau einen(!) R-Modulisomorphismus $f\colon X \to \prod_i M_i$, welcher für jeden Index j das folgende Diagramm kommutativ macht:



(3) Für jede Familie $(g_i)_i$ von R-Modulhomomorphismen $g_i\colon M_i \to N$ gibt es genau einen R-Modulhomomorphismus $g\colon \bigoplus_i M_i \to N$, der für jeden Index j das folgende Diagramm kommutativ macht:



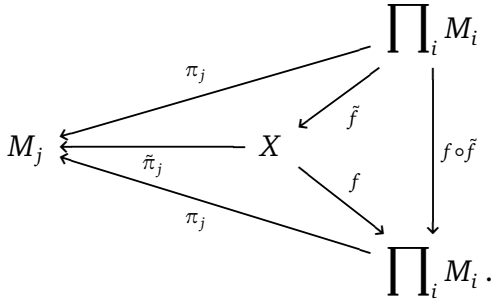
Überdies hat man die Formel $g = \sum_i (g_i \circ \pi_i)$.

(4) Eine zu (2) analoge Eindeutigkeitsaussage gilt auch in der Situation von (3).

Beweis. Wir beweisen zunächst die Existenz von f in (1). Hierzu setze man $f(n) = (f_i(n))_i$ und rechnet nach, dass dies einen R-Modulhomomorphismus f wie in (1) stiftet. Für die Eindeutigkeitsaussage beachte man, dass die geforderte Gleichung $\pi_j \circ f = f_j$ bereits bestimmt, dass f wie eben konstruiert gegeben sein muss.

Zum Beweis von (2) beachte man, dass es laut (1) genau ein f gibt, welches die Diagramme aus (2) kommutativ macht. Da X zusammen mit $(\tilde{\pi}_i)_i$ eine analoge Eigenschaft erfüllt, erhalten wir auch einen R-Modulhomomorphismus $\tilde{f}\colon \prod_i M_i \to X$ mit $\tilde{\pi}_j \circ \tilde{f} = \pi_j$ für jeden Index j. Nun ist $f \circ \tilde{f}\colon X \to \prod_i M_i$ aber eine Abbildung mit

$$\pi_j \circ (f \circ \tilde{f}) = (\pi_j \circ f) \circ \tilde{f} = \tilde{\pi}_j \circ \tilde{f} = \pi_j = \pi_j \circ \mathrm{id}_{\prod_i M_i};$$



Die Eindeutigkeitsaussage in (1) liefert dann aber $f \circ \tilde{f} = \mathrm{id}_{\prod_i M_i}$ und in analoger Weise bestätigt man $\tilde{f} \circ f = \mathrm{id}_X$. Bei f handelt es sich also tatsächlich um einen Isomorphismus.

Die Aussagen (3) und (4) beweist man analog — siehe Aufgabe 12.2. □

Korollar 6.8. *Für jede Familie $(M_i)_i$ von R-Moduln und R-Moduln M, N haben wir kanonische Isomorphismen von abelschen Gruppen:*

$$\mathrm{Hom}_R\big(N, \prod_i M_i\big) \xrightarrow{\sim} \prod_i \mathrm{Hom}_R(N, M_i),$$
$$\mathrm{Hom}_R\big(\bigoplus_i M_i, N\big) \xrightarrow{\sim} \prod_i \mathrm{Hom}_R(M_i, N).$$

(Ist R kommutativ, so handelt es sich sogar um R-Modulisomorphismen.)

Beweis. Hier sei $\pi_j\colon \prod_i M_i \to M_j$ wie oben. Wir betrachten die Abbildung

$$\Psi\colon \mathrm{Hom}_R\big(N, \prod_i M_i\big) \longrightarrow \prod_i \mathrm{Hom}_R(N, M_i), \quad f \longmapsto (\pi_i \circ f)_i.$$

Man rechnet leicht nach, dass es sich hierbei um einen Homomorphismus von abelschen Gruppen handelt (ja, sogar einen R-Modulhomomorphismus, falls R kommutativ ist). Nun liefert Eindeutigkeitsaussage in Satz 6.7 (1) unmittelbar die Injektivität von Ψ und die überdies darin enthaltene Existenzaussage liefert die Surjektivität.

Für den zweiten Teil betrachte man die Abbildung

$$\mathrm{Hom}_R\big(\bigoplus_i M_i, N\big) \longrightarrow \prod_i \mathrm{Hom}_R(M_i, N), \quad g \longmapsto (g \circ \iota_i)_i$$

(mit $\iota_j\colon M_j \to \bigoplus_i M_i$) und argumentiere wie zuvor. □

Bemerkung. Mit Blick auf Korollar 6.8 mag man sich fragen, ob auch

$$\mathrm{Hom}_R\big(\prod_i M_i, N\big) \quad \text{und} \quad \prod_i \mathrm{Hom}_R(M_i, N)$$

isomorph sind? — Das ist i.Allg. allerdings nicht der Fall: Es ist beispielsweise

$$\prod_{m=1}^{\infty} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Q}) = \{(\text{Nullabbildung: } \mathbb{Z}/m\mathbb{Z} \to \mathbb{Q})_{m\in\mathbb{N}}\}$$

einelementig, aber

$$\mathrm{Hom}_{\mathbb{Z}}\big(\prod_{m=1}^{\infty} (\mathbb{Z}/m\mathbb{Z}), \mathbb{Q}\big)$$

enthält mehr als nur ein Element. Die Behauptete Gleichheit ist leicht zu sehen, da in $\mathbb{Z}/m\mathbb{Z}$ jedes Element (additiv) endliche Ordnung besitzt und also von einem $\mathbb{Z}$-Modulhomomorphismus auf ein Element von $\mathbb{Q}$ mit endlicher Ordnung abgebildet werden muss. Das einzige derartige Element ist $0 \in \mathbb{Q}$. Die zweite Behauptung folgt daraus, dass es einen $\mathbb{Z}$-Modulhomomorphismus $\prod_m(\mathbb{Z}/m\mathbb{Z}) \to \mathbb{Q}$ gibt, der $(1_{\mathbb{Z}/1\mathbb{Z}}, 1_{\mathbb{Z}/2\mathbb{Z}}, \ldots)$ auf $1_{\mathbb{Q}}$ abbildet. Letzteres ist allerdings etwas schwieriger einzusehen und soll an dieser Stelle nicht bewiesen werden.

Sei $(M_i)_i$ eine Familie von Untermoduln eines R-Moduls M und $(g_i)_i$ die zugehörige Folge von Inklusionsabbildungen $g_i\colon M_i \hookrightarrow M$ ($g_i = \mathrm{id}_M|_{M_i}$). Dann *identifizieren* wir $\bigoplus_i M_i$ mit seinem Bild $g(\bigoplus_i M_i) \subseteq M$ unter der Abbildung g aus Satz 6.7 (3), *sofern diese injektiv ist*. In diesem Sinne gilt dann

$$„\bigoplus_i M_i \subseteq M“$$

und wir haben

$$„\bigoplus_i M_i = M“$$

falls g sogar surjektiv ist. Es ist wichtig hierbei im Hinterkopf zu behalten, dass M hier sicher nicht (als Menge) gleich $\bigoplus_i M_i$ gemäß der in (6.4) gegebenen Definition ist. Allerdings stellt die Eindeutigkeit von g in Satz 6.7 (3) sicher, dass wir — falls g injektiv ist — klar sagen können, welchem Element M ein beliebiges Element von $\bigoplus_i M_i$ entspricht.

Wir illustrieren die obige Konvention anhand eines Beispiels. Aus der *linearen Algebra* kennt man sicherlich bereits Aussagen wie

$$„\mathbb{R}\begin{pmatrix}1\\0\end{pmatrix} \oplus \mathbb{R}\begin{pmatrix}0\\1\end{pmatrix} = \mathbb{R}^2.“ \tag{6.5}$$

Hierbei sind die Summanden auf der linken Seite natürlich eindimensionale Unterräume von $\mathbb{R}^2$ und ihre Elemente sind Tupel aus reellen Zahlen. Ihre direkte Summe im Sinne der in (6.4) gegebenen Definition ist also

$$\mathbb{R}\begin{pmatrix}1\\0\end{pmatrix} \oplus \mathbb{R}\begin{pmatrix}0\\1\end{pmatrix} = \left\{ \left(\begin{pmatrix}\lambda\\0\end{pmatrix}, \begin{pmatrix}0\\\mu\end{pmatrix} \right) : \lambda, \mu \in \mathbb{R} \right\} =: \left\{ \begin{pmatrix}\lambda & 0\\0 & \mu\end{pmatrix} : \lambda, \mu \in \mathbb{R} \right\},$$

wobei wir in der letzten Gleichung (für die Dauer dieses Beispiels) lediglich eine abkürzende Notation eingeführt haben. Wir haben die beiden Inklusionen

$$\iota_1\colon \mathbb{R}\begin{pmatrix}1\\0\end{pmatrix} \hookrightarrow \mathbb{R}\begin{pmatrix}1\\0\end{pmatrix} \oplus \mathbb{R}\begin{pmatrix}0\\1\end{pmatrix}, \quad \begin{pmatrix}\lambda\\0\end{pmatrix} \mapsto \begin{pmatrix}\lambda & 0\\0 & 0\end{pmatrix},$$

$$\iota_2\colon \mathbb{R}\begin{pmatrix}0\\1\end{pmatrix} \hookrightarrow \mathbb{R}\begin{pmatrix}1\\0\end{pmatrix} \oplus \mathbb{R}\begin{pmatrix}0\\1\end{pmatrix}, \quad \begin{pmatrix}0\\\mu\end{pmatrix} \mapsto \begin{pmatrix}0 & 0\\0 & \mu\end{pmatrix}.$$

Die Abbildung

$$g\colon \mathbb{R}\begin{pmatrix}1\\0\end{pmatrix} \oplus \mathbb{R}\begin{pmatrix}0\\1\end{pmatrix} \to M,$$

welche man mittels Satz 6.7 (3) durch Anwendung auf

$$g_1 = \mathrm{id}_M|_{\mathbb{R}\binom{1}{0}} \quad \text{und} \quad g_2 = \mathrm{id}_M|_{\mathbb{R}\binom{0}{1}}$$

erhält, bildet also wie folgt ab:

$$\begin{aligned} g\left(\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}\right) &= g\left(\begin{pmatrix}\lambda & 0\\ 0 & 0\end{pmatrix} + \begin{pmatrix}0 & 0\\ 0 & \mu\end{pmatrix}\right) = g\left(\begin{pmatrix}\lambda & 0\\ 0 & 0\end{pmatrix}\right) + g\left(\begin{pmatrix}0 & 0\\ 0 & \mu\end{pmatrix}\right) \\ &= (g \circ \iota_1)\left(\begin{pmatrix}\lambda\\ 0\end{pmatrix}\right) + (g \circ \iota_2)\left(\begin{pmatrix}0\\ \mu\end{pmatrix}\right) \\ &= \mathrm{id}_M|_{\mathbb{R}\binom{1}{0}}\left(\begin{pmatrix}\lambda\\ 0\end{pmatrix}\right) + \mathrm{id}_M|_{\mathbb{R}\binom{0}{1}}\left(\begin{pmatrix}0\\ \mu\end{pmatrix}\right) \\ &= \begin{pmatrix}\lambda\\ 0\end{pmatrix} + \begin{pmatrix}0\\ \mu\end{pmatrix} = \begin{pmatrix}\lambda\\ \mu\end{pmatrix}. \end{aligned}$$

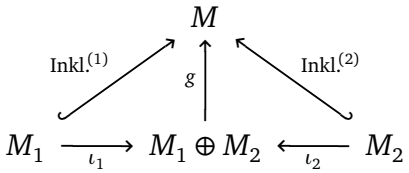
Diese ist offensichtlich bijektiv und in diesem Sinne gilt auch (6.5).

Proposition 6.9 (Direktheitskriterium)**.** *Sei M ein R-Modul mit Untermoduln M_1 und M_2. Dann gilt genau dann $M_1 \oplus M_2 = M$, wenn $M_1 \cap M_2 = \{0\}$ und die* ***Summe von M_1 und M_2,***

$$M_1 + M_2 := \{\, x_1 + x_2 : x_1 \in M_1,\, x_2 \in M_2 \,\},$$

gleich M ist.

Beweis. Es gilt zu überprüfen, wann die Abbildung g, welche das Diagramm



kommutativ macht, ein Isomorphismus ist.

„$\Longleftarrow$“: Sei $M = M_1 + M_2$ und $M_1 \cap M_2 = \{0\}$. Aus Satz 6.7 (3) haben wir die Formel

$$g = \mathrm{Inkl.}^{(1)} \circ \pi_1 + \mathrm{Inkl.}^{(2)} \circ \pi_2.$$

Wegen $M = M_1 + M_2$ ist jedes $m \in M$ von der Form $m = m_1 + m_2$ mit geeigneten Elementen $m_1 \in M_1$ und $m_2 \in M_2$. Dann ist aber

$$\begin{aligned} g(m_1, m_2) &= \mathrm{Inkl.}^{(1)} \circ \pi_1(m_1, m_2) + \mathrm{Inkl.}^{(2)} \circ \pi_2(m_1, m_2) \\ &= \mathrm{Inkl.}^{(1)}(m_1) + \mathrm{Inkl.}^{(2)}(m_2) = m_1 + m_2 = m. \end{aligned}$$

Also ist g surjektiv. Ferner ist g auch injektiv, denn für $(m_1, m_2) \in \ker g$ folgt mit obiger Formel leicht $m_1 + m_2 = 0$, also $m_1, m_2 \in M_1 \cap M_2 = \{0\}$, weswegen $\ker g = \{0\}$ ist. Also ist g ein Isomorphismus.

„$\Longrightarrow$“: Sei nun g ein Isomorphismus. Insbesondere gibt es zu jedem $m \in M$ ein $(m_1, m_2) \in M_1 \oplus M_2$ mit $g(m_1, m_2) = m$. Die obige Formel zeigt dann $m =$

$m_1 + m_2$, also, da $m \in M$ beliebig war, $M = M_1 + M_2$. Sei nun $m \in M_1 \cap M_2$. Dann ist $g(m,0) = g(0,m)$, also (da g injektiv ist) $(m,0) = (0,m)$ und daher $m = 0$. Es folgt $M_1 \cap M_2 = \{0\}$. □

6.4. Freie Moduln

Sei I eine beliebige Indexmenge und R ein Ring. Wir fassen R als R-Modul über sich selbst auf und betrachten den ***freien R-Modul über I***

$$R^{(I)} = \bigoplus_{i \in I} R.$$

Wir schreiben — zumindest für den Moment — $\boldsymbol{i} = \iota_i(1_R)$, denken uns in Zukunft aber i als ein Element von $R^{(I)}$, meinen damit jedoch formal $\boldsymbol{i}$. Mit dieser Notation schreibt sich jedes Element von $R^{(I)}$ in eindeutiger Weise als Summe

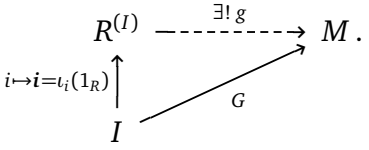
$$\sum_{i \in I} \lambda_i \boldsymbol{i}$$

mit Skalaren $\lambda_i \in R$ (höchstens endlich viele von 0_R verschieden). Im Falle $I = \{1, 2, \ldots, n\}$ mit $n \in \mathbb{N}$ schreiben wir auch R^n statt $R^{(I)}$.

Stellt man sich die Elemente von $R^{(I)}$ als mit I indizierte Tupel vor, so ist $\boldsymbol{i}$ nichts Anderes, als das Tupel

$$(\ldots, 0_R, 0_R, \underbrace{1_R}_{(i\text{-te Stelle})}, 0_R, 0_R, \ldots).$$

Proposition 6.10. *Sei I eine beliebige Menge. Für jeden R-Modul M und jede Abbildung $G\colon I \to M$ gibt es* genau einen *R-Modulhomomorphismus $g\colon R^{(I)} \to M$ mit $g(\boldsymbol{i}) = G(i)$ für alle $i \in I$:*



Man hat einen Isomorphismus von abelschen Gruppen

$$\mathrm{Abb}(I, M) \xrightarrow{\sim} \mathrm{Hom}_R(R^{(I)}, M), \quad G \longmapsto g.$$

(Ist R kommutativ, so handelt es sich sogar um R-Modulisomorphismen.)

Beweis. Man rechnet leicht nach, dass es sich bei der Abbildung

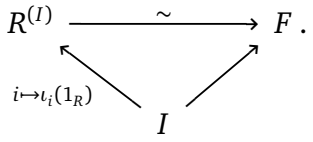
$$\mathrm{Hom}_R(R, M) \to R, \quad f \mapsto f(1_R),$$

um einen R-Modulisomorphismus handelt. Damit und mit Satz 6.7 (3) bzw. Korollar 6.8 folgt auch schon die Behauptung. (Siehe auch Aufgabe 13.1.) □

Man beachte, dass es sich bei Proposition 6.10 um eine direkte Verallgemeinerung der folgenden aus der linearen Algebra bekannten Aussage handelt: *Für jeden K-Vektorraum V mit Basis $(b_i)_{i \in I}$ und jede Abbildung $G\colon I \to W$ in einen K-Vektorraum W, gibt es genau eine lineare Abbildung $g\colon V \to W$ mit $g(b_i) = G(i)$.* — Man kann

die Bilder von Basisvektoren beliebig vorschreiben (Existenz von g), hat damit dann aber auch die fragliche lineare Abbildung völlig bestimmt (Eindeutigkeit von g).

Bemerkung 6.11. Ein R-Modul F heißt ***frei***, falls es eine Abbildung $I \to F$ von einer Menge I und einen R-Modulisomorphismus $R^{(I)} \to F$ gibt derart, dass folgendes Diagramm kommutiert:



Ganz ähnlich wie in Satz 6.7 (2) und (4) überlegt man sich, dass dies genau dann der Fall ist, wenn die Aussage von Proposition 6.10 auch gültig bleibt, wenn man darin $R^{(I)}$ und $i \mapsto \iota_i(1_R)$ durch F respektive die Abbildung $I \to F$ ersetzt. Wir sagen auch F sei ***frei über I***, um den Bezug zur Abbildung $I \to F$ zu betonen.

Beispiele 6.12.

(1) Jeder Ring R ist als Modul über sich selbst frei (über $\{1_R\}$ in naheliegender Weise).
(2) $R^n = R^{(\{1,\dots,n\})}$ ist frei für jedes $n \in \mathbb{N}_0$. (Spezialfall: $R^0 = R^{(\emptyset)}$ ist der Null-R-Modul, der nur aus dem Nullelement besteht.)
(3) $\mathbb{Z}/2\mathbb{Z}$ (oder allgemeiner: $\mathbb{Z}/n\mathbb{Z}$ mit $n > 1$) ist nicht frei als $\mathbb{Z}$-Modul, denn jeder freie $\mathbb{Z}$-Modul ist isomorph zu $\mathbb{Z}^{(I)}$ für eine geeignete Indexmenge I und $\mathbb{Z}^{(I)}$ besteht entweder aus genau einem ($I = \emptyset$) oder unendlich vielen Elementen, jedoch nie aus genau 2 (respektive n) Elementen.
(4) Ist $\mathfrak{a}$ ein Ideal eines kommutativen Rings R mit Elementen $x, y \in \mathfrak{a}$, so ist $x \cdot y + (-y) \cdot x = 0$. Man überlegt sich leicht, dass $\mathfrak{a}$ als R-Modul daher nicht frei über einer Menge mit mehr als einem Element sein kann. Ist $\mathfrak{a}$ aber frei über einer (dann notwendigerweise einelementigen) Menge, so ist $\mathfrak{a}$ ein Hauptideal. Insbesondere ist das von 2 und X erzeugte Ideal von $\mathbb{Z}[X]$ als $\mathbb{Z}[X]$-Modul nicht frei (siehe [33, Beispiel 6.5]).
(5) Auch Hauptideale eines Ringes sind i.Allg. nicht automatisch frei als Modul über selbigem Ring: Man betrachte etwa den kommutativen Ring $\mathbb{Z}/4\mathbb{Z}$ mit dem von $2 + 4\mathbb{Z}$ erzeugten Hauptideal $\mathfrak{a}$. (Man überlege sich weshalb $\mathfrak{a}$ hier als $\mathbb{Z}/4\mathbb{Z}$-Modul nicht frei ist; Es scheitert hier an Nullteilerfreiheit, aber auch schon elementarer daran, dass $\mathfrak{a}$ bereits aus Kardinalitätsgründen nicht isomorph zu $(\mathbb{Z}/4\mathbb{Z})^{(I)}$ für irgendeine Menge I sein kann.)

6.5. Faktorenmoduln, Exaktheit, und Splitting

6.5.1. Faktorenmoduln. Sei M ein R-Modul und M' ein Untermodul. Wir betrachten die Faktorgruppe M/M' der zugrundeliegenden abelschen Gruppen. Auf dieser lässt sich durch

$$R \times (M/M') \longrightarrow M/M', \quad (\lambda, x + M') \longmapsto (\lambda x) + M'$$

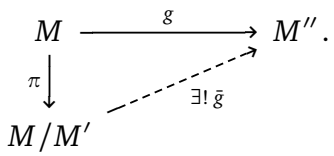
eine Skalarmultiplikation einführen[2] und man rechnet leicht nach, dass M/M' so zu einem R-Modul wird und es sich bei der kanonischen Projektion

$$\pi\colon M \longrightarrow M/M', \quad x \longmapsto x + M'$$

um einen R-Modulhomomorphismus handelt. Für eine grafische Veranschaulichung von Faktormoduln siehe Abbildung 21 auf Seite 137.

Proposition 6.13. *Seien M und M'' jeweils R-Moduln und M' ein Untermodul von M, sowie $g\colon M \to M''$ ein R-Modulhomomorphismus mit $\ker g \supseteq M'$. Dann gelten die folgenden Aussagen:*

(1) Es gibt genau einen R-Modulhomomorphismus $\bar{g}\colon M/M' \to M''$, welcher folgendes Diagramm kommutativ macht:



(2) Durch die in (1) beschriebene Zuordnung $g \mapsto \bar{g}$ erhält man einen kanonischen Isomorphismus von abelschen Gruppen

$$\{\, g \in \mathrm{Hom}_R(M, M'') : \ker g \supseteq M' \,\} \xrightarrow{\sim} \mathrm{Hom}_R(M/M', M'').$$

(Ist R kommutativ, so handelt es sich sogar um einen R-Modulisomorphismus.)

(3) Speziell in der Situation $\ker g = M'$ erhält man durch $\bar{g}$ einen Isomorphismus von $M/\ker g$ auf $\mathrm{im}\, g$.

Beweis. Diese Aussage ist im Wesentlichen bereits aus der Gruppentheorie im Rahmen des ersten Homomorphiesatzes bekannt. Es bleibt hier lediglich noch die Verträglichkeit mit der Skalarmultiplikation nachzurechnen. Die Details seien den Leserinnen und Lesern zur freiwilligen Übung überlassen. □

6.5.2. Exaktheit. Sei $(M_i)_i$ eine (endliche oder unendliche) Folge von R-Moduln zusammen mit einer Folge von R-Modulhomomorphismen $f_i\colon M_i \to M_{i-1}$. Wir visualisieren dies in der Form des Diagramms[3]

$$\ldots \longrightarrow M_{i+1} \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} M_{i-1} \longrightarrow \ldots$$

und nennen dieses Diagramm eine ***Sequenz***.[4] Diese Sequenz heißt ***exakt an der Stelle i*** (oder ***exakt bei M_i***, sofern hierdurch die Position unverwechselbar beschrieben

[2] Hierbei ist es freilich notwendig sich zunächst davon zu überzeugen, dass die Zuordnung $x+M' \mapsto (\lambda x)+M'$ unabhängig von der Wahl des Repräsentanten x der Restklasse $x+M'$ ist. Das ist aber einfach: jeder Repräsentant x' von $x+M'$ schreibt sich als $x' = x+m'$ mit einem $m' \in M'$ und dann ist wegen $\lambda m' \in M'$ auch $\lambda x' = \lambda x + \lambda m'$ ein Repräsentant der Nebenklasse $(\lambda x)+M'$.

[3] Man kann sich die Position der Indizes so merken: Der in f_i *unten* stehende Index *erniedrigt* den Index von M_i; Man bildet also von M_i nach M_{i-1} ab.

[4] Der Begriff ***Folge*** ist auch in Gebrauch.

wird), falls $\operatorname{im} f_{i+1} = \ker f_i$ gilt. Die Sequenz heißt ***exakt***, falls sie dies an jeder[5] Stelle ist.

Wir schreiben im Folgenden oft auch 0 für den ***Null-R-Modul***, also denjenigen Modul, dessen zugrundeliegende abelsche Gruppe die einelementige Gruppe ist.[6] Eine Sequenz der Form

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

nennt man auch ***kurz***. Ist diese exakt, so spricht man von einer ***kurzen exakten Sequenz***.

Lemma 6.14. *Seien M', M, M'' jeweils R-Moduln.*

(1) Die Sequenz $0 \longrightarrow M' \xrightarrow{f} M$ ist genau dann exakt, wenn f injektiv ist.

(2) Die Sequenz $M \xrightarrow{g} M'' \longrightarrow 0$ ist genau dann exakt, wenn g surjektiv ist.

(3) Die kurze Sequenz $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ ist genau dann exakt, wenn f injektiv, g surjektiv und $\operatorname{im} f = \ker g$ ist.

Beweis. Die fraglichen Aussagen sind unmittelbare Folgerungen aus der Definition von Exaktheit. □

6.5.3. Splitting. Wir betrachten nun eine kurze exakte Sequenz

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0\,.$$

Dann denken wir uns M' als mit $f(M') \subseteq M$ identifiziert und fassen M' so als Untermodul von M auf. Da g surjektiv ist, liefert Proposition 6.13 (3) unmittelbar $M/M' \cong M''$ via des durch g induzierten Isomorphismus $\bar{g}\colon M/M' \to M''$. Etwas behutsamer — ohne M' mit $f(M')$ zu identifizieren — stellt man diesen Sachverhalt durch das folgende kommutative Diagramm mit exakten Zeilen dar:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\
 & & \wr\downarrow{\scriptstyle f} & & \| & & \uparrow{\scriptstyle \bar{g}}\wr & & \\
0 & \longrightarrow & f(M') & \xrightarrow{\text{Inkl.}} & M & \xrightarrow{\pi} & M/f(M') & \longrightarrow & 0\,.
\end{array}$$

Wir stellen uns in der vorliegenden Situation in der Regel vor, dass $f(M')$ und $M/f(M')$ in gewisser Weise „kleiner“, oder wenigstens einfacher zu verstehen sind als M.

[5] An etwaigen Randstellen, also solchen i, für die entweder f_{i+1} oder f_i nicht definiert sind, wird hierbei keine Exaktheit gefordert.

[6] Man sieht selbstverständlich sofort, dass „der“ Null-R-Modul bis auf eindeutige Isomorphie eindeutig bestimmt ist und es somit gerechtfertigt ist, hier den bestimmten Artikel zu gebrauchen.

Bemerkung 6.15. Seien M_1 und M_2 zwei R-Moduln. Dann ist die folgende kurze Sequenz exakt:

$$0 \longrightarrow M_1 \xrightarrow{\iota_1} M_1 \oplus M_2 \xrightarrow{\pi_2} M_2 \longrightarrow 0\,.$$

Lemma 6.16 (Splittinglemma)**.** *Für eine kurze exakte Sequenz*

$$0 \longrightarrow M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0$$

sind folgende Aussagen äquivalent:

(1) Es gibt einen Isomorphismus $\Psi\colon M_1 \oplus M_2 \to M$, welcher das folgende Diagramm kommutativ macht:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{f} & M & \xrightarrow{g} & M_2 & \longrightarrow & 0 \\ & & \| & & \wr\uparrow\Psi & & \| & & \\ 0 & \longrightarrow & M_1 & \xrightarrow{\iota_1} & M_1 \oplus M_2 & \xrightarrow{\pi_2} & M_2 & \longrightarrow & 0\,. \end{array}$$

*(2) f besitzt eine **Retraktion** $r\colon M \to M_1$. (D.h. es existiert ein R-Modulhomomorphismus r mit $r \circ f = \mathrm{id}_{M_1}$.)*

*(3) g besitzt einen **Schnitt** $s\colon M_2 \to M$. (D.h. es existiert R-Modulhomomorphismus s mit $g \circ s = \mathrm{id}_{M_2}$.)*

Beweis. Für die Implikation (1) $\Longrightarrow$ (2) beachte man $(\pi_1 \circ \Psi^{-1}) \circ f = \pi_1 \circ \iota_1 = \mathrm{id}_{M_1}$, weswegen $r = \pi_1 \circ \Psi^{-1}$ das Gewünschte leistet.

Zum Beweis von (2) $\Longrightarrow$ (3) beachte man, dass es zu jedem $m_2 \in M_2$ wegen der Surjektivität von g ein $x \in M$ mit $g(x) = m_2$ gibt. Dieses x ist i.Allg. sicher nicht eindeutig bestimmt, aber $s(m_2) := x - (f \circ r)(x)$ hängt tatsächlich nur von m_2 ab,[7] denn ist $y \in M$ ein zweites Element mit $g(y) = m_2$, so ist $g(x - y) = 0$ und daher $x - (f \circ r)(x) = y - (f \circ r)(y)$ wegen

$$(f \circ r)|_{\ker g} = (f \circ r)|_{\mathrm{im}\, f} \overset{1}{=} (\mathrm{id}_M)|_{\mathrm{im}\, f} = (\mathrm{id}_M)|_{\ker g};$$

Hierbei ist $\overset{1}{=}$ eine bekannte mengentheoretische Konsequenz: Schränkt man den Wertebereich der *injektiven* Abbildung f auf ihr Bild $\mathrm{im}\, f$ ein, so ist die so erhaltene Abbildung bijektiv; Für diese ist r aber nach Voraussetzung ein Linksinverses und dann (hier geht die Bijektivität ein!) auch ein Rechtsinverses (vgl. auch Abbildung 19). Man verifiziert nun leicht, dass es sich bei der oben definierten Abbildung $s\colon M_2 \to M$

[7] Zur Motivation mache man sich klar, dass im Endeffekt die Gültigkeit von (2) auch (1) impliziert. Hierin erkennt man M als (im Wesentlichen) nichts anderes als $M_1 \oplus M_2$; Die Abbildungen f, g, r, s spielen hierbei die Rollen von $\iota_1, \pi_2, \pi_1, \iota_2$. Man möchte im aktuellen Beweisabschnitt also ι_2 durch die bereits bekannten Abbildungen ι_1, π_2, π_1 ausdrücken. Natürlich soll $\iota_2(m_2) = (0, m_2)$ gelten. Mit der Wahl eines π_2-Urbildes (m_1, m_2) hat man also schon fast das gewünschte Element in der Hand, muss aber noch die erste Koordinate „vergessen“. Hierfür beachte man $(0, m_2) = (m_1, m_2) - (m_1, 0) = (m_1, m_2) - (\iota_1 \circ \pi_1)(m_1, m_2)$, was sich unmittelbar in $s(m_2) := x - (f \circ r)(x)$ wiederfindet.

um einen R-Modulhomomorphismus handelt. Dieser erfüllt nach Konstruktion (mit m_2 und x wie oben)

$$\begin{aligned}(g\circ s)(m_2) &= g(s(m_2)) = g(x-(f\circ r)(x))\\ &= g(x)-((g\circ f)\circ r)(x) = m_2 - 0 = m_2,\end{aligned}$$

und also $g\circ s = \mathrm{id}_{M_2}$. Das zeigt (3).

Zum Beweis von (3) $\Longrightarrow$ (1) definieren wir $\Psi(m_1,m_2) = f(m_1)+s(m_2)$, also $\Psi = f\circ\pi_1 + s\circ\pi_2$. Dann gilt jedenfalls

$$\begin{aligned}\Psi\circ\iota_1 &= (f\circ\pi_1 + s\circ\pi_2)\circ\iota_1 = f\circ\pi_1\circ\iota_1 + s\circ\pi_2\circ\iota_1\\ &= f\circ\mathrm{id}_{M_1} + s\circ 0_{M_1\to M_2} = f,\end{aligned}$$

und in ähnlicher Weise $g\circ\Psi = \pi_2$. Also kommutiert das Diagramm in (1) und es verbleibt lediglich der Nachweis der Injektivität und Surjektivität von Ψ.
Sei $(m_1,m_2)\in M_1\oplus M_2$ mit $\Psi(m_1,m_2)=0$ gegeben. Dann ist $f(m_1) = s(-m_2)$ und Vorschalten von g liefert

$$0 = (g\circ f)(m_1) = (g\circ s)(-m_2) = -m_2.$$

Wir haben also bereits $f(m_1) = f(m_1)+s(0) = \Psi(m_1,m_2) = 0$; Da f injektiv ist, folgt $m_1 = 0$ und insgesamt $(m_1,m_2) = (0,0)$, weswegen Ψ injektiv ist.
Sei $x\in M$ gegeben. Dann ist $x-(s\circ g)(x)\in\ker g = \mathrm{im}\, f$. Also gibt es $m_1\in M_1$ mit

$$f(m_1) = x-(s\circ g)(x) \quad \text{bzw.} \quad x = f(m_1)+s(g(x)) = \Psi(m_1, g(x))\in\mathrm{im}\,\Psi,$$

was die Surjektivität von Ψ beweist. □

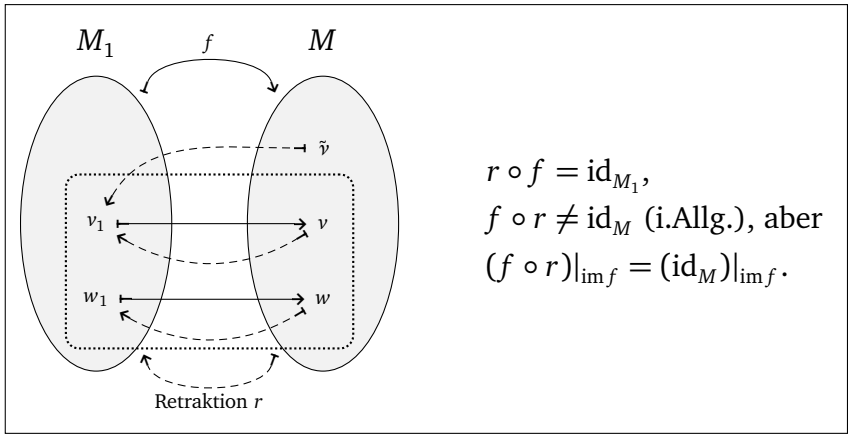


Abbildung 18. Zum Beweis von Lemma 6.16: Bei der Retraktion r zu f handelt es sich um eine linksinverse Abbildung zu f, jedoch nicht notwendigerweise um eine Rechtsinverse (in der hier gezeichneten Situation ist $(f\circ r)(\tilde{v}) = v \neq \tilde{v}$ und also $f\circ r\neq\mathrm{id}_M$). Auf der Menge $\mathrm{im}\, f\subseteq M$ stimmt die Abbildung $f\circ r$ hingegen doch mit der identischen Abbildung überein.

