Algebra

Vorlesungsskript im Wintersemester 2018/2019

Universität zu Köln

Dr. Stephan Ehlen

WWW.STEPHANEHLEN.DE

Die Hauptquellen für dieses Vorlesungsskript sind die Bücher mit dem Titel „Algebra“ von S. Bosch [2] und J.C. Jantzen und J. Schwermer [3] sowie ein Vorlesungsskript von J. H. Bruinier aus dem Wintersemester 2014/2015 an der TU Darmstadt, welches er mir freundlicherweise zur Verfügung gestellt hat. Weitere ggf. hin und wieder genutzen Bücher sind die gleichnamigen Bücher von M. Artin [1], S. Lang [5] und E. Kunz [4]. Eine weitere Quelle ist auch das Skript „Algebra und Zahlentheorie“ von W. Soergel (Uni Freiburg). Das Skript dient ausschließlich zur Ergänzung der Vorlesung und erhebt keinen Anspruch auf Vollständigkeit. Weiterhin sind alle Resultate natürlich wohlbekannt und ich erhebe absolut keinen Anspruch auf Originalität. *Bei Fragen, Kommentaren und insbesondere, falls Sie die sicherlich vorhandenen (Tipp-)fehler finden, schreiben Sie mir bitte eine Email: algebra@stephanehlen.de.*

STAND: 27. JANUAR 2019; Das Skript wird während des Semesters laufend aktualisiert.

Inhaltsverzeichnis

Notation

Liste einiger häufig benutzter Symbole.

$\mathbb{N}$	$= \{1,2,3,4,\ldots\}$, die natürlichen Zahlen
$\mathbb{N}_0$	$= \{0,1,2,3,4,\ldots\} = \mathbb{N} \cup \{0\}$
$\mathbb{Z}$	$= \{0,1,-1,2,-2,3,-3,\ldots\}$, die ganzen Zahlen
$\mathbb{Q}$	der Körper der rationalen Zahlen
$\mathbb{R}$	der Körper der reellen Zahlen
$\mathbb{C}$	der Körper der komplexen Zahlen
$\subset$	Sind A und B Mengen, so bedeutet $A \subset B$, dass A in B enhalten ist und Gleichheit ist nicht ausgeschlossen (d.h. $(A \subset B) \Leftrightarrow (a \in A \Rightarrow a \in B)$)
$\subsetneq$	$A \subset B$ und $A \neq B$
S_n	die symmetrische Gruppe (Permutationen von n Elementen)
$\mathrm{Abb}(A,B)$	die Menge der Abbildungen von A nach B
$\mathrm{Aut}(G)$	die Gruppe der Automorphismen von G
$\lvert A \rvert$	Die Anzahl der Elemente der Menge A (wir lassen gelegentlich $\lvert A \rvert = \infty$ zu)
$m \mid n$	m teilt n (zum Beispiel in $\mathbb{Z}$: es ex. ein $x \in \mathbb{Z}$, so dass $mx = n$ gilt)
$m \nmid n$	m teilt *nicht* n

1. Einführung

In diesem Kapitel möchte ich Ihnen die Beschäftigung mit den doch relativ abstrakten Methoden der Algebra etwas schmackhaft machen.

1.1 Algebraische Gleichungen

Das Wort Algebra stammt aus dem Arabischen („al-jabr“) und bedeutet soviel wie das Rechnen mit Gleichungen (wörtlicher: das Zusammenfügen gebrochener Teile). Der Begriff wurde im 9. Jhd. geprägt, basierend auf einem Rechenlehrbuch des persischen Mathematikers al-Chwarizmi.

In der Algebra beschäftigen wir uns mit dem Lösen von *algebraischen*, d.h. polynomiellen Gleichungen.

Beispiel 1.1

$$1 \cdot x^2 + 2 \cdot x - 1 = 0$$

Hierbei ist x, die **Unbekannte** oder **Variable** von den bekannten Größen, auch *Koeffizienten* genannt, zu unterscheiden.

In der *Linearen Algebra* wurden (Systeme von) lineare(n) Gleichungen behandelt. Im Falle einer Variablen hieße dies, dass nur x und keine höheren Potenzen (wie $x^2, \dots$) in der Gleichung auftauchen.

Es stellt sich die Frage, ob es allgemeine Lösungsformeln für solche algebraischen Gleichungen gibt. Wir tasten uns langsam vor:

Beispiel 1.2 — Lineare Gleichungen. Seien a, b vorgegeben (zum Beispiel reelle Zahlen), mit $a \neq 0$. Betrachten wir die Gleichung

$$ax + b = 0.$$

Wir stellen fest, dass diese genau eine Lösung besitzt, nämlich

$$x = -\frac{b}{a}.$$

Beispiel 1.3 — Quadratische Gleichungen. Es seien a, b, c vorgegeben. Wir betrachten die quadrati-

sche Gleichung

$$ax^2+bx+c=0 \tag{1.1}$$

OBdA können wir $a\neq 0$ annehmen (falls $a=0$, so sind wir in Beispiel 1.2). Wir erhalten die Lösungen von (1.1) durch die Formel

$$x=\frac{-b\pm\sqrt{D}}{2a},$$

wobei $D=b^2-4ac$ ist. Wir sehen, dass es folgende Fälle gibt (falls $a,b,c\in\mathbb{R}$ sind):

(i) Falls $D=0$ ist, so gibt es genau eine reelle Lösung.
(ii) Falls $D>$ ist, so gibt es zwei verschiedene reelle Lösungen.
(iii) Und falls $D<0$ ist, so gibt es keine reellen, aber zwei verschiedene komplexe Lösungen.

Beispiel 1.4 — Kubische Gleichungen. Wir betrachten nun eine Gleichung vom Grad 3 und beschränken uns dabei der Einfachheit halber auf eine solche Gleichung der Form

$$x^3+ax+b=0. \tag{1.2}$$

Die allgemeineren Gleichungen dritten Grades können mittels einfacher Substitutionen auf diese Gleichung zurückgeführt werden. Von Cardano wurde 1545 überliefert, dass dieser Fall bereits 1515 von del Ferro (im Wesentlichen) gelöst wurde. Man findet in diesem Fall alle Lösungen durch die Formel

$$\underbrace{\sqrt[3]{-\frac{b}{2}+\sqrt{D}}}_{=u}+\underbrace{\sqrt[3]{-\frac{b}{2}-\sqrt{D}}}_{=v},$$

wobei

$$D=\left(\frac{a}{3}\right)^3+\left(\frac{b}{2}\right)^2.$$

Die beiden dritten Wurzeln müssen so in $\mathbb{C}$ gewählt werden, dass $uv=-\frac{a}{3}$ gilt.

Es ist leicht nachzurechnen, dass diese Formel dann in der Tat eine Lösung liefert:

$$\begin{aligned}(u+v)^3+a(u+v)+b &= u^3+3u^2v+3uv^2+v^3+a(u+v)+b\\ &= -\frac{b}{2}+\sqrt{D}-a(u+v)-\frac{b}{2}-\sqrt{D}+a(u+v)+b=0.\end{aligned}$$

Im allgemeinen Fall ergeben sich so durch die Möglichkeiten bei der Wahl der 3. Wurzel, 3 Lösungen (ggf. mit Vielfachheiten gezählt) und es handelt sich in der Tat um eine allgemeine Lösungsformel für (1.2).

Beispiel 1.5 — Quartische Gleichungen. Es gibt explizite Lösungsformeln auch für polynomielle Gleichungen 4. Grades, welche ebenfalls von Cardano 1545 veröffentlicht aber von Ferrari gefunden wurden. Wir belassen es an dieser Stelle dabei, auf die Literatur zu verweisen (einige Fälle finden sich beispielsweise in [2, Abschnitt 6.2]).

Bemerkung 1.1 — Gleichungen vom Grad 5 und höher. Nach Cardano hat man sich längere Zeit an Lösungsformeln für quintische Gleichungen versucht (noch 1728 hat Euler dies scheinbar versucht). Der Suche wurde spätestens 1824 mit dem Satz von Abel-Ruffini ein jähes Ende gesetzt (Ruffini hat seinen Beweis bereits 1799 veröffentlicht, er enthielt jedoch Lücken, die 1824 von Abel geschlossen wurden). Dieser besagt nämlich, dass die allgemeine Gleichung n-ten Grades für $n\geq 5$ **nicht** *durch Radikale auflösbar* ist. Das bedeutet, dass es keine allgemeine Lösungsformel gibt, die nur Wurzelausdrücke (sowie rationale Ausdrücke in den Koeffizienten) benutzt, so wie es diese für die Gleichungen vom Grad ≤ 4 gibt. In Spezialfällen kann es jedoch natürlich schon der Fall sein, dass so ein Ausruck für die speziellen Lösungen **einer** Gleichung existiert. Den Beweis dieses Satzes werden wir gegen Ende des Semesters erbringen.

1.2 Galoistheorie

Der Satz von Abel-Ruffini ist jedoch nicht das Ende der Geschichte. Der Held der Algebra-Vorlesung ist der französische Mathematiker Évariste Galois (1811 – 1832), der leider nur 20 Jahre alt wurde (er starb in einem Duell). Galois hat in den letzten 2 Jahren vor seinem Tod (ja, mit 18-20 Jahren), die Grundlagen für einen Großteil dieser Vorlesung geliefert. Es gelang Galois, eine differenziertere Antwort auf die Frage der Auflösbarkeit zu geben. Er stellte eine Beziehung zwischen polynomialen Gleichungen in $\mathbb{C}$ und der Gruppentheorie her. Genauer gilt für eine Polynomfunktion $f : \mathbb{C} \to \mathbb{C}$, dass $f(x) = 0$ genau dann (durch Radikale) auflösbar ist, wenn die so genannte Galois-Gruppe von f auflösbar ist.

Wir geben ein (zugegebenermaßen zu diesem Zeitpunkt vermutlich etwas kryptisches, aber hoffentlich doch motivierendes) Beispiel.

Beispiel 1.6 Sei $\zeta_5 = e^{\frac{2\pi i}{5}}$ eine 5-te Einheitswurzel in der komplexen Ebene. Das heißt, ζ_5 ist eine Nullstelle des Polynoms

$$p(X) = X^5 - 1$$

vom Grade 5. Wir können p jedoch recht einfach faktorisieren:

$$p(X) = (X-1)q(X)$$

mit $q(X) = X^4 + X^3 + X^2 + X + 1$. Und da $\alpha_1 := \zeta_5 \neq 1$, ist ζ_5 bereits Nullstelle von q. Die weiteren 3 Nullstellen von q sind $\alpha_2 := \zeta_5^2, \alpha_3 := \zeta_5^3$ und $\alpha_4 := \zeta_5^4$.

Man kann dem Polynom q (oder der Körpererweiterung $\mathbb{Q}(\zeta_5)$ nun wie folgt eine Gruppe zuordnen: Wir stellen zunächst fest, dass es folgende Relationen zwischen den Nullstellen von q gibt:

(i) $\alpha_1^2 = \alpha_2$
(ii) $\alpha_1^3 = \alpha_3$
(iii) $\alpha_1^4 = \alpha_4$
(iv) $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = -1$

Die Gruppe G sei gegeben durch alle Permutationen der Nullstellen $\alpha_1, \alpha_2, \alpha_3$ und α_4, so dass diese Relationen erhalten bleiben. Wir stellen also fest, dass eine solche Permutation σ wegen der Relationen (i)-(iii) bereits durch das Bild $\sigma(\alpha_1)$ bestimmt ist. Es gibt also 4 solche Permutationen und die Gruppe G kann man mit der additiven Gruppe $(\mathbb{Z}/4\mathbb{Z}, +)$ identifizieren:

$$G = \{\sigma_0 = \mathrm{id}, \sigma_1 : \zeta_5 \mapsto \zeta_5^2, \sigma_3 : \zeta_5 \mapsto \zeta_5^3, \sigma_2 : \zeta_5 \mapsto \zeta_5^4\} \cong \mathbb{Z}/4\mathbb{Z},$$

wobei der Gruppenisomorphismus durch $\sigma_j \mapsto j$ gegeben ist (wir wiederholen diese Begriffe in Kürze).

Zu den modernen Gebieten, in denen die Galois-Theorie angewandt wird, zählen unter Anderem:

(i) (algebraische) Zahlentheorie (SS 2019)
(ii) Arithmetische Geometrie
(iii) Langlands-Programm

1.3 Konstruktion mit Zirkel und Lineal

Gegeben sei eine Menge an Punkten $E \subset \mathbb{C} \cong \mathbb{R}^2$ in der Ebene (die wir mit $\mathbb{C}$ identifizieren) und gesucht ist die Menge der Punkte $\hat{E}$, die sich aus E mittels elementarer euklidischer Operationen konstruieren lassen. Diese elementaren Operationen sind:

(i) Konstruiere eine Gerade durch zwei verschiedene Punkte (Lineal)
(ii) Konstruiere einen Kreis, dessen Mittelpunkt in E liegt und der durch einen weiteren Punkt in E verläuft (Zirkel).

Alle so konstruierbaren geometrischen Figuren nennen wir elementare euklidische Figuren. Wir können neue Punkte als Schnittpunkte elementarer euklidischer Figuren "konstruieren".

Beispiel 1.7 Sei $E = \{0, 1\}$ gegeben. Wir wollen $\frac{1}{2}$ konstruieren (oder allgemeiner den Mittelpunkt auf der Strecke zwischen zwei Punkten). Die Lösung wird in Abbildung 1.1 illustriert.

Definiere nun induktiv:

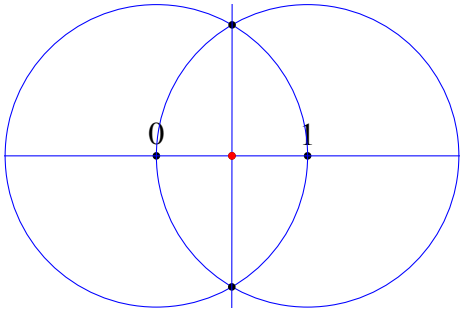


Abbildung 1.1: Konstruktion von $\frac{1}{2}$ mit Zirkel und Lineal

- E_1: Menge der Schnittpunkte elementarer euklidischer Figuren (die man aus $E = E_0$ erhält).
- E_2: Menge der Schnittpunkte elementarer euklidischer Figuren (die man aus E_1 erhält).
- Setze $\hat{E} := \bigcup_{j=0}^{\infty} E_j$ = Menge der aus E konstruierbaren Punkte.
- Ein Punkt $p \in \mathbb{C}$ heißt *aus E (elementar) konstruierbar*, wenn er ein Schnittpunkt elementarer euklidischer Figuren ist (den man *induktiv* nach **endlich** vielen Konstruktionsschritten erhält). Also: p konstruierbar heißt genau $p \in \hat{E}$.

Aus der Antike sind folgende klassischen Konstruktionsprobleme überliefert.

(i) **Winkeldreiteilung**: Gegeben einen Winkel α, unterteile ihn in 3 gleich große Winkel. Dies entspricht (mit etwas Überlegung) der Frage, ob für $E = \{0, 1, \cos(\alpha)\}$ gilt, dass $\cos(\alpha/3) \in \hat{E}$.

(ii) **Das Delische Problem der Würfelverdopplung**: Konstruiere zu einem gegebenen Würfel einen Würfel mit doppeltem Volumen. Dies ist äquivalent zu folgendem Konstruktionsproblem: gegeben $E = \{0, 1\}$, ist dann $\sqrt[3]{2} \in \hat{E}$?

(iii) **Quadratur des Kreises**: Gegeben einen Kreis, konstruiere ein Quadrat mit dem gleichen Flächeninhalt. Dies ist äquivalent zur Konstruktion von $\sqrt{\pi}$ aus $E = \{0, 1\}$.

(iv) **Konstruktion eines regelmäßigen n-Ecks**. Dies ist äquivalent zu der Frage, ob für $E = \{0, 1\}$ der Punkt $e^{\frac{2\pi i}{n}}$ konstruierbar, d.h. in $\hat{E}$ enthalten ist.

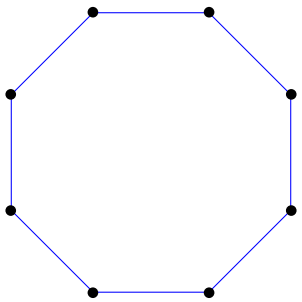


Abbildung 1.2: Das regelmässige 8-Eck.

Bemerkung 1.2 Man hat sich sehr(!) lange Zeit vergeblich an diesen Problemen versucht (manche Hobby-Mathematiker machen das noch heute). Mit algebraischen Methoden kann man jedoch zeigen, dass: (ii) und (iii) *unlösbar* sind (mit Zirkel und Lineal wie oben beschrieben)! Wir werden dies schon bald beweisen können, und dazu die Theorie der Körpererweiterungen benutzen. Bei (i) und (iv) kommt es auf α bzw. n an und wir werden später algebraische Kriterien für die Lösbarkeit angeben. Für das regelmäßige n-Eck waren in der Antike beispielsweise Konstruktionen für $n \in \{2, 3, 4, 5, 6, 8\}$ bekannt. C. F. Gauß konnte 1796 zeigen, dass das regelmässige 17-Eck konstruierbar ist.

2. Gruppen

In diesem Kapitel erinnern wir an die Definition einer Gruppe und leiten einfache Eigenschaften her. Wir behandeln Gruppenhomomorphismen und Nebenklassen, Normalteiler und Faktorgruppen.

2.1 Monoide und Gruppen

Definition 2.1 — Halbgruppe, Monoid, Gruppe.

(i) Eine *Halbgruppe* ist ein Paar $(G,\circ)$ gegeben durch eine nicht-leere Menge G mit einer (inneren) Verknüpfung $\circ : G\times G\to G$, die assoziativ ist.
(ii) Ein Element $e\in G$ in einer Halbgruppe wird *neutrales Element* (oder *Einselement*) genannt, falls für alle $g\in G$ gilt: $e\circ g = g\circ e = g$.
(iii) Eine Halbgruppe $(G,\circ)$ mit neutralem Element e wird *Monoid* genannt.
(iv) Ein Element $h\in G$ in einem Monoiden heißt zu $g\in G$ *invers*, falls $h\circ g = g\circ h = e$ gilt.
(v) Eine *Gruppe* ist ein Monoid $(G,\circ)$, in dem jedes Element ein Inverses besitzt.
(vi) Gruppen, Halbgruppen und Monoiden heißen *abelsch* oder *kommutativ*, falls $g\circ h = h\circ g$ für alle $g,h\in G$ gilt.

Bemerkung 2.1 In Monoiden und Gruppen gilt:
(i) Das neutrale Element in einem Monoid ist eindeutig bestimmt.
(ii) Ist h ein zu g inverses Element, so ist dies eindeutig bestimmt.

Beweis. (i) Seien $(G,\circ)$ ein Monoid und $e,e'\in G$ neutrale Elemente. Dann folgt: $e = e'\circ e = e'$ weil e' und e neutrale Elemente sind.
(ii) Seien $(G,\circ)$ ein Monoid mit neutralem Element $e\in G$, $g\in G$ ein Element und und $h,h'\in G$ zu g invers, d.h. $g\circ h = h\circ g = e$ sowie $g\circ h' = h'\circ g = e$. Damit ist $h = h\circ e = h\circ(g\circ h') = (h\circ g)\circ h' = e\circ h' = h'$. ■

Bemerkung 2.2 In einer Gruppe $(G,\circ)$ gilt die Kürzungsregel: sind $g_1,g_2,g_3\in G$, so gilt, dass aus $g_1\circ g_2 = g_1\circ g_3$ folgt: $g_2 = g_3$. Genauso: Aus $g_2\circ g_1 = g_3\circ g_1$ folgt: $g_2 = g_3$.

Beweis. Wir beweisen nur exemplarisch die zweite Folgerung, die erste geht exakt analog. Es gelte also $g_2\circ g_1 = g_3\circ g_1$. Dann folgt $g_2 = g_2\circ e = g_2\circ(g_1\circ g_1^{-1}) = (g_2\circ g_1)\circ g_1^{-1} = (g_3\circ g_1)\circ g_1^{-1} = g_3\circ(g_1\circ g_1^{-1}) = g_3\circ e = g_3$. ■

Notation 2.1 Es sei $(G,\circ)$ ein Monoid.

(i) Häufig wird die Verknüpfung weggelassen und wir schreiben einfach gh für $g \circ h$ (*multiplikative Schreibweise*).
(ii) Unter Benutzung der multiplikativen Schreibweise ist es oft auch praktisch, das neutrale Element mit 1 zu bezeichnen.
(iii) Potenzen mit natürlichen Zahlen als Exponenten sind induktiv erklärt durch $g^n := g \circ g^{n-1}$ und $g^1 := g$ sowie $g^0 := e$. Für negative Exponenten $n < 0$ ist die Potenz dann durch $g^n := (g^{-1})^{-n}$ erklärt.
(iv) Oft wird **bei abelschen Gruppen** die Verknüpfung auch in *additiver Schreibweise* geschrieben. Das heißt: ist $+$ die Verknüpfung auf unserer Gruppe G, so schreiben wir $a+b$ und anstatt zu potenzieren, „multiplizieren“ wir mit ganzen Zahlen: für $n \in \mathbb{N}$ und $g \in G$ ist dann also

$$n \cdot g := ng := \underbrace{g + \ldots + g}_{n \text{ mal}};$$

das inverse Element wird mit $-g$ bezeichnet und das neutrale Element mit 0.

Beispiel 2.1 (i) $(\mathbb{N}, +)$ ist eine abelsche Halbgruppe (aber kein Monoid)
(ii) $(\mathbb{N}_0, +)$ ist ein abelscher Monoid.
(iii) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind, zusammen mit der gewöhnlichen Addition, abelsche Gruppen.
(iv) $\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}$ sind, zusammen mit der gewöhnlichen Multiplikation, abelsche Gruppen (wir schreiben auch $\mathbb{Q}^\times, \mathbb{R}^\times$ und $\mathbb{C}^\times$)
(v) Genauso sind $\mathbb{Q}^+ := \{x \in \mathbb{Q} \mid x > 0\}$ und analog $\mathbb{R}^+$ abelsche Gruppen mit der Multiplikation.

Beispiel 2.2 Sei M eine Menge und $S(M)$ die Menge der bijektiven Abbildungen $M \to M$. Dann ist $S(M)$ mit der Komposition von Abbildungen $\circ$ eine Gruppe; für $M = \{1, 2, \ldots, n\}$ wird $S_n := S(M)$ die *symmetrische Gruppe* (von n Elementen) genannt. (Die Menge $\mathrm{Abb}(M, M)$ der Abbildungen von M in sich selbst ist übrigens ein Monoid, der $S(M)$ als Untermonoid (siehe Definition 2.2) enthält.)

Beispiel 2.3 Ist G eine Gruppe und M irgendeine Menge, so ist die Menge der Abbildungen $G^M := \mathrm{Abb}(M, G)$ von M nach G eine Gruppe mit der punktweisen Multiplikation: für $f, g \in G^M$ definiert man $(f \cdot g)(x) := f(x)g(x)$.

Beispiel 2.4 Sei K ein Körper und V ein K-Vektorraum. Dann bildet die Menge $\mathrm{GL}(V)$ der bijektiven linearen Abbildungen auf V eine Gruppe mit der Komposition von Abbildungen als Verknüpfung.

Beispiel 2.5 Man definiert das (direkte) Produkt einer Familie von Gruppen $(G_j)_{j \in J}$, indem man die Verknüpfung komponentenweise erklärt: sind $(g_j)_{j \in J}, (h_j)_{j \in J} \in G := \prod_{j \in J} G_j$, so definiert man

$$(g_j)_{j \in J} (h_j)_{j \in J} := (g_j h_j)_{j \in J}.$$

Also, zum Beispiel ist $\mathbb{Z} \times \mathbb{Z} = \{(m, n) \mid m, n \in \mathbb{Z}\}$ eine Gruppe mit komponentenweiser Addition: $(m_1, m_2) + (n_1, n_2) = (m_1 + n_1, m_2 + n_2)$.

Definition 2.2 Sei G ein Monoid mit neutralem Element e. Eine Teilmenge H heißt *Untermonoid*, falls H unter der Verknüpfung auf G abgeschlossen ist und damit selbst ein Monoid ist, d.h.:
(i) Für alle $g, h \in H$ ist auch $gh \in H$,
(ii) und es ist $e \in H$.
Ist G eine Gruppe, so heißt eine Teilmenge $H \subset G$ *Untergruppe*, falls zusätzlich gilt
(iii) für alle $g \in H$ ist auch $g^{-1} \in H$.

Bemerkung 2.3 Die Definition ist so gewählt, dass ein Untermonoid mit der Einschränkung der Verknüpfung auf G selbst wieder ein Monoid ist (und analog für Untergruppen). Insbesondere ist wegen (ii) stets $H \neq \emptyset$.

Beispiel 2.6 Sei K ein Körper. Die Menge $K^{n\times n}$ ist eine abelsche Gruppe mit der Matrizenaddition. Mit der Matrizenmultiplikation bildet $K^{n\times n}$ einen Monoiden. Der Untermonoid $\mathrm{GL}_n(K)$ der invertierbaren $n\times n$-Matrizen ist eine Gruppe (mit der Multiplikation) – diese ist für $n>1$ nicht abelsch.

Beispiel 2.7 (i) $\{e\}$ und G sind trivialerweise Untergruppen einer Gruppe G
(ii) Ist $g\in G$, so ist $\langle g\rangle := \{g^n \mid n\in\mathbb{Z}\}\subset G$, die *von g erzeugte zyklische Untergruppe* eine Untergruppe von G.
(iii) Der Schnitt von beliebigen Familien von Untergruppen ist wieder eine Untergruppe.

Definition 2.3 Sei G ein Monoid und $g\in G$. Falls es ein $n\in\mathbb{N}$ gibt, so dass $g^n=e$ gilt, so nennen wir das kleinste solche n, die *Ordnung* von g. Falls es so eine Potenz nicht gibt, sagen wir g hat unendliche Ordnung. Wir schreiben auch $\mathrm{ord}(g)$ für die Ordnung von g und $\mathrm{ord}(g)=\infty$, falls g unendliche Ordnung hat. Es gilt offensichtlich $|\langle g\rangle| = \mathrm{ord}(g)$.

Außerdem nennt man auch $|G|$, also die Anzahl der Elemente von G, die *Ordnung der Gruppe G*.

Beispiel 2.8 (i) In der additiven Gruppe $\mathbb{Z}$ hat jedes Element $n\neq 0$ unendliche Ordnung. Es gilt $\mathbb{Z}=\langle 1\rangle$.
(ii) Die Matrix

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$$

hat Ordnung 4 in der Gruppe $\mathrm{GL}_2(\mathbb{R})$, denn $S^2=-E_2$ (das Negative der Einheitsmatrix E_2), $S^3=-S$ und $S^4=E_2$.

2.1.1 Homomorphismen

Homomorphismen von Monoiden bzw. Gruppen sind diejenigen Abbildungen zwischen Monoiden/Gruppen, welche die entsprechende Struktur (eines Monoiden bzw. einer Gruppe) erhalten.

Definition 2.4 Seien $(G,\circ),(G',\star)$ Monoide mit neutralen Elementen e und e' und $\varphi: G\to G'$ eine Abbildung. Dann nennen wir φ einen *(Monoid-)Homomorphismus*, falls gilt:
(i) $\varphi(e)=e'$,
(ii) $\varphi(g\circ h)=\varphi(g)\star\varphi(h)$ für alle $g,h\in G$.
Falls G und G' Gruppen sind, so heißt φ *Gruppenhomomorphismus*. In diesem Falle muss man (i) nicht fordern (leichte Übung).

Falls $G=G'$, so wird φ ein *Endomorphismus* genannt und wenn dieser bijektiv ist, so heißt er *Automorphismus*. Die Menge der Automorphismen von G bezeichnen wir mit $\mathrm{Aut}(G)$. Im allgemeinen werden bijektive Gruppenhomomorphismen Gruppen-*Isomorphismen* genannt.

Wir bezeichnen mit

$$\mathrm{Kern}\,\varphi := \{g\in G \mid \varphi(g)=e'\}\subset G$$

den *Kern* von φ und mit

$$\mathrm{Bild}\,\varphi := \varphi(G) := \{\varphi(g) \mid g\in G\}\subset G'$$

das *Bild* von φ.

Bemerkung 2.4 Sei G eine Gruppe und $g\in G$. Die Abbildung $\varphi:\mathbb{Z}\to G$, $n\mapsto g^n$ ist ein Gruppenhomomorphismus. Ihr Bild ist gegeben durch $\mathrm{Bild}\,\varphi=\langle g\rangle$ und es gilt $\mathrm{ord}(g)=|\langle g\rangle|$.

Bemerkung 2.5 Seien $(G,\circ),(G',\star)$ Gruppen und $\varphi: G\to G'$ ein Gruppenhomomorphismus.
(i) Es gilt $\varphi(g^{-1})=\varphi(g)^{-1}$ für alle $g\in G$.
(ii) Allgemein gilt $\varphi(g^n)=\varphi(g)^n$ für alle $n\in\mathbb{Z}$ (und alle $g\in G$).
(iii) Die Menge $\mathrm{Kern}\,\varphi\subset G$ ist eine Untergruppe von G und $\mathrm{Bild}\,\varphi\subset G'$ ist eine Untergruppe von G'.

(iv) Verkettungen von Gruppenhomomorphismen sind Gruppenhomomorphismen: Ist $\psi : G' \to H$ ein weiterer Gruppenhomomorphismus, so ist $\psi \circ \varphi : G \to H$ ein Gruppenhomomorphismus.

(v) Die Menge $Z(G) := \{g \in G \mid gh = hg \text{ für alle } h \in G\}$ ist eine Untergruppe von G und wird das *Zentrum* von G genannt. Falls G abelsch ist, so ist $Z(G) = G$.

Beweis. Wir zeigen die ersten 3 Punkte, die weiteren Punkte sind eine Übung:

(i) Es ist $e' = \varphi(g \circ g^{-1}) = \varphi(g) \star \varphi(g^{-1})$, woraus die Behauptung folgt.

(ii) Beweis per Induktion für alle $n \in \mathbb{N}_0$: Der Fall $n = 0$ ist klar. Und $\varphi(g^{n+1}) = \varphi(g^n \circ g) = \varphi(g^n) \star \varphi(g) = \varphi(g)^n \star \varphi(g) = \varphi(g)^{n+1}$ per Induktionsannahme und Definition.
Zusammen mit (i) folgt die Behauptung für negative n.

(iii) Es seien $e \in G$ und $e' \in G'$ die neutralen Elemente.
  (a) Seien $g, h \in \operatorname{Kern} \varphi$. Dann ist $\varphi(g \circ h) = \varphi(g) \circ \varphi(h) = e' \star e' = e'$ und somit $g \circ h \in \operatorname{Kern} \varphi$.
  (b) Außerdem ist $\varphi(e) = e'$ und somit $e \in \operatorname{Kern} \varphi$.
  (c) Mit $g \in \operatorname{Kern} \varphi$ gilt $\varphi(g^{-1}) = \varphi(g)^{-1} = e'$ nach (i).

Damit ist $\operatorname{Kern} \varphi \subset G$ eine Untergruppe.
Für $\operatorname{Bild} \varphi \subset G'$ gilt:
  (a) Es ist $\varphi(e) = e'$ und somit $e' \in \operatorname{Bild} \varphi$.
  (b) Sind $a, b \in \operatorname{Bild} \varphi$, so gibt es $g, h \in G$ mit $\varphi(g) = a, \varphi(h) = b$.
  Damit ist $a \star b = \varphi(g) \star \varphi(h) = \varphi(g \circ h) \in \operatorname{Bild} \varphi$.
  (c) Genauso: ist $a = \varphi(g) \in \operatorname{Bild} \varphi$, so ist $a^{-1} = \varphi(g^{-1}) \in \operatorname{Bild} \varphi$.

Somit ist $\operatorname{Bild} \varphi$ eine Untergruppe von G'.

■

2.2 Nebenklassen

In diesem Abschnitt sei nun G eine Gruppe mit neutralem Element $1 \in G$ und $H \subset G$ eine Untergruppe. Wir lassen die Verknüpfung, wie angekündigt, nun meist weg, um Schreibarbeit zu sparen.

Definition 2.5 Sei $g \in G$. Eine Menge der Form

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

wird *Linksnebenklasse* genannt. Genauso sind *Rechtsnebenklassen* definiert (also definiert man die Rechtsnebenklasse als $Hg := \{hg \mid h \in H\}$).

Die Menge der Linksnebenklassen wird mit $G/H := \{gH \mid g \in G\}$ bezeichnet. Analog wird die Menge der Rechtsnebenklassen mit $H\backslash G := \{Hg \mid g \in G\}$ bezeichnet. Wir bezeichnen mit $[G : H] := |G/H|$ den *Index von H in G* (die Anzahl der Linksnebenklassen).

Wichtig
Will man die Verknüpfung (z.B. $\circ$) auf der Gruppe hervorheben, so kann man auch

$$g \circ H = \{g \circ h \mid h \in H\}$$

ausschreiben. Zum Beispiel: Ist unsere Gruppe $G = \mathbb{Z}$ mit der Addition "+" gegeben, und $H = 5\mathbb{Z} = \{0, 5, -5, 10, -10, \ldots\}$ die von der 5 erzeugte Untergruppe (alle durch 5 teilbaren ganzen Zahlen), so ist die Nebenklasse der 3 gegeben durch

$$3 + 5\mathbb{Z} = \{3, 8, -2, 13, -7, \ldots\},$$

also durch alle ganzen Zahlen, die bei der Division durch 5 den Rest 3 lassen. Es wäre hierbei sehr verwirrend $3H$ für die Nebenklasse zu schreiben, $3 + H$, also mit Verknüpfung in der Notation, ist hier viel besser verständlich.

Insgesamt ist

$$G/H = \mathbb{Z}/5\mathbb{Z} = \{5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}.$$

Proposition 2.1 Für zwei Linksnebenklassen gH und $g'H$ sind folgende Bedingungen äquivalent:
(i) $gH = g'H$
(ii) $gH \cap g'H \neq \emptyset$
(iii) $g \in g'H$
(iv) $(g')^{-1}g \in H$.

Beweis.
"(i) $\Rightarrow$ (ii)":
Klar.
"(ii) $\Rightarrow$ (iii)":
Sei $x \in gH \cap g'H \neq \emptyset$. Dann ist $x = gh$ für ein $h \in H$ sowie $x = g'h'$ für ein $h' \in H$. Damit ist dann also $gh = g'h'$ und deshalb $g = g'h'h^{-1} \in g'H$.
"(iii) $\Rightarrow$ (iv)":
Es existiert nach Annahme ein $h \in H$, so dass $g = g'h$ gilt. Es folgt $(g')^{-1}g = h \in H$.
"(iv) $\Rightarrow$ (i)":
Sei $(g')^{-1}g = h \in H$. Es folgt $g = g'h$ sowie $g' = gh^{-1}$. Sei $h' \in H$, dann ist $gh' = g'hh' \in g'H$. Deshalb gilt $gH \subset g'H$. Und genauso ist $g'h' = gh^{-1}h' \in gH$. Es folgt $g'H \subset gH$ und somit die Behauptung. ■

Bemerkung 2.6 Wir definieren eine Relation $\sim$ auf G: Es gelte $g \sim g'$ genau dann, wenn $gH = g'H$ gilt. Dies definiert (nach Proposition 2.1) eine Äquivalenzrelation auf G.

Übung 2.1 Sei G eine Gruppe und $H \subset G$ eine Untergruppe.
(i) Die Abbildung $g \mapsto g^{-1}$ induziert eine Bijektion $G/H \to H\backslash G$ (Insbesondere ist der Index nicht davon abhängig, ob man ihn über Links- oder Rechtsnebenklassen definiert.)
(ii) Alle (Links- oder Rechts-)Nebenklassen von H in G sind gleichmächtig (d.h. es gibt jeweils eine bijektive Abbildung zwischen je zwei Nebenklassen).

■

Satz 2.1 — Lagrange. Sei G eine endliche Gruppe. Es gilt

$$|G| = |H| \cdot [G : H].$$

Beweis. Der Beweis folgt direkt aus der Übung, denn zwei verschiedene Nebenklassen sind disjunkt und G ist die disjunkte Vereinigung aller verschiedener Nebenklassen: Da alle Nebenklassen die gleiche Anzahl an Elementen haben, folgt die Behauptung. ■

Korollar 2.1 Ist $H \subset G$ eine Untergruppe, dann ist ihre Ordnung $|H|$ ein Teiler der Ordnung $|G|$ von G.

Satz 2.2 — Kleiner Fermat'scher Satz. Sei G eine endliche Gruppe und sei $g \in G$. Dann ist $\mathrm{ord}(g)$ ein Teiler von $|G|$ und es gilt $g^{|G|} = 1$.

Beweis. Sei $H := \langle g \rangle$ die von g erzeugte Untergruppe von G. Nach Satz 2.1 gilt dann, dass $\mathrm{ord}(g) = |H|$ ein Teiler von $|G|$ ist. Weiterhin folgt $g^{|G|} = 1$, da $g^{|G|} = (g^{|H|})^{[G:H]} = (g^{\mathrm{ord}(g)})^{[G:H]} = 1$. ■

2.3 Normalteiler, Faktorgruppen, Isomorphiesätze

Definition 2.6 Eine Untergruppe $H \subset G$ einer Gruppe G heißt *Normalteiler*, falls $gH = Hg$ für alle $g \in G$ gilt. In diesem Falle nennt man gH dann auch die *Restklasse* von g modulo H.

Bemerkung 2.7 (i) Ist G kommutativ, so ist jede Untergruppe ein Normalteiler.
(ii) In jeder Gruppe sind die triviale Untergruppe $\{1\} \subset G$ und die gesamte Gruppe G Normalteiler.
(iii) Eine Gruppe G heißt *einfach*, wenn Sie nur die Normalteiler G und $\{1\}$ besitzt.

Übung 2.2 $H \subset G$ ist genau dann Normalteiler, wenn $gHg^{-1} \subset H$ für alle $g \in G$ gilt. ∎

Bemerkung 2.8 Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus. Dann ist Kern φ ein Normalteiler von G.

Beweis. Sei $g \in G$ und $H := \operatorname{Kern}\varphi$. Zu zeigen ist, dass $gHg^{-1} \subset H$ ist. Sei $h \in H$, dann ist $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e'$ und somit ist $ghg^{-1} \in H = \operatorname{Kern}\varphi$. ■

Es stellt sich die Frage, ob die Umkehrung auch gilt: gegeben einen Normalteiler $N \subset G$, gibt es irgendeinen Gruppenhomomorphismus, dessen Kern gleich N ist? Dies ist in der Tat der Fall und wir werden jetzt sehen, warum dies der Fall ist.

Definition 2.7 Sei G eine Gruppe. Wir definieren nun für einen Normalteiler $N \subset G$ eine Gruppenstruktur auf G/N wie folgt: Seien gN und hN zwei Restklassen modulo N. Dann definieren wir die Verknüpfung $\circ$ auf G/N durch

$$gN \circ hN := (gh)N$$

für alle Nebenklassen $gN, hN \in G/N$. D.h. wir definieren das Produkt als die Restklasse des Elementes gh.

Wichtig
Man beachte, dass diese Definition *Repräsentanten* benutzt und man muss die *Wohldefiniertheit* (d.h. Unabhängigkeit von der Wahl der Repräsentanten) der Definition überprüfen.
Dies machen wir nun.

Lemma 2.1 Die Verknüpfung zweier Nebenklassen wie in Definition 2.7 definiert, ist wohldefiniert.

