universität innsbruck
Institut für Mathematik

Algebra I + II

Tim Netzer
Wintersemester 2024/25
Sommersemester 2025

Inhaltsverzeichnis

Kapitel 1

Einleitung und Motivation

Fast die gesamte Theorie dieser Vorlesung hat sich aus Fragen entwickelt, die bereits in der Antike gestellt wurden. Exakte Lösungen der Probleme konnten aber erst deutlich später gegeben werden, als die abstrakte Theorie weit genug entwickelt war. Diese Entwicklung werden wir im Verlauf der Vorlesung nachvollziehen. Als Motivation für die kommenden Begriffe und Ergebnisse schauen wir uns aber zunächst einige der klassischen Fragen an.

1.1 Konstruktion mit Zirkel und Lineal

Bei der Konstruktion mit Zirkel und Lineal startet man mit einer Teilmenge $M \subseteq \mathbb{R}^2$ und konstruiert dann iterativ neue Punkte. Dabei sind drei elementare Konstruktionsschritte erlaubt:

Definition 1.1.1. Sei $M \subseteq \mathbb{R}^2$ gegeben.

(i) Seien $p_1, p_2, q_1, q_2 \in M$ mit $p_1 \neq p_2, q_1 \neq q_2$. Sei G_1 die Gerade durch p_1, p_2 und G_2 die Gerade durch q_1, q_2. Falls sich G_1 und G_2 in genau einem Punkt x schneiden, so heißt x *in einem Schritt vom Typ 1 aus M konstruierbar*.

(ii) Seien $p_1, p_2, q, q_1, q_2 \in M$ mit $p_1 \neq p_2$. Sei G die Gerade durch p_1, p_2 und K der Kreis mit Radius $\|q_1 - q_2\|$ um den Mittelpunkt q. Falls x ein Schnittpunkt von G und K ist, so heißt x *in einem Schritt vom Typ 2 aus M konstruierbar*.

(iii) Seien $p, p_1, p_2, q, q_1, q_2 \in M$ mit $p \neq q$. Sei K_1 der Kreis mit Radius $\|p_1 - p_2\|$ um den Punkt p und K_2 der Kreis mit Radius $\|q_1 - q_2\|$ um den Punkt

q. Falls x ein Schnittpunkt von K_1 und K_2 ist, dann heißt x *in einem Schritt vom Typ 3 aus* M *konstruierbar*.

Wir definieren $M^{(0)} = M$ und iterativ $M^{(i+1)}$ als die Vereinigung von $M^{(i)}$ mit der Menge aller Punkte, die in einem Schritt (irgendeines Typs) aus $M^{(i)}$ konstruierbar sind. Dann gilt $M = M^{(0)} \subseteq M^{(1)} \subseteq M^{(2)} \subseteq \cdots$ und wir setzen

$$\mathrm{Kon}(M) = \bigcup_{i \geq 0} M^{(i)}.$$

$\mathrm{Kon}(M)$ ist also die Menge aller Punkte, die in endlich vielen Schritten aus M konstruierbar sind. △

Um die Konstruktion mit Zirkel und Lineal besser algebraisch beschreiben zu können, identifizieren wir ab jetzt $\mathbb{R}^2$ mit dem Körper $\mathbb{C}$ der komplexen Zahlen.

Satz 1.1.2. *Es sei* $0, 1 \in M \subseteq \mathbb{C}$. *Dann gilt:*

(i) $\mathrm{Kon}(M)$ *ist ein Teilkörper von* $\mathbb{C}$, *der* $\mathbb{Q}$ *enthält und abgeschlossen unter komplexer Konjugation ist.*

(ii) Für $x \in \mathbb{C}$ *mit* $x^2 \in \mathrm{Kon}(M)$ *gilt* $x \in \mathrm{Kon}(M)$.

Beweis. Aufgabe 5. □

Die klassischen Konstruktionsprobleme der Antike kann man nun exakt formulieren:

Problem 1.1.3 (Dreiteilung des Winkels)**.** *Gegeben sei ein Winkel in der Ebene. Gibt es eine Möglichkeit, ihn mit Zirkel und Lineal in drei gleich große Teile zu zerteilen?*
In exakter Formulierung: Es sei $\varphi \in (0, \pi)$ *und* $e^{i\varphi} := \cos\varphi + i \sin\varphi \in \mathbb{C}$. *Gilt stets* $e^{i\varphi/3} \in \mathrm{Kon}(\{0, 1, e^{i\varphi}\})$? △

Problem 1.1.4 (Konstruktion regulärer Vielecke)**.** *Welche regulären* n*-Ecke lassen sich mit Zirkel und Lineal konstruieren?*
In exakter Formulierung: Für welche n *gilt* $e^{2\pi i/n} \in \mathrm{Kon}(\{0, 1\})$? △

Problem 1.1.5 (Quadratur des Kreises)**.** *Gegeben sei ein Kreis. Kann man mit Zirkel und Lineal ein Quadrat mit gleichem Flächeninhalt konstruieren?*
In exakter Formulierung zum Beispiel: Gilt $\sqrt{\pi} \in \mathrm{Kon}(\{0, 1\})$? △

Problem 1.1.6 (Würfelverdoppelung). *Gegeben sei ein Würfel (durch seine Kantenlänge). Kann man daraus die Kantenlänge eines Würfels von doppeltem Volumen konstruieren?*
In exakter Formulierung zum Beispiel: Gilt $\sqrt[3]{2} \in \mathrm{Kon}(\{0,1\})$? △

Um diese Probleme zu lösen, müssen wir den Körper $\mathrm{Kon}(M)$ und seine Eigenschaften untersuchen und verstehen.

1.2 Nullstellen durch Radikale berechnen

Sei k ein Körper und $p \in k[x]$ ein Polynom. Wir wollen die Nullstellen von p in k (oder einem größeren Körper) berechnen.

Beispiel 1.2.1. (i) In k gelte $1+1 \neq 0$ und sei $p = x^2 + ax + b \in k[x]$. Dann sind die Nullstellen von p gerade

$$\lambda_{1,2} = \frac{-a \pm \sqrt{a^2 - 4b}}{2}.$$

Ersetzt man nämlich zunächst x durch $x - a/2$, erhält man

$$q(x) = p\left(x - \frac{a}{2}\right) = x^2 + b - \frac{a^2}{4}$$

und die Nullstellen von q sind offensichtlich $\gamma_{1,2} = \pm\sqrt{\frac{a^2}{4} - b}$. Daraus erhält man für p die Nullstellen $\lambda_{1,2} = \gamma_{1,2} - \frac{a}{2}$.
(ii) In k gelte $1+1 \neq 0$ und $1+1+1 \neq 0$. Sei $p = x^3 + ax + b \in k[x]$ (einen quadratischen Term kann man wieder durch eine Translation einfach loswerden). Dann besitzt das Polynom p die folgende Nullstelle:

$$\gamma_1 = \sqrt[3]{-\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}} + \sqrt[3]{-\frac{b}{2} - \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}}.$$

Das ist die sogenannte *Cardanische Formel*.
(iii) Auch für Polynome vom Grad 4 gibt es noch eine Lösungsformel, welche die Nullstellen anhand von $+, -, \cdot, /$ und (höheren) Wurzeln aus den Koeffizienten von p berechnet. Das sind die Formeln von Ferrari. △

Problem 1.2.2 (Lösung polynomialer Gleichungen mit Radikalen)**.** *Gibt es eine Formel, die nur mit* $+, -, \cdot, /$ *und höheren Wurzeln die Nullstellen jedes Polynoms vom Grad* 5 *(oder höher) aus seinen Koeffizienten berechnet?*
Für welche Polynome entstehen die Nullstellen überhaupt auf solche Weise aus den Koeffizienten? △

Auch hier kommt wieder ein Körper ins Spiel. Sei etwa $p \in \mathbb{Q}[x]$ gegeben. Dann zerfällt p über $\mathbb{C}$ vollständig in Linearfaktoren:

$$p = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_d)$$

mit $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$. Sei nun K der kleinste Körper zwischen $\mathbb{Q}$ und $\mathbb{C}$, der alle Nullstellen $\alpha_1, \ldots, \alpha_d$ enthält. Wir nennen ihn den *Zerfällungskörper* von p. Ob man die α_i wie oben aus den Koeffizienten von p berechnen kann, spiegelt sich nun in einer (relativ komplizierten) Eigenschaft dieses Körpers wieder. Um diese zu überprüfen, übersetzt man sie gewöhnlich in eine Eigenschaft von Gruppen, anhand der sogenannten *Galoistheorie*. Dort lässt sich die Eigenschaft dann besser entscheiden und man kommt zu einer Lösung des Nullstellenproblems.

1.3 Lineare Diophantische Gleichungen

In der linearen Algebra betrachtet man lineare Gleichungssysteme über Körpern. Ganz anders wird die Frage, wenn man sich für solche Systeme über Ringen interessiert. Ein System linearer diophantischer Gleichungen ist von der Gestalt

$$Ax = b$$

mit $A \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ und $b \in \mathbb{Z}^m$. Es sollen nun alle Lösungen $x \in \mathbb{Z}^n$ gefunden werden. Der klassische Gauß-Algorithmus funktioniert dabei nicht ohne weiteres, da man dabei durch Einträge der Matrix teilen muss, was in $\mathbb{Z}$ im Allgemeinen nicht möglich ist. Bringt man die Matrix dagegen über $\mathbb{Q}$ auf Dreiecksgestalt, ist im Allgemeinen überhaupt nicht klar, wie man alle ganzzahligen Lösungen ablesen kann. Man muss die Theorie der linearen Algebra also nochmal neu entwicklen, diesmal für Ringe. Das führt zur sogenannten *Modultheorie*.

Alle genannten Probleme werden wir im Lauf der Vorlesung betrachten und teilweise lösen können. Dabei sind nur wenige Vorkenntnisse aus der linearen Algebra nötig. Außer gewissen grundlegenden Konzepten der Mathematik benötigen

wir den Begriff des Vektorraums, der Basis und der Dimension. Außerdem verwenden wir die komplexen Zahlen und einige ihrer Eigenschaften. Alle anderen Konzepte und Ergebnisse werden im Skript eingeführt.

Die Inhalte der Vorlesung werden auch in vielen Lehrbüchern der Algebra behandelt. Im Anhang finden Sie dazu eine (unvollständige) Liste.

Ich danke den bisherigen Hörern dieser Vorlesung und zwei meiner Kollegen für viele Hinweise auf Fehler und Verbesserungen im ursprünglichen Skript; ganz besonders Martin Berger, Tom Drescher, Tobias Olsacher und Florian und Lukas Willmann. Trotzdem kann das Skript natürlich immer noch Fehler beinhalten und ich bin für Hinweise auf diese sehr dankbar.

Kapitel 2

Gruppen

Eine der wichtigsten algebraischen Strukturen ist die Gruppe. Obwohl der Begriff aus der linearen Algebra bekannt ist, führen wir ihn hier nochmal neu ein, um dann tiefere Ergebnisse der Gruppentheorie zu beweisen. In Zusammenhang mit der Galoistheorie ermöglicht uns das später starke Aussagen über Körper.

2.1 Grundlagen

Definition 2.1.1. (i) Eine **Gruppe** ist eine Menge G, zusammen mit einer zweistelligen Verknüpfung

$$*\colon G \times G \to G,$$

die folgende Bedingungen erfüllt:

(Assoziativgesetz) $\quad \forall f, g, h \quad (f * g) * h = f * (g * h),$

(neutrales Element) $\quad \exists e \forall g \quad e * g = g * e = g,$

(inverse Elemente) $\quad \forall g \exists h \quad g * h = h * g = e.$

(ii) Gilt zusätzlich

(Kommutativgesetz) $\forall g, h \quad g * h = h * g$

so nennt man G eine **kommutative** oder **abelsche** Gruppe.
(iii) Eine **Untergruppe** von G ist eine nichtleere Teilmenge $H \subseteq G$ mit

(Abgeschlossenheit unter $*$) $\quad g, h \in H \Rightarrow g * h \in H,$

(Abgeschlossenheit unter Inversen) $h \in H, g \in G$ invers zu $h \Rightarrow g \in H$.

Wir verwenden dafür auch die Schreibweise $H < G$. △

Bemerkung 2.1.2. Streng genommen ist die Definition oben zunächst problematisch. Zuerst wird die Existenz (mindestens) eines neutralen Elements e gefordert, das in der Bedingung als gebundene Variable auftaucht. In der Definition von inversen Elementen wird dann aber auf dieses e referenziert. Das ist aus logischer Sicht sinnlos, und formal richtig müsste das neutrale Element eigentlich ebenso wie die Verknüpfung Teil der gegebenen Gruppenstruktur sein, eine Gruppe also als ein Tripel $(G, *, e)$ mit den geforderten Eigenschaften definiert werden.
Es stellt sich aber heraus dass das neutrale Element, wenn es denn existiert, eindeutig bestimmt ist (das ist eine leichte Übungsaufgabe). Mit diesem Wissen ist die obige Definition also in Ordnung, und in den meisten Lehrbüchern findet man dann auch genau diese. △

Beispiel 2.1.3. (i) Beispiele für abelsche Gruppen sind $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ (oder jeder beliebige Körper) mit $+$ und $e = 0$. Dabei sind die kleineren jeweils Untergruppen in den größeren.
(ii) Für $n \in \mathbb{N}$ sei

$$\mathbb{Z}/n\mathbb{Z} := \{0, 1, \ldots, n-1\}$$

versehen mit der Addition wie auf einer Uhr. Wir addieren also wie gewöhnlich, identifizieren aber n mit 0, $n+1$ mit 1 usw... Auf diese Weise erhalten wir eine abelsche Gruppe mit n Elementen. Sie ist aber *keine Untergruppe* von $\mathbb{Z}$, denn die Verknüpfung ist eine andere. In $\mathbb{Z}$ gilt $(n-1)+1 = n$, in $\mathbb{Z}/n\mathbb{Z}$ gilt $(n-1)+1 = 0$.
(iii) Für einen Körper K ist $K \setminus \{0\}$ mit $\cdot$ und $e = 1$ eine abelsche Gruppe.
(iv) Die Menge $\mathrm{GL}_n(K)$ der invertierbaren Matrizen mit Einträgen aus K ist mit Matrixmultiplikation und $e = I$ ebenfalls eine Gruppe, die für $n \geq 2$ nicht abelsch ist.
(v) Für jede Menge X bilden die bijektiven Abbildungen von X nach X eine Gruppe $S(X)$ bezüglich der Hintereinanderausführung $\circ$, das neutrale Element ist dabei die identische Abbildung id_X. Falls X mindestens 3 Elemente hat, ist $S(X)$ nicht abelsch. $S(X)$ wird als **Permutationsgruppe** oder **Symmetriegruppe** von X bezeichnet.
Im Fall $X = \{1, \ldots, n\}$ schreiben wir statt $S(X)$ auch S_n und verwenden für Permutationen $\sigma \in S_n$ auch die bereits bekannte Matrixschreibweise

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

oder die Darstellung als Produkt von Zykeln

$$(1, \sigma(1), \sigma(\sigma(1)), \ldots).$$

(vi) Sind $(G, *)$ und $(H, \cdot)$ Gruppen, so ist das kartesische Produkt $G \times H$ ebenfalls eine Gruppe mit der komponentenweise definierten Verknüpfung

$$(g, h) \circ (g', h') := (g * g', h \cdot h').$$

Das neutrale Element ist dabei (e_G, e_H) und das inverse Element zu (g, h) ist (g^{-1}, h^{-1}). △

Bemerkung 2.1.4. (i) Das Assoziativgesetz erlaubt uns, Klammern bei komplizierteren Ausdrücken meistens ganz wegzulassen.
(ii) Man beachte nochmals, dass die Definition der inversen Elemente auf das neutrale Element e Bezug nimmt. Dieses ist eindeutig bestimmt. Um über inverse Element sprechen zu können, muss man es aber kennen. Das inverse Element zu einem festen Element ist dann ebenfalls eindeutig bestimmt.
(iii) Untergruppen enthalten immer das neutrale Element e und sind für sich selbst betrachtet Gruppen.
(vi) In abelschen Gruppen wird die Verknüpfung oft mit $+$ bezeichnet und das neutrale Element mit 0. Das zu g inverse Element wird dann mit $-g$ bezeichnet. In nicht-abelschen Gruppen verwenden wir oft $\cdot$ und 1 oder $\circ$ und id für die Verknüpfung und das neutrale Element. Das zu g inverse Element wird dann mit g^{-1} bezeichnet. Oft lassen wir $\cdot$ auch einfach weg, schreiben also gh statt $g \cdot h$. △

Besonders interessiert uns die Frage, welche Untergruppen eine Gruppe haben kann. Für die ganzen Zahlen ist das leicht zu erkennen:

Lemma 2.1.5. *Jede Untergruppe von $(\mathbb{Z}, +)$ ist von der Gestalt*

$$n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$$

für ein $n \in \mathbb{Z}$.

Beweis. Sei $H < \mathbb{Z}$. Der Fall $H = \{0\}$ ist trivial, also sei $n \in H \setminus \{0\}$ ein Element von kleinstem Betrag. Dann gilt $n\mathbb{Z} \subseteq H$, weil H eine Untergruppe ist. Sei umgekehrt $h \in H$. Division mit Rest liefert

$$h = nx + r$$

mit $x, r \in \mathbb{Z}$, $|r| < |n|$. Wegen $r = h - nx \in H$ folgt daraus $r = 0$, weil n von minimalem Betrag gewählt war. Somit gilt $h \in n\mathbb{Z}$. □

Wenn man Abbildungen zwischen mathematischen Strukturen betrachtet, fordert man sinnvollerweise immer eine Strukturerhaltungseigenschaft. Für Gruppen führt das zum Begriff des Gruppenhomomorphismus:

Definition 2.1.6. (i) Seien $(G, *), (H, \circ)$ Gruppen. Ein **Gruppenhomomorphismus** ist eine Abbildung $\varphi\colon G \to H$ mit

$$\varphi(g * h) = \varphi(g) \circ \varphi(h)$$

für alle $g, h \in G$.
(ii) Ein **Isomorphismus** ist ein bijektiver Homomorphismus φ. Das ist äquivalent dazu, dass es einen Homomorphismus $\psi\colon H \to G$ gibt mit $\varphi \circ \psi = \mathrm{id}_H, \psi \circ \varphi = \mathrm{id}_G$.
(iii) Zwei Gruppen G, H heißen **isomorph** ($H \cong G$), falls es einen Isomorphismus zwischen ihnen gibt. △

Beispiel 2.1.7. (i) Lineare Abbildungen $f\colon V \to W$ zwischen Vektorräumen sind Gruppenhomomorphismen.
(ii) Die Multiplikation mit einem festen Körperelement $g \in K$ ist ein Gruppenhomomorphismus

$$\begin{aligned} \mathrm{m}_g\colon (K, +) &\to (K, +) \\ h &\mapsto gh. \end{aligned}$$

Betrachtet man stattdessen die Gruppe $(K \setminus \{0\}, \cdot)$, ist es kein Homomorphismus.
(iii) Die Exponentialfunktion $\exp\colon (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ ist ein Gruppenisomorphismus. Insbesondere $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$.
(iv) Die Menge $\{-1, 1\}$ ist bezüglich $\cdot$ eine Gruppe. Sie ist isomorph zu $\mathbb{Z}/2\mathbb{Z}$ mit $+$.
(v) Die Signatur von Permutationen

$$\mathrm{sgn}\colon S_n \to \{1, -1\}$$

ist ein Gruppenhomomorphismus.
(vi) Die Determinante ist ein Gruppenhomomorphismus

$$\det\colon \mathrm{GL}_n(K) \to K \setminus \{0\}.$$ △

Bemerkung 2.1.8. (i) Gruppenhomomorphismen bilden stets die neutralen Elemente aufeinander ab und inverse Elemente auf die entsprechenden Inversen: $\varphi(g)^{-1} = \varphi(g^{-1})$.
(ii) Zwei isomorphe Gruppen sind völlig identisch, bis auf die Namen ihrer Elemente. Wir müssen zwischen ihnen nicht mehr unterscheiden. △

Der Begriff der *Nebenklasse*, den wir jetzt definieren, entspricht dem eines affinen Untervektorraums aus der linearen Algebra:

Definition 2.1.9. (i) Für eine Untergruppe $H < G$ und $g \in G$ heißt die Menge

$$gH := \{gh \mid h \in H\}$$

eine **Linksnebenklasse** von H in G. Analog heißt

$$Hg := \{hg \mid h \in H\}$$

Rechtsnebenklasse. Es gilt

$$gH = \tilde{g}H \Leftrightarrow g^{-1}\tilde{g} \in H.$$

Genauso ist $Hg = H\tilde{g}$ äquivalent zu $g\tilde{g}^{-1} \in H$.
(ii) Wir bezeichnen mit $G/H := \{gH \mid g \in G\}$ die Menge der Linksnebenklassen und analog mit $H\backslash G$ die Menge der Rechtsnebenklassen.
(iii) Eine Untergruppe $H < G$ heißt **Normalteiler** oder **normale Untergruppe** von G, falls $gH = Hg$ für alle $g \in G$ gilt. Das ist äquivalent zu

$$h \in H, g \in G \Rightarrow g^{-1}hg \in H.$$

Wir schreiben dafür $H \lhd G$. △

Bemerkung/Beispiel 2.1.10. (i) In einer abelschen Gruppe gilt stets

$$g^{-1}hg = hg^{-1}g = he = h,$$

also ist jede Untergruppe normal.
(ii) Wir betrachten $G = S_3$ und darin die Untergruppe $H = \{\mathrm{id}, (23)\}$. Wir berechnen

$$(13) \circ H = \{(13), (132)\}, \quad H \circ (13) = \{(13), (123)\}.$$

Diese beiden Mengen stimmen nicht überein, also ist H keine normale Untergruppe von S_3. △

Lemma 2.1.11. *Für einen Gruppenhomomorphismus $\varphi\colon G \to H$ ist*

$$\ker(\varphi) := \{g \in G \mid \varphi(g) = e_H\}$$

eine normale Untergruppe von G und

$$\mathrm{im}(\varphi) := \{\varphi(g) \mid g \in G\}$$

eine Untergruppe von H. Es ist φ genau dann injektiv, wenn $\ker(\varphi) = \{e_G\}$.

Beweis. Offensichtlich sind $\ker(\varphi)$ und $\mathrm{im}(\varphi)$ jeweils Untergruppen. Für $h \in \ker(\varphi)$ und $g \in G$ gilt

$$\varphi(g^{-1}hg) = \varphi(g)^{-1}\varphi(h)\varphi(g) = \varphi(g)^{-1}e_H\varphi(g) = e_H,$$

also $g^{-1}hg \in \ker(\varphi)$. Damit ist $\ker(\varphi)$ eine normale Untergruppe.
Für die Injektivität sei $\ker(\varphi) = \{e_G\}$ und $\varphi(g_1) = \varphi(g_2)$ für gewisse $g_1, g_2 \in G$. Dann gilt

$$e_H = \varphi(g_1)^{-1}\varphi(g_2) = \varphi(g_1^{-1}g_2),$$

also $g_1^{-1}g_2 \in \ker(\varphi)$, also $g_1^{-1}g_2 = e_G$, also $g_1 = g_2$. □

Proposition 2.1.12. *Sei $H < G$. Dann gilt für $g, g_1, g_2 \in G$ stets*

$$g_1H = g_2H \text{ oder } g_1H \cap g_2H = \emptyset$$

sowie

$$\#gH = \#H = \#Hg.$$

Insbesondere ist G disjunkte Vereinigung seiner Linksnebenklassen sowie seiner Rechtsnebenklassen und deren Anzahl (falls G endlich ist) stimmt überein.

Beweis. Sei $g \in g_1H \cap g_2H$, also $g = g_1h_1 = g_2h_2$ mit $h_1, h_2 \in H$. Damit ist $g_1 = g_2h_2h_1^{-1} \in g_2H$ und somit $g_1H \subseteq g_2H$. Die andere Inklusion folgt analog (ebenso für Rechtsnebenklassen).
Wegen $g = ge \in gH$ für alle $g \in G$ ist G also die disjunkte Vereinigung der Nebenklassen.
Die surjektive Abbildung $H \to gH,\ h \mapsto gh$ ist injektiv aufgrund der Existenz des Inversen von g (analog für Rechtsnebenklassen). Daraus folgt die Gleichheit der Mächtigkeiten und damit insbesondere die Gleichheit ihrer Anzahl. □

Wir können nun den ersten wichtigen Satz über mögliche Untergruppen einer Gruppe beweisen. Er formuliert eine notwendige Bedingung, schließt also die Existenz von Untergruppen mit gewissen Eigenschaften aus.

Satz 2.1.13 (Satz von Lagrange)**.** *Sei G eine endliche Gruppe und $H < G$. Dann ist die Mächtigkeit von H ein Teiler der Mächtigkeit von G.*

Beweis. G wird disjunkt zerlegt durch die Nebenklassen von H, die alle gleich viele Elemente wie H haben. Damit ist die Aussage klar. □

Bemerkung 2.1.14. (i) Eine Gruppe mit 8 Elementen kann höchstens Untergruppen mit der Mächtigkeit $1, 2, 4, 8$ haben.
(ii) Eine Gruppe G mit Primzahlmächtigkeit hat nur die beiden trivialen Untergruppen $\{e\}$ und G. △

Definition 2.1.15. Sei G endlich und $H < G$. Dann heißt

$$|G : H| := \frac{\#G}{\#H} = \#(G/H) = \#(H\backslash G)$$

der **Index** von H in G. △

Der folgende Satz zeigt, warum die Normalität einer Untergruppe interessant ist. Die beschriebene Konstruktion ist analog zur Konstruktion eines Faktorraums aus der linearen Algebra.

Satz 2.1.16. *Sei $H \lhd G$. Dann ist die Menge G/H auf folgende Weise mit einer wohldefinierten Verknüpfung versehen, die sie zu einer Gruppe macht:*

$$(g_1H) \cdot (g_2H) := (g_1g_2)H.$$

Die Projektion

$$\begin{aligned} \pi \colon G &\to G/H \\ g &\mapsto gH \end{aligned}$$

ist ein surjektiver Gruppenhomomorphimus mit $\ker(\pi) = H$.

Beweis. Wir zeigen zunächst die Wohldefiniertheit. Sei dazu

$$g_1H = \tilde{g}_1H,\ g_2H = \tilde{g}_2H,$$

also $g_1^{-1}\tilde{g}_1 \in H, g_2^{-1}\tilde{g}_2 \in H$. Aufgrund der Normalität gibt es ein $h \in H$ mit

$$g_1^{-1}\tilde{g}_1\tilde{g}_2 = \tilde{g}_2 h.$$

Damit gilt $(g_1g_2)^{-1}(\tilde{g}_1\tilde{g}_2) = g_2^{-1}g_1^{-1}\tilde{g}_1\tilde{g}_2 = g_2^{-1}\tilde{g}_2 h \in H$, also

$$(g_1g_2)H = (\tilde{g}_1\tilde{g}_2)H.$$

Nachdem die Wohldefiniertheit gezeigt ist, folgen die Gruppeneigenschaften direkt aus denen von G:

$$\begin{aligned}(fH \cdot gH) \cdot hH = (fg)H \cdot hH = ((fg)h)H = (f(gh))H \\ = fH \cdot (gh)H = fH \cdot (gH \cdot hH)\end{aligned}$$

$$eH \cdot gH = (eg)H = gH = (ge)H = gH \cdot eH$$

$$gH \cdot g^{-1}H = (gg^{-1})H = eH.$$

Die Homomorphie-Eigenschaft der Projektion ist ebenfalls klar:

$$\pi(gh) = (gh)H = gH \cdot hH = \pi(g) \cdot \pi(h).$$

Es gilt schließlich

$$\ker(\pi) = \{g \in G \mid gH = eH\} = \{g \in G \mid g^{-1}e \in H\} = H. \qquad \square$$

Definition 2.1.17. Für eine normale Untergruppe $H \lhd G$ heißt die Gruppe G/H **Faktorgruppe** oder **Restklassengruppe** von G nach H. $\triangle$

Beispiel 2.1.18. Wir betrachten $\mathbb{Z}$ als Gruppe mit $+$. Für $n \in \mathbb{N}$ ist die Menge $H = n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ eine Untergruppe. Da $\mathbb{Z}$ abelsch ist, ist H eine normale Untergruppe, also ist

$$\mathbb{Z}/n\mathbb{Z}$$

wie oben eine Gruppe. Für die Nebenklasse $m + n\mathbb{Z}$ schreiben wir auch einfach $\overline{m}$. Für $a, b \in \mathbb{Z}$ schreiben wir auch

$$a \equiv b \bmod n$$

falls $\overline{a} = \overline{b}$ in $\mathbb{Z}/n\mathbb{Z}$ gilt (Sprechweise: a kongruent b modulo n). Dies ist äquivalent zu $n \mid (a - b)$ in $\mathbb{Z}$. Es gilt zum Beispiel in $\mathbb{Z}/3\mathbb{Z}$

$$\overline{2} + \overline{1} = \overline{2+1} = \overline{3} = \overline{0}.$$

Man überlegt sich leicht, dass diese Definition von $\mathbb{Z}/n\mathbb{Z}$ wirklich genau mit der bereits bekannten übereinstimmt. $\triangle$

Wir beenden diesen Abschnitt mit einem vielleicht zunächst überraschenden Satz:

Satz 2.1.19. *Jede Gruppe G mit $\#G = n$ ist isomorph zu einer Untergruppe von S_n.*

Beweis. Für $g \in G$ ist die Abbildung

$$\begin{aligned} m_g \colon G &\to G \\ h &\mapsto gh \end{aligned}$$

bijektiv und es gilt

$$m_{fg} = m_f \circ m_g, \quad m_g^{-1} = m_{g^{-1}}.$$

Weiter ist

$$m_g = \mathrm{id} \Leftrightarrow g = e.$$

Also ist die Abbildung

$$\begin{aligned} G &\to S(G) \\ g &\mapsto m_g \end{aligned}$$

ein injektiver Gruppenhomomorphismus und damit G isomorph zu seinem Bild, einer Untergruppe von $S(G) \cong S_n$. □

2.2 Homomorphie- und Isomorphiesätze

Für das Studium von Gruppen und Homomorphismen ist der Homomorphiesatz ein wichtiges Werkzeug. Er drückt die universelle Eigenschaft der Faktorkonstruktion aus und wird im Folgenden oft verwendet.

Satz 2.2.1 (Homomorphiesatz)**.** *Für einen Gruppenhomomorphismus*

$$\varphi \colon G \to H$$

ist der folgende Homomorphismus wohldefiniert und injektiv:

$$\begin{aligned} \overline{\varphi} \colon G/\ker(\varphi) &\to H \\ g\ker(\varphi) &\mapsto \varphi(g). \end{aligned}$$

Insbesondere gilt $G/\ker(\varphi) \cong \mathrm{im}(\varphi)$.

Beweis. Setze $N = \ker(\varphi)$. Für die Wohldefiniertheit sei $g_1 N = g_2 N$, also $g_1^{-1} g_2 \in N$, also

$$e_H = \varphi(g_1^{-1} g_2) = \varphi(g_1)^{-1} \varphi(g_2),$$

also $\varphi(g_1) = \varphi(g_2)$. Für die Injektivität reicht es, $\ker(\overline{\varphi}) = \{e\}$ zu zeigen. Aus $e = \overline{\varphi}(gN) = \varphi(g)$ folgt aber $g \in \ker(\varphi) = N$, also $gN = eN$ in G/N. Aus $\mathrm{im}(\varphi) = \mathrm{im}(\overline{\varphi})$ folgt die besagte Isomorphie. □

Als erste Anwendung erhalten wir eine Klassifizierung von sogenannten zyklischen Gruppen.

Definition 2.2.2. (i) Sei G eine Gruppe und $A \subseteq G$. Dann bezeichnet $\langle A \rangle$ die kleinste Untergruppe von G, die A enthält. Offensichtlich gilt

$$\langle A \rangle = \bigcap_{A \subseteq H < G} H = \left\{ a_1 a_2 \cdots a_r \mid r \in \mathbb{N}, a_i \in A \text{ oder } a_i^{-1} \in A \right\}.$$

(ii) Sei $g \in G$. Dann heißt $\langle g \rangle$ eine **zyklische Gruppe**. △

Korollar 2.2.3. *Jede zyklische Gruppe ist isomorph zu $\mathbb{Z}$ oder zu $\mathbb{Z}/n\mathbb{Z}$ für ein $n \in \mathbb{Z}$. Insbesondere ist jede zyklische Gruppe abelsch.*

Beweis. Wir betrachten die folgende Abbildung, die offensichtlich ein Homomorphismus ist:

$$\begin{aligned} \varphi \colon \mathbb{Z} &\to G \\ z &\mapsto g^z. \end{aligned}$$

Es gilt $\mathrm{im}(\varphi) = \langle g \rangle$ und nach Lemma 2.1.5 gilt $\ker(\varphi) = n\mathbb{Z}$ für ein $n \in \mathbb{Z}$, also folgt die Aussage aus dem Homomorphiesatz. □

Korollar 2.2.4. *Jede Gruppe G mit $\#G = p$ prim ist zyklisch und damit abelsch.*

Beweis. Für $e \neq g \in G$ ist $1 < \#\langle g \rangle$ ein Teiler von $|G| = p$ nach Satz 2.1.13. Also gilt $G = \langle g \rangle$. □

Auch die Isomorphiesätze sind immer wieder nützlich.

Satz 2.2.5 (1. Isomorphiesatz)**.** *Seien $H < G$ und $N \lhd G$. Für*

$$HN := \{hn \mid h \in H, n \in N\}$$

gilt dann:

(i) $HN < G$,

(ii) $(H \cap N) \lhd H$ *und* $N \lhd HN$,

(iii) $H/(H \cap N) \cong HN/N$.

Beweis. (*i*) HN ist offensichtlich nicht leer und für $h_1, h_2 \in H, n_1, n_2 \in N$ gilt $h_1 n_1 h_2 n_2 = h_1 h_2 \tilde{n}_1 n_2$ für ein $\tilde{n}_1 \in N$ aufgrund der Normalität. Also $h_1 n_1 h_2 n_2 \in HN$. Analog ist

$$(h_1 n_1)^{-1} = \underbrace{n_1^{-1}}_{\in N} h_1^{-1} = \underbrace{\overset{-1}{h_1}}_{\in H} n$$

für ein $n \in N$. Damit ist HN eine Untergruppe von G.
(*ii*) $H \cap N$ ist offensichtlich eine Untergruppe von H. Für $n \in H \cap N$ und $h \in H$ gilt $h^{-1}nh \in N$ aufgrund der Normalität von N und $h^{-1}nh \in H$ aufgrund der Untergruppeneigenschaft von H. Damit ist $(H \cap N) \lhd H$. Wegen $e \in H$ gilt $N \subseteq HN$ und offensichtlich ist es dann eine normale Untergruppe.
Für (*iii*) verwenden wir den Homomorphiesatz. Zunächst gibt es einen Homomorphismus

$$\begin{aligned} \varphi\colon H &\to HN/N \\ h &\mapsto hN. \end{aligned}$$

Er ist offensichtlich surjektiv, denn für $h \in H, n \in N$ gilt $hnN = hN$. Nun gilt

$$\ker(\varphi) = \{h \in H \mid hN = eN\} = \{h \in H \mid h \in N\} = H \cap N.$$

Die Isomorphie folgt also aus der Aussage des Homomorphiesatzes. □

Satz 2.2.6 (2. Isomorphiesatz)**.** *Seien* $H, N \lhd G$ *und* $H < N$. *Dann ist* $N/H \lhd G/H$ *und*

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

Beweis. Aufgabe 11. □

2.3 Gruppenoperationen

Definition 2.3.1. (*i*) Sei G eine Gruppe und X eine Menge. Eine Abbildung

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto g \cdot x \end{aligned}$$

heißt **Gruppenoperation** von G auf X, falls gilt:

(a) $\forall x \in X \quad e \cdot x = x$,

(b) $\forall g, h \in G, x \in X \quad g \cdot (h \cdot x) = (gh) \cdot x$.

(ii) Für eine Gruppenoperation $G \times X \to X$ und $x \in X$ heißt

$$Gx := \{g \cdot x \mid g \in G\}$$

die **Bahn** von x und

$$\mathrm{Stab}(x) := G_x := \{g \in G \mid g \cdot x = x\}$$

der **Stabilisator** von x. △

Bemerkung/Beispiel 2.3.2. (i) Die Gruppe $G = \mathrm{GL}_n(K)$ operiert auf $X = K^n$ durch Matrixmultiplikation:

$$\begin{aligned} \mathrm{GL}_n(K) \times K^n &\to K^n \\ (A, v) &\mapsto Av. \end{aligned}$$

Dabei gibt es zwei Möglichkeiten für die Bahnen. Für $v = 0$ gilt $Gv = \{0\}$, für $v \neq 0$ gilt $Gv = K^n \setminus \{0\}$. Der Stabilisator $\mathrm{Stab}(v)$ besteht aus denjenigen Matrizen, für die v ein Eigenvektor zum Eigenwert 1 ist. Zum Beispiel gilt $\mathrm{Stab}(0) = \mathrm{GL}_n(K)$.
(ii) Die Gruppe $\mathrm{O}_n(\mathbb{R})$ der orthogonalen Matrizen operiert wie in (i) auf $\mathbb{R}^n$. Die Bahnen sind dabei gerade die Sphären um den Ursprung.
(iii) Die Gruppenverknüpfung einer Gruppe G ist eine Operation von G auf sich selbst:

$$\begin{aligned} G \times G &\to G \\ (g, h) &\mapsto gh. \end{aligned}$$

Wegen der Existenz von Inversen gilt $Gh = G$ und $\mathrm{Stab}(h) = \{e\}$ für alle $h \in G$.
(iv) G operiert auf sich selbst aber zum Beispiel auch durch **Konjugation**:

$$\begin{aligned} G \times G &\to G \\ (g, h) &\mapsto ghg^{-1}. \end{aligned}$$

Für $h \in G$ ist dann $\mathrm{Stab}(h) = \{g \in G \mid gh = hg\}$ die Menge aller Elemente, die mit h kommutieren. Die Bahn $Gh = \{ghg^{-1} \mid g \in G\}$ nennt man auch die **Konjugationsklasse** von h in G.

(v) Sei $H < G$ eine Untergruppe. Dann operiert G auf der Menge G/H der Linksnebenklassen durch

$$\begin{aligned} G \times G/H &\to G/H \\ (g, fH) &\mapsto (gf)H. \end{aligned}$$

Um die Wohldefiniertheit nachzuweisen, benötigt man hier nicht die Normalität!
(vi) Für eine Gruppenoperation $G \times X \to X$ liefert jedes $g \in G$ eine Abbildung

$$\begin{aligned} m_g \colon X &\to X \\ x &\mapsto g \cdot x. \end{aligned}$$

Dabei gilt aufgrund der Axiome $m_e = \mathrm{id}_X$ und $m_{gh} = m_g \circ m_h$. Insbesondere gilt $m_{g^{-1}} = (m_g)^{-1}$ und alle m_g sind bijektiv, also $m_g \in S(X)$. Man kann eine Gruppenoperation von G auf X also wahlweise auch einfach definieren als einen Gruppenhomomorphismus $G \to S(X)$. △

Lemma 2.3.3. *Sei $G \times X \to X$ eine Gruppenoperation. Dann gilt:*

(i) Bahnen sind entweder disjunkt oder identisch, liefern also eine disjunkte Zerlegung von X.

(ii) Für jedes $x \in X$ ist $\mathrm{Stab}(x)$ eine Untergruppe von G.

Beweis. (*i*): $Gx \cap Gy \neq \emptyset$ bedeutet $g_1 x = g_2 y$ für gewisse $g_1, g_2 \in G$. Daraus folgt

$$x = ex = (g_1^{-1} g_1)x = g_1^{-1}(g_1 x) = g_1^{-1}(g_2 y) = (g_1^{-1} g_2)y \in Gy$$

und damit offensichtlich $Gx \subseteq Gy$. Die andere Inklusion folgt analog.
(ii): $e \in \mathrm{Stab}(x)$ folgt aus der Definition von Gruppenoperation, also $\mathrm{Stab}(x) \neq \emptyset$. Für $g, h \in \mathrm{Stab}(x)$ gilt

$$(gh)x = g(hx) = gx = x$$

$$g^{-1}x = g^{-1}(gx) = (g^{-1}g)x = ex = x,$$

also $gh, g^{-1} \in \mathrm{Stab}(x)$. □

Definition 2.3.4. (i) Eine Gruppenoperation heißt **transitiv**, falls es nur eine Bahn gibt, also $Gx = X$ für alle $x \in X$ gilt.
(ii) Eine Teilmenge $V \subseteq X$ heißt **vollständiges Vertretersystem der Bahnen**, falls für jede Bahn Gx gilt

$$\#(Gx \cap V) = 1.$$ △

Satz 2.3.5 (Bahnengleichung). *Sei X eine endliche Menge, $G \times X \to X$ eine Gruppenoperation und $V \subseteq X$ ein vollständiges Vertretersystem der Bahnen. Dann gilt*

$$\#X = \sum_{v \in V} |G : \mathrm{Stab}(v)|.$$

Beweis. Für $x \in X$ betrachte die Abbildung

$$\begin{aligned} \pi \colon G &\to Gx \\ g &\mapsto gx. \end{aligned}$$

Dann gilt

$$\begin{aligned} \pi(g_1) = \pi(g_2) &\Leftrightarrow g_1 x = g_2 x \\ &\Leftrightarrow g_2^{-1} g_1 x = x \\ &\Leftrightarrow g_2^{-1} g_1 \in \mathrm{Stab}(x) \\ &\Leftrightarrow g_1 \mathrm{Stab}(x) = g_2 \mathrm{Stab}(x). \end{aligned}$$

Also induziert π eine bijektive Abbildung zwischen $G/\mathrm{Stab}(x)$ und Gx und es gilt $|G : \mathrm{Stab}(x)| = \#Gx$. Da die Bahnen X disjunkt zerlegen, folgt daraus die Aussage. □

Beispiel 2.3.6. Wir betrachten die offensichtlich transitive Operation

$$\begin{aligned} S_n \times \{1, \ldots, n\} &\to \{1, \ldots, n\} \\ (\sigma, i) &\mapsto \sigma(i). \end{aligned}$$

Für jedes $i \in \{1, \ldots, n\}$ gilt also

$$n = \#\{1, \ldots, n\} = |S_n : \mathrm{Stab}(i)| = \frac{\#S_n}{\#\mathrm{Stab}(i)} = \frac{n!}{\#\mathrm{Stab}(i)},$$

also $\#\mathrm{Stab}(i) = (n-1)!$ △

Definition 2.3.7. (*i*) Für eine Gruppe G nennt man

$$Z(G) := \{g \in G \mid \forall h \in G \; gh = hg\}$$

das **Zentrum** von G.
(*ii*) Für $h \in G$ heißt

$$C_G(h) = \{g \in G \mid gh = hg\}$$

der **Zentralisator** von h in G. △

Lemma 2.3.8. *Es gilt $Z(G) \lhd G$ und $C_G(h) < G$ für alle $h \in G$.*

Beweis. Aufgabe 13. □

Korollar 2.3.9 (Klassengleichung)**.** *Sei G eine endliche Gruppe und V ein Vertretersystem aller Konjugationsklassen in G mit mindestens 2 Elementen. Dann gilt*

$$\#G = \#Z(G) + \sum_{v \in V} |G : C_G(v)|.$$

Beweis. Die Aussage ist eine direkte Anwendung der Bahnengleichung auf die Operation von G auf sich selbst durch Konjugation (siehe Beispiel 2.3.2 (iii)). Man beachte dabei nur, dass $\mathrm{Stab}(v) = C_G(v)$ gilt, die Bahn Gv gerade die Konjugationsklasse von v ist und die Konjugationsklasse eines Elementes genau dann nur ein Element hat, wenn das Element im Zentrum liegt. □

Korollar 2.3.10. *Sei p eine Primzahl und G eine Gruppe mit $\#G = p^r > 1$. Dann gilt $Z(G) \neq \{e\}$.*

Beweis. In der Klassengleichung ist p ein Teiler der linken Seite und ebenfalls ein Teiler von $|G : C_G(v)|$ für $v \in V$, da dann $C_G(v) \neq G$. Also ist p ein Teiler von $\#Z(G)$ und insbesondere $\#Z(G) > 1$. □

2.4 Existenz von Untergruppen und Sylow-Sätze

Wir wollen uns nun mit der Frage beschäftigen, was für Untergruppen man in einer gegebenen Gruppe wirklich finden kann. Das ermöglicht uns später in Kombination mit der Galoistheorie starke Ergebnisse.

Definition 2.4.1. Sei G eine Gruppe. Die **Ordnung** $\mathrm{ord}(g)$ eines Elements $g \in G$ ist die Mächtigkeit der Untergruppe $\langle g \rangle$. △

Lemma 2.4.2. *Sei G eine Gruppe und $g \in G$.*
(i) Es gilt $g^z = e$ für $z \in \mathbb{Z}$ genau dann, wenn $\mathrm{ord}(g) \mid z$. Insbesondere ist die Ordnung von g die kleinste positive Zahl n mit $g^n = e$.
(ii) Falls $g^p = e$ für eine Primzahl p gilt, folgt $g = e$ oder $\mathrm{ord}(g) = p$.

Beweis. Wie in Korollar 2.2.3 betrachten wir den Homomorphismus

$$\varphi \colon \mathbb{Z} \to \langle g \rangle; \quad z \mapsto g^z.$$

Dann gilt $\ker(\varphi) = n\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z} \cong \langle g \rangle$, woraus $n = \operatorname{ord}(g)$ folgt. Wegen

$$g^z = e \;\Leftrightarrow\; z \in \ker(\varphi) \;\Leftrightarrow\; n \mid z$$

ist Aussage (i) klar und (ii) folgt direkt daraus. □

Das nächste Ergebnis ist unter anderem die Grundlage für einen ersten einfachen Primzahltest und wird auch in der Kryptographie verwendet.

Korollar 2.4.3 (Kleiner Satz von Fermat)**.** *Sei p eine Primzahl und $a \in \mathbb{N}$ mit $1 \leq a < p$. Dann gilt*

$$p \mid a^{p-1} - 1.$$

Beweis. Die Menge $\mathbb{Z}/p\mathbb{Z}$ ist mit $+$ und $\cdot$ sogar ein Körper. Dazu benötigt man dass p eine Primzahl ist (Aufgabe 16). Insbesondere ist

$$G = (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$$

eine Gruppe bezüglich $\cdot$, die genau $p-1$ Elemente hat. Wegen $\overline{a} \in G$ gilt nach Satz 2.1.13 $\operatorname{ord}(\overline{a}) \mid p-1$, also $n \cdot \operatorname{ord}(\overline{a}) = p-1$, also

$$\overline{a^{p-1}} = \overline{a}^{p-1} = \left(\overline{a}^{\operatorname{ord}(\overline{a})}\right)^n = \overline{1}^n = \overline{1}.$$

Das bedeutet aber in $\mathbb{Z}$ gerade $p \mid a^{p-1} - 1$. □

Nach Satz 2.1.13 gilt $\operatorname{ord}(g) \mid \#G$ für alle $g \in G$. Eine erste teilweise Umkehrung dieser Aussage ist der folgende Satz.

Proposition 2.4.4 (Lemma von Cauchy)**.** *Sei G eine endliche Gruppe und p eine Primzahl mit $p \mid \#G$. Dann gibt es in G ein Element g mit $\operatorname{ord}(g) = p$.*

Beweis. Wir betrachten die Menge

$$X = \{(g_1, \ldots, g_p) \in G^p \mid g_1 \cdots g_p = e\},$$

und sehen dass $\#X = (\#G)^{p-1}$ gelten muss. Man kann nämlich die ersten $p-1$ Einträge eines Tupels beliebig vorgeben, der letzte Eintrag ist dann eindeutig bestimmt. Inbesondere gilt $p \mid \#X$.
Nun betrachten wir die folgende (wohldefinierte!) Gruppenoperation:

$$\begin{aligned} \mathbb{Z}/p\mathbb{Z} \times X &\to X \\ \left(\overline{i}, (g_1, \ldots, g_p)\right) &\mapsto (g_{i+1}, g_{i+2}, \ldots, g_p, g_1, g_2, \ldots, g_i). \end{aligned}$$

Die Mächtigkeit jeder Bahn ist ein Teiler von $\#\mathbb{Z}/p\mathbb{Z} = p$, wie wir im Beweis der Bahnengleichung gesehen haben. Damit hat jede Bahn entweder 1 oder p Elemente. Es gibt aber Bahnen mit einem Element, zum Beispiel die Bahn von $(e, \dots, e) \in X$. Weil die Bahnen X disjunkt zerlegen und weil $p \mid \#X$ gilt, muss die Anzahl der einelementigen Bahnen deshalb ebenfalls durch p teilbar sein. Insbesondere ist sie echt größer als 1. Also gibt es ein $e \neq g \in G$ mit $(g, \dots, g) \in X$, also $g^p = e$. Mit Lemma 2.4.2 (ii) folgt die Aussage. □

Für abelsche Gruppen erhalten wir eine komplette Umkehrung des Satzes von Lagrange:

Satz 2.4.5. *Sei G eine endliche abelsche Gruppe. Dann gibt es für jeden Teiler n von $\#G$ eine Untergruppe H von G mit $\#H = n$.*

Beweis. Wir beweisen die Aussage per Induktion über $\#G$. Für $\#G = 1$ ist nichts zu zeigen. Sei also $\#G > 1$. Für $n = 1$ ist die Aussage ebenfalls klar. Sei also $n > 1$ und p eine Primzahl mit $p \mid n$. Wegen $p \mid \#G$ gibt es nach dem Lemma von Cauchy eine Untergruppe U von G mit $\#U = p$. Da G abelsch ist, ist U eine normale Untergruppe und damit G/U wieder eine Gruppe und wegen

$$\#(G/U) = \frac{\#G}{p} < \#G$$

finden wir nach Induktionsannahme eine Untergruppe $\tilde{H} < G/U$ mit

$$\#\tilde{H} = \frac{n}{p}.$$

Sei $\pi\colon G \to G/U$ die kanonische Projektion. Dann ist

$$H := \pi^{-1}(\tilde{H})$$

aber eine Untergruppe von G mit Mächtigkeit n wie gewünscht. Die Untergruppeneigenschaft ist dabei klar. Für die Mächtigkeit betrachten wir die surjektive Einschränkung $\tilde{\pi}\colon H \to \tilde{H}$. Wegen $\ker(\pi) \subseteq H$ gilt

$$U = \ker(\pi) = \ker(\tilde{\pi}),$$

also nach dem Homomorphiesatz $H/U \cong \tilde{H}$. Für die Mächtigkeiten bedeutet das

$$\frac{n}{p} = \#\tilde{H} = \#(H/U) = \frac{\#H}{\#U} = \frac{\#H}{p},$$

also $\#H = n$. □

Eine ebenfalls vollständige Umkehrung des Satzes von Lagrange erhalten wir für Gruppen mit Primzahlpotenz-Mächtigkeit:

Proposition 2.4.6. *Sei p eine Primzahl und G eine Gruppe mit $\#G = p^r$. Dann gibt es für jedes $0 \leq k \leq r$ eine Untergruppe H von G mit $\#H = p^k$.*

Beweis. Wir beweisen die Aussage per Induktion über r. Für $r = 1$ ist nichts zu zeigen, sei also $r > 1$. Sei ebenfalls $k > 0$. Nach Korollar 2.3.10 gilt $Z(G) \neq \{e\}$, also $p \mid \#Z(G)$ nach Satz 2.1.13 und deshalb gibt es nach dem Lemma von Cauchy ein $g \in Z(G)$ mit $\mathrm{ord}(g) = p$. Weil g im Zentrum liegt, ist $U = \langle g \rangle$ eine normale Untergruppe von G und wir betrachten den kanonischen Gruppenhomomorphismus

$$\pi \colon G \to G/U.$$

Es gilt $\#(G/U) = p^{r-1}$ und nach Induktionsvoraussetzung gibt es eine Untergruppe $\tilde{H} < G/U$ mit $\#\tilde{H} = p^{k-1}$. Mit dem selben Argument wie im letzten Beweis ist dann

$$H := \pi^{-1}(\tilde{H})$$

eine Untergruppe von G mit Mächtigkeit p^k. □

Für allgemeine Gruppen gibt es keine vollständige Umkehrung des Satzes von Lagrange, nur eine teilweise:

Satz 2.4.7 (1. Sylowsatz)**.** *Sei G eine endliche Gruppe mit $\#G = p^r m$, wobei p eine Primzahl mit $p \nmid m$ sei. Dann gibt es für jedes $0 \leq k \leq r$ eine Untergruppe H von G mit $\#H = p^k$.*

Beweis. Zunächst zeigen wir die Existenz einer Untergruppe mit p^r Elementen. Dazu verwenden wir Induktion über $n = \#G$. Im Fall $n = 1$ ist nichts zu zeigen. Wir nehmen also an, dass die Aussage für alle Gruppen mit Mächtigkeiten $< n$ bereits bewiesen ist.
1. Fall: G besitzt eine echte Untergruppe H mit $p^r \mid \#H$. Dann gibt es nach Induktionsvoraussetzung in H eine Untergruppe der Mächtigkeit p^r und das ist auch eine Untergruppe von G.
2. Fall: Für jede echte Untergruppe H von G gilt $p^r \nmid \#H$, also $p \mid |G : H|$. Die Klassengleichung besagt

$$\#G = \#Z(G) + \sum_{v \in V} |G : C_G(v)|,$$

wobei alle in der Summe auftretenden $C_G(v)$ echte Untergruppen von G sind. Daraus folgt $p \mid \#Z(G)$ und nach dem Lemma von Cauchy gibt es ein $g \in Z(G)$ mit $\mathrm{ord}(g) = p$. Da die Untergruppe $U = \langle g \rangle$ im Zentrum von G enthalten ist, ist sie eine normale Untergruppe von G und wir betrachten den kanonischen Gruppenhomomorphismus

$$\pi \colon G \to G/U.$$

Es gilt $\#(G/U) = p^{r-1}m < n$ und nach Induktionsvoraussetzung gibt es eine Untergruppe $\tilde{H} < G/U$ mit $\#\tilde{H} = p^{r-1}$. Genau wie im letzten Beweis erhalten wir damit die Untergruppe $H = \pi^{-1}(\tilde{H})$ mit $\#H = p^r$. Nach unserer Annahme in diesem 2. Fall muss nun $H = G$ sein und damit sind wir im Fall von Proposition 2.4.6. □

Beispiel 2.4.8. (i) Sei G eine Gruppe mit $\#G = 12 = 2^2 \cdot 3$. Dann gibt es in G Untergruppen mit

$$1, 2, 3, 4, 12$$

Elementen.
(ii) Wir betrachten zunächst allgemein die Gruppe S_n und den Gruppenhomomorphimus

$$\mathrm{sgn} \colon S_n \to \{1, -1\}.$$

Dann ist $A_n := \ker(\mathrm{sgn})$ eine normale Untergruppe in S_n, genannt die **alternierende Gruppe**. A_n besteht also gerade aus den Permutationen, die ein Produkt einer geraden Anzahl von Transpositionen sind. Wegen $S_n/A_n \cong \{1, -1\}$ folgt sofort $\#A_n = \#S_n/2 = n!/2$, also zum Beispiel $\#A_4 = 12$. In A_4 gibt es allerdings keine Untergruppe mit Mächtigkeit 6 (Aufgabe 18). △

Definition 2.4.9. Sei p eine Primzahl mit $\#G = p^r m$ und $p \nmid m$.
(i) $H < G$ heißt p-**Untergruppe** von G, falls $\#H = p^k$ für ein $0 \leq k \leq r$ gilt.
(ii) $H < G$ heißt p-**Sylow-Untergruppe**, falls $\#H = p^r$ gilt. △

Satz 2.4.10 (2. Sylowsatz). *Sei G eine endliche Gruppe mit $\#G = p^r m$, wobei p eine Primzahl mit $p \nmid m$ sei. Seien H eine p-Untergruppe und S eine p-Sylow-Untergruppe von G. Dann gibt es ein $g \in G$ mit*

$$H \subseteq gSg^{-1}.$$

Insbesondere ist jede p-Untergruppe in einer p-Sylow-Untergruppe enthalten und je zwei p-Sylow-Untergruppen sind zueinander konjugiert.