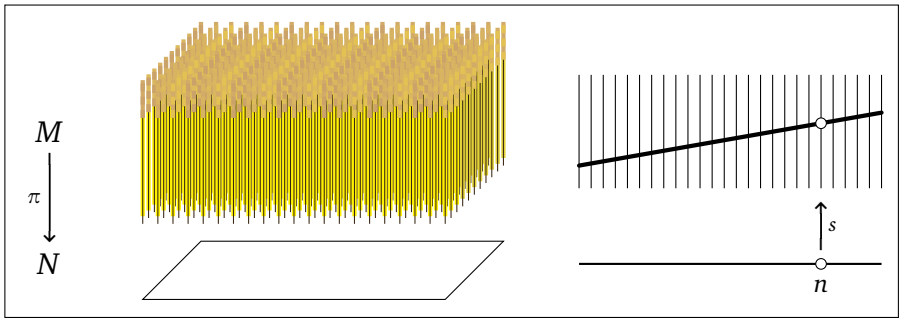


Abbildung 19. Zum Begriff von Schnitten und Retraktionen. Man stelle sich $\pi\colon M \to N$ als eine Projektion von einem größeren Modul M auf einen kleineren Modul N vor. Über jedem Punkt n von N stelle man sich die Faser $\pi^{-1}(n) = m + \ker r$ (mit geeignetem $m \in M$) wie einen Getreidehalm auf einem Getreidefeld ($= N$) vor. Ein Schnitt s von r wählt dann zu jedem Halm einen „Schnittpunkt“ $s(n) \in r^{-1}(n)$ aus. Dann gilt automatisch $\pi \circ s = \mathrm{id}_N$. Anschaulich gesprochen, setzt s hierbei einen „Schnitt durch das Getreidefeld“. Stellt man sich nun N als Teilmenge von M vor (anschaulich: das Getreidefeld berühre den Boden), so kann man den „Boden“ N auch als Schnitt durch das Getreidefeld auffassen und die Projektion π drückt alle Halme auf die Stelle im Boden aus der diese wachsen. — Hier „zieht“ (retrahiert) man die Halme zurück.

Für eine anschauliche Interpretation der Begriffe *Schnitt* und *Retraktion* sei auf Abbildung 19 verwiesen. Für interessante analytische Anwendung von Schnitten in der komplexen Analysis zur Fortsetzung holomorpher Funktionen, siehe etwa [32, Kapitel 4].

Gilt eine (und dann alle) der äquivalenten Bedingungen aus Lemma 6.16, so sagt man, dass die kurze exakte Sequenz

$$0 \longrightarrow M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0$$

zerfalle oder ***spalte*** (Engl.: *split*).

Beispiel 6.17. Wir betrachten die kurze exakte Sequenz

$$0 \longrightarrow 2\mathbb{Z} \xhookrightarrow{\text{Inkl.}} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0\,.$$

Diese zerfällt offensichtlich nicht, da es zu π keinen Schnitt gibt: Ja, überhaupt gar keinen $\mathbb{Z}$-Modulhomomorphismus $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$, der nicht bereits die Nullabbildung ist.

In obigem Beispiel gilt $\mathbb{Z} \ncong 2\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})$, was offensichtlich auch etwaiges Zerfallen der fraglichen kurzen exakten Sequenz ausschließt. Dass hingegen umgekehrt aus

$M \cong M_1 \oplus M_2$ i.Allg. *nicht* folgt, dass die kurze exakte Sequenz

$$0 \longrightarrow M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0$$

zerfällt, wird durch das nächste Beispiel illustriert; Zerfallen einer kurzen exakten Sequenz ist mehr als die bloße Isomorphie $M \cong M_1 \oplus M_2$ und behauptet nämlich auch, dass f und g für M die Rollen von ι_1 bzw. π_2 spielen.

Beispiel 6.18. Wir betrachten die kurze exakte Sequenz

$$0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z} \oplus \bigoplus_{\mathbb{N}} (\mathbb{Z}/2\mathbb{Z}) \xrightarrow{g} \bigoplus_{\mathbb{N}} (\mathbb{Z}/2\mathbb{Z}) \longrightarrow 0$$

mit $\mathbb{Z}$-Modulhomomorphismen f, g gegeben durch

$$f(x) = (2x, 0_{\mathbb{Z}/2\mathbb{Z}}, 0_{\mathbb{Z}/2\mathbb{Z}}, \ldots), \quad g(x, y_1, y_2, \ldots) = (x + 2\mathbb{Z}, y_1, y_2, \ldots).$$

Man beachte, dass der mittlere $\mathbb{Z}$-Modul in der Sequenz die direkte Summe der äußeren beiden Moduln ist. Trotzdem zerfällt die fragliche kurze exakte Sequenz nicht! — Denn sonst müsste es zu g einen Schnitt

$$s\colon \bigoplus_{\mathbb{N}} (\mathbb{Z}/2\mathbb{Z}) \longrightarrow \mathbb{Z} \oplus \bigoplus_{\mathbb{N}} (\mathbb{Z}/2\mathbb{Z})$$

geben: $g \circ s = \mathrm{id}$. Dieser müsste dann jedoch das Element $v = (1_{\mathbb{Z}/2\mathbb{Z}}, 0_{\mathbb{Z}/2\mathbb{Z}}, 0_{\mathbb{Z}/2\mathbb{Z}}, \ldots)$ auf ein Element in $g^{-1}(v) = \{(x, 0_{\mathbb{Z}/2\mathbb{Z}}, 0_{\mathbb{Z}/2\mathbb{Z}}, \ldots) : x \text{ ungerade}\}$ abbilden, aber diese Menge enthält gar kein Element endlicher Ordnung.

6.5.4. Splitting bei freien Moduln. Wenn es sich in der Situation von Lemma 6.16 bei M_2 um einen freien R-Modul handelt, so hat man „genug Freiheit“, um einen Schnitt von g zu konstruieren, und so das Zerfallen der kurzen exakten Sequenz in Lemma 6.16 gewährleisten zu können:

Satz 6.19. *Sei I eine Indexmenge und*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} R^{(I)} \longrightarrow 0$$

eine kurze exakte Sequenz. Dann sind die drei (äquivalenten) Aussagen (1)–(3) aus dem Splittinglemma (Lemma 6.16) erfüllt. Insbesondere ist $M \cong M' \oplus R^{(I)}$.

Beweis. Es genügt Lemma 6.16 (3) nachzuweisen. Wir wollen also eine Abbildung $s\colon R^{(I)} \to M$ mit $g \circ s = \mathrm{id}_{R^{(I)}}$. Da g gemäß Lemma 6.14 (2) surjektiv ist, gibt es zu jedem $i \in I$ ein Element $S(i) \in M$ mit $g(S(i)) = \boldsymbol{i}$. So erhalten wir eine Abbildung $S\colon I \to M$ und Proposition 6.10 liefert nun einen R-Modulhomomorphismus $s\colon R^{(I)} \to M$ mit $s(\boldsymbol{i}) = S(i)$:

$$\begin{array}{ccccc} M & & \xrightarrow{\quad g \quad} & & R^{(I)} \longrightarrow 0\,. \\ {\scriptstyle S}\uparrow & \nwarrow^{s} & & & \uparrow{\scriptstyle \mathrm{id}_{R^{(I)}}} \\ I & & \xrightarrow[i \mapsto \iota_i(1_R) = \boldsymbol{i}]{} & & R^{(I)} \end{array}$$

Ferner ist

$$(g \circ s)(\boldsymbol{i}) = g(s(\boldsymbol{i})) = g(S(i)) = \boldsymbol{i} = \mathrm{id}_{R^{(I)}}(\boldsymbol{i})$$

und zusammen mit der Eindeutigkeitsaussage in Proposition 6.10 folgt hieraus $g \circ s = \mathrm{id}_{R^{(I)}}$, wie gewünscht. □

In der Modultheorie gibt es den Begriff eines ***projektiven Moduls*** und auch den dazu dualen Begriff eines ***injektiven Moduls***. Beide Begriffe sind ubiquitär in einem Teilgebiet der Algebra, welches als ***homologische Algebra*** bezeichnet wird. Dieses wiederum erwuchs aus der algebraischen Topologie und homologische Methoden durchziehen mittlerweile weite Teile der Mathematik von Topologie, Gruppentheorie, algebraischer Geometrie etc. Eine mögliche Definition für einen R-Modul P projektiv genannt zu werden, lautet, dass jede kurze exakte Sequenz

$$0 \longrightarrow M' \longrightarrow M \longrightarrow P \longrightarrow 0$$

von R-Moduln spaltet. Mit dieser Sprache besagt Satz 6.19 also kurz: *alle freien Moduln sind projektiv*.

KAPITEL 7

Matrizen und Smith-Normalform

Unser Ziel in diesem Kapitel ist ein genaueres Verständnis von Modulhomomorphismen zwischen freien Moduln über einem Hauptidealbereich, was uns zur *Smith-Normalform* führt. In Kapitel 8 lässt sich dieses Verständnis dann auf nicht notwendigerweise freie Moduln über einem Hauptidealbereich ausdehnen.

Die Darstellung in den späteren Abschnitten orientiert sich lose an [1] und [30]. Für mehr Informationen ist vielleicht auch ein Blick in [2] oder [7] hilfreich.

7.1. Noethersche Ringe und Moduln

In § 6.4 hatten wir freie Moduln als die naheliegenste Verallgemeinerung von Vektorräumen mit gewählter Basis behandelt. Aus der *linearen Algebra* weiß man, dass unter Berufung auf das *Zornsche Lemma*, Lemma 2.14 gezeigt werden kann, dass jeder Vektorraum eine Basis besitzt. Ganz anders verhält es sich mit Freiheit von Moduln. Man sollte die Eigenschaft eines Moduls frei zu sein, als eine sehr seltene Eigenschaft betrachten. Schlimmer noch: Freiheit geht schnell verloren. Die Beispiele $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, $n \mapsto n + 2\mathbb{Z}$, und $\langle 2, X\rangle \subset \mathbb{Z}[X]$ aus Beispiel 6.12 zeigen nämlich, dass weder homomorphe Bilder freier Moduln, noch Untermoduln freier Moduln selbst frei zu sein brauchen. Welcher dieser beiden Defekte schlussendlich für die Theorie unbequemer ist, braucht hier nicht diskutiert werden; Schließlich scheitert es ohnehin an beiden Stellen. Es drängt sich also die Frage auf, ob es eine andere „Endlichkeitsbedingung“ für Moduln gibt, welche ihre Praxistauglichkeit durch größere Robustheit unter üblichen Konstruktionen der Modultheorie gewinnt (z.B. Faktorbildung, Übergang zu Untermoduln, etc.). Eine derartige Endlichkeitsbedingung ist Thema des vorliegenden Abschnittes.

In diesem gesamten Abschnitt sei R stets ein *kommutativer* Ring. (Man käme auch ohne die Kommutativitätsvoraussetzung aus, müsste dann aber vorsichtiger zwischen Links-, Rechts-, und beidseitigen Idealen unterscheiden.) Ein R-Modul M heißt ***noethersch***, falls jede aufsteigende Kette

$$M_0 \subseteq M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$$

von R-Untermoduln von M ab einem gewissen Punkt stationär wird, also $M_n = M_{n+1} = \dots$ für ein n erfüllt. Ein kommutativer Ring R heißt bekanntlich ***noethersch***, falls dieser als Modul über sich selbst noethersch ist; Da Untermoduln in diesem Fall genau die Ideale von R sind, ist dies äquivalent zu der aus der *Einführung in die*

Algebra bekannten Definition des Begriffs „noethersch.“ Wie dort beweist man leicht das folgende Ergebnis (vgl. [33, Satz 8.11] oder [16, Satz 2.8.8]):

Satz 7.1. *Sei R ein kommutativer Ring. Für einen R-Modul M sind die folgenden Eigenschaften äquivalent:*

(1) M ist noethersch;
(2) Jede nichtleere Menge von Untermoduln von M besitzt (bezüglich der durch Inklusion induzierten partiellen Ordnung) ein maximales Element;
(3) Alle Untermoduln von M sind endlich erzeugt.

Beweis. (1) $\Longrightarrow$ (2): Wir argumentieren via Kontraposition; Ist (2) falsch, so kann man leicht eine unendliche, nicht-stationäre Kette von Untermoduln von M konstruieren, weshalb M dann nicht noethersch ist.

(2) $\Longrightarrow$ (3): Zu gegebenem Untermodul M' von M wende man (2) an, um ein maximales Element in der Menge der endlich erzeugten Untermoduln von M' zu finden. Man sieht leicht, dass dieses dann mit M' übereinstimmen muss. Also folgt (3).

(3) $\Longrightarrow$ (1): Sei jeder Untermodul von M endlich erzeugt. Betrachte eine beliebige aufsteigende Kette $M_0 \subseteq M_1 \subseteq M_2 \subseteq \ldots$ und definiere $M_\infty = \bigcup_i M_i$. Dabei handelt es sich um einen Untermodul von M und dieser ist nach Voraussetzung endlich erzeugt, etwa $M_\infty = \langle x_0, \ldots, x_j \rangle$. Nun gibt es ein n für welches M_n alle diese Erzeuger enthält. Ab diesem Punkt ist die Kette dann aber stationär. □

Unser nächstes Ergebnis gibt ein brauchbares Werkzeug um für einen Modul M die Noether-Eigenschaft nachzuweisen, wenn sich dieser in geeigneter Weise in Teile zerlegen lässt, für die die Noether-Eigenschaft bereits bekannt ist.

Proposition 7.2. *Sei R ein kommutativer Ring.*

(1) Ist $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ eine kurze exakte Sequenz von R-Moduln, so ist M genau dann noethersch, wenn dies auf M' und M'' zutrifft.
(2) Sind $M_1, \ldots, M_n$ noethersche R-Moduln, so ist auch $\bigoplus_{i=1}^n M_i$ noethersch.

Beweis. Zum Beweis von (1) seien M' und M'' beide noethersch und

$$M_\bullet\colon M_0 \subseteq M_1 \subseteq M_2 \subseteq \ldots$$

eine aufsteigende Kette von R-Untermoduln von M. Die Ketten

$$f^{-1}(M_0) \subseteq f^{-1}(M_1) \subseteq f^{-1}(M_2) \subseteq \ldots \quad \text{und} \quad g(M_0) \subseteq g(M_1) \subseteq g(M_2) \subseteq \ldots$$

sind beide ab einem gewissen Index stationär; Ab einem Index, ab dem beide Ketten gleichzeitig stationär sind, ist dann aber auch die Kette $M_\bullet$ von dort an stationär. (Wegen der Exaktheit. — Da die Kette unter g ab dem betrachteten Punkt stationär ist, kann ein Zuwachs der Ausgangskette nur durch Hinzukommen von Elementen im Kern von g passieren, aber das ist wegen $\ker g = \operatorname{im} f$ und der Stationarität der f^{-1}-Kette ausgeschlossen.)

Als nächstes sei M noethersch. Eine aufsteigende Kette in M' (oder M'') führt durch Abbildung mit f (oder Zurückziehen mit g^{-1}) auf eine (dann notwendigerweise

schließlich stationäre) Kette in M. Hieraus erhält man leicht, dass die ursprüngliche Kette schließlich stationär ist. Zum Beweis von (2) benutze man die offensichtliche kurze exakte Sequenz

$$0 \longrightarrow M_n \xrightarrow[x_n \mapsto (0,\ldots,0,x_n)]{\iota_n} \bigoplus_{i=1}^{n} M_i \xrightarrow[(x_1,\ldots,x_{n-1},x_n)\mapsto(x_1,\ldots,x_{n-1})]{(\pi_1,\ldots,\pi_{n-1})} \bigoplus_{i=1}^{n-1} M_i \longrightarrow 0\,.$$

und führe eine Induktion mittels (1). □

Korollar 7.3. *Sei R ein (kommutativer) noetherscher Ring. Dann sind alle endlich erzeugten R-Moduln noethersch.*

Beweis. Jeder endlich erzeugte R-Modul M passt in eine kurze exakte Sequenz

$$0 \longrightarrow \ker g \xhookrightarrow{\text{Inkl.}} \bigoplus_{i=1}^{n} R \xrightarrow{g} M \longrightarrow 0\,.$$

Die Aussage folgt nun aus Proposition 7.2. □

Beispiele 7.4.

(1) Jeder R-Modul mit nur endlich vielen Untermoduln ist noethersch. Insbesondere sind endliche Ringe und endliche R-Moduln noethersch.
(2) Jeder Körper ist noethersch (beachte (1)) und jeder endlich-dimensionale Vektorraum ist noethersch (via Korollar 7.3).
(3) Jeder Hauptidealbereich ist noethersch (denn alle seine Ideale sind endlich erzeugbar — nämlich stets von *einem* Element).
(4) Der Ring $\mathbb{Z}$ der ganzen Zahlen ist ein Hauptidealbereich und daher noethersch und jeder Faktorring $\mathbb{Z}/n\mathbb{Z}$ ist noethersch (wegen (1), oder auch mittels Proposition 7.2 (1)).
(5) Der ***hilbertsche Basissatz*** (siehe [33, Satz 8.13] oder [16, § 3.2]): Ist R noethersch, so ist auch der Polynomring $R[X]$ noethersch, und damit (mittels Induktion) auch der Polynomring $R[X_1,\ldots,X_n]$ in n Unbestimmten. Insbesondere, mit (2), ist der Polynomring (in n Unbestimmten) über einem Körper noethersch.
(6) Unendlich-dimensionale Vektorräume lassen sich nach Definition nicht von endlich vielen Elementen erzeugten. Demnach sind diese nicht noethersch.
(7) Sei R ein kommutativer Ring. Der Polynomring $R' = R[\{X_i : i \in \mathbb{N}\}]$ in abzählbar vielen Variablen ist nicht noethersch. Man überlegt sich etwa, dass das Ideal $\langle X_i : i \in \mathbb{N}\rangle$ nicht endlich erzeugt ist. Dennoch ist R' als R'-Modul endlich erzeugt (man wähle $1_{R'}$ als Erzeuger).

Bemerkung. Aus den obigen Beispielen folgt, dass ein K-Vektorraum V genau dann endlich-dimensional ist, wenn dieser noethersch ist. Ist $\dim_K V < \infty$, so ist

$$\dim_K V = \sup\{\, n \in \mathbb{N} : \exists \text{ Kette von Unterräumen } M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_n \text{ von } V \,\}.$$

In diesem Sinne mag man die Noether-Eigenschaft als eine mögliche Verallgemeinerung des Begriffs der Endlichdimensionalität von Vektorräumen auf die Situation von Moduln ansehen. Da auch nicht-freie Moduln noethersch sein können, ist die Noether-Eigenschaft oft brauchbarer (weil weniger restriktiv), als etwa die Eigenschaft frei über einer endlichen Menge zu sein.

7.2. Homomorphismen zwischen freien Moduln, Matrixdarstellung

Sei R ein *kommutativer* Ring. Mittels Korollar 6.8 und Proposition 6.10 erhalten wir eine Serie kanonischer R-Modulisomorphismen[1]

$$\begin{aligned}\mathrm{Hom}_R(R^m,R^n) &= \mathrm{Hom}_R\Big(\bigoplus_{j=1}^{m} R, \bigoplus_{i=1}^{n} R\Big) = \mathrm{Hom}_R\Big(\bigoplus_{j=1}^{m} R, \prod_{i=1}^{n} R\Big)\\ &\cong \prod_{i=1}^{n} \mathrm{Hom}_R\Big(\bigoplus_{j=1}^{m} R, R\Big) \cong \prod_{i=1}^{n}\prod_{j=1}^{m} \mathrm{Hom}_R(R,R)\\ &\cong \prod_{i=1}^{n}\prod_{j=1}^{m} \mathrm{Abb}(\{\bullet\},R) \cong \prod_{i=1}^{n}\prod_{j=1}^{m} R =: R^{n\times m}.\end{aligned}$$

(Man beachte, dass die Kommutativität von R hier wichtig war, um hier sogar von R-Modulisomorphismen, statt lediglich Isomorphismen von abelschen Gruppen, sprechen zu dürfen.) Der so durch Zusammensetzung erhaltene R-Modulisomorphismus hat die Gestalt

$$[\,\cdot\,]_m^n\colon \mathrm{Hom}_R(R^m,R^n) \longrightarrow R^{n\times m}, \quad f \longmapsto [f]_m^n := \Big(\big(\pi_i^{(n)} \circ f \circ \iota_j^{(m)}\big)(1_R)\Big)_{i,j=1}^{n,m}$$

mit den bekannten Projektions- und Inklusionsabbildungen

$$\pi_i^{(n)}\colon R^n \longrightarrow R, \quad \iota_j^{(m)}\colon R \longrightarrow R^m.$$

(Zum besseren Verständnis: $\iota_j^{(m)}(1_R)$ liefert das j-te Standardbasiselement im freien R-Modul R^m, dessen Bild unter f dann berechnet wird. Anschließend stellt man dieses Bild — ein Element des freien R-Moduls R^n — vermöge Projektion gemäß der Standardbasis des R^n dar. Dieses Vorgehen ist völlig analog zu der aus der linearen Algebra bekannten Methode zur Berechnung von *Darstellungsmatrizen* für lineare Abbildungen zwischen Vektorräumen bezüglich *bereits gewählter* Basen.)

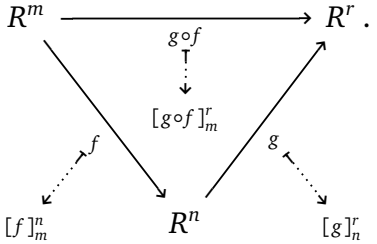
Die Elemente von $R^{n\times m}$ nennen wir ***Matrizen*** (Singular: die ***Matrix***), und manchmal auch ***($n\times m$)-Matrizen***, um den Bezug auf n und m zu betonen. Eine $n\times m$-Matrix notieren wir (wie in der linearen Algebra) in Tabellenform mit n Zeilen und m Spalten:

$$\begin{array}{c}\text{Zeilen}\\ \downarrow\end{array}\begin{pmatrix} A_{11} & \cdots & A_{1m}\\ \vdots & & \vdots\\ A_{n1} & \cdots & A_{nm}\end{pmatrix}.$$

$$\xrightarrow{\text{Spalten}}$$

[1] Hierbei ist wichtig, dass wir die freien Moduln R^m und R^n jeweils als mit bereits gewählten Basen ausgestattet sehen: $(1_R, 0_R, 0_R, \ldots)$, $(0_R, 1_R, 0_R, \ldots)$, etc.

Durch die Abbildungen $[\,\cdot\,]_m^n$ $(m,n \in \mathbb{N}_0)$ haben wir nun Vorschriften, die R-Modulhomomorphismen von R^m nach R^n in sehr konkrete Objekte überführen. Natürlich kann man solche Homomorphismen auch verketten, sofern Zielbereich und Definitionsbereich geeignet zusammenpassen. Wir betrachten daher nun ein kommutatives Diagramm der Form



Dies legt die Definition

$$[g\,]_n^r \cdot [f\,]_m^n := [g \circ f\,]_m^r$$

nahe. *Wie sieht dieses Produkt konkret aus?* Wir benutzen die Formel

$$\mathrm{id}_{R^n} = \sum_{i=1}^{n} \iota_i^{(n)} \circ \pi_i^{(n)}$$

im (s,j)-ten Eintrag C_{sj} der Matrix $C = [g \circ f\,]_m^r$ (mit $1 \le s \le r$ und $1 \le j \le m$)

$$C_{sj} = \big(\pi_s^{(r)} \circ g \circ f \circ \iota_j^{(m)}\big)(1_R) = \big(\pi_s^{(r)} \circ g \circ \mathrm{id}_{R^n} \circ f \circ \iota_j^{(m)}\big)(1_R),$$

und erhalten so

$$\begin{aligned} C_{sj} &= \Big(\pi_s^{(r)} \circ g \circ \Big(\textstyle\sum_i \iota_i^{(n)} \circ \pi_i^{(n)}\Big) \circ f \circ \iota_j^{(m)}\Big)(1_R) \qquad (\text{mit } \textstyle\sum_i = \sum_{i=1}^{n}) \\ &= \Big(\textstyle\sum_i \Big(\big(\pi_s^{(r)} \circ g \circ \iota_i^{(n)}\big) \circ \big(\pi_i^{(n)} \circ f \circ \iota_j^{(m)}\big)\Big)\Big)(1_R) \\ &= \textstyle\sum_i \big(\pi_s^{(r)} \circ g \circ \iota_i^{(n)}\big)\Big(\big(\pi_i^{(n)} \circ f \circ \iota_j^{(m)}\big)(1_R)\Big). \end{aligned}$$

Die inneren Terme sind jeweils von der Bauart $u(r)$ mit einem R-Modulhomomorphismus $u\colon R \to R$. Wir schreiben nun r als $r = r \cdot 1_R$ und fassen den ersten Faktor als *Skalar* auf, welches wir sodann aus dem Argument von u herausziehen dürfen: $u(r) = u(r \cdot 1_R) = ru(1_R)$. Da die R-Skalarmultiplikation auf R nichts anderes als die Multiplikation der Ringstruktur von R ist und R ja als kommutativ vorausgesetzt ist, dürfen wir sogar $u(r) = u(1_R)r$ schreiben. Damit ergibt sich dann

$$C_{sj} = \sum_i \big(\pi_s^{(r)} \circ g \circ \iota_i^{(n)}\big)(1_R) \cdot \big(\pi_i^{(n)} \circ f \circ \iota_j^{(m)}\big)(1_R).$$

Insgesamt hat man also

$$[g\,]_n^r \cdot [f\,]_m^n = (C_{sj})_{s,j=1}^{r,m} = \Big(\sum_i B_{si}A_{ij}\Big)_{s,j=1}^{r,m} \quad \text{mit} \quad B = [g\,]_n^r, \quad A = [f\,]_m^n.$$

Das ist die wohl-bekannte Formel für ***Matrixmultiplikation***! (Siehe auch Abbildung 20 auf Seite 122.)

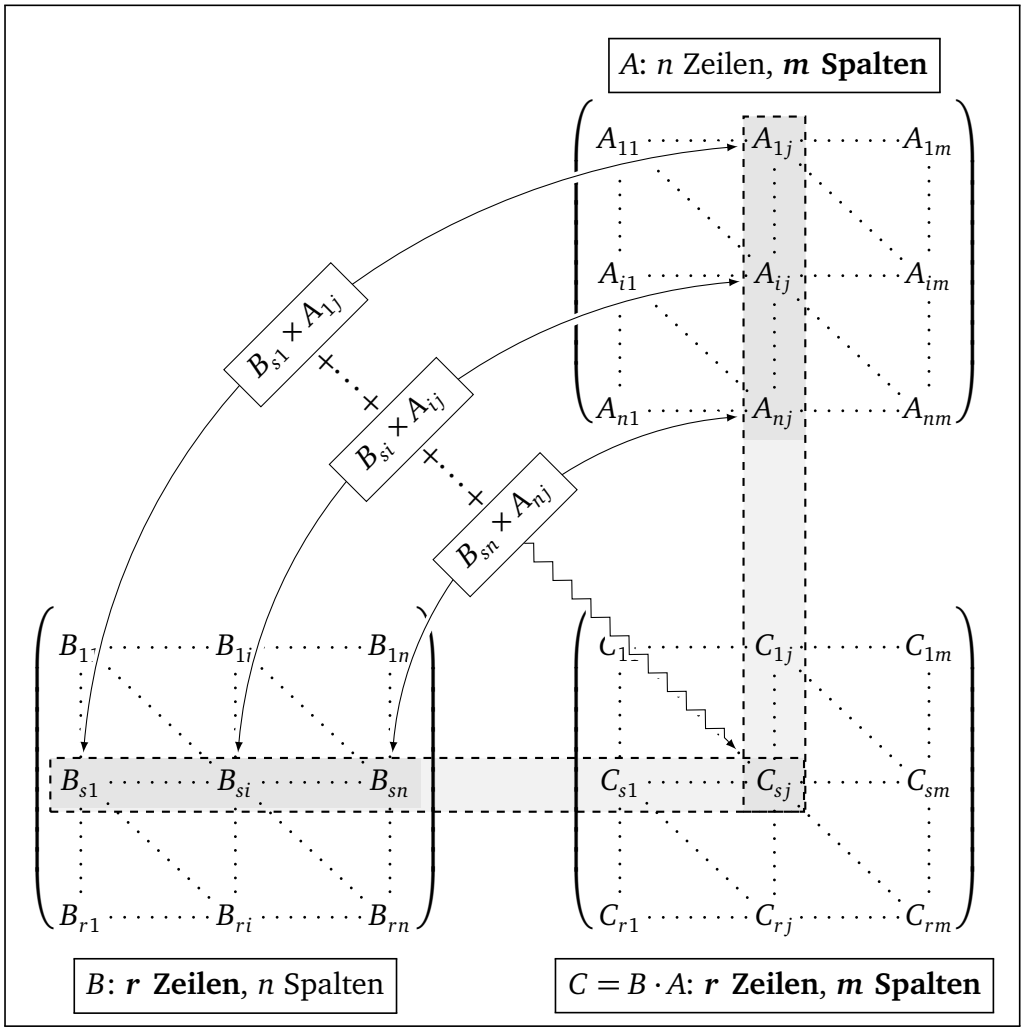


Abbildung 20. Veranschaulichung der Matrixmultiplikation nach dem bekannten Schema „Zeile mal Spalte“.
(Adaptiert nach Alain Matthes, `https://www.TeXample.net`.)

Die Abbildung $[\,\cdot\,]_m^n$ kann man auch leicht *explizit umkehren*. Zu einer Matrix $A \in R^{n\times m}$ betrachten wir nun die Abbildung

$$f_A \colon R^m \longrightarrow R^n, \quad x \longmapsto A \cdot x,$$

wobei wir hier stillschweigend Spaltenmatrizen aus $R^{n\times 1}$ mit Elementen von R^n identifizieren (und analog für $R^{m\times 1}$) und für „$\cdot$“ in obiger Formel die eben definierte Matrixmultiplikation benutzen. Man rechnet leicht nach, dass es sich bei f_A um einen R-Modulhomomorphismus handelt. Außerdem rechnet man ebenfalls leicht nach,

dass die so erhaltenen Abbildungen

$$\mathrm{Hom}_R(R^m,R^n) \underset{f_A \longleftarrow\shortmid A}{\overset{f \longmapsto [f]_m^n}{\underset{\longleftarrow}{\overset{\longrightarrow}{\sim}}}} R^{n\times m}$$

zueinander inverse R-Modulisomorphismen sind.

Bemerkung. Zusammenfassend sehen wir also, dass das Diagramm

$$\begin{array}{ccc} \mathrm{Hom}_R(R^n,R^r)\times\mathrm{Hom}_R(R^m,R^n) & \xrightarrow{(g,f)\mapsto g\circ f} & \mathrm{Hom}_R(R^m,R^r) \\ \wr\downarrow (g,f)\mapsto([g]_n^r,[f]_m^n) & & \wr\downarrow h\mapsto[h]_m^r \\ R^{r\times n}\times R^{n\times m} & \xrightarrow{(B,A)\mapsto B\cdot A} & R^{r\times m} \end{array}$$

kommutiert. Überdies bildet $\mathrm{Hom}_R(R^n,R^n)$ mit der Verknüpfung von Abbildungen als Multiplikation einen (i.Allg. nicht kommutativen) Ring, und das obige Diagramm zeigt für $n=m=r$, dass $\mathrm{Hom}_R(R^n,R^n)$ als Ring isomorph zu $R^{n\times n}$ ist.

7.3. Smith-Normalform: Existenz

Im vorangegangenen Abschnitt hatten wir gesehen, dass sich R-Modulhomomorphismen zwischen R^m und R^n mittels Matrizen beschreiben lassen: Homomorphismen und Matrizen sind jeweils nur verschiedene Seiten ein und derselben Medaille! In diesem Abschnitt zeigen wir, dass sich diese Matrizen auf eine gewisse Normalform bringen lassen. Auf der Matrizen-Seite zeigen sich deratige Untersuchungen in einem mehr oder minder algorithmischen Gewandt. Den Leserinnen und Lesern sollte diesbezüglich aber schon aus der *linearen Algebra* bekannt sein, dass auf der Homomorphismen-Seite derartige Ergebnisse *tiefe* Einblicke in die *Struktur* von $\mathrm{Hom}_R(R^m,R^n)$ erlauben. Die weitere Substantiierung dieser Behauptung ist Hauptinhalt von Kapitel 8, wo wir durch Diskussion diverser Anwendungen auch sehen werden, *weshalb* ein Verständnis von $\mathrm{Hom}_R(R^m,R^n)$ überhaupt wünschenswert ist. Für den Rest des Kapitels stellen wir die Matrizen-Seite in den Vordergrund.

Eine Matrix $A\in R^{n\times n}$ heißt ***invertierbar***, falls Sie als Element des Rings $R^{n\times n}$ eine Einheit ist. Wie in der linearen Algebra kann man ***elementare Zeilen- und Spaltenumformungen*** einführen. Diese bestehen aus

- Addition einer mit einem beliebigen Element des zugrundeliegenden Rings multiplizierte Zeile/Spalte zu einer anderen Zeile/Spalte,
- Vertauschen zweier Zeilen oder Vertauschen zweier Spalten,
- Multiplikation einer Zeile/Spalte mit einer Einheit des zugrundeliegenden Rings.

Zeilenumformungen lassen sich durch Multiplikation *von links* mit geeigneten Matrizen (sogenannten ***Elementarmatrizen***) realisieren. Beispielsweise haben wir in

hoffentlich selbsterklärender *Blockschreibweise* für $i < j$

$$\begin{pmatrix} 1_R & & & & \\ & \ddots & & & \\ & & 1_R & \cdots & \lambda \\ & & & \ddots & \vdots \\ & & & & 1_R \end{pmatrix} \cdot \begin{pmatrix} \text{---} & A_{1\bullet} & \text{---} \\ & \vdots & \\ \text{---} & A_{i\bullet} & \text{---} \\ & \vdots & \\ \text{---} & A_{j\bullet} & \text{---} \\ & \vdots & \\ \text{---} & A_{n\bullet} & \text{---} \end{pmatrix} = \begin{pmatrix} \text{---} & A_{1\bullet} & \text{---} \\ & \vdots & \\ - & A_{i\bullet} + \lambda A_{j\bullet} & - \\ & \vdots & \\ \text{---} & A_{j\bullet} & \text{---} \\ & \vdots & \\ \text{---} & A_{n\bullet} & \text{---} \end{pmatrix}. \tag{7.1}$$

Wir verzichten darauf die übrigen Elementarmatrizen explizit auszuschreiben; Ist man daran interessiert, wie diese konkret aussehen, so braucht man nur die gewünschte Umformung auf die ***n*×*n*-Einheitsmatrix** $\mathbf{1}_n$ loszulassen. Alternativ kann man diese auch sehr prägnant wie folgt beschreiben: Sei E_{ij} die $n\times n$-Matrix, welche nur aus Nulleinträgen besteht, bis auf eine Eins im Eintrag der zur i-ten Spalte und j-ten Zeile gehört. Die folgende Liste gibt $n\times n$-Matrizen und deren Wirkung bei Linksmultiplikation an eine andere Matrix an ($i \neq j$):

- $\mathbf{1}_n + \lambda E_{ij}$: Addition des λ-fachen der j-ten Zeile zur i-ten Zeile (siehe (7.1));
- $\mathbf{1}_n + E_{ij} + E_{ji} - E_{ii} - E_{jj}$: Vertauschen der i-ten und j-ten Spalte;
- $\mathbf{1}_n + (\lambda - 1_R)E_{ii}$: Multiplikation der i-ten Zeile mit λ.