Beweis. Seien $g,h,g',h' \in G$ mit $gN = g'N$ sowie $hN = h'N$, d.h. g und g' sind beides Repräsentanten der Klasse gN und h,h' sind beides Repräsentanten der Klasse hN. Dann ist zu zeigen. dass unsere Definition nicht von der Wahl der Repräsentanten abhängt, d.h., dass $(gN)(hN) = (g'N)(h'N)$ gilt.
Per Definition ist $(g'N)(h'N) = (g'h')N$ sowie $(gN)(hN) = (gh)N$.
D.h. es ist $(gh)N = (g'h')N$ zu zeigen, was nach Proposition 2.1 äquivalent zu $(g'h')^{-1}(gh) \in N$ ist.
Wir rechnen dann aus:

$$(g'h')^{-1}(gh) = (h')^{-1}(g')^{-1}gh.$$

Nach Proposition 2.1 ist $n := (g')^{-1}g \in N$. Weiterhin, da N Normalteiler ist, existiert ein $n' \in N$, so dass $nh = hn'$ gilt. Wir erhalten

$$(g'h')^{-1}(gh) = (h')^{-1}(g')^{-1}gh. = (h')^{-1}nh = (h')^{-1}hn'.$$

Nach Annahme und Proposition 2.1 ist $(h')^{-1}h \in N$ und somit ist die Behauptung gezeigt. ■

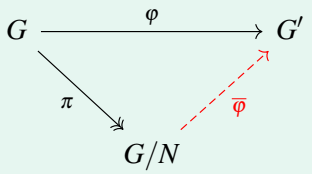
Proposition 2.2 Ist G eine Gruppe und N ein Normalteiler, so ist G/N mit der gerade definierten Verknüpfung eine Gruppe. Das neutrale Element ist $1N = N$ und das zu gN inverse Element ist $g^{-1}N$. Wir nennen G/N auch die *Faktor- oder Restklassengruppe* von G modulo N.

Bemerkung 2.9 Wir erhalten in dieser Situation nun einen natürlichen Gruppenhomomorphismus, die *kanonische Projektion* $\pi : G \to G/N$, gegeben durch $g \mapsto gN$. Die kanonische Projektion ist ein Epimorphismus, also ein surjektiver Gruppenhomomorphismus. In einem Diagramm benutzen wir auch einen Doppelpfeil

$$G \xrightarrow{\varphi} \!\!\!\!\rightarrow\; G/N,$$

um anzudeuten, dass es sich um einen surjektiven Homomorphismus handelt. (Ein injektiver Homomorphismus wird durch einen Pfeil mit einem Haken am „Ausgangspunkt“ angedeutet: $\hookrightarrow$.)

Satz 2.3 — Homomorphiesatz. Es sei G eine Gruppe und $N \subset G$ ein Normalteiler. Die kanonische Projektion $\pi : G \to G/N$ erfüllt die folgende universelle Eigenschaft: Für jeden Gruppenhomomorphismus $\varphi : G \to G'$ mit $N \subset \operatorname{Kern} \varphi$ gibt es einen eindeutig bestimmten Gruppenhomomorphismus $\bar{\varphi} : G/N \to G'$, so dass gilt: $\varphi = \bar{\varphi} \circ \pi$, d.h. das folgende Diagramm is kommutativ:



(Man sagt auch, dass φ durch G/N faktorisiert.)

Bemerkung 2.10 In der Situation von Satz 2.3 gilt außerdem, dass $\operatorname{Bild} \bar{\varphi} = \operatorname{Bild} \varphi$, $\operatorname{Kern} \bar{\varphi} = \pi(\operatorname{Kern} \varphi)$ und $\operatorname{Kern} \varphi = \pi^{-1}(\operatorname{Kern} \bar{\varphi})$.

Beweis von Satz 2.3. Die Eindeutigkeit einer solchen Abbildung ist leicht zu überprüfen: Wir nehmen an, dass $\bar{\varphi}$ mit den geforderten Eigenschaften existiert. Falls nun $\psi : G/N \to G'$ eine weitere Abbildung ist, so dass auch $\varphi = \psi \circ \pi$ gilt, dann muss $\psi(gN) = \varphi(g) = \bar{\varphi}(gN)$ für alle $g \in G$ gelten und damit $\psi = \bar{\varphi}$. Nun zeigen wir die Existenz: Wir definieren $\bar{\varphi}$ so, wie es also sein muss: $\bar{\varphi}(gN) := \varphi(g)$. Wir müssen die Wohldefiniertheit überprüfen: falls $hN = gN$ gilt, so ist $h = gg'$ mit $g' \in N$. Damit erhalten wir, dass $\varphi(h) = \varphi(gg') = \varphi(g)\varphi(g') = \varphi(g)$, da $\varphi(g') = 1$ ist, weil $N \subset \operatorname{Kern} \varphi$ nach Annahme. ∎

Korollar 2.2 Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus und sei $N := \operatorname{Kern} \varphi$. Dann sind $\operatorname{Bild} \varphi$ und G/N kanonisch isomorph: Es existiert ein eindeutig bestimmter Isomorphismus von Gruppen $\bar{\varphi} : G/N \to \operatorname{Bild} \varphi$ mit $\bar{\varphi}(gN) = \varphi(g)$ für alle $g \in G$.

Beispiel 2.9 Sei K ein Körper. Die aus der linearen Algebra bekannte Determinante ist ein surjektiver Gruppenhomomorphismus

$$\det : \mathrm{GL}_n(K) \to K^\times = K \setminus \{0\}.$$

Der Kern ist gegeben durch die *spezielle lineare Gruppe* $\mathrm{SL}_n(K) \subset \mathrm{GL}_n(K)$, also alle Matrizen mit Determinante $1 \in K$. Es handelt sich bei der Gruppe $\mathrm{SL}_n(K)$ also um einen Normalteiler in $\mathrm{GL}_n(K)$ und die Faktorgruppe $\mathrm{GL}_n(K)/\mathrm{SL}_n(K)$ ist nach Korollar 2.2 isomorph zu $K^\times$.

Satz 2.4 — 1. Isomorphiesatz. Sei $H \subset G$ eine Untergruppe einer Gruppe G und sei $N \subset G$ ein Normalteiler. Dann ist $HN := \{hn \mid h \in H, n \in N\} \subset G$ eine Untergruppe und $N \cap H$ ein Normalteiler in H und es gilt

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

(Diese Notation bedeutet, dass es einen kanonischen Isomorphismus zwischen $H/(H \cap N)$ und HN/N gibt.)

Beispiel 2.10 Wir erinnern noch mal daran, dass es sehr wichtig ist, trotz aller Bequemlichkeit, im konkreten Falle die Verknüpfung zu beachten! Sei $G = \mathbb{Z}$ mit der Addition, $H = 2\mathbb{Z}$ und $N = 3\mathbb{Z}$. (Da G abelsch ist, sind alle Untergruppen Normalteiler.) Dann ist das "Produkt" der Untergruppen von oben in diesem Fall die "Summe" $H + N = \mathbb{Z}$ (überzeugen Sie sich davon!) und man sieht ebenso leicht, dass $H \cap N = 6\mathbb{Z}$. Der 1. Isomorphiesatz besagt nun, dass $2\mathbb{Z}/6\mathbb{Z}$ zu $\mathbb{Z}/3\mathbb{Z}$ isomorph ist. Zur Übung überlege man sich, wie man dieses Beispiel leicht verallgemeinern kann.

Beweis. Wir zeigen zunächst, dass HN eine Untergruppe von G ist: es ist klar, dass $1 \in HN$ und mit $hg \in HN$ (d.h. $h \in H$ und $g \in N$) ist auch $(hg)^{-1} = g^{-1}h^{-1} = h^{-1}g'$ für ein $g' \in N$ in HN enthalten, da N ein Normalteiler

ist. Weiterhin ist mit $h_1g_1 \in HN$ und $h_2g_2 \in HN$ auch das Produkt $(h_1g_1)(h_2g_2) = (h_1h_2')(g_1g_2) \in HN$ für ein $h_2' \in H$, wieder unter Ausnutzung der Normalteilereigenschaft von N.

Nun zeigen wir, dass $N \cap H \subset H$ ein Normalteiler ist. Sei $h \in H$ und $g \in N \cap H$. Da N ein Normalteiler ist, existiert ein $g' \in N$, so dass $hg = g'h$ gilt. Da jedoch $g, h \in H$ sind, gilt auch $g' = hgh^{-1} \in H$ und damit ist $N \cap H$ ein Normalteiler in H.

Wir betrachten nun den kanonischen Homomorphismus

$$\varphi : H \hookrightarrow HN \xrightarrow{\pi} HN/N$$

mit der kanonischen Projektion π. Der Homomorphismus φ ist surjektiv: sei $gN \in HN/N$ mit $g \in HN$. Dann können wir g als $g = hh'$ mit $h \in H$ und $h' \in N$ schreiben. Es ist also $gN = hh'N = hN$. Damit ist $gN = hN = \varphi(h)$.

Der Kern von φ ist $\operatorname{Kern}\varphi = H \cap N$: ist $g \in \operatorname{Kern}(\varphi)$, so gilt $g \in H$ und $g \in N$, also $g \in H \cap N$. Damit folgt die Behauptung aus Korollar 2.2. ■

Satz 2.5 — 2. Isomorphiesatz. Seien $N, H \subset G$ Normalteiler einer Gruppe G mit $N \subset H$. Dann ist N auch ein Normalteiler in H und H/N ist Normalteiler von G/N (da $H \subset G$, ist H/N eine Teilmenge von G/N). Dann gilt:

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

(Man kann also N sozusagen "rauskürzen".)

Beweis. N ist ein Normalteiler in H: da $gN = Ng$ für alle $g \in G$ gilt, gilt dies insbesondere für alle $g \in H$.

Dass H/N eine Untergruppe von G/N ist, folgt direkt daraus, dass H eine Untergruppe von G ist. Diese ist ein Normalteiler, da H Normalteiler in G ist: Sei $hN \in H/N$ und $gN \in G/N$, dann ist $hN \cdot gN = hgN = gh'N = gN \cdot h'N$ für ein $h' \in H$.

Betrachten wir die kanonische Projektion $\pi_H : G \to G/H$, so erhalten wir, da $N \subset H = \operatorname{Kern}\pi_H$ ist, nach Satz 2.3 einen Homomorphismus $\bar{\pi}_H : G/N \to G/H$, $gN \mapsto gH$ dessen Kern gleich $H/N = \pi_H(H)$ ist. Die Behauptung folgt nun aus Korollar 2.2 und der Tatsache, dass π_H und damit auch $\bar{\pi}_H$ surjektiv ist. ■

Beispiel 2.11 Es lohnt sich wieder, den Fall $\mathbb{Z}/m\mathbb{Z}$ zu betrachten. Seien $m, n \in \mathbb{Z}$, $m, n \neq 0$. Dann sind $mn\mathbb{Z} \subset m\mathbb{Z}$ Normalteiler von $\mathbb{Z}$ und es gilt nach Satz 2.5, dass $m\mathbb{Z}/mn\mathbb{Z}$ eine Untergruppe von $\mathbb{Z}/m\mathbb{Z}$ ist und es gilt

$$(\mathbb{Z}/mn\mathbb{Z})/(m\mathbb{Z}/mn\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}.$$

Wir sehen also: zu jedem Teiler d von $0 \neq m \in \mathbb{Z}$ besitzt $\mathbb{Z}/m\mathbb{Z}$ eine Untergruppe der Ordnung d, nämlich $d'\mathbb{Z}/m\mathbb{Z}$ wobei $d' = m/d$ ist. Die Faktorgruppe $(\mathbb{Z}/m\mathbb{Z})/(d'\mathbb{Z}/m\mathbb{Z})$ ist isomorph zu $\mathbb{Z}/d'\mathbb{Z}$. Zum Beispiel hat $\mathbb{Z}/10\mathbb{Z}$ die nicht-trivialen Untergruppen $2\mathbb{Z}/10\mathbb{Z}$ und $5\mathbb{Z}/10\mathbb{Z}$. Im nächsten Abschnitt werden wir in Satz 2.6 sehen, dass dies auch alle nicht-trivialen Untergruppen sind.

2.4 Erzeuger und zyklische Gruppen

Etwas allgemeiner als im Beispiel 2.7, (ii):

Definition 2.8 Sei $M \subset G$ eine Teilmenge einer Gruppe G. Wir definieren die *von M erzeugte Untergruppe* von G durch

$$\langle M \rangle := \bigcap_{\substack{H \subset G \text{ Untergruppe} \\ M \subset H}} H.$$

(Dies ist die kleinste Untergruppe von G, die M enthält.) Man nennt M ein *Erzeugendensystem* von H, falls $H = \langle M \rangle$ gilt und sagt dann auch, dass M die Untergruppe H erzeugt. Eine Gruppe G heißt *endlich erzeugt*, falls es eine endliche Teilmenge $M \subset G$ gibt mit $G = \langle M \rangle$.

Bemerkung 2.11 Besteht $M = \{g\}$ nur aus einem Element, so erhalten wir die gleiche Definition wie zuvor. Allgemeiner, ist $M = \{m_1, \ldots, m_r\}$ endlich und G abelsch, so ist $\langle M \rangle = \{m_1^{n_1} \cdots m_r^{n_r} \mid n_1, \ldots, n_r \in \mathbb{Z}\}$.

Definition 2.9 Eine Gruppe G heißt *zyklisch*, falls es ein $g \in G$ gibt mit $G = \langle g \rangle$.

Bemerkung 2.12 Eine Gruppe ist genau dann zyklisch, wenn es einen surjektiven Gruppenhomomorphismus $\mathbb{Z} \to G$ gibt.

Beweis. Ist $G = \langle g \rangle$ zyklisch, so ist der gesuchte Homomorphismus durch $n \mapsto g^n$ gegeben. Sei umgekehrt $\varphi : \mathbb{Z} \to G$ surjektiv und setze $g := \varphi(1)$. Ist also $h \in G$, dann existiert ein $n \in \mathbb{Z}$ mit $h = \varphi(n) = g^n$ und somit gilt $G = \langle g \rangle$. ■

Satz 2.6 Sei $G = \langle g \rangle$ eine **zyklische** Gruppe. Jede Untergruppe von G ist zyklisch. Ist $n = |G|$ endlich, so gibt es zu jedem Teiler d von n genau eine Untergruppe der Ordnung d. Sie ist gegeben durch $\langle g^{n/d} \rangle$ und man erhält so alle Untergruppen.

Beweis. Sei H eine Untergruppe von G. OBdA ist $H \neq \{1\}$. Dann gibt es ein kleinstes $m \in \mathbb{N}$, so dass $h := g^m \in H$ ist. Wir behaupten, dass H von h erzeugt wird. Klar ist $\langle h \rangle \subset H$. Sei also $h' = g^s \in H$ beliebig, dann können wir s schreiben als $s = qm + r$, wobei $0 \leq r < m$ ist. Es ist somit $h' h^{-q} = g^r \in H$ und da m minimal war, muss $r = 0$ sein und damit ist $h' = h^q$ und die Behauptung ist bewiesen. Der Zusatz im Falle endlicher Ordnung folgt nun unmittelbar. ■

Übung 2.3 Der zweite Teil von Satz 2.6 ist eine Art Umkehrung vom Satz von Lagrange (Satz 2.1). Für allgemeine Gruppen ist die Aussage von Satz 2.6 falsch! Ein Beispiel ist die alternierende Gruppe $A_4 \subset S_4$, welche die Ordnung 12 hat, jedoch keine Untergruppe der Ordnung 6 besitzt. Beweisen Sie dies als Übung! ■

Korollar 2.3 Sei $H \subset \mathbb{Z}$ eine Untergruppe. Dann existiert ein $m \in \mathbb{Z}$ mit $H = m\mathbb{Z}$.

Beweis. Da $\mathbb{Z}$ zyklisch ist, ist auch H nach Satz 2.6 zyklisch und damit folgt die Behauptung. ■

Proposition 2.3 Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus und $G = \langle g \rangle$ sei zyklisch. Dann sind auch $\operatorname{Kern} \varphi$ und $\operatorname{Bild} \varphi$ zyklisch.

Beweis. Für $\operatorname{Kern} \varphi$ folgt die Aussage mit Satz 2.6, da dies eine Untergruppe der zyklischen Gruppe G ist. Sei $g' \in \operatorname{Bild} \varphi$, dann existiert ein $h \in G$, so dass $\varphi(h) = g'$ und außerdem existiert ein $n \in \mathbb{Z}$, so dass $h = g^n$. Damit ist aber $g' = \varphi(h) = \varphi(g^n) = \varphi(g)^n$ und damit gilt $\operatorname{Bild} \varphi = \langle \varphi(g) \rangle$. ■

Beispiel 2.12 Da $\mathbb{Z}$ zyklisch ist, ist auch $\mathbb{Z}/m\mathbb{Z}$ für jedes $m \in \mathbb{Z}$ als Bild der kanonischen Projektion zyklisch.

Satz 2.7 Sei G eine zyklische Gruppe. Falls G unendlich viele Elemente hat, so ist G zu $\mathbb{Z}$ isomorph, andernfalls ist G zu $\mathbb{Z}/m\mathbb{Z}$ isomorph, wobei $m = |G|$. Also: $\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z}$ (für alle $m \in \mathbb{N}$) sind bis auf Isomorphie die einzigen zyklischen Gruppen.

Beweis. In jedem Fall ist der Homomorphismus $\varphi : \mathbb{Z} \to G = \langle g \rangle$, gegeben durch $m \mapsto g^m$ surjektiv. Der Kern ist eine Untergruppe von $\mathbb{Z}$, also existiert ein $m \in \mathbb{Z}$ mit $\operatorname{Kern} \varphi = m\mathbb{Z}$. 1. Fall: $m = 0$, d.h. φ ist injektiv und somit auch $G \cong \mathbb{Z}$. 2. Fall: $m \neq 0$. Dann folgt aus Korollar 2.2, dass $G \cong \mathbb{Z}/m\mathbb{Z}$. (Bemerkung: man kann im Prinzip immer Korollar 2.2 anwenden, auch für $m = 0$, aber $\mathbb{Z}/0\mathbb{Z}$ ist zwar kanonisch isomorph zu $\mathbb{Z}$ aber per Definition schon ein etwas komisches Objekt; denn: $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}/\{0\} = \{n\{0\} \mid n \in \mathbb{Z}\}$, also eine Menge, die für jedes $n \in \mathbb{Z}$ eine Menge enthält, deren einziges Element die 0 ist – diese 0 ist aber eine 0 mit einem „Etikett“: n und die Gruppenstruktur ist die von $\mathbb{Z}$ induzierte (auf den „Etiketten“– das ist irgendwie unnötig kompliziert, also belassen wir es vielleicht lieber bei der Fallunterscheidung.) ■

Korollar 2.4 Sei G eine Gruppe, deren Ordnung $|G| = p$ eine Primzahl ist. Dann ist G zyklisch und somit $G \cong \mathbb{Z}/p\mathbb{Z}$.

Beweis. Sei $g \in G$ und $g \neq 1$, dann gilt $\text{ord}(g) \mid p$ (diese Notation heißt: $\text{ord}(g)$ teilt p). Damit muss dann aber $\text{ord}(g) = 1$ oder $\text{ord}(g) = p$ gelten. Im ersten Fall wäre aber $g = 1$, was wir ausgeschlossen haben und somit gilt $\text{ord}(g) = p$. Es ist also $|\langle g \rangle| = p = |G|$ und damit $G = \langle g \rangle$ und die Behauptung folgt aus Satz 2.7. ■

2.5 Die symmetrische Gruppe S_n

Sei M eine Menge. Wir haben bereits gesehen, dass

$$S(M) = \{f : X \to X \mid f \text{ ist bijektiv}\} \subset \text{Abb}(M, M),$$

die *symmetrische Gruppe* von M, eine Gruppe ist.

Definition 2.10 Die symmetrische Gruppe S_n vom Grad n ist die Gruppe $S(M_n)$, wobei $M_n := \{1, \ldots, n\}$. Die Elemente von S_n heißen *Permutationen* (von n Elementen).

Bemerkung 2.13
- Die Gruppe S_n hat $n!$ Elemente.
- Für $n \geq 3$ ist S_n nicht abelsch.

Notation: Man kann eine Permutation σ natürlich angeben, indem man die Elemente $1, \ldots, n$ und ihre Bilder $\sigma(1), \ldots, \sigma(n)$ vollständig auflistet. Zum Beispiel ($n = 4$)

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

bezeichnet die Permutation

$$\begin{aligned} &\sigma : M_4 \to M_4. \\ &\quad 1 \mapsto 2 \\ &\quad 2 \mapsto 3 \\ &\quad 3 \mapsto 1 \\ &\quad 4 \mapsto 4 \end{aligned}$$

Alternativ: *Zykelschreibweise*

$$\sigma = (123)(4) = (123).$$

Bei der Zykelschreibweise zerlegt man eine Permutation in *Zykel* der Form $(a_1, a_2, \ldots, a_r)$, wobei diese Notation bedeuten soll, dass $a_1 \mapsto a_2, a_2 \mapsto a_3, \ldots, a_{r-1} \mapsto a_r, a_r \mapsto a_1$. Zwei Zykel $(a_1, a_2, \ldots, a_r)$ und $(b_1, b_2, \ldots, b_s)$ heißen *disjunkt*, falls $a_i \neq b_j$ für alle i, j. Zykel der Länge 1 kann man auch weglassen (sie entsprechen der Identität).

Proposition 2.4 Jede Permutation $\sigma \in S_n$ kann in disjunkte Zykel zerlegt werden.

Beweisskizze. Man starte mit $a_1 = 1, a_2 = \sigma(1), \ldots$. Da M_n endlich ist und σ bijektiv ist, kann es kein Element geben mit $\sigma(a_i) = a_j$ und $i > j$ außer wenn $\sigma(a_i) = 1$ ist (denn $\sigma(a_{j-1}) = a_j$). Damit ist $(a_1, a_2, \ldots, a_i)$ mit $\sigma(a_i) = 1$ der erste Zykel. Ist die Länge des Zykels nun schon n, so sind wir fertig. Außerdem sind wir fertig, wenn es keine Elemente von M_n mehr gibt (außer $a_1, \ldots, a_i$, die nicht von σ festgehalten werden. Gibt es noch ein Element $b_1 \in M_n$ weches ungleich aller a_j ist, mit $\sigma(b_1) \neq \sigma(b_1)$, so beginnen wir hier unseren neuen Zykel. ■

Definition 2.11 Ein Element $\tau \in S_n$ heißt *Transposition*, falls es $k, \ell \in \{1, \ldots, n\}$ mit $k \neq \ell$ gibt, sodass

$$\begin{aligned} \tau(k) &= \ell, \\ \tau(\ell) &= k, \\ \tau(j) &= j \quad \forall j \in \{1, \ldots, n\} \setminus \{k, \ell\}. \end{aligned}$$

Man kann zeigen, dass sich jede Permutation als Produkt von endlich vielen Transpositionen schreiben lässt (siehe Lineare Algebra).

Man definiert die Signum-Abbildung

$$\operatorname{sign} : S_n \to \{\pm 1\}$$

gewöhnlich durch die Anzahl der Fehlstände einer Permutation. Es ist $\operatorname{sign}(\sigma) = 1$, falls σ eine gerade Anzahl an Fehlstellen hat und ansonsten $\operatorname{sign}(\sigma) = -1$.

Wir erinnern an den folgenden bekannten Satz (zum Beispiel aus der Linearen Algebra), aus der sich auch eine Alternative Definition für sign durch die Anzahl der Transpositionen in einer Zerlegung von σ ergibt.

Satz 2.8 Die Abbildung

$$\operatorname{sign} : S_n \to \{\pm 1\}$$

ist ein Gruppenhomomorphismus. Das heißt, für alle $\sigma, \tau \in S_n$ gilt: $\operatorname{sign}(\sigma \circ \tau) = \operatorname{sign}(\sigma) \cdot \operatorname{sign}(\tau)$.

Außerdem gilt: Ist $\sigma = \tau_1 \circ \ldots \circ \tau_r$ eine Zerlegung der Permutation $\sigma \in S_n$ in Transpositionen, so ist $\operatorname{sign}(\sigma) = (-1)^r$.

Definition 2.12 Der Kern der Signum-Abbildung wird mit $A_n := \operatorname{Kern}(\operatorname{sign})$ bezeichnet und die *alternierende Gruppe* genannt. Sie besteht also aus allen geraden Permutationen.

Bemerkung 2.14 A_n ist eine Normalteiler von S_n und hat $\frac{n!}{2}$ Elemente.

2.6 Direkte und semidirekte Produkte

Wir haben bereits in Beispiel 2.5 das direkte Produkt von Gruppen kennen gelernt. Jetzt wollen wir uns mit der Frage beschäftigen, wie man eine Gruppe als direktes Produkt von einigen Untergruppen identifiziert.

Wir beschränken uns auf den Fall von zwei Untergruppen. Sind H_1 und H_2 Gruppen, so ist das Produkt

$$H_1 \times H_2$$

wieder eine Gruppe mit den komponentenweisen Operationen.

Bemerkung 2.15

- Sind H_1, H_2 endliche Gruppen, so gilt
$$|H_1 \times H_2| = |H_1||H_2|.$$
- Sind H_1 und H_2 abelsch, so ist $H_1 \times H_2$ abelsch.

Die Gruppe $H_1 \times H_2$ ist in folgendem Sinne ein *inneres direktes Produkt* der Untergruppen $H_1 \times \{1\}$ und $\{1\} \times H_2$:

Definition 2.13 Sei G eine Gruppe und $H_1, H_2 \subset G$ seien Untergruppen. Dann heißt G *inneres direktes Produkt* von H_1 und H_2, falls gilt

(i) Jedes Element $g \in G$ lässt sich eindeutig als Produkt $g = h_1 h_2$ mit $h_1 \in H_1$ und $h_2 \in H_2$ schreiben

(ii) H_1 und H_2 sind Normalteiler in G.

Falls G inneres direktes Produkt von H_1 und H_2 ist, so liefert die Multiplikationsabbildung

$$H_1 \times H_2 \to G, (h_1, h_2) \mapsto h_1 h_2$$

einen Isomorphismus von Gruppen.

Beispiel 2.13 Ein Beispiel zur Motivation: Wir haben gesehen: Die Gruppe $G = \mathbb{Z}/6\mathbb{Z}$ ist zyklisch. Sie hat u.a. die Untergruppen $H_1 = 2\mathbb{Z}/6\mathbb{Z}$ und $H_2 = 3\mathbb{Z}/2\mathbb{Z}$. Wir haben ebenfalls mit Hilfe des Homomorphiesatzes schon gesehen, dass $H_1 \cong \mathbb{Z}/3\mathbb{Z}$ ist und $H_2 \cong \mathbb{Z}/2\mathbb{Z}$. Betrachten wir das direkte Produkt $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ und listen alle Elemente auf

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \{(\bar{0},\bar{0}),(\bar{1},\bar{0}),(\bar{0},\bar{1}),(\bar{1},\bar{1}),(\bar{0},\bar{2}),(\bar{1},\bar{2})\},$$

wobei wir vereinfachend $\bar{m}$ für die Restklasse von $m \in \mathbb{Z}$ in der jeweiligen Faktorgruppe geschrieben haben. Wir stellen fest, dass das Element $(\bar{1},\bar{1})$ die Gruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ erzeugt, denn es ist $2(\bar{1},\bar{1}) = (\bar{0},\bar{2})$ und $3(\bar{1},\bar{1}) = (\bar{1},\bar{0})$, $4(\bar{1},\bar{1}) = (\bar{0},\bar{1})$ und $5(\bar{1},\bar{1}) = (\bar{1},\bar{2})$. Damit erhalten wir durch $(\bar{1},\bar{1}) \mapsto \bar{1} \in \mathbb{Z}/6\mathbb{Z}$ einen Isomorphismus zwischen dem direkten Produkt $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong H_1 \times H_2$ und der Gruppe G.

Wir geben nun ein Kriterium an, wann sich eine Gruppe generell in das Produkt von zwei Untergruppen zerlegen lässt.

Satz 2.9 Seien H_1 und H_2 Untergruppen der Gruppe G. Betrachte die Abbildung

$$\varphi : H_1 \times H_2 \to G, (h_1,h_2) \mapsto h_1h_2.$$

(i) φ ist genau dann surjektiv, wenn $G = H_1H_2 = \{h_1h_2 \mid h_1 \in H_1, h_2 \in H_2\}$.
(ii) φ ist genau dann injektiv, wenn $H_1 \cap H_2 = \{1\}$ gilt.
(iii) φ ist genau dann ein Gruppenhomomorphismus, wenn H_1 und H_2 miteinander vertauschen, d.h. $h_1h_2 = h_2h_1$ für alle $h_1 \in H_1$ und alle $h_2 \in H_2$.
(iv) φ ist genau dann ein Gruppenisomorphismus, wenn H_1 und H_2 Normalteiler in G sind mit $H_1 \cap H_2 = \{1\}$ und $G = H_1H_2$.

Beweis. (i) Das ist klar.
(ii) $\varphi(h_1,h_2) = \varphi(h_1',h_2')$ ist äquivalent zu $(h_1')^{-1}h_1 = (h_2')h_2^{-1}$. Dieses Element ist in $H_1 \cap H_2$. Ist also $H_1 \cap H_2 = \{1\}$, so ist $h_1' = h_1$ und $h_2' = h_2$ und φ ist injektiv. Ist umgekeht φ injektiv und $g \in H_1 \cap H_2$, so ist $\varphi(g,g^{-1}) = gg^{-1} = 1$ und damit folgt $g = 1$.
(iii) Es ist einerseits $\varphi((h_1,h_2)(h_1',h_2')) = \varphi(h_1h_1',h_2h_2') = h_1h_1'h_2h_2'$ und andererseits $\varphi(h_1,h_2)\varphi(h_1',h_2') = h_1h_2h_1'h_2'$. Es muss also $h_1'h_2 = h_2h_1'$ für alle $h_1' \in H_1$ und alle $h_2 \in H_2$ sein.
(iv) Sind H_1,H_2 normal mit $H_1 \cap H_2 = \{1\}$, so vertauschen H_1 und H_2 miteinander: man betrachtet den Kommutator $[h_1,h_2] = h_1h_2h_1^{-1}h_2^{-1}$, der in H_1 enthalten ist, da H_1 normal ist und in H_2 enthalten ist, da H_2 normal ist. Damit ist $[h_1,h_2] = 1$ und somit vertauschen H_1 und H_2. Die Abbildung φ ist also gemäß (i-iii) ein Gruppenisomorphismus nach unseren Annahmen.
Falls umgekehrt φ ein Isomorphismus ist, so gilt nach (i-ii), dass $G = H_1H_2$ und $H_1 \cap H_2 = \{1\}$. Nach (iii) vertauschen H_1 und H_2. Wir behaupten, dass H_1 und H_2 sogar Normalteiler sind. Sei $g \in G$ und schreibe $G = h_1h_2$ mit $h_1 \in H_1$ und $h_2 \in H_2$ (dies geht wegen (i)). Dann ist $gH_1 = h_1h_2H_1 = h_2h_1H_1 = h_2H_1 = H_1h_2 = H_1h_1h_2 = H_1g$. Somit ist H_1 normal. Für H_2 folgt dies ganz genauso.

■

Beispiel 2.14 Sei $H_1 = \{z \in \mathbb{C} \mid |z| = 1\}$ sowie $H_2 = \mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$. Dies sind Untergruppen von $G = \mathbb{C}^\times$ mit der Multiplikation. Es ist

$$H_1 \cap H_2 = \{1\}$$

sowie

$$H_1H_2 = \mathbb{C}^\times = G,$$

denn $z = \frac{z}{|z|}|z|$. Die beiden Untergruppen sind Normalteiler in G, da G abelsch ist. Nach Satz 2.9 ist die Abbildung $\varphi : H_1 \times H_2 \to \mathbb{C}^\times, (z,r) \mapsto zr$ ein Gruppenisomorphismus.

Bemerkung 2.16 Wir machen folgende Beobachtung: Wir können H_1 mit dem Normalteiler $H_1 \times \{1\}$ in

$G = H_1 \times H_2$ identifizieren. Die Faktorgruppe G/H_1 ist isomorph zu H_2, denn der Kern der Projektion auf den 2. Faktor $H_1 \times H_2 \to H_2$ ist durch H_1 gegeben und die Aussage folgt dann aus dem Homomorphiesatz. In dieser Situation liefert die Inklusion $\iota_2 : H_2 \hookrightarrow G$ ein Rechtsinverses zur kanonischen Projektion $\pi_2 : G \to G/H_1 \cong H_2$, d.h. es gilt $\pi_2 \circ \iota_2 = \mathrm{id}_{H_2}$.

Man kann dies auch so formulieren: zunächst mal liefern die Inklusion $H_1 \hookrightarrow G$ und die kanonische Projektion (bzw. Projektion auf die 2. Komponente) $\pi_2 : G \to H_2$ immer eine *kurze exakte Sequenz*:

$$1 \longrightarrow H_1 \xrightarrow{\iota_1} G \xrightarrow{\pi_2} H_2 \longrightarrow 1.$$

Hierbei steht die 1 einfach für $\{1\}$, die triviale Gruppe, die nur aus dem Einselement besteht. Die Sequenz heißt per Definition exakt, falls $\mathrm{Kern}(\pi_2) = \mathrm{Bild}(\iota_1)$ gilt und ι_1 injektiv sowie π_2 surjektiv ist (d.h. die Gleichheit vom Kern der nachfolgenden Abbildung mit dem Bild der vorangegangenen Abbildung gilt für jeden Pfeil in dem Diagramm). Die Aussage, dass ι_2 ein Rechtsinverses zu π_2 ist, bedeutet, dass die Sequenz an der Stelle π_2 spaltet:

$$1 \longrightarrow H_1 \xrightarrow{\iota_1} G \underset{\iota_2}{\overset{\pi_2}{\rightleftarrows}} H_2 \longrightarrow 1.$$

Generell sagt man, dass eine kurze exakte Sequenz

$$1 \longrightarrow N \xrightarrow{f} G \xrightarrow{g} H \longrightarrow 1$$

an der Stelle g spaltet, falls es einen Gruppenhomomorphismus $h : H \to G$ gibt, so dass $g \circ h = \mathrm{id}_H$ ist. Man notiert die Sequenz dann genau wie oben als

$$1 \longrightarrow N \xrightarrow{f} G \underset{h}{\overset{g}{\rightleftarrows}} H \longrightarrow 1 \tag{2.1}$$

Mit anderen Worten: g liefert einen Isomorphismus zwischen $\mathrm{Bild}(h)$ und H.

Dass die Sequenz an der Stelle g spaltet, reicht aber nicht aus, damit $G \cong N \times H$ gilt. Dazu muss außerdem das Bild von h ein Normalteiler in G sein (Übung).

Man kann die Bemerkung also so verstehen: Wenn eine kurze exakte Sequenz von Gruppen (2.1) an der Stelle g durch $h : H \to G$ spaltet und $\mathrm{Bild}(h)$ ein Normalteiler von G ist, so ist $G \cong G/N \times N$.

Aber was passiert in dem Falle, dass die Sequenz (2.1) zwar spaltet, das Bild aber kein Normalteiler ist? Dann ist die Gruppe G zwar kein direktes Produkt, aber es gibt dennoch einen Weg, sie aus den Gruppen N und G/N irgendwie zusammenzubauen: die sind die sogenannten semidirekten Produkte.

Die Details werden wir in einer Übung behandeln, hier beschränken wir uns auf die Definition und einen Satz ohne Beweis.

Erinnerung: mit $\mathrm{Aut}(G)$ wir die Gruppe der Automorphismen von G bezeichnet.

Definition 2.14 Es seien H und N zwei Gruppen und $\alpha : H \to \mathrm{Aut}(N)$ ein Gruppenhomomorphismus. Dann definieren wir eine Verknüpfung auf der Menge $N \times H$ durch

$$(n,h)(n',h') = (n\alpha(h)(n'), hh').$$

In der Übung zeigen Sie, dass diese Verknüpfung die Menge $N \times H$ auch zu einer Gruppe macht.

Das neutrale Element ist $(1,1)$ und das zu (n,h) inverse Element ist

$$(n,h)^{-1} = ((\alpha(h^{-1})(n^{-1})), h^{-1}).$$

Wir schreiben $N \rtimes_\alpha H$ für diese Gruppe. Sie heißt *semidirektes Produkt* von N und H bezüglich α.

Bemerkung 2.17 Ist $\alpha(h) = \mathrm{id}_N$ für alle $h \in H$, so ist das zugehörige semidirekte Produkt in Wirklichkeit ein direktes Produkt.

Der Beweis des folgenden Satzes ist eine Übung.

Satz 2.10 Sei G eine Gruppe und $N \subset G$ ein Normalteiler. Dann ist G isomorph zu einem semidirekten Produkt von N und G/N, genau dann, wenn die kurze exakte Sequenz

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\pi} G/N \longrightarrow 1 \tag{2.2}$$

rechts (an der Stelle π) spaltet, d.h. wenn es einen Gruppenhomomorphismus $\varphi : G/N \to G$ gibt mit $\pi \circ \varphi = \mathrm{id}_{G/N}$.

Das semidirekte Produkt ist dann gegeben durch $\alpha : G/N \to \mathrm{Aut}(N)$ definiert durch

$$\alpha(gN) = n \mapsto \varphi(gN) n \varphi(gN)^{-1}.$$

Beispiel 2.15 — Die Diedergruppe D_n. Die Diedergruppe ist das semidirekte Produkt von $N = \mathbb{Z}/n\mathbb{Z}$ und $H = \mathbb{Z}/2\mathbb{Z}$, bezüglich $\alpha : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ gegeben durch

$$\alpha(0) = \mathrm{id}, \quad \alpha(1) = x \mapsto -x.$$

(Dies ist ein Automorphismus, da N abelsch ist.) Das heißt, die Multiplikation in D_n ist definiert durch

$$(n_1, h_1)(n_2, h_2) = (n_1 + (-1)^{h_1} n_2, h_1 + h_2).$$

Wir werden später sehen, dass dies die Symmetriegruppe eines regelmäßigen n-Ecks ist. Der Normalteiler N entspricht den Drehungen und H einer von einer Spiegelung erzeugten Untergruppe.

3. Ringe und Polynome

3.1 Ringe

Ein *Ring* ist eine abelsche Gruppe (wir benutzen stets die additive Schreibweise), auf der zusätzlich eine mit der Addition verträgliche Multiplikation definiert ist. Ringe sind uns wohlbekannte mathematische Strukturen und vielleicht sogar etwas natürlicher als Gruppen, denn das uns vermutlich am besten bekannte Beispiel sind die ganzen Zahlen $\mathbb{Z}$. Am wichtigsten für diese Vorlesungen werden Polynomringe sein.

Definition 3.1 Ein *Ring* (mit Eins) ist eine Menge R mit zwei Verknüpfungen $+$ und $\cdot$, so dass

(i) $(R,+)$ eine abelsche Gruppe (mit neutralem Element 0)
(ii) $(R,\cdot)$ ein Monoid (mit neutralem Element $1 \in R$) ist
(iii) und die Distributivgesetze

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

für alle $a,b,c \in R$ gelten.

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

Eine Teilmenge $S \subset R$ heißt *Unterring*, falls S unter Addition und Multiplikation abgeschlossen ist und so auch ein Ring ist (S muss also eine Untergruppe bzgl. $+$ und ein Untermonoid bzgl. $\cdot$ sein, die Distributivgesetze muss man nicht wieder nachprüfen). Man nennt so ein Paar $S \subset R$ auch eine *Ringerweiterung* (R ist eine Ringerweiterung von S).