Beweis. Sei S_p die Menge aller p-Sylow-Untergruppen von G. Offensichtlich operiert G auf S_p durch Konjugation:

$$\begin{aligned} G \times S_p &\to S_p \\ (g, U) &\mapsto gUg^{-1}. \end{aligned}$$

Sei $\Omega \subseteq S_p$ die Bahn von S unter dieser Operation, also

$$\Omega = \left\{ gSg^{-1} \mid g \in G \right\}.$$

Offensichtlich gilt $S < \mathrm{Stab}(S) < G$, also $p^r = \#S \mid \#\mathrm{Stab}(S)$ und damit ist p kein Teiler von

$$\#\Omega = |G : \mathrm{Stab}(S)| = \frac{\#G}{\#\mathrm{Stab}(S)}.$$

Die Untergruppe H operiert genau wie G durch Konjugation auf Ω (nur im Gegensatz zu G nicht unbedingt transitiv). Dabei sind die Bahnenlängen Potenzen von p oder 1, denn das sind die einzigen Teiler von $\#H$. Da die Bahnen Ω dabei disjunkt zerlegen und p kein Teiler von $\#\Omega$ ist, muss mindestens eine Bahn der Länge 1 auftreten. Es gibt also $S' = gSg^{-1} \in \Omega$ mit

$$hS'h^{-1} = S' \text{ für alle } h \in H.$$

Wie im Beweis des ersten Isomorphiesatzes zeigt man damit leicht, dass HS' eine Untergruppe von G ist, $S' \lhd HS'$ und $H \cap S' \lhd H$ gilt sowie

$$H/(H \cap S') \cong HS'/S'.$$

Die Mächtigkeit der linken Seite sowie die von S' ist aber jeweils eine Potenz von p und damit ist auch $\#(HS')$ eine p-Potenz. Da S' eine p-Sylow-Untergruppe in G ist, folgt aus $S' \subseteq HS'$ dann schon $S' = HS'$. Das impliziert $H \subseteq S'$, die gewünschte Aussage. □

Satz 2.4.11 (3. Sylowsatz)**.** *Sei G eine endliche Gruppe mit $\#G = p^r m$, wobei p eine Primzahl mit $p \nmid m$ sei. Sei s die Anzahl der p-Sylow-Untergruppen von G. Dann gilt*

$$s \mid m \text{ und } s \equiv 1 \bmod p.$$

Beweis. Wie im letzten Beweis betrachten wir die Menge S_p aller p-Sylow-Untergruppen und die Operation

$$\begin{aligned} G \times S_p &\to S_p \\ (g, U) &\mapsto gUg^{-1}. \end{aligned}$$

Da je zwei p-Sylow-Untergruppen zueinander konjugiert sind, ist die Operation transitiv, d.h. mit beliebigem $S \in S_p$ und der Notation des letzten Beweises gilt $\Omega = S_p$. Dort wurde aber gezeigt, dass p kein Teiler von

$$\#\Omega = |G : \mathrm{Stab}(S)| = \frac{\#G}{\#\mathrm{Stab}(S)}$$

ist, also $s = \#\Omega \mid m$. Lässt man nun S anstatt G auf S_p operieren, so gibt es wieder ein $S' \in S_p$ mit Bahnenlänge 1 und dafür gilt $S \subseteq S'$, wie im letzten Beweis gezeigt. Das impliziert aber $S = S'$, also gibt es genau eine Bahn mit Bahnenlänge 1, alle anderen Bahnenlängen sind Vielfache von p. Daraus folgt

$$s = \#\Omega \equiv 1 \bmod p. \qquad \square$$

Korollar 2.4.12. *Bis auf Isomorphie gibt es nur eine Gruppe mit* 15 *Elementen, nämlich die zyklische Gruppe* $\mathbb{Z}/15\mathbb{Z}$.

Beweis. Sei G eine Gruppe mit $\#G = 15 = 3 \cdot 5$. Sei s_3 die Anzahl der 3-Sylow-Untergruppen und s_5 die Anzahl der 5-Sylow-Untergruppen von G. Es gilt $s_3 \mid 5$ und $s_3 \equiv 1 \bmod 3$ und daraus folgt $s_3 = 1$. Analog folgt $s_5 = 1$. Die (einzige) 3-Sylow-Untergruppe S_3 und die (einzige) 5-Sylow-Untergruppe S_5 müssen dann aber normale Untergruppen in G sein. Außerdem gilt $S_3 \cap S_5 = \{e\}$, weil die Ordnung eines Elements im Durchschnitt ein Teiler von 3 und von 5 sein muss. Für $g \in S_3, h \in S_5$ gilt dann

$$ghg^{-1}h^{-1} \in S_3 \cap S_5,$$

aufgrund der Normalität, also $ghg^{-1}h^{-1} = e$, also $gh = hg$. Die Elemente von S_3 und S_5 kommutieren also miteinander. Damit ist die folgende Abbildung ein Homomorphismus:

$$\begin{aligned} S_3 \times S_5 &\to G \\ (g, h) &\mapsto gh. \end{aligned}$$

Wegen $S_3 \cap S_5 = \{e\}$ ist er injektiv. Da beide Gruppen aber 15 Elemente haben, ist er surjektiv und damit ein Isomorphismus.
Es gilt aber $S_3 \cong \mathbb{Z}/3\mathbb{Z}$ und $S_5 \cong \mathbb{Z}/5\mathbb{Z}$ nach Korollar 2.2.4 und Korollar 2.2.3. Damit ist G isomorph zu $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ und diese Gruppe ist wiederum isomorph zu $\mathbb{Z}/15\mathbb{Z}$ (Aufgabe 19). $\square$

2.5 Auflösbare Gruppen

Der Begriff einer auflösbaren Gruppe ist zunächst sehr abstrakt. Er wird aber gebraucht, um später die Existenz von Lösungsformeln für polynomiale Gleichungen zu untersuchen. Sei G stets eine Gruppe.

Definition 2.5.1. (i) Für $g, h \in G$ heißt $[g,h] := ghg^{-1}h^{-1}$ der **Kommutator** von g und h.
(ii) Die von allen Kommutatoren erzeugte Untergruppe von G heißt **Kommutator-Untergruppe** und wird mit $K(G)$ bezeichnet. △

Lemma 2.5.2. *(i) Es gilt $[g,h]^{-1} = [h,g]$. Inbesondere besteht die Kommutator-Untergruppe aus allen endlichen Produkten von Kommutatoren, d.h.*

$$K(G) = \{[g_1,h_1]\cdots[g_n,h_n] \mid n \in \mathbb{N}, g_i, h_i \in G\}\,.$$

(ii) $K(G)$ ist eine normale Untergruppe in G.
(iii) Für $N \lhd G$ gilt

$$G/N \text{ abelsch } \Leftrightarrow K(G) \subseteq N.$$

$K(G)$ ist also die kleinste normale Untergruppe mit abelscher Faktorgruppe.

Beweis. (i) ist klar:

$$[g,h]^{-1} = (ghg^{-1}h^{-1})^{-1} = hgh^{-1}g^{-1} = [h,g].$$

Für (ii) rechnet man direkt nach

$$f^{-1}[g_1,h_1][g_2,h_2|\cdots[g_n,h_n]f = \underbrace{[f^{-1}g_1f, f^{-1}h_1f]}_{\in K(G)}\cdots\underbrace{[f^{-1}g_nf, f^{-1}h_nf]}_{\in K(G)}.$$

(iii) G/N ist genau dann abelsch, wenn für alle $g, h \in G$ gilt

$$ghN = gN\cdot hN = hN\cdot gN = hgN,$$

also

$$N \ni (gh)(hg)^{-1} = ghg^{-1}h^{-1} = [g,h],$$

also $K(G) \subseteq N$. □

Lemma 2.5.3. *(i) Für abelsche Gruppen gilt $K(G) = \{e\}$.*
(ii) Für alle $n \geq 1$ gilt $K(S_n) = A_n$.
(iii) Für $n = 1,2,3$ gilt $K(A_n) = \{\mathrm{id}\}$.
(iv) $K(A_4) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ist abelsch.
(v) Für $n \geq 5$ gilt $K(A_n) = A_n$.

Beweis. (i) folgt aus Lemma 2.5.2 (iii) und ist auch direkt klar, da in abelschen Gruppen immer

$$[g,h] = ghg^{-1}h^{-1} = gg^{-1}hh^{-1} = e$$

gilt.
(ii) Für $n = 1$ ist die Aussage klar. Für $n \geq 2$ gilt

$$S_n/A_n \cong \{1,-1\} \cong \mathbb{Z}/2\mathbb{Z}$$

und das ist eine abelsche Gruppe. Damit gilt nach Lemma 2.5.2 (iii)

$$K(S_n) \subseteq A_n.$$

Für $n = 2$ gilt offensichtlich $A_2 = \{\mathrm{id}\}$ und damit Gleichheit. Für $n \geq 3$ ist jedes Element von A_n ein Produkt von 3-Zyklen (Aufgabe 17). Für i,j,k paarweise verschieden gilt aber

$$(ijk) = (ik)(jk)(ik)^{-1}(jk)^{-1} = [(ik),(jk)] \in K(S_n).$$

Daraus folgt $A_n \subseteq K(S_n)$.
(iii) ist klar, da die Gruppen A_n für $n \leq 3$ abelsch sind. (iv) ist Aufgabe 22.
Für (v) reicht es zu zeigen, dass für $n \geq 5$ jeder 3-Zykel in S_n ein Kommutator von 3-Zykeln ist. Seien dazu $i,j,k \in \{1,\ldots,n\}$ paarweise veschieden. Wähle dann zwei weitere unterschiedliche Elemente $l,m \in \{1,\ldots,n\}$ und berechne

$$(ijk) = [(ijl),(ikm)] \in K(A_n). \qquad \square$$

Definition 2.5.4. (i) Eine **Normalreihe** für G ist eine Folge von normalen Untergruppen

$$\{e\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = G.$$

Man beachte dabei, dass jedes G_{i+1} nur eine normale Untergruppe in G_i sein muss, nicht etwa in G. Die Gruppen G_i/G_{i+1} heißen **Faktoren** der Normalreihe.
(ii) G heißt **auflösbar**, wenn G eine Normalreihe mit abelschen Faktoren besitzt. $\triangle$

Wir setzen nun $K^0(G) := G$ und iterativ

$$K^{i+1}(G) := K(K^i(G)).$$

Auf diese Weise erhalten wir eine absteigende Folge von Untergruppen von G, die jeweils normale Untergruppen in der vorhergehenden Gruppe sind, mit abelschen Faktoren.

Satz 2.5.5. *G ist genau dann auflösbar, wenn*

$$K^n(G) = \{e\}$$

für ein $n \in \mathbb{N}$ gilt.

Beweis. Falls $K^n(G) = \{e\}$ gilt, ist

$$\{e\} = K^n(G) \lhd K^{n-1}(G) \lhd \cdots \lhd K^1(G) \lhd K^0(G) = G$$

offensichtlich eine Normalreihe mit abelschen Faktoren, also ist G auflösbar. Sei umgekehrt

$$\{e\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

eine Normalreihe mit abelschen Faktoren. Wir zeigen induktiv

$$K^i(G) \subseteq G_i$$

und daraus folgt dann die Behauptung. Für $i = 0$ ist die Aussage klar. Es gelte nun $K^i(G) \subseteq G_i$ für ein i. Es ist G_i/G_{i+1} abelsch, also $K(G_i) \subseteq G_{i+1}$ nach Lemma 2.5.2 (iii). Somit gilt

$$K^{i+1}(G) = K(K^i(G)) \subseteq K(G_i) \subseteq G_{i+1}. \qquad \square$$

Korollar 2.5.6. *Für $n \leq 4$ ist S_n auflösbar, für $n \geq 5$ nicht.*

Beweis. Folgt aus Satz 2.5.5 und Lemma 2.5.3. $\square$

Satz 2.5.7. *(i) Jede Untergruppe einer auflösbaren Gruppe ist auflösbar.*
(ii) Für $N \lhd G$ gilt

$$G \text{ auflösbar } \Leftrightarrow G/N \text{ und } N \text{ auflösbar.}$$

Beweis. (i) folgt direkt aus Satz 2.5.5, da für $H < G$ offensichtlich $K(H) < K(G)$ gilt. Für (ii) sei zunächst G auflösbar, also $K^n(G) = \{e\}$. Nach (i) ist dann auch N auflösbar. Sei $\pi \colon G \to G/N$ die kanonische (surjektive) Projektion. Dann überlegt man sich leicht

$$K^n(G/N) = \pi\left(K^n(G)\right) = \{e\},$$

also ist auch G/N auflösbar.

Gelte nun umgekehrt $K^n(G/N) = \{e\}$ und $K^m(N) = \{e\}$. Dann gilt wieder

$$\pi\left(K^n(G)\right) = K^n\left(G/N\right) = \{e\},$$

also $K^n(G) \subseteq \ker(\pi) = N$. Daraus folgt

$$K^{n+m}(G) \subseteq K^m(N) = \{e\},$$

also ist G auflösbar. □

Satz 2.5.8. *Sei G eine Gruppe mit $\#G = p^r$, wobei p eine Primzahl sei. Dann ist G auflösbar.*

Beweis. Wir verwenden vollständige Induktion über r, der Fall $r = 0$ ist trivial. Für $r > 1$ hat G nach Korollar 2.3.10 ein nichttriviales Zentrum $Z(G) \lhd G$. Es ist aber $Z(G)$ abelsch und damit auflösbar und $\#(G/Z(G)) = p^k$ für ein $k < r$. Nach Induktionsvoraussetzung ist damit $G/Z(G)$ auflösbar und nach Satz 2.5.7 damit auch G. □

Kapitel 3

Ringe

Eine weitere wichtige Struktur in der Algebra ist der Ring. Im Gegensatz zu einer Gruppe besitzt ein Ring zwei verschiedene Verknüpfungen. Die aus der linearen Algebra bekannten Körper sind Spezialfälle von Ringen.

3.1 Grundlagen

Definition 3.1.1. (i) Ein **Ring** ist eine Menge R zusammen mit zwei Verknüpfungen

$$\begin{aligned} +&\colon R \times R \to R \\ \cdot&\colon R \times R \to R, \end{aligned}$$

genannt Addition und Multiplikation, sodass gilt:

- R ist bezüglich Addition eine abelsche Gruppe (das neutrale Element bezeichnen wir mit 0).
- Die Multiplikation ist assoziativ und besitzt ein neutrales Element 1.
- Addition und Multiplikation erfüllen das Distributivgesetz, d.h. für alle $a, b, c \in R$ gilt

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c), \quad (b + c) \cdot a = (b \cdot a) + (c \cdot a).$$

(ii) Der Ring R heißt **kommutativ**, falls die Multiplikation kommutativ ist.

(*iii*) Ein **Teilring** von R ist eine Teilmenge $S \subseteq R$ mit $0, 1 \in S$, die mit den von R vererbten Verknüpfungen selbst ein Ring ist. Anders formuliert muss S abgeschlossen unter $+$ und $\cdot$ sein und zu jedem Element das additiv Inverse enthalten.
(*iv*) Die Menge

$$R^\times := \{a \in R \mid \exists b \in R \, ab = ba = 1\}$$

heißt Menge der **Einheiten** von R. Sie bildet eine Gruppe bezüglich Multiplikation. Das multiplikativ inverse Element von $a \in R^\times$ ist eindeutig bestimmt, wir bezeichnen es mit a^{-1}.
(*v*) Ein **Ringhomomorphismus** ist eine Abbildung $\varphi\colon R \to S$ zwischen Ringen, die für alle $a, b \in R$ erfüllt:

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

$$\varphi(1_R) = 1_S.$$

Dabei definieren wir Kern und Bild als

$$\ker(\varphi) := \{a \in R \mid \varphi(a) = 0_S\}$$

$$\operatorname{im}(\varphi) := \{\varphi(a) \mid a \in R\}.$$

(*vi*) Ein **Isomorphismus** ist ein bijektiver Ringhomomorphismus. Zwei Ringe sind **isomorph** (in Zeichen $R \cong S$), falls es einen Isomorphismus zwischen ihnen gibt. △

Beispiel 3.1.2. (*i*) Das bekannteste Beispiel eines kommutativen Ringes sind die ganzen Zahlen $\mathbb{Z}$ mit $+$ und $\cdot$. Es ist aber jeder Körper insbesondere auch ein Ring, also zum Beispiel $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Wir erhalten eine Kette von Teilringen

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}.$$

In einem Körper K gilt immer $K^\times = K \setminus \{0\}$. Im Unterschied zu einem Körper müssen in einem Ring aber inverse Elemente bezüglich $\cdot$ nicht immer existieren. Es gilt zum Beispiel $\mathbb{Z}^\times = \{-1, 1\}$.
(*ii*) Der einzige Ringhomomorphismus $\varphi\colon \mathbb{Z} \to \mathbb{Z}$ ist die Identität. Das Gleiche stimmt für Homomorphismen von $\mathbb{Q}$ und $\mathbb{R}$ in sich selbst (Aufgabe 27). Auf $\mathbb{C}$ gibt es außer der Identität aber zum Beispiel noch die komplexe Konjugation.
(*iii*) Die Menge der Polynome

$$K[x] = \left\{c_0 + c_1 x + c_2 x^2 + \cdots + c_d x^d \mid d \in \mathbb{N}, c_i \in K\right\}$$

über einem Körper bildet einen kommutativen Ring mit der bekannten Addition und Multiplikation von Polynomen. Allgemeiner kann K dabei selbst ein beliebiger kommutativer Ring sein. Für jedes $a \in K$ ist die Auswertungsabbildung

$$\begin{aligned} \mathrm{e}_a \colon K[x] &\to K \\ p &\mapsto p(a) \end{aligned}$$

ein Ringhomomorphismus. Für ein Polynom

$$0 \neq p = c_0 + c_1 x + c_2 x^2 + \cdots + c_d x^d \in K[x]$$

mit $c_d \neq 0$ definieren wir den **Grad** von p als $\deg(p) := d$. Dabei heißt c_d auch der **Leitkoeffizient** von p. Wir setzen zusätzlich $\deg(0) := -\infty$.
(*iv*) Für jeden Ring R ist die Menge $\mathrm{Mat}_n(R)$ der $n \times n$-Matrizen mit Einträgen aus R erneut ein Ring, der im Allgemeinen nicht kommutativ ist. Dabei ist die Addition komponentenweise definiert, die Multiplikation ist die bekannte Matrixmultiplikation. Die Nullmatrix ist das neutrale Element bezüglich $+$, die Einheitsmatrix das neutrale Element bezüglich $\cdot$.
(*v*) Sei M eine Menge. Dann bildet die Menge $\mathcal{F}(M, \mathbb{R})$ aller reellwertigen Abbildungen auf M einen kommutativen Ring bezüglich punktweise definierter Addition und Multiplikation:

$$(f + g)(m) := f(m) + g(m)$$

$$(f \cdot g)(m) := f(m) \cdot g(m).$$

Auch hier kann statt $\mathbb{R}$ ein beliebiger Ring R gewählt werden (wobei $\mathcal{F}(M, R)$ dann nicht mehr unbedingt kommutativ ist). Die Auswertungsabbildung in einem festen Punkt $m \in M$ ist ein Ringhomomorphismus:

$$\begin{aligned} \mathrm{e}_m \colon \mathcal{F}(M, R) &\to R \\ f &\mapsto f(m). \end{aligned}$$

Die Menge $\mathcal{C}(M, \mathbb{R})$ aller stetigen Funktionen ist ein Teilring von $\mathcal{F}(M, \mathbb{R})$ (wenn M beispielsweise ein metrischer Raum ist).
(*vi*) Die Menge

$$\mathbb{Z}[i] := \mathbb{Z} + \mathbb{Z}i = \{a + bi \mid a, b \in \mathbb{Z}\}$$

ist ein Teilring von $\mathbb{C}$, genannt der **Ring der ganzen gaußschen Zahlen**.

(vii) Sei G Gruppe und R ein Ring. Dann ist der **Gruppenring** von G über R definiert als Menge aller formalen endlichen Linearkombinationen von Gruppenelementen mit Koeffizienten aus R:

$$RG := \left\{ \sum_{g \in G} c_g g \mid c_g \in R, \text{ nur endlich viele } c_g \neq 0 \right\}.$$

Dabei addiert man Elemente koeffizientenweise, d.h.

$$\sum_g c_g g + \sum_g d_g g := \sum_g (c_g + d_g) g.$$

Die Multiplikation definiert man über die Gruppenverknüpfung von G und das Distributivgesetz:

$$\left(\sum_g c_g g \right) \cdot \left(\sum_g d_g g \right) := \sum_{g,h} \underbrace{c_g d_h}_{\in R} \underbrace{gh}_{\in G} = \sum_g \left(\sum_h c_{gh^{-1}} d_h \right) g.$$

Es gibt dann einen injektiven Ringhomomorphismus

$$\begin{aligned} R &\to RG \\ a &\mapsto ae \end{aligned}$$

und einen injektiven Gruppenhomomorphismus (vorausgesetzt R ist nicht der Nullring)

$$\begin{aligned} G &\to (RG)^\times \\ g &\mapsto 1g. \end{aligned}$$

$(viii)$ Sind R, S Ringe, so ist das kartesische Produkt $R \times S$ mit komponentenweise definierten Verknüpfungen ein Ring. △

Bemerkung 3.1.3. (i) Da R mit $+$ eine abelsche Gruppe ist, gelten alle bereits bewiesenen Aussage dafür. Beispielsweise sind das neutrale Element und die inversen Elemente eindeutig bestimmt und Ringhomomorphismen bilden 0 auf 0 ab. Für die Multiplikation ist das schwieriger, da es keine inversen Elemente geben muss. Das neutrale Element 1 ist aber trotzdem eindeutig bestimmt. Für Homomorphismen fordern wir, dass 1 auf 1 abgebildet wird.

(ii) In Ringen gelten einige einfache Rechenregeln, wie zum Beispiel

$$0 \cdot a = 0$$

oder

$$-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$$

für alle $a, b \in R$.
(iii) Um die Anzahl von Klammern zu verringern, vereinbaren wir, dass Multiplikation stärker bindet als Addition.Wir schreiben also

$$a \cdot b + c \cdot d$$

anstelle von

$$(a \cdot b) + (c \cdot d).$$

Wiederum lassen wir $\cdot$ oft einfach weg, schreiben also ab anstelle von $a \cdot b$.
(iv) Die Umkehrabbildung eines Isomorphismus ist automatisch wieder ein Ringhomomorphismus.
(v) Ein Ringhomomorphismus φ ist genau dann injektiv, wenn $\ker(\varphi) = \{0\}$ gilt. Das folgt direkt aus Lemma 2.1.11, da jeder Ringhomomorphismus insbesondere ein Gruppenhomomorphismus der additiven Gruppen ist.
(vi) Das Bild $\mathrm{im}(\varphi)$ eines Ringhomomorphismus $\varphi\colon R \to S$ ist ein Teilring von S.
(vii) Die meisten der von uns betrachteten Ringe sind kommutativ. △

Ideale spielen in einem Ring in etwa die Rolle von normalen Untergruppen in Gruppen. Insbesondere kann man mit Idealen wieder eine Faktorkonstruktion durchführen.

Definition 3.1.4. Ein **Ideal** ist eine nicht-leere Teilmenge $I \subseteq R$, welche die beiden folgenden Bedingungen erfüllt:

- $a, b \in I \Rightarrow a + b \in I$
- $a \in I, b \in R \Rightarrow a \cdot b \in I$ und $b \cdot a \in I$.

Wir verwenden dafür die Notation $I \lhd R$. △

Bemerkung/Beispiel 3.1.5. (i) Jeder Ring R besitzt die beiden trivialen Ideale $\{0\}, R$.
(ii) Ein Ideal $I \lhd R$ ist im Regelfall *kein* Teilring von R. Es gilt nämlich

$$1 \in I \Leftrightarrow I = R.$$

Das folgt unmittelbar aus der zweiten Bedingung in der Definition von Idealen. Noch etwas allgemeiner kann ein echtes Ideal $I \lneq R$ niemals ein Element enthalten, das invertierbar bezüglich der Multiplikation ist. Insbesondere gibt es in Körpern nur die beiden trivialen Ideale $\{0\}, K$.
(iii) Ein Ideal ist insbesondere eine Untergruppe der additiven Gruppe des Rings. Für $a \in I$ gilt nämlich

$$-a = (-1) \cdot a \in I$$

wegen der zweiten Bedingung der Idealdefinition. Da die Addition kommutativ ist, ist es automatisch eine normale Untergruppe. Insbesondere ist R/I eine abelsche Gruppe bezüglich der im letzten Kapitel definierten Addition:

$$(a + I) + (b + I) := (a + b) + I.$$

Es gilt $a + I = b + I \Leftrightarrow a - b \in I$. Wir sagen dazu auch, dass a **kongruent** b **modulo** I ist.
(iv) Für $n \in \mathbb{Z}$ ist $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ ein Ideal in $\mathbb{Z}$. Wegen (iii) und Lemma 2.1.5 ist jedes Ideal in $\mathbb{Z}$ von dieser Gestalt.
(v) Der Kern $\ker(\varphi)$ eines Ringhomomorphismus $\varphi\colon R \to S$ ist ein Ideal in R. Beispielsweise ist die Menge

$$I_m := \{f \in \mathcal{F}(M, R) \mid f(m) = 0\}$$

für jedes $m \in M$ ein Ideal im Ring $\mathcal{F}(M, \mathbb{R})$. Allgemeiner ist das Urbild $\varphi^{-1}(J)$ eines Ideals $J \lhd S$ ein Ideal in R.
(vi) Das Bild $\varphi(I)$ eines Ideals $I \lhd R$ unter einem Homomorphismus $\varphi\colon R \to S$ ist im Allgemeinen kein Ideal in S. Ist φ hingegen surjektiv, stimmt die Aussage.
(vii) Jeder Ringhomomorphismus $\varphi\colon K \to R$ von einem Körper in einen Ring ($\neq \{0\}$) ist injektiv! Es ist nämlich $\ker(\varphi)$ ein Ideal in K mit $1 \notin \ker(\varphi)$, also $\ker(\varphi) = \{0\}$. △

Satz 3.1.6. *Für einen Körper K hat der Matrixring $\mathrm{Mat}_n(K)$ nur die beiden trivialen Ideale.*

Beweis. Sei $J \lhd \mathrm{Mat}_n(K)$ und $0 \neq M \in J$. Wir zeigen $J = \mathrm{Mat}_n(K)$. Sei $E_{ij} \in \mathrm{Mat}_n(K)$ die Matrix mit einer 1 an der (i, j)-Position und Nullen überall sonst. Es gilt $\lambda E_{ij} = \lambda I_n \cdot E_{ij}$ und die E_{ij} spannen $\mathrm{Mat}_n(K)$ als K-Vektorraum auf. Also genügt es $E_{ij} \in J$ für alle i, j zu zeigen. Aufgrund der Gleichung

$$E_{ki}E_{ij}E_{jl} = E_{kl}$$

genügt es aber, das für *eine* Matrix E_{ij} zu zeigen. Falls der Eintrag von M an einer Stelle (i, j) gerade $m \neq 0$ ist, so gilt aber

$$E_{ij} = m^{-1} \cdot E_{ii} M E_{jj} \in J. \qquad \square$$

Satz 3.1.7. *Für ein Ideal $I \lhd R$ ist die folgende Multiplikation auf R/I wohldefiniert und macht R/I (zusammen mit der bereits bekannten Addition) zu einem Ring:*

$$(a + I) \cdot (b + I) := (a \cdot b) + I.$$

Die kanonische Projektion

$$\begin{aligned} \pi \colon R &\to R/I \\ a &\mapsto a + I \end{aligned}$$

ist ein surjektiver Ringhomomorphismus mit $\ker(\pi) = I$.

Beweis. Es gelte $a_1 + I = a_2 + I$ und $b_1 + I = b_2 + I$, also $a_1 - a_2 \in I, b_1 - b_2 \in I$. Aus der zweiten Idealeigenschaft folgt

$$a_1(b_1 - b_2) \in I \text{ und } (a_1 - a_2)b_2 \in I.$$

Durch Addition erhalten wir mit der ersten Idealeigenschaft

$$a_1 b_1 - a_2 b_2 \in I,$$

d.h. gerade $a_1 b_1 + I = a_2 b_2 + I$. Das zeigt die Wohldefiniertheit. Wiederum folgen die Axiome (Assoziativgesetz, Distributivgesetz) direkt aus denen in R. Das neutrale Element bezüglich $\cdot$ ist offensichtlich $1 + I$. Ebenso offensichtlich ist π ein Ringhomomorphismus mit I als Kern. $\square$

Definition 3.1.8. Wir nennen R/I den **Faktorring** oder **Restklassenring** von R nach I. $\triangle$

Für Ringe kann man einen Homomorphiesatz beweisen, genauso wie für Gruppen:

Satz 3.1.9 (Homomorphiesatz)**.** *Sei $\varphi \colon R \to S$ ein Ringhomomorphismus. Dann ist* $\ker(\varphi)$ *ein Ideal und die folgende Abbildung ist ein wohldefinierter injektiver Ringhomomorphismus:*

$$\begin{aligned} \overline{\varphi} \colon R/\ker(\varphi) &\to S \\ a + I &\mapsto \varphi(a). \end{aligned}$$

Insbesondere gilt $R/\ker(\varphi) \cong \operatorname{im}(\varphi)$.

Beweis. Offensichtlich ist $\ker(\varphi)$ ein Ideal in R. Mit Satz 2.2.1 wissen wir bereits, dass $\overline{\varphi}$ ein wohldefinierter injektiver Gruppenhomomorphismus ist. Nach Definition der Multiplikation im Faktorring ist es aber offensichtlich auch ein Ringhomomorphimus. □

Lemma 3.1.10. *Sei R ein Ring, $I, J \lhd R$ und $M \subseteq R$.*
(i) $I \cap J$ ist ein Ideal in R. Es ist das größte Ideal, das in I und J enthalten ist.
(ii) $I + J := \{a + b \mid a \in I, b \in J\}$ ist ein Ideal in R. Es ist das kleinste Ideal, das I und J enthält.
(iii) $I \cdot J := \{\sum_{i=1}^{n} a_i b_i \mid n \in \mathbb{N}, a_i \in I, b_i \in J\}$ ist ein Ideal in R. Es gilt

$$I \cdot J \subseteq I \cap J,$$

aber im Allgemeinen keine Gleichheit.
(iv) Sei Λ eine beliebige Indexmenge und $I_\lambda \lhd R$ für alle $\lambda \in \Lambda$. Für alle $\lambda, \gamma \in \Lambda$ gelte $I_\lambda \subseteq I_\gamma$ oder $I_\gamma \subseteq I_\lambda$. Dann ist

$$\bigcup_{\lambda \in \Lambda} I_\lambda$$

ein Ideal in R. Ohne die Inklusionsbedingung stimmt das im Allgemeinen nicht.
(v) Es gilt

$$\bigcap_{M \subseteq I \lhd R} I = \left\{ \sum_{i=1}^{n} a_i m_i b_i \mid n \in \mathbb{N}, a_i, b_i \in R, m_i \in M \right\}$$

und diese Menge ist das kleinste Ideal, das M enthält. Es heißt **das von M erzeugte Ideal** *und wird auch mit (M) bezeichnet.*

Beweis. Aufgabe 29. □

Satz 3.1.11 (Chinesischer Restsatz)**.** *Sei R ein Ring und $I_1, \ldots, I_n \lhd R$ Ideale mit*

$$I_i + I_j = R \quad \text{für } i \neq j.$$

Dann induzieren die kanonischen Projektionen einen Isomorphismus

$$R/(I_1 \cap \cdots \cap I_n) \cong R/I_1 \times \cdots \times R/I_n.$$

Insbesondere gibt es für jede Wahl von $a_1, \ldots, a_n \in R$ ein Element $a \in R$ mit

$$a \equiv a_i \bmod I_i$$

für $i = 1, \ldots, n$.

Beweis. Wir betrachten den Homomorphismus

$$\begin{aligned}\pi\colon R &\to R/I_1 \times \cdots \times R/I_n\\ a &\mapsto (a+I_1,\ldots,a+I_n)\end{aligned}$$

für den offensichtlich $\ker(\pi) = I_1 \cap \cdots \cap I_n$ gilt. Aufgrund des Homomorphiesatzes genügt es zu zeigen, dass π surjektiv ist.
Das beweisen wir zunächst im Fall $n = 2$. Nach Voraussetzung gibt es Elemente $b_1 \in I_1, b_2 \in I_2$ mit

$$b_1 + b_2 = 1.$$

Es gilt also

$$\begin{aligned} b_1 \equiv 0,\ b_2 \equiv 1 \mod I_1\\ b_1 \equiv 1,\ b_2 \equiv 0 \mod I_2.\end{aligned}$$

Für beliebige $a_1, a_2 \in R$ und $a := a_1b_2 + a_2b_1$ gilt dann

$$a \equiv a_1 \bmod I_1 \text{ und } a \equiv a_2 \bmod I_2,$$

die gewünschte Aussage.
Im Fall von $n \geq 3$ setze $J := \bigcap_{i\geq 2} I_i$. Nach Voraussetzung gibt es $c_2,\ldots,c_n \in I_1, d_2 \in I_2, \ldots, d_n \in I_n$ mit $c_i + d_i = 1$. Dann gilt

$$1 = \prod_{i=2}^{n}(c_i + d_i) = \underbrace{\prod_{i=2}^{n} c_i + \cdots +}_{\in I_1} \underbrace{\prod_{i=2}^{n} d_i}_{\in J}.$$

Also ist für die beiden Ideale I_1, J die Voraussetzung aus dem Fall $n = 2$ erfüllt, also gibt es $b_1 \in R$ mit

$$b_1 \equiv 1 \bmod I_1 \quad \text{und} \quad b_1 \equiv 0 \bmod J = \bigcap_{i=2}^{n} I_i,$$

also $b_1 \equiv 0 \bmod I_i$ für $i = 2,\ldots,n$. Analog erhält man für alle $j = 1,\ldots,n$ Elemente $b_j \in R$ mit

$$b_j \equiv 1 \bmod I_j \quad \text{und} \quad b_j \equiv 0 \bmod I_i \text{ für } i \neq j.$$

Das Element

$$a := a_1b_1 + \cdots + a_nb_n$$

erfüllt dann wie im Fall $n = 2$ die gewünschten Kongruenzen. □

Beispiel 3.1.12. In einer Wohngemeinschaft leben drei Personen, die in regelmäßigen Abständen morgens duschen möchten. Die WG hat zwar zwei Duschen, aber eben keine drei. Person A duscht nun an Tag 1 und dann immer alle drei Tage. Person B duscht einen Tag später, also am Tag 2, und dann nur alle 7 Tage. Person C schließlich duscht am dritten Tag und dann alle 4 Tage. Solange höchstens zwei Personen gleichzeitig morgens duschen wollen, geht alles in Ordnung. Problematisch wird es nur, wenn alle 3 Personen gleichzeitig duschen möchten. Nun ist die Frage, ob dieser Fall wirklich eintritt, und wenn ja, wann zum ersten Mal. Wenn nach x Tagen dieser Fall eintritt, dann hat x die Gestalt

$$\begin{aligned} x &= 1 + 3k \\ x &= 2 + 7m \\ x &= 3 + 4n, \end{aligned}$$

mit positiven ganzen Zahl k, m, n. Anders formuliert fragen wir uns also, ob es eine positive Zahl x gibt mit

$$\begin{aligned} x &\equiv 1 \bmod 3 \\ x &\equiv 2 \bmod 7 \\ x &\equiv 3 \bmod 4. \end{aligned}$$

Wir wollen also gerade ein System linearer Kongruenzen in $\mathbb{Z}$ lösen. Die dabei auftretenden Ideale sind $I_1 = (3), I_2 = (7), I_3 = (4)$. Man überprüft, dass die Voraussetzungen aus dem chinesischen Restsatz erfüllt sind. Also gibt es in der Tat irgendwann ein Duschproblem und man kann wie im Beweis des chinesischen Restsatzes auch genau bestimmen, wann (Aufgabe 30). △

Definition 3.1.13. (i) $0 \neq a \in R$ heißt **Nullteiler**, falls $b \neq 0$ in R existiert mit $ab = 0$ oder $ba = 0$.
(ii) Der Ring $R \neq \{0\}$ heißt **nullteilerfrei**, falls er keine Nullteiler besitzt. Ein kommutativer nullteilerfreier Ring wird auch **Integritätsring** oder **Integritätsbereich** genannt. △

Bemerkung/Beispiel 3.1.14. (i) Jeder Körper ist ein Integritätsring. Das folgt aus der Existenz von multiplikativ inversen Elementen. $\mathbb{Z}$ ist ebenfalls ein Integritätsring. Auch der Polynomring $R[x]$ über einem Integritätsring R ist wieder ein Integritätsring. Dort gilt nämlich für Polynome

$$\deg(p \cdot q) = \deg(p) + \deg(q),$$

da sich die Leitkoeffizienten beim Multiplizieren nicht aufheben können. Mit diesem Argument sieht man auch

$$R[x]^\times = R^\times.$$

(ii) Der Ring $\mathrm{Mat}_2(\mathbb{R})$ hat beispielsweise den Nullteiler

$$M = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Es gilt $M \cdot M = 0$.
(iii) Der Ring $\mathcal{C}([0,1], \mathbb{R})$ besitzt ebenfalls viele Nullteiler.
(iv) In einem Integritätsring können wir Produkte kürzen, obwohl Division im Allgemeinen nicht möglich ist! Aus $ab = ac$ mit $a \neq 0$ folgt nämlich

$$0 = ab - ac = a(b - c)$$

und aufgrund der Nullteilerfreiheit $b - c = 0$, also $b = c$. △

Satz 3.1.15. *Sei R ein kommutativer Ring und $p \in R[x]$ ein Polynom. Dann gilt für $a \in R$*

$$p(a) = 0 \Leftrightarrow p = (x - a) \cdot q \text{ für ein } q \in R[x].$$

Ist R ein Integritätsring, so hat $0 \neq p$ höchstens $\deg(p)$ viele verschiedene Nullstellen in R.

Beweis. "⇐": Für $p = (x - a) \cdot q$ gilt

$$p(a) = (a - a) \cdot q(a) = 0 \cdot q(a) = 0.$$

"⇒": Wir betrachten $\tilde{p} := p(x + a) \in R[x]$. Dann gilt $\tilde{p}(0) = p(a) = 0$, d.h. $\tilde{p}$ hat keinen konstanten Term. Das bedeutet aber gerade, dass man die Variable x aus $\tilde{p}$ ausklammern kann, also

$$\tilde{p} = x \cdot \tilde{q}$$

für ein $\tilde{q} \in R[x]$. Daraus folgt

$$p = \tilde{p}(x - a) = (x - a) \cdot \tilde{q}(x - a),$$

also können wir $q := \tilde{q}(x - a)$ wählen.

Sei nun R nullteilerfrei und $p \in R[x]$ habe in R die verschiedenen Nullstellen $a_1, \ldots, a_n$. Dann gilt $p = (x - a_1) \cdot q_1$ und wegen

$$0 = p(a_2) = \underbrace{(a_2 - a_1)}_{\neq 0} \cdot q_1(a_2)$$

und der Nullteilerfreiheit von R muss $q_1(a_2) = 0$ gelten. Iterativ sehen wir

$$p = (x - a_1) \cdots (x - a_n) \cdot q$$

für ein $0 \neq q \in R[x]$ und damit

$$\deg(p) = n + \deg(q) \geq n. \qquad \square$$

Korollar 3.1.16 (Polynominterpolation)**.** *Sei K ein Körper und $a_1, \ldots, a_d \in K$ paarweise verschieden sowie $b_1, \ldots, b_d \in K$. Dann gibt es genau ein Polynom $p \in K[x]$ mit $\deg(p) \leq d - 1$ und*

$$p(a_i) = b_i \quad \textit{für } i = 1, \ldots, d.$$

Beweis. *Existenz*: Das Polynom

$$p_i := \frac{1}{\prod_{j \neq i}(a_i - a_j)} \prod_{j \neq i}(x - a_j)$$

erfüllt

$$\deg(p_i) = d - 1, \quad p_i(a_i) = 1 \quad \text{und} \quad p_i(a_j) = 0 \text{ für } j \neq i.$$

Somit ist

$$p = b_1 p_1 + \cdots + b_n p_n$$

ein gewünschtes Interpolationspolynom vom Grad höchstens $d - 1$.
Eindeutigkeit: Falls p, q beides Interpolationspolynome sind, so hat das Polynom $p - q$ Grad höchstens $d - 1$ und d verschiedene Nullstellen in K. Nach Satz 3.1.15 muss es das Nullpolynom sein, also $p = q$. $\square$

Satz 3.1.17. *Für $0 \neq n \in \mathbb{Z}$ sind äquivalent:*

(i) *$\mathbb{Z}/n\mathbb{Z}$ ist ein Körper.*

(ii) *$\mathbb{Z}/n\mathbb{Z}$ ist nullteilerfrei.*

(iii) *n ist eine Primzahl.*

Beweis. Übungsaufgabe. $\square$

3.2 Noethersche Ringe und Hauptidealringe

Ab jetzt seien alle Ringe kommutativ!

Definition 3.2.1. Ein Ring R heißt **noethersch**, falls jedes Ideal $I \lhd R$ von einer endlichen Menge erzeugt wird, also von der Gestalt

$$I = (a_1, \ldots, a_m) = \left\{ \sum_{i=1}^{m} b_i a_i \mid b_i \in R \right\}$$

für ein $m \in \mathbb{N}$ und $a_1, \ldots, a_m \in R$ ist. R heißt **Hauptidealring**[1], wenn jedes Ideal von einem Element erzeugt wird, also von der Gestalt

$$I = (a) = \{ba \mid b \in R\}$$

ist. △

Beispiel 3.2.2. (i) Jeder Körper ist ein Hauptidealring. Es gilt

$$\{0\} = (0) \text{ und } K = (1).$$

Andere Ideale gibt es nicht.
(ii) Bemerkung/Beispiel 3.1.5 (iv) besagt gerade, dass $\mathbb{Z}$ ein Hauptidealring ist. Es ist ja gerade $n\mathbb{Z} = (n)$. △

Satz 3.2.3. *Für jeden Körper K ist der Polynomring $K[x]$ ein Hauptidealring.*

Beweis. Der Beweis geht ganz analog zu Lemma 2.1.5, nur dass wir statt Division mit Rest in $\mathbb{Z}$ hier Polynomdivision benutzen. Sei also $I \lhd K[x]$ ein Ideal. Der Fall $I = \{0\} = (0)$ ist trivial. Sei also $I \neq \{0\}$ und $p \in I \setminus \{0\}$ ein Polynom von kleinstem Grad. Offensichtlich gilt dann

$$(p) \subseteq I.$$

Um die andere Inklusion zu zeigen, wählen wir $0 \neq q \in I$ beliebig. Durch Polynomdivision (die über einem allgemeinen Körper immer möglich ist) erhalten wir eine Gleichung

$$q = fp + r$$

mit Polynomen $f, r \in K[x]$ und $\deg(r) < \deg(p)$. Aus $r = q - fp \in I$ folgt wegen der Wahl von p schon $r = 0$, also $q = fp \in (p)$. □

[1] seltsamerweise hat niemand den Begriff *schwere-noethersch* in Erwägung gezogen

Konstruktion 3.2.4. Für einen Ring R definieren wir den Polynomring über R in **mehreren Variablen** iterativ als

$$R[x_1, \ldots, x_n] := (R[x_1, \ldots, x_{n-1}])\,[x_n].$$

Wenn R ein Integritätsring ist, ist der Polynomring ebenfalls ein Integritätsring. Man sieht leicht, dass man eine isomorphe Darstellung durch folgende Beschreibung bekommt:

$$R[x_1, \ldots, x_n] := \left\{ \sum_{\alpha \in \mathbb{N}^n} c_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid c_\alpha \in R, \text{ nur endlich viele } c_\alpha \neq 0 \right\}.$$

Dabei wird wie gewohnt addiert und multipliziert, zum Beispiel in $\mathbb{Z}[x_1, x_2, x_3]$

$$(1 + x_1x_2 - x_2^3) + (x_1x_2 + 7x_1x_3^2) = 1 + 2x_1x_2 - x_2^3 + 7x_1x_3^2.$$

$$(1+x_1x_2-x_2^3)\cdot(x_1x_2+7x_1x_3^2) = x_1x_2+7x_1x_3^2+x_1^2x_2^2+7x_1^2x_2x_3^2-x_1x_2^4-7x_1x_2^3x_3^2.$$

Dabei heißt ein Term der Gestalt

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} =: \underline{x}^\alpha$$

ein **Monom** und

$$\deg(\underline{x}^\alpha) := |\alpha| := \alpha_1 + \cdots + \alpha_n$$

sein **Grad**. Für ein Polynom

$$0 \neq p = \sum_{\alpha \in \mathbb{N}^n} c_\alpha \underline{x}^\alpha \in R[x_1, \ldots, x_n]$$

setzen wir $\deg(p) := \max\{\deg(\underline{x}^\alpha) \mid c_\alpha \neq 0\}$. So ist beispielsweise

$$p = 1 - x_1^2 + x_1x_2^4 - 12x_1x_3^{15} \in \mathbb{Z}[x_1, x_2, x_3]$$

ein Polynom über $\mathbb{Z}$ vom Grad 16 in drei Variablen. △

Bemerkung 3.2.5. (i) Satz 3.2.3 stimmt nicht für Polynomringe in mehr als einer Variablen über einem Körper. Zum Beispiel ist das Ideal

$$(x_1, x_2) \lhd \mathbb{Q}[x_1, x_2]$$

nicht von einem Element erzeugt (Aufgabe 33). Man beachte allerdings Satz 3.2.8 unten.
(ii) Satz 3.2.3 stimmt ebenfalls nicht, wenn K kein Körper ist. So ist zum Beispiel das Ideal $I = (2, x) \subseteq \mathbb{Z}[x]$ kein Hauptideal (Aufgabe 33). △

Beispiel 3.2.6. Der Ring $\mathbb{Z}[i]$ der ganzen Gaußschen Zahlen ist ein Hauptidealring. Dazu zeigt man, dass Division mit Rest existiert, es also für $0 \neq a, b \in \mathbb{Z}[i]$ stets eine Darstellung

$$b = xa + r$$

mit $x, r \in \mathbb{Z}[i]$ und $|r| < |a|$ gibt. Danach wiederholt man das Argument aus dem Beweis von Satz 3.2.3 bzw. Lemma 2.1.5. △

Satz 3.2.7. *Für einen Ring R sind äquivalent:*

(i) *R ist noethersch.*

(ii) *Jede aufsteigende abzählbare Kette von Idealen wird konstant.*

(iii) *Jede nichtleere Menge von Idealen enthält ein maximales Ideal.*

Beweis. (*i*)⇒(*ii*): Sei

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

eine Kette von Idealen in R. Nach Lemma 3.1.10 (iv) ist $I = \bigcup_{i \geq 1} I_i$ ein Ideal in R, also $I = (a_1, \ldots, a_m)$, da R noethersch ist. Wegen $a_i \in I$ für $i = 1, \ldots, m$ und da die Kette aufsteigend ist, gibt es ein $n \in \mathbb{N}$ mit

$$a_1, \ldots, a_m \in I_n.$$

Damit gilt $I = (a_1, \ldots, a_m) \subseteq I_n$, also $I_n = I_{n+1} = \cdots = I$.
(*ii*)⇒(*iii*): Angenommen eine nichtleere Menge von Idealen in R hat kein maximales Element. Dann kann man daraus offensichtlich eine echt aufsteigende Folge von Idealen wählen, die nicht konstant wird, ein Widerspruch.
(*iii*)⇒(*i*): Sei I ein Ideal in R und $\mathcal{M}$ die Menge aller endlich erzeugten Ideale von R, die in I enthalten sind. Dann ist $\mathcal{M}$ nicht leer, da zum Beispiel $(0) \in \mathcal{M}$. Wegen (*iii*) muss es ein maximales Element $(a_1, \ldots, a_m) \in \mathcal{M}$ geben. Wäre $(a_1, \ldots, a_m) \subsetneq I$, so gäbe es ein $a \in I \setminus (a_1, \ldots, a_m)$ und dann wäre

$$(a_1, \ldots, a_m) \subsetneq (a_1, \ldots, a_m, a) \in \mathcal{M}.$$

Das widerspricht der Maximalität, also ist $I = (a_1, \ldots, a_m)$ ein endlich endlich erzeugtes Ideal. □

Satz 3.2.8 (Hilbertscher Basissatz)**.** *Sei R ein noetherscher Ring. Dann ist der Polynomring $R[x]$ wieder noethersch. Insbesondere ist der Polynomring $K[x_1, \ldots, x_n]$ in mehreren Variablen über einem Körper noethersch, ebenso wie $\mathbb{Z}[x_1, \ldots, x_n]$.*

Beweis. Angenommen $I \lhd R[x]$ ist ein nicht endlich erzeugtes Ideal. Wähle iterativ Elemente $p_1, p_2, \ldots \in I$ so, dass p_{n+1} von minimalem Grad aus $I \setminus (p_1, \ldots, p_n)$ ist. Ist $d_n = \deg(p_n)$, so gilt $d_1 \leq d_2 \leq \cdots$. Sei nun $c_n \in R$ der Leitkoeffizient des Polynoms p_n. Betrachte das Ideal

$$J := (c_n \mid n \in \mathbb{N}) \lhd R.$$

Da J nach Annahme an R endlich erzeugt ist, gibt es eine Gleichung

$$c_{m+1} = \sum_{i=1}^{m} b_i c_i$$

mit $b_i \in R$. Setze nun

$$g := p_{m+1} - \sum_{i=1}^{m} b_i p_i x^{d_{m+1}-d_i}.$$

Nach Konstruktion gilt $\deg(g) < \deg(p_{m+1})$, denn die Leitkoeffizienten heben sich gegenseitig gerade auf. Andererseits gilt wegen $p_{m+1} \in I \setminus (p_1, \ldots, p_m)$ auch $g \in I \setminus (p_1, \ldots, p_m)$. Das ist ein Widerspruch zur Wahl von p_{m+1}.
Da K als Körper ein noetherscher Ring ist (sogar ein Hauptidealring), und der Polynomring $K[x_1, \ldots, x_n]$ iterativ als $(K[x_1, \ldots, x_{n-1}])\,(x_n)$ definiert ist, ist es damit also offensichtlich ein noetherscher Ring. Dasselbe gilt für $\mathbb{Z}[x_1, \ldots, x_n]$. □

Lemma 3.2.9. *Sei $\varphi\colon R \twoheadrightarrow S$ ein surjektiver Ringhomomorphismus und R noethersch. Dann ist auch S noethersch. Insbesondere ist für einen noetherschen Ring R und $I \lhd R$ der Faktorring R/I wieder noethersch. Dasselbe stimmt für die Eigenschaft "Hauptidealring".*

Beweis. Aufgabe 35. □

3.3 Primideale und maximale Ideale

Sei wieder R stets ein kommutativer Ring.

Definition 3.3.1. (i) Ein Ideal $\mathfrak{p} \lhd R$ heißt **Primideal**, falls $\mathfrak{p} \neq R$ und für alle $a, b \in R$ gilt

$$ab \in \mathfrak{p} \;\Rightarrow\; a \in \mathfrak{p} \text{ oder } b \in \mathfrak{p}.$$

(ii) Ein Ideal $\mathfrak{m} \lhd R$ heißt **maximales Ideal**, falls $\mathfrak{m} \neq R$ und $\mathfrak{m}$ maximal als echtes Ideal ist, d.h. aus $\mathfrak{m} \subseteq I \lhd R$ folgt $I = \mathfrak{m}$ oder $I = R$. △

Bemerkung/Beispiel 3.3.2. (i) In $\mathbb{Z}$ gilt

$$(n) \text{ Primideal } \Leftrightarrow \ n \text{ Primzahl (oder } n = 0).$$

Es bedeutet nämlich $ab \in (n)$ gerade $n \mid ab$ und für eine Primzahl n folgt (mit der eindeutigen Primfaktorzerlegung von a und b) daraus $n \mid a$ oder $n \mid b$, also $a \in (n)$ oder $b \in (n)$. Ist umgekehrt n keine Primzahl, so wählen wir eine echte Zerlegung $n = ab$ und erhalten $ab \in (n)$, aber $a \notin (n), b \notin (n)$.
(ii) In einem nullteilerfreien Hauptidealring R ist jedes Primideal $(a) \neq \{0\}$ automatisch ein maximales Ideal. Es bedeutet $(a) \subseteq (b)$ ja gerade $bc = a \in (a)$ für ein $c \in R$. Aus der Primidealeigenschaft folgt also $b \in (a)$ oder $c \in (a)$. Im ersten Fall gilt $(b) \subseteq (a)$, also $(a) = (b)$, im zweiten Fall gilt $c = c'a$ für ein $c' \in R$. Damit folgt aus $bc'a = a$ durch kürzen $bc' = 1$, also $(b) = R$. Ohne Nullteilerfreiheit kann man nicht kürzen, und die Aussage stimmt dann auch nicht (vergleiche Aufgabe 37).
(iii) Im Ring $\mathcal{C}([0,1], \mathbb{R})$ erhalten wir für jedes $X \subseteq [0,1]$ ein Ideal

$$I_X := \{f \in \mathcal{C}([0,1]) \mid f \equiv 0 \text{ auf } X\}.$$

Es ist genau dann ein Primideal wenn $\#X = 1$ gilt und dann ist es automatisch auch ein maximales Ideal. Jedes maximale Ideal ist von dieser Gestalt (Aufgabe 38).
(iv) Im Polynomring $\mathbb{R}[x, y]$ ist

$$(x) = \{x \cdot p \mid p \in \mathbb{R}[x, y]\}$$

ein Primideal, aber kein maximales Ideal (Übungsaufgabe). △

Bemerkung 3.3.3. (i) Es ist $\mathfrak{p} \lhd R$ genau dann ein Primideal, wenn $R \setminus \mathfrak{p}$ die 1 enthält und abgeschlossen unter $\cdot$ ist.
(ii) Es ist $\{0\}$ genau dann ein Primideal, wenn R ein Integritätsbereich ist. △

Satz 3.3.4. *Für ein Ideal $I \lhd R$ gilt:*

(i) I Primideal $\Leftrightarrow$ R/I Integritätsbereich.

(ii) I maximales Ideal $\Leftrightarrow$ R/I Körper.

Insbesondere ist jedes maximale Ideal ein Primideal.

Beweis. Für (i) sei I prim und in R/I gelte

$$0 = 0 + I = (a + I)(b + I) = ab + I.$$

Das bedeutet in R gerade $ab \in I$ und daraus folgt $a \in I$ oder $b \in I$. Daraus folgt $a + I = 0$ oder $b + I = 0$. Also ist R/I nullteilerfrei.
Sei umgekehrt R/I nullteilerfrei und in R gelte $ab \in I$. Das bedeutet in R/I gerade

$$0 = ab + I = (a + I)(b + I)$$

und daraus folgt $a + I = 0$ oder $b + I = 0$, also $a \in I$ oder $b \in I$. Also ist I ein Primideal.
Für (ii) sei zunächst I maximal. Für $0 \neq a + I \in R/I$ gilt $a \notin I$, also ist

$$I \subsetneq I + (a) \lhd R,$$

und aus der Maximalität von I folgt $I + (a) = R$. Also gibt es eine Gleichung

$$i + ba = 1$$

mit $i \in I, b \in R$. In R/I bedeutet das

$$1 = 1 + I = (i + ba) + I = (i + I) + (b + I)(a + I) = (b + I)(a + I),$$

also ist $a + I$ in R/I multiplikativ invertierbar. Also ist R/I ein Körper.
Sei umgekehrt R/I ein Körper und $I \subsetneq J \lhd R$. Wähle $a \in J \setminus I$. Dann gilt in R/I

$$0 \neq a + I,$$

also gibt es $b \in R$ mit

$$1 = 1 + I = (a + I)(b + I) = ab + I,$$

d.h. $1 - ab \in I$. Damit gilt

$$1 = \underbrace{ab}_{\in J} + \underbrace{(1 - ab)}_{\in I \subseteq J} \in J,$$

also $J = R$. Somit ist I maximal.
Da Körper insbesondere Integritätsringe sind, ist also jedes maximale Ideal ein Primideal. □

Satz 3.3.5. *Sei $I \lneq R$ ein echtes Ideal. Dann gibt es ein maximales Ideal $\mathfrak{m}$ mit*

$$I \subseteq \mathfrak{m} \lhd R.$$

Beweis. Wir verwenden das Zorn'sche Lemma. Sei dazu

$$\mathcal{M} := \{J \lneq R \mid I \subseteq J\}.$$

Dann ist $I \in \mathcal{M}$, also $\mathcal{M} \neq \emptyset$. $\mathcal{M}$ ist partiell geordnet durch $\subseteq$ und jede Kette $(I_\lambda)_{\lambda\in\Lambda}$ in $\mathcal{M}$ besitzt nach Lemma 3.1.10 (iv) in $\mathcal{M}$ eine obere Schranke, nämlich

$$\tilde{I} = \bigcup_{\lambda\in\Lambda} I_\lambda.$$

Dabei folgt $\tilde{I} \neq R$ aus der Tatsache, dass $1 \in \tilde{I}$ schon $1 \in I_\lambda$ für ein λ bedeuten würde und damit $I_\lambda = R$, ein Widerspruch.
Mit dem Zorn'schen Lemma besitzt $\mathcal{M}$ nun bezüglich $\subseteq$ ein maximales Element und das ist offensichtlich ein gewünschtes maximales Ideal. □

3.4 Der Quotientenkörper

Konstruktion 3.4.1. So wie wir von $\mathbb{Z}$ zu $\mathbb{Q}$ übergehen können, können wir zu jedem Integritätsring einen sogenannten Quotientenkörper konstruieren. Sei also R ein Integritätsring. Auf der Menge

$$\{(a, b) \mid a, b \in R, b \neq 0\}$$

definieren wir eine Äquivalenzrelation:

$$(a, b) \sim (c, d) \;:\Leftrightarrow\; ad = bc.$$

Um nachzurechnen, dass es sich dabei wirklich um eine Äquivalenzrelation handelt, benötigt man Nullteilerfreiheit und Kommutativität von R!
Die Äquivalenzklasse von (a, b) bezeichnen wir dann mit $\frac{a}{b}$ und die Menge aller Äquivalenzklassen mit $\mathrm{Quot}(R)$:

$$\mathrm{Quot}(R) := \left\{\frac{a}{b} \mid a, b \in R, b \neq 0\right\}.$$

Auf $\mathrm{Quot}(R)$ sind nun Addition und Multiplikation definiert durch

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

wobei man die Wohldefiniertheit nachrechnen muss. Damit ist aber $\mathrm{Quot}(R)$ dann ein kommutativer Ring mit Nullelement $\frac{0}{1}$ und Einselement $\frac{1}{1}$. Das additiv Inverse zu $\frac{a}{b}$ ist $\frac{-a}{b}$, und für $0 \neq \frac{a}{b}$ existiert sogar das multiplikativ inverse Element $\frac{b}{a}$. Somit ist $\mathrm{Quot}(R)$ ein Körper, genannt der **Quotientenkörper** von R. Die Abbildung

$$\begin{aligned} \iota\colon R &\to \mathrm{Quot}(R) \\ a &\mapsto \frac{a}{1} \end{aligned}$$

ist ein injektiver Ringhomomorphismus, wir können also R als Teilring der Körpers $\mathrm{Quot}(R)$ auffassen. △

Korollar 3.4.2. *R ist genau dann ein Integritätsring, wenn er Teilring eines Körpers ist.*

Beispiel 3.4.3. (i) Der Quotientenkörper von $\mathbb{Z}$ ist $\mathbb{Q}$.
(ii) Für jeden Integritätsring R ist $R[x_1, \ldots, x_n]$ wieder ein Integritätsring, also existiert der Quotientenkörper $\mathrm{Quot}\left(R[x_1, \ldots, x_n]\right)$. Wir nennen ihn den Körper der **rationalen Funktionen** über R und bezeichnen ihn mit $R(x_1, \ldots, x_n)$. △

Der Quotientenkörper ist der kleinste Körper, in dem ein Integritätsring enthalten ist:

Proposition 3.4.4. *Sei R ein Integritätsring, K ein Körper und*

$$\varphi\colon R \hookrightarrow K$$

ein injektiver Homomorphimus. Dann existiert genau ein Homomorphismus $\tilde{\varphi}\colon \mathrm{Quot}(R) \to K$ mit

$$\tilde{\varphi} \circ \iota = \varphi.$$

Beweis. Für $0 \neq b \in R$ ist $0 \neq \varphi(b) \in K$, also existiert dort $\varphi(b)^{-1}$. Wir definieren also

$$\tilde{\varphi}\left(\frac{a}{b}\right) := \varphi(a)\varphi(b)^{-1}$$

und rechnen direkt nach, dass es sich dabei um einen wohldefinierten Ringhomomorphismus $\tilde{\varphi}\colon \mathrm{Quot}(R) \to K$ handelt. Es gilt

$$(\tilde{\varphi} \circ \iota)(a) = \tilde{\varphi}\left(\frac{a}{1}\right) = \varphi(a)\varphi(1)^{-1} = \varphi(a),$$

also ist $\tilde{\varphi}$ eine gewünschte Fortsetzung. Für jede solche Fortsetzung $\tilde{\varphi}$ muss gelten

$$\tilde{\varphi}\left(\frac{a}{b}\right) = \tilde{\varphi}\left(\frac{a}{1} \cdot \left(\frac{b}{1}\right)^{-1}\right) = \tilde{\varphi}(\iota(a))\tilde{\varphi}(\iota(b))^{-1} = \varphi(a)\varphi(b)^{-1},$$

also ist $\tilde{\varphi}$ eindeutig bestimmt. □

3.5 Teilbarkeit

Sei in diesem Abschnitt R stets ein Integritätsbereich.