Man überlegt sich leicht, dass sämtliche Elementarmatrizen invertierbar sind und sich Spaltenumformungen durch Multiplikation *von rechts* mit der zur analogen Zeilenumformung gehörigen Elementarmatrix schreiben lassen.

Zusätzlich zu den Elementarmatrizen betrachten wir zu $x, y, \lambda, \mu \in R$ mit $1_R = x\lambda + y\mu$ noch Matrizen der Bauart

$$\left(\begin{array}{cc|ccc} x & -\mu & & & \\ y & \lambda & & & \\ \hline & & 1_R & & \\ & & & \ddots & \\ & & & & 1_R \end{array}\right). \tag{7.2}$$

(Die augenscheinliche Sonderstellung der ersten beiden Zeilen/Spalten ist hier tatsächlich irrelevant, da man den oberen Block mit Zeilen- und Spaltenvertauschungen geeignet umher bewegen kann.) Auch diese Matrizen sind invertierbar, wie man sich leicht anhand der Formel

$$\begin{pmatrix} \lambda & \mu \\ -y & x \end{pmatrix} \cdot \begin{pmatrix} x & -\mu \\ y & \lambda \end{pmatrix} = \begin{pmatrix} 1_R & \\ & 1_R \end{pmatrix}$$

überlegt (hierbei geht $1_R = x\lambda + y\mu$ ein).

Bemerkung. Sei R ein kommutativer Ring. Wir schreiben im Folgenden kurz $1 = 1_R$ und $0 = 0_R$. Sind wieder $x, y, \lambda, \mu \in R$ mit $1 = x\lambda + y\mu$ gegeben, aber x zusätzlich

als invertierbar vorausgesetzt, so lässt sich die Matrix

$$A = \begin{pmatrix} x & -\mu \\ y & \lambda \end{pmatrix}$$

als ein Produkt von Elementarmatrizen schreiben: In der Tat erhält man durch Sukzessive Zeilenumformungen

$$\begin{aligned} A &\rightsquigarrow \begin{pmatrix} 1 & -\mu/x \\ y & \lambda \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & -\mu/x \\ 0 & \lambda + y\mu/x \end{pmatrix} = \begin{pmatrix} 1 & -\mu/x \\ 0 & 1/x \end{pmatrix} \\ &\rightsquigarrow \begin{pmatrix} 1 & -\mu/x \\ 0 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Die erste Zeilenumformung (Multiplikation der ersten Zeile mit $1/x \in R^\times$) wird durch Linksmultiplikation mit der Elementarmatrix

$$\begin{pmatrix} 1/x & \\ & 1 \end{pmatrix}$$

bewirkt. Die nächste Zeilenumformung (Addition des $-y$-fachen der ersten Zeile zur zweiten Zeile) wird durch Linksmultiplikation mit der Elementarmatrix

$$\begin{pmatrix} 1 & \\ -y & 1 \end{pmatrix}$$

bewirkt. Wir haben also beispielsweise

$$\begin{pmatrix} 1 & -\mu/x \\ 0 & \lambda + y\mu/x \end{pmatrix} = \begin{pmatrix} 1 & \\ -y & 1 \end{pmatrix} \cdot \begin{pmatrix} 1/x & \\ & 1 \end{pmatrix} \cdot A$$

und (indem man die übrigen beiden Umformungen auch noch explizit notiert)

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \mu/x \\ & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & \\ & x \end{pmatrix} \cdot \begin{pmatrix} 1 & \\ -y & 1 \end{pmatrix} \cdot \begin{pmatrix} 1/x & \\ & 1 \end{pmatrix} \cdot A.$$

Linksmultiplikation mit dem Inversen des Matrixprodukts vor A liefert dann

$$A = \begin{pmatrix} x & \\ & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & \\ y & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & \\ & 1/x \end{pmatrix} \cdot \begin{pmatrix} 1 & \\ -\mu/x & 1 \end{pmatrix};$$

Also ist A ein Produkt von Elementarmatrizen, wie behauptet.
(Falls man statt der Invertierbarkeit von x die Invertierbarkeit einer der übrigen Einträge fordert, kann man ganz ähnliche Rechnungen durchführen und kommt zu demselben Ergebnis.)
Im Allgemeinen ist x allerdings nicht invertierbar und tatsächlich gibt es Hauptidealbereiche R und Matrizen der Bauart (7.2), die sich nicht als Produkt von Elementarmatrizen schreiben lassen. (Siehe etwa die fundamentale Arbeit von Cohn [11, Seite 23].)

Satz 7.5 (Smith Normalform, Existenz)**.** *Sei R ein Hauptidealbereich und $A \in R^{n\times m}$ eine beliebige Matrix. Dann gibt es invertierbare Matrizen $S \in R^{n\times n}$ und $T \in R^{m\times m}$, sowie $r \geq 0$ von 0_R verschiedene Elemente $d_1, d_2, \ldots, d_r$ mit*

$$\langle d_1\rangle \supseteq \langle d_2\rangle \supseteq \ldots \supseteq \langle d_r\rangle \supsetneq \{0_R\}.$$

und

$$SAT = \left(\begin{array}{ccc|c} d_1 & & & 0 \cdots \\ & d_2 & & \vdots \\ & & \ddots & \\ & & d_r & \\ \hline 0 & \cdots & 0 & 0 \cdots \\ \vdots & & & \vdots \ddots \end{array}\right) \in R^{n\times m}.$$

Die Matrix rechter Hand bezeichnet man als ***Smith-Normalform*** *von A. Überdies lassen sich die Matrizen S und T als Produkte von $n\times n$- bzw. $m\times m$-Elementarmatrizen und Matrizen der Bauart (7.2) (mit $1_R = x\lambda + y\mu$) schreiben.*

Beweis. Mit $\langle A\rangle$ bezeichnen wir das Ideal von R, welches durch alle Einträge von A erzeugt wird.[2] Wir beginnen mit einer Vorüberlegung: Ist $U \in R^{n\times n}$ beliebig, so sind die Einträge von UA Linearkombinationen der Einträge von A, weswegen $\langle UA\rangle \subseteq \langle A\rangle$ gilt. Ist U invertierbar, so haben wir ferner

$$\langle A\rangle = \langle U^{-1}UA\rangle \subseteq \langle UA\rangle \subseteq \langle A\rangle$$

und also $\langle A\rangle = \langle UA\rangle$. Analoge Überlegungen gelten auch für Rechtsmultiplikation mit (invertierbaren) Matrizen $V \in R^{m\times m}$. (Für eine Verallgemeinerung dieser Überlegungen siehe Lemma 7.8.)

Die Einträge von A bezeichnen wir wie üblich mit A_{ij}. Wir betrachten zunächst den Fall $\langle A_{11}\rangle \neq \langle A\rangle$ und unterscheiden drei Fälle:

(1) Falls A_{11} nicht alle Elemente der ersten Zeile teilt, sagen wir A_{11} teilt nicht A_{12}, so betrachten wir das Ideal $\langle A_{11}, A_{12}\rangle$. Da R ein Hauptidealbereich ist, gilt $\langle A_{11}, A_{12}\rangle = \langle d\rangle$ für ein $d \neq 0_R$. Nun hat d eine Darstellung der Form $d = xA_{11} + yA_{12}$ mit $x, y \in R$ und wir haben auch $A_{11} = d\lambda$ und $A_{12} = d\mu$ für geeignete $\lambda, \mu \in R$. Es folgt

$$\begin{aligned} d &= xd\lambda + yd\mu = d(x\lambda + y\mu) \\ &\Longrightarrow d(x\lambda + y\mu - 1_R) = 0_R \Longrightarrow x\lambda + y\mu - 1_R = 0_R, \end{aligned}$$

[2] Da $A \in R^{n\times m}$ angenommen ist und $R^{n\times m}$ für $n \neq m$ kein Ring ist, sollte es hier schwer fallen die Notation $\langle A\rangle$ mit einem etwaig von A erzeugten Ideal zu verwechseln (was hier auch nicht gemeint ist).

da R ein Integritätsbereich ist. Also ist $1_R = x\lambda + y\mu$ und wir beachten

$$\left(\begin{array}{cc|c} A_{11} & A_{12} & A_{13}\cdots A_{1m} \\ * & * & *\cdots\cdots* \\ \hline * & * & *\cdots\cdots* \\ \vdots & \vdots & \vdots\quad\quad\vdots \\ * & * & *\cdots\cdots* \end{array}\right) \cdot \left(\begin{array}{cc|c} x & -\mu & \\ y & \lambda & \\ \hline & & 1_R \\ & & \ddots \\ & & 1_R \end{array}\right) = \left(\begin{array}{cc|c} d & \star & A_{13}\cdots A_{1m} \\ * & * & *\cdots\cdots* \\ \hline * & * & *\cdots\cdots* \\ \vdots & \vdots & \vdots\quad\quad\vdots \\ * & * & *\cdots\cdots* \end{array}\right),$$

wobei der Eintrag „$\star$“ für $A_{11}(-\mu)+A_{12}\lambda \in \langle A_{11}, A_{12}\rangle = \langle d\rangle$ steht und durch d teilbar ist. Nun iteriert man die Fallunterscheidung mit der Matrix rechter Hand als neue Matrix A. (Man beachte, dass gemäß unserer Vorüberlegung das von den Einträgen der Matrix rechter Hand erzeugte Ideal von R mit $\langle A\rangle$ übereinstimmt.)

(2) Falls A_{11} nicht alle Elemente der ersten Spalte teilt, so können wir analog zum ersten Fall argumentieren.

(3) Wir dürfen davon ausgehen, dass A_{11} alle Elemente der ersten Zeile und der ersten Spalte teilt. Durch Abziehen von geeigneten Vielfachen der ersten Zeile/Spalte von allen übrigen Zeilen und Spalten finden wir also invertierbare Matrizen X und Y (die Produkte von Elementarmatrizen sind) mit

$$XAY = \left(\begin{array}{c|c} d & \\ \hline & *\cdots\cdots* \\ & \vdots\quad\quad\vdots \\ & *\cdots\cdots* \end{array}\right).$$

Wegen der Annahme $\langle A_{11}\rangle \neq \langle A\rangle$ teilt d *nicht* alle Elemente „$*$“. Durch Addition einer geeigneten Zeile zur ersten Zeile landen wir also wieder im ersten Fall. Die Folge der so erhaltenen Einträge d ist — nach Übergang zu den davon erzeugten Idealen — aufsteigend und durch $\langle A\rangle$ beschränkt. Da R noetherisch ist (siehe Beispiel 7.4 (3)), sehen wir, dass endlich vielen Durchführungen der obigen Schritte irgendwann $\langle d\rangle = \langle A\rangle$ erreicht wird.

Im nächsten Schritt dürfen wir davon ausgehen invertierbare Matrizen X, Y wie im dritten Fall zu haben, wobei $d_1 = d$ alle übrigen Matrixeinträge teilt. Wir führen die bisherigen Überlegungen nun auch mit dem kleineren Block

$$\left(\begin{array}{cc} * & *\cdots\cdots* \\ * & *\cdots\cdots* \\ \vdots & \vdots\quad\quad\vdots \\ * & *\cdots\cdots* \end{array}\right) \quad \text{in} \quad XAY = \left(\begin{array}{c|c} d_1 & \\ \hline & \begin{array}{cc} * & *\cdots\cdots* \\ * & *\cdots\cdots* \\ \vdots & \vdots\quad\quad\vdots \\ * & *\cdots\cdots* \end{array} \end{array}\right).$$

durch und erhalten Matrizen invertierbare Matrizen X' und Y' mit

$$\left(\begin{array}{c|ccc} 1_R & 0_R & 0_R & \cdots\ 0_R \\ \hline 0_R & & & \\ 0_R & & X' & \\ \vdots & & & \\ 0_R & & & \end{array}\right) XAY \left(\begin{array}{c|ccc} 1_R & 0_R & 0_R & \cdots\ 0_R \\ \hline 0_R & & & \\ 0_R & & Y' & \\ \vdots & & & \\ 0_R & & & \end{array}\right) = \left(\begin{array}{cc|ccc} d_1 & & & & \\ & d_2 & & & \\ \hline & & * & \cdots & * \\ & & \vdots & & \vdots \\ & & * & \cdots & * \end{array}\right)$$

und einem Element d_2, welches alle Elemente „$*$“ teilt und von d_1 geteilt wird. Induktiv erhält man die Behauptung des Satzes. □

Beispiel 7.6. Der Beweis von Satz 7.5 liefert ein (im Wesentlichen) konstruktives Verfahren, welches dem aus der linearen Algebra bekannten Gauß-Algorithmus ähnelt. Wir betrachten die Matrix

$$A = X\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} - \begin{pmatrix} 1 & 3 & 0 & 2 \\ 0 & 0 & 0 & -1 \\ 0 & 1 & 1 & 1 \\ 0 & 2 & 0 & 3 \end{pmatrix} = \begin{pmatrix} X-1 & -3 & 0 & -2 \\ 0 & X & 0 & 1 \\ 0 & -1 & X-1 & -1 \\ 0 & -2 & 0 & X-3 \end{pmatrix}$$

über dem Polynomring $\mathbb{C}[X]$. Mögliche Umformungsschritte wie im Beweis von Satz 7.5 sehen etwa so aus:

$$A \rightsquigarrow \begin{pmatrix} -3 & X-1 & 0 & -2 \\ X & 0 & 0 & 1 \\ -1 & 0 & X-1 & -1 \\ -2 & 0 & 0 & X-3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -3 & X-1 & 0 & -2 \\ 0 & \frac{1}{3}X(X-1) & 0 & 1-\frac{2}{3}X \\ 0 & -\frac{1}{3}(X-1) & X-1 & -1+\frac{2}{3} \\ 0 & -\frac{2}{3}(X-1) & 0 & X-3+\frac{4}{3} \end{pmatrix}$$

$$\rightsquigarrow \left(\begin{array}{c|ccc} 1 & & & \\ \hline & \frac{1}{3}X(X-1) & 0 & 1-\frac{2}{3}X \\ & -\frac{1}{3}(X-1) & X-1 & -\frac{1}{3} \\ & -\frac{2}{3}(X-1) & 0 & X-\frac{5}{3} \end{array}\right) \rightsquigarrow \left(\begin{array}{c|ccc} 1 & & & \\ \hline & -(X-1) & 3(X-1) & -1 \\ & X(X-1) & 0 & 3-2X \\ & -2(X-1) & 0 & 3X-5 \end{array}\right)$$

$$\rightsquigarrow \left(\begin{array}{c|ccc} 1 & & & \\ \hline & 1 & -(X-1) & 3(X-1) \\ & 2X-3 & X(X-1) & 0 \\ & 5-3X & -2(X-1) & 0 \end{array}\right)$$

$$\rightsquigarrow \left(\begin{array}{c|ccc} 1 & & & \\ \hline & 1 & -(X-1) & 3(X-1) \\ & 0 & X(X-1)+(2X-3)(X-1) & -3(X-1)(2X-3) \\ & 0 & -2(X-1)+(X-1)(5-3X) & -3(X-1)(5-3X) \end{array}\right)$$

$$\rightsquigarrow \left(\begin{array}{cc|cc} 1 & & & \\ & 1 & & \\ \hline & & (X-1)^2 & (X-1)(2X-3) \\ & & (X-1)^2 & (X-1)(3X-5) \end{array}\right).$$

Für das weitere Vorgehen beachten wir (auf diese Gleichungen kann man mit dem erweiterten euklidischen Algorithmus auch gelangen, ohne sie vorher zu sehen)

$$\langle (X-1)^2, (X-1)(2X-3)\rangle = \langle X-1\rangle,$$
$$\underline{1}(X-1)(2X-3) + \underline{(-2)}(X-1)^2 = -(X-1),$$

sowie (vergleiche den ersten Fall in der Fallunterscheidung im Beweis von Satz 7.5)

$$\begin{pmatrix} (X-1)^2 & (X-1)(2X-3) \\ (X-1)^2 & (X-1)(3X-5) \end{pmatrix} \cdot \begin{pmatrix} 2 & -(2X-3) \\ -1 & X-1 \end{pmatrix}$$
$$= \begin{pmatrix} X-1 & 0 \\ -(X-3)(X-1) & (X-2)(X-1)^2 \end{pmatrix}.$$

Nun sieht man

$$A \rightsquigarrow \begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & d_3 & \\ & & & d_4 \end{pmatrix} \quad \text{mit} \quad \begin{cases} d_1 = 1, \\ d_2 = 1, \\ d_3 = X-1, \\ d_4 = (X-1)^2(X-2). \end{cases}$$

Da es sich bei $K[X]$ sogar um einen euklidischen Ring handelt, hätte man in Beispiel 7.6 auch ganz ohne das umständliche Arbeiten mit (7.2) auskommen können. Wir illustrieren dies hier jedoch lieber anhand von Matrizen mit ganzzahligen Einträgen, da dort die Arithmetik (übungsbedingt?) einfacher scheint.

Beispiel. Es sei eine Smith-Normalform von

$$\begin{pmatrix} 20 & 17 \end{pmatrix} \in \mathbb{Z}^{1\times 2}$$

zu bestimmen. Der euklidische Algorithmus liefert

$$\begin{cases} 20 = 1 \cdot 17 + 3, \\ 17 = 5 \cdot \ 3 + 2, \\ \ 3 = 1 \cdot \ 2 + 1. \end{cases}$$

Wir ziehen nun also ein mal die zweite Spalte von der ersten ab, dann fünf mal die neue erste Spalte von der zweiten und abschließend ein mal die neue zweite Spalte von der vormals neuen ersten. In Zeichen:

$$\begin{pmatrix} 20 & 17 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 17 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 \end{pmatrix}.$$

Nun teilt der erste Eintrag den zweiten Eintrag und abermaliges Abziehen führt auf die Matrix $\begin{pmatrix} 1 & 0 \end{pmatrix}$ in Smith-Normalform. Zur Illustration wollen wir uns nun noch überlegen, dass Arbeiten mit (7.2) auf dasselbe Ergebnis führt (modulo der Freiheit mit Einheiten zu multiplizieren, aber wir wählen hier schon alle Zahlen so, dass am Ende alles übereinstimmt). Löst man in der obigen Anwendung des euklidischen

Algorithmus rückwärts jeweils nach dem Rest auf, so erhält man schließlich $6 \cdot 20 - 7 \cdot 17 = 1$. Aus Fall (1) im Beweis von Satz 7.5 entnehmen wir, dass wir das Produkt

$$\begin{pmatrix} A_{11} & A_{12} \end{pmatrix} \cdot \begin{pmatrix} x & -\mu \\ y & \lambda \end{pmatrix} \quad \text{mit} \quad (A_{11}, A_{12}, \lambda, \mu, x, y) = (20, 17, 20, 17, 6, 7)$$

zu betrachten haben, also

$$\begin{pmatrix} 20 & 17 \end{pmatrix} \cdot \begin{pmatrix} 6 & -17 \\ -7 & 20 \end{pmatrix} = \begin{pmatrix} 1 & 0 \end{pmatrix}.$$

Beispiel 7.7. Wir wollen die Matrix

$$A = \begin{pmatrix} 2 & -2 \\ 1 & 3 \end{pmatrix} \in \mathbb{Z}^{2\times 2}$$

über $\mathbb{Z}$ auf Smith-Normalform transformieren und auch passende invertierbare Matrizen S und T wie in Satz 7.5 bestimmen. Hierzu betrachten wir die Blockmatrix

$$\left(\begin{array}{c|c} \mathbf{0}_2 & \mathbf{1}_2 \\ \hline \mathbf{1}_2 & A \end{array}\right) = \left(\begin{array}{cc|cc} & & 1 & \\ & & & 1 \\ \hline 1 & & 2 & -2 \\ & 1 & 1 & 3 \end{array}\right).$$

Wendet man nun das Verfahren aus dem Beweis von Satz 7.5 auf den zu A gehörigen Block an und führt die entsprechenden Operationen aber auf der gesamten Blockmatrix durch, so baut man sukzessive auch die Matrizen S und T in den zusätzlichen Blöcken auf. (Die Anordnung sorgt dafür, dass der obere Einheitsmatrixblock nur auf A angewandte Spaltenumformungen „registriert“ und analog mit dem linken unteren Einheitsmatrixblock und auf A angewandte Zeilenumformungen.) Dieses Verfahren mag den Leserinnen und Lesern vielleicht aus der linearen Algebra unter dem Namen ***Gauß–Jordan-Algorithmus*** bekannt sein. Wir illustrieren dies nur kurz und gehen davon aus, dass sich die Leserin oder der Leser die Details selbst überlegt. Durch Umformung erhält man

$$\left(\begin{array}{cc|cc} & & 1 & \\ & & & 1 \\ \hline 1 & & 2 & -2 \\ & 1 & 1 & 3 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|cc} & & 1 & \\ & & & 1 \\ \hline & 1 & 1 & 3 \\ 1 & & 2 & -2 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|cc} & & 1 & -3 \\ & & & 1 \\ \hline & 1 & 1 & 3 \\ 1 & -2 & 0 & -8 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|cc} & & 1 & 3 \\ & & & -1 \\ \hline & 1 & 1 & 0 \\ 1 & -2 & 0 & 8 \end{array}\right).$$

Man beachte, dass die letzte Matrix im unteren rechten Block in Smith-Normalform sind. Die Diagonaleinträge sind hier lediglich bis auf Multiplikation mit Einheiten (Assoziiertheit!) wohl-bestimmt. — Siehe auch Satz 7.9. Man beachte außerdem

$$\begin{pmatrix} & 1 \\ 1 & -2 \end{pmatrix} \cdot A \cdot \begin{pmatrix} 1 & 3 \\ & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix}.$$

(Für eine geometrische Interpretation der hiesigen Überlegungen siehe Abbildung 23 auf Seite 141.)

7.4. Smith-Normalform: Eindeutigkeit

Unser nächstes Ziel ist eine Eindeutigkeitsaussage zu Satz 7.5. Dies gelingt mit gewissen aus Determinanten gewonnenen Invarianten, welche ihre Nützlichkeit daraus schöpfen, invariant unter dem Prozess zu sein, welcher von einer Matrix auf ihre Smith-Normalform führt. Damit lassen sich dann die Daten aus der Smith-Normalform alleinig aus der Ausgangsmatrix bestimmen und müssen daher *a-fortiori* eindeutig sein.

Zur Realisierung des oben angerissenen Programms sei R zunächst nur als Integritätsbereich vorausgesetzt. Wir identifizieren R mit seinem Bild unter der kanonischen Abbildung in seinen zugehörigen Quotientenkörper $K = \mathrm{Quot}(R)$; Wir erlauben uns also „$R \subseteq K$“ zu schreiben. Eine Matrix A über R ist damit auch eine Matrix über K. Ist A quadratisch, so ist (über K) ihre ***Determinante*** $\det A \in K$ (wie aus der linearen Algebra bekannt) wohl-definiert. Mit dem Entwicklungssatz von Laplace sieht man, dass $\det A$ sogar ein Element von R ist. Die üblichen Rechenregeln für Determinanten gelten auch in R, da diese schon im Körper K gültig sind; Mehr Details hierzu kennen die Leserinnen und Leser bereits aus [33, Kapitel 7] unter dem Stichwort „*universelle Identitäten*“.

Zu einer $n\times m$-Matrix A (nicht notwendigerweise quadratisch!) ist ein ***k×k-Minor*** definiert als Determinante einer beliebigen $k\times k$-Matrix, die man durch Streichen von $n-k$ Zeilen und $m-k$ Spalten von A erhält. (Die so erhaltenen Matrizen nennen wir ***k×k-Streichungsmatrizen***.)

Beispiele (Streichungsmatrizen und Minoren).

- Die 3×3-Matrix
$$A = \begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{pmatrix}$$
hat als einzigen 3×3-Minor die Determinante von A selbst. Ferner hat A die 2×2-Streichungsmatrizen
$$\begin{pmatrix} & A_{12} & A_{13} \\ & A_{22} & A_{23} \\ & & \end{pmatrix}, \quad \begin{pmatrix} A_{11} & & A_{13} \\ A_{21} & & A_{23} \\ & & \end{pmatrix}, \quad \begin{pmatrix} A_{11} & A_{12} & \\ A_{21} & A_{22} & \\ & & \end{pmatrix},$$
sowie sechs weitere (via Streichen der ersten/zweiten Zeile allen Spaltenkombinationen). Die obigen drei Matrizen liefern dann drei der insgesamt neun 2×2-Minoren von A:
$$A_{12}A_{23} - A_{13}A_{22}, \quad A_{11}A_{23} - A_{13}A_{21}, \quad A_{11}A_{22} - A_{12}A_{21}.$$
Die 1×1-Minoren sind sämtliche Einträge von A.
- Die 2×3-Matrix
$$A = \begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \end{pmatrix}$$

hat keinen 3×3-Minor. Ferner hat A als 2×2-Streichungsmatrizen nur

$$\begin{pmatrix} & A_{12} & A_{13} \\ & A_{22} & A_{23} \end{pmatrix}, \quad \begin{pmatrix} A_{11} & & A_{13} \\ A_{21} & & A_{23} \end{pmatrix}, \quad \begin{pmatrix} A_{11} & A_{12} & \\ A_{21} & A_{22} & \end{pmatrix}.$$

Die zugehörigen 2×2-Minoren sehen genau so aus wie die im Beispiel zuvor explizit angegebenen 2×2-Minoren.

Bemerkung. Man kennt Minoren vermutlich schon aus der mehrdimensionalen Analysis vom ***Hauptminorenkriterium*** für positive/negative Definitheit einer symmetrischen Matrix (manchmal auch Hurwitz-Kriterium oder Sylvester-Kriterium genannt).

Lemma 7.8. *Sei R ein Integritätsbereich und A eine beliebige $n\times m$-Matrix über R. Sei $\mathfrak{I}_k(A)$ das Ideal von R welches von allen $k\times k$-Minoren von A erzeugt wird. Für beliebige Matrizen $U \in R^{n\times n}$ und $V \in R^{m\times m}$ gilt dann*

$$\mathfrak{I}_k(UA) \subseteq \mathfrak{I}_k(A), \quad \textit{und} \quad \mathfrak{I}_k(AV) \subseteq \mathfrak{I}_k(A).$$

Ist U oder V invertierbar, so ist die jeweils relevante Inklusion sogar eine Gleichheit.

Beweis. Der Zusatz zur Invertierbarkeit ist eine formale Konsequenz aus den Inklusionen; Man vergleiche hierzu die Argumente zu $\langle A\rangle$ aus dem Beweis von Satz 7.5.

Wir beweisen nur die Inklusion „$\mathfrak{I}_k(UA) \subseteq \mathfrak{I}_k(A)$“. — Die Inklusion „$\mathfrak{I}_k(AV) \subseteq \mathfrak{I}_k(A)$“ funktioniert ganz ähnlich. Wir haben

$$UA = \begin{pmatrix} \sum_\ell U_{1\ell}A_{\ell 1} & \cdots\cdots & \sum_\ell U_{1\ell}A_{\ell m} \\ \vdots & & \vdots \\ \sum_\ell U_{n\ell}A_{\ell 1} & \cdots\cdots & \sum_\ell U_{n\ell}A_{\ell m} \end{pmatrix} \in R^{n\times m} \quad \big(\text{mit } \textstyle\sum_\ell = \sum_{\ell=1}^{n}\big).$$

Die $k\times k$-Streichungsmatrix S, welche die Zeilen $i_1 < i_2 < \ldots < i_k$ und Spalten $j_1 < \ldots < j_k$ von UA übrig lässt, hat die Form

$$S = \begin{pmatrix} \sum_\ell U_{i_1\ell}A_{\ell j_1} & \cdots\cdots & \sum_\ell U_{i_1\ell}A_{\ell j_k} \\ \sum_\ell U_{i_2\ell}A_{\ell j_1} & \cdots\cdots & \sum_\ell U_{i_2\ell}A_{\ell j_k} \\ \vdots & & \vdots \\ \sum_\ell U_{i_k\ell}A_{\ell j_1} & \cdots\cdots & \sum_\ell U_{i_k\ell}A_{\ell j_k} \end{pmatrix} = \begin{pmatrix} \text{——} & \sum_\ell U_{i_1\ell}A_{\ell j_\bullet} & \text{——} \\ \text{——} & \sum_\ell U_{i_2\ell}A_{\ell j_\bullet} & \text{——} \\ & \vdots & \\ \text{——} & \sum_\ell U_{i_k\ell}A_{\ell j_\bullet} & \text{——} \end{pmatrix}.$$

Linearität der Determinante in der ersten Zeile liefert

$$\det S = \sum_{\ell_1} U_{i_1\ell_1} \det \begin{pmatrix} \text{——} & A_{\ell_1 j_\bullet} & \text{——} \\ \text{——} & \sum_\ell U_{i_2\ell}A_{\ell j_\bullet} & \text{——} \\ & \vdots & \\ \text{——} & \sum_\ell U_{i_k\ell}A_{\ell j_\bullet} & \text{——} \end{pmatrix}.$$

Setzt man dies für die übrigen $k-1$ Zeilen fort, so erhält man

$$\det S = \sum_{\ell_1}\sum_{\ell_2}\dots\sum_{\ell_k}(U_{i_1\ell_1}U_{i_2\ell_2}\cdots U_{i_k\ell_k})\det\begin{pmatrix} \text{—} & A_{\ell_1 j_\bullet} & \text{—} \\ \text{—} & A_{\ell_2 j_\bullet} & \text{—} \\ & \vdots & \\ \text{—} & A_{\ell_k j_\bullet} & \text{—} \end{pmatrix}.$$

Mit der Alternierungseigenschaft der Determinante folgt dann

$$\det S = \sum_{(\ell_\bullet,\sigma)}(\operatorname{sgn}\sigma)(U_{i_1\ell_1}U_{i_2\ell_2}\cdots U_{i_k\ell_k})\det\begin{pmatrix} \text{—} & A_{\sigma(\ell_1) j_\bullet} & \text{—} \\ \text{—} & A_{\sigma(\ell_2) j_\bullet} & \text{—} \\ & \vdots & \\ \text{—} & A_{\sigma(\ell_k) j_\bullet} & \text{—} \end{pmatrix},$$

wobei die Summation über alle k-Tupel $\ell_\bullet = (\ell_1, \ell_2, \dots, \ell_k)$ mit paarweise verschiedenen Einträgen aus $\{1,\dots,n\}$ zu erstrecken ist und $\sigma \in \operatorname{Sym}(\{\ell_1, \ell_2, \dots, \ell_k\})$ die Permutation bezeichne, welche die Einträge von $\ell_\bullet$ der Größe nach ordnet. Die Determinanten rechter Hand sind nun aber stets $k\times k$-Minoren von A und damit erweist sich $\det S$ als eine Linearkombination von diesen; Es folgt $\det S \in \mathfrak{I}_k(A)$ und also insgesamt $\mathfrak{I}_k(UA) \subseteq \mathfrak{I}_k(A)$. □

Wir illustrieren die Rechnung aus Lemma 7.8 anhand eines Beispiels. Letztlich ist darin auch schon die gesamte Rechnung abgebildet, doch wirkt diese hier wegen fehlender Indizes deutlich lesbarer.

Beispiel. Wir berechnen

$$\det\left(\begin{pmatrix}1&2\\3&4\end{pmatrix}\begin{pmatrix}5&6\\7&8\end{pmatrix}\right) = \det\begin{pmatrix}1\cdot5+2\cdot7 & 1\cdot6+2\cdot8\\ 3\cdot5+4\cdot7 & 3\cdot6+4\cdot8\end{pmatrix}.$$

Unter Ausnutzung von Linearität in Zeilen erhalten wir

$$\begin{aligned} d &= 1\cdot\det\begin{pmatrix}5 & 6\\ 3\cdot5+4\cdot7 & 3\cdot6+4\cdot8\end{pmatrix} + 2\cdot\det\begin{pmatrix}7 & 8\\ 3\cdot5+4\cdot7 & 3\cdot6+4\cdot8\end{pmatrix} \\ &= 1\cdot3\cdot\det\begin{pmatrix}5&6\\5&6\end{pmatrix} + 1\cdot4\cdot\det\begin{pmatrix}5&6\\7&8\end{pmatrix} + 2\cdot3\cdot\det\begin{pmatrix}7&8\\5&6\end{pmatrix} + 2\cdot4\cdot\det\begin{pmatrix}7&8\\7&8\end{pmatrix}. \end{aligned}$$

Die äußeren beiden auftretenden Determinanten verschwinden offenbar, da die zugehörigen Matrizen zwei gleiche Spalten besitzen.

$$d = 1\cdot4\cdot\det\begin{pmatrix}5&6\\7&8\end{pmatrix} - 2\cdot3\cdot\det\begin{pmatrix}5&6\\7&8\end{pmatrix}.$$

Dieselbe Rechnung mit Variablen und offensichtlichen Bezeichnungen sieht dabei so aus:

$$\begin{aligned}\det\left(\begin{pmatrix}u_{11} & u_{12}\\ u_{21} & u_{22}\end{pmatrix}\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\right) &= \det\begin{pmatrix}u_{11}a_{11}+u_{12}a_{21} & u_{11}a_{12}+u_{12}a_{22}\\ u_{21}a_{11}+u_{22}a_{21} & u_{21}a_{12}+u_{22}a_{22}\end{pmatrix}\\ &= u_{11}u_{21}\det\begin{pmatrix}a_{11} & a_{12}\\ a_{11} & a_{12}\end{pmatrix}+u_{11}u_{22}\det\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}+\\ &\quad+u_{12}u_{21}\det\begin{pmatrix}a_{21} & a_{22}\\ a_{11} & a_{12}\end{pmatrix}+u_{12}u_{22}\det\begin{pmatrix}a_{21} & a_{22}\\ a_{21} & a_{22}\end{pmatrix}\\ &= u_{11}u_{22}\det A-u_{12}u_{21}\det A.\end{aligned}$$

Satz 7.9 (Smith Normalform, Eindeutigkeit)**.** *Sei R ein Hauptidealbereich und $A\in R^{n\times m}$ eine beliebige Matrix. Dann sind r und die Ideale $\langle d_1\rangle\supseteq\langle d_2\rangle\supseteq\ldots\supseteq\langle d_r\rangle\supsetneq\{0_R\}$ aus Satz 7.5 durch die Matrix A eindeutig bestimmt.*

Beweis. Für eine Matrix

$$D=\left(\begin{array}{ccc|c}d_1 & & & 0\cdots\\ & d_2 & & \vdots\\ & & \ddots & \\ & & d_r & \\ \hline 0 & \cdots & \cdots & 0\cdots\\ \vdots & & & \vdots\ddots\end{array}\right) \tag{7.3}$$

in Smith-Normalform (mit $\langle d_1\rangle\supseteq\langle d_2\rangle\supseteq\ldots\supseteq\langle d_r\rangle\supsetneq\{0_R\}$) bestätigt man leicht

$$\mathfrak{I}_k(D)=\begin{cases}\langle d_1d_2\cdots d_k\rangle & \text{für } k\le r,\\ \{0_R\} & \text{für } k>r.\end{cases} \tag{7.4}$$

Ist nun $SAT=D$ wie in Satz 7.5, so folgt mit Lemma 7.8 induktiv ($k=1,2,\ldots$), dass $\mathfrak{I}_k(D)$ und damit auch r sowie die Ideale $\langle d_k\rangle$ bereits völlig durch $\mathfrak{I}_k(A)$ bestimmt sind. Das liefert schon die avisierte Eindeutigkeitsaussage. □

Bemerkung. Man beachte, dass (7.4) für $k=1$ die Gleichung $\mathfrak{I}_1(A)=\langle d_1\rangle$ liefert. Nun ist $\mathfrak{I}_1(A)$ aber genau das von allen Einträgen von A erzeugte Ideal, also $\langle A\rangle$ in der Notation aus dem Beweis vom Existenzsatz zur Smith-Normalform (Satz 7.5). Insbesondere erkennen wir die dort angestellte Vorüberlegung als einen Spezialfall von Lemma 7.8 für $k=1$.