Bemerkung 3.1
(i) $0\cdot a = 0$ für alle $a \in R$, denn $0\cdot a = (0+0)\cdot a = 0\cdot a + 0\cdot a$, woraus die Behauptung durch die Kürzungsregel für Gruppen folgt.
(ii) Es gilt $(-a)\cdot b = a\cdot(-b) = -(a\cdot b)$ für alle $a,b \in R$ (leichte Übung).
(iii) *Vorsicht:* Bei der Multiplikation gilt die Kürzungsregel im Algemeinen nicht: also $a\cdot b = c\cdot b$ (für $b \neq 0$) impliziert nicht notwendigerweise $a = c$! ($a\cdot b = c\cdot b$ ist äquivalent zu $(a-c)\cdot b = 0$ und hieraus folgt im Allgemeinen eben nicht, dass $(a-c) = 0$ gelten muss; Beispiele kennen wir aus der Matrixmultiplikation).
(iv) Wir lassen den Nullring $R = \{0\}$ in der Definition prinzipiell zu. In diesem Falle gilt $1 = 0$ in R. Der Nullring ist jedoch der einzige Ring, in dem dies gelten kann, denn: ist $R \neq \{0\}$ und $a \in R, a \neq 0$, so ist $1\cdot a = a$ und $0\cdot a = 0$, so dass $1 \neq 0$ gelten muss.

Definition 3.2 Sei R ein Ring. Dann bezeichnen wir mit

$$R^\times = \{a \in R \mid \text{es existiert ein } b \in R \text{ mit } ab = ba = 1\}$$

die *Einheiten* von R. Die Menge $R^\times$ ist eine Gruppe mit der Multiplikation. Falls $R \neq \{0\}$ ist und $R^\times = R \setminus \{0\}$ gilt, heißt R ein *Schiefkörper* und falls R zusätzlich kommutativ ist, so heißt R ein *Körper*.

Definition 3.3 (i) Ein Element $a \in R$ heißt *Nullteiler*, falls es ein $b \in R \setminus \{0\}$ gibt mit $ab = 0$ oder $ba = 0$.
(ii) Ein Ring heißt *nullteilerfrei* oder *Integritätsring*, falls $R \neq \{0\}$ ist und $0 \in R$ der einzige Nullteiler ist. (In der Literatur werden Integritätsringe auch oft *Integritätsbereiche* genannt.)
(iii) Zwei Elemente $a, b \in R$ (einem kommutativen) Ring heißen *assoziiert*, wenn es ein $c \in R^\times$ gibt mit $a = cb$.

Beispiel 3.1 (i) $\mathbb{Z}$ ist ein Integritätsring, $\mathbb{Z}^\times = \{\pm 1\}$.
(ii) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper.

Beispiel 3.2 Die *Hamiltonschen Quaternionen* $\mathbb{H}$ bilden einen Schiefkörper, der kein Körper ist. Diese sind wie folgt definiert: Als abelsche Gruppe ist $\mathbb{H} = \mathbb{R}^4$ mit der Addition, wobei es üblich ist, die Basiselemente mit $\mathbf{1}, i, j$ und k zu bezeichnen. Wir führen eine Multiplikation auf $\mathbb{H}$ ein, indem wir zunächst für die Basivektoren definieren:

$$\mathbf{1}^2 = 1, \qquad i^2 = j^2 = -\mathbf{1}$$
$$\mathbf{1}x = x\mathbf{1} = x \text{ für alle } x \in \mathbb{H}$$
$$ij = -ji = k.$$

Die Multiplikation setzt man dann $\mathbb{R}$-linear auf ganz $\mathbb{H}$ fort, d.h.

$$\begin{aligned}(a_1\mathbf{1} + b_1 i + c_1 j + d_1 k)(a_2\mathbf{1} + b_2 i + c_2 j + d_2 k - b_1) = {} & (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)\mathbf{1} \\ & + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)i \\ & + (a_1c_2 + c_1a_2 + d_1b_2 - d_2b_1)j \\ & + (a_1d_2 + d_1a_2 + b_1c_2 - b_2c_1)k.\end{aligned}$$

Man erhält durch $x \mapsto x\mathbf{1}$ eine Einbettung von $\mathbb{R}$ in $\mathbb{H}$. (D.h. $\mathbb{R} \subset \mathbb{H}$ ist ein Unterring, der ein Körper ist.)

Bemerkung 3.2 Die Hamiltonschen Quaternionen sind ein Beispiel einer sogenannten *Quaternionen-Algebra*. Diese sind im Allgemeinen als ein vierdimensionaler Vekorraum über einem Körper K definiert mit einer Basis $\{1, i, j, k\}$. Und zu $a, b \in K$ definiert man eine Multiplikation durch die Regeln $i^2 = a$, $j^2 = b$, sowie $ij = k$ und $ji = -k$. Diese setzt man dann wieder K-linear fort. Für $K = \mathbb{R}$ und $a = b = -1$ erhält man die Hamiltonschen Quaternionen.

Beispiel 3.3 Weitere Beispiele von Ringen:
(i) Die $n \times n$-Matrizen $K^{n\times n}$ über einem Körper K, welche für $n \geq 2$ nicht kommutativ sind.
(ii) Die Menge R^M der Abbildungen von einer Menge M in einen Ring R bildet einen Ring mit punktweiser Addition und Multiplikation.
(iii) Für $M = \{1, \ldots, n\}$ kann man R^M als Menge $R^n = R \times \ldots \times R$ (n faches kartesisches Produkt) identifizieren und erhält eine Ringstruktur auf R^n, welche der komponentenweisen Addition und Multiplikation entspricht.

Das folgende Beispiel ist eine eigene Definition wert.

Definition 3.4 Sei R ein kommutativer Ring. Dann definieren wir den *Polynomring* $R[X]$ über R wie folgt: als Menge sei $R[X]$ gegeben durch

$$R[X] := \{(a_n)_{n\in\mathbb{N}_0} \mid a_n \in R, \quad a_n = 0 \text{ für fast alle } n \in \mathbb{N}_0\},$$

d.h. $R[X]$ besteht aus allen Folgen von Elementen aus R, bei denen alle bis auf endlich viele Folgeglieder gleich Null sind. Als Menge ist dies eine Teilmenge von $R^{\mathbb{N}_0}$. Die Addition erklären wir auch punktweise wie

bei $R^{\mathbb{N}_0}$, d.h. $(a+b)_n = a_n + b_n$ für $a,b \in R[X]$ und für alle $n \in \mathbb{N}_0$, die Multiplikation jedoch wie folgt: Sind $a,b \in R[X]$, so definieren wir $(a \cdot b)_n := \sum_{j+k=n} a_j b_k$.

Der Polynomring $R[X]$ ist tatsächlich ein Ring (nachrechnen!), das neutrale Element der Addition ist die Nullabbildung und das der Multiplikation ist die Folge mit $a_0 = 1$ und $a_i = 0$ für alle $i > 0$. Anstatt die Elemente als Folgen (oder Abbildungen) zu schreiben, schreiben wir $f \in R[X]$ in der Form

$$f = \sum_{n \in \mathbb{N}_0} a_n X^n = \sum_{n=0}^{N} a_n X^n,$$

wobei N so groß gewählt sei, dass $a_n = 0$ für $n > N$. Addition und Multiplikation schreiben sich dann so:

$$\sum_{i \in \mathbb{N}_0} a_i X^i + \sum_{i \in \mathbb{N}_0} b_i X^i = \sum_{i \in \mathbb{N}_0} (a_i + b_i) X^i,$$

$$\sum_{i \in \mathbb{N}_0} a_i X^i \cdot \sum_{i \in \mathbb{N}_0} b_i X^i = \sum_{i \in \mathbb{N}_0} \left(\sum_{j+k=i} a_j b_k \right) X^i,$$

Im Folgenden verstehen wir unter einem Ring **stets einen kommutativen Ring** (ansonsten wird dies erwähnt).

3.2 Ideale

Die Bezeichnung *Ideal* wurde von *Richard Dedekind* (1831-1916) eingeführt und ist aus dem Begriff der *idealen Zahlen* entstanden, welcher von *Ernst Kummer* (1810-1893) geprägt wurde. Für uns spielen Ideale vor allem deshalb eine wichtige Rolle, weil wir für ein Ideal $\mathfrak{a}$ eines Ringes R einen Faktorring $R/\mathfrak{a}$ definieren können, analog zur Faktorgruppe G/N, wobei $N \subset G$ ein Normalteiler ist.

Definition 3.5 Sei R ein Ring. Eine Teilmenge $\mathfrak{a} \subset R$ heißt *Ideal* in R, falls gilt:
(i) $\mathfrak{a} \subset R$ ist eine Untergruppe von R mit der Addition
(ii) und $\mathfrak{a}$ ist abgeschlossen unter Multiplikation mit Elementen aus R, d.h. mit $a \in \mathfrak{a}$ und $x \in R$ ist stets auch $xa \in \mathfrak{a}$.

Bemerkung 3.3 Man kann Ideale auch in nicht-kommutativen Ringen definieren. Dabei muss man dann aber zwischen Linksidealen und Rechtsidealen unterscheiden. Unsere Definition entspricht den Linksidealen und Rechtsideale sind so definiert, dass man in (ii) fordert, dass mit $a \in \mathfrak{a}$ und $x \in R$ auch $ax \in \mathfrak{a}$ ist.

Beispiel 3.4
(i) Ist $x \in R$, so kann man stets das *von x erzeugte Hauptideal* $(x) := Rx := \{rx \mid r \in R\}$ definieren. Es handelt sich offensichtlich um das kleinste Ideal von R, welches x enthält.
(ii) Etwas allgemeiner: sind $x_1, \ldots, x_n \in R$, so kann man das *von $x_1, \ldots, x_n$ erzeugte Ideal* definieren:

$$(x_1, \ldots, x_n) := Rx_1 + \ldots + Rx_n = \{r_1 x_1 + \ldots + r_n x_n \mid r_1, \ldots, r_n \in R\}.$$

Das Ideal $(x_1, \ldots, x_n)$ ist das kleinste Ideal von R, welches alle Elemente $x_1, \ldots, x_n$ enthält.
(iii) Sind $\mathfrak{a}$ und $\mathfrak{b}$ Ideale, so erhält man Ideale $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{a} \cdot \mathfrak{b}$ und $\mathfrak{a} \cap \mathfrak{b}$, wobei

$$\mathfrak{a} + \mathfrak{b} := \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}, \quad \mathfrak{a} \cdot \mathfrak{b} := \{\sum_{i=1}^{n} a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, n \in \mathbb{N}\}$$

(Übung)
(iv) Noch allgemeiner: Ist $(x_i)_{i \in I}$ eine Familie von Elementen aus R, so definiert man das von dieser Familie erzeugte Ideal als $\sum_{i \in I} Rx_i = \{r_1 x_1 + \ldots + r_n x_n \mid r_i \in R, n \in \mathbb{N}\}$, also als die Menge aller endlichen Linearkombinationen (mit Koeffizienten in R) von Elementen aus der Familie $(x_i)_{i \in I}$.

Definition 3.6 Ist $\mathfrak{a} = \sum_{i \in I} Rx_i$ wie im Beispiel, so heißt die Familie $(x_i)_{i \in I}$ ein *Erzeugendensystem* von $\mathfrak{a}$. Gibt es endlich viele Elemente, so dass $\mathfrak{a} = (x_1, \ldots, x_n)$ gilt, so heißt $\mathfrak{a}$ *endlich erzeugt*. Ideale der Form (x) heißen *Hauptideale*. Ein Integritätsring in dem jedes Ideal ein Hauptideal ist, heißt *Hauptidealring*.

Übung 3.1 In einem Integritätsring gilt $(a) = (b)$ für zwei Hauptideale genau dann, wenn a und b assoziiert sind. ∎

Beispiel 3.5 Die Untergruppen $m\mathbb{Z} \subset \mathbb{Z}$ sind Hauptideale. Wir haben bereits gesehen, dass dies die einzigen Untergruppen von $\mathbb{Z}$ sind, und somit ist $\mathbb{Z}$ ein Hauptidealring.

Beispiel 3.6 Die Elemente des Hauptideals $(2) = 2\mathbb{Z} \subset \mathbb{Z}$ sind alle geraden ganzen Zahlen und die Elemente von $(3) = 3\mathbb{Z}$ sind alle ganzzahligen Vielfachen von 3. Der Schnitt $(2) \cap (3)$ besteht also aus allen durch 2 und 3 teilbaren Zahlen, das sind also alle durch 6 teilbaren Zahlen. Das Ideal $(2) + (3)$ enthält genau die ganzen Zahlen m, welche sich als $m = 2x + 3y$ schreiben lassen mit $x, y \in \mathbb{Z}$ (dies ist ganz $\mathbb{Z}$, denn $1 = -2 + 3 \in (2) + (3)$).

3.3 Homomorphismen

Definition 3.7 Seien R, S Ringe. Eine Abbildung $f : R \to S$ wird *Ringhomomorphismus* genannt, falls gilt

(i) f ist ein Gruppenhomomorphismus bzgl. der Addition: $f(a+b) = f(a) + f(b)$ für alle $a, b \in R$

(ii) f ist ein Monoidhomomorphismus bzgl. der Multiplikation: $f(ab) = f(a)f(b)$ für alle $a, b \in R$ sowie $f(1) = 1$.

Die Bezeichnungen (Ring-)*Endomorphismus*, (Ring-)*Automorphismus* und (Ring-)*Isomorphismus* werden wie üblich definiert.

Bemerkung 3.4 (i) Die Verkettung von Ringhomomorphismen ist wieder ein Ringhomomorphismus.

(ii) Ist $f : R \to S$ ein Ringhomomorphismus, so ist $\mathrm{Kern}(f) := \{a \in R \mid f(a) = 0\} \subset R$ ein Ideal.

(iii) Das $\mathrm{Bild}(f) \subset S$ ist ein Unterring von S.

(iv) Es gilt $f(R^\times) \subset S^\times$ und die induzierte Abbildung $f : R^\times \to S^\times$ ist ein Gruppenhomomorphismus.

Beweis. Wir beweisen nur (ii) und (iv), die anderen beiden Punkte sind Ihnen als Übung überlassen:

(ii) Da ein Ringhomomorphismus insbesondere ein Homomorphismus von (abelschen) Gruppen ist, ist $\mathrm{Kern}(f)$ in jedem Falle eine Untergruppe von R. Mit $a \in \mathrm{Kern}(f)$ gilt auch $f(xa) = f(x)f(a) = f(x) \cdot 0 = 0$ und somit $xa \in \mathrm{Kern}(f)$ und somit ist $\mathrm{Kern}(f)$ ein Ideal.

(iv) Sei $x \in R^\times$ eine Einheit. Dann existiert also ein $y \in R$ mit $xy = yx = 1$. Da bei einem Ringhomomorphismus stets $f(1) = 1$ gilt, ist $f(x)f(y) = f(xy) = f(1) = 1 = f(yx) = f(y)f(x)$ und damit $f(x) \in S^\times$. Dass es sich bei der Einschränkung von f auf $R^\times \to S^\times$ um einen Gruppenhomomorphismus handelt ist klar.

∎

Bemerkung 3.5 **Vorsicht**: Dass wir die Ideale einführen, hat seine Berechtigung. Während der Kern eines Gruppenhomomorphismus eine Untergruppe (gar ein Normalteiler) ist, hat der Kern eines Ringhomomorphismus **keine** Ringstruktur. Denn ist $f : R \to S$ ein Ringhomomorphismus und ist $S \neq \{0\}$ nicht der Nullring, so ist $1 \notin \mathrm{Kern}(f)$, da $f(1) = 1$ gefordert wird und $1 \neq 0$ gilt.

Übung 3.2 Ein Ringhomomorphismus von einem Körper K in einen Ring $R \neq \{0\}$ ist stets injektiv. ∎

Beispiel 3.7 — Multiplikation mit ganzen Zahlen. Sei R ein Ring. Dann gibt es stets einen eindeutig bestimmten Ringhomomorphismus $\varphi : \mathbb{Z} \to R$, denn da $\varphi(1) = 1$ gelten muss, ist auch das Bild aller $n \in \mathbb{N}$ durch $\varphi(n) = \varphi(1 + \ldots + 1) = 1 + \ldots + 1$ eindeutig bestimmt (genauso für $\varphi(-n) = -\varphi(n)$ und $\varphi(0) = 0$). Man erhält so eine Multiplikationsabbildung $m \cdot a := \varphi(m) \cdot a$ für $m \in \mathbb{Z}$ und $a \in R$.

Beispiel 3.8 — Einsetzungshomomorphismus. Ist R ein Ring, $x \in R$ und $R[X]$ der Polynomring über

R, so erhalten wir den *Einsetzungshomomorphismus*

$$\phi_x : R[X] \to R, \quad f = \sum_j a_j X^j \mapsto f(x) := \sum_j a_j x^j.$$

Dies ist ein Ringhomomorphismus, wie sich leicht nachrechnen lässt.

3.4 Faktorringe

Definition 3.8 Sei R ein Ring und $\mathfrak{a} \subset R$ ein Ideal. Die Menge

$$R/\mathfrak{a} := \{x + \mathfrak{a} \mid x \in R\}$$

wird *Faktorring* (oder *Restklassenring*) genannt.

Die Menge ist zunächst einfach die Menge der Linksnebenklassen von $\mathfrak{a}$ als Untergruppe der additiven abelschen Gruppe R, von der wir schon wissen, dass sie eine abelsche Gruppe ist (die Addition wird hierbei durch $(x+\mathfrak{a})+(y+\mathfrak{a}) := (x+y)+\mathfrak{a}$ definiert). $R/\mathfrak{a}$ ist aber in der Tat auch ein Ring!

Proposition 3.1 Erklären wir analog eine Multiplikation auf $R/\mathfrak{a}$ durch

$$(x+\mathfrak{a}) \cdot (y+\mathfrak{a}) := (x \cdot y) + \mathfrak{a}$$

für $x+\mathfrak{a}, y+\mathfrak{a} \in R/\mathfrak{a}$, so wird $R/\mathfrak{a}$ zu einem (kommutativen) Ring.

Beweis. Es ist zunächst die Wohldefiniertheit der Multiplikation zu zeigen: Seien also $x+\mathfrak{a} = x'+\mathfrak{a} \in R/\mathfrak{a}$ sowie $y+\mathfrak{a} = y'+\mathfrak{a} \in R/\mathfrak{a}$, dann gilt $x - x' \in \mathfrak{a}$ sowie $y - y' \in \mathfrak{a}$. Es ist zu zeigen, dass dann $xy+\mathfrak{a} = x'y'+\mathfrak{a}$ gilt. Dies ist äquivalent zu $xy - x'y' \in \mathfrak{a}$. Mit $x - x'$ ist auch $y(x-x') = xy - x'y \in \mathfrak{a}$ (da $\mathfrak{a}$ ein Ideal ist) und, ebenso, da $y - y' \in \mathfrak{a}$ gilt, ist auch $x'(y-y') = x'y - x'y' \in \mathfrak{a}$. Damit ist nun aber auch die Summe $y(x-x') + x'(y-y') = xy - x'y + x'y - x'y' = xy - x'y'$ in $\mathfrak{a}$ enthalten, woraus die Wohldefiniertheit der Multiplikation folgt.

Es ist noch zu zeigen, dass $R/\mathfrak{a}$ mit der Multiplikation ein (kommutativer) Monoid ist. Die Verknüpfung ist aber klarerweise assoziativ; dies folgt aus der Assoziativität der Multiplikation in R. Außerdem ist $1+\mathfrak{a}$ das neutrale Element, denn $(1+\mathfrak{a})(x+\mathfrak{a}) = 1 \cdot x + \mathfrak{a} = x + \mathfrak{a}$ per Definition und da 1 das neutrale Element in R ist, sowie analog: $(x+\mathfrak{a})(1+\mathfrak{a}) = x \cdot 1 + \mathfrak{a} = x + \mathfrak{a}$.

Um den Beweis abzuschließen, müssen wir noch zeigen, dass die Distributivgesetze gelten. Dies folgt jedoch sofort aus der Gültigkeit der Distributivgesetze in R. ∎

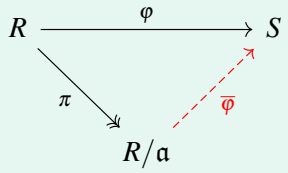
Beispiel 3.9 — $\mathbb{Z}/m\mathbb{Z}$. Sei $m \in \mathbb{N}$. Dann hat $\mathbb{Z}/m\mathbb{Z}$ also die Struktur eines kommutativen Ringes.

Die *kanonische Projektion*

$$\pi : R \to R/\mathfrak{a}, \quad x \mapsto x + \mathfrak{a}$$

ist ein surjektiver Ringhomomorphismus. Dieser erfüllt die gleiche universelle Eigenschaft wie die kanonische Projektion im Falle eines Normalteilers einer Gruppe.

Satz 3.1 — Homomorphiesatz. Sei $\varphi : R \to S$ ein Ringhomomorphismus und $\mathfrak{a} \subset R$ ein Ideal mit $\mathfrak{a} \subset \operatorname{Kern} \varphi$. Dann existiert genau ein Ringhomomorphismus $\bar{\varphi} : R/\mathfrak{a} \to S$, so dass das Diagramm



kommutiert. Es gilt $\operatorname{Bild} \bar{\varphi} = \operatorname{Bild} \varphi$, $\operatorname{Kern} \bar{\varphi} = \pi(\operatorname{Kern} \varphi)$ sowie $\operatorname{Kern} \varphi = \pi^{-1}(\operatorname{Kern} \bar{\varphi})$.

Beweis. Der Beweis folgt fast direkt aus von Satz 2.3, da φ ja auch ein Gruppenhomomorphismus ist und die $R/\mathfrak{a}$ zugrunde liegende Gruppe genau die Faktorgruppe ist. Der nach dem Homomorphiesatz für Gruppen eindeutig bestimmte Gruppenhomomorphismus $\bar{\varphi} : R/\mathfrak{a} \to S$ ist aber automatisch auch ein Ringhomomorphismus, denn $\varphi(x)$ ist als Ringhomomorphismus vorausgesetzt und es gilt $\bar{\varphi}(x+\mathfrak{a}) = \varphi(x)$ für alle $x+\mathfrak{a} \in R/\mathfrak{a}$. Genauer: es gilt $\bar{\varphi}((x+\mathfrak{a})(y+\mathfrak{a})) = \varphi(x)\varphi(y) = \bar{\varphi}(x+\mathfrak{a})\bar{\varphi}(y+\mathfrak{a})$. ■

Korollar 3.1 Ist $\varphi : R \to S$ ein surjektiver Ringhomomorphismus, so gilt $R/\operatorname{Kern}\varphi \cong S$.

Beispiel 3.10 — Einsetzungshomomorphismus. Sei R ein Ring und $x \in R$ ein festes Element. Wir betrachten wieder den Einsetzungshomomorphismus ϕ_x.

Es ist klar, dass ϕ_x surjektiv ist, denn zu jedem $a \in \mathbb{R}$ ist das konstante Polynom $f_a = a \in R[X]$ und $f_a(x) = a$. Der Kern von ϕ_x ist gegeben durch das Ideal $\operatorname{Kern}(\phi_x) = \{f \in R[X] \mid f(x) = 0\}$ aller Polynome, welche x als Nullstelle besitzen. Wir erhalten dann aus dem Homomorphiesatz, dass $R[X]/\operatorname{Kern}(\phi_x) \cong R$.

Das Beispiel lässt sich auch etwas verallgemeinern und die folgende Konstruktion wird später von entscheidender Bedeutung sein. Ist $R \subset S$ eine Ringerweiterung, so können wir in Polynome aus $R[X]$ auch Elemente aus S einsetzen und erhalten zu $x \in S$ ebenfalls einen Ringhomomorphismus $\phi_x : R[X] \to S, f \mapsto f(x)$. Zum Beispiel: Ist $R = \mathbb{R}$ und $S = \mathbb{C}$, so können wir den Einsetzungshomomorphismus $\phi_i : \mathbb{R}[X] \to \mathbb{C}$ betrachten. Durch Polynomdivision sieht man leicht ein (wir machen das in Kürze noch im Detail), dass $\operatorname{Kern}(\phi_i) = (X^2+1)$ ist (Ein Polynom besitzt i genau dann als Nullstelle, wenn es durch X^2+1 teilbar und somit im von X^2+1 erzeugten Ideal in $\mathbb{R}[X]$ enthalten ist).

Nach dem Homomorphiesatz gilt also $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$.

Die Isomorphiesätze übertragen sich analog, wir werden dies in den Übungen behandeln. Zur Vollständigkeit geben wir die Sätze hier ohne Beweis an.

Satz 3.2 — 1. Isomorphiesatz. Sei $\mathfrak{a} \subset R$ ein Ideal und $S \subset R$ ein Unterring. Dann ist $S+\mathfrak{a} \subset R$ ein Unterring von R und $\mathfrak{a} \subset S+\mathfrak{a}$ ein Ideal. Es gilt

$$S/(\mathfrak{a} \cap S) \cong (S+\mathfrak{a})/\mathfrak{a}.$$

Satz 3.3 — 2. Isomorphiesatz. Seien $\mathfrak{a}, \mathfrak{b} \subset R$ Ideale mit $\mathfrak{a} \subset \mathfrak{b}$. Dann ist die Faktorgruppe $\mathfrak{b}/\mathfrak{a}$ ein Ideal von $R/\mathfrak{a}$ und es gilt

$$(R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}) \cong R/\mathfrak{b}.$$

3.5 Primideale, maximale Ideale

Bemerkung 3.6 Eine kurze Erinnerung: Eine natürliche Zahl $p \in \mathbb{N}$ (mit $p > 1$) wird *Primzahl* genannt, wenn aus für $a, b \in \mathbb{N}$ mit $p \mid ab$ schon $p \mid a$ oder $p \mid b$ folgt (Primeigenschaft).

Dies ist (in $\mathbb{Z}$ bzw. $\mathbb{N}$) zu folgender Aussage äquivalent: $p > 1$ ist eine Primzahl genau dann, wenn ihre einzigen positiven Teiler 1 und p sind.

Beweis. Angenommen p sei eine Primzahl (gemäß obiger Definition und sei $a \in \mathbb{N}$ ein Teiler von p. OBdA sei $a < p$. Das heißt also, es existiert ein $b \in \mathbb{N}$, so dass $p = ab$ ist. Damit ist aber auch p ein Teiler von ab und somit, da p eine Primzahl ist, gilt schon $p \mid a$ oder $p \mid b$. Da jedoch $a < p$ gilt, muss $p \mid b$ und somit schon $p = b$ und damit auch $a = 1$ gelten. Hat p umgekehrt nur die Teiler 1 und p in den natürlichen Zahlen, so folgt die Primeigenschaft aus der Eindeutigkeit der Primfaktorisierung in den natürlichen Zahlen, also dem *Fundamentalsatz der Arithmetik*. ■

Bemerkung 3.7 Die sicherlich allgemein bekanntere „Definition“ einer Primzahl (p hat nur die positiven Teiler 1 und p) kann man auch als *Unzerlegbarkeit* oder *Irreduzibilität* (in $\mathbb{Z}$) bezeichnen. Unter der Annahme der Existenz einer eindeutigen Primfaktorzerlegung folgt aus Unzerlegbarkeit also die Primeigenschaft. Wir kommen auf diese Definitionen in Kürze wieder zurück.

Proposition 3.2 Sei $m \in \mathbb{N}$. Dann sind folgende Aussagen äquivalent:
(i) Die Zahl m ist eine Primzahl.
(ii) Der Ring $\mathbb{Z}/m\mathbb{Z}$ ist ein Integritätsring.
(iii) Der Ring $\mathbb{Z}/m\mathbb{Z}$ ist ein Körper.

Im Folgenden schreiben wir stets $\bar{a} = a + m\mathbb{Z}$ für die Restklassen in $\mathbb{Z}/m\mathbb{Z}$.

Beweis. Ist m eine Primzahl und sind $\bar{a}, \bar{b} \in \mathbb{Z}/m\mathbb{Z}$ mit $\bar{a}\bar{b} = 0$, so folgt $m \mid ab$. Da m eine Primzahl ist, folgt bereits $m \mid a$ oder $m \mid b$. Dies ist äquivalent zu $\bar{a} = \bar{0}$ oder $\bar{b} = \bar{0}$ und damit ist $\mathbb{Z}/m\mathbb{Z}$ in diesem Falle ein Integritätsring.

Es gelte (ii) und es sei $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ mit $\bar{a} \neq \bar{0}$. Dann ist die Multiplikationsabbildung $\varphi_{\bar{a}} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \bar{x} \mapsto \overline{ax}$ injektiv, denn aus $\overline{ax} = \overline{ay}$ folgt schon $x = y$ im Integritätsring (siehe Übung). Da $\varphi_{\bar{a}}$ jedoch eine Abbildung zwischen endlichen Mengen gleicher Kardinalität ist, folgt hieraus bereits, dass φ_a auch surjektiv ist. Damit existiert zu jedem $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ mit $\bar{a} \neq \bar{0}$ insbesondere ein $\bar{b} \in \mathbb{Z}/m\mathbb{Z}$, so dass $\varphi_{\bar{a}}(\bar{b}) = \bar{1}$ ist und somit $\bar{a}\bar{b} = \bar{1}$. Damit ist $\bar{a}$ also eine Einheit und $\mathbb{Z}/m\mathbb{Z}$ bereits ein Körper.

Es bleibt die Implikation (iii) $\Rightarrow$ (i) zu zeigen. Sei also $\mathbb{Z}/m\mathbb{Z}$ ein Körper. Falls m keine Primzahl wäre, d.h. m hat nichttriviale Teiler, zum Beispiel $m = ab$ mit $a, b > 1$, so hat $\mathbb{Z}/m\mathbb{Z}$ Nullteiler, denn $\bar{a}\bar{b} = \bar{0}$ obwohl $\bar{a}, \bar{b} \neq \bar{0}$. Damit muss m eine Primzahl sein. ■

Bemerkung 3.8 Der Beweis zeigt, dass also die folgende, allgemeinere Aussage gilt: Ein endlicher (kommutativer) Integritätsring ist ein Körper.

Notation 3.1 Für eine Primzahl p ist $\mathbb{Z}/p\mathbb{Z}$ also ein Körper mit p Elementen. Wir verwenden hierfür die Notation $\mathbb{F}_p$.

Definition 3.9 Sei R ein Ring.
(i) Ein Ideal $\mathfrak{p} \subset R$ heißt *Primideal*, falls $\mathfrak{p} \neq R$ ist und gilt: sind $a, b \in R$ mit $ab \in \mathfrak{p}$, so gilt schon $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.
(ii) Ein Ideal $\mathfrak{m} \subset R$ heißt *maximales Ideal*, falls $\mathfrak{m} \neq R$ ist und gilt: ist $\mathfrak{a} \subset R$ ein Ideal mit $\mathfrak{m} \subset \mathfrak{a}$, so gilt $\mathfrak{a} = \mathfrak{m}$ oder $\mathfrak{a} = R$.

Beispiel 3.11 Ein Ring R ist genau dann ein Integritätsring, wenn das Nullideal (0) ein Primideal ist.

Bemerkung 3.9 Ein Ring R ist genau dann ein Körper, wenn $(0) \subset R$ das einzige maximale Ideal in R ist, d.h. (0) und R sind die einzigen Ideale in R.

Beweis. Sei R ein Körper und $\mathfrak{a} \subset R$ ein Ideal, $\mathfrak{a} \neq (0)$ und $a \in \mathfrak{a}$ mit $a \neq 0$. Dann ist schon $1 = a^{-1}a \in \mathfrak{a}$ und damit gilt $\mathfrak{a} = R$.

Besitzt R umgekehrt nur die Ideale (0) und R, so sei $a \in R \setminus \{0\}$ und wir betrachten das Hauptideal $(a) \subset R$. Dann muss also schon $(a) = R$ gelten, woraus folgt, dass es ein $b \in R$ gibt mit $ba = 1$. Somit ist R ein Körper. ■

Beispiel 3.12 Zur Veranschaulichung halten wir die Situation in den ganzen Zahlen fest.
(i) In den ganzen Zahlen $\mathbb{Z}$ ist ein Ideal $m\mathbb{Z}$ (mit $m \in \mathbb{N}_0$) genau dann ein Primideal, wenn m eine Primzahl oder $m = 0$ ist.
(ii) In $\mathbb{Z}$ ist ein Ideal $m\mathbb{Z}$ (mit $m \in \mathbb{N}_0$) genau dann maximal, wenn m eine Primzahl ist.

Die Aussagen im Beispiel lassen sich auch leicht elementar beweisen, folgen aber auch aus der folgenden, allgemeineren Aussage zusammen mit Proposition 3.2.

Proposition 3.3 Sei R ein Ring und $\mathfrak{a} \subsetneq R$ ein Ideal. Es gelten:
(i) Das Ideal $\mathfrak{a}$ ist genau dann ein Primideal, wenn $R/\mathfrak{a}$ ein Integritätsring ist.
(ii) Es ist $\mathfrak{a}$ genau dann ein maximales Ideal, wenn $R/\mathfrak{a}$ ein Körper ist.

Bevor wir diese Proposition beweisen, halten wir noch fest:

Bemerkung 3.10 (i) Sei $\varphi : R \to S$ ein Ringhomomorphismus und $\mathfrak{b} \subset S$ ein Ideal. Dann ist $\mathfrak{a} := \varphi^{-1}(\mathfrak{b}) \subset R$ ein Ideal.

(ii) Im Allgemeinen ist as Bild eines Ideals kein Ideal mehr. Ist jedoch $\varphi : R \to S$ ein **surjektiver** Ringhomomorphismus und $\mathfrak{a} \subset R$ ein Ideal, so ist das Bild $\varphi(\mathfrak{a})$ ein Ideal in S.

Beweis. (i) Das kann man explizit nachrechnen oder, etwas leichter, so einsehen: Sei $\psi : R \to S \to S/\mathfrak{b}$ die Verkettung von φ mit der kanonischen Projektion $S \to S/\mathfrak{b}$. Dann gilt $\mathrm{Kern}(\psi) = \varphi^{-1}(\mathfrak{b}) = \mathfrak{a}$ und somit ist $\mathfrak{a} \subset R$ ein Ideal als Kern eines Ringhomomorphismus.

(ii) Klar ist: $\varphi(\mathfrak{a}) \subset S$ ist eine Untergruppe bzgl. der Addition. Zur Mutliplikation mit Elementen aus S: Ist nun $a' = \varphi(a) \in \varphi(\mathfrak{a})$ und $s \in S$, so existiert ein $r \in R$ mit $\varphi(r) = s$, da φ surjektiv ist. Somit ist $sa' = \varphi(r)\varphi(a) = \varphi(ra) \in \varphi(\mathfrak{a})$.

■

Beweis. Die Forderung $\mathfrak{a} \neq R$ ist äquivalent zu $R/\mathfrak{a} \neq \{0\}$.

(i) Sei $\mathfrak{a} \subset R$ ein Primideal und $x+\mathfrak{a}, y+\mathfrak{a} \in R/\mathfrak{a}$ mit $(x+\mathfrak{a})(y+\mathfrak{a}) = 0$. Dann gilt also $xy+\mathfrak{a} = \mathfrak{a}$, also $xy \in \mathfrak{a}$. Da $\mathfrak{a}$ ein Primideal ist, folgt schon $x \in \mathfrak{a}$ oder $y \in \mathfrak{a}$ und somit $x+\mathfrak{a} = 0$ oder $y+\mathfrak{a} = 0$ und damit ist $R/\mathfrak{a}$ ein Integritätsring.
Ist umgekehrt $R/\mathfrak{a}$ ein Integritätsring und $x, y \in R$ mit $xy \in \mathfrak{a}$. Es gilt also $(x+\mathfrak{a})(y+\mathfrak{a}) = 0 \in R/\mathfrak{a}$ und dies impliziert nun $x+\mathfrak{a} = 0$ oder $y+\mathfrak{a} = 0$. Es folgt $x \in \mathfrak{a}$ oder $y \in \mathfrak{a}$.

(ii) Die kanonische Projektion $\pi : R \to R/\mathfrak{a}$ liefert eine Bijektion zwischen: a) den Idealen von $R/\mathfrak{a}$ und b) den Idealen $\mathfrak{b}$ von R mit $\mathfrak{a} \subset \mathfrak{b} \subset R$.
Es ist $R/\mathfrak{a}$ genau dann ein Körper, wenn es nur die Ideale (0) und $R/\mathfrak{a}$ in $R/\mathfrak{a}$ gibt, was also gleichbedeutend mit der Maximalität von $\mathfrak{a}$ ist.

■

Korollar 3.2 Jedes maximale Ideal ist ein Primideal.

3.6 Chinesischer Restsatz

Als Ergänzung zu den Übungsaufgaben (in denen wir den Chinesischen Restsatz für $\mathbb{Z}$ behandelt haben) formulieren wir nun den Chinesischen Restsatz für (allgemeine) Ringe.

Definition 3.10 Zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ eines Rings R heißen *koprim*, falls $\mathfrak{a} + \mathfrak{b} = R$ gilt.

Satz 3.4 Sei R ein Ring und $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ seien paarweise koprime Ideale in R. Mit $\pi_i : R \to R/\mathfrak{a}_i$ bezeichnen wir jeweils die kanonische Projektion und es sei

$$\varphi : R \to R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n, \quad x \mapsto (\pi_1(x), \ldots, \pi_n(x)). \tag{3.1}$$

Dann ist φ ein surjektiver Ringhomomorphismus und induziert damit einen Isomorphismus von Ringen

$$R/\bigcap_i \mathfrak{a}_i \cong R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n. \tag{3.2}$$

Beweis. Es ist klar, dass φ ein Ringhomomorphismus ist. Wir zeigen nun, dass φ surjektiv ist. Dazu halten wir fest, dass die Ideale $\mathfrak{a}_j$ und $\mathfrak{b}_j := \cap_{i \neq j} \mathfrak{a}_i$ für jedes $j = 1, \ldots, n$ koprim sind. Das sieht man so: Sei $j \in \{1, \ldots, n\}$. Da $\mathfrak{a}_j$ zu jedem $\mathfrak{a}_i$ für $i \neq j$ koprim ist, gibt es zu $i \neq j$ je ein $a_i \in \mathfrak{a}_j$ und $b_i \in \mathfrak{a}_i$, so dass $a_i + b_i = 1$ für alle i ist. Damit ist dann aber

$$1 = \prod_{i \neq j} (a_i + b_i) \in \mathfrak{a}_j + \prod_{i \neq j} \mathfrak{a}_i \subset \mathfrak{a}_j + \mathfrak{b}_j.$$

Da also $\mathfrak{a}_j$ und $\mathfrak{b}_j$ für alle j koprim sind, gibt es $x_j \in \mathfrak{a}_j$ und $y_j \in \mathfrak{b}_j$ mit $x_j + y_j = 1$ bzw. $y_j = 1 - x_j$. Es gilt dann also $\pi_j(y_j) = 1 + \mathfrak{a}_j$ und $\pi_i(y_j) = 0$ für alle $i \neq j$. Sei also $(s_1 + \mathfrak{a}_1, \ldots, s_n + \mathfrak{a}_n) \in R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n$, dann ist $\varphi(s_1 y_1 + \ldots + s_n y_n) = (s_1 + \mathfrak{a}_1, \ldots, s_n + \mathfrak{a}_n)$ – also ist φ surjektiv. Der Kern ist offensichtlich der Schnitt $\cap_i \mathrm{Kern}\, \pi_i = \cap_i \mathfrak{a}_i$ und damit folgt die Behauptung aus dem Homomorphiesatz (bzw. Korollar 3.1). ■

Für die Version des Chinesischen Restsatzes in den ganzen Zahlen $\mathbb{Z}$: siehe Aufgabe H9.

3.7 Division mit Rest, euklidische Ringe

In den ganzen Zahlen kennen wir das Prinzip der *Division mit Rest*: Sind a und $b \neq 0$ ganze Zahlen, so existieren eindeutig bestimmte ganze Zahlen q und r mit $0 \leq r < |b|$, so dass

$$a = qb + r$$

gilt. Dabei ist also qb das betraglich größte ganzzahlige Vielfache von b, welches kleiner oder gleich a ist und r der (hier als nicht-negativ normierte) Rest, welcher bei ganzzahliger Division von a durch b entsteht.

Beispiel 3.13 (i) Für $a = 11$ und $b = 5$, erhalten wir $q = 2$ und $r = 1$.
(ii) Für $a = 10$ und $b = 5$, erhalten wir $q = 2$ und $r = 0$.
(iii) Für $a = -21$ und $b = 4$, erhalten wir $q = -6$ und $r = 3$.

Ein ähnliches Verfahren ist die *Polynomdivision* (mit Rest). Zunächst definieren wir (als Ersatz für den Absolutbetrag in $\mathbb{Z}$) den *Grad* eines Polynoms $0 \neq f = \sum_i a_i X^i \in R[X]$ durch

$$\operatorname{grad}(f) := \max\{i \in \mathbb{N}_0 \mid a_i \neq 0\}.$$

Wir definieren außerdem den Grad des Nullpolynoms als $\operatorname{grad}(0) = -\infty$. Wir verwenden die Konvention, dass $-\infty \leq m$ ist für alle $m \in \mathbb{Z}$ und außerdem $-\infty + (-\infty) = -\infty + m = -\infty$ für alle $m \in \mathbb{Z}$.

Der Koeffizient a_n mit $n = \operatorname{grad} f$ heißt der *führende Koeffizient* oder *Leitkoeffizient* von f. Falls dieser gleich 1 ist, so heißt f *normiert*.

Wir halten nun zunächst ein paar Eigenschaften der Gradabbildung fest.

Bemerkung 3.11 Für alle $f, g \in R[X]$ gilt
(i) $\operatorname{grad}(f+g) \leq \max\{\operatorname{grad} f, \operatorname{grad} g\}$,
(ii) $\operatorname{grad}(f \cdot g) \leq \operatorname{grad} f + \operatorname{grad} g$.
In (ii) gilt Gleichheit, falls der führende Koeffizient von f oder g kein Nullteiler in R ist. Falls R ein Integritätsring ist, so gilt in (ii) also stets: $\operatorname{grad}(f \cdot g) = \operatorname{grad} f + \operatorname{grad} g$.

Beweis. Dies ist eine leichte Übung. ■

Bemerkung 3.12 Ist R ein Integritätsring, so auch $R[X]$ und die Einheiten sind $R[X]^\times = R^\times$.

Beweis. Sei R also ein Integritätsring und $f, g \in R[X]$ mit $fg = 0$. Dann ist also $\operatorname{grad} fg = -\infty$ und damit nach Bemerkung 3.11 bereits $\operatorname{grad} f = -\infty$ oder $\operatorname{grad} g = -\infty$ bzw. $f = 0$ oder $g = 0$. ■

Satz 3.5 Sei R ein Ring und $0 \neq g = \sum_i a_i X^i \in R[X]$ ein Polynom mit $\operatorname{grad} g = d$, dessen führender Koeffizient a_d eine Einheit in R sei. Dann gibt es zu jedem $f \in R[X]$ eindeutig bestimmte Polynome $q, r \in R[X]$ mit $\operatorname{grad} r < \operatorname{grad} g$ sowie

$$f = qg + r.$$

Beweis. Da der führende Koeffizient von g eine Einheit ist, gilt stets $\operatorname{grad}(qg) = \operatorname{grad}(q) + \operatorname{grad}(g) = \operatorname{grad}(q) + d$.

Wir zeigen zunächst die **Existenz** per Induktion nach $n = \operatorname{grad} f$.
Für $n < d$ können wir $g = 0$ und $r = f$ nehmen.
Ist $f = \sum_i b_i X^i$ mit $b_n \neq 0$ und $n \geq d$, so ist

$$f_1 := f - b_n a_d^{-1} X^{n-d} g$$

ein Polynom mit $\operatorname{grad} f_1 < n$. Nach Induktionsvoraussetzung existieren q_1, r_1 mit $\operatorname{grad}(r_1) < \operatorname{grad}(g)$ sowie

$$f_1 = q_1 g + r_1.$$

Daraus folgt

$$f = f_1 + b_n a_d^{-1} X^{n-d} g = (q_1 + b_n a_d^{-1} X^{n-d}) g + r_1$$

und wir haben die Existenz von einem passenden $q = q_1 + b_n a_d^{-1} X^{n-d}$ und $r = r_1$ bewiesen.

Nun zur **Eindeutigkeit**: Seien q, r sowie q', r' Polynome mit den gewünschten Eigenschaften und $f = qg + r = q'g + r'$, so ist $r - r' = g(q' - q)$ und damit $\operatorname{grad}(q - q') + d = \operatorname{grad}(r - r') < d$. Das ist aber nur möglich, falls $\operatorname{grad}(q - q') = -\infty$ und damit $q = q'$ und es folgt direkt $r = r'$. ■

Beispiel 3.14 Wir betrachten das Polynom $f = X^5 + 2X^3 + X^2 + X + 1$. Wir führen die Polynomdivision für $g = X^2 + 1$ durch. Wir verfahren wie im Beweis aber führen den Induktionsschritt so lange durch bis das Verfahren endet:

(i) $f_1 = f - X^3(X^2 + 1) = X^3 + X^2 + X + 1$
(ii) $f_2 = f_1 - X(X^2 + 1) = X^2 + 1$
(iii) $f_3 = f_2 - (X^2 + 1) = 0$
(iv) Also ist $r_2 = 0$, $q_2 = 1$, $f_2 = q_2 g$
(v) $r_1 = 0$, $q_1 = q_2 + X = X + 1$,
(vi) $r = 0$, $q = q_1 + X^3 = X^3 + X + 1$ und

$$f = qg = (X^3 + X + 1)(X^2 + 1) = X^5 + 2X^3 + X^2 + X + 1.$$

Beispiel 3.15 Man kann das Verfahren auch genau wie das schriftliche Verfahren zur Polynomdivision durchführen, welches man aus der Schule kennt. Zum Beispiel für $f = X^5 + 2X^2 - X + 3$ und $g = X^2 + 1$ sieht das so aus:

$$\begin{array}{rl} X^5 & +2X^2 - X + 3 = \left(X^2 + 1\right)\left(X^3 - X + 2\right) + 1 \\ \underline{-X^5 - X^3} & \\ -X^3 + 2X^2 - X & \\ \underline{X^3 \qquad + X} & \\ 2X^2 & +3 \\ \underline{-2X^2} & \underline{-2} \\ & 1 \end{array}$$

Hier ist also $q = X^3 - X + 2$ und $r = 1$.

Im Polynomring $K[X]$ über einem Körper kann man die Polynomdivision also stets durchführen. Die Ringe $\mathbb{Z}$ und $K[X]$ sind Beispiele für sogenannte *euklidische Ringe*.

Definition 3.11 Ein Ring R zusammen mit einer Abbildung $\delta : R \setminus \{0\} \to \mathbb{N}_0$ heißt *euklidischer Ring*, falls gilt: zu $f, g \in R$ mit $g \neq 0$ gibt es $q, r \in R$, so dass

$$f = qg + r \text{ und } \delta(r) < \delta(g) \text{ oder } r = 0.$$

Die Abbildung δ wird als *Grad-* oder *Normabbildung* von R bezeichnet.

Bemerkung 3.13 Vorsicht: in einem euklidischen Ring wird die Eindeutigkeit von q und r so wie in den Beispielen **nicht** verlangt.

Beispiel 3.16 Beispiele für euklidische Ringe sind:

(i) Körper (hierbei ist δ beliebig, da stets $r = 0$ gewählt werden kann).
(ii) Die ganzen Zahlen $\mathbb{Z}$ mit $\delta(x) = |x|$;
(iii) Der Polynomring $K[X]$ über einem Körper K mit der Gradabbildung;
(iv) Die Gaußschen ganzen Zahlen $\mathbb{Z}[i] = \{m + ni \mid m, n \in \mathbb{Z}\}$ (siehe Übung). Die Normabbildung ist hier gegeben durch $\delta(m + ni) := m^2 + n^2$.

Die Eigenschaft, ein euklidischer Ring zu sein, ist ziemlich stark, wie auch der folgende Satz zeigt.

Satz 3.6 Jeder euklidische Ring ist ein Hauptidealring.

Beweis. Sei R ein euklidischer Ring und $\mathfrak{a} \subset R$ ein Ideal. Es sei $a \in \mathfrak{a}$ ein Element von minimalem Grad in $\mathfrak{a}$ (jede Teilmenge von $\mathbb{N}_0$ besitzt ein minimales Element, also auch $\delta(\mathfrak{a})$). Natürlich ist $(a) \subset \mathfrak{a}$. Ist nun umgekehrt $b \in \mathfrak{a}$, so gibt es $q, r \in R$ mit $b = qa + r$, wobei $\delta(r) < \delta(a)$ oder $r = 0$. Da jedoch mit a auch qa und somit auch $r = b - qa \in \mathfrak{a}$ ist, muss, aufgrund der Minimalität des Grades von a, schon $r = 0$ gelten und es ist also $b = qa$ und somit $\mathfrak{a} = (a)$. ■

Beispiel 3.17 Die Gaußschen ganzen Zahlen $\mathbb{Z}[i]$ sowie der Polynomring $K[X]$ über einem Körper K sind als euklidische Ringe also Hauptidealringe.

Beispiel 3.18 Ein wichtiges Nicht-Beispiel: Der Polynomring $\mathbb{Z}[X]$ über $\mathbb{Z}$ ist **kein** Hauptidealring (und damit auch nicht euklidisch). Man kann hier die Division mit Rest eben nur für Polynome mit führendem Koeffizienten ± 1 durchführen. Das Ideal $(2, X)$ ist ein Beispiel für ein Ideal, welches **kein** Hauptideal ist. Explizit ist das Ideal $(2, X)$ gegeben durch

$$(2, X) = \{\sum_i a_i X^i \mid a_0 \text{ gerade } \}.$$

Beweis. Angenommen $(2, X) = (f)$ wäre ein Hauptideal. Dann muss es $g, h \in \mathbb{Z}[X]$ geben mit $2 = gf$ und $X = hf$. Es folgt dann aber, dass $\text{grad}(f) = 0$ ist und damit $f = \pm 1$ oder ± 2. Den ersten Fall, $f = \pm 1$ können wir ausschließen, da $1 \notin (2, X)$. Es muss also $f = \pm 2$ sein. Damit hat die Gleichung $X = 2h$ keine Lösung $h \in \mathbb{Z}[X]$ und somit ist $(2, X)$ kein Hauptideal. ■

Im Folgenden beschäftigen wir uns noch mit *Teilbarkeit*, dem *größten gemeinsamen Teiler* sowie dem *kleinsten gemeinsamen Vielfachen*.

Definition 3.12 Sei R ein Integritätsring und $a, b \in R$. Dann sagen wir, dass a das Element b *teilt*, falls es ein $c \in R$ gibt mit $ac = b$ (oder äquivalent $b \in (a)$ gilt). Wir schreiben dann $a \mid b$ und sagen auch, dass a ein *Teiler* von b sei.

Ist dies nicht der Fall, so sagen wir, dass a das Element b *nicht teilt* und schreiben auch $a \nmid b$.

Definition 3.13 Sei R ein Integritätsring und $a_1, \ldots, a_n \in R$.

(i) Ein Element $d \in R$ heißt *größter gemeinsamer Teiler* von $a_1, \ldots, a_n$, falls gilt:
  (a) Es gilt $d \mid a_i$ für alle $i = 1, \ldots, n$ (d ist ein gemeinsamer Teiler der a_i).
  (b) Und ist $d' \in R$ ein anderer gemeinsamer Teiler der a_i, so gilt $d' \mid d$.

(ii) Ein Element $a \in R$ heißt *kleinstes gemeinsames Vielfaches* von $a_1, \ldots, a_n$, falls gilt:
  (a) Es ist $a_i \mid a$ für alle i (a ist gemeinsames Vielfaches der a_i).
  (b) Und ist $a' \in R$ ein anderes Vielfaches aller a_i, so gilt $a \mid a'$.

Bemerkung 3.14
(i) Existiert ein größter gemeinsame Teiler d von $a_1, \ldots, a_n$, so ist er eindeutig bis auf Assoziiertheit. Wir schreiben auch $d = \text{ggT}(a_1, \ldots, a_n)$.
(ii) Existiert ein kleinstes gemeinsames Vielfaches a von $a_1, \ldots, a_n$, so ist es eindeutig bis auf Assoziiertheit. Wir schreiben auch $a = \text{kgV}(a_1, \ldots, a_n)$.

Satz 3.7 Sei R ein Hauptidealring und seien $a_1, \ldots, a_n \in R$. Es gilt folgende Charakterisierung des kgV und des ggT durch Ideale.
(i) Es ist $(a_1, \ldots, a_n) = (\text{ggT}(a_1, \ldots, a_n))$
(ii) und $(a_1) \cap \ldots \cap (a_n) = (\text{kgV}(a_1, \ldots, a_n))$.
Insbesondere existieren ggT und kgV in Hauptidealringen stets.

Beweis. (i) Sei $(a_1, \ldots, a_n) = (d)$ für ein $d \in R$. Dann gibt es zu jedem i ein $x_i \in R$, so dass $a_i = dx_i$ ist, da $a_i \in (a_1, \ldots, a_n)$. Also gilt $d \mid a_i$ für alle i. Sei nun d' irgendein gemeinsamer Teiler von $a_1, \ldots, a_n$.

Da $(a_1,\dots,a_n)=(d)$ gilt, gibt es $y_1,\dots,y_n\in R$ so dass

$$\sum_{i=1}^{n} y_i a_i = d$$

ist. Außerdem existieren also $y_i'\in R$, so dass $d'y_i'=a_i$ gilt und somit ist

$$d=\sum_{i=1}^{n} y_i a_i = \left(\sum_{i=1}^{n} y_i y_i'\right) d',$$

d.h. $d'\mid d$ und somit ist $d=\mathrm{ggT}(a_1,\dots,a_n)$.

(ii) Sei $a\in R$ mit $(a_1)\cap\ldots\cap(a_n)=(a)$. Es ist dann $a\in(a_i)$ für alle i und somit ist a ein gemeinsames Vielfaches der a_i. Ist a' ein weiteres gemeinsames Vielfaches, so gilt $a'\in(a_1)\cap\ldots\cap(a_n)=(a)$ und deshalb gibt es ein $x\in R$ mit $ax=a'$, d.h. $a\mid a'$ und $a=\mathrm{kgV}(a_1,\dots,a_n)$.

■

Bemerkung 3.15 Die Aussage von Satz 3.7 gilt auch allgemeiner in jedem Integritätsring unter der Voraussetzung, dass die betrachteten Ideale Hauptideale sind, denn im Beweis haben wir nur benutzt, dass diese konkreten Ideale Hauptideale sind.

In einem euklidischen Ring existiert stets ein größter gemeinsamer Teiler und der Euklidische Algorithmus liefert ein konstruktives Verfahren, um in zu bestimmen.

Satz 3.8 — Euklidischer Algorithmus. Sei R ein euklidischer Ring mit der Gradabbildung $\delta: R\setminus\{0\}\to\mathbb{N}_0$ und seien $a,b\in R\setminus\{0\}$. Wir definieren die Folge $(c_i)_{i\in\mathbb{N}_0}$ zunächst durch

$$c_0=a,$$
$$c_1=b.$$

Seien nun $c_0,\dots,c_i$ bereits definiert. Falls $c_i\neq 0$, so seien $q_i,r_i\in R$ mit

$$c_{i-1}=q_i c_i+r_i$$

und $\delta(r_i)<\delta(c_i)$. Dann setzen wir $c_{i+1}:=r_i$. Falls jedoch $c_i=0$, so sei $c_{i+1}:=0$.

Es gilt: Es gibt ein kleinstes $n\in\mathbb{N}_0$ mit $c_{n+1}=0$. Ab c_{n+1} ist die Folge also stationär gleich Null. Für dieses n gilt dann, dass c_n ein größter gemeinsamer Teiler von a und b ist, d.h. $c_n=\mathrm{ggT}(a,b)$.

Beweis. Der Beweis ist eine Übung. ■

Beispiel 3.19 Wir berechnen den ggT von $a=105$ und $b=14$. Es ist also

$$c_0=a=105,\quad c_1=b=14.$$

Wir berechnen weiterhin

$$c_0=105=\underbrace{14}_{=c_1}\cdot 7+7 \quad \text{also } q_1=7,\ r_1=7,$$

d.h. $c_2=7$ und

$$c_1=14=\underbrace{7}_{=c_2}\cdot 2+0 \quad \text{also } q_2=2,\ r_2=0,$$

d.h. $c_3=0$. Die Folge ist also gegeben durch $105,14,7,0,0,\dots$ und damit ist der Index n in Satz 3.8 gegeben durch $n=2$ und $c_2=7=\mathrm{ggT}(105,14)$.

3.8 Primfaktorzerlegung, faktorielle Ringe

Wir kommen nun zur Diskussion aus Abschnitt 3.5 zurück.

Definition 3.14 Sei R ein Integritätsring und $p \in R$ mit $p \neq 0$ und $p \notin R^\times$.

(i) Wir nennen p *irreduzibel*, falls für alle $x, y \in R$ mit $p = xy$ gilt, dass $x \in R^\times$ oder $y \in R^\times$ ist; andernfalls heißt p *reduzibel*;

(ii) Wir nennen p *prim* (oder *Primelement*), falls für alle $x, y \in R$ mit $p \mid xy$ gilt, dass $p \mid x$ oder $p \mid y$. Dies ist also äquivalent dazu, dass das von p erzeugte Hauptideal (p) ein Primideal ist.

In diesem Abschnitt behandeln wir die Zerlegung von Elementen in einem Integritätsring in Primfaktoren.

Bemerkung 3.16 Wenn wir im Folgenden von einem Produkt von Elementen sprechen, so meinen wir stets ein **endliches** Produkt.

Satz 3.9 Sei R ein Integritätsring. Die folgenden beiden Bedingungen sind äquivalent:

(i) Jedes $a \in R \setminus \{0\}$ mit $a \notin R^\times$ lässt sich eindeutig (bis auf Assoziiertheit und Reihenfolge der Faktoren) als Produkt von irreduziblen Elementen schreiben.

(ii) Jedes $a \in R \setminus \{0\}$ mit $a \notin R^\times$ lässt sich als Produkt von Primelementen schreiben.

Definition 3.15 Ein Ring in dem die äquivalenten Bedingungen aus Satz 3.9 gelten, heißt *faktoriell*.

Bemerkung 3.17 Wir werden im Beweis von Satz 3.9 sehen, dass in einem faktoriellen Ring irreduzible Elemente stets prim sind. Da die Umkehrung immer gültig ist, sind in einem faktoriellen Ring also die Primelemente genau die irreduzible Elemente.

Bevor wir den Satz beweisen, halten wir noch fest:

Bemerkung 3.18 Im Allgemeinen sind die beiden Eigenschaften irreduzibel und prim *nicht äquivalent*, es gilt jedoch stets: Sei R ein Integritätsring und $p \in R$ ein Primelement. Dann ist p irreduzibel.

Beweis. Angenommen es gilt $p = xy$ mit $x, y \in R$. Dann gilt also (da $1 \cdot p = xy$ ist), dass $p \mid xy$ und damit, da p prim ist, bereits $p \mid x$ oder $p \mid y$. ObdA gelte also $p \mid x$ und es sei $x = ap$ für ein $a \in R$. Dann ist $p = xy = apy = pay$ und somit, nach der Kürzungsregel, $1 = ay$ und damit $y \in R^\times$. Demnach ist also p irreduzibel. ∎

Beispiel 3.20 Wir geben ein Beispiel eines Ringes mit irreduziblen Elementen, die nicht prim sind: Der Ring sei $R = \mathbb{Z}[\sqrt{-5}] = \{x + y\sqrt{-5} \mid x, y \in \mathbb{Z}\}$. In den Übungen zeigen Sie, dass die Elemente $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ alle irreduzibel sind. Klarerweise gilt $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Demnach ist zum Beispiel 2 ein Teiler von $(1 + \sqrt{-5})(1 - \sqrt{-5})$. Es ist aber leicht zu sehen, dass zum Beispiel $2 \nmid 1 + \sqrt{-5}$ und damit ist 2 **nicht** prim in R.

Beweis von Satz 3.9. Es gelte (i). Wir zeigen, dass dann jedes irreduzible Element in R schon prim ist. Sei also $a \in R$ irreduzibel und es seien $x, y \in R$ mit $a \mid xy$. Wir müssen zeigen, dass $a \mid x$ oder $a \mid y$. Ist x oder y eine Einheit, ist die Behauptung trivial. Nehmen wir also an, dass x und y keine Einheiten sind und seien $x = x_1 \cdots x_m$ sowie $y = y_1 \cdots y_n$ die Zerlegungen von x und y in irreduzible Elemente. Es ist also a ein Teiler von $xy = x_1 \cdots x_m \cdot y_1 \cdots y_n$ und damit ist a als irreduzibles Element zu einem der x_i oder einem der y_i assoziiert und damit gilt $a \mid x$ oder $a \mid y$ und a ist ein Primelement. Damit ist dann aber jede Zerlegung eines Elementes $a \in R \setminus \{0\}$ mit $a \notin R^\times$ in irreduzible Elemente bereits eine Zerlegung in Primelemente und es gilt demnach (ii).

Es gelte nun (ii). Da Primelemente nach Bemerkung 3.18 stets irreduzibel sind, müssen wir nur noch die Eindeutigkeit zeigen. Diese folgt aus dem folgenden Lemma 3.1. ∎

Lemma 3.1 Sei R ein Integritätsring. Für $a \in R$ seien $p_1, \ldots, p_r$ Primelemente und $q_1, \ldots, q_s$ irreduzible

Elemente mit

$$a = p_1 \cdots p_r = q_1 \cdots q_s.$$

Dann gilt $r = s$ und jedes p_i ist zu genau einem Faktor q_j assoziiert (nach Umnummerierung können wir annehmen, dass p_i zu q_i assoziiert ist).

Beweis. Wir beweisen die Aussage per Induktion nach r. Sei zunächst $r = 1$. Es gilt $p_1 \mid q_1 \cdots q_s$ und damit gibt es ein j, so dass $p_1 \mid q_j$, da p_1 prim ist. Da jedoch q_j irreduzibel ist, gibt es ein $x \in R^\times$, so dass $xp_1 = q_j$. Daraus folgt, dass

$$1 = q_1' \cdots q_{j-1} \cdot q_{j+1} \cdots q_s$$

und damit muss $s = 1$ gelten und p_1 ist zu q_1 assoziiert.

Der Induktionsschritt geht genauso: aus $p_1 \mid q_1 \cdots q_s$ folgt, dass es ein j gibt, so dass $p_1 \mid q_j$. Da jedoch q_j irreduzibel ist, gibt es ein $x \in R^\times$, so dass $xp_1 = q_j$. Es ist somit

$$p_2 \cdots p_r = q_1' \cdots q_{j-1} \cdot q_{j+1} \cdots q_s$$

mit $q_1' := x^{-1}q_1$. Die Behauptung folgt also aus der Induktionsannahme, denn $a' = p_2 \cdots p_r = q_1' \cdots q_{j-1} \cdot q_{j+1} \cdots q_s$ ist eine Element aus R, für das eine Zerlegung in $r-1$ Primfaktoren und $s-1$ irreduzible Elemente vorliegt. Nach Induktionsannahme ist $r - 1 = s - 1$ sowie p_i zu q_i assoziiert und die Behauptung folgt. ■

Bemerkung 3.19 Lemma 3.1 zeigt insbesondere: Besitzt ein Element $a \in R$ eine Zerlegung in Primelemente, so ist diese Zerlegung stets bis auf Reihenfolge und Assoziiertheit eindeutig, denn Primelemente sind insbesondere irreduzibel, also kann man Lemma 3.1 auf zwei Zerlegungen in Primelemente anwenden.

Bemerkung 3.20 Assoziiertheit von Elementen ist eine Äquivalenzrelation. Sei P ein vollständiges Repräsentantensystem der Primelemente in R bzgl. der Äquivalenzrelation „Assoziiertheit“. Dann lässt sich jedes Element $a \in R \setminus \{0\}$ *eindeutig* als Produkt der Form

$$a = \varepsilon \prod_{p \in P} p^{\nu_p(a)}$$

schreiben, wobei $\varepsilon \in R^\times$ und die Exponenten $\nu_p(a) \in \mathbb{N}_0$ eindeutig bestimmt sind. Da das Produkt endlich ist, sind alle bis auf endlich viele Exponenten $\nu_p(a) = 0$. Falls $a \in R^\times$, so sind alle Exponenten $\nu_p(a) = 0$.

In den ganzen Zahlen $\mathbb{Z}$ ist es zum Beispiel üblich, als P die Menge der Primzahlen (positive Primelemente) zu nehmen.

3.8.1 Im Hauptidealring

Wir haben zuvor in Beispiel 3.20 gesehen, dass irreduzible Elemente nicht unbedingt prim sein müssen. In einem Hauptidealring (wie unserem einleitenden Beispiel $\mathbb{Z}$) fallen die Begriffe irreduzibel und prim jedoch in der Tat immer zusammen.

Satz 3.10 Sei R ein Hauptidealring und $p \in R \setminus \{0\}$ mit $p \notin R^\times$. Die folgenden Aussagen sind äquivalent:

(i) Das Element p ist irreduzibel.
(ii) Das Element p ist prim (oder: das Hauptideal (p) ist prim).
(iii) Das Hauptideal (p) ist maximal.

Beweis. Die Implikation (iii) $\Rightarrow$ (ii) ist einfach: Ist (p) ein maximales Ideal, so ist (p) auch ein Primideal und damit p ein Primelement.

(ii) $\Rightarrow$ (i) ist der Inhalt von Bemerkung 3.18.

Es bleibt also (i) $\Rightarrow$ (iii) zu zeigen. Es sei also p irreduzibel. Sei also $\mathfrak{a}$ ein Ideal mit $(p) \subset \mathfrak{a} \subset R$. Da R ein Hauptidealring ist gibt es ein $a \in R$ mit $\mathfrak{a} = (a)$. Ist a eine Einheit, so gilt $(a) = R$.

Sei also a keine Einheit. Da aber $p \in (a)$ ist, gilt $p = xa$ für ein $x \in R$. Da a keine Einheit ist, muss nun x eine Einheit sein, da p irreduzibel ist und damit gilt nun $(p) = (a)$. Damit ist gezeigt, dass (p) maximal ist. ■

Wir wollen nun zeigen, dass Hauptidealringe auch faktoriell sind. Dazu ist es günstig, eine etwas allgemeinere Aussage zu zeigen.

Definition 3.16 Ein Ring R heißt *noethersch*, falls jede aufsteigende Kette von Idealen $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset R$ stationär wird, d.h. es existiert $n \in \mathbb{N}$, so dass $\mathfrak{a}_i = \mathfrak{a}_n$ für alle $i \geq n$ ist.

Lemma 3.2 Sei R ein noetherscher Integritätsring. Dann kann man jedes Element in $a \in R \setminus \{0\}$ mit $a \notin R^\times$ als endliches Produkt von irreduziblen Elementen schreiben.

Beweis. Sei $a \in R \setminus \{0\}$ mit $a \notin R^\times$. Wir nehmen an, a kann nicht als Produkt von irreduziblen Elementen geschrieben werden. Damit ist a insbesondere nicht selbst irreduzibel.

Da a nicht irreduzibel ist, existieren $a_1, b_1 \in R \setminus \{0\}$, so dass $a = a_1 b_1$ und $a_1, b_1 \notin R^\times$. Dies liefert eine echte Inklusion von Idealen $(a) \subsetneq (a_1)$.

Da a nicht als Produkt von irreduziblen Elementen geschrieben werden kann, kann auch einer der Faktoren a_1 oder b_1 nicht als Produkt von irreduziblen Elementen geschrieben werden. OBdA sei dieser Faktor a_1. Dann kann a_1 wieder nicht irreduzibel sein und wir erhalten Elemente $a_2, b_2 \in R \setminus \{0\}$ mit $a_2, b_2 \notin R^\times$ und $a_1 = a_2 b_2$. Dies liefert eine echte Inklusion von Idealen $(a) \subsetneq (a_1) \subsetneq (a_2)$.

Wieder können wir annehmen, dass a_2 nicht als Produkt von irreduziblen Elementen geschrieben werden kann. Wir erhalten also induktiv eine unendliche, (echt) aufsteigende Kette von Idealen $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \ldots$. Da R noethersch ist, kann es eine solche (unendliche) echt aufsteigende Kette von Idealen jedoch nicht geben und somit kann es ein solches a auch nicht geben. ■

Satz 3.11 Jeder Hauptidealring ist noethersch.

Beweis. Sei R ein Hauptidealring und $\mathfrak{a}_1 = (a_1) \subset \mathfrak{a}_2 = (a_2) \subset \ldots \subset R$ eine aufsteigende Kette von Idealen in R. Wir können die Vereinigung

$$\mathfrak{a} := \bigcup_{i=1}^{\infty} \mathfrak{a}_i$$

bilden. Diese ist wieder ein Ideal in R und somit existiert ein $a \in R$ mit $\mathfrak{a} = (a)$.

Da jedoch a selbst ein Element von $\mathfrak{a}$ ist, gibt es also ein $n \in \mathbb{N}$, so dass $a \in \mathfrak{a}_n = (a_n)$ ist. Damit ist dann aber $a \in \mathfrak{a}_i$ für alle $i \geq n$ und somit $(a) = \mathfrak{a}_i$, woraus die Behauptung folgt. ■

Damit erhalten wir nun relativ leicht:

Korollar 3.3 Jeder Hauptidealring ist faktoriell.

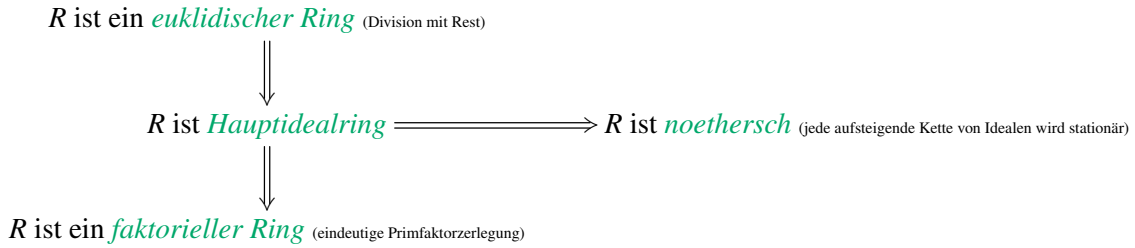
Beweis. Da in Hauptidealringen Primelemente und irreduzible Eemente zusammenfallen (Satz 3.10), müssen wir, um die Bedingung (ii) in Satz 3.9 zu erhalten, nur zeigen, dass jedes Element aus $R \setminus (\{0\} \cup R^\times)$ als Produkt von irreduziblen Elementen geschrieben werden kann. Da Hauptidealringe noethersch sind (Satz 3.11) folgt dies aus Lemma 3.2. ■

Bemerkung 3.21 Eine Ergänzung zu Beispiel 3.20: Man kann zeigen, dass der Ring $R = \mathbb{Z}[\sqrt{-5}]$ noethersch ist. Nach Lemma 3.2 kann man also jede von Null verschiedene Nichteinheit in R in ein Produkt von irreduziblen Elementen zerlegen. Wie wir gesehen haben, ist eine solche Zerlegung in R jedoch nicht eindeutig.

3.9 Übersicht

Es ist an der Zeit, die Struktur einiger neuer Begriffe aus diesem Kapitel fest zu halten.

Sei R ein Integritätsring. Dann gelten die folgenden Implikationen:



3.10 Quotientenkörper

Sei R ein faktorieller Ring. Wir betrachten die Menge $X := \{(a,b) \mid a \in R, b \in R \setminus \{0\}\}$. Die Relation

$$(a,b) \sim (a',b') \Leftrightarrow ab' = a'b$$

definiert eine Äquivalenzrelation auf X. Dies ist leicht nachzurechnen (man muss benutzen, dass R ein Integritätsring ist).

Sei $Q(R) = X/\sim$ die Menge der Äquivalenzklassen. Wir schreiben die Äqivalenzklasse von (a,b) als Bruch

$$\frac{a}{b}.$$

Auf $Q(R)$ führen wir zwei Verknüpfungen ein:

(i) Die Addition:

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}$$

(ii) Die Multiplikation

$$\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}.$$

Es ist leicht zu zeigen, dass wir so einen Körper erhalten (Übung).

Definition 3.17 Der Körper $Q(R)$ wird Quotientenkörper von R genannt.

Bemerkung 3.22 Wir erhalten einen injektiven Ringhomomorphismus

$$R \to Q(R), \quad a \mapsto \frac{a}{1},$$

wodurch wir R als Unterring von $Q(R)$ auffassen können.

Beispiel 3.21 (i) Es ist $Q(\mathbb{Z}) = \mathbb{Q}$.

(ii) Ist K ein Körper, so wird der Körper $K(X) := Q(K[X])$ als *Körper der rationalen Funktionen* in einer Variablen und Koeffizienten in K bezeichnet.

Bemerkung 3.23 Sei R ein faktorieller Ring und P ein Repräsentantensystem der Primelemente von R (bzgl. Assoziiertheit). Dann lässt sich jedes Element $x = \frac{a}{b} \in Q(R)^\times$ eindeutig schreiben als

$$x = \frac{a}{b} = \varepsilon \prod_{p \in P} p^{\nu_p(x)},$$

wobei $\varepsilon \in R^\times$ und $\nu_p(x) \in \mathbb{Z}$ mit $\nu_p(x) = 0$ für fast alle p ist. Insbesondere: $x \in R$ genau dann, wenn $\nu_p(x) \geq 0$ für alle $p \in P$.

3.11 Primfaktorzerlegung in $R[X]$

In diesem Abschnitt sei stets R ein faktorieller Ring und P ein Repräsentantensystem der Primelemente in R. Wir erweitern die Definition der Funktionen $\nu_p(x)$ aus Bemerkung 3.23 auf $x = 0$ durch $\nu_p(0) = \infty$ für alle p und auf Polynome $f = \sum_i a_i X^i \in Q(R)[X]$ durch

$$\nu_p(f) := \min_i \nu_p(a_i).$$

Bemerkung 3.24 (i) Für $f \in Q(R)[X]$ ist $\nu_p(f) = \infty$ äquivalent zu $f = 0$.
(ii) Es ist $f \in R[X]$ genau dann, wenn $\nu_p(f) \geq 0$ für alle $p \in P$ gilt.

Lemma 3.3 Sei R ein faktorieller Ring und $p \in R$ ein Primelement. Sei $pR = (p) \subset R$ das von p erzeugte Hauptideal in R und $\pi : R \to R/pR$ die kanonische Projektion. Dann definieren wir eine Abbildung „Reduktion modulo p“:

$$\varphi : R[X] \to (R/pR)[X],$$

gegeben durch

$$f = \sum_i a_i X^i \mapsto \sum_i \pi(a_i) X^i.$$

Diese Abbildung ist ein Ringhomomorphismus und es gilt $\operatorname{Kern}(\varphi) = \{f \in R[X] \mid \nu_p(f) > 0\} = pR[X]$. Insbesondere ist auch $R[X]/pR[X] \cong (R/pR)[X]$.

Beweis. Man kann leicht nachrechnen, dass es sich um einen Ringhomomorphismus handelt.

Es ist $\varphi(f) = 0$ genau dann, wenn $\pi(a_i) = 0$ für alle i und dies ist äquivalent zu $\nu_p(a_i) > 0$ für alle i. Damit ist die Behauptung bewiesen. ■

Lemma 3.4 — Lemma von Gauß. Sei R ein faktorieller Ring und $p \in R$ ein Primelement. Dann gilt für $f, g \in Q(R)[X]$:

$$\nu_p(fg) = \nu_p(f) + \nu_p(g).$$

Beweis. Für $f, g \in Q(R)$ folgt dies direkt aus der Primfaktorzerlegung in R. Weiterhin: ist $f \in Q(R)$ und $g \in Q(R)[X]$, so ist die Aussage ebenfalls klar, da man in diesem Falle für $g = \sum_i a_i X^i$ errechnet, dass

$$\nu_p(fg) = \min_i \nu_p(f a_i) = \nu_p(f) + \min_i \nu_p(a_i) = \nu_p(f) + \nu_p(g)$$

gilt.

Wir nehmen nun an, dass $f, g \neq 0$ seien und durch Multiplikation mit $a \in Q(R)^\times$ können wir auch annehmen, dass $f, g \in R[X]$ seien mit $\nu_p(f) = \nu_p(g) = 0$ (man multipliziere f bzw. g mit einem kgV der Nenner der Koeffizienten von f bzw. g und teile durch einen ggT der Zähler).

Es ist zu zeigen, dass $\nu_p(fg) = 0$ gilt.

Dazu betrachten wir den Homomorphismus φ „Reduktion modulo p“ aus Lemma 3.3:

$$\varphi : R[X] \to (R/pR)[X].$$

Aus $\operatorname{Kern} \varphi = \{f \in R[X] \mid \nu_p(f) > 0\}$ folgt $\varphi(f), \varphi(g) \neq 0$.

Da R/pR und damit auch $(R/pR)[X]$ Integritätsringe sind gilt $\varphi(fg) = \varphi(f)\varphi(g) \neq 0$. Daraus folgt $\nu_p(fg) = 0$ wie behauptet. ■

Korollar 3.4 Sei R ein faktorieller Ring und $h \in R[X]$ normiert. Falls $h = fg$ für normierte Polynome $f, g \in Q(R)[X]$ gilt, so sind bereits $f, g \in R[X]$.

Definition 3.18 Seien R ein faktorieller Ring und $f \in R[X]$. Dann heißt f *primitiv*, falls $\nu_p(f) = 0$ für alle Primelemente $p \in R$ gilt.

Bemerkung 3.25 Seien R faktoriell und $f \in Q(R)[X]$. Dann gibt es ein $a \in Q(R)^\times$, so dass $f = a\tilde{f}$ gilt und $\tilde{f} \in R[X]$ primitiv ist.

Beweis. Nehme

$$a = \prod_{p \in P} p^{\nu_p(f)} \neq 0$$

und $\tilde{f} = a^{-1} f$. Da $\nu_p(\tilde{f}) = 0$ für alle p gilt, ist $\tilde{f} \in R[X]$. ■

Satz 3.12 — Satz von Gauß. Sei R ein faktorieller Ring. Dann ist auch $R[X]$ faktoriell. Die Primelemente in $R[X]$ sind gegeben durch
(i) Die Primelemente in R
(ii) und die primitiven Polynome in $R[X]$, welche prim in $Q(R)[X]$ sind.
Insbesondere ist ein primitives Polynom $q \in R[X]$ genau dann prim in $R[X]$, wenn es prim in $Q(R)[X]$ ist.

Beweis. Ist $q \in R$ prim, so ist R/qR ein Integritätsring. Damit ist auch der Polynomring $(R/qR)[X]$ ein Integritätsring und da $(R/qR)[X] \cong R[X]/qR[X]$ ist (Lemma 3.3), ist $q \in R[X]$ ein Primelement.

Sei nun $q \in R[X]$ primitiv und prim in $Q(R)[X]$. Weiterhin seien $f, g \in R[X]$ mit $q \mid fg$. Da q in $Q(R)[X]$ prim ist, gilt $q \mid f$ oder $q \mid g$ in $Q(R)[X]$. OBdA gelte $q \mid f$ in $Q(R)[X]$ und es sei $h \in Q(R)[X]$ mit $f = qh$. Es ist dann

$$0 \leq \nu_p(f) = \nu_p(qh) = \nu_p(q) + \nu_p(h) = \nu_p(h),$$

nach dem Lemma von Gauß und wegen der Primitivität von q. Daraus folgt aber $h \in R[X]$ und damit $q \mid f$ in $R[X]$.

Um zu zeigen, dass $R[X]$ faktoriell ist und die angegebenen Elemente die einzigen Primelemente in $R[X]$ sind, reicht es zu zeigen, dass sich jede von Null verschiedene Nichteinheit in $R[X]$ als Produkt von Primelementen vom Typ (i) und (ii) schreiben lässt.

Dazu sei $f \in R[X]$ und $f \neq 0$ sowie $f \notin R^\times$. Wir schreiben $f = a\tilde{f}$, wobei $a \in R$ und $\tilde{f}$ primitiv ist (a ist der ggT der Koeffizienten von f).

Da $Q(R)[X]$ als Polynomring über einem Körper ein Hauptidealring ist, können wir f in $Q(R)[X]$ als Produkt von Primelementen schreiben:

$$\tilde{f} = \varepsilon f_1 \cdots f_r,$$

wobei $f_1, \ldots, f_r$ primitive Polynome sind, welche in $Q(R)[X]$ prim sind und $\varepsilon \in Q(R)^\times$ (man beachte Bemerkung 3.25). Die Faktoren $f_1, \ldots, f_r$ sind dann aber bereits Primelemente in $R[X]$. Weiterhin gilt nach dem Lemma von Gauß, dass

$$0 = \nu_p(\tilde{f}) = \nu_p(\varepsilon) + \nu_p(f_1) + \ldots + \nu_p(f_r) = \nu_p(\varepsilon),$$

womit $\varepsilon \in R^\times$ gilt. Damit erhält man die Primfaktorzerlegung von f aus der Primfaktorzerlegung von $a \in R$ und der Primfaktorzerlegung $\tilde{f} = \varepsilon f_1 \cdots f_r$, welche nur aus Elementen des angegebenen Typs besteht. ■

3.12 Irreduzibilitätskriterien

In diesem Abschnitt sei R ein faktorieller Ring und $K = Q(R)$ sein Quotientenkörper. Wir geben zwei gängige Kriterien an, mit denen man bestimmen kann, ob ein Polynom $f \in K[X] \setminus \{0\}$ irreduzibel ist. Nach dem Satz von Gauß kann man dabei so vorgehen: es sei $c \in K$, so dass $\tilde{f} = cf \in R[X]$ primitiv ist. Dann ist f genau dann irreduzibel in $K[X]$, wenn $\tilde{f}$ irreduzibel in $R[X]$ ist (bzw. prim, da $R[X]$ und $K[X]$ faktoriell sind). Wir bezeichnen wieder mit

$$\varphi_p : R[X] \to R/pR[X]$$

den kanonischen Homomorphismus „Reduktion der Koeffizienten modulo p“.

Satz 3.13 — Eisenstein-Kriterium. Sei R ein faktorieller Ring und $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ ein primitives Polynom vom Grad $n > 0$. Angenommen, $p \in R$ sei ein Primelement mit

$$p \nmid a_n, \quad p \mid a_i \text{ für } i < n, \text{ aber } p^2 \nmid a_0.$$

Dann ist f irreduzibel in $R[X]$ und somit auch in $K[X]$.

Beweis. Unter den gegebenen Voraussetzungen ist $\varphi_p(f) = \varphi_p(a_n)X^n$. Angenommen, es sei $f = gh \in R[X]$ reduzibel mit $\operatorname{grad}(g), \operatorname{grad}(h) > 0$, dann ist also $\varphi_p(a_n)X^n = \varphi_p(f) = \varphi_p(gh) = \varphi_p(g)\varphi_p(h)$. Damit f (ein primitives Polynom) reduzibel sein kann, muss $\operatorname{grad}(f) = n \geq 2$ gelten. Da $p \nmid a_n$, also $\varphi_p(a_n) \neq 0$ ist, gilt $\operatorname{grad}(\varphi_p(g)) = \operatorname{grad}(g), \operatorname{grad}(\varphi_p(h)) = \operatorname{grad}(h) > 0$. Denn wäre der führende Koeffizient von g oder h durch p teilbar, so wäre auch a_n durch p teilbar. Ist $k = Q(R/pR)$ der Quotientenkörper von R/pR, so ist der Polynomring $k[X]$ als euklidischer Ring faktoriell. Damit ist dann aber klar, dass $\varphi_p(g) = aX^k$ und $\varphi_p(h) = bX^\ell$ sein müssen mit $a, b \in R/pR$ und $k, \ell > 0$. Damit folgt aber, dass jeweils der konstante Koeffizient von g und h durch p teilbar ist und damit a_0 durch p^2 teilbar sein muss, was im Widerspruch zu unserer Annahme steht. ■

Ganz ähnlich beweist man das Reduktionskriterium:

Satz 3.14 — Reduktionskriterium. Sei R ein faktorieller Ring, $p \in R$ ein Primelement und $0 \neq f = \sum_{i=0}^{n} a_i X^i \in R[X]$ mit $p \nmid a_n$. Falls $\varphi_p(f)$ irreduzibel in $R/(p)[X]$ ist, so ist f irreduzibel in $Q(R)[X]$. Ist f zusätzlich primitiv, so ist f auch in $R[X]$ irreduzibel.

Beweis. Sei $f \in R[X]$ zunächst primitiv. Angenommen, f sei reduzibel in $R[X]$, z.B. $f = gh$ mit $g, h \in R[X]$ und $\operatorname{grad}(g), \operatorname{grad}(h) > 0$. Wie bereits eben fest gestellt kann dann aber, da $p \nmid a_n$ angenommen wurde, p nicht den höchsten Koeffizienten von g bzw. h teilen. Da $\varphi_p(f) = \varphi_p(g)\varphi_p(h)$ gilt, ist dies eine Zerlegung von f in $R/(p)[X]$ wobei also $\operatorname{grad} \varphi_p(g), \varphi_p(h) > 0$ gilt. Damit ist $\varphi_p(f)$ nicht irreduzibel und die Behauptung ist in diesem Falle gezeigt.

Ist f nicht primitiv, so schreiben wir wieder $f = c\tilde{f}$, wobei $c \in K$ sei und $\tilde{f} \in R[X]$ primitiv ist. Auf $\tilde{f}$ können wir die Argumentation von eben anwenden. Nach dem Satz von Gauß (Satz 3.12) gilt: ist das primitive Polynom $\tilde{f} \in R[X]$ irreduzibel, so ist $\tilde{f}$ auch in $K[X]$ irreduzibel. Und in $K[X]$ ist $\tilde{f}$ genau dann irreduzibel, wenn f irreduzibel ist. ■

Beispiel 3.22 Die p-ten Einheitswurzeln sind die Nullstellen des Polynoms $f(X) = X^p - 1 \in \mathbb{Z}[X]$. Dieses Polynom ist jedoch ganz sicher nicht irreduzibel, denn $f(1) = 0$. Wir berechnen

$$g(X) := \frac{f(X)}{X-1} = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \ldots + X^1 + 1.$$

Wir können das Eisentein-Kriterium nicht direkt auf $g \in \mathbb{Z}[X]$ anwenden. Es ist jedoch $g(X)$ genau dann irreduzibel in $\mathbb{Z}[X]$, wenn $g(X+1)$ irreduzibel ist (der Einsetzungshomomorphismus $X \mapsto X+1$ ist ein Isomorphismus). Wir erhalten

$$g(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \sum_{j=1}^{p-1} \binom{p}{j} X^{j-1}.$$

Wir erinnern uns, dass für $j \geq 1$ gilt, dass $p \mid \binom{p}{j}$ und $\binom{p}{1} = p$ gilt, so dass der 0-te Koeffizient von $g(X+1)$ zwar durch p, aber nicht durch p^2 teilbar ist. Damit ist $g(X+1)$ und somit auch $g(X)$ nach dem Eisenstein-Kriterium irreduzibel.

3.13 Polynomringe in mehreren Variablen[1]

Analog zum Polynomring $R[X]$ in einer Variablen, kann man den Polynomring $R[X_1,\dots,X_n]$ in mehreren Variablen durch Iteration konstruieren:

$$R[X_1,\dots,X_n] := (\dots((R[X_1])[X_2])[X_3]\dots)[X_n].$$

Also zum Beispiel $R[X,Y] := (R[X])[Y]$. Deutlich allgemeiner kann man auch für einen kommutativen Monoiden M den Polynomring $R[M]$ wie folgt definieren:

$$R[M] := \{(a_\mu)_{\mu\in M} \mid a_\mu = 0 \text{ für alle bis auf endlich viele } \mu\}.$$

Dies ist also wieder die Menge aller Abbildungen $a : M \to R$, so dass $a(\mu) = 0$ für fast alle $\mu \in M$.

Die Verknüpfungen $+$ und $\cdot$ sind analog zu einer Variablen wie folgt definiert:

$$(a_\mu)_{\mu\in M} + (b_\mu)_{\mu\in M} := (a_\mu + b_\mu)_{\mu\in M}$$

sowie

$$(a_\mu)_{\mu\in M} \cdot (b_\mu)_{\mu\in M} := (c_\mu)_{\mu\in M}$$

mit

$$c_\mu := \sum_{\lambda+\nu=\mu} a_\lambda \cdot b_\nu.$$

Hierdurch wird $R[M]$ ein Ring.

Beispiel 3.23 (i) Für $M = \mathbb{N}_0$ erhalten wir $R[\mathbb{N}_0] = R[X]$.
(ii) Für $M = \mathbb{N}_0^n$ erhalten wir $R[\mathbb{N}_0^n] \cong R[X_1,\dots,X_n]$.

Wir halten an dieser Stelle nur folgenden einfachen Satz fest, dessen Beweis eine Übung ist.

Satz 3.15 Ist R ein Integritätsring, so auch der Polynomring $R[X_1,\dots,X_n]$ und es gilt $R[X_1,\dots,X_n]^\times = R^\times$.

[1] In der Vorlesung vorerst übersprungen.

4. Körpererweiterungen

In diesem Kapitel kommen wir darauf zurück, die Lösungen von algebraischen Gleichungen zu studieren. Ist L ein Körper und K ein Teilkörper, so nennt man das Paar $K \subset L$ eine Körpererweiterung. Der Zusammenhang zu algebraischen Gleichungen ergibt sich so: Angenommen $K = \mathbb{Q}$ und es sei $f \in \mathbb{Q}[X]$ ein Polynom. Ist dann $\alpha \in \mathbb{C}$ eine Nullstelle von f, so kann man den Unterring

$$\mathbb{Q}[\alpha] = \{g(\alpha) \mid g \in \mathbb{Q}[X]\} \subset \mathbb{C}$$

betrachten. Dies ist der kleinste Unterring von $\mathbb{C}$, in dem α enthalten ist und es handelt sich um das Bild des Einsetzungshomomorphismus $\phi_\alpha : \mathbb{Q}[X] \to \mathbb{C}, \quad g \mapsto g(\alpha)$. Es handelt sich bei $\mathbb{Q}[\alpha]$ sogar um einen Körper, denn $\mathbb{Q}[X]$ ist ein Hauptidealring und ist $\mathrm{Kern}(\phi_\alpha) = (q)$, so muss q ein Primelement sein, denn $\mathbb{Q}[\alpha] = \mathrm{Bild}(\phi_\alpha) \subset \mathbb{C}$ ist ein Integritätsring. Damit ist aber das von q erzeugte Hauptideal nach 3.10 schon maximal und somit $\mathbb{Q}[\alpha] \cong \mathbb{Q}[X]/(q)$ ein Körper. Wir schreiben deshalb auch $\mathbb{Q}(\alpha)$ anstatt $\mathbb{Q}[\alpha]$ (weil $\mathbb{Q}(\alpha)$ somit auch das Bild unter dem Einsetzungshomomorphismus vom Körper $\mathbb{Q}(X)$ der rationalen Funktionen ist). Man sagt in dieser Situation, dass $\mathbb{Q}(\alpha)$ aus $\mathbb{Q}$ durch *Adjunktion* der Nullstelle α von f entsteht.

4.1 Primkörper

Wir erinnern an die Definition der Charakteristik eines Körpers (siehe auch H26).

Definition 4.1 Sei K ein Körper und $\varphi : \mathbb{Z} \to K$ der eindeutig bestimmte Ringhomomorphismus von $\mathbb{Z}$ nach K (gegeben durch $n \mapsto n \cdot 1$). Sei $p \in \mathbb{N}_0$ ein Erzeuger des Hauptideals $\mathrm{Kern}(\varphi) = (p)$. Die Zahl p wird die *Charakteristik* von K genannt (schreibe $\mathrm{Char}(K) = p$).

Bemerkung 4.1 Die Charakteristik eines Körpers (oder allgemeiner eines Integritätsringes) ist entweder gleich 0 oder eine Primzahl.

Definition 4.2 Sei K ein Körper. Der *Primkörper* P von K ist der kleinste Unterkörper von K, also

$$P = \bigcap_{L \subset K \text{ Teilkörper}} L.$$

Satz 4.1 Sei K ein Körper mit Primkörper P.
(i) Es ist $\mathrm{Char}(K) = p > 0$ genau dann, wenn $P = \mathbb{F}_p$ ist.
(ii) Es ist $\mathrm{Char}(K) = 0$ genau dann, wenn $P = \mathbb{Q}$ ist.

Beweis. Die eine Richtung („⇐“) folgt direkt, da $\mathrm{Char}(P) = \mathrm{Char}(K)$ ist und $\mathrm{Char}(\mathbb{F}_p) = p$ sowie $\mathrm{Char}(\mathbb{Q}) = 0$ gilt.

Zur Implikation „⇒“: Wir halten zunächst fest, dass $\mathrm{Bild}(\varphi)$ der kleinste Unterring von K ist.

Falls der Homomorphismus $\varphi : \mathbb{Z} \to K$ injektiv ist, erhalten wir, dass $\varphi(\mathbb{Z}) \subset K$ ein zu $\mathbb{Z}$ isomorpher Teilring von K ist. Da zu jedem $0 \neq n \in \varphi(\mathbb{Z})$ ein multiplikatives Inverses $n^{-1} \in K$ existieren muss, erhalten wir eine Fortsetzung $\tilde{\varphi} : \mathbb{Q} \to K$ von φ gegeben durch $\frac{m}{n} \mapsto \varphi(m)\varphi(n)^{-1}$, welche immernoch injektiv ist und deren Bild $P = \tilde{\varphi}(\mathbb{Q}) \cong \mathbb{Q}$ der kleinste Teilkörper von K sein muss.

Falls $\operatorname{Kern}\varphi = (p)$ für eine Primzahl p ist, so ist $\mathrm{Bild}(\varphi) \subset K$ isomorph zu $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ nach dem Homomorphiesatz. Dieser Teilkörper ($\mathrm{Bild}(\varphi)$) ist auch der kleinste Teilkörper von K ■

4.2 Algebraische Körpererweiterungen

Definition 4.3 Eine *Körpererweiterung* ist ein Paar von Körpern K und L, wobei $K \subset L$ ein Teilkörper von L sei. Der Körper L heißt auch ein Erweiterungskörper von K. Wir schreiben auch L/K für die Körpererweiterung $K \subset L$.

Bemerkung 4.2 Etwas allgemeiner sprechen wir auch von einer Körpererweiterung, wenn K und L Körper sind und $\iota : K \hookrightarrow L$ ein Homomorphismus (von Körpern, der ja automatisch injektiv ist und damit kann man K mit dem Bild $\iota(K) \subset L$ identifizieren).

Bemerkung 4.3 Ist $K \subset L$ eine Körpererweiterung, so können wir L als Vektorraum über K auffassen; dazu schränkt man die Multiplikation $L \times L \to L$ auf $K \times L \to L$ ein, um eine Skalarmultiplikation zu erhalten.

Definition 4.4 Ist $K \subset L$ eine Körpererweiterung, so bezeichnen wir die Dimension $[L : K] := \dim_K L$ als den *Grad* von L über K.

Ist $[L : K]$ endlich, so heißt die Körpererweiterung $K \subset L$ *endlich* und ansonsten heißt sie *unendlich*.

Satz 4.2 — Gradsatz. Es seien $K \subset L \subset M$ Körpererweiterungen. Dann gilt für den Grad von M über K die Formel

$$[M : K] = [M : L] \cdot [L : K].$$

Falls einer der Grade unendlich ist, so ist die Gleichung so zu verstehen, dass $[M : K]$ unendlich ist genau dann, wenn mindestens einer der Grade $[M : L]$ oder $[L : K]$ unendlich ist.

Beweis. Falls $[M : L] = m \in \mathbb{N}$ und $[L : K] = n \in \mathbb{N}$ ist, so seien

$$v_1, \ldots, v_m \in M$$

und

$$w_1, \ldots, w_n \in L$$

jeweils Basen von M/L bzw. L/K.

Wir behaupten, dass dann die Produkte $w_1v_1, \ldots, w_nv_m$ eine Basis von M/K bilden. Klar ist, dass diese ein Erzeugendensystem bilden, denn ist $x \in M$, so können wir x schreiben als

$$x = \sum_{i=1}^{m} a_i v_i$$

mit $a_i \in L$. Jedes $a_i \in L$ lässt sich wiederum schreiben als

$$a_i = \sum_{j=1}^{n} b_{ij} w_j,$$

mit $b_{ij} \in K$, so dass

$$x = \sum_{i=1}^{m} \sum_{j=1}^{n} b_{ij} v_i w_j$$

ist.

Lineare Unabhängigkeit sieht man ähnlich: sind $b_{ij} \in K$ mit

$$0 = \sum_{i,j} b_{ij} v_i w_j = \sum_{i=1}^{m} (\sum_{j=1}^{n} b_{ij} w_j) v_i,$$

so folgert man, dass zunächst

$$\sum_{j=1}^{n} b_{ij} w_j = 0$$

sein muss für alle i, woraus $b_{ij} = 0$ für alle i, j folgt, da die w_j und v_i jeweils Basen sind.

Ist eine der Erweiterungen L/K oder M/L unendlich, so sieht man mit dem gleichen Argument ein, dass M/K unendlich sein muss (denn zu je r über L linear unabhängigen Elementen $x_1, \ldots, x_r \in M$ und s über K linear unabhängigen Elementen $y_1, \ldots, y_s \in L$, erhält man stets rs über K linear unabhängige Elemente $x_i y_j \in M$). ■

Beispiel 4.1 Zwei Beispiele für Körpererweiterungen, die wir gut kennen sind:

(i) Die Erweiterung $\mathbb{Q} \subset \mathbb{R}$ ist unendlich (denn ein endlich-dimensionaler Vektorraum über $\mathbb{Q}$ ist abzählbar, $\mathbb{R}$ ist aber überabzählbar).

(ii) Die Erweiterung $\mathbb{R} \subset \mathbb{C}$ hat Grad $[\mathbb{C} : \mathbb{R}] = 2$, denn eine Basis ist gegeben durch 1 und i.

(iii) Außerdem gilt $[L : K] = 1$ genau dann, wenn $K = L$ gilt.

Wir erinnern an dieser Stelle erneut an den Einsetzungshomomorphismus: Sei L/K eine Körpererweiterung und $\alpha \in L$, dann ist der zugehörige Einsetzungshomomorphismus definiert als

$$\begin{aligned} \phi_\alpha : K[X] &\to L \\ f = \sum_i a_i X^i &\mapsto f(\alpha) := \sum_i a_i \alpha^i. \end{aligned}$$

Definition 4.5 Sei L/K eine Körpererweiterung und $\alpha \in L$. Dann heißt α *algebraisch (über K)*, falls es ein $0 \neq f \in K[X]$ gibt mit $f(\alpha) = 0$. Andernfalls nennt man α *transzendent* über K. Die Erweiterung L/K heißt *algebraisch*, falls alle Elemente aus L algebraisch über K sind.

Beispiel 4.2 (i) $i \in \mathbb{C}$ ist algebraisch über $\mathbb{Q}$, denn i ist Nullstelle von $X^2 + 1 \in \mathbb{Q}[X]$.

(ii) $\zeta_n := e^{\frac{2\pi i}{n}}$ mit $n \in \mathbb{N}$ ist algebraisch über $\mathbb{Q}$, denn ζ_n ist Nullstelle von $X^n - 1 \in \mathbb{Q}[X]$.

Bemerkung 4.4 Sei L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K. Dann existiert ein eindeutig bestimmtes normiertes Polynom $f \in K[X] \setminus \{0\}$ minimalen Grades, so dass $f(\alpha) = 0$ ist.

Beweis. Der Polynomring $K[X]$ ist ein Hauptidealring. Sei $\mathrm{Kern}(\phi_\alpha) = (f)$ mit $g \in K[X]$ und $f \neq 0$, sowie $\mathrm{grad}(f) \geq 1$, da α algebraisch ist. Wir können annehmen, dass f normiert ist und damit ist f eindeutig bestimmt, denn je zwei Erzeuger des Hauptideals (f) sind assoziiert und die Einheiten in $K[X]$ sind nur die Einheiten $K^\times$ aus K. Der Grad von f ist offenbar minimal, wie gefordert. ■

Definition 4.6 Das Polynom in Bemerkung 4.4 wird *Minimalpolynom* von $\alpha \in L$ über K genannt.

Satz 4.3 Sei L/K eine Körpererweiterung und $\alpha \in L$ algebraisch mit Minimalpolynom f über K. Es gelten:

(i) Das Minimalpolynom $f \in K[X]$ ist irreduzibel.

(ii) Der Ring $K[\alpha] = \{g(\alpha) \mid g \in K[X]\} \subset L$ ist ein Körper (wir schreiben auch $K(\alpha) = K[\alpha]$ für diesen

Körper, siehe auch Definition 4.7). Die Körpererweiterung $K \subset K(\alpha)$ ist endlich und ihr Grad ist

$$[K(\alpha) : K] = \text{grad}(f).$$

Beweis. (i) Es gilt $\text{Kern}(\phi_\alpha) = (f)$ für den Einsetzungshomomorphismus ϕ_α, wie oben gesehen. Der Ring $K[\alpha]$ ist nach dem Homomorphiesatz (Korollar 3.1) isomorph zu $K[X]/(f)$ und als Teilring des Körpers L ein Integritätsring. Damit ist (f) ein Primideal und somit f ein Primelement. Damit ist f auch irreduzibel.

(ii) Da $K[X]$ ein Hauptidealring ist, ist (f) als Primideal aber auch schon ein maximales Ideal (nach Satz 3.10) und damit $K[X]/(f) \cong K[\alpha]$ ein Körper. Wir müssen noch zeigen, dass die Erweiterung den Grad $n := \text{grad}(f)$ hat. Wir behaupten, dass $1 = \alpha^0, \alpha = \alpha^1, \alpha^2, \ldots, \alpha^{n-1}$ eine Basis von $K[\alpha]/K$ ist. Es ist $\alpha^i = \phi_\alpha(X^i)$ für $i \in \mathbb{N}_0$.

Lineare Unabhängigkeit:
Angenommen es existieren $a_0, \ldots, a_{n-1} \in K$, so dass

$$\sum_{i=0}^{n-1} a_i \alpha^i = 0$$

ist. Dann ist also

$$0 = \sum_{i=0}^{n-1} a_i \alpha^i = \sum_{i=0}^{n-1} a_i \phi_\alpha(X^i) = \phi_\alpha\left(\sum_{i=0}^{n-1} a_i X^i\right)$$

und damit $g := \sum_{i=0}^{n-1} a_i X^i \in \text{Kern}\,\phi_\alpha$. Da g jedoch $\text{grad}(g) \leq n-1$ hat und $n = \text{grad}(f)$ minimal ist, folgt $g = 0$ und somit $a_0 = a_1 = \ldots = a_{n-1} = 0$.

Erzeugendensystem:
Sei $g \in K[X]$. Es existieren $q, r \in K[X]$ mit $\text{grad}(r) < \text{grad}(f)$ oder $r = 0$, so dass

$$g = qf + r.$$

Damit ist $\phi_\alpha(g) = \phi_\alpha(r)$. Ist also $\beta = g(\alpha) \in K[\alpha]$, und schreiben wir r als

$$r = \sum_{i=0}^{n-1} b_i X^i, \quad \text{mit } b_i \in K$$

so bedeutet dies, dass

$$\beta = \sum_{i=0}^{n-1} b_i \alpha^i$$

gilt, wodurch wir einsehen, dass $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ ein Erzeugendensystem von $K[\alpha]/K$ ist.

■

Satz 4.4 Jede endliche Körpererweiterung ist algebraisch.

Beweis. Sei L/K eine endliche Körpererweiterung vom Grad $[L : K] = n$ und $\alpha \in L$. Dann sind $1, \alpha, \alpha^2, \ldots, \alpha^n$ linear abhängig (da dies $n+1$ Elemente eines n-dimensionalen K-Vektorraums sind). Es existieren also $c_0, \ldots, c_n \in K$, so dass

$$c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_n\alpha^n = 0$$

ist und $(c_0, \ldots, c_n) \neq (0, \ldots, 0)$. Also ist

$$f = \sum_{i=0}^{n} c_i X^i \in K[X]$$

mit $f(\alpha) = 0$ und damit ist α algebraisch über K. ■

Bemerkung 4.5 Die Umkehrung von Satz 4.4 gilt *nicht*! Es gibt also nicht endliche algebraische Körpererweiterungen. Ein Beispiel ist der algebraische Abschluss von $\mathbb{Q}$ in $\mathbb{C}$:

$$\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} \mid \alpha \text{ algebraisch über } \mathbb{Q}\}.$$

Siehe Beispiel 4.3.

Definition 4.7 Sei L/K eine Körpererweiterung und $(\alpha_i)_{i\in I} \subset L$ eine Familie von Elementen aus L. Der Körper $K((\alpha_i)_{i\in I})$ ist der von der Familie $(\alpha_i)_{i\in I}$ *erzeugte* Teilkörper von L, also der kleinste Zwischenkörper von $K \subset L$, welcher alle Elemente der Familie enthält:

$$K((\alpha_i)_{i\in I}) = \bigcap_{\substack{Z\subset L \text{ Teilkörper} \\ K\subset Z \\ \alpha_i \in Z \text{ für alle } i\in I}} Z.$$

Bemerkung 4.6 Ist die Familie endlich, so besteht $K(\alpha_1,\dots,\alpha_n)$ aus allen Quotienten der Form

$$\frac{f(\alpha_1,\dots,\alpha_n)}{g(\alpha_1,\dots,\alpha_n)}$$

mit $f,g \in K[X_1,\dots,X_n]$ und $g \neq 0$.

Definition 4.8 Eine Körpererweiterung L/K heißt *endlich erzeugt*, falls es $\alpha_1,\dots,\alpha_n \in L$ gibt, so dass $L = K(\alpha_1,\dots,\alpha_n)$ gilt. Sie heißt *einfach*, falls es ein $\alpha \in L$ gibt mit $L = K(\alpha)$. Die Zahl $[K(\alpha) : K]$ heißt auch der *Grad von α über K*.

Satz 4.5 Es sei $L = K(\alpha_1,\dots,\alpha_n)$ eine endlich erzeugte Körpererweiterung über K mit $\alpha_1,\dots,\alpha_n$ algebraisch über K. Dann ist L endlich (und damit algebraisch) über K.

Beweis. Für $n = 1$ folgt die Aussage aus Satz 4.3. Per Induktion nach n führt man die Aussage direkt auf diesen Fall zurück: Ist $L = K(\alpha_1,\dots,\alpha_n)$, so ist $L = (K(\alpha_1,\dots,\alpha_{n-1}))(\alpha_n)$. Per Induktionsannahme ist dann $K(\alpha_1,\dots,\alpha_{n-1})$ endlich über K und wie im Fall $n = 1$ ist L endlich über $K(\alpha_1,\dots,\alpha_{n-1})$, denn ist α_n algebraisch über K, so ist α_n auch algebraisch über $K(\alpha_1,\dots,\alpha_{n-1})$. Damit ist

$$[L : K] = [L : K(\alpha_1,\dots,\alpha_{n-1})][K(\alpha_1,\dots,\alpha_{n-1}) : K]$$

nach Satz 4.2 ebenfalls endlich. ■

Korollar 4.1 Sei L/K eine Körpererweiterung. Folgende Aussagen sind äquivalent:

(i) L/K ist endlich.
(ii) L/K wird von endlich vielen über K algebraischen Elementen erzeugt.
(iii) L ist eine endlich erzeugte algebraische Körpererweiterung von K.

Beispiel 4.3 Ein Beispiel einer unendlichen algebraischen Körpererweiterung ist

$$\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} \mid \alpha \text{ algebraisch über } \mathbb{Q}\}.$$

Dies ist ein Körper, denn sind $\alpha,\beta \in \overline{\mathbb{Q}}$, so ist $\mathbb{Q}(\alpha,\beta)/\mathbb{Q}$ eine algebraische Erweiterung, weshalb auch $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in \overline{\mathbb{Q}}$ (für $\beta \neq 0$) sind. Aber es muss $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$ sein, weil es Zwischenkörper beliebigen Grades gibt. Zum Beispiel ist $\sqrt[n]{2} \in \overline{\mathbb{Q}}$ und das Minimalpolynom von $\sqrt[n]{2}$ über $\mathbb{Q}$ ist $X^n - 2$ (nach Eisenstein-Kriterium für $p = 2$).

Korollar 4.2 Sei L/K eine Körpererweiterung. Dann sind folgende Aussagen äquivalent:
(i) L/K ist algebraisch.
(ii) L/K wird über K von algebraischen Elementen erzeugt.

Beweis. (i) $\Rightarrow$ (ii): klar.
(ii) $\Rightarrow$ (i): Es gelte $L = K((\alpha_i)_{i\in I})$, wobei alle α_i algebraisch über K sind und es sei $\alpha \in L$. Es ist

$$K((\alpha_i)_{i\in I}) = \bigcup_{S\subset I \text{ endlich}} K((\alpha_i)_{i\in S}).$$

Denn: jeder der Körper auf der rechten Seite ist in der linken enthalten, also auch die Vereinigung. Damit folgt die Inklusion "$\supset$". Für die Inklusion "$\subset$" reicht es zu zeigen, dass die rechte Seite ein Teilkörper von L ist. Mit $\alpha \in K(\alpha_i)_{i\in S_1}$ und $\beta \in K(\alpha_i)_{i\in S_2}$ sind $\alpha, \beta \in K(\alpha_i)_{i\in S_1\cup S_2}$ und damit auch $\alpha \pm \beta$ und $\alpha \times \beta$ und $\alpha \times \beta^{-1}$ in $K(\alpha_i)_{i\in S_1\cup S_2}$ und damit in der rechten Seite enthalten. Deshalb ist die rechte Seite ein Teilkörper von L, welcher alle α_i (mit $i \in I$) enthält und somit folgt die Inklusion "$\subset$".

Damit gibt es also $j_1, \ldots, j_n \in I$ sowie $a_1, \ldots, a_n \in K$ mit $\alpha \in K(\alpha_{j_1}, \ldots, \alpha_{j_n}) =: L_\alpha$, einer Erweiterung, die von endlich vielen algebraischen Elementen erzeugt wird. Damit ist L_α nach Korollar 4.1 eine endliche und damit nach Satz 4.4 auch eine algebraische Erweiterung von K. Mithin is $\alpha \in L_\alpha$ algebraisch über K. ■

Satz 4.6 Es seien $K \subset L \subset M$ Körpererweiterungen.
(i) Ist $\alpha \in M$ algebraisch über L und L/K algebraisch, so ist α algebraisch über K.
(ii) Die Erweiterung M/K ist genau dann algebraisch, wenn M/L und L/K algebraisch sind.

Beweis. (i) Sei $\alpha \in M$ und

$$f = \sum_{i=0}^{n-1} a_i X^i \in L[X]$$

das Minimalpolynom von α über L. Dann sind $a_0, \ldots, a_{n-1}$ algebraisch über K und somit $Z = K(a_0, \ldots, a_{n-1})$ endlich über K nach Satz 4.5. Da auch $Z(\alpha)/Z$ endlich ist, folgt die Endlichkeit von $Z(\alpha)/K$ aus dem Gradsatz. Damit ist $\alpha \in Z(\alpha)$ algebraisch über K.

(ii) Wenn beide Erweiterungen algebraisch sind, so folgt aus i), dass M/K auch algebraisch ist. Die umgekehrte Richtung ist klar, denn:
(a) Ist $\alpha \in M$ algebraisch über K, so ist α auch algebraisch über L (denn $K[X] \subset L[X]$).
(b) Jedes $\alpha \in L$ ist algebraisch über K, da $L \subset M$.

■

4.3 Zerfällungskörper, normale Körpererweiterungen

Bevor wir Zerfällungskörper behandeln, sei an Aufgabe H31 erinnert: Ist $f \in K[X]$ ein von Null verschiedenes Polynom mit $n = \text{grad}(f)$, so besitzt f höchstens n Nullstellen in K, mit Vielfachheiten gezählt.

Definition 4.9 Sei K ein Körper und $f \in K[X] \setminus \{0\}$ mit $n = \text{grad}(f) \geq 1$. Ein (minimaler) *Zerfällungskörper* von f ist eine Körpererweiterung L/K, so dass
(i) f in $L[X]$ vollständig in Linearfaktoren zerfällt
(ii) und sind $\alpha_1, \ldots, \alpha_n \in L$ die Nullstellen von f in L, so gilt $L = K(\alpha_1, \ldots, \alpha_n)$.

Lemma 4.1 — Kronecker-Verfahren. Sei K ein Körper und $f \in K[X]$ mit $f \notin K$. Dann gibt es einen Erweiterungskörper $K \subset L$, so dass f in L eine Nullstelle besitzt. (Das heißt, dass es ein $\alpha \in L$ gibt, so dass $f(\alpha) = 0$ ist.)

Beweis. Die folgende Konstruktion haben wir bereits (indirekt) gesehen: Wir können ohne Beschränkung der Allgemeinheit annehmen, dass f irreduzibel ist, denn für ein reduzibles Polynom reicht es aus, einen Erweiterungskörper zu konstruieren, in dem einer der irreduziblen Faktoren eine Nullstelle bsitzt.

Ist f irreduzibel, so ist $(f) \subset K[X]$ im Hauptidealring $K[X]$ ein maximales Ideal und somit $L := K[X]/(f)$

ein Körper. Der Ringhomomorphismus

$$K \hookrightarrow K[X] \to L$$

gegeben durch die Verkettung der Inklusion $K \hookrightarrow K[X]$ und die kanonische Projektion $\pi : K[X] \to L$ ist, da K ein Körper ist, injektiv und somit können wir K als Teilkörper von L auffassen. Es bleibt zu zeigen, dass f in L eine Nullstelle besitzt. Sei $\alpha := \pi(X)$. Dann gilt für

$$f = \sum_i a_i X^i,$$

dass

$$f(\alpha) = \sum_i a_i \pi(X)^i = \pi\left(\sum_i a_i X^i\right) = \pi(f) = 0 \in L,$$

da π ein Homomorphismus ist. ■

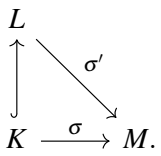
Satz 4.7 Seien K ein Körper und $f \in K[X] \setminus K$. Dann existiert ein Zerfällungskörper von f.

Beweis. Dies folgt per Induktion nach $\operatorname{grad}(f)$ aus Lemma 4.1, denn ist $K \subset K_1$ die in Lemma 4.1 konstruierte Körpererweiterung und ist $\alpha \in K_1$ eine Nullstelle von f, so ist f in $K_1[X]$ durch $(X - \alpha)$ teilbar. Das Polynom $g := f/(X - \alpha)$ hat Grad $n - 1$ und nach Induktionsvoraussetzung existiert ein Zerfällungskörper Z von g über K_1, welcher auch Zerfällungskörper von f über K ist. ■

Definition 4.10 Seien L/K und M/K Körpererweiterungen des Körpers K. Ein Homomorphismus $\sigma : L \to M$ heißt *K-Homomorphismus*, falls $\sigma|_K = \mathrm{id}_K$ ist, d.h. es ist $\sigma(x) = x$ für alle $x \in K$.

Man sagt in diesem Falle auch, dass σ eine *Fortsetzung der Identität* $K \to K$ auf $L \to M$ sei und wir schreiben $\mathrm{Hom}_K(L, M)$ für die Menge der K-Homomorphismen $L \to M$. Für $L = M$ schreiben wir auch einfach $\mathrm{Hom}_K(L)$ und $\mathrm{Aut}_K(L)$ für die K-Homomorphismen $L \to L$, die Automorphismen von L sind.

Etwas allgemeiner: Ist L/K eine Körpererweiterung und ist $\sigma : K \to M$ ein Körperhomomorphismus, so heißt ein Homomorphismus $\sigma' : L \to M$ eine *Fortsetzung von σ*, falls seine Einschränkung auf K durch σ gegeben ist ($\sigma'|_K = \sigma$); d.h. das folgende Diagramm ist kommutativ:



Wir bezeichnen mit $\mathrm{Hom}_\sigma(L, M)$ die Menge der Fortsetzungen von σ auf $L \to M$.

Bemerkung 4.7 Ist L/K eine endliche Erweiterung, so ist $\mathrm{Aut}_K(L) = \mathrm{Hom}_K(L)$.

Beweis. Homomorphismen zwischen Körpern sind immer injektiv. Ist L/K endlich, so ist L endlich-dimensionsional als K-Vektorraum. Jedes Element $\sigma \in \mathrm{Hom}_K(L)$ ist auch ein K-Vektorraumhomomorphismus $L \to L$ und im endlich-dimensionalen Fall ist injektiv äquivalent zu surjektiv bzw. bijektiv. (Ein bijektiver Körperhomomorphismus ist bereis ein Isomorphismus.) ■

Wir machen folgende Beobachtung:

Bemerkung 4.8 Ist L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K mit $f \in K[X] \setminus \{0\}$ und $f(\alpha) = 0$. Sei $\sigma \in \mathrm{Hom}_K(L, L)$. Dann ist $f(\sigma(\alpha)) = 0$.

Das heißt, ein K-Homomorphismus von L bildet Nullstellen von f auf Nullstellen von f ab.

Notation 4.1 Ist $\sigma : K \to L$ ein Homomorphismus und $f \in K[X]$, so induziert σ einen Homomorphismus $K[X] \to L[X]$ (indem man σ auf die Koeffizienten von f anwendet). Wir bezeichnen das Bild von f unter diesem

Homomorphismus mit f^σ, d.h. ist

$$f = \sum_i a_i X^i$$

mit $a_i \in K$, so ist

$$f^\sigma = \sum_i \sigma(a_i) X^i \in L[X].$$

Proposition 4.1 Seien $K(\alpha)/K$ eine einfache algebraische Erweiterung, f das Minimalpolynom von α über K sowie $\sigma : K \hookrightarrow L$ ein Körperhomomorphismus.

Dann ist die Abbildung

$$\begin{aligned} \mathrm{Hom}_\sigma(K(\alpha), L) &\to \{\beta \in L \mid f^\sigma(\beta) = 0\} \\ \sigma' &\mapsto \sigma'(\alpha) \end{aligned}$$

bijektiv. In anderen Worten: die Fortsetzungen von σ entsprechen genau den Nullstellen von f^σ in L. (Insbesondere ist jede Fortseztung eindeutig durch das Bild von α bestimmt und die Anzahl der Fortsetzungen ist gleich der Anzahl der verschiedenen Nullstellen von f^σ in L, also $\leq \mathrm{grad}(f)$.

Bemerkung 4.9 Wir betrachten eine einfache algebraische Körpererweiterungen $K(\alpha)/K$ und es sei f das Minimalpolynom von α über K.

Dann besagt Proposition 4.1 auch, dass die Elemente aus $\mathrm{Hom}_K(K(\alpha)) = \mathrm{Aut}_K(K(\alpha))$ die verschiedenen Nullstellen von f in $K(\alpha)$ permutieren.

Dabei ist die Anzahl $|\mathrm{Aut}_K(K(\alpha))|$ der verschiedenen K-Homomorphismen von $K(\alpha)$ nach $K(\alpha)$ genau gleich der Anzahl der verschiedenen Nullstellen von f in $K(\alpha)$.

Beispiel 4.4

(i) Die Erweiterung $\mathbb{Q}(i)/\mathbb{Q}$ ist Zerfällungskörper des Polynoms X^2+1. Demnach hat $\mathrm{Aut}_\mathbb{Q}(\mathbb{Q}(i))$ zwei Elemente, die durch das Bild von i eindeutig bestimmt sind. Dabei sind die verschiedenen Bilder die Nullstellen von X^2+1. Also gibt es die beiden Möglichkeiten $i \mapsto i$ (die Identität) und $i \mapsto -i$.

(ii) Wir betrachten die Erweiterung $L = \mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$. Das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}$ ist $f = X^4 - 2$. Die Nullstellen von f in L sind jedoch nur $\pm\sqrt[4]{2}$. Damit gibt es wieder nur 2 Elemente in $\mathrm{Aut}_\mathbb{Q}(L)$. Betrachten wir hingegen $M = \mathbb{Q}(\sqrt[4]{2}, i)$, so erhalten wir die Elemente aus $\mathrm{Hom}_\mathbb{Q}(L, M)$ genau durch alle 4 verschiedenen Nullstellen von f in M. Wir können sie dadurch angeben, dass wir das Bild von $\sqrt[4]{2}$ angeben: Wir erhalten die Identität sowie die 3 Möglichkeiten $\sqrt[4]{2} \mapsto -\sqrt[4]{2}$, $\sqrt[4]{2} \mapsto i\sqrt[4]{2}$, $\sqrt[4]{2} \mapsto -i\sqrt[4]{2}$.

Beweis von Proposition 4.1. Wir zeigen zunächst, dass die Abbildung überhaupt Sinn macht. Sei also $\sigma' : K(\alpha) \to L$ eine Fortsetzung von σ und $\beta = \sigma'(\alpha)$. Dann ist

$$f^\sigma(\beta) = \sum_i \sigma(a_i)\sigma'(\alpha)^i = \sum_i \sigma'(a_i\alpha^i) = \sigma'(f(\alpha)) = \sigma'(0) = 0.$$

Also ist β in der Tat eine Nullstelle von f^σ in L. Wir zeigen nun, dass die Abbildung $\sigma' \mapsto \sigma'(\alpha)$ injektiv ist: Seien σ' und σ'' zwei Fortsetzungen von σ mit $\sigma'(\alpha) = \sigma''(\alpha)$. Dann ist auch $\sigma'(\alpha^i) = \sigma'(\alpha)^i = \sigma''(\alpha)^i$ für alle i. Ist $n = \mathrm{grad}(f)$, so lässt sich jedes Element $x \in K(\alpha)$ schreiben als

$$x = \sum_{i=0}^{n-1} c_i \alpha^i$$

mit $c_i \in K$. Deshalb erhalten wir

$$\sigma'(x) = \sigma'\left(\sum_{i=0}^{n-1} c_i\alpha^i\right) = \sum_{i=0}^{n-1} \sigma(c_i)\sigma'(\alpha)^i = \sum_{i=0}^{n-1} \sigma(c_i)\sigma''(\alpha)^i = \sigma''\left(\sum_{i=0}^{n-1} c_i\alpha^i\right) = \sigma''(x)$$

und damit $\sigma' = \sigma''$, woraus die Injektivität folgt.

Es bleibt die Surjektivität zu zeigen. Sei also $\beta \in L$ eine Nullstelle von f^σ. Wir definieren $\sigma' : K(\alpha) \to L$ durch

$$\sigma'(x) := \sigma'\left(\sum_{i=0}^{n-1} c_i \alpha^i\right) := \sum_{i=0}^{n-1} \sigma(c_i)\beta^i$$

für alle $x = \sum_{i=0}^{n-1} c_i \alpha^i \in K(\alpha)$. Es ist klar, dass dies ein Homomorphismus ist, welcher σ fortsetzt und $\sigma'(\alpha) = \beta$ erfüllt. ■

Proposition 4.2 Sei $K(\alpha_1, \ldots, \alpha_n)$ (mit $n > 1$) eine endlich erzeugte algebraische Erweiterung von K und $\sigma : K \to L$ ein Körperhomomorphismus. Falls die Minimalpolynome aller α_i über L vollständig in Linearfaktoren zerfallen, so existiert eine Fortsetzung von σ auf $K(\alpha_1, \ldots, \alpha_n)$.

Beweis. Der Beweis ist eine Übung. ■

Satz 4.8 Sei K ein Körper und $f \in K[X]$ ein nichtkonstantes Polynom. Es gibt bis auf K-Isomorphie genau einen Zerfällungskörper von f.

Beweis. Die Existenz haben wir in Satz 4.7 bewiesen. Seien Z und Z' Zerfällungskörper von f:

$$Z = K(\alpha_1, \ldots, \alpha_n)$$
$$Z' = K(\alpha'_1, \ldots, \alpha'_n),$$

hierbei seien jeweils $\alpha_1, \ldots, \alpha_n \in Z$ bzw. $\alpha'_1, \ldots, \alpha'_n \in Z'$ die Nullstellen von f in Z bzw. Z'. Da das Minimalpolynom von jedem α_i bzw. α'_i ein Teiler von f ist, können wir Proposition 4.2 anwenden. Somit existiert ein K-Homomorphismus (notw. injektiv) $\sigma : Z \hookrightarrow Z'$. Genauso existiert ein K-Homomorphismus $\sigma' : Z' \hookrightarrow Z$. Da Z und Z' endlich-dimensionale K-Vektorräume sind und σ und σ' insbesondere injektive K-Vektorraumhomomorphismen sind, müssen diese schon bijektiv sein. (die Einbettungen zeigen, dass $[Z : K] \leq [Z' : K]$ und $[Z' : K] \leq [Z : K]$ ist und somit haben Z und Z' die gleiche Dimension als K-Vektorräume. Ein injektiver K-Vektorraumhomomorphismus zwischen Vektorräumen der gleichen Dimension ist schon bijektiv). ■

Proposition 4.3 Ist $\sigma : K \to M$ ein Körperhomomorphismus und L/K eine endliche Körpererweiterung, so ist die Anzahl der Fortsetzungen von σ nach L durch den Grad $[L : K]$ beschränkt.

Beweis. Ist $L = K(\alpha)$, so ist dies die Aussage von Proposition 4.1. Ist L/K nicht einfach, so gibt es dennoch $\alpha_1, \ldots, \alpha_n \in L$, welche algebraisch über K sind mit $L = K(\alpha_1, \ldots, \alpha_n)$, denn L/K wird nach Korollar 4.1 von endlich vielen über K algebraischen Elementen erzeugt. Die Aussage folgt dann per Induktion nach der Anzahl n, denn die Anzahl der Fortsetzungen von σ nach $L' := K(\alpha_1, \ldots, \alpha_{n-1})$ ist durch den Grad $[L' : K]$ beschränkt. Ist σ' eine solche Fortsetzung, so ist die Anzahl der Fortsetzungen von σ' nach L durch den Grad $[L : L']$ beschränkt und die Behauptung folgt aus dem Gradsatz. ■

Definition 4.11 Sei L/K eine Körpererweiterung. Dann nennen wir die Erweiterung L/K *normal*, falls sie
(i) algebraisch ist
(ii) und jedes irreduzible Polynom $f \in K[X]$, welches eine Nullstelle in L besitzt, bereits vollständig über L in Linearfaktoren zerfällt.

Satz 4.9 Eine endliche Körpererweiterung L/K ist genau dann normal, wenn sie der Zerfällungskörper eines Polynoms $f \in K[X]$ ist.

Beweis. „⇒“: Eine endliche Körpererweiterung wird von endlich vielen über K algebraischen Elementen $\alpha_1, \ldots, \alpha_n$ erzeugt. Ist L/K normal ist L somit Zerfällungskörper des Produkts der Minimalpolynome der α_i.

„⇐“: Wir zeigen zunächst folgende Aussage unter der Annahme, dass L ein Zerfällungskörper des Polynoms $f \in K[X]$ ist:

Hilfsaussage: Alle Fortsetzungen einer Einbettung $\iota : K \hookrightarrow M$ von K in einen Körper M auf L haben das selbe Bild in M, d.h. sind σ und τ Fortsetzungen von ι auf L, so gilt $\sigma(L) = \tau(L)$.

Beweis der Hilfsaussage (unter der Annahme, dass L Zerfällungskörper von $f \in K[X]$ sei): Seien $\alpha_1, \ldots, \alpha_n \in L$ die Nullstellen von f in L, so dass $L = K(\alpha_1, \ldots, \alpha_n)$ sei und

$$f = \prod_{i=1}^{n} (X - \alpha_i).$$

Es ist

$$f^\iota = f^\sigma = \prod_{i=1}^{n} (X - \sigma(\alpha_i)) = f^\tau = \prod_{i=1}^{n} (X - \tau(\alpha_i)),$$

da $f \in K[X]$ und σ und τ Fortsetzungen von ι sind. Falls es also solche Fortsetzungen σ, τ gibt, so zerfällt f^ι über M in Linearfaktoren und die Bilder $\sigma(L)$ und $\tau(L)$ werden von den Nullstellen $\{\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\}$ bzw. $\{\tau(\alpha_1), \ldots, \tau(\alpha_n)\}$ über $\iota(K)$ erzeugt. Es sind also $\sigma(L)$ sowie $\tau(L)$ beides Zerfällungskörper von f^ι über $\iota(K)$, die beide in M enthalten sind, müssen also notwendigerweise gleich sein (die Mengen $\{\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\}$ und $\{\tau(\alpha_1), \ldots, \tau(\alpha_n)\}$ stimmen überein, da es jeweils genau die Nullstellen von f^ι in M sind).

Wir zeigen nun, dass diese Hilfsaussage impliziert, dass L/K normal ist. Sei $g \in K[X]$ irreduzibel und $\beta \in L$ sei eine Nullstelle von g in L. Weiterhin seien $\gamma_1, \ldots, \gamma_n \in L$, so dass

$$L = K(\beta, \gamma_1, \ldots, \gamma_n)$$

gelte. Sei M ein Zerfällungskörper über L des Produkts von g mit allen Minimalpolynomen (über K) der γ_i. Wir sehen L als Teilkörper von M an.

Dann können wir die Einbettung $K \hookrightarrow M$ für jede Nullstelle $\beta_1, \ldots, \beta_m$ von g in M nach $K(\beta)$ fortsetzen und, nach Proposition 4.2, weiter zu $\sigma_i : L \to M$ (mit $\sigma_i(\beta) = \beta_i$). Wir können annehmen, dass $\sigma_1 \,|_L = \mathrm{id}_L$ ist.

Da die Bilder aller dieser Fortsetzungen übereinstimmen, $\sigma_i(L) = \sigma_1(L) = L \subset M$, zerfällt g über L vollständig in Linearfaktoren. ■

Beispiel 4.5 (i) $\mathbb{Q}(\sqrt{2})$ ist normal über $\mathbb{Q}$ (als Zerfällungskörper von $X^2 - 2$).
(ii) $\mathbb{Q}(\sqrt[3]{2})$ ist nicht normal über $\mathbb{Q}$. Denn: Wir können $\mathbb{Q}(\sqrt[3]{2})$ in $\mathbb{R}$ einbetten, die anderen beiden Nullstellen von $X^3 - 2$ liegen jedoch in $\mathbb{C} \setminus \mathbb{R}$.

Bemerkung 4.10 Aus dem Kriterium in Satz 4.9 folgt leicht:
(i) Sind $K \subset L \subset M$ endliche Körpererweiterungen und ist M/K normal, dann ist auch M/L normal.
(ii) Körpererweiterungen vom Grad 2 sind stets normal.

Satz 4.10 Sei L/K eine endliche Körpererweiterung. Dann existiert eine (bis auf nicht-kanonische Isomorphie) eindeutig bestimmte minimale endliche Körpererweiterung N/L, so dass N/K normal ist. Diese wird die *normale Hülle* von L/K genannt. (Hierbei ist Minimalität bezüglich Inklusion gemeint.)

Beweis. L wird von endlich vielen über K algebraischen Elementen erzeugt. Der Zerfällungskörper N/L des Produkts f der Minimalpolynome der Erzeuger von L/K ist natürlich nach Konstruktion normal über K. Dies ist sicher die kleinste Erweiterung, die normal ist, denn f (bzw. sämtliche irreduziblen Faktoren von f, die Minimalpolynome der Erzeuger von L/K) muss über einer solchen Erweiterung Linearfaktoren zerfallen. Die Eindeutigkeit folgt aus der Eindeutigkeit des Zerfällungskörpers ■

4.4 Vielfachheit von Nullstellen, separable Erweiterungen

Unter einer *mehrfache Nullstelle* eines Polynoms verstehen wir eine Nullstelle der Vielfachheit > 1. Wir sagen, das Polynom $f \in K[X]$ habe mehrfache Nullstellen in einer Körpererweiterung L/K, falls f mindestens eine

Nullstelle der Vielfachheit > 1 in L besitzt.

Definition 4.12 Ein Polynom $f \in K[X]$ heißt *separabel*, falls f in einem Zerfällungskörper über K keine mehrfachen Nullstellen hat.

Ein über K algebraisches Element $\alpha \in L$ einer Körpererweiterung L/K heißt separabel, falls sein Minimalpolynom separabel ist.

Die Erweiterung L/K heißt separabel, falls sie algebraisch ist und alle $\alpha \in L$ separabel sind.

Definition 4.13 Sei K ein Körper und

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

ein Polynom. Dann definieren wir die algebraische *Ableitung* von f als

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

Die Ableitung ist kein Homomorphismus, sondern eine sogenannte Derivation, d.h.:

Lemma 4.2 — Ableitungsregeln. Es gelten die folgenden Ableitungsregeln:
(i) $(f+g)' = f' + g'$ für alle $f, g \in K[X]$,
(ii) $(fg)' = f'g + fg'$ für alle $f, g \in K[X]$.

Beweis. Der Beweis ist eine Übung. ■

Lemma 4.3 Sei K ein Körper und $f \in K[X]$ sowie $\alpha \in K$ eine Nullstelle von f. Dann ist α genau dann eine mehrfache Nullstelle von f, wenn α auch eine Nullstelle von f' ist.

Beweis. Das Element α ist genau dann mehrfache Nullstelle von f, wenn es ein $g \in K[X]$ gibt, so dass $f = g(X-\alpha)^2$ ist. Nach Lemma 4.2 ist dann

$$f' = 2(X-\alpha)g + (X-\alpha)^2 g'$$

immernoch durch $(X-\alpha)$ teilbar und somit ist $f'(\alpha) = 0$. Ist umgekehrt $f'(\alpha) = 0$ und $f = (X-\alpha)h$ für ein $h \in K[X]$, so ist $f' = h + (X-\alpha)h'$ und damit $h(\alpha) = 0$ und α mehrfache Nullstelle von f. ■

Proposition 4.4 Sei K ein Körper und $f \in K[X] \setminus K$ irreduzibel. Dann sind folgende Aussagen äquivalent:
(i) f ist nicht separabel.
(ii) Die Ableitung von f ist das Nullpolynom: $f' = 0$.
(iii) Die Charakteristik von K ist $p > 0$ und es gibt ein $g \in K[X] \setminus K$ mit $f(X) = g(X^p)$.
(iv) Jede Nullstelle von f in einer beliebigen Körpererweiterung L/K ist eine mehrfache Nullstelle.

Beweis.
(i) $\Rightarrow$ (ii):
Falls f nicht separabel ist, so besitzt f mindestens eine mehrfache Nullstelle α (in einer Erweiterung L/K). Da f irreduzibel ist, ist f bis auf einen konstanten Faktor in K das Minimalpolynom von α über K. Nach Lemma 4.3 ist auch $f'(\alpha) = 0$. Wäre nun $f' \neq 0$, so wäre $f' \in K[X]$ ein Polynom kleineren Grades, welches α als Nullstelle hat. Durch Normieren von f' würde man ein normiertes, von Null verschiedenes Polynom in $K[X]$ mit kleinerem Grad als $\operatorname{grad}(f)$ erhalten, welches α als Nullstelle besitzt. Dies ist ein Widerspruch zur Minimalität von $\operatorname{grad}(f)$.
(ii) $\Leftrightarrow$ (iii):
Dies ist klar, denn in Charakteristik 0 kann f' niemals das Nullpolynom ($f \notin K$) sein. In Charakteristik p geht dies nur, wenn f von der angegebenen Form ist (und dann ist f' auch stets gleich Null).
(ii) $\Rightarrow$ (iv):

Ist die Ableitung $f' = 0$, so ist jede Nullstelle von f auch Nullstelle von f' und somit eine mehrfache Nullstelle von f.
(iv) $\Rightarrow$ (i):
Dies ist klar. ■

Korollar 4.3 In Charakteristik 0 ist jede algebraische Körpererweiterung separabel.

Beweis von Korollar 4.3. Dies folgt aus Proposition 4.4 (i) $\Rightarrow$ (iii). ■

Bemerkung 4.11 Einen Körper K für den gilt, dass alle irreduziblen Polynome aus $K[X]$ separabel sind, nennt man auch *vollkommen*. Wir haben also gesehen, dass Körper der Charakteristik 0 und endliche Körper vollkommen sind.

Außerdem sind auch endliche Körper vollkommen. Dies behandeln wir in den Übungen.

Beispiel 4.6 Um eine nicht-separable Körpererweiterung zu erhalten muss man also schon etwas kreativer werden: Sei p eine Primzahl. Wir bezeichnen mit $\mathbb{F}_p(t)$ den Körper der rationalen Funktionen über dem endlichen Körper $\mathbb{F}_p$ (dies ist der Quotientenkörper des Polynomrings $\mathbb{F}_p[t]$). Die Charakteristik von $\mathbb{F}_p(t)$ ist p. Aus dem Eisenstein-Kriterium folgt, dass das Polynom $X^p - t \in \mathbb{F}_p(t)[X]$ irreduzibel ist. Es ist aber nach Proposition 4.4 nicht separabel. Der Grund ist die Existenz des Frobenius-Homomorphismus': in der Erweiterung $\mathbb{F}_p(\sqrt[p]{t}) := \mathbb{F}_p(t)[X]/(X^p - t)$ von $\mathbb{F}_p(t)$ zerfällt das Polynom $X^p - t$ in $X^p - t = (X - \sqrt[p]{t})^p$.

Lemma 4.4 Es seien $K \subset L \subset M$ endliche algebraische Körpererweiterungen und N/K eine weitere Körpererweiterung. Dann gilt für die Anzahl der K-Homomorphismen von M nach N die Formel

$$|\mathrm{Hom}_K(M,N)| = \sum_{\sigma \in \mathrm{Hom}_K(L,N)} |\mathrm{Hom}_\sigma(M,N)|.$$

Beweis. Ist $\tau \in \mathrm{Hom}_K(M,N)$, so kann man τ auf L einschränken und erhält ein Element in $\mathrm{Hom}_K(L,N)$. Jedes $\tau \in \mathrm{Hom}_K(M,N)$ ist also eine Fortsetzung eines $\sigma \in \mathrm{Hom}_K(L,N)$. Weiterhin ist jede Fortsetzung nach M eines $\sigma \in \mathrm{Hom}_K(L,N)$ per Definition ein Element in $\mathrm{Hom}_K(M,N)$ und somit ist $\mathrm{Hom}_K(M,N)$ die disjunkte Vereinigung der Mengen $\mathrm{Hom}_\sigma(M,N)$, wobei σ durch $\mathrm{Hom}_K(L,N)$ läuft. ■

Satz 4.11 Sei L/K eine endliche Körpererweiterung. Die folgenden Aussagen sind äquivalent:
(i) L/K ist separabel.
(ii) L wird über K von separablen Elementen erzeugt.
(iii) Ist N/L eine Körpererweiterung, so dass N/K normal ist, so ist $|\mathrm{Hom}_K(L,N)| = [L:K]$.

Beweis.
(i) $\Rightarrow$ (ii):
Das ist klar.
(ii) $\Rightarrow$ (iii):
Zunächst betrachten wir den Fall, dass $L = K(\alpha)$ einfach sei. Dann sind die Nullstellen des Minimalpolynoms f von α über K alle verschieden in N und (nach Proposition 4.1) $|\mathrm{Hom}_K(L,N)| = \mathrm{grad}(f)$, da f über L vollständig in Linearfaktoren zerfällt. Die Implikation folgt nun per Induktion nach $[L:K]$, wobei man im Induktionsschritt genau die gleiche Argumentation sowie Lemma 4.4 und den Gradsatz anwende.
(iii) $\Rightarrow$ (i):
Angenommen (iii) gelte und L/K sei nicht separabel. Dann gibt es ein $\alpha \in L$, welches nicht über K separabel ist. Wir wissen nach Satz 4.10, dass es eine endliche Erweiterung N/L gibt, so dass N/K normal ist.

Aus Lemma 4.4 erhalten wir, dass

$$|\mathrm{Hom}_K(L,N)| = \sum_{\sigma \in \mathrm{Hom}_K(K(\alpha),N)} |\mathrm{Hom}_\sigma(L,N)|.$$

Nach Proposition 4.3 ist $\mathrm{Hom}_\sigma(L,N)$ für jedes σ durch den Grad $[L:K(\alpha)]$ beschränkt. Ist jedoch α nicht separabel über K, so ist die Anzahl der verschiedenen Nullstellen des Minimalpolynoms f von α in N **kleiner** als $\mathrm{grad}(f) = [K(\alpha):K]$ und damit $|\mathrm{Hom}_K(K(\alpha),N)| < [K(\alpha):K]$ nach Proposition 4.1. Damit wäre nun

$$|\mathrm{Hom}_K(L,N)| < [K(\alpha):K][L:K(\alpha)] = [L:K],$$

was ein Widerspruch zu (iii) ist. ■

Proposition 4.5 Seien $K \subset L \subset M$ algebraische Körpererweiterungen. Dann ist M/K genau dann separabel, wenn M/L und L/K separabel sind.

Beweis. Sei M/K separabel. Sei $\alpha \in M$. Dann ist das Minimalpolynom f von α über L ein Teiler (in $L[X]$) des Minimalpolynoms g von α über K. Da g separabel ist, muss f separabel sein. Da nach Voraussetzung alle $\alpha \in M$ separabel über K sind, sind auch alle Elemente von $L \subset M$ separabel über K.

Seien also M/L und L/K als separabel vorausgesetzt und sei $\alpha \in M$. Sei f das Minimalpolynom von α über L (nach Voraussetzung separabel) . Sei $K \subset Z \subset L$ der von den Koeffizienten von f erzeugte Zwischenkörper. Dies ist eine endliche separable Erweiterung von K nach dem vorher gesagten. Sei außerdem N die normale Hülle von M/Z. Da f separabel ist, ist $Z(\alpha)/Z$ eine endliche separable Erweiterung. Es ist also insbesondere $|\mathrm{Hom}_K(Z,N)| = [Z:K]$ nach Satz 4.11. Wir behaupten, dass

$$|\mathrm{Hom}_K(Z(\alpha),N)| = [Z(\alpha):Z]|\mathrm{Hom}_K(Z,N)|$$

und damit folgt die Behauptung nach Satz 4.11 und dem Gradsatz. In der Tat, da f separabel ist, hat f genau $[Z(\alpha):Z] = \mathrm{grad}(f)$ Nullstellen in N und zu jedem $\sigma \in \mathrm{Hom}_K(Z,N)$ und jeder Nullstelle $\beta \in N$ von f existiert eine Fortsetzung von σ nach $Z(\alpha)$. Daraus folgt sicher

$$|\mathrm{Hom}_K(Z(\alpha),N)| \geq [Z(\alpha):Z]|\mathrm{Hom}_K(Z,N)| = [Z(\alpha):Z][Z:K] = [Z(\alpha):K]$$

Da aber auch $|\mathrm{Hom}_K(Z(\alpha),N)| \leq [Z(\alpha):K]$ gilt (Proposition 4.3), muss Gleichheit gelten. ■

Satz 4.12 — Satz vom primitiven Element. Sei L/K eine endliche separable Körpererweiterung. Dann existiert ein $\alpha \in L$, so dass $L = K(\alpha)$ ist.

Beweis. Der Fall, dass K und damit auch L nur endlich viele Elemente hat, ist eine Hausaufgabe. Wir nehmen also an, dass K unendlich viele Elemente habe. Da L/K endlich ist, ist L endlich erzeugt. Seie also $\alpha_1, \alpha_2, \ldots, \alpha_m \in L$ mit $L = K(\alpha_1, \alpha_2, \ldots, \alpha_m)$. Ist $m = 1$, so sind wir fertig. Wir beweisen die Aussage per Induktion nach m. Im Induktionsschritt müssen wir nur den Fall betrachten, dass $L = K(\alpha,\beta)$ ist. Sei N die normale Hülle von L über K. Da L/K separabel ist, gilt $|\mathrm{Hom}_K(L,N)| = [L:K] =: n$. Seien $\sigma_1, \ldots, \sigma_n$ die verschiedenen Elemente von $\mathrm{Hom}_K(L,N)$ und betrachte das Polynom

$$f := \prod_{i \neq j} [(\sigma_i(\alpha) - \sigma_j(\alpha)) + (\sigma_i(\beta) - \sigma_j(\beta))X].$$

Es ist klarerweise $f \in N[X]$ und $f \neq 0$, denn falls $\sigma_i(\alpha) = \sigma_j(\alpha)$ **und** $\sigma_i(\beta) = \sigma_j(\beta)$ gilt, so folgt $i = j$ (da die σ_i eindeutig durch die Bilder von α und β bestimmt sind).

Es existiert nun ein $\gamma \in K$ mit $f(\gamma) \neq 0$, da K unendlich viele Elemente hat und f nur endlich viele verschiedene Nullstellen.

Daraus folgt, dass die n Elemente

$$\sigma_i(\alpha + \beta\gamma) = \sigma_i(\alpha) + \sigma_i(\beta)\gamma \in N$$

($i = 1, \ldots, n$) alle verschieden sind. Ist nun $g \in K[X]$ das Minimalpolynom von $\alpha + \beta\gamma \in L$ über K, so sind $\sigma_1(\alpha + \beta\gamma), \ldots, \sigma_n(\alpha + \beta\gamma)$ verschiedene Nullstellen von g in N und somit muss $\mathrm{grad}(g) \geq n$ sein. Damit ist $[K(\alpha + \beta\gamma):K] \geq n = [L:K]$ und daraus folgt, dass $\alpha + \beta\gamma \in L$ schon L über K erzeugt und die Behauptung folgt. ■

4.5 Galoistheorie

Definition 4.14 Sei K ein Körper. Ein (Körper-)Isomorphismus $K \to K$ heißt *Automorphismus* von K. Die Menge $\mathrm{Aut}(K)$ ist eine Gruppe. Ist L/K eine Körpererweiterung, so nennen wir die Untergruppe $\mathrm{Gal}(L/K) \subset \mathrm{Aut}(L)$ aller Automorphismen σ von L mit $\sigma|_K = \mathrm{id}_K$, die *Galoisgruppe* von L/K. Analog zur Definition von $\mathrm{Hom}_K(L,M)$ schreibt man auch: $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$.

Ist $f \in K[X]$ ein Polynom, so nennen wir die Galoisgruppe $\mathrm{Gal}(L/K)$ eines Zerfällungskörpers L von f über K auch die *Galoisgruppe von f*.

Lemma 4.5 Für eine Körpererweiterung gilt stets

$$|\mathrm{Gal}(L/K)| \leq [L:K].$$

Beweis. Dies folgt direkt aus Proposition 4.3. ■

Definition 4.15 Eine algebraische Körpererweiterung heißt *Galoiserweiterung*, falls sie *normal* und *separabel* ist.

Beispiel 4.7 Sei $K(\alpha)$ eine quadratische separable Erweiterung, d.h. $[K(\alpha):K] = 2$. Dann ist $K(\alpha)$ sicherlich stets eine Galoiserweiterung (denn $K(\alpha)$ ist in jedem Falle Zerfällungskörper des Minimalpolynoms von α).

Bemerkung 4.12 Ist L/K eine endliche Galoiserweiterung, so gilt

$$|\mathrm{Gal}(L/K)| = [L:K].$$

Beweis. Dies folgt direkt aus Satz 4.11, (iii), da L/K normal und separabel ist sowie $\mathrm{Gal}(L/K) = \mathrm{Hom}_K(L,L)$ ist. ■

Definition 4.16 Sei L ein Körper und $G \subset \mathrm{Aut}(L)$ eine Untergruppe.
Wir definieren den *Fixkörper* von G durch

$$L^G := \{x \in L \mid \sigma(x) = x \text{ für alle } \sigma \in G\} \subset L.$$

Bemerkung 4.13 Der Fixkörper $L^G \subset L$ ist ein Teilkörper von L.

Beweis. Es ist z.B. mit $x,y \in L^G$ auch $\sigma(x+y) = \sigma(x)+\sigma(y) = x+y$ für alle $\sigma \in G$ und somit $x+y \in L^G$, sowie $0 \in L^G$ und $-x \in L^G$ für $x \in L^G$. Genauso rechnet man nach, dass mit $x,y \in L^G$ auch $xy \in L^G$ ist und für $x \in L^G \setminus \{0\}$ ist $\sigma(x^{-1}) = \sigma(x)^{-1} = x^{-1}$ und somit sind auch alle Inversen in L^G. Klar ist, dass $0,1 \in L^G$ sind. ■

Satz 4.13 Sei L ein beliebiger Körper und $G \subset \mathrm{Aut}(L)$ eine endliche Gruppe von Automorphismen von L. Es gilt:

(i) Die Körpererweiterung L/L^G ist algebraisch und das Minimalpolynom von $\alpha \in L$ über L^G ist gegeben durch

$$f_\alpha = \prod_{\beta \in G\alpha} (X - \beta),$$

wobei $G\alpha = \{\sigma(\alpha) \mid \sigma \in G\} \subset L$ (auch die Bahn von α unter der Operation von G genannt).

(ii) L/L^G ist eine endliche Galoiserweiterung mit Galoisgruppe G.

Beweis. Setze $K := L^G$.

(i) Für $\sigma \in G$ gilt

$$f_\alpha^\sigma = \prod_{\beta \in G\alpha} (X - \sigma(\beta)) = \prod_{\beta \in G\alpha} (X - \beta)$$

und somit ist $f_\alpha \in K[X]$.
Es ist $f_\alpha(\alpha) = 0$ und somit ist das Minimalpolynom m_α von α ein Teiler von f in $K[X]$. Da aber auch $m_\alpha(\sigma(\alpha)) = \sigma(m_\alpha(\alpha)) = 0$ für alle $\sigma \in G$ ist, muss auch f_α ein Teiler von m_α sein. Da beide Polynome normiert sind, stimmen sie überein.

(ii) Nach (i) zerfallen alle irreduziblen Polynome aus $K[X]$, welche eine Nullstelle in L besitzen schon über L und somit ist L/K normal. Genauso ist die Erweiterung separabel, denn die Minimalpolynome aller $\alpha \in L$ haben keine mehrfachen Nullstellen nach (i).
Es bleibt zu zeigen, dass der Grad $[L : K]$ endlich ist und die Galoisgruppe gleich G ist. Aus (i) folgt, dass $[K(\alpha) : K] \leq |G|$ ist für alle $\alpha \in L$. Ist nun aber $K \subset Z \subset L$ ein beliebiger Zwischenkörper, so dass Z/K endlich ist, so besagt der Satz von primitiven Element (Satz 4.12), dass ein $\alpha \in Z$ existiert, so dass $Z = K(\alpha)$ ist und somit $[Z : K] \leq |G|$. Damit muss schon $[L : K]$ endlich sein und damit $[L : K] \leq |G|$ gelten. Da G eine Untergruppe von $\mathrm{Gal}(L/K)$ ist, muss gelten:

$$|G| \leq |\mathrm{Gal}(L/K)| = [L : K] \leq |G|$$

und somit $|G| = [L : K] = |\mathrm{Gal}(L/K)|$, woraus auch $G = \mathrm{Gal}(L/K)$ folgt.

■

Satz 4.14 — Hauptsatz der Galoistheorie. Sei L/K eine endliche Galoiserweiterung mit Galoisgruppe $G = \mathrm{Gal}(L/K)$. Zu einem Zwischenkörper $K \subset Z \subset L$ können wir die Galoisgruppe $\mathrm{Gal}(L/Z)$ bilden und umgekehrt können wir zu einer Untergruppe $H \subset G$ den Fixkörper $K \subset L^H \subset L$ betrachten. Dies liefert zueinander inverse Bijektionen ϕ und ψ

$$\begin{aligned} \{\text{Zwischenkörper } K \subset Z \subset L\} &\leftrightarrow \{\text{Untergruppen von } G\} \\ Z &\overset{\phi}{\mapsto} \mathrm{Gal}(L/Z) \\ L^H &\overset{\psi}{\longmapsto} H. \end{aligned}$$

Weiterhin gilt:

(i) Die Abbildungen ϕ und ψ sind inklusionsumkehrend, d.h., sind $H \subset H' \subset G$ Untergruppen von G, so ist $K = L^G \subset L^{H'} \subset L^H$ sowie: ist $K \subset Z \subset Z' \subset L$, so ist $\mathrm{Gal}(L/Z') \subset \mathrm{Gal}(L/Z) \subset \mathrm{Gal}(L/K)$.

(ii) Die Normalteiler von G entsprechen genau den Zwischenkörpern von L/K, die normal über K sind und für diese ist

$$G/H \cong \mathrm{Gal}(L^H/K)$$

wobei der Isomorphismus induziert wird durch die Abbildung $G \to \mathrm{Gal}(L^H/K)$ gegeben durch $\sigma \mapsto \sigma|_{L^H}$.

Bemerkung 4.14 Die Erweiterungen L/Z im Satz sind stets Galoiserweiterungen. Wir hatten gesehen, dass wenn L/K normal ist, auch L/Z für einen Zwischenkörper normal ist und aus L/K separabel folgt genauso L/Z separabel (und auch Z/K, aber das ist hierfür nicht relevant).

Beweis von Satz 4.14.

(i) Da L/K endlich ist, ist auch G endlich und hat die Ordnung $|G| = [L : K]$ (siehe Bemerkung 4.12). Wir überlegen zunächst, warum die Definitionen von ϕ und ψ Sinn ergeben. Zu ψ sei auf Bemerkung 4.13 verwiesen, wonach zu einer Untergruppe H von G der Fixkörper L^H ein Zwischenkörper von L/K ist (K ist natürlich in L^H enthalten). Zu ϕ: Ist $K \subset Z \subset L$ ein Zwischenkörper, so ist $\mathrm{Gal}(L/Z) = \mathrm{Aut}_Z(L)$ klarerweise eine Untergruppe von $\mathrm{Aut}_K(L) = \mathrm{Gal}(L/K)$.
Wir haben bereits in Satz 4.13 gezeigt, dass $\phi \circ \psi = \mathrm{id}$ die Identität auf der Menge der Untergruppen

von G ist. Für jede Untergruppe H von G ist $\psi(H) = L^H$ ein Zwischenkörper von L/K wobei nach Satz 4.13 die Erweiterung L/L^H eine Galoiserweiterung mit Galoisgruppe H ist. Damit ist $\phi(\psi(H)) = \mathrm{Gal}(L/L^H) = H$.
Wir zeigen nun, dass auch $\psi \circ \phi = \mathrm{id}$ die Identität auf der Menge der Zwischenkörper von L/K ist. Sei Z ein Zwischenkörper. Dann ist L/Z eine Galoiserweiterung, denn sie ist normal (dies ist Bemerkung 4.10, (i)) und separabel (dies ist Proposition 4.5). Sei $H := \phi(Z) \subset G$. Wir erinnern daran, dass

$$\psi(H) = L^H = \{x \in L \mid \sigma(x) = x \text{ für alle } \sigma \in H\}$$

und damit $Z \subset L^H$, denn $\sigma(x) = x$ für alle $\sigma \in \mathrm{Gal}(L/Z) = H$ und alle $x \in Z$. Andererseits ist nach Satz 4.13 die Erweiterung L/L^H eine Galois-Erweiterung mit Galoisgruppe H und somit $[L : L^H] = |H|$ aber auch $[L : Z] = |H|$, da L/Z eine Galoiserweiterung ist und damit $[L : Z] = |\mathrm{Gal}(L/Z)| = |H|$ ist. Es gilt also $Z = L^H$, d.h. $\psi(\phi(Z)) = \psi(H) = L^H = Z$.
Dass die beiden Abbildungen inklusionsumkehrend sind, ist klar.

(ii) Ist nun Z ein Zwischenkörper und Z/K normal, so ist Z/K eine Galoiserweiterung. Sei $H = \phi(Z) = \mathrm{Gal}(L/Z)$ die entsprechende Untergruppe von G. Es ist also $Z = L^H$. Wir müssen zeigen, dass H ein Normalteiler in G ist.
Ist $\sigma \in G$, so erhalten wir ein Element in $\mathrm{Gal}(L^H/K)$ durch Einschränkung: $\sigma \mapsto \sigma|_{L^H}$. A priori ist $\sigma|_{L^H}$ eine Abbildung $L^H \to L$. Da aber L^H/K normal ist, besitzt jede solche Einschränkung das selbe Bild, und beschränkt sich somit zu einem Automorphismus von L^H wie wir im Beweis von Satz 4.9 gesehen haben. Im Übrigen lässt sich jeder Homomorphismus $L^H \to L$ so gewinnen, denn L/L^H ist normal, so dass die Minimalpolynome der Erzeuger von L/L^H über L komplett in Linearfaktoren zerfallen und sich somit jeder K-Homomorphismus $L^H \to L$ zu einem K-Homomorphismus $L \to L$ erweitern lässt (siehe Proposition 4.2).
Diese Einschränkungsabbildung ist also ein surjektiver Gruppenhomomorphismus $\varphi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(L^H/K)$. Der Kern dieser Abbildung ist gegeben durch

$$\mathrm{Kern}\,\varphi = \{\sigma \in G \mid \sigma(x) = x \text{ für alle } x \in L^H\} = \mathrm{Gal}(L/Z) = H$$

und somit ist H ein Normalteiler (als Kern eines Gruppenhomomorphismus). Zudem ist ihr Bild (also $\mathrm{Gal}(L^H/K)$) nach dem Homomorphiesatz (bzw. Korollar 2.2) isomorph zu G/H, wie behauptet.
Sei nun umgekehrt $H \subset G$ ein Normalteiler. Es ist nur noch zu zeigen, dass dann L^H/K normal ist. Wir wissen, dass L/K normal ist und damit ist auch L/L^H normal. Sei nun $\sigma : L^H \to L$ ein K-Homomorphismus. Wir können σ auf L ausdehnen und so der Einfachheit halber $\sigma \in \mathrm{Gal}(L/K)$ für den Moment annehmen.
Wir zeigen nun, dass allgemein für jede Untergruppe H gilt, dass $\sigma(L^H) = L^{\sigma H \sigma^{-1}}$ ist. Damit folgt dann, dass, falls H normal ist, dass $\sigma(L^H) = L^H$ für jedes $\sigma \in \mathrm{Gal}(L/K)$ gilt.
Ist $x \in \sigma(L^H)$, so existiert ein $y \in L^H$ mit $x = \sigma(y)$. Sei außerdem $\tau \in H$, so ist $\sigma(\tau(\sigma^{-1}(x))) = \sigma(\tau(y)) = \sigma(y) = x$ und somit gilt $\sigma(L^H) \subset L^{\sigma H \sigma^{-1}}$. Da aber sowohl $L^{\sigma H \sigma^{-1}}$ als auch $\sigma(L^H)$ Zwischenkörper von L/K sind, die den gleichen (endlichen) Grad über K haben, muss $\sigma(L^H) = L^{\sigma H \sigma^{-1}}$ gelten.
Dass deshalb L^H normal über K sein muss kann man so einsehen: Startet man mit einem K-Homomorphismus σ von L^H nach L, so zeigt unser Argument, dass σ de facto ein K-Automorphismus von L^H ist. Wie im Beweis von Satz 4.11 impliziert dies, dass L^H/K normal ist.
Wenn Sie der letzte Satz nicht überzeugt oder Sie sich nicht an den Beweis erinnern, so kann man auch folgende Überlegung anstellen: ist $\alpha \in L^H \subset L$ und f das Minimalpolynom von f über K, so permutiert $\mathrm{Gal}(L/K)$ die Nullstellen von f in L und diese Operation ist transitiv, d.h. die Menge der Nullstellen von f in L ist durch $\{\sigma(\alpha) \mid \sigma \in \mathrm{Gal}(L/K)\}$ gegeben. Es ist aber nach unserer Argumentation $\sigma(\alpha) \in L^H$ für jedes $\sigma \in \mathrm{Gal}(L/K)$ und somit sind alle Nullstellen von f schon in L^H enthalten. Also ist L^H normal.
Damit haben wir den Beweis abgeschlossen.

■

Beispiel 4.8 Eine *biquadratische Erweiterung* von $\mathbb{Q}$ ist eine Erweiterung der Form $L := \mathbb{Q}(\sqrt{k}, \sqrt{\ell})$, wobei $k, \ell \in \mathbb{Z}$ mit $\sqrt{k}, \sqrt{\ell} \notin \mathbb{Z}$ und ℓ nicht von der Form $x^2 k$ mit $x \in \mathbb{Q}$, so dass $\sqrt{\ell} \notin \mathbb{Q}(\sqrt{k})$ ist. (Alternativ kann

man auch sagen, L/K heißt biquadratisch, wenn $[L:K]=4$ ist und $L=K(\alpha,\beta)$ gilt mit $\alpha^2,\beta^2\in K$.)

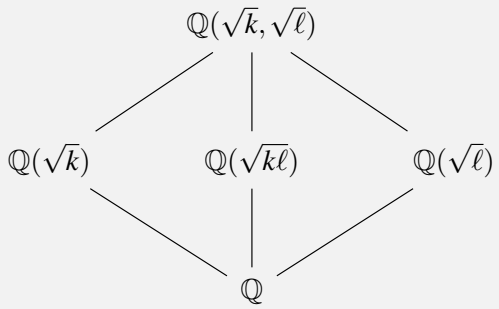
Eine biquadratische Erweiterung ist stets eine Galoiserweiterung mit Galoisgruppe (isomorph zu) $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Dies kann man so sehen: Da L der Zerfällungskörper von $(X^2-k)(X^2-\ell)$ ist, ist $L/\mathbb{Q}$ normal und separabel ist die Erweiterung, da wir in Charakteristik 0 sind. Somit ist es eine Galoiserweiterung.

Die Bedingungen an k und ℓ stellen sicher, dass $[L:\mathbb{Q}]=4$ ist. Damit gibt es nur 2 Möglichkeiten für die Galoisgruppe von $L/\mathbb{Q}$. Da es aber mindestens die 2 echten Zwischenkörper $\mathbb{Q}(\sqrt{k})$ und $\mathbb{Q}(\sqrt{\ell})$ gibt, kann $\mathrm{Gal}(L/\mathbb{Q})$ nach dem Hauptsatz der Galoistheorie nicht zyklisch sein. (Denn: $\mathbb{Z}/4\mathbb{Z}$ hat nur eine echte, nicht-triviale Untergruppe.)

Die Gruppe $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ hat aber insgesamt 3 nicht-triviale Untergruppen. Diese sind alle zyklisch und werden erzeugt von $(1,0)$, $(0,1)$ bzw. $(1,1)$. Nach dem Haupsatz der Galoistheorie gibt es also 3 (nicht-triviale) Zwischenkörper. Wir können $\mathrm{Gal}(L/\mathbb{Q})$ wie folgt mit $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ identifizieren: In $\mathrm{Gal}(L/\mathbb{Q})$ gibt es in jedem Falle die Elemente σ,τ, gegeben durch $\sigma(\sqrt{k})=-\sqrt{k},\sigma(\sqrt{\ell})=\sqrt{\ell}$ sowie $\tau(\sqrt{k})=\sqrt{k},\tau(\sqrt{\ell})=-\sqrt{\ell}$. Man kann jetzt beispielsweise einen Gruppenhomomorphismus auf den Erzeugern von $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ definieren durch $(1,0)\mapsto\sigma$ und $(0,1)\mapsto\tau$. Damit ist der Homomorphismus eindeutig bestimmt und injektiv, da σ und τ beide nicht die Identität sind und außerdem $(1,1)\mapsto\sigma\circ\tau\neq\mathrm{id}_L$ ist.

Wir erhalten also die Zwischenkörper $L^{\langle\sigma\rangle}=\mathbb{Q}(\sqrt{\ell})$, $L^{\langle\tau\rangle}=\mathbb{Q}(\sqrt{k})$, $L^{\langle\tau\circ\sigma\rangle}=\mathbb{Q}(\sqrt{k\ell})$ und die trivialen Zwischenkörper $L=L^{\mathrm{id}_L}$ und $\mathbb{Q}=L^{\mathrm{Gal}(L/\mathbb{Q})}$.

Das entsprechende Körperdiagramm sieht so aus:



Übung 4.1 Analog kann man zum Beispiel $L=\mathbb{Q}(\sqrt{p_1},\ldots,\sqrt{p_n})$ für alles verschiedene Primzahlen $p_1,\ldots,p_n$ betrachten. Man kann per Induktion zeigen, dass $L/\mathbb{Q}$ eine Galoiserweiterung mit Galoisgruppe $\mathrm{Gal}(L/\mathbb{Q})\cong(\mathbb{Z}/2\mathbb{Z})^n$ ist. Außerdem gilt $\mathbb{Q}(\sqrt{p_1},\ldots,\sqrt{p_n})=\mathbb{Q}(\sqrt{p_1}+\ldots+\sqrt{p_n})$. ∎

Beispiel 4.9 Die Körpererweiterung $\mathbb{Q}(\sqrt[4]{2},i)/\mathbb{Q}$ ist eine Galoiserweiterung vom Grad 8. Sie ist nämlich Zerfällungskörper von $X^4-2=(X-\sqrt[4]{2})(X+\sqrt[4]{2})(X-i\sqrt[4]{2})(X+i\sqrt[4]{2})$.

Um die Aussage über den Grad zu sehen, stellen wir zunächst fest, dass X^4-2 das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}$ ist. In Kürze werden wir deutlich bessere Methoden entwickeln, um dies zu zeigen aber im vorliegende Fall ist leicht zu sehen, dass kein Produkt von 1, 2 oder 3 Linearfaktoren in dem Produkt $X^4-2=(X-\sqrt[4]{2})(X+\sqrt[4]{2})(X-i\sqrt[4]{2})(X+i\sqrt[4]{2})$ Koeffizienten in $\mathbb{Q}$ hat.

Damit hat $L_1:=\mathbb{Q}(\sqrt[4]{2})$ den Grad 4 über $\mathbb{Q}$. Da aber $\sqrt[4]{2}\in\mathbb{R}$ ist, erhalten wir, dass $L/\mathbb{Q}$ den Grad 8 hat.

Es ist also $|\mathrm{Gal}(L/\mathbb{Q})|=8$.

Wir wollen nun zeigen, dass $G:=\mathrm{Gal}(L/\mathbb{Q})\cong D_4$ isomorph zur Diedergruppe D_4 ist. Sei dazu σ der Automorphismus von L, welcher durch $\sqrt[4]{2}\mapsto i\sqrt[4]{2}$ und $i\mapsto i$ definiert wird (Fortsetzung der Identität von $\mathbb{Q}(i)$ auf L). Außerdem sei τ der Automorphismus von L, welcher durch $i\mapsto -i$ und $\sqrt[4]{2}\mapsto\sqrt[4]{2}$ definiert ist (Fortsetzung der Identität von L_1 auf L).

Dann hat σ Ordnung 4 und τ hat Ordnung 2. Es ist $\tau(\sigma(\sqrt[4]{2}))=\tau(i\sqrt[4]{2})=-i\sqrt[4]{2}$ aber $\sigma(\tau(\sqrt[4]{2}))=\sigma(\sqrt[4]{2})=i\sqrt[4]{2}$. Also ist G nicht kommutativ und es gibt insgesamt nur 2 nicht-abelsche Gruppen der Ordnung 8 – die Diedergruppe D_4 und die Quaternionengruppe Q (dies ist die endliche (multiplikative) Untergruppe der Hamiltonschen Quaternionen mit den Elementen $\pm1,\pm i,\pm j,\pm k$; es ist eine nette Übungsaufgabe zu seigen, dass dies die einzigen nicht-abelschen Gruppen der Ordnung 8 sind). In der Quaternionengruppe gibt es 6 Elemente der Ordnung 4. In G gibt es jedoch nur 2 Elemente der Ordnung 4 (σ und σ^3), also haben wir es mit der Diedergruppe zu tun. Man kann das auch ohne das Wissen um die Klassifikation der Gruppen der Ordnung 8 beweisen, indem man einfach nachrechnet, dass die durch $\sigma\mapsto(1,2,3,4)$ und $\tau\mapsto(2,4)$

definierte Abbildung $\mathrm{Gal}(L/\mathbb{Q}) \to D_4$ (definiert als Untergruppe der S_4 wie in Beispiel 5.7), ein injektiver Gruppenhomomorphismus ist.

Die Gruppe G hat 3 Untergruppen der Ordnung 4 (diese sind Normalteiler) und weitere 5 Untergruppen der Ordnung 2, von denen nur eine ein Normalteiler ist. Demnach hat $K \subset L$ also 8 echte Zwischenkörper, von denen 3 auch Galois über $\mathbb{Q}$ sind.

5. Etwas mehr Gruppentheorie

5.1 Gruppenoperationen

In Kapitel 2 haben wir uns eher mit "abstrakten Gruppen" beschäftigt. Das ist auch sehr wichtig, aber es ist aus verschiedenen Gründen oft hilfreich Gruppen nicht ausschließlich für sich genommen zu betrachten, sondern als "auf einer Menge operierend". Diese Menge kann auch die Gruppe selber sein und selbst dann ist diese Perspektive oft nützlich.

Wir beginnen mit einem Beispiel: eine der ersten Gruppen, die man im Studium kennenlernt, ist die symmetrische Gruppe S_n ($n \in \mathbb{N}$). Die Definition dieser Gruppe(n) beinhaltet bereits die Beschreibung der Gruppe als eine Menge von Abbildungen, die auf einer anderen Menge ($\{1,2,\dots,n\}$) operiert. Gegeben irgendeine Menge M, haben wir außerdem die Gruppe $S(M)$ der bijektiven Abbildungen $M \to M$ definiert. Auch diese Gruppen nennt man symmetrische Gruppen und wenn M die endliche Ordnung n hat, dann ist $S(M)$ (nicht-kanonisch) isomorph zu S_n. Aber auch alle anderen endlichen "abstrakten" Gruppen findet man so wieder:

Satz 5.1 — Cayley. Jede Gruppe G kann in eine symmetrische Gruppe eingebettet werden.

Bemerkung 5.1 Formulieren wir den Satz etwas konkreter: gegeben G, existiert ein injektiver Gruppenhomomorphismus $\iota_G : G \to S(G)$ in die symmetrische Gruppe $S(G)$ (welche man, falls G endlich ist mit $n = |G|$, mit S_n identifizieren kann).

Beweis. Für jedes $g \in G$ definieren wir die Abbildung

$$\varphi_g : G \to G, \quad h \mapsto gh.$$

Da φ_g bijektiv ist, gilt also $\varphi_g \in S(G)$ – das Inverse von φ_g ist durch $\varphi_{g^{-1}}$ gegeben. Außerdem gilt $\varphi_g \circ \varphi_h = \varphi_{gh}$ und damit ist die Abbildung $G \to S(G)$ gegeben durch $g \mapsto \varphi_g$ ein Gruppenhomomorphismus. Dieser ist injektiv, denn wenn $\varphi_g = \mathrm{id}_G$ gilt, dann ist $gh = h$ für alle $h \in G$ und damit $g = 1$. (Ist G endlich und nummeriert man nun die Elemente von G in irgendeiner Weise als $g_1,\dots,g_n$, so erhält man einen (nicht-kanonischen) Isomorphismus $S(G) \cong S_n$.) ■

Definition 5.1 Sei G eine Gruppe und M irgendeine Menge. Eine *Gruppenoperation* von G auf M ist ein Homomorphismus $G \to S(M)$. Wir sagen auch, dass *G auf M operiert*.

In anderen Worten, bei einer Gruppenoperation von G auf M definiert man zu jedem Element g aus G eine bijektive Abbildung $\pi_g : M \to M$ und das in einer Weise, die mit der Gruppenstruktur von G kompatibel ist. Es gilt also $\pi_g \circ \pi_h = \pi_{gh}$ (sowie $\pi_1 = \mathrm{id}_M$).

Beispiel 5.1 Die Gruppe S_n operiert auf $M = \{1,2,\ldots,n\}$ (schon per Definition ist der Homomorphismus in Definition 5.1 einfach die Identität).

Notation 5.1 Sei $\alpha : G \to S(M)$ eine Gruppenoperation. Wenn im Zusammenhang klar ist, welche Gruppenoperation gemeint ist, schreiben wir diese oft auch vereinfachend als Multiplikation, zum Beispiel $g \cdot x$ für $\alpha(g)(x)$ oder sogar einfach gx für $g \in G$ und $x \in M$.

Beispiel 5.2 Sei G eine Gruppe. Dann operiert G auf sich selbst ($M = G$) durch verschiedene Operationen, insbesondere:

(i) *Linksmultiplikation* (wie im Beweis von Satz 5.1), d.h. der Homomorphismus $G \to S(G)$ ist gegeben durch $g \mapsto \varphi_g$, wobei $\varphi_g : G \to G$ durch $\varphi_g(h) = gh$ für alle $h \in G$ definiert ist.

(ii) *Konjugation*: $g \in G$ operiert durch die Abbildung $h \mapsto ghg^{-1}$.

Dass man diese Notation sehr natürlich verwenden kann, zeigt das folgende einfache Resultat:

Proposition 5.1 Die Gruppe G operiere auf der Menge M. Es gilt:

(i) Falls $y = gx$ ist mit $g \in G$ und $x, y \in M$, dann ist $g^{-1}y = x$.

(ii) Sei $g \in G$, dann gilt für $x \neq y$ stets $gx \neq gy$ (oder anders: falls $gx = gy$ gilt, so ist $x = y$).

Beweis. Angenommen $y = gx$, dann gilt auch $g^{-1}y = g^{-1}(gx) = (g^{-1}g)x = 1x = x$ (man mache sich noch mal klar, wie dies in der Notation der ursprünglichen Definition (Definition 5.1) aussähe, damit klar wird, das hier etwas wirklich Neues gezeigt wird, und nicht etwa das Rechnen in einer Gruppe wiederholt wird.)

Es gelte nun $gx = gy$. Dann folgt schon $x = y$ da es sich bei der Abbildung $x \mapsto gx$ um eine bijektive und damit insbesondere injektive Abbildung handelt. ■

Definition 5.2 Sei G eine Gruppe, die auf einer Menge M operiert. Wir definieren die *Bahn* (oder auch Orbit) von $x \in M$ als

$$\text{Bahn}(x) := Gx := \{gx \mid g \in G\} \subset M$$

sowie den *Stabilisator* von $x \in M$ in G als

$$\text{Stab}(x) := G_x := \{g \in G \mid gx = x\} \subset G$$

Ein Punkt $x \in M$ wird *Fixpunkt* von G genannt, wenn $G_x = G$ bzw $\text{Bahn}(x) = \{x\}$ gilt. Falls es nur eine Bahn gibt, so sagen wir, dass G *transitiv* auf M operiert.

Bemerkung 5.2 Dass G transitiv auf M operiert ist gleichbedeutend mit folgender Formulierung: Es gibt ein $x_0 \in M$, so dass für alle $x \in M$ ein $g \in G$ existiert mit $gx_0 = x$.

Beispiel 5.3 Eines der wichtigsten Beispiele für diese Vorlesung ist die Operation der Galoisgruppe: Sei L/K eine Körpererweiterung. Sei $\sigma \in \text{Aut}_K(L)$ und $\alpha \in L$ algebraisch über K mit Minimalpolynom $f_\alpha \in K[X]$. Dann ist $\sigma(\alpha)$ wieder eine Nullstelle von f_α. Also: Die Gruppe $\text{Aut}_K(L)$ operiert auf den Nullstellen von f_α in L, d.h. wir erhalten eine Gruppenoperation der Gruppe $\text{Aut}_K(L)$ auf der Menge $M = \{\beta \in L \mid f_\alpha(\beta) = 0\}$ durch $\pi_\sigma = \sigma|_M$. Diese ist nach Proposition 4.1 transitiv.

Etwas spezieller sei L/K der Zerfällungskörper eines Polynoms irreduziblen Polynoms $f \in K[X]$. Hat f den Grad n, so hat f also n verschiedene Nullstellen $\alpha_1, \ldots, \alpha_n$ in L. Die Operation der Galoisgruppe $\text{Gal}(L/K)$ auf diesen n Nullstellen ist damit auch *transitiv* und außerdem ist ein Element $\sigma \in \text{Gal}(L/K)$ schon vollständig durch die Bilder $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$ bestimmt. Wir können damit $\text{Gal}(L/K)$ als eine Untergruppe von S_n realisieren.

Satz 5.2 Sei G eine Gruppe, die auf einer Menge M operiere. Es gilt

(i) Verschiedene Bahnen sind disjunkt.

(ii) Der Stabilisator G_x von $x \in M$ ist eine Untergruppe von G und $G_{gx} = gG_xg^{-1}$.

(iii) Es gilt $gx = hx$ genau dann wenn g und h in der gleichen Linksnebenklasse von G_x liegen (d.h.

$gG_x = hG_x$). Insbesondere gilt die *Bahnformel*:

$$|\mathrm{Bahn}(x)| = [G : G_x].$$

(iv) Wenn M endlich ist, so seien $x_1, \ldots, x_r \in M$ Repräsentanten der verschiedenen Bahnen der Operation von G auf M. Es gilt dann

$$|M| = \sum_{i=1}^{r} [G : G_{x_i}]$$

(diese Formel wird auch oft Bahnformel genannt).

Beispiel 5.4 Eine Gruppe G operiert auf der Menge G/H der Nebenklassen von H in G durch $X \mapsto gX$ für $g \in G$ und $X \in G/H$. Die Bahn von H ist gegeben durch $\mathrm{Bahn}(H) = \{gH \mid g \in G\}$, also die Menge der Nebenklassen G/H (die Operation ist transitiv). Der Stabilisator von H ist $\mathrm{Stab}(H) = \{g \in G \mid gH = H\} = H$ und die Aussage von Satz 5.2, (iii) ist gerade die Definition des Index $[G : H]$.

Beispiel 5.5 Eine Untergruppe $H \subset G$ operiert auf G auch durch Rechtsmultiplikation mit dem Inversen: $\pi_h(g) := gh^{-1}$. Dabei ist die Bahn eines Elementes $g \in G$ gegeben durch die Linksnebenklasse $\mathrm{Bahn}(g) = gH$. Der Stabilisator ist trivial $\mathrm{Stab}(g) = \{1\}$ und damit lautet in diesem Falle Satz 5.2, (iv) für eine endliche Gruppe G:

$$|G| = [G : H] \cdot |H|,$$

was genau die Aussage vom Satz von Lagrange ist (Satz 2.1). Man könnte also im Prinzip auch zuerst Satz 5.2 beweisen und dann Satz 2.1 daraus folgern. Allerdings benutzt der Beweis vom Satz von Lagrange im Prinzip das exakt gleiche Argument, wie der nun folgende Beweis – erkennen Sie das Argument wieder?

Beweis von Satz 5.2.

(i) Wir zeigen: Falls $\mathrm{Bahn}(x) \cap \mathrm{Bahn}(y) \neq \emptyset$, dann muss schon $\mathrm{Bahn}(x) = \mathrm{Bahn}(y)$ gelten.
Sei $z \in \mathrm{Bahn}(x) \cap \mathrm{Bahn}(y)$. Dann existieren also $g, h \in G$, so dass $z = gx = hy$ ist.
Damit ist aber $x = g^{-1}hy$ und somit für $a \in \mathrm{Bahn}(x)$ mit $a = g'x$ auch $a \in \mathrm{Bahn}(y)$, da $a = g'g^{-1}hy$ gilt sowie analog mit $b \in \mathrm{Bahn}(y)$, $b = h'y$ auch $b \in \mathrm{Bahn}(y)$, da $b = h'h^{-1}gx$ ist.

(ii) (a) Klar ist $1 \in G_x$. Außerdem, sind mit $g, h \in G_x$ auch $gh \in G_x$, denn $ghx = gx = x$.
Ist $g \in G_x$, so ist auch $g^{-1} \in G_x$, denn $g^{-1}x = g^{-1}gx = 1 \cdot x = x$, da $g \in G_x$.
Damit ist G_x eine Untergruppe von G.

(b) Wir berechnen noch den Stabilisator von gx: Sei $h \in G$ und es gelte $h(gx) = gx$, dann ist also $g^{-1}hgx = x$, d.h. $g^{-1}hg \in G_x$, was gleichbedeutend mit $h \in gG_xg^{-1}$ ist. Umgekehrt, ist $h = gg'g^{-1}$ mit $g' \in G_x$, so ist $hgx = gg'g^{-1}gx = gg'x = gx$ und damit ist $h \in G_x$.

(iii) Angenommen es gelte $gx = hx$ mit $x \in M$ und $g, h \in G$.
Dann ist $h^{-1}g \in G_x$ und das heißt genau, dass $gG_x = hG_x$ (genauer: $h^{-1}g = \alpha \in G_x$, also $g \in hG_x$ und genauso $g^{-1}h = \alpha^{-1} \in G_x$, also $h \in gG_x$ und damit folgt die Gleichheit der Nebenklassen).
Also ist die Anzahl $|Bahn(x)|$ gleich der Anzahl der verschiedenen Nebenklassen von G_x in G und die Formel folgt.

(iv) Für die zweite Formel bemerke man, dass M die disjunkte Vereinigung der Bahnen ist: Jedes M ist in einer Bahn enthalten, denn $x \in \mathrm{Bahn}(x)$. Gleichzeitig ist jedes x in nur genau einer Bahn enthalten, da verschiedene Bahnen disjunkt sind, nach (i).

■

Bemerkung 5.3 In Satz 5.2 ist $|G| = \infty$ zugelassen. Es kann dann auch $|\mathrm{Bahn}(x)| = \infty$ sein, und in diesem Fall hat der Stabilisator von x unendlichen Index in G.

Beispiel 5.6 Die Gruppe G operiert auf sich selbst durch Konjugation wie oben beschrieben. Dabei nennt

man $\mathrm{Bahn}(g)$ für $g \in G$ auch die *Konjugationsklasse* von g. Der Stabilisator ist gegeben durch $\mathrm{Stab}(g) := \{h \in G \mid hg = gh\}$ und wird *Zentralisator* (wir schreiben hierfür $Z_G(g)$) von g in G genannt.

In diesem Zusammenhang ist der folgende Satz erwähnenswert, der in Kürze einige wichtige Anwendungen finden wird.

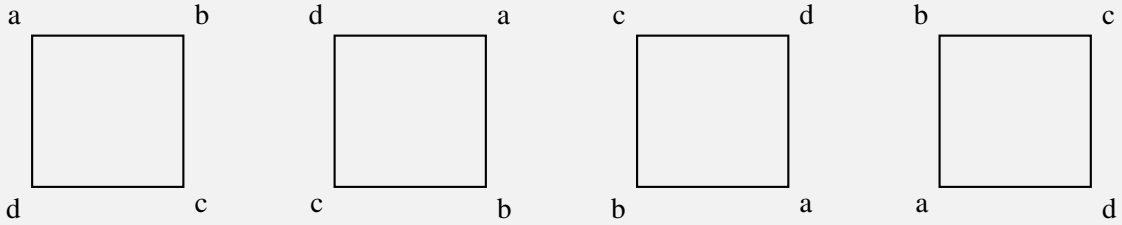
Satz 5.3 Für eine endliche Gruppe G gilt die *Klassengleichung*:

$$|G| = |Z(G)| + \sum_{j=1}^{n} [G : Z_G(x_j)] = |Z(G)| + \sum_{j=1}^{n} |K_j|,$$

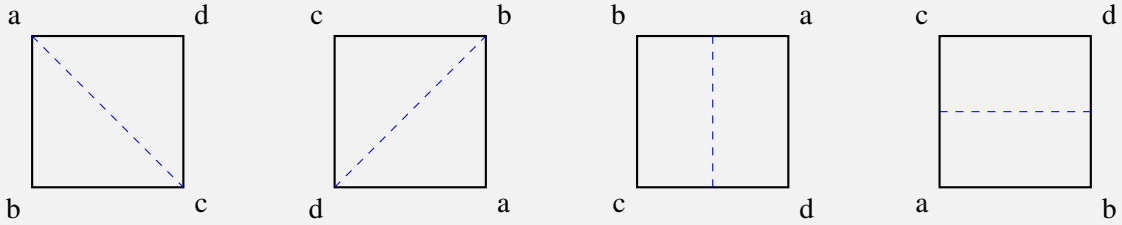
wobei $x_1, \ldots, x_n$ Repräsentanten der n verschiedenen Konjugationsklassen $K_j := \{gx_jg^{-1} \mid g \in G\} \neq \{1\}$ mit mehr als einem Element seien.

Beweis. Der Beweis ist eine Übung. ■

Beispiel 5.7 Ein geometrisches Beispiel: Seien $M = \{a,b,c,d\}$ die Ecken eines Quadrats und D_4 sei die Gruppe der Symmetrien des Quadrats (diese *Diedergruppe* (vom Grad 4) haben wir bereits abstrakt in den Übungen kennen gelernt – Achtung: hier gehen die Bezeichnungen auseinander, manche Autoren bezeichnen die gleiche Gruppe als D_8, da sie 8 Elemente hat). Dies sind alle Permutationen von M, welche die geometrische Figur, das Quadrat, erhalten. Das sollte man sich so vorstellen: Die Seiten des Quadrats verbinden die Ecken und diese Verbindungen dürfen nicht aufgelöst werden. Wie kann ich die Ecken nun noch permutieren? Die ersten 4 Elemente dieser Gruppe sind die Identität und die 3 nicht-trivialen Drehungen:



Außerdem gibt es noch 4 Spiegelungen:



Man kann sich leicht überlegen, dass dies alle Symmetrien sind. Wir gehen mal den mühsamen Weg und überlegen uns, dass alle weiteren Permutationen der Menge M keine Symmetrien des Quadrates sind: Zunächst mal sind die 4 Transpositionen (a,b), (b,c), (a,d) und (c,d) sind klarerweise keine Element von D_4, denn alle von diesen haben die Eigenschaft, dass danach einzelne Ecken nicht mehr die gleichen Nachbarn haben. Zum Beispiel bei (a,b): hier hat c jetzt die Nachbarn a und d (anstatt b und d).

Wir wissen, dass S_4 insgesamt $4! = 24$ Elemente hat. 8 davon haben wir als Elemente von D_4 identifiziert und 4 ausgeschlossen. Nun schauen wir uns die 3-er Zykel an: diese erhalten Nachbarschaft ebenso nicht, z.B. bei (a,b,c) hat a nach dem Permutieren die Nachbarn b und c, vorher jedoch b und d, weshalb es sich nicht um eine Symmetrie des Quadrats handelt. Von den 3-er Zykeln gibt es insgesamt 8 und alle müssen also ausgeschlossen werden.

Ähnliche Überlegungen führen dazu, noch die vier 4-er Zykel (a,b,d,c), (a,c,b,d), (a,c,d,b) sowie (a,d,b,c) auszuschließen (wieder mit dem Nachbarschaftskriterium). Damit haben wir nun $4+8+4 = 16$ Elemente ausgeschlossen, es verbleiben nur 8 und die haben wir oben schon aufgelistet.

Wir sehen schon an den Drehungen, dass D_4 transitiv auf M operiert, die Bahn von a ist die ganze Menge $M = \mathrm{Bahn}(a)$. Der Stabilisator von a ist gegeben durch die Identität und die erste Spiegelung (b,c).

Damit bestätigt sich die Bahngleichung, nach der die Länge der Bahn eines Elementes ($= 4$) gleich dem Index des Stabilisators in der Gruppe D_4 sein soll und in der Tat ist der Index einer 2-elementigen Untergruppe in der 8-elementigen Gruppe D_4 nach dem Satz von Lagrange gleich 4.

Satz 5.4 — Cauchy. Sei G eine endliche Gruppe und p eine Primzahl mit $p \mid |G|$. Dann enthält G ein Element der Ordnung p.

Beweis. Wir beweisen den Satz per Induktion nach $m \in \mathbb{N}$, wobei die Gruppenordnung gegeben sei durch $|G| = mp$.

Für $m = 1$ ist die Aussage schon in Korollar 2.4 enthalten.

(i) Wir zeigen den Satz zunächst für abelsche Gruppen. Sei also $m > 1$ und die Aussage sei für abelsche Gruppen der Ordnung pn mit $n < m$ bewiesen. Sei $g \in G$ mit $g \neq 1$. Falls die Ordnung von g durch p teilbar ist, so hat $h = g^{\mathrm{ord}(g)/p}$ Ordnung p und wir sind fertig. Falls jedoch p nicht die Ordnung von g teilt, betrachten wir die zyklische Untergruppe $H := \langle g \rangle$ und es ist G/H eine abelsche Gruppe der Ordnung pn mit $n < m$. Damit gibt es in G/H ein Element $g'H$ der Ordnung p. Dann ist die Ordnung $\mathrm{ord}(g')$ durch p teilbar, denn falls $(g')^s = 1$ ist, so ist $(g'H)^s = (g')^s H = H$ und damit sind wir im Fall von oben.

(ii) Für nicht-abelsche Gruppen kann man nicht ganz genau so verfahren, weil nicht jede Untergruppe ein Normalteiler ist! Sei wieder $m > 1$ und die Aussage sei für beliebige Gruppen der Ordnung pn mit $n < m$ bewiesen.
Es sei also G nicht abelsch von der Ordnung pm und es sei $x \in G$ mit $x \notin Z(G)$. Dann betrachten wir die Operation von G auf sich selbst durch Konjugation. Die Ordnung der Bahn Gx eines $x \in G$ ist gleich

$$|Gx| = [G : Z_G(x)]$$

nach Satz 5.2.
Dann enthält also die Bahn Gx von x mehr als ein Element. Nun teilt entweder p die Ordnung der Untergruppe $Z_G(x) \subset G$ oder p teilt den Index $[G : Z_G(x)]$ (dies folgt aus dem Satz von Lagrange). Im ersten Fall können wir die Induktionsannahme auf $Z_G(x)$ anwenden, denn $Z_G(x) \neq G$, da $|Gx| \neq 1$ und erhalten so ein Element der Ordnung p in $Z_G(x) \subset G$.
Wir nehmen nun an, dass für alle $x \in G$, $x \notin Z(G)$ gelte, dass p **nicht** die Gruppenordnung $Z_G(x)$ teilt und damit p ein Teiler von $[G : Z_G(x)]$ für alle $x \in G$ mit $x \notin Z(G)$ ist.
Die Klassengleichung besagt dann, dass

$$|G| = |Z(G)| + \sum_{j=1}^{k} [G : Z_G(x_j)],$$

wobei $x_1, \ldots, x_k$ Repräsentanten der Konjugationsklassen sind. Da p die Ordnung der Gruppe G teilt und p alle Indizes auf der rechten Seite teilt, muss p auch ein Teiler von $|Z(G)|$, der Ordnung des Zentrums sein. Damit können wir nun den schon bewiesenen Fall, den einer abelschen Gruppe, auf $Z(G)$ anwenden und erhalten so ein Element $g \in Z(G) \subset G$ der Ordnung p.

■

Bemerkung 5.4 Die Aussage des Satzes von Cauchy lässt sich nicht auf beliebige Teiler der Gruppenordnung verallgemeinern. Ein Beispiel hatten wir schon erwähnt: Die alternierende Gruppe A_4 hat Ordnung $12 = 4 \cdot 3$. Sie besitzt jedoch keine Untergruppe der Ordnung 6.

Übung 5.1 Sei G eine endliche Gruppe, die auf einer endlichen Menge M operiere. Die Anzahl der Bahnen sei r und für $g \in G$ sei $\mathrm{Fix}_g(M) := \{x \in M \mid gx = x\}$ die Menge der Elemente aus M, die durch g fest gehalten werden.

Die Anzahl der Bahnen r ist gleich der durchschnittlichen Anzahl der Fixpunkte der verschiedenen Elemente aus G, d.h.

$$r = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}_g(M)|.$$

■

Beispiel 5.8 Eine Ergänzung zur Diedergruppe D_4: Wenn nach $\mathrm{Fix}_\sigma(M)$ für $\sigma \in D_4$ fragen, so sehen wir, dass die echten Drehungen keine Ecke fest halten. Bei den ersten beiden Spiegelungen werden jeweils zwei Ecken fest gehalten, bei den anderen beiden keine. Damit berechnet sich die Formel in Übung 5.1 zu

$$1 = \frac{1}{8}(4+0+0+0+2+2+0+0),$$

was ja in der Tat korrekt ist.

5.2 p-Gruppen und Sylowsätze

Definition 5.3 Sei $p \in \mathbb{N}$ eine Primzahl und G eine Gruppe. Die Gruppe G heißt *p-Gruppe*, falls die Ordnung jedes Elementes von G eine p-Potenz ist.

Bemerkung 5.5 Eine endliche Gruppe ist genau dann eine p-Gruppe, wenn ihre Ordnung eine p-Potenz ist.

Satz 5.5 Sei G eine endliche, nicht-triviale p-Gruppe. Dann gilt: $p \mid Z(G)$ und damit ist insbesondere $Z(G) \neq \{1\}$.

Beweis. Der Beweis ist Übung - man benutze die Klassengleichung. ■

Übung 5.2 Jede Gruppe G der Ordnung $|G| = p^2$ (p Primzahl) ist abelsch. Welche Fälle gibt es? ■

Definition 5.4 Eine absteigende Kette von Untergruppen

$$G = G_k \supset G_{k-1} \supset \ldots \supset G_0 = \{1\},$$

für irgendein $k \in \mathbb{N}$, so dass G_{j-1} für $j = 1, \ldots, k$ jeweils Normalteiler in G_j ist, nennt man eine *Normalreihe* von G. Die Quotienten G_j/G_{j-1} heißen *Faktoren* der Normalreihe.

Definition 5.5 Eine Gruppe $G \neq \{1\}$, welche als Normalteiler nur G und $\{1\}$ besitzt, wird *einfach* genannt. Dies ist also gleichbedeutend damit, dass jede Normalreihe von G mit nur echten Inklusionen (keine Gleichheit in der Kette) die Länge 1 besitzt. Eine *Kompositionsreihe* einer Gruppe G ist eine Normalreihe in der alle Faktoren einfache Gruppen sind.

Beispiel 5.9 Wir wissen bereits, dass die endlichen Gruppen von Primzahlordnung stets einfach sind.

Bemerkung 5.6 Der *Satz von Jordan-Hölder* besagt, dass alle Kompositionsreihen einer endlichen Gruppe äquivalent sind, d.h., dass die Länge aller Kompositionsreihen gleich ist und die auftretenden Faktoren bis auf Isomorphie (und Permutation) eindeutig bestimmt sind.

Korollar 5.1 — Struktur von p-Gruppen. Sei G eine p-Gruppe der Ordnung p^k. Dann gibt es eine absteigende Kette von Untergruppen

$$G = G_k \supset G_{k-1} \supset \ldots \supset G_0 = \{1\},$$

so dass $|G_j| = p^j$ und G_{j-1} für $j = 1, \ldots, k$ jeweils Normalteiler in G_j ist (also existiert eine Normalreihe von G in der die Faktoren jeweils zyklisch von Ordnung p sind; diese Normalreihe ist also eine Kompositionsreihe von G).

Beweis. Wir können eine Induktion nach k durchführen: Für $k = 0$ ist die Aussage trivial, $G = G_0$.

Sei $k > 0$ und die Behauptung sei für $k-1$ bewiesen. Nach Satz 5.5 ist $Z(G) \neq \{1\}$. Nach dem Satz von Cauchy existiert ein $g \in Z(G)$ mit $\mathrm{ord}(g) = p$ und dementsprechend ist $|\langle g \rangle| = p$. Die von g erzeugte Untergruppe ist ein Normalteiler von G, da $g \in Z(G)$ ist, und die Gruppe $G' = G/\langle g \rangle$ hat Ordnung $|G'| = p^{k-1}$.

Damit gibt es nach Induktionsvoraussetzung eine absteigende Kette von Untergruppen von G':

$$G' = G'_k \supset G'_{k-1} \supset \ldots \supset G'_1 = \{1\},$$

wobei $|G'_j| = p^{j-1}$ und G'_{j-1} jeweils ein Normalteiler in G'_j ist.

Wir betrachten die kanonische Projektion $\pi : G \to G'$ und definieren $G_j := \pi^{-1}(G'_j)$ für $j = 1, \ldots, k$ sowie $G_0 = \{1\}$. Die G_j sind dann Untergruppen von G (Urbilder von Untergruppen unter Homomorphismen sind Untergruppen) und wir erhalten eine absteigende Kette

$$G = G_k \supset G_{k-1} \supset \ldots \supset G_0 = \{1\}.$$

Es gilt außerdem $|G_j| = p^j = |G'_j| \cdot p$ nach dem Satz von Lagrange, denn $G'_j \cong G_j/\langle g\rangle$, d.h. $[G_j : \langle g\rangle] = |G'_j| = p^{j-1}$. Zu guter Letzt stellen wir fest, dass G_{j-1} ein Normalteiler in G_j ist, da $G'_{j-1} \subset G'_j$ Normalteiler ist (Urbilder von Normalteilern unter Homomorphismen sind Normalteiler). ■

Bemerkung 5.7 Die Klassifikation der endlichen einfachen Gruppen wurde erst 2004 engültig abgeschlossen (das Ergebnis war im Prinzip seit 1980 bekannt, aber es gab zahlreiche Lücken). Der Beweis der gesamten Klassifikation erstreckt sich über viele (wohl über 500), teils sehr lange Arbeiten, mit insgesamt ca. 15.000 Seiten. Demnach gibt es folgende unendliche Familien von endlichen einfachen Gruppen: die zyklischen Gruppen von Primzahlordnung, die alternierenden Gruppen A_n für $n \geq 5$ und sogenannte Gruppen vom Lie-Typ über endlichen Körpern. Daneben gibt es noch 26 „sporadische Gruppen".

Definition 5.6 Eine Untergruppe $H \subset G$ einer endlichen Gruppe heißt *p-Sylow-(Unter-)Gruppe* (kurz einfach: p-Sylow), falls H eine p-Gruppe ist, und es gibt $k, m \in \mathbb{N}$, so dass $|H| = p^k$ und $|G| = p^k m$ aber $p \nmid m$.

Bemerkung 5.8 Eine p-Sylow-Gruppe $H \subset G$ ist stets eine eine maximale p-Gruppe in G, d.h. nicht echt in einer p-Untergruppe von G enthalten. Denn: ist H eine p-Sylow-Untergruppe und $H' \subset G$ eine p-Gruppe in G mit $H \subset H'$, $|H| = p^k$ und $|H'| = p^{k'}$, so ist $k' \geq k$ und damit, da k maximal angenommen wurde, schon $k = k'$ und $H = H'$. Die Umkehrung werden wir jetzt in Satz 5.6 zeigen.

Satz 5.6 — Sylowsätze. Sei G eine endliche Gruppe, p eine Primzahl und p^r die größte p-Potenz, welche die Gruppenordnung $|G|$ teilt. Es gilt:

(i) G besitzt p-Sylow-Untergruppen.
(ii) Je zwei p-Sylow-Untergruppen sind zueinander konjugiert.
(iii) Jede Untergruppe von G, die eine p-Gruppe ist, ist in einer p-Sylow-Untergruppe enthalten.
(iv) Die Anzahl s der p-Sylow-Untergruppen von G ist ein Teiler von $m := |G|/p^r$ und es gilt $s \equiv 1 \mod p$.

Bemerkung 5.9 Erinnerung: Die Schreibweise $a \equiv b \mod p$ bedeutet, dass a kongruent zu b modulo p ist, d.h. p teilt $a - b$ bzw. die Restklassen von a und b in $\mathbb{Z}/p\mathbb{Z}$ sind identisch.

Beweis.

(i) Wir benutzen Induktion nach $|G|$. Wir können annehmen, dass p die Ordnung $|G|$ teilt. Falls G eine echte Untergruppe $H \subsetneq G$ besitzt, so dass p nicht den Index $[G : H]$ teilt, folgt die Aussage aus der Induktionsannahme, da dann p^r die Ordnung $|H| < |G|$ teilt. Gibt es eine solche Unterguppe nicht, so erhalten wir genau wie im Beweis des Satzes von Cauchy (Satz 5.4) aus der Klassengleichung, dass p die Ordnung des Zentrums teilt und es damit (nach dem Satz von Cauchy) ein Element $g \in Z(G)$ mit $\mathrm{ord}(g) = p$ gibt.
Es ist dann aber $\langle g\rangle$ ein Normalteiler von G und $G/\langle g\rangle$ eine Gruppe kleinerer Ordnung, die nach Induktionsannahme also eine p-Sylow-Untergruppe (der Ordnung p^{r-1}) enthält deren Urbild unter der kanonischen Projektion eine p-Sylow-Untergruppe von G ist.

(ii)+(iii) Wir betrachten die Menge X aller p-Sylow-Untergruppen von G. Die Gruppe G operiert auf X durch Konjugation, denn $|gHg^{-1}| = |H|$. Um die Lesbarkeit zu verbessern, verwenden wir im Beweis die

folgende Notation: Ist $x = P \in X$ eine p-Sylow-Untergruppe, dann verwenden wir den Buchstaben x, wenn wir $x = P$ als Element von X zusammen mit der Gruppenoperation von G durch Konjugation auffassen und wir schreiben P, wenn wir P einfach als Untergruppe von G auffassen.
Wir zeigen zunächst einen Hilfssatz:

Lemma 5.1 Sei nun $H \subset G$ eine p-Gruppe und $P = x \in X$ ein Fixpunkt von H unter der Konjugationsoperation. Dann gilt $H \subset P$.

Beweis. Da $P = x \in X$ ein Fixpunkt von H ist gilt also $hPh^{-1} = P$ für alle $h \in H$ und daraus folgt, dass $HP = PH$ eine Untergruppe von G ist. (Klar ist, dass $1 \in HP$ und mit $h_1p_1, h_2p_2 \in HP$ ist auch $h_1p_1h_2p_2 = h_1h_2p_1'p_2 \in HP$ für ein $p_1' \in P$. Die Rechnung für die Inversen geht genauso.)
Nach dem Satz von Lagrange ist die Ordnung dieser Untergruppe gleich $|PH| = [PH : H]|H|$.
Wir zeigen nun: Der Index $[PH : H]$ ist eine p-Potenz.
Denn: P operiert auf PH/H durch Linksmultiplikation mit nur einer Bahn, $\text{Bahn}(H) = PH/H$, deren Ordnung nach der Bahnformel ein Teiler der Gruppenordnung von P ist.
Es folgt: PH ist eine p-Untergruppe von G. Da aber $P \subset PH$ ist, muss nun schon $P = PH$ gelten, denn die Ordnung von P als p-Untergruppe von G ist maximal. Aus $PH = P$ folgt nun $H \subset P$. ■

Wir beweisen nun (ii) und (iii) gleichzeitig. Es sei eine p-Sylow-Untergruppe $P \subset G$ gegeben und $H \subset G$ sei eine p-Gruppe. Wir schreiben nun $x = P$ für P als Element der Menge X der p-Sylow-Untergruppen von G, auf der G wie oben durch Konjugation operiert. Es ist sicher $P \subset G_x$ und damit ist die Ordnung der Bahn $|Gx|$ nicht durch p teilbar, denn $|Gx| = [G : G_x]$ nach der Bahnformel und p teilt nicht $[G : G_x]$, da $p^r m = |G| = |G_x|[G : G_x]$ gilt mit $p \nmid m$ sowie $p^r \mid |G_x|$.
Schränkt man die Operation jedoch auf H ein, so zerfällt die Bahn Gx in Bahnen $Hy_1, \ldots, Hy_s$ unter H und eine jede solche Bahn hat p-Potenz-Ordnung, da H eine p-Gruppe ist. Wir erhalten

$$|Gx| = \sum_{i=1}^{s} |Hy_i|$$

und da also p die linke Seite nicht teilt, muss es also auf der rechten Seite eine Bahn geben, deren Ordnung $1 = p^0$ ist, d.h. es gibt einen Fixpunkt unter H.
Sei $Q \subset G$ also eine von H fixierte p-Sylow-Untergruppe von G. Das Lemma besagt nun, dass $H \subset Q$ und damit ist H, wie behauptet, in einer p-Sylow-Untergruppe enthalten. Ist nun P' irgendeine p-Sylow-Untergruppe von G, so liefert die gleiche Argumentation ein $Q \in Gx$ mit $P' \subset Q$, was dann aus Ordnungsgründen schon $P' = Q$ impliziert. Da also $P' = Q \in Gx$ ist, existiert ein $g \in G$ mit $Q = gPg^{-1}$, d.h. P' ist zu P konjugiert.

(iv) Wir haben gesehen, dass $X = Gx$ ist für $x \in X$ beliebig, die Operation von G durch Konjugation auf den p-Sylow-Untergruppen also transitiv ist. Es gilt nach Bahnformel und Lagrange also $p^r m = |G_x||X|$ aber, wie oben gesehen, bereits $p^r \mid |G_x|$ und somit ist $s = |X|$ ein Teiler von m.
Wenden wir nun die Argumentation aus dem vorherigen Teil auf eine p-Sylow-Untergruppe $H = P$ an, so erhalten wir, dass s zur Anzahl der Fixpunkte unter der Konjugationsoperation von P auf X modulo p kongruent ist. Wir haben gesehen, dass es einen Fixpunkt gibt und nach dem Lemma kann es nur einen Fixpunkt, nämlich P selbst, geben. Damit ist $s \equiv 1 \bmod p$.

■

Beispiel 5.10 Ein Beispiel zur Illustration der Sylowsätze: Sei G eine beliebige Gruppe der Ordnung $15 = 3 \cdot 5$. Dann besitzt G also nicht-triviale 3- und 5-Sylow-Untergruppen. Sei s_3 die Anzahl der 3-Sylow-Untergruppen und s_5 die Anzahl der 5-Sylow-Untergruppen. Dann ist s_3 ein Teiler von 5, und damit $s_3 = 1$ oder $s_3 = 5$. Außerdem muss aber $s_3 \equiv 1 \pmod 3$ sein und damit gilt schon $s_3 = 1$. Genauso für die Anzahl der 5-Sylow-Untergruppen, welche ein Teiler von 3 und $1 \pmod 5$ sein muss und damit gilt auch $s_5 = 1$. In den Übungen zeigen Sie (deutlich allgemeiner), dass $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$ gilt. Man überlegt sich dazu: wenn es nur eine p-Sylow-Untergruppe ist, so ist diese ein Normalteiler von G. Wir bezeichnen mit P_3 und P_5 die 3- bzw. 5-Sylow-Untergruppen von G. Es gilt $P_3 \cap P_5 = \{1\}$. Die Untergruppe $P_3 \cdot P_5$ ist somit isomorph zum direkten Produkt $P_3 \times P_5$, hat also 15 Elemente und damit gilt schon $P_3 \times P_5 \cong G$.

5.3 Auflösbare Gruppen

Definition 5.7 Eine Gruppe G heißt *auflösbar*, wenn es eine absteigende Folge von Untergruppen

$$G = G_k \supset G_{k-1} \supset \ldots \supset G_0 = \{1\}$$

gibt, so dass G_{j-1} für $j = 1,\ldots,k$ Normalteiler in G_j und G_j/G_{j-1} abelsch ist. In anderen Worten: Eine Gruppe heißt auflösbar, falls sie eine Normalreihe mit abelschen *Faktoren* G_j/G_{j-1} besitzt.

Bemerkung 5.10 Klarerweise sind alle abelschen Gruppen auflösbar.

Korollar 5.2 Jede endliche p-Gruppe ist auflösbar.

Beweis. Die entsprechende Folge von Untergruppen erhalten wir aus Korollar 5.1. Da der Index $[G_j : G_{j-1}] = p$ ist, wissen wir, dass G_j/G_{j-1} zyklisch von Ordnung p und damit abelsch ist. ■

Übung 5.3 Seien p und q Primzahlen. Jede Gruppe der Ordnung pq is auflösbar. ■

Satz 5.7 — Feit-Thompson (1963). Jede endliche Gruppe ungerader Ordnung ist auflösbar.

Beweis. Der Beweis ist sehr kompliziert. Die Originalarbeit umfasst 255 Seiten. ■

Eine spezielle (nicht notwendigerweise strikt) absteigende Kette von Untergruppen erhält man durch Bilden von *Kommutatoren*.

Definition 5.8 Sei G eine Gruppe und $a,b \in G$, so nennen wir $[a,b] := aba^{-1}b^{-1}$ den Kommutator von a und b. Für zwei Untergruppen $H,H' \subset G$ kann man den Kommutator $[H,H'] := \langle\{[h,h'] \mid h \in H, h' \in H'\}\rangle$, also die von allen Kommutatoren der Form $[h,h']$ erzeugte Untergruppe von G, betrachten.

Die Untergruppe $[G,G]$ von G heißt die *Kommutatoruntergruppe*.

Bemerkung 5.11
(i) Eine Gruppe G ist genau dann abelsch, wenn $[G,G] = \{1\}$ gilt.
(ii) Die Gruppe $[G,G]$ besteht aus allen endlichen Produkten von Kommutatoren $[a,b]$ aus G.
(iii) Die Kommutatoruntergruppe $[G,G]$ ist ein Normalteiler in G. Sie ist der **kleinste Normalteiler** $N \subset G$, **so dass** G/N **abelsch** ist.

Beweis. Die ersten beiden Punkte sind klar, man muss sich für den zweiten Punkt nur vergewissern, dass das Inverse $[a,b]^{-1}$ wieder ein Kommutator ist, nämlich $[a,b]^{-1} = [b,a] = bab^{-1}a^{-1}$.

Sei also $N \subset G$ ein Normalteiler in G, so dass G/N abelsch ist. Sei $[a,b] = aba^{-1}b^{-1} \in [G,G]$. Es ist $baN = bNaN = aNbN = abN$, da G/N abelsch vorausgesetzt wurde und somit $[a,b] = aba^{-1}b^{-1} = ab(ba)^{-1} \in N$, woraus $[G,G] \subset N$ folgt.

Der Vollständigkeit halber zeigen wir noch, dass auch $[G,G]$ ein Normalteiler von G ist und $G/[G,G]$ abelsch ist. Es ist für $g,a,b \in G$: $g[a,b] = gaba^{-1}b^{-1} = [x,y]g$ für $x = gag^{-1}$ und $y = gbg^{-1}$, denn $[x,y]g = xyx^{-1}y^{-1}g = gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1}g = gaba^{-1}b^{-1}$. Die Kommutativität von $G/[G,G]$ sehen wir so: Seien $g,h \in G$ und wir schreiben $\bar{g} = g[G,G]$ sowie $\bar{h} = h[G,G]$ für die Restklassen. Zu zeigen ist $\bar{g}\bar{h} = \bar{h}\bar{g}$ oder $\bar{g}\bar{h}\bar{g}^{-1}\bar{h}^{-1} = 1$. Dies folgt aus $ghg^{-1}h^{-1} = [g,h] \in [G,G]$ per Definition. ■

Wir definieren nun eine Kette von Untergruppen von G durch:

(i) $D^0G := G$,
(ii) $DG = D^1G := [G,G]$,
(iii) $D^{j+1}G := [D^jG, D^jG]$ für $j = 1,2,\ldots$.

Wir erhalten also eine Kette $G = D^0G \supset D^1G \supset \ldots$. Falls wir auf diesem Wege eine Normalreihe erhalten können, so ist die Gruppe auflösbar! Die Umkehrung gilt auch, wie der folgende Satz zeigt.

Satz 5.8 Eine Gruppe G ist genau dann auflösbar, wenn es ein $n \in \mathbb{N}$ gibt, so dass $D^nG = \{1\}$ gilt.

Beweis. Falls $D^n G = \{1\}$ ist, so ist G auflösbar, da $D^{j-1}G \subset D^j G$ ein Normalteiler ist und $D^j G/D^{j-1}G$ abelsch ist nach Bemerkung 5.11. Ist G umgekehrt auflösbar, so existiert eine absteigende Kette von Untergruppen

$$G = G_k \supset G_{k-1} \supset \ldots \supset G_0 = \{1\},$$

so dass G_{j-1} für $j = 1,\ldots,k$ Normalteiler in G_j und G_j/G_{j-1} abelsch ist. Wir zeigen nun, dass $D^j G \subset G_{k-j}$ für $j = 0,\ldots,k$. Für $j = 0$ ist $D^0 G = G = G_k$; also ist die Behauptung richtig. Angenommen es gelte bereits $D^j G \subset G_{k-j}$ für ein j. Dann ist $[G_{k-j}, G_{k-j}] \subset G_{k-j-1}$, da G_{k-j}/G_{k-j-1} abelsch ist (siehe Bemerkung 5.11). Deshalb ist auch $D^{j+1}G = [D^j G, D^j G] \subset [G_{k-j}, G_{k-j}] \subset G_{k-j-1}$.

Es folgt also insbesondere, dass $D^k G \subset G_0 = \{1\}$ ist und somit $D^k G = \{1\}$. ■

Satz 5.9 Es gelten:

(i) Sei G eine endliche auflösbare Gruppe. Dann lässt sich jede echt absteigende Normalreihe mit abelschen Faktoren zu einer Normalreihe verfeinern in der alle Faktoren zyklisch von Primzahlordnung sind.

(ii) Untergruppen auflösbarer Gruppen sind auflösbar.

(iii) Ist $H \subset G$ ein Normalteiler, so ist G genau dann auflösbar, wenn H und G/H auflösbar sind.

(iv) Ein Produkt von Gruppen $G_1 \times \ldots \times G_r$ ist genau dann auflösbar, wenn alle Faktoren $G_1,\ldots,G_r$ auflösbar sind.

Beweis. Der Beweis ist Ihnen als Übung überlassen. Siehe auch Abschnitt 5.4 in [2]. ■

Beispiel 5.11 Ein gutes Beispiel liefern die symmetrischen und alternierenden Gruppen. Sei S_n die symmetrische Gruppe auf n Elementen und $A_n \subset S_n$ die alternierende Gruppe (Untergruppe der geraden Permutationen). Es gilt:

$$[S_n, S_n] = A_n \text{ für } n \geq 2,$$

sowie

$$[A_2, A_2] = [A_3, A_3] = \{1\}, \quad [A_4, A_4] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \text{(Kleinsche Vierergruppe)}$$

und

$$[A_n, A_n] = A_n \text{ für } n \geq 5.$$

Beweisskizze. (i) Wir zeigen zunächst $[S_n, S_n] = A_n$. Es ist klar, dass für alle $\sigma, \tau \in S_n$ gilt, dass $[\sigma, \tau] \in A_n$, d.h. dass $\operatorname{sign}([\sigma,\tau]) = \operatorname{sign}(\sigma\tau\sigma^{-1}\tau^{-1}) = 1$ gilt, denn sign ist ein Homomorphismus. Außerdem kann man jede gerade Permutation als ein Produkt von 3-er Zykeln schreiben. Sei $(a,b,c) \in A_n$ ein 3-er-Zykel, dann können wir diesen leicht als Kommutator schreiben:

$$(a,b,c) = (a,c)(b,c)(a,c)(b,c) = (a,c)(b,c)(a,c)^{-1}(b,c)^{-1},$$

wie man leicht nachrechnet.

(ii) Die Aussagen zu A_2, A_3 und A_4 werden in den Übungen behandelt.

(iii) Wir zeigen nun $[A_n, A_n] = A_n$. Hierzu zerlegen wir einen 3-er Zykel noch mal anders: Ist $(a,b,c) \in A_n$ ein 3-er Zykel so seien $d, e \in \{1,\ldots,n\}$ von a,b,c verschieden (man bemerke, dass dies nur für $n \geq 5$ möglich ist). Wir erhalten

$$(a,b,c) = (a,b,d)(a,c,e)(a,b,d)^{-1}(a,c,e)^{-1},$$

wie man wieder leicht verifiziert. Da jedes Element aus A_n als Produkt von 3-er-Zykeln schreiben kann, folgt $A_n \subset [A_n, A_n]$ und damit die Behauptung.

■

Korollar 5.3 Die symmetrische Gruppe S_n ist für $n \leq 4$ auflösbar und für $n \geq 5$ ist S_n *nicht auflösbar*.

6. Anwendungen der Galoistheorie

6.1 Fundamentalsatz der Algebra

Satz 6.1 — Fundamentalsatz der Algebra. Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen, d.h.: jedes nicht-konstante Polynom $f \in \mathbb{C}[X]$ besitzt eine Nullstelle in $\mathbb{C}$ (und zerfällt damit über $\mathbb{C}$ in Linearfaktoren).

Wir benutzen 2 Aussagen, die Sie aus der Analysis kennen:

(i) Jedes Polynom $f \in \mathbb{R}[X]$ von ungeradem Grad hat eine Nullstelle in $\mathbb{R}$ (dies folgt aus dem Zwischenwertsatz).

(ii) Jedes $a \in \mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$ hat eine Quadratwurzel in $\mathbb{R}$, d.h. es existiert ein $b \in \mathbb{R}$ mit $b^2 = a$.

Aus Punkt (ii) folgt: Jedes Polynom vom Grad 2 hat eine Nullstelle in $\mathbb{C}$. Denn: Man muss nach der p-q-Formel nur Wurzeln aus komplexen Zahlen in $\mathbb{C}$ ziehen können. Dafür löst man $(a+ib)^2 = x+iy$ für festes $z = x+iy \in \mathbb{C}$ mit $x, y \in \mathbb{R}$. Man sieht sofort, dass $x = a^2 - b^2$ sowie $2ab = y$. Hieraus ergibt sich dann

$$a^2 - \frac{y^2}{4a^2} = x$$

oder

$$a^4 - xa^2 - \frac{y^2}{4} = 0,$$

also eine normierte quadratische Gleichung in a^2 und deshalb ist

$$a^2 = \frac{x}{2} \pm \frac{1}{2}\sqrt{x^2+y^2}.$$

Hieraus folgt, da $b^2 = a^2 - x$ ist, dass

$$b^2 = \frac{-x}{2} \pm \frac{1}{2}\sqrt{x^2+y^2},$$

wobei die Vorzeichen in beiden Fällen gleich zu wählen sind. Man beachte, dass dabei jeweils für die Wahl $+$ die rechte Seite sicher nicht-negativ ist und damit (unter Benutzung von (ii)) Lösungen a und b in $\mathbb{R}$ existieren.

Beweis von Satz 6.1. Sei $f \in \mathbb{C}[X]$ und L der Zerfällungskörper von f über $\mathbb{C}$. Wir wollen zeigen, dass $L = \mathbb{C}$ gilt. Geht man zur normalen Hülle N von L über $\mathbb{R}$ über, so erhält man eine endliche Galois-Erweiterung von $\mathbb{R}$ vom Grad

$$[N : \mathbb{R}] = 2^k m$$

mit $2 \nmid m$. Die Galois-Gruppe $G = \mathrm{Gal}(N/\mathbb{R})$ enthält eine 2-Sylow-Untergruppe H (der Ordnung 2^k) und damit hat die Erweiterung $N^H/\mathbb{R}$ nach dem Hauptsatz der Galoistheorie den ungeraden Grad

$$[N^H : \mathbb{R}] = m.$$

Da aber jedes Polynom ungeraden Grades bereits eine Nullstelle in $\mathbb{R}$ hat, muss $m = 1$ sein (jedes Element in N^H hat ungeraden Grad über $\mathbb{R}$, damit wäre ein Minimalpolynom ein irreduzibles Polynom mit ungeradem Grad über $\mathbb{R}$ und dies kann nur ein Linearfaktor sein).

Damit hat die Erweiterung $N/\mathbb{C}$ den Grad 2^{k-1}. Falls $N \neq \mathbb{C}$ wäre (also $k \geq 2$), so wäre also die Galois-Gruppe $\mathrm{Gal}(N/\mathbb{C})$ eine nicht-triviale 2-Gruppe. Aus dem Struktursatz über p-Gruppen folgt, dass $\mathrm{Gal}(N/\mathbb{C})$ eine Untergruppe G' vom Index 2 besitzt. Aus dem Hauptsatz der Galoistheorie folgt, dass $Z = N^{G'}$ eine nicht-triviale Erweiterung von $\mathbb{C}$ ist,

$$\mathbb{C} \subset Z \subset N,$$

wobei $[N : Z] = 2^{k-2} = |G'| \geq 1$ und somit $[Z : \mathbb{C}] = 2 = 2^{k-1}/2^{k-2}$.

Da aber jedes Polynom vom Grad 2 schon eine Nullstelle in $\mathbb{C}$ hat, muss $Z = \mathbb{C}$ sein und somit gleich $k = 1$ und damit auch $N = \mathbb{C}$ gelten. ■

6.2 Konstruktion mit Zirkel und Lineal

Wir erinnern an den folgenden Satz (siehe Folien).

Satz 6.2 Sei $\hat{E} \subset \mathbb{C}$ der Körper der aus E=$\{0,1\}$ mit Zirkel und Lineal konstruierbaren Punkte und sei $z \in \mathbb{C}$ Dann sind äquivalent:

(i) Es ist $z \in \hat{E}$.

(ii) Es gibt eine Körperkette $\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_n \subset \mathbb{C}$ mit $z \in K_n$ und $[K_i : K_{i-1}] = 2$ für $i = 1, \ldots, n$ (man sagt, K_n ensteht aus $\mathbb{Q}$ durch sukzessive Adjunktion von Quadratwurzeln). Insbesondere ist $[K_n : \mathbb{Q}] = 2^n$ eine Potenz von 2.

6.2.1 Konstruktion von regelmäßigen n-Ecken / Einheitswurzeln

Lemma 6.1 Sei K ein Körper und $H \subset K^\times$ eine endliche Untergruppe der multiplikativen Gruppe $K^\times$. Dann ist H zyklisch.

Beweis. Der Beweis ist eine Übung (es war Aufgabe H35). Man nehme ein Element $a \in H$ von maximaler Ordnung in H und zeige $H = \langle a \rangle$. ■

Bemerkung 6.1 Sei Z_n der Zerfällungskörper von $X^n - 1$ über $\mathbb{Q}$. Die Menge U_n der n-ten Einheitswurzeln in Z_n (also genau der Nullstellen von $X^n - 1$) ist eine Untergruppe von $Z_n^\times$, Denn: sicherlich ist $U_n \subset Z_n^\times = Z_n \setminus \{0\}$ und sind $\lambda, \mu \in U_n$, so ist $(\lambda\mu)^n = \lambda^n \mu^n = 1$ also ist auch $(\lambda\mu) \in U_n$. Die Gruppe U_n ist dann als endliche Untergruppe der multiplikativen Gruppe eine zyklische Gruppe. Da sie Ordnung n hat ist sie isomorph zu $\mathbb{Z}/n\mathbb{Z}$.

Ihre Erzeuger werden *primitive n-te Einheitswurzeln* genannt. Ist ζ_n eine primitive n-te Einheitswurzel, so gilt bereits $Z_n = \mathbb{Q}(\zeta_n)$ (denn jede andere Nullstelle von $X^n - 1$ ist als Potenz von ζ_n schon in $\mathbb{Q}(\zeta_n)$ enthalten).

Definition 6.1 Der Zerfällungskörper $\mathbb{Q}(\zeta_n)$ des Polynoms $X^n - 1$ über $\mathbb{Q}$ heißt *n-ter Kreisteilungskörper* (wobei ζ_n eine primitive n-te Einheitswurzel sei).

Bemerkung 6.2 Die Gruppe U_n enthält genau $\varphi(n)$ verschiedene primitive n-te Einheitswurzeln, wobei $\varphi(n)$ die *Eulersche φ-Funktion* ist:

$$\varphi(n) := |\{1 \leq a \leq n \mid \mathrm{ggT}(a,n) = 1\}|.$$

(Man bemerke, dass für $n > 1$ auch $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ gilt, da die Einheiten in $\mathbb{Z}/n\mathbb{Z}$ genau die Erzeuger von $\mathbb{Z}/n\mathbb{Z}$ als additive Gruppe sind.)

Eingebettet in $\mathbb{C}$ erhält man primitive n-te Einheitswurzeln ganz konkret als $e^{\frac{2\pi ia}{n}}$ wobei $\mathrm{ggT}(a,n) = 1$ sei.

Beispiel 6.1 Es ist zum Beispiel $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$ und generell für eine Primzahl p ist $\varphi(p) = p - 1$.

Definition 6.2 Sei $\mathbb{Q}(\zeta_n)$ der n-te Kreisteilungskörper. Das Minimalpolynom $\Phi_n \in \mathbb{Q}[X]$ von ζ_n über $\mathbb{Q}$ wird das n-te Kreisteilungspolynom genannt.

Proposition 6.1 Es gilt

$$\Phi_n = \prod_{\zeta \in U_n \text{ primitiv}} (X - \zeta).$$

Das Polynom Φ_n ist offenbar normiert und hat den Grad $\varphi(n)$. Damit ist $\mathbb{Q}(\zeta_n)$ eine Galoiserweiterung über $\mathbb{Q}$ vom Grad

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n).$$

Beweis. Es ist klar, dass jedes $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ die primitive Einheitswurzel ζ_n wieder auf eine primitive n-te Einheitswurzel abbildet (σ beschränkt sich zu einem Gruppenautomorphismus von U_n, damit bleibt die Ordnung der Elemente erhalten). Außerdem sind die Elemente aus $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ eindeutig durch das Bild von ζ_n bestimmt. Damit ist der Grad der Erweiterung durch $\varphi(n)$ beschränkt.

Sei $f \in \mathbb{Q}[X]$ das Minimalpolynom von ζ_n über $\mathbb{Q}$. Es ist also noch zu zeigen, dass jede primitive n-te Einheitswurzel auch eine Nullstelle von f ist (womit dann $f = \Phi_n$ folgt). Da f ein Teiler von $X^n - 1$ ist, gibt es ein g in $\mathbb{Q}[X]$ mit

$$X^n - 1 = f \cdot g.$$

Da f normiert ist, ist auch g normiert und somit $g \in \mathbb{Z}[X]$ nach Korollar 3.4.

Sei nun p eine Primzahl mit $p \nmid n$. Dann ist ζ_n^p eine primitive n-te Einheitswurzel. Falls $f(\zeta_n^p) \neq 0$ wäre, so gilt $g(\zeta^p) = 0$ und somit ist ζ_n eine Nullstelle von $g(X^p)$ und es folgt also $f \mid g(X^p)$. Es existiert demnach ein $h \in \mathbb{Q}[X]$ mit $g(X^p) = f(X)h(X)$ und es folgt wieder, dass $h \in \mathbb{Z}[X]$ und normiert ist. Wendet man nun aber die Abbildung $\varphi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ (Reduktion modulo p) an, so erhält man wegen des Frobenius-Homomorphimus eine Faktorisierung

$$(\varphi(g)(X))^p = \varphi(g)(X^p) = \varphi(f)\varphi(h)(X).$$

Wir behaupten, dass $\mathrm{ggT}(\varphi(f), \varphi(g)) \neq 1$ ist. In der Tat, ist α eine Nullstelle von $\varphi(f)$ (in einer Körpererweiterung von $\mathbb{F}_p$), so ist α also auch eine Nullstelle von $\varphi(g)^p$ und damit auch von g.

Daraus folgt dann aber, dass $\varphi(X^n - 1) = \varphi(f)\varphi(g)$ mehrfache Nullstellen hat. Da wir aber angenommen haben, dass $p \nmid n$ gilt, ist ja de Ableitung von $X^n - 1$ nicht identisch 0, weshalb dies nicht sein kann. Also muss bereits $f(\zeta_n^p) = 0$ sein.

Zum Schluss sei nun $\zeta \neq \zeta_n$ eine primitive n-te Einheitswurzel. Da U_n zyklisch ist und ζ_n ein Erzeuger von U_n ist, gibt also ein $m \in \mathbb{N}$ mit $\mathrm{ggT}(m,n) = 1$ und $\zeta = \zeta_n^m$. Damit lässt sich ζ aus ζ_n durch iteriertes Potenzieren mit Primzahlen gewinnen, die koprim zu n sind. In jedem Zwischenschritt erhalten wir eine neue primitive n-te Einheitswurzel, die nach obigem Argument eine Nullstelle von f ist. Es folgt also $f(\zeta) = 0$ und die Behauptung ist bewiesen. ∎

Satz 6.3 Sei $n \in \mathbb{N}$ und $n \geq 3$. Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $\varphi(n)$ eine Potenz von 2 ist.

Beweis. Wir haben uns schon überlegt, dass die Konstruktion des regelmäßigen n-Ecks äquivalent zur Konstruktion von $\zeta_n := e^{\frac{2\pi i}{n}}$ ist. Nach Satz 6.2 ist die Konstruierbarkeit von ζ_n äquivalent dazu, dass ζ_n in einem Körper enthalten ist, der durch sukzessive Adjunktion von Quadratwurzeln entsteht. Ist also der Grad $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ keine Zweierpotenz, so ist ζ_n nicht konstruierbar, denn dann kann auch kein

Erweiterungskörper von $\mathbb{Q}(\zeta_n)$ Zweierpotenzgrad haben.

Ist umgekehrt $\varphi(n)$ eine Zweierpotenz, so ist die Ordnung der Galoisgruppe $G := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ eine Zweierpotenz und somit ist G eine 2-Gruppe. Nach dem Satz über die Struktur von p-Gruppen (Korollar 5.1) gibt es eine absteigende Kette von Untergruppen

$$G = G_n \supset G_{n-1} \supset \ldots \supset G_0 = 1,$$

so dass $|G_j| = 2^j$ und G_{j-1} ist normal in G_j (die Faktoren sind zyklisch von Ordnung 2). Nach dem Hauptsatz der Galoistheorie (Satz 4.14) entpricht dieser Kette eine aufsteigende Kette von Zwischenkörpern

$$\mathbb{Q} = K_0 \subset K_1 \subset \ldots K_n = \mathbb{Q}(\zeta_n),$$

mit $[K_i : K_{i-1}] = 2$ für $i = 1, \ldots, n$. Damit ist $\zeta_n \in \mathbb{Q}(\zeta_n)$ nach Satz 6.2 konstruierbar. ■

Definition 6.3 Für $n \in \mathbb{N}_0$ heißt $F_n = 2^{2^n} + 1$ die n-te *Fermatsche Zahl*. Eine Primzahl heißt *Fermat-Primzahl*, falls sie eine Fermatsche Zahl ist.

Bemerkung 6.3 Die ersten 5 Fermat-Zahlen

$$F_0 = 3,$$
$$F_1 = 5,$$
$$F_2 = 17,$$
$$F_3 = 257,$$
$$F_4 = 65537$$

sind Primzahlen. Diese Zahlen sind nach Pierre de Fermat (1607-1665) benannt. Dieser hatte vermutet, dass alle Fermatschen Zahlen prim sind. Allerdings ist dies definitiv falsch, denn die ersten 5 Fermatschen Zahlen sind die bisher einzig bekannten Fermat-Primzahlen! Zum Beispiel ist $F_5 = 4294967297 = 641 \cdot 6700417$. Es ist nicht bekannt, ob es unendlich viele Fermat-Primzahlen gibt. (Man weiß auch nicht, ob es unendlich viele zusammengesetzte Fermatsche Zahlen gibt.) Die Fermat-Zahl F_33 ist die kleinste Fermat-Zahl (eine Zahl mit 2.585.827.973 Stellen), von der bis heute (Stand Januar 2019) nicht bekannt ist, ob sie prim oder zusammengesetzt ist.

Lemma 6.2 Ist p eine Primzahl dann ist $\varphi(p) = p - 1$ eine Zweierpotenz genau dann, wenn p eine Fermat-Primzahl ist.

Beweis. Klar ist, dass $p-1$ eine Zweierpotenz ist, falls p eine Fermat-Primzahl ist. Ist umgekehrt p eine Primzahl, so dass $\varphi(p) = 2^k$ gilt, dann ist $p = 2^k + 1$. Schreiben wir $k = 2^r n > 0$ mit n ungerade, so erhalten wir, dass

$$p = 2^k + 1 = 1 - (-2^{2^r})^n$$

und da

$$1 - a^n = (1-a)(a^{n-1} + a^{n-2} + \ldots + a^0)$$

gilt, kann p keine Primzahl sein, falls $n > 1$ gilt. Für $n = 1$ ist $p = 2^{2^r} + 1$ also eine Fermat-Primzahl. ■

Korollar 6.1 Das regelmäßige n-Eck ist für n prim genau dann mit Zirkel und Lineal konstruierbar, wenn n eine Fermat-Primzahl ist.

Auch allgemeiner kann man das Ergebnis konkretisieren. Wir brauchen zunächst ein Lemma.

Lemma 6.3 Die Funktion $\varphi : \mathbb{N}_0 \to \mathbb{N}_0$ ist *multiplikativ*, d.h. falls m und n natürliche Zahlen sind mit

ggT$(m,n) = 1$, dann gilt

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Beweis. Das kann man zum Beispiel mit Hilfe des Chinesischen Restsatzes sehen. Sind m und n teilerfremd, so ist $\mathbb{Z}/mn\mathbb{Z}$ isomorph zu $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Die Einheiten in $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sind gegeben durch $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. Es ist also einerseits $\varphi(mn) = |(\mathbb{Z}/mn\mathbb{Z})^\times|$ und andererseits ist dies gleich $|(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(m)\varphi(n)$. ■

Satz 6.4 Für $n \geq 2$ sind folgende Aussagen äquivalent:
(i) $\varphi(n)$ ist eine Potenz von 2.
(ii) Es existieren verschiedene Fermat-Primzahlen $p_1, \ldots, p_r$ und ein $m \in \mathbb{N}$ mit $n = 2^m p_1 \cdot \ldots \cdot p_r$.

Beweis. Ist n von der in (ii) angegebenen Form, so folgt aus der Multiplikativität von φ zusammen mit $\varphi(2^m) = 2^{m-1}$, dass $\varphi(n)$ eine Zweierpotenz ist.

Bevor wir die andere Richtung beweisen, halten wir noch fest, dass für eine Primzahl p stets gilt, dass

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

(Anschaulich sieht man das so: es gibt in jedem Intervall der Länge p von 1 bis $p^k - 1$ jeweils $p-1$ zu p teilerfremde Zahlen und p^{k-1} solche Intervalle.)

Sei nun umgekehrt $\varphi(n)$ eine Potenz von 2. Wir schreiben die Primfaktorisierung von n als

$$n = 2^m p_1^{n_1} \cdots p_r^{n_r}.$$

Falls $\varphi(n)$ eine Zweierpotenz ist, so ist auch $\varphi(p_i^{n_i}) = (p_i - 1)p_i^{n_i - 1}$ für alle i eine Zweierpotenz. Damit muss aber $p_i = 2$ sein oder $n_i = 1$ und p_i eine Fermat-Primzahl. Dies beweist die Behauptung. ■

Korollar 6.2 Die folgenden Werte von n sind die ersten 100 Werte, für die das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar ist: 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272, 320, 340, 384, 408, 480, 510, 512, 514, 544, 640, 680, 768, 771, 816, 960, 1020, 1024, 1028, 1088, 1280, 1285, 1360, 1536, 1542, 1632, 1920, 2040, 2048, 2056, 2176, 2560, 2570, 2720, 3072, 3084, 3264, 3840, 3855, 4080, 4096, 4112, 4352, 4369, 5120, 5140, 5440, 6144, 6168, 6528, 7680, 7710, 8160, 8192, 8224, 8704, 8738, 10240, 10280, 10880, 12288, 12336, 13056, 13107.

6.3 Auflösbarkeit von algebraischen Gleichungen

Todo.

Literaturverzeichnis

[1] Michael Artin. *Algebra*. Birkhäuser Advanced Texts: Basler Lehrbücher. [Birkhäuser Advanced Texts: Basel Textbooks]. Birkhäuser Verlag, Basel, 1993 (siehe Seite 2).

[2] Bosch, Siegfried. *Algebra*. Springer-Lehrbuch. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013 (siehe Seiten 2, 8, 72).

[3] Jens Carsten Jantzen und Joachim Schwermer. *Algebra*. Springer-Lehrbuch. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014 (siehe Seite 2).

[4] Ernst Kunz. *Algebra*. 1994 (siehe Seite 2).

[5] Serge Lang. *Algebra*. third. Band 211. Graduate Texts in Mathematics. Springer-Verlag, New York, 2002 (siehe Seite 2).