Definition 3.5.1. Für $a, b \in R$ definieren wir:
(i) $a \mid b :\Leftrightarrow \exists c \in R : \ ac = b$ (in Worten: a **teilt** b).
(ii) $a \sim b :\Leftrightarrow \exists e \in R^\times : \ ae = b$ (in Worten: a und b sind **assoziiert**).
(iii) Eine **Teilerkette** ist eine Folge

$$a_1, a_2, \ldots, a_n, \ldots$$

von Elementen in R mit

$$a_{i+1} \mid a_i$$

für alle i. Die Teilerkette heiß **echt**, falls $a_i \nmid a_{i+1}$ für alle i gilt.
(iv) $0 \neq a$ heißt **irreduzibel**, falls $a \notin R^\times$ und aus $a = bc$ stets $b \in R^\times$ oder $c \in R^\times$ folgt.
(v) $0 \neq a$ heißt **prim**, falls $a \notin R^\times$ und aus $a \mid bc$ stets $a \mid b$ oder $a \mid c$ folgt. △

Bemerkung 3.5.2. (i) $a \mid b$ ist äquivalent zu $(b) \subseteq (a)$. Eine Teilerkette ist also eine Folge $a_1, a_2, \ldots$ mit

$$(a_1) \subseteq (a_2) \subseteq \cdots$$

und die Teilerkette ist echt, wenn alle Inklusionen echte Inklusionen sind.
(ii) $a \sim b$ ist äquivalent zu $a \mid b$ und $b \mid a$, also zu $(a) = (b)$. In $\mathbb{Z}$ ist jedes Element a genau zu a und $-a$ assoziiert.
(iii) a ist genau dann prim, wenn (a) ein Primideal ist.
(iv) In einem Körper gibt es weder irreduzible noch Primelemente. △

Lemma 3.5.3. *Primelemente sind irreduzibel.*

Beweis. Sei a prim und gelte $a = bc$. Dann gilt inbesondere $a \mid bc$, also o.B.d.A $a \mid b$, d.h. $ad = b$ für ein $d \in R$. Daraus folgt $a = adc$ und mit der Kürzungsregel folgt $1 = dc$, also $c \in R^\times$. Also ist a irreduzibel. □

Die Umkehrung gilt im Allgemeinen nicht:

Beispiel 3.5.4. Wir betrachten den folgenden Teilring der komplexen Zahlen:

$$R = \mathbb{Z}[\sqrt{-5}] := \left\{ a + ib\sqrt{5} \mid a, b \in \mathbb{Z} \right\} \subseteq \mathbb{C}.$$

Dann ist das Element $2 \in R$ irreduzibel, aber nicht prim: es sei dazu

$$2 = (a + ib\sqrt{5})(c + id\sqrt{5}) = (ac - 5bd) + i(ad + bc)\sqrt{5}.$$

Durch Vergleich von Real- und Imaginärteil erhalten wir

$$ac - 5bd = 2,\ ad + bc = 0.$$

Wegen

$$4 = (ac - 5bd)^2 + 5(ad + bc)^2 = (a^2 + 5b^2)(c^2 + 5d^2)$$

folgt daraus direkt $b = d = 0$ und damit $2 = ac$. Sei also o.B.d.A. $a = 1$. Dann ist aber $a + ib\sqrt{5} = 1$ in R invertierbar. Also ist 2 irreduzibel.
2 ist hingegen nicht prim. Es gilt

$$2 \cdot 3 = 6 = (1 + i\sqrt{5})(1 - i\sqrt{5}),$$

also $2 \mid (1 + i\sqrt{5})(1 - i\sqrt{5})$. Es gilt aber $2 \nmid (1 \pm i\sqrt{5})$, wie man direkt sieht.
Wir sehen hier auch, dass Elemente (hier die 6) verschiedene Zerlegungen als Produkt von irreduziblen Elementen haben können. △

Lemma 3.5.5. *Gibt es in R keine echten unendlichen Teilerketten, so ist jedes Element $0 \neq a \in R$ entweder invertierbar oder Produkt von endlich vielen irreduziblen Elementen. Dies stimmt in noetherschen Integritätsringen immer.*

Beweis. Ist a keine Einheit und nicht irreduzibel, so schreiben wir $a = bc$ mit $b, c \notin R^\times$. Es gilt also $b \mid a, c \mid a$ und $a \nmid b, c$. Wir iterieren den Prozess mit b und c. Da es keine unendlichen echten Teilerketten gibt, müssen alle Faktoren irgendwann irreduzibel sein.
Da es in noetherschen Ringen keine unendlich echt aufsteigenden Idealketten gibt (Satz 3.2.7), gibt es auch keine unendlichen echten Teilerketten (vgl. Bemerkung 3.5.2 (i)). □

Eine Zerlegung in irreduzible Elemente muss nicht eindeutig sind, eine in Primelemente hingegen schon, bis auf Reihenfolge und assoziierte Elemente:

Proposition 3.5.6. *Seien $p_1, \dots, p_m \in R$ prim, $q_1, \dots, q_n \in R$ irreduzibel, und es gelte*

$$p_1 \cdots p_m = q_1 \cdots q_n.$$

Dann gilt $m = n$ und die Reihenfolge der q_i kann so gewählt werden, dass $p_i \sim q_i$ für $i = 1, \dots, m$ gilt. Insbesondere ist eine Primfaktorzerlegungen eines Elements immer eindeutig bis auf Reihenfolge und assoziierte Elemente.

Beweis. Aus $p_1 \cdots p_m = q_1 \cdots q_n$ folgt $p_1 \mid q_1 \cdots q_n$. Da p_1 prim ist, existiert ein i mit $p_1 \mid q_i$. Nach Umnummerierung nehmen wir $i = 1$ an, d.h. $p_1 \mid q_1$. Da q_1 irreduzibel ist, folgt entweder $p_1 \in R^\times$ oder $p_1 \sim q_1$. Der erste Fall ist nicht möglich, weil p_1 prim ist. Also gilt $p_1 \sim q_1$ und damit nach Kürzung (und ignorieren von Einheiten)

$$p_2 \cdots p_m = q_2 \cdots q_n.$$

Wir setzen diese Schlussweise nun einfach iterativ fort. Ist $m < n$, so haben wir am Ende $u := q_{m+1} \cdots q_n \in R^\times$. Das würde aber

$$1 = uu^{-1} = q_{m+1} q_{m+2} \cdots q_n u^{-1} = q_{m+1}(q_{m+2} \cdots q_n u^{-1})$$

implizieren, also also $q_{m+1} \in R^\times$, ein Widerspruch zur Irreduzibilität von q_{m+1}. Im umgekehrten Fall $m > n$ haben wir $p_{n+1} \cdots p_m = 1$, was auf denselben Widerspruch führt. Also ist $m = n$ und es folgt die erste Behauptung. Die zweite Behauptung ist klar, da Primelemente irreduzibel sind. □

Definition 3.5.7. Ein Integritätsbereich, in dem jedes Element $0 \neq a \in R \setminus R^\times$ ein endliches Produkt von Primelementen ist, heißt **faktorieller Ring**. △

Bemerkung 3.5.8. Nach Proposition 3.5.6 besitzt jedes Element eines faktoriellen Rings eine eindeutige Primfaktorzerlegung, bis auf Reihenfolge und assoziierte Elemente. Daraus folgt auch direkt, dass es in einem faktoriellen Ring keine echten unendlichen Teilerketten geben kann. △

Proposition 3.5.9. *In einem faktoriellen Ring sind irreduzible Elemente prim.*

Beweis. Sei q irreduzibel und $q = p_1 \cdots p_m$ eine Darstellung als Produkt von Primelementen. Aus Proposition 3.5.6 folgt $m = 1$ und $q \sim p_1$ ist somit prim. □

Beispiel 3.5.10. Der Ring $\mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell. Beispielsweise ist 2 irreduzibel und nicht prim.

Satz 3.5.11. *Nullteilerfreie Hauptidealringe sind faktoriell.*

Beweis. Wir zeigen zuerst dass irreduzible Elemente prim sind. Sei dazu a irreduzibel. Dann ist (a) sogar ein maximales Ideal in R, man argumentiert genau wie in Bemerkung 3.3.2 (ii). Als maximales Ideal ist (a) aber nach Satz 3.3.4 ein Primideal und damit ist a prim.
Als Hauptidealring ist R nun insbesondere noethersch und damit besitzt a nach Lemma 3.5.5 eine Darstellung als Produkt von irreduziblen Elementen, die automatisch prim sind. □

Beispiel 3.5.12. Es sind also $\mathbb{Z}$, $K[x]$ und $\mathbb{Z}[i]$ faktorielle Ringe. △

In einem faktoriellen Ring können wir den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache von zwei Elementen genau wie in $\mathbb{Z}$ definieren:

Definition 3.5.13. Sei R ein faktorieller Ring und $a, b \in R \setminus \{0\}$. Wir schreiben

$$a = e_1 \cdot p_1^{\nu_1} \cdots p_n^{\nu_n} \qquad b = e_2 \cdot p_1^{\mu_1} \cdots p_n^{\mu_n}$$

mit $e_1, e_2 \in R^\times$ und Primelementen $p_1, \ldots, p_n$. Dabei sind die Exponenten $\nu_i, \mu_i \in \mathbb{N}$ eindeutig bestimmt.
(i) Es heißt

$$\mathrm{ggT}(a, b) := p_1^{\min(\nu_1, \mu_1)} \cdots p_n^{\min(\nu_n, \mu_n)}$$

der **größte gemeinsame Teiler** von a, b. Beachte, dass er nur bis auf Einheiten eindeutig bestimmt ist. Wir setzen

$$\mathrm{ggT}(a, 0) := \mathrm{ggT}(0, a) = a, \quad \mathrm{ggT}(0, 0) := 0.$$

(ii) Es heißt

$$\mathrm{kgV}(a, b) := p_1^{\max(\nu_1, \mu_1)} \cdots p_n^{\max(\nu_n, \mu_n)}$$

das **kleinste gemeinsame Vielfache** von a, b. Es ist ebenfalls nur bis auf Einheiten eindeutig bestimmt. Wir setzen

$$\mathrm{kgV}(a, 0) := \mathrm{kgV}(0, a) = 0, \quad \mathrm{kgV}(0, 0) := 0.$$

(iii) Offensichtlich kann man ggT und kgV analog auch für mehr als zwei Elemente definieren, zum Beispiel iterativ, oder direkt über die entsprechende Formel mit $\min$ und $\max$. △

Lemma 3.5.14. *Für $a, b, c \in R$ gilt*

$$\mathrm{ggT}(a,b) \mid a \text{ und } \mathrm{ggT}(a,b) \mid b$$

sowie

$$c \mid a \text{ und } c \mid b \Rightarrow c \mid \mathrm{ggT}(a,b).$$

Es gilt

$$(a,b) = (c) \Rightarrow c = \mathrm{ggT}(a,b)$$

und in einem Hauptidealring insbesondere stets

$$\mathrm{ggT}(a,b) = xa + yb$$

für gewisse $x, y \in R$.

Beweis. Alle Aussage folgen leicht aus der Existenz der eindeutigen Primfaktorzerlegung aller Elemente. □

Im Rest dieses Abschnitts befassen wir uns mit Teilbarkeit in Polynomringen. Der wichtigste Satz ist dabei der Satz von Gauß 3.5.21. Die Aussagen sind wichtig für die Körpertheorie im nächsten Kapitel. Sei dazu ab jetzt stets R ein faktorieller Ring.

Definition 3.5.15. (i) Für ein Polynom

$$p = c_0 + c_1 x + \cdots + c_d x^d \in R[x]$$

definieren wir seinen **Inhalt** $\mathcal{I}(p)$ durch

$$\mathcal{I}(p) := \mathrm{ggT}(c_0, \ldots, c_d).$$

Beachte wieder, dass $\mathcal{I}(p)$ nur bis auf Einheiten eindeutig bestimmt ist.
(ii) $p \in R[x]$ heißt **primitiv**[2], falls $\mathcal{I}(p) \in R^\times$ (man sagt dazu auch: die Koeffizienten von p sind teilerfremd). △

Bemerkung/Beispiel 3.5.16. (i) Für $p = 2x + 4 \in \mathbb{Z}[x]$ gilt

$$\mathcal{I}(p) = \mathrm{ggT}(4,2) = 2 \in \mathbb{Z} \setminus \mathbb{Z}^\times,$$

[2]Trifft ein primitives Element einen schwere-noetherschen Ring...

p ist also nicht primitiv. Betrachtet man stattdessen $p = 2x + 4 \in \mathbb{Q}[x]$, so gilt $\mathcal{I}(p) = 1$ (oder jedes andere Element $\neq 0$). Also ist p primitiv. Inhalt und Primitivität hängen also stark vom Ring R ab.
(ii) Für $p = 2x^3 + 9x + 12 \in \mathbb{Z}[x]$ gilt

$$\mathcal{I}(p) = \mathrm{ggT}(12, 9, 0, 2) = 1 \in \mathbb{Z}^\times,$$

also ist p primitiv.
(iii) Für einen Körper K ist jedes $0 \neq p \in K[x]$ primitiv.
(iv) Jedes Polynom $p \in R[x]$ lässt sich schreiben als

$$p = \mathcal{I}(p) \cdot p_0$$

mit einem primitiven $p_0 \in R[x]$.
(v) Ist $p \in R[x] \setminus R$ irreduzibel, so ist p insbesondere primitiv. Aus der Darstellung

$$p = \underbrace{\mathcal{I}(p)}_{\in R} \cdot \underbrace{p_0}_{\in R[x]\setminus R}$$

folgt $\mathcal{I}(p) \in R^\times$, da $p_0 \notin R^\times = R[x]^\times$. Primitivität ist also ein erster einfacher Test für Irreduzibilität. △

Satz 3.5.17 (Lemma von Gauß)**.** *Für $p, q \in R[x]$ gilt*

$$\mathcal{I}(pq) = \mathcal{I}(p) \cdot \mathcal{I}(q).$$

Insbesondere ist das Produkt von zwei primitiven Polynomen wieder primitiv.

Beweis. Wir zeigen zunächst die zweite Aussage. Schreibe

$$p = a_0 + a_1 x + \cdots + a_m x^m, \quad q = b_0 + b_1 x + \cdots + b_n x^n$$

sowie

$$pq = c_0 + c_1 x + \cdots + c_{n+m} x^{n+m}.$$

Sei nun $d \in R$ ein beliebiges Primelement. Wir wählen dann k, ℓ minimal mit $d \nmid a_k, d \nmid b_\ell$. Diese k, l existieren, da p und q primitiv sind. Es ist dann

$$c_{k+\ell} = \sum_{r+s=k+\ell} a_r b_s = a_k b_\ell + \sum_{\substack{r+s=k+\ell \\ r<k \,\vee\, s<\ell}} a_r b_s.$$

Da d prim ist, wird der Term $a_k b_\ell$ aber von d nicht geteilt, jeder andere Summand rechts jedoch schon. Damit ist d kein Teiler von $c_{k+\ell}$. Da d ein beliebiger Primfaktor war, ist pq primitiv.
Schreibe jetzt allgemeine $p, q \in R[x]$ als

$$p = \mathcal{I}(p) \cdot p_0 \quad q = \mathcal{I}(q) \cdot q_0$$

mit primitiven p_0, q_0. Dann gilt

$$\mathcal{I}(pq) = \mathcal{I}(p)\mathcal{I}(q)\mathcal{I}(p_0 q_0),$$

da man Faktoren aus R offensichtlich aus $\mathcal{I}(\cdot)$ herausziehen kann. Es ist aber, wie eben gezeigt, $\mathcal{I}(p_0 q_0) \in R^\times$ und daraus folgt die Aussage. □

Satz 3.5.18. *Sei $K = \mathrm{Quot}(R)$ und $p, q \in R[x]$. Dann gilt*

$$p \mid q \text{ in } R[x] \quad \Leftrightarrow \quad p \mid q \text{ in } K[x] \text{ und } \mathcal{I}(p) \mid \mathcal{I}(q) \text{ in } R.$$

Beweis. "⇒" ist klar mit Satz 3.5.17. Für "⇐" gelte

$$q = p \cdot h \text{ und } \mathcal{I}(q) = \mathcal{I}(p) \cdot a$$

für ein $h \in K[x]$ und ein $a \in R$. Nach Ausklammern des Hauptnenners der Koeffizienten von h und des Inhalts über R können wir

$$h = \frac{b}{c} \cdot h_0$$

mit $b, c \in R$ und $h_0 \in R[x]$ primitiv schreiben. Dann gilt

$$\mathcal{I}(p)p_0 \cdot \frac{b}{c} h_0 = ph = q = \mathcal{I}(q)q_0 = a\mathcal{I}(p)q_0$$

und nach Multiplikation mit c sowie Kürzen von $\mathcal{I}(p)$ also

$$b \cdot p_0 h_0 = ac \cdot q_0.$$

Nach Anwendung von $\mathcal{I}(\cdot)$ auf beide Seiten und Multiplikation mit $\mathcal{I}(p_0 h_0)^{-1}$ (beachte dazu Satz 3.5.17) sehen wir, dass $c \mid b$ in R gilt, also $\frac{b}{c} \in R$ und damit $h \in R[x]$. Also gilt $p \mid q$ in $R[x]$. □

Korollar 3.5.19. *Sei $K = \mathrm{Quot}(R)$, $a \in R$ und $p \in R[x] \setminus R$.*
(i) Ist a irreduzibel in R, so auch in $R[x]$.
(ii) Ist p irreduzibel in $R[x]$, so auch in $K[x]$.
(iii) Ist p primitiv in $R[x]$ und irreduzibel in $K[x]$, so ist p auch irreduzibel in $R[x]$.

Beweis. (i) ist klar (aufgrund der Nullteilerfreiheit von R). Für (ii) sei $p = qh$ mit $q, h \in K[x]$. Dabei können wir $q \in R[x]$ annehmen (indem wir q mit dem Hauptnenner seiner Koeffizienten multiplizieren und h dadurch teilen). Ebenso können wir q als primitiv in $R[x]$ annehmen. Dann gilt $\mathcal{I}(q) \in R^\times$ und damit natürlich $\mathcal{I}(q) \mid \mathcal{I}(p)$ in R. Nach Satz 3.5.18 gilt dann $q \mid p$ schon in $R[x]$ und aus der Irreduzibilität folgt $q \in R[x]^\times \subseteq K[x]^\times$ oder $q \sim p$ in $R[x]$ und damit auch $q \sim p \in K[x]$. Also ist p irreduzibel in $K[x]$.
Für (iii) gelte $q \mid p$ in $R[x]$. Wir müssen $q \in R^\times$ oder $q \sim p$ in $R[x]$ zeigen. Es gilt nach Satz 3.5.18

$$q \mid p \text{ in } K[x] \quad \text{und} \quad \mathcal{I}(q) \mid \mathcal{I}(p) \in R^\times$$

Aus der ersten Bedingung (und der Irreduzibilität von p in $K[x]$) folgt

$$\deg(q) = 0 \text{ oder } \deg(q) = \deg(p).$$

Aus der zweiten Bedingung folgt direkt $\mathcal{I}(q) \in R^\times$. Damit gilt im Fall $\deg(q) = 0$ schon $q \in R^\times$. Im Fall $\deg(q) = \deg(p)$ gilt $aq = p$ für ein $a \in R$ und nach Anwenden von $\mathcal{I}(\cdot)$ folgt aus der Primitivität von p, q dann $a \in R^\times$, also $q \sim p$. Somit ist p irreduzibel in $R[x]$. □

Beispiel 3.5.20. $p = 1 + x + x^2$ ist irreduzibel in $\mathbb{Z}[x]$. Wenn nämlich $p = qh$ eine Zerlegung ist und q etwa Grad 2 hätte, so müsste $h \in \mathbb{Z}$ gelten und mit Vergleich des konstanten Koeffizienten also o.B.d.A. $h = 1 \in \mathbb{Z}^\times$. Also können wir $\deg(q) = \deg(h) = 1$ annehmen und wiederum mit Vergleich des konstanten Koeffizienten $q = 1 + ax, h = 1 + bx$. Nach Ausmultiplizieren und Koeffizientenvergleich erhalten wir $a + b = 1, ab = 1$, was in $\mathbb{Z}$ offensichtlich nicht möglich ist. Also ist p auch irreduzibel in $\mathbb{Q}[x]$. Die Irreduzibilität in $\mathbb{Q}[x]$ direkt zu zeigen wäre etwas schwieriger gewesen. △

Es gibt nun außer $\mathbb{Z}, K[x]$ und $\mathbb{Z}[i]$ noch viel mehr faktorielle Ringe. Zum Beispiel $\mathbb{Z}[x_1, \ldots, x_n], K[x_1, \ldots, x_n]$ und $\mathbb{Z}[i][x_1, \ldots, x_n]$:

Satz 3.5.21 (Satz von Gauß)**.** *Ist R faktoriell, so auch $R[x]$.*

Beweis. Zunächst zeigen wir, dass in $R[x]$ keine echten unendlichen Teilerketten existieren können. Für eine Teilerkette

$$p_1, p_2, \ldots, p_n, \ldots$$

in $R[x]$ muss aber

$$\deg(p_1) \geq \deg(p_2) \geq \cdots \geq \deg(p_n) \geq \cdots$$

gelten und weiter ist nach Satz 3.5.18

$$\mathcal{I}(p_1), \mathcal{I}(p_2), \ldots, \mathcal{I}(p_n), \ldots$$

eine Teilerkette in R. Die Ungleichungskette der Grade wird offensichtlich irgendwann stationär. Nach Bemerkung 3.5.8 wird auch die Teilerkette der Inhalte irgendwann stationär. Das impliziert aber $p_n \sim p_m$ in $R[x]$ für groß genügende n, m, d.h. die Teilerkette ist nicht echt.
Nach Lemma 3.5.5 gibt es in $R[x]$ also immer Zerlegungen in irreduzible Elemente. Nun müssen wir nur noch zeigen, dass irreduzible Elemente prim sind.
Sei also $p \in R[x]$ irreduzibel. Es gelte $p \mid qh$ in $R[x]$. Dann gilt insbesondere $p \mid qh$ in $K[x]$. Falls $p \in R[x] \setminus R$, ist p nach Korollar 3.5.19 irreduzibel in $K[x]$ und der Hauptidealring $K[x]$ ist faktoriell (Satz 3.5.11). Deshalb ist p prim in $K[x]$ und es folgt o.B.d.A. $p \mid q$ in $K[x]$. Dieselbe Schlussfolgerung stimmt erst recht, wenn $p \in R$, da dann $p \in K^\times$. Nun gilt in R aber auch $\mathcal{I}(p) \mid \mathcal{I}(q)$ und mit Satz 3.5.18 folgt $p \mid q$ in $R[x]$. Also ist p prim. □

Satz 3.5.22 (Eisenstein-Kriterium). *Sei R ein faktorieller Ring, $a \in R$ prim und $p = c_0 + c_1 x + \cdots + c_d x^d \in R[x]$ primitiv. In R gelte*

$$a \mid c_i \text{ für } i = 0, \ldots, d-1 \quad \text{und} \quad a^2 \nmid c_0.$$

Dann ist p irreduzibel in $R[x]$.

Beweis. Es gelte $p = qh$ mit $q, h \in R[x]$. Schreibe

$$q = q_0 + q_1 x + \cdots + q_m x^m, \quad h = h_0 + h_1 x + \cdots + h_n x^n$$

mit $0 \leq m, n \leq d$ und $m + n = d$. Es gilt dann $c_0 = q_0 h_0$ und wegen $a^2 \nmid c_0$ folgt o.B.d.A. $a \nmid q_0$. Da a prim ist, folgt aus $a \mid c_0 = q_0 h_0$ dann $a \mid h_0$.
Da p primitiv ist, muss $a \nmid c_d$ gelten. Wegen $c_d = q_m h_n$ folgt daraus $a \nmid h_n$. Sei nun $k \leq n$ minimal mit $a \nmid h_k$. Dann ist

$$c_k = \sum_{i+j=k} q_i h_j = \underbrace{q_0 h_k}_{a \nmid} + \underbrace{q_1 h_{k-1} + \cdots}_{a \mid}$$

und daraus folgt $a \nmid c_k$. Das impliziert $d = k = n$ und $m = 0$, also $q \in R$. Aus der Primitivität von p folgt damit direkt $q \in R^\times = R[x]^\times$. □

Beispiel 3.5.23. (i) Das Polynom $p = x^3 + 4x^2 + 2x - 2 \in \mathbb{Z}[x]$ ist irreduzibel. (ii) Für eine Primzahl $d \geq 2$ betrachte $p = x^d - 1 \in \mathbb{Z}[x]$. Offensichtlich hat p die Nullstelle 1 und ist nach Satz 3.1.15 deshalb nicht irreduzibel. In der Tat gilt

$$p = (x-1)(1 + x + x^2 + \cdots + x^{d-1}),$$

wie man mit einem Teleskop-Argument sofort sieht. Wir nennen

$$\Phi_d := 1 + x + x^2 + \cdots + x^{d-1} \in \mathbb{Z}[x]$$

das d-**te Kreisteilungspolynom**. Es gilt

$$\begin{aligned} x \cdot \Phi_d(x+1) &= p(x+1) \\ &= (x+1)^d - 1 \\ &= x^d + \binom{d}{1} x^{d-1} + \binom{d}{2} x^{d-2} + \cdots + \binom{d}{d-1} x, \end{aligned}$$

also

$$\Phi_d(x+1) = x^{d-1} + \binom{d}{1} x^{d-2} + \cdots + \binom{d}{d-2} x + \binom{d}{d-1}.$$

Wir können nun das Eisenstein-Kriterium mit $a = d$ auf $\Phi_d(x+1)$ anwenden. Für eine Primzahl d gilt

$$d \mid \binom{d}{i}$$

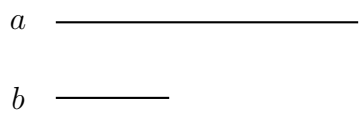
für all $i = 1, \ldots, d-1$ und offensichtlich gilt

$$d^2 \nmid \binom{d}{d-1} = d.$$

Also ist $\Phi_d(x+1)$ irreduzibel und, da die Transformation $q \mapsto q(x-1)$ ein Ringisomorphismus von $\mathbb{Z}[x]$ ist, damit auch Φ_d selbst. △

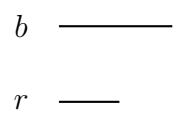
3.6 Euklidische Ringe

Der Euklidische Algorithmus war ursprünglich eine geometrische Methode der Griechen, um das Längenverhältnis zweier Strecken zu bestimmen. Dabei gingen sie wie folgt vor. Gegeben seien zwei Strecken a und b:

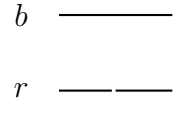


Im ersten Schritt wird die Strecke b so oft wie möglich voll in a abgetragen. Der Rest wird mit r bezeichnet. Es handelt sich dabei also genau um Teilung mit Rest:

Da r kürzer als b ist, kann die Prozedur nun mit b anstelle von a und r anstelle von b wiederholt werden:



Wenn die Prozedur nach endlich vielen Schritten aufgeht, haben wir eine Einheit gefunden, in der wir sowohl a als auch b ausdrücken können. Es wird also ein gemeinsamer Teiler beider Strecken produziert. Hier zum Beispiel nehmen wir an dass r genau 2 mal in b passt:



Es ist also $b = 2r$, und weil ursprünglich $a = 2b + r$ galt, finden wir $a = 5r$. In der Einheit r lässt sich also sowohl a als auch b ganzahlig ausdrücken, und das Verhältnis von a zu b war also genau 5 zu 2. Im Allgemeinen wird die Prozedur mehr als zwei Schritte erfordern. Trotzdem kann man durch Rückeinsetzung die ursprünglichen Strecken in der letzten erhaltenen Strecke ausdrücken.
Dieser Prozess ist nun auch deutlich abstrakter algebraisch möglich. Dazu benötigt man einen Ring, in dem Teilung mit Rest sinnvoll möglich ist.

Definition 3.6.1. Ein **euklidischer Ring** ist ein kommutativer nullteilerfreier Ring R, zusammen mit einer **Gradfunktion**

$$g\colon R \setminus \{0\} \to \mathbb{N},$$

so dass für alle $a, b \in R, b \neq 0$ Elemente $r, s \in R$ existieren mit

$$a = sb + r$$

wobei entweder $r = 0$ oder $g(r) < g(b)$ gilt. △

Beispiel 3.6.2. (i) $\mathbb{Z}$ ist ein euklidischer Ring, wobei die Gradfunktion die Betragsfunktion ist.
(ii) Der Polynomring $k[x]$ über einem Körper k ist ein euklidischer Ring mit $g(p) := \deg(p)$ für Polynome p. Man überlegt sich leicht, dass die gewünschte Division mit Rest für Polynome immer möglich ist. Dabei muss man verwenden, dass durch die Koeffizienten der Polynome geteilt werden kann, also die Körpereigenschaft von k.
(iii) Der Ring $\mathbb{Z}[i]$ der ganzen Gaußschen Zahlen ist ein euklidischer Ring, wobei der Betrag komplexer Zahlen als Gradfunktion dient (vergleiche Beispiel 3.2.6). △

Lemma 3.6.3. *Jeder euklidische Ring ist ein Hauptidealring, und damit insbesondere faktoriell.*

Beweis. Man wiederholt wie in Beispiel 3.2.6 einfach den Beweis von Satz 3.2.3 oder Lemma 2.1.5. □

Algorithmus 3.6.4 (Euklidischer Algorithmus)**.** Sei R ein euklidischer Ring mit Gradfunktion g. Seien $a, b \in R$ gegeben. Der euklidische Algorithmus läuft folgendermaßen ab:
(i) Gilt $b = 0$, so wird a als Ergebnis ausgegeben und der Algorithmus endet.
(ii) Falls $b \neq 0$, berechne

$$a = sb + r \text{ mit } r = 0 \text{ oder } g(r) < g(b).$$

Ersetze a durch b, b durch r und starte erneut bei (i). △

Satz 3.6.5. *Der euklidische Algorithmus endet nach endlich vielen Schritten und gibt* $\mathrm{ggT}(a, b)$ *als Ergebnis aus.*

Beweis. In jedem Schritt vom Typ (ii) wird $g(r) \in \mathbb{N}$ echt kleiner, also bricht der Algorithmus nach endlich vielen Schritten ab. An der Gleichung

$$a = sb + r$$

sieht man außerdem unmittelbar

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

Gilt im letzten Schritt nun also $r = 0$, d.h. $a = sb$, so folgt

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

und das ist genau die Ausgabe des euklidischen Algorithmus (im letzten Schritt wird a nochmals durch b ersetzt). □

Bemerkung 3.6.6. Merkt man sich alle Rechenschritte im euklidischen Algorithmus, so bekommt man Elemente $r, s \in R$ mit

$$\mathrm{ggT}(a,b) = ra + sb.$$

Dazu löst man alle enstandenen Gleichungen jeweils nach dem Rest auf, und ersetzt iterativ vom vorletzten Schritt an die Reste durcheinander. △

Beispiel 3.6.7. (*i*) Wir berechnen $\mathrm{ggT}(280, 63)$ in $\mathbb{Z}$. Der euklidische Algorithmus läuft folgendermaßen ab:

$$\begin{aligned} 280 &= 4 \cdot 63 + 28 \\ 63 &= 2 \cdot 28 + 7 \\ 28 &= 4 \cdot 7 + 0. \end{aligned}$$

Also gilt $\mathrm{ggT}(280, 63) = 7$. Durch Rückwärtsauflösen der Gleichungen erhält man

$$\begin{aligned} 7 &= 63 - 2 \cdot 28 \\ &= 63 - 2 \cdot (280 - 4 \cdot 63) \\ &= -2 \cdot 280 + 9 \cdot 63. \end{aligned}$$

(*ii*) Wir berechnen $\mathrm{ggT}(t^3 + t^2 + 1, t^2 + 1)$ in $\mathbb{Q}[t]$:

$$\begin{aligned} t^3 + t^2 + 1 &= (t+1) \cdot (t^2+1) - t \\ t^2 + 1 &= (-t) \cdot (-t) + 1 \\ (-t) &= (-t) \cdot 1 + 0. \end{aligned}$$

Also gilt $\mathrm{ggT}(t^3 + t^2 + 1, t^2 + 1) = 1$ und

$$\begin{aligned} 1 &= (t^2+1) + t \cdot (-t) \\ &= (t^2+1) + t \cdot ((t^3 + t^2 + 1) - (t+1)(t^2+1)) \\ &= t \cdot (t^3 + t^2 + 1) - (t^2 + t - 1) \cdot (t^2 + 1). \end{aligned}$$

△

Kapitel 4

Körper

In diesem Kapitel werden wir fast alle in der Einleitung genannten Probleme lösen. Dazu studieren wir Körper und ihre Eigenschaften.

4.1 Grundlagen

Definition 4.1.1. (i) Ein **Körper** ist ein kommutativer Ring K mit

$$K^\times = K \setminus \{0\}.$$

(ii) Ein **Körperhomomorphismus** ist ein Ringhomomorphismus zwischen Körpern.
(iii) Eine **Körpererweiterung** ist eine Inklusion $k \subseteq K$, wobei k ein Teilring von K und selbst ein Körper ist. Dabei heißt k **Teilkörper** von K und K **Oberkörper** von k. Statt $k \subseteq K$ schreibt man manchmal auch K/k. Dies ist nicht mit einer Restklassenkonstruktion zu verwechseln. △

Bemerkung/Beispiel 4.1.2. (i) $\mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ sind Körper. Also ist beispielsweise $\mathbb{Q} \subseteq \mathbb{R}$ eine Körpererweiterung.
(ii) Für eine Primzahl p ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper mit p Elementen.
(iii) Für einen Integritätsbereich R ist $\mathrm{Quot}(R)$ ein Körper. Ein Beispiel dafür ist

$$K(x_1, \ldots, x_n) = \mathrm{Quot}\left(K[x_1, \ldots, x_n]\right) = \left\{ \frac{p}{q} \mid p, q \in K[x_1, \ldots, x_n], q \neq 0 \right\}.$$

(iv) Ist $k \subseteq K$ eine Körpererweiterung, so ist insbesondere K ein k-Vektorraum. Als Skalarmultiplikation verwendet man einfach die eingeschränkte Körpermul-

tiplikation

$$\cdot\colon k \times K \to K$$

und rechnet alle Axiome eines Vektorraums nach. △

Konstruktion 4.1.3. Für einen Körper K betrachten wir den (einzigen) Ringhomomorphismus:

$$\begin{aligned} \iota\colon \mathbb{Z} &\to K \\ z &\mapsto \underbrace{1 + \cdots + 1}_{z \text{ mal}}. \end{aligned}$$

Es ist $\ker(\iota)$ ein Ideal in $\mathbb{Z}$ und nach Lemma 3.1.5 (iv) also von der Gestalt $\ker(\iota) = n\mathbb{Z}$ für ein $n \in \mathbb{Z}$. Nach dem Homomorphiesatz gibt es einen Isomorphismus

$$\mathbb{Z}/\ker(\iota) \cong \iota(\mathbb{Z}) \subseteq K.$$

Da K als Körper nullteilerfrei ist, muss auch $\mathbb{Z}/\ker(\iota)$ nullteilerfrei sein. Nach Satz 3.3.4 ist $\ker(\iota)$ damit ein Primideal, d.h. n muss eine Primzahl oder 0 sein. Im Fall $\ker(\iota) = \{0\}$ ist ι injektiv und induziert nach Proposition 3.4.4 einen injektiven Homomorphismus von $\mathbb{Q}$ nach K. Im Fall $\ker(\iota) = (p)$ gilt mit dem Homomorphiesatz $\iota(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$ und das ist bereits ein Körper. Also enthält jeder Körper entweder $\mathbb{Q}$ oder $\mathbb{Z}/p\mathbb{Z}$ als Teilkörper. Wir bezeichnen ab sofort manchmal $\mathbb{Z}/p\mathbb{Z}$ mit $\mathbb{F}_p$ und $\mathbb{Q}$ mit $\mathbb{F}_0$. △

Definition 4.1.4. Sei K ein Körper und $\iota\colon \mathbb{Z} \to K$ wie oben.
(i) Die Zahl p mit $\ker(\iota) = (p)$ heißt die **Charakteristik** des Körpers K. Sie wird auch mit $\mathrm{char}(K)$ bezeichnet.
(ii) Der Körper $\mathrm{Quot}\,(\iota(\mathbb{Z}))$ heißt **Primkörper** von K. Es ist offensichtlich der kleinste Teilkörper von K. △

Bemerkung/Beispiel 4.1.5. (i) Die Charakteristik von $\mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ ist 0. Die Charakteristik des Körpers $\mathbb{Z}/p\mathbb{Z}$ ist p.
(ii) Hat K Charakteristik $p > 0$, so gilt für alle $a \in K$

$$\underbrace{a + \cdots + a}_{p \text{ mal}} = (\underbrace{1 + \cdots + 1}_{p \text{ mal}}) \cdot a = 0 \cdot a = 0.$$

(iii) Ist $\varphi\colon K \to L$ ein Ringhomomorphismus zwischen Körpern, so gilt $\mathrm{char}(K) = \mathrm{char}(L)$. Ringhomomorphismen bilden nämlich 1 auf 1 ab und sind zwischen Körpern automatisch injektiv. Also erhält sich die Charakteristik unter Körpererweiterungen. △

Lemma 4.1.6. *Ist K ein Körper mit $\mathrm{char}(K) = p > 0$, so ist die Abbildung*

$$\begin{aligned} \rho\colon K &\to K \\ a &\mapsto a^p \end{aligned}$$

ein (injektiver) Ringhomomorphismus. Ist K endlich, so ist ρ bijektiv und wird **Frobenius-Automorphismus** *von K genannt.*

Beweis. Offensichtlich ist ρ multiplikativ und bildet 1 auf 1 ab. Für die Additivität berechnet man

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \cdots + \binom{p}{p-1} ab^{p-1} + b^p$$

und beachtet, dass alle auftretenden Koeffizienten $\binom{p}{i}$ Vielfache von p sind. Nach Bemerkung 4.1.5 (ii) verschwinden in K also alle Zwischenterme. Ringhomomorphismen zwischen Körpern sind automatisch injektiv und damit im endlichen Fall auch bijektiv. □

Definition 4.1.7. Seien $k \subseteq K$ wobei K ein Körper und k ein Teilring ist, sowie $A \subseteq K$ eine Teilmenge.
(i) Die Menge

$$k[A] := \bigcap_{\substack{R \subseteq K \text{ Teilring} \\ A \cup k \subseteq R}} R$$

ist offensichtlich der kleinste Teilring von K, der A und k enthält. Er heißt der von A in K über k **erzeugte Teilring**.
(ii) Die Menge

$$k(A) := \bigcap_{\substack{L \subseteq K \text{ Teilkörper} \\ A \cup k \subseteq L}} L$$

ist offensichtlich der kleinste Teilkörper von K, der A und k enthält. Er heißt der von A in K über k **erzeugte Teilkörper**. △

Bemerkung/Beispiel 4.1.8. (i) Ist $A = \{a_1, \ldots, a_n\}$ endlich, so gilt

$$k[A] = k[a_1, \ldots, a_n] = \{p(a_1, \ldots, a_n) \mid p \in k[x_1, \ldots, x_n]\}$$

und

$$\begin{aligned} k(A) &= k(a_1, \ldots, a_n) \\ &= \left\{ \frac{p(a_1, \ldots, a_n)}{q(a_1, \ldots, a_n)} \mid p, q \in k[x_1, \ldots, x_n], q(a_1, \ldots, a_n) \neq 0 \right\} \\ &= \operatorname{Quot}(k[A]) . \end{aligned}$$

(*ii*) Es gilt $k[A \cup B] = (k[A])[B]$ und $k(A \cup B) = (k(A))(B)$.
(*iii*) Es gilt beispielsweise

$$\mathbb{Q}[\sqrt{2}] = \left\{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \right\} \subseteq \mathbb{R}.$$

Hier ist $\mathbb{Q}[\sqrt{2}]$ sogar schon ein Körper, also gilt

$$\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2}). \qquad \triangle$$

Wenn ein Oberkörper von k schon geeignete Elemente $a_1, \ldots, a_n$ enthält, kann man $k(a_1, \ldots, a_n)$ wie eben definieren. Andererseits kann es sein, dass die Existenz eines solchen Oberkörpers noch gar nicht sichergestellt ist. Dann verwendet man die folgende Konstruktion:

Konstruktion 4.1.9. Sei k ein Körper und $p \in k[x]$ irreduzibel. Dann ist $(p) \lhd k[x]$ ein Primideal und nach Bemerkung 3.3.2 (ii) deshalb sogar maximal. Also ist $K := k[x]/(p)$ nach Satz 3.3.4 ein Körper. Die Einschränkung der kanonischen Projektion π

$$\begin{aligned} \pi \colon k &\to k[x]/(p) \\ a &\mapsto a + (p) \end{aligned}$$

ist injektiv, da (p) als echtes Ideal keine Einheiten enthält. Damit können wir $k \subseteq K$ auffassen. Mit $p = \sum_{i=1}^{d} c_i x^i$ und $\overline{x} := \pi(x) = x + (p) \in K$ erhalten wir in K

$$p(\overline{x}) = \sum_i \pi(c_i)\pi(x)^i = \pi(p) = 0.$$

Also haben wir eine Körpererweiterung von k konstruiert, in der p eine Nullstelle hat. $\triangle$

Beispiel 4.1.10. (*i*) Man sieht leicht, dass zum Beispiel $\mathbb{C}$ gerade mit $p = x^2 + 1$ aus $\mathbb{R}$ hervorgeht.
(*ii*) Kennt man $\mathbb{R}$ theoretisch noch nicht, so kann man den Körper $\mathbb{Q}(\sqrt{2})$ auch mit $p = x^2 - 2 \in \mathbb{Q}[x]$ wie oben konstruieren. $\triangle$

4.2 Algebraische Erweiterungen und Körpergrad

Sei ab jetzt stets $k \subseteq K$ eine Körpererweiterung.

Definition 4.2.1. (i) Ein Element $a \in K$ heißt **algebraisch über** k, falls es ein $0 \neq p \in k[x]$ gibt mit

$$p(a) = 0.$$

(ii) Ist a nicht algebraisch über k, so heißt a **transzendent** über k.
(iii) Die Körpererweiterung $k \subseteq K$ heißt **algebraisch**, falls jedes Element $a \in K$ algebraisch über k ist. △

Bemerkung/Beispiel 4.2.2. (i) Das Element $i \in \mathbb{C}$ ist algebraisch über $\mathbb{R}$ (sogar über $\mathbb{Q}$). Es ist Nullstelle des Polynoms $p = x^2+1$. Ebenso ist $\sqrt{2} \in \mathbb{R}$ algebraisch über $\mathbb{Q}$, da es Nullstelle von $p = x^2 - 2$ ist.
(ii) Die Variable $x \in K = k(x) = \mathrm{Quot}\,(k[x])$ ist transzendent über k.
(iii) Das Element $\pi \in \mathbb{R}$ ist transzendent über $\mathbb{Q}$. Das ist allerdings sehr schwer zu zeigen!
(iv) Jedes Element $a \in k$ ist algebraisch über k. Es ist Nullstelle von $p = x - a \in k[x]$. △

Definition 4.2.3. (i) Für eine Körpererweiterung $k \subseteq K$ nennen wir die k-Vektorraumdimension

$$\dim_k(K) =: [K : k]$$

den **Grad** der Körpererweiterung.
(ii) Wir nennen die Körpererweiterung $k \subseteq K$ **endlich**, wenn $[K : k] < \infty$ gilt. △

Beispiel 4.2.4. Es gilt (Übungsaufgabe)

$$[\mathbb{C} : \mathbb{R}] = 2, \quad [\mathbb{R} : \mathbb{Q}] = \infty, \quad \left[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right] = 2. \qquad \triangle$$

Korollar 4.2.5. *Sei K ein endlicher Körper. Dann gilt $\#K = p^r$ für eine Primzahl p und ein $r \geq 1$.*

Beweis. K muss als endlicher Körper eine Charakteristik $p > 0$ haben. Also ist $\mathbb{F}_p \subseteq K$ eine Körpererweiterung. Es gilt

$$[K : \mathbb{F}_p] = r$$

für ein $r \in \mathbb{N}$. Die Elemente von K sind also gerade die $\mathbb{F}_p$-Linearkombinationen von r Basisvektoren und davon gibt es genau p^r viele. □

Beispiel 4.2.6. Es kann keinen Körper mit 6 Elementen geben, da 6 keine Primzahlpotenz ist. △

Satz 4.2.7 (Gradformel)**.** *Für Körper $k \subseteq K \subseteq L$ gilt*

$$[L : k] = [L : K] \cdot [K : k] .$$

Beweis. Sei $(v_i)_{i\in I}$ eine K-Basis von L und $(w_j)_{j\in J}$ eine k-Basis von K. Jedes Element $a \in L$ hat eine (endliche) Summendarstellung

$$a = \sum_{i\in I} b_i v_i$$

mit $b_i \in K$. Jedes der b_i hat wiederum eine Darstellung

$$b_i = \sum_{j\in J} c_{ij} w_j$$

mit $c_{ij} \in k$. Daraus erhält man in L

$$a = \sum_{i\in I} \sum_{j\in J} c_{ij} w_j v_i = \sum_{(j,i)\in J\times I} c_{ij} \cdot w_j v_i,$$

also ist $\mathcal{B} := (w_j v_i)_{(j,i)\in J\times I}$ ein Erzeugendensystem von L als k-Vektorraum. Es gelte nun für gewisse $c_{ij} \in k$ in L

$$0 = \sum_{(j,i)\in J\times I} c_{ij} w_j v_i = \sum_{i\in I} \underbrace{\left(\sum_{j\in J} c_{ij} w_j \right)}_{\in K} v_i.$$

Aus der linearen Unabhängigkeit der v_i über K folgt $\sum_{j\in J} c_{ij} w_j = 0$ für alle $i \in I$ und aus der linearen Unabhängigkeit der w_j über k dann $c_{ij} = 0$ für alle i, j. Damit ist $\mathcal{B}$ eine Basis von L als k-Vektorraum und das beweist die Aussage, denn $\#\mathcal{B} = \#I \cdot \#J$. □

Beispiel 4.2.8. Es gilt (Übungsaufgabe)

$$\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3} \right) \right] : \mathbb{Q}] = 4.$$ △

Der folgende Satz zeigt, dass die Begriffe von algebraischer und endlicher Körpererweiterung eng zusammenhängen:

Satz 4.2.9. *Seien $k \subseteq K \subseteq L$ Körper.*

(i) Ist die Erweiterung $k \subseteq K$ endlich, so auch algebraisch.

(ii) Für $a \in K$ sind äquivalent:

(1) a ist algebraisch über k,

(2) $k[a] = k(a)$,

(3) $k(a)$ ist endlich über k,

(4) $k(a)$ ist algebraisch über k.

(iii) Sind $k \subseteq K$ und $K \subseteq L$ algebraisch, so auch $k \subseteq L$.

(iv) Jede von endlich vielen algebraischen Elementen erzeugte Erweiterung ist endlich (und damit algebraisch).

(v) Die Menge $\{a \in K \mid a$ algebraisch über $k\}$ ist ein Zwischenkörper von k und K.

Beweis. (i): Wenn K ein endlich-dimensionaler k-Vektorraum ist, können für $a \in K$ die Elemente

$$1, a, a^2, \ldots, a^n, \ldots$$

Dim(K) = d, linearkombination hat d+1 elemente

nicht alle linear unabhängig über k sein. Also gibt es eine Gleichung

$$0 = \sum_{i=1}^{d} c_i a^i$$

mit gewissen $c_i \in k$, nicht alle 0. Das bedeutet aber gerade, dass a algebraisch über k ist.
(ii): "$(1) \Rightarrow (2)$": Wir betrachten den Einsetzungshomomorphismus

$$\begin{aligned} \varphi\colon k[x] &\to K \\ p &\mapsto p(a) \end{aligned}$$

und erhalten aus dem Homomorphiesatz

$$k[x]/\ker(\varphi) \cong k[a].$$

Da $k[a]$ als Teilring des Körpers K nullteilerfrei ist, ist $\ker(\varphi)$ ein Primideal, und nach Voraussetzung gilt $\ker(\varphi) \neq \{0\}$. Im Hauptidealring $k[x]$ ist $\ker(\varphi)$ also

sogar maximal, also ist $k[a] \cong k[x]/\ker(\varphi)$ schon ein Körper. Also gilt $k[a] = k(a)$.
"$(2) \Rightarrow (1)$": Es gelte o.B.d.A $a \neq 0$. Dann ist $a^{-1} \in k(a) = k[a]$, also gibt es ein $p \in k[x]$ mit $a^{-1} = p(a)$. Dann gilt aber $a \cdot p(a) - 1 = 0$, also ist a Nullstelle des Polynoms $xp - 1 \in k[x]$ und damit algebraisch über k.
"$(1)\&(2) \Rightarrow (3)$": Da a algebraisch über k ist, gibt es eine Gleichung

$$c_0 + c_1 a + \cdots + c_d a^d = 0$$

mit $c_i \in k, c_d \neq 0$. Das bedeutet Iterativ umschreiben dann kann man alle a, ausdrücken

$$a^d = -\frac{c_0}{c_d} - \frac{c_1}{c_d} a - \cdots - \frac{c_{d-1}}{c_d} a^{d-1},$$

also wird $k(a) = k[a]$ schon von den Elementen $1, a, a^2, \ldots, a^{d-1}$ als k-Vektorraum aufgespannt. Daraus folgt die Endlichkeit.
"$(3) \Rightarrow (4)$" folgt aus (i).
"$(4) \Rightarrow (1)$" ist trivial.
Für (iii) sei $a \in L$ fest gewählt. Dann ist a algebraisch über K und damit schon über $k(b_1, \ldots, b_n)$ für gewisse $b_i \in K$ (z.B. den Koeffizienten eines Polynoms, welches a als Nullstelle hat). Die b_i wiederum sind alle algebraisch über k. Wir betrachten nun die Körperkette

$$k \subseteq k(b_1) \subseteq k(b_1, b_2) \subseteq \cdots \subseteq k(b_1, \ldots, b_n) \subseteq k(b_1, \ldots, b_n, a),$$

in der jeder Schritt durch Adjunktion eines algebraischen Elements entsteht. Nach (ii) ist jede einzelne Erweiterung endlich und mit der Gradformel damit auch die ganze Erweiterung $k \subseteq k(b_1, \ldots, b_b, a)$. Nach (i) ist sie damit algebraisch und insbesondere ist a algebraisch über k.
Für (iv) sei $K = k(a_1, \ldots, a_n)$ erzeugt von den über k algebraischen Elementen $a_1, \ldots, a_n$. Wieder ist jeder Schritt in der Körperkette

$$k \subseteq k(a_1) \subseteq k(a_1, a_2) \subseteq \cdots \subseteq k(a_1, \ldots, a_n)$$

nach (ii) endlich und mit der Gradformel ist die ganze Erweiterung endlich.
Für (v) sehen wir, dass mit über k algebraischen Elementen $a, b \in K$ die Elemente $a + b, a \cdot b, a^{-1} \in k(a, b)$ ebenfalls algebraisch über k sein müssen (mit (iv)). □

Beispiel 4.2.10. (*i*) Das Element $\sqrt{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$. Damit gilt $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$ und jedes Element aus diesem Körper erfüllt eine Polynomgleichung über $\mathbb{Q}$.
(*ii*) Die Menge

$$\overline{\mathbb{Q}} := \{a \in \mathbb{C} \mid a \text{ algebraisch über } \mathbb{Q}\}$$

ist ein Körper mit $\mathbb{Q} \subseteq \overline{\mathbb{Q}} \subseteq \mathbb{C}$. △

Konstruktion 4.2.11. Sei wieder $k \subseteq K$ eine Körpererweiterung und $a \in K$. Wir betrachten den Einsetzungshomomorphismus

$$\begin{aligned} \mathrm{e}_a \colon k[x] &\to K \\ p &\mapsto p(a). \end{aligned}$$

Laut Homomorphiesatz gilt

$$k[x]/\ker(\mathrm{e}_a) \hookrightarrow K$$

und mit Satz 3.3.4 ist $\ker(\mathrm{e}_a)$ also ein Primideal. Da $k[x]$ ein Hauptidealring ist, gilt außerdem $\ker(\mathrm{e}_a) = (p_a)$ für ein $p_a \in k[x]$. Dabei ist entweder $p_a = 0$ (im Fall, dass a transzendent über k ist) oder $\deg(p_a) > 0$ (im Fall, dass a algebraisch über k ist). Im zweiten Fall ist p_a also irreduzibel und ist p_a zusätzlich normiert (d.h. der Leitkoeffizient ist 1), so ist es eindeutig bestimmt. Aus $(p_a) = (q_a)$ folgt nämlich $p_a \sim q_a$ und aus der Normiertheit folgt dann $p_a = q_a$. Außerdem ist p_a irreduzibel in $k[x]$, da (p_a) ein Primideal ist. △

Definition 4.2.12. Sei $k \subseteq K$ Körpererweiterung und $a \in K$ algebraisch über k. Dann heißt das (eindeutig bestimmte) normierte Polynom $p_a \in k[x]$ mit

$$\ker(\mathrm{e}_a) = (p_a)$$

das **Minimalpolynom** von a über k. Wir bezeichnen es mit $\mathrm{Min}(a, k)$. △

Lemma 4.2.13. *Sei $k \subseteq K$ und $a \in K$ algebraisch über k. Dann ist $p = \mathrm{Min}(a, k)$ eindeutig bestimmt durch die folgenden Eigenschaften:*

(i) $p \in k[x]$ *ist irreduzibel und normiert.*

(ii) *Es gilt* $p(a) = 0$.