KAPITEL 8

Endlich erzeugte Moduln über Hauptidealbereichen

Unser Ziel in diesem Kapitel ist der in § 6.1 angekündigte Struktursatz für endlich erzeugte Moduln über Hauptidealbereichen, den wir hier als Satz 8.2 notieren. Anschließend studieren wir einige Anwendungen. Unsere Darstellung orientiert sich lose an [30] und [2].

8.1. Der Hauptsatz

Der noch zu besprechende Satz 8.2 (bzw. dessen Beweis) fußt auf der Bestimmung eines Faktormoduls $R^n/\operatorname{im} f$ für einen R-Modulhomomorphismus $f\colon R^m \to R^n$ (siehe (8.2) weiter unten). Hierzu sollen unsere Überlegungen zu Homomorphismen zwischen freien Moduln und Normalformen aus Kapitel 7 zur Anwendung gebracht werden. Der Übergang zur Smith-Normalform korrespondiert auf Homomorphismen-Ebene zum Übergang zu einem anderen Modulhomomorphismus $f_D\colon R^m \to R^n$ und man steht vor der Aufgabe die Moduln $R^n/\operatorname{im} f$ und $R^n/\operatorname{im} f_D$ miteinander zu vergleichen. Ein ganz allgemeines derartiges Vergleichsresultat wird durch das folgende Lemma zur Verfügung gestellt.

Lemma 8.1. *Sei R ein Ring und ein kommutatives Quadrat*

$$\begin{array}{ccc} M' & \xrightarrow{f} & M \\ \downarrow{\scriptstyle \Phi'} & & \downarrow{\scriptstyle \Phi} \\ N' & \xrightarrow{g} & N \end{array}$$

von R-Moduln und R-Modulhomomorphismen gegeben. Dann gilt:

(1) Es gibt genau einen R-Modulhomomorphismus $\alpha\colon M/\operatorname{im} f \to N/\operatorname{im} g$, der das folgende Diagramm kommutativ macht, wobei die unbeschrifteten Pfeile jeweils die kanonischen Homomorphismen bezeichnen:

$$\begin{array}{ccccccc} M' & \xrightarrow{f} & M & \longrightarrow & M/\operatorname{im} f & \longrightarrow & 0 \\ \downarrow{\scriptstyle \Phi'} & & \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \exists!\,\alpha} & & \\ N' & \xrightarrow{g} & N & \longrightarrow & N/\operatorname{im} g & \longrightarrow & 0\,. \end{array}$$

(2) Ist Φ surjektiv, so ist auch α surjektiv.

(3) Ist Φ' surjektiv und Φ injektiv, so ist α injektiv.

Beweis. Bezeichne π_f die kanonische Projektion $M \to M/\operatorname{im} f$, und π_g die kanonische Projektion $N \to N/\operatorname{im} g$.

(1): Wir wollen einsehen, dass sich Existenz und Eindeutigkeit von α direkt aus Proposition 6.13 ergeben. Damit ist dann auch direkt die Kommutativität des entstehenden Diagramms klar. Hierzu betrachten wir die Verkettung von $\pi_g \circ \Phi$ und es gilt lediglich nachzuweisen, dass deren Kern $\operatorname{im} f$ enthält. Sei also $m = f(m') \in \operatorname{im} f$ beliebig. Wegen der Kommutativität des Ausgangsquadrats ist $\Phi(m) = \Phi(f(m')) = g(\Phi'(m')) \in \operatorname{im} g$ und dies wird von π_g auf Null abgebildet, wie gewünscht.

(2): Ist Φ surjektiv, so ist auch $\alpha \circ \pi_f = \pi_g \circ \Phi$ surjektiv. Dann muss aber auch schon α surjektiv sein.

(3): Sei nun Φ injektiv und Φ' surjektiv. Es gilt zu zeigen, dass α injektiv ist. Im Zuge unseres Beweises von (1) hatten wir uns α mittels Proposition 6.13 beschafft. Dies liefert auch gleich die Injektivität von α, wenn wir $\ker(\pi_g \circ \Phi) = \operatorname{im} f$ einsehen. (Tatsächlich verbleibt nur der Nachweis von „$\subseteq$“, da wir die umgekehrte Inklusion bereits beim Beweis von (1) gesehen haben.) Sei also $m \in \ker(\pi_g \circ \Phi)$. Dann ist $\Phi(m) \in \ker \pi_g$ und es gibt ein $n' \in N'$ mit $\Phi(m) = g(n')$. Da außerdem Φ' surjektiv ist, gibt es $m' \in M'$ mit $n' = \Phi'(m')$. Nun ist

$$\Phi(f(m')) = g(\Phi'(m')) = g(n') = \Phi(m).$$

Die Injektivität von Φ impliziert nun $m = f(m') \in \operatorname{im} f$. □

Bemerkung. Die Beweistechnik vom Beweis von Lemma 8.1 bezeichnet man aus evidenten Gründen als ***Diagrammjagd***. Solche Diagrammjagden sind oft sehr einfach visuell am Diagramm selbst durchführbar, aber notorisch kryptisch, wenn man diese auf Papier aufschreibt (siehe oben!). Man probiere selbst den Beweis von Lemma 8.1 anhand des dortigen Diagramms zu führen, ohne auf den hier notieren Beweis zu schauen.[1]

Wir kommen nun zum Schlüsselergebnis unserer Untersuchungen der Modultheorie von Hauptidealbereichen:

Satz 8.2 (Hauptsatz)**.** *Sei R ein Hauptidealbereich und M ein endlich erzeugter R-Modul. Dann gelten die folgenden Aussagen:*

(1) Es existieren Zahlen k und ℓ, sowie Ideale $R \supset \mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \ldots \supseteq \mathfrak{a}_\ell \supset \{0_R\}$ mit einem Isomorphismus

$$M \cong R^k \oplus \bigoplus_{i=1}^{\ell} (R/\mathfrak{a}_i).$$

[1] Aluffi [1, Seite 182] schreibt im Zusammenhang mit Diagrammjagden: „*Dear reader: don't shy away from trying this, for it is excellent, indispensable practice. Miss this opportunity and you will forever feel unsure about such manipulations.*“

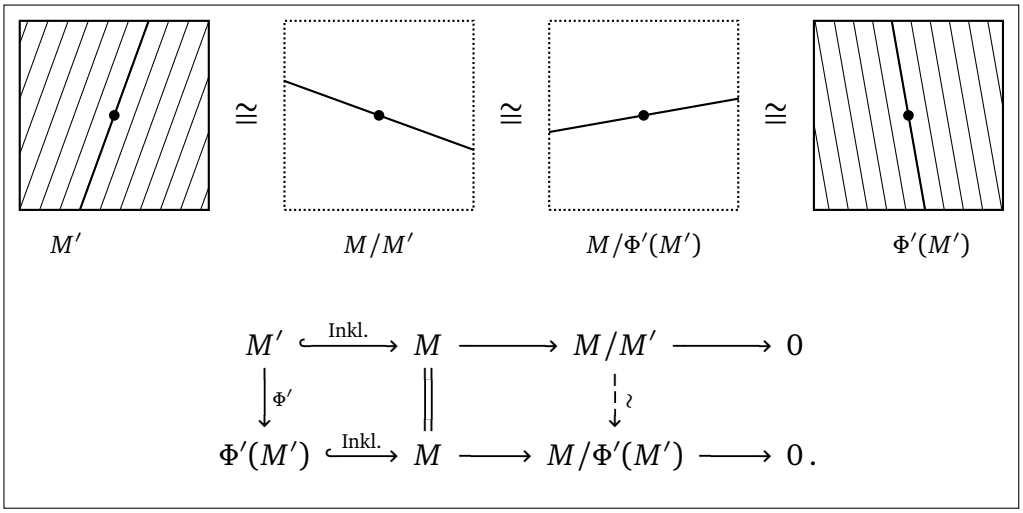


Abbildung 21. Veranschaulichung von Lemma 8.1, wenn f und g jeweils die Inklusionen von Untermoduln von $M = N$ darstellen: Ein Untermodul M' (dicke Linie durch den Nullpunkt) in einem R-Modul M. Die dünnen Linien zeigen Nebenklassen $x + M'$ mit $x \in M$. Die Nebenklassen bilden den Faktormodul M/M'. Tauscht man M' durch eine isomorphe Kopie $\Phi'(M') \subseteq M$, so ändern sich zwar die den Nebenklassen zugrunde liegenden Mengen, aber man erhält dennoch isomorphe Faktormoduln.

(2) Es existieren Zahlen k und s, Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ (nicht notwendigerweise verschieden) und Exponenten $\nu_1, \ldots, \nu_s \in \mathbb{N}$ mit einem Isomorphismus

$$M \cong R^k \oplus \bigoplus_{j=1}^{s} (R/\mathfrak{p}_j^{\nu_j}).$$

(3) Die Zahlen k, ℓ, s, sowie die oben auftretenden Ideale in (1) und (2), sowie deren Vielfachheiten, sind jeweils eindeutig bestimmt (wobei Eindeutigkeit bei (2) bis auf offensichtliche Permutation der Primideale nebst zugehöriger Exponenten zu verstehen ist).

Bemerkung 8.3. Sei R ein Hauptidealbereich und M ein R-Modul.

(1) Die Zahl k in Satz 8.2 lässt sich auch charakterisieren als die maximale Anzahl linear unabhängiger Elemente in M und wird auch als ***Rang von M*** bezeichnet.
(2) Die Isomorphismen in Satz 8.2 (1) und (2) sind im Allgemeinen nicht eindeutig bestimmt. Das Bild von $R^k \oplus 0 \oplus \ldots$ in M unter dem Isomorphismus

$$M \cong R^k \oplus \bigoplus_{i=1}^{\ell} (R/\mathfrak{a}_i) \tag{8.1}$$

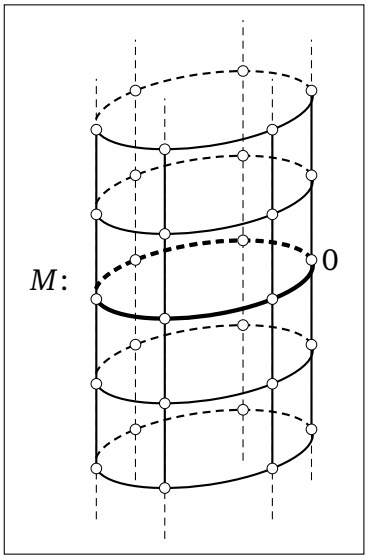


Abbildung 22. Veranschaulichung des $\mathbb{Z}$-Moduls $M = \mathbb{Z} \oplus (\mathbb{Z}/6\mathbb{Z})$ als auf einem Zylinder angeordnete Punkte: Die Summe zweier Punkte erhält man durch Addition der jeweiligen Höhen und Drehung auf den eingezeichneten Kreisen (in offensichtlicher Weise). Die Torsionselemente von M sind genau die Elemente mit Höhe 0, also die Punkte auf dem dick gezeichneten Kreis, und auch keine weiteren Elemente (jedes Element mit Höhe $\neq 0$ „entkommt“ bei Skalarmultiplikation mit Elementen aus $\mathbb{Z} \setminus \{0\}$ gen Unendlich, ohne das Nullelement zu treffen).

ist ebenfalls im Allgemeinen nicht eindeutig bestimmt. (In Abbildung 22 kann man ein Beispiel hierfür erkennen; Man überlege sich die zugehörigen Details.)

(3) Hingegen das Bild von $0 \oplus \bigoplus_{i=1}^{\ell}(R/\mathfrak{a}_i)$ in M unter obigem Isomorphismus (8.1) ist wohl-bestimmt; Es stimmt mit dem ***Torsionsuntermodul von M***

$$\mathrm{Tor}(M) = \{\, x \in M : \lambda x = 0 \text{ für ein } \lambda \in R \setminus \{0_R\} \,\}$$

überein. Die Elemente von $\mathrm{Tor}(M)$ heißen ***Torsionselemente***. Gilt $\mathrm{Tor}(M) = \{0\}$, so nennen wir M ***torsionsfrei*** und ein Modul M mit $\mathrm{Tor}(M) = M$ (äquivalent: $k = 0$ in Satz 8.2) heißt ***Torsionsmodul***. Man vergleiche auch Abbildung 22! Ferner schreibt sich (8.1) damit auch als

$$M \cong R^k \oplus \mathrm{Tor}(M).$$

Der erste Faktor R^k ist frei. Da $R^{(I)}$ für jede Indexmenge torsionsfrei ist folgt, dass alle freien Moduln torsionsfrei sind. Für jeden endlich erzeugten Modul M über einem Hauptidealbereich gilt somit gemäß der obigen Zerlegung: M ist genau dann frei, wenn M torsionsfrei ist. Man erkennt für diese Moduln $\mathrm{Tor}(M)$ gewissermaßen als eine „Obstruktion“ zu Freiheit. Das präzisere Studium derartiger Gedankengänge gehört in das Gebiet der homologischen Algebra.

(4) Die eben hergestellte Beziehung zwischen Freiheit und Torsionsfreiheit scheitert über nicht-Hauptidealbereichen R i.Allg. sogar im endlich erzeugten Fall. Die Untermoduln $\langle 2, X\rangle \subset \mathbb{Z}[X]$ und $\langle X, Y\rangle \subset \mathbb{C}[X, Y]$ sind nämlich als Untermoduln freier Moduln selbstverständlich torsionsfrei. Allerdings sind diese nicht frei (siehe Beispiel 6.12 (4)).

Beweis von Satz 8.2. Nach Voraussetzung gibt es (nach Definition von „endlich erzeugt“) für ein $n \in \mathbb{N}_0$ einen surjektiven R-Modulhomomorphismus $g\colon R^n \twoheadrightarrow M$. Der Kern von g ist ein Untermodul des (laut Beispiel 7.4 (3) und Proposition 7.2 (2)) noetherschen Moduls R^n, und daher endlich erzeugt laut Satz 7.1. Wir haben also einen surjektiven R-Modulhomomorphismus $R^m \twoheadrightarrow \ker g$. Dessen Verknüpfung mit der Inklusion $\ker g \hookrightarrow R^n$ bezeichnen wir mit f. Wir fassen dies in folgendem kommutativen Diagramm (mit exakten Zeilen und Spalten) zusammen:

$$\begin{array}{ccccccccc} & & & & 0 & & & & \\ & & & & \uparrow & & & & \\ 0 & \longrightarrow & \ker g & \xhookrightarrow{\text{Inkl.}} & R^n & \xrightarrow{g} & M & \longrightarrow & 0\,. \\ & & & & \uparrow\!\!\uparrow & \nearrow_{f} & & & \\ & & & & R^m & & & & \end{array}$$

Hierbei ist

$$M = \operatorname{im} g \cong R^n / \ker g = R^n / \operatorname{im} f. \tag{8.2}$$

Dies führt auf die folgende *fundamentale Beobachtung*:

Wir können M allein durch die Kenntnis von f beschreiben!

Die Abbildung f ist von der Form $f = (x \mapsto Ax)$ mit einer geeigneten Matrix $A \in R^{n\times m}$. Diese Matrix lässt sich nun mittels Satz 7.5 via zweier invertierbarer Matrizen $S \in R^{n\times n}$ und $T \in R^{m\times m}$ in Smith-Normalform überführen, sagen wir $SAT = D$, mit D wie in (7.3). Wir schreiben im Folgenden f_X für den einer Matrix X (über R) zugeordneten R-Modulhomomorphismus. Aus Lemma 8.1 ergibt sich nun der dritte vertikale Isomorphismus im folgenden Diagramm

$$\begin{array}{ccccccc} R^m & \xrightarrow{f} & R^n & \longrightarrow & R^n/\operatorname{im} f & \longrightarrow & 0 \\ \wr\downarrow{\scriptstyle f_{T^{-1}}} & & \wr\downarrow{\scriptstyle f_S} & & \wr\downarrow{\scriptstyle \exists} & & \\ R^m & \xrightarrow{f_D} & R^n & \longrightarrow & R^n/\operatorname{im} f_D & \longrightarrow & 0\,. \end{array}$$

Also ist $M \cong R^n/\operatorname{im} f \cong R^n/\operatorname{im} f_D$. (Siehe auch Abbildung 21 für eine Veranschaulichung davon.) Wir haben (siehe (7.3)!)

$$\operatorname{im} f_D = R\begin{pmatrix} d_1 \\ 0_R \\ \vdots \\ 0_R \\ \vdots \end{pmatrix} \oplus R\begin{pmatrix} 0_R \\ d_2 \\ \vdots \\ 0_R \\ \vdots \end{pmatrix} \oplus \ldots \oplus R\begin{pmatrix} 0_R \\ 0_R \\ \vdots \\ d_r \\ \vdots \end{pmatrix},$$

wobei in den Spalten jeweils nur die d_j-Einträge von Null verschieden sind. Daraus folgert man leicht mittels Proposition 6.13 (3)

$$M \cong R^n / \operatorname{im} f_D \cong \bigoplus_{j=1}^{r} (R/\langle d_j \rangle) \oplus R^k \quad \text{mit} \quad k = n - r. \tag{8.3}$$

Gilt $\langle d_j \rangle = R$, so ist der zugehörige Summand R/R trivial und kann weggelassen werden.[2] Insgesamt erhält man also (1) mit $\mathfrak{a}_i = \langle d_{i+h} \rangle$, wobei h minimal mit der Eigenschaft $\langle d_{1+h} \rangle \neq R$ gewählt ist.

(Man mache sich in Fortsetzung von Beispiel 7.7 anhand von Abbildung 23 klar, dass die hier erhaltenen Isomorphismen auch konkret berechnet werden können, wenn man zu einem endlich erzeugten R-Modul M Erzeuger von M, sowie Erzeuger des Kerns der Surjektion von $R^n \to M$ kennt, welche die Standardbasiselemente von R^n auf die fraglichen Erzeuger von M abbildet.)

Für (2) benutzen wir (1). Jedes dort auftretende Ideal $\mathfrak{a}_i$ wird von einem Element a_i erzeugt. Dieses zerlegt sich im Hauptidealbereich R, der ja auch faktoriell ist, in eine Einheit mal Potenzen paarweise nichtassoziierter Primelemente von R. Wir haben etwa

$$\mathfrak{a}_i = \langle p_1^{\nu_{i1}} p_2^{\nu_{i2}} \cdots p_t^{\nu_{it}} \rangle.$$

Dann ist

$$M \cong R^k \oplus \bigoplus_{i=1}^{\ell} (R/\mathfrak{a}_i) \cong R^k \oplus \bigoplus_{i=1}^{\ell} \bigoplus_{j=1}^{t} (R/\langle p_j^{\nu_{ij}} \rangle)$$

nach dem aus der *Einführung in die Algebra* bekannten *Chinesischen Restsatz*.

Zum Beweis der Eindeutigkeitsaussage (3) zeigen wir zunächst, dass man den Schritt von (1) zu (2) auch umkehren kann. In der Tat, ordnet man die Summanden aus (2) nach den Primelementen und (pro Primelement) nach aufsteigenden Exponenten, also etwa

$$M \cong R^k \oplus \bigoplus_{j=1}^{t} \bigoplus_{\iota=1}^{\ell(j)} (R/\mathfrak{p}_j^{\eta_{\iota j}}), \quad (\forall j\colon \eta_{1j} \leq \eta_{2j} \leq \ldots \leq \eta_{\ell(j)j})$$

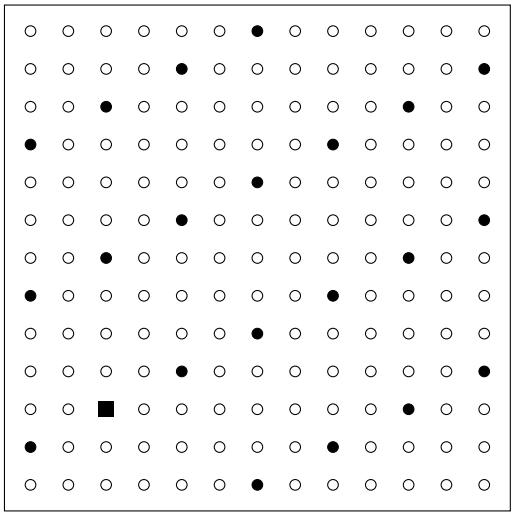
so kann man mit dem chinesischen Restsatz wieder Summanden, die zu *verschiedenen* Primidealen gehören, zu *einem* Term $R/\mathfrak{a}_i$ wie in (1) zusammenfassen, wobei man noch auf die Kettenbedingung

$$R \supset \mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \ldots \supseteq \mathfrak{a}_\ell \supset \{0_R\}$$

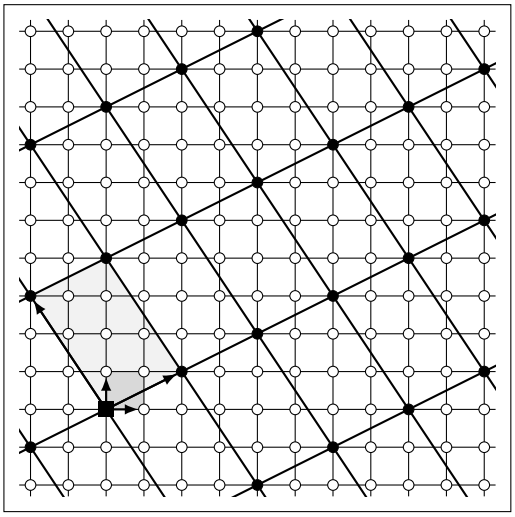
zu achten hat. Man stellt fest, dass die Kettenbedingung nur erfüllt wird, wenn man die Primidealpotenzen wie folgt zusammenfasst:[3] Man setze $\ell = \max\{\, \ell(j) : 1 \leq j \leq t \,\}$

[2] Das trägt der Tatsache Rechnung, dass man bei der Wahl von Erzeugern von M, also der Wahl des surjektiven Homomorphismus $g\colon R^n \to M$ auch n künstlich groß wählen kann, indem man überflüssig viele Erzeuger wählt.

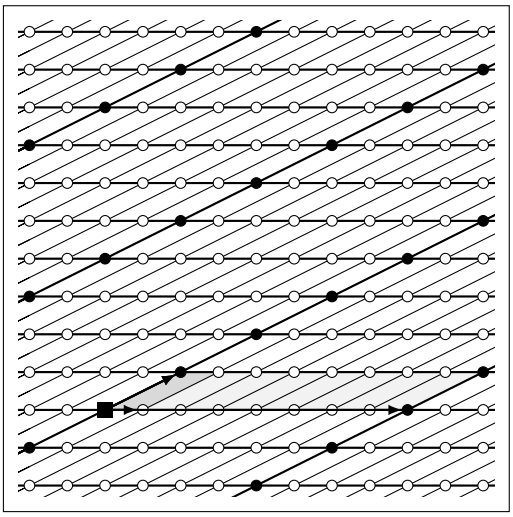
[3] Diese Überlegung mag beim ersten Lesen wegen der vielen Indizes und Parameter recht unverständlich wirken. Wir geben im Anschluss an diesen Beweis ein konkretes Beispiel hierzu, anhand



(a) Links: Veranschaulichung des freien $\mathbb{Z}$-Moduls $M = \mathbb{Z}^2 = \mathbb{Z}\binom{1}{0} \oplus \mathbb{Z}\binom{0}{1}$ und des darin enthaltenen (freien) Untermoduls $M' = \mathbb{Z}\binom{2}{1} \oplus \mathbb{Z}\binom{-2}{3}$ (schwarze Punkte), jeweils ohne Markierung von etwaig gewählten Basen. Das Nullelement $0 \in M$ ist durch ein Quadrat markiert.



(b) Dieselben Moduln wie oben, aber dieses mal mit eingezeichneten Gitterlinien, die von der Wahl der Basis $\binom{1}{0}$, $\binom{0}{1}$ von M und der Basis $\binom{2}{1}$, $\binom{-2}{3}$ von M' herrühren. Die Struktur des Faktormoduls M/M' ist hier nicht unmittelbar ersichtlich.



(c) Wieder dieselben Moduln, aber nun mit eingezeichneten Basen $\binom{2}{1}$, $\binom{1}{0}$, sowie $\binom{2}{1}$, $\binom{8}{0}$. Hier ergibt sich $M/M' = (\mathbb{Z}\binom{2}{1} \oplus \mathbb{Z}\binom{1}{0})/(\mathbb{Z}\binom{2}{1} \oplus \mathbb{Z}8\binom{1}{0}) \cong (\mathbb{Z}/\mathbb{Z}) \oplus (\mathbb{Z}/8\mathbb{Z}) \cong \mathbb{Z}/8\mathbb{Z}$.

Abbildung 23. Fortführung von Beispiel 7.7. Dort wurden für eine Matrix A invertierbare Matrizen $S, T \in \mathbb{Z}^{2\times 2}$ bestimmt derart, dass $SAT = \left(\begin{smallmatrix} 1 & \\ & 8 \end{smallmatrix}\right)$ in Smith-Normalform ist. Man beachte $AT = \left(\begin{smallmatrix} 2 & 8 \\ 1 & 0 \end{smallmatrix}\right)$ und vergleiche dies mit den in der Abbildung gewählten Basen.

und

$$\begin{cases} \mathfrak{a}_1 = \langle p_1^{\nu_{11}} p_2^{\nu_{12}} \cdots p_t^{\nu_{1t}} \rangle, \\ \mathfrak{a}_2 = \langle p_1^{\nu_{21}} p_2^{\nu_{22}} \cdots p_t^{\nu_{2t}} \rangle, \\ \quad \vdots \\ \mathfrak{a}_\ell = \langle p_1^{\nu_{\ell 1}} p_2^{\nu_{\ell 2}} \cdots p_t^{\nu_{\ell t}} \rangle, \end{cases}$$

mit Exponenten $\nu_{\bullet\bullet} \in \mathbb{N}_0$ gegeben durch

$$\nu_{ij} = \begin{cases} \eta_{\iota j} & \text{falls } \iota := i - (\ell - \ell(j)) \geq 1, \\ 0 & \text{sonst.} \end{cases}$$

Die Darstellungen aus (1) und (2) kann man also in eindeutiger Weise ineinander umrechnen. Es genügt daher die Eindeutigkeit der Daten in (2) zu zeigen. Der technische Vorteil besteht hierbei darin, dass $R/\mathfrak{p}$ ein Körper ist. (Die Primideale eines Hauptidealbereichs sind nämlich stets maximal, da diese jeweils von einem primen und also irreduziblen Element erzeugt werden und irreduzible Elemente maximale Ideale erzeugen.)

Wir beginnen zunächst mit dem Beweis der Eindeutigkeit von k. (Hierfür könnten wir tatsächlich auch mit (1) arbeiten.) Wir fassen R als Teilring seines Quotientenkörpers $K = \mathrm{Quot}(R)$ auf und beschäftigen uns mit einem Isomorphismus

$$M \cong R^k \oplus \bigoplus_{j=1}^{s} (R/\mathfrak{p}_j^{\nu_j})$$

wie in (2). Mit Korollar 6.8 folgt

$$\mathrm{Hom}_R(M,K) \cong \prod_{u=1}^{k} \mathrm{Hom}_R(R,K) \times \prod_{j=1}^{s} \mathrm{Hom}_R(R/\mathfrak{p}_j^{\nu_j}, K).$$

Laut Proposition 6.10 ist $\mathrm{Hom}_R(R,K) \cong K$. Andererseits besteht $\mathrm{Hom}_R(R/\mathfrak{a},K)$ für beliebige Ideale $\mathfrak{a} \supsetneq \{0_R\}$ nur aus der Nullabbildung, denn für jedes $f \in \mathrm{Hom}_R(R/\mathfrak{a},K)$ und $x \in R/\mathfrak{a}$ gilt für ein beliebiges Element $y \in \mathfrak{a} \setminus \{0_R\}$

$$\begin{aligned} f(x) &= 1_K f(x) = 1_R f(x) = y^{-1} y f(x) = y^{-1} f((y \bmod \mathfrak{a})x) \\ &= y^{-1} f((0 \bmod \mathfrak{a})x) = y^{-1} f(0_{R/\mathfrak{a}}) = y^{-1} 0_K = 0_K. \end{aligned}$$

Insgesamt ergibt sich also

$$\mathrm{Hom}_R(M,K) \cong K^k.$$

Nun lässt sich die auf $\mathrm{Hom}_R(M,K)$ (punktweise!) definierte R-Skalarmultiplikation aber auch in offensichtlicher Weise zu einer K-Skalarmultiplikation erweitern. Damit wird $\mathrm{Hom}_R(M,K)$ zu einem K-Vektorraum und der obige R-Modulisomorphismus erweist sich sogar als Isomorphismus von K-Vektorräumen, wie man unschwer erkennt, wenn man sich an dessen explizite Beschreibung in Korollar 6.8 entsinnt. Insbesondere handelt es sich bei k um die *Dimension* von $\mathrm{Hom}_R(M,K)$ als K-Vektorraum;

dessen die Idee hoffentlich als ganz offensichtlich erkannt werden kann und klar wird, dass die Schwierigkeit hier ganz und gar in der notwendig umständigen Notation begründet liegt.

Da diese — wie aus der linearen Algebra bekannt — eindeutig bestimmt ist, ist k eindeutig durch M bestimmt.

Zum Beweis der Eindeutigkeit der Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ nebst zugehöriger Exponenten $\nu_1, \ldots, \nu_s \in \mathbb{N}$ (bis auf Permutationen) bedienen wir uns einer ähnlichen Idee. Es sei N ein beliebiger R-Modul. Man beachte, dass zu beliebigem Primideal $\mathfrak{p}$ von R und Exponent $\nu \in \mathbb{N}$ die Skalarmultiplikation beim Faktormodul $\mathfrak{p}^{\nu-1}N/\mathfrak{p}^{\nu}N$ mit einem Skalar $\lambda \in R$ nur von der Restklasse λ mod $\mathfrak{p}$ abhängt. So wird $\mathfrak{p}^{\nu-1}N/\mathfrak{p}^{\nu}N$ zu einem $R/\mathfrak{p}$-Modul, also zu einem $R/\mathfrak{p}$-Vektorraum. (Man beachte unsere eingangs erwähnte Vorbemerkung, dass $R/\mathfrak{p}$ wirklich ein Körper ist.) Die Zahl

$$d_{\mathfrak{p}}^{\nu}(N) := \dim_{R/\mathfrak{p}}(\mathfrak{p}^{\nu-1}N/\mathfrak{p}^{\nu}N) \tag{8.4}$$

ist also wohl-definiert. Tatsächlich ist diese sogar invariant unter R-Modulisomorphismen, wie man sich mittels Lemma 8.1 überlegen kann, da dieses einen R-Modulisomorphismen zwischen den in (8.4) auftretenden Faktormoduln liefert und für die eben definierte Skalarmultiplikation unmittelbar sieht, dass diese von jenem Isomorphismus respektiert wird. Man bestätigt leicht die folgenden Rechenregeln (siehe unten):

- $d_{\mathfrak{p}}^{\nu}(M_1 \oplus M_2) = d_{\mathfrak{p}}^{\nu}(M_1) + d_{\mathfrak{p}}^{\nu}(M_2) < \infty$ für alle endlich erzeugten R-Moduln M_1 und M_2;
- $d_{\mathfrak{p}}^{\nu}(R) = 1$;
- $d_{\mathfrak{p}}^{\nu}(R/\mathfrak{q}^{\eta}) = 0$ jedes Primideal $\mathfrak{q} \neq \mathfrak{p}$ von R und jeden Exponenten $\eta \in \mathbb{N}$;
- $d_{\mathfrak{p}}^{\nu}(R/\mathfrak{p}^{\eta}) = 1$ falls $\nu \leq \eta$, und $= 0$ sonst.

Daraus folgert man leicht

$$d_{\mathfrak{p}}^{\nu}(M) = k + \#\{1 \leq j \leq s : \mathfrak{p} = \mathfrak{p}_j \text{ und } \nu \leq \nu_j\}.$$

Das liefert die Eindeutigkeitsaussage. (Tatsächlich erhalten wir unter Berücksichtigung von $\lim_{\nu\to\infty} d_{\mathfrak{p}}^{\nu}(M) = k$ einen zweiten Beweis für die Eindeutigkeit von k.)

Wir skizzieren abschließend noch ein paar Kernpunkte zu den oben erwähnten Rechenregeln. Die erste sei den Leserinnen und Lesern überlassen. Für die übrigen drei seien $\mathfrak{p} = \langle p \rangle$ und $\mathfrak{q} = \langle q \rangle$ zwei verschiedene Primideale von R. Nun sind alle drei Moduln R, $R/\mathfrak{q}^{\eta}$ und $R/\mathfrak{p}^{\eta}$ von einem Element erzeugbar (nämlich 1_R, $1_R + \mathfrak{q}^{\eta}$ bzw. $1_R + \mathfrak{p}^{\eta}$). Da sich dies auf den Faktormodul in (8.4) überträgt, ist die zugehörige Dimension als $R/\mathfrak{p}$-Vektorraum höchstens 1. Wegen $p^{\nu-1} \notin \mathfrak{p}^{\nu}$ folgt daraus schon $d_{\mathfrak{p}}^{\nu}(R) = 1$. Ferner ist $p + \mathfrak{q}^{\eta} \in R/\mathfrak{q}^{\eta}$ eine Einheit und dementsprechend ist $\mathfrak{p}^{\nu}N = N$ für $N = R/\mathfrak{q}^{\eta}$. Das zeigt $d_{\mathfrak{p}}^{\nu}(R/\mathfrak{q}^{\eta}) = 0$. Nun sei $N = R/\mathfrak{p}^{\eta}$. Ist $\nu > \eta$, so ist $\mathfrak{p}^{\nu-1}N$ der Nullmodul und es folgt $d_{\mathfrak{p}}^{\nu}(R/\mathfrak{p}^{\eta}) = 0$. Analog sieht man für $\nu \leq \eta$ wegen $p^{\nu-1} \notin \mathfrak{p}^{\eta}$, dass $d_{\mathfrak{p}}^{\nu}(R/\mathfrak{p}^{\eta})$ nicht gleich 0 (und somit gleich 1) ist. □

Wir diskutieren anhand eines Beispiels, wie man in Satz 8.2 von (2) auf (1) kommt.

Beispiel. Man betrachte

$$\begin{aligned} M := &((\mathbb{Z}/2^2\mathbb{Z}) \oplus (\mathbb{Z}/2^3\mathbb{Z}) \oplus (\mathbb{Z}/2^3\mathbb{Z})) \oplus \\ &\oplus ((\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/3^5\mathbb{Z})) \oplus \\ &\oplus (\mathbb{Z}/5\mathbb{Z}) \oplus \\ &\oplus ((\mathbb{Z}/7^2\mathbb{Z}) \oplus (\mathbb{Z}/7^2\mathbb{Z})). \end{aligned}$$

Wir denken uns die Summanden als $\mathbb{Z}/p_j^{\eta_{ij}}\mathbb{Z}$ und tabellieren die Exponenten wie folgt:

$\iota \setminus j$	1	2	3	4
1	2	1		
2	3	1		2
3	3	5	1	2

Liest man dieses Schema nun zeilenweise, wobei Leerstände als Null-Exponenten zu verstehen sind, so erhält man

$$M \cong (\mathbb{Z}/2^2 3^1\mathbb{Z}) \oplus (\mathbb{Z}/2^3 3^1 7^2\mathbb{Z}) \oplus (\mathbb{Z}/2^3 3^5 5^1 7^2\mathbb{Z}).$$

Man beachte ferner $2^2 3^1 \mid 2^3 3^1 7^2 \mid 2^3 3^5 5^1 7^2$ und man macht sich leicht klar, dass die hier gefundene Gruppierung der Exponenten die einzige ist, welche diese Teilerkettenbedingung realisiert. (Man erprobe dies etwa dadurch, dass man die Spalten mit Leerständen in obiger Tabelle nach oben schiebt.)

Beispiel. Wir berechnen $d_\mathfrak{p}^\nu(M)$ für

$$M = R^{10} \oplus (R/\mathfrak{p}) \oplus (R/\mathfrak{p}) \oplus (R/\mathfrak{p}^2) \oplus (R/\mathfrak{p}^4) \oplus (R/\mathfrak{q}),$$

wobei $\mathfrak{p} \neq \mathfrak{q}$ zwei verschiedene Primideale von R bezeichnen mögen. Unter Ausnutzung der im Beweis von Satz 8.2 gegebenen Rechenregeln erhält man beispielsweise

$$\begin{aligned} d_\mathfrak{p}^2(M) &= 10 d_\mathfrak{p}^2(R) + d_\mathfrak{p}^2(R/\mathfrak{p}) + d_\mathfrak{p}^2(R/\mathfrak{p}) + d_\mathfrak{p}^2(R/\mathfrak{p}^2) + d_\mathfrak{p}^2(R/\mathfrak{p}^4) + d_\mathfrak{p}^2(R/\mathfrak{q}) \\ &= 10 \cdot 1 + 0 + 0 + 1 + 1 + 0 = 12. \end{aligned}$$

Ganz analog berechnet man die übrigen Einträge in der folgenden Tabelle:

ν	1	2	3	4	5	6	…
$d_\mathfrak{p}^\nu(M)$	14	12	11	11	10	10	…
$d_\mathfrak{p}^\nu(M) - d_\mathfrak{p}^{\nu+1}(M)$	2	1	0	1	0	0	…

Aus der letzten Zeile lässt sich offenbar die Anzahl der Summanden $R/\mathfrak{p}^\nu$ ablesen, welche in M vorkommen. Ferner gibt der konstante Rest der mittleren Zeile den Rang von M an.

Bemerkung 8.4. Man beachte die „fundamentale Beobachtung“ aus dem Beweis von Satz 8.2 und beachte, dass diese eine Strategie suggeriert, um die Invarianten und

den Isomorphismus aus Satz 8.2 (1) explizit zu berechnen. Was man hierzu benötigt ist eine exakte Sequenz

$$R^m \xrightarrow{f} R^n \twoheadrightarrow M \longrightarrow 0,$$

bei der man $[f]_m^n$ berechnen, und anschließend auf Smith-Normalform bringen kann. Unter diesem Gesichtspunkt studiere man erneut Abbildung 23 und beachte auch die Zusatzaufgaben auf Seite 153.

Zur Illustration der in Bemerkung 8.4 erwähnten Strategie geben wir ein Beispiel. Eine kompliziertere Variante davon ist Aufgabe 15.1.

Beispiel. Angenommen, wir haben eine abelsche Gruppe G von der wir wissen, dass sie von vier Elementen $a, b, c, d \in G$ erzeugt wird: $G = \langle a, b, c, d\rangle$. Ferner sei bekannt, dass zwischen a, b, c und d die folgenden ***Relationen*** gelten:

$$20a = 12b + 3c, \quad 4b = c, \quad c = d.$$

(Mit Blick auf die letzte Relation sehen wir schon, dass c und d gleich sind und man sich auf $G = \langle a, b, c\rangle$ einschränken könnte. Wir kürzen hier allerdings absichtlich nicht ab.) Wir betrachten nun den surjektiven $\mathbb{Z}$-Modulhomomorphismus $g\colon \mathbb{Z}^4 \to G$ mit

$$\begin{pmatrix}1\\0\\0\\0\end{pmatrix} \mapsto a, \quad \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \mapsto b, \quad \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \mapsto c, \quad \begin{pmatrix}0\\0\\0\\1\end{pmatrix} \mapsto d.$$

Die oben angegebenen Relationen liefert die folgenden Elemente im Kern von g:

$$\begin{pmatrix}20\\-12\\-3\\0\end{pmatrix}, \begin{pmatrix}0\\4\\-1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\-1\end{pmatrix} \in \ker g.$$

Wir gehen davon aus, dass die obigen Relationen alle Relationen sind, in dem Sinne, dass sich alle weiteren Relationen zwischen den Erzeugern a, b, c und d von G aus diesen ableiten lassen; oder äquivalent: wir nehmen an, dass die obigen drei Vektoren den Kern von g erzeugen. Unsere eben getroffene Annahme garantiert, dass der $\mathbb{Z}$-Modulhomomorphismus $f\colon \mathbb{Z}^3 \to \mathbb{Z}^4$ mit

$$f\begin{pmatrix}1\\0\\0\end{pmatrix} = \begin{pmatrix}20\\-12\\-3\\0\end{pmatrix}, \quad f\begin{pmatrix}0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\4\\-1\\0\end{pmatrix}, \quad f\begin{pmatrix}0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\1\\-1\end{pmatrix}$$

genau $\operatorname{im} f = \ker g$ erfüllt. Natürlich ist

$$[f]_3^4 = \begin{pmatrix} 20 & 0 & 0 \\ -12 & 4 & 0 \\ -3 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix}.$$

Wir transformieren $[f]_3^4$ nun auf Smith-Normalform. Durchführung des bekannten Gauß-artigen Verfahrens liefert:

$$[f]_3^4 \rightsquigarrow \ldots \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix}.$$

Wie in (8.3) ergibt sich

$$G \cong \frac{\mathbb{Z}}{1\mathbb{Z}} \oplus \frac{\mathbb{Z}}{1\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4\mathbb{Z}} \oplus \frac{\mathbb{Z}}{0\mathbb{Z}} \cong \frac{\mathbb{Z}}{4\mathbb{Z}} \oplus \mathbb{Z}$$

und es genügen tatsächlich zwei statt vier Erzeuger. Mit etwas mehr Geduld könnte man sich nun auch noch Matrizen überlegen, welche $[f]_3^4$ auf Smith-Normalform transformieren und daraus ergäben sich dann auch explizite Darstellungen von Elementen (als $\mathbb{Z}$-Linearkombinationen der ursprünglich gewählten Erzeuger a, b, c und d von G), welche unter dem eben notierten Isomorphismus die Rollen von $(1_{\mathbb{Z}/4\mathbb{Z}}, 0_{\mathbb{Z}})$ und $(0_{\mathbb{Z}/4\mathbb{Z}}, 1_{\mathbb{Z}})$ übernehmen können.

8.2. Klassifikation endlich erzeugter abelscher Gruppen

Wir erkennen nun Beispiel 6.1 leicht als Spezialfall von Satz 8.2 (1). Zur Illustration bestimmen wir alle abelschen Gruppen $72 = 2^3 3^2$ Elementen bis auf Isomorphie (siehe auch [33, Beispiel 5.4]). Die Zahl 72 könnte hier problemlos durch eine beliebige andere Zahl ausgetauscht werden, deren Primfaktorzerlegung man kennt. Im Verlauf des Beispiels zeigt sich allerdings schnell, dass „spannende“ Effekte erst sichtbar werden, wenn man eine Zahl mit hinreichend reichhaltiger Primfaktorzerlegung wählt.

Beispiel 8.5 (Isomorphietypen abelscher Gruppen mit 72 Elementen)**.** Da es sich bei den abelschen Gruppen mit genau $72 = 2^3 3^2$ Elementen genau um die $\mathbb{Z}$-Moduln mit genau 72 Elementen handelt, ist Satz 8.2 anwendbar. Sei M also ein $\mathbb{Z}$-Modul mit 72 Elementen. Jedes Element von M hat endliche Ordnung. Man sieht also, dass M ein Torsionsmodul ist und Satz 8.2 liefert einen Isomorphismus

$$M \cong \bigoplus_{i=1}^{\ell} (\mathbb{Z}/a_i\mathbb{Z})$$

mit (o.B.d.A. positiven) ganzen Zahlen $1 < a_1 \mid a_2 \mid \ldots \mid a_\ell$ (a_1 teilt a_2, a_2 teilt a_3, etc.). Ferner ist

$$72 = \#M = \#\Big(\bigoplus_{i=1}^{\ell}(\mathbb{Z}/a_i\mathbb{Z})\Big) = \prod_{i=1}^{\ell}\#(\mathbb{Z}/a_i\mathbb{Z}) = a_1a_2\cdots a_\ell.$$

Zusammen mit der eindeutigen Primfaktorzerlegung in $\mathbb{Z}$ liefert dies hinreichend starke Einschränkungen an die a_i, um diese zu bestimmen. Schreiben wir abkürzend C_d für den $\mathbb{Z}$-Modul $\mathbb{Z}/d\mathbb{Z}$, so haben wir nur die folgenden Möglichkeiten:

ℓ	$a_1 \mid \ldots \mid a_\ell$	Isomorphietyp von M gemäß …	
		Satz 8.2 (1)	Satz 8.2 (2)
1	72	C_{72}	$C_{2^3} \oplus C_{3^2}$
2	2 | 36	$C_2 \oplus C_{36}$	$C_2 \oplus C_{2^2} \oplus C_{3^2}$
2	3 | 24	$C_3 \oplus C_{24}$	$C_{2^3} \oplus C_3 \oplus C_3$
2	6 | 12	$C_6 \oplus C_{12}$	$C_2 \oplus C_{2^2} \oplus C_3 \oplus C_3$
3	2 | 2 | 18	$C_2 \oplus C_2 \oplus C_{18}$	$C_2 \oplus C_2 \oplus C_2 \oplus C_{3^2}$
3	2 | 6 | 6	$C_2 \oplus C_6 \oplus C_6$	$C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_3$

Aufgrund der Eindeutigkeitsaussage in Satz 8.2 sind auch alle diese Isomorphietypen paarweise verschieden (und treten selbstverständlich auch auf, da wir ja in der Tabelle entsprechende Moduln auch angegeben haben).

Beispiel 8.6 (Isomorphietypen von endlichen abelschen Gruppen)**.** In Verallgemeinerung von Beispiel 8.5 erkennt man mittels der Klassifikation aus Satz 8.2 (2) und der zugehörigen Eindeutigkeitsaussage Folgendes: Ist $n = p_1^{\nu_1}\cdots p_t^{\nu_t}$ die Primfaktorzerlegung von $n > 1$, so gilt für die Anzahl $a(n)$ der Isomorphietypen abelscher Gruppen mit genau n Elementen

$$a(n) = p(\nu_1)\cdots p(\nu_t),$$

wobei $p(\nu)$ die Anzahl der Möglichkeiten bezeichne, mit denen man ν in eine Summe positiver ganzer Zahlen zerlegen kann;[4] Beispielsweise haben wir

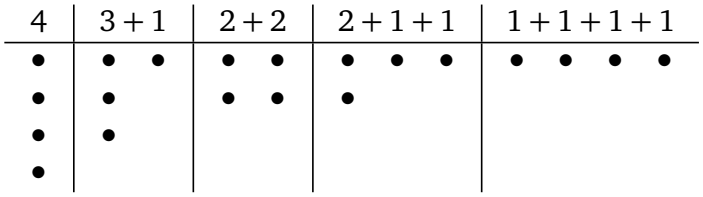
$$p(1) = 1, \quad p(2) = 2, \quad p(3) = 3, \quad p(4) = 5,$$

wegen $2 = 1+1$, $3 = 2+1 = 1+1+1$ und

$$4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1.$$

[4]Hier ist einer der seltenen Fälle in dieser Vorlesung, wo der Buchstabe p nicht für eine Primzahl steht. Die Bezeichnung $p(\cdot)$ für die hier angesprochene Partitionsfunktion ist allerdings hinreichend ubiquitär, dass es unseriös gewirkt hätte, diese umzubenennen.

Man veranschaulicht sich solche Partitionen auch gerne mittels sogenannten ***Ferrers-Diagrammen***, hier etwa für $p(4)$:



Gemäß der obigen Formel reproduzieren wir auch das Ergebnis aus Beispiel 8.5, dass es genau $a(72) = a(2^3\,3^2) = p(3)p(2) = 3 \cdot 2 = 6$ verschiedene Isomorphietypen von abelschen Gruppen mit genau 72 Elementen gibt.

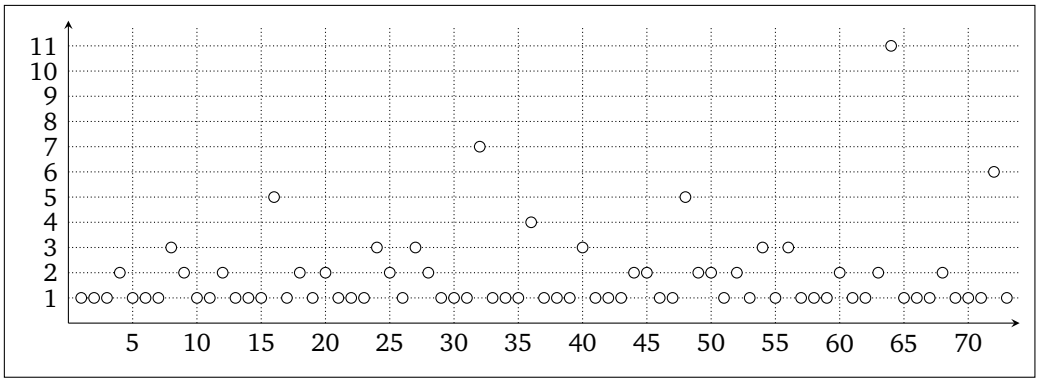


Abbildung 24. Plot der Werte $a(1), a(2), \ldots, a(73)$, wobei $a(n)$ die Anzahl der verschiedenen Isomorphietypen abelscher Gruppen mit genau n Elementen bezeichnet.

8.3. $K[X]$-Moduln und Normalformen

Das nächste Beispiel ist eine Fortsetzung von Beispiel 6.2 und von seiner Aussage her natürlich nichts Neues. Die Absicht ist hier nur hervorzuheben, dass Satz 8.2 auch die Klassifikation endlich-dimensionaler Vektorräume mit einschließt. (Man beachte allerdings, dass wir während des Beweises von Satz 8.2 (3) auch schon auf den Dimensionsbegriff für Vektorräume zurückgegriffen haben.)

Beispiel 8.7 (Vektorraumdimension)**.** Sei K ein Körper und V ein endlich erzeugter K-Modul, also ein endlich-dimensionaler K-Vektorraum. Dann ist V natürlich torsionsfrei (denn für $x \in V$ und $\lambda \in K \setminus \{0_K\}$ ist $\lambda^{-1}(\lambda x) = (\lambda^{-1}\lambda)x = 1_K x = x$, also $\lambda x \neq 0$) und Satz 8.2 liefert $V \cong K^k$ für eine eindeutig bestimmte Zahl $k \in \mathbb{N}_0$. Selbstverständlich ist $k = \dim_K V$ die wohl-bekannte Vektorraumdimension.

Sei K ein Körper. Wir hatten bereits in Beispiel 6.3 festgestellt, dass jeder K-Vektorraum V zusammen mit einem Endomorphismus $f\colon V \to V$ und der dadurch

induzierten Skalarmultiplikation

$$K[X] \times V \longrightarrow V, \quad (P, v) \longmapsto Pv := (P(f))(v)$$

zu einem $K[X]$-Modul wird.

Beispiel. $(X^2 - X + 3, v) \mapsto f(f(v)) - f(v) + 3\,\mathrm{id}_V(v)$.

Tatsächlich entsteht jeder $K[X]$-Modul V auf diese Weise, denn die Einschränkung der Skalarmultiplikation auf $K \times V$ (siehe Bemerkung 6.6) macht V zu einem K-Vektorraum und durch die Vorschrift $v \mapsto Xv$ erhält man einen K-Vektorraum-Endomorphismus f von V, der bezüglich der zuvor beschriebenen Operation auch die $K[X]$-Modulstruktur auf V reproduziert.

Die obige Diskussion liefert also zueinander inverse Operationen[5]

$$\{K[X]\text{-Moduln } V\} \underset{\sim}{\rightleftarrows} \left\{\begin{array}{l}\text{Paare } (V, f)\\ \text{mit } K\text{-Vektorraum } V\\ \text{und } f \in \mathrm{Hom}_K(V, V)\end{array}\right\}.$$

Zwischen zwei K-Vektorräumen V und W gibt es im Allgemeinen viele Homomorphismen. *Welche davon sind auch $K[X]$-Modulhomomorphismen, wenn auf V und W auch jeweils $K[X]$-Modulstrukturen gegeben sind?* Die fraglichen $K[X]$-Modulstrukturen seien gegeben durch Abbildungen $f \in \mathrm{Hom}_K(V, V)$ und $g \in \mathrm{Hom}_K(W, W)$. Ist $\Phi\colon V \to W$ ein $K[X]$-Modulhomomorphismus, so gilt für jedes $v \in V$

$$(\Phi \circ f)(v) = \Phi(f(v)) = \Phi(Xv) = X\Phi(v) = g(\Phi(v)) = (g \circ \Phi)(v).$$

Wir haben also $\Phi \circ f = g \circ \Phi$, d.h. das Diagramm

$$\begin{array}{ccc} V & \xrightarrow{\Phi} & W \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} \\ V & \xrightarrow{\Phi} & W \end{array}$$

kommutiert. Umgekehrt rechnet man auch leicht nach, dass jeder K-Vektorraumhomomorphismus $\Phi\colon V \to W$ mit $\Phi \circ f = g \circ \Phi$ sogar ein $K[X]$-Modulhomomorphismus ist. Wir fassen dies durch Ergänzung des obigen Schaubildes wie folgt suggestiv

[5] Hier sollte man etwas Vorsicht walten lassen, da die Gesamtheit aller $K[X]$-Moduln von der hier die Rede ist, *keine Menge*, sondern eine *echte Klasse* bildet. Derartigen mengentheoretischen Problemen kann man mithilfe von Klassen, oder Grothendieck-Universen ausweichen, aber der zweckmäßigste Zugang ist vielleicht, diese hier einfach zu ignorieren; Tatsächlich wenden wir im Folgenden den Dualismus zwischen $K[X]$-Moduln V und Paaren (V, f) ohnehin stets nur für einzelne Moduln an.

zusammen:

$$\left\{\begin{array}{l}K[X]\text{-Moduln } V\\ \hline K[X]\text{-Modulhom. } \Phi\colon V\to W\end{array}\right\} \begin{array}{c}\longrightarrow\\[-4pt] \overset{\sim}{\longleftarrow}\end{array} \left\{\begin{array}{l}\text{Paare } (V,f)\\ \text{mit } K\text{-Vektorraum } V\\ \text{und } f\in \mathrm{Hom}_K(V,V)\\ \hline K\text{-Vektorraumhom.}\\ \Phi\colon (V,f)\to(W,g)\\ \text{mit } \Phi\circ f = g\circ\Phi\end{array}\right\}.$$

Sei (V,f) nun ein $K[X]$-Modul, der als K-Vektorraum endliche Dimension hat. Dann ist $\mathrm{Hom}_K(V,V)$ endlich-dimensional und die unendliche Folge von K-linearen Abbildungen

$$v\longmapsto X^0v,\quad v\longmapsto X^1v,\quad v\longmapsto X^2v,\quad \dots$$

ist K-linear abhängig. Es gibt also ein Polynom $P\in K[X]$ derart, dass *für alle* $v\in V$ die Gleichung $Pv=0$ gilt. (Das normierte Polynom kleinsten Grades mit dieser Eigenschaft ist das aus der linearen Algebra bekannte ***Minimalpolynom von*** f.) Insbesondere ist V als $K[X]$-Modul ein Torsionsmodul.[6] Mit Satz 8.2 (2) finden wir also einen $K[X]$-Modulisomorphismus

$$\Phi\colon V\xrightarrow{\sim}\bigoplus_{j=1}^{s}(K[X]/\mathfrak{p}_j^{\nu_j})$$

für geeignete Primideale $\mathfrak{p}_1,\dots,\mathfrak{p}_s$ und Exponenten $\nu_1,\dots,\nu_s\in\mathbb{N}$.

In jedem $K[X]$-Modul $K[X]/\mathfrak{q}$ mit Ideal $\mathfrak{q}=\langle P^\nu\rangle$, $P\in K[X]$ irreduzibel und normiert, und $\nu\in\mathbb{N}$, bildet

$$\mathscr{B}\colon \underbrace{1,\ X,\ \dots,X^{\deg P-1}}_{\text{Block aus }\deg P\text{ Elementen}},\ \underbrace{P,\ XP,\ \dots,X^{\deg P-1}P}_{\text{Block aus }\deg P\text{ Elementen}},\ \dots,\ \underbrace{P^{\nu-1},\ XP^{\nu-1},\ \dots,X^{\deg P-1}P^{\nu-1}}_{\text{Block aus }\deg P\text{ Elementen}}$$

nach Reduktion modulo $\mathfrak{q}$ eine K-Basis von $K[X]/\mathfrak{q}$ als K-Vektorraum. Wählt man für jeden Summanden $K[X]/\mathfrak{p}_j^{\nu_j}$ mit $\mathfrak{p}_j=\langle P_j\rangle$ und $P_j\in K[X]$ normiert eine Basis nach diesem Schema so erhält man ein kommutatives Diagramm von K-Vektorräumen

$$\begin{array}{ccc} V & \xrightarrow{\quad f\quad} & V\\ \Phi\downarrow\wr & & \Phi\downarrow\wr\\ \displaystyle\bigoplus_{j=1}^{s}(K[X]/\mathfrak{p}_j^{\nu_j}) & \xrightarrow[\text{(Komponentenweise)}]{Q\mapsto XQ \bmod \mathfrak{p}_j^{\nu_j}} & \displaystyle\bigoplus_{j=1}^{s}(K[X]/\mathfrak{p}_j^{\nu_j})\\ \downarrow\wr & & \downarrow\wr\\ \displaystyle\bigoplus_{j=1}^{s}K^{\nu_j\deg P_j} & \xrightarrow{\quad v\mapsto Av\quad} & \displaystyle\bigoplus_{j=1}^{s}K^{\nu_j\deg P_j}, \end{array}$$

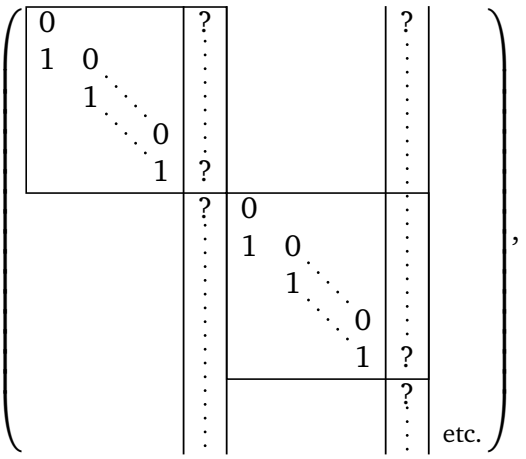
wobei das obere Quadrat kommutiert, da Φ ein $K[X]$-Modulisomorphismus ist, und die Matrix A so gewählt sei, dass auch das untere Quadrat kommutiert.

[6] Achtung: *Als K-Modul* (also als K-Vektorraum) ist V natürlich frei und insbesondere *torsionsfrei*.

Wie sieht A aus? — Da die mittlere horizontale Abbildung in obigem Diagramm die einzelnen Summanden respektiert, hat A jedenfalls schon mal Blockdiagonalgestalt, bestehend aus s Blöcken und der j-te Block besteht aus der Darstellungsmatrix der linearen Abbildung

$$K[X]/\mathfrak{q} \longrightarrow K[X]/\mathfrak{q}, \quad Q \mapsto XQ \bmod \mathfrak{q}, \quad (\mathfrak{q} = \mathfrak{p}_j^{\nu_j})$$

bezüglich der oben gewählten Basis. Wir lassen den Index j für den Moment weg und betrachten die Basis $\mathscr{B}$ von oben. Die darzustellende lineare Abbildung, die als Multiplikation mit $X \bmod \mathfrak{p}^\nu$ wirkt, bildet den i-ten Vektor in den Blöcken von $\mathscr{B}$ auf den $(i+1)$-ten Vektor ab, sofern dieser sich noch im selben Block befindet. (Mit „Block“ meinen wir die oben mit geschweiften Klammern gruppierten Vektoren). Die fragliche Darstellungsmatrix sieht also wie folgt aus:



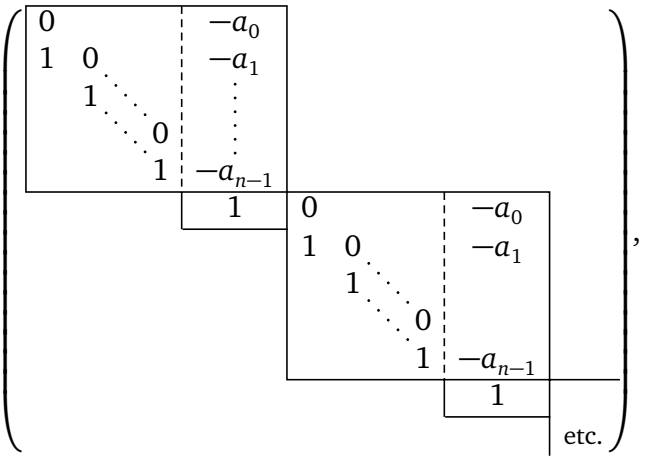
wobei hier jede $(\deg P)$-te Spalte eine noch näher zu bestimmende „?“-Spalte ist. Um auch diese zu bestimmen, schreiben wir

$$P = X^n + a_{n-1}X^{n-1} + a_1X + a_0$$

und bemerken

$$\begin{aligned} X(X^{\deg P-1}P^i) &= X^nP^i = (P - a_{n-1}X^{n-1} - \ldots - a_1X - a_0)P^i \\ &= P^{i+1} - a_{n-1}X^{n-1}P^i - \ldots - a_1XP^i - a_0P^i. \end{aligned} \tag{8.5}$$

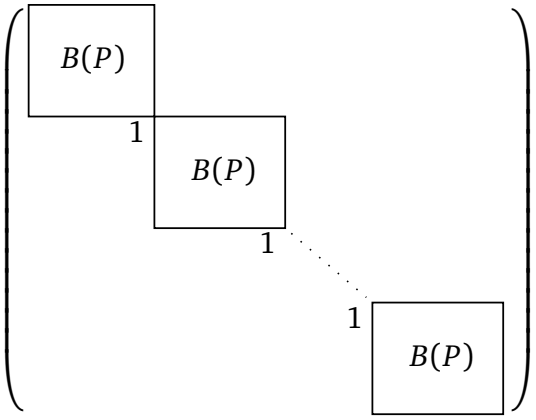
Die obige Matrix hat also die Form



also Blockdiagonalform mit quadratischen Blöcken

$$B(P) = \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & -a_1 \\ & \ddots & 0 & \vdots \\ & & 1 & -a_{n-1} \end{pmatrix} \in K^{n\times n},$$

die durch sogenannte ***Verkettungseinsen*** miteinander verbunden sind:



(Man beachte, dass unter dem letzten $B(P)$-Block keine Verkettungseins mehr auftritt, da der Term P^{i+1} in (8.5) für $i = \nu - 1$ nach Reduktion modulo $\mathfrak{q} = \langle P^\nu \rangle$ wegfällt.) Die Matrix $B(P)$ heißt ***Begleitmatrix zum Polynom P***. Die Matrix A besteht nun aus Blöcken dieser Bauart. Die so erhaltene Normalform nennt man oft ***(primäre) rationale Normalform***, oder auch gelegentlich ***Frobenius-Normalform***, obwohl man in der Literatur auch häufig Varianten hiervon findet, die von einer anderen Basiswahl $\mathscr{B}$ herrühren; In jedem Fall ist das zugrundeliegende Prinzip aber Satz 8.2 (ob in der Form (2), oder (1)).

Man kann auch hier wieder zugehörige Eindeutigkeitsaussagen treffen, aber wir verzichten auf die zugehörigen Ausführungen.

Speziell wenn der Körper K algebraisch abgeschlossen ist, sind die obigen Primideale $\mathfrak{p}_j$ von der Form $\mathfrak{p}_j = \langle X - x_j \rangle$ für geeignete $x_j \in K$. Die zugehörigen Matrizen $B(X - x_j)$ haben die Form $B(X - x_j) = (x_j) \in K^{1\times 1}$. Wir erhalten das folgende Resultat:

Korollar 8.8 (Jordansche Normalform)**.** *Sei V ein Vektorraum über einem algebraisch abgeschlossenen Körper K und $f : V \to V$ ein Endomorphismus. Dann gibt es eine Basis von V bezüglich der sich f als Blockdiagonalmatrix darstellt, wobei die Blöcke auf der Diagonalen konstant sind, auf der ersten unteren Nebendiagonalen konstant Eins sind, und sonst überall Nullen als Einträge haben.*

Wir schließen mit der folgenden Serie von Behauptungen, die der Leserin oder dem Leser zur freiwilligen Übung überlassen sein. (*Achtung:* Hierzu sollte man mit den hier geführten Beweisen sehr vertraut sein!)

- Sei nun K ein Körper und B eine beliebige $n\times n$-Matrix über K. Der $K[X]$-Modul (K^n, f_B) mit $f_B \colon K^n \to K^n$, $v \mapsto Bv$ ist dann (als $K[X]$-Modul!) isomorph zum Faktormodul $(K[X])^n/M'$, wobei M' das Bild des $K[X]$-Homomorphismus

$$(K[X])^n \longrightarrow (K[X])^n, \quad \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \longmapsto \left(X \begin{pmatrix} 1_K & & \\ & \ddots & \\ & & 1_K \end{pmatrix} - B \right) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

  bezeichne. (Für mehr Details siehe Aufgabe 15.3!)
- Man benutze die obige Aussage für $K = \mathbb{C}$ und

$$B = \begin{pmatrix} 1 & 3 & 0 & 2 \\ 0 & 0 & 0 & -1 \\ 0 & 1 & 1 & 1 \\ 0 & 2 & 0 & 3 \end{pmatrix}$$

  um zu zeigen, dass der $\mathbb{C}[X]$-Modul $(\mathbb{C}^n, f_B)$ isomorph zu

$$\frac{\mathbb{C}[X]}{\langle X-1\rangle} \oplus \frac{\mathbb{C}[X]}{\langle (X-1)^2(X-2)\rangle} \cong \frac{\mathbb{C}[X]}{\langle X-1\rangle} \oplus \frac{\mathbb{C}[X]}{\langle (X-1)^2\rangle} \oplus \frac{\mathbb{C}[X]}{\langle X-2\rangle}$$

  ist. (Einige Vorarbeit wurde schon in Beispiel 7.6 geleistet; Man reflektiere auch erneut über Bemerkung 8.4 und erinnere sich an (8.3).)
- Man folgere aus den obigen Ergebnissen, dass es eine invertierbare Matrix $T \in \mathbb{C}^{4\times 4}$ mit

$$T^{-1}BT = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & 1 & 1 & \\ & & & 2 \end{pmatrix}$$

gibt. (Das gewünschte Lernziel hier ist die Einsicht, dass das Vorgehen aus Beispiel 7.6 zur Bestimmung der rationalen Normalform einer durch eine Matrix gegebenen linearen Abbildung hergenommen werden kann.)

Als letzte Anwendung geben wir noch ein unscheinbares Ergebnis aus der *linearen Algebra* an, für dessen Beweis die hier entwickelte Theorie instrumentell ist. Ungeachtet der Einfachheit der folgenden Aussage, ist mir dennoch kein Beweis davon bekannt, welcher mit weniger starken Mitteln auskommt.

Korollar 8.9. *Sei K ein beliebiger Körper und A eine $n\times n$-Matrix über K. Dann ist A ähnlich zu ihrer Transponierten.*

Beweis. Es gilt $K_A^n \cong K_{A^{\mathrm{T}}}^n$ (als $K[X]$-Moduln) nachzuweisen. Gemäß der obigen Kommentare ist der Isomorphietyp dieser Moduln allerdings durch die Smith-Normalform von $X\mathbf{1}_n - A$ bzw. von $X\mathbf{1}_n - A^{\mathrm{T}} = (X\mathbf{1}_n - A)^{\mathrm{T}}$ bestimmt. Jene Smith-Normalformen stimmen allerdings gemäß Aufgabe 14.3 überein. Daraus folgt die Behauptung. □

8.4. Wohin nun?

Wir haben nun zwei große Anwendungsbeispiele für den *Hauptsatz* (Satz 8.2) gesehen:

- die Klassifikation endlich erzeugter abelscher Gruppen (§ 8.2) und
- die Frobenius-Normalform (§ 8.3).

Das angesprochene Klassifikationsergebnis war uns bereits aus der *Einführung in die Algebra* jedenfalls für *endliche* abelsche Gruppen bekannt ([33, Satz 5.3]). Tatsächlich hatten wir mit [33, Proposition 5.1] aber fast schon den ganzen Hauptsatz für $R = \mathbb{Z}$ in der Hand. Was fehlte, war die allgemeine Form der Eindeutigkeitsaussage in Satz 8.2 (3). Damals scheiterte es jedoch nicht an technischer Fähigkeit, sondern eher an Faulheit. Unter Ausnutzung vom Sylow-Satz zur Existenz von p-Untergruppen ließ sich der Eindeutigkeitsbeweis im Falle endlicher Gruppen nämlich in abgekürzter Form behandeln.

Hingegen die Frobenius-Normalform ist häufig nicht aus der *linearen Algebra* bekannt. Dennoch mag man in vielerlei Anwendungen auch damit auskommen, vom ursprünglich gegebenem Körper K zu einem algebraischen Abschluss überzugehen und die zu betrachtende lineare Abbildung (bzw. Matrix) über jenem Abschluss auf Jordan-Normalform zu transformieren. Das erlaubt zwar immer noch keine Transformation auf Normalform mit Matrizen mit Einträgen aus K, doch die im Anschluss über dem algebraischen Abschluss arbeitend gewinnbare Information reicht gegebenenfalls trotzdem bereits zur Lösung von welchem Problem auch immer, das den Drang zur Untersuchung der fraglichen linearen Abbildung überhaupt erst aufgeworfen hat.

Die obige Reflexion mag vielleicht zu fragen anregen, inwieweit der hier zum Beweis von Satz 8.2 investierte Aufwand sich überhaupt auszahlt; Leserinnen und Leser sollten sich an dieser Stelle auch fragen, wie viele Hauptidealbereiche wir

überhaupt kennen! ($\mathbb{Z}$, Körper K und den Polynomring $K[X]$, $\mathbb{Z}[\mathrm{i}]$. Kennen Sie mehr?) Wir geben zwei Antworten.

Zum einen hatten wir schon eingangs in § 6.1 in Kapitel 6 besprochen, dass wir mit Satz 8.2 nun von außen unverwandt aussehende Strukturergebnisse als Konsequenz einer umfassenderen Theorie erkennen. Das allein sollte ein gewisses Maß an intellekuteller Befriedigung stiften.

Als zweiten Grund ist zu nennen, dass Hauptidealbereiche und Moduln über diesen tatsächlich in der (mathematischen) Praxis auftreten, uns aber in dieser Lehrveranstaltung der Rahmen nicht gestattet, dies näher zu beleuchten. Quellen solcher Beispiele sind etwa die *algebraische Zahlentheorie* und die *algebraische Geometrie*. In [33, Kapitel 10] hatten wir beispielsweise gesehen, dass Ringerweiterungen von $\mathbb{Z}$ (wie etwa $\mathbb{Z}[\mathrm{i}]$) benutzt werden können, um Diophantische Gleichungen zu lösen. — Ein Problemkreis, der Zahlentheoretikerinnen und Zahlentheoretiker schon seit der Antike beschäftigt! Bei $\mathbb{Z}[\mathrm{i}]$ handelt es sich zwar um einen Hauptidealbereich, doch stellt sich im Zuge der Beschäftigung mit algebraische Zahlentheorie heraus, dass die natürlichen Untersuchungsobjekte R leider nur selten Hauptidealbereiche sind, sondern nur sogenannte „Dedekind-Ringe“. Dieser Defekt löst sich allerdings beispielsweise dann auf, wenn man von den fraglichen R zu Lokalisierungen $R_{\mathfrak{p}} \coloneqq S^{-1}R$ mit $S = R \setminus \mathfrak{p}$ übergeht. Ähnlich zu unserer früheren Bemerkung, dass die Jordan-Normalform über einem algebraischen Abschluss vielleicht schon zur Lösung einiger Probleme hinreicht, kann man sich nun hoffentlich denken, dass der Übergang von R zur Lokalisierung $R_{\mathfrak{p}}$ (welcher auch einen Übergang von R-Moduln zu $R_{\mathfrak{p}}$-Moduln mitbringt) einige Information über den ursprünglichen Ring (oder Modul) zu liefern vermag. Auf Moduln über $R_{\mathfrak{p}}$ lässt sich nun aber Satz 8.2 anwenden.

An dieser Stelle sei erwähnt, dass es auch weitere Konstruktionen gibt, welche den Einsatz von weiteren Methoden erlauben, etwa der Übergang zu sogenannten „Komplettierungen“. Der Übergang zu Lokalisierung und Komplettierung ist ubiquitär in der algebraischen Geometrie. Tatsächlich gibt es auch eine geometrische Sichtweise auf die algebraische Zahlentheorie und, diese verallgemeinernd, liefert die Theorie glatter algebraischen Kurven (abermals beim Übergang „zum Lokalen“) einen weiteren großen Fundus an Hauptidealbereichen, die wirklich in der Praxis auftreten.

Die obigen Ausführungen geben nun hoffentlich den Eindruck, dass der Nutzen von Satz 8.2 durch die in § 8.2 und § 8.3 diskutierten Anwendungen noch nicht erschöpft ist, obgleich uns hier der zeitliche Rahmen fehlt, um weiteren interessanten Anwendungen den nötigen Platz einzuräumen. Interessierte Leserinnen und Leser finden vielleicht Freude an [20] für eine motivierte Einführung die Zahlentheorie oder [28, 25] für eine fortgeschrittene Beschäftigung mit der algebraischen Zahlentheorie. Speziell die Anschauung hinter dem geometrischen Blickwinkel findet man in [15] und dem sehr umfangreichen Werk [14] zur kommutativen Algebra. Wirklich ernste Beschäftigung mit algebraischer Geometrie findet man in [19] (Achtung: sehr anspruchsvoll!) und [9] (auch sehr anspruchsvoll, entwickelt aber alle benötigte kommutative Algebra *in-situ*).

Teil 3

Anfänge affiner algebraischer Geometrie

KAPITEL 9

Hilberts Nullstellensatz

Für einen Körper K schreiben wir $\mathbb{A}_K^n = K^n$ für die *Menge* aller n-Tupel von Elementen aus K (ohne dabei an eine zusätzliche Vektorraumstruktur oder Ähnliches zu denken). Wir nennen $\mathbb{A}_K^n$ den ***affinen n-Raum über K***. Im Folgenden arbeiten wir häufig mit dem Polynomring $A = K[X_1, \ldots, X_n]$ und in konkreten Beispielen schreiben wir aus Bequemlichkeit oft X statt X_1, Y statt X_2 und Z statt X_3.

9.1. Simultane Nullstellen von Polynomen

Polynome im Polynomring $A = K[X_1, \ldots, X_n]$ fungieren als Funktionen auf $\mathbb{A}_K^n$: Zu $\boldsymbol{x} \in \mathbb{A}_K^n$ und $f \in A$ liefert das Bild $f(\boldsymbol{x})$ von f unter dem Einsetzungshomomorphismus

$$K[X_1, \ldots, X_n] \longrightarrow K, \quad X_i \longmapsto \{i\text{-te Komponente von } \boldsymbol{x}\}$$

ein wohl-bestimmtes Element von K.

Für eine Menge $\mathscr{A} \subseteq A$ von Polynomen sei

$$V(\mathscr{A}) = \{\, \boldsymbol{x} \in \mathbb{A}_K^n : f(x) = 0_K \text{ für alle } f \in \mathscr{A} \,\}$$

die ***Nullstellenmenge von*** $\mathscr{A}$ oder auch ***Verschwindungsmenge von*** $\mathscr{A}$. Wir schreiben auch $V(f)$ für $V(\{f\})$. (Siehe Abbildung 25 und Abbildung 26 für Anschauungsmaterial.)

Ist K algebraisch abgeschlossen, so hat jedes (multivariate) nichtkonstante Polynom $f \in A$ Nullstellen; Wir haben $V(f) \neq \emptyset$. Um dies einzusehen, sei o.E. X_1 eine Unbekannte, die in f vorkommt. Dann schreiben wir f_1 für das Bild von f unter dem Homomorphismus mit

$$K[X_1, \ldots, X_n] \longrightarrow K[X], \quad X_i \longmapsto \begin{cases} X & \text{falls } i = 1, \\ 0_K & \text{sonst.} \end{cases}$$

Das (univariate) Polynom $f_1 \in K[X]$ hat nun im algebraisch abgeschlossenen Körper K eine Nullstelle x_1. Offensichtlich gilt dann

$$f(x_1, 0_K, \ldots, 0_K) = f_1(x_1) = 0_K,$$

also $(x_1, 0_K, \ldots, 0_K) \in V(f)$.

Bemerkung. Man beachte, dass die obige Überlegung die algebraische Abgeschlossenheit von K vorausgesetzt hat. Über $K = \mathbb{R}$ haben wir aber beispielsweise $V(X^2+1) = \emptyset$.

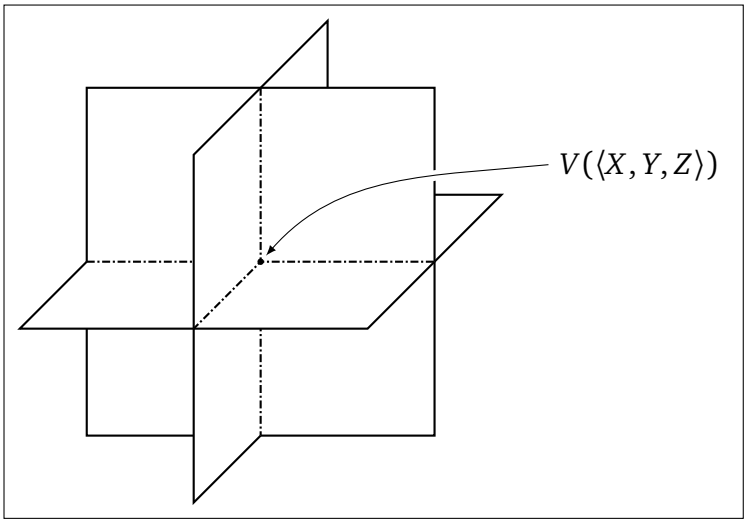


Abbildung 25. $V(\langle X,Y,Z\rangle) = \{(0_K,0_K,0_K)\}$ in $\mathbb{A}_K^3$ entsteht als Durchschnitt der drei Hyperebenen $V(X) = \{(x,y,z) \in \mathbb{A}_K^3 : x = 0\}$, $V(Y)$ und $V(Z)$.

Die Situation wird deutlich komplizierter, wenn man nach simultanen Nullstellen von zwei oder mehr Polynomen sucht. Aus der *linearen Algebra* kennt man bereits Systeme linearer Gleichungen. Schon bei einer Variablen braucht es bekanntermaßen keine Lösungen zu geben:

$$V(X) \cap V(X-1) = V(\{X, X-1\}) = \emptyset.$$

Man kann natürlich auch kompliziertere *Systeme* betrachten.

Beispiel. Das lineare Gleichungssystem

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 5 & 6 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \stackrel{!}{=} \begin{pmatrix} 4 \\ 7 \end{pmatrix}$$

besitzt die Lösungsmenge[1]

$$\begin{aligned} &V(\{X+2Y+3Z-4,\, 5Y+6Z-7\}) \\ &\quad = V(\{2X-Y-1,\, \tfrac{5}{3}X+Z-2\}) \\ &\quad = \{(x,y,z) \in \mathbb{A}_K^2 : y = 2x-1,\, z = -\tfrac{5}{3}x+2\}, \end{aligned}$$

eine Gerade! (Das verblüfft natürlich nicht; Zwei Ebenen schneiden sich aus Dimensionsgründen entweder gar nicht, in einer Geraden, oder sind gar völlig identisch.)

[1] K sei hier ein beliebiger Körper mit Charakteristik $\neq 3$ (damit die hier benötigte Division durch 3 durchführbar ist).

Obgleich wir doch lineare Gleichungssysteme bestens verstehen, sollte uns die dafür in der linearen Algebra aufgewendete Mühe suggerieren, dass es im allgemeinen, nichtlinearen Fall schwierig sein wird, einer guten Lösungstheorie habhaft zu werden. Wir beschäftigen uns hier also nur mit der deutlich bescheideneren Absicht die Frage nach der *Existenz von Lösungen* zu beantworten.

Leitfrage: *Wann ist* $V(\mathscr{A}) \neq \emptyset$?

Ist $\mathfrak{a}$ das von $\mathscr{A}$ erzeugte Ideal, so gilt offensichtlich $V(\mathfrak{a}) = V(\mathscr{A})$. Zu gegebener Menge $\mathscr{V} \subseteq \mathbb{A}_K^n$ kann man auch die Menge $I(\mathscr{V})$ der Polynome betrachten, die auf $\mathscr{V}$ verschwinden:

$$I(\mathscr{V}) = \{ f \in A : f(\boldsymbol{x}) = 0_K \text{ für alle } \boldsymbol{x} \in \mathscr{V} \}.$$

Vom algebraischen Blickwinkel aus, sind natürlich primär diejenigen Mengen $\mathscr{V}$ interessant, die als Mengen der Form $V(\mathfrak{a})$ für ein Ideal $\mathfrak{a}$ von A auftreten.
Ist $\mathscr{V} = \emptyset$, so haben wir $I(\mathscr{V}) = I(\emptyset) = A$, da die Auswahlbedingung in der Definition von $I(\,\cdot\,)$ hier „leer“ ist.

Wie sieht $I(V(\mathfrak{a}))$ aus? Nach Definition von $V(\mathfrak{a})$ verschwinden auf $V(\mathfrak{a})$ natürlich alle Polynome aus $\mathfrak{a}$, weswegen wir $\mathfrak{a} \subseteq I(V(\mathfrak{a}))$ haben. Tatsächlich muss hierin keine Gleichheit gelten:

Beispiel 9.1. In $\mathbb{A}_K^n$ ist $V(\{X^2\}) = \{0_K\} = V(\{X\})$. Wir haben

$$I(V(\{X^2\})) = \langle X \rangle \supsetneq \langle X^2 \rangle.$$

Beispiel 9.1 legt folgende Begriffsbildung nahe: Sei $\mathfrak{a}$ ein Ideal von[2] A. Das ***Radikal von*** $\mathfrak{a}$ ist gegeben durch

$$\operatorname{rad}(\mathfrak{a}) = \{ f \in R : f^n \in \mathfrak{a} \text{ für ein } n \in \mathbb{N} \}.$$

(Häufig schreibt man auch $\sqrt{\mathfrak{a}} = \operatorname{rad}(\mathfrak{a})$ aus offensichtlichen Gründen, obwohl hier zu beachten ist, dass $\operatorname{rad}(\mathfrak{a})$ im Allgemeinen beliebige n-te Wurzeln von Elementen aus $\mathfrak{a}$ und nicht bloß Quadratwurzeln enthält.) Das Radikal eines Ideals ist selbst ein Ideal, wie man beispielsweise unter Zuhilfenahme des binomischen Lehrsatzes nachrechnen kann; Alternativ beachte man das weiter unten notierte Lemma 9.8.

Man beachte weiter: Ist $\mathfrak{a} \neq A$, also $1_A \notin \mathfrak{a}$, so ist auch $1 \notin \operatorname{rad}(\mathfrak{a})$ und daher $\operatorname{rad}(\mathfrak{a}) \neq A$. Überdies haben wir $I(V(\mathfrak{a})) \supseteq \operatorname{rad}(\mathfrak{a})$. *Kann $I(V(\mathfrak{a}))$ größer sein?* — Nein, wie der folgende berühmte Satz sagt:

Satz 9.2 (Hilberts Nullstellensatz)**.** *Sei K ein algebraisch abgeschlossener Körper und $A = K[X_1, \ldots, X_n]$ der zugehörige Polynomring in n Unbestimmten. Dann ist*

$$I(V(\mathfrak{a})) = \operatorname{rad}(\mathfrak{a}).$$

Der Beweis von Satz 9.2 benötigt etwas Vorarbeit und wir erledigen diese und den Beweis in § 9.2. Hier halten wir jedenfalls noch fest, dass Satz 9.2 eine brauchbare Antwort auf unsere zuvor aufgeworfene Leitfrage liefert:

[2] Man definiert das Radikal eines Ideals auch für Ideale eines beliebigen kommutativen Rings.

Korollar 9.3. *Sei K ein algebraisch abgeschlossener Körper und $A = K[X_1, \ldots, X_n]$ der zugehörige Polynomring in n Unbestimmten. Dann hat jede Menge von Polynomen $f_1, \ldots, f_r$ mit $\langle f_1, \ldots, f_r \rangle \subsetneq A$ eine gemeinsame Nullstelle.*

Beweis. Sei $\mathfrak{a} = \langle f_1, \ldots, f_r \rangle$. Nach Voraussetzung ist $\mathfrak{a} \neq A$. Insbesondere ist auch $\operatorname{rad}(\mathfrak{a}) \neq A$, denn anderenfalls wäre $1_A \in \operatorname{rad}(\mathfrak{a})$ und somit $1_A = 1_A^n \in \mathfrak{a}$ für ein $n \in \mathbb{N}$, was allerdings unserer Voraussetzung $\mathfrak{a} \neq A$ widerspricht. Unter Ausnutzung von Satz 9.2 ergibt sich nun schließlich $I(V(\mathfrak{a})) = \operatorname{rad}(\mathfrak{a}) \neq A = I(\emptyset)$, also $V(\mathfrak{a}) \neq \emptyset$. □

9.2. Beweis des Nullstellensatzes

Die mathematische Literatur enthält einen reichhaltigen Fundus an Beweisen des Nullstellensatzes. Der hier geführte Beweis entspricht einer Variante von Artin und Tate [3] eines zuvor von Zariski [37] gegebenen Beweises. (Siehe auch [4, 24].)

Seien R und A kommutative Ringe und $\iota\colon R \to A$ ein Ringhomomorphismus. Analog wie in unseren Überlegungen zu Körpererweiterungen wird A damit zu einem R-Modul und wir nennen A eine ***R-Algebra***. (Formal wäre es hier besser den Homomorphismus ι als die fragliche R-Algebra zu bezeichnen, aber für den Umfang der hier benötigten Überlegungen soll uns diese unpräzise Sprechweise genügen.)

Lemma 9.4 (Artin–Tate, 1951)**.** *Sei $R \subseteq B \subseteq A$ eine Inklusionskette von kommutativen Ringen. Ferner sei R noethersch, A als R-Algebra endlich erzeugt, und A als B-Modul endlich erzeugt. Dann ist B als R-Algebra endlich erzeugt.*

Beweis. Seien $a_1, \ldots, a_n$ Erzeuger von A als R-Algebra und $v_1, \ldots, v_m$ Erzeuger von A als B-Modul. Wir schreiben

$$a_i = \sum\nolimits_j \beta_{ij} v_j, \quad \text{sowie} \quad v_i v_j = \sum\nolimits_k \beta_{ijk} v_k$$

mit Elementen $\beta_{ij}, \beta_{ijk} \in B$. Sei $B_0 = R[\{\, \beta_{ij}, \beta_{ijk} : i, j, k \,\}]$ die von diesen Elementen erzeugte R-Algebra. Wir haben die Inklusionskette $R \subseteq B_0 \subseteq B$. Da sich jedes Element von A als Polynom in den Elementen a_i schreiben lässt, sehen wir durch iterierte Anwendung der obigen Gleichungen, dass sich jedes Element von A als B_0-Linearkombination der Elemente $v_1, \ldots, v_m$ schreiben lässt: A ist als B_0-Modul endlich erzeugt. Da R noethersch ist, gilt dies auch für B_0 (man stelle B_0 als einen Quotientenring eines Polynomrings in mehreren Unbekannten über R da und berufe sich dann auf Beispiel 7.4 (5) in Kombination mit Proposition 7.2). Darum ist auch A als (endlich erzeugter) B_0-Modul noethersch und somit der B_0-Untermodul $B \subseteq A$ endlich erzeugt (Satz 7.1). Da B_0 als R-Algebra endlich erzeugt ist, folgt nun auch die endliche Erzeugtheit von B als R-Algebra. □

Lemma 9.5. *Man betrachte $L = K(X_1, \ldots, X_m)$, den Quotientenkörper des Polynomrings $K[X_1, \ldots, X_m]$ in $m \geq 1$ Unbestimmten. Dann ist L als K-Algebra nicht endlich erzeugt.*

Beweis. Angenommen wir hätten $L = K[y_1, \ldots, y_r]$, wobei jedes y_i von der Form f_i/g_i mit Polynomen f_i, g_i in den Variablen $X_1, \ldots, X_m$ ist. Wir behaupten, dass dies

ein Widerspruch ist, da

$$\frac{1}{(g_1 \cdots g_r)+1} \in K(X_1, \ldots, X_m) = L$$

nicht in $R = K[y_1, \ldots, y_r]$ liegen kann. In der Tat sieht man, dass jedes Element in $K[y_1, \ldots, y_r]$ von der Form f/g ist, wo g sich nur aus irreduziblen Faktoren von $g_1 \cdots g_r$ zusammensetzt. (Das sieht man anhand der üblichen Rechenregeln für Summen- und Produktbildung von Brüchen.) Nun haben aber die multivariaten Polynome $g_1 \cdots g_r$ und $(g_1 \cdots g_r) + 1$ keine irreduziblen Faktoren gemeinsam; Das widerspricht der Tatsache, dass der Polynomring $K[X_1, \ldots, X_m]$ faktoriell ist! □

Proposition 9.6 (Zariski, 1947)**.** *Sei K ein Körper und A eine endlich erzeugte K-Algebra. Falls A ein Körper ist, so ist die Erweiterung A/K endlich (und insbesondere algebraisch).*

Beweis. Wegen der endlichen Erzeugtheit von A als K-Algebra, gibt es Elemente $x_1, \ldots, x_n \in A$ mit $A = K[x_1, \ldots, x_n]$. Zwecks Erzeugung eines Widerspruchs gehen wir davon aus, dass nicht alle diese Elemente algebraisch über K sind. Wir wählen aus diesen Erzeugern nun sukzessive Elemente, bis die übrigen Erzeuger algebraisch abhängig über dem von den bisher gewählten Erzeugern erzeugten Körper sind. Nach Umnummerierung haben wir also Elemente $x_1, \ldots, x_m$ $(m \leq n)$ derart, dass die übrigen Elemente $x_{m+1}, \ldots, x_n$ algebraisch über $L = K(x_1, \ldots, x_m)$ sind.[3]
Gemäß Lemma 9.4 angewandt auf $K \subseteq L \subseteq A$ sehen wir, dass L als K-Algebra endlich erzeugt ist. Da jedoch L und $K(X_1, \ldots, X_m)$ (vermöge $x_i \mapsto X_i$) K-isomorph sind, widerspricht dies Lemma 9.5. □

Korollar 9.7. *Sei K ein Körper und A eine endlich erzeugte K-Algebra und $\mathfrak{m} \subseteq A$ ein maximales Ideal von A. Dann ist $A/\mathfrak{m}$ eine endliche (und insbesondere algebraische) Erweiterung von K. Ist K algebraisch abgeschlossen, so ist $A/\mathfrak{m} \cong K$ (vermöge der durch die K-Algebrastruktur induzierte Abbildung $K \hookrightarrow A \twoheadrightarrow A/\mathfrak{m}$).*

Beweis. Wähle A in Proposition 9.6 als $A/\mathfrak{m}$. □

Lemma 9.8. *Sei R ein kommutativer Ring und $\mathfrak{a}$ ein Ideal von R. Dann ist*

$$\operatorname{rad}(\mathfrak{a}) = \bigcap_{\substack{\mathfrak{p} \supseteq \mathfrak{a} \\ \mathfrak{p} \text{ Primideal}}} \mathfrak{p}.$$

Beweis. Wir zeigen zunächst die Inklusion „$\subseteq$“ von der behaupteten Gleichheit. Ist $f \in \operatorname{rad}(\mathfrak{a})$, so ist $f^n \in \mathfrak{a}$ für ein geeignetes n. Ist $\mathfrak{p} \supseteq \mathfrak{a}$ nun ein beliebiges Primideal, so ist auch $f^n \in \mathfrak{p}$ und dann (induktiv mittels der Primideal-Eigenschaft) $f \in \mathfrak{a}$.

Nun behandeln wir die umgekehrte Inklusion. Sei $f \in R \setminus \operatorname{rad}(\mathfrak{a})$. Wir wollen die Existenz eines Primideals $\mathfrak{p} \supseteq \mathfrak{a}$ einsehen, welches f nicht enthält. Sei $\mathscr{A}$ die Menge aller Ideale, welche $\mathfrak{a}$ enthalten, aber keine Potenz von f enthalten. Diese Menge ist nicht leer (denn sie enthält $\mathfrak{a}$) und lässt sich via Inklusion partiell ordnen. Jede Kette darin enthält ein maximales Element (man betrachte die Vereinigung aller in der

[3] Hier ist $\{x_1, \ldots, x_m\}$ natürlich eine *Transzendenzbasis* im Sinne von § 2.4.

Kette vorkommenden Ideale). Nach dem *Lemma von Zorn* besitzt $\mathscr{A}$ ein maximales Element $\mathfrak{p}$. Wir zeigen, dass dies ein Primideal ist. Seien $x, y \in R \setminus \mathfrak{p}$. Da die beiden Ideale $\mathfrak{p} + (x)$ und $\mathfrak{p} + (y)$ jeweils echt größer sind als $\mathfrak{p}$, folgt wegen der Maximalität von $\mathfrak{p}$ in $\mathscr{A}$, dass es Exponenten n und m mit

$$f^m \in \mathfrak{p} + (x) \quad \text{und} \quad f^n \in \mathfrak{p} + (y)$$

gibt. Dann ist aber $f^{m+n} \in \mathfrak{p} + (xy)$, also $\mathfrak{p} + (xy) \notin \mathscr{A} \ni \mathfrak{p}$ und daher $xy \notin \mathfrak{p}$. Also ist $\mathfrak{p}$ prim, enthält $\mathfrak{a}$, aber enthält keine Potenz von f. Das zeigt die Behauptung. □

Lemma 9.9. *Sei K ein Körper und $A = K[X_1, \ldots, X_n]$ der zugehörige Polynomring. Zu $\boldsymbol{x} \in \mathbb{A}^n_K$ betrachte man das Ideal $\mathfrak{m}_{\boldsymbol{x}} = \langle X_1 - x_1, \ldots, X_n - x_n \rangle$ nebst der kanonischen Projektion $\pi\colon A \to A/\mathfrak{m}_{\boldsymbol{x}}$. Dann ist das Diagramm*

$$\begin{array}{ccc} A & \xrightarrow[(\textit{Auswertung bei } \boldsymbol{x})]{f \mapsto f(\boldsymbol{x})} & K \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \lambda \mapsto \lambda X_1^0 \cdots X_n^0} \\ A/\mathfrak{m}_{\boldsymbol{x}} & \xleftarrow[\pi]{} & A \end{array}$$

kommutativ. Insbesondere ist $\mathfrak{m}_{\boldsymbol{x}}$ ein maximales Ideal.

Beweis. Für ein beliebiges Polynom $f \in A$ schreibe man $X_j = x_j + (X_j - x_j)$ für alle in f vorkommenden Variablen und expandiere die entstehenden Ausdrücke. Damit erhält man $f = f(\boldsymbol{x}) + \ldots$, wobei die Punkte für ein Element von $\mathfrak{m}_{\boldsymbol{x}}$ stehen. Das zeigt die Kommutativität des Diagramms. Darauf folgt auch die Maximalität von $\mathfrak{m}_{\boldsymbol{x}}$, da man unmittelbar nachrechnen kann, dass es sich bei dem Ring

$$A/\mathfrak{m}_{\boldsymbol{x}} = \{\, \lambda X_1^0 \cdots X_n^0 \bmod \mathfrak{m}_{\boldsymbol{x}} : \lambda \in K \,\}$$

um einen Körper handelt. □

Beispiel. Wir betrachten den Punkt $\boldsymbol{x} = (1, 2) \in \mathbb{A}^2_{\mathbb{C}}$ und das zugehörige maximale Ideal $\mathfrak{m}_{\boldsymbol{x}} = \langle X - 1, Y - 2 \rangle$, sowie das Polynom $f = XY + Y - 3 \in \mathbb{C}[X, Y]$. Wir haben

$$\begin{aligned} f &= (\underline{1} + (X-1))(\underline{2} + (Y-2)) + (\underline{2} + (Y-2))\underline{-3} \\ &= \underline{1 \cdot 2 + 2 - 3} + \underline{1}(Y-2) + (X-1)(\underline{2} + (Y-2)) + (Y-2) \\ &= \underbrace{1 \cdot 2 + 2 - 3}_{=f(\boldsymbol{x})} + \underbrace{(X-1)(2 + (Y-2)) + 2(Y-2)}_{\in \mathfrak{m}_{\boldsymbol{x}}}. \end{aligned}$$

Also gilt $f + \mathfrak{m}_{\boldsymbol{x}} = f(\boldsymbol{x}) X_1^0 \cdots X_n^0 + \mathfrak{m}_{\boldsymbol{x}}$, wie es auch im allgemeinen Fall in Lemma 9.9 behauptet wird.

Beweis von Satz 9.2. Die Inklusion $\operatorname{rad}(\mathfrak{a}) \subseteq I(V(\mathfrak{a}))$ ist einfach, denn zu $f \in \operatorname{rad}(\mathfrak{a})$ gibt es $n \in \mathbb{N}$ mit $f^n \in \mathfrak{a}$. Dann ist $f(\boldsymbol{x})^n = 0_K$ für alle $\boldsymbol{x} \in V(\mathfrak{a})$. Da K nullteilerfrei ist, folgt $f(\boldsymbol{x}) = 0_K$ für alle $\boldsymbol{x} \in V(\mathfrak{a})$, also $f \in I(V(\mathfrak{a}))$.
Sei nun $f \in A \setminus \operatorname{rad}(\mathfrak{a})$. Wir wollen $f \notin V(\mathfrak{a})$ zeigen. Hierzu konstruieren wir ein $\boldsymbol{x} \in V(\mathfrak{a})$ mit $f(\boldsymbol{x}) \neq 0_K$. Laut Lemma 9.8 gibt es ein Primideal $\mathfrak{p} \supseteq \operatorname{rad}(\mathfrak{a})$, welches f nicht enthält. Wir betrachten den Integritätsbereich $B = A/\mathfrak{p}$ und das Bild $\bar{f}$ von

f in diesem. Wegen $\bar{f} \neq 0_B$ ist $\bar{f}$ im Quotientenkörper Quot(B) von B invertierbar und wir betrachten den Integritätsbereich $C = B[\bar{f}^{-1}] \subseteq \mathrm{Quot}(B)$. Dieser enthält ein maximales Ideal $\mathfrak{m} \subset C$.
Da C eine endlich erzeugte K-Algebra ist,[4] ist $C/\mathfrak{m} \cong K$ laut Korollar 9.7. Wir betrachten nun den Punkt $\boldsymbol{x} \in \mathbb{A}_K^n$, dessen Koordinaten die Bilder der Variablen X_i unter der Verkettung

$$\begin{array}{ccccc} & & A/\mathfrak{p} & \hookrightarrow & (A/\mathfrak{p})[\bar{f}^{-1}] \longrightarrow ((A/\mathfrak{p})[\bar{f}^{-1}])/\mathfrak{m} \\ & \nearrow & & & \searrow^{\sim} \\ K[X_1,\ldots,X_n] = A & & \xrightarrow{\qquad\qquad\psi\qquad\qquad} & & K\,. \end{array}$$

sind: $\boldsymbol{x} = (\psi(X_1),\ldots,\psi(X_n))$.

Nach Konstruktion gilt

$$\mathfrak{a} \subseteq \mathrm{rad}(\mathfrak{a}) \subseteq \mathfrak{p} \subseteq \psi^{-1}(\{0_K\}) \supseteq \langle X_1 - \psi(X_1),\ldots,X_n - \psi(X_n)\rangle = \mathfrak{m}_{\boldsymbol{x}}.$$

Das Ideal rechter Hand ist maximal gemäß Lemma 9.9, weshalb $\mathfrak{a} \subseteq \psi^{-1}(\{0_K\}) = \mathfrak{m}_{\boldsymbol{x}}$ gilt. Es folgt $V(\mathfrak{a}) \supseteq V(\mathfrak{m}_{\boldsymbol{x}}) \ni \boldsymbol{x}$. (Vgl. Abbildung 26.)
Ferner gilt $f \notin \mathfrak{m}_{\boldsymbol{x}}$, da f in obigem Diagramm auf die Einheit $\bar{f}$ in $(A/\mathfrak{p})[\bar{f}^{-1}]$ abgebildet wird und daher nicht in $\mathfrak{m}$ enthalten sein kann, weswegen man durch Verfolgen des oberen Pfades $\psi(f) \neq 0_K$ sieht. Durch Betrachtung des kommutativen Diagramms (siehe Lemma 9.9)

$$\begin{array}{ccccc} K & \xleftarrow{g\mapsto g(\boldsymbol{x})} & A & \xrightarrow{\psi} & K \\ \downarrow{\scriptstyle \lambda\mapsto\lambda X_1^0\cdots X_n^0} & & \downarrow{\scriptstyle \pi} & \nearrow & \\ A & \xrightarrow{\pi} & A/\mathfrak{m}_{\boldsymbol{x}} = A/\ker\psi & & \end{array}$$

folgt also $f(\boldsymbol{x}) \neq 0_K$. □

9.3. Abschließende Bemerkungen

Bemerkung. Nur der letzte Teil von Satz 9.2 ($C/\mathfrak{m} \cong K$) benutzt die algebraische Abgeschlossenheit von K. Wenn man bereit ist statt $\mathbb{A}_K^n$ die (für nicht algebraische abgeschlossene K größere) Menge der maximalen Ideale von $K[X_1,\ldots,X_n]$ zu betrachten, so kann man mit der hier benutzten Beweisstrategie auch zu einer allgemeineren Formulierung von Hilberts Nullstellensatz gelangen. (Siehe etwa [9, § 3.2, insbesondere Corollary 6].)

[4] Beachte, dass B als K-Algebra endlich erzeugt ist, nämlich von den Restklassen der Unbekannten $X_1,\ldots,X_n$. Darum ist auch $B[\bar{f}^{-1}]$ als K-Algebra endlich erzeugt.

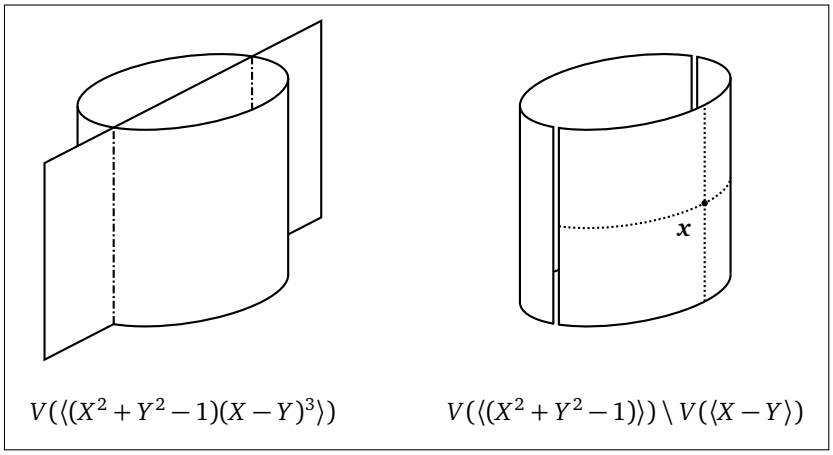


Abbildung 26. Illustration zum Beweis von Satz 9.2 mit $A = \mathbb{C}[X, Y, Z]$ (die Bilder nutzen allerdings nur reelle Koordinaten, was uns für Anschauungszwecke genügen soll): Für $\mathfrak{a} = \langle (X^2 + Y^2 - 1)(X - Y)^3 \rangle$ ist das Polynom $f = X - Y$ nicht im Ideal $\langle (X - Y)^3 \rangle$ enthalten, aber sehr wohl in $\mathrm{rad}(\langle (X - Y)^3 \rangle) = \langle X - Y \rangle$. Dennoch ist f nicht in $\mathrm{rad}(\mathfrak{a})$ enthalten. Wir haben nämlich $f \notin \mathrm{rad}(\langle X^2 + Y^2 - 1 \rangle) = \langle X^2 + Y^2 - 1 \rangle$. Schränkt man die Betrachtung nun auf $V(\langle X^2 + Y^2 - 1 \rangle)$ ein (das macht der Übergang zu $B = A/\langle X^2 + Y^2 - 1 \rangle$), so sieht man, dass f (bzw. $\bar{f}$) dort trotzdem Nullstellen besitzt. Um diesen „aus dem Weg zu gehen" betrachtet man nur Ideale von B, welche f nicht enthalten. Diese Ideale entsprechen den Idealen von $B[\bar{f}^{-1}]$. Das Wählen eines maximalen Ideals hiervon entspricht dann dem Wählen eines Punktes $\boldsymbol{x}$ auf $V(\langle X^2 + Y^2 - 1 \rangle) \subseteq V(\mathfrak{a})$, auf dem f nicht verschwindet.

Korollar 9.10 (Hilberts Nullstellensatz, schwache Form)**.** *Sei K ein algebraisch abgeschlossener Körper und $A = K[X_1, \ldots, X_n]$ der zugehörige Polynomring in n Unbestimmten. Dann sind die maximalen Ideale von A genau die Ideale $\mathfrak{m}_{\boldsymbol{x}} = \langle X_1 - x_1, \ldots, X_n - x_n \rangle$ mit $\boldsymbol{x} \in \mathbb{A}^n_K$.*

Beweis. Die Maximalität der Ideale der Form $\mathfrak{m}_{\boldsymbol{x}}$ hatten wir schon in Lemma 9.9 eingesehen. Sei nun umgekehrt $\mathfrak{m}$ ein beliebiges maximales Ideal von A. Wegen

$$I(V(\mathfrak{m})) = \mathrm{rad}(\mathfrak{m}) = \mathfrak{m} \neq A = I(\emptyset)$$

ist $V(\mathfrak{m}) \neq \emptyset$ und enthält also ein $\boldsymbol{x} \in \mathbb{A}^n_K$. Dann ist aber

$$A \supsetneq \mathfrak{m}_{\boldsymbol{x}} \supseteq I(\langle \boldsymbol{x} \rangle) \supseteq I(V(\mathfrak{m})) = \mathrm{rad}(\mathfrak{m}) = \mathfrak{m}.$$

Aus der Maximalität von $\mathfrak{m}$ folgt nun $\mathfrak{m} = \mathfrak{m}_{\boldsymbol{x}}$. □

ANHANG A

Übungsaufgaben

1. Übung

1.1. *(Alternative Charakterisierung von Primkörpern)*
Beweisen Sie Bemerkung 1.2: *für jeden Körper K ist dessen Primkörper k durch den Schnitt aller Teilkörper von K gegeben.*

1.2. *(Endlicher Körper mit 6 Elementen?)*
Zeigen Sie, dass es *keinen* Körper mit genau 6 Elementen gibt.
(Hinweis: betrachten Sie einen potentiell existenten solchen Körper als Vektorraum über seinem Primkörper.)

1.3. *(Zwischenkörper sind Unterräume)*
Sei $\iota\colon K \to L$ eine Körpererweiterung und Z ein Zwischenkörper davon. Zeigen Sie, dass Z ein Unterraum von L (bezüglich der durch ι induzierten Vektorraumstruktur auf L) ist.
(Hinweis: das kann man natürlich sehr einfach direkt nachrechnen. Man kann aber auch etwas eleganter Lemma 1.6 benutzen. Sehen Sie wie?)

2. Übung

2.1. *(Rechnen mit Potenzbasen)*
Wir betrachten die Körpererweiterung $\mathbb{C}/\mathbb{Q}$ und $x \in \mathbb{C}$. Dann bezeichne $\mathbb{Q}(x)$ den kleinsten Zwischenkörper von $\mathbb{C}/\mathbb{Q}$, der x enthält. Im Folgenden sei x eine beliebige komplexe Nullstelle des Polynoms $X^3 - 2X + 2 \in \mathbb{Q}[X]$.

(a) Zeigen Sie, dass $\{1, x, x^2\}$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}(x)$ ist.

(b) Sei $y \in \mathbb{Q}(x)$ beliebig. Begründen Sie, dass $\mathbb{Q}(y) \in \{\mathbb{Q}, \mathbb{Q}(x)\}$. (Hinweis: Satz 1.7.)

(c) Stellen Sie die Elemente

$$(1 - x + 2)(x^4 + 1), \quad x^{-1} \quad \text{und} \quad (1 + x)^{-1}$$

von $\mathbb{Q}(x)$ als $\mathbb{Q}$-Linearkombinationen bezüglich der $\mathbb{Q}$-Basis $\{1, x, x^2\}$ dar.

2.2. *(Quadrate und ungerade einfache Erweiterungen)*
Es sei $\iota\colon K \to L$ eine Körpererweiterung mit ungeradem Grad $[L : K]$. Ferner sei $x \in L$ beliebig. Zeigen Sie $K(x) = K(x^2)$.
(Hinweis: Betrachten Sie das Minimalpolynom m_x von x über K und schreiben

Sie dieses in der Form $m_x = XP(X^2) + Q(X^2)$ mit Polynomen $P, Q \in K[X]$. Was sagt es Ihnen nun, dass x eine Nullstelle von m_x in L ist?)

2.3. *(Einfache transzendente Erweiterungen)*
Beweisen Sie Satz 2.5: *Sei $\iota\colon K \to L$ eine Körpererweiterung und $x \in L$ transzendent über K. Dann ist die Körpererweiterung $K \to \mathrm{Quot}(K[X])$ K-isomorph zu der von ι induzierten Körpererweiterung $K \to K(x)$.*
(Hinweis: Sie können den Beweis von Satz 2.1 übertragen.)

3. Übung

3.1. *(Transzendente Erweiterungen)*
Es bezeichne $\mathbb{A} \subseteq \mathbb{C}$ die Menge aller komplexen Zahlen, welche algebraisch über $\mathbb{Q}$ sind.
(a) Zeigen Sie, dass $\mathbb{A}/\mathbb{Q}$ eine Körpererweiterung unendlichen Grades ist.
(b) Zeigen Sie, dass die Menge $\mathbb{A}$ abzählbar ist.
(c) Folgern Sie, dass es in $\mathbb{R}$ Elemente gibt, die transzendent über $\mathbb{Q}$ sind.

3.2. *(Zerfällungskörper bestimmen)*
Bestimmen Sie für jedes der folgenden Polynome $P \in \mathbb{Q}[X]$ jeweils den Zerfällungskörper $\iota\colon \mathbb{Q} \to L$ mit $L \subseteq \mathbb{C}$ und $\iota = \mathrm{id}_L|_{\mathbb{Q}}$, sowie dessen Grad $[L : \mathbb{Q}]$. Zerlegen Sie auch das Polynom $\iota^* P \in L[X]$ in ein Produkt von Linearfaktoren. (Hinweis: siehe Beispiel 2.11.)
(a) $X^2 - 11$;
(b) $X^4 - 2$;
(c) $X^4 - 9X^2 + 4X + 12$.

3.3. *(Grade von Zerfällungskörpern)*
Sei K ein Körper und $P \in K[X]$ ein (nicht notwendigerweise irreduzibles) Polynom vom Grad n, sowie $\iota\colon K \to L$ ein Zerfällungskörper von P.
(a) Zeigen Sie, dass $[L : K]$ ein Teiler von $n!$ ist.
(Hinweis: Schreiben Sie $L = K(x_1, \ldots, x_n)$ mit den Nullstellen $x_1, \ldots, x_n$ von P in L und führen Sie eine Induktion; Betrachten Sie hierzu die Körpererweiterungen $K \to K(x_n)$ und $L/K(x_n)$.)
(b) Belegen Sie anhand zweier Beispiele, dass sowohl der Fall $n < [L : K] < n!$, wie auch der Fall $[L : K] = n!$ eintreten können. (Hinweis: Aufgabe 3.2.)

4. Übung

4.1. *(Minimalpolynome berechnen)*
Betrachten Sie die folgenden Teilkörper von $\mathbb{C}$

$$K_1 = \mathbb{Q}, \quad K_2 = \mathbb{Q}(\sqrt{2}), \quad K_3 = \mathbb{Q}(\mathrm{i}\sqrt{3}), \quad L = \mathbb{Q}(\sqrt{2} + \mathrm{i}\sqrt{3}).$$

(a) Zeigen Sie $K_j \subseteq L$ für $j = 1, 2, 3$.
(b) Bestimmen Sie für $j = 1, 2, 3$ jeweils das Minimalpolynom von $x = \sqrt{2} + \mathrm{i}\sqrt{3}$ über K_j. (Hinweis: Berechnen Sie x^2, x^3 und x^4 wie in Beispiel 2.2. Durch

nähere Inspektion von x^3 sollten Sie auch $K_2 \subseteq L$ und $K_3 \subseteq L$ bestätigen können.)

4.2. *(Endliche Körper)*
Es sei $q = p^n$ eine Primzahlpotenz und $\mathbb{F}_q$ ein endlicher Körper mit genau q Elementen. Zeigen Sie:

(a) Für alle $x \in \mathbb{F}_q$ gilt $x^q - x = 0_{\mathbb{F}_q}$. (Hinweis: für $x = 0_{\mathbb{F}_q}$ ist das klar. Für alle anderen x kann man in der endlichen Gruppe $\mathbb{F}_q^\times$ arbeiten.)

(b) $\mathbb{F}_q$ ist eindeutig bis auf Isomorphie; d.h. für jeden Körper F mit $\#F = q$ gibt es einen Isomorphismus $j\colon \mathbb{F}_q \to F$. (Hinweis: Proposition 2.10.)

(c) $\mathrm{Aut}(\mathbb{F}_2) = \{\mathrm{id}_{\mathbb{F}_2}\}$, aber $\mathrm{Aut}(\mathbb{F}_4) \supsetneq \{\mathrm{id}_{\mathbb{F}_4}\}$. (Siehe Beispiel 1.4.)

4.3. *(Eindeutigkeit des algebraischen Abschlusses)*
Beweisen Sie Proposition 2.15: *Je zwei algebraische Abschlüsse von K sind K-isomorph.*
(Hinweis: Sind $\iota_a\colon K \to K^a$ und $\iota\colon K \to L$ zwei algebraische Abschlüsse von K, so können Sie Lemma 2.13 benutzen, um einen K-Homomorphismus $j\colon L \to K^a$ zu finden und anschließend zeigen, dass dieser surjektiv ist. Dafür kann man zu $x \in K^a$ das Minimalpolynom m_x von x über L anschauen und dann $j^* m_x$ betrachten.)

5. Übung

5.1. *(Transzendente Erweiterungen, II)*
Wir betrachten die Körpererweiterung $\mathbb{C}/\mathbb{Q}$. Sei $x \in \mathbb{R} \subset \mathbb{C}$ transzendent über $\mathbb{Q}$. Zeigen Sie, dass $\mathscr{B} = \{x\}$ eine Transzendenzbasis von $L = \mathbb{Q}(x, \mathrm{i})$ ist. Geben Sie überdies eine weitere Transzendenzbasis $\mathscr{B}'$ von L an derart, dass *keiner* der beiden Körper $\mathbb{Q}(\mathscr{B})$ und $\mathbb{Q}(\mathscr{B}')$ im jeweils anderen enthalten ist.

5.2. *(Separabilitätsgrad und Konstruktion von K-Homomorphismen)*
Betrachten Sie den Zwischenkörper $L = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$ der Körpererweiterung $\mathbb{C}/\mathbb{Q}$, sowie den Körper $\mathbb{A} \subset \mathbb{C}$ aus Aufgabe 3.1. Bei der Erweiterung $\mathbb{A}/\mathbb{Q}$ handelt es sich um einen algebraischen Abschluss von $\mathbb{Q}$. (Das müssen Sie hier nicht zeigen.)

(a) Bestimmen Sie den Grad $[L : \mathbb{Q}]$, sowie den Separabilitätsgrad $[L : \mathbb{Q}]_s$.

(b) Geben Sie alle $\mathbb{Q}$-Homomorphismen $L \to \mathbb{A}$ an.
(Hinweis: Anhand der vorangegangenen Teilaufgabe sollte Ihnen klar sein, wie viele $\mathbb{Q}$-Homomorphismen Sie finden müssen. Nun können Sie diese durch schrittweise Fortsetzung von $\mathrm{id}_{\mathbb{A}}|_{\mathbb{Q}}\colon \mathbb{Q} \to \mathbb{A}$ konstruieren. — Eine dafür geeignete Vorgehensweise kennen Sie bereits aus Beispiel 2.11.)

(c) Wie viele $\mathbb{Q}$-Automorphismen $L \to L$ gibt es? Geben Sie diese an!

5.3. *(Grad und Separabilitätsgrad)*
Es sei $\iota\colon K \to L$ eine Körpererweiterung mit $[L : K] < \infty$.

(a) Seien $x_1, x_2 \in L$ beliebige Elemente. Zeigen Sie, dass der Separabilitätsgrad der *Multiplikationsformel* $[K(x_1, x_2) : K]_s = [K(x_1, x_2) : K(x_1)]_s \cdot [K(x_1) : K]_s$ genügt.

(Hinweis: Sei $\iota_a\colon K \to K^a$ ein algebraischer Abschluss von K. Identifizieren Sie K-Homomorphismen $j\colon K(x_1, x_2) \to K^a$ mit Paaren $(x_1^*, x_2^*) \in K^a \times K^a$, wobei x_1^* eine Nullstelle in K^a des Minimalpolynoms von x_1 über K und x_2^* eine Nullstelle in K^a des Minimalpolynoms von x_2 über $K(x_1)$ sei. — Im letzten Fall ist K^a mittels $j|_{K(x_1)}$ als Körpererweiterung von $K(x_1)$ aufzufassen.)

(b) Beweisen Sie Proposition 3.4: *Es gilt* $[L : K]_s \leq [L : K]$ *und* $\iota\colon K \to L$ *ist genau dann separabel wenn hierin Gleichheit gilt.*
(Hinweis: Führen Sie mittels der ersten Teilaufgabe einen Induktionsbeweis.)

6. Übung

6.1. *(Endliche Körper sind perfekt)*
Ein Körper K heißt *perfekt* (oder *vollkommen*), falls jedes irreduzible Polynom über diesem automatisch separabel ist. Laut Korollar 3.7 ist jeder Körper mit Charakteristik 0 perfekt. Sei also K ein Körper mit Charakteristik $p \neq 0$ und $\phi\colon K \to K$, $x \mapsto x^p$ der Frobenius-Endomorphismus. Zeigen Sie:

(a) K ist genau dann perfekt, wenn der Frobenius-Endomorphismus surjektiv ist.
(Hinweis: Für die eine Richtung können Sie Korollar 3.7 und die Surjektivität von ϕ benutzen, um ein etwaiges separables Polynom zu zerlegen. Ist hingegen ϕ *nicht* surjektiv, so betrachten Sie zu $a \in K \setminus \phi(K)$ das Polynom $X^p - a \in K[X]$ und zeigen, dass dieses irreduzibel aber *nicht* separabel ist. Sie können die Überlegungen aus Beispiel 3.3 benutzen.)

(b) Folgern Sie, dass jeder endliche Körper perfekt ist.

6.2. *(Normalität prüfen)*
Sei $\mathbb{F}_{81}$ ein endlicher Körper mit genau 81 Elementen. Betrachten Sie die offensichtliche Körpererweiterung $\mathbb{F}_{81} \to L$ mit $L = \mathrm{Quot}(\mathbb{F}_{81}[T])$, sowie deren Zwischenkörper $K = \mathbb{F}_{81}(T^{10}) \subseteq L$. Zeigen Sie, dass die Erweiterung L/K normal ist.
(Hinweis: Sie haben schon mehrfach Polynome der Bauart $X^n - a$ faktorisiert. — Wie sahen diese Faktorisierungen aus? Gegebenenfalls hilft es, sich darauf zu berufen, dass die Einheitengruppe $\mathbb{F}_{81}^\times$ zyklisch ist.)

6.3. *(Galois-Hülle)*
Es sei $\iota\colon K \to L$ eine separable Körpererweiterung.

(a) Zeigen Sie, dass es eine separable Körpererweiterung $L \to L^g$ gibt derart, dass deren Verkettung mit ι eine normale, separable Körpererweiterung $\iota_g\colon K \to L^g$ stiftet.
(Hinweis: Falls ι nicht bereits normal ist, „fehlen“ in L laut Satz 3.10 gewissermaßen noch Elemente. Diese braucht man bloß noch hinzuadjungieren, um Normalität herzustellen, und sich überlegen, dass einem dabei die Separabilität nicht abhanden kommt.)

(b) Zeigen Sie: Hat $\iota\colon K \to L$ endlichen Grad, so kann die Erweiterung $L \to L^g$ auch mit endlichem Grad gewählt werden.

(c) Seien $K \subseteq L$ nun Teilkörper eines algebraisch abgeschlossenen Körpers K^a. Begründen sie kurz, dass man L^g in der vorherigen Teilaufgabe ebenfalls als Teilkörper von K^a wählen kann, der K und L enthält.
(Hinweis: Hier ist *fast* nichts zu tun; Die Aufgabe soll nur noch mal das generelle Prinzip verdeutlichen, dass man viele nützliche Konstruktionen auch innerhalb eines zuvor fixierten algebraischen Abschlusses durchführen kann, ohne diesen verlassen zu müssen.)

(Bemerkung: Ist die obige Körpererweiterung $L \to L^g$ minimal in dem Sinne, dass kein echter Zwischenkörper von $L \to L^g$ die Rolle von L^g einnehmen kann, so nennt man $L \to L^g$ die *Galois-Hülle von* $\iota\colon K \to L$.)

7. Übung

7.1. *(Separabilität prüfen)*

(a) Untersuchen Sie jeweils für welche $n \in \mathbb{N}_0$ die folgenden Polynome separabel sind.

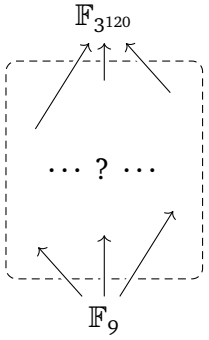
$$X^n - 1 \in \mathbb{Q}[X], \quad X^n - 1 \in \mathbb{F}_4[X], \quad X^n + X^2 \in \mathbb{C}[X].$$

(b) Betrachten Sie für jedes der obigen Polynome $P_n \in K[X]$ jeweils einen Zerfällungskörper $\iota\colon K \to L$. Für welche $n \in \mathbb{N}_0$ ist dieser jeweils separabel?
(Hinweis: Die Antwort ist vielleicht überraschend kurz — siehe Bemerkung 3.9.)

7.2. *(Zwischenkörperverband von $\mathbb{F}_{q^n}/\mathbb{F}_q$)*

(a) Beweisen Sie die letzte Aussage von Satz 4.7: *Seien q eine Primzahlpotenz und n, k natürliche Zahlen. Genau dann hat $\mathbb{F}_{q^n}$ einen — und dann auch nur einen — zu $\mathbb{F}_{q^k}$ $\mathbb{F}_q$-isomorphen Teilkörper, wenn k ein Teiler von n ist.*

(b) Zeichnen Sie ein Diagramm, welches alle Zwischenkörper der Erweiterung $\mathbb{F}_{3^{120}}/\mathbb{F}_9$ zeigt und mit den zugehörigen Körpergraden annotiert ist (wie in Beispiel 4.8).
(Hinweis: Ihr Diagramm sollte — einschließlich $\mathbb{F}_9$ und $\mathbb{F}_{3^{120}}$ — insgesamt zwölf Zwischenkörper enthalten.)



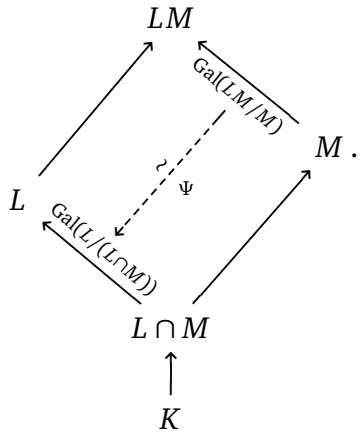
7.3. *(Der Translationssatz)*

Es seien L und M seien beide Zwischenkörper einer Körpererweiterung Z/K. Ferner sei L/K eine Galois-Erweiterung und $LM := K(L \cup M)$ der kleinste Zwischenkörper von Z/K, der $L \cup M$ enthält. Zeigen Sie die folgenden Aussagen:

(a) Die Erweiterung LM/M ist eine Galois-Erweiterung.
(Achtung: es wurde von keiner der Erweiterungen Z/K oder M/K angenommen, dass diese algebraisch zu sein brauchen.)

(b) Die Abbildung $\Psi\colon \mathrm{Gal}(LM/M) \to \mathrm{Gal}(L/(L\cap M))$, $\sigma \mapsto (\sigma|_L)$, ist wohldefiniert. Bei dieser handelt es sich außerdem um einen Gruppenisomorphismus; Insbesondere ist $\mathrm{Gal}(LM/M) \cong \mathrm{Gal}(L/(L\cap M))$.
(Hinweis: Zum Nachweis der Surjektivität von Ψ können Sie $\mathrm{Fix}(\Psi(\mathrm{Gal}(LM/M))) = L\cap M$ zeigen, und anschließend die Galois-Korrespondenz benutzen.)

Man veranschaulicht sich die Situation der aus der vorliegenden Aufgabe üblicherweise an folgendem Diagramm:



8. Übung

8.1. *(Minimalpolynome via Galois-Gruppen)*
Es sei L/K eine Galois-Erweiterung und $x \in L$ beliebig. Ferner sei $U = \mathrm{Gal}(L/K(x))$, sowie $G = \mathrm{Gal}(L/K)$. Für $\sigma \in G$ sei $\sigma U = \{\, \sigma\circ\tau : \tau \in U \,\}$ die Linksnebenklasse von U bezüglich σ. Zeigen Sie die folgenden Aussagen:

(a) Der Wert $\sigma(x)$ ist unabhängig vom Repräsentant σ von σU.

(b) Das Polynom $\prod_{\sigma U}(X - \sigma(x))$ ist das Minimalpolynom m_x von x über K, wobei das Produkt über alle verschiedenen Linksnebenklassen σU zu erstrecken ist.

(c) Es gilt $\prod_{\sigma\in G}(X - \sigma(x)) = m_x^{[L:K(x)]}$.

8.2. *(Primitive Elemente in abelschen Galois-Erweiterungen)*

(a) Sei L/K eine Galois-Erweiterung mit abelscher Galois-Gruppe. Ferner sei L Zerfällungskörper des irreduziblen Polynoms $P \in K[X]$. Zeigen Sie: Für jede Nullstelle x von P in L ist $L = K(x)$. (Hinweis: Benutzen Sie Satz 5.3 (3).)

(b) Zeigen Sie, dass es bis auf Isomorphie genau zwei Gruppen der Ordnung 6 gibt, nämlich eine zyklische Gruppe und die symmetrische Gruppe $\mathfrak{S}_3 = \mathrm{Sym}(\{1,2,3\})$.
(Hinweis: Hier ist Ihr Wissen aus der *Einführung in die Algebra* gefragt.)

(c) Sei $L = \mathbb{Q}(\zeta, \sqrt[3]{2}) \subseteq \mathbb{C}$ mit $\zeta = \exp(2\pi\mathrm{i}/3)$. Folgern Sie aus den vorherigen beiden Teilaufgaben $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathfrak{S}_3$.

8.3. *(X^3-2 und Galois-Gruppen)*
Betrachten Sie die Körpererweiterung $L = \mathbb{Q}(\zeta, \sqrt[3]{2}) \subseteq \mathbb{C}$ über $\mathbb{Q}$ mit $\zeta = \exp(2\pi i/3)$ aus Aufgabe 8.2 (c).

(a) Fertigen Sie wie in Beispiel 4.8 ein Diagramm mit allen Zwischenkörpern und den Teilmengeninklusionen zwischen diesen an.
(b) Annotieren Sie dieses Diagramm mit den Graden der dabei entstehenden Körpererweiterungen.
(c) Markieren Sie auch, bei welchen der auftretenden Erweiterungen es sich um Galois-Erweiterungen handelt.

9. Übung

9.1. *(Die Diskriminante)*
Es sei L/K ein Zerfällungskörper eines normierten separablen Polynoms $P \in K[X]$ und $P = \prod_{j=1}^{n}(X - x_j)$ mit geeigneten Elementen $x_1, \ldots, x_n \in L$. Die *Diskriminante* $\operatorname{disc}(P)$ *von* P ist definiert durch

$$\operatorname{disc}(P) = (\Delta(P))^2, \quad \text{mit} \quad \Delta(P) = \prod_{1 \le j < k \le n} (x_j - x_k).$$

(a) Zeigen Sie, dass $\operatorname{disc}(P)$ ein Element von K ist. (Hinweis: Satz 5.3 (1).)
(b) Die Galois-Gruppe $\operatorname{Gal}(P) = \operatorname{Gal}(L/K)$ operiert bekanntlich treu auf den Nullstellen von P, was einen Isomorphismus von $\operatorname{Gal}(P)$ auf eine Untergruppe der symmetrischen Gruppe $\operatorname{Sym}(\{x_1, \ldots, x_n\})$ stiftet. Der Körper K habe Charakteristik $\neq 2$. Zeigen Sie, dass diese Untergruppe genau dann in der alternierenden Gruppe in $\operatorname{Sym}(\{x_1, \ldots, x_n\})$ enthalten ist, wenn $\operatorname{disc}(P)$ ein Quadrat in K ist.
(Hinweis: Der Zusatz „in K“ im letzten Satz ist ausschlaggebend. Zeigen Sie, dass $\Delta(P)$ genau dann von einem Element von $\operatorname{Gal}(P)$ fixiert wird, wenn dieses eine Permutation mit positivem Vorzeichen auf $\{x_1, \ldots, x_n\}$ bewirkt. Die Forderung an die Charakteristik von K stellt $\Delta(P) \neq -\Delta(P)$ sicher.)
(c) Interessanterweise kann man die Diskriminante eines Polynoms anhand von dessen Koeffizienten berechnen *ohne* die Nullstellen des Polynoms zu bestimmen, z.B.

$$\operatorname{disc}(X^3 + bX^2 + cX + d) = b^2c^2 - 4c^3 - 4b^3d - 27d^2 + 18bcd \quad (\text{für } b, c, d \in K).$$

Benutzen Sie dies in Kombination mit Bemerkung 5.14, um die Galois-Gruppen der kubischen Polynome

$$P_1 = X^3 - X - 1 \in \mathbb{Q}[X] \quad \text{und} \quad P_2 = X^3 - 3X - 1 \in \mathbb{Q}[X]$$

bis auf Isomorphie zu bestimmen.
(Hinweis: Es ist hier *nicht* nötig oder gefordert, die fraglichen Polynome zu faktorisieren oder gar die Elemente der Galois-Gruppen explizit zu konstruieren. Ebenfalls ist es nicht gefordert, die angegebene Formel für die Diskriminante zu beweisen.)

9.2. *(Galois-Gruppen bestimmen)*
Betrachten Sie das Polynom $P = X^5 - 2 \in \mathbb{Q}[X]$ und dessen Zerfällungskörper $L = \mathbb{Q}(\varrho, \zeta) \subset \mathbb{C}$ mit $\varrho = \sqrt[5]{2}$ und $\zeta = \exp(2\pi\mathrm{i}/5)$.

(a) Zeigen Sie $[L : \mathbb{Q}] = 20$ und konstruieren Sie alle Elemente von $G = \mathrm{Gal}(L/\mathbb{Q})$.

(b) Zeichnen Sie die Operation der Galoisgruppe G auf $V(P) = \{\zeta^\nu \varrho : \nu \in \mathbb{Z}\}$. Benutzen Sie hierzu folgende Vorlage:
`https://www.math.tugraz.at/~mtechnau/downloads/2021-w-algebra-X5-2.pdf`
`https://www.math.tugraz.at/~mtechnau/downloads/2021-w-algebra-X5-2.tex`
(Hinweis: Sobald Sie das Abbildungsverhalten eines Elements $f \in G$ kennen, können Sie natürlich leicht $f \circ f$, $f \circ f \circ f$, usw. bestimmen, und sich dadurch Rechenaufwand sparen.)

(c) Bestimmen Sie den Isomorphietyp von G.

(d) Wählen Sie exemplarisch eine (nicht-triviale!) Untergruppe U von G und bestimmen Sie den zugehörigen Fixkörper $\mathrm{Fix}(U)$. (Hinweis: vgl. Beispiel 5.15.)

9.3. *(Elementarsymmetrische Polynome)*
Im Folgenden sei $n \in \mathbb{N}$ und $T_1, \ldots, T_n, X$ seien verschiedene Variablen. Wir schreiben zur Abkürzung $\boldsymbol{T} = \{T_1, \ldots, T_n\}$. Die *elementarsymmetrischen Polynome* $E_1, \ldots, E_n \in \mathbb{Z}[\boldsymbol{T}]$ seien definiert durch

$$P := \prod_{u=1}^{n} (X - T_u) =: X^n - E_1 X^{n-1} \pm \ldots + (-1)^n E_n X^0 \in (\mathbb{Z}[\boldsymbol{T}])[X].$$

Für $n = 3$ hat man beispielsweise $E_1 = T_1 + T_2 + T_3$, $E_2 = T_1T_2 + T_1T_3 + T_2T_3$ und $E_3 = T_1T_2T_3$. Sei K ein Körper. Wir betrachten den Körper $L = \mathrm{Quot}(K[\boldsymbol{T}])$ als Körpererweiterung von K und darin den Zwischenkörper $k = K(E_1, \ldots, E_n)$.

Die symmetrische Gruppe $\mathrm{Sym}(\boldsymbol{T})$ operiert auf L durch Vertauschen der Variablen. Ein Element von L heißt *symmetrisch*, falls es invariant unter dieser Operation ist.

(a) Welche der folgenden Elemente von L sind symmetrisch? (Hier sei $n = 3$.)

$$1_L, \quad E_2, \quad T_1T_2 + T_3, \quad \frac{T_1 + T_2 + T_3}{4(T_1T_2T_3)^9}, \quad \mathrm{disc}(P) = \prod_{1 \le u < v \le n} (T_u - T_v)^2.$$

(b) Zeigen Sie, dass L/k eine Galois-Erweiterung ist. (Hinweis: Betrachten Sie P.)

(c) Zeigen Sie: Die Operation von P auf den Nullstellen von P (also auf $\boldsymbol{T}$) induziert einen Gruppenisomorphismus $\mathrm{Gal}(L/k) \cong \mathrm{Sym}(\boldsymbol{T})$.
(Hinweis: Es ist im Wesentlichen nur einzusehen, dass jede Permutation der Unbekannten durch ein Element der Galois-Gruppe bewirkt werden kann. Konstruieren Sie ein solches Element; Starten Sie dafür mit einem geeigneten Ringhomomorphismus $K[\boldsymbol{T}] \to L$.)

(d) Zeigen Sie $k = \{f \in L : f \text{ ist symmetrisch}\}$. (Hinweis: $\mathrm{Fix}(\mathrm{Gal}(L/k))$.)

(e) Was hat diese Aufgabe mit der Formel

$$\operatorname{disc}(X^3+bX^2+cX+d) = b^2c^2-4c^3-4b^3d-27d^2+18bcd \quad (b,c,d\in K)$$

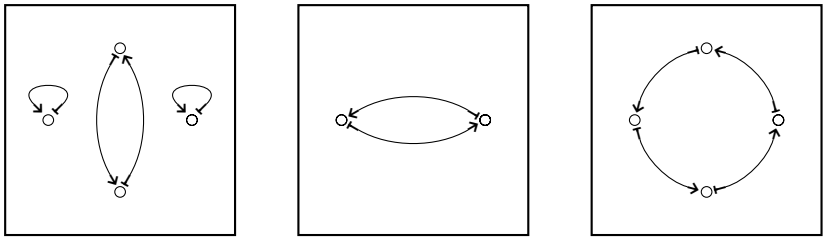
aus Aufgabe 9.1 zu tun? (Hinweis: Betrachten Sie P und $E_1,\dots,E_n$.)

10. Übung

10.1. *(Operation der Galois-Gruppe eines Polynoms)*
Gegeben seien die folgenden Polynome über $\mathbb{Q}$:

$$P_1 = X^4-2, \quad P_2 = X^4-1, \quad P_3 = X^2-4X+2.$$

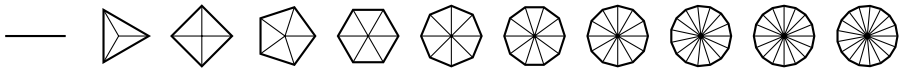
Die folgenden Abbildungen zeigen jeweils die Operation eines Elements von $\mathrm{Gal}(P_u)$ $(u=1,2,3)$ auf den Nullstellen von P_u (weiße Punkte; eingebettet in $\mathbb{C}$):



(i) (ii) (iii)

(a) Ordnen Sie den Abbildungen (i)–(iii) jeweils eine Zahl $u\in\{1,2,3\}$ zu derart, dass die in der Abbildung gezeigte Operation durch ein Element von $\mathrm{Gal}(P_u)$ bewirkt werden kann.
(b) Ist die in der ersten Teilaufgabe zu bestimmende Zuordnung eindeutig?

10.2. *(Konstruierbarkeit von regelmäßigen n-Ecken)*
Zeigen Sie, dass das regelmäßige n-Eck $\{\exp(2\pi i\nu/n) : \nu\in\mathbb{N}\}\subseteq\mathbb{C}$ genau dann mit Zirkel und Lineal konstruierbar ist, wenn $\varphi(n)$ eine Zweierpotenz ist.



2 3 4 5 6 8 10 12 15 16 17

(Hinweis: Sie können den Beweis von Korollar 5.22 übertragen. Beachten Sie jedoch, dass $(\mathbb{Z}/n\mathbb{Z})^\times$ nicht immer zyklisch ist [z.B. $(\mathbb{Z}/8\mathbb{Z})^\times\cong C_2\times C_2$]. Das macht die Konstruktion des benötigten Körperturms etwas komplizierter.)

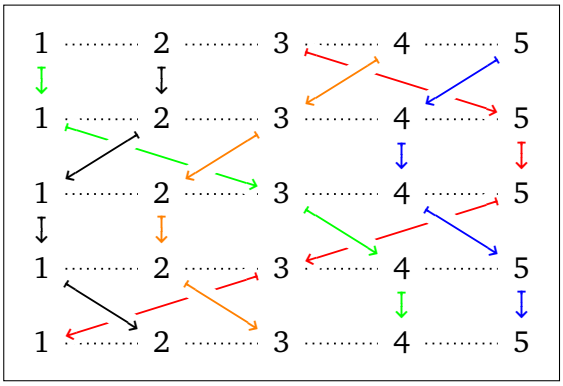
10.3. *(Beipiele für (nicht-)auflösbare Gruppen)*
(a) Zeigen Sie, dass die folgenden Gruppen auflösbar sind:
(1) Alle abelschen Gruppen G;
(2) Alle Diedergruppen D_{2n} $(n\in\mathbb{N})$;
(3) Alle symmetrischen Gruppen $\mathfrak{S}_n$ mit $1\le n\le 4$;
(4) Die Gruppe $\begin{pmatrix}\mathbb{F}_5^\times & \mathbb{F}_5\\ 0 & 1\end{pmatrix}$ (siehe auch Aufgabe 9.2).

(Hinweis: Hier ist es gegebenenfalls schneller, direkt mit der Definition zu arbeiten, anstatt Kommutatorgruppen zu berechnen. Bei $\mathfrak{S}_4$ muss man ein wenig nachdenken, kommt aber auch ohne viel Rechenarbeit zum Ziel.)

(b) Beweisen Sie Satz 5.30: *Für $n \geq 5$ ist die symmetrische Gruppe $\mathfrak{S}_n$ nicht auflösbar.*
(Hinweis: Ist $N \lhd \mathfrak{S}_n$ und $\mathfrak{S}_n/N$ abelsch, so benutzen Sie

$$(1\,2\,3) \circ (3\,4\,5) \circ (1\,2\,3)^{-1} \circ (3\,4\,5)^{-1} = (1\,4\,3),$$

um $(1\,4\,3) \in N$ einzusehen. Zeigen Sie auf ähnliche Weise, dass N alle 3-Zyklen enthält. Folgern Sie hieraus $N = A_n$ mittels Aufgabe 7.3 aus der *Einführung in die Algebra*. Wie folgt dann, dass $\mathfrak{S}_n$ nicht auflösbar ist? Alternativ zeigen Sie $\mathfrak{S}_n^{(t)} = A_n$ für $t \in \mathbb{N}$.)



11. Übung

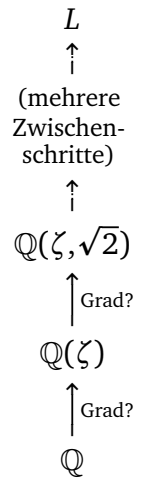
11.1. *(Verträglichkeit von Auflösbarkeit mit diversen Gruppentheorie-Konzepten)* Beweisen Sie Korollar 5.27: *Untergruppen auflösbarer Gruppen sind auflösbar und homomorphe Bilder von auflösbaren Gruppen sind auflösbar (d.h. ist $\psi\colon G \to H$ ein Grupperhomomorphismus, und G auflösbar, so ist auch* $\operatorname{im}\psi$ *auflösbar). Ist G eine Gruppe mit auflösbarem Normalteiler N und auflösbarer Quotientengruppe G/N, so ist auch G auflösbar.*

11.2. *(Radikalerweiterungen und Auflösbarkeit; qualitativ)* Alle Adjunktionen in der folgenden Aufgabe sind bezüglich der Körpererweiterung $\mathbb{C}/\mathbb{Q}$ zu verstehen. Für jede komplexe Zahl z sei $\sqrt[3]{z}$ eine beliebige Kubikwurzel von z. (Zur Erinnerung: Für $z \neq 0$ haben Sie drei verschiedene Möglichkeiten für „$\sqrt[3]{z}$“. Hier geht es nur darum, sich darauf geeinigt zu haben, bei mehrfachem Auftreten von $\sqrt[3]{z}$ stets *dieselbe* Zahl zu meinen.) Das irreduzible Polynom $P = X^6 - 2X^3 - 1 \in \mathbb{Q}[X]$ hat in $\mathbb{C}$ die sechs Nullstellen $\zeta^{2k}\sqrt[3]{1 \pm \sqrt{2}}$ $(k = 1, 2, 3)$ mit $\zeta = \exp(2\pi\mathrm{i}/6)$ und bei $R/\mathbb{Q}$ mit $R = \mathbb{Q}(x_1)$ und $x_1 = \sqrt[3]{1 + \sqrt{2}}$ handelt es sich um eine Radikalerweiterung, denn wir haben

$R = \mathbb{Q}(x_0, x_1)$ mit $x_0 = \sqrt{2}$ und

$$x_0^6 = 8 \in \mathbb{Q} \quad \text{und} \quad x_1^6 = 3 + 2\sqrt{2} \in \mathbb{Q}(x_0).$$

Nun sei $L/\mathbb{Q}$ mit $L \subseteq \mathbb{C}$ der Zerfällungskörper von $(X^6 - 1)P$.



(a) Verfahren Sie *wie im Beweis von Lemma 5.28* und konstruieren Sie einen Körperturm (mit zugehörigem Turm von Galois-Gruppen) der nebenstehenden Form, wobei in jedem „Schritt $K \to K(x)$“ nur ein Element $x \in L$ mit $x^6 \in K$ adjungiert werden soll. Bei der Betrachtung der Liste „$x_{j,1}, x_{j,2}, \ldots, x_{j,n}$“ (in der Notation aus dem Beweis von Lemma 5.28) dürfen Sie Wiederholungen vermeiden, um unnötig viele triviale (Grad 1) Schritte in Ihrem Turm zu vermeiden.

(b) Bestätigen Sie ohne Lemma 5.24, dass für jedem Ihrer Schritte $K \to K(x)$ die zugehörige Faktorgruppe $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/K(x))$ abelsch ist.
(Hinweis: Betrachten Sie $[K(x) : K]$; Damit, und zusammen mit Ihrer Kenntnis kleiner Gruppen, sollte die Frage schon fast banal sein.)

11.3. *(Moduln als Operationen)*
Sei $(R, +, \cdot)$ ein Ring und $(M, \dot{+})$ eine abelsche Gruppe zusammen mit einer Abbildung $*\colon R \times M \to M$, welche für alle $\lambda, \mu \in R$ und $v, w \in M$ die folgenden Axiome erfüllt:

- $\lambda * (v \dot{+} w) = (\lambda * v) \dot{+} (\lambda * w)$,
- $(\lambda + \mu) * v = (\lambda * v) \dot{+} (\mu * v)$,
- $(\lambda \cdot \mu) * v = \lambda * (\mu * v)$,
- $1_R * v = v$.

Dann bezeichnen wir $(M, \dot{+}, *)$ als einen ***Links-R-Modul***. Zeigen Sie, dass die Abbildungen

$$\{\text{Abbildungen } *\colon R \times M \to M \text{ mit Axiomen wie oben}\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \mathrm{Hom}(R, \mathrm{End}(M, \dot{+})),$$

gegeben durch

$$\Phi(*) = \begin{cases} R \to \mathrm{End}(M, \dot{+}), \\ \lambda \mapsto \begin{cases} M \to M, \\ v \mapsto \lambda * v \end{cases} \end{cases} \quad \text{und} \quad \Psi(\varphi) = \begin{cases} R \times M \to M, \\ (\lambda, v) \mapsto (\varphi(\lambda))(v), \end{cases}$$

zueinander inverse Bijektionen sind. (Dabei ist $R' = \mathrm{End}(M, \dot{+})$ als Ring mit punktweise definierter Addition und Verkettung von Abbildungen als Multiplikation aufzufassen und $\mathrm{Hom}(R, R')$ bezeichnet hier die Menge der Ringhomomorphismen von R nach R'.)

(Bemerkung: Diese Aufgabe zeigt, dass Links-R-Moduln die naheliegende Verallgemeinerung von Gruppen-Links-Operationen darstellen.)

12. Übung

12.1. *($K[X]$-Moduln)*
Es sei K ein Körper. Betrachten Sie die beiden Matrizen

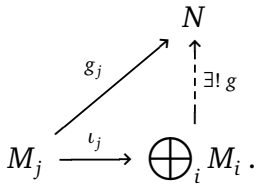
$$A := „\begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix}“ := \begin{pmatrix} 1_K & 1_K \\ 0_K & (1_K + 1_K + 1_K) \end{pmatrix} \quad \text{und} \quad B := „\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}“.$$

Die Matrix A liefert auf dem K-Vektorraum $V = K^2$ eine $K[X]$-Modulstruktur mittels

$$K[X] \times V \longrightarrow V, \quad (P, v) \longmapsto P(A) \cdot v,$$

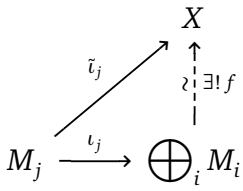
wobei $P(A) \in K^{2\times 2}$ durch Einsetzen von A in das Polynom P gegeben sei, und $P(A) \cdot v$ die Matrix–Vektor-Multiplikation bezeichne. Wir nennen den so erhaltenen $K[X]$-Modul V_A. Analog sei V_B definiert.
Zeigen Sie die folgenden Aussagen:
(a) Für $K = \mathbb{Q}$ sind V_A und V_B (als $K[X]$-Moduln) isomorph.
(b) Für $K = \mathbb{F}_2$ sind V_A und V_B (als $K[X]$-Moduln) *nicht* isomorph.
(Hinweis: Mit Blick auf Beispiel 6.3 sollte Ihnen klar werden, dass es sich hier im Kern nur um ein Ähnlichkeitsproblem von Matrizen handelt, welches Sie aus der *linearen Algebra* bereits sehr gut kennen und lösen können. Die eigentliche Aufgabe ist hier vornehmlich, zwischen der bereits bekannten Sprache der linearen Algebra und der Sprache der Modultheorie zu übersetzen.)

12.2. *(Direkte Summen von R-Moduln)*
Beweisen Sie die Aussagen (3) und (4) von Satz 6.7: Sei $(M_i)_i$ eine Familie von R-Moduln und N ein R-Modul.
(a) Für jede Familie $(g_i)_i$ von R-Modulhomomorphismen $g_i \colon M_i \to N$ gibt es genau einen R-Modulhomomorphismus $g \colon \bigoplus_i M_i \to N$, der für jeden Index j das folgende Diagramm kommutativ macht:



Überdies hat man die Formel $g = \sum_i (g_i \circ \pi_i)$.
(b) Ist X ein R-Modul zusammen mit R-Modulhomomorphismen $\tilde{\iota}_j \colon M_j \to X$ derart, dass die Aussage in (a) auch für X statt $\bigoplus_i M_i$ und $\tilde{\iota}_j$ statt ι_j gilt, so gibt es genau einen(!) R-Modulisomorphismus $f \colon \bigoplus_i M_i \to X$, welcher

für jeden Index j das folgende Diagramm kommutativ macht:



(Hinweis: Sie können sich am in der Vorlesung geführten Beweis von Satz 6.7 (1) orientieren. Beachten Sie auch Aufgabe T1.2 aus der *Einführung in die Algebra*.)

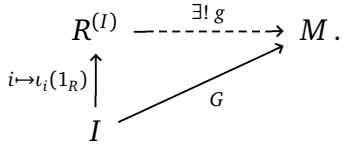
12.3. *(Direkte Summen von Moduln)*
Im Folgenden wird Ihnen jeweils eine rationale 3×3-Matrix A oder B gegeben, welche $V = \mathbb{Q}^3$,wie in Aufgabe 12.1, um eine $\mathbb{Q}[X]$-Modulstruktur augmentiert. Wir schreiben dann V_A bzw. V_B für V, um auf diese Zusatzstruktur hinzuweisen. Entscheiden Sie jeweils unter Angabe einer Begründung, ob die folgenden Aussagen stimmen:

(a) „Für $A = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 0 & 0 \\ 3 & 1 & 0 \end{pmatrix}$ ist $V_A = \mathbb{Q}[X]\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \oplus \mathbb{Q}[X]\begin{pmatrix} 1 \\ -6 \\ 3 \end{pmatrix}$;“

(b) „Für $B = \begin{pmatrix} 1 & 4 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix}$ ist $V_B = \mathbb{Q}[X]\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \oplus \mathbb{Q}[X]\begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}$.“

13. Übung

13.1. *(Freie Moduln)*
Beweisen Sie Proposition 6.10: *Sei I eine beliebige Menge. Für jeden R-Modul M und jede Abbildung $G\colon I \to M$ gibt es* genau einen *R-Modulhomomorphismus $g\colon R^{(I)} \to M$ mit $g(\boldsymbol{i}) = G(i)$ für alle $i \in I$:*



Man hat einen Isomorphismus von abelschen Gruppen

$$\mathrm{Abb}(I, M) \xrightarrow{\sim} \mathrm{Hom}_R(R^{(I)}, M), \quad G \longmapsto g.$$

Ist R kommutativ, so handelt es sich sogar um R-Modulisomorphismen.
(Hinweis: Im Wesentlichen braucht man sich bloß auf Satz 6.7 (3) berufen. Vermutlich fällt Ihre Lösung hier also sehr kurz aus.)

13.2. *(Freie Moduln und Faktormoduln)*
Wir betrachten den $\mathbb{Z}$-Modul $\mathbb{Z}[\mathrm{i}] = \{z \in \mathbb{C} : \mathrm{Re}\, z \in \mathbb{Z},\ \mathrm{Im}\, z \in \mathbb{Z}\}$ der *ganzen gaußschen Zahlen* (mit der offensichtlichen Addition und Skalarmultiplikation),

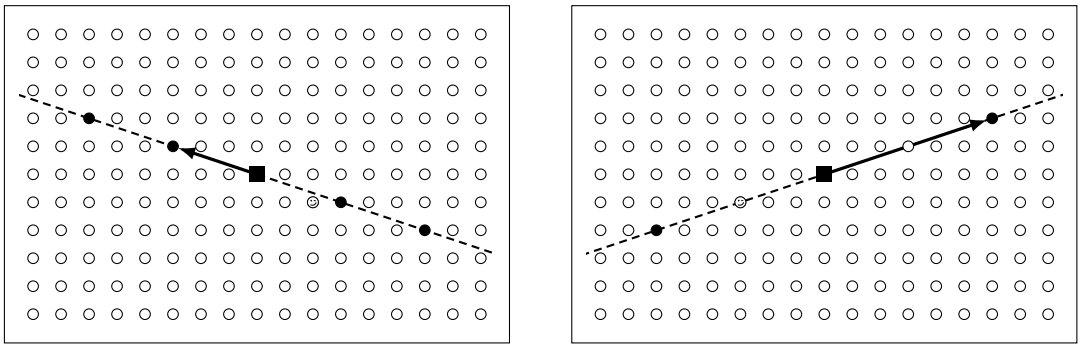
sowie die zwei Untermoduln $U = \mathbb{Z}(-3+\mathrm{i}) := \{\lambda(-3+\mathrm{i}) : \lambda \in \mathbb{Z}\}$ und $V = \mathbb{Z}(6+2\mathrm{i})$ von $\mathbb{Z}[\mathrm{i}]$.

(a) Zeigen Sie, dass $\mathbb{Z}[\mathrm{i}]$ ein freier $\mathbb{Z}$-Modul ist.

(b) Zeigen Sie, dass der Faktormodul $\mathbb{Z}[\mathrm{i}]/U$ frei ist.

(c) Zeigen Sie, dass der Faktormodul $\mathbb{Z}[\mathrm{i}]/V$ *nicht* frei ist.
(Hinweis: Kann in einem freien $\mathbb{Z}$-Modul M die Gleichung $\lambda m = 0_M$ mit $\lambda \in \mathbb{Z} \setminus \{0_\mathbb{Z}\}$ und $m \in M \setminus \{0_M\}$ gelten?)

Hinweis: Folgendes ist vielleicht hilfreich:



(Gezeichnet sind die Untermoduln U bzw. V [jeweils schwarze Punkte] im Modul $\mathbb{Z}[\mathrm{i}]$ [alle Punkte]. Der Nullpunkt ist durch ein Quadrat markiert und die Pfeile deuten jeweils auf $-3+\mathrm{i} \in U$ bzw. $6+2\mathrm{i} \in V$.)

13.3. *(So technisch, dass es wohl ein Hilfssatz sein muss…)*
Sei K ein Körper und $B \in K^{n\times n}$ eine beliebige quadratische Matrix. Wir fassen B auch als Matrix über $K[X]$ auf und betrachten die Matrix

$$A = X\begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} - B = \begin{pmatrix} X-B_{11} & & -B_{1n} \\ & \ddots & \vdots \\ -B_{21} & & \\ \vdots & & -B_{(n-1)n} \\ -B_{n1} & & X-B_{nn} \end{pmatrix} =: \begin{pmatrix} | & & | \\ A_{\bullet 1} & \cdots & A_{\bullet n} \\ | & & | \end{pmatrix}$$

mit Spalten $A_{\bullet 1}, \ldots, A_{\bullet n}$. Sei nun $P = (P_1, \ldots, P_n) \in (K[X])^n$ ein beliebiges Element. Zeigen Sie, dass es Polynome $Q_1, \ldots, Q_n \in K[X]$ und Körperelemente $r_1, \ldots, r_n \in K$ gibt derart, dass

$$\begin{pmatrix} P_1 \\ \vdots \\ P_n \end{pmatrix} = \sum_{j=1}^{n} Q_j A_{\bullet j} + \begin{pmatrix} r_1 X^0 \\ \vdots \\ r_n X^0 \end{pmatrix} = A \cdot \begin{pmatrix} Q_1 \\ \vdots \\ Q_n \end{pmatrix} + \begin{pmatrix} r_1 X^0 \\ \vdots \\ r_n X^0 \end{pmatrix}.$$

(Hinweis: Führen Sie eine Induktion über $\max\limits_{1\le i\le n} \deg P_i$. Für den Induktionsschritt können Sie Polynomdivision benutzen: Ziehen Sie ein geeignetes (polynomielles) Vielfaches einer geeigneten Spalte $A_{\bullet j}$ von P ab, um den Grad eines der P_j-Einträge zu verringern.)

14. Übung

14.1. *(Artinsche Moduln)*
Sei R ein kommutativer Ring. Ein R-Modul M heißt ***artinsch***, falls jede fallende Kette $M_0 \supseteq M_1 \supseteq \ldots$ von Untermoduln $M_0, M_1, \ldots$ von M ab einem gewissen (ggf. von der Kette abhängigen) Index n stationär wird:

$$M_0 \supseteq M_1 \supseteq \ldots \supseteq M_{n-1} \supseteq M_n = M_{n+1} = M_{n+2} = \ldots \quad \text{(ab hier nur noch Gleichheit!)}.$$

(Im Gegensatz zu der Noether-Eigenschaft, wo von aufsteigenden Ketten die Rede ist, geht es hier um absteigende Ketten.) Zeigen Sie:

(a) Für jede kurze exakte Sequenz $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ von R-Moduln ist M genau dann artinsch, wenn dies auf M' und M'' zutrifft.
(Hinweis: Sie können sich am Beweis von Proposition 7.2 (1) orientieren.)

(b) Ist der kommutative Ring R als Modul über sich selbst artinsch, so ist jedes Primideal $\mathfrak{p}$ von R ein maximales Ideal.
(Hinweis: Folgern Sie zunächst unter der Annahme, dass R artinsch ist, dass auch der Integritätsbereich $R/\mathfrak{p}$ artinsch ist und betrachten Sie in diesem zu einem Element $x \neq 0_{R/\mathfrak{p}}$ von $R/\mathfrak{p}$ die Kette $\langle x \rangle \supseteq \langle x^2 \rangle \supseteq \langle x^3 \rangle \supseteq \ldots$ und folgern Sie, dass x in $R/\mathfrak{p}$ invertierbar ist. Was sagt Ihnen das nun über das Primideal $\mathfrak{p}$?)

14.2. *(Smith Normalform bestimmen, Teil I)*
Betrachen Sie die Matrix

$$A = \begin{pmatrix} 1 & 0 & -1 & 2 \\ 1 & 2 & 1 & 0 \\ 1 & 0 & 2 & 2 \\ 1 & 2 & 2 & 0 \end{pmatrix} \in \mathbb{Z}^{4\times 4}.$$

(a) Bestimmen Sie die Smith-Normalform von A, d.h. finden Sie ganze Zahlen $d_1, \ldots, d_4 \in \mathbb{Z}$ derart, dass es (in $\mathbb{Z}^{4\times 4}$) invertierbare Matrizen $S, T \in \mathbb{Z}^{4\times 4}$ mit

$$SAT = \operatorname{diag}(d_1, d_2, d_3, d_4)$$

gibt und die Teilbarkeitsbedingung $d_i \mid d_{i+1}$ für $i = 1, 2, 3$ erfüllt ist.
(Hinweis: Der Beweis von Satz 7.5 liefert Ihnen ein Verfahren, welches dem aus der linearen Algebra bekannten Verfahren zur Rangbestimmung einer Matrix ähnelt, und Sie auf die gewünschte Diagonalgestalt bringt. Die in der Vorlesung noch nicht besprochenen Schritte des Beweises können Sie schon jetzt im Vorlesungsskriptum nachlesen.)

(b) Bestimmen Sie auch die Matrizen S und T wie in Teil (a).
(Hinweis: Betrachten Sie die Blockmatrix $\begin{pmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{1} & A \end{pmatrix} \in \mathbb{Z}^{8\times 8}$, wobei $\mathbf{0} \in \mathbb{Z}^{4\times 4}$ die Nullmatrix und $\mathbf{1} \in \mathbb{Z}^{4\times 4}$ die Einheitsmatrix bezeichne. Führen Sie an dieser ganzen Matrix nun Umformungen durch, welche den A-Teil auf Smith-Normalform D bringen und erhalten Sie so eine Blockmatrix

$\begin{pmatrix} \mathbf{0} & T \\ S & D \end{pmatrix} \in \mathbb{Z}^{8\times 8}$; Die Blöcke S und T sollten nun das Gewünschte leisten. — Können Sie sich das erklären? Einen Spezialfall dieses Verfahrens kennen Sie sicher schon aus der linearen Algebra zur Bestimmung der Inversen einer quadratischen Matrix B mit Einträgen aus einem Körper (***Gauß–Jordan-Verfahren***). Hierbei betrachtet man auch die Blockmatrix $(\,\mathbf{1}\ B\,)$ und formt mit Zeilenumformungen um, bis aus dem B-Teil die Einheitsmatrix geworden ist. Im Block daneben steht dann bekanntlich die gesuchte Inverse B^{-1}.)

14.3. *(Smith-Normalform der Transponierten)*
Es sei $A \in R^{n\times m}$ eine beliebige Matrix über einem Hauptidealbereich R. Zeigen Sie, dass A und ihre Transponierte A^{T} diesselbe Smith-Normalform besitzen, in dem Sinne, dass r und die Ideale $\langle d_1\rangle \supseteq \langle d_2\rangle \supseteq \ldots \supseteq \langle d_r\rangle \supsetneq \{0_R\}$ aus Satz 7.5 für A und A^{T} übereinstimmen.

15. Übung

15.1. *(Erzeuger und Relationen)*
Stellen Sie sich ein Szenario vor, bei dem Sie (aus irgendwelchen Gründen) an einer abelschen Gruppe $(G,+)$ interessiert sind. Im Zuge Ihrer bisherigen Untersuchungen konnten Sie feststellen, dass sich G von den drei (nicht notwendigerweise verschiedenen) Elementen $a, b, c \in G$ erzeugen lässt, und zwischen diesen die folgenden Beziehungen gelten:

$$2a + c = 0, \quad 8b - c = 0, \quad a - 3c = 0, \quad a - c = 0.$$

(0 bezeichne hier das neutrale Element in G und Ausdrücke wie $2a$ sind natürlich als $a+a$ zu verstehen.) Bestimmen Sie alle möglichen Isomorphietypen von G (im Sinne von Beispiel 6.1), welche die obigen Voraussetzungen erfüllen!
(Hinweis: Sie sollten erwarten hier mehrere mögliche Isomorphietypen zu erhalten, denn immerhin erfüllt schon die einelementige Gruppe alle obigen Voraussetzungen. Wenn man günstig argumentiert, genügt es *eine* Smith-Normalform auszurechnen, um gewissermaßen *das allgemeinste* G zu finden, welches die obigen Voraussetzungen erfüllt, und dann alle gesuchten Isomorphietypen durch Faktorbildung aus diesem allgemeinsten G abzulesen.)

15.2. *(Der Hauptsatz und $\mathbb{Z}$-Moduln)*
Betrachten Sie die Untermoduln $U = \mathbb{Z}(-3+\mathrm{i})$ und $V = \mathbb{Z}(6+2\mathrm{i})$ des $\mathbb{Z}$-Moduls $\mathbb{Z}[\mathrm{i}]$ aus Aufgabe 13.2. Bestimmen Sie für $M = \mathbb{Z}[\mathrm{i}]/U$ bzw. $M = \mathbb{Z}[\mathrm{i}]/V$ jeweils Zahlen $k, \ell \in \mathbb{N}_0$ und Ideale $\mathbb{Z}[\mathrm{i}] \supset \mathfrak{a}_1 \supseteq \ldots \supseteq \mathfrak{a}_\ell \supset \{0\}$ (wie aus Satz 8.2 (1)) mit

$$M \cong \mathbb{Z}^k \oplus \bigoplus_{i=1}^{\ell} (\mathbb{Z}/\mathfrak{a}_i).$$

(Hinweis: Zumindest für U kann man die Lösung eigentlich auch schon direkt aus Aufgabe 13.2 entnehmen. Tatsächlich wäre es hier aber eher im Sinne des

Aufgabenstellers, wenn Sie einen $\mathbb{Z}$-Modulhomomorphismus $f\colon \mathbb{Z} \to \mathbb{Z}^2$ mit $M \cong \mathbb{Z}^2/\operatorname{im} f$ fänden und die gesuchten Kenngrößen an der Smith-Normalform von $[f]_1^2 \in \mathbb{Z}^{2\times 1}$ abläsen.)

15.3. *(In Richtung Jordan-Normalform)*
Es sei K ein Körper und $B \in K^{n\times n}$. Dann wird der K-Vektorraum $V = K^n$ wie in Aufgabe 12.1 zu einem $K[X]$-Modul (den wir zur Unterscheidung als V_B notieren), wobei die Skalarmultiplikation von X mit $v \in V_B$ wie Anwenden der Matrix B auf den Vektor v wirkt. Betrachten Sie den $K[X]$-Modulhomomorphismus $g\colon (K[X])^n \to V_B$, welcher für $i = 1,\dots,n$ den i-ten Standardeinheitsvektor von $(K[X])^n$ auf den i-ten Standardeinheitsvektor in V_B abbildet.

(a) Für $K = \mathbb{Q}$, $n = 2$ ist $g(X,0)$ die erste Spalte von B. — Wieso? Beschreiben Sie in ähnlicher Weise auch, wie das Element $g(X^2+1, X-3) \in V_B$ aussieht.

(b) Zeigen Sie, dass g surjektiv ist, und der Kern von g von den Spalten der Matrix $A := X \cdot \mathbf{1}_n - B \in (K[X])^n$ aus Aufgabe 13.3 erzeugt wird:

$$\ker g = \operatorname{span}_{K[X]}\left\{\begin{pmatrix}|\\ A_{\bullet 1}\\ |\end{pmatrix},\dots,\begin{pmatrix}|\\ A_{\bullet n}\\ |\end{pmatrix}\right\} = \operatorname{im}\begin{pmatrix}(K[X])^n \to (K[X])^n\\ Q \mapsto A\cdot Q\end{pmatrix}.$$

(Hinweis: Mit dem richtigen Hilfssatz ist die Aufgabe fast schon trivial …)
(Bemerkung: Die Aufgabe impliziert $V_B \cong (K[X])^n/\operatorname{im}(v \mapsto Av)$. Dies ermöglicht es, den Isomorphietyp von V_B anhand der Smith-Normalform von A abzulesen.)

Literaturverzeichnis

[1] P. Aluffi. *Algebra: Chapter 0*. Providence, RI: AMS, 2009.

[2] E. Artin. *Algebra*. London: Pearson, 2nd edition, 2014.

[3] E. Artin and J. T. Tate. A note on finite ring extensions. *J. Math. Soc. Japan*, 3: 74–77, 1951.

[4] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra. Student economy edition*. Boulder: Westview Press, 2016.

[5] J. Bak and D. J. Newman. *Complex analysis*. Undergraduate Texts in Mathematics. New-York, NY: Springer, 3rd edition, 2010.

[6] M. Bhargava. Galois groups of random integer polynomials and van der Waerden's conjecture, 2021. Preprint: arXiv:2111.06507 [math.NT].

[7] T. S. Blyth. *Module theory. An approach to linear algebra*. University of St Andrews, 2018. Elektronische Ausgabe. Online verfügbar: `https://research-repository.st-andrews.ac.uk/handle/10023/12643`.

[8] S. Bosch. *Algebra*. Berlin: Springer, 8th edition, 2013.

[9] S. Bosch. *Algebraic geometry and commutative algebra*. London: Springer, 2013.

[10] S. K. Chebolu and J. Mináč. Counting irreducible polynomials over finite fields using the inclusion–exclusion principle. *Math. Mag.*, 84(5):369–371, 2011.

[11] P. M. Cohn. On the structure of the GL_2 of a ring. *Publ. Math., Inst. Hautes Étud. Sci.*, 30:365–413, 1966.

[12] K. Conrad. Expository papers. Online verfügbar: `https://kconrad.math.uconn.edu/blurbs/`, 2019.

[13] J. D. Dixon and B. Mortimer. *Permutation groups*. Number 163. New-York: Springer, 1996.

[14] D. Eisenbud. *Commutative algebra. With a view toward algebraic geometry*. Berlin: Springer, 1995.

[15] D. Eisenbud and J. Harris. *The geometry of schemes*. New York, NY: Springer, 2000.

[16] Chr. Elsholtz. Einführung in die Algebra. Vorlesungsskriptum. Für angemeldete Benutzer online verfügbar: `https://tc.tugraz.at/main/course/view.php?id=352`, 2019.

[17] C. F. Gauß. *Untersuchungen über höhere Arithmetik. (*Disquisitiones arithmeticae*.)*. Berlin: Springer, 1889. Herausgegeben von H. Maser. Online verfügbar: `https://gdz.sub.uni-goettingen.de/id/PPN373456743`.

[18] R. Gilmer. A note on the algebraic closure of a field. *Am. Math. Mon.*, 75: 1101–1102, 1968.
[19] R. Hartshorne. *Algebraic geometry*. New York, NY: Springer, 1983.
[20] K. Ireland and M. Rosen. *A classical introduction to modern number theory*. New York, NY: Springer, 2nd edition, 1990.
[21] H. Iwaniec and E. Kowalski. *Analytic number theory*. Providence, RI: American Mathematical Society (AMS), 2004.
[22] Z. Jelonek. A simple proof of the existence of the algebraic closure of a field. *Zesz. Nauk. Uniw. Jagiell., Univ. Iagell. Acta Math.*, 1100:131–132, 1993.
[23] Chr. Karpfinger and K. Meyberg. *Algebra. Gruppen, Ringe, Körper.* Berlin: Springer, 4th edition, 2017.
[24] E. Kunz. *Introduction to commutative algebra and algebraic geometry*. London: Springer, 2013.
[25] S. Lang. *Algebraic number theory*. New York, NY: Springer, 2nd edition, 1994.
[26] S. Lang. *Algebra*. New York, NY: Springer, 3rd edition, 2002.
[27] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory. I. Classical theory*. Cambridge: Cambridge University Press, 2007.
[28] J. Neukirch. *Algebraische Zahlentheorie*. Berlin: Springer, 2007.
[29] M. Rosen. *Number theory in function fields*. Number 210. New York, NY: Springer, 2002.
[30] W. Soergel. Kommutative Algebra und Geometrie. Vorlesungsskriptum. Online verfügbar: `https://home.mathematik.uni-freiburg.de/soergel/Skripten/XXKAG.pdf`, 2019.
[31] E. M. Stein and R. Shakarchi. *Complex analysis*. Princeton, NJ: Princeton University Press, 2003.
[32] M. Technau. Einführung in die komplexe Analysis. Vorlesungsskriptum. Online verfügbar: `https://www.math.tugraz.at/~mtechnau/downloads/einfkomplanalysis.pdf`, 2021.
[33] M. Technau. Einführung in die Algebra. Vorlesungsskriptum. Online verfügbar: `https://www.math.tugraz.at/~mtechnau/downloads/einfalgebra.pdf`, 2023.
[34] E. C. Titchmarsh. *The theory of the Riemann zeta-function. 2nd ed., rev. by D. R. Heath-Brown*. Oxford Science Publications. Oxford: Clarendon Press, 1986.
[35] B. L. van der Waerden. Die Seltenheit der Gleichungen mit Affekt. *Math. Ann.*, 109:13–16, 1933.
[36] J. Wolfahrt. *Einführung in die Zahlentheorie und Algebra*. Braunschweig: Vieweg, 1996.
[37] O. Zariski. A new proof of Hilbert's Nullstellensatz. *Bull. Am. Math. Soc.*, 53: 362–368, 1947.

Index