Pflichtmodul Algebra

– **Vorlesungsskript** –

Algebra

Dietrich Burde

2024

Inhaltsverzeichnis

1 Einleitung

Die Vorlesung *Algebra* ist Bestandteil des Bachelor-Studiengangs in Mathematik der Universität Wien. Es stellt den Kernpunkt der Ausbildung im Bereich der Algebra im Bachelorstudium dar. Aufbauend auf Vorkenntnisse aus linearer Algebra und Zahlentheorie werden die Studierenden mit dem abstrakt-strukturellen Zugang zur Algebra vertraut gemacht. Die Studierenden erhalten eine fundierte Ausbildung auf den zentralen Teilgebieten der Algebra.

Das Wort *Algebra* kommt aus dem Arabischen - al-ğabr - das Zusammenfügen gebrochener Teile, und bezeichnet das Rechnen mit Gleichungen in Unbekannten. Als Begründer der Algebra gilt der Grieche *Diophantos von Alexandria*, der wahrscheinlich zwischen 100 v. Chr. und 350 n. Chr. lebte. Sein 13 Bände umfassendes Werk *Arithmetica* ist das älteste bis heute erhaltene, in dem Gleichungen in Unbekannten verwendet werden. Bei Gleichungen geht es hauptsächlich um Polynomgleichungen wie etwa

$$x^5 - 4x + 2 = 0$$

in einer Unbekannten x. Allerdings kann man auch mehrere Unbekannte betrachten, wie etwa

$$y^2 = x^3 - 36x.$$

Diese Gleichungen sollen in gewissen Zahlbereichen gelöst werden. Das sind oft Körper wie $\mathbb{R}$ oder $\mathbb{C}$. Es können aber auch ganzzahlige Lösungen gemeint sein. Für $\mathbb{Z}$ oder $\mathbb{Q}$ spricht man von *Diophantischen Gleichungen*, und das ist ein Zweig der Zahlentheorie. Sind die Exponenten höchstens 1, spricht man von linearen Gleichungen, oder linearen Gleichungssystemen, die in der linearen Algebra behandelt werden. Lineare und quadratische Gleichungen in einer Variablen sind leicht zu lösen. Interessanter wird es aber schon bei kubischen Gleichungen. Es bedurfte schon einiger Anstrengungen, um auch nur eine Lösung in einem Spezialfall zu finden. Das gelang

Tartaglia im Jahr 1535 mit der Gleichung

$$x^3 + ax = b,$$

mit reellen Zahlen $a, b > 0$. Er zeigte, dass

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

eine reelle Lösung ist. Cardano konnte 1545 die allgemeine kubische Gleichung $x^3 + ax^2 + bx + c = 0$ auf den obigen Fall $x^3 + px + q = 0$ reduzieren und fand Lösungsformeln, mit Ferrari auch für Grad 4. Er motivierte damit auch die Einführung komplexen Zahlen.

In der Neuzeit wurde die Theorie der Gleichungen weiter ausgebaut, durch Leonhard Euler, Joseph-Louis Lagrange und insbesondere auch durch Carl Friedrich Gauß , der 1799 den *Fundamentalsatz der Algebra* bewies: jede Polynomgleichung

$$a_n x^n + \cdots a_1 x + a_0 = 0$$

vom Grad $n \geq 1$ besitzt genau n Lösungen in den komplexen Zahlen.
Um 1830 entwickelte Évariste Galois (1811-1832) die Galoistheorie. Diese kann als der Beginn der modernen Algebra verstanden werden. Galois und unabhängig Niels Henrik Abel lösten das lange offene Problem der Lösung algebraischer Gleichungen von höherem als viertem Grad, wobei man unter Lösung damals die Darstellung durch die üblichen Rechenoperationen und Wurzelausdrücke (Radikale genannt) verstand, indem sie zeigten, dass dies ab dem fünften Grad im Allgemeinen nicht mehr möglich ist (Satz von Abel-Ruffini). Von Galois stammen in diesem Zusammenhang die Anfänge der Gruppentheorie, vor allen Dingen Permutationsgruppen, und Körpertheorie, also endliche Körper, auch Galois-Felder genannt, und Körpererweiterungen. Natürlich kamen dann auch viele weitere algebraische Strukturen hinzu, oft motiviert aus der Zahlentheorie oder Geometrie und anderen Bereichen.

Notationen: Mit $\mathbb{N}$ bezeichnen wir die natürlichen Zahlen $0, 1, 2, \ldots$.

2 Gruppen

2.1 Gruppenaxiome

Definition 2.1. Eine Gruppe G ist eine nicht-leere Menge zusammen mit einer binären Operation $(a, b) \mapsto ab$ von $G \times G \to G$, die die folgenden Axiome erfüllt:

(1) *Assoziativität.* Für alle $g, h, k \in G$ gilt

$$(gh)k = g(hk).$$

(2) *Existenz eines neutralen Elements.* Es existiert ein Element $e \in G$ mit

$$eg = g = ge$$

für alle $g \in G$.

(3) *Existenz eines inversen Elements.* Für jedes $g \in G$ existiert ein Element $g^{-1} \in G$ mit

$$gg^{-1} = e = g^{-1}g.$$

Ein $e \in G$ mit $eg = g = ge$ ist automatisch eindeutig, denn für ein zweites solches Element $e' \in G$ hat man $e' = ee' = e$. Ebenso ist das inverse Element eindeutig.

Bemerkung 2.1.1. Man kann in Definition 2.1 die Bedingungen (2) und (3) durch die folgenden schwächeren Bedingungen (2′) bzw. (3′) ersetzen:

(2′) *Existenz eines links-neutralen Elements.* Es existiert ein Element $e \in G$ mit

$$eg = g$$

für alle $g \in G$.

(3′) *Existenz eines links-inversen Elements.* Für jedes $g \in G$ existiert ein Element $g^{-1} \in G$ mit

$$g^{-1}g = e.$$

Lemma 2.1.2. *Sei G eine Gruppe. Dann gelten die* Kürzungsregeln*, d.h., aus $gh = gk$ folgt $h = k$ und aus $hg = kg$ folgt $h = k$. Ist G endlich, so sind die Kürzungsregeln äquivalent zu Axiom* (3)*.*

Beweis. Angenommen es gilt $gh = gk$ für $g, h, k \in G$. Durch Anwendung von (3) erhalten wir

$$h = g^{-1}gh = g^{-1}gk = k.$$

Aus $hg = kg$ folgt ebenso $h = k$. Angenommen G ist endlich und es gelten die Kürzungsregeln. Dann ist die Linksmultiplikation $L_g \colon x \mapsto gx$ für jedes $g \in G$ injektiv. Da G endlich ist, ist L_g dann auch für jedes $g \in G$ surjektiv. Daraus folgt aber Axiom (3). □

Definition 2.2. Eine Gruppe G heißt *abelsch*, falls sie das Kommutativitätsgesetz erfüllt, d.h.,

$$gh = hg$$

für alls $g, h \in G$.

In diesem Fall schreibt man oft $a + b$ für ab, $-a$ für a^{-1} und 0 für das neutrale Element e. Das ist aber nicht immer der Fall. Für einen Körper K hat man zwei abelsche Gruppen, nämlich $(K, +)$ mit der Addition, und auch $(K^\times, \cdot)$, die multiplikative Gruppe der Elemente ungleich Null in K.

Beispiel 2.1.3. *Hier sind weitere Beispiele von Gruppen.*

1. *Die Gruppe $(\mathbb{Z}, +)$ der ganzen Zahlen bezüglich Addition. Diese unendliche abelsche Gruppe wird auch manchmal multiplikativ geschrieben und mit $C_\infty = \{g^n \mid g \in \mathbb{Z}\}$ bezeichnet.*

2. *Die Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$. Sie ist gegeben durch die Restklassen*

$$\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

modulo n. Multiplikativ geschrieben wird sie mit $C_n = \{e, g, g^2, \ldots, g^{n-1}\}$ bezeichnet, wobei der Buchstabe C für "cyclic" steht. Es gilt $g^n = g^0 = e$.

3. *Die Gruppe $GL_n(K)$. Sie besteht aus allen invertierbaren $n \times n$-Matrizen*

mit Koeffizienten in einem Körper K. Sie heißt die allgemeine lineare Gruppe vom Grad n. Für $n = 1$ ist $GL_1(K) = K^\times$.

4. *Die Diedergruppe D_n für $n \geq 3$. Sie besteht aus den Isometrien der Ebene, die ein reguläres n-Eck fixieren, wobei die Operation die Komposition von Isometrien ist. Die Gruppe D_n hat $2n$ Elemente und ist durch*

$$D_n = \{e, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots r^{n-1}s\}$$

gegeben. Dabei ist r eine Drehung um den Winkel $\frac{2\pi}{n}$, und s eine Spiegelung, so dass $srs^{-1} = r^{-1}$ und $s^2 = e$. Die Elemente $s, rs, r^2s, \ldots r^{n-1}s$ sind Spiegelungen und die Elemente $e, r, \ldots, r^{n-1}$ sind Drehungen des n-Ecks mit $r^n = e$.

5. *Die "freie" Gruppe F_2. Diese Gruppe besteht aus allen reduzierten Wörtern in zwei verschiedenen Buchstaben a und b und ihrer Inversen. Zwei Wörter werden verknüpft, indem man sie hintereinander schreibt. Reduziert bedeutet, dass man so weit wie möglich kürzt, also z.B.*

$$ba^{-2}bb^{-1}a^2b = ba^{-2}a^2b = b^2.$$

Das neutrale Element ist das leere *Wort e.*

Definition 2.3. Sei X eine Menge. Dann ist die Menge aller Bijektionen $f\colon X \to X$ eine Gruppe bezüglich der Komposition von Abbildungen. Sie wird mit $\mathrm{Sym}(X)$ bezeichnet.

Für $X = \{1, 2, \ldots, n\}$ ist $\mathrm{Sym}(X)$ die symmetrische Gruppe S_n mit $n!$ Elementen. Die Diedergruppe D_3 besteht aus den Drehungen und Spiegelungen eines regelmäßigen Dreiecks, mit den Ecken $1, 2, 3$ in der Ebene, die das Dreieck in sich überführen. Die Drehungen sind $\mathrm{id}, (123), (132)$, und die Spiegelungen $(12), (13), (23)$. Hier bedeutet (123) zum Beispiel die Bijektion $\pi\colon \{1, 2, 3\} \to \{1, 2, 3\}$ mit $\pi(1) = 2$, $\pi(2) = 3$ und $\pi(3) = 1$. Also hat man

$$D_3 = \{\mathrm{id}, (12), (13), (23), (123), (132)\} = S_3.$$

Für $n \geq 4$ hat S_n aber mehr Elemente als D_n. Die Komposition von Elementen $\pi_1, \pi_2 \in S_3$ definieren wir durch

$$(\pi_1 \circ \pi_2)(i) = \pi_1(\pi_2(i))$$

für alle $i \in \{1, 2, 3\}$. Für $\pi_1 = (12)$ und $\pi_2 = (23)$ gilt etwa

$$\begin{aligned}(\pi_1 \circ \pi_2)(1) &= \pi_1(1) = 2,\\ (\pi_1 \circ \pi_2)(2) &= \pi_1(3) = 3,\\ (\pi_1 \circ \pi_2)(3) &= \pi_1(2) = 1.\end{aligned}$$

Das bedeutet $(12) \circ (23) = (123)$. Auf diese Weise kann man die Gruppentafel von S_3 bestimmen.

$\circ$	id	(123)	(132)	(23)	(13)	(12)
id	id	(123)	(132)	(23)	(13)	(12)
(123)	(123)	(132)	id	(12)	(23)	(13)
(132)	(132)	id	(123)	(13)	(12)	(23)
(23)	(23)	(13)	(12)	id	(123)	(132)
(13)	(13)	(12)	(23)	(132)	id	(123)
(12)	(12)	(23)	(13)	(123)	(132)	id

Lemma 2.1.4. *Sei S eine nicht-leere Teilmenge einer Gruppe G. Angenommen, die folgenden zwei Eigenschaften gelten:*

(S1) Für alle $a, b \in S$ gilt $ab \in S$.

(S2) Für alle $a \in S$ gilt $a^{-1} \in S$.

Dann ist S mit der Verknüpfung von G eine Gruppe.

Beweis. Wegen (S1) definiert die binäre Operation auf G auch eine binäre Operation auf S, die die Assoziativität vererbt. Nach Voraussetzung enthält S mindestens ein Element a. Für jedes $a \in S$ liegt sein Inverses a^{-1} und das Produkt $e = aa^{-1}$ wegen (S1) und (S2) wieder in S. Daher folgen die Gruppenaxiome für S aus denen für G. □

Definition 2.4. Jede nicht-leere Teilmenge S einer Gruppe G, die (S1) und (S2) erfüllt, heißt *Untergruppe* von G.

Beispiel 2.1.5. 1. *Die "triviale"Gruppe $\{e\}$ und die ganze Gruppe G sind Untergruppen von G.*

2. *Das* Zentrum *einer Gruppe G, definiert durch*

$$Z(G) = \{g \in G \mid gx = xg \; \forall\, x \in G\},$$

ist eine Untergruppe von G.

3. *Der Schnitt beliebig vieler Untergruppen von G ist eine Untergruppe von G.*

4. *Die Teilmenge $n\mathbb{Z}$ von $\mathbb{Z}$ für $n \in \mathbb{Z}$ ist eine Untergruppe von $\mathbb{Z}$.*

Lemma 2.1.6. *Sei X eine Teilmenge einer Gruppe G. Dann gibt es eine kleinste Untergruppe von G, die X enthält.*

Beweis. Der Schnitt S aller Untergruppen von G, die X enthalten, ist wieder eine Untergruppe von G, die X enthält. Offensichtlich ist sie die kleinste solche Untergruppe. S enthält mit X auch alle endlichen Produkte von Elementen aus X und deren Inverse. Aber die Menge solcher Produkte erfüllt (S1) und (S2) und ist daher eine Untergruppe S' von G, die X enthält. Offensichtlich gilt $S = S'$. □

Definition 2.5. Die kleinste Untergruppe von G, die X enthält, wird mit $\langle X \rangle$ bezeichnet und heißt die *von X erzeugte Untergruppe*. Wir sagen, dass X die Gruppe G *erzeugt* falls $G = \langle X \rangle$, d.h., falls jedes Element von G als endliches Produkt von Elementen aus X und deren Inversen geschrieben werden kann.

Wir setzen $\langle \emptyset \rangle = \{e\} = 1$, welches die triviale Gruppe ist. Die Gruppe, die durch eine Rotation r um den Winkel $\frac{2\pi}{n}$ erzeugt wird, ist durch $C_n = \langle r \rangle = \{e, r, r^2, \ldots, r^{n-1}\}$ gegeben.

Definition 2.6. Eine Gruppe G heißt *zyklisch*, falls sie von einem Element erzeugt ist.

Man beachte, dass zyklische Gruppen abelsch sind, da alle Elemente r^k und r^ℓ kommutieren. Insbesondere sind die Gruppen C_n und C_∞ zyklisch. Die Gruppen $GL_n(K)$ sind für $n > 1$ nicht zyklisch, da sie nicht abelsch sind.

2.2 Gruppenhomomorphismen

Definition 2.7. Eine Abbildung $\varphi\colon G \to H$ zwischen zwei Gruppen heißt *Gruppenhomomorphismus*, falls

$$\varphi(gh) = \varphi(g) \cdot \varphi(h)$$

für alle $g, h \in G$. Ein bijektiver Gruppenhomomorphismus heißt *Gruppenisomorphismus*. Dann heißen die Gruppen G und H *isomorph* und wir schreiben $G \cong H$.

Ist e das neutrale Element von G und e' das neutrale Element von H, dann gilt $\varphi(e) = e'$ für jeden Gruppenhomomorphismus $\varphi\colon G \to H$:

$$\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$$

impliziert durch Kürzung mit $\varphi(e)$, dass $e' = \varphi(e)$. Weiterhin gilt $\varphi(g^{-1}) = \varphi(g)^{-1}$ für alle $g \in G$, weil

$$\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e) = e'.$$

Das Inverse eines Gruppenisomorphismus ist wieder ein Gruppenisomorphismus.

Beispiel 2.2.1. *Wir geben drei Beispiele von Gruppenhomomorphismen.*

1. *Sei H eine Untergruppe von G. Dann ist die Einbettung $H \hookrightarrow G$ ein Gruppenhomomorphismus.*

2. *Die Abbildung $\varphi\colon \mathbb{Z} \to \mathbb{Z}$, $x \mapsto nx$, für ein $n \in \mathbb{Z}$ ist ein Gruppenhomomorphismus.*

3. *Die Exponentialabbildung* $\exp\colon (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ *ist ein Gruppenisomorphismus.*

Definition 2.8. Eine Gruppenhomomorphismus $\varphi\colon G \to G$ heißt *Endomorphismus*. Ist er bijektiv, so heißt er *Automorphismus*. Die Automorphismen einer Gruppe G bilden eine Gruppe unter Komposition, die mit $\mathrm{Aut}(G)$ bezeichnet wird.

Zum Beispiel ist die Konjugationsabbildung

$$i_g\colon G \to G, x \mapsto gxg^{-1}$$

ein Automorphismus von G. Die Abbildung ist bijektiv, und es gilt

$$i_g(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = i_g(x)i_g(y)$$

für alle $g, h \in G$. Also ist i_g ein bijektiver Gruppenhomomorphismus, also ein Automorphismus. Er heißt auch *innerer Automorphismus* von G.

Definition 2.9. Die inneren Automorphismen von G bilden eine Untergruppe von $\mathrm{Aut}(G)$, die mit $\mathrm{Inn}(G)$ bezeichnet wird.

Es gilt

$$(gh)x(gh)^{-1} = g(hxh^{-1})g^{-1}$$

für alle $g, h \in G$, was $i_{gh}(x) = (i_g \circ i_h)(x)$ bedeutet. Die Gruppe $\mathrm{Inn}(G)$ ist genau dann trivial, wenn G abelsch ist.

Definition 2.10. Sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus. Der *Kern* von φ ist durch

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

gegeben und das *Bild* von φ ist durch

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

gegeben.

Es ist leicht zu sehen, dass $\ker(\varphi)$ eine Untergruppe von G ist, und $\mathrm{im}(\varphi)$ eine Untergruppe von H. Weiterhin ist φ genau dann injektiv, wenn $\ker(\varphi)$ trivial ist.

Wir wollen noch eine Anwendung von Gruppenhomomorphismen geben, nämlich den Satz von Cayley.

Satz 2.2.2 (Cayley)**.** *Für jede Gruppe G gibt es einen injektiven Gruppenhomomorphismus $L\colon G \hookrightarrow \mathrm{Sym}(G)$. Insbesondere ist jede endliche Gruppe der Ordnung n isomorph zu einer Untergruppe der S_n.*

Beweis. Man betrachte die Abbildung $L\colon G \to \mathrm{Sym}(G)$, die durch $g \mapsto L_g$ gegeben ist. Wir haben

$$(L_a \circ L_b)(x) = L_{ab}(x)$$

für alle $a, b, x \in G$, und $L_a \in \mathrm{Sym}(G)$ für alle $a \in G$, da jede Abbildung L_a bijektiv ist. In der Tat, $L_e = \mathrm{id}$ und

$$L_a \circ L_{a^{-1}} = \mathrm{id} = L_{a^{-1}} \circ L_a.$$

Also ist L ein Gruppenhomomorphismus. Er ist injektiv, weil die Kürzungsregeln in G gelten; siehe Lemma 2.1.2. □

2.3 Nebenklassen und Faktorgruppen

Sei S eine Teilmenge einer Gruppe G. Definiere Mengen

$$aS = \{as \mid s \in S\},\ Sa = \{sa \mid s \in S\}.$$

Definition 2.11. Sei G eine Gruppe und H eine Untergruppe von G. Die Mengen der Form aH heißen *Linksnebenklassen* von H, und die Mengen der Form Ha heißen *Rechtsnebenklassen* von H.

Wegen $e \in H$ gilt $aH = H$ genau dann wenn $a \in H$.

Satz 2.3.1. *Sei H eine Untergruppe von G.*

(a) *Ein Element $a \in G$ liegt in einer Linksnebenklasse C von H genau dann wenn $C = aH$.*

(b) *Zwei Nebenklassen sind entweder gleich oder disjunkt.*

(c) *Es gilt $aH = bH$ genau dann wenn $a^{-1}b \in H$.*

(d) *Je zwei Nebenklassen haben die gleiche Kardinalität.*

Beweis. (a): Falls $C = aH$ gilt, haben wir $a \in aH$. Umgekehrt, wenn a in der Linksnebenklasse bH liegt, dann folgt $a = bh$ für ein $h \in H$, und

$$aH = bhH = bH.$$

(b): Angenommen, zwei Nebenklassen C und C' sind nicht disjunkt. Dann gibt es ein a in C und in C', so dass $C = aH = C'$ wegen (a).

(c): Falls $a^{-1}b \in H$, dann folgt $H = a^{-1}bH$ und $aH = aa^{-1}bH = bH$. Umgekehrt, falls $aH = bH$ gilt, dann hat man $H = a^{-1}bH$ und $a^{-1}b \in H$.

(d): The Abbildung $L_{ba^{-1}} \colon aH \to bH$, gegeben durch $ah \mapsto bh$ ist eine Bijektion. □

Definition 2.12. Sei H eine Untergruppe von G. Der *Index* $(G : H)$ von H in G ist die Kardinalität der Menge $\{aH \mid a \in G\}$, d.h., die Anzahl der Linksnebenklassen von H in G.

Für die triviale Untergruppe $H = 1$ gilt $(G : 1) = |G|$. Das ist die *Ordnung* von G, d.h., die Anzahl der Elemente in G. Wir haben

$$G = \bigcup_{a \in G} aH.$$

Da je zwei Nebenklassen gleich oder disjunkt sind, bilden sie eine Partition von G.

Theorem 2.3.2 (Lagrange)**.** *Sei G eine endliche Gruppe, und H eine Untergruppe. Dann gilt*

$$(G : 1) = (G : H)(H : 1).$$

Insbesondere teilt die Ordung einer Untergruppe die Ordnung von G.

Beweis. Die Linksnebenklassen von H in G bilden eine Partition von G. Es gibt $(G : H)$ Nebenklassen, und jede hat $(H : 1)$ Elemente. □

Definition 2.13. Die Ordnung eines Gruppenelements $g \in G$ ist definiert als die Ordnung der zyklischen Untergruppe, die durch g erzeugt wird, d.h., $\mathrm{ord}(g) = |\langle g \rangle|$.

Die Abbildung $\psi \colon \mathbb{Z} \to \langle g \rangle$, $k \mapsto g^k$ ist ein surjektiver Gruppenhomomorphismus mit $\langle g \rangle \cong \mathbb{Z}$ für $\mathrm{ord}(g) = \infty$ und $\langle g \rangle \cong \mathbb{Z}/m\mathbb{Z}$ für $\mathrm{ord}(g) = m$, siehe Beispiel 2.3.16. Ist $\mathrm{ord}(g) = m \in \mathbb{N}$, so folgt aus diesem Isomorphismus

$$g^k = e \Leftrightarrow k \in m\mathbb{Z}.$$

Insbesondere ist die Ordnung von g ist auch die kleinste positive Zahl $k \geq 1$ mit $g^k = e$. Existiert keine solche Zahl, so hat man $\mathrm{ord}(g) = \infty$.

Korollar 2.3.3. *Die Ordnung von g teilt die Ordnung von G für jedes $g \in G$, und es gilt*

$$g^{|G|} = e.$$

Beweis. Man wende Lagrange für die Untergruppe $H = \langle g \rangle$ an und benutze $(H : 1) = \mathrm{ord}(g)$. Aus $\mathrm{ord}(g) \mid \mathrm{ord}(G)$ folgt $\mathrm{ord}(G) \in \mathrm{ord}(g)\mathbb{Z}$, und daher $g^{\mathrm{ord}(G)} = e$. □

Bemerkung 2.3.4. Für die Gruppe $U(n) = (\mathbb{Z}/n\mathbb{Z})^\times$ der invertierbaren Elemente in $\mathbb{Z}/n\mathbb{Z}$ bedeutet $a^{|G|} = e$ auch $a^{\varphi(n)} = 1$, wegen $|U(n)| = \varphi(n)$. Für $n = p$ Primzahl ist das der "kleine Fermat": $a^{p-1} \equiv 1 \bmod p$ für $p \nmid a$.

Korollar 2.3.5. *Jede Gruppe von Primzahlordnung p ist isomorph zu der zyklischen Gruppe C_p.*

Beweis. Sei G eine Gruppe der Ordung p. Dann hat jedes Element die Ordung 1 oder p, weil das die einzigen positiven Teiler von p sind. Da G nicht-trivial ist, gibt es ein Element $g \in G$ der Ordnung p. Sei $H = \langle g \rangle \subseteq G$ die zyklische Untergruppe von G, die durch g erzeugt wird. Dann ist $|H| = p$ und $H = G = \{e, g, g^2, \dots g^{p-1}\}$. □

Zu je zwei Gruppen G und H kann man das *direkte Produkt* $G \times H$ bilden. Es ist das kartesische Produkt von G und H mit der Komposition $(g, h)(g', h') = (gg', hh')$. Diese erfüllt alle Gruppenaxiome. Eine endliche Gruppe G mit $\mathrm{ord}(G) = n$ ist zyklisch genau dann, wenn sie ein Element der Ordnung n hat. Man beachte, dass das direkte Produkt $C_n \times C_n$ die Ordung n^2 hat, aber kein Element der Ordung n^2 für $n \geq 2$. Also ist sie nicht zyklisch. Allerdings gilt nun der folgende Satz.

Satz 2.3.6. *Jede Untergruppe einer zyklischen Gruppe ist zyklisch.*

Beweis. Sei G eine zyklische Gruppe mit Erzeuger g. Für eine Untergruppe $H \subseteq G$ werden wir $H = \langle g^n \rangle$ für ein $n \in \mathbb{N}$ zeigen. Also ist H zyklisch. Die triviale Gruppe ist offenbar von dieser Form. Also können wir annehmen, dass H nicht-trivial ist. Sei n die kleinste positive ganze Zahl mit $g^n \in H$. Ein solches n muss existieren, da H nicht-trivial ist, und somit irgendeine Potenz von g enthalten muss. Wir behaupten, dass jedes $h \in H$ eine Potenz von g^n ist. Wir wissen, dass $h = g^m$ für ein $m \in \mathbb{Z}$. Mit dem Euklidischen Algorithmus in $\mathbb{Z}$ erhalten wir $m = qn + r$ für ganze Zahlen q und r mit $0 \leq r < n$. Also ist

$$h = g^m = (g^n)^q g^r,$$

und $g^r = (g^n)^{-q} h$. Wegen $g^n \in H$ zeigt das $g^r \in H$. Da n aber minimnal war, impliziert $0 \leq r < n$ nun $r = 0$. Also gilt $n \mid m$ und $h = g^m \in \langle g^n \rangle$. das zeigt $H = \langle g^n \rangle$. □

Definition 2.14. Eine Untergruppe N von G heißt *normal* oder *Normalteiler*, falls $gN = Ng$ für alle $g \in G$. Wir schreiben $N \triangleleft G$.

Offenbar ist eine Untergruppe N von G genau dann ein Normalteiler, falls $gNg^{-1} = N$ für alle $g \in G$. In einer abelschen Gruppe ist jede Untergruppe

ein Normalteiler. In nicht-abelschen Gruppen muss nicht jede Untergruppe ein Normalteiler sein.