Beweis. In Konstruktion 4.2.11 haben wir schon gesehen, dass $\mathrm{Min}(a,k)$ die gewünschten Eigenschaften hat. Erfülle also umgekehrt $p \in k[x]$ die Eigenschaften und bezeichne mit p_a das Minimalpolynom von a über k. Wegen (ii) gilt $p \in \ker(\mathrm{e}_a) = (p_a)$, also $p_a \mid p$. Da p nach (i) irreduzibel ist, folgt $p_a \sim p$ und wieder aus der Normiertheit beider Polynome damit $p = p_a$. □

Beispiel 4.2.14. (i) Es gilt

$$\mathrm{Min}(\sqrt{2},\mathbb{Q}) = x^2 - 2 \text{ und } \mathrm{Min}(\sqrt[3]{2},\mathbb{Q}) = x^3 - 2.$$

Beide Polynome erfüllen jeweils die Bedingungen (i) und (ii) aus Lemma 4.2.13.
(ii)Wir betrachten $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. Dann gilt (Aufgabe 50)

$$\mathrm{Min}(\sqrt{2}+i,\mathbb{R}) = x^2 - 2\sqrt{2}x + 3 \qquad \mathrm{Min}(\sqrt{2}+i,\mathbb{Q}) = x^4 - 2x^2 + 9.$$

Also hängt das Minimalpolynom stark vom Körper k ab.
(iii) Sei p eine Primzahl und

$$a = e^{\frac{2\pi i}{p}} = \cos\left(\frac{2\pi}{p}\right) + i\sin\left(\frac{2\pi}{p}\right) \in \mathbb{C}.$$

Dann gilt

$$\mathrm{Min}\,(a,\mathbb{Q}) = \Phi_p = 1 + x + \cdots + x^{p-1},$$

das p-te Kreisteilungspolynom. Offensichtlich ist a ja eine Nullstelle von $x^p - 1$ und dieses Polynom faktorisiert

$$x^p - 1 = (x-1)\cdot\Phi_p$$

(vergleiche Beispiel 3.5.23 (ii)), wobei a keine Nullstelle von $x - 1$ ist. Also gilt $\Phi_p(a) = 0$ und Φ_p ist nach Beispiel 3.5.23 (ii) irreduzibel sowie offensichtlich normiert. △

Zur Berechnung eines Körpergrads benutzt man gewöhnlich die Dimensionsformel und/oder den folgenden Satz:

Satz 4.2.15. *Sei $k \subseteq K$ eine Körpererweiterung und $a \in K$ algebraisch über k. Dann gilt*

$$[k(a) : k] = \deg\left(\mathrm{Min}(a,k)\right).$$

Beweis. Sei $p_a = \mathrm{Min}(a,k) = c_0 + c_1 x + \cdots + c_{d-1}x^{d-1} + x^d$, also $\deg(p_a) = d$. Wegen $p_a(a) = 0$ gilt

$$a^d = -c_0 - c_1 a - \cdots - c_{d-1}a^{d-1}.$$

Also ist $1, a, \ldots, a^{d-1}$ ein Erzeugendensystem des k-Vektorraums $k[a] = k(a)$. Wir zeigen nun die lineare Unabhängigkeit. Gelte also

$$0 = b_0 + b_1 a + \cdots + b_{d-1}a^{d-1}$$

für gewisse $b_0, \ldots, b_{d-1} \in k$. Das bedeutet aber gerade, dass für das Polynom $q = b_0 + b_1 x + \cdots + b_{d-1}x^{d-1} \in k[x]$ gilt $q(a) = 0$, also $q \in (p_a)$. Wegen

$$\deg(q) \leq d - 1 < d = \deg(p_a)$$

folgt daraus aber $q = 0$, also $b_i = 0$ für alle i. Also sind $1, a, \ldots, a^{d-1}$ über k linear unabhängig. Das zeigt

$$[k(a) : k] = d = \deg(\mathrm{Min}(a,k)).$$ □

Beispiel 4.2.16. (i) Mit Satz 4.2.15 und Beispiel 4.2.14 folgt sofort

$$\Big[\mathbb{R}(\sqrt{2}+i) : \mathbb{R}\Big] = 2 \text{ und } \Big[\mathbb{Q}(\sqrt{2}+i) : \mathbb{Q}\Big] = 4.$$

Aus der zweiten Gleichung können wir auch

$$\mathbb{Q}(\sqrt{2}+i) = \mathbb{Q}(\sqrt{2}, i)$$

ablesen. Dabei ist "$\subseteq$" klar. Wenden wir nun die Gradformel auf die Kette

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, i)$$

an, sehen wir, dass $\big[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}\big] \leq 4$ gelten muss. Aus $\big[\mathbb{Q}(\sqrt{2}+i) : \mathbb{Q}\big] = 4$ folgt dann die Gleichheit.
(ii) Mit Satz 4.2.15 und Beispiel 4.2.14 folgt $\big[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\big] = 3$. △

Korollar 4.2.17. *Für jede Primzahl p gilt*

$$\Big[\mathbb{Q}\left(e^{\frac{2\pi i}{p}}\right) : \mathbb{Q}\Big] = p - 1.$$

Beweis. Klar mit Satz 4.2.15 und Beispiel 4.2.14 (iii). □

4.3 Lösung der antiken Konstruktionsprobleme

Wir erinnern nochmal an die Konstruktion mit Zirkel und Lineal. Wir starten mit einer Menge $M \subseteq \mathbb{C}$, von der wir $0, 1 \in M$ annehmen. Wir setzen $M_0 = M$ und definieren iterativ $M^{(i+1)}$ als die Vereinigung von $M^{(i)}$ mit der Menge aller Punkte, die in einem Schritt (irgendeines Typs) aus $M^{(i)}$ konstruierbar sind. Dann ist

$$\mathrm{Kon}(M) = \bigcup_{i=0}^{\infty} M_i$$

die Menge aller Elemente von $\mathbb{C}$, die man in endlich vielen Schritten mit Zirkel und Lineal aus M konstruieren kann. Wir wissen bereits, dass

$$k := \mathbb{Q}(M \cup \overline{M}) \subseteq \mathrm{Kon}(M) \subseteq \mathbb{C}$$

eine Körperkette ist. Außerdem ist $\mathrm{Kon}(M)$ abgeschlossen unter komplexer Konjugation (Satz 1.1.2).

Proposition 4.3.1. *Sei $L \subseteq \mathbb{C}$ ein unter komplexer Konjugation abgeschlossener Körper. Wenn $a \in \mathbb{C}$ in einem Schritt aus L konstruierbar ist, so gibt es ein $b \in L$ mit $a \in L(\sqrt{b})$.*

Beweis. Wir untersuchen die drei Konstruktionstypen nacheinander.
1. Fall: a entsteht durch das Schneiden zweier Geraden. Es gibt also $p_1 \neq p_2, q_1 \neq q_2 \in L$ und $r, s \in \mathbb{R}$ mit

$$a = p_1 + r(p_2 - p_1) = q_1 + s(q_2 - q_1).$$

Also gilt

$$\frac{a - p_1}{p_2 - p_1} = r = \overline{r} = \frac{\overline{a} - \overline{p}_1}{\overline{p}_2 - \overline{p}_1}$$

und damit

$$\overline{a} = (a - p_1)\frac{\overline{p}_2 - \overline{p}_1}{p_2 - p_1} + \overline{p}_1.$$

Mit den q_i erhält man die analoge Gleichung. Setzt man die beiden rechten Seiten dann gleich und löst nach a auf, erhält man $a \in L$. Man kann also $b = 1$ wählen.
2. Fall: a entsteht durch das Schneiden eines Kreises mit einer Geraden. Es gibt also $p_1 \neq p_2, q_1, q_2, q \in L$ und $r \in \mathbb{R}$ mit

$$a = p_1 + r(p_2 - p_1)$$

und

$$|a-q|^2 = |q_1-q_2|^2 = (q_1-q_2)\overline{(q_1-q_2)} \in L.$$

Setzt man die erste Gleichung in die zweite ein, ergibt sich für r eine quadratische Gleichung mit Koeffizienten aus L. Mit der Lösungsformel für quadratische Gleichungen sehen wir, dass ein $b \in L$ existiert mit $r \in L(\sqrt{b})$. Dann gilt mit der ersten Gleichung auch $a \in L(\sqrt{b})$.

3. Fall: a entsteht durch das Schneiden zweier Kreise. Es gibt also $p \neq q, p_1, p_2, q_1, q_2 \in L$ mit

$$|a-p|^2 = |p_1-p_2|^2 \text{ und } |a-q|^2 = |q_1-q_2|^2.$$

Die erste Gleichung ergibt nach Auflösung nach $\overline{a}$ gerade

$$\overline{a} = \frac{(p_1-p_2)(\overline{p}_1-\overline{p}_2)}{a-p} + \overline{p}$$

und analog

$$\overline{a} = \frac{(q_1-q_2)(\overline{q}_1-\overline{q}_2)}{a-q} + \overline{q}.$$

Nach Gleichsetzung der beiden rechten Seiten erhält man für a eine quadratische Gleichung mit Koeffizienten aus L. Wieder ergibt sich die Aussage aus der Lösungformel für quadratische Gleichungen. □

Satz 4.3.2. *Jedes $a \in \mathrm{Kon}(M)$ ist algebraisch über $k = \mathbb{Q}(M \cup \overline{M})$. Es gilt stets*

$$[k(a) : k] = 2^r$$

für ein $r \in \mathbb{N}$.

Beweis. Um a zu erhalten, konstruiert man ausgehend von M eine endliche Folge von Punkten $a_1, a_2, \ldots, a_n, a$. Nach Proposition 4.3.1 gilt also

$$[k(a_1) : k] \leq 2.$$

Konjugiert man die Koeffizienten von $\mathrm{Min}(a_1, k)$, erhält man eine polynomiale Gleichung für $\overline{a}_1$ über k (k ist abgeschlossen unter komplexer Konjugation) und damit über $k(a_1)$. Also gilt

$$[k(a_1, \overline{a}_1) : k(a_1)] \leq 2.$$

Mit der Gradformel ist also

$$[k(a_1, \overline{a}_1) : k] = 1, 2 \text{ oder } 4.$$

Der Körper $k(a_1, \overline{a}_1)$ ist aber wieder abgeschlossen unter komplexer Konjugation und wir können iterieren. Wiederum mit der Gradformel sieht man schließlich, dass

$$[k(a_1, \overline{a}_1, \ldots, a_n, \overline{a}_n, a) : k] = 2^s$$

für ein $s \in \mathbb{N}$ gilt. Wegen

$$k \subseteq k(a) \subseteq k(a_1, \overline{a}_1, \ldots, a_n, \overline{a}_n, a)$$

und der Gradformel ist $[k(a) : k]$ ein Teiler von 2^s und damit ebenfalls eine Zweierpotenz. □

Mit dem vorangegangenen Satz können wir nun (fast) alle antiken Konstruktionsprobleme lösen.

Satz 4.3.3 (Quadratur des Kreises). *Für $M = \{0, 1\}$ gilt*

$$\sqrt{\pi} \notin \mathrm{Kon}(M).$$

Also kann man zu einem gegebenen Kreis mit Radius 1 mit Zirkel und Lineal kein Quadrat mit gleichem Flächeninhalt konstruieren.

Beweis. Es gilt $\mathbb{Q}(M \cup \overline{M}) = \mathbb{Q}$ und π ist transzendent über $\mathbb{Q}$ (ohne Beweis). Mit Satz 4.3.2 gilt also $\pi \notin \mathrm{Kon}(M)$ und damit erst recht $\sqrt{\pi} \notin \mathrm{Kon}(M)$. □

Satz 4.3.4 (Würfelverdoppelung). *Für $M = \{0, 1\}$ gilt*

$$\sqrt[3]{2} \notin \mathrm{Kon}(M).$$

Also lässt sich zu einem Würfel mit Volumen 1 mit Zirkel und Lineal kein Würfel mit Volumen 2 konstruieren.

Beweis. Es gilt $\mathbb{Q}(M \cup \overline{M}) = \mathbb{Q}$ und $\left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] = 3$ (siehe Beispiel 4.2.16 (ii)). Die Aussage folgt nun wieder mit Satz 4.3.2, da 3 keine Zweierpotenz ist. □

Satz 4.3.5 (Dreiteilung des Winkels). *Mit $M = \{0, 1, e^{\pi i/3}\}$ gilt*

$$e^{\pi i/9} \notin \mathrm{Kon}(M).$$

Also lässt sich ein Winkel von $60°$ mit Zirkel und Lineal nicht in drei gleich große Winkel aufteilen.

Beweis. Beachte zunächst, dass $M = \{0, 1\}$ als Anfangsmenge genügt, da $e^{\pi i/3}$ daraus konstruierbar ist. Wäre $e^{\pi i/9}$ nun konstruierbar aus $\mathbb{Q}$, so auch

$$a = \mathrm{Re}\left(e^{\pi i/9}\right) = \cos\left(\frac{\pi}{9}\right).$$

Es gilt aber die allgemeine trigonometrische Formel

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

und daraus erhält man

$$\mathrm{Min}(a, \mathbb{Q}) = x^3 - \frac{3}{4}x - \frac{1}{8}.$$

Die Irreduzibilität kann man direkt nachrechnen. Man kann aber auch die Transformation $x \mapsto \frac{1}{2}(x+1)$, das Eisensteinkriterium über $\mathbb{Z}$ und dann Korollar 3.5.19 (ii) verwenden. Also gilt

$$\left[\mathbb{Q}\left(\cos\left(\frac{\pi}{9}\right)\right) : \mathbb{Q}\right] = 3$$

und das ist keine Zweierpotenz. □

Satz 4.3.6 (Konstruktion regelmäßiger p-Ecke)**.** *Ist p eine Primzahl und das regelmäßige p-Eck mit Zirkel und Lineal konstruierbar, so ist $p-1$ eine Zweierpotenz. Insbesondere kann man ein regelmäßiges 7-Eck nicht mit Zirkel und Lineal konstruieren.*

Beweis. Laut Korollar 4.2.17 gilt

$$\left[\mathbb{Q}\left(e^{2\pi i/p}\right) : \mathbb{Q}\right] = p - 1.$$

Aus der Konstruierbarkeit folgt, dass dies eine Zweierpotenz sein muss. □

Für die Umkehrung des letzten Satzes siehe Korollar 4.6.12. Das einzige noch offene Problem aus der Einleitung ist nun die Frage nach der Lösbarkeit von polynomialen Gleichungen. Dieses Problem ist deutlich schwieriger als die Konstruktionsprobleme und erfordert noch mehr Theorie der Körper.

4.4 Der Zerfällungskörper und der algebraische Abschluss

Sei $k \subseteq K$ eine Körpererweiterung und $0 \neq p \in k[x]$ ein Polynom. Wir erinnern nochmal an Satz 3.1.15. Für $a \in K$ gilt

$$p(a) = 0 \Leftrightarrow (x - a) \mid p \text{ in } K[x].$$

Insbesondere hat p höchstens $\deg(p)$ viele verschiedene Nullstellen in K.

Definition 4.4.1. Sei $k \subseteq K$ eine Körpererweiterung.
(i) $p \in k[x]$ **zerfällt über** K **in Linearfaktoren**, falls $b \in k, a_1, \ldots, a_n \in K$ existieren mit

$$p = b(x - a_1)(x - a_2) \cdots (x - a_n) \in K[x].$$

(ii) K heißt **Zerfällungskörper** von p über k, falls p über K zerfällt und mit den a_i wie in (i) gilt

$$K = k(a_1, \ldots, a_n).$$

(iii) Einen Zerfällungskörper einer ganzen Familie von Polynomen über k definiert man analog. Alle Polynome der Familie müssen zerfallen und der Körper ensteht durch Adjunktion aller Nullstellen der Polynome. △

Beispiel 4.4.2. (i) Ein Zerfällungskörper von $x^2 - 2$ über $\mathbb{Q}$ ist gerade

$$\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2}).$$

Ein Zerfällungskörper von $x^2 + 1$ über $\mathbb{R}$ ist $\mathbb{C}$.
(ii) Der Körper $\mathbb{Q}(\sqrt[3]{2})$ ist kein Zerfällungskörper von $p = x^3 - 2$ über $\mathbb{Q}$. Es gilt nämlich $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ und

$$x^3 - 2 = (x - \sqrt[3]{2}) \left(x^2 + \sqrt[3]{2}x + \sqrt[3]{2}^2 \right),$$

wobei der quadratische Faktor über $\mathbb{R}$ nicht zerfällt. Es ist aber

$$K := \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$$

ein Zerfällungskörper von p über $\mathbb{Q}$. Der quadratische Faktor hat nämlich die Nullstellen

$$\lambda_{1,2} = -\frac{1}{2} \left(\sqrt[3]{2} \pm i\sqrt{3}\sqrt[3]{2} \right) \in K.$$

Außerdem gilt $K = \mathbb{Q}(\sqrt[3]{2}, \lambda_1, \lambda_2)$, wobei "$\supseteq$" schon klar ist und die andere Inklusion aus

$$i\sqrt{3} = \frac{\lambda_2 - \lambda_1}{\sqrt[3]{2}}$$

folgt. Aus der Gradformel folgt hier sofort

$$[K : \mathbb{Q}] = 6 = 3!$$

(iii) Der Zerfällungskörper von $x^d - 1$ (bzw. Φ_d) über $\mathbb{Q}$ ist $\mathbb{Q}(e^{\frac{2\pi i}{d}})$. Die Nullstellen von $x^d - 1$ in $\mathbb{C}$ sind gerade die d-ten Einheitswurzeln und $e^{\frac{2\pi i}{d}}$ erzeugt als primitive Einheitswurzel alle anderen. Falls d prim ist, gilt laut Korollar 4.2.17

$$\left[\mathbb{Q}\left(e^{\frac{2\pi i}{d}}\right) : \mathbb{Q}\right] = d - 1. \qquad \triangle$$

Lemma 4.4.3. *Sei $p \in k[x]$ und K ein Zerfällungskörper von p über k. Dann gilt*

$$[K : k] \leq \deg(p)!$$

Beweis. Aufgabe 57. □

Satz 4.4.4. *Zu jedem $p \in k[x]$ existiert ein Zerfällungskörper.*

Beweis. Es genügt zu zeigen, dass eine Körpererweiterung $k \subseteq L$ existiert, in der p eine Nullstelle hat. Nach Abspaltung von Linearfaktoren über L iterieren wir dann den Prozess und adjungieren am Schluss alle nötigen Nullstellen an k. Da jedes Polynom ein Produkt von irreduziblen Polynomen ist, können wir o.B.d.A. zusätzlich annehmen, dass p irreduzibel ist. Dann entsteht L aber gerade durch Konstruktion 4.1.9. □

Wir wollen nun die Eindeutigkeit des Zerfällungskörpers zeigen. Ein Homomorphismus $\varphi\colon k \to k'$ von Körpern setzt sich offensichtlich zu einem Ringhomomorphismus $\Phi\colon k[x] \to k'[x]$ mit $\Phi(x) = x$ fort. Für ein Polynom $p = \sum_{i=0}^{d} c_i x^i \in k[x]$ gilt dabei

$$\Phi(p) = \sum_{i=0}^{d} \varphi(c_i) x^i =: p^{(\varphi)}.$$

Die folgende Aussage ist zwar technisch, wird im Folgenden aber immer wieder benutzt werden.

Proposition 4.4.5. *Es seien $k \subseteq K$ und $k' \subseteq K'$ Körpererweiterungen sowie $\varphi\colon k \to k'$ ein Homomorphismus. Sei $a \in K$ algebraisch über k und $p = \mathrm{Min}(a,k) \in k[x]$. Dann ist die Anzahl der Homomorphismen $\psi\colon k(a) \to K'$ mit $\psi_{|k} = \varphi$ gleich der Anzahl der verschiedenen Nullstellen von $p^{(\varphi)}$ in K'.*

Beweis. Sei $\psi\colon k(a) \to K'$ eine Fortsetzung von φ. Für ein Polynom $q \in k[x]$ gilt dann

$$\psi(q(a)) = q^{(\varphi)}(\psi(a))$$

und insbesondere

$$0 = \psi(0) = \psi(p(a)) = p^{(\varphi)}(\psi(a)).$$

Daraus sehen wir zweierlei. Erstens ist ψ durch seinen Wert auf a schon eindeutig bestimmt, zweitens muss $\psi(a)$ immer eine Nullstelle von $p^{(\varphi)}$ sein. Damit gibt es höchstens so viele Abbildungen ψ wie Nullstellen von $p^{(\varphi)}$ in K'.
Sei nun $b \in K'$ eine Nullstelle von $p^{(\varphi)}$. Wir müssen noch zeigen, dass ein ψ existiert mit $\psi(a) = b$. Jedes Element von $k(a) = k[a]$ ist von der Form $q(a)$ für ein $q \in k[x]$. Wir definieren also einfach

$$\psi(q(a)) := q^{(\varphi)}(b).$$

Dabei müssen wir zunächst die Wohldefiniertheit zeigen. Seien also $q, \tilde{q} \in k[x]$ mit $q(a) = \tilde{q}(a)$. Das bedeutet $(q - \tilde{q})(a) = 0$ und wegen $p = \mathrm{Min}(a, K)$ folgt

$$q - \tilde{q} = ph$$

für ein $h \in k[x]$. Daraus folgt $q^{(\varphi)} - \tilde{q}^{(\varphi)} = p^{(\varphi)}h^{(\varphi)}$ und nach Einsetzen von b dann

$$q^{(\varphi)}(b) - \tilde{q}^{(\varphi)}(b) = \underbrace{p^{(\varphi)}(b)}_{=0} h^{(\varphi)}(b) = 0.$$

Das zeigt die Wohldefiniertheit. Die Abbildung ψ ist aber nun offensichtlich ein Homomorphismus $\psi\colon k(a) \to K'$ mit $\psi_{|k} = \varphi$ und $\psi(a) = b$. □

Satz 4.4.6. *Sei $\varphi\colon k \to k'$ ein Isomorphismus, $p \in k[x]$ und K ein Zerfällungskörper von p sowie K' ein Zerfällungskörper von $p^{(\varphi)}$. Dann gibt es mindestens einen und höchstens $[K : k]$ viele Isomorphismen $\psi\colon K \to K'$ mit $\psi_{|k} = \varphi$. Falls alle Nullstellen von $p^{(\varphi)}$ in K' verschieden sind, gibt es genau $[K : k]$ viele solche Fortsetzungen ψ.*

Beweis. Sei p_1 ein irreduzibler Faktor von p in $k[x]$ und $a_1 \in K$ mit $p_1(a_1) = 0$. Dann gilt $\mathrm{Min}(a_1, k) = p_1$ und nach Proposition 4.4.5 gibt es so viele Fortsetzungen $\varphi_1 \colon k(a_1) \to K'$ von φ, wie $p_1^{(\varphi)}$ verschiedene Nullstellen in K' hat. Das sind mindestens eine und höchstens

$$\deg\left(p_1^{(\varphi)}\right) = \deg(p_1) = [k(a_1) : k]$$

viele. Wir iterieren diesen Prozess nun mit φ_1 anstelle von φ und $k(a_1)$ anstelle von k. Dafür zerlegen wir p in $k(a_1)[x]$ in irreduzible Faktoren und wählen eine Nullstelle a_2 eines nicht-linearen irreduziblen Faktors. Auf diese Weise erhalten wir schließlich Fortsetzungen $\psi \colon K \to K'$ von φ.
Da sich sowohl der Körpergrad als auch die Anzahl der Fortsetzungen in jedem Schritt multipliziert, gibt es höchstens $[K : k]$ viele Fortsetzungen. Hat $p^{(\varphi)}$ lauter verschiedene Nullstellen in K', so gibt es in jedem Schritt die maximale Anzahl von Fortsetzungen, also exakt $[K : k]$ viele insgesamt.
Jeder Homomorphismus zwischen Körpern ist injektiv und jede Fortsetzung ψ bildet also verschiedene Nullstellen von p in K auf verschiedene Nullstellen von $p^{(\varphi)}$ in K' ab. Da man das Argument auch mit φ^{-1} durchführen kann, haben p und $p^{(\varphi)}$ jeweils gleich viele verschiedene Nullstellen in ihren Zerfällungskörpern und die werden durch ψ permutiert. Also ist ψ auch surjektiv und damit ein Isomorphismus. □

Definition 4.4.7. Seien $k \subseteq L, k \subseteq K$ Körpererweiterungen.
(*i*) Ein Homomorphismus $\varphi \colon L \to K$ heißt k-**Homomorphismus**, falls

$$\varphi_{|k} = \mathrm{id}_k.$$

(*ii*) L und K sind **isomorph über** k, falls es einen Isomorphismus zwischen L und K gibt, der ein k-Homomorphismus ist. △

Bemerkung 4.4.8. Jeder k-Homomorphismus $\varphi \colon K \to K$ ist k-linear. Es gilt für $a \in k, b \in K$

$$\varphi(ab) = \varphi(a)\varphi(b) = a\varphi(b).$$

Insbesondere ist φ durch die Werte auf einer k-Basis von K eindeutig bestimmt. Man beachte aber, dass die Vorgabe von Werten auf einer Basis im Allgemeinen nicht zu einem Homomorphismus führt. Die Multiplikativität ist nicht automatisch sichergestellt. △

Korollar 4.4.9. *Der Zerfällungskörper eines Polynoms $p \in k[x]$ ist bis auf Isomorphie über k eindeutig bestimmt.*

Beweis. Satz 4.4.6 mit $\varphi = \mathrm{id}_k$. □

Definition 4.4.10. (i) Ein Körper K heißt **algebraisch abgeschlossen**, falls jedes Polynom aus $K[x] \setminus K$ in K eine Nullstelle hat (und damit natürlich alle Polynome über K zerfallen).
(ii) Für eine Körpererweiterung $k \subseteq K$ heißt K **algebraischer Abschluss von** k, falls K algebraisch abgeschlossen und $k \subseteq K$ eine algebraische Erweiterung ist. △

Bemerkung 4.4.11. Jeder algebraisch abgeschlossene Körper ist unendlich. Wenn $k = \{a_1, \ldots, a_n\}$ nämlich endlich ist, hat das Polynom

$$p = (x - a_1) \cdots (x - a_n) + 1 \in k[x]$$

offensichtlich keine Nullstelle in k. △

Satz 4.4.12. *Jeder Körper k besitzt (bis auf Isomorphie über k) einen eindeutig bestimmten algebraischen Abschluss.*

Beweis. Existenz: Zunächst zeigen wir die Existenz einer algebraischen Körpererweiterung $k \subseteq L$, wobei jedes nichtkonstante Polynom über k in L eine Nullstelle hat. Das Argument ist eine Verallgemeinerung von Konstruktion 4.1.9. Sei dazu

$$R = k\left[x_p \mid p \in k[x] \setminus k\right]$$

der Polynomring über k in so vielen Variablen, wie es nichtkonstante Polynome über k gibt (beachte, dass in jedem Polynom aus R nur endlich viele Variablen auftreten). In R betrachten wir das Ideal

$$I := (p(x_p) \mid p \in k[x] \setminus k)$$

und zeigen $I \neq R$. Wäre nämlich o.B.d.A.

$$1 = \sum_{i=1}^{m} g_i(x_{p_1}, \ldots, x_{p_m}) p_i(x_{p_i})$$

mit gewissen $g_i \in k[x_{p_1}, \ldots, x_{p_m}]$ und $p_i \in k[x] \setminus k$, so wählen wir (zum Beispiel im Zerfällungskörper von $p_1 \cdots p_m$ über k) Elemente a_i mit $p_i(a_i) = 0$. Setzen wir dann a_i für x_{p_i} in die obere Gleichung ein, ergibt sich $1 = 0$, ein Widerspruch. Mit Satz 3.3.5 finden wir ein maximales Ideal $\mathfrak{m}$ mit

$$I \subseteq \mathfrak{m} \lhd R.$$

Der Körper $L := R/\mathfrak{m}$ kann dann als Erweiterungskörper von k aufgefasst werden. Das Element $x_p + \mathfrak{m} \in L$ ist dann aber eine Nullstelle von p, da $p(x_p) \in \mathfrak{m}$. Damit ist $k \subseteq L$ auch eine algebraische Erweiterung.
Wir iterieren den Prozess nun und erhalten eine aufsteigende Folge von algebraischen Körpererweiterungen

$$k = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots .$$

Dabei hat jedes nichtkonstante Polynom mit Koeffizienten aus L_i eine Nullstelle in L_{i+1}. Dann ist

$$K := \bigcup_{i \geq 0} L_i$$

auf kanonische Weise ein algebraischer Oberkörper von k. Jedes nichtkonstante Polynom aus $K[x]$ liegt dann bereits in einem $L_i[x]$ und hat also in $L_{i+1} \subseteq K$ eine Nullstelle. Damit ist K algebraisch abgeschlossen, also ein algebraischer Abschluss von k.
Eindeutigkeit: Seien $k \subseteq K$ und $k \subseteq K'$ zwei algebraische Abschlüsse von k. Wir zeigen die Existenz eines Isomorphismus $\varphi\colon K \to K'$ mit $\varphi_{|k} = \mathrm{id}_k$ mit dem Zorn'schen Lemma. Sei dazu

$$\mathcal{M} := \left\{ \varphi\colon L \to L' \text{ Isomorphismus} \mid k \subseteq L \subseteq K, k \subseteq L' \subseteq K', \varphi_{|k} = \mathrm{id}_k \right\}.$$

Wegen $(\mathrm{id}_k\colon k \to k) \in \mathcal{M}$ ist $\mathcal{M}$ nicht leer und wir versehen es mit der folgenden partiellen Ordnung:

$$\begin{aligned} (\varphi\colon L \to L') &\preceq (\tilde{\varphi}\colon \tilde{L} \to \tilde{L}') \\ &:\Leftrightarrow L \subseteq \tilde{L}, L' \subseteq \tilde{L}', \tilde{\varphi}_{|L} = \varphi. \end{aligned}$$

Man sieht leicht, dass jede Kette in $\mathcal{M}$ eine obere Schranke besitzt. Also gibt es nach dem Zorn'schen Lemma in $\mathcal{M}$ ein maximales Element $\varphi\colon L \to L'$. Wäre nun $L \subsetneq K$, so gäbe es $a \in K \setminus L$, wobei a sogar algebraisch über k und damit über L ist. Sei $p = \mathrm{Min}(a, L)$. Da K' algebraisch abgeschlossen ist, besitzt $p^{(\varphi)}$ in K' eine Nullstelle b. Nach Proposition 4.4.5 kann man φ damit zu einem Isomorphismus $\psi\colon L(a) \to L'(b)$ fortsetzen, ein Widerspruch zur Maximalität. Dasselbe Argument funktioniert auch mit φ^{-1} und zeigt also $L = K, L' = K'$. □

Bemerkung/Beispiel 4.4.13. (i) $\mathbb{C}$ ist der algebraische Abschluss von $\mathbb{R}$. Es ist $\mathbb{C}$ nämlich algebraisch abgeschlossen und $\mathbb{R} \subseteq \mathbb{C}$ ist endlich und damit algebraisch.

(ii) $\mathbb{C}$ ist nicht der algebraische Abschluss von $\mathbb{Q}$, da die Erweiterung $\mathbb{Q} \subseteq \mathbb{C}$ nicht algebraisch ist. Der algebraische Abschluss von $\mathbb{Q}$ ist (Aufgabe 56)

$$\overline{\mathbb{Q}} = \{a \in \mathbb{C} \mid a \text{ algebraisch über } \mathbb{Q}\} .$$

(iii) Die Erweiterung von k zum algebraischen Abschluss muss nicht endlich sein. Für $k = \mathbb{F}_p$ ist sie es beispielsweise nicht, wie man leicht mit Bemerkung 4.4.11 sieht.
(iv) Wir bezeichnen den algebraischen Abschluss des Körpers k von nun an auch mit $\overline{k}$. △

Korollar 4.4.14. *Sei $k \subseteq L$ eine algebraische Körpererweiterung und $k \subseteq K$ mit K algebraisch abgeschlossen. Dann gibt es einen k-Homomorphismus $\varphi\colon L \to K$.*

Beweis. Man kann beispielsweise die Argumente aus dem Eindeutigkeitsteil des Beweises von Satz 4.4.12 wiederholen. Andererseits kann man auch folgendermaßen argumentieren. Sei $\overline{L}$ der algebraische Abschluss von L und

$$\overline{k} = \{a \in K \mid a \text{ algebraisch über } k\} .$$

Dann sind $\overline{L}$ und $\overline{k}$ beides algebraische Abschlüsse von k und damit isomorph über k. Ein Isomorphismus liefert durch Einschränkung auf L den gewünschten Homomorphismus. □

4.5 Normale und separable Erweiterungen

Der Begriff einer normalen und separablen Körpererweiterung ist nötig, um später den Hauptsatz der Galoistheorie beweisen zu können.

Definition 4.5.1. Eine algebraische Körpererweiterung $k \subseteq K$ heißt **normal**, falls jedes irreduzible Polynom $p \in k[x]$, welches in K eine Nullstelle hat, in K bereits zerfällt. △

Beispiel 4.5.2. (i) Ist K algebraisch abgeschlossen, so ist die Erweiterung $k \subseteq K$ trivialerweise normal. Beispielsweise ist $\mathbb{R} \subseteq \mathbb{C}$ normal.
(ii) Die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ ist nicht normal (vergleiche dazu Beispiel 4.4.2). △

Satz 4.5.3. *Für eine algebraische Körpererweiterung $k \subseteq K \subseteq \overline{k}$ sind äquivalent:*

(i) $k \subseteq K$ *ist normal.*

(ii) K *ist Zerfällungskörper einer Menge von Polynomen über* k*.*

(iii) Jeder k*-Homomorphismus* $\varphi\colon K \to \overline{k}$ *erfüllt* $\varphi(K) \subseteq K$*.*

Beweis. "$(i) \Rightarrow (ii)$" Für jedes $a \in K$ hat $\mathrm{Min}(a, k)$ in K die Nullstelle a und zerfällt deshalb dort bereits in Linearfaktoren. Damit ist K offensichtlich der Zerfällungskörper der Minimalpolynome aller seiner Elemente über k.
"$(ii) \Rightarrow (iii)$" Sei K der Zerfällungskörper der Familie $(p_i)_{i\in I}$ von Polynomen $p_i \in k[x]$ und $\varphi\colon K \to \overline{k}$ ein k-Homomorphismus. Sei $a \in K$ eine Nullstelle von einem p_i. Dann gilt

$$0 = \varphi(0) = \varphi(p_i(a)) = p_i(\varphi(a)),$$

da φ ein k-Homomorphismus ist. Als Nullstelle von p_i in $\overline{k}$ liegt $\varphi(a)$ also sogar in K. Da K von solchen Nullstellen erzeugt wird, gilt $\varphi(K) \subseteq K$.
"$(iii) \Rightarrow (i)$" Sei $p \in k[x]$ irreduzibel und $a \in K$ sei eine Nullstelle von p. Sei $b \in \overline{k}$ eine beliebige weitere Nullstelle von p. Wir zeigen $b \in K$, daraus folgt die Aussage. Nach Proposition 4.4.5 gibt es aber einen k-Homomorphismus $\varphi\colon k(a) \to \overline{k}$ mit $\varphi(a) = b$. Wie im Beweis der Eindeutigkeit in Satz 4.4.12 kann man φ auf ganz K fortsetzen. Daraus folgt $b \in \varphi(K) \subseteq K$. □

Beispiel 4.5.4. (i) Es sind

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \qquad \mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) \qquad \mathbb{Q} \subseteq \mathbb{Q}\left(e^{\frac{2\pi i}{d}}\right)$$

normale Körpererweiterungen. Laut Beispiel 4.4.2 sind es nämlich Zerfällungskörper.
(ii) Jede Körpererweiterung mit $[K : k] = 2$ ist normal (Aufgabe 59). △

Korollar 4.5.5. *Sind* $k \subseteq L \subseteq K$ *algebraische Erweiterungen und ist* K *normal über* k*, so auch über* L*. Im Allgemeinen ist* L *aber nicht normal über* k*.*

Beweis. Die Normalität von K über L folgt zum Beispiel aus Satz 4.5.3 (ii). Als Gegenbeispiel zur Normalität von L über k betrachten wir die Körperkette

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}).$$

Die Erweiterung $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ ist normal, nicht aber die Erweiterung $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$. □

Definition 4.5.6. (i) Ein irreduzibles Polynom $p \in k[x]$ heißt **separabel**, falls p in $\overline{k}$ (oder seinem Zerfällungskörper) $\deg(p)$ viele verschiedene Nullstellen besitzt.
(ii) Für eine Körpererweiterung $k \subseteq K$ heißt $a \in K$ **separabel über** k, falls a algebraisch über k ist und $\mathrm{Min}(a, k)$ separabel ist.
(iii) Eine algebraische Körpererweiterung $k \subseteq K$ heißt **separabel**, falls jedes $a \in K$ separabel über k ist. △

Bemerkung 4.5.7. Sei $k \subseteq L \subseteq K$ eine Körperkette. Wenn K separabel über k ist, sind sowohl K über L als auch L über k separabel. Für L über k ist das trivial, für K über L liegt es daran, dass $\mathrm{Min}(a, L)$ in $L[x]$ ein Teiler von $\mathrm{Min}(a, k)$ ist. △

Definition 4.5.8. Sei R ein kommutativer Ring. Dann heißt die Abbildung

$$\begin{aligned} \partial \colon R[x] &\to R[x] \\ \sum_{i=0}^{d} c_i x^i &\mapsto \sum_{i=1}^{d} i c_i x^{i-1} \end{aligned}$$

formale Ableitung. △

Lemma 4.5.9. *Sei R ein kommutativer Ring und ∂ die formale Ableitung auf $R[x]$. Dann gilt für $r, s \in R, p, q \in R[x]$*

$$\partial(rp + sq) = r\partial(p) + s\partial(q)$$

$$\partial(pq) = p\partial(q) + q\partial(p)$$

$$\partial(r) = 0.$$

Beweis. Aufgabe 47. □

Satz 4.5.10. *Sei k ein Körper und $p \in k[x]$ irreduzibel. Dann gilt*

$$p \text{ separabel} \Leftrightarrow \partial(p) \neq 0.$$

Beweis. Sei o.B.d.A. p normiert.
"⇒": Es gibt paarweise verschiedene $a_1, \ldots, a_d \in \overline{k}$ mit

$$p = (x - a_1) \cdots (x - a_d).$$

In $\overline{k}[x]$ gilt dann

$$\partial(p) = \sum_{i=1}^{d} \prod_{j \neq i} (x - a_j)$$

und jeder Linearfaktor $(x - a_i)$ teilt jeden Summanden außer dem i-ten, also nicht $\partial(p)$. Daraus folgt $\partial(p) \neq 0$.
"$\Leftarrow$": Aus $\partial(p) \neq 0$ und $\deg(\partial(p)) < \deg(p)$ folgt $p \nmid \partial(p)$. Da p irreduzibel ist, sind p und $\partial(p)$ dann schon teilerfremd im Hauptidealring $k[x]$. Nach Lemma 3.5.14 gibt es eine Darstellung

$$1 = fp + g\partial(p)$$

mit $f, g \in k[x]$ und $p, \partial(p)$ können also keine gemeinsame Nullstelle in $\overline{k}$ haben. Wäre nun p nicht separabel, so gäbe es $a \in \overline{k}$ mit

$$(x - a)^2 \mid p \quad \text{in } \overline{k}[x],$$

also $p = (x - a)^2 q$. Nun berechnet man

$$\partial(p) = (x - a)\left(2q + (x - a)\partial(q)\right),$$

also haben p und $\partial(p)$ in $\overline{k}$ die gemeinsame Nullstelle a, ein Widerspruch. □

Bemerkung 4.5.11. Dem Beweis von Satz 4.5.10 sieht man an, dass für die Separabilität von p schon eine einzige Nullstelle in $\overline{k}$ mit Vielfachheit 1 genügt. △

Korollar 4.5.12. *(i) Falls $\mathrm{char}(k) = 0$ gilt, ist jedes irreduzible Polynom $p \in k[x]$ separabel. Insbesondere ist jede algebraische Körpererweiterung $k \subseteq K$ separabel.*
(ii) Falls $\mathrm{char}(k) = d$ gilt, so ist ein irreduzibles $p \in k[x]$ genau dann inseparabel, wenn ein $q \in k[x]$ existiert mit $p(x) = q(x^d)$.

Beweis. (i) folgt mit Satz 4.5.10 aus der Tatsache, dass für $p \in k[x] \setminus k$ stets $\partial(p) \neq 0$ gilt. Ist $c \neq 0$ nämlich der Leitkoeffizient von p, so ist $\deg(p) \cdot c \neq 0$ der Leitkoeffizient von $\partial(p)$.
Für (ii) sieht man ganz analog, dass alle Koeffizienten von $\partial(p)$ genau dann Null sind, wenn die Grade bei allen auftretenden Koeffizienten von p Vielfache von d waren. □

Definition 4.5.13. Ein Körper k heißt **vollkommen**, falls jedes irreduzible Polynom $p \in k[x]$ separabel ist.[1] △

[1] Trifft ein schwere-noetherscher Ring auf einen vollkommenen Körper…

Beispiel 4.5.14. Jeder Körper von Charakteristik 0 ist vollkommen (Korollar 4.5.12 (i)) $\triangle$

Satz 4.5.15. *Sei k ein Körper mit $\operatorname{char}(k) = d > 0$. Dann gilt*

$$k \text{ vollkommen} \;\Leftrightarrow\; k = k^d \left(:= \left\{a^d \mid a \in k\right\}\right).$$

Beweis. "$\Rightarrow$": Für $a \in k$ beliebig betrachten wir $p = x^d - a \in k[x]$. Da offensichtlich $\partial(p) = 0$ gilt muss p reduzibel sein, nach Satz 4.5.10. Also gibt es $q, h \in k[x]$ mit q irreduzibel und $p = qh$. Es gibt nun ein $b \in \overline{k}$ mit $q(b) = 0$, insbesondere $p(b) = 0$, also

$$b^d = a.$$

Damit gilt in $\overline{k}[x]$ (mit Lemma 4.1.6)

$$qh = p = x^d - a = x^d - b^d = (x - b)^d.$$

Aus der Eindeutigkeit der Primfaktorzerlegung in $\overline{k}[x]$ folgt $q = (x - b)^m$ für ein m. Da k nach Annahme vollkommen ist, hat das irreduzible Polynom q lauter verschiedene Nullstellen in $\overline{k}$, und daraus folgt $m = 1$. Aus

$$x - b = q \in k[x]$$

folgt dann $b \in k$, die gewünschte Aussage.
"$\Leftarrow$": Sei $p \in k[x]$ mit $\partial(p) = 0$. Im Beweis von Korollar 4.5.12 haben wir gesehen, dass

$$p = c_0 + c_1 x^d + c_2 x^{2d} + \cdots + c_n x^{nd}$$

gelten muss. Wähle nun $b_i \in k$ mit $b_i^d = c_i$. Dann gilt

$$p = b_0^d + b_1^d x^d + b_2^d x^{2d} + \cdots + b_n^d x^{nd} = \left(b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n\right)^d.$$

Also ist p nicht irreduzibel. Mit Satz 4.5.10 folgt, dass alle irreduziblen Polynome in $k[x]$ separabel sind. Damit ist k offensichtlich vollkommen. $\square$

Beispiel 4.5.16. (i) Jeder endliche Körper ist vollkommen. Das folgt mit Satz 4.5.15 aus Lemma 4.1.6.
(ii) Sei p eine Primzahl. Dann ist der Körper $\mathbb{F}_p(t)$ nicht vollkommen (siehe Aufgabe 69). $\triangle$

Satz 4.5.17 (Satz vom primitiven Element)**.** *Sei $k \subseteq K$ eine endliche separable Erweiterung. Dann gibt es ein $a \in K$ mit $K = k(a)$.*

Beweis. Wir führen den Beweis nur im Fall, dass k unendlich ist. Wir können außerdem $K = k(b, c)$ mit algebraischen Elementen $b, c \in K$ annehmen, weil man das Ergebnis dann iterieren kann. Seien $p = \mathrm{Min}(b, k), q = \mathrm{Min}(c, k)$ sowie

$$b = \beta_1, \beta_2 \ldots, \beta_d \text{ und } c = \gamma_1, \gamma_2 \ldots, \gamma_e$$

die (jeweils paarweise verschiedenen) Nullstellen von p und q in $\overline{k}$. Da k unendlich ist, gibt es ein $\delta \in k$ mit

$$\delta \neq \frac{\beta_1 - \beta_i}{\gamma_j - \gamma_1}$$

für alle $i = 1, \ldots, d, j = 2, \ldots, e$. Wir setzen

$$a := \beta_1 + \delta\gamma_1 = b + \delta c \in K$$

und zeigen $k(b, c) = k(a)$, wobei "$\supseteq$" klar ist. Die beiden Polynome

$$q, p(a - \delta x) \in k(a)[x]$$

haben die gemeinsame Nullstelle $c = \gamma_1$. Eine weitere gemeinsame Nullstelle haben sie nicht, denn für $j \geq 2$ folgt aus $0 = p(a - \delta\gamma_j)$ schon $a - \delta\gamma_j = \beta_i$ für ein i und genau das ist nach Wahl von δ nicht der Fall. Es gilt also

$$x - c = \mathrm{ggT}(q, p(a - \delta x)) \text{ in } \overline{k}[x].$$

Der größte gemeinsame Teiler kann aber auch in $k(a)[x]$ berechnet werden (zum Beispiel wegen Lemma 3.5.14) und daraus folgt $c \in k(a)$ und somit auch $b \in k(a)$. Das zeigt $k(b, c) \subseteq k(a)$. □

4.6 Galoistheorie

Die Galoistheorie erlaubt es uns, Fragen der Körpertheorie in Fragen der Gruppentheorie zu übersetzen. Erst damit können wir die Frage nach der Lösbarkeit von polynomialen Gleichungen beantworten.

Definition 4.6.1. Sei $k \subseteq K$ eine Körpererweiterung. Wir definieren ihre **Galoisgruppe** folgendermaßen:

$$\mathrm{Gal}(K, k) := \{\varphi \colon K \to K \mid \varphi \, k\text{-Isomorphismus}\}.$$

Elemente von $\mathrm{Gal}(K, k)$ nennen wir auch k**-Automorphismen** von K. △

Bemerkung/Beispiel 4.6.2. (*i*) Offensichtlich ist $\mathrm{Gal}(K,k)$ eine Gruppe bezüglich der Hintereinanderausführung von Funktionen. Das neutrale Element ist id_K.
(*ii*) Wir berechnen $\mathrm{Gal}(\mathbb{C},\mathbb{R})$. Wegen $\mathbb{C}=\mathbb{R}(i)$ gibt es nach Proposition 4.4.5 so viele $\mathbb{R}$-Homomorphismen von $\mathbb{C}$ wie Nullstellen von x^2+1 in $\mathbb{C}$ und das sind genau i und $-i$. Bilden wir i auf i ab, erhalten wir die Identität. Bilden wir i auf $-i$ ab, erhalten wir die komplexe Konjugation κ. Es gilt $\kappa\circ\kappa=\mathrm{id}$. Beide Homomorphismen sind Automorphismen, also

$$\mathrm{Gal}(\mathbb{C},\mathbb{R})=\{\mathrm{id}_{\mathbb{C}},\kappa\}\cong\mathbb{Z}/2\mathbb{Z}.$$

Ganz analog berechnet man

$$\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2}),\mathbb{Q}\right)=\{\mathrm{id},\varphi\}\cong\mathbb{Z}/2\mathbb{Z},$$

wobei φ gerade $\sqrt{2}$ auf $-\sqrt{2}$ abbildet.
(*iii*) Wir bestimmen $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt[3]{2}\right),\mathbb{Q}\right)$. Es muss $\sqrt[3]{2}$ durch jeden $\mathbb{Q}$-Automorphismus auf eine Nullstelle von x^3-2 abgebildet werden und davon gibt es in $\mathbb{Q}(\sqrt[3]{2})$ nur eine. Also gilt

$$\mathrm{Gal}\left(\mathbb{Q}(\sqrt[3]{2}),\mathbb{Q}\right)=\{\mathrm{id}\}.$$

(*iv*) Wir bestimmen

$$\mathrm{Gal}\left(\mathbb{Q}\left(e^{\frac{2\pi i}{p}}\right),\mathbb{Q}\right)$$

für eine Primzahl p. Das Minimalpolynom Φ_p von $a=e^{\frac{2\pi i}{p}}$ hat in $K=\mathbb{Q}\left(e^{\frac{2\pi i}{p}}\right)$ die $p-1$ verschiedenen Nullstellen $a,a^2,\ldots,a^{p-1}$. Nach Proposition 4.4.5 gibt es also $p-1$ viele $\mathbb{Q}$-Homomorphismen von K, also $\varphi_1,\ldots,\varphi_{p-1}$ bestimmt durch

$$\varphi_i(a)=a^i.$$

Dabei handelt es sich jeweils sogar um Automorphismen (Übungsaufgabe). Damit sieht man

$$\mathrm{Gal}\left(\mathbb{Q}\left(e^{\frac{2\pi i}{p}}\right),\mathbb{Q}\right)=\{\varphi_1,\ldots,\varphi_{p-1}\}\cong(\mathbb{Z}/p\mathbb{Z})^\times. \qquad \triangle$$

Lemma 4.6.3. *Sei $p\in k[x]$ und K der Zerfällungskörper von p über k.*

(i) Es gilt $\#\,\mathrm{Gal}(K,k)\le[K:k]$, insbesondere ist die Galoisgruppe der Erweiterung endlich.

(ii) Falls alle Nullstellen von p verschieden sind, gilt $\#\operatorname{Gal}(K,k) = [K:k]$.

Beweis. Direkte Folgerung aus Satz 4.4.6 mit $\varphi = \mathrm{id}_k$. □

Definition 4.6.4. Sei $k \subseteq K$ eine Körpererweiterung, $G = \operatorname{Gal}(K,k)$ und $H < G$ eine Untergruppe. Dann definieren wir

$$\operatorname{Fix}(H) := \{b \in K \mid \varphi(b) = b \text{ für alle } \varphi \in H\}. \qquad \triangle$$

Bemerkung/Beispiel 4.6.5. (i) Man sieht leicht, dass $\operatorname{Fix}(H)$ für jede Untergruppe H der Galoisgruppe ein Zwischenkörper der Erweiterung ist:

$$k \subseteq \operatorname{Fix}(H) \subseteq K.$$

Die Körperaxiome folgen aus der Tatsache, dass die betrachteten Abbildungen φ Homomorphismen sind. Die Aussage $k \subseteq \operatorname{Fix}(H)$ bedeutet gerade, dass alle φ k-Homomorphismen sind.
(ii) Umgekehrt gilt für jeden Zwischenkörper $k \subseteq L \subseteq K$ offensichtlich

$$\operatorname{Gal}(K,L) < \operatorname{Gal}(K,k).$$

(iii) Wir haben also Zuordnungen

$$\begin{aligned} \{\text{Untergruppen von } \operatorname{Gal}(K,k)\} &\leftrightarrow \{\text{Zwischenkörper von } k \subseteq K\} \\ H &\mapsto \operatorname{Fix}(H) \\ \operatorname{Gal}(K,L) &\hookleftarrow L \end{aligned}$$

Beide Zuordnungen sind inklusionsumkehrend, für $H_1 < H_2 < \operatorname{Gal}(K,k)$, $k \subseteq L_1 \subseteq L_2 \subseteq K$ gilt also

$$\operatorname{Fix}(H_1) \supseteq \operatorname{Fix}(H_2) \text{ und } \operatorname{Gal}(K,L_1) \supseteq \operatorname{Gal}(K,L_2).$$

Weiter gilt offensichtlich

$$H \subseteq \operatorname{Gal}(K, \operatorname{Fix}(H)) \text{ und } L \subseteq \operatorname{Fix}(\operatorname{Gal}(K,L)).$$

Im Allgemeinen gilt aber keine Gleichheit. In Beispiel 4.6.2 (iii) etwa gilt

$$\operatorname{Fix}(\operatorname{Gal}(K,k)) = K. \qquad \triangle$$

Proposition 4.6.6 (Lemma von Artin)**.** *Sei $k \subseteq K$ eine Körpererweiterung und $H < \operatorname{Gal}(K,k)$ endlich. Dann gilt*

$$[K : \operatorname{Fix}(H)] \leq \#H.$$

Beweis. Sei $n = \#H$ und $H = \{\varphi_1, \dots, \varphi_n\}$. Sei $m > n$ und $a_1, \dots, a_m \in K$. Wir zeigen, dass $a_1, \dots, a_m$ linear abhängig über $\mathrm{Fix}(H)$ sein müssen, das beweist die Aussage. Dazu betrachten wir das homogene lineare Gleichungssystem

$$\begin{aligned}
\varphi_1(a_1)x_1 + \varphi_1(a_2)x_2 + \cdots + \varphi_1(a_m)x_m &= 0 \\
\varphi_2(a_1)x_1 + \varphi_2(a_2)x_2 + \cdots + \varphi_2(a_m)x_m &= 0 \\
&\vdots \\
\varphi_n(a_1)x_1 + \varphi_n(a_2)x_2 + \cdots + \varphi_n(a_m)x_m &= 0.
\end{aligned}$$

Wegen $m > n$ gibt es eine nichttriviale Lösung $(b_1, \dots, b_m) \in K^m$ und wir wählen sie dabei mit einer maximalen Anzahl von Nullen in den Einträgen. Sei außerdem o.B.d.A. $b_1 = 1$. Für alle i, j gilt nun

$$0 = \varphi_j(0) = \varphi_j\left(\sum_k \varphi_i(a_k)b_k\right) = \sum_k (\varphi_j \circ \varphi_i)(a_k)\varphi_j(b_k).$$

Für festes j durchlaufen die Elemente $\varphi_j \circ \varphi_i$ mit i die ganze Gruppe H und damit ist auch $(\varphi_j(b_1), \dots, \varphi_j(b_m)) \in K^m$ eine Lösung des Gleichungssystems. Aufgrund der Homogenität ist dann auch

$$(b_1 - \varphi_j(b_1), \dots, b_m - \varphi_j(b_m)) \in K^m$$

eine Lösung. Angenommen es gilt nun $b_i \notin \mathrm{Fix}(H)$ für ein i. Dann gibt es ein j mit $\varphi_j(b_i) \neq b_i$, also ist

$$\begin{aligned}
(b_1 - \varphi_j(b_1), \dots, b_m - \varphi_j(b_m)) &= (1 - 1, b_2 - \varphi_j(b_2), \dots, b_m - \varphi_j(b_m)) \\
&= (0, b_2 - \varphi_j(b_2), \dots, \underbrace{b_i - \varphi_j(b_i)}_{\neq 0}, \dots, \dots, b_m - \varphi_j(b_m))
\end{aligned}$$

eine nichttriviale Lösung mit einer Null mehr. Das ist ein Widerspruch und zeigt $b_i \in \mathrm{Fix}(H)$ für alle i. Wenn etwa $\varphi_1 = \mathrm{id}$ gilt, zeigt die erste Zeile des Gleichungssystems also die lineare Abhängigkeit der a_i über $\mathrm{Fix}(H)$. □

Definition 4.6.7. Eine Körpererweiterung heißt **Galois-Erweiterung**, falls sie endlich, normal und separabel ist. △

Beispiel 4.6.8. (*i*) Mit $\mathrm{char}(k) = 0$, $p \in k[x]$ und K dem Zerfällungskörper von p über k ist $k \subseteq K$ eine Galoiserweiterung. Das folgt aus Satz 4.2.9, Satz 4.5.3 und Korollar 4.5.12. Beispiele dafür sind

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}),\ \mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i),\ \mathbb{Q} \subseteq \mathbb{Q}\left(e^{\frac{2\pi i}{d}}\right),\ \mathbb{R} \subseteq \mathbb{C}.$$

(ii) Ist $k \subseteq L \subseteq K$ eine Körperkette und K über k galoisch, so auch K über L (nach Korollar 4.5.5 und Bemerkung 4.5.7). Für L über k stimmt das im Allgemeinen nicht (die Normalität kann scheitern, siehe Korollar 4.5.5). △

Satz 4.6.9 (Hauptsatz der Galoistheorie). *Es sei $k \subseteq K$ eine Galois-Erweiterung. Dann sind die Zuordnungen $\mathrm{Fix}(\cdot)$ und $\mathrm{Gal}(K, \cdot)$ zueinander inverse inklusionsumkehrende Bijektionen zwischen Untergruppen von $G = \mathrm{Gal}(K, k)$ und Zwischenkörpern von k und K. Weiter gilt für $H < G$:*

(i) $\#H = [K : \mathrm{Fix}(H)]$ *und* $|G : H| = [\mathrm{Fix}(H) : k]$

(ii) $H \lhd G \Leftrightarrow \mathrm{Fix}(H)$ *normal über* k.

In diesem Fall ist $k \subseteq \mathrm{Fix}(H)$ wieder eine Galois-Erweiterung und es gilt

$$\mathrm{Gal}\left(\mathrm{Fix}(H), k\right) \cong G/H.$$

$$\begin{array}{ccc} K & & \{\mathrm{id}\} \\ r\,| & & |\,r \\ L = \mathrm{Fix}(H) & & H = \mathrm{Gal}(K, L) \\ s\,| & & |\,s \\ k & & G \end{array}$$

Beweis. Mit dem Satz vom primitiven Element ist K als Galois-Erweiterung der Zerfällungskörper eines separablen Polynoms über k. Nach Lemma 4.6.3 gilt also $\#\,\mathrm{Gal}(K, k) = [K : k]$. Dasselbe Argument kann man natürlich auch für jeden Zwischenkörper $k \subseteq L \subseteq K$ auf die Galois-Erweiterung $L \subseteq K$ anwenden und erhält also

$$\#\,\mathrm{Gal}(K, L) = [K : L]\,.$$

Sei nun $H < G := \mathrm{Gal}(K, k)$ eine Untergruppe. Wegen $H \subseteq \mathrm{Gal}(K, \mathrm{Fix}(H))$ gilt mit dem Lemma von Artin

$$\#H \leq \#\,\mathrm{Gal}(K, \mathrm{Fix}(H)) = [K : \mathrm{Fix}(H)] \leq \#H.$$

Das beweist $\mathrm{Gal}(K, \mathrm{Fix}(H)) = H$ und die erste Gleichung in (i). Die zweite Gleichung in (i) folgt direkt aus

$$\#G = [K : k] = [K : \mathrm{Fix}(H)] \cdot [\mathrm{Fix}(H) : k] = \#H \cdot [\mathrm{Fix}(H) : k]\,.$$

Nun gilt offensichtlich $\mathrm{Gal}(K, \mathrm{Fix}(\mathrm{Gal}(K,k))) = \mathrm{Gal}(K,k)$, also

$$[K:k] = \#\,\mathrm{Gal}(K,k) = \#\,\mathrm{Gal}(K,\mathrm{Fix}(\mathrm{Gal}(K,k))) = [K:\mathrm{Fix}(\mathrm{Gal}(K,k))]$$

und damit $\mathrm{Fix}(\mathrm{Gal}(K,k)) = k$. Auch hier erhält man dieselbe Aussage für jeden Zwischenkörper:

$$\mathrm{Fix}(\mathrm{Gal}(K,L)) = L.$$

Damit ist gezeigt, dass die Zuordnungen $\mathrm{Gal}(K,\cdot)$ und $\mathrm{Fix}(\cdot)$ beidseitig invers zueinander sind.
Für (ii) sei $H < G$ und $L = \mathrm{Fix}(H)$. Dann gilt für $\varphi \in G$

$$\varphi(L) = \mathrm{Fix}(\varphi H \varphi^{-1}),$$

denn

$$\begin{aligned} a \in \mathrm{Fix}(\varphi H \varphi^{-1}) &\Leftrightarrow \left(\varphi\tau\varphi^{-1}\right)(a) = a \,\forall \tau \in H \\ &\Leftrightarrow \left(\tau\varphi^{-1}\right)(a) = \varphi^{-1}(a) \,\forall \tau \in H \\ &\Leftrightarrow \varphi^{-1}(a) \in \mathrm{Fix}(H) = L \\ &\Leftrightarrow a \in \varphi(L). \end{aligned}$$

Ist H nun eine normale Untergruppe in G, so gilt $\varphi H \varphi^{-1} = H$ und somit $\varphi(L) = L$ für alle $\varphi \in G$. Wir wollen mit Satz 4.5.3 (iii) daraus die Normalität von L über k schließen. Wir können mit Korollar 4.4.14

$$k \subseteq L \subseteq K \subseteq \overline{k}$$

annehmen und wählen einen beliebigen k-Homomorphismus $\psi\colon L \to \overline{k}$. Mit Proposition 4.4.5 existiert eine Fortsetzung $\varphi\colon K \to \overline{k}$ von ψ und da K normal über k ist, gilt mit Satz 4.5.3 sogar $\varphi\colon K \to K$. Es ist also $\varphi \in G$ und wir wissen deshalb $\psi(L) = \varphi(L) \subseteq L$. Mit Satz 4.5.3 (iii) ist also L normal über k.
Sei umgekehrt L normal über k. Dann gilt wieder mit Satz 4.5.3 $\varphi(L) \subseteq L$ für alle $\varphi \in G$, also

$$\mathrm{Fix}(\varphi H \varphi^{-1}) \subseteq \mathrm{Fix}(H).$$

Nach Anwendung von $\mathrm{Gal}(K,\cdot)$ erhalten wir also $H \subseteq \varphi H \varphi^{-1}$ und aufgrund der Mächtigkeiten damit $H = \varphi H \varphi^{-1}$. Dies stimmt für alle $\varphi \in G$, also ist H eine normale Untergruppe.
In diesem Fall betrachten wir schließlich den Gruppenhomomorphismus

$$\begin{aligned} \pi\colon G &\to \mathrm{Gal}(L,k) \\ \varphi &\mapsto \varphi_{|L}. \end{aligned}$$

Er ist wohldefiniert, da aufgrund der Normalität von L über k stets $\varphi(L) \subseteq L$ gilt. Es gilt offensichtlich $\ker(\pi) = \mathrm{Gal}(K, L) = \mathrm{Gal}(K, \mathrm{Fix}(H)) = H$. Außerdem ist π surjektiv. Jeder k-Homomorphismus $\psi\colon L \to L$ lässt sich fortsetzen zu $\varphi\colon K \to \overline{k}$ und aufgrund der Normalität von K über k also zu $\varphi \in G$ mit $\pi(\varphi) = \psi$. Mit dem Homomorphiesatz folgt

$$G/H \cong \mathrm{Gal}(L, k). \qquad \square$$

Beispiel 4.6.10. Wir wollen alle Teilkörper der Galoiserweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}(e^{2\pi i/5})$$

finden. Setze $\xi := e^{2\pi i/5}$. Wir wissen bereits $[\mathbb{Q}(\xi) : \mathbb{Q}] = 4$, also hat jeder echte Zwischenkörper laut Gradformel Grad 2 über $\mathbb{Q}$. Aus Beispiel 4.6.2 (*iii*) wissen wir

$$\mathrm{Gal}(\mathbb{Q}(\xi), \mathbb{Q}) = (\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, 3, 4\}\,.$$

Man kann nun leicht sämtliche Untergruppen dieser Gruppe bestimmen:

$$\{1\}, \{1, 2, 3, 4\}, \{1, 4\}.$$

Also gibt es genau einen echten Zwischenkörper, und zwar den Fixkörper der Abbildung

$$\varphi_4\colon \xi \mapsto \xi^4.$$

Fixiert wird durch φ_4 das Element

$$\chi := \xi + \xi^4 = 2\cos(2\pi/5),$$

da $\varphi_4(\xi^4) = \xi^{16} = \xi$. Andererseits gilt $\chi \notin \mathbb{Q}$, da

$$\varphi_2(\chi) = \xi^2 + \xi^3 = 2\cos(4\pi/5) \neq \chi.$$

Also ist

$$\mathrm{Fix}\left(\{1, 4\}\right) = \mathbb{Q}(\chi)$$

der eindeutig bestimmte nichttriviale Zwischenkörper der Erweiterung. $\triangle$

Eine erste Folgerung, in deren Beweis wir Ergebnisse der Gruppentheorie in die Körpertheorie übertragen, ist der Fundamentalsatz der Algebra:

Korollar 4.6.11 (Fundamentalsatz der Algebra)**.** *$\mathbb{C}$ ist algebraisch abgeschlossen.*

Beweis. Da jedes Polynom in einer endlichen Erweiterung eine Nullstelle hat, genügt es zu zeigen, dass $\mathbb{C}$ keine echte endliche Körpererweiterung besitzt. Angenommen $\mathbb{C} \subseteq K$ ist eine endliche Körpererweiterung. Nach dem Satz vom primitiven Element gilt $K = \mathbb{R}(a)$ für ein $a \in K$, und wenn wir K durch den Zerfällungskörper von $\mathrm{Min}(a, \mathbb{R})$ ersetzen, können wir K als Galoiserweiterung von $\mathbb{R}$ annehmen. Wir können also den Hauptsatz der Galois-Theorie verwenden. Wegen

$$[K : \mathbb{R}] = [K : \mathbb{C}] \cdot [\mathbb{C} : \mathbb{R}] = 2\,[K : \mathbb{C}]$$

gilt $2 \mid \#\,\mathrm{Gal}(K, \mathbb{R})$. Sei $H < \mathrm{Gal}(K, \mathbb{R}) =: G$ eine 2-Sylow-Untergruppe und $L = \mathrm{Fix}(H)$:

$$\begin{array}{rc} K & \{\mathrm{id}\} \\ 2^r \mid & \mid 2^r \\ L & H \\ \text{ungerade} \mid & \mid \text{ungerade} \\ \mathbb{R} & G \end{array}$$

In $\mathbb{R}$ hat aber nach dem Zwischenwertsatz jedes Polynom von ungeradem Grad eine Nullstelle. Also sind die einzigen irreduziblen Polynome von ungeradem Grad vom Grad 1, also besitzt $\mathbb{R}$ keine echte ungerade Körpererweiterung. Das bedeutet $L = \mathbb{R}$ und $[K : \mathbb{R}] = 2^r$. Für die Untergruppe $\mathrm{Gal}(K, \mathbb{C}) < G$ gilt also $\#\,\mathrm{Gal}(K, \mathbb{C}) = 2^{r-1}$ und wir zeigen $r - 1 = 0$. Wäre $r > 1$, könnten wir eine Untergruppe $H_1 < \mathrm{Gal}(K, \mathbb{C})$ mit $\#H_1 = 2^{r-2}$ wählen. Für $L_1 = \mathrm{Fix}(H_1)$ wäre dann $[L_1 : \mathbb{C}] = 2$. In $\mathbb{C}[x]$ gibt es aber keine quadratischen irreduziblen Polynome, da man in $\mathbb{C}$ immer Wurzeln ziehen kann. Also hat $\mathbb{C}$ auch keine quadratische Erweiterung, ein Widerspruch. Wir haben also $\#\,\mathrm{Gal}(K, \mathbb{C}) = 1$ und damit $K = \mathbb{C}$ gezeigt. □

Wir zeigen nun noch die Umkehrung von Satz 4.3.6:

Korollar 4.6.12. *Sei p eine Primzahl mit $p - 1 = 2^r$ für ein $r \geq 1$. Dann ist das regelmäßige p-Eck mit Zirkel und Lineal aus $0, 1$ konstruierbar.*

Beweis. Es ist $\mathbb{Q} \subseteq \mathbb{Q}\left(e^{2\pi i/p}\right)$ nach Beispiel 4.6.8 (i) eine Galoiserweiterung. Mit Korollar 4.2.17 und dem Hauptsatz der Galoistheorie erhalten wir für

$$G := \mathrm{Gal}\left(\mathbb{Q}\left(e^{2\pi i/p}\right), \mathbb{Q}\right)$$

gerade

$$\#G = 2^r.$$

Mit dem ersten Sylowsatz gibt es nun eine Kette von Untergruppen

$$\{\mathrm{id}\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_r = G$$

mit $\#H_i = 2^i$ für alle i (man wähle zuerst H_{r-1} in G, dann H_{r-2} in H_{r-1}...). Durch Bildung der Fixkörper erhalten wir eine Körperkette

$$\mathbb{Q} = L_r \subseteq L_{r-1} \subseteq \cdots \subseteq L_0 = \mathbb{Q}\left(e^{2\pi i/p}\right)$$

mit $[L_i : L_{i+1}] = 2$ für alle i. Jede Körpererweiterung vom Grad 2 entsteht aber durch Adjunktion einer Quadratwurzel, wie man sich leicht überlegt. Körperoperationen und Ziehen von Quadratwurzeln ist aber nach Satz 1.1.2 mit Zirkel und Lineal möglich. Das beweist die Aussage. □

4.7 Unlösbarkeit von polynomialen Gleichungen

Zum Abschluss der Körpertheorie beantworten wir schließlich die Frage nach Auflösbarkeit von polynomialen Gleichungen.

Definition 4.7.1. (*i*) Eine Körpererweiterung $k \subseteq K$ heißt **mit Radikalen auflösbar**, falls es eine Körperkette

$$k = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_m = K$$

gibt, wobei $k_{i+1} = k_i(a_i)$ mit $a_i^{d_i} \in k_i$ für alle $i = 0, \ldots, m-1$ gilt.
(*ii*) Für $p \in k[x]$ heißt die Gleichung „$p = 0$“ **mit Radikalen auflösbar**, wenn es eine Körpererweiterung $k \subseteq K$ gibt, die mit Radikalen auflösbar ist, und p über K in Linearfaktoren zerfällt. △

Lemma 4.7.2. *Sei $k \subseteq K$ mit Radikalen auflösbar. Dann gibt es einen Erweiterungskörper L von K, sodass die Erweiterung $k \subseteq L$ mit Radikalen auflösbar und zusätzlich normal ist. Dabei bleiben die in der Auflösung verwendeten Exponenten gleich.*

Beweis. Da $k \subseteq K$ mit Radikalen auflösbar ist, können wir k_i, a_i und d_i wie in Definition 4.7.1 (*i*) wählen. Für jedes $i = 0, \ldots, m-1$ seien

$$a_i = a_{i1}, a_{i2}, \ldots, a_{in_i}$$

die Nullstellen von $\mathrm{Min}(a_i, k) =: p_i$ in $\overline{K}$. Da p_i ein Teiler von $x^{d_i} - a_i^{d_i}$ ist, gilt $a_{ij}^{d_i} = a_i^{d_i} \in k_i = k(a_0, \ldots a_{i-1})$ für alle i, j.

Wir konstruieren nun eine neue Körperkette, indem wir an k diese Elemente in der folgende Reihenfolge iterativ adjungieren:

$$a_0 = a_{01}, a_{02}, \ldots, a_{0n_0}, a_1 = a_{11}, \ldots, a_{1n_1}, a_2 = a_{21}, \ldots, a_{m-1}, \ldots, a_{m-1n_{m-1}}.$$

Jeder einzelne Schritt ist dabei die Adjunktion einer Wurzel aus dem vorhergehenden Körper. Der insgesamt entstehende Körper L ist der Zerfällungskörper der Polynome $p_0, \ldots, p_{m-1}$ über k und damit ist die Erweiterung $k \subseteq L$ normal. □

Der folgende Satz gilt noch deutlich allgemeiner, zum Beispiel ist auch die Rückrichtung wahr. Wir beschränken uns aber auf den für uns relevanten Teil:

Satz 4.7.3. *Sei $p \in \mathbb{Q}[x]$ und K der Zerfällungskörper von p über $\mathbb{Q}$. Falls die Gleichung „$p = 0$" mit Radikalen auflösbar ist, so ist $\mathrm{Gal}(K, \mathbb{Q})$ eine auflösbare Gruppe.*

Beweis. Sei $\mathbb{Q} = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_m$ eine Körperkette wie in Definition 4.7.1, also $K \subseteq k_m$. Wir können o.B.d.A. annehmen, dass $k_1 = \mathbb{Q}(\xi)$ mit $\xi := e^{\frac{2\pi i}{n}}$ gilt, wobei n von allen d_i geteilt wird. Mithilfe von Lemma 4.7.2 können wir zusätzlich annehmen, dass $\mathbb{Q} \subseteq k_m$ eine normale und damit galoissche Erweiterung ist. Es genügt zu zeigen, dass $\mathrm{Gal}(k_m, \mathbb{Q})$ auflösbar ist. Da K als Zerfällungskörper über $\mathbb{Q}$ normal ist, gilt

$$\mathrm{Gal}(K, \mathbb{Q}) \cong \mathrm{Gal}(k_m, \mathbb{Q}) / \mathrm{Gal}(k_m, K)$$

und als Quotient einer auflösbaren Gruppe ist $\mathrm{Gal}(K, \mathbb{Q})$ mit Satz 2.5.7 dann auflösbar.
Wegen $\xi_i := \xi^{n/d_i} \in k_i$ für alle $i \geq 1$ sind die Erweiterungen $k_i \subseteq k_{i+1}$ normal, denn das Polynom $x^{d_i} - a_i^{d_i} \in k_i[x]$ hat in k_{i+1} die d_i verschiedenen Nullstellen

$$a_i, a_i\xi_i, a_i\xi_i^2, \ldots, a_i\xi_i^{d_i-1}.$$

Also ist k_{i+1} als Zerfällungskörper von $x^{d_i} - a_i^{d_i}$ über k_i normal. Dies liefert uns die Normalreihe

$$\{\mathrm{id}_{k_m}\} = \mathrm{Gal}(k_m, k_m) \trianglelefteq \mathrm{Gal}(k_m, k_{m-1}) \trianglelefteq \cdots \trianglelefteq \mathrm{Gal}(k_m, k_0) = \mathrm{Gal}(k_m, \mathbb{Q})$$

mit den Faktoren

$$\mathrm{Gal}(k_m, k_i) / \mathrm{Gal}(k_m, k_{i+1}) \cong \mathrm{Gal}(k_{i+1}, k_i).$$

Insgesamt haben wir den Beweis also auf die folgende Behauptung reduziert: Für $\mathrm{char}(k) = 0$, $K = k(a)$ mit $a^d \in k$ und $\xi = e^{\frac{2\pi i}{d}} \in k$ ist $G = \mathrm{Gal}(K, k)$ abelsch. Wie eben gezeigt ist a Nullstelle von $p = x^d - a^d \in k[x]$ und p hat in K die verschiedenen Nullstellen $a, \xi a, \xi^2 a, \ldots, \xi^{d-1} a$. Jedes Element von G bildet a auf eine andere Nullstelle von p ab. Falls also $\varphi(a) = a\xi^i$ und $\psi(a) = a\xi^j$ ist, so gilt

$$(\psi \circ \varphi)(a) = \psi(a\xi^i) = \psi(a)\xi^i = a\xi^j\xi^i = a\xi^{j+i} = a\xi^{i+j} = \cdots = (\varphi \circ \psi)(a).$$

Da ein Homomorphismus durch den Wert auf a schon eindeutig bestimmt ist, gilt $\psi \circ \varphi = \varphi \circ \psi$. □

Satz 4.7.4. *Sei d eine Primzahl, $p \in \mathbb{Q}[x]$ irreduzibel vom Grad d und habe genau 2 Nullstellen in $\mathbb{C} \setminus \mathbb{R}$. Für den Zerfällungskörper K von p über $\mathbb{Q}$ gilt dann*

$$\mathrm{Gal}(K, \mathbb{Q}) \cong S_d.$$

Beweis. Das Polynom p hat in $\mathbb{C}$ die verschiedenen Nullstellen $a_1, \ldots, a_d$ und jedes $\varphi \in \mathrm{Gal}(K, \mathbb{Q}) =: G$ permutiert diese. So erhalten wir einen injektiven Gruppenhomomorphismus

$$\iota \colon G \hookrightarrow S_d.$$

Da p reelle Koeffizienten hat, gilt für alle i

$$0 = \overline{0} = \overline{p(a_i)} = p(\overline{a}_i),$$

also ist $\overline{a}_i$ wieder eine Nullstelle von p. Damit gehört die komplexe Konjugation κ zu G und $\iota(\kappa) \in S_d$ ist eine Transposition, da p genau zwei nichtreelle Nullstellen hat. Außerdem gilt

$$\#G = [K : \mathbb{Q}] = [K : \mathbb{Q}(a_1)]\,[\mathbb{Q}(a_1) : \mathbb{Q}] = d \cdot [K : \mathbb{Q}(a_1)]\,,$$

also besitzt G nach dem 1. Sylow-Satz eine Untergruppe der Mächtigkeit d, d.h. ein Element φ der Ordnung d. Da d prim ist, muss $\iota(\varphi) \in S_d$ ein Zykel der Länge d sein, wie man sich (durch Zerlegung in elementfremde Zykel) leicht überlegt. Eine Transposition und ein d-Zykel erzeugen aber bereits ganz S_d (Übungsaufgabe). Also ist ι surjektiv. □

Als Höhe- und Schlusspunkt der Körpertheorie erhalten wir folgendes Ergebnis, das die Frage nach der Auflösbarkeit von Gleichungen vom Grad 5 negativ beantwortet. Fast die gesamte hier entwickelte Theorie wird dafür benutzt.

Korollar 4.7.5. *Für $p = x^5 - 4x + 2 \in \mathbb{Q}[x]$ ist die Gleichung „$p = 0$“ nicht mit Radikalen auflösbar.*

Beweis. Mit dem Eisenstein-Kriterium zur Primzahl 2 sieht man, dass p irreduzibel ist. Die Ableitung $p' = 5x^4 - 4$ ist negativ im Intervall $I = [-\sqrt[4]{4/5}, \sqrt[4]{4/5}]$ und positiv außerhalb. Also ist p innerhalb von I streng monoton fallend und außerhalb von I streng monoton steigend. Damit hat p höchstens 3 reelle Nullstellen. Man berechnet nun

$$p(-2) < 0,\ p(-1) > 0,\ p(1) < 0,\ p(2) > 0$$

und nach dem Zwischenwertsatz hat p also genau drei reelle Nullstellen. Mit Satz 4.7.4 gilt für den Zerfällungskörper K von p

$$\mathrm{Gal}(K, \mathbb{Q}) \cong S_5$$

und diese Gruppe ist nach Korollar 2.5.6 nicht auflösbar. Mit Satz 4.7.3 ist die Gleichung „$p = 0$“ also nicht mit Radikalen auflösbar. □

Kapitel 5

Moduln

In der linearen Algebra untersucht man lineare Gleichungssysteme über Körpern. Dafür gibt es Lösungsmethoden wie den Algorithmus von Gauß. Die zugrundeliegende Theorie ist die Theorie der Vektorräume und linearen Abbildungen. Möchte man nun ein lineares Gleichungssystem über einem Ring lösen, funktionieren viele der Konzepte nicht mehr so einfach, da durch Skalare nicht mehr geteilt werden kann. Die ganze Theorie muss also angepasst werden. Der wichtigste Begriff dabei ist der eines *Moduls*. Dabei handelt es sich um eine Verallgemeinerung von Vektorräumen, indem der zugrundeliegende Skalarkörper durch einen (kommutativen) Ring ersetzt wird.

5.1 Grundlagen

Definition 5.1.1. Sei R ein kommutativer Ring. Ein R**-Modul** ist eine abelsche Gruppe $(M, +)$ mit einer Operation (genannt Skalarmultiplikation)

$$\begin{aligned} R \times M &\to M \\ (r, m) &\mapsto r \cdot m \end{aligned}$$

so dass für alle $r, s \in R$, $m, n \in M$ gilt:

(*i*) $r \cdot (m + n) = (r \cdot m) + (r \cdot n)$.

(*ii*) $(r + s) \cdot m = (r \cdot m) + (s \cdot m)$

(*iii*) $(rs) \cdot m = r \cdot (s \cdot m)$

(iv) $1 \cdot m = m$. △

Beispiel 5.1.2. (i) Ist $R = k$ ein Körper, so ist ein R-Modul genau dasselbe wie ein k-Vektorraum.
(ii) Für jeden Ring R ist R^n auf kanonische Weise ein R-Modul.
(iii) Ist $I \lhd R$ ein Ideal, so ist I ein R-Modul, wobei die Skalarmultiplikation einfach die Ringmultiplikation ist. So ist zum Beispiel $3\mathbb{Z}$ ein $\mathbb{Z}$-Modul und (x, y) ein $k[x, y]$-Modul. Es sind die R-Untermoduln von R sogar genau die Ideale in R.
(iv) Ist $I \lhd R$ ein Ideal, so ist der Faktorring R/I auf kanonische Weise ein R-Modul. So ist zum Beispiel $\mathbb{Z}/3\mathbb{Z}$ ein $\mathbb{Z}$-Modul.
(v) Jede abelsche Gruppe G kann als $\mathbb{Z}$-Modul aufgefasst werden. Dabei definiert man folgende Skalarmultiplikation

$$\begin{aligned} \mathbb{Z} \times G &\to G \\ (z, g) &\mapsto z \cdot g := \underbrace{g + \cdots + g}_{z \text{ mal}}. \end{aligned}$$

(vi) Sei k ein Körper, V ein k-Vektorraum und $f\colon V \to V$ eine k-lineare Abbildung. Dann wird V zu einem Modul über dem Polynomring $k[x]$, durch folgende Skalarmultiplikation:

$$\begin{aligned} k[x] \times V &\to V \\ (p, v) &\mapsto p(f)(v), \end{aligned}$$

wobei wir für $p = c_0 + c_1 x + \cdots + c_d x^d$ definieren

$$p(f)(v) := c_0 v + c_1 f(v) + c_2 f(f(v)) + \cdots + c_d \underbrace{f(f(\cdots f}_{d \text{ mal}}(v)))). \qquad \triangle$$

Bemerkung 5.1.3. Wie üblich vereinbaren wir, dass Skalarmultiplikation stärker bindet als Addition, schreiben also statt $(r \cdot m) + (s \cdot n)$ auch $r \cdot m + s \cdot n$. Auch hier lassen wir das Symbol $\cdot$ oft weg und schreiben also $rm + sn$. △

Definition 5.1.4. (i) Sei M ein R-Modul. Ein R-**Untermodul** U von M ist eine Untergruppe U von M, mit $ru \in U$ für alle $r \in R, u \in U$.
(ii) Seien M, N zwei R-Moduln. Ein R-**Modulhomomorphismus** ist eine Abbildung $f\colon M \to N$ mit

$$f(m + n) = f(m) + f(n) \text{ und } f(rm) = rf(m)$$

für alle $m, n \in M, r \in R$.
(iii) Ein R-**Modulisomorphismus** ist ein R-Modulhomomorphismus, für den ein beidseitig inverser R-Modulhomomorphismus existiert. Zwei R-Moduln M, N heißen **isomorph**, wenn es einen Modulisomorphismus zwischen ihnen gibt. $\triangle$

Bemerkung/Beispiel 5.1.5. (i) Sei R ein (kommutativer) Ring und $A \in \mathrm{Mat}_{m,n}(R)$. Dann ist die Lösungsmenge des linearen Gleichungssystems $Ax = 0$ ein Untermodul von R^n.
(ii) *Nicht* jeder Untermodul von R^n ist die Lösungsmenge eines linearen Gleichungssystems (im Gegensatz zum Vektorraumfall). Ein Beispiel ist $2\mathbb{Z} \subseteq \mathbb{Z}$.
(iii) Sei M ein R-Modul und $W \subseteq M$. Dann ist

$$\mathrm{span}_R(W) := \left\{ \sum_{i=1}^{d} r_i w_i \mid d \in \mathbb{N}, r_i \in R, w_i \in W \right\}$$

der kleinste Untermodul von M, der W enthält.
(iv) Sei k ein Körper, V ein k-Vektorraum, $f\colon V \to V$ k-linear. Wir fassen V wie in Beispiel 5.1.2 als $k[x]$-Modul auf. Dann ist ein k-Untervektorraum $U \subseteq V$ genau dann ein $k[x]$-Untermodul, wenn U f-invariant ist (d.h. wenn $f(U) \subseteq U$ gilt).
(v) Für jeden Modulhomomorphismus $f\colon M \to N$ ist $f(M)$ ein Untermodul von N und

$$\ker(f) := \{m \in M \mid f(m) = 0\}$$

ein Untermodul von M.
(vi) Ein Modulhomomorphismus $f\colon M \to N$ ist genau dann injektiv, wenn

$$\ker(f) = \{0\}$$

gilt.
(vii) Für jeden R-Untermodul $U \subseteq M$ ist die Faktorgruppe M/U auf offensichtliche Weise wieder ein R-Modul.
($viii$) Auch für Moduln gilt der Homomorphiesatz: Ist $f\colon M \to N$ ein Homomorphismus von R-Moduln, so ist der folgende Homomorphismus wohldefiniert und injektiv:

$$\begin{aligned} \overline{f}\colon M/\ker(f) &\hookrightarrow N \\ m + \ker(f) &\mapsto f(m). \end{aligned}$$

$\triangle$

Definition 5.1.6. (i) Ein R-Modul M heißt **endlich erzeugt**, falls es eine endliche Teilmenge $W \subseteq M$ gibt mit $M = \mathrm{span}_R(W)$.
(ii) Eine Familie $(b_i)_{i\in I}$ mit $b_i \in M$ heißt **Basis** von M, falls für alle $m \in M$ *eindeutig bestimmte* $r_i \in R$ existieren (nur endlich viele $r_i \neq 0$) mit

$$m = \sum_{i\in I} r_i b_i.$$

(iii) Ein Modul heißt **frei**, falls er eine Basis besitzt.
(iv) Sind $M_1, \ldots, M_d$ Untermoduln von M, so definieren wir

$$M_1 + \cdots + M_d := \{m_1 + \cdots + m_d \mid m_i \in M_i\}.$$

(v) Hat jedes Element $m \in M_1 + \cdots + M_d$ eine *eindeutige* Darstellung

$$m = m_1 + \cdots + m_d$$

mit $m_i \in M_i$, so schreiben wir statt $M_1 + \cdots + M_d$ auch $M_1 \oplus \cdots \oplus M_d$ und nennen die Summe **direkt**. △

Bemerkung/Beispiel 5.1.7. (i) Jeder k-Vektorraum ist ein freier k-Modul.
(ii) Für jeden Ring R ist R^n ein freier R-Modul. Er besitzt beispielsweise die Standardbasis $e_1, \ldots, e_n$.
(iii) Ist M ein freier R-Modul mit Basis $(b_1, \ldots, b_n)$, so ist M isomorph zu R^n. Einen R-Modulisomorphismus $f\colon M \to R^n$ erhält man beispielsweise, indem man b_i auf e_i abbildet.
(iv) Im Gegensatz zu Vektorräumen besitzt *nicht* jeder Modul eine Basis! So ist etwa $M = \mathbb{Z}/2\mathbb{Z}$ ein $\mathbb{Z}$-Modul ohne Basis. Die einzige mögliche Wahl wäre $b_1 = 1$ und dafür gilt

$$0 = 0 \cdot b_1 = 2 \cdot b_1,$$

die Skalare sind in der Darstellung also nicht eindeutig bestimmt. Also ist M als $\mathbb{Z}$-Modul nicht frei! Wir können M aber natürlich auch als $\mathbb{Z}/2\mathbb{Z}$-Modul auffassen, dann ist er frei (das ist ein Spezialfall von (i)).
(v) Ist $(b_1, \ldots, b_d)$ eine Basis von M, so gilt insbesondere

$$M = \mathrm{span}_R(b_1) \oplus \cdots \oplus \mathrm{span}_R(b_d).$$

Die Direktheit dieser Summe ist aber schwächer als die Basiseigenschaft. Für die Direktheit der Summe müssen nur die Summanden $r_i b_i$ in der Darstellung von

m eindeutig sein, für die Basiseigenschaft benötigt man die Eindeutigkeit der r_i. Betrachtet man etwa den $\mathbb{Z}$-Modul $M = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so gilt

$$M = \operatorname{span}_{\mathbb{Z}}((1,0)) \oplus \operatorname{span}_{\mathbb{Z}}((0,1)),$$

aber $((1,0),(0,1))$ ist keine Basis (das sieht man wie in (ii)).
(vi) $M_1 + \cdots + M_d$ ist der kleinste Untermodul von M welcher alle M_i enthält, stimmt also genau mit $\operatorname{span}_R(M_1 \cup \cdots \cup M_d)$ überein.
(vii) Für zwei Untermoduln M_1, M_2 von M gilt

$$M = M_1 \oplus M_2$$

genau dann wenn $M = M_1 + M_2$ und $M_1 \cap M_2 = \{0\}$.
$(viii)$ Für einen Untermodul M_1 von M muss es im Allgemeinen keinen Untermodul M_2 von M geben mit $M = M_1 \oplus M_2$ (Aufgabe 72). Für Vektorräume stimmt das hingegen, wie man durch Basisergänzung leicht zeigen kann.
(ix) Ein Untermodul eines freien Moduls muss nicht unbedingt selbst wieder frei sein, ein Untermodul eines endlich erzeugten Moduls muss selbst nicht unbedingt wieder endlich erzeugt sein (Aufgabe 72). △

Proposition 5.1.8. *Sei R ein noetherscher Ring, M ein endlich erzeugter R-Modul, sowie $N \subseteq M$ ein R-Untermodul. Dann ist N selbst endlich erzeugt.*

Beweis. Wir beweisen die Aussage zunächst im Fall $M = R^n$ per Induktion über n. Der Fall $n = 1$ ist dabei einfach die Aussage dass R noethersch ist. Im allgemeinen Fall betrachten wir die Projektion $\pi\colon R^n \to R$ auf die erste Koordinate, das Ideal

$$I := \pi(N) \subseteq R$$

sowie den Untermodul

$$K := N \cap \ker(\pi) \subseteq N.$$

Da R noethersch ist, gibt es $n_1, \ldots, n_d \in N$ mit $I = (\pi(n_1), \ldots, \pi(n_d))$. Damit gilt nun

$$N = \operatorname{span}_R\{n_1, \ldots, n_d\} + K,$$

wie man sich leicht überlegt. K besteht aber genau aus den Elementen von N mit Null in der ersten Komponente. Damit kann K offensichtlich als Untermodul von R^{n-1} aufgefasst werden und ist somit nach Induktionsvoraussetzung endlich erzeugt. Damit ist aber auch N endlich erzeugt.

Im allgemeinen Fall gelte $M = \operatorname{span}_R\{m_1, \dots, m_n\}$ und wir betrachten den surjektiven Modulhomomorphismus

$$\begin{aligned} \varphi\colon R^n &\twoheadrightarrow M \\ (r_1, \dots, r_n) &\mapsto r_1 m_1 + \dots + r_n m_n. \end{aligned}$$

Dann ist $\varphi^{-1}(N) \subseteq R^n$ ein Untermodul und somit endlich erzeugt. Wegen

$$N = \varphi(\varphi^{-1}(N))$$

ist dann aber auch N endlich erzeugt. □

Zum Abschluss dieses Abschnitts wollen wir noch die Eindeutigkeit der Länge einer Basis beweisen (falls eine solche exisitiert). Das folgende Lemma wird es uns erlauben, die Aussage auf den Vektorraumfall zurückzuführen.

Lemma 5.1.9. *Sei M ein R-Modul, $W \subseteq M$ und $I \lhd R$ ein Ideal.*

(i) Es ist $IM := \left\{ \sum_{k=1}^{d} i_k m_k \mid d \in \mathbb{N}, i_k \in I, m_k \in M \right\}$ ein R-Untermodul von M.

(ii) Die folgende Skalarmultiplikation ist wohldefiniert und macht den R-Modul M/IM sogar zu einem R/I-Modul:

$$\begin{aligned} R/I \times M/IM &\to M/IM \\ (r + I, m + IM) &\mapsto rm + IM. \end{aligned}$$

(iii) Aus $M = \operatorname{span}_R(W)$ folgt $M/IM = \operatorname{span}_{R/I}(w + IM \mid w \in W)$.

(iv) Ist $(b_j)_{j\in J}$ eine Basis des R-Moduls M, so ist $(b_j + IM)_{j\in J}$ eine Basis des R/I-Moduls M/IM.

Beweis. Aufgabe 73. □

Satz 5.1.10. *Sei $R \neq 0$ und M ein freier R-Modul. Dann haben je zwei Basen von M dieselbe Mächtigkeit. Jedes Erzeugendensystem hat mindestens diese Mächtigkeit.*

Beweis. Wir führen die Aussage mit Lemma 5.1.9 auf den Vektorraumfall zurück, wo die Aussage aus der linearen Algebra bekannt ist. Seien dazu also $(a_i)_{i\in I}$ sowie $(b_j)_{j\in J}$ zwei Basen des R-Moduls M, sowie $W \subseteq M$ ein Erzeugendensystem.

Wir wählen ein maximales Ideal $\mathfrak{m} \subseteq R$ (mit Satz 3.3.5) und erhalten aus Lemma 5.1.9, dass

$$(a_i + \mathfrak{m}M)_{i\in I} \text{ und } (b_j + \mathfrak{m}M)_{j\in J}$$

jeweils Basen des $R/\mathfrak{m}$-Moduls $M/\mathfrak{m}M$ sind, sowie $\{w + \mathfrak{m}M \mid w \in W\}$ ein Erzeugendensystem. Es ist aber $R/\mathfrak{m}$ ein Körper (Satz 3.3.4), also ist $M/\mathfrak{m}M$ ein Vektorraum über $R/\mathfrak{m}$, und somit gilt

$$\#I = \#J \leq \#\{w + \mathfrak{m}M \mid w \in W\} \leq \#W. \qquad \square$$

Definition 5.1.11. Der **Rang** eines freien R-Moduls M ist definiert als die (eindeutig bestimmte) Mächtigkeit einer R-Basis von M. $\triangle$

5.2 Lineare Gleichungen und Moduln über Hauptidealringen

In diesem Abschnitt sei stets $R \neq 0$ ein *nullteilerfreier Hauptidealring*, also beispielsweise ein Körper $k, \mathbb{Z}, k[x]$ oder $\mathbb{Z}[i]$. Den Quotientenkörper von R bezeichnen wir mit K. Gegeben sei nun eine Matrix $A \in \mathrm{Mat}_{m,n}(R)$ und ein $b \in R^m$. Wir wollen das lineare Gleichungssystem $Ax = b$ über R lösen, also die folgende Menge möglichst gut beschreiben:

$$L(A, b) := \{a \in R^n \mid Aa = b\}.$$

Für $z \in L(A, b)$ gilt offensichtlich genau wie in der linearen Algebra

$$L(A, b) = z + L(A, 0)$$

und $L(A, 0)$ besitzt laut Proposition 5.1.8 als Untermodul von R^n ein endliches Erzeugendensystem. Wir können also die Lösungsmenge mit endlich vielen Daten vollständig angeben. In Wirklichkeit gibt es hier sogar immer eine Basis, wie wir später sehen werden. Wir fragen uns aber zuerst, wie wir Lösungen des Gleichungssystems algorithmisch finden können.
Sei dazu

$$\mathrm{GL}_n(R) := \mathrm{Mat}_n(R)^\times$$

die Menge der $n \times n$-Matrizen, die im Matrixring über R eine inverse Matrix besitzen. Man beachte dass $\mathrm{GL}_n(R)$ im Allgemeinen kleiner als $\mathrm{GL}_n(K) \cap \mathrm{Mat}_n(R)$

ist, da die inverse Matrix einer Matrix über R nicht unbedingt Einträge aus R besitzen muss. An der Formel

$$A \cdot A^{\mathrm{adj}} = \det(A) \cdot I_n$$

sieht man aber, dass eine Matrix genau dann über R invertierbar ist, wenn $\det(A) \in R^\times$ gilt.

Satz 5.2.1 (Smith-Normalform)**.** *Sei R ein nullteilerfreier Hauptidealring und $A \in \mathrm{Mat}_{m,n}(R)$. Dann gibt es $S \in \mathrm{GL}_m(R), T \in \mathrm{GL}_n(R)$ und*

$$r_1, \ldots, r_{\min(n,m)} \in R \text{ mit } r_1 \mid r_2 \mid \cdots \mid r_{\min(m,n)}$$

mit

$$SAT = \begin{pmatrix} r_1 & 0 & 0 & 0 \\ 0 & r_2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \end{pmatrix}.$$

Beweis. Wir geben in Algorithmus 5.2.2 einen expliziten Algorithmus an, der die Smith Normalform produziert. Die dabei auftretenden Transformationen können alle durch Multiplikation von links und rechts mit über R invertierbaren Matrizen ausgeführt werden. □

Algorithmus 5.2.2. Sei $A = (a_{ij})_{i,j} \in \mathrm{Mat}_{m,n}(R)$ nicht die Nullmatrix.
(i) Durch Vertauschung von Zeilen und Spalten können wir $a_{11} \neq 0$ erreichen. Vertauschen von Zeilen oder Spalten entsteht durch Multiplikation von links bzw. rechts mit den entsprechenden Elementarmatrizen, die auch über R invertierbar sind.
(ii) Die Idee ist nun, an der Stelle $(1,1)$ den größten gemeinsamen Teiler von a_{11} und a_{21} zu erzeugen und damit dann den Eintrag $(2,1)$ zu eliminieren. Da R ein Hauptidealring ist, gilt

$$(a_{11}, a_{21}) = (\alpha)$$

wobei $\alpha = \mathrm{ggT}(a_{11}, a_{21}) \in R$ ist. Es gibt also Gleichungen

$$ra_{11} + sa_{21} = \alpha,\ t\alpha = a_{11},\ u\alpha = a_{21}$$

mit $r, s, t, u \in R$. Die Matrix

$$E = \begin{pmatrix} r & s & 0 \\ -u & t & 0 \\ 0 & 0 & I_{m-2} \end{pmatrix}$$

ist über R invertierbar, denn es gilt

$$\det(E) \cdot \alpha = (rt + su)\alpha = ra_{11} + sa_{21} = \alpha,$$

also $\det(E) = 1$.
In der Matrix EM steht nun an der Stelle $(1,1)$ gerade α, an der Stelle $(2,1)$ steht 0. Wir iterieren diesen Prozess und erhalten $a_{i1} = 0$ für $i = 2, \ldots, m$.
(iii) Nun wiederholen wir Schritt (ii) und elimieren diesmal alle Einträge a_{1j} für $j = 2, \ldots, n$. Dabei multiplizieren wir die Matrix M von rechts mit invertierbaren Matrizen.
(iv) Dummerweise können nun an den Stellen a_{i1} wieder Einträge $\neq 0$ entstanden sein (wenn wir in Schritt (iii) ein Vielfaches einer Spalte zu einem Vielfachen der ersten Spalte addiert haben). Wir starten nun mit Schritt (ii) erneut, und erreichen wieder $a_{i1} = 0$ für $i = 2, \ldots, m$. Danach verwenden wir wieder Schritt (iii) ..... Man beachte nun, dass der Eintrag a_{11} jedes Mal durch einen seiner Teiler ersetzt wird. Ein Hauptidealring ist noethersch, also gibt es keine unendlichen Teilerketten. Nach endlich vielen Schritten ändert sich a_{11} also nicht mehr, also gilt $a_{11} \mid a_{i1}, a_{1j}$ für alle i, j. Nun können wir alle a_{i1}, a_{1j} gleichzeitig eliminieren, durch Addition eines Vielfachen der ersten Zeile/Spalte zu den anderen Zeilen/Spalten.
(v) Wir ignorieren die erste Zeile und Spalte von M und starten erneut mit Schritt (i). Dabei erhalten wir am Schluss eine Matrix der gewünschten Diagonalform. Nur die Teilerbedingung an die Diagonaleinträge müssen noch nicht erfüllt sein. Wenn also r_i kein Teiler von r_{i+1} ist, so addieren wir zunächst die $(i+1)$-te Spalte von M zur i-ten, und verwenden dann die Schritte (ii) und (iii) um die entstandene 2×2-Matrix

$$\begin{pmatrix} r_i & 0 \\ r_{i+1} & r_{i+1} \end{pmatrix}$$

wieder zu diagonalisieren. Keine andere Spalte von M ist davon betroffen. Dabei wird r_i durch einen Teiler von $\mathrm{ggT}(r_i, r_{i+1})$ ersetzt, und r_{i+1} durch ein Vielfaches von sich selbst. Am Ende gilt also die Teilerbedingung. Wir führen diese Operation in wahlloser Weise immer dann aus, wenn sie noch nötig ist. Wiederum kann das nicht unendlich oft der Fall sein, weil sonst aus einem r_i eine unendliche Teilerkette entstehen würde.
(vi) Die Matrizen S und T erhalten wir, indem wir alle Zeilen- bzw. Spaltentransformationen simultan an I_m bzw. I_n ausführen. △

Bemerkung 5.2.3. (i) Wenn man die Smith-Normalform und die Matrizen S, T kennt, kann man das Gleichungssystem $Ax = b$ über R einfach lösen. Man löst

zunächst das System $SATx = Sb$, von dem man die Lösungen in R leicht ablesen kann. Dadurch erhält man durch Anwendung von T auf die Lösungen gerade die Lösungsmenge des ursprünglichen Systems.
(ii) Im Algorithmus muss immer wieder ein Vielfaches der i-ten Zeile/Spalte zu einem Vielfachen der j-ten Zeile/Spalte addiert werden. Das Skalieren dieser j-ten Zeile/Spalte ist über einem Ring im Allgemeinen nicht invertierbar. Wir beheben das Problem, indem wir gleichzeitig die i-te Zeile/Spalte ebenfalls durch eine geeignete Linearkombination der beiden Zeilen/Spalten ersetzen. Genau das ist in der Matrix E aus Schritt (ii) des Algorithmus kodiert. Dadurch wird auch automatisch der gewünschte Eintrag eliminiert.
(iii) Im Algorithmus sehen wir, dass wir in R immer wieder $\mathrm{ggT}(a, b)$ und eine Darstellung

$$\mathrm{ggT}(a, b) = ra + sb$$

berechnen müssen. Das tut man wenn möglich mit dem euklidische Algorithmus, den wir in Abschnitt 3.6 beschrieben haben. △

Wir zeigen nun an zwei Beispielen, wie ein lineares Gleichungssystem über einem euklidischen Ring gelöst wird, indem wir die Smith-Normalform der Koeffizientenmatrix berechnen.

Beispiel 5.2.4. Wir wollen herausfinden, für welche Werte $a, b, c \in \mathbb{Z}$ das folgende Gleichungssystem ganzzahlige Lösungen besitzt, und diese bestimmen:

$$\begin{aligned} 4x - 11y - 2z &= a \\ 5x + 13y + 4z &= b \\ -10x + 23y + 8z &= c. \end{aligned}$$

Dazu betrachten wir die Koeffizientenmatrix

$$A = \begin{pmatrix} 4 & -11 & -2 \\ 5 & 13 & 4 \\ -10 & 23 & 8 \end{pmatrix}$$

und verwenden den Algorithmus zur Bestimmung der Smith-Normalform. Die Matrix E aus dem ersten Schritt des Algorithmus der SNF lautet

$$E_1 = \begin{pmatrix} -1 & 1 & 0 \\ -5 & 4 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

und wir erhalten

$$E_1 A = \begin{pmatrix} 1 & 24 & 6 \\ 0 & 107 & 26 \\ -10 & 23 & 8 \end{pmatrix}.$$

Wir können nun erfreulicherweise direkt alles unter und rechts der 1 eliminieren:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 107 & 26 \\ 0 & 263 & 68 \end{pmatrix}.$$

Wir rechnen nun mit dem unteren rechten 2×2-Block weiter. Wir erhalten

$$E_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 59 & -24 \\ 0 & -263 & 107 \end{pmatrix}$$

sowie

$$E_2 \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 107 & 26 \\ 0 & 263 & 68 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -98 \\ 0 & 0 & 438 \end{pmatrix}.$$

Nun eliminieren wir noch die -98 und erhalten als Smith-Normalform

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 438 \end{pmatrix}.$$

Wenn wir die jeweiligen Zeilen- und Spaltenoperationen noch an der Einheitsmatrix ausführen, erhalten wir als Basiswechselmatrizen

$$S = \begin{pmatrix} -1 & 1 & 0 \\ -55 & -4 & -24 \\ 245 & 18 & 107 \end{pmatrix} \text{ und } T = \begin{pmatrix} 1 & -24 & -2358 \\ 0 & 1 & 98 \\ 0 & 0 & 1 \end{pmatrix}.$$

Statt des ursprünglichen Systems lösen wir nun also das System

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 438 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = S \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} -a + b \\ -55a - 4b - 24c \\ 245a + 18b + 107c \end{pmatrix}.$$

Somit hat das System genau dann eine Lösung, wenn 438 ein Teiler von $245a + 18b + 107c$ ist, die Lösung lautet dann

$$(x, y, z) = (-a + b, -55a - 4b - 24c, (245a + 18b + 107c)/438).$$

Durch Anwendung von T darauf erhält man die eindeutige Lösung des ursprünglichen Systems:

$$(x, y, z) = 1/438 \cdot (12a + 42b - 18c, -80a + 12b - 26c, 245a + 18b + 107c). \qquad \triangle$$

Beispiel 5.2.5. Wir wollen ein lineares Gleichungssystem über dem Polynomring $\mathbb{Q}[t]$ lösen:

$$\begin{aligned} tx + (t^2 + 1)y &= t^4 + 2t^2 + t \\ t^2x - ty &= t^2. \end{aligned}$$

Wenn wir die Koeffizientenmatrix

$$A = \begin{pmatrix} t & t^2 + 1 \\ t^2 & -t \end{pmatrix}$$

von links mit

$$E_1 = \begin{pmatrix} 1 & 0 \\ -t & 1 \end{pmatrix}$$

multiplizieren, erhalten wir

$$\begin{pmatrix} t & 1 + t^2 \\ 0 & -t(t^2 + 2) \end{pmatrix}.$$

Wir multiplizieren nun von rechts mit

$$E_2 = \begin{pmatrix} -t & -(t^2 + 1) \\ 1 & t \end{pmatrix}$$

und erhalten

$$\begin{pmatrix} 1 & 0 \\ -t(t^2 + 2) & -t^2(t^2 + 2) \end{pmatrix}.$$

Hier haben wir nun an der Stelle $(2, 1)$ wieder einen nichttrivialen Eintrag erhalten. Diesen können wir aber direkt mit der 1 eliminieren. Insgesamt erhält man die SNF

$$\begin{pmatrix} 1 & 0 \\ 0 & -t^2(t^2 + 2) \end{pmatrix}$$

sowie

$$S = \begin{pmatrix} 1 & 0 \\ t^3 + t & 1 \end{pmatrix} \text{ und } T = \begin{pmatrix} -t & -(t^2 + 1) \\ 1 & t \end{pmatrix}.$$

Das transformierte Gleichungssystem $SATx = Sb$ lautet dann

$$\begin{pmatrix} 1 & 0 \\ 0 & -t^2(t^2+2) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} t(t^3+2t+1) \\ t^2(t^5+3t^3+t^2+2t+2) \end{pmatrix}$$

und wir erhalten die eindeutige Lösung

$$(x, y) = (t(t^3+2t+1), -(t^3+t+1)).$$

Durch Multiplikation mit T erhalten wir die eindeutige Lösung der ursprünglichen Systems:

$$(x, y) = (t+1, t^2). \qquad \triangle$$

Mit Hilfe der Smith Normalform können wir nun einen eleganten Beweis des sogenannten Elementarteilersatzes geben.

Satz 5.2.6 (Elementarteilersatz)**.** *Es sei R ein nullteilerfreier Hauptidealring und $M \subseteq R^n$ ein R-Untermodul. Dann gilt:*

(i) *M ist frei vom Rang $m \leq n$.*

(ii) *Es gibt eine Basis $(b_1, \ldots, b_n)$ von R^n und $r_1, \ldots, r_m \in R$ mit*

$$r_1 \mid r_2 \mid \cdots \mid r_m,$$

so dass $(r_1 b_1, \ldots, r_m b_m)$ eine Basis von M ist.

Beweis. Mit Proposition 5.1.8 wissen wir bereits dass M endlich erzeugt ist. Wir wählen also Erzeuger $m_1, \ldots, m_d$ und schreiben sie in die Spalten der Matrix A:

$$A = (m_1, \ldots, m_d) \in \mathrm{Mat}_{n,d}(R).$$

Mit Satz 5.2.1 erhalten wir die Smith Normalform

$$AT = S^{-1} \begin{pmatrix} r_1 & 0 & 0 & 0 \\ 0 & r_2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \end{pmatrix}. \tag{5.1}$$

Als Basis $b_1, \ldots, b_n$ von R^n wählen wir nun die Spalten von S^{-1}. Es seien nun $r_1, \ldots, r_m$ genau die Diagonaleinträge $r_i \neq 0$. Dabei gilt $m \leq n$ und wir zeigen nun dass $r_1 b_1, \ldots, r_m b_m$ wirklich eine Basis von M bildet. An Gleichung 5.1 sieht

man, dass alle $r_i b_i$ in M liegen. Es sind ja gerade Spalten der Matrix auf der rechten Seite, und die linke Seite zeigt dass diese Linearkombinationen der m_i sind. Multipliziert man die Gleichung von rechts mit T^{-1} sieht man genauso, dass alle m_i Linearkombinationen der $r_i b_i$ sind, und damit bilden $r_1 b_1, \dots, r_m b_m$ ein Erzeugendensystem von M. Mit $b_1, \dots, b_n$ sind aber natürlich auch $r_1 b_1, \dots, r_m b_m$ linear unabhängig über R. Dafür verwenden wir $r_i \neq 0$ und die Nullteilerfreiheit von R. Damit ist der Satz bewiesen. □

Korollar 5.2.7. *Sei R ein nullteilerfreier Hauptidealring und M ein endlich erzeugter R-Modul. Dann gibt es Primelemente $p_1, \dots, p_d \in R$ sowie $m, e_1, \dots e_d \in \mathbb{N}$ mit*

$$M \cong R^m \times R/(p_1^{e_1}) \times \cdots \times R/(p_d^{e_d}).$$

Frei ist M genau dann, wenn $M^{\mathrm{tor}} = \{0\}$, wobei

$$M^{\mathrm{tor}} := \{m \in M \mid \exists r \in R, r \neq 0 \colon rm = 0\}.$$

Beweis. Sei $M = \mathrm{span}_R(w_1, \dots, w_n)$ und betrachte den surjektiven R-Modulhomomorphismus

$$\begin{aligned} \pi \colon R^n &\twoheadrightarrow M \\ e_i &\mapsto w_i, \quad i = 1, \dots, n. \end{aligned}$$

Es ist $\ker(\pi)$ ein Untermodul von R^n und mit dem Homomorphiesatz gilt $M \cong R^n/\ker(\pi)$. Wir betrachten also nur noch den Modul $R^n/\ker(\pi)$. Nach Satz 5.2.6 gibt es eine Basis $b_1, \dots, b_n$ von R^n und Ringelemente $r_1, \dots, r_m$, so dass $r_1 b_1, \dots, r_m b_m$ eine Basis von $\ker(\pi)$ ist. Wir betrachten nun den Basiswechsel-Isomorphismus

$$\begin{aligned} \varphi \colon R^n &\to R^n \\ b_i &\mapsto e_i, \quad i = 1, \dots, n \end{aligned}$$

und sehen dass $\varphi(\ker(\pi))$ gerade $r_1 e_1, \dots, r_m e_m$ als Basis hat. Also gilt

$$R^n/\ker(\pi) \cong R^n/\left(\mathrm{span}_R(r_1 e_1, \dots, r_m e_m)\right) \cong R/(r_1) \times \cdots \times R/(r_m) \times R^{n-m}.$$

Jedes Element r_i kann in R aber in Primfaktoren zerlegt werden. Mit dem chinesischen Restsatz (Satz 3.1.11) gilt

$$R/(ab) \cong R/(a) \times R/(b)$$

für teilerfremde Elemente $a, b \in R$. Daraus folgt die gewünschte Isomorphie.
Es ist nun offensichtlich $M^{\mathrm{tor}} = \{0\}$ äquivalent dazu, dass in der Zerlegung von M kein Faktor vom Typ $R/(p_i^{e_i})$ auftritt, also zu $M \cong R^m$. □

Korollar 5.2.8 (Struktursatz für endlich erzeugte abelsche Gruppen)**.** *Sei G eine endlich erzeugte abelsche Gruppe. Dann gibt es Primzahlen $p_1, \dots, p_d \in \mathbb{Z}$ und Zahlen $m, e_1, \dots, e_d \in \mathbb{N}$ mit*

$$G \cong \mathbb{Z}^m \times \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_d^{e_d}\mathbb{Z}.$$

Beweis. Jede abelsche Gruppe ist ein $\mathbb{Z}$-Modul, wie in Beispiel 5.1.2 (v) beschrieben. Also folgt die Aussage direkt aus Korollar 5.2.7, da Gruppenhomomorphismen hier dasselbe wie Modulhomomorphismen sind. □

5.3 Das Tensorprodukt

Tensorprodukte tauchen in vielen Gebieten der Algebra auf. Es sind Konstruktionen, mit denen man Bilinearität in Linearität verwandeln kann. Ihre explizite Konstruktion ist relativ mühsam, deshalb führt man sie oft erst über ihre wichtigste Eigenschaft ein (ihre sogenannte *universelle Eigenschaft*). Beweise mit Tensorprodukten sollte man dann am besten auch nur mit Hilfe dieser Eigenschaft führen, alles andere ist meistens viel zu mühsam.

Definition 5.3.1. Seien M, N zwei R-Moduln. Ein **Tensorprodukt** von M und N ist ein R-Modul T, zusammen mit einer R-bilinearen Abbildung

$$\varphi\colon M \times N \to T,$$

so dass jede andere R-bilineare Abbildung $\psi\colon M \times N \to P$ eindeutig *linear* über T faktorisiert:

$$\begin{array}{ccc} M \times N & \xrightarrow{\varphi} & T \\ & \searrow^{\psi} & \downarrow{\scriptstyle \exists!\tilde{\psi}} \\ & & P \end{array}$$

Für jeden R-Modul P und jede R-bilineare Abbildung $\psi\colon M \times N \to P$ muss es also eine eindeutige R-lineare Abbildung $\tilde{\psi}\colon T \to P$ geben mit

$$\psi = \tilde{\psi} \circ \varphi.$$ △

Satz 5.3.2. *Für je zwei R-Moduln M, N existiert ein Tensorprodukt. Es ist bis auf eindeutige Isomorphie eindeutig bestimmt. Wir bezeichnen es auch mit*

$$M \otimes_R N.$$

Beweis. Existenz: Sei F der freie R-Modul mit Basis $((m,n))_{(m,n)\in M\times N}$. Elemente von F sind also endliche formale R-Linearkombinationen von Elementen aus $M \times N$. In F betrachten wir nun den Untermodul U, der von allen Elementen der folgenden Gestalt erzeugt wird:

$$\begin{aligned}(m+m',n)-(m,n)-(m',n)\\(m,n+n')-(m,n)-(m,n')\\(rm,n)-r(m,n)\\(m,rn)-r(m,n).\end{aligned}$$

Dabei erlauben wir alle $m, m' \in M, n, n' \in N$ und $r \in R$. Dann ist F/U ein Tensorprodukt von M und N. Wir betrachten dazu die Abbildung

$$\begin{aligned}\varphi\colon M\times N &\to F/U\\(m,n) &\mapsto (m,n)+U,\end{aligned}$$

die nach Definition von U offensichtlich R-bilinear ist. Sei nun $\psi\colon M \times N \to P$ eine weitere R-bilineare Abbildung in einen R-Modul P. Wir erhalten damit zunächst eine wohldefinierte R-lineare Abbildung

$$\begin{aligned}\Psi\colon F &\to P\\(m,n) &\mapsto \psi(m,n),\end{aligned}$$

da F die Tupel (m,n) gerade als Basis hat. Aufgrund der Bilinearität von ψ liegt U aber im Kern von Ψ, also gibt es den wohldefinierten Morphismus

$$\begin{aligned}\tilde{\psi}\colon F/U &\to P\\(m,n)+U &\mapsto \psi(m,n),\end{aligned}$$

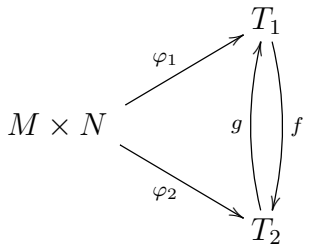
der offensichtlich $\psi = \tilde{\psi} \circ \varphi$ erfüllt. Durch diese Bedingung ist aber $\tilde{\psi}$ auch eindeutig bestimmt, da F/U von den Elementen

$$\varphi(m,n) = (m,n)+U$$

erzeugt wird.
Eindeutigkeit: Seien

$$\varphi_1\colon M\times N\to T_1 \text{ und } \varphi_2\colon M\times N\to T_2$$

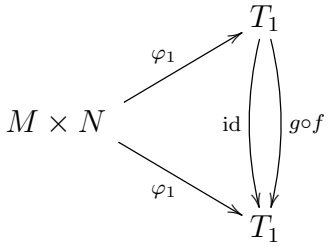
zwei Tensorprodukte von M und N. Da φ_2 bilinear ist und T_1 die universelle Eigenschaft des Tensorprodukts erfüllt, gibt es genau einen Morphismus $f\colon T_1 \to T_2$ mit $\varphi_2 = f \circ \varphi_1$. Umgekehrt gibt es genau einen Morphismus $g\colon T_2 \to T_1$ mit $\varphi_1 = g \circ \varphi_2$:



Dann ist aber $g \circ f\colon T_1 \to T_1$ ein Morphismus mit

$$(g \circ f) \circ \varphi_1 = g \circ (f \circ \varphi_1) = g \circ \varphi_2 = \varphi_1,$$

und aus der Eindeutigkeit von $\tilde{\psi}$ in der universellen Eigenschaft von T_1 folgt $g \circ f = \mathrm{id}_{T_1}$:



Genauso folgt $f \circ g = \mathrm{id}_{T_2}$, und damit die Aussage. □

Bemerkung/Beispiel 5.3.3. (i) Die Restklasse $(m,n)+U$ bezeichnen wir auch mit $m \otimes n$, und nennen sie einen **Elementartensor**. Es ist jedoch nicht jedes Element in $M \otimes_R N$ ein Elementartensor, man muss auch Summen zulassen:

$$M \otimes_R N = \left\{ \sum_{i=1}^{d} m_i \otimes n_i \mid d \in \mathbb{N}, m_i \in M, n_i \in N \right\}.$$

Nach Konstruktion gelten die folgenden Rechenregeln in $M \otimes_R N$:

$$\begin{aligned} (m+m') \otimes n &= m \otimes n + m' \otimes n \\ m \otimes (n+n') &= m \otimes n + m \otimes n' \\ (rm) \otimes n &= r \cdot (m \otimes n) = m \otimes (rn) \end{aligned}$$

(ii) Will man eine wohldefinierte lineare Abbildung $M \otimes_R N \to P$ angeben, gibt man gewöhnlich zunächst eine R-bilineare Abbildung $M \times N \to P$ an, und verwendet die universelle Eigenschaft des Tensorprodukts. Zum Beispiel gilt folgende Aussage: Sind

$$f\colon M \to P \text{ und } g\colon N \to Q$$

Morphismen, so gibt es einen Morphismus

$$f \otimes g\colon M \otimes_R N \to P \otimes_R Q$$

mit

$$(f \otimes g)(m \otimes n) = f(m) \otimes g(n).$$

Das sieht man am besten folgendermaßen. Die Abbildung

$$\begin{aligned} f \times g\colon M \times N &\to P \otimes_R Q \\ (m, n) &\mapsto f(m) \otimes g(n) \end{aligned}$$

ist R-bilinear. Mit der universellen Eigenschaft von $M \otimes_R N$ folgt nun die Existenz von $f \otimes g$.
(iii) In manchen Fällen kann man das Tensorprodukt auch konkreter realisieren als im oberen Beweis. Beispielsweise gilt für einen Ring R stets

$$R^m \otimes_R R^n \cong \mathrm{Mat}_{m,n}(R) \cong R^{mn}.$$

Dazu betrachtet man die bilineare Abbildung

$$\begin{aligned} R^m \times R^n &\to \mathrm{Mat}_{m,n}(R) \\ (v, w) &\mapsto vw^t = (v_i w_j)_{i,j} \end{aligned}$$

und rechnet die universelle Eigenschaft nach (Aufgabe 85). Die Elementartensoren sind dabei gerade die Matrizen vom Rang 1.
Auf ähnliche Weise zeigt man

$$R[x] \otimes_R R[y] \cong R[x, y].$$

(iv) Über das Tensorprodukt kann man **Koeffizientenerweiterung** durchführen. Sei dazu zunächst $\varphi\colon R \to S$ ein Ringhomomorphismus. Dann kann man jeden S-Modul N auch als R-Modul auffassen, vermöge

$$r \cdot n := \varphi(r) \cdot n.$$

Umgekehrt kann man einen R-Modul M aber nicht notwendigerweise auch als S-Modul auffassen. Deshalb bemerkt man zunächst, dass S vermöge φ selbst ein R-Modul ist:

$$r \cdot s := \varphi(r) \cdot s.$$

Dann betrachtet man den R-Modul

$$M_S := M \otimes_R S.$$

Auf M_S ist nun sogar eine Skalarmultiplikation aus S wohldefiniert:

$$s \cdot \sum_i m_i \otimes s_i := \sum_i m_i \otimes ss_i.$$

Auf diese Weise kann man M_S als S-Modul auffassen (Aufgabe 84).
Ist zum Beispiel V ein k-Vektorraum und $\varphi\colon k \to K$ eine Körpererweiterung, so ist $V_K = V \otimes_k K$ ein K-Vektorraum. Zum Beispiel gilt

$$\mathbb{R}^n_{\mathbb{C}} = \mathbb{R}^n \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C}^n.$$

(v) Tensorprodukte von Moduln können unerwartete Eigenschaften haben. Betrachten wir beispielsweise $\mathbb{Q}$ und $\mathbb{Z}/n\mathbb{Z}$ als $\mathbb{Z}$-Moduln, so gilt

$$\mathbb{Q} \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) = \{0\}.$$

Das sieht man am besten so:

$$\begin{aligned} q \otimes \overline{m} &= (n \cdot \frac{q}{n}) \otimes \overline{m} = n \cdot \left(\frac{q}{n} \otimes \overline{m}\right) = \frac{q}{n} \otimes (n \cdot \overline{m}) \\ &= \frac{q}{n} \otimes \overline{0} = \frac{q}{n} \otimes (0 \cdot \overline{0}) = 0 \cdot \left(\frac{q}{n} \otimes \overline{0}\right) = 0. \end{aligned}$$ △

5.4 Ganze Ringerweiterungen und Hilberts Nullstellensatz

In diesem Abschnitt verallgemeinern wir den Begriff einer algebraischen Körpererweiterung auf Ringe. Wenn man sich die Beispiele und Beweise aus dem Körperkapitel anschaut, sieht man dass eine algebraische Gleichung fast immer erstmal normiert wurde, indem man durch den Leitkoeffizienten dividiert. Über Ringen geht das im Allgemeinen nicht. Also müssen wir die Normiertheit der Gleichung eben von Anfang an voraussetzen. Anstelle von *algebraisch* sagt man im Ringkontext dann *ganz*, was sich mit Bemerkung 5.4.2 (ii) unten erklären lässt.

Definition 5.4.1. Sei $R \subseteq S$ eine Ringerweiterung.
(i) Ein Element $b \in S$ heißt **ganz über** R, falls $a_0, \ldots, a_{n-1} \in R$ existieren mit

$$a_0 + a_1 b + \cdots + a_{n-1} b^{n-1} + b^n = 0.$$

Eine solche Gleichung heißt **Ganzheitsgleichung** für b über R.
(ii) S heißt **ganz über** R, falls jedes Element $b \in S$ ganz über R ist. △

Bemerkung 5.4.2. (i) Wichtig am Begriff der Ganzheit ist, dass die Gleichung für b *normiert* sein muss. Sind R und S Körper, so kann man jede nichttriviale Gleichung normieren. Also ist ein ganzes Element dann einfach ein algebraisches Element.
(ii) Für $\mathbb{Z} \subseteq \mathbb{Q}$ sind die einzigen über $\mathbb{Z}$ ganzen Elemente von $\mathbb{Q}$ die Elemente aus $\mathbb{Z}$ selbst. Das stimmt noch allgemeiner für die Inklusion $R \subseteq K$ eines nullteilerfreien faktoriellen Rings in seinen Quotientenkörper (Aufgabe 88).
(iii) Für $R \subseteq S$ und $b_1, \ldots, b_m \in S$ erinnern wir an die Definition von $R[b_1, \ldots, b_m]$ als den Teilring von S, der von $b_1, \ldots, b_m$ und R erzeugt wird, also

$$R[b_1, \ldots, b_m] = \left\{ \sum_{e \in \mathbb{N}^m} a_e b_1^{e_1} \cdots b_m^{e_m} \mid a_e \in R \right\}.$$

Wenn man S als R-Modul auffasst, ist $R[b_1, \ldots, b_m]$ ein Untermodul, also insbesondere selbst ein R-Modul. △

Der folgende Satz ist eine Variante von Satz 4.2.9 für Ringerweiterungen bzw. für deren Ganzheit:

Satz 5.4.3. *Sei $R \subseteq S$ eine Ringerweiterung und $b_1, \ldots, b_m \in S$. Dann sind die folgenden Aussagen äquivalent:*

(i) $b_1, \ldots, b_m$ *sind ganz über* R.

(ii) $R[b_1, \ldots, b_m]$ *ist als* R*-Modul endlich erzeugt.*

(iii) $R[b_1, \ldots, b_m]$ *ist ganz über* R.

Beweis. (i) $\Rightarrow$ (ii): Durch Auflösen einer Ganzheitsgleichung für b_1 nach b_1^n erhält man

$$b_1^n = -\left(a_{n-1} b_1^{n-1} + \cdots + a_0\right)$$

für gewisse $a_i \in R$. Man kann die n-te Potenz von b_1 also immer durch niedrigere Potenzen von b_1 und Koeffizienten aus R ersetzen. Verfährt man analog mit den

anderen b_i sieht man, dass $R[b_1, \ldots, b_m]$ von endlich vielen Produkten $b_1^{e_1} \cdots b_m^{e_m}$ erzeugt wird.
$(ii) \Rightarrow (iii)$: Endlich viele Elemente $1 = c_1, \ldots, c_n$ erzeugen den R-Modul $M := R[b_1, \ldots, b_m]$. Sei nun $c \in M$ beliebig gewählt. Da M auch ein Ring ist, gilt $c \cdot c_i \in M$ und es gibt also $a_{ij} \in R$ mit

$$c \cdot c_i = \sum_{j=1}^{n} a_{ij} c_j.$$

Für die Matrix

$$A = (a_{ij})_{i,j} \in \mathrm{Mat}_n(R)$$

gilt dann

$$A \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = c \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}.$$

Also liegt $(c_1, \ldots, c_n)^t$ im Kern von

$$N := cI_n - A.$$

Es gilt nun

$$\mathrm{adj}(N) \cdot N = \det(N) \cdot I_n$$

und also

$$\det(N) \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0.$$

Aus $c_1 = 1$ folgt $\det(N) = 0$. An der Leibnizformel zur Berechnung der Determinante sieht man aber

$$\det(N) = c^n + a_{n-1} c^{n-1} + \cdots + a_m$$

für gewisse $a_i \in R$. Das liefert eine Ganzheitsgleichung für c über R.
$(iii) \Rightarrow (i)$ ist trivial. □

Der folgende Satz kann als Verallgemeinerung der Aussage von Satz 4.2.9 (ii) (2)⇒ (3) verstanden werden, auf den Fall von mehr als einem Erzeuger. Er ist außerdem eine wichtige Grundlage der klassischen algebraischen Geometrie, wie wir in Korollar 5.4.6 unten sehen.

Satz 5.4.4 (Hilberts Nullstellensatz, körpertheoretische Form). *Sei $k \subseteq K$ eine Körpererweiterung und K sei als Ring über k endlich erzeugt. Dann ist die Erweiterung $k \subseteq K$ endlich (und damit algebraisch).*

Beweis. Es gibt $\alpha_1, \ldots, \alpha_n \in K$ mit $K = k[\alpha_1, \ldots, \alpha_n]$. Wir beweisen die Aussage per Induktion über n.
$n = 1$: Es ist $K = k[\alpha]$ ein Körper, und also gibt es ein Polynom $p \in k[t]$ mit $\alpha^{-1} = p(\alpha)$. Daraus folgt $\alpha \cdot p(\alpha) - 1 = 0$, und also ist α algebraisch über k. Damit ist die Erweiterung endlich.
$n - 1 \to n$: Es ist $K = k(\alpha_1)[\alpha_2, \ldots, \alpha_n]$, denn K ist ein Körper. Aus der Induktionsannahme folgt, dass $\alpha_2, \ldots, \alpha_n$ algebraisch über $k(\alpha_1)$ sind. Es genügt nun zu zeigen, dass α_1 algebraisch über k ist. Dann ist die gesamte Erweiterung K/k algebraisch und damit endlich. Dass $\alpha_2, \ldots, \alpha_n$ algebraisch über $k(\alpha_1)$ sind bedeutet, dass es für sie Identitäten

$$u_i \alpha_i^d + \sum_{j=0}^{d-1} r_{ij} \alpha_i^j = 0$$

mit $u_i, r_{ij} \in k[\alpha_1]$ gibt (eventuelle Nenner wurden dabei hochmultipliziert). Sei $u := u_2 \cdots u_n \in k[\alpha_1]$. Dann sind $\alpha_2, \ldots, \alpha_n$ ganz über dem Ring $k[\alpha_1, 1/u]$, und somit ist K nach Satz 5.4.3 eine ganze Ringerweiterung von $k[\alpha_1, 1/u]$. Angenommen α_1 ist transzendent über k, d.h. $k[\alpha_1]$ ist ein Polynomring. Dann können wir ein irreduzibles $p \in k[\alpha_1]$ wählen mit $p \nmid u$ (es gibt unendlich viele irreduzible Polynome im faktoriellen Ring $k[\alpha_1]$). Für p^{-1} wiederum gibt es nun eine Ganzheitsgleichung

$$p^{-m} + b_1 p^{-(m-1)} + \cdots + b_m = 0$$

mit $b_i \in k[\alpha_1, 1/u]$. Multiplikation mit p^m und einer genügend hohen Potenz von u liefert

$$u^r + a_1 p + \cdots + a_m p^m = 0$$

mit $a_i \in k[\alpha_1]$. Daraus folgt $p \mid u$, ein Widerspruch. □

Korollar 5.4.5. *Sei R als Ring über k endlich erzeugt und $\mathfrak{m}$ ein maximales Ideal in R. Dann ist $R/\mathfrak{m}$ eine endliche Körpererweiterung von k.*

Beweis. $R/\mathfrak{m}$ ist als Ring über k immer noch endlich erzeugt und andererseits ein Körper. Also folgt die Aussage aus Satz 5.4.4. □

Korollar 5.4.6 (Hilberts Nullstellensatz, geometrische Form)**.** *Sei k ein algebraisch abgeschlossener Körper und $I \trianglelefteq k[x_1, \ldots, x_n]$ ein echtes Ideal. Dann existiert ein $a \in k^n$ mit $p(a) = 0$ für alle $p \in I$. Das von I definierte polynomiale Gleichungssystem besitzt also über k eine Lösung.*

Beweis. Wähle ein maximales Ideal $\mathfrak{m}$ von $k[x_1, \ldots, x_n]$ mit $I \subseteq \mathfrak{m}$. Nach Korollar 5.4.5 ist $k[x_1, \ldots, x_n]/\mathfrak{m}$ eine endliche Körpererweiterung von k. Da k algebraisch abgeschlossen ist, gilt also $k[x_1, \ldots, x_n]/\mathfrak{m} = k$. Setze $a_i := \overline{x_i}$, die Restklasse von x_i in $k[x_1, \ldots, x_n]/\mathfrak{m} = k$. Für jedes $p \in k[x_1, \ldots, x_n]$ gilt dann

$$p(a) = p(\overline{x}) = \overline{p},$$

und für $p \in I$ (sogar für $p \in \mathfrak{m}$) ist also $p(a) = 0$. □

Bemerkung 5.4.7. (i) Ohne Korollar 5.4.5 bekäme man im letzten Beweis nur die Aussage, dass das von I definierte Gleichungssystem über *irgendeinem* Erweiterungskörper von k, nämlich $k[x_1, \ldots, x_n]/\mathfrak{m}$, eine Lösung besitzt. Mit Korollar 5.4.5 sehen wir, dass es eine endliche Körpererweiterung ist, die im algebraischen abgeschlossenen Fall also trivial sein muss.
(ii) Ist k nicht algebraisch abgeschlossen, stimmt die Aussage von Korollar 5.4.5 nicht. Das sieht man zum Beispiel für $k = \mathbb{Q}$ und $I = (x^2 - 2)$ oder $k = \mathbb{R}$ und $I = (x^2 + 1)$.
(iii) Korollar 5.4.6 besagt, dass ein polynomiales Gleichungssystem

$$p_1 = 0, \ldots, p_r = 0$$

mit $p_i \in k[x_1, \ldots, x_n]$ genau dann *keine* Lösung über k besitzt, wenn es eine Identität

$$f_1 p_1 + \cdots + f_r p_r = 1$$

mit $f_i \in k[x_1, \ldots, x_n]$ gibt. Diese letzte Bedingung, und damit die Lösbarkeit eines Gleichungssystems, kann man unter gewissen Voraussetzungen algorithmisch testen. △

Kapitel 6

Nicht-kommutative Algebra

Bisher haben wir fast ausschließlich kommutative Ringe betrachtet. In diesem Kapitel geben wir eine kurze Einführung in die Theorie der nicht-kommutativen Ringe.

6.1 Schiefkörper

Sei hier stets R ein Ring, von dem wir bewusst nicht voraussetzen, dass er kommutativ ist.

Definition 6.1.1. (i) Der Ring R heißt **einfach**, wenn er nur die beiden trivialen (beidseitigen) Ideale $\{0\}$ und R hat.
(ii) Der Ring R heißt **Schiefkörper**, wenn $R^\times = R \setminus \{0\}$ gilt.
(iii) Das **Zentrum** von R ist die Menge

$$Z(R) := \{a \in R \mid \forall b \in R\colon ab = ba\}. \qquad \triangle$$

Bemerkung 6.1.2. (i) Für kommutative Ringe stimmen die Eigenschaften *einfach*, *Schiefkörper* und *Körper* überein. Wenn ein kommutativer Ring nur die beiden trivialen Ideal hat, ist $\{0\}$ offensichtlich ein maximales Ideal. Also ist $R = R/\{0\}$ nach 3.3.4 (ii) ein Körper.
Für nicht-kommutative Ringe gilt im Allgemeinen nur, dass Schiefkörper einfach sind (mit dem Argument aus 3.1.5 (ii)), die Umkehrung nicht. Nach Satz 3.1.6 ist der Matrixring $\mathrm{Mat}_m(K)$ über einem Körper einfach, aber für $n \geq 2$ ist nicht jede Matrix außer der Nullmatrix invertierbar. Also ist $\mathrm{Mat}_m(K)$ kein Schiefkörper.

(*ii*) Ist $I \trianglelefteq R$ ein (beidseitiges) Ideal, so ist R/I wieder ein Ring. Die Ideale in R/I entsprechen genau den Idealen von R, die I enthalten. Wenn I also ein maximales Ideal war, ist R/I einfach.
(*iii*) Es ist $Z(R)$ stets ein kommutativer Teilring von R. In einem Schiefkörper R ist $Z(R)$ sogar ein kommutativer Schiefkörper, also ein Körper, der in R enthalten ist (siehe dazu Aufgabe 95). △

Der Beweis des folgenden berühmten Satzes ist nicht leicht, aber sehr elegant.

Satz 6.1.3 (Wedderburn). *Jeder endliche Schiefkörper ist kommutativ, also ein Körper.*

Beweis. Wir beweisen die Aussage per Induktion über die Mächtigkeit des Schiefkörpers R. Für $\#R = 2$ gilt $R \cong \mathbb{Z}/2\mathbb{Z}$, also stimmt die Aussage.
Sei nun R ein beliebiger endlicher Schiefkörper. Dann ist $K := Z(R)$ ein endlicher Körper der in R enthalten ist, insbesondere kann R als K-Vektorraum aufgefasst werden. Wenn $\#K = q$ gilt, folgt $\#R = q^m$ für ein $m \in \mathbb{N}$ (hierbei ist m die Dimension von R als K-Vektorraum). Wir zeigen im Folgenden $m = 1$, das impliziert $R = K$ und damit die Aussage.
Für $a \in R \setminus K$ ist der *Zentralisator*

$$C_R(a) := \{b \in R \mid ba = ab\}$$

ein Schiefkörper (Aufgabe 95), der echt in R enthalten ist. Nach Induktionsvoraussetzung ist $C_R(a)$ kommutativ, also ein Körper. Aus der Kette

$$K \subseteq C_R(a) \subsetneq R$$

sehen wir, dass $\#C_R(a) = q^n$ für einen echten Teiler n von m gelten muss (denn $C_R(a)$ ist ein K-Vektorraum und R ist ein $C_R(a)$-Vektorraum).
Wir verwenden nun die Klassengleichung 2.3.9 für die multiplikative Gruppe $R^\times$:

$$\#R^\times = \#Z(R^\times) + \sum_a \frac{\#R^\times}{\#C_{R^\times}(a)},$$

also

$$q^m - 1 = (q-1) + \sum_a \frac{q^m - 1}{q^{n_a} - 1}.$$

Dabei läuft die Summe über ein vollständiges Vertretersystem der Konjugationsklassen in $R^\times$ mit mindestens 2 Elementen. Die n_a sind somit alles echte Teiler von m.

Das Polynom $t^m - 1 \in \mathbb{Z}[t]$ besitzt eine Faktorisierung in Kreisteilungspolynome:

$$t^m - 1 = \prod_{k=1}^{m} \left(t - e^{2\pi i k/m}\right) = \prod_{d|m} \underbrace{\prod_{\substack{1 \le k \le m \\ \mathrm{ggT}(k,m) = d}} \left(t - e^{2\pi i k/m}\right)}_{=:\Phi_{m/d}} = \prod_{d|m} \Phi_{m/d}.$$

Man beachte, dass das Polynom $\Phi_{m/d}$ wirklich nur vom Qotienten m/d abhängt. Man beachte ausserdem, dass wir die Kreisteilungspolynome Φ_d in Beispiel 3.5.23 schon für Primzahlen d definiert haben. Für diesen Fall stimmt die Definition hier mit der alten überein. Außerdem haben alle Φ_d Koeffizienten aus $\mathbb{Z}$ (Aufgabe 96).
Setzt man in diese Gleichung für t nun q ein, sieht man

$$\Phi_m(q) \mid q^m - 1 \text{ und } \Phi_m(q) \mid \frac{q^m - 1}{q^{n_a} - 1}$$

für alle a. An der Klassengleichung sehen wir deshalb, dass $\Phi_m(q)$ auch ein Teiler von $q - 1$ sein muss. Insbesondere gilt damit

$$|\Phi_m(q)| \le q - 1.$$

Aufgrund der Definition von Φ_m gilt aber

$$|\Phi_m(q)| = \prod_{\substack{1 \le k \le m \\ \mathrm{ggT}(k,m) = 1}} |q - e^{2\pi i k/m}|.$$

Wegen $q \ge 2$ gilt aber

$$|q - 1| < |q - e^{2\pi i k/m}|$$

für alle k in diesem Produkt, ausser im Fall $m = 1$. Es ergibt sich also nur im Fall $m = 1$ kein Widerspruch. Das beweist die Aussage. □

Bemerkung 6.1.4. Wie im kommutativen Fall kann man die Bedingung *endlicher Schiefkörper* auch noch äquivalent abschwächen zu *endlicher nullteilerfreier Ring*. Für $a \in R \setminus \{0\}$ ist nämlich die Linksmultiplikationsabbildung

$$\begin{aligned} {}_a m \colon R &\to R \\ b &\mapsto ab \end{aligned}$$

aufgrund der Nullteilerfreiheit injektiv, also auch surjektiv. Da 1 im Bild liegt, besitzt a ein Rechtsinverses. Mit der Multiplikation m_a von rechts sieht man die Existenz eines Linksinversen. Diese müssen aber übereinstimmen, wie man leicht sieht. Damit gilt $a \in R^\times$. △

Wir kennen bisher keinen Schiefkörper, der kein Körper ist. Satz 6.1.3 sagt, dass wir auch keinen endlichen finden können. Die bekanntesten Beispiele behandeln wir im nächsten Abschnitt.

6.2 Quaternionen

Definition 6.2.1. Seien K ein Körper und $a, b \in K \setminus \{0\}$. Der **Ring der Quaternionen** $Q_K(a,b)$ ist der K^4, versehen mit Basisvektoren

$$1, i, j, k$$

und der durch folgende Regeln definierten Multiplikation (K-bilinear fortgesetzt):

$$ij = k = -ji,\ i^2 = a \cdot 1,\ j^2 = b \cdot 1. \qquad \triangle$$

Bemerkung 6.2.2. (i) Durch die oben angegebenen Regeln ist wirklich eine Ringstruktur auf K^4 definiert. Es soll dabei natürlich der erste Basisvektor 1 das neutrale Element sein. Es ergeben sich die noch fehlenden Multiplikationsregeln für Basisvektoren automatisch. Es ist etwa

$$ik = iij = a1j = aj.$$

Aufgrund des Distributivgesetzes ergibt sich damit auch die Multiplikationsvorschrift für zwei beliebige Elemente von K^4. Natürlich kann man die Multiplikationsvorschrift auch ganz explizit hinschreiben, sie lässt sich nur sehr schwer merken:

$$\begin{aligned}&(r,s,t,u) \cdot (v,w,x,y)\\ &= (rv + swa + txb - uyab, rw + sv - tyb + uxb,\\ &\qquad rx + sya + tv - uwa, ry + sx - tw + uv).\end{aligned}$$

Der Körper K ist in K^4 enthalten, indem man ihn entlang des ersten Basisvektors einbettet, ein Element $r \in K$ also mit $r1 = (r,0,0,0) \in K^4$ identifiziert. Auf diese Weise ist $Q_K(a,b)$ eine Ringerweiterung von K und K ist sogar im Zentrum von $Q_K(a,b)$ enthalten.
(ii) Oft schreibt man statt des Tupels (v,w,x,y) auch

$$v + wi + xj + yk,$$

wie man es von den komplexen Zahlen gewöhnt ist. Man kann dann beim Multiplizieren wie gewohnt vorgehen und muss sich nur die oben angegebenen Regeln merken.
(iii) Manchmal wird auch nur der Ring $Q_K(-1,-1)$ als Ring der Quaternionen bezeichnet. △

Definition 6.2.3. Für ein Element $p = v + wi + xj + yk \in Q_K(a,b)$ der Quaternionen definieren wir das **konjugierte Element** als

$$\overline{p} := v - wi - xj - yk \in Q_K(a,b)$$

und die **Norm** als

$$N(p) := p\overline{p} = v^2 - aw^2 - bx^2 + aby^2 \in K. \qquad \triangle$$

Lemma 6.2.4. *(i) Für $p, q \in Q_K(a,b)$ gilt $\overline{pq} = \overline{q}\,\overline{p}$.*
(ii) Für $p, q \in Q_K(a,b)$ gilt $N(pq) = N(p)N(q)$.
(iii) Es gilt $p \in Q_K(a,b)^\times \Leftrightarrow N(p) \neq 0$.

Beweis. (i) rechnet man einfach nach, bzw. sieht es der oben explizit angegebenen vollständigen Definition der Multiplikation direkt an.
(ii): Es gilt

$$N(pq) = pq\overline{pq} = pq\overline{q}\,\overline{p} = pN(q)\overline{p} = p\overline{p}N(q) = N(p)N(q).$$

Dabei haben wir $N(q) \in K \subseteq Z(Q_K(a,b))$ benutzt.
(iii): Aus $pq = 1$ folgt $1 = N(1) = N(pq) = N(p)N(q)$ und daraus $N(p) \neq 0$. Gilt umgekehrt $N(p) \neq 0$, so setzen wir

$$q = \frac{1}{N(p)}\overline{p}$$

und berechnen

$$pq = \frac{1}{N(p)}p\overline{p} = \frac{N(p)}{N(p)} = 1$$

und ganz analog $qp = 1$. Also gilt $p \in Q_K(a,b)^\times$. □

Satz 6.2.5. *Sei* $\mathrm{char}(K) \neq 2$.
(i) $Q_K(a,b)$ ist einfach.
(ii) Für jeden Teilkörper $K \subseteq \mathbb{R}$ ist $Q_K(-1,-1)$ ein Schiefkörper.
(iii) Für $0 \neq b \in K$ gilt

$$Q_K(1,b) \cong \mathrm{Mat}_2(K).$$

Insbesondere ist $Q_K(1,b)$ kein Schiefkörper.

Beweis. (i) ist Aufgabe 97. Für (ii) stellt man fest, dass für $0 \neq (v, w, x, y) \in K^4$ in K stets

$$v^2 - (-1)w^2 - (-1)x^2 + (-1)(-1)y^2 = v^2 + w^2 + x^2 + y^2 \neq 0$$

gilt. Also ist jedes $0 \neq p$ in $Q_K(a, b)$ invertierbar.
Für (iii) liefert die Abbildung

$$\begin{aligned} Q_K(1, b) &\to \mathrm{Mat}_2(K) \\ i &\mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ j &\mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix} \end{aligned}$$

einn Isomorphismus, wie man direkt nachrechnet. □

6.3 Algebren

Sei in diesem Abschnitt stets K ein Körper. Der Begriff einer K-Algebra kann auf verschiedene Weisen definiert werden. Es handelt sich dabei um einen Vektorraum, in dem auch multipliziert werden kann. Alternativ kann man es als Ring mit einer skalaren Multiplikation definieren. Am einfachsten ist aber folgende Definition:

Definition 6.3.1. (i) Eine **K-Algebra** ist ein (nicht notwendigerweise kommutativer) Ring A, zusammen mit einem Ringhomomorphismus $K \to Z(A)$.
(ii) Eine **K-Unteralgebra** der K-Algebra A ist ein Teilring $B \subseteq A$ der das Bild von K unter dem Homomorphismus enthält. △

Bemerkung 6.3.2. (i) Der Ringhomomorphismus in der vorangegangenen Definition hat bewusst keinen Namen. Es ist notwendigerweise injektiv, also fasst man K meist einfach als Teilring von A auf. Die Elemente von K müssen aber im Zentrum enthalten sein, also mit jedem anderen Ringelement kommutieren.
(ii) Man kann Elemente von K mit Elementen aus A multiplizieren und erhält Elemente aus A als Ergebnis. Damit bildet A einen K-Vektorraum. Gleichzeitig kann man aber auch je zwei Elemente aus A miteinander multiplizieren, da A auch ein Ring ist. Das geht in Vektorräumen normalerweise nicht. △

Beispiel 6.3.3. (i) Der Matrixring $\mathrm{Mat}_m(K)$ wird zu einer K-Algebra, indem man Elemente von K als konstante Diagonalmatrizen der Größe m auffasst.
(ii) Der Polynomring $K[t]$ ist eine (kommutative) k-Algebra.
(iii) Der Quaternionenring $Q_K(a,b)$ ist eine K-Algebra.
(iv) Jeder Schiefkörper ist eine Algebra über seinem Zentrum $K = Z(R)$. $\triangle$

Im folgenden untersuchen wir Unteralgebren von Matrix-Algebren. Für eine K-Unteralgebra $A \subseteq \mathrm{Mat}_m(K)$ nennt man einen Untervektorraum $V \subseteq K^m$ **A-invariant**, falls

$$Mv \in V$$

für alle $v \in V$ und $M \in A$ gilt. Es gibt stets die sogenannten *trivialen invarianten Unterräume* $\{0\}$ und K^m.

Satz 6.3.4 (Satz von Burnside)**.** *Sei K ein algebraisch abgeschlossener Körper. Falls die K-Unteralgebra $A \subseteq \mathrm{Mat}_m(K)$ nur die beiden trivialen invarianten Unterräume besitzt, gilt $A = \mathrm{Mat}_m(K)$.*

Beweis. A operiert transitiv auf K^m: für jedes $0 \neq v \in K^m$ ist ja

$$\{0\} \subsetneq \{Mv \mid M \in A\}$$

ein A-invarianter Unterraum, stimmt also mit K^m überein. Wir zeigen zunächst, dass A eine Matrix von Rang 1 enthält. Sei dazu $0 \neq P \in A$. Falls $\mathrm{rang}(P) \geq 2$ ist, wähle $v_1, v_2 \in K^m$ mit Pv_1, Pv_2 linear unabhängig. Wähle dann $M \in A$ mit $MPv_1 = v_2$. Dann sind also $PMPv_1$ und Pv_1 linear unabhängig und $PMP - \lambda P \neq 0$ gilt also für alle $\lambda \in K$. Es gibt aber ein $\lambda_0 \in K$, für welches $PM - \lambda_0 I_d$ auf dem Raum $P(K^m)$ nicht invertierbar ist, denn K ist algebraisch abgeschlossen und jede lineare Abbildung besitzt somit einen Eigenwert. Also hat

$$(PM - \lambda_0 I_d)P$$

einen echt kleineren Rang als P, ist aber nicht Null. Iterativ erhalten wir also eine Matrix Q vom Rang 1 in A.
Jede andere Matrix mit demselben Bild wie Q ist dann aber ebenfalls in A, und damit auch jede beliebige andere Matrix vom Rang 1. Dafür benötigt man nochmal die Transitivität von A auf K^m (Übungsaufgabe 98). Da jede Matrix eine Summe von Matrizen von Rang 1 ist, folgt $A = \mathrm{Mat}_m(K)$. $\square$

Bemerkung 6.3.5. Sei $A \subseteq \mathrm{Mat}_m(\mathbb{C})$ sogar eine $*$-Unteralgebra, d.h. mit M gehöre auch M^* zu A. Falls A einen echten invarianten Unterraum $V \subseteq \mathbb{C}^m$ besitzt, so ist auch $V^\perp$ ein solcher invarianter Unterraum. Dafür verwendet man,

dass A abgeschlossen unter $*$ ist (Aufgabe 99). Nach einem unitären Basiswechsel haben alle Matrizen in A Blockgestalt, d.h. A ist eine Unteralgebra von einer Algebra

$$\mathrm{Mat}_{m_1}(\mathbb{C}) \oplus \mathrm{Mat}_{m_2}(\mathbb{C})$$

mit $1 \leq m_1, m_2$ und $m_1 + m_2 = m$. Wir sind damit in einer einfacheren Situation. Falls es keinen invarianten Unterraum gibt, gilt nach Satz 6.3.4 bereits $A = \mathrm{Mat}_m(\mathbb{C})$. Wir erhalten iterativ, dass A eine Unteralgebra von

$$\mathrm{Mat}_{m_1}(\mathbb{C}) \oplus \cdots \oplus \mathrm{Mat}_{m_r}(\mathbb{C})$$

und für jeden Faktor die Projektion von A auf $\mathrm{Mat}_{m_i}(\mathbb{C})$ surjektiv ist. △

Beispiel 6.3.6. Sei $A \subseteq \mathrm{Mat}_m(\mathbb{C})$ eine *kommutative* $*$-Unteralgebra. Wir können also o.B.d.A. annehmen, dass

$$A \subseteq \mathrm{Mat}_{m_1}(\mathbb{C}) \oplus \cdots \oplus \mathrm{Mat}_{m_r}(\mathbb{C})$$

mit $m_1 + \cdots + m_r = m$, und die Projektion auf jeden d_i-Block auf A surjektiv ist. Andererseits kommutieren die Elemente von A miteinander, und mit Beispiel 6.3.8 (i) folgt daraus $d_i = 1$ für alle i. *Die Algebra A besteht also nur aus Diagonalmatrizen* (nach unitärer Konjugation). △

Definition 6.3.7. Eine K-Algebra A heißt **zentral**, wenn $Z(A) = K$ gilt. △

Beispiel 6.3.8. (i) Für jeden Körper K ist $\mathrm{Mat}_m(K)$ eine zentrale K-Algebra.
(ii) Für $\mathrm{char}(K) \neq 2$ ist $Q_K(a, b)$ eine zentrale K-Algebra. (Aufgabe 100). △

Kapitel 7

Anwendungen und Verschiedenes

In diesem Kapitel schauen wir uns einige Anwendungen der algebraischen Konzepte dieser Vorlesung an. In der *Kodierungstheorie* versucht man, Daten so zu strukturieren, dass man eventuelle Fehler bei einer Datenübertragung entdecken und sogar rückgängig machen kann. Dabei kommen häufig endliche Körper ins Spiel. In der *Kryptographie* versucht man hingegen, Daten so zu verschlüsseln, dass sie von einem unerwünschten Mithörer nicht verstanden werden können. Besonders in der modernen Public-Key-Verschlüsselung kommen dabei interessante mathematische Konzepte zum Einsatz. Danach besprechen wir noch einige abstraktere Konzepte, die für die weiterführenden Vorlesungen nützlich sind.

7.1 Kodierungstheorie

In vielen Bereichen von Technik und Gesellschaft werden heute große Datenmengen generiert und übertragen. Bei der Datenübertragung kommt es jedoch leicht zu Fehlern, die die Daten im schlimmsten Fall unbrauchbar werden lassen. Deshalb versucht man mit der Kodierungstheorie, die Daten so aufzubereiten, dass kleinere Fehler entdeckt und bestenfalls korrigiert werden können. Die Anwendungen im Internet, in Handys, CDs etc. sind unzählig. Ein sehr einfaches Beispiel sind die ISBN Nummern auf Büchern.

Beispiel 7.1.1 (ISBN-10)**.** Die (heute nicht mehr genutzte) ISBN-10 Nummer eines Buchs besteht aus einer Zahl mit 10 Ziffern:

$$x_1 x_2 \cdots x_{10}.$$

Dabei tragen nur die ersten 9 Ziffern wirkliche Information über das Buch (Land, Verlag…), die zehnte Ziffer x_{10} ist eine sogenannte *Prüfziffer*. Sie wird so bestimmt, dass die folgende *Prüfgleichung* erfüllt ist:

$$x_1 + 2x_2 + 3x_3 + \cdots + 9x_9 + 10x_{10} \equiv 0 \bmod 11.$$

Wegen $10 \equiv -1 \bmod 11$ kann man das also auch umformen zu

$$x_{10} \equiv x_1 + 2x_2 + \cdots + 9x_9 \bmod 11.$$

Also ist x_{10} eine Ziffer zwischen 0 und 10, und damit sie immer einstellig bleibt, schreibt man statt 10 dann X.
Wenn die ersten 9 Ziffern also 247810378 lauten, berechnet man

$$1 \cdot 2 + 2 \cdot 4 + 3 \cdot 7 + 4 \cdot 8 + 5 \cdot 1 + 6 \cdot 0 + 7 \cdot 3 + 8 \cdot 7 + 9 \cdot 8 = 217.$$

Wegen $217 \equiv 8 \bmod 11$ erhält man also $x_{10} = 8$ und somit die ISBN-10 Nummer

$$2478103788.$$

Wäre die zweite Ziffer eine 5 gewesen, hätte die Summe 219 ergeben, und $219 \equiv 10 \bmod 11$. Man hätte $x_{10} = \mathrm{X}$ und damit

$$257810378\mathrm{X}$$

erhalten.
Man überlegt sich nun, dass jede der Ziffern x_i durch die anderen Ziffern eindeutig bestimmt ist. Für jedes $i = 0, \ldots, 10$ gilt im Körper $\mathbb{F}_{11}$ nämlich

$$x_i = -\frac{1}{i} \sum_{j \neq i} j x_j.$$

Diese Beobachtung hat nun folgende Implikationen:

(i) Wird genau eine Ziffer einer gültigen ISBN-10 Nummer abgeändert, ist die Prüfgleichung nicht mehr erfüllt. Solch ein einfacher Fehler wird also immer entdeckt.

(ii) Wird genau eine Ziffer abgeändert, und weiß man um welche es sich handelt (oder ist etwa eine Ziffer unlesbar), so kann sie anhand der Prüfgleichung rekonstruiert werden. Ohne Kenntnis der Fehlerstelle funktioniert das jedoch nicht.

Sogar ein weiterer (oft auftretender) Typ von Fehler kann erkannt werden. Werden nämlich in einer gültigen ISBN-10 Nummer zwei verschiedene Ziffern vertauscht, so ist die Prüfgleichung nicht mehr erfüllt. Falls nämlich x_i und x_j vertauscht werden, ändert sich die linke Seite der Prüfgleichung um

$$ix_i + jx_j - ix_j - jx_i = (i-j)(x_i - x_j).$$

Diese Differenz ist aber kein Vielfaches von 11, denn 11 ist prim, und beide Faktoren sind ≤ 10. △

Beispiel 7.1.2 (ISBN-13)**.** Um mehr Ziffern zur Verfügung zu haben, wurde die ISBN-13 Nummer eingeführt. Sie besteht aus 13 Ziffern

$$x_1 \cdots x_{13},$$

wobei die ersten 12 Ziffern die eigentliche Information tragen, und x_{13} so bestimmt ist, dass die folgende Prüfgleichung erfüllt ist:

$$x_1 + 3x_2 + x_3 + \cdots + 3x_{12} + x_{13} \equiv 0 \bmod 10.$$

Auch hier ist wieder jede Ziffer durch die anderen eindeutig bestimmt, da $1, 3 \in (\mathbb{Z}/10\mathbb{Z})^\times$ gilt. Einfache Fehler werden also entdeckt, und können bei Wissen um ihre Position auch korrigiert werden. Vertauschung von zwei Ziffern wird hier allerdings nicht mehr immer erkannt. △

Wir befassen uns nun etwas allgemeiner und mathematischer mit Kodierungsmöglichkeiten.

Definition 7.1.3. (i) Ein **Alphabet** $\mathcal{A}$ ist eine endliche Menge.
(ii) Ein **Wort über** $\mathcal{A}$ ist ein Tupel $x = (x_1, \ldots, x_k) \in \mathcal{A}^k$. Dabei heißt k die **Wortlänge**.
(iii) Eine **Kodierungsregel** ist eine injektive Abbildung

$$\varphi\colon \mathcal{A}^k \to \mathcal{A}^n$$

für gewisse $k, n \in \mathbb{N}$.
(iv) Für eine gegebene Kodierungsregel $\varphi\colon \mathcal{A}^k \to \mathcal{A}^n$ nennt man Elemente von $\mathcal{A}^k$ **Informationswörter** und für ein Informationswort $x \in \mathcal{A}^k$ heißt $\varphi(x) \in \mathcal{A}^n$ das zugeordnete **Codewort**. Die Menge $\varphi(\mathcal{A}^k)$ aller Codewörter heißt **Code**. △

Die definierten Begriffe haben folgende Interpretation: Die Informationswörter tragen die eigentliche Information, die gespeichert und/oder übermittelt werden soll. Man arbeitet stattdessen aber mit den zugeordneten Codewörtern. Aufgrund der Injektivität von φ kann die eigentliche Information aus einem Codewort zurückermittelt werden. Das Codewort selbst hat aber zusätzliche Struktur, die Fehlererkennung und/oder -korrektur möglich macht.

Beispiel 7.1.4. (i) Im ISBN-10 Code ist $\mathcal{A} = \mathbb{F}_{11}$ und

$$\begin{aligned} \varphi\colon \mathbb{F}_{11}^9 &\to \mathbb{F}_{11}^{10} \\ (x_1, \dots, x_9) &\mapsto (x_1, \dots, x_9, x_{10}) \end{aligned}$$

mit $x_{10} = \sum_{i=1}^{9} i x_i$. Dabei sind strenggenommen $x_1, \dots, x_9$ sogar immer nur aus der Menge $\{0, 1, \dots, 9\} \subseteq \mathbb{F}_{11}$. Die Kodierungsregel ist hier sogar eine lineare Abbildung der $\mathbb{F}_{11}$-Vektorräume.
(ii) Im ISBN-13 Code haben wir $\mathcal{A} = \mathbb{Z}/10\mathbb{Z}$ und die Kodierungsregel

$$\begin{aligned} \varphi\colon (\mathbb{Z}/10\mathbb{Z})^{12} &\to (\mathbb{Z}/10\mathbb{Z})^{13} \\ (x_1, \dots, x_{12}) &\mapsto (x_1, \dots, x_{12}, x_{13}) \end{aligned}$$

mit $x_{13} = -(x_1 + 3x_2 + x_3 + \cdots + 3x_{12})$. Hier ist φ ein $\mathbb{Z}/10\mathbb{Z}$-Modulhomomorphismus.
(iii) Der d-Wiederholungscode hat die Kodierungsregel

$$\begin{aligned} \varphi\colon \mathcal{A}^k &\to \mathcal{A}^{dk} \\ (x_1, \dots, x_k) &\mapsto (\underbrace{x_1, \dots, x_k, x_1, \dots, x_k, \dots, x_1, \dots, x_k}_{d \text{ mal}}) \end{aligned}$$ △

Definition 7.1.5. Sei $\mathcal{A}$ ein Alphabet und $n \in \mathbb{N}$. Die **Hamming-Distanz** zweier Elemente $v = (v_1, \dots, v_n), w = (w_1, \dots, w_n) \in \mathcal{A}^n$ ist definiert durch

$$d(v, w) := \#\{i \mid 1 \leq i \leq n, v_i \neq w_i\}. \qquad \triangle$$

Lemma 7.1.6. *Die Hamming-Distanz ist eine Metrik auf $\mathcal{A}^n$.*

Beweis. Aufgabe 101. □

Bemerkung 7.1.7. Gegeben eine Kodierungsregel φ, geht man in der Praxis folgendermaßen vor. Wenn die eigentliche Information aus $x \in \mathcal{A}^k$ besteht, wird stattdessen das Codewort $\varphi(x) \in \mathcal{A}^n$ versendet. Der Empfänger erhält dann ein

Wort $r \in \mathcal{A}^n$, das aufgrund von Fehlern in der Übertragung von $\varphi(x)$ verschieden sein kann. Er sucht nun das zu r nahegelegenste Codewort $c = \varphi(y) \in \varphi(\mathcal{A}^k)$ (bezügliche der Hamming-Distanz) und schließt mit der Injektivität von φ auf die ursprüngliche Information y. Natürlich kann das schiefgehen, und in einem $y \neq x$ resultieren. Wir analysieren nun, unter welchen Bedingungen auf diese Weise immer die richtige Information x rekonstruriert wird. Danach untersuchen wir, wie man das nahegelegenste Codewort zu einem $r \in \mathcal{A}^n$ finden kann. △

Definition 7.1.8. Sei $e \in \mathbb{N}$. Ein Code $\mathcal{C} \subseteq \mathcal{A}^n$ heißt e-**fehlerkorrigierend**, falls die abgeschlossenen Bälle in $\mathcal{A}^n$ mit Radius e um Elemente von $\mathcal{C}$ paarweise disjunkt sind. △

Bemerkung 7.1.9. Wenn $\mathcal{C}$ e-fehlerkorrigierend ist, und bei der Übertragung von einem $c \in \mathcal{C}$ nur an höchstens e Stellen ein Fehler gemacht wurde, dann liefert die oben beschriebene Vorgehensweise das richtige c zurück. Das empfangene Wort r liegt dann nämlich im e-Ball um c und also in keinem anderen e-Ball um ein Element des Codes. Also ist c das nächstgelegene Wort im Code. △

Definition 7.1.10. Für $\mathcal{C} \subseteq \mathcal{A}^k$ definieren wir die **Minimaldistanz von** $\mathcal{C}$ als

$$d_{\min}(\mathcal{C}) =: \min\{d(v,w) \mid v,w \in \mathcal{C}, v \neq w\}. \qquad \triangle$$

Lemma 7.1.11. *Ein Code mit Minimaldistanz d ist genau dann e-fehlerkorrigierend, wenn $e \leq \lfloor \frac{d-1}{2} \rfloor$ gilt.*

Beweis. Offensichtlich ist $\lfloor \frac{d-1}{2} \rfloor$ der größtmögliche ganzzahlige Radius disjunkter Bälle um Elemente des Codes. □

Beispiel 7.1.12. (i) Die Minimaldistanz des ISBN-13 Codes ist 2, wie man sich leicht überlegt. Also ist der Code 0-fehlerkorrigierend. Man kann mit ihm zwar eventuell Fehler erkennen, nicht jedoch korrigieren.
(ii) Die Minimaldistanz des d-Wiederholungscodes ist gerade d, für $d = 2e+1$ ist er also e-fehlererkennend. Wenn man ein Informationswort x also durch d-fache Wiederholung kodiert hat, und bei der Übertragung maximal e Fehler gemacht wurden, müssen mindestens $d - e = 2e + 1 - e = e + 1$ der Wiederholungen mit x übereinstimmen. Das sind echt mehr als die Hälfte der Wiederholungen, und man erhält das richtige Wort x als dasjenige, das am häufigsten wiederholt auftaucht. Genau das tut der oben beschriebene Algorithmus. △

Um einen guten fehlerkorrigierenden Code zu erhalten, muss man also eine möglichst große Minimaldistanz erreichen. Wir beschränken uns dabei nun auf lineare Codes über endlichen Körpern. Sei dazu stets q eine Primzahlpotenz und $\mathbb{F}_q$ der Körper mit q Elementen (vergleiche Aufgaben 48 und 58).

Definition 7.1.13. Ein **linearer** (n, k)**-Code über** $\mathbb{F}_q$ ist ein k-dimensionaler $\mathbb{F}_q$-Untervektorraum von $\mathbb{F}_q^n$. △

Lemma 7.1.14. *Sei* $\mathcal{C} \subseteq \mathbb{F}_q^n$ *ein linearer Code. Dann gilt*

$$d_{\min}(\mathcal{C}) = \min\{d(v, 0) \mid 0 \neq v \in \mathcal{C}\}.$$

Beweis. Für $v, w \in \mathcal{C}$ gilt offensichtlich

$$d(v, w) = d(v - w, 0)$$

und da $\mathcal{C}$ ein Vektorraum ist gilt $v - w \in \mathcal{C}$. □

Ab jetzt betrachten wir nur noch lineare Codes, und lassen das Wort *linear* deshalb wieder weg. Einen linearen Code kann man beispielsweise durch die Wahl einer Basis angeben. Schreibt man die Basisvektoren in eine Matrix, erhält man dabei auch gleich eine Abbildungsmatrix für die Kodierungsregel φ. Andererseits ist er natürlich auch als Lösungsmenge eines linearen Gleichungssystems beschreibbar. Das führt zur sogenannten Prüfmatrix.

Definition 7.1.15. Sei $\mathcal{C}$ ein (n, k)-Code über $\mathbb{F}_q$.
(i) Eine **Erzeugermatrix von** $\mathcal{C}$ ist eine $n \times k$-Matrix, deren Spalten eine Basis von $\mathcal{C}$ bilden.
(ii) Eine Erzeugermatrix E ist **in Standardform**, wenn sie von der Gestalt

$$E = \begin{pmatrix} I_k \\ E' \end{pmatrix}$$

mit $E' \in \mathrm{Mat}_{n-k,k}(\mathbb{F}_q)$ ist.
(iii) Eine **Prüfmatrix** für $\mathcal{C}$ ist eine Matrix $P \in \mathrm{Mat}_{n-k,n}(\mathbb{F}_q)$ mit

$$x \in \mathcal{C} \Leftrightarrow Px = 0$$

für alle $x \in \mathbb{F}_q^n$. △

Bemerkung 7.1.16. (i) Aus der linearen Algebra weiß man, dass jeder Code eine Erzeugermatrix und eine Prüfmatrix besitzt. Beide sind jedoch im Allgemeinen nicht eindeutig.
(ii) Dass eine Erzeugermatrix in Standardform vorliegt bedeutet gerade, dass die dadurch definierte Kodierungsregel einfach an das Informationswort ein zusätzliches Wort anhängt. Man überlegt sich aber leicht, dass nicht jeder Code eine Erzeugermatrix in Standardform besitzt.
(iii) Der Rang einer Prüfmatrix P ist automatisch $n-k$, da sie einen Unterraum der Dimension k definiert. △

Lemma 7.1.17. *Sei $E \in \mathrm{Mat}_{n,k}(\mathbb{F}_q)$ die Erzeugermatrix des Codes $\mathcal{C}$ und sei $P \in \mathrm{Mat}_{n-k,n}(\mathbb{F}_q)$ eine Matrix vom Rang $n-k$. Dann ist P genau dann eine Prüfmatrix für $\mathcal{C}$ wenn*

$$PE = 0$$

gilt. Ist $E = \begin{pmatrix} I_k \\ E' \end{pmatrix}$ in Standardform, so ist also $P = \begin{pmatrix} -E' & I_{n-k} \end{pmatrix}$ eine Prüfmatrix.

Beweis. Aus der Rangbedigung folgt $\dim \ker(P) = k$. Es bedeutet $PE = 0$ aber gerade $\mathcal{C} \subseteq \ker(P)$, und das ist also äquivalent zu $\mathcal{C} = \ker(P)$. Es gilt nun offensichtlich

$$\begin{pmatrix} -E' & I_{n-k} \end{pmatrix} \begin{pmatrix} I_k \\ E' \end{pmatrix} = -E' + E' = 0$$

und $\begin{pmatrix} -E' & I_{n-k} \end{pmatrix}$ hat Rang $n-k$. □

Beispiel 7.1.18. (i) Der ISBN-10 Code im Sinne von Beispiel 7.1.4 (i) ist ein linearer $(10,9)$-Code über $\mathbb{F}_{11}$. Er besitzt beispielsweise die Basis

$$(1,0,\ldots,0,1),(0,1,0,\ldots,0,2),\ldots,(0,\ldots,0,1,9).$$

Die dazugehörende Erzeugermatrix

$$E = \begin{pmatrix} 1 & 0 & & 0 \\ 0 & 1 & & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & & 1 \\ 1 & 2 & \cdots & 9 \end{pmatrix}$$

hat Standardform und liefert die Kodierungsregel

$$\begin{aligned}\varphi\colon \mathbb{F}_{11}^{9} &\to \mathbb{F}_{11}^{10}\\ x &\mapsto Ex.\end{aligned}$$

Eine Prüfmatrix ist also beispielsweise

$$(-1,-2,-3,-4,-5,-6,-7,-8,-9,1).$$

(ii) Der d-Wiederholungscode ist ein linearer Code in $\mathbb{F}_q^{dk}$ mit Basisvektoren

$$(e_1,\dots,e_1),\dots,(e_k,\dots,e_k),$$

wobei $e_1,\dots,e_k$ die Standardbasisvektoren von $\mathbb{F}_q^k$ sind. Die dazugehörende Erzeugermatrix

$$E=\begin{pmatrix} 1 & 0 & \cdots & & \cdots & 0\\ 0 & 1 & & & & 0\\ \vdots & \vdots & & & & \vdots\\ 0 & 0 & & & & 1\\ 1 & 0 & \cdots & & \cdots & 0\\ 0 & 1 & & & & 0\\ \vdots & \vdots & & & & \vdots\\ 0 & 0 & & & & 1\\ \vdots & \vdots & & & & \vdots \end{pmatrix}$$

hat Standardform und liefert die Kodierungsregel

$$\begin{aligned}\varphi\colon \mathbb{F}_q^{k} &\to \mathbb{F}_q^{dk}\\ x &\mapsto Ex.\end{aligned}$$

(iii) Die folgende Matrix E in Standardform definiert einen $(7,4)$-Code über $\mathbb{F}_q$:

$$E=\begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ 1 & 0 & 1 & 1\\ 1 & 1 & 0 & 1\\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

Man erhält eine Prüfmatrix

$$P = \begin{pmatrix} -1 & 0 & -1 & -1 & 1 & 0 & 0 \\ -1 & -1 & 0 & -1 & 0 & 1 & 0 \\ 0 & -1 & -1 & -1 & 0 & 0 & 1 \end{pmatrix}. \qquad \triangle$$

Wir untersuchen nun die Minimaldistanz von linearen Codes und damit Ihre Kapazität zur Fehlerkorrektur.

Satz 7.1.19 (Singletonschranke)**.** *Sei $\mathcal{C}$ ein linearer (n, k)-Code über $\mathbb{F}_q$. Dann gilt*

$$d_{\min}(\mathcal{C}) \leq n - k + 1.$$

Beweis. Sei $d = d_{\min}(\mathcal{C})$ und

$$\pi \colon \mathbb{F}_q^n \to \mathbb{F}_q^{n-d+1}$$

die Projektion auf die ersten $n - d + 1$ Komponenten. Da sich zwei verschiedene Elemente in $\mathcal{C}$ an mindestens d Stellen unterscheiden, ist π auf $\mathcal{C}$ eingeschränkt injektiv. Aus der Dimensionsformel für lineare Abbildungen folgt $k \leq n - d + 1$ und daraus die Aussage. □

Lemma 7.1.20. *Sei $\mathcal{C}$ ein linearer (n, k)-Code über $\mathbb{F}_q$ mit Prüfmatrix P. Dann ist $d_{\min}(\mathcal{C})$ gerade die minimale Anzahl von linear abhängigen Spalten von P.*

Beweis. Die Elemente von $\mathcal{C}$ sind gerade diejenigen $c \in \mathbb{F}_q^n$ mit $Pc = 0$. Die Minimaldistanz ist die kleinste Anzahl von Einträgen $\neq 0$ für solche $c \neq 0$, also gerade die minimale Zahl von linear abhängigen Spalten von P. □

Beispiel 7.1.21. (i) Der ISBN-10 Code hat Minimaldistanz 2, wie man beispielsweise auch an der Prüfmatrix sehen kann. Die Singletonschranke liefert hier ebenfalls $10 - 9 + 1 = 2$. In diesem Sinne ist der ISBN-10 Code also optimal.
(ii) Der d-Wiederholungscode hat Minimaldistanz d, auch das kann man an den Spalten der Prüfmatrix sehen. Die Singletonschranke liefert für (dk, k)-Codes aber die obere Schranke

$$dk - k + 1 = k(d - 1) + 1,$$

was im Allgemeinen deutlich größer ist.
(iii) Der Code aus Beispiel 7.1.18 (iii) hat Minimaldistanz 3, wie man an der Prüfmatrix sieht. Die Singletonschranke für $(7, 4)$-Codes ist 4. $\triangle$

Diese Singletonschranke für die Minimaldistanz eines linearen Codes lässt sich in der Tat immer verwirklichen, und zwar durch die sogenannten *Reed-Solomon-Codes*.

Definition 7.1.22. Seien $k, n \in \mathbb{N}$ mit $k \leq n$, sowie

$$\mathbf{P}_k = \{g \in \mathbb{F}_q[x] \mid \deg(g) \leq k-1\} \cong \mathbb{F}_q^k$$

der k-dimensionale Vektorraum der Polynome vom Grad kleiner k. Es seien $a_1, \ldots, a_n \in \mathbb{F}_q$ paarweise verschieden (insbesondere also $n \leq q$). Dann heißt das Bild der folgenden linearen Abbildung ein **Reed-Solomon-Code** mit Parametern n, k und Auswertungsvektor $(a_1, \ldots, a_n)$:

$$\begin{aligned} \varphi\colon \mathbf{P}_k &\to \mathbb{F}_q^n \\ g &\mapsto (g(a_1), \ldots, g(a_n)). \end{aligned}$$ △

Satz 7.1.23. *Jeder Reed-Solomon-Code mit Parametern n, k ist ein linearer (n, k)-Code mit Minimaldistanz $n - k + 1$.*

Beweis. Nach Satz 3.1.15 hat jedes Polynom aus $\mathbf{P}_k \setminus \{0\}$ höchstens $k - 1 < n$ Nullstellen in $\mathbb{F}_q$. Also ist φ injektiv und $\varphi(\mathbf{P}_k)$ damit ein linearer (n, k)-Code. Aus demselben Grund hat für $0 \neq g \in \mathbf{P}_k$ das Tupel $\varphi(g) = (g(a_1), \ldots, g(a_n))$ höchstens $k - 1$ Nulleinträge, also mindestens $n - k + 1$ nichtverschwindende Einträge. Das beweist die Aussage. □

Konstruktion 7.1.24. Wir wählen für $\mathbf{P}_k$ die Basis $1, x, x^2, \ldots, x^{k-1}$ und erhalten für den Reed-Solomon-Code die Erzeugermatrix

$$E = \begin{pmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{k-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{k-1} \\ \vdots & \vdots & & \vdots & \\ 1 & a_n & a_n^2 & \cdots & a_n^{k-1} \end{pmatrix}.$$

Die Konstruktion einer Prüfmatrix ist etwas komplizierter. Zu gegebenem $r = (r_1, \ldots, r_n) \in \mathbb{F}_q^n$ wollen wir entscheiden, ob es ein Polynom $g \in \mathbf{P}_k$ gibt mit $g(a_i) = r_i$ für alle i. Wenn wir uns auf $i \leq k$ beschränken, ist solch ein Polynom nach Korollar 3.1.16 eindeutig bestimmt, und wir können es explizit hinschreiben:

$$g = \sum_{i=1}^{k} r_i \prod_{j=1,\ldots,k, j\neq i} \frac{x - a_j}{a_i - a_j}.$$

Dieses Polynom g muss nun auch $g(a_s) = r_s$ für $s = k+1, \ldots, n$ erfüllen, damit r zum Code gehört. Das liefert die $n-k$ Bedingungen

$$\sum_{i=1}^{k} r_i \prod_{j=1,\ldots,k,j\neq i} \frac{a_s - a_j}{a_i - a_j} - r_s = 0, \quad s = k+1, \ldots, n.$$

Hier handelt es sich um lineare Gleichungen an die r_i, und man kann eine Prüfmatrix direkt ablesen:

$$P = \begin{pmatrix} \prod_{j=1,\ldots,k,j\neq 1} \frac{a_{k+1}-a_j}{a_1-a_j} & \cdots & \prod_{j=1,\ldots,k,j\neq k} \frac{a_{k+1}-a_j}{a_k-a_j} & -1 & 0 & \cdots \\ & \vdots & & & & \\ \prod_{j=1,\ldots,k,j\neq 1} \frac{a_n-a_j}{a_1-a_j} & \cdots & \prod_{j=1,\ldots,k,j\neq k} \frac{a_n-a_j}{a_k-a_j} & 0 & \cdots & -1 \end{pmatrix}.$$

△

Für spezielle Reed-Solomon-Codes kann man die Prüfmatrix noch deutlich einfacher hinschreiben. Dazu zunächst folgendes Lemma und den darauffolgenden Satz:

Lemma 7.1.25. *Sei G eine abelsche Gruppe. Dann gibt es für je zwei Elemente $g, h \in G$ ein Element $x \in G$ mit*

$$\operatorname{ord}(x) = \operatorname{kgV}\left(\operatorname{ord}(g), \operatorname{ord}(h)\right).$$

Beweis. Wir nehmen zunächst an, dass $\operatorname{ord}(g)$ und $\operatorname{ord}(h)$ teilerfremd sind. Wir setzen $x := gh$ und nehmen $e = x^n = g^n h^n$ an. Das impliziert $g^n = h^{-n}$ und damit

$$\operatorname{ord}(g^n) = \operatorname{ord}(h^{-n}) \mid \operatorname{ord}(h).$$

Andererseits gilt auch $\operatorname{ord}(g^n) \mid \operatorname{ord}(g)$ und die Teilerfremdheit impliziert also $\operatorname{ord}(g^n) = \operatorname{ord}(h^{-n}) = 1$, also $g^n = h^{-n} = h^n = e$. Damit muss n ein Vielfaches von $\operatorname{ord}(g)$ und $\operatorname{ord}(h)$ sein, also ein Vielfaches des kleinsten gemeinsamen Vielfachen. Damit ist die Ordnung von x offensichtlich genau dieses kleinste gemeinsame Vielfache, welches hier übrigens einfach das Produkt der Ordnungen ist.
Im allgemeinen Fall betrachte die Primfaktorisierung

$$\operatorname{ord}(g) = p_1^{e_1} \cdots p_n^{e_n}$$
$$\operatorname{ord}(h) = p_1^{f_1} \cdots p_n^{f_n}$$

mit o.B.d.A

$$e_1 \geq f_1, \ldots, e_k \geq f_k \text{ und } e_{k+1} \leq f_{k+1}, \ldots, e_n \leq f_n.$$

Für

$$\tilde{g} := g^{p_{k+1}^{e_{k+1}} \cdots p_n^{e_n}} \text{ und } \tilde{h} := h^{p_1^{f_1} \cdots p_k^{f_k}}$$

gilt dann

$$\operatorname{ord}(\tilde{g}) = p_1^{e_1} \cdots p_k^{e_k} \text{ und } \operatorname{ord}(\tilde{h}) = p_{k+1}^{f_{k+1}} \cdots p_n^{f_n}.$$

Diese Ordnungen sind teilerfremd, und für $x = \tilde{g} \cdot \tilde{h}$ gilt also nach dem bereits gezeigten

$$\operatorname{ord}(x) = \operatorname{ord}(\tilde{g})\operatorname{ord}(\tilde{h}) = p_1^{e_1} \cdots p_k^{e_k} p_{k+1}^{f_{k+1}} \cdots p_n^{f_n} = \operatorname{kgV}\left(\operatorname{ord}(g), \operatorname{ord}(h)\right),$$

die gewünschte Aussage. □

Satz 7.1.26. *Sei K ein endlicher Körper. Dann ist die multiplikative Gruppe $K^\times$ zyklisch.*

Beweis. Sei $a \in K^\times$ ein Element von maximaler Ordnung m. Dann ist die Ordnung jedes anderen Elements von $K^\times$ ein Teiler von m, wegen Lemma 7.1.25. Damit ist jedes $b \in K^\times$ eine Nullstelle von $x^m - 1 \in K[x]$, und daraus folgt $\#K^\times \leq m$. Damit ist also $K^\times = \langle a \rangle$ zyklisch. □

Bemerkung 7.1.27. Es gibt also stets einen Gruppenisomorphismus

$$\left(\mathbb{F}_q^\times, \cdot\right) \to \left(\mathbb{Z}/(q-1)\mathbb{Z}, +\right).$$

Diesen explizit zu bestimmen, d.h. wirklich einen Erzeuger für $\mathbb{F}_q^\times$ zu finden, ist im Allgemeinen aber schwer. △

Nach Satz 2.4.5 und Aufgabe 21 gibt es also für jedes $n \mid (\#K - 1)$ ein Element $a \in K^\times$ mit Ordnung n.

Definition 7.1.28. Für $n \mid (q-1)$ sei $a \in \mathbb{F}_q^\times$ ein Element der Ordnung n. Für jedes $k \leq n$ definiert der Auswertungsvektor $(1, a, a^2, \ldots, a^{n-1})$ dann einen **zyklischen Reed-Solomon-Code** mit Erzeuger a und Parametern n, k. △

Satz 7.1.29. *Sei $\mathcal{C} \subseteq \mathbb{F}_q^n$ ein zyklischer Reed-Solomon-Code mit Parametern n, k und Erzeuger $a \in \mathbb{F}_q^\times$. Dann ist folgende Matrix eine Prüfmatrix für $\mathcal{C}$:*

$$P = \begin{pmatrix} 1 & a & \cdots & a^{n-1} \\ 1 & a^2 & \cdots & a^{2(n-1)} \\ \vdots & \vdots & & \vdots \\ 1 & a^{n-k} & \cdots & a^{(n-k)(n-1)} \end{pmatrix}.$$

Beweis. Die Determinante der linken $(n-k) \times (n-k)$-Teilmatrix von P ist

$$\prod_{1 \leq i < j \leq n-k} (a^j - a^i).$$

Da a Ordnung n hat, ist diese Determinante ungleich 0, also hat P genau Rang $n-k$. Nach Lemma 7.1.17 genügt es nun, $PE = 0$ zu zeigen, wobei

$$E = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & a & a^2 & \cdots & a^{(k-1)} \\ \vdots & \vdots & & \vdots & \\ 1 & a^{n-1} & a^{(n-1)\cdot 2} & \cdots & a^{(n-1)(k-1)} \end{pmatrix}$$

die Erzeugermatrix des Codes ist. Für $i = 1, \ldots, n-k$ und $j = 1, \ldots, k$ ist der (i,j)-Eintrag von PE aber gerade

$$\sum_{s=0}^{n-1} a^{is} a^{s(j-1)} = \sum_{s=0}^{n-1} (a^{i+j-1})^s = \frac{(a^{i+j-1})^n - 1}{a^{i+j-1} - 1} = 0,$$

wobei wird gerade $\mathrm{ord}(a) = n$ und $i + j - 1 < n$ verwendet haben. □

Wir beschäftigen uns nun mit einem Algorithmus zur Dekodierung, also mit der folgenden Frage: Gegeben sei ein linearer Code $\mathcal{C} \subseteq \mathbb{F}_q^n$ und $r \in \mathbb{F}_q^n$, wie findet man den/einen nächstgelegenen Punkt zu r in $\mathcal{C}$?
Für jedes $c \in \mathcal{C}$ gilt offensichtlich $d(r,c) = d(r-c, 0)$. Wenn dabei c ganz $\mathcal{C}$ durchläuft, durchläuft $r - c$ die gesamte Nebenklasse $r + \mathcal{C}$ (im gruppentheoretischen Sinn in der abelschen Gruppe $\mathbb{F}_q^n$). Anstatt den nächsten Punkt zu r im Code zu suchen, können wir also ebensogut den nächsten Punkt zu 0 in der Nebenklasse $r + \mathcal{C}$ suchen und ihn dann von r subtrahieren.
Da man sehr häufig immer bezüglich desselben Codes dekodieren möchte, listet man als Vorbereitung des Algorithmus zunächst alle Nebenklassen von $\mathcal{C}$ in $\mathbb{F}_q^n$ auf. In jeder Nebenklasse wählen wir dann ein Element von kleinstem Abstand zu 0 (genannt **Nebenklassenführer**).
Besonders leicht ist das mit Hilfe einer Prüfmatrix $P \in \mathrm{Mat}_{n-k,n}(\mathbb{F}_q)$ für $\mathcal{C}$. Es ist dann nämlich $r \equiv s \mod \mathcal{C}$ genau dann wenn $Pr = Ps$ gilt. Also parametrisiert $\mathbb{F}_q^{n-k}$ als Bild von P genau die Nebenklassen von $\mathcal{C}$. Wenn man für jedes $v \in \mathbb{F}_q^{n-k}$ also einen Nebenklassenführer f_v von $P^{-1}(v)$ gefunden hat, so ist für jedes $r \in \mathbb{F}_q^n$

$$r - f_{Pr}$$

ein nächstgelegenes Wort im Code. Man muss also nur Pr berechnen, und in der Liste den gewählten Nebenklassenführer f_{Pr} finden. Dieser Algorithmus zur Dekodierung nennt sich **Syndromdekodierung**.

Beispiel 7.1.30. (i) Wir betrachten den $(7,4)$-Code $\mathcal{C} \subseteq \mathbb{F}_2^7$ aus Beispiel 7.1.18 (iii), mit folgender Erzeuger- und Prüfmatrix (beachte dass $1 = -1$ in $\mathbb{F}_2$ gilt):

$$E = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \qquad P = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Wir wissen bereits dass $d_{\min}(\mathcal{C}) = 3$ gilt, der Code also 1-fehlerkorrigierend ist. Es gibt hier $\#\mathbb{F}_2^3 = 2^3 = 8$ Nebenklassen von $\mathcal{C}$ in $\mathbb{F}_2^7$, die wir in folgender Tabelle samt aller Nebenklassenführer auflisten.

$v \in \mathbb{F}_2^3$	Nebenklassenführer von $P^{-1}(v)$
$(0,0,0)^t$	0
$(0,0,1)^t$	e_7
$(0,1,0)^t$	e_6
$(0,1,1)^t$	e_2
$(1,0,0)^t$	e_5
$(1,0,1)^t$	e_3
$(1,1,0)^t$	e_1
$(1,1,1)^t$	e_4

Empfängt man etwa $r = e_5 + e_6 = (0,0,0,0,1,1,0)^t$, so berechnet man zunächst $Pr = (1,1,0)^t$ und liest den entsprechenden Nebenklassenführer e_1 ab. Der nächstgelegenste Punkt zu r im Code ist also

$$r - e_1 = (1,0,0,0,1,1,0)^t.$$

Jede Nebenklasse besitzt hier genau einen Nebenklassenführer, also existiert zu jedem $r \in \mathbb{F}_2^7$ genau ein Element im Code von kleinstem Abstand. Haben wir in der Übertragung höchstens einen Fehler gemacht, wird das richtige Codewort rekonstruiert.

(ii) Wir betrachten den $(6,3)$-Code $\mathcal{C}$ über $\mathbb{F}_2$ mit folgender Erzeuger- und Prüfmatrix:

$$E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \qquad P = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Man sieht an den Spalten von P dass $d_{\min}(\mathcal{C}) = 3$ gilt, der Code also einen Fehler korrigieren kann. Es gibt auch hier $\#\mathbb{F}_2^3 = 8$ Nebenklassen, die hier wiederum mit allen Nebenklassenführern aufgelistet sind:

$v \in \mathbb{F}_2^3$	Nebenklassenführer von $P^{-1}(v)$
$(0,0,0)$	0
$(0,0,1)$	e_6
$(0,1,0)$	e_5
$(0,1,1)$	e_1
$(1,0,0)$	e_4
$(1,0,1)$	e_2
$(1,1,0)$	e_3
$(1,1,1)$	$e_1+e_4, e_2+e_5, e_3+e_6$

Die letzte aufgelistete Nebenklasse besitzt hier 3 Nebenklassenführer. Für alle $r \in \mathbb{F}_2^6$ mit $Pr = (1,1,1)^t$ existieren also 3 Punkte im Code mit minimalen Abstand. Zusammen mit der 1-Fehlerkorrektur bedeutet das natürlich, dass diese Elemente nicht durch einen Fehler aus dem Code entstehen können. △

7.2 Kryptographie

In der Kryptographie möchte man eine Nachricht so veschlüsseln, dass man sie einem Empfänger zukommen lassen kann, ohne dass ein eventueller unerwünschter Zuhörer den Inhalt versteht. Der Empfänger selbst soll den Inhalt jedoch selbstverständlich verstehen können. Dazu ändert man die eigentliche Information zunächst ab, d.h. man *verschlüsselt* sie. Der Empfänger muss die Nachricht dann wieder *entschlüsseln*, um die ursprüngliche Information zu erhalten. Gewöhnlich müssen Sender und Empfänger dazu vorher eine geheime Vereinbarung über

den Schlüssel getroffen haben. Nur in der modernen Public-Key-Verschlüsselung kann das teilweise umgangen werden. In der Standardnotation der Kryptographie wird die Senderin gewöhnlich Alice (kurz A) und der Empfänger Bob (kurz B) genannt. Die unerwünschte Zuhörerin heißt Eve (kurz E).
Eine sehr alte und bekannte Verschlüsselungsmethode ist die **Cäsar-** oder auch **Ersetzungs-Verschlüsselung**. Dabei vereinbaren Alice und Bob einfach eine beliebige Ersetzungsregel für Buchstaben. Jeder Buchstabe der eigentlichen Nachricht (*Klartext*) wird gemäß der Regel von Alice ersetzt, und der entstandene *Geheimtext* wird dadurch unverständlich. Bob macht die Ersetzung dann rückgängig, und erhält wieder den Klartext.

Klartext	a	b	c	⋯	x	y	z
Geheimtext	d	j	o	⋯	t	q	l

Oft wird dabei auch nur eine Verschiebung der Buchstaben verwendet, anstatt einer beliebigen Permutation. Dadurch kann die Ersetzungsregel deutlich einfacher vereinbart werden, etwa einfach durch den Buchstaben, durch den a ersetzt wird:

Klartext	a	b	c	⋯	x	y	z
Geheimtext	f	g	h	⋯	c	d	e

Solch eine Ersetzungs-Verschlüsselung ist für Eve aber relativ leicht zu knacken. Ist etwa bekannt dass nur eine Verschieberegel benutzt wurde, kann man einfach alle 26 möglichen Ersetzungsregeln durchprobieren, und mit sehr großer Wahrscheinlichkeit wird nur eine davon einen sinnvollen Klartext produzieren. Hat E keine Kenntnis über die benutzte Ersetzungsregeln, müsste sie allerdings

$$26! \sim 2^{88}$$

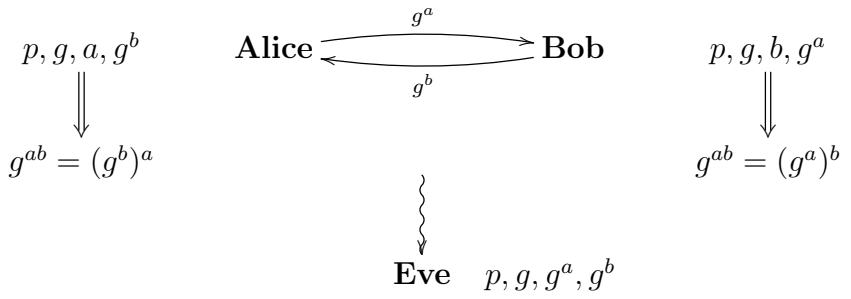
Ersetzungsregeln durchprobieren, was nicht möglich ist. Aber auch hier ist die Verschlüsselung leicht zu knacken, und zwar durch eine *Häufigkeitsanalyse* (allerdings hat es nach Cäsar ca. 600 Jahre gedauert, bis jemand auf diese Idee kam). Dazu bemerkt man, dass die verschiedenen Buchstaben in einer Sprache mit unterschiedlicher Häufigkeit vorkommen. Im Deutschen ist etwa das e der mit Abstand häufigste Buchstabe, gefolgt von n, i ... Wenn also ein langer Geheimtext vorliegt, wird der am häufigsten vorkommende Buchstabe vermutlich dem e entsprechen, der zweithäufigste dem n.... Wenn man so eine Weile herumprobiert, hat man den Geheimtext normalerweise schnell entschlüsselt.

Um dieses Problem zu umgehen, wurde ab dem 16. Jahrhundert die *Vigenère - Verschlüsselung* verwendet. Dabei wird nicht eine einzelne Ersetzungsregel verwendet, sondern von Buchstabe zu Buchstabe des Klartexts jeweils eine andere. Gewöhnlich benutzt man dazu folgendes Diagramm:

Klartext	a	b	c	···	x	y	z
Geheimtext	a	b	c	···	x	y	z
	b	c	d	···	y	z	a
	c	d	e	···	z	a	b
	⋮						
	y	z	a	···	v	w	x
	z	a	b	···	w	x	y

A und B vereinbaren nun ein *Schlüsselwort*, das die Abfolge der Ersetzungsregeln (anhand des ersten Buchstabens jeder Zeile) angibt. Lautet der Schlüssel beispielsweise BACH, so wird der erste Buchstabe des Klartexts mit der Ersetzungsregel aus Zeile 2 verschlüsselt, der zweite Buchstabe mit Zeile 1, der dritte Buchstabe mit Zeile 3, und der vierte Buchstabe mit Zeile 8. Danach beginnt man wieder mit Zeile 2... Eine klassische Häufigkeitsanalyse versagt hier völlig. Derselbe Buchstabe im Geheimtext kann je nach Position ja für zwei verschiedenen Buchstaben im Klartext stehen, und umgekehrt können zwei gleiche Buchstaben im Klartext zu verschiedenen Buchstaben im Geheimtext werden!
Erst im 19. Jahrhundert wurde eine Methode allgemein bekannt, die auch solch eine Verschlüsselung knacken kann. Es gibt in jeder Sprache einige kurze Worte, die relativ häufig vorkommen, im Deutschen beispielsweise "und", "der", "die" und "das". Ist nun das Schlüsselwort im Vergleich zum Klartext relativ kurz, kommt mit einiger Wahrscheinlichkeit eines dieser Wort öfters in einem Abstand vor, der ein Vielfaches der Schlüsselwortlänge ist. Das Wort wird also immer gleich verschlüsselt, und führt zu kurzen Buchstabenketten im Geheimtext, die immer wieder auftreten! Findet man also solche kurzen sich wiederholenden Buchstabenketten, hat man einen Hinweis auf die Länge des Schlüsselworts (sie ist ein Teiler der Distanzen dieser Buchstabenketten). Dann kann man den Geheimtext gemäß dieser Länge in Einzeltexte zerlegen, auf die man dann die klassische Häufigkeitsanalyse anwenden kann. Dann setzt man die entschlüsselten Einzeltexte wieder richtig zusammen, und hat den gesamten Klartext entschlüsselt.
Ist nun das Schlüsselwort im Vergleich zum Klartext relativ lang, wird aber auch diese Methode versagen. Und falls das Schlüsselwort genau gleich lang wie der Klartext ist, ist die Verschlüsselung auch in der Tat *nicht knackbar!* Denn selbst

wenn E einen Supercomputer zur Verfügung hätte, der alle möglichen Schlüsselworte durchprobieren könnte, würde sie dabei *alle möglichen Texte* der gleichen Länge des Klartexts produzieren! Das nutzt ihr natürlich überhaupt nichts. Hier sehen wir also: ist es A und B möglich, ein geheimes Schlüsselwort zu vereinbaren, so können sie später Nachrichten derselben Länge absolut sicher verschlüsseln!
Natürlich ist es heute in den meisten Fällen undenkbar, vor einer Nachrichtenübermittlung (z.B. an Amazon) persönlich vor Ort vorbeizukommen und ein langes geheimes Schlüsselwort zu vereinbaren. Hier kommt nun das erste Public-Key-Verfahren ins Spiel, das **Diffie-Hellman-Verfahren** zum öffentlichen Schlüsselaustausch. Dabei können A und B über einen unsicheren Kanal Informationen austauschen, die zur Erstellung eines Schlüssels führen, den E nicht kennt. Wie der Schlüssel genau aussieht können A und B vorher nicht beeinflussen, er trägt also noch nicht die eigentliche Nachricht. Er kann aber dann wie gerade beschrieben zur sicheren Verschlüsselung der eigentlichen Nachricht verwendet werden.



Alice und Bob vereinbaren öffentlich eine Primzahl p und ein Element $g \in \mathbb{Z}/p\mathbb{Z}$. Alle auftretenden Rechnungen werden in $\mathbb{Z}/p\mathbb{Z}$ geführt (bzw. eigentlich in der multiplikativen Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$). Alice wählt nun zusätzlich eine Zahl $a \in \{1, \ldots, p-1\}$, die sie geheim hält. Bob wählt eine Zahl $b \in \{1, \ldots, p-1\}$, die er geheim hält. Dann sendet Alice an Bob die Zahl $g^a \in \mathbb{Z}/p\mathbb{Z}$ und Bob sendet an Alice $g^b \in \mathbb{Z}/p\mathbb{Z}$. Sowohl Alice als auch Bob können nun g^{ab} ausrechnen. Alice benutzt dazu die Formel

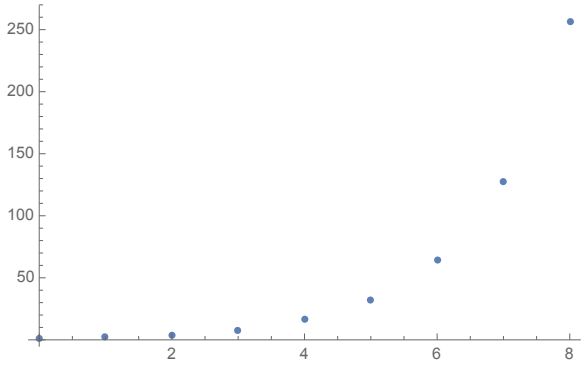
$$g^{ab} = (g^b)^a$$

und Bob verwendet

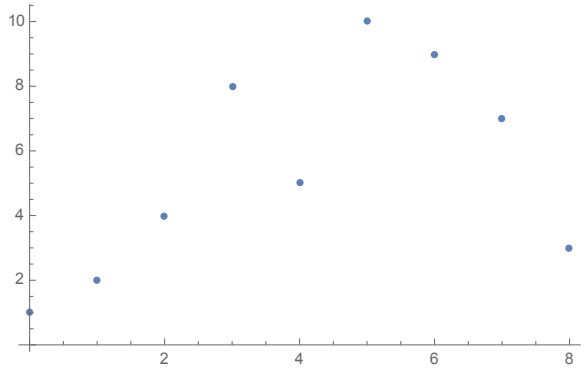
$$g^{ab} = (g^a)^b.$$

Diese Zahl ist nun der vereinbarte Schlüssel. Eve hingegen kennt nur die Zahlen p, g, g^a und g^b. Die einzige bisher bekannte Methode, daraus auch g^{ab} zu berech-

nen, besteht daraus, zunächst die Zahlen a oder b, und damit dann g^{ab} ausrechnen. Eve muss also den Logarithmus zur Basis g aus g^a berechnen. Die Berechnung eines klassischen Logarithmus in $\mathbb{Z}$ ist nicht allzu schwierig. Da Exponentialfunktionen monoton wachsend sind, kann man den Logarithmus relativ effizient durch einen Schachtelungs-Algorithmus ausrechnen.



Deshalb rechnen wir aber gerade in $\mathbb{Z}/p\mathbb{Z}$. Hier sieht eine Exponentialfunktion folgendermaßen aus:



Aufgrund des unvorhersagbaren Sprungverhaltens der Exponentialfunktion ist hier im Allgemeinen keine Möglichkeit bekannt, den Logarithmus anders als durch Durchprobieren aller Zahlen im Definitionsbereich der Exponentialfunktion zu berechnen. Für großes p ist das praktisch nicht durchführbar. Somit kann Eve das vereinbarte Schlüsselwort $g^{ab} \in \mathbb{Z}/p\mathbb{Z}$ nicht berechnen!
Allen Berechnungen kann man anstatt $(\mathbb{Z}/p\mathbb{Z})^\times$ natürlich eine beliebige andere Gruppe zugrunde legen, solange das Logarithmus-Problem, also die Berechnung von a aus g und g^a dort schwer ist. In additiver Schreibweise handelt es sich übrigens um die Frage nach der Berechenbarkeit von a aus g und $a \cdot g$.

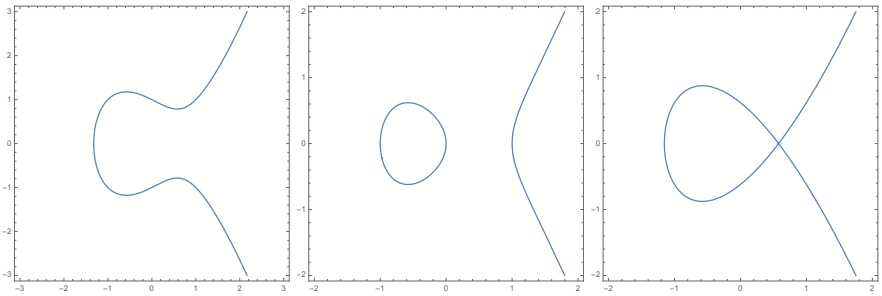
In der Praxis wird dabei oft auch die Gruppe einer *elliptischen Kurve* verwendet. Sei dazu K ein beliebiger Körper.

Definition 7.2.1. Seien $r, s \in K$. Dann heißt die Menge

$$C = \{(a, b) \in \overline{K}^2 \mid b^2 = a^3 + ra + s\}$$

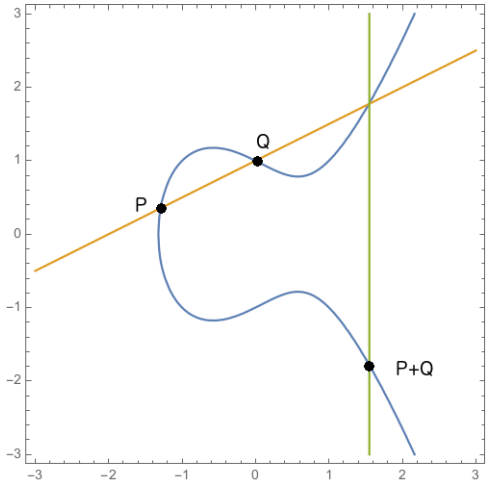
eine **elliptische Kurve über** K. Falls für einen Punkt $(a, b) \in C$ sogar $a, b \in K$ gilt, so heißt (a, b) ein **rationaler Punkt** der Kurve. △

Die folgenden Bilder zeigen für $K = \mathbb{R}$ die rationalen Punkte der elliptischen Kurven für die verschiedenen Parameter $(r, s) = (-1, 1), (r, s) = (-1, 0)$ und $(r, s) = (-1, 2/\sqrt{27})$:



Die rationalen Punkte einer elliptischen Kurve C kann man mit einer Gruppenstruktur versehen, die man am besten geometrisch erklärt. Dazu verbindet man zwei Punkte P und Q der Kurve mit einer Geraden (im Fall $P = Q$ nimmt man die Tangente an die Kurve in P) . Diese schneidet C in einem weiteren Punkt. Diesen Punkt spiegelt man noch an der x-Achse, und definiert so $P + Q$. Damit man so wirklich eine Gruppe erhält, muss man die Kurve *projektiv* betrachten, also einen Punkt O im unendlichen hinzufügen. Dieser Punkt ist dann genau das neutrale Element der Gruppe. Spiegelt man P an der x-Achse, erhält man $-P$.

Für die Kryptographie verwendet man als Körper K hier meistens $\mathbb{F}_p$ mit p prim oder $\mathbb{F}_{2^n}$. Das Logarithmus-Problem ist in der entstehenden Gruppe nochmals schwieriger als in $\mathbb{F}_p^\times$ und deshalb kann man die gleiche Sicherheit mit kleineren Zahlen und damit kürzeren Rechenzeiten erreichen.



Nun wollen wir noch eine weitere wichtige Public-Key-Verschlüsselung kennenlernen, und zwar die **RSA-Methode**. Hier erstellt Bob sowohl einen geheimen Schlüssel nur für sich selbst, sowie einen öffentlichen Schlüssel für alle anderen. Jede Person, also zum Beispiel Alice, kann mit Hilfe des öffentlichen Schlüssels eine Nachricht verschlüsseln und an ihn schicken. Entschlüsselt werden kann sie erst mit Hilfe von Bobs geheimem Schlüssel. Hier wird die Nachricht direkt verschlüsselt, ohne in einem ersten Schritt einen geheimen Schlüssel zu erzeugen, der anschließend für die Verschlüsselung verwendet wird.

Definition 7.2.2. Für $n \in \mathbb{N}$ sei

$$\varphi(n) := \#\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}.$$

Die so definierte Funktion $\varphi\colon \mathbb{N} \to \mathbb{N}$ heißt **Eulersche Phi-Funktion**. △

Wir wissen bereits, dass $a \in (\mathbb{Z}/n\mathbb{N})^{\times}$ äquivalent zu $\mathrm{ggT}(a,n) = 1$ ist. Die Eulersche Phi-Funktion gibt also die Anzahl der zu n teilerfremden Zahlen $< n$ an.

Proposition 7.2.3. *Sei p eine Primzahl, $e \in \mathbb{N}$, sowie $n, m \in \mathbb{N}$ teilerfremd. Dann gilt:*

(i) $\varphi(p^e) = p^{e-1}(p-1)$

(ii) $\varphi(mn) = \varphi(m)\varphi(n)$.

Also gilt mit der Primfaktorzerlegung $n = p_1^{e_1} \cdots p_r^{e_r}$ von n immer

$$\varphi(n) = p_1^{e_1-1}(p_1-1)\cdots p_r^{e_r-1}(p_r-1).$$

Beweis. Aufgabe 102. □

Bob wählt nun zwei Primzahlen p, q und berechnet $n = pq$. Nach Proposition 7.2.3 kann er auch

$$\varphi(n) = (p-1)(q-1)$$

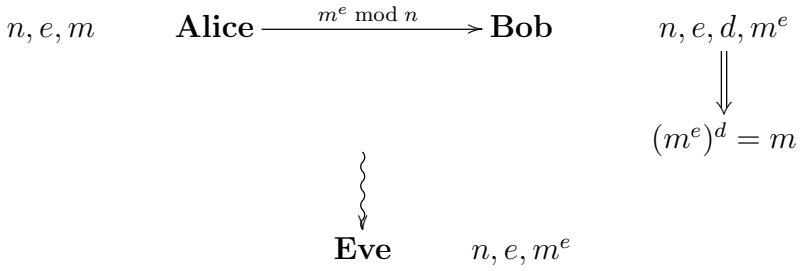
leicht berechnen. Schließlich wählt Bob noch eine zu $\varphi(n)$ teilerfremde Zahl e und berechnet

$$d := e^{-1} \in (\mathbb{Z}/\varphi(n)\mathbb{Z})^\times.$$

Das lässt sich mit dem Euklidischen Algorithmus relativ leicht machen. Es gilt also

$$de = k\varphi(n) + 1$$

für ein $k \in \mathbb{N}$. Öffentlich bekannt gegeben werden von Bob nun die Zahlen n, e, die Zahl d hingegen hält er geheim. Die Zahlen $p, q, \varphi(n)$ werden nicht mehr benötigt und können von Bob gelöscht werden.



Alice möchte nun die Nachricht $m \in \mathbb{Z}/n\mathbb{Z}$ an Bob übermitteln. Dazu berechnet sie m^e modulo n, und schickt das Ergebnis an Bob. Gilt $\mathrm{ggT}(m, n) = 1$ so rechnet Bob nun in $\mathbb{Z}/n\mathbb{Z}$:

$$(m^e)^d = m^{ed} = m^{k\varphi(n)+1} = (m^{\varphi(n)})^k \cdot m = 1^k \cdot m = m.$$

Dabei haben wir den Satz von Lagrange in der Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ benutzt:

$$m^{\varphi(n)} \equiv 1 \bmod n.$$

Im Fall $\mathrm{ggT}(m, n) \neq 1$ können wir o.B.d.A. annehmen $\mathrm{ggT}(m, n) = p$, woraus folgt

$$m^{ed} \equiv 0 \bmod p.$$

Weiters ist $\mathrm{ggT}(m, q) = 1$ und damit wiederum mit dem Satz von Lagrange

$$m^{\varphi(q)} \equiv 1 \bmod q.$$

Dies liefert in $\mathbb{Z}/q\mathbb{Z}$:

$$\begin{aligned} m^{ed} &= m^{ed-1}m = m^{k\varphi(n)}m = m^{k(p-1)(q-1)}m \\ &= (m^{q-1})^{k(p-1)}m = 1^{k(p-1)}m = m. \end{aligned}$$

Insgesamt haben wir also

$$m^{ed} \equiv m \bmod p \qquad \text{sowie} \qquad m^{ed} \equiv m \bmod q.$$

Da p und q zwei verschiedene Primzahlen sind, impliziert das

$$m^{ed} \equiv m \bmod n.$$

Bob hat also die Nachricht entschlüsselt.
Warum kann Eve nun die Nachricht nicht entschlüsseln? Eve kennt e, n und m^e. Sie muss also die e-te Wurzel aus m^e in $\mathbb{Z}/n\mathbb{Z}$ ziehen. Das ist aber ein schweres Problem. Die offensichtliche Vorgehensweise wäre natürlich, wie Bob ebenfalls zunächst $d = e^{-1}$ in $\mathbb{Z}/\varphi(n)\mathbb{Z}$ zu berechnen. Dazu muss sie aber zunächst $\varphi(n)$ kennen. Für Bob war das leicht, da er $n = pq$ direkt als Produkt zweier Primzahlen konstruiert hat und deshalb $\varphi(n) = (p-1)(q-1)$ direkt ablesen kann. Eve müsste nun umgekehrt die Primfaktorzerlegung von n und damit dann $\varphi(n)$ berechnen. *Zerlegung in Primfaktoren* ist aber ein schwieriges Problem und bei groß genug gewählten p, q für n praktisch nicht durchführbar! Eine andere Methode zur Bestimmung von m aus m^e, e und n ist nicht bekannt.
Die RSA-Methode kann auch zum *Signieren* einer (nicht verschlüsselten) Nachricht verwendet werden. Wenn Bob etwa an Alice eine Nachricht $m \in \mathbb{Z}/n\mathbb{Z}$ schicken möchte, dann sendet er ihr sowohl m also auch $m^d \in \mathbb{Z}/n\mathbb{Z}$. Alice berechnet nun

$$(m^d)^e = m^{de} = m \in \mathbb{Z}/n\mathbb{Z}$$

und vergleicht das Ergebnis mit m. Da es übereinstimmt, stammt die Nachricht von Bob. Eve kann auf dieselbe Weise keine Nachricht signieren, da sie dazu wiederum d kennen müsste. Bob gibt übrigens durch das Versenden von m und m^d keine relevante Information über d bekannt. Eve müsste in $\mathbb{Z}/n\mathbb{Z}$ den Logarithmus zur Basis m aus m^d berechnen. Das ist schwer, wie wir uns oben bei Diffie-Hellman schon überzeugt haben.

7.3 Kategorientheorie

Hier lernen wir eine Sichtweise kennen, anhand derer man viele der bisherigen Konzepte, und viele Konzepte der Mathematik überhaupt, besser einordnen und

verstehen kann.

Definition 7.3.1. (i) Eine **Kategorie** $\mathcal{C}$ besteht aus einer Klasse

$$\mathrm{Obj}(\mathcal{C})$$

(von sogenannten **Objekten**) und für alle $X, Y \in \mathrm{Obj}(\mathcal{C})$ jeweils einer Menge

$$\mathcal{C}(X, Y)$$

(von sogenannten **Morphismen**), sowie einer partiellen Verknüpfung von Morphismen

$$\begin{aligned} \mathcal{C}(X,Y) \times \mathcal{C}(Y,Z) &\to \mathcal{C}(X,Z) \\ (f,g) &\mapsto g \circ f \end{aligned}$$

welche folgenden zwei Bedingungen genügt:

(1) $\forall X \in \mathrm{Obj}(\mathcal{C})\ \exists \mathrm{id}_X \in \mathcal{C}(X,X)$ mit

$$\mathrm{id}_X \circ f = f,\ g \circ \mathrm{id}_X = g$$

für alle $f \in \mathcal{C}(Y,X), g \in \mathcal{C}(X,Y)$.

(2) Für alle $f \in \mathcal{C}(W,X), g \in \mathcal{C}(X,Y), h \in \mathcal{C}(Y,Z)$ gilt

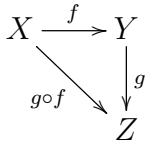
$$h \circ (g \circ f) = (h \circ g) \circ f.$$

(ii) Ein $f \in \mathcal{C}(X,Y)$ heißt **Isomorphismus**, falls $g \in \mathcal{C}(Y,X)$ existiert mit

$$g \circ f = \mathrm{id}_X,\ f \circ g = \mathrm{id}_Y.$$

(iii) Zwei Objekte $X, Y \in \mathrm{Obj}(\mathcal{C})$ heißen **isomorph** (in Zeichen $X \cong Y$), falls in $\mathcal{C}(X,Y)$ ein Isomorphismus existiert. △

Grafisch stellt man Ausschnitte aus Kategorien gewöhnlich durch (kommutative) Pfeildiagramme dar:



Beispiel 7.3.2. (i) Die **Kategorie $\mathcal{M}\mathrm{en}$ der Mengen** hat als Objekte die Mengen und als Morphismen die Abbildungen, wobei die Verknüpfung gerade die Hintereinanderausführung ist. Ein Isomorphismus ist eine bijektive (also invertierbare) Abbildung, und zwei Mengen sind isomorph wenn sie die gleiche Mächtigkeit besitzen.
(ii) Für jeden festen Körper K hat die **Kategorie K-$\mathcal{V}ec$ der K-Vektorräume** als Objekte die K-Vektorräume und als Morphismen die K-linearen Abbildungen.
(iii) Die **Kategorie $\mathcal{T}\mathrm{op}$ der topologischen Räume** hat als Objekte die topologischen Räume und als Morphismen die stetigen Abbildungen. Ein Isomorphismus ist gerade ein Homöomorphismus, und isomorphe Objekte sind homöomorphe Räume.
(iv) Morphismen müssen nicht immer Abbildungen sein. Sei etwa $(G, \cdot)$ eine feste Gruppe. Wir definieren eine Kategorie $\mathcal{C}_G$ durch

$$\mathrm{Obj}(\mathcal{C}_G) := \{*\}$$

und

$$\mathcal{C}_G(*, *) := G.$$

Die Gruppenverknüpfung $\cdot$ dient uns dabei als Verknüpfung von Morphismen

$$\cdot \colon \mathcal{C}_G(*, *) \times \mathcal{C}_G(*, *) \to \mathcal{C}_G(*, *)$$

und man überprüft leicht die Bedingungen (1) und (2). Auf diese Weise lässt sich G als eigene Kategorie auffassen. Jeder Morphismus ist hier ein Isomorphismus. △

Definition 7.3.3. Ein **kovarianter** (bzw. **kontravarianter**) **Funktor** von der Kategorie $\mathcal{C}$ in die Kategorie $\mathcal{D}$ besteht aus einer Abbildung

$$\mathcal{F} \colon \mathrm{Obj}(\mathcal{C}) \to \mathrm{Obj}(\mathcal{D})$$

sowie Abbildungen

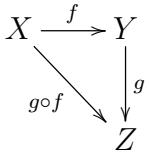
$$\mathcal{F} \colon \mathcal{C}(X, Y) \to \mathcal{D}(\mathcal{F}(X), \mathcal{F}(Y))$$

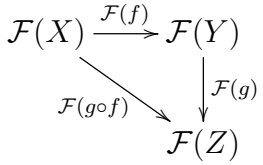
$$(\text{bzw. } \mathcal{F} \colon \mathcal{C}(X, Y) \to \mathcal{D}(\mathcal{F}(Y), \mathcal{F}(X)))$$

mit

(1) $\mathcal{F}(\mathrm{id}_X) = \mathrm{id}_{\mathcal{F}(X)}$

(2) $\mathcal{F}(g \circ f) = \mathcal{F}(g) \circ \mathcal{F}(f)$ (bzw. $\mathcal{F}(g \circ f) = \mathcal{F}(f) \circ \mathcal{F}(g)$).





△

Beispiel 7.3.4. (*i*) Die Bildung des Dualraums ist ein kontravarianter Funktor von K-$\mathcal{V}ek$ in sich selbst.
(*ii*) Sei X ein fest gewählter K-Vektorraum. Dann ist die Zuordnung

$$V \mapsto X \otimes V$$

ein kovarianter Funktor von K-$\mathcal{V}ek$ in sich selbst. Eine lineare Abbildung $\varphi\colon V \to W$ wird dabei auf

$$\mathrm{id}_X \otimes \varphi\colon X \otimes V \to X \otimes W$$

abgebildet.
(*iii*) Es gibt den kovarianten Funktor $\mathcal{T}\mathrm{op} \to \mathcal{M}\mathrm{en}$, der jedem topologischen Raum die Menge seiner Zusammenhangskomponenten zuordnet. Stetige Abbildungen erhalten Zusammenhang, also induzieren sie Abbildungen zwischen den Mengen der Zusammenhangskomponenten.
(*iv*) Sei $\mathcal{C}$ eine Kategorie, in der die Objekte wirklich aus Mengen und die Morphismen wirklich aus Abbildungen zwischen diesen bestehen (wie z.B. $\mathcal{T}\mathrm{op}$, K-$\mathcal{V}ec$, ...). Der **Vergiss-Funktor** ist ein kovarianter Funktor $\mathcal{C} \to \mathcal{M}\mathrm{en}$, der einfach eine eventuelle zusätzliche Struktur auf den Objekten der Kategorie (z.B. eine Topologie, eine Vektorraumstruktur,...) vergisst. Ebenso vergisst er die Tatsache, dass Morphismen eventuell sehr spezielle Abbildungen sind, und betrachtet sie einfach nur noch als Abbildungen. △

Lemma 7.3.5. *Sei $\mathcal{F}\colon \mathcal{C} \to \mathcal{D}$ ein Funktor und in $\mathcal{C}$ gelte $X \cong Y$. Dann gilt in $\mathcal{D}$*

$$\mathcal{F}(X) \cong \mathcal{F}(Y).$$

Beweis. Sei o.B.d.A. $\mathcal{F}$ kovariant. Sei $f \in \mathcal{C}(X,Y)$ ein Isomorphismus mit inversem Morphismus $g \in \mathcal{C}(Y,X)$. Dann gilt $g \circ f = \mathrm{id}_X$ und nach Anwendung von $\mathcal{F}$ also

$$\mathrm{id}_{\mathcal{F}(X)} = \mathcal{F}(\mathrm{id}_X) = \mathcal{F}(g \circ f) = \mathcal{F}(g) \circ \mathcal{F}(f).$$

Analog bekommt man $\mathcal{F}(f) \circ \mathcal{F}(g) = \mathrm{id}_{\mathcal{F}(Y)}$ und damit $\mathcal{F}(X) \cong \mathcal{F}(Y)$. □

Bemerkung 7.3.6. Oft möchte man die Isomorphie von zwei Objekten einer Kategorie entscheiden (sind zwei Vektorräume isomorph, sind zwei topologische Räume homöomorph,....?) Wenn sie isomorph sind, kann man oft einen Isomorphismus angeben und hat die Frage damit entschieden. Wenn sie nicht isomorph sind, ist die Frage oft schwieriger. Man muss dann Eigenschaften der Objekte finden, die sie voneinander unterscheiden und die Isomorphie ausschließen. Etwas konzeptioneller formuliert wendet man zunächst einen Funktor an. Sind die Objekte dann nicht isomorph, waren sie es vorher auch nicht.
Haben beispielsweise zwei topologische Räume eine unterschiedliche Anzahl von Zusammenhangskomponenten, können sie nicht homöoorph sein. Diese Argumentation entspricht der Anwendung des Funktors aus Beispiel 7.3.4 (iii). Sind die Dualräume von zwei Vektorräumen nicht isomorph, so sind es die Räume selbst auch nicht. Das entspricht dem Funktor aus Beispiel 7.3.4 (i). Noch banaler ist folgende Beobachtung: haben zwei Vektorräume nicht dieselbe Mächtigkeit (als Mengen), so sind sie nicht isomorph. Extrem abgehoben kann man sagen, dass man diese Beobachtung aus dem Vergissfunktor und Lemma 7.3.5 erhält. △

7.4 Garbentheorie

In diesem Abschnitt befassen wir uns kurz mit dem sehr allgemeinen Begriff einer Garbe, der in vielen Bereichen der Mathematik auftritt.

Definition 7.4.1. Sei X ein topologischer Raum. Eine **Ring-Prägarbe** $\mathcal{F}$ auf X besteht aus den folgenden Daten:

(i) Für jede offene Teilmenge $U \subseteq X$ ein Ring $\mathcal{F}(U)$, wobei $\mathcal{F}(\emptyset) = \{0\}$ gelte.

(ii) Für je zwei offene Teilmengen $U \subseteq V$ ein Ringhomomorphismus

$$r_{V,U} \colon \mathcal{F}(V) \to \mathcal{F}(U),$$

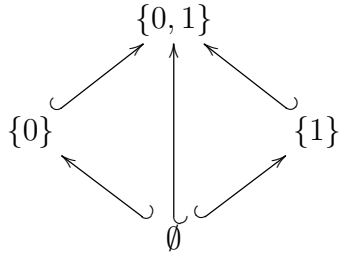
genannt die **Restriktion von** V **auf** U. Dabei gelte für drei offene Mengen $U \subseteq V \subseteq W$ stets

$$r_{V,U} \circ r_{W,V} = r_{W,U}$$

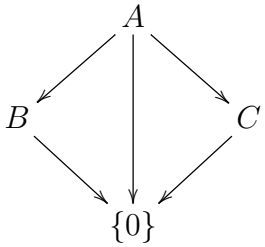
sowie $r_{U,U} = \mathrm{id}_{\mathcal{F}(U)}$. △

Bemerkung 7.4.2. (i) Offensichtlich kann man eine **Gruppen-, Vektorraum-, Mengen-, etc.-**Prägarbe ganz analog definieren, wenn man den Begriff Ring und Ringhomomorphismus jeweils entsprechend ersetzt.
(ii) Noch etwas allgemeiner formuliert man das so: Der topologische Raum X kann als eigene Kategorie $\mathcal{X}$ aufgefasst werden. Dabei sind die Objekte gerade die offenen Teilmengen, und die Morphismen sind die Inklusionen. Für eine beliebige weitere Kategorie $\mathcal{K}$ ist eine **Prägarbe mit Werten in** $\mathcal{K}$ (oder eine $\mathcal{K}$**-Prägarbe**) dann einfach ein kontravarianter Funktor von $\mathcal{X}$ nach $\mathcal{K}$. Wir wollen uns im folgenden aber immer auf Ringe beschränken. △

Beispiel 7.4.3. (i) Seien X, W topologische Räume. Für $U \subseteq X$ offen sei $\mathcal{C}(U, W)$ die Menge aller stetigen Funktionen von U nach W (je nach weiterer Struktur von W kann das z.B. auch ein Ring sein). Wiederum mit der Restriktion von Funktionen auf kleinere Definitionsbereiche erhalten wir eine Prägarbe $\mathcal{C}$ auf X, genannt die **Prägarbe der stetigen Funktionen mit Werten in** W. So ähnlich kann man Prägarben von differenzierbaren- oder holomorphen Funktionen definieren.
(ii) Sei $X = \{0, 1\}$ versehen mit der feinstmöglichen Topologie. Der Verband der offenen Mengen sieht also folgendermaßen aus:



Eine Prägarbe auf X besteht also aus einem kommutativen Diagramm von Ringen des folgenden Typs



(iii) Sei $\mathcal{F}$ eine Prägarbe auf X, und $U \subseteq X$ offen. Jede offene Teilmenge von U ist eine offene Teilmenge von X, und somit kann man $\mathcal{F}$ einfach auf U einschränken. Die so entstehende Prägarbe auf U bezeichnen wir mit $\mathcal{F}_{|U}$. △

Um die Lokalität der Bedingung an die verwendeten Funktionen in Beispiel 7.4.3 (i) axiomatisch zu erfassen, definiert man nun den Begriff einer Garbe.

Definition 7.4.4. Sei X ein topologischer Raum. Eine **Garbe** auf X ist eine Prägarbe $\mathcal{F}$, die zusätzlich folgende Bedingung erfüllt:
Für jedes offene $U \subseteq X$, jede offene Überdeckung $U = \bigcup_{i \in I} U_i$ und jede Auswahl von Elementen $s_i \in \mathcal{F}(U_i)$ mit

$$r_{U_i, U_i \cap U_j}(s_i) = r_{U_j, U_i \cap U_j}(s_j)$$

für alle $i, j \in I$, gibt es *genau ein* $s \in \mathcal{F}(U)$ mit

$$r_{U, U_i}(s) = s_i$$

für alle $i \in I$. △

Bemerkung/Beispiel 7.4.5. (i) Denkt man sich jedes $\mathcal{F}(U)$ wirklich als Menge von auf U definierten Funktionen, so sagt die Garbeneigenschaft, dass die Bedingung an die betrachteten Funktionen *lokal* ist. Für vorgegebene Funktionen s_i auf U_i, die auf allen paarweisen Schnitten übereinstimmen, gibt es natürlich immer genau eine global auf U definierte Funktion s, die alle s_i fortsetzt. Dieses s muss aber nun automatisch die in $\mathcal{F}$ geforderten Bedingungen erfüllen.
(ii) Die in Beispiel 7.4.3 (i) betrachtete Prägarbe $\mathcal{C}$ der stetigen Funktionen ist sogar eine Garbe, denn Stetigkeit ist eine lokale Bedingungen.
(iii) Die in Beispiel 7.4.3 (ii) betrachtete Prägarbe ist nicht notwendigerweise eine Garbe. Die Bedingung ist hier, dass jedes Paar von Elementen $b \in B, c \in C$ genau ein gemeinsames Urbild in A hat.
(iv) Die Einschränkung $\mathcal{F}_{|U}$ einer Garbe $\mathcal{F}$ auf eine offene Teilmenge $U \subseteq X$ ist offensichtlich wieder eine Garbe. △

Definition 7.4.6. Seien $(X, \mathcal{F}), (Y, \mathcal{G})$ topologische Räume mit (Prä-)Garben. Ein **Morphismus von (Prä-)Garben** besteht aus den folgenden Daten:

- Eine stetige Abbildung $f\colon X \to Y$.

- Für jede offene Menge $U \subseteq Y$ ein Ringhomomorphismus

$$f_U^* \colon \mathcal{G}(U) \to \mathcal{F}(f^{-1}(U))$$

so dass für $U \subseteq V \subseteq Y$ das folgende Diagramm stets kommutiert:

$$\begin{array}{ccc} \mathcal{G}(V) & \xrightarrow{f_V^*} & \mathcal{F}(f^{-1}(V)) \\ {\scriptstyle r_{V,U}}\downarrow & & \downarrow{\scriptstyle r_{f^{-1}(V),f^{-1}(U)}} \\ \mathcal{G}(U) & \xrightarrow[f_U^*]{} & \mathcal{F}(f^{-1}(U)) \end{array}$$

Wir schreiben oft auch einfach f^* statt f_U^*, und bezeichnen den gesamten Homomomorphismus mit (f, f^*). △

Bemerkung/Beispiel 7.4.7. (i) Morphismen von (Prä-)Garben kann man auf die offensichtliche Weise hintereinander ausführen. Ebenso ist die Identität ein offensichtlicher Morphismus. Deshalb erhalten wir auch einen kanonischen Begriff von **(Prä-)Garbenisomorphismus**, als Morphismus mit beidseitigem Inversen. Es ist (f, f^*) genau dann ein Isomorphismus, wenn f ein Homöomorphismus und alle f_U^* Isomorphismen der jeweiligen Ringe sind.
(ii) Die Abbildung f_U^* nennt man auch die **Zurückziehung** von Elementen aus $\mathcal{G}(U)$ nach $\mathcal{F}(f^{-1}(U))$. Sind $\mathcal{F}, \mathcal{G}$ Garben von Funktionen, handelt es sich dabei oft wirklich um die Zurückziehung durch Komposition mit f. Man benötigt dabei dann die Bedingung, dass alle Zurückziehungen von Funktionen aus $\mathcal{G}$ die in $\mathcal{F}$ spezifierte Bedingung erfüllen.
(iii) Sind X, Y topologische Räume mit der Garbe der stetigen Funktionen mit Werten in W, dann erhält man für jede stetige Funktion $f \colon X \to Y$ einen Morphismus, indem man f^* als Zurückziehung mittels f definiert. △

Konstruktion 7.4.8. Um das lokale Verhalten einer (Prä-)Garbe an einem Punkt zu erfassen, definiert man den Begriff eines *Halms*. Sei dazu $(X, \mathcal{F})$ eine (Prä-) Garbe und $x \in X$. Auf der Menge

$$\mathcal{M} := \{(U, s) \mid x \in U, U \subseteq X \text{ offen}, s \in \mathcal{F}(U)\}$$

definiert man folgende Äquivalenzrelation:

$$(U, s) \sim (V, t) \ :\Leftrightarrow\ \exists W \subseteq U \cap V \text{ offen}, x \in W, \text{ mit } r_{U,W}(s) = r_{V,W}(t).$$

Im Fall einer Garbe von Funktionen bedeutet das: zwei auf Umgebungen von x definierte Funktionen sind äquivalent, wenn sie auf einer kleinen offenen Umgebung von x übereinstimmen. Die Menge

$$\mathcal{F}_x := \mathcal{M}/\sim = \{[(U,s)] \mid (U,s) \in \mathcal{M}\}$$

der Äquivalenzklassen trägt nun eine kanonische Ringstruktur:

$$[(U,s)] \dot{+} [(V,t)] := [(U \cap V, r_{U,U\cap V}(s) \dot{+} r_{V,U\cap V}(t))].$$

Etwas abstrakter formuliert ist $\mathcal{F}_x$ gerade der *direkte Limes* des gerichteten Systems der Ringe $\mathcal{F}(U)$ mit Restriktionsabbildungen, wobei U alle offenen Umgebungen von x durchläuft. △

Definition 7.4.9. Der Ring $\mathcal{F}_x$ heißt **Halm der (Prä-)Garbe $\mathcal{F}$ am Punkt** x. △

Bemerkung 7.4.10. (i) Für offenes $U \subseteq X$ mit $x \in U$ gibt es den kanonischen Homomorphismus

$$\begin{aligned} \mathcal{F}(U) &\to \mathcal{F}_x \\ s &\mapsto [(U,s)]. \end{aligned}$$

(ii) Ist $\varphi = (f, f^*)\colon (X,\mathcal{F}) \to (Y,\mathcal{G})$ ein Garbenmorphismus, so induziert er für jedes $x \in X$ einen kanonischen Morphismus der Halme

$$\begin{aligned} \varphi_x\colon \mathcal{G}_{f(x)} &\to \mathcal{F}_x \\ [(U,s)] &\mapsto [(f^{-1}(U), f^*(s))]. \end{aligned}$$ △

Satz 7.4.11. *Sei $\varphi = (f, f^*)\colon (X,\mathcal{F}) \to (Y,\mathcal{G})$ ein Morphismus von Garben, wobei f ein Homöomorphismus der topologischen Räume sei. Dann ist φ genau dann ein Isomorphismus, wenn für alle $x \in X$ die induzierten Morphismen φ_x der Halme Isomorphismen sind.*

Beweis. Ist φ ein Isomorphismus, so sind alle φ_x offensichtlich ebenfalls Isomorphismen, denn der Umkehrmorphismus von φ induziert die Umkehrmorphismen der φ_x.
Seien also umgekehrt alle φ_x Isomorphismen. Da f ein Homöomorphismus ist, können wir nach Umbenennung der Elemente $X = Y$ und $f = \mathrm{id}$ annehmen. Wir müssen nun zeigen, dass für jedes offene $U \subseteq X$ die Abbildung

$$f^*\colon \mathcal{G}(U) \to \mathcal{F}(U)$$

ein Ringisomorphismus ist. Dafür zeigen wir die Bijektivität. Sei also zunächst $s \in \mathcal{G}(U)$ mit $f^*(s) = 0$. Dann ist für jedes $x \in U$ auch das Bild von $f^*(s)$ in $\mathcal{F}_x$ Null, und aufgrund der Kommutativität des Diagramms

$$\begin{array}{ccc} \mathcal{G}(U) & \xrightarrow{f^*} & \mathcal{F}(U) \\ \downarrow & & \downarrow \\ \mathcal{G}_x & \xrightarrow[\varphi_x]{} & \mathcal{F}_x \end{array}$$

und der Injektivität von φ_x folgt, dass das Bild von s in $\mathcal{G}_x$ ebenfalls immer Null ist. Das bedeutet, dass jedes $x \in U$ eine offene Umgebung $U_x \subseteq U$ besitzt, mit $r_{U,U_x}(s) = 0$. Diese Mengen U_x liefern eine offene Überdeckung von U, und aus der Eindeutigkeitsbedingung im Garbenaxiom für $\mathcal{G}$ folgt direkt $s = 0$.
Für die Surjektivität von f^* sei $t \in \mathcal{F}(U)$ gegeben. Wir bilden t nach $\mathcal{F}_x$ ab und verwenden die Surjektivität von φ_x: es gibt ein $s_x \in \mathcal{G}_x$ mit

$$\varphi_x(s_x) = t \in \mathcal{F}_x.$$

Es wird s_x repräsentiert von einem Element $\tilde{s}_x \in \mathcal{G}(U_x)$, wobei $U_x \subseteq U$ eine offene Umgebung von x ist. Dann sind $f^*(\tilde{s}_x)$ und $r_{U,U_x}(t)$ zwei Elemente von $\mathcal{F}(U_x)$, die in $\mathcal{F}_x$ dasselbe Element repräsentieren. Wir können also o.B.d.A ihre Gleichheit annehmen (nach eventueller Verkleinerung von U_x):

$$f^*(\tilde{s}_x) = r_{U,U_x}(t).$$

Für $x, y \in U$ haben wir nun also $\tilde{s}_x \in \mathcal{G}(U_x)$ und $\tilde{s}_y \in \mathcal{G}(U_y)$, und nach Restriktion auf $U_x \cap U_y$ werden beide Elemente mittels f^* auf dasselbe abgebildet, nämlich die Einschränkung von t. Aus der bereits bewiesenen Injektivität von f^* (auf allen U) folgt also

$$r_{U_x,U_x\cap U_x}(\tilde{s}_x) = r_{U_y,U_x\cap U_y}(\tilde{s}_y).$$

Da die U_x die Menge U offen überdecken, gibt es laut Garbenaxiom für $\mathcal{G}$ ein $s \in \mathcal{G}(U)$ mit $r_{U,U_x}(s) = \tilde{s}_x$ für alle $x \in U$. Es gilt nun $f^*(s) = t$. Dafür genügt es aufgrund des Garbenaxioms an $\mathcal{F}$, die Gleichheit nach Restriktion auf alle Mengen U_x zu zeigen. Es gilt aber

$$r_{U,U_x}(t) = f^*(\tilde{s}_x) = f^*(r_{U,U_x}(s)) = r_{U,U_x}(f^*(s)).$$

Das beweist die Behauptung. □

Bemerkung 7.4.12. (i) Der Beweis von Satz 7.4.11 zeigt, dass die Injektivität aller φ_x die Injektivität aller f^* induziert. Für die Surjektivität der f^* haben wir aber außer der Surjektivität der φ_x auch noch die Injektivität von f^* verwendet. Im Allgemeinen impliziert die Surjektivität aller φ_x auch *nicht* die Surjektivität aller f^*.
(ii) Ohne genauer ins Detail zu gehen impliziert die Bemerkung aus (i), dass der Funktor $(X, \mathcal{F}) \mapsto \mathcal{F}(X)$ kein *exakter* Funktor ist. Man kann *Garbenkohomologie* deshalb als abgeleitete Funktorenfolge dieses Funktors definieren. △

Man kann eine Prägarbe immer eindeutig zu einer Garbe erweitern:

Satz 7.4.13. *Sei $\mathcal{F}$ eine Prägarbe auf X. Dann gibt es eine Garbe $\mathcal{F}^+$ auf X, sowie einen Morphismus $\iota = (\mathrm{id}, f^*) \colon (X, \mathcal{F}^+) \to (X, \mathcal{F})$, mit der folgenden universellen Eigenschaft:*
Jeder Morphismus $\varphi \colon (Y, \mathcal{G}) \to (X, \mathcal{F})$ von einer Garbe nach $(X, \mathcal{F})$ faktorisiert eindeutig durch ι:

$$\begin{array}{ccc} (Y, \mathcal{G}) & \xrightarrow{\varphi} & (X, \mathcal{F}) \\ & \searrow^{\exists!} & \uparrow{\scriptstyle \iota} \\ & & (X, \mathcal{F}^+) \end{array}$$

Dadurch ist $\mathcal{F}^+$ bis auf eindeutige Isomorphie eindeutig bestimmt. Man nennt $\mathcal{F}^+$ die **Garbifizierung von** *$\mathcal{F}$.*

Beweis. Für $U \subseteq X$ offen definieren wir $\mathcal{F}^+(U)$ als die Menge aller Abbildungen

$$s \colon U \to \bigsqcup_{x \in U} \mathcal{F}_x$$

mit den folgenden beiden Eigenschaften:

(1) $s(x) \in \mathcal{F}_x$ für alle $x \in U$.

(2) Für alle $x \in U$ gibt es eine offene Umgebung $U_x \subseteq U$ von x, und ein $t \in \mathcal{F}(U_x)$ mit
$$s(y) = t \text{ in } \mathcal{F}_y \text{ für alle } y \in U_x.$$

Wir betrachten also die *lokal konstanten* Abbildungen in die disjunkte Vereinigung der Halme über U. Offensichtlich trägt $\mathcal{F}^+(U)$ mit punktweise definierten Verknüpfungen eine Ringstruktur, und wir erhalten mit der wirklichen Restriktion

auf kleiner Definitionsmengen eine Prägarbe. Aufgrund der Lokalität der Bedingung (2) ist $\mathcal{F}^+$ aber sogar eine Garbe auf X.
Die Abbildungen $f^*\colon \mathcal{F}(U) \to \mathcal{F}^+(U)$ sind die offensichtlichen: jedes $t \in \mathcal{F}(U)$ definiert eine auf ganz U konstant durch t gegebene Funktion s. Der Beweis der universellen Eigenschaft ist Aufgabe 103. □

Bemerkung 7.4.14. Der Konstruktion von $\mathcal{F}^+$ sieht man direkt an, dass der Morphismus ι Isomorphismen aller Halme induziert:

$$\mathcal{F}_x \cong \mathcal{F}^+_x \qquad \text{für alle } x \in X.$$

Insbesondere kann Satz 7.4.11 ohne die Garbenbedingung nicht stimmen. △

Literaturverzeichnis

[1] Siegfried Bosch, *Algebra*, Springer, 7. Auflage, 2009.

[2] Gerd Fischer, *Lehrbuch der Algebra*, Viehweg und Teubner, 2. überarbeitete Auflage, 2011.

[3] Klaus Hulek, *Elementare algebraische Geometrie*, Vieweg, 2000.

[4] Ernst Kunz, *Algebra*, Vieweg und Teubner, 1. Auflage, 1991.

[5] Serge Lang, *Algebra*, Springer, 3rd revised edition, 2002.

[6] Igor R. Shafarevich, *Basic algebraic geometry 1*, Springer, 2013.

[7] Ian Nicholas Stewart, *Galois Theory*, Chapman and Hall/CRC, 4th edition, 2015.

[8] Gernot Stroth, *Algebra: Einführung in die Galoistheorie*, De Gruyter, 2. Auflage, 2013.

Übungsaufgaben

Aufgabe 1. Für eine komplexe Zahl $z = a + ib \in \mathbb{C}$ setzen wir

$$\mathrm{Re}(z) := a,\ \mathrm{Im}(z) := b,\ \overline{z} := a - ib,\ |z| = \sqrt{a^2 + b^2}.$$

(a) Zeigen Sie, dass für komplexe Zahlen z, z_1, z_2 gilt:
(i) $\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2,\ \overline{z_1 z_2} = \overline{z}_1 \overline{z}_2,\ \overline{z^{-1}} = \overline{z}^{-1}$
(ii) $z + \overline{z} = 2\mathrm{Re}(z),\ z - \overline{z} = 2i\mathrm{Im}(z),\ z \cdot \overline{z} = |z|^2$
(iii) $|z| = |\overline{z}|,\ |z_1 z_2| = |z_1| \cdot |z_2|,\ |z^{-1}| = |z|^{-1}$
(iv) $|z_1 + z_2| \leq |z_1| + |z_2|$
(v) Finden Sie eine Formel für $\mathrm{Re}(z_1 z_2),\ \mathrm{Im}(z_1 z_2)$.

(b) Finden Sie alle komplexen Lösungen der folgenden Gleichungen:

$$z^2 = -1,\ z^2 = -5,\ 2z^2 - 5z + 2 = 0.$$

Aufgabe 2. Für $\varphi \in \mathbb{R}$ setzen wir $e^{i\varphi} := \cos(\varphi) + i \sin(\varphi) \in \mathbb{C}$.

(a) Zeigen Sie, dass für $\varphi, \psi \in \mathbb{R}$ stets gilt
(i) $|e^{i\varphi}| = 1,\ \overline{e^{i\varphi}} = e^{i(-\varphi)}$
(ii) $e^{i\varphi} \cdot e^{i\psi} = e^{i(\varphi+\psi)}$ (Hinweis: Verwenden Sie die Additionstheoreme für Sinus und Cosinus)

(b) Zeigen Sie, dass für jedes $0 \neq z \in \mathbb{C}$ eindeutig bestimmte $r \in (0, \infty), \varphi \in [0, 2\pi)$ existieren mit

$$z = r \cdot e^{i\varphi}.$$

(Diese Darstellung von z heißt *Darstellung in Polarkoordinaten*).

(c) Zeigen Sie, dass für die Darstellung $z_1 = re^{i\varphi},\ z_2 = se^{i\psi}$ in Polarkoordinaten gilt:

$$z_1 z_2 = rse^{i(\varphi+\psi)},\ |z_1| = r.$$

Veranschaulichen Sie sich damit die Multiplikation von komplexen Zahlen geometrisch.

Aufgabe 3. Zeigen Sie, dass es für $n \geq 1$ genau n verschiedene komplexe Lösungen der Gleichung

$$z^n = 1$$

gibt (diese Lösungen heißen *n-te Einheitswurzeln*). Geben Sie diese Einheitswurzeln in Polarkoordinaten an und veranschaulichen Sie sich ihre Lage in der komplexen Zahlenebene.

Aufgabe 4. Zeigen Sie, dass es für $n \geq 1$ immer eine n-te Einheitswurzel gibt, durch deren Potenzen man alle anderen n-ten Einheitswurzeln erhält (eine solche Einheitswurzel heißt *primitive n-te Einheitswurzel*).

Aufgabe 5. Beweisen Sie Satz 1.1.2.

Aufgabe 6. Seien G, H Gruppen und $\varphi\colon G \to H$ ein Gruppenhomomorphismus. Zeigen Sie:
(i) $\varphi(e_G) = e_H$ und $\varphi(g^{-1}) = \varphi(g)^{-1}$ für alle $g \in G$.
(ii) Ist φ bijektiv, so ist $\varphi^{-1}\colon H \to G$ ebenfalls ein Gruppenhomomorphismus.
Bestimmen Sie alle Gruppenhomomorphismen $\varphi\colon (\mathbb{Z}, +) \to (\mathbb{Z}, +)$.

Aufgabe 7. Sei G eine Gruppe und $H < G$ eine Untergruppe. Zeigen Sie die Äquivalenz der folgenden Aussagen:
(i) $gH = Hg$ für alle $g \in G$.
(ii) $\forall h \in H, g \in G : \ g^{-1}hg \in H$.
Eine Untergruppe, welche diese Bedingungen erfüllt, heißt **normale Untergruppe** von G. Zeigen Sie, dass eine Untergruppe $H < G$ mit $|G : H| = 2$ automatisch ein Normalteiler von G ist.

Aufgabe 8. Bestimmen Sie (bis auf Isomorphie) sämtliche Gruppen mit 1,2,3 und 4 Elementen.

Aufgabe 9. Entscheiden Sie für die folgenden Gruppen, welche isomorph sind und welche nicht:

$$\mathbb{Z}/12\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$(\mathbb{R}, +),\ (\mathbb{R} \setminus \{0\}, \cdot),\ (\mathbb{R}_{>0}, \cdot),\ (\mathbb{C} \setminus \{0\}, \cdot).$$

Aufgabe 10. Zeigen Sie:
(i) Die Menge $S^1 := \{z \in \mathbb{C} \mid |z| = 1\}$ ist eine Untergruppe von $(\mathbb{C} \setminus \{0\}, \cdot)$.
(ii) Es gilt $(\mathbb{Z}, +) \lhd (\mathbb{R}, +)$ und $\mathbb{R}/\mathbb{Z} \cong S^1$.

Aufgabe 11. Beweisen Sie den zweiten Isomorphiesatz (Satz 2.2.6).

Aufgabe 12. Seien G_1, G_2 Gruppen. Zeigen Sie:
(i) Die Menge $G_1 \times G_2$ ist mit komponentenweise definierter Verknüpfung eine Gruppe. Für $i = 1, 2$ ist die Abbildung

$$\begin{aligned} \pi_i \colon G_1 \times G_2 &\to G_i \\ (g_1, g_2) &\mapsto g_i \end{aligned}$$

ein surjektiver Gruppenhomomorphismus.
(ii) Sei $H < G_1 \times G_2$ mit $\pi_i(H) = G_i$ für $i = 1, 2$. Dann gilt

$$N_1 := \{g \in G_1 \mid (g, e) \in H\} \lhd G_1$$

$$N_2 := \{g \in G_2 \mid (e, g) \in H\} \lhd G_2.$$

(iii] Die Abbildung

$$\begin{aligned} \pi \colon G_1 \times G_2 &\to G_1/N_1 \times G_2/N_2 \\ (g_1, g_2) &\mapsto (g_1 N_1, g_2 N_2) \end{aligned}$$

ist ein Gruppenhomomorphismus. Die Menge $\pi(H)$ ist der Graph eines Isomorphismus von G_1/N_1 nach G_2/N_2.

Aufgabe 13. Beweisen Sie Lemma 2.3.8.

Aufgabe 14. (i) Eine Gruppe G mit 55 Elementen operiere auf einer Menge X mit 39 Elementen. Zeigen Sie, dass es mindestens ein Element $x \in X$ geben muss mit $g \cdot x = x$ für alle $g \in G$ (ein solches Element heißt **Fixpunkt** der Operation).
(ii) Finden Sie ein Beispiel für eine Gruppenoperation wie in (i), die genau einen Fixpunkt hat.

Aufgabe 15. Sei G eine Gruppe mit n Elementen und $X = \mathrm{Abb}(G, \{1, \ldots, n\})$ die Menge aller Abbildungen von G in die Menge $\{1, \ldots, n\}$.
(i) Zeigen Sie, dass die folgende Vorschrift eine Gruppenoperation von G auf X definiert:

$$\begin{aligned} G \times X &\to X \\ (g, f) &\mapsto (g \cdot f \colon h \mapsto f(hg)). \end{aligned}$$

(ii) Bestimmen Sie alle Fixpunkte dieser Operation.
(iii) Zeigen Sie, dass jede Untergruppe $H < G$ der Stabilisator eines geeigneten $f \in X$ ist.

Aufgabe 16. Zeigen Sie:
(i) Für $n \in \mathbb{Z}$ ist auf $\mathbb{Z}/n\mathbb{Z}$ die folgende Multiplikation wohldefiniert:

$$(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) := (ab) + n\mathbb{Z}.$$

(ii) Ist p eine Primzahl, so ist $\mathbb{Z}/p\mathbb{Z}$ mit $+$ und $\cdot$ ein Körper.
(iii) Seien $a, p \in \mathbb{N}$ mit p prim und $1 \leq a < p$. Dann gilt in $\mathbb{Z}$:

$$p \mid a^{p-1} - 1.$$

Hinweis zu (iii): Betrachten Sie die multiplikative Gruppe $(\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$.

Aufgabe 17. Zeigen Sie, dass für $n \geq 3$ jedes Element von A_n ein Produkt von Zykeln der Länge 3 ist.

Aufgabe 18. Zeigen Sie, dass A_4 keine Untergruppe mit 6 Elementen hat.

Aufgabe 19. Zeigen Sie, dass

$$(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/mn\mathbb{Z}$$

genau dann gilt, wenn m und n teilerfremd sind.

Aufgabe 20. Bestimmen Sie (bis auf Isormorphie) alle Gruppen mit $5, 6, 7$ Elementen.

Aufgabe 21. Zeige Sie, dass jede Untergruppe einer zyklischen Gruppe zyklisch ist.

Aufgabe 22. Zeigen Sie $K(A_4) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ und $K^2(A_4) = \{\mathrm{id}\}$.

Aufgabe 23. Seien G, H Gruppen. Zeigen Sie:
(i) Die Menge

$$\mathrm{Aut}(G) := \{\varphi \colon G \to G \mid \varphi \text{ Gruppenisomorphismus}\}$$

ist bezüglich Hintereinanderausführung von Abbildungen eine Gruppe (genannt die *Automorphismengruppe* von G).

(ii) Sei $\theta \colon H \to \mathrm{Aut}(G)$ ein Gruppenhomomorphismus. Dann macht die folgende Verknüpfung die Menge $G \times H$ zu einer Gruppe:

$$(g, h) \cdot (g', h') := (g \cdot \theta(h)(g'), h \cdot h').$$

Um Verwechslung mit der komponentenweise definierten Verknüpfung zu vermeiden, bezeichnet man diese Gruppe dann mit $G \rtimes_\theta H$.

(iii) Die Abbildung

$$\begin{aligned} \iota \colon G &\to G \rtimes_\theta H \\ g &\mapsto (g, e) \end{aligned}$$

ist ein injektiver Gruppenhomomorphismus und $\mathrm{im}(\iota)$ ist eine normale Untergruppe in $G \rtimes_\theta H$.

Aufgabe 24. Seien G eine endliche Gruppe und p, q zwei verschiedene Primzahlen. Zeigen Sie:

(i) Falls G nur eine einzige p-Sylow-Untergruppe besitzt, so ist diese eine normale Untergruppe in G.

(ii) Ist S eine p-Sylow-Untergruppe und T eine q-Sylow-Untergruppe von G, so gilt $S \cap T = \{e\}$.

(iii) Jede Gruppe mit 30 Elementen besitzt eine nichttriviale normale Untergruppe.

Aufgabe 25. Sei G eine Gruppe und $S < G$ eine Untergruppe. Wir setzen

$$\mathrm{Nor}_G(S) := \left\{ g \in G \mid gSg^{-1} = S \right\}.$$

Zeigen Sie $S \lhd \mathrm{Nor}_G(S) < G$.

Sei nun $H \lhd G$ eine normale Untergruppe und $S < H$ eine p-Sylow-Untergruppe von H. Zeigen Sie:

(i) Für jedes $g \in G$ existiert ein $h \in H$ mit $gSg^{-1} = hSh^{-1}$.

(ii) Es gilt $\mathrm{Nor}_G(S) \cdot H = G$.

Aufgabe 26. Im Matrixring $\mathrm{M}_2(\mathbb{C})$ betrachten wir die folgende Teilmenge:

$$\mathbb{H} := \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \mid a, b \in \mathbb{C} \right\}.$$

Zeigen Sie:

(i) $\mathbb{H}$ ist ein nicht-kommutativer Teilring von $\mathrm{M}_2(\mathbb{C})$.

(ii) $\mathbb{H}^\times = \mathbb{H} \setminus \{0\}$.

(iii) Die folgende Teilmenge von $\mathbb{H}$ bildet eine Untergruppe bezüglich Multiplikation

$$G = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\}.$$

(iv) Bestimmen Sie alle Untergruppen von G und zeigen Sie, dass alle normale Untergruppen in G sind.

Aufgabe 27. (i) Zeigen Sie, dass der einzige Ringhomomorphismus von $\mathbb{Q}$ nach $\mathbb{Q}$ sowie von $\mathbb{R}$ nach $\mathbb{R}$ jeweils die Identität ist.
(ii) Bestimmen Sie alle Ringhomomorphismen $\varphi\colon \mathbb{C} \to \mathbb{C}$ mit $\varphi(\mathbb{R}) \subseteq \mathbb{R}$.

Aufgabe 28. Sei $\varphi\colon R \to S$ ein Ringhomomorphismus. Zeigen Sie:
(i) $\varphi(R)$ ist ein Teilring von S.
(ii) Für jedes Ideal $J \lhd S$ ist $\varphi^{-1}(J)$ ein Ideal in R.
(iii) Ist φ surjektiv, so ist für jedes Ideal $I \lhd R$ auch $\varphi(I)$ ein Ideal in S.
(iv) Stimmt Aussage (iii) auch ohne Surjektivität?

Aufgabe 29. Beweisen Sie Lemma 3.1.10.

Aufgabe 30. Bestimmen Sie alle ganzzahligen Lösungen des folgenden Systems linearer Kongruenzen:

$$\begin{aligned} x &\equiv 1 \bmod 3 \\ x &\equiv 2 \bmod 7 \\ x &\equiv 3 \bmod 4. \end{aligned}$$

Aufgabe 31. Sei R ein kommutativer Ring und $I \lhd R$ ein Ideal. Wir definieren:

$$\sqrt{I} := \{a \in R \mid \ a^m \in I \text{ für ein } m \geq 1\}\,.$$

Zeigen Sie:
(i) $\sqrt{I}$ ist ein Ideal in R mit $I \subseteq \sqrt{I}$.
(ii) Es gilt $\sqrt{\sqrt{I}} = \sqrt{I}$.
Berechnen sie im Ring $R = \mathbb{Z}$

$$\sqrt{2\mathbb{Z}},\ \sqrt{4\mathbb{Z}},\ \sqrt{6\mathbb{Z}}.$$

Für welche $n \in \mathbb{Z}$ gilt $\sqrt{n\mathbb{Z}} = n\mathbb{Z}$?

Aufgabe 32. Sei R ein kommutativer Ring, M eine nichtleere und unter Multiplikation abgeschlossene Teilmenge von R, sowie $I \lhd R$ ein Ideal mit $I \cap M = \emptyset$.
Zeigen Sie:
(i) Es gibt ein Ideal $\mathfrak{p} \lhd R$, welches maximal ist bezüglich der Eigenschaften

$$I \subseteq \mathfrak{p}, \quad \mathfrak{p} \cap M = \emptyset.$$

(ii) Jedes solche Ideal $\mathfrak{p}$ ist ein Primideal in R.

Aufgabe 33. Zeigen Sie, dass die beiden folgenden Ideale jeweils nicht von einem Element als Ideal erzeugt werden:

$$(x_1, x_2) \lhd \mathbb{Q}[x_1, x_2], \quad (2, x) \lhd \mathbb{Z}[x].$$

Aufgabe 34. (i) Zeigen Sie, dass im Ring $\mathbb{Z}[i]$ Division mit Rest existiert, es also für $a, b \in \mathbb{Z}[i]$ immer $c, r \in \mathbb{Z}[i]$ gibt mit

$$b = ca + r$$

und $|r| < |a|$ (der Betrag ist hier der bekannte Betrag von komplexen Zahlen).
(ii) Beweisen Sie, dass $\mathbb{Z}[i]$ ein Hauptidealring ist.

Aufgabe 35. Sei $\varphi\colon R \twoheadrightarrow S$ ein surjektiver Ringhomomorphismus und R noethersch. Zeigen Sie, dass S dann auch noethersch ist. Zeigen Sie dasselbe auch für die Eigenschaft "Hauptidealring".

Aufgabe 36. Sei R ein Integritätsring. Zeigen Sie, dass $R[x]$ genau dann ein Hauptidealring ist, wenn R ein Körper ist.

Aufgabe 37. Bestimmen Sie sämtliche Ideale in $\mathbb{Z}/12\mathbb{Z}$ und entscheiden Sie, welche davon Primideale sind.

Aufgabe 38. Sei $R = \mathcal{C}([0,1], \mathbb{R})$ der Ring der stetigen reellwertigen Funktionen auf $[0,1]$. Zeigen Sie:
(i) Für jedes echte Ideal $I \lneq R$ gibt es ein $a \in [0,1]$ mit $f(a) = 0$ für alle $f \in I$.
(ii) Für jedes $a \in [0,1]$ ist die Menge

$$\mathfrak{m}_a := \{f \in R \mid f(a) = 0\}$$

ein maximales Ideal in R.
(iii) Jedes maximale Ideal in R ist von der Gestalt $\mathfrak{m}_a$ für ein $a \in [0,1]$.
(iv) Für $a \in (0,1)$ ist die Menge

$$I_a := \{f \in R \mid \exists \epsilon > 0\colon\ f \equiv 0 \text{ auf } (a - \epsilon, a + \epsilon)\}$$

ein Ideal in R, aber kein Primideal.
(v) Es gibt ein Primideal $\mathfrak{p}_a$ in R mit

$$I_a \subseteq \mathfrak{p}_a \subsetneq \mathfrak{m}_a.$$

Insbesondere ist $\mathfrak{p}_a$ nicht maximal.
(Hinweis: Verwenden Sie hierfür Aufgabe 32.)

Aufgabe 39. (*i*) Bestimmen Sie den Quotientenkörper des Rings $\mathbb{Z}[i]$ der ganzen Gauss'schen Zahlen.

(*ii*) Zeigen Sie, dass zwei isomorphe Integritätsringe auch isomorphe Quotientenkörper besitzen.

(*iii*) Geben Sie zwei nicht-isomorphe Integritätsringe an, deren Quotientenkörper isomorph sind.

Aufgabe 40. Überprüfen Sie die folgenden Polynome auf Irreduzibilität im Polynomring $\mathbb{Q}[x]$:

$$\begin{aligned} p_1 &= x^2 - 2x + 2 \\ p_2 &= x^{10} + 2x^8 + 4x^6 + 6x^4 + 8x^2 + 10 \\ p_3 &= 3x^2 - 9x - 27 \\ p_4 &= x^4 + x^3 + 2x^2 + x + 1. \end{aligned}$$

Welche der Polynome sind auch irreduzibel in $\mathbb{Z}[x]$?

Aufgabe 41. Zeigen Sie, dass für eine Primzahl $p \in \mathbb{Z}$ und $i = 1, \ldots, p-1$ in $\mathbb{Z}$ stets

$$p \mid \binom{p}{i}$$

gilt. Stimmt die Aussage auch, wenn p keine Primzahl ist?

Aufgabe 42. Sei R ein faktorieller Ring und $\mathfrak{p} \lhd R$ ein Primideal. Durch Anwendung der kanonischen Projektion $R \to R/\mathfrak{p}$ auf die Koeffizienten von Polynomen erhalten wir einen Homomorphismus $\varphi\colon R[x] \to (R/\mathfrak{p})[x]$. Zeigen Sie:

(*i*) Sei $p \in R[x]$ primitiv mit Leitkoeffizient nicht in $\mathfrak{p}$. Falls dann $\varphi(p)$ irreduzibel in $(R/\mathfrak{p})[x]$ ist, so ist p auch irreduzibel in $R[x]$.

(*ii*) $1 + x^3 + x^5$ ist irreduzibel in $\mathbb{Z}[x]$.

Aufgabe 43. Bestimmen Sie alle irreduziblen Polynome in $\mathbb{C}[x]$ und in $\mathbb{R}[x]$. Ist der Grad aller irreduziblen Polynome in $\mathbb{Q}[x]$ beschränkt?

Aufgabe 44. Wir betrachten die Menge $R := \{p \in \mathbb{Q}[x] \mid p'(0) = 0\}$. Zeigen Sie:

(*i*) R ist ein Teilring von $\mathbb{Q}[x]$.

(*ii*) Jedes Element in R ist ein Produkt von endlich vielen irreduziblen Elementen aus R.

(*iii*) R ist nicht faktoriell.

Aufgabe 45. (*i*) Zeigen Sie, dass $\mathbb{Q}[\sqrt{2}] := \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$ ein Teilkörper von $\mathbb{R}$ ist.
(*ii*) Zeigen Sie, dass die Ringe $\mathbb{Q}[\sqrt{2}]$ und $\mathbb{Q}[x]/(x^2 - 2)$ isomorph sind.

Aufgabe 46. Sei R ein kommutativer Ring und $M \subseteq R$ mit $1 \in M$ und $M \cdot M \subseteq M$. Zeigen Sie:
(*i*) Die folgende Setzung definiert eine Äquivalenzrelation auf $R \times M$:

$$(r, m) \sim (s, n) \;:\Leftrightarrow\; \exists p \in M \colon p(rn - sm) = 0$$

(*ii*) Auf der Menge der Äquivalenzklassen von $\sim$ sind die beiden folgenden Verknüpfungen wohldefiniert und machen sie zu einem kommutativen Ring:

$$\begin{aligned}[(r, m)] + [(s, n)] &:= [(rn + sm, mn)] \\ [(r, m)] \cdot [(s, n)] &:= [(rs, mn)].\end{aligned}$$

Diesen Ring bezeichnet man auch mit $M^{-1}R$ und nennt ihn die *Lokalisierung* von R nach M. Für die Äquivalenzklasse $[(r, m)]$ schreibt man auch $\frac{r}{m}$.
(*iii*) Die Abbildung

$$\begin{aligned}\iota \colon R &\to M^{-1}R \\ r &\mapsto \frac{r}{1}\end{aligned}$$

ist ein Ringhomomorphismus. Falls M keine Nullteiler von R enthält ist ι injektiv. Für $m \in M$ ist $\iota(m)$ in $M^{-1}R$ invertierbar.

Aufgabe 47. Sei R ein kommutativer Ring und $\partial \colon R[x] \to R[x]$ die formale Ableitungsabbildung (d.h. $\partial(\sum_{i=0}^{d} c_i x^i) := \sum_{i=1}^{d} i c_i x^{i-1}$). Zeigen Sie für $p, q \in R[x]$ und $r \in R$ die folgenden Aussagen:
(*i*) $\partial(p + q) = \partial(p) + \partial(q),\ \partial(rp) = r\partial(p)$.
(*ii*) $\partial(pq) = p\partial(q) + q\partial(p)$.

Aufgabe 48. Sei k ein Körper und $q \in k[x]$ ein Polynom. Zeigen Sie:
(*i*) Es gibt eine Körpererweiterung $k \subseteq K$, so dass q in $K[x]$ in Linearfaktoren zerfällt.
(*ii*) Falls $\mathrm{ggT}(q, \partial(q)) = 1$ in $k[x]$ gilt, so hat q in K (wie in (*i*)) keine doppelte Nullstelle (d.h. alle Linearfaktoren sind verschieden).
(*iii*) Sei p eine Primzahl, $n = p^r$ für ein $r \in \mathbb{N}$ und $q = x^n - x \in \mathbb{F}_p[x]$. Dann gilt $\mathrm{ggT}(q, \partial(q)) = 1$ in $\mathbb{F}_p[x]$.
(*iv*) Für jede Primzahl p und jedes $r \in \mathbb{N}$ gibt es einen Körper mit genau p^r Elementen.

Aufgabe 49. Bestimmen Sie das Minimalpolynom von $\sqrt{2}+\sqrt{3}$ über $\mathbb{Q}$, den Körpergrad $\left[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}\right]$ sowie eine Basis des $\mathbb{Q}$-Vektorraums

$$\mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

Aufgabe 50. Zeigen Sie

$$\mathrm{Min}(\sqrt{2}+i, \mathbb{R}) = x^2 - 2\sqrt{2}x + 3 \text{ und } \mathrm{Min}(\sqrt{2}+i, \mathbb{Q}) = x^4 - 2x^2 + 9.$$

Aufgabe 51. Seien $m, n \in \mathbb{N}$ teilerfremde Zahlen, für die man sowohl ein gleichseitiges m-Eck als auch ein gleichseitiges n-Eck mit Zirkel und Lineal aus $0, 1$ konstruieren kann. Zeigen Sie, dass man dann auch ein gleichseitiges mn-Eck mit Zirkel und Lineal aus $0, 1$ konstruieren kann.

Aufgabe 52. Sei K ein algebraisch abgeschlossener Körper (d.h. jedes Polynom aus $K[x]$ zerfällt in $K[x]$ in Linearfaktoren). Zeigen Sie, dass K unendlich ist.

Aufgabe 53. Sei $k \subseteq K$ eine Körpererweiterung. Wir definieren

$$\mathrm{Aut}(K,k) := \left\{\varphi\colon K \to K \mid \varphi \text{ bijektiver Ringhomomorphismus}, \varphi_{|_k} = \mathrm{id}_k\right\}.$$

Zeigen Sie:

(*i*) $\mathrm{Aut}(K,k)$ ist eine Gruppe bezüglich Hintereinanderausführung.

(*ii*) Für jede Untergruppe $H < \mathrm{Aut}(K,k)$ ist

$$\mathrm{Fix}(H) := \{a \in K \mid \forall \varphi \in H\colon\ \varphi(a) = a\}$$

ein Körper zwischen k und K.

(*iii*) Für jeden Zwischenkörper $k \subseteq L \subseteq K$ ist $\mathrm{Aut}(K,L)$ eine Untergruppe von $\mathrm{Aut}(K,k)$.

(*iv*) Es gilt $L \subseteq \mathrm{Fix}\left(\mathrm{Aut}(K,L)\right)$ und $H \subseteq \mathrm{Aut}\left(K, \mathrm{Fix}(H)\right)$.

Aufgabe 54. Sei K ein Körper, $P \subseteq K[x_1, \ldots, x_n]$, $I = (P)$ das von P erzeugte Ideal und $V \subseteq K^n$. Wir definieren

$$\mathcal{V}(P) := \{a \in K^n \mid \forall p \in P\colon\ p(a) = 0\}$$
$$\mathcal{I}(V) := \{p \in K[x_1, \ldots, x_n] \mid \forall a \in V\colon\ p(a) = 0\}.$$

Zeigen Sie:

(*i*) $\mathcal{V}(P) = \mathcal{V}(I) = \mathcal{V}(\sqrt{I})$.

(Siehe Aufgabe 31 für die Definition von $\sqrt{I}$.)

(*ii*) Es gibt eine endliche Teilmenge $P' \subseteq P$ mit $\mathcal{V}(P) = \mathcal{V}(P')$.

(*iii*) $\mathcal{I}(V)$ ist ein Ideal in $K[x_1, \ldots, x_n]$ mit $\sqrt{\mathcal{I}(V)} = \mathcal{I}(V)$.

(*iv*) $I \subseteq \mathcal{I}\left(\mathcal{V}(I)\right)$ und $V \subseteq \mathcal{V}\left(\mathcal{I}(V)\right)$.

Aufgabe 55. Sei R ein kommutativer Ring und $I \lhd R$ ein Ideal. Für $a \in R \setminus \sqrt{I}$ betrachten wir die Menge $M = \{1, a, a^2, a^3, \ldots\}$, die Lokalisierung $M^{-1}R$ und den kanonischen Homomorphismus $\iota\colon R \to M^{-1}R$ (vergleiche Aufgabe 46). Zeigen Sie:

(i) Das von $\iota(I)$ in $M^{-1}R$ erzeugte Ideal ist nicht der ganze Ring $M^{-1}R$.
(ii) Es gibt ein maximales Ideal $\mathfrak{m} \lhd M^{-1}R$ mit $\iota(I) \subseteq \mathfrak{m}$.
(iii) Es gibt ein Primideal $\mathfrak{p} \lhd R$ mit $I \subseteq \mathfrak{p}$ und $a \notin \mathfrak{p}$.
(iv) $\sqrt{I}$ ist der Durchschnitt aller über I liegenden Primideale.

Aufgabe 56. Sei $k \subseteq K$ eine Körpererweiterung und K algebraisch abgeschlossen. Zeigen Sie, dass die folgende Menge der algebraische Abschluss von k ist:

$$\{a \in K \mid a \text{ algebraisch über } k\}\,.$$

Aufgabe 57. Sei $p \in k[x]$ und K der Zerfällungskörper von p über k. Zeigen Sie

$$[K : k] \leq \deg(p)!$$

Aufgabe 58. Zeigen Sie, dass es für eine Primzahlpotenz $q = p^r$ bis auf Isomorphie genau einen Körper mit q Elementen gibt.

Aufgabe 59. Zeigen Sie, dass jede Körpererweiterung vom Grad 2 normal ist.

Aufgabe 60. Zeigen Sie, dass jedes irreduzible Polynom aus $\mathbb{F}_d[x]$ (wobei d eine Primzahl ist) separabel ist.
Hinweis: Verwenden Sie Satz 4.5.10 und die Surjektivität des Frobenius-Automorphismus.

Aufgabe 61. Zeigen Sie, dass die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}, i)$ normal ist.

Aufgabe 62. Sei p eine Primzahl, $\xi := e^{2\pi i/p} \in \mathbb{C}$ und $K := \mathbb{Q}(\xi)$. Zeigen Sie, dass für jedes $j = 1, \ldots, p-1$ genau ein $\mathbb{Q}$-Automorphismus φ_j von K existiert mit

$$\varphi_j(\xi) = \xi^j.$$

Aufgabe 63. Berechnen Sie ein primitives Element für die Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

Aufgabe 64. Sei $p \in k[x]$ ein Polynom vom Grad d und K sein Zerfällungskörper über k. Zeigen Sie:

(i) Es gibt einen injektiven Gruppenhomomorphismus $\mathrm{Gal}(K, k) \hookrightarrow S_d$.
(ii) Finden Sie ein Beispiel für ein irreduzibles Polynom $p \in k[x]$, für das der Homomorphismus aus (i) nicht surjektiv ist.
(iii) Berechnen Sie $\mathrm{Gal}(K, k)$ im Fall $p = x^3 - 2$.

Aufgabe 65. Sei n eine Primzahl und $\sigma, \tau \in S_n$ Zykel der Länge 2 und n. Zeigen Sie, dass σ, τ schon die ganze Permutationsgruppe erzeugen.

Aufgabe 66. Bestimmen Sie sämtliche Zwischenkörper der Erweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

Aufgabe 67. Sei $p \in k[x]$ ein irreduzibles Polynom sowie K sein Zerfällungskörper über k. Zeigen Sie, dass es für je zwei Nullstellen $a, b \in K$ von p ein $\varphi \in \mathrm{Gal}(K, k)$ gibt mit $\varphi(a) = b$.

Aufgabe 68. Seien $a_1, a_2, a_3, a_4 \in \mathbb{C}$ derart, dass das Polynom

$$f := (x - a_1)(x - a_2)(x - a_3)(x - a_4)$$

Koeffizienten in $\mathbb{Q}$ hat. Wir setzen

$$\begin{aligned} b_1 &:= (a_1 + a_2)(a_3 + a_4) \\ b_2 &:= (a_1 + a_3)(a_2 + a_4) \\ b_3 &:= (a_1 + a_4)(a_2 + a_3) \end{aligned}$$

und $g := (x - b_1)(x - b_2)(x - b_3)$. Zeigen Sie: Die Koeffizienten von g liegen ebenfalls in $\mathbb{Q}$. (Tipp: Es ist nicht nötig, die Koeffizienten auszurechnen! Verwenden Sie den Hauptsatz der Galoistheorie.)

Aufgabe 69. Sei $k = \mathbb{F}_2(t)$ mit einer Variablen t. Zeigen Sie, dass

$$p := x^2 - t \in k[x]$$

irreduzibel, der Körper $K := k[x]/(p)$ der Zerfällungskörper von p, aber die Erweiterung $k \subseteq K$ keine Galoiserweiterung ist.

Aufgabe 70. Für $i = 1, \ldots, n$ definieren wir Polynome $s_i \in \mathbb{Q}[y_1, ..., y_n]$ durch

$$x^n + s_1 x^{n-1} + \cdots + s_{n-1} x + s_n = (x + y_1) \cdots (x + y_n).$$

Eine rationale Funktion $f \in \mathbb{Q}(y_1, ..., y_n)$ heißt **symmetrisch**, wenn für jede Permutation $\pi \in S_n$

$$f(y_{\pi(1)}, ..., y_{\pi(n)}) = f(y_1, ..., y_n)$$

gilt. Zeigen Sie:
(i) Die Polynome s_i sind symmetrisch.
(ii) Die Erweiterung $\mathbb{Q}(s_1, ..., s_n) \subseteq \mathbb{Q}(y_1, ..., y_n)$ ist Galoissch.
(iii) Die Galois-Gruppe der Erweiterung aus (ii) ist isomorph zu S_n.
Was kann man mithilfe des Hauptsatzes der Galoistheorie über symmetrische rationale Funktionen aussagen?

Aufgabe 71. Zeigen Sie: Für jede endliche Gruppe G gibt es eine Galoiserweiterung $K \subseteq L$ mit $\mathrm{Gal}(L, K) \cong G$. (Tipp: Verwenden Sie Aufgabe 70.)

Aufgabe 72. (i) Finden Sie ein Bespiel für einen freien R-Modul M mit Untermodul $N \subseteq M$, so dass N nicht frei ist.
(ii) Finden Sie ein Beispiel für einen R-Modul M mit Untermodul $N \subseteq M$, sodass kein Untermodul $N' \subseteq M$ existiert mit

$$N \oplus N' = M.$$

(iii) Finden Sie ein Bespiel für einen endlich erzeugten R-Modul M mit Untermodul $N \subseteq M$, so dass N nicht endlich erzeugt ist.

Aufgabe 73. Beweisen Sie Lemma 5.1.9.

Aufgabe 74. Sei M ein R-Modul und $N \subseteq M$ ein Untermodul. Zeigen Sie:
(i) Sind N und M/N endlich erzeugt, so auch M.
(ii) Ist M endlich erzeugt, so auch M/N, aber nicht unbedingt N.

Aufgabe 75. Sei R ein kommutativer Ring. Zeigen Sie dass R genau dann noethersch ist, wenn alle Primideale von R endlich erzeugt sind.

Aufgabe 76. Sei R ein nullteilerfreier Hauptidealring und $M \subseteq R^n$ ein Untermodul. Zeigen Sie, dass M genau dann die Lösungsmenge eines homogenen linearen Gleichungssystems über R ist, wenn ein Untermodul $N \subseteq R^n$ existiert mit $R^n = M \oplus N$.

Aufgabe 77. Seien R ein Integritätsring und M ein R-Modul. Zeigen Sie:
(i) Es ist

$$M^{\mathrm{tor}} := \{m \in M \mid \exists 0 \neq r \in R : rm = 0\}$$

ein Untermodul von M.
(ii) Für $N := M/M^{\mathrm{tor}}$ gilt

$$N^{\mathrm{tor}} = \{0\}.$$

Aufgabe 78. Bestimmen Sie bis auf Isomorphie sämtliche abelschen Gruppen mit $8, 9, 10, 11$ und 12 Elementen.

Aufgabe 79. Bestimmen Sie in Abhängigkeit von $a, b, c \in \mathbb{Z}$ sämtliche ganzzahligen Lösungen des folgenden linearen Gleichungssystems:

$$\begin{aligned} 4x - 11y - 2z &= a \\ -5x + 13y + 4z &= b \\ -10x + 23y + 8z &= c \end{aligned}$$

Aufgabe 80. Sei R ein kommutativer Ring und A, B, M, N jeweils R-Moduln. Zeigen Sie:

(i) Es ist

$$\mathrm{Hom}_R(A,B) := \{f\colon A \to B \mid f \text{ Modulhomomorphismus}\}$$

mit punktweiser Addition und skalarer Multiplikation wieder ein R-Modul.

(ii) Für jeden Modulhomomorphismus $\varphi\colon A \to B$ liefern die folgenden Abbildungen wieder Modulhomomorphismen:

$$\begin{aligned}\varphi^*\colon \mathrm{Hom}_R(B,M) &\to \mathrm{Hom}_R(A,M)\\ f &\mapsto f\circ\varphi.\end{aligned}$$

$$\begin{aligned}\varphi_*\colon \mathrm{Hom}_R(M,A) &\to \mathrm{Hom}_R(M,B)\\ f &\mapsto \varphi\circ f.\end{aligned}$$

(iii) Finden Sie ein Beispiel, in dem φ injektiv, aber φ^* nicht surjektiv ist, sowie eines, in dem φ surjektiv aber φ_* nicht injektiv ist.

Aufgabe 81. Bestimmen Sie im Ring $\mathbb{F}_2[x]$ den größten gemeinsamen Teiler von

$$p = x^7 + x^4 + x + 1 \text{ und } q = x^3 + x$$

sowie eine Darstellung

$$\mathrm{ggT}(p,q) = rp + sq$$

mit $r, s \in \mathbb{F}_2[x]$.

Aufgabe 82. Bestimmen Sie über dem Ring $\mathbb{Q}[t]$ die Smith-Normalform der folgenden Matrix:

$$\begin{pmatrix} t & 0 & 0\\ 0 & t-1 & 0\\ 0 & 0 & t^2 \end{pmatrix}$$

Aufgabe 83. Zeigen Sie, dass $\mathbb{Z}[\sqrt{-2}]$ ein euklidischer Ring ist.

Aufgabe 84. Sei $\varphi\colon R \to S$ ein Ringhomomorphismus und M ein R-Modul. Zeigen Sie, dass die in der Vorlesung definierte Skalarmultiplikation von S auf

$$M \otimes_R S$$

wohldefiniert ist und $M \otimes_R S$ dadurch ein S-Modul wird.

Aufgabe 85. Zeigen Sie, dass die R-bilineare Abbildung

$$\begin{aligned} R^m \times R^n &\to \mathrm{Mat}_{m,n}(R) \\ (v, w) &\mapsto vw^t \end{aligned}$$

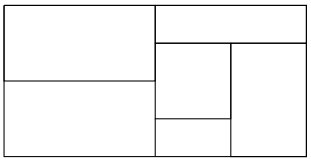
die universelle Eigenschaft des Tensorproduktes erfüllt. Also gilt

$$R^m \otimes_R R^n \cong \mathrm{Mat}_{m,n}(R).$$

Aufgabe 86. Zeigen Sie

$$(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/\mathrm{ggT}(m,n)\mathbb{Z}.$$

Aufgabe 87. Sei $R \subseteq \mathbb{R}^2$ ein Rechteck, aufgeteilt in endlich viele Rechtecke $R_1, \ldots, R_n$, die sich nur an den Rändern berühren. Seien a_i, b_i jeweils die Seitenlängen von R_i und a, b die Seitenlängen von R. Zeigen Sie:
(i) In $\mathbb{R} \otimes_{\mathbb{Q}} \mathbb{R}$ gilt $a \otimes b = \sum_{i=1}^n a_i \otimes b_i$.
(ii) Wenn jedes R_i mindestens eine rationale Seitenlänge hat, so hat auch R mindestens eine rationale Seitenlänge.



Aufgabe 88. Sei R ein nullteilerfreier faktorieller Ring und $K = \mathrm{Quot}(R)$ sein Quotientenkörper. Zeigen Sie, dass die einzigen über R ganzen Elemente von K die Elemente aus R selbst sind.

Aufgabe 89. Sei K ein algebraisch abgeschlossener Körper und $I \subseteq K[x_1, \ldots, x_n]$ ein Ideal. Wir betrachten dessen Nullstellenmenge

$$\mathcal{V}(I) = \{a \in K^n \mid \forall p \in I \colon p(a) = 0\}$$

und deren sogenannten Verschwindungsideal

$$\mathcal{I}(\mathcal{V}(I)) = \{p \in K[x_1, \ldots, x_n] \mid \forall a \in \mathcal{V}(I) \colon p(a) = 0\}$$

(vergleiche Aufgabe 54). Zeigen Sie

$$\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}.$$

Hinweis: Wenden Sie für $p \in \mathcal{I}(\mathcal{V}(I))$ Hilberts Nullstellensatz auf das von I und $tp - 1$ in $K[x_1, \ldots, x_n, t]$ erzeugte Ideal an.

Aufgabe 90. Sei K ein Körper. Zeigen Sie:
(i) $K[x,y]/(x^2-y)$ ist isomorph zum Polynomring $K[t]$ in einer Variablen.
(ii) $K[x,y]/(xy-1)$ ist nicht isomorph zu $K[t]$.

Aufgabe 91. Sei R ein noetherscher Ring und $I \lhd R$ ein Ideal. Zeigen Sie, dass es in R nur endlich viele minimale Primideale über I gibt.

Aufgabe 92. Sei R ein Ring, $I \lhd R$ ein Ideal und $\pi\colon R \to R/I$ die kanonische Projektion. Zeigen Sie, dass die Zuordnung

$$J \mapsto \pi(J)$$

eine Bijektion liefert, zwischen der Menge aller Ideale von R, welche I enthalten, und der Menge aller Ideale von R/I. Zeigen Sie weiter, dass sich dabei gerade Primideale entsprechen.

Aufgabe 93. Für einen Ring R bezeichnen wir mit $\operatorname{Spec}(R)$ die Menge seiner Primideale. Für ein Ideal $I \lhd R$ definieren wir

$$\mathcal{V}(I) := \{\mathfrak{p} \in \operatorname{Spec}(R) \mid I \subseteq \mathfrak{p}\}\,.$$

Zeigen Sie, dass die Mengen $\mathcal{V}(I)$ die Axiome für abgeschlossene Mengen einer Topologie erfüllen.

Aufgabe 94. Seien R, S Ringe. Bestimmen Sie $\operatorname{Spec}(R \times S)$ in Abhängigkeit von $\operatorname{Spec}(R)$ und $\operatorname{Spec}(S)$.

Aufgabe 95. Sei R ein Ring und $a, b \in R$ mit $a \in C_R(b) \cap R^\times$. Zeigen Sie, dass dann auch $a^{-1} \in C_R(b)$ gilt. Insbesondere gilt dann

$$Z(R) \cap R^\times = Z(R)^\times.$$

Aufgabe 96. Für $d \mid m \in \mathbb{N}$ definieren wir

$$\Phi_{m/d} := \prod_{\substack{1 \le k \le m \\ \operatorname{ggT}(k,m) = d}} \left(t - e^{\frac{2\pi i k}{m}}\right).$$

Zeigen Sie:
(i) Die Definition $\Phi_{m/d}$ hängt wirklich nur vom Quotienten m/d ab.
(ii) Ist m/d eine Primzahl, so stimmt die Definition von $\Phi_{m/d}$ mit der aus Beispiel 3.5.23 (ii) überein.
(iii) Die Koeffizienten von $\Phi_{m/d}$ sind ganze Zahlen.

Aufgabe 97. (*i*) Zeigen Sie, dass für $\mathrm{char}(K) \neq 2$ der Quaternionenring $Q_K(a,b)$ einfach ist.
(*ii*) Für welche $a, b \in \mathbb{C} \setminus \{0\}$ ist $Q_{\mathbb{C}}(a,b)$ ein Schiefkörper?

Aufgabe 98. Vervollständigen Sie den Beweis des Satzes von Burnside (Satz 6.3.4): Falls $A \subseteq \mathrm{Mat}_m(K)$ eine Unteralgebra ist, die transitiv auf K^m operiert und eine Matrix von Rang 1 enthält, gilt $A = \mathrm{Mat}_m(K)$.

Aufgabe 99. Sei $A \subseteq \mathrm{Mat}_m(\mathbb{C})$ eine $\mathbb{C}$-Unteralgebra, die unter $*$ abgeschlossen ist. Sei $V \subseteq \mathbb{C}^m$ ein A-invarianter Unterraum. Zeigen Sie, dass dann auch $V^\perp$ ein A-invarianter Unterraum ist.

Aufgabe 100. Zeigen Sie, dass $\mathrm{Mat}_m(K)$ und für $\mathrm{char}(K) \neq 2$ auch $Q_K(a,b)$ eine zentrale K-Algebra ist.

Aufgabe 101. Zeigen Sie, dass die Hamming-Distanz eine Metrik auf $\mathcal{A}^k$ definiert.

Aufgabe 102. Beweisen Sie Proposition 7.2.3.

Aufgabe 103. Beweisen Sie die universelle Eigenschaft der Garbifizierung im Beweis von Satz 7.4.13.