Beispiel 2.3.7. *Sei* $G = GL_2(\mathbb{Z}) = \{A \in M_2(\mathbb{Z}) \mid \det(A) = \pm 1\}$ *und* $N = \{\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) \mid n \in \mathbb{Z}\}$. *Dann ist* G *eine Gruppe, und* N *eine Untergruppe von* G*, die nicht normal ist.*

Für $g = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \in G$ haben wir

$$g \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} g^{-1} = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \notin N.$$

Lemma 2.3.8. *Der Kern eines Gruppenhomomorphismus* $\varphi\colon G \to H$ *ist stets ein Normalteiler von* G*.*

Beweis. Sei $N = \ker(\varphi)$. Es genügt, $aNa^{-1} \subseteq N$ für alle $a \in G$ zu zeigen, da daraus auch $a^{-1}Na \subseteq N$ folgt. Das kann man umschreiben als $aN \subseteq Na$ und $Na \subseteq aN$, was $aN = Na$ für alle $a \in G$ bedeutet.
Sei also $x \in N$, d.h., $\varphi(x) = e_H$. Dann ist

$$\begin{aligned} \varphi(axa^{-1}) &= \varphi(a)\varphi(x)\varphi(a)^{-1} \\ &= \varphi(a)e_H\varphi(a)^{-1} \\ &= e_H. \end{aligned}$$

□

Beispiel 2.3.9. *Der Kern des Gruppenhomomorphismus* $\det\colon GL_n(K) \to K^\times$ *ist ein Normalteiler in* $GL_n(K)$*, der durch*

$$SL_n(K) = \{A \in GL_n(K) \mid \det(A) = 1\}$$

gegeben ist.

Das Argument kann man auch für $GL_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \det(A) = \pm 1\}$ rechtfertigen, d.h.,

$$SL_n(\mathbb{Z}) \triangleleft GL_n(\mathbb{Z}),$$

siehe auch Beispiel 2.3.7.

Lemma 2.3.10. *Jede Untergruppe* H *von* G *mit* $(G : H) = 2$ *ist normal.*

Beweis. Ist $(G : H) = 2$, dann ist $G = H \cup gH$ als disjunkte Vereinigung. Also ist gH das Komplement von H in G. Das gleiche Argument zeigt, dass auch Hg das Komplement von H in G ist. Also gilt $gH = G \setminus H = Hg$ für alle $g \in G$. □

Beispiel 2.3.11. *Die Untergruppe $C_n = \{e, r, r^2, \ldots, r^{n-1}\}$ in D_n hat Index 2, and ist deshalb ein Normalteiler.*

Lemma 2.3.12. *Sei N ein Normalteiler einer Gruppe G. Die Menge der Nebenklassen G/N wird mit der Multiplikation $aN \cdot bN = abN$ zu einer Gruppe, der sogenannten Faktorgruppe. Die Abbildung $\pi\colon G \to G/N$, $a \mapsto aN$ ist ein Gruppenhomomorphismus mit* $\ker(\pi) = N$.

Beweis. Die Multiplikation ist wohldefiniert, weil $(ab)N$ nicht von der Wahl der Repräsentanten abhängt. Ist $xN = aN$ und $yN = bN$ für irgenwelche $x, y \in G$, so folgt

$$\begin{aligned}(ab)N &= a(bN) = a(yN) = a(Ny)\\ &= (aN)y = (xN)y = x(Ny)\\ &= x(yN) = (xy)N.\end{aligned}$$

Hier haben wir wesentlich benutzt, dass N normal ist. Man prüft nun die Gruppenaxiome leicht nach. Das neutrale Element von G/N ist $eN = N$, und das Inverse zu aN ist $a^{-1}N$. Wir haben

$$\pi(ab) = abN = aN \cdot bN = \pi(a)\pi(b),$$

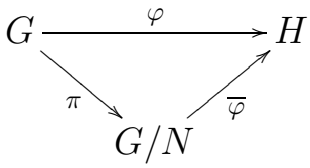
und π ist offensichtlich surjektiv. Es gilt wegen Satz 2.3.1, Teil (c),

$$\begin{aligned}\ker(\pi) &= \{a \in G \mid \pi(a) = eN\}\\ &= \{a \in G \mid aN = eN\}\\ &= \{a \in G \mid a \in N\}\\ &= N.\end{aligned}$$

□

Der Homomorphismus $\pi\colon G \to G/N$ hat eine universelle Eigenschaft.

Satz 2.3.13 (Homomorphiesatz). *Sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus, und N ein Normalteiler von G mit $N \subseteq \ker(\varphi)$. Dann existiert genau ein Gruppenhomomorphismus $\overline{\varphi}\colon G/N \to H$, so dass das Diagramm*



kommutiert, d.h., mit $\varphi = \overline{\varphi} \circ \pi$. Es gilt $\operatorname{im}(\overline{\varphi}) = \operatorname{im}(\varphi)$ und $\ker(\overline{\varphi}) = \pi(\ker(\varphi))$. Insbesondere ist $\overline{\varphi}$ genau dann injektiv, wenn $\ker(\varphi) = N$ gilt.

Beweis. Für jede Abbildung $\overline{\varphi}$ mit $\varphi = \overline{\varphi} \circ \pi$ gilt $\overline{\varphi}(aN) = \varphi(a)$. Daher ist $\overline{\varphi}$ eindeutig bestimmt, falls es existiert. Die Existenz erscheint trivial, weil wir ja $\overline{\varphi}$ einfach durch $\overline{\varphi}(aN) = \varphi(a)$ definieren können. Das macht aber nur dann Sinn, wenn aus $aN = bN$ schon $\varphi(a) = \varphi(b)$ folgt. Das nennt man die *Wohldefiniertheit* von $\overline{\varphi}$, und die müssen wir jetzt zeigen. In der Tat, aus $aN = bN$ folgt $b^{-1}a \in N \subseteq \ker(\varphi)$. Das bedeutet

$$e_H = \varphi(b^{-1}a) = \varphi(b)^{-1}\varphi(a),$$

also $\varphi(a) = \varphi(b)$. Weiterhin gilt

$$\overline{\varphi}(aN)\overline{\varphi}(bN) = \varphi(a)\varphi(b) = \varphi(ab) = \overline{\varphi}(abN) = \overline{\varphi}(aN \cdot bN).$$

Also ist $\overline{\varphi}$ ein Gruppenhomomorphismus. Weiterhin gilt $\operatorname{im}(\overline{\varphi}) = \operatorname{im}(\varphi)$ und $\ker(\overline{\varphi}) = \pi(\ker(\varphi))$ nach Definition. Da π surjektiv ist, ist $\ker(\varphi)$ das Urbild von $\ker(\overline{\varphi})$ unter π, d.h.,

$$\ker(\varphi) = \pi^{-1}(\ker(\overline{\varphi})).$$

Nun ist $\overline{\varphi}$ genau dann injektiv, wenn $\ker(\overline{\varphi}) = N$ trivial ist, d.h., wenn $\ker(\varphi) = \pi^{-1}(N) = N$ ist. □

Korollar 2.3.14. *Sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus. Dann gilt*

$$G/\ker(\varphi) \cong \varphi(G).$$

Beweis. Nach Satz 2.3.13 mit $N = \ker(\varphi)$ existiert ein eindeutig bestimmter Homomorphismus $\overline{\varphi}\colon G/\ker(\varphi) \to \varphi(G)$ mit $\varphi = \overline{\varphi} \circ \pi$. Er ist injektiv wegen $\ker(\varphi) = N$ und surjektiv wegen $\operatorname{im}(\overline{\varphi}) = \operatorname{im}(\varphi) = \varphi(G)$. Also ist er ein Isomorphismus. □

Beispiel 2.3.15. *Für $G = GL_n(K)$ und $\varphi = \det\colon GL_n(K) \to K^\times$ gilt* $\ker(\varphi) = SL_n(K)$ *und $\varphi(G) = K^\times$. Also erhalten wir*

$$GL_n(K)/SL_n(K) \cong K^\times.$$

Beispiel 2.3.16. *Sei $G = \langle g \rangle$ eine endliche zyklische Gruppe. Dann ist $\varphi\colon \mathbb{Z} \to G$, $k \mapsto g^k$ ein Gruppenhomomorphismus mit* $\ker(\varphi) = m\mathbb{Z}$ *für ein $m \in \mathbb{Z}$ und $\varphi(\mathbb{Z}) = G$. Wir erhalten dann*

$$\mathbb{Z}/m\mathbb{Z} \cong G.$$

Für zwei Untergruppen H und N von G bezeichne

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

das Komplexprodukt.

Satz 2.3.17 (1. Isomorphiesatz)**.** *Sei G eine Gruppe, H eine Untergruppe und N ein Normalteiler. Dann ist HN eine Untergruppe von G, N ein Normalteiler in HN und $H \cap N$ ein Normalteiler in H. Die Einbettung $H \subseteq HN$ induziert einen Isomorphismus*

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

Beweis. Die Menge HN erfüllt die Untergruppenaxiome (S1) und (S2). Für Elemente $h_1n_1, h_2n_2 \in HN$ gilt

$$(h_1n_1)(h_2n_2) = h_1(n_1h_2)n_2 \in h_1h_2N,$$

weil $n_1h_2 \in Nh_2 = h_2N$ ist, also $n_1h_2 = h_2n$ für ein $n \in N$ gilt. Das zeigt (S1). Für $hn \in HN$ gilt

$$(hn)^{-1} = n^{-1}h^{-1} = (h^{-1}n^{-1}h)h^{-1} \in NH,$$

weil $h^{-1}n^{-1}h = n' \in N$ gilt. Also gilt $(S2)$. Wegen $N \lhd G$ gilt erst recht $N \lhd HN$. Die Komposition

$$H \hookrightarrow HN \to HN/N$$

ist ein surjektiver Homomorphismus mit Kern $H \cap N$, der deswegen ein Normalteiler in H ist. In der Tat, $\varphi\colon H \to HN/N$ ist durch $h \mapsto hN$ gegeben, mit

$$\begin{aligned}\ker(\varphi) &= \{a \in H \mid aN = N\} \\ &= \{a \in H \mid a \in N\} \\ &= H \cap N.\end{aligned}$$

Aus Korollar 2.3.14 folgt dann

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

□

Einen surjektiven Homomorphismus bezeichnet man auch als *Epimorphismus.*

Satz 2.3.18 (2. Isomorphiesatz)**.** *Sei G eine Gruppe, H und N Normalteiler mit $N \subseteq H$. Dann ist N auch Normalteiler in H, und man kann H/N als Normalteiler von G/N auffassen. Es gibt einen Epimorphismus $G/N \to G/H$, der einen Isomorphismus*

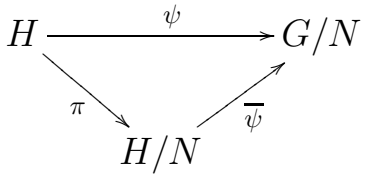
$$(G/N)/(H/N) \cong G/H.$$

induziert.

Beweis. Wegen $N \triangleleft G$ gilt auch $N \triangleleft H$. Die Inklusion $H \hookrightarrow G$ induziert den Homomorphismus

$$\psi\colon H \hookrightarrow G \to G/N,$$

der den Kern N hat. nach dem Homomorphiesatz gibt es also einen eindeutig bestimmen Homomorphismus $\overline{\psi}\colon H/N \to G/N$, so dass das Diagramm



kommutiert, d.h., mit $\psi = \overline{\psi} \circ \pi$. Wegen $\ker(\psi) = N$ ist $\overline{\psi}$ injektiv. Also können wir H/N mit der Untergruppe $\mathrm{im}(\overline{\psi})$ von G/N identifizieren. Der Epimorphismus $G \to G/H$ induziert wegen $N \subseteq H$ auch einen Epimorphismus

$$\varphi\colon G/N \to G/H,\ aN \mapsto aH$$

mit

$$\begin{aligned}\ker(\varphi) &= \{aN \in G/N \mid aH = H\} \\ &= \{aN \in G/N \mid a \in H\} \\ &= H/N.\end{aligned}$$

Nun folgt die Behauptung aus Korollar 2.3.14. □

Beispiel 2.3.19. *Wir haben*

$$(\mathbb{Z}/16\mathbb{Z})/(8\mathbb{Z}/16\mathbb{Z}) \cong \mathbb{Z}/8\mathbb{Z}.$$

2.4 Symmetrische Gruppen

Nach dem Satz von Cayley (Satz 2.2.2) kann jede endliche Gruppe als Untergruppe einer symmetrischen Gruppe aufgefasst werden. Es lohnt sich daher, symmetrische Gruppen und ihre Elemente etwas genauer zu betrachten. Jedes Element $\pi \in S_n$ ist eine Permutation der Zahlen in $X = \{1, 2, \ldots, n\}$, die man zunächst in zweireihiger Notation darstellen kann:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \pi(1) & \pi(2) & \pi(3) & \cdots & \pi(n) \end{pmatrix}.$$

Es ist aber oft günstiger, π als Produkt von sogenannten *Zykeln* darzustellen.

Definition 2.15. Seien $i_1, \ldots, i_k$ verschiedene ganze Zahlen aus X. Ein Element $\pi \in S_n$ heißt *k-Zykel*, falls

$$\pi(i_1) = i_2, \ldots, \pi(i_{k-1}) = i_k, \pi(i_k) = i_1,$$

und π alle übrigen Elemente aus X fixiert. Man schreibt $\pi = (i_1 \ldots i_k)$. Wir nennen $\{i_1, \ldots, i_k\}$ den *Träger* des k-Zykels.

Ein 1-Zykel fixiert alle $i \in X$, also haben wir $(i) = \mathrm{id}$. Ein 2-Zykel (ij) heißt auch *Transposition*. Wegen $(ij)^2 = \mathrm{id}$ hat eine Transposition die Ordnung 2 in der Gruppe S_n. Allgemeiner hat ein k-Zykel die Ordnung k.

Bemerkung 2.4.1. Je zwei Zykel $\sigma, \tau \in S_n$ mit disjunkten Trägern kommutieren, d.h., $\sigma\tau = \tau\sigma$.

Lemma 2.4.2. *Sei $\alpha = (i_1 \cdots i_k)$ ein k-Zykel und $\tau \in S_n$. Dann ist $\tau\alpha\tau^{-1}$ wieder ein k-Zykel, gegeben durch*

$$\tau\alpha\tau^{-1} = (\tau(i_1) \cdots \tau(i_k)).$$

Beweis. Wegen $(\tau^{-1}\tau)(i_r) = i_r$ und $\alpha(i_r) = i_{r+1 \bmod k}$ gilt

$$\tau\alpha\tau^{-1}(\tau(i_r)) = \tau(i_{r+1 \bmod k})$$

für alle $1 \leq r \leq k$. Sei $1 \leq j \leq n$ gegeben mit $j \neq i_r$ für jedes r. Dann ist $\alpha(j) = j$, weil j nicht im k-Zykel α enthalten ist. Also ist $\tau\alpha\tau^{-1}(\tau(j)) = \tau(j)$, und $\tau\alpha\tau^{-1}$ fixiert jede Zahl, die nicht von der Form $\tau(i_r)$ ist für ein i, und wir haben

$$\tau\alpha\tau^{-1} = (\tau(i_1) \cdots \tau(i_k)).$$

□

Nicht jede Permutation ist ein Zykel, aber jede Permutation kann, im wesentlichen eindeutig, als Produkt von Zyklen geschrieben werden:

Satz 2.4.3 (Zykelzerlegung)**.** *Sei $\sigma \in S_n$. Dann gibt es ein $r \in \mathbb{N}$ und Zyklen $\sigma_1, \ldots, \sigma_r$ der Länge mindestens zwei mit paarweise disjunkten Trägern und*

$$\sigma = \sigma_1 \cdots \sigma_r.$$

Dabei sind r und $\{\sigma_1, \ldots, \sigma_r\}$ eindeutig durch σ bestimmt.

Der Satz folgt leicht durch Induktion über die Anzahl der $i \in X$, die durch σ nicht fixiert werden, und ist dem Leser als Übung überlassen.

Beispiel 2.4.4.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 4 & 2 & 1 & 3 & 6 & 8 \end{pmatrix} = (15)(27634)(8).$$

Satz 2.4.5. *Jedes $\sigma \in S_n$ ist für $n \geq 2$ ein Produkt von Transpositionen.*

Beweis. Wegen Satz 2.4.3 genügt es zu zeigen, dass jeder k-Zykel ein Produkt von Transpositionen ist. Für $k = 1$ gilt $(1) = (12)^2$, und für $k \geq 2$ gilt

$$(i_1 i_2 \cdots i_k) = (i_1 i_2)(i_2 i_3) \cdots (i_{k-1} i_k).$$

□

Beispiel 2.4.6.

$$(13526) = (13)(35)(52)(26).$$

Definition 2.16. Das *Signum* von $\pi \in S_n$ ist definiert durch

$$sgn(\pi) = \prod_{i<j} \frac{\pi(i) - \pi(j)}{i - j}.$$

Es definiert eine Abbildung $sgn\colon S_n \to \{\pm 1\}$ durch $\pi \mapsto sgn(\pi)$.

Satz 2.4.7. *Die Abbildung* $sgn\colon S_n \to C_2$ *ist ein Gruppenhomomorphismus, d.h.,*

$$sgn(\sigma\tau) = sgn(\sigma)sgn(\tau)$$

für alle $\sigma, \tau \in S_n$.

Den Beweis kennen wir aus der linearen Algebra.

Definition 2.17. Die *alternierende Gruppe* A_n ist definiert als der Kern des Signum-Homomorphismus.

Offenbar gilt $A_1 = A_2 = 1$ und $|A_n| = \frac{n!}{2}$ für $n \geq 2$. Als Kern ist A_n ein Normalteiler von S_n mit Faktorgruppe $S_n/A_n \cong C_2$. Da Transpositionen das Signum -1 haben, liegen sie nicht in A_n. Aber alle Elemente, die ein Produkt von einer geraden Anzahl von Transpositionen sind, liegen in A_n. Umgekehrt sind alle Elemente von A_n ein (eventuell leeres) Produkt von einer geraden Anzahl von Transpositionen, siehe Satz 2.4.5.

Lemma 2.4.8. *Jedes Element von* A_n, $n \geq 3$ *ist ein Produkt von* 3*-Zykeln. Also wird* A_n *von* 3*-Zykeln erzeugt.*

Beweis. Es gilt $(1) = (123)^3$. Jedes $\pi \in A_n$ ist ein Produkt von einer geraden Anzahl von Transpositionen. Aber das Produkt von je zwei Transpositionen kann immer als Produkt von 3-Zykeln geschrieben werden. Entweder ist $(ij)(ij) = (1)$, oder $(ij)(jl) = (ijl)$, oder

$$(ij)(kl) = (ij)(jk)(jk)(kl) = (ijk)(jkl)$$

für paarweise verschiedene i, j, k, l. □

Beispiel 2.4.9. *Wir haben* $A_3 = \{(1), (123), (132)\}$. *Wegen Korollar* 2.3.5 *ist jede Gruppe der Ordnung* 3 *isomorph zu* C_3, *d.h.,* $A_3 \cong C_3$.

2.5 Gruppen kleiner Ordung

Wir möchten mit elementaren Mitteln alle Gruppen der Ordung $n \leq 8$ bis auf Isomorphie bestimmen. Zunächst einmal gibt es zu jedem $n \in \mathbb{N}$ eine zyklische Gruppe der Ordnung n, nämlich C_n. Zudem kennen wir schon die S_3 mit 6 Elementen, und die D_4 mit 8 Elementen. Wir können auch direkte Produkte von diesen Gruppen betrachten. Wir benötigen noch eine andere wichtige Gruppe der Ordnung 8.

Definition 2.18. Sei Q_8 die von

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

erzeugte Untergruppe von $GL_2(\mathbb{C})$. Sie heißt *Quaternionengruppe*.

Es gilt

$$K = IJ = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = -JI$$

und $J^2 = I^2 = K^2 = -E$, also $J^4 = I^4 = K^4 = E$. Somit besteht Q_8 aus den Matrizen

$$\begin{aligned} Q_8 &= \{E, -E, I, -I, J, -J, K, -K\} \\ &= \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right), \left(\begin{smallmatrix} -i & 0 \\ 0 & i \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -i \\ -i & 0 \end{smallmatrix}\right)\}. \end{aligned}$$

Da Gruppen der Ordnung p mit p prim isomorph zu C_p sind, gibt es je eine Gruppe der Ordnung $1, 2, 3$. Für $|G| = 4$ gibt es mehr als nur eine Gruppe.

Satz 2.5.1. *Jede Gruppe der Ordnung* 4 *ist isomorph zu* C_4 *oder* $C_2 \times C_2$.

Beweis. Sei G eine Gruppe der Ordnung 4. Falls G ein Element der Ordnung 4 hat, gilt $G \cong C_4$. Andernfalls gilt $G = \{e, a, b, c\}$ und die Ordnung von a, b, c ist ein echter Teiler von 4 nach Lagrange, aber nicht 1, weil die Elemente verschieden von e sind. Also haben a, b, c die Ordnung 2 und es gilt $a^2 = b^2 = c^2 = e$. Wir behaupten, dass $ab = c$ gilt, weil alle anderen Wahlen für ab unmöglich sind. Aus $ab = e$ würde zum Beispiel $a = b^{-1}$ folgen, also $b = b^{-1} = a$, ein Widerspruch. $ab = a$ würde $b = e$

bedeuten und $ab = b$ wiederum $a = e$. In der gleichen Weise sehen wir, dass $ba = c = ab, ca = b = ac$ und $cb = a = bc$ gilt. Mit diesen Relationen und $C_2 = \{\pm 1\}$ sieht man leicht, dass die Abbildung $f\colon G \to C_2 \times C_2$ mit

$$f(e) = (1,1),\ f(a) = (-1,1),\ f(b) = (1,-1),\ f(c) = (-1,-1)$$

ein Isomorphismus ist. □

Satz 2.5.2. *Jede Gruppe gerader Ordnung hat eine ungerade Anzahl von Elementen der Ordnung* 2.

Beweis. Für $a \in G$ sei $U_a = \{a, a^{-1}\}$. Es gilt $|U_a| = 2$, außer für Elemente der Ordnung 1 und 2, wo $a = a^{-1}$ gilt. Sei k die Anzahl der Elemente der Ordnung 2 in G. Es gibt genau ein Element der Ordnung 1. Wir haben die disjunkte Vereinigung

$$G = \bigcup_{a \in G} U_a$$

und somit

$$|G| = \sum_{a \in G} |U_a| = |U_e| + k \cdot 1 + \ell \cdot 2.$$

Wegen $|U_e| = 1$ muss k ungerade sein. □

Wir wollen diesen Satz auf Gruppen der Ordnung 6 anwenden.

Lemma 2.5.3. *Sei G eine Gruppe der Ordnung* 6. *Dann besitzt G ein Element der Ordnung* 2 *und ein Element der Ordnung* 3.

Beweis. Hat G ein Element der Ordnung 6, so ist $G \cong C_6 \cong C_2 \times C_3$, und die Behauptung ist richtig. Andernfalls haben alle Elemente außer e die Ordnung 2 oder 3 wegen Lagrange. Nach Satz 2.5.2 gibt es 1, 3 oder 5 Elemente der Ordnung 2. Angenommen, es gäbe 5 solche Elemente. Dann hätte G mindestens drei Erzeuger a, b, c, denn für 2 Erzeuger der Ordnung 2 wäre $G \cong C_2 \times C_2$. Dann wären aber auch alle Elemente a, b, c, ab, ac, bc, abc verschieden wegen der Kürzungsregel. Somit wäre

$$G = \{e, a, b, c, ab, ac, bc, abc\} \cong C_2 \times C_2 \times C_2,$$

und G hätte mehr als 6 Elemente, ein Widerspruch. Also hat G ein oder drei Elemente der Ordung 2 und mindestens ein Element der Ordnung 3. □

Satz 2.5.4. *Jede Gruppe der Ordnung* 6 *ist isomorph zu* C_6 *oder* S_3.

Beweis. Wegen Lemma 2.5.3 gibt es Elemente $a, b \in G$ mit $\mathrm{ord}(a) = 2$ und $\mathrm{ord}(b) = 3$. Dann sind die Elemente e, a, b, ab, b^2, ab^2 wegen den Kürzungsregeln alle verschieden. Da G sechs Elemente hat, folgt

$$G = \{e, a, b, ab, b^2, ab^2\}.$$

Nun bestimmen wir ba. Es muss eines der 6 Elemente sein. $ba = e$ ist unmöglich, da sonst $b = a^{-1}$ und $2 = \mathrm{ord}(a) = \mathrm{ord}(a^{-1}) = \mathrm{ord}(b) = 3$. $ba = a$ oder $ba = b$ würde $b = e$ oder $a = e$ bedeuten. Auch $ba = b^2$ ist unmöglich. Angenommen, $ba = ab$. Dann besteht die Gruppe genau aus den Elementen $\{a^i b^j \mid i = 0, 1,\ j = 0, 1, 2\} = C_2 \times C_3 \cong C_6$. Andernfalls gilt $ba = ab^2 = ab^{-1}$. Das ist genau die Definition von D_3. Mit $a = (12)$ und $b = (123)$ ist das die Gruppe S_3, wie wir schon gesehen haben. □

Lemma 2.5.5. *Jede abelsche Gruppe der Ordnung* 8 *ist isomorph zu* C_8, $C_2 \times C_4$ *oder* $C_2 \times C_2 \times C_2$.

Beweis. Ohne die Klassifikation endlich-erzeugter abelscher Gruppen zu verwenden, kann man wie folgt argumentieren. Falls G ein Element der Ordung 8 hat, gilt $G \cong C_8$. Wenn G kein Element der Ordnung 4 hat, so haben alle Elemente außer e die Ordnung 2 und wir erhalten $G \cong C_2 \times C_2 \times C_2$ wie in Beweis von Lemma 2.5.3. Es bleibt der Fall, das G ein Element a mit $\mathrm{ord}(a) = 4$ hat. Sei $N = \langle a \rangle$ und b irgendein Element in $G \setminus N$. Dann ist $bN \neq N$ und

$$G = N \cup bN = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

Angenommen, alle Elemente in $G \setminus N$ hätten Ordnung 4. Dann hätte b^2 die Ordnung 2, weswegen dann $b^2 \in N$ gälte. Aber das einzige Element der Ordnung 2 in N ist a^2, also hat man $a^2 = b^2$ und mit $a^4 = e$ dann

$$(a^3b)^2 = a^3ba^3b = a^6b^2 = a^8 = e.$$

Das ist ein Widerspruch zu $\mathrm{ord}(a^3b) = 4$. Also gibt es doch ein Element b der Ordnung 2 in $G \setminus N$. Wir haben $N = \langle a \rangle \cong C_4$ und $K = \langle b \rangle \cong C_2$, und G ist das direkte Produkt beider Gruppen. In der Tat gilt $N \cap K = 1$, $N, K \trianglelefteq G$ und $NK = G$, wegen

$$|NK| = \frac{|N||K|}{|N \cap K|} = \frac{4 \cdot 2}{1} = 8.$$

Also ist $G \cong N \times K \cong C_4 \times C_2$. □

Satz 2.5.6. *Jede nicht-abelsche Gruppe der Ordnung* 8 *ist isomorph zu* D_4 *oder* Q_8.

Beweis. Da G nicht-abelsch ist, haben alle Elemente bis auf e die Ordnung 2 oder 4. Gilt $g^2 = e$ für alle $g \in G$ dann ist G abelsch. Also gibt es ein Element $x \in G$ der Ordnung 4. Sei $y \in G \setminus \langle x \rangle$. Die Untergruppe $\langle x, y \rangle$ enthält $\langle x \rangle$ als echte Teilmenge, also gilt $\langle x, y \rangle = G$. Nach Vorraussetzung kommutieren x und y nicht. Da $\langle x \rangle$ Index 2 in G hat, ist es ein Normalteiler. Also gilt

$$yxy^{-1} \in \langle x \rangle = \{e, x, x^2, x^3\}.$$

Da yxy^{-1} Ordnung 4 hat, folgt $yxy^{-1} = x$ oder $yxy^{-1} = x^3 = x^{-1}$. Der erste Fall isr unmöglich, denn x und y kommutieren nicht. Also gilt $yxy^{-1} = x^{-1}$. Die Gruppe $G/\langle x \rangle$ hat Ordnung 2, also gilt

$$y^2 \in \langle x \rangle = \{e, x, x^2, x^3\}.$$

Da y Ordnung 2 oder 4 hat, hat y^2 Ordnung 1 oder 2. Also $y^2 = 1$ oder $y^2 = x^2$. Also haben wir $G = \langle x, y \rangle$ mit entweder

$$x^4 = e, y^2 = e, yxy^{-1} = x^{-1},$$

oder

$$x^4 = e, y^2 = x^2, yxy^{-1} = x^{-1}.$$

Es ist nun leicht zu sehen, dass $G \cong D_4$ im ersten Fall, und $G \cong Q_8$ im zweiten Fall. □

Sei $f(n)$ die Anzahl der nicht-isomorphen Gruppen der Ordnung n. Dann ist die Klassifikation der Gruppen mit $n \leq 8$ wie folgt gegeben:

n	$f(n)$	Gruppen
1	1	1
2	1	C_2
3	1	C_3
4	2	$C_4, C_2 \times C_2$
5	1	C_5
6	2	C_6, S_3
7	1	C_7
8	5	$C_8, C_2 \times C_4, C_2 \times C_2 \times C_2, Q_8, D_4$

Bemerkung 2.5.7. Die Resultate in diesem Abschnitt sind Spezialfälle allgemeinerer Resultate. Satz 2.5.1 kann für alle Gruppen der Ordnung p^2 verallgemeinert werden. Es gibt genau zwei verschiedene Gruppen der Ordnung p^2, nämlich $C_p \times C_p$ und C_{p^2}. Lemma 2.5.3 ist ein Spezialfall des Satzes von *Cauchy*: für jede Primzahl p, die die Gruppenordnung teilt, gibt es ein Element der Ordnung p in G. Auch Satz 2.5.4 gilt allgemeiner: jede Gruppe der Ordnung $2p$ für eine ungerade Primzahl p ist isomorph zu C_{2p} oder D_p.

Bemerkung 2.5.8. Die Funktion $f(n)$ hat in der *Online Encyclopedia of Integer Sequences* OEIS sogar die erste Nummer, nämlich A000001. Diese Funktion wächst rasant für Primzahlpotenzen p^n, siehe Higman's Arbeit [3]. In der Tat haben wir

$$p^{\frac{2}{27}n^2(n-6)} \leq f(p^n) \leq p^{\frac{2}{27}n^3+O(n^{5/2})}$$

Was die Klassifikation von endlichen Gruppen im allgemeinen betrifft, so gibt es das *Millennium-Projekt* von Besche, Eick und O'Brian [1]. Sie haben alle Gruppen der Ordnung $n \leq 2000$ klassifiziert. Die Arbeit wurde 2002 publiziert (ein kleiner Fehler in der Anzahl wurde 2022 von Burell korrigiert). Die meisten Gruppen gibt es tendenziell für Potenzen von 2. Es gibt genau 49.910.531.351 verschiedene Gruppen der Ordnung $n \leq 2000$. Mehr als 99% von ihnen haben die Ordnung 2^{10}. Es gilt $f(2^{10}) = 49.487.367.289$. Die anderen Werte für $f(2^k)$, mit $k = 1, \ldots 9$ sind

$$1,\ 2,\ 5,\ 14,\ 51,\ 267,\ 2328,\ 56092,\ 10494213.$$

2.6 Gruppenoperationen

Definition 2.19. Sei G eine Gruppe und X eine Menge. Eine *Gruppenoperation* von G auf X ist eine Abbildung $(g, x) \mapsto gx$, $G \times X \to X$ mit

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

(2) $ex = x$ für das neutrale Element $e \in G$ und alle $x \in X$.

Eine Gruppenoperation von G auf X ist nichts anderes als ein Gruppenhomomorphismus $G \to \mathrm{Sym}(X)$. Die Operation definiert nämlich Linksmultiplikationen $L_g \in \mathrm{Sym}(X)$, und die Axiome besagen dann, daß $L\colon G \to$

$\mathrm{Sym}(X)$, $g \mapsto L(g) = L_g$ ein Homomorphismus ist.

Die Operation hießt *treu*, falls L injektiv ist, d.h., falls gilt

$$gx = x \text{ für alle } x \in X \text{ impliziert } g = e.$$

Beispiel 2.6.1. 1. *Jede Gruppe G operiert auf jeder Menge X durch die triviale Operation, d.h., durch $gx = x$ für alle $g \in G$ und alle $x \in X$.*

2. *Die Gruppe $GL_n(K)$ operiert auf K^n durch Matrix Multiplikation, also durch $(A, x) \mapsto Ax$.*

3. *Die symmetrische Gruppe S_n operiert durch Permutationen auf der Menge $X = \{1, 2, \ldots, n\}$.*

4. *Jede Gruppe G operiert auf sich selbst durch Konjugation: mit $X = G$ ist die Operation durch $(g, x) \mapsto gxg^{-1}$ gegeben.*

5. *Für jede Gruppe G operiert die Automorphismengruppe $\mathrm{Aut}(G)$ auf G.*

6. *Die Gruppe $SL_2(\mathbb{C})$ der komplexen 2×2-Matrizen $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ mit Determinante $\det(A) = 1$ operiert auf der Riemannschen Zahlenkugel $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ durch Möbius Transformationen*

$$(A, z) \mapsto A \cdot z = \frac{az + b}{cz + d},$$

mit $A \cdot \infty = a/c$ und $A \cdot (-d/c) = \infty$.

Wir wollen die Axiome für das letzte Beispiel nachprüfen. Die Einheitsmatrix I operiert durch $Iz = \frac{1z+0}{0z+1} = z$. Für zwei Matrizen $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ hat man

$$\begin{aligned} A \cdot (B \cdot z) = A \cdot \left(\frac{\alpha z + \beta}{\gamma z + \delta}\right) &= \frac{a\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right) + b}{c\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right) + d} \\ &= \frac{(a\alpha + b\gamma)z + (a\beta + b\delta)}{(c\alpha + d\gamma)z + (c\beta + d\delta)} \\ &= \begin{pmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{pmatrix} \cdot z \\ &= (AB) \cdot z. \end{aligned}$$

Definition 2.20. Sei G eine Gruppe, die auf einer Menge X operiert. Für $x \in X$ heißt die Menge

$$Gx = \{gx \mid g \in G\} \subseteq X$$

die *Bahn* von x. Man sagt auch G-Orbit und schreibt $O(x)$.

Beispiel 2.6.2. *Operiert G auf such selbst durch Konjugation, so sind die G-Orbiten nichts anderes als die Konjugationsklassen. Hier ist für $x \in X = G$ die Konjugationsklasse von x die Menge*

$$\{gxg^{-1} \mid g \in G\}.$$

Zwei Bahnen Gx und Gy sind entweder disjunkt oder gleich, denn aus

$$gx = hy \in Gx \cap Gy$$

folgt $x = g^{-1}hy$, also $Gx \subseteq Gy$, und $y = h^{-1}gx$, also $Gy \subseteq Gx$. Also ist X die disjunkte Vereinigung aller Bahnen.

Definition 2.21. Sei G eine Gruppe, die auf einer Menge X operiert. Für $x \in X$ heißt die Menge

$$G_x = \{g \in G \mid gx = x\} \subseteq G$$

der *Stabilisator* von x, oder die Isotropiegruppe von x.

In der Tat ist G_x eine Untergruppe von G, aber im allgemeinen kein Normalteiler.

Beispiel 2.6.3. *Operiert G auf such selbst durch Konjugation, so sind die Stabilisatoren gerade die* Zentralisatoren. *Hier ist für $x \in X$ der* Zentralisator *von x in G die Menge*

$$C_G(x) = \{g \in G \mid gx = xg\}.$$

Das Zentrum $Z(G)$ von G ist gerade der Schnitt über alle Zentralisatoren,

$$Z(G) = \bigcap_{x \in G} C_G(x) = \{g \in G \mid gx = xg \; \forall \, x \in G\}.$$

Beispiel 2.6.4. *Sei G eine Gruppe, die durch Konjugation auf sich selbst operiert und H eine Untergruppe von G. Dann ist der Stabilisator von H genau der Normalisator von H in G. Hier ist der* Normalisator $N_G(H)$ *von H in G gegeben durch*

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

Definition 2.22. Eine Gruppenoperation einer Gruppe G auf einer nichtleeren Menge X heißt *transitiv*, falls es nur eine Bahn gibt, d.h., falls für alle $x, y \in X$ ein $g \in G$ existiert mit $gx = y$.

Dann ist $Gx = X$ für alle $x \in X$.

Beispiel 2.6.5. *1. Die Gruppe S_n operiert transitiv auf $X = \{1, 2, \ldots, n\}$.*

2. Die Konjugationsoperation einer nicht-trivialen Gruppe G ist nicht transitiv.

3. Die Operation von $GL_n(K)$ auf K^n durch Matrix Multiplkation ist nicht transitiv.

Für 1. benutze man, dass 1 auf jede Zahl in X abbildet werden kann unter einer Permutation von S_n. Wäre die Operation in 2. transitiv, so wäre jeder Orbit gleich G. Wegen $g \cdot e = geg^{-1} = e$ wäre also G trivial, Widerspruch. Für 3. genügt es zu bemerken, dass die Bahn von 0 nicht gleich X ist.

2.7 Die Klassengleichung

Definition 2.23. Sei G eine Gruppe, die auf X operiert. Eine G-invariante Abbildung zwischen G-Mengen X und Y ist eine Abbildung $\varphi\colon X \to Y$ mit $\varphi(gx) = g\varphi(x)$ für alle $x \in X$ und alle $g \in G$. Die Abbildung φ heißt *Isomorphismus von G-Mengen*, falls φ bijektiv und G-invariant ist.

Theorem 2.7.1 (Orbit-Stabilisator-Theorem)**.** *Sei G eine Gruppe, die auf X operiert. Dann ist die Abbildung*

$$\varphi\colon G/G_x \to Gx,\ gG_x \mapsto gx$$

ein Isomorphismus von G-Mengen und es gilt

$$|Gx| = (G : G_x) = \frac{|G|}{|G_x|}.$$

Beweis. Die Abbildung φ ist wohldefiniert: aus $gG_x = hG_x$ folgt $g^{-1}h \in G_x$, also $gx = g(g^{-1}hx) = hx$. Sie ist injektiv, weil aus $gx = hx$ folgt $g^{-1}hx = x$, also $g^{-1}h \in G_x$ und deshalb $gG_x = hG_x$. Sie ist surjektiv nach Konstruktion. Wir überlassen es dem Leser zu zeigen, dass die Abbildung G-invariant ist. □

Für die Konjugationsoperation von G auf sich selbst und einer Untergruppe H von G erhält man das folgende Resultat.

Korollar 2.7.2. *Die Anzahl der Konjugierten gHg^{-1} einer Untergruppe H von G ist durch $(G : N_G(H))$ gegeben.*

Da X die disjunkte Vereinigung seiner G-Bahnen ist, folgt aus $|Gx| = (G : G_x)$ die *Bahnengleichung*:

Korollar 2.7.3 (Bahnengleichung)**.** *Ist $(x_i)_{i\in I}$ ein Vertretersystem für die G-Bahnen in X, so gilt*

$$|X| = \sum_{i\in I} (G : G_{x_i}).$$

Die Bahnengleichung wird zur *Klassengleichung* für die Konjugationsoperation.

Satz 2.7.4 (Klassengleichung)**.**

$$\begin{aligned} |G| &= \sum_{x\in\mathcal{C}} (G : C_G(x)) \\ &= |Z(G)| + \sum_{y\in\mathcal{C}'} (G : C_G(y)), \end{aligned}$$

wobei x ein Vertretersystem $\mathcal{C}$ für die Konjugationsklassen durchläuft, und y ein Vertretersystem $\mathcal{C}'$ für die Konjugationsklassen mit mehr als einem Element.

Man beachte, dass jeder Summand ein Teiler von $|G|$ ist, also jede Konjugationsklasse eine Ordung hat, die ein Teiler von $|G|$ ist. Das folgt nicht aus Lagrange, da Konjugationsklassen keine Untergruppen sein müssen.

Die folgende Tabelle zeigt die Konjugationsklassen in S_4. Sie sind durch den Zykeltyp bestimmt.

Zykeltyp	Elemente
1	(1)
(ab)	$(12), (13), (14), (23), (24), (34)$
(abc)	$(123), (132), (124), (142), (134), (143), (234), (243)$
$(ab)(cd)$	$(12)(34), (13)(24), (14)(23)$
$(abcd)$	$(1234), (1432), (1324), (1423), (1243), (1342)$

Beispiel 2.7.5. *Die Klassengleichung für S_4 lautet*

$$|S_4| = 24 = 1 + 6 + 8 + 3 + 6.$$

Wir haben $Z(S_4) = 1$.

Die Klassengleichung hat einige wichtige Konsequenzen. Zunächst wollen wir die Klassifikation endlicher abelscher Gruppen aus der elementaren Zahlentheorie in Erinnerung rufen.

Theorem 2.7.6. *Sei A eine endliche abelsche Gruppe. Dann gibt es ein $k \in \mathbb{N}$, Primzahlen $p_1, \ldots, p_k$ und positive ganze Zahlen $n_1, \ldots, n_k$ mit*

$$A \cong \prod_{j=1}^{k} \mathbb{Z}/p_j^{n_j}\mathbb{Z}.$$

Dabei sind k und die Paare (p_j, n_j) bis auf Reihenfolge eindeutig durch A bestimmt.

Korollar 2.7.7. *Sei A eine endliche abelsche Gruppe und p eine Primzahl, die $|A|$ teilt. Dann besitzt A ein Element der Ordnung p.*

Beweis. Wegen $|A| = \prod_{j=1}^{k} p_j^{n_j}$ bedeutet $p \mid |A|$, dass $p = p_i$ für ein i. Also hat A eine Untergruppe, die isomorph zu einer zyklischen Gruppe $\mathbb{Z}/p^n\mathbb{Z}$ ist. Ihr Erzeuger g hat Ordnung p^n. Dann hat das Element $g^{p^{n-1}}$ die Ordung p, denn $\operatorname{ord}(g^k) = \frac{n}{\gcd(k,n)}$ in einer zyklischen Gruppe der Ordung n. □

Nun folgt mit Hilfe der Klassengleichung eine Verallgemeinerung, die als der Satz von Cauchy bekannt ist.

Satz 2.7.8 (Cauchy)**.** *Sei G eine endliche Gruppe und p eine Primzahl, die $|G|$ teilt. Dann besitzt G ein Element der Ordnung p.*

Beweis. Wir machen eine Induktion über $|G|$. Angenommen, es gibt ein Element $y \in G \setminus Z(G)$ mit $p \nmid (G : C_G(y))$. Dann folgt $p \mid |C_G(y)|$ wegen

$$(G : 1) = (G : C_G(y)) \cdot (C_G(y) : 1).$$

Nach Induktionsannahme gibt es ein Element der Ordung p in $C_G(y)$, und somit auch in G. Also dürfen wir annehmen, dass p *alle* Terme $(G : C_G(y))$ in der Klassengleichung für nicht-zentrale Elemente y teilt. Aber dann haben wir $p \mid |Z(G)|$. Da $Z(G)$ abelsch ist, gibt es wegen Korollar 2.7.7 ein Element der Ordnung p in $Z(G) \subseteq G$. □

Der Satz von Cauchy ist sehr nützlich für die Strukturtheorie endlicher Gruppen.

Satz 2.7.9. *Jede Gruppe der Ordnung $2p$ für eine Primzahl $p > 2$ ist isomorph zu C_{2p} oder D_p.*

Beweis. Nach Cauchy's Theorem gibt es für jeden Primteiler p von $|G|$ ein Element der Ordung p in G. Wegen $|G| = 2p$ und $p > 2$ können wir das für 2 und p anwenden. Sei s also ein Element der Ordnung 2, und r ein Element der Ordnung p. Dann ist $C_p = \langle r \rangle$ ein Normalteiler von G wegen $(G : C_p) = 2$, siehe Lemma 2.3.10. Offensichtlich gilt $s \notin C_p$, so dass $G = C_p \cup C_p s$. Das bedeutet $G = \{1, r, \ldots, r^{p-1}, s, rs, \ldots, r^{p-1}s\}$. Da C_p normal ist gilt $srs^{-1} = r^k$ für ein $k \in \mathbb{Z}$. Wegen $s^2 = e$ haben wir

$$r = s^2 r s^{-2} = s(srs^{-1})s^{-1} = r^{k^2}.$$

Das bedeutet $k^2 \equiv 1 \mod p$, also $p \mid (k-1)(k+1)$. Es folgt also entweder $k \equiv 1 \mod p$ oder $k \equiv -1 \mod p$. In ersten Fall ist G abelsch (jede Gruppe, die durch kommutierende Elemente erzeugt wird, ist kommutativ), d.h., $G = \langle r, s \mid r^p = s^2 = e, rs = sr \rangle \cong C_{2p}$. Im zweiten Fall haben wir $srs^{-1} = r^{-1}$, so dass $G \cong D_p$. □

Definition 2.24. Eine endliche Gruppe G heißt *p-Gruppe*, falls sie Primzahlpotenzordnung hat, d.h., falls $|G| = p^m$.

Satz 2.7.10. *Eine endliche Gruppe G ist genau dann eine p-Gruppe falls jedes Element eine p-Potenz Ordung hat.*

Beweis. Ist $|G| = p^m$, dann hat wegen des Satzes von Lagrange jedes Element eine Ordnung, die p^m teilt, also eine p-Potenz ist. Für die Umkehrung nehmen wir an, es gäbe eine Primzahl $q \neq p$ mit $q \mid |G|$. Dann gäbe es ein Element $g \in G$ mit $\mathrm{ord}(g) = q \neq p^k$ wegen Cauchys Theorem. Das ist ein Widerspruch zur Voraussetzung. Also gilt $|G| = p^m$ für ein $m \in \mathbb{N}$. □

Satz 2.7.11. *Sei G eine nicht-triviale endliche p-Gruppe. Dann ist $Z(G)$ nicht-trivial.*

Beweis. Nach Voraussetzung ist $(G : 1)$ eine p-Potenz. Also sind alle Terme über $y \in \mathcal{C}'$ in der Klassengleichung durch p teilbar. Das bedeutet $p \mid |Z(G)|$. □

Satz 2.7.12. *Eine Gruppe der Ordnung p^n hat Normalteiler von jeder möglichen Ordnung $1, p, \ldots, p^n$.*

Beweis. Wir machen eine Induktion über n. Wegen Korollar 2.7.7 besitzt $Z(G)$ ein Element g der Ordnung p. Also ist $N = \langle g \rangle$ ein Normalteiler der Ordnung p. Es gilt $|G/N| = p^{n-1}$, und wir können die Induktionsvoraussetzung anwenden. Da die Normalteiler von G/N zu den Normalteilern von G, die N enthalten korrespondieren, folgt die Behauptung für G. □

Lemma 2.7.13. *Sei H eine Untergruppe von G mit $H \subseteq Z(G)$, so dass G/H zyklisch ist. Dann ist G abelsch.*

Beweis. Sei a ein Element in G, dessen Bild in G/H ein Erzeuger ist. Dann kann man jedes Element von G schreiben als $g = a^j h$ mit $h \in H$ und $j \in \mathbb{Z}$. Wegen $H \subseteq Z(G)$ haben wir

$$\begin{aligned} a^i h \cdot a^j h' &= a^i a^j h h' \\ &= a^j a^i h' h \\ &= a^j h' \cdot a^i h. \end{aligned}$$

□

Satz 2.7.14. *Jede Gruppe der Ordnung p^2 mit einer Primzahl p ist abelsch und deshalb isomorph zu $C_p \times C_p$ oder C_{p^2}.*

Beweis. Wegen Lagrange gilt $|Z(G)| \in \{1, p, p^2\}$ und wegen Satz 2.7.11 können wir Ordnung 1 ausschliessen, d.h., $|G/Z(G)| \in \{1, p\}$. In beiden Fällen ist $G/Z(G)$ zyklisch, so dass G abelsch ist wegen Lemma 2.7.13. □

Gruppen der Ordnung p^3 müssen nicht notwenig abelsch sein, wie wir in Satz 2.5.6 für $p = 2$ gesehen haben. Zusammen mit Lemma 2.5.5, oder mit Theorem 2.7.6 haben wir folgende Klassifikation.

Satz 2.7.15. *Jede Gruppe G der Ordnung 2^3 ist isomorph zu einer der Gruppen $C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$ oder D_4, Q_8.*

Auch für $p > 2$ gibt es nicht-abelsche Gruppen der Ordnung p^3. Die *Heisenberggruppe* über $\mathbb{Z}/(p)$ ist definiert durch

$$\mathrm{Heis}(\mathbb{Z}/(p)) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z}/(p) \right\}.$$

Sie ist offensichtlich nicht-abelsch und hat die Ordnung p^3. Für $p = 2$ erhält man $\mathrm{Heis}(\mathbb{Z}/(2)) \cong D_4$. Für $p > 2$ haben alle nicht-trivialen Elemente in $\mathrm{Heis}(\mathbb{Z}/(p))$ die Ordnung p, da

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & 0 & \frac{p(p-1)}{2}ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I,$$

weil $\frac{p(p-1)}{2} \equiv 0 \bmod p$ für alle $p > 2$. Eine weitere nicht-abelsche Gruppe der Ordnung p^3 ist wie folgt gegeben. Sei

$$\mathrm{Aff}(\mathbb{Z}/(p^2)) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{Z}/(p^2), a \neq 0 \right\} \subseteq GL_2(\mathbb{Z}/(p^2))$$

die *affine Gruppe* über $\mathbb{Z}/(p^2)$. Sie hat die Ordnung $p^2\varphi(p^2) = p^3(p-1)$ und besitzt einen eindeutigen Normalteiler $\Gamma(p)$ der Ordnung p^3, gegeben durch

$$\Gamma(p) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{Z}/(p^2), a^p = 1 \text{ in } (\mathbb{Z}/(p^2))^\times \right\}.$$

Er ist der Kern des Homomorphismus $\mathrm{Aff}(\mathbb{Z}/(p^2)) \to (\mathbb{Z}/(p^2))^\times$ gegeben durch

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mapsto a^p,$$

und hat ein Element der Ordnung p^2, nämlich $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Deshalb sind $\Gamma(p)$ und $\mathrm{Heis}(\mathbb{Z}/(2))$ für $p > 2$ nicht isomorph. Für $p = 2$ sind sie allerdings beide isomorph zu D_4.

Theorem 2.7.16 (Hölder 1893)**.** *Jede Gruppe der Ordnung p^3 für eine Primzahl $p > 2$ ist isomorph zu einer der Gruppen $C_p \times C_p \times C_p$, $C_p \times C_{p^2}$, C_{p^3},* Heis$(\mathbb{Z}/p)$ *oder* $\Gamma(p)$.

2.8 Die Sylowsätze

Definition 2.25. Sei G eine endliche Gruppe und p ein Primteiler von $|G|$. Eine Untergruppe von G heißt *p-Sylowgruppe* von G falls ihre Ordnung die höchste p-Potenz ist, die $|G|$ teilt.

Eine p-Sylowgruppe ist also eine maximale p-Untergruppe von G. Für $p \nmid |G|$ ist offenbar die triviale Gruppe eine p-Sylowgruppe von G.

Beispiel 2.8.1. *1. $P = \{(1), (123), (132)\}$ ist eine 3-Sylowgruppe von S_4.*

2. $P = \{(1), (1234), (13)(24), (1432), (24), (14)(23), (13), (12)(34)\}$ ist eine 2-Sylowgruppe von S_4. Sie ist isomorph zu D_4.

Hier haben wir $|S_4| = 24 = 2^3 \cdot 3$, und $r = (1234)$, $s = (24)$ für D_4.

Für die Sylowsätze benötigen wir folgendes Lemma.

Lemma 2.8.2. *Sei H eine p-Gruppe, die auf einer endlichen Menge X operiert und sei X^H die Menge der Punkte, die von H fixiert wird, d.h.*

$$X^H = \{x \in X \mid hx = x \; \forall \, h \in H\}.$$

Dann gilt

$$|X| \equiv |X^H| \bmod p.$$

Insbesondere folgt

$$|H| \equiv |Z(H)| \bmod p.$$

Beweis. Es gilt $(H : \mathrm{Stab}(x_0)) = |Hx_0|$ wegen Theorem 2.7.1. Da H eine p-Gruppe ist, muss dieser Index eine p-Potenz sein. Also besteht Hx_0 entweder nur aus einem Element, oder $|Hx_0|$ ist durch p teilbar. Da X die disjunkte Vereinigung seiner Bahnen ist, folgt die erste Behauptung. Wendet man diese auf die Konjugationsoperation an, so erhält man die zweite Behauptung. □

Theorem 2.8.3 (Sylow I)**.** *Sei G eine endliche Gruppe und p eine Primzahl. Gilt $p^r \mid |G|$ für ein $r \geq 1$, dann hat G eine Untergruppe der Ordnung p^r.*

Beweis. Wegen Satz 2.7.12 genügt es die Aussage für den Fall zu beweisen, wo $p^r \mid\mid |G|$ die höchste p-Potenz ist, die $|G|$ teilt. Denn wenn G eine Untergruppe der Ordnung p^r hat, so hat sie auch Untergruppen aller möglichen kleineren Ordnungen $1, p, p^2, \ldots, p^r$. Wir können also annehmen, dass $|G| = p^r m$ mit $p \nmid m$ ist. Sei

$$X = \{S \subseteq G \mid |S| = p^r\}.$$

Definiere eine G-Operation auf X durch

$$(g, A) \mapsto gA = \{ga \mid a \in A\}.$$

Sei $A \in X$, i.e., $A = \{g_1, \ldots, g_{p^r}\}$ und sei

$$H = \mathrm{Stab}(A) = \{g \in G \mid gA = A\}.$$

Für jedes $g_i \in A$ ist die Abbildung $h \mapsto hg_i$, $H \to A$ injektiv wegen des Kürzungsgesetzes, und so gilt

$$(H : 1) \leq |A| = p^r.$$

In der Gleichung

$$(G : 1) = (G : H)(H : 1)$$

ist $(G : 1) = p^r m$ mit $p \nmid m$ und $(H : 1) = p^k$ mit $k \leq r$, und $(G : H)$ ist die Anzahl der Elemente in dem Orbit von A. Also genügt es, eine *einzige* Menge A zu finden, für die p nicht die Anzahl der Elemente in ihrer Bahn teilt. Denn dann können wir, für dieses spezielle A, schliessen, dass die Untergruppe $H = \mathrm{Stab}(A)$ Ordnung p^r hat, und wir sind fertig. Die Anzahl der Elemente in X ist

$$|X| = \binom{p^r m}{p^r} = \frac{(p^r m)(p^r m - 1) \cdots (p^r m - i) \cdots (p^r m - p^r + 1)}{p^r (p^r - 1) \cdots (p^r - i) \cdots (p^r - p^r + 1)}.$$

Wegen $i < p^r$ ist die p-Potenz, die $p^r m - i$ teilt gleich der p-Potenz, die i teilt. Das gleiche gilt für $p^r - i$. Also sind die entsprechenden Terme über und unter dem Bruchstrich durch die gleiche p-Potenz teilbar, so dass p *kein Teiler* von $|X|$ ist. Da die Bahnen eine Partition von X bilden, muss mindestens eine Bahn (für eine Menge A) nicht durch p teilbar sein. Das zeigt die Behauptung. □

Korollar 2.8.4. *Für p-Gruppen gilt die Umkehrung des Theorems von Lagrange. Für jeden Teiler $d \mid |G|$ gibt es eine Untergruppe der Ordnung d.*

Im allgemeinen gilt die Umkehrung von Lagrange nicht. Die Gruppe A_4 hat Ordnung 12, und $d = 6$ ist ein Teiler von 12. Es gibt aber keine Untergruppe der Ordnung 6 von A_4:

Beispiel 2.8.5. *Die Untergruppen von A_4 sind wie folgt gegeben:*

Ordnung	#	*Untergruppen*
1	1	$\{(1)\}$
2	3	$\{(1),(12)(34)\}$, $\{(1),(13)(24)\}$, $\{(1),(14)(23)\}$
3	4	$\{(1),(123),(132)\}$, $\{(1),(243),(234)\}$, $\{(1),(142),(124)\}$, $\{(1),(134),(143)\}$
4	1	$\{(1),(12)(34),(13)(24),(14)(23)\}$
12	1	$\{(1),(12)(34),(13)(24),(14)(23),(123),(243),(142),(134),(132),(143),(234),(124)\}$

Nach Sylow I gibt es Untergruppen der Ordnung 2, 2^2, und 3. Die Gruppe der Ordnung 4 ist die eindeutige 2-Sylowgruppe von A_4, und die vier Gruppen der Ordnung 3 sind die 3-Sylowgruppen von A_4.

Bemerkung 2.8.6. Sylow I impliziert den Satz von Cauchy. Gilt $p \mid |G|$, so hat G eine Untergruppe H der Ordnung p. Dann hat jedes Element $h \in H$ außer e die Ordnung p.

Lemma 2.8.7. *Sei P eine p-Sylowgruppe von G und H eine p-Untergruppe. Falls H die p-Sylowgruppe P normalisiert, d.h., falls $H \subseteq N_G(P)$ gilt, dann folgt $H \subseteq P$. Insbesondere normalisiert P keine andere p-Sylowgruppe von G ausser sich selbst.*

Beweis. Da H und P Untergruppen von $N_G(P)$ sind, und P normal in $N_G(P)$, ist HP eine Untergruppe. Der zweite Isomorphiesatz gibt

$$H/H \cap P \cong HP/P.$$

Daher ist $(HP : P)$ eine p-Potenz, denn $(H : 1)$ ist eine p-Potenz nach Voraussetzung. Wir haben aber

$$(HP : 1) = (HP : P)(P : 1),$$

und $(P : 1)$ ist die größte p-Potenz, die $(G : 1)$ teilt, also auch die größte p-Potenz, die $(HP : 1)$ teilt. Also gilt $(HP : P) = p^0 = 1$ und $H \subseteq P$. □

Theorem 2.8.8 (Sylow II)**.** *Je zwei p-Sylowgruppen von G sind konjugiert, also isomorph.*

Beweis. Sei X die Menge der p-Sylowgruppen in G, und operiere G auf X durch Konjugation, d.h., durch

$$(g, P) \mapsto gPg^{-1}.$$

Sei O eine der G-Bahnen. Wir wollen $O = X$ zeigen. Sei $P \in O$ und P operiere durch die Aktion von G. Die G-Bahn O spaltet sich unter dieser Operation auf in mehrere P-Bahnen, wovon eine P sein wird. Das muss auch die *einzige* einelementige Bahn sein, da $\{Q\}$ genau dann eine P-Bahn ist, wenn P das Q normalisiert. Das passiert wegen Lemma 2.8.7 aber nur für $Q = P$. Also ist die Anzahl der Elemente in jeder P-Bahn, die verschieden von $\{P\}$ ist, durch p teilbar und wir haben

$$|O| \equiv 1 \bmod p.$$

Angenommen es gibt eine p-Sylowgruppe P, die nicht in X liegt. Dann zeigt das vorangegangene Argument, dass die Anzahl der Elemente in jeder P-Bahn durch p teilbar ist, da es keine einelementigen Bahnen gibt in diesem Fall. Also erhalten wir $|O| \equiv 0 \bmod p$, einen Widerspruch. Also gibt es kein P mit $P \notin O$, und es folgt $O = X$. □

Theorem 2.8.9 (Sylow III)**.** *Sei s_p die Anzahl der p-Sylowgruppen in G und sei $|G| = p^r m$ mit $p \nmid m$. Dann gilt $s_p \mid m$, und $s_p = (G : N_G(P))$ für jede p-Sylowgruppe P of G. Wir haben*

$$s_p \equiv 1 \bmod p.$$

Beweis. Im Beweis von Sylow II haben wir schon gezeigt, dass $s_p = |O| \equiv 1 \bmod p$. Sei P eine p-Sylowgruppe von G. In Korollar 2.7.2 haben wir gezeigt, dass die Anzahl der Konjugierten von P durch $(G : N_G(H))$ gegeben

ist. Aber das ist gerade s_p. Weiterhin gilt

$$\begin{aligned}(G : N_G(P)) &= \frac{(G:1)}{(N_G(P):1)} \\ &= \frac{(G:1)}{(N_G(P):P)(P:1)} \\ &= \frac{m}{(N_G(P):P)},\end{aligned}$$

welches ein Faktor von m ist. Also hat man $s_p \mid m$. □

Korollar 2.8.10. *Jede p-Untergruppe von G ist in einer p-Sylowgruppe enthalten.*

Beweis. Sei H eine p-Untergruppe von G und operiere H auf der Menge X der p-Sylowgruppen von G durch Konjugation. Da $|X| = s_p$ nicht durch p teilbar ist wegen Sylow III, muss X^H nicht-leer sein wegen Lemma 2.8.2. Das bedeutet, es gibt mindestens eine H-Bahn, die aus einer einzigen p-Sylowgruppe besteht. Aber dann normalisiert H die Gruppe P und Lemma 2.8.7 impliziert $H \subseteq P$. □

Korollar 2.8.11. *Eine p-Sylowgruppe von G ist genau dann normal, wenn sie die einzige p-Sylowgruppe ist.*

Beweis. Angenommen, P ist normal. Dann ist P wegen Sylow II die einzige p-Sylowgruppe, denn jede andere p-Sylowgruppe Q erfüllt $Q = gPg^{-1} = P$. Umgekeht sei $s_p = 1$. Dann ist $gPg^{-1} = P$, so dass P normal ist. □

Korollar 2.8.12. *Angenommen G hat nur eine einzige p-Sylowgruppe für jede Primzahl p mit $p \mid |G|$. Dann ist G das direkte Produkt seiner p-Sylowgruppen.*

Beweis. Es seien $P_1, \ldots, P_k$ die Sylowgruppen von G. Es gilt $|P_i| = p_i^{r_i}$ mit verschiedenen Primzahlen p_i, die $|G|$ teilen. Wegen Korollar 2.8.11 ist jedes P_i normal in G, so dass das Produkt $P_1 \cdots P_k$ ebenfalls normal in G ist. Mit Induktion über k folgt nun, dass $|P_1 \cdots P_k| = p_1^{r_1} \cdots p_k^{r_k}$ gilt. Für $k = 1$ gibt es nichts zu zeigen, so dass wir $k \geq 2$ und $|P_1 \cdots P_{k-1}| = p_1^{r_1} \cdots p_{k-1}^{r_{k-1}}$ annehmen können. Dann ist $P_1 \cdots P_{k-1} \cap P_k = 1$, so dass $(P_1 \cdots P_{k-1})P_k$ das direkte Product von $P_1 \cdots P_{k-1}$ und P_k ist, und daher Ordnung $p_1^{r_1} \cdots p_k^{r_k}$

hat. Nun ist G das direkte Produkt seiner p-Sylowgruppen, da G das Produkt von ihnen ist, jede davon normal in G ist, und alle Schnitte $P_j \cap (P_1 \cdots P_{j-1} P_{j+1} \cdots P_k)$ trivial sind. □

Dieses Korollar kann man anwenden, um zu zeigen, dass Gruppen gewisser Ordnung abelsch sind.

Beispiel 2.8.13. *Jede Gruppe G der Ordnung 99 ist kommutativ.*

Wir haben $99 = 3^2 \cdot 11$ und $s_{11} \mid 9$, $s_{11} \equiv 1 \bmod 11$. Das bedeutet $s_{11} = 1$. Also gibt es genau eine 11-Sylowgruppe H in G, und sie ist normal in G. Ebenso gilt $s_3 \mid 11$ und $s_3 \equiv 1 \bmod 3$, also $s_3 = 1$. Also gibt es genau eine 3-Sylowgruppe K in G, und sie ist normal in G. Aus Korollar 2.8.12 folgt $G = H \times K$, wo H und K kommutativ sind. Also ist G abeslch.

Bemerkung 2.8.14. Das gleiche Argument zeigt, dass jede Gruppe der Ordnung p^2q mit Primzahlen $p < q$ und $q \not\equiv 1 \bmod p$ kommutativ ist.

Definition 2.26. Eine nicht-triviale Gruppe G heißt *einfach*, falls sie als Normalteiler nur G und die triviale Gruppe $1 = \{e\}$ mit dem neutralen Element e hat.

Gruppen der Ordnung p^n mit $n \geq 2$ sind nicht einfach wegen Satz 2.7.12. Für $n = 1$ sind sie einfach, wegen Lagrange. Die Gruppe $\mathbb{Z}$ ist nicht einfach, da $2\mathbb{Z}$ ein echter Normalteiler ist. Die Gruppe $GL_2(\mathbb{R})$ ist nicht einfach, da $SL_2(\mathbb{R})$ ein echter Normalteiler ist.
Man kann leicht zeigen, dass eine kommutative Gruppe genau dann einfach ist, wenn sie Primzahlordnung hat, also isomorph zu einer zyklischen Gruppe C_p ist. Die kleinste nicht-abelsche einfache Gruppe ist A_5, die Ordnung 60 hat.

Bemerkung 2.8.15. Ein großes Projekt in der Mathematik des 20. Jahrhunderts war die Klassifikation der *endlichen* einfachen (nicht-abelschen) Gruppen. Um die 100 Mathematiker haben hierzu Beiträge geleistet, die zusammmen über 10000 Seiten füllen. Die Klassifikation ist inzwischen abgeschlossen, die letzten Lücken wurden 2004 geschlossen:

Es gibt 18 unendliche *Serien* von einfachen Gruppen, nämlich die zyklischen Gruppen C_p mit $p \in \mathbb{P}$, die alternierenden Gruppen A_n mit $n \geq 5$, und 16 Serien vom Lie-Typ, die komplizierter zu beschreiben sind. Hinzu kommen

26 sogenannte *sporadische* Gruppen, die in keine dieser Serien passen. Die kleinste dieser sporadischen Gruppen hat Ordnung 7920, die größte wird das *Monster* genannt und hat die Ordnung

$$\begin{aligned}|M| &= 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \\ &\simeq 8 \cdot 10^{53}.\end{aligned}$$

Lemma 2.8.16. *Sei G eine endliche Gruppe und p die kleinste Primzahl, die $|G|$ teilt. Dann ist jede Untergruppe H vom Index p normal in G.*

Beweis. Sei H eine Untergruppe von G mit $(G : H) = p$. G operiere auf der Menge der Linksnebenklassen G/H durch Linksmultiplikation. Diese Aktion ist nicht-trivial, und induziert daher einen nicht-trivialen Gruppenhomomorphismus

$$\theta : G \to \mathrm{Sym}(G/H) = S_p.$$

Da die Aktion transitiv ist, ist $\ker(\theta)$ der größte Normalteiler N von G, der in H enthalten ist. Angenommen, $N \neq H$. Es gilt

$$(G : N) = (G : H)(H : N) = p(H : N).$$

Da wir $(H : N) > 1$ annehmen, existiert eine Primzahl q, die diesen Index teilt. Da p die kleinste Primzahl ist, die $|G|$ teilt, haben wir $p \leq q$. Also gilt

$$pq \mid (G : N) = \frac{|G|}{|N|} = |\mathrm{im}(\theta)| \mid p! = |S_p|.$$

Aber $pq \mid p!$ ist unmögich für $q \geq p$, Widerspruch. Also ist $N = H$, und das ist ein Normalteiler von G. □

Wir können dieses Lemma zusammen mit den Sylowsätzen anwenden, um zu zeigen, daß Gruppen von gewisser Ordnung nicht einfach sein können.

Satz 2.8.17. *Sei G eine Gruppe der Ordung pq^r für Primzahlen $p < q$ mit $r \geq 1$. Dann ist G nicht einfach.*

Beweis. Sei H eine q-Sylowgruppe von G. Wegen Lemma 2.8.16 ist H normal. es gilt $|H| = q^r$, also ist H ein echter Normalteiler. □

Wir erwähnen noch ein berühmtes Resultat von Burnside.

Theorem 2.8.18 (Burnside 1901)**.** *Sei G eine Gruppe der Ordnung $p^r q^s$ für Primzahlen $p < q$ und $r, s \geq 1$. Dann ist G nicht einfach.*

Dieser Satz kann nicht auf Gruppenordnungen mit drei verschiedenen Primzahlen verallgemeinert werden, da $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$, und A_5 einfach ist.

Wir wollen nun noch zeigen, dass nicht nur Gruppen von Primzahlordnung zyklisch sind, sondern auch solche der Ordnung pq mit zwei verschiedenen Primzahlen $p < q$, sofern p nicht $q - 1$ teilt. Dazu benötigen wir zuerst das folgende Lemma.

Lemma 2.8.19. *Sind p und q zwei verschiedene Primteiler von $|G|$ mit $s_p = s_q = 1$, dann kommutieren die Elemente der p-Sylowgruppe mit den Elementen der q-Sylowgruppe.*

Beweis. Sei P die p-Sylowgruppe und Q die q-Sylowgruppe von G. Da die Ordnungen von P und Q relativ prim sind, folgt $P \cap Q = 1$ wegen Lagrange. Die Untergruppen P und Q sind normal in G wegen Korollar 2.8.11. Für $a \in P$ und $b \in Q$ gilt

$$aba^{-1}b^{-1} = (aba^{-1})b^{-1} = a(ba^{-1}b^{-1}) \in P \cap Q = 1,$$

so dass $ab = ba$. □

Satz 2.8.20. *Sei G eine Gruppe der Ordnung pq mit Primzahlen $p < q$ und $q \not\equiv 1 \bmod p$. Dann ist G zyklisch.*

Beweis. Wegen Cauchys Theorem hat G ein Element a der Ordnung p und ein Element b der Ordnung q. Sei $P = \langle a \rangle$ und $Q = \langle b \rangle$. Diese Untergruppen haben Ordnung p und q, und P ist eine p-Sylowgruppe, Q ist eine q-Sylowgruppe. Wegen Sylow III gilt $s_p \mid q$ und $s_p \equiv 1 \bmod p$. Wegen $q \not\equiv 1 \bmod p$ muss $s_p = 1$ gelten, so dass P normal in G ist. Ebenso folgt $s_q \mid p$ und $s_q \equiv 1 \bmod q$. Wegen $1 < p < q$ und $q \not\equiv 1 \bmod p$ muss auch $s_q = 1$ gelten. Daher ist Q normal in G. Nun können wir Lemma 2.8.19 anwenden, um zu zeigen, dass die Elemente von P mit den Elementen von Q kommutieren. Insbesondere kommutieren die Erzeuger a und b, d.h., $ab = ba$, und $\mathrm{ord}(a)$, $\mathrm{ord}(b)$ sind teilerfremd. Deshalb gilt $\mathrm{ord}(ab) = pq$, und ab erzeugt G. □

Zum Beispiel ist $f(n) = 1$ für $n = 15, 33, 35, 51, 65, 69, 77, 85, 87, 91, 95$ mit $n = pq$ und

$$\begin{aligned}(p, q) &= (3, 5), (3, 11), (5, 7), (3, 17), (5, 13), (3, 23), (7, 11), \\ &= (5, 17), (3, 29), (7, 13), (5, 19).\end{aligned}$$

Das sind alle Beispiele dieser Art für $n < 100$.

Bemerkung 2.8.21. Es gilt $f(n) = 1$ genau dann wenn $\gcd(n, \varphi(n)) = 1$ ist. Das wurde 1947 von von Tibor Szele bewiesen, in der Arbeit *Über die endichen Ordnungszahlen, zu denen nur eine Gruppe gehört*, siehe [8].

2.9 Semidirekte Produkte

Das *semidirekte* Produkt zweier Gruppen N und Q ist eine Verallgemeinerung des direkten Produktes $N \times Q$, unter Verwendung eines Gruppenhomomorphismus $\theta\colon Q \to \mathrm{Aut}(N)$.
Dazu wollen wir zuerst nochmal an die Gruppe $\mathrm{Inn}(G)$ der inneren Automorphismen von G erinnern. Die Elemente sind von der Form i_g, gegeben durch $i_g(x) = gxg^{-1}$.

Lemma 2.9.1. *Sei G eine Gruppe. Dann gilt $G/Z(G) \cong \mathrm{Inn}(G)$.*

Beweis. Die Abbildung $\varphi\colon G \to \mathrm{Aut}(G)$, $g \mapsto i_g$ ist ein Gruppenhomomorphismus mit Kern $Z(G)$. Nach Korollar 2.3.14 gilt $G/\ker(\varphi) \cong \mathrm{im}(\varphi)$. □

Beispiel 2.9.2. *Für die Quaternionengruppe Q_8 gilt $\mathrm{Inn}(Q_8) \cong C_2 \times C_2$.*

In der Tat, wegen $Z(Q_8) = \{\pm 1\}$ gilt $\mathrm{Inn}(Q_8) \cong Q_8/\{\pm 1\} \cong C_2 \times C_2$. Man kann zeigen, dass $\mathrm{Aut}(Q_8) \cong S_4$ gilt.

Lemma 2.9.3. *Die Untergruppe $\mathrm{Inn}(G)$ ist normal in $\mathrm{Aut}(G)$.*

Beweis. Sei $g \in G$ und $\alpha \in \mathrm{Aut}(G)$. Dann gilt

$$\begin{aligned}(\alpha \circ i_g \circ \alpha^{-1})(x) &= \alpha(g \cdot \alpha^{-1}(x) \cdot g^{-1}) \\ &= \alpha(g) \cdot x \cdot \alpha(g)^{-1} \\ &= i_{\alpha(g)}(x).\end{aligned}$$

□

Definition 2.27. Sei G eine Gruppe. Die Faktorgruppe

$$\mathrm{Out}(G) = \mathrm{Aut}(G)/Inn(G)$$

wird die *äußere Automorphismengruppe* von G genannt.

Ein wichtiges Problem ist, zu entscheiden wann die Gruppe $\mathrm{Out}(G)$ trivial ist.

Bemerkung 2.9.4. Es gilt $\mathrm{Out}(S_n) = 1$ für alle $n \geq 1$ mit $n \neq 6$.

Kommen wir jetzt zum semidirekten Produkt. Sei N ein Normalteiler von G. Jedes Element $g \in G$ definiert einen Automorphismus von N durch $n \mapsto gng^{-1}$, und das definiert einen Homomorphismus

$$\theta\colon G \to \mathrm{Aut}(N),\ g \mapsto i_{g|N}.$$

Angenommen, es existiert eine Untergruppe Q von G, so dass der kanonische Homomorphismus $\pi\colon G \to G/N$ die Gruppe Q isomorph auf G/N abbildet. Dann können wir G aus dem Tripel $(N, Q, \theta_{|Q})$ rekonstruieren. Jedes $g \in G$ kann nämlich eindeutig in der Form $g = nq$ mit $n \in N$ und $q \in Q$ geschrieben werden, wobei q das eindeutige Element von Q sein muss, dass auf $gN \in G/N$ abgebildet wird, und n gleich gq^{-1} sein muss. Also haben wir eine bijektive Korrespondenz der Mengen

$$G \leftrightarrow N \times Q.$$

Das Produkt zweier Elemente $g = nq$ und $g' = n'q'$ ist wie folgt gegeben,

$$\begin{aligned} gg' &= (nq)(n'q') \\ &= n(qn'q^{-1})qq' \\ &= n \cdot \theta(q)(n') \cdot qq'. \end{aligned}$$

Wir definieren nun das semidirekte Produkt genau nach dieser obigen Annahme.

Definition 2.28. Eine Gruppe G ist das *semidirekte Produkt* seiner Untergruppen N und Q, falls N ein Normalteiler ist und $G \to G/N$ einen Isomorphismus $Q \to G/N$ induziert. Wir schreiben dann $G = N \rtimes Q$.

Wir schreiben oft auch genauer $G = N \rtimes_\theta Q$, wobei $\theta\colon Q \to \mathrm{Aut}(N)$ die Operation von Q auf N durch innere Automorphismen ergibt. Man beachte, dass Q kein Normalteiler von G sein muss.

Bemerkung 2.9.5. Es ist leicht zu zeigen, dass G genau dann ein semidirektes Produkt seiner Untergruppen N und Q ist, falls N ein Normalteiler ist, $NQ = G$ und $N \cap Q = 1$ gilt.

Das semidirekte Produkt $N \rtimes_\theta Q$ wird wie folgt aus zwei Gruppen N und Q und einem Homomorphismus $\theta\colon Q \to \mathrm{Aut}(N)$ konstruiert. Es sei $G = N \times Q$ als Menge. Man definiere die Komposition in G durch

$$(n, q)(n', q') = (n \cdot \theta(q)(n'), qq'). \tag{2.1}$$

Satz 2.9.6. *Mit dieser Komposition ist G eine Gruppe, und es gilt $G \cong N \rtimes_\theta Q$.*

Beweis. Wir schreiben ${}^q n$ für $\theta(q)(n)$. Dann gilt

$$\begin{aligned}((n, q)(n', q'))(n'', q'') &= (n \cdot {}^q n' \cdot {}^{qq'} n'', qq'q'') \\ &= (n, q)((n', q')(n'', q'')).\end{aligned}$$

Also gilt das Assoziativgesetz in G. Wegen $\theta(1) = 1$ und ${}^q 1 = 1$ hat man

$$(1, 1)(n, q) = (n, q) = (n, q)(1, 1).$$

Also ist $(1, 1)$ das neutrale Element. Wegen

$$\begin{aligned}(n, q)({}^{q^{-1}} n^{-1}, q^{-1}) &= (1, 1) \\ &= ({}^{q^{-1}} n^{-1}, q^{-1})(n, q),\end{aligned}$$

ist $({}^{q^{-1}} n^{-1}, q^{-1})$ das inverse Element von (n, q). Also ist G eine Gruppe. Es ist nicht schwer zu sehen, dass N ein Normalteiler ist mit $QN = G$ und $N \cap Q = 1$. Also ist $G \cong N \rtimes Q$. betrachtet man N und Q als Untergruppen von G, dann ist die Operation von Q auf N durch θ gegeben. □

Beispiel 2.9.7. 1. *Für D_n mit $n \geq 2$ wählen wir $N = \langle r \rangle = C_n$, $Q = \langle s \rangle = C_2$ und $\theta(s)(r^i) = r^{-i}$, und erhalten*

$$D_n = N \rtimes_\theta Q = C_n \rtimes_\theta C_2.$$

2. *Es gilt $S_n = A_n \rtimes C_2$, da A_n ein Normalteiler vom Index 2 in S_n ist, so dass $Q = \{(12)\}$ isomorph auf S_n/A_n abgebildet wird.*

3. *Die Gruppe C_{p^2}, für p prim, ist kein semidirektes Produkt von nicht-trivialen Untergruppen, da sie nur eine Untergruppe der Ordnung p hat, und $C_p \times C_p$ nicht isomorph zu C_{p^2} ist.*

4. *Man kann auch zeigen, dass Q_8 nicht als semidirektes Produkt von zwei nicht-trivialen Untergruppen geschrieben werden kann.*

Beispiel 2.9.8. *Das direkte Produkt $N \times Q$ ist genau dann ismomorph zum semidirekten Produkt $N \rtimes_\theta Q$, wenn θ der triviale Homomorphismus $Q \to \mathrm{Aut}(N)$ ist, gegeben durch $\theta(q)(n) = n$ für alle $q \in Q, n \in N$.*

Beispiel 2.9.9. *Jede Gruppe der Ordnung 6 ist ein semidirektes Produkt, nämlich $C_6 \cong C_3 \times C_2$ und $S_3 \cong C_3 \rtimes_\theta C_2$.*

Es gibt nämlich nur zwei Homomorphismen $\theta\colon C_2 \to \mathrm{Aut}(C_3) \cong C_2$. Der triviale Homomorphismus ergibt das direkte Produkt $C_3 \times C_2$, und der andere ergibt $C_3 \rtimes_\theta C_2$. Den hatten wir schon im Beispiel 2.9.7 für D_3 gesehen, und es gilt $D_3 \cong S_3$.

2.10 Auflösbare und nilpotente Gruppen

Auflösbare Gruppen spielen bei der Auflösung (daher der Name!) von polynomialen Gleichungen

$$X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 = 0$$

durch Radikale eine zentrale Rolle.

Definition 2.29. Sei G eine Gruppe. Eine Kette von absteigenden Untergruppen

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_i \supseteq G_{i+1} \supseteq \cdots \supseteq G_n = 1$$

heißt *Subnormalreihe*, wenn G_i normal in G_{i-1} ist für jedes i. Ist zusätzlich G_i normal in G für alle i, dann heißt sie *Normalreihe* von G.

Die Quotientengruppen G_i/G_{i+1} heißen *Faktoren* der Reihe, und die *Länge* der Reihe ist die Anzahl der strkten Inklusionen. Wir schreiben auch

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_i \triangleright G_{i+1} \triangleright \cdots \triangleright G_n = 1$$

für eine Subnormalreihe, oder

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_j \triangleleft G_{j+1} \triangleleft \cdots \triangleleft G_n = G.$$

als aufsteigende Reihe.

Definition 2.30. Eine Subnormalreihe von G heißt *Kompositionsreihe*, wenn alle Quotienten nicht-trivial und einfach sind.

Mit anderen Worten, eine Subnormalreihe ist eine Kompositionsreihe, falls sie keine echte *Verfeinerung* hat, die auch eine Subnormalreihe ist. Verfeinerung bedeutet hier, dass jede Untergruppe der ersten Reihe auch als Term in der zweiten (verfeinerten) Reihe vorkommt. Jede endliche Gruppe besitzt eine Kompositionsreihe.

Beispiel 2.10.1. *Die symmetrische Gruppe S_3 hat eine Kompositionsreihe*

$$S_3 \triangleright A_3 \triangleright 1$$

mit einfachen Faktoren C_2 und C_3.

Definition 2.31. Eine Gruppe G heißt *auflösbar*, falls sie eine Subnormalreihe mit abelschen Faktorgruppen hat.

In diesem Fall nennt man diese Reihe auch *auflösbare Reihe*. Zum Beispiel ist die Gruppe S_3 auflösbar, siehe oben.

Beispiel 2.10.2. *Jede abelsche Gruppe ist auflösbar.*

Beispiel 2.10.3. *Die Gruppe S_4 hat eine Kompositionsreihe*

$$S_4 \triangleright A_4 \triangleright V_4 \triangleright \langle (12)(34) \rangle \triangleright 1,$$

wobei $V_4 \cong C_2 \times C_2$ aus $\{(1), (12)(34), (13)(24), (14)(23)\}$ besteht. Die Faktoren sind C_2, C_3, C_2, C_2, also abelsch. Somit ist S_4 auflösbar.

In der Tat sind die Gruppen S_n für $n \leq 4$ auflösbar, aber nicht auflösbar für alle $n \geq 5$. Das wurde zuerst von Galois gezeigt.

Theorem 2.10.4. *(Galois) Die Gruppe A_n ist einfach für jedes $n \geq 5$.*

Beweis. Die Beweisidee ist wie folgt. Man kann zeigen, dass jeder nicht-triviale Normalteiler N von A_n einen 3-Zykel enthält für $n \geq 5$, und dann alle 3-Zykel enthält. Da wegen Lemma 2.4.8 das Erzeugnis aller 3-Zykel schon A_n ist, folgt $N = A_n$. □

Eine einfache Gruppe ist auflösbar genau dann wenn sie abelsch ist. Die Gruppe A_n für $n \geq 5$ ist also nicht auflösbar, da sie einfach und nicht-abelsch ist.

Korollar 2.10.5. *Die einzigen Normalteiler von S_n für $n \geq 5$ sind $1, A_n$ and S_n. Insbesondere ist S_n nicht auflösbar für $n \geq 5$.*

Beweis. Sei N ein Normalteiler in S_n. Dann ist auch $N \cap A_n$ ein Normalteiler in A_n. Da A_n aber einfach ist, gilt entweder $N \cap A_n = A_n$ oder $N \cap A_n = 1$. Im ersten Fall gilt $N \supseteq A_n$. Da A_n Index 2 in S_n hat, folgt $N = A_n$ oder $N = S_n$. Im Fall $N \cap A_n = 1$ ist die Abbildung $n \mapsto nA_n$ von N nach $S_n/A_n \cong C_2$ injektiv, so dass N die Ordnung 1 oder 2 hat. Aber N kann nicht Ordnung 2 haben, da keine Konjugationsklasse in S_n außer $\{1\}$ aus einem einzigen Element bestehen kann, und N ja die disjunkte Vereinigung aller Konjugationsklassen ist, die triviale Konjugationsklasse eingeschlossen. Somit hat S_n, $n \geq 5$ nur eine einzige Kompositionsreihe, nämlich

$$S_n \triangleright A_n \triangleright 1.$$

Ihre Faktoren sind C_2 und die nicht-abelsche Gruppe A_n. □

Satz 2.10.6. *Jede Untergruppe und jede Quotientengruppe einer auflösbaren Gruppe ist auflösbar.*

Beweis. Sei $G \triangleright G_1 \triangleright \cdots \triangleright G_n$ eine auflösbare Reihe für G und H eine Untergruppe von G. Der Homomorphismus $H \cap G_i \to G_i/G_{i+1}$ mit $x \mapsto xG_{i+1}$ hat den Kern

$$(H \cap G_i) \cap G_{i+1} = H \cap G_{i+1}.$$

Deshalb ist $H \cap G_{i+1}$ ein Normalteiler von $H \cap G_i$ und der Quotient

$$(H \cap G_i)/(H \cap G_{i+1})$$

ist abelsch, weil er injektiv in die abelsche Gruppe G_i/G_{i+1} abgebildet wird. Insgesamt folgt, dass

$$H \triangleright (H \cap G_1) \triangleright \cdots \triangleright (H \cap G_n)$$

eine auflösbare Reihe für H ist.

Sei N ein Normalteiler von G. Wir konstruieren nun eine auflösbare Reihe für G/N aus der auflösbaren Reihe von G. Es gilt $NG_i \triangleright NG_{i+1}$, da N und G_{i+1} beide NG_i normaliseren in G. Also erhalten wir die Normalreihe

$$G = NG_0 \triangleright NG_1 \triangleright \cdots \triangleright NG_n = N.$$

Reduktion modulo N ergibt

$$\overline{G} = G/N \triangleright \overline{G}_1 \triangleright \cdots \triangleright \overline{G}_n = \{\overline{1}\}$$

mit $\overline{G}_i = (NG_i)/N \cong G_i/(N \cap G_i)$. Die natürliche Abbildung $G_i \to \overline{G}_i$ ist surjektiv. Also ist auch $G_i \to \overline{G}_i/\overline{G}_{i+1}$ surjektiv und Null auf G_{i+1}, so dass $\overline{G}_i/\overline{G}_{i+1}$ eine Quotientengruppe von G_i/G_{i+1} ist für alle i, also ebenfalls abelsch ist. Damit haben wir gezeigt, dass die obige Normalreihe eine auflösbare Reihe für G/N ist. □

Satz 2.10.7. *Sei N ein Normalteiler von G und seien N und G/N auflösbar. Dann ist G auflösbar.*

Beweis. Sei $\overline{G} = G/N$ und seien

$$\overline{G} \triangleright \overline{G}_1 \triangleright \cdots \triangleright \overline{G}_n = 1,$$
$$N \triangleright N_1 \triangleright \cdots \triangleright N_m = 1$$

auflösbaren Reihen für $\overline{G}$ bzw. N. Sei G_i das inverse Bild von $\overline{G}_i$ in G, d.h., mit $G_i \mapsto \overline{G}_i$ unter der Quotientenabbildung $G \to G/N$. Dann gilt

$$G_i/G_{i+1} \cong \overline{G}_i/\overline{G}_{i+1},$$

und somit ist

$$G \triangleright G_1 \triangleright \cdots \triangleright (G_n = N) \triangleright N_1 \triangleright \cdots \triangleright N_m$$

eine auflösbare Reihe für G. □

Korollar 2.10.8. *Jede p-Gruppe ist auflösbar.*

Beweis. Sei G eine nicht-triviale p-Gruppe. Wir zeigen die Behauptung mit Induktion über $|G|$. Da $Z(G)$ nicht-trivial ist wegen Satz 2.7.11, ist $G/Z(G)$ auflösbar nach Induktionsannahme. Da $Z(G)$ abelsch und somit auflösbar ist, ist wegen Satz 2.10.7 auch G auflösbar. □

Für eine auflösbare Gruppe G gibt es eine *kanonische* auflösbare Reihe, nämlich die *abgeleitete Reihe*. Das ist übrigens die kürzeste auflösbare Reihe für G. Der *Kommutator* von zwei Elementen x, y in G ist definiert als

$$[x, y] := xyx^{-1}y^{-1} = (xy)(yx)^{-1}.$$

Also bedeutet $[x, y] = e$, dass x und y kommutieren, d.h., $xy = yx$.

Definition 2.32. Sei G eine Gruppe. Die *abgeleitete Gruppe*, oder auch die *Kommutatoruntergruppe* von G ist die Gruppe, die von allen Kommutatoren von G erzeugt wird. Sie wird mit G' bzw. $[G, G]$ bezeichnet.

Man beachte, dass G' nicht nur aus Kommutatoren bestehen muss. Sie ist nur *erzeugt* von allen Kommutatoren.

Definition 2.33. Eine Untergruppe H von G heißt *charakteristisch*, falls $\varphi(H) \subseteq H$ für alle $\varphi \in \mathrm{Aut}(G)$ gilt.

Lemma 2.10.9. *Die Kommutatoruntergruppe von G ist eine charakteristische Untergruppe von G, und daher auch ein Normalteiler von G.*

Beweis. Seien x, y in G und $\varphi \in \mathrm{Aut}(G)$. Dann gilt

$$\begin{aligned}\varphi([x, y]) &= \varphi(xyx^{-1}y^{-1}) \\ &= \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1} \\ &= [\varphi(x), \varphi(y)].\end{aligned}$$

Also werden die Erzeuger von G' auf G' abgebildet. Deshalb folgt $\varphi(G') \subseteq G'$ für alle Automorphismen von G. Betrachtet man die inneren Automorphismen, so folgt $gG'g^{-1} \subseteq G'$ für alle $g \in G$. Also ist G' ein Normalteiler von G. □

Beispiel 2.10.10. 1. *Eine Gruppe G ist abelsch genau dann wenn $G' = 1$.*

2. *Für $n \geq 3$ gilt $D_n' = \langle r^2 \rangle$, mit $[r, s] = r(sr^{-1}s^{-1}) = r^2$.*

3. *Für $n \geq 5$ gilt $A_n' = A_n$, da $[(abd), (ace)] = (abc)$ für verschiedene a, b, c, d, e, und da A_n von allen 3-Zykeln erzeugt wird.*

4. *Es gilt $A_4' = V_4$, welches die normale 2-Sylowgruppe von A_4 ist.*

5. *Es gilt $Q_8' = \{\pm 1\} = Z(Q_8)$.*

Satz 2.10.11. *Die Kommutatoruntergruppe G' ist der kleinste Normalteiler N von G, so dass G/N abelsch ist.*

Beweis. Wir zeigen zuerst, dass G/G' abelsch ist. Der kanonische Homomorphismus $\pi\colon G \to G/G'$ bildet g auf $\overline{g} = gG'$ ab. Es gilt

$$[\overline{g}, \overline{h}] = \overline{[g, h]} = \overline{1}$$

für alle g, h, wegen $[g, h] \in G'$. Also kommutieren alle $\overline{g}, \overline{h}$ in G/G'.
Sei N ein Normalteiler von G mit G/N abelsch. Dann ist das Bild von $[g, h]$ in G/N wieder trivial, so dass $[g, h] \in N$. Da diese Elemente G' erzeugen, gilt $N \supseteq G'$. □

Beispiel 2.10.12. *Für $n \geq 5$ gilt $S_n' = A_n$, da A_n der kleinste Normalteiler von S_n mit abelschem Quotient ist.*

Definition 2.34. Die *abgeleitete Reihe* von G ist gegeben durch

$$G = G^{(0)} \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \cdots$$

mit $G^{(i+1)} = [G^{(i)}, G^{(i)}] = (G^{(i)})'$ für alle i.

Wir haben $G = G^{(0)}$, $G' = G^{(1)} = [G, G]$, $G'' = G^{(2)} = [[G, G], [G, G]]$ und so weiter.

Beispiel 2.10.13. *Die abgeleitete Reihe von S_n für $n \geq 5$ ist*

$$S_n \triangleright A_n \trianglerighteq A_n \trianglerighteq \cdots$$

und endet nicht mit der trivialen Gruppe.

Es stellt sich heraus, dass eine Gruppe G genau dann auflösbar ist, wenn ihre abgeleitete Reihe mit der trivialen Gruppe endet.

Satz 2.10.14. *Eine Gruppe G ist genau dann auflösbar, wenn $G^{(s)} = 1$ für ein $s \geq 0$ gilt.*

Beweis. Gilt $G^{(s)} = 1$, dann ist die abgeleitete Reihe natürlich eine auflösbare Reihe für G. Sei umgekehrt

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_s = 1$$

eine auflösbare Reihe für G. Da G/G_1 abelsch ist, gilt $G_1 \supseteq G'$ nach Satz 2.10.11. Nun ist $G'G_2$ eine Untergruppe von G_1, und wegen

$$G'/(G' \cap G_2) \cong G'G_2/G_2 \subseteq G_1/G_2$$

sehen wir, dass die Kommutativität von G_1/G_2 die von $G'/(G' \cap G_2)$ impliziert. Das bedeutet aber $G'' \subset G' \cap G_2 \subseteq G_2$. Fahren wir in dieser Weise fort, folgt $G^{(i)} \subseteq G_i$ für alle i, und deshalb $G^{(s)} = 1$. □

Der zweite Teil des Beweises zeigt auch, dass die abgeleitete Reihe einer auflösbaren Gruppe die kürzeste auflösbare Reihe ist.

Definition 2.35. Das kleinste $i \geq 0$ mit $G^{(i)} = 1$, beziehungsweise die Anzahl der Faktoren in der abgeleiteten Reihe von G heißt die *Auflösbarkeitsklasse*, oder *abgeleitete Länge* von G.

Beispiel 2.10.15. 1. *Für $n \geq 3$ ist D_n auflösbar der Klasse 2, mit abgeleiteter Reihe $D_n \triangleright \langle r^2 \rangle \triangleright 1$.*

2. *S_4 ist auflösbar der Klasse 3, mit $S_4 \triangleright A_4 \triangleright V_4 \triangleright 1$.*

3. *Q_8 ist auflösbar der Klasse 2, mit $Q_8 \triangleright \{\pm 1\} \triangleright 1$.*

Satz 2.10.16. *Sei G eine Gruppe der Ordnung pq mit verschiedenen Primzahlen p und q. Dann ist G auflösbar.*

Beweis. Wegen Sylow III gilt für die Anzahl n_p der p-Sylowgruppen $n_p \equiv 1 \bmod p$ und $n_p \mid q$. Daraus folgt $n_p = 1$ für $q < p$, so dass G eine eindeutige p-Sylowgruppe P hat, die deshalb Normalteiler von G ist. Also hat G die auflösbare Reihe $G \triangleright P \triangleright 1$, mit den zyklischen Faktoren $G/P \cong C_q$ und $P \cong C_p$. □

Bemerkung 2.10.17. Burnside zeigte 1904, dass alle Gruppen der Ordnung $p^a q^b$ für Primzahlen $p < q$ und alle $a, b \in \mathbb{N}$ auflösbar sind. Feit und Thompson bewiesen 1963 sogar, dass *alle Gruppen ungerader Ordnung* auflösbar sind. Der Beweis ist 255 Seiten lang und füllt einen kompletten Band des Pacific Journal of Mathematics.

Eine spezielle Klasse auflösbarer Gruppen ist durch *nilpotente* Gruppen gegeben.

Definition 2.36. Eine aufsteigende Reihe von Untergrupppen

$$1 = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_n = G$$

heißt *aufsteigende Zentralreihe* für G, falls $G_i \trianglelefteq G$ und $G_{i+1}/G_i \subseteq Z(G/G_i)$ gilt für alle i. Eine absteigende Reihe

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = 1$$

heißt *absteigende Zentralreihe*, falls $G_i \trianglelefteq G$ und $G_i/G_{i+1} \subseteq Z(G/G_{i+1})$ gilt für alle i.

Die Bedingung $G_i \trianglelefteq G$ is nötig, damit die Faktorgruppe G/G_i Sinn macht. Es impliziert auch, dass G_i normal in G_{i+1} ist für alle i.

Definition 2.37. Die aufsteigende Reihe

$$1 \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \cdots,$$

wobei $Z_1(G) = Z(G)$ und $Z_i(G)$ rekursiv durch

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$$

definiert ist für alle $i \geq 0$, heißt *obere Zentralreihe* für G, wenn sie mit G endet.
Die absteigende Reihe

$$G^0 = G \supseteq G^1 \supseteq G^2 \supseteq \cdots$$

definiert durch $G^0 = G$ und $G^{i+1} = [G, G_i] = [G_i, G]$ für alle $i \geq 0$, heißt *untere Zentralreihe* für G, wenn sie mit der trivialen Gruppe endet.

Man kann nachprüfen, dass beide Reihen Zentralreihen sind, sofern sie terminieren. Auch das folgende Lemma ist nicht schwer zu zeigen.

Satz 2.10.18. *Für eine Gruppe G sind die folgenden Bedingungen äquivalent:*

(1) $G^c = 1$ *für ein* $c \geq 0$.

(2) $Z_c(G) = G$ *für ein* $c \geq 0$.

(3) G *hat eine Zentralreihe.*

Man beachte dass $G^c = 1$ genau dann gilt wenn $Z_c(G) = G$.

Definition 2.38. Eine Gruppe G heißt *nilpotent*, falls sie eine der drei Bedingungen aus Satz 2.10.18 erfüllt. Die kleinste Zahl $c \geq 0$ mit $G^c = 1$ bzw. $Z_c(G) = G$ heißt dann *Nilpotenzklasse* von G.

Eine Gruppe hat Nilpotenzklasse 0 genau dann, wenn sie trivial ist, und Nilpotenzklasse 1 genau dann, wenn sie abelsch ist und nicht-trivial. G ist nilpotent der Klasse 2 genau dann, wenn $G/Z(G)$ abelsch und nicht-trivial ist.

Korollar 2.10.19. *Sei G eine nicht-triviale nilpotente Gruppe. Dann ist $Z(G)$ nicht-trivial.*

Beweis. Falls $Z(G) = 1$ gilt, so gibt es kein $c \geq 0$ mit $Z_c(G) = G$. Das ist ein Widerspruch zu Satz 2.10.18. □

Beispiel 2.10.20. *Die Gruppe S_3 ist auflösbar, aber nicht nilpotent.*

Es gilt $Z(S_3) = 1$, also kann S_3 nicht nilpotent sein.

Satz 2.10.21. *Jede nilpotente Gruppe ist auflösbar.*

Beweis. Es gilt $G^{(i)} \leq G^i$ für alle $i \geq 0$. Also impliziert $G^c = 1$ auch $G^c = 1$. □

Umgekehrt gibt es Gruppen, die auflösbar sind, aber nicht nilpotent, wie wir mit $S_3 \cong D_3$ bereits gesehen haben. Diedergruppen liefern weitere solche Beispiele.

Beispiel 2.10.22. *Sei $n \geq 3$ ungerade. Dann ist D_n auflösbar, aber nicht nilpotent.*

Für ungerades $n \geq 3$ gilt $D_n^i = \langle r \rangle$ für alle $i \geq 3$. Also gibt es kein $c \geq 0$ mit $D_n^c = 1$. Diedergruppen können auch für gerade n nilpotent sein.

Bemerkung 2.10.23. Die Diedergruppe D_n ist für $n \geq 3$ genau dann nilpotent, wenn $n = 2^m$ für ein $m \geq 2$ gilt.

Satz 2.10.24. *Jede Gruppe der Ordnung p^3 für p prim ist nilpotent der Klasse $c \leq 2$.*

Beweis. Ist G abelsch, so gilt $c = 1$. Ist G nicht-abelsch, so kann $Z(G)$ nicht Ordnung p^2 haben, da sonst $G/Z(G)$ Ordnung p hätte, also zyklisch wäre und somit G abelsch, nach Lemma 2.7.13. Also gilt $|Z(G)| = p$ wegen $|Z(G)| \neq 1$. Nun ist $|G/Z(G)| = p^2$, weswegen $G/Z(G)$ abelsch ist nach Satz 2.7.14. Aus Satz 2.10.11 folgt $G' \subseteq Z(G)$. Wegen $Z(G) \subseteq G'$ folgt $G' = Z(G)$, und daher $G'' = 1$. □

Insbesondere sind die Gruppen $Q_8, D_4, \mathrm{Heis}(\mathbb{Z}/(p))$ und $\Gamma(p)$ nilpotent der Klasse 2. Wir zeigen nun, dass p-Gruppen immer nilpotent sind.

Satz 2.10.25. *Jede p-Gruppe ist nilpotent.*

Beweis. Sei $|G| = p^n$. Wir führen den Beweis mit Induktion über n. Für $n = 0$ ist G trivial, also nilpotent. Für nicht-triviales G ist auch $Z(G)$ nicht-trivial wegen Korollar 2.10.19. Also ist $G/Z(G)$ eine p-Gruppe kleinerer Ordnung. Nach Induktionsvoraussetzung ist sie nilpotent, d.h.,

$$(G/Z(G))^c = 1$$

für ein c. Sei π der kanonische Homomorphismus $\pi\colon G \to G/Z(G)$. Da π surjektiv ist, gilt

$$\pi(G^c) = (G/Z(G))^c = 1.$$

Also ist $G^c \leq \ker(\pi) = Z(G)$, und somit

$$G^{c+1} = [G^c, G] \leq [Z(G), G] = 1.$$

□

3 Ringe

3.1 Ringaxiome

Definition 3.1. Ein *Ring* R ist eine Menge zusammen mit zwei Abbildungen $+, \cdot \colon R \times R \to R$, genannt Addition und Multiplikation, mit folgenden Eigenschaften.

(1) Das Paar $(R, +)$ bildet eine abelsche Gruppe. Das neutrale Element wird mit 0 bezeichnet, und das additive Inverse zu a mit $-a$.

(2) Die Multiplikation ist assoziativ und es gibt ein Einselement $1 = 1_R$ bezüglich Multiplikation mit $1 \cdot a = a \cdot 1 = a$ für alle $a \in R$.

(3) Es gilt das *Distributivgesetz*, d.h. für alle $a, b, c \in R$ gilt

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

Gilt weiterhin $a \cdot b = b \cdot a$ für alle $a, b \in R$, so heisst der Ring R *kommutativ*.

Das Axiom (2) kann man auch so formulieren, dass man sagt, $(R, \cdot)$ ist ein *Monoid*. In jedem Ring R gelten die Beziehungen $0 \cdot a = a \cdot 0 = 0$ für alle $a \in R$ und $(-a) \cdot b = a \cdot (-b) = -a \cdot b$ für alle $a, b \in R$. Gilt $1 = 0$, so ist

$$a = a \cdot 1 = a \cdot 0 = 0$$

für alle $a \in R$. Dieser Ring wird als *Nullring* bezeichnet.

Beispiel 3.1.1. 1. *Die Mengen* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *bilden bezüglich der gewöhnlichen Addition und Multiplikation einen kommutativen Ring.*

2. *Die Menge* $\mathbb{N}$ *bildet bezüglich der gewöhnlichen Addition und Multiplikation keinen Ring, da* $(\mathbb{N}, +)$ *keine Gruppe ist.*

3. *Die Menge $M_n(K)$ der $n \times n$-Matrizen mit Koeffizienten in einem Körper K bilden einen Ring bezüglich Matrizenaddition und Matrizenmultiplikation. Für $n \geq 2$ ist dieser Ring nicht kommutativ.*

4. *Sind R, S zwei Ringe, so ist deren Produkt $R \times S$, versehen mit der komponentenweisen Addition und Multiplikation, wieder ein Ring.*

5. *Sei $(A, +)$ eine abelsche Gruppe. Dann ist die Menge $\mathrm{End}(A)$ aller Gruppenendomorphismen $\varphi\colon A \to A$ ein Ring, wenn man Summe und Produkt durch*

$$\begin{aligned}(\varphi + \psi)(x) &= \varphi(x) + \psi(x),\\ (\varphi \cdot \psi)(x) &= \varphi(\psi(x))\end{aligned}$$

definiert, für alle $x \in A$, $\varphi, \psi \in \mathrm{End}(A)$.

6. *Ist K ein Körper, so ist der Polynomring $K[X]$ ein kommutativer Ring.*

Bemerkung 3.1.2. Ein *Körper* ist ein kommutativer Ring K, der nicht der Nullring ist, in dem jedes Element $a \in K^\times$ ein Inverses bezüglich der Multiplikation besitzt. Mit anderen Worten, $(K^\times, \cdot)$ ist eine abelsche Gruppe.

Definition 3.2. Eine Abbildung $\varphi\colon R \to S$ eines Ringes R in einen Ring S heißt *(Ring)homomorphismus*, falls

$$\begin{aligned}\varphi(a + b) &= \varphi(a) + \varphi(b),\\ \varphi(a \cdot b) &= \varphi(a) \cdot \varphi(b),\\ \varphi(1_A) &= 1_B\end{aligned}$$

für alle $a, b \in R$ gilt.

Beispiel 3.1.3. *Die Abbildung*

$$\varphi\colon \mathbb{Z} \to \mathbb{Z},\ \varphi(n) = 2 \cdot n$$

ist kein Ringhomomorphismus, denn die 1 wird nicht auf die 1 abgebildet.

Verknüpfungen von Ringhomomorphismen sind Ringhomomorphismen und die Identitätsabbildung auf einem Ring ist ein Ringhomomorphismus. Monomorphismus, Endomorphismus, Isomorphismus sind analog definiert, wie bei Gruppen.

Definition 3.3. Eine Teilmenge S eines Ringes R heißt *Unterring* von R, falls S mit den Verknüpfungen $+, \cdot$ von R, eingeschränkt auf S, einen Ring bildet mit $1_S = 1_R$.

Mit anderen Worten, $S \subseteq R$ ist ein Unterring, wenn $1_R \in S$, $a - b \in S$ und $a \cdot b \in S$ für alle $a, b \in S$.

Beispiel 3.1.4. *(Übungsaufgabe)* 1. *Die Menge* $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ *ist ein Unterring von* $\mathbb{C}$. *Er wird der Ring der* Gaußschen ganzen Zahlen *genannt.*

2. *Das* Zentrum $Z(R) = \{x \in R \mid xy = yx \text{ für alle } x, y \in R\}$ *ist ein Unterring von* R.

Der Ring $\mathbb{Z}[i]$ kann zum Beispiel verwendet werden, um zu untersuchen, welche ganzen Zahlen als Summe zweier Quadratzahlen geschrieben werden können. In $\mathbb{Z}[i]$ gilt nämlich für alle $a, b \in \mathbb{Z}$, dass

$$a^2 + b^2 = (a + bi)(a - bi).$$

Eine ungerade Primzahl p kann genau dann als $p = a^2 + b^2$ mit $a, b \in \mathbb{Z}$ dargestellt werden kann, wenn $p \equiv 1 \bmod 4$ gilt (Fermat).

3.2 Ideale und Restklassenringe

Definition 3.4. Eine Teilmenge I eines Ringes R heißt *Linksideal*, falls $(I, +)$ eine Untergruppe von $(R, +)$ ist und $x \cdot a \in I$ für alle $a \in I$ und alle $x \in R$, d.h. $RI \subseteq I$ gilt. Sie heißt *Rechtsideal*, wenn $(I, +) \leq (R, +)$ und $IR \subseteq I$ gilt, und *(beidseitiges) Ideal*, wenn I ein Rechts-und Linksideal ist.

Für kommutative Ring fallen die Begriffe Linksideal, Rechtsideal und beidseitiges Ideal zusammen. Man spricht dann nur von Ideal.

Beispiel 3.2.1. *Sei* $R = \mathbb{Z} \times \mathbb{Z}$. *Dann ist* $S = \{(n, n) \mid n \in \mathbb{Z}\}$ *ein Unterring von* R, *aber kein Ideal.*

Mit $a = (1, 1) \in S$ und $x = (1, 0) \in R$ gilt $x \cdot a = (1, 0) \cdot (1, 1) = (1, 0) \notin S$. Also ist S kein Ideal.

Beispiel 3.2.2. *Sei $R = M_2(K)$ der Ring der 2×2-Matrizen über einem Körper K. Dann ist*

$$I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in K \right\}$$

ein Linksideal in R, aber kein Rechtsideal, und

$$J = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in K \right\}$$

ein Rechtsideal in R, aber kein Linksideal.

Man kann leicht folgendes Resultat zeigen.

Lemma 3.2.3. *Für zwei Ideale I, J in R sind auch folgende Teilmengen*

$$\begin{aligned} I + J &= \{a + b \mid a \in I, b \in J\} \\ IJ &= \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J \right\} \\ I \cap J &= \{x \in R \mid x \in I, x \in J\} \end{aligned}$$

wieder Ideale. Es gilt $IJ \subseteq I \cap J$.

Die Summe $I + J$ von zwei Idealen ist das kleinste Ideal von R, das I und J umfasst.

Beispiel 3.2.4. *Sei $R = \mathbb{Z}$ und $I = n\mathbb{Z}$, $J = m\mathbb{Z}$ für $n, m \in \mathbb{Z}$. Dann sind I und J Ideale in R und es bezeichne $(m, n) = \gcd(m, n)$, $[m, n] = \mathrm{l}cm(m, n)$. Dann gilt*

$$\begin{aligned} I + J &= (m, n)\mathbb{Z}, \\ IJ &= (mn)\mathbb{Z}, \\ I \cap J &= [m, n]\mathbb{Z}. \end{aligned}$$

Sei $d = (m, n)$. Wegen $d \mid m$ ist jedes Vielfache von m auch ein Vielfaches von d. Also ist $I \subseteq d\mathbb{Z}$. Ebenso folgt $J \subseteq d\mathbb{Z}$, also $I + J \subseteq d\mathbb{Z}$. Wegen des Euklidischen Algorithmus gibt es $a, b \in \mathbb{Z}$ mit $d = am + bn$. Wegen $am \in I$ und $bn \in J$ folgt $d\mathbb{Z} \subseteq I + J$. Also gilt $I + J = d\mathbb{Z}$.
Die weiteren Behauptungen folgen ebenfalls leicht. Insbesondere gibt es $m, n \in \mathbb{Z}$ mit $IJ \neq I \cap J$.

Satz 3.2.5. *Sei I ein Ideal in $\mathbb{Z}$. Dann gibt es ein $n \in \mathbb{Z}$ mit $I = n\mathbb{Z}$. Für zwei Ideale $m\mathbb{Z}$ und $n\mathbb{Z}$ gilt*

$$m\mathbb{Z} \supseteq n\mathbb{Z} \iff m \mid n.$$

Beweis. Für $I = 0$ ist nichts zu zeigen. Sei also $n \in I$ die kleinste positive Zahl in I. Da I ein Ideal ist, folgt $n\mathbb{Z} \subseteq I$. Ein solches $n \in \mathbb{N}$ existiert, da mit $k \in \mathbb{Z}$ auch $-k \in \mathbb{Z}$ gilt. Sei $a \in \mathbb{Z}$. Dann existieren $q \in \mathbb{Z}$, $r \in \mathbb{N}$ mit

$$a = qn + r,\ 0 \leq r < n.$$

Also ist $r = a - qn \in I$. Da n die kleinste positive Zahl in I war, folgt $r = 0$. Also ist $a = qn$, also $I \subseteq n\mathbb{Z}$. Zusammen folgt $I = n\mathbb{Z}$.
Gilt $n\mathbb{Z} \subseteq m\mathbb{Z}$, so ist $n \in m\mathbb{Z}$, also $n = km$ für ein $k \in \mathbb{Z}$, d.h. $m \mid n$. Gilt umgekehrt $n = km$, und $r \in \mathbb{Z}$, so ist $nr = kmr$, also $n\mathbb{Z} \subseteq m\mathbb{Z}$. □

Satz 3.2.6 (Restklassenring)**.** *Sei R ein Ring und $I \subseteq R$ ein Ideal. Dann ist $R/I = \{x+I \mid x \in R\}$ bezüglich der von der Addition auf R induzierten Addition auf R/I eine abelsche Gruppe. Es gilt:*

(1) *Die Multiplikationsabbildung*

$$R/I \times R/I \to R/I,$$
$$(x + I, y + I) \mapsto (x \cdot y) + I$$

ist wohldefiniert.

(2) *Die Menge R/I bildet bezüglich der obigen Addition bzw. Multiplikation einen Ring, den Restklassenring (Faktorring), von R modulo I.*

Wir schreiben für die Restklassen $x + I$ oft auch kurz $[x]$. Die Abbildung $\pi\colon R \to R/I$, definiert durch $x \mapsto x + I$, ist ein surjektiver Ringhomomorphismus, genannt die *natürliche Projektion.*

Beispiel 3.2.7. *Für $R = \mathbb{Z}$ und $I = n\mathbb{Z}$ erhält man den Faktorring $\mathbb{Z}/n\mathbb{Z}$.*

Die unterliegende additive Gruppe ist die zyklische Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$. Insbesondere enthält $\mathbb{Z}/n\mathbb{Z}$ genau n Elemente: $[0], [1], \ldots, [n-1]$. In diesem Ring gilt, für $n = km$

$$[k] \cdot [m] = [n] = [0].$$

Ist n also zusammengesetzt, so unterscheidet sich die Multiplikation von der bei Körpern. Man hat $[k], [m] \neq [0]$, aber $[k] \cdot [m] = [0]$, sogenannte *Nullteiler.*

Bemerkung 3.2.8. Die Arithmetik in den Restklassenringen der Form $\mathbb{Z}/n\mathbb{Z}$ kann zum Beispiel verwendet werden, um zu zeigen, dass gewisse Gleichungen keine ganzzahligen Lösungen besitzen. Man betrachte etwa die Gleichung

$$x^2 + y^2 = 2023$$

über $\mathbb{Z}$. Angenommen sie hätte eine Lösung in $\mathbb{Z}$. Wir betrachten die kanonische Projektion $\pi\colon \mathbb{Z} \to 4\mathbb{Z}$. Da π ein surjektiver Ringhomomorphismus ist, hat die Gleichung auch eine Lösung in $\mathbb{Z}/4\mathbb{Z}$. Jedoch ist $[a^2] = [a]^2$ immer $[0]$ oder $[1]$ in $\mathbb{Z}/4\mathbb{Z}$ und $[2023] = [3]$. Eine Summe aus zwei Restklassen $[0], [1]$ kann aber nur $[0], [1], [2]$ ergeben, ein Widerspruch.

Bemerkung 3.2.9. Die Isomorphiesätze für Gruppen lassen sich analog für Ringe formulieren (und beweisen).

1. Ist $\varphi\colon R \to S$ ein Rinhomomorphismus, so ist $\ker(\varphi)$ ein Ideal in R, $\mathrm{im}(\varphi)$ ein Unterring von S und $R/\ker(\varphi) \cong \mathrm{im}(\varphi)$ für den Faktorring.

2. Sind $S \subseteq R$ ein Unterring von R und I ein Ideal von R, so ist $I + S$ ein Unterring von R, $S \cap I$ ein Ideal von S und $(S + I)/I \cong S/(S \cap I)$.

3. Sind $J \subseteq I$ Ideale in R, dann ist I/J ein Ideal in R/J und $(R/J)/(I/J) \cong R/I$.

3.3 Einheiten, Nullteiler, Integritätsringe

Definition 3.5. Sei R ein Ring. Ein Element $a \in R$ heißt *Einheit* oder *invertierbar*, wenn es ein $b \in R$ gibt mit $ab = ba = 1$. Die Einheiten eines Ringes R bilden eine Gruppe bezüglich Multiplikation, die mit $R^\times$ oder $U(R)$ bezeichnet wird. Sie heißt die *Einheitengruppe* von R.

Man beachte, dass ein Ringisomorphismus einen Gruppenisomorphismus seiner Einheitengruppen induziert.

Beispiel 3.3.1. 1. *Es gilt* $\mathbb{Z}^\times = \{\pm 1\} \cong C_2$.

2. *Es gilt* $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\} \cong C_4$. *(Übung)*

3. *Es gilt* $(\mathbb{Z}/14\mathbb{Z})^\times = \{[1], [3], [5], [9], [11], [13]\} \cong C_6$.

4. *Die Einheitengruppe des Matrizenringes* $M_n(K)$ *ist die Gruppe* $GL_n(K)$.

Bemerkung 3.3.2. Die *prime Restklassengruppe* $(\mathbb{Z}/n\mathbb{Z})^\times$ hat $\varphi(n)$ Elemente. Sie ist zyklisch dann und nur dann, wenn

$$n = 2, 4, p^k, 2p^k$$

gilt, mit ungerader Primzahl p und $k \in \mathbb{N}$, siehe Theorem 3.11.16.

Bemerkung 3.3.3. Ein *Körper* ist ein kommutativer Ring K, dessen Einheitengruppe mit der multiplikativen Gruppe $(K \setminus 0, \cdot)$ übereinstimmt. Insbesondere ist $1 \neq 0$, also K nicht der Nullring.

Für $a \in R$ definiert man die Potenzen a^n rekursiv durch $a^0 = 1$ und $a^{n+1} = a^n \cdot a$.

Definition 3.6. Ein Element a in R heißt *Linksnullteiler*, falls ein $x \neq 0$ in R existiert mit $ax = 0$. Es heißt *Rechtsnullteiler*, falls ein $y \neq 0$ in R existiert mit $ya = 0$. Ein Element, das sowohl ein Links- als auch Rechtsnullteiler ist, heißt *Nullteiler*. Ein Element $a \in R$ heißt *nilpotent*, wenn es ein $n \in \mathbb{N}$ gibt mit $a^n = 0$.

Beispiel 3.3.4. *Die Nullteiler des Ringes* $\mathbb{Z}/12\mathbb{Z}$ *sind gegeben durch die Nicht-Einheiten*

$$[0], [2], [3], [4], [6], [8], [9], [10],$$

und die nilpotenten Elemente sind gegeben durch $[0]$ *und* $[6]$.

Lemma 3.3.5. *Sei* R *ein Ring und* $a \in R$ *nilpotent. Dann sind* $1 - a$ *und* $1 + a$ *Einheiten von* R.

Beweis. Sei $a^n = 0$ mit $n \in \mathbb{N}$. Dann gilt

$$\begin{aligned} 1 &= 1 - a^n \\ &= (1 - a)(1 + a + a^2 + \cdots + a^{n-1}) \\ &= (1 + a + a^2 + \cdots + a^{n-1})(1 - a), \end{aligned}$$

und $1 - a$ ist eine Einheit. Ersetzt man a durch $-a$, so folgt auch, dass $1 + a$ eine Einheit ist. □

Allgemeine Ringe sind für viele unserer Fragestellungen zu kompliziert und ungeeignet. Deshalb wollen wir ab jetzt annehmen, dass alle Ringe *kommutativ* sind. Wir nennen einen Ring *nullteilerfrei*, wenn nur Null ein Nullteiler ist, d.h., aus $xy = 0$ folgt, dass entweder $x = 0$ oder $y = 0$ gilt.

Definition 3.7. Sei R (immer kommutativ) ein Ring mit $1 \neq 0$. R heißt *Integritätsring*, wenn er nullteilerfrei ist.

Beispiel 3.3.6. *Jeder Körper ist ein Integritätsring, und jeder Unterring eines Integritätsringes ist ein Integritätsring. Insbesondere sind* $\mathbb{Z}, \mathbb{Z}[i]$ *und* $\mathbb{Z}/p\mathbb{Z}$*,* p *prim, Integritätsringe.*

Beispiel 3.3.7. *Der Produktring* $R \times S$ *zweier Integritätsringe ist kein Integritätsring.*

Es gilt nämlich $(1,0)\cdot(0,1) = (0,0)$, mit $(1,0), (0,1) \in R\backslash 0$. Allgemeiner ist $R \times S$, R und S verschieden vom Nullring, kein Integritätsring.

In R schreiben wir $n \cdot x$ für $(1_R + \cdots + 1_R) \cdot x$ mit n Summanden. Die Abbildung $\chi\colon \mathbb{Z} \to R$ mit $n \mapsto n \cdot 1_R$ ist ein Ringhomomorphismus. Sein Kern ist ein Ideal in $\mathbb{Z}$, also von der Form $m\mathbb{Z}$ für eine eindeutig bestimmte natürliche Zahl m.

Definition 3.8. Die *Charakteristik* eines Ringes R ist die eindeutig bestimmte natürliche Zahl m mit $\ker(\chi) = m\mathbb{Z}$. Ist χ injektiv, so gilt $m = 0$. Ansonsten ist m die kleinste positive Zahl für die $n \cdot 1_R = 0$ gilt. Sie wird mit $char(R)$ bezeichnet.

Beispiel 3.3.8. *Es gilt* $char(\mathbb{Z}) = 0$*,* $char(\mathbb{Q}) = 0$ *und* $char(\mathbb{Z}/n\mathbb{Z}) = n$ *für alle* $n > 0$*.*

Lemma 3.3.9. *Sei* R *ein Integritätsring mit* $char(R) \neq 0$*. Dann ist die Charakteristik von* R *eine Primzahl.*

Beweis. Ist $char(R) = n = ab$ mit $1 < a, b < n$, so hat man

$$0 = n \cdot 1_R = (a \cdot 1_R)(b \cdot 1_R)$$

Da R keine Nullteiler hat, ist entweder $a \cdot 1_R = 0$ oder $b \cdot 1_R = 0$. Das steht aber im Widerspruch zur Minimalität von n in 3.8. Also ist n nicht zusammengesetzt. □

3.4 Hauptidealringe und Euklidische Ringe

Für $a \in R$ ist die Menge $(a) = \{xa \mid a \in R\}$ ein Ideal. Solche Ideale werden *Hauptideale* genannt. Man schreibt auch $Ra = aR = (a)$. Ist a eine Einheit,

so ist $(a) = (1) = R$, denn $a \in (1) = R$ und $1 \in (a)$ wegen $1 = a \cdot a^{-1} \in (a)$. Für jede Teilmenge $M \subseteq R$ ist

$$(M) = \left\{ \sum_{i=1}^{m} x_i a_i \mid m \in \mathbb{N}, x_i \in R, a_i \in M \right\}$$

ein Ideal in R. Es ist das kleinste Ideal von R, das M enthält. Man erhält es als Schnitt über alle Ideale, die M enthalten. Man bezeichnet (M) als das von M *erzeugte* Ideal in R.

Definition 3.9. Ein Ideal I in R heißt *endlich erzeugt*, wenn es eine endliche Menge M in R gibt mit $(M) = I$. Ist $M = \{a_1, \ldots, a_n\}$, so schreibt man auch

$$I = (a_1, \ldots, a_n).$$

Definition 3.10. Ein Integritätsring R, in dem jedes Ideal ein Hauptideal ist, heißt *Hauptidealring*, oder einfach nur *HIR*.

Beispiel 3.4.1. 1. *Nach Satz* 3.2.5 *ist* $\mathbb{Z}$ *ein Hauptidealring. Jedes Ideal* I *hat die Form* $(n) = n\mathbb{Z}$ *für ein* $n \in \mathbb{N}$.

2. $\mathbb{Z}/4\mathbb{Z}$ *ist kein Hauptidealring, obwohl alle Ideale Hauptideale sind.*

Allerdings ist $\mathbb{Z}/4\mathbb{Z}$ kein Integritätsring wegen $[2] \cdot [2] = [0]$.

Viele Hauptidealringe besitzen noch eine stärkere Eigenschaft, nämlich dass sie Euklidisch sind.

Definition 3.11. Ein Integritätsring R heißt *Euklidisch*, falls es eine Abbildung $d\colon R \setminus 0 \to \mathbb{N}$ gibt, so dass zu je zwei Elementen $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ existieren mit

$$a = qb + r,$$

wobei entweder $r = 0$ oder $d(r) < d(b)$ ist. Die Abbildung d heißt dann *Gradabbildung*, oder *Euklidische Funktion*.

Zum Beispiel ist $\mathbb{Z}$ mit der Gradabbildung $f(n) = |n|$ Euklidisch. Der Name Gradabbildung kommt von dem Beispiel des Polynomringes $K[X]$, wo $d(f) = \deg(f)$ tatsächlich der Grad von f ist. Dieser Ring ist auch Euklidisch, wenn K ein Körper ist. Der folgende Satz ist sehr hilfreich für die Untersuchung von Hauptidealringen.

Satz 3.4.2. *Jeder Euklidische Ring R ist ein Hauptidealring.*

Beweis. Zu gegebenem Ideal $I \neq 0$ besitzt die Menge $\{d(b) \mid b \in I \setminus 0\}$ nicht-negativer ganzer Zahlen ein kleinstes Element, d.h., es existiert ein $c \neq 0$ in I mit $d(c) \leq d(b)$ für alle $b \neq 0$ in I. Nach Annahme existieren nun für jedes $b \in I$ $q, r \in R$ mit $b = qc + r$ mit $r = 0$ oder $d(r) < d(c)$. Da c minimal war, folgt $r = 0$ und $b = qc \in (c)$. Also ist $(c) \subseteq I \subseteq (c)$, d.h. $I = (c)$ ist ein Hauptideal. □

Beispiel 3.4.3. *Der Ring $\mathbb{Z}[i]$ ist Euklidisch, und daher ein Hauptidealring.*

Tatsächlich ist es leichter zu zeigen, dass $\mathbb{Z}[i]$ mit $d(a + bi) = a^2 + b^2$ Euklidisch ist, als die Definition von Hauptidealring zu verwenden.

Bemerkung 3.4.4. Die Umkehrung des obigen Satzes gilt nicht. Es gibt Hauptidealringe, die nicht Euklidisch sind. Das bekannteste Beispiel dürfte der Ring

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$$

sein. Zum Beweis siehe Frage 998716 in StackExchange Mathematics, und deren Links. Ein etwas unbekannteres Beispiel ist der Faktorring

$$\mathbb{R}[x, y]/(x^2 + y^2 + 1).$$

Sei $d \in \mathbb{Z}$ quadratfrei. Die Menge

$$\mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d} \mid x, y \in \mathbb{Q}\} \subseteq \mathbb{C}$$

ist ein Unterkörper von $\mathbb{C}$. Sei $z = a+b\sqrt{d}$ ein Element, dann definiert man die *Norm* von z durch

$$N(z) = z\overline{z} = x^2 - dy^2,$$

wobei $\overline{z} = x - y\sqrt{d}$ das zu z konjugierte Element genannt wird, auch wenn z reell ist. Man kann nachrechnen, dass $N(wz) = N(w)N(z)$ gilt für alle $z, w \in \mathbb{Q}(\sqrt{d})$. Dann definiert man

$$\mathcal{O}_d = \{a + b\omega_d \mid a, b \in \mathbb{Z}\},$$

wobei

$$\omega_d = \begin{cases} \sqrt{d}, & \text{if } d \equiv 2, 3(4), \\ \frac{1}{2}(1 + \sqrt{d}), & \text{if } d \equiv 1(4). \end{cases}$$

Als Unterring von $\mathbb{C}$ ist $\mathcal{O}_d$ ein Integritätsring, den man den *Ring der ganzen Zahlen* in $\mathbb{Q}(\sqrt{d})$ nennt. Für $d = 1$ erhält man $\mathcal{O}_1 = \mathbb{Z}$ in $\mathbb{Q}$, und für $d = -1$ hat man $\mathcal{O}_{-1} = \mathbb{Z}[i]$ in $\mathbb{Q}(i)$. Wir nennen einen Ring $\mathcal{O}_K$ der ganzen Zahlen eines Zahlkörpers K, der ein endlicher-dimensionaler Vektorraum über $\mathbb{Q}$ ist, *Norm-Euklidisch*, falls er Euklidisch ist mit der Norm $|N(z)| = |z\overline{z}|$ ist. Für $K = \mathbb{Q}(\sqrt{d})$ mit $d \neq 1$ und d quadratfrei gilt $\dim_{\mathbb{Q}}(K) = 2$, weswegen man K einen *quadratischen* Zahlkörper nennt.

Theorem 3.4.5. *Die Ringe $\mathcal{O}_d$ für quadratfreies $d < 0$ sind genau dann Euklidisch, wenn*

$$d = -1, -2, -3, -7, -11$$

gilt, und in diesen Fällen ist $\mathcal{O}_d$ Norm-Euklidisch.

Für quadratfreies $d > 0$ kennt man nur die Klassifikation der Norm-Euklidischen Ringe.

Theorem 3.4.6. *Die Ringe $\mathcal{O}_d$ für quadratfreies $d > 0$ sind genau dann Norm-Euklidisch, wenn*

$$d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$$

gilt.

Bemerkung 3.4.7. M. Harper [2] zeigte, dass der Ring $\mathcal{O}_{14}$ Euklidisch ist, obwohl er nicht Norm-Euklidisch ist. Allerdings kennt bisher niemand die Gradabbildung dazu explizit.

Auch die Frage, welche $\mathcal{O}_d$ Hauptidealringe sind, ist nur für $d < 0$ bekannt, siehe [7].

Theorem 3.4.8 (Baker-Heegner-Stark)**.** *Die Ringe $\mathcal{O}_d$ für quadratfreies $d < 0$ sind genau dann Hauptidealringe, wenn*

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

gilt.

Für $d > 0$ hat Gauß vermutet, dass $\mathcal{O}_d$ ein Hauptidealring für unendliche viele (quadratfreie) d ist. Die bekannte Liste dieser Zahlen beginnt mit $d = 1, 2, 3, 5, 6, 7, 11, 13, 14$.

3.5 Polynomringe

Wir erinnern nochmal daran, dass alle Ringe kommutativ sind.

Definition 3.12. Sei R ein Ring. Der *Polynomring* $R[X]$ in einer Unbestimmten X ist die Menge aller formalen Summen

$$\sum_{i=0}^{n} a_i X^i$$

mit $n \in \mathbb{N}_0$ und $a_i \in R$, zusammen mit folgender Addition und Multiplikation

$$\sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{m} b_i X^i = \sum_{i=0}^{\max(n,m)} (a_i + b_i) X^i,$$
$$\left(\sum_{i=0}^{n} a_i X^i\right)\left(\sum_{i=0}^{m} b_i X^i\right) = \sum_{i=0}^{n+m} \left(\sum_{p+q=i} a_p b_q\right) X^i$$

Hier setzen wir $a_i = 0$ für $i \geq n+1$ und $b_i = 0$ für $i \geq m+1$.

Das Nullelement von $R[X]$ ist das Nullpolynom $0 = 0X^0$, und das Einselement ist $1 = 1X^0$. Die Abbildung

$$R \hookrightarrow R[X], \quad a \mapsto aX^0$$

ist ein injektiver Ringhomomorphismus. Er gestattet es, R als Unterring von $R[X]$ aufzufassen.

Definition 3.13. Sei $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ ein Polynom. Der *Grad* von f ist die größte natürliche Zahl $n \in \mathbb{N}_0$ mit $a_n \neq 0$, oder $-\infty$, falls alle $a_i = 0$ sind, d.h., $\deg(0) = -\infty$. Man schreibt $\deg(f) = n$ und a_n heißt der *Leitkoeffizient* von f. Ein Polynom $f \neq 0$ heißt *normiert*, falls $a_n = 1$ gilt mit $n = \deg(f)$.

Das einzige normierte Polynom vom Grad 0 ist $1X^0 = 1 = 1_R$. Nur das Nullpolynom hat Grad $-\infty$.

Lemma 3.5.1. *Es seien $f, g \in R[X]$ Polynome über R. Dann gilt*

$$\deg(f+g) \leq \max\{\deg(f), \deg(g)\},$$
$$\deg(fg) \leq \deg(f) + \deg(g)$$

Sind die Leitkoeffizienten von f und g keine Nullteiler, also zum Beispiel wenn R ein Integritätsring ist, so gilt die Gleichheit

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

Beweis. Ist entweder $f = 0$ oder $g = 0$, so gilt die Behauptung, wenn man die Konventionen $(-\infty) + (-\infty) = -\infty$ und $(-\infty) + n = -\infty$ beachtet. Andernfalls gilt $\deg(f) = n$, $\deg(g) = m$ mit $n, m \in \mathbb{N}_0$. Ist $f = \sum_{i=0}^{n} a_i X^i$ und $g = \sum_{i=0}^{m} b_i X^i$, so ist $a_i + b_i = 0$ für $i > \max(n, m)$. Also ist der Grad von $f + g$ höchstens so gross wie $\max(n, m)$. Für die zweite Ungleichung beachte man, dass $\sum_{p+q=i} a_p b_q = 0$ ist für $i \geq n + m$. Der Koeffizient vom Grad $n+m$ in fg ist $a_n b_m$. Ist R ein Integritätsring, oder sind a_n, b_m keine Nullteiler in R, so folgt aus $a_n, b_m \neq 0$ auch $a_n b_m \neq 0$. Dann gilt

$$\deg(fg) = n + m = \deg(f) + \deg(g).$$

□

Korollar 3.5.2. *Der Polynomring $R[X]$ ist genau dann ein Integritätsring, wenn R ein Integritätsring ist. Dann hat man $R[X]^\times = R^\times$.*

Beweis. Ist $R[X]$ nullteilerfrei, so auch sein Unterring R. Sei R nullteilerfrei und $f \in R[X]$ ein Nullteiler von $R[X]$ mit $fg = 0$ für ein $g \neq 0$. Dann folgt wegen Lemma 3.5.1

$$-\infty = \deg(0) = \deg(fg) = \deg(f) + \deg(g),$$

also $\deg(f) = -\infty$ und $f = 0$. Somit ist auch $R[X]$ nullteilerfrei.
Sei nun $f \in R[X]^\times$. Dann gibt es ein $g \in R[X]$ mit $fg = 1$. Lemma 3.5.1 ergibt

$$0 = \deg(fg) = \deg(f) + \deg(g),$$

also $\deg(f) = \deg(g) = 0$ und damit $f, g \in R^\times$. Somit ist

$$R[X]^\times \subseteq R^\times \subseteq R[X]^\times.$$

□

Satz 3.5.3. *Sei $g \neq 0$ ein Polynom in $R[X]$, dessen Leitkoeffizient eine Einheit in R ist. Dann existieren zu jedem Polynom $f \in R[X]$ eindeutig bestimmte Polynome $q, r \in R[X]$, so dass $f = qg + r$ mit $\deg(r) < \deg(g)$ gilt.*

Beweis. Die Fälle $f = 0$ bzw. $f \neq 0, \deg(f) < \deg(g)$ sind klar mit $q = 0$ und $r = f$. Sei also $m = \deg(f) \geq \deg(g) = n$. Wir führen eine Induktion über m. Sei $f = \sum_{i=0}^{m} a_i X^i$ und $g = \sum_{i=0}^{n} b_i X^i$ mit $b_n \in R^\times$. Der Grad des Polynoms

$$h = f - a_m b_n^{-1} X^{m-n} g$$

ist echt kleiner als m, weil sich das Leitmonom $a_m X^m$ von f mit dem von $a_m b_n^{-1} X^{m-n} g$ weghebt. Also gibt es nach Induktionsvoraussetzung $q_0, r \in R[X]$ mit $\deg(r) < n$, so dass $h = q_0 g + r$ ist. Daraus folgt

$$\begin{aligned} f &= (a_m b_n^{-1} X^{m-n} + q_0)g + r \\ &= qg + r. \end{aligned}$$

Nun fehlt nur noch die Eindeutigkeit von q und r zu zeigen. Angenommen, $f = q_1 g + r_1 = q_2 g + r_2$ mit $\deg(r_1), \deg(r_2) < \deg(g)$. Dann ist

$$(q_2 - q_1)g = r_2 - r_1.$$

Da b_n eine Einheit in R ist, gilt nach Lemma 3.5.1

$$\begin{aligned} \deg(g) > \deg(r_2 - r_1) &= \deg((q_2 - q_1)g \\ &= \deg(q_2 - q_1) + \deg(g). \end{aligned}$$

Das kann nur stimmen, wenn $q_2 - q_1$ das Nullpolynom vom Grad $-\infty$ ist, also für $q_2 = q_1$, und dann $r_2 = r_1$. □

Korollar 3.5.4. *Sei K ein Körper. Dann ist $K[X]$ mit der Gradfunktion $d(f) = \deg(f)$ ein Euklidischer Ring.*

3.6 Primideale und maximale Ideale

Definition 3.14. Sei R ein Ring.

(1) Ein Ideal $P \subset R$ heißt *prim* oder *Primideal*, wenn $P \neq R$ und wenn für alle $a, b \in R$ aus $ab \in P$ auch $a \in P$ oder $b \in P$ folgt.

(2) Ein Ideal $M \subset R$ heißt *maximal* oder *maximales Ideal*, wenn $M \neq R$ und wenn es kein Ideal I gibt mit $M \subsetneq I \subsetneq R$, d.h. wenn für alle Ideale $I \subseteq R$ mit $M \subseteq I$ gilt $I = M$ oder $I = R$.

Das Ideal $I = 0$ ist nach Definition genau dann ein Primideal, wenn R ein Integritätsring ist. In einem Körper ist $I = 0$ das einzige maximale Ideal. In $\mathbb{Z}$ ist jedes Ideal von der Form $n\mathbb{Z}$ mit $n \in \mathbb{N}$.

Beispiel 3.6.1. *Sei $m \in \mathbb{N}$. Ein Ideal $m\mathbb{Z}$ in $\mathbb{Z}$ ist genau dann prim, wenn $m = 0$ oder m prim ist. Es ist genau dann maximal, wenn m prim ist.*

Das folgt direkt aus den Definitionen. Allerdings kann man auch den folgenden Satz anwenden.

Satz 3.6.2. *Sei R ein Ring.*

(1) *Ein Ideal $P \subset R$ ist genau dann prim, wenn R/P ein Integritätsbereich ist.*

(2) *Ein Ideal $M \subset R$ ist genau dann maximal, wenn R/M ein Körper ist.*

Beweis. Zu (1): Ist $P \subset R$ ein Primideal, so ist $P \neq R$ und somit $R/P \neq 0$. Gilt $[a][b] = 0$ für $a, b \in R/P$, so ist $ab \in P$, also entweder $a \in P$ oder $b \in P$. Das bedeutet, entweder $[a] = 0$ oder $[b] = 0$. Somit ist R/P nullteilerfrei. Sei umgekehrt R/P ein Integritätsbereich. Da $R/P \neq 0$ ist, gilt $R \neq P$. Ist $ab \in P$, so folgt $[a][b] = 0$. Da R/P nullteilerfrei ist, folgt $[a] = 0$ oder $[b] = 0$. Das bedeutet, $a \in P$ oder $b \in P$.

Zu (2): Für jedes Ideal $I \supseteq M$ ist das Bild $\pi(I)$ unter der Restklassenabbildung $\pi\colon R \to R/M$ ein Ideal in R/M. Umgekehrt ist für jedes Ideal $J \subseteq R/M$ das Urbild $\pi^{-1}(J)$ ein Ideal in R, das M enthält. Dann sind

$$\begin{aligned} \{\text{Ideale } I \subseteq R \text{ mit } M \subseteq I\} &\longleftrightarrow \{\text{Ideale } J \subseteq R/M\} \\ I &\mapsto \pi(I) \\ \pi^{-1}(J) &\mapsfrom J \end{aligned}$$

zueinander inverse Bijektionen. Ist R/M ein Körper, so hat R/M nur die zwei Ideale 0 und R/M. In der Tat, jeder Körper K hat nur die beiden Ideale 0 und K, weil jedes Ideal $I \neq 0$ ein $a \neq 0$ enthält, also auch $1 = aa^{-1}$ enthält, und somit $I = (1) = R$ gilt. Mit den obigen Bijektionen folgt

daraus, dass M ein maximales Ideal in R ist.

Ist umgekehrt M ein maximales Ideal von R, so ist R/M nicht der Nullring. Mit der obigen Bijektion folgt, dass R/M nur die Ideale 0 und R/M besitzt. Jeder Ring S, der nicht der Nullring ist und nur die Ideale 0 und S besitzt ist ein Körper, weil jedes $s \neq 0$ in S invertierbar ist. Denn (s) ist ein Ideal ungleich Null, also $(s) = S$, und somit $sx = 1$ für ein $x \in S$. Also ist R/M ein Körper. □

Beispiel 3.6.3. *Der Ring $\mathbb{Z}/mZ$ ist genau dann ein Körper, wenn m eine Primzahl ist. Wir schreiben dann $m = p$ und $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.*

Ist $m = p$ prim, so ist $p\mathbb{Z}$ ein maximales Ideal in $\mathbb{Z}$. Also ist $Z/p\mathbb{Z}$ ein Körper. Ist m nicht prim, so ist $\mathbb{Z}/m\mathbb{Z}$ nicht nullteilerfrei, und daher kein Körper.

Korollar 3.6.4. *Jedes maximale Ideal in R ist ein Primideal.*

Beweis. Ist M ein maximales Ideal in R, so ist R/M ein Körper, also insbesondere ein Integritätsring. Somit ist M prim. □

Tatsächlich ist es nicht so klar, dass ein Ring R (immer kommutativ) überhaupt ein maximales Ideal besitzt. Um das zu zeigen, braucht man das Zornsche Lemma.

Satz 3.6.5. *Jeder Ring $R \neq 0$ besitzt ein maximales Ideal.*

Beweis. Die Menge $\mathcal{M}$ aller Ideale $I \neq (1)$ in R ist nicht leer, da $(0) \in \mathcal{M}$. Sie ist durch die Inklusionsrelation geordnet. Um Zorns Lemma anzuwenden, müssen wir zeigen, dass jede Kette in $\mathcal{M}$ eine obere Schranke in $\mathcal{M}$ hat. Sei T also eine Kette von Idealen $I \neq (1)$. Dann betrachte man

$$J := \bigcup_{I \in T} I.$$

Dann ist J ein Ideal in R, denn für alle $x, y \in J$ existiert ein $I \in T$ mit $x, y \in I$. Da I ein Ideal ist, folgt $x - y \in I$ und $rx \in I$ für alle $r \in R$. Weiterhin gilt $1 \notin J$, da $1 \notin I$ für alle $I \in T$. Also gilt $J \in \mathcal{M}$, und J ist offensichtlich eine obere Schranke der Kette T. Aus Zorns Lemma folgt die Existenz eines maximalen Elementes für $\mathcal{M}$. □

Korollar 3.6.6. *Sei I ein echtes Ideal in R. Dann gibt es ein maximales Ideal M in R mit $I \subseteq M$.*

Beweis. Man betrachte im obigen Satz den Ring R/I und verwende die Bijektion aus dem Beweis von (2) in Satz 3.6.2. □

3.7 Bruchringe und Quotientenkörper

In der kommutativen Algebra werden sogenannte *Lokalisierungen* eines Ringes R bezüglich einer multiplikativ abgeschlossenen Teilmenge S studiert. Man erhält einen neuen Ring $S^{-1}R$, in dem die Elemente von S invertierbar sind. Er heißt auch *Ring der Brüche*. Ist R ein Integritätsring, so erhält man mit $S = R \setminus 0$ den sogenannten *Quotientenkörper* von R. Für $R = \mathbb{Z}$ ist das genau die Konstruktion, aus der man $\mathbb{Q}$ erhält.

Definition 3.15. Eine Teilmenge S von R heißt *multiplikativ abgeschlossen*, wenn gilt

(1) $1 \in S$,

(2) Aus $a \in S$, $b \in S$ folgt $ab \in S$.

Beispiel 3.7.1. 1. *Sei I ein Ideal in R. Dann ist $R \setminus I$ genau dann multiplikativ abgeschlossen, wenn I ein Primideal ist.*

2. *Ist R ein Integritätsring, so ist $R \setminus 0$ multiplikativ abgeschlossen.*

3. *Die Menge aller Nicht-Nullteiler in R ist multiplikativ abgeschlossen.*

4. *Die Menge aller Einheiten in R ist multiplikativ abgeschlossen.*

Sei S eine multiplikative abgeschlossenen Teilmenge von R. Wir definieren eine Relation auf der Menge aller geordneten Paare von $R \times S$ wie folgt. Für zwei Paare $(a, s), (b, t) \in R \times S$ sei

$$(a, s) \sim (b, t) \Longleftrightarrow (at - bs)u = 0 \text{ für irgendein } u \in S.$$

Lemma 3.7.2. *Die Relation $\sim$ definiert eine Äquivalenzrelation auf $R \times S$.*

Beweis. Es ist klar, dass $(a, s) \sim (a, s)$ gilt, und $(a, s) \sim (b, t)$ auch $(b, t) \sim (a, s)$ impliziert. Es ist also nur die Transitivität zu zeigen. Es gelte also $(a, s) \sim (b, t)$ und $(b, t) \sim (c, r)$. Es existieren also $v, w \in S$ mit

$$(at - bs)v = 0, \quad (br - ct)w = 0.$$

Daraus folgt

$$(at - bs)rvw = 0, \quad (br - ct)svw = 0,$$

und damit $atrvw = bsrvw = ctsvw$, so dass

$$(ar - cs)tvw = 0.$$

Da S multiplikativ abgeschlossen ist, haben wir $tvw \in S$, also $(a, s) \sim (c, r)$. □

Wir schreiben einfach $\frac{a}{s}$ für die Äquivalenzklasse von (a, s).

Definition 3.16. Der *Ring der Brüche* bezüglich S ist der Ring

$$S^{-1}R := \{a/s \mid (a, s) \in R \times S\},$$

wobei die Addition und die Multiplikation auf $S^{-1}R$ durch

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st},$$
$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

gegeben sind.

Bemerkung 3.7.3. Addition und Multiplikation sind wohldefiniert, d.h. hängen nicht von der Wahl der Vertreter (a, s) und (b, t) ab. Das Nachrechnen der Ringaxiome ist Routine. Der Ring $S^{-1}R$ hat das Nullelement $\frac{0}{1}$ und das Einselement $\frac{1}{1}$. Die Abbildung $\varphi\colon R \to S^{-1}R$ mit $r \mapsto \frac{r}{1}$ ist ein Ringhomomorphismus mit Kern

$$\ker(\varphi) = \{r \in R \mid \text{ es existiert ein } s \in S \text{ mit } rs = 0\ \}.$$

Es gilt genau dann $S^{-1}R = 0$ wenn $0 \in S$.

Definition 3.17. Sei R ein Integritätsring. Dann ist $S = R\backslash 0$ multiplikativ abgeschlossen und $S^{-1}R$ ein Körper. Er heißt der *Quotientenkörper* von R und wird mit $Quot(R)$ bezeichnet.

Die Abbildung $\varphi\colon R \to S^{-1}R$ ist dann injektiv, da S keine Nullteiler enthält. Also kann man R mit seinem Bild in $S^{-1}R$ identifizieren. Wie schon erwähnt ist $Quot(\mathbb{Z}) = \mathbb{Q}$. Ein anderes Beispiel ist $Quot(\mathbb{Z}[i]) = \mathbb{Q}(i)$.

3.8 Teilbarkeit und faktorielle Ringe

In der elementaren Zahlentheorie wurde die eindeutige Primfaktorzerlegung von ganzen Zahlen studiert. Solche Zerlegungen sind nicht nur für den Ring $\mathbb{Z}$ interessant, sondern auch allgemein für Integritätsringe. Allerdings haben Primfaktorzerlegungen dort nicht immer so schöne Eigenschaften wie in $\mathbb{Z}$.

Definition 3.18. Sei R ein Integritätsring.

(1) Für Elemente $a, b \in R$ sagt man a *teilt* b, oder $a \mid b$, falls es ein $c \in R$ gibt mit $ac = b$.

(2) Zwei Elemente $a, b \in R$ heißen *assoziiert*, oder $a \sim b$, falls $a \mid b$ und $b \mid a$ gilt.

(3) Ein Element $p \in R$ heißt *prim* oder *Primelement*, falls $p \neq 0$ und p keine Einheit ist, und für alle $a, b \in R$ mit $p \mid ab$ folgt $p \mid a$ oder $p \mid b$.

(4) Ein Element $u \in R$ heißt *irreduzibel*, falls $u \neq 0$ und u keine Einheit ist, und aus einer Darstellung $u = ab$ mit $a, b \in R$ immer folgt, dass a oder b eine Einheit ist.

Beispiel 3.8.1. *Für $R = \mathbb{Z}$ sind die Primelemente genau alle Zahlen $\{\pm p\}$, wobei p eine Primzahl ist. Ebenso sind auch alle irreduziblen Elemente gegeben. Die Begriffe prim und irreduzibel sind also äquivalent in $\mathbb{Z}$.*

Zwei ganze Zahlen m und n sind genau dann assoziiert, wenn $m = \pm n$ gilt, d.h., wenn sie sich durch eine Einheit in $\mathbb{Z}$ unterscheiden. Sind allgemein $a, b \in R$ assoziiert, so gilt $a = \mu b$ und $b = \nu a$ für $\mu, \nu \in R$, also $b = \nu\mu b$, und somit $b(1 - \nu\mu) = 0$. Ist $b \neq 0$, so sind μ, ν Einheiten. Für $b = 0$ ist $a = 0$ und $b = 1 \cdot a$. Also gilt

$$a \sim b \Longleftrightarrow a = \mu b \text{ mit einer Einheit } \mu.$$

Ein Körper hat gar keine Primelemente, da alle Elemente ungleich Null Einheiten sind. Ebenso hat er auch keine irreduziblen Elemente.

Wir können obige Begriffe auch idealtheoretisch beschreiben.

Lemma 3.8.2. *Sei R ein Integritätsring.*

(1) Es gilt $(a) \supseteq (b) \Longleftrightarrow a \mid b$. "To contain is to divide".

(2) Es gilt $a \sim b \iff (a) = (b)$.

(3) Ein Element $p \in R$ *ist genau dann prim, wenn* $p \neq 0$ *und* (p) *ein Primideal in* R *ist.*

(4) Ist R *ein Hauptidealring, dann ist ein Element* $u \in R$ *genau dann irreduzibel, wenn* (u) *ein maximales Ideal in* R *ist.*

Beweis. Wir überlassen $(1) - (3)$ dem Leser. (4) folgt aus (1), weil in einem Hauptidealring jedes Ideal von der Form (a) ist. Also ist (a) genau dann maximal wenn a keine nicht-trivialen Teiler hat, genau dann wenn a irreduzibel ist. □

Das folgende Beispiel zeigt, dass (4) nicht in jedem Integritätsring gelten muss.

Beispiel 3.8.3. *Das Polynom* X *in* $R = \mathbb{Z}[X]$ *ist ein irreduzibles Element, aber das Ideal* (X) *ist nicht maximal.*

In der Tat, da $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$ kein Körper ist, kann (X) kein maximales Ideal sein. Die Aussage in (4) kann verbessert werden, idem man sagt, dass ein Element $r \in R$ genau dann irreduzibel ist, wenn das Ideal (a) maximal unter den Hauptidealen in R ist. Für Hauptidealringe sind die Begriffe prim und irreduzibel sogar äquivalent.

Satz 3.8.4. *Sei* R *ein Integritätsring.*

(1) Jedes Primelement in R *ist irreduzibel.*

(2) In einem Hauptidealring R *ist ein Element genau dann prim wenn es irreduzibel ist.*

(3) In einem Hauptidealring R *ist ein Ideal ungleich Null genau dann prim wenn es maximal ist.*

Beweis. Zu (1). Sei p ein Primelement in R und $p = ab$. Dann gilt $a \mid p$ und $b \mid p$. Da p prim ist, folgt auch $p \mid a$ oder $p \mid b$. Im ersten Fall ist $p \sim a$ und deshalb $b \in R^\times$, und im zweiten Fall $p \sim b$, also $a \in R^\times$. Also ist p irreduzibel.

Zu (2). Sei $u \in R$ irreduzibel. Wegen Lemma 3.8.2, (4) für Hauptidealringe

ist (u) ein maximales Ideal, also auch ein Primideal. Somit ist u ein Primelement. Die Umkehrung gilt allgemein wegen (1).

Zu (3). Das folgt aus Lemma 3.8.2, (3) und (4). □

Satz 3.8.5. *Der Polynomring $R[X]$ ist genau dann ein Hauptidealring, wenn R ein Körper ist.*

Beweis. Die Abbildung $R[X] \to R$, $f \mapsto f(0)$ ist ein Ringepimorphismus mit Kern (X). Nach dem Isomorphiesatz gilt also $R[X]/(X) \cong R$. Sei $R[X]$ ein Hauptidealring. Dann ist das Ideal $I = (X)$ prim, da $R[X]/(X) \cong R$ als Unterring von $R[X]$ selbst ein Integritätsring ist. Wegen 3.8.4, (2) ist (X) auch maximal, und somit $R/I \cong R$ ein Körper. Umgekehrt sei R ein Körper. Dann ist $R[X]$ ein Euklidischer Ring mit der Gradfunktion $d(f) = \deg(f)$, also auch ein Hauptidealring, siehe Satz 3.4.2. □

Definition 3.19. Sei R ein Integritätsring und $a, b \in R$.

(1) Ein *größter gemeinsamer Teiler*, oder ein *ggT* von a und b ist ein $d \in R$ mit $d \mid a$, $d \mid b$ und der Eigenschaft, dass für alle $r \in R$ mit $r \mid a$, $r \mid b$ folgt $r \mid d$. Wir schreiben $d = \gcd(a, b)$.

(2) Ein *kleinstes gemeinsames Vielfaches*, oder ein *kgV* von a und b ist ein $v \in R$ mit $a \mid v$, $b \mid v$, und der Eigenschaft, dass für alle $s \in R$ mit $a \mid s$, $b \mid s$ folgt $v \mid s$. Wir schreiben $v = \mathrm{l}cm(a, b)$.

Satz 3.8.6. *Sei R ein Integritätsring und $a, b \in R$.*

(1) Falls es in R einen ggT von a und b gibt, so ist er bis auf eine Einheit eindeutig.

(2) Falls es ein $d \in R$ gibt mit $(d) = (a, b)$, so ist d ein ggT von a und b.

(3) Falls es in R ein kgV von a und b gibt, so ist es bis auf eine Einheit eindeutig.

(4) Falls es ein $v \in R$ gibt mit $(v) = (a) \cap (b)$, so ist v ein kgV von a und b.

Beweis. Zu (1). Sind d und e zwei ggTs, so gilt $d \mid e$ und $e \mid d$. Damit gilt $d \sim e$, also $d = \mu e$ für eine Einheit μ.

Zu (2). Aus $(d) = (a, b)$ folgt $(a) \subseteq (d)$, $(b) \subseteq (d)$, also $d \mid a$, $d \mid b$. Wegen $d \in (a, b)$ gibt es $x, y \in R$ mit $d = xa + yb$. Gilt also $r \mid a$, $r \mid b$, so folgt $r \mid d$. Also ist d ein ggT von a und b.

Ähnlich zeigt man (3) und (4). □

Falls ein ggT oder kgV existiert, ist er also im wesentlichen eindeutig. Für Hauptidealringe haben wir folgdenes Resultat.

Satz 3.8.7. *Sei R ein Hauptidealring und $a, b \in R$. Dann gibt es einen ggT $d = \gcd(a, b)$ und es gilt $(d) = (a, b) = (a) + (b)$. Ebenso gibt es ein kgV $v = \mathrm{lcm}(a, b)$ und es gilt $(v) = (a) \cap (b)$.*

Beweis. Da R ein Hauptidealring ist, gibt es zu dem Ideal (a, b) ein $d \in R$ mit $(d) = (a, b)$. Wegen 3.8.6, (2) ist d ein ggT von a und b. Nach Definition ist (a, b) das kleinste Ideal das a und b enthält. Also gilt in jedem Ring $(a, b) = (a) + (b)$.

Da auch das Ideal $(a) \cap (b)$ ein Hauptideal ist, gibt es ein $v \in R$ mit $(v) = (a) \cap (b)$. Wegen 3.8.6, (4) ist v ein kgV von a und b. □

Definition 3.20. Zwei Elemente $a, b \in R$ heißen *teilerfremd*, falls 1 ein ggT von a und b ist. Zwei Ideale I und J in einem Ring heißen *teilerfremd*, falls $I + J = R$ gilt.

Aus Satz 3.8.7 folgt

Satz 3.8.8. *Sei R ein Hauptidealring. Dann sind a und b aus R genau dann teilerfremd, wenn die Ideale (a) und (b) teilerfremd sind. In diesem Fall gibt es $r, s \in R$ mit $ra + sb = 1$.*

Definition 3.21. Ein *faktorieller Ring* ist ein Integritätsring R, in dem sich jedes Element $a \in R$ mit $a \neq 0$, $a \notin R^\times$ als ein endliches Produkt von Primelementen schreiben läßt.

Wir nennen diese Darstellung als Produkt von Primelementen eine *Primfaktorzerlegung*. Das leere Produkt ist dabei eingeschlossen, also ist ein Körper auch ein faktoreller Ring. Er hat keine Nicht-Einheiten ungleich Null.

Bemerkung 3.8.9. Man kann leicht zeigen, dass Primfaktorzerlegungen, wenn sie existieren, *eindeutig* in folgendem Sinne sind. Gilt

$$\prod_{i=1}^{n} p_i = \prod_{j=1}^{m} q_j$$

mit Primelementen $p_i, q_j \in R$, so folgt $m = n$ und es gibt eine Permutation $\sigma \in S_n$ und Einheiten ε_i in R mit $p_j = \varepsilon_j \cdot q_{\sigma(j)}$ für alle $j = 1, \ldots, n$.

Satz 3.8.10. *Ein Integritätsring R is genau dann faktoriell, wenn sich jedes Element $r \neq 0, r \notin R^\times$ als ein endliches Produkt von irreduziblen Elementen schreiben läßt, und diese Zerlegung bis auf Reihenfolge und Einheiten eindeutig ist.*

Beweis. Sei R faktoriell und $r \neq 0$ keine Einheit. Dann existiert eine eindeutige Zerlegung in Primelemente, d.h., $r = p_1 \cdots p_n$. Jedes Primelement ist aber irreduzibel nach Satz 3.8.4. Also erhalten wir eine eindeutige Zerlegung in irreduzible Elemente. Hat jedes Element eine Zerlegung in irreduzible Elemente, dann ist jedes irreduzible Element u auch prim. Denn hat man $u \mid ab$, so gibt es ein $c \in R$ mit $uc = ab$. Nun ersetze man a, b, c durch eine Zerlegung in irreduzible Elemente, d.h.,

$$a = p_1 \cdots p_r,\ b = q_1 \cdots q_s,\ c = r_1 \cdots r_t.$$

Dann erhält man aber auf beiden Seiten von $uc = ab$ im wesentlichen die gleiche Zerlegung, wegen der Eindeutigkeit der Zerlegungen,

$$ur_1 \cdots r_t = p_1 \cdots p_r \cdot q_1 \cdots q_s.$$

Also ist $u = p_i$ für ein i, oder $u = q_j$ für ein j und es folgt entweder $u \mid a$ oder $u \mid b$. Somit ist u auch prim und R faktoriell. □

Korollar 3.8.11. *Sei R ein faktorieller Ring. Dann ist ein Element $a \in R$ genau dann prim wenn es irreduzibel ist.*

Beispiel 3.8.12. 1. *Jeder Körper ist ein faktorieller Ring.*

2. *$\mathbb{Z}$ ist ein faktorieller Ring.*

3. *$\mathcal{O}_{-5} = \mathbb{Z}[\sqrt{-5}]$ ist kein faktorieller Ring.*

Zu 3. Sei $R = \mathcal{O}_{-5}$. Die Normabbildung $N\colon \mathcal{O}_d \to \mathbb{Z}$ ist durch

$$N(z) = z\overline{z} = (a + b\sqrt{-5})(a - \sqrt{-5}) = a^2 + 5b^2$$

gegeben. Es ist leicht zu sehen, dass z eine Einheit ist, genau dann wenn $N(z) = 1$ gilt. Das bedeutet, $R^\times = \{\pm 1\}$. Das Element $z = 6$ hat folgende Zerlegungen in irreduzible Elemente,

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

Nun ist 2 kein Primelement, denn $2 \mid 6$, aber 2 teilt keinen der beiden Faktoren $1 \pm \sqrt{-5}$. Dazu bemerkt man, dass aus $z \mid w$ in R folgt $N(z) \mid N(w)$ in $\mathbb{Z}$. Aber

$$N(2) = 4 \nmid 6 = N(1 \pm \sqrt{-5}).$$

Andererseits ist 2 aber irreduzibel. Angenommen $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$, und ein Faktor, sagen wir der erste, wäre keine Einheit, d.h., $a^2 + 5b^2 \neq 1$. Dann gilt $(a + b\sqrt{-5}) \mid 2$ in R, also $a^2 + 5b^2 \mid 4$ in $\mathbb{Z}$. Dann bleibt nur $4 = 2 \cdot 2$ und $a^2 + 5b^2 = 2$, was aber keine Lösung in $\mathbb{Z}$ hat, ein Widerspruch. Wegen Korollar 3.8.11 kann R also nicht faktoriell sein.

Lemma 3.8.13. *Sei R ein faktorieller Ring. Dann gibt es zu gegebenem $a \neq 0$ in R nur endlich viele verschiedene Hauptideale (b) mit $(b) \supseteq (a)$ in R.*

Beweis. Ist a eine Einheit, so ist $(a) = R$ und die Aussage klar. Andernfalls hat man eine Zerlegung $a = u_1 \cdots u_n$ in irreduzible Elemente. Für $(b) \supseteq (a)$ gilt $b \mid a$, also $a = bq$ mit einem $q \in R$. Wegen der Eindeutigkeit der Zerlegung muss es $1 \leq i_1 < \cdots < i_m \leq n$ geben mit $b \sim u_{i_1} \cdots u_{i_m}$. Das sind nur endlich viele Möglichkeiten für (b). □

Satz 3.8.14. *Ein Integritätsbereich R ist genau dann ein faktorieller Ring, wenn jedes irreduzible Element prim ist und jede aufsteigene Kette von Hauptidealen*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

stationär wird.

Beweis. Sei R ein faktorieller Ring. Dann ist nach Korollar 3.8.11 jedes irreduzible Element prim. Wegen Lemma 3.8.13 wird jede aufsteigende Kette

von Hauptidealen stationär.

Sei umgekehrt R ein Integritätsring mit aufsteigender Kettenbedingung für Hauptideale. Betrachte die Menge H aller Hauptideale (a) in R mit $a \neq 0$, $a \notin R^\times$, so dass a kein Produkt von irreduziblen Elementen ist. Wir müssen zeigen, dass $H = \emptyset$ ist und nehmen das Gegenteil an. Dann enthält H ein maximales Element I, denn andernfalls hätte man zu jedem $J_1 \in H$ ein $J_2 \in H$ mit $J_1 \subsetneq J_2$, und so durch Fortsetzen des Verfahrens eine aufsteigende Kette von Hauptidealen, die nicht stationär wäre. Sei $I = (a)$ für ein $a \in R$. Dann ist $a \neq 0$, keine Einheit und muss reduzibel sein. Also gibt es Nicht-Einheiten $b, c \in R$ mit $a = bc$. Man erhält echte Inklusionen $(a) \subsetneq (b)$ und $(a) \subsetneq (c)$. Also gehören wegen der Maximalität von (a) die Ideale (b) und (c) nicht zu H. Also sind b und c das Produkt irreduzibler Elemente, und somit auch $a = bc$. Das ist ein Widerspruch zu $(a) \in H$. Also ist H leer. □

Die aufsteigende Kettenbedingung kann man überhaupt für *alle* Ideale in einem beliebigen Ring fordern. Dann erhält man eine weitere wichtige Klasse von Ringen.

Definition 3.22. Ein Ring R heißt *Noethersch*, wenn jede aufsteigende Kette von Idealen

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

stationär wird.

Satz 3.8.15. *Sei R ein Ring. Dann sind die folgenden Aussagen äquivalent.*

(1) R ist Noethersch.

(2) Jede nicht-leere Menge von Idealen in R hat ein maximales Element bezüglich Inklusion.

(3) Jedes Ideal in R ist endlich erzeugt.

Beweis. (1) $\Rightarrow$ (2): Ist M eine nicht-leere Menge von Idealen, die kein maximales Element hat, so gibt es zu jedem $I_1 \in M$ ein $I_2 \in M$ mit $I_1 \subsetneq I_2$. Somit erhält man eine aufsteigende Kette von Idealen, die nicht stationär wird, im Widerspruch zur Annahme. Also folgt (2).

(2) $\Rightarrow$ (3): Sei I ein Ideal in R und $\mathcal{M}$ die Menge aller Ideale in R, die

endlich erzeugt sind und in I enthalten sind. Dann ist $\mathcal{M}$ nicht-leer. Sei M ein maximales Element in $\mathcal{M}$ und $a \in I$. Dann gilt $(a) + M \in \mathcal{M}$ und $M \subseteq (a) + M$. Wegen der Maximalität folgt $M = (a) + M$, also $a \in M$. Also ist $I \subseteq M \subseteq I$, d.h., $I = M$. Da M nach Definition von $\mathcal{M}$ endlich erzeugt ist, folgt (3).

(3) $\Rightarrow$ (1): Ist $I_1 \subseteq I_2 \subseteq I_2 \subseteq \cdots$ eine aufsteigende Kette von Idealen in R, so ist ihre Vereinigung I wieder ein Ideal. Es ist endlich-erzeugt nach Voraussetzung, d.h., $I = (a_1, \ldots, a_m)$. Zu jedem $1 \leq j \leq m$ existiert ein n_j mit $a_j \in I_{n_j}$. Ist n_0 die größte der Zahlen n_j, so gilt $I = I_{n_0}$, und die Kette wird stationär. Also folgt (1). □

Korollar 3.8.16. *Jeder Hauptidealring ist faktoriell und Noethersch. Wir haben die Implikationen*

$$\textit{Euklidisch} \implies \textit{Hauptidealring} \implies \textit{faktoriell}$$

Beweis. Sei R ein Hauptidealring. Nach Satz 3.8.4 ist jedes irreduzible Element prim. Offensichtlich ist jedes Ideal in R von einem Element erzeugt. Nach (3) des obigen Satzes 3.8.15 ist R also Noethersch. Somit ist R faktoriell nach Satz 3.8.14. Euklidische Ringe sind Hauptidealringe nach Satz 3.4.2, und deshalb faktoriell. □

Beispiel 3.8.17. *Alle Ringe $\mathcal{O}_d$ mit*

$$d = -163, -67, -43, -19, -11, -7, -3, -2, -1, 1, 2, 3, 5, 6, 7, 11, 13, 14, \ldots$$

sind faktoriell, siehe Theorem 3.4.8.

Bemerkung 3.8.18. Die Umkehrungen der Implikationen aus Korollar 3.8.16 gelten im allgemeinen nicht. Wir werden noch sehen, dass $\mathbb{Z}[X]$ ein faktorieller Ring ist. Er ist aber kein Hauptidealring, da $\mathbb{Z}$ kein Körper ist, siehe Satz 3.8.5. Allerdings, Ganzzahlringe in Zahlkörpern sind genau dann faktoriell, wenn sie Hauptidealringe sind. Das gilt insbesondere für die Ringe $\mathcal{O}_d$.

3.9 Der Satz von Gauß

Der Satz von Gauß besagt, dass der Poylnomring $R[X]$ über einem faktoriellen Ring R wieder faktoriell ist. Für $R = \mathbb{Z}$ erhält man also, dass

der Ring $\mathbb{Z}[X]$ faktoriell ist. Der Beweis führt über den Quotientenkörper $K = Quot(R)$. Da $K[X]$ ein Hauptidealring ist wegen Satz 3.8.5, ist er auch faktoriell. Die kanonische Einbettung von R nach K liefert eine Einbettung von $R[X]$ nach $K[X]$. Allerdings muß man nun überlegen, wie man aus Primfaktorzerlegungen in $K[X]$ solche in $R[X]$ erhalten kann. Sei $p \in R$ prim. Man betrachte die Abbildung (Bewertung) $\nu_p \colon R \to \mathbb{N} \cup \{\infty\}$,

$$x \mapsto \sup\{n \in \mathbb{N} \mid p^n \mid x\}.$$

Definition 3.23 (Primbewertungen auf Quotientenkörpern)**.** Sei R ein faktorieller Ring mit Quotientenkörper K und $p \in R$ prim. Man setze die Abbildung ν_p auf K fort durch

$$\nu_p\left(\frac{a}{b}\right) = \nu_p(a) - \nu_p(b) \in \mathbb{Z} \cup \{\infty\}$$

für eine Klasse $\frac{a}{b} \in K$. Für $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ definiere man

$$\nu_p(f) = \min\{\nu_p(a_i) \mid i = 0, \ldots, n\}.$$

Bemerkung 3.9.1. Für $f \in K[X]$ gilt $f \in R[X] \subseteq K[X]$ genau dann, wenn $\nu_p(f) \geq 0$ für alle Primelemente $p \in R$.

Lemma 3.9.2 (Lemma von Gauß)**.** *Sei R ein faktorieller Ring mit Quotientenkörper K und $p \in R$ prim. Dann gilt für alle $f, g \in K[X]$*

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

Sind zudem f, g beide normiert und $fg \in R[X]$, so folgt $f, g \in R[X]$.

Beweis. 1. Die "Gradgleichung"gilt offensichtlich für $f, g \in K$, wie man leicht mit der Primfaktorzerlegung von Zähler und Nenner nachrechnet.

2. Sei $S = \{0, 1, \ldots, n\}$. Ist $f \in K$ und $g = \sum_{j=0}^{n} b_j X^j \in K[X]$, so folgt

$$\begin{aligned}
\nu_p(fg) &= \nu_p\left(\sum_{j=0}^{n} f b_j X^j\right) \\
&= \min\{\nu_p(f b_j) \mid j \in S\} \\
&= \min\{\nu_p(f) + \nu_p(b_j) \mid j \in S\} \\
&= \nu_p(f) + \min\{\nu_p(b_j) \mid j \in S\} \\
&= \nu_p(f) + \nu_p(g).
\end{aligned}$$

3. Wir zeigen nun, dass die Gradformel für $f, g \in R[X]$ mit $\nu_p(f) = \nu_p(g) = 0$ gilt. Die natürliche Projektion $R \to R/(p)$ induziert einen Ringhomomorphismus

$$\pi\colon R[X] \to R/(p)[X].$$

Da p prim ist, ist (p) ein Primdeal in R und daher $R/(p)$ ein Integritätsring, wegen Satz 3.6.2. Nach Korollar 3.5.2 ist dann auch $R/(p)[X]$ ein Integritätsring. Nach Konstruktion gilt

$$\ker(\pi) = \{h \in R[X] \mid \nu_p(h) > 0\}.$$

Wegen $\nu_p(f) = \nu_p(g) = 0$ gilt $\pi(f), \pi(g) \neq 0$. Da $R/(p)[X]$ nullteilerfrei ist, folgt $\pi(fg) \neq 0$, also $fg \notin \ker(\pi)$, und deshalb $\nu_p(fg) = 0$. Damit gilt die Gradgleichung auch in diesem Fall.

4. Nun können wir den allgemeinen Fall behandeln. Seien $f, g \in K[X]$. Dann gibt es Elemente $c, d \in K^\times$ mit $cf, dg \in R[X]$ und $\nu_p(cf) = \nu_p(dg) = 0$. Man kann zum Beispiel mit dem Produkt aller Nenner multiplizieren und durch geeignete p-Potenzen dividieren. Mit den vorangegangenen Fällen folgt nun

$$\begin{aligned}
\nu_p(cd) + \nu_p(fg) &\overset{2.}{=} \nu_p(cdfg) \\
&= \nu_p(cf \cdot dg) \\
&\overset{3.}{=} \nu_p(cf) + \nu_p(dg) \\
&\overset{2.}{=} \nu_p(c) + \nu_p(f) + \nu_p(d) + \nu_p(g) \\
&\overset{1.}{=} \nu_p(cd) + \nu_p(f) + \nu_p(g).
\end{aligned}$$

Das ergibt die Behauptung.

Da f, g normiert sind, folgt $\nu_p(f), \nu_p(g) \leq 0$, und fg ist ebenfalls normiert. Da die Koeffizienten von fg sogar in R liegen, gilt $\nu_p(fg) = 0$. Also liefert die Gradgleichung

$$0 = \nu_p(fg) = \nu_p(f) + \nu_p(g),$$

und somit $\nu_p(f) = \nu_p(g) = 0$. Da dies für alle Primelemente p gilt, folgt, dass in f und g keine echten Nenner auftreten können. Also gilt $f, g \in R[X]$. □

Definition 3.24. Sei R ein faktorieller Ring. Ein Polynom f in $R[X]$ heißt *primitiv*, wenn $\nu_p(f) = 0$ für alle Primelemente $p \in R$ gilt.

Bemerkung 3.9.3. Ist $f \in R[X]$, so heißt

$$c(f) = \prod_p p^{\nu_p(f)}$$

der *Inhalt* von f. Dabei läuft das Produkt über ein Repräsentantensystem von Primelementklassen, mit genau einem Primelement in der Äquivalenzklasse bezüglich Assoziiertheit. Ein Polynom f ist genau dann primitiv, wenn sein Inhalt 1 ist.

Lemma 3.9.4. *Sei R ein faktorieller Ring mit Quotientenkörper K. Dann gelten die folgenden Aussagen.*

(1) Ist $q \in R$ prim in R, so auch in $R[X]$.

(2) Ist $q \in R[X]$ primitiv und prim in $K[X]$, so ist q schon prim in $R[X]$.

(3) Jedes Polynom $f \neq 0$, f keine Einheit in $R[X]$ ist ein Produkt von Primelementen von R und von primitiven Polynomen in $R[X]$, die prim in $K[X]$ sind.

Beweis. Zu (1). Wie wir im Beweis von Lemma 3.9.2 gesehen haben, ist $R/(q)[X]$ ein Integritätsring, da q prim in R ist. Der kanonische Ringhomomorphismus

$$R[X]/(q) \to R/(q)[X],$$

der $r + qR[X]$ auf $r + qR$ abbildet für $r \in R$, und $[X]$ auf X, zeigt, dass auch $R[X]/(q)$ ein Integritätsring ist. Also ist das von q erzeugte Ideal in $R[X]$ prim. Dann ist q prim in $R[X]$ wegen Lemma 3.8.2.

Zu (2). Sei $q \in R[X]$ primitiv und prim in $K[X]$. Seien $f, g \in R[X]$ mit $q \mid fg$. Dann ist q auch auch in $K[X]$ ein Teiler von fg. Da q prim in $K[X]$ ist, ist q ein Teiler von f oder g in $K[X]$. Ohne Einschränkung gelte $q \mid f$, d.h., es gibt ein $h \in K[X]$ mit $f = qh$. Da q primitiv ist und wegen Lemma 3.9.2 gilt

$$\begin{aligned} \nu_p(h) &= \nu_p(qh) - \nu_p(q) \\ &= \nu_p(f) - \nu_p(q) \\ &= \nu_p(f) \geq 0. \end{aligned}$$

Also ist $h \in R[X]$, siehe Bemerkung 3.9.1. Insbesondere ist q ein Teiler von f in $R[X]$. Somit ist q prim in $R[X]$.

Zu (3). Sei $f \neq 0$ in $R[X]$. Wir dürfen annehmen, dass f primitiv ist. Ansonsten multiplizieren wir den größten gemeinsamen Teiler der Koeffizienten von f aus und erhalten eine Zerlegung $f = cg$ mit $c \neq 0$ in R und einem primitiven Polynom $g \in R[X]$. Da R faktoriell ist, besitzt c eine Primfaktorzerlegung in R, wenn es nicht eine Einheit ist. Nach (1) ist eine solche Primfaktorzerlegung von c auch eine in $R[X]$. Sei also f jetzt primitiv mit $\deg(f) > 0$. Der Ring $K[X]$ ist als Hauptidealring über einem Körper faktoriell. Aufgefasst als Element von $K[X]$ besitzt f somit eine Primfaktorzerlegung der Form $f = p_1 \cdots p_n$ mit Primelementen $p_i \in K[X]$. Indem wir mit den Nennern der Koeffizienten dieser Polynome multiplizieren und jeweils durch den größten gemeinsamen Teiler der entstehenden Koeffizienten dividieren, erhalten wir $c_1, \ldots, c_n \in R \setminus 0$ und primitive Polynome $q_1, \ldots, q_n \in R[X]$ mit

$$f = \frac{q_1}{c_1} \cdots \frac{q_n}{c_n} = \frac{1}{c} \cdot q_1 \cdots q_n,$$

wobei $c = \frac{1}{c_1} \cdots \frac{1}{c_n}$. Da f und alle q_i primitiv sind, folgt aus Lemma 3.9.2

$$\begin{aligned} \nu_p(c) &= \nu_p(f) - \sum_{i=1}^{n} \nu_p(q_i) \\ &= 0 \end{aligned}$$

für alle Primelemente p in R. Also folgt $c \in R$. Da $\frac{1}{c} = c_1 \cdots c_n$ ist sogar $c \in R^\times$. Also ist

$$f = (cq_1) \cdots q_2 \cdots q_n$$

eine Faktorisierung der gewünschten Form. □

Aus diesem Lemma erhalten wir insbesondere, dass jedes nicht-triviale Element in $R[X]$ eine Primfaktorzerlegung besitzt. Also ist $R[X]$ faktoriell.

Theorem 3.9.5 (Satz von Gauß)**.** *Sei R ein faktorieller Ring. Dann ist auch $R[X]$ faktoriell.*

Beispiel 3.9.6. *Der Polynomring $(\mathbb{Z}[i])[X]$ ist faktoriell.*

In der Tat ist $\mathbb{Z}[i]$ Euklidisch, also ein Hauptidealring und ein faktorieller Ring.

Korollar 3.9.7. *Sei R ein faktorieller Ring mit Quotientenkörper K und sei $f \in R[X]$ ein primitives Polynom. Dann sind die folgenden Aussagen äquivalent.*

(1) Das Polynom f ist prim in $R[X]$.

(2) Das Polynom f ist irreduzibel in $R[X]$.

(3) Das Polynom f ist prim in $K[X]$.

(4) Das Polynom f ist irreduzibel in $K[X]$.

Beweis. In faktoriellen Ringen sind die Begriffe prim und irreduzibel nach Korollar 3.8.11 äquivalent. Der Ring $R[X]$ ist in der Tat faktoriell nach dem Satz von Gauss. Ebenso ist $K[X]$ ein faktorieller Ring. Also gelten (1) $\Leftrightarrow$ (2) und (3) $\Leftrightarrow$ (4).

(3) $\Leftrightarrow$ (1): Das folgt aus Lemma 3.9.4, (2).

(1) $\Leftrightarrow$ (3): Die Primfaktorzerlegung von f in $R[X]$ besteht, wie wir gesehen haben, aus Primelementen von R und primitiven Polynomen in $R[X]$, die prim in $K[X]$ sind. Da f in $R[X]$ prim ist, besteht diese Produktzerlegung aus nur einem Faktor. Da f primitiv ist, ist f kein Primelement von R. Also muß f ein Primelement von $K[X]$ sein. □

Bemerkung 3.9.8. Sei R ein faktorieller Ring. Der Satz von Gauß impliziert induktiv, dass auch der iterierte Polynomring $R[X_1, \ldots, X_n]$ ein faktorieller Ring ist. Hierbei ist $R[X_1, X_2] = (R[X_1])[X_2]$, und

$$R[X_1, \ldots, X_k] = (R[X_1, \ldots, X_{k-1}])[X_k]$$

für alle $k \geq 2$.

3.10 Irreduzibilitätskriterien für Polynome

Kriterien, die in gewissen Fällen die Irreduzibilität von Polynomen zeigen, sind unter anderem nützlich wegen der folgenden Konstruktion von neuen Körpern.

Satz 3.10.1. *Sei K ein Körper und $f \in K[X]$ ein irreduzibles Polynom. Dann ist der Restklassenring*

$$K[X]/(f)$$

ein Körper.

Beweis. Wegen Satz 3.8.5 ist $R = K[X]$ ein Hauptidealring. Aus Lemma 3.8.2 folgt, dass (f) ein maximales Ideal in R ist, da f irreduzibel ist. Wegen Satz 3.6.2, Teil (2) ist der Restklassenring $R/(f)$ deshalb ein Körper. □

Beispiel 3.10.2. *Das Polynom $X^2 + 1$ ist irreduzibel in $\mathbb{R}[X]$. Der Restklassenring ist isomorph zu $\mathbb{C}$,*

$$\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}.$$

Die Auswertungsabbildung $\mathbb{R}[X] \to \mathbb{C}$ mit $f \mapsto f(i)$ ist ein surjektiver Ringhomomorphismus, dessen Kern das Ideal ist, welches von dem Minimalpolynom von i erzeugt wird, also von $X^2 + 1$. Hierbei ist $\mathbb{R}[X]$ Euklidisch, also ein Hauptidealring. Deswegen folgt $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$ nach dem ersten Isomorphiesatz.

Bemerkung 3.10.3. Im allgemeinen ist $R[X]/(f)$ kein Körper, auch wenn f irreduzibel in R ist. Es gilt $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$, siehe Beispiel 3.8.3, welches kein Körper ist. Aber X ist irreduzibel in $\mathbb{Z}[X]$.

Theorem 3.10.4 (Nullstellenkriterium)**.** *Sei K ein Körper und $f \in K[X]$ mit $\deg(f) > 1$. Hat f eine Nullstelle in K, so ist f reduzibel in $K[X]$. Hat f Grad 2 oder 3, so ist f genau dann irreduzibel, wenn f keine Nullstelle in K hat.*

Beweis. Polynomdivision von f durch $X - a$ ergibt $f = q(X - a) + r$ mit eindeutig bestimmten $q, r \in K[X]$ und $\deg(r) < 1$. Nach Voraussetzung folgt $0 = f(a) = r$ und $f = (X - a)q$ ist in $K[X]$ reduzibel.
Für die zweite Behauptung nehme man an, f sei reduzibel. Also existieren $g, h \in K[X]$ mit $f = gh$, und g, h sind nicht Null und keine Einheiten in $K[X]$. Insbesondere ist $\deg(g) > 0$ und $\deg(h) > 0$. Wegen

$$\deg(g) + \deg(h) = \deg(gh) = \deg(f) \in \{2, 3\}$$

ist einer der beiden Grade gleich 1. Ohne Einschränkung sei $\deg(g) = 1$. Also ist $g = aX + b$ mit $a \neq 0$, und somit $f(-b/a) = g(-b/a)h(-b/a) = 0$. Also hat f eine Nullstelle in K. □

Für Polynome von Grad $n \geq 4$ gilt die Aussage im allgemeinen nicht mehr. So hat $f = (x^2+1)^2$ keine Nullstellen in $\mathbb{R}[X]$, ist aber reduzibel.

Korollar 3.10.5. *Sei K ein Körper und $f \in K[X]$ mit $f \neq 0$. Dann hat f höchstens* $\deg(f)$ *Nullstellen in K.*

Beweis. Sind $a_1, \ldots, a_n$ Nullstellen von f, dann folgt induktiv aus der Polynomdivision, dass

$$(X - a_1) \cdots (X - a_n) \mid f$$

gilt, wobei der Fall $n = 1$ im Beweis von 3.10.4 gezeigt wurde. Also gilt $n \leq \deg(f)$. □

Bemerkung 3.10.6. Die Aussage von Korollar 3.10.5 gilt auch für Polynome in $R[X]$, wobei R ein Integritätsring ist, aber nicht notwendig ein Körper. Zwar muß dann $R[X]$ kein Euklidischer Ring sein, aber die Polynomdivision für normierte Polynome gilt in jedem Ring R, siehe Satz 3.5.3. Damit kann man den Beweis mit Induktion auch für $R[X]$ machen. Allerdings benötigt man, dass R keine Nullteiler hat. Ist $f(a) = 0$ und $f = (X - a)q + f(a)$ mit $b \neq a$ und $f(b) = 0$, dann hat man $0 = f(b) = (b - a)q(b)$ und man möchte $q(b) = 0$ schließen für den Induktionsschritt. In der Tat, wenn R Nullteiler hat, so wird die Aussage falsch:

$$f = X^2 - 1$$

hat 4 Nullstellen in $R = \mathbb{Z}/8\mathbb{Z}$.

Sei f ein reduzibles Polynom in $R[X]$. Dann hat man $f = gh$ mit $g, h \in R[X]$. Im allgemeinen kann man nicht schliessen, dass $\deg(g) > 0$ und $\deg(h) > 0$ gilt. Zum Beispiel ist $f = 2(X + 1) \in \mathbb{Z}[X]$ reduzibel, weil 2 keine Einheit ist. Ist f allerdings primitiv, also etwa ein normiertes Polynom, so folgt die Aussage. Das werden wir im Beweis des folgenden Resultates brauchen.

Theorem 3.10.7 (Reduktionskriterium)**.** *Sei R ein faktorieller Ring mit Quotientenkörper K, p ein Primelement in R und $\pi\colon R[X] \to R/(p)[X]$ der von der kanonischen Projektion $R \to R/(p)$ induzierte Ringhomomorphismus. Sei $f \in R[X]$ ein Polynom vom Grad* $\deg(f) > 0$*, dessen Leitkoeffizient nicht durch p teilbar ist. Dann gelten folgende Aussagen.*

(1) Ist f primitiv und $\pi(f)$ in $R/(p)[X]$ irreduzibel, so ist f in $R[X]$ irreduzibel.

(2) Ist $\pi(f)$ in $R/(p)[X]$ irreduzibel, so ist f in $K[X]$ irreduzibel.

Beweis. Zu (1): Angenommen, f ist reduzibel in $R[X]$, d.h., $f = gh$, wobei $g, h \in R[X]$ und weder f noch g ein Einheit ist. Da f primitiv ist, können g und h keine Konstanten sein. Also gilt $\deg(f) > 0$ und $\deg(g) > 0$. Dann ist das Produkt der höchsten Koeffizienten von g und h gerade der höchste Koeffizient von f. Da dieser nicht von p geteilt wird, werden auch die höchsten Koeffizienten von g und h nicht von p geteilt. Denn R und $R/(p)$ sind Integritätsringe, so dass $\deg(gh) = \deg(g) + \deg(h)$ und $\deg(\pi(g)\pi(h)) = \deg(\pi(g)) + \deg(\pi(h))$ gilt. Also ist $\deg(\pi(g)) = \deg(g) > 0$ und $\deg(\pi(h)) = \deg(h) > 0$ in $R/(p)[X]$. Wegen

$$\pi(f) = \pi(gh) = \pi(g)\pi(h)$$

ist also $\pi(f)$ in $R/(p)[X]$ reduzibel, Widerspruch. Also ist f irreduzibel in $R[X]$.

Zu (2): Wir können $f = c \cdot g$ schreiben, wobei $c \in R$ der ggT der Koeffizienten von f ist und g dann primitiv ist. Da $\pi(f)$ irreduzibel in $R/(p)[X]$ ist, gilt das erst recht für $\pi(g)$. Nach (1) ist g also irreduzibel in $R[X]$. Nach Korollar 3.9.7 ist g dann auch irreduzibel in $K[X]$. Da K ein Körper ist, ist c aber eine Einheit in $K[X]$. Also ist auch f irreduzibel in $K[X]$. □

Beispiel 3.10.8. *Das Polynom $f = -8X^3 - 4X + 1 \in \mathbb{Z}[X]$ ist irreduzibel in $\mathbb{Z}[X]$ (und in $\mathbb{Q}[X]$).*

In der Tat, Reduktion modulo $p = 3$ in $R = \mathbb{Z}$ liefert das Polynom $\pi(f) = X^3 - X + 1 \in \mathbb{F}_3[X]$, das keine Nullstelle in $\mathbb{F}_3$ hat. Also ist $\pi(f)$ irreduzibel in $\mathbb{F}_3[X]$ nach dem Nullstellenkriterium. Da f primitiv ist, folgt die Behauptung aus dem Reduktionskriterium.

Man kann das folgende Kriterium anwenden, um zu sehen, dass gewisse Polynome keine rationalen Nullstellen haben.

Satz 3.10.9 (Rationaler Nullstellentest)**.** *Sei $f = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ ein Polynom vom Grad n und $a = \frac{r}{s}$ eine rationale Nullstelle von f mit $\gcd(r, s) = 1$. Dann gilt $r \mid a_0$ und $s \mid a_n$ in $\mathbb{Z}$.*

Beweis. Wir dürfen annehmen, dass f primitiv ist, indem wir den ggT herausziehen. Damit ändert man nicht die Menge der rationalen Nullstellen und die Teilbarkeitbedingungen gelten erst recht. Wegen $f\left(\frac{r}{s}\right) = 0$ ist $sX - r$ ein Teiler von f in $\mathbb{Q}[X]$. Nach dem Lemma von Gauss ist dann $f = (sX - r)g$ mit einem primitiven Polynom $g \in \mathbb{Z}[X]$. Jedes Vielfache von $sX - r$ in $\mathbb{Z}[X]$ hat aber einen Leitkoeffizienten, der durch s teilbar ist, und einen konstanten Term, der durch r teilbar ist, also insbesondere auch f. □

Beispiel 3.10.10. *Das Polynom $f = 2X^3 + X - 1$ hat keine rationalen Nullstellen.*

Sei $\frac{r}{s}$ eine Nullstelle von f. Dann gilt $r \mid -1$ und $s \mid 2$. Also sind die potentiellen rationalen Nullstellen gerade ± 1 und $\pm\frac{1}{2}$. Doch keine davon ist eine Nullstelle, wie man leicht ausrechnet.

Bemerkung 3.10.11. Das Reduktionskriterium ist zwar oft recht hilfreich, hat aber auch seine Grenzen. Zum Beispiel ist das Polynom $f = X^4 + 1$ irreduzibel in $\mathbb{Z}[X]$, aber reduzibel über $\mathbb{F}_p$ für *jede* Primzahl p.

Theorem 3.10.12 (Eisensteinsches Irreduzibiliätskriterium)**.** *Sei R ein faktorieller Ring mit Quotientenkörper K und $f = a_n X^n + \cdots + a_1 X + a_0 \in R[X]$ ein primitives Polynom vom Grad n. Sei p ein Primelement in R mit $p \mid a_0, \ldots a_{n-1}$ und $p \nmid a_n$, $p^2 \nmid a_0$. Dann ist f irreduzibel in $R[X]$ und $K[X]$.*

Beweis. Wegen Korollar 3.9.7 genügt es zu zeigen, dass f irreduzibel in $R[X]$ ist. Angenommen, $f = gh$ ist reduzibel, mit $g, h \in R[X]$ und $\deg(g) > 0$, $\deg(h) > 0$. Sei $g = b_r X^r + \cdots + b_0$ und $h = c_s X^s + \cdots + c_0$ mit $b_r, c_s \neq 0$. Es gilt

$$r + s = \deg(g) + \deg(h) = \deg(f) = n,$$

da R ein Integritätsring ist. Wegen $r, s > 0$ folgt auch $r, s < n$. Wir haben $a_n = b_r c_s$ und $a_0 = b_0 c_0$. Da $p \nmid a_n$ folgt $p \nmid b_r, c_s$ und da $p^2 \nmid a_0$ teilt p genau eines der Elemente b_0 und c_0. Ohne Einschränkung gelte $p \mid b_0$, $p \nmid c_0$. Sei t maximal mit der Eigenschaft, daß $p \mid b_i$ für alle i mit $0 \leq i \leq t$. Dann ist

$$a_{t+1} = b_{t+1} c_0 + (b_t c_1 + \cdots + b_0 c_{t+1})$$

und jeder Summand in der Klammer ist durch p teilbar, aber nicht der Term $b_{t+1} c_0$. Also ist a_{t+1} nicht durch p teilbar. Nach Voraussetzung geht das nur

für $t+1=n$. Aber dann ist $r=\deg(g)\geq t+1=n$, im Widerspruch zu $r<n$. □

Beispiel 3.10.13. *Sei $f=X^n-p\in\mathbb{Z}[X]$ mit p prim und $n\geq 1$. Dann ist f irreduzibel in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$. Insbesondere ist $\sqrt[n]{p}$ irrational.*

Das folgt aus Eisenstein mit der Primzahl p in $\mathbb{Z}$. Manchmal kann man Eisenstein nicht direkt anwenden, sondern erst nach einer Substitution $X\mapsto X+a$. Eine echte Zerlegung von $f(X)$ induziert eine von $f(X+a)$ und umgekehrt, also ändert sich an der Irreduzibilität nichts.

Beispiel 3.10.14. *Sei p ein Primzahl. Das Kreisteilungspolynom*

$$\frac{X^p-1}{X-1}=X^{p-1}+\cdots+X+1\in\mathbb{Z}[X]$$

ist irreduzibel in $\mathbb{Q}[X]$.

Hier können wir Eisenstein nicht direkt anwenden. Wir können aber zeigen, dass $f(X+1)$ irreduzibel ist, und daher auch $f(X)$. Wir haben

$$\begin{aligned}f(X+1)&=\frac{(X+1)^p-1}{X}\\&=\frac{1}{X}((X+1)^p-1)\\&=X^{p-1}+\binom{p}{1}X^{p-2}+\cdots+\binom{p}{p-1}.\end{aligned}$$

Hier können wir Eisenstein mit der Primzahl p anwenden, da $p\mid\binom{p}{k}$ für $k=1,\ldots,p-1$ und $p^2\nmid\binom{p}{p-1}=p$ gilt.

Bemerkung 3.10.15. Es gibt irreduzible Polynome in $\mathbb{Z}[X]$ wie etwa $f=X^4+10X^2+1$ oder $f=X^3+X+1$, auf die man Eisenstein für keine Translation anwenden kann.

3.11 Anwendungen in der Zahlentheorie

Die elementare Zahlentheorie liefert Motivationen und ein reiches Beispielmaterial für die Algebra. Umgekehrt aber kann man auch viele klassische Resultate der Zahlentheorie mit algebraischen Mittel kurz und elegant beweisen. Wir wollen in diesem Abschnitt einige dieser Resultate vorstellen.

Definition 3.25. Sei R ein kommutativer Ring. Zwei Ideale I und J in R heißen *teilerfremd*, wenn $I + J = R$ gilt.

Die Definition ist äquivalent dazu, dass es ein $a \in I$ und ein $b \in J$ gibt mit $a + b = 1$. Für Ideale I und J gilt immer $IJ \subseteq I \cap J$, siehe Lemma 3.2.3, aber für teilerfremde Ideale gilt sogar $IJ = I \cap J$. In der Tat, sei $x \in I \cap J$. Da I und J teilerfremd sind, existieren $a \in I$ und $b \in J$ mit $a + b = 1$. Dann gilt $x = x \cdot 1 = xa + xb \in IJ + IJ = IJ$.

Für den Ring $\mathbb{Z}$ existieren $m, n \in \mathbb{Z}$ mit $I = m\mathbb{Z}$ und $J = n\mathbb{Z}$, und es gilt $m\mathbb{Z} + n\mathbb{Z} = \gcd(m, n)\mathbb{Z}$, siehe Beispiel 3.2.4. Also sind die Ideale $m\mathbb{Z}$ und $n\mathbb{Z}$ genau dann teilerfremd, wenn m und n teilerfremd sind.

Satz 3.11.1 (Chinesischer Restsatz)**.** *Seien I und J teilerfremde Ideale in R. Dann definiert die Zuordnung $x \mapsto (x + I, x + J)$ einen Ringhomomorphismus $\varphi\colon R \to R/I \times R/J$, der einen Ringisomorphismus*

$$R/IJ \xrightarrow{\cong} R/I \times R/J$$

induziert.

Beweis. Nach dem Homomorphiesatz für Ringe, siehe Bemerkung 3.2.9, gilt $R/\ker(\varphi) \cong \operatorname{im}(\varphi)$. Nach Konstruktion gilt $\ker(\varphi) = I \cap J$. Da I und J teilerfremd sind, folgt die Gleichheit $IJ = I \cap J$. Also gilt $\ker(\varphi) = IJ$. Wir zeigen nun, dass φ surjektiv ist, und deshalb auch $\operatorname{im}(\varphi) = R/I \times R/J$ folgt. Seien $x, y \in R$. Nach Voraussetzung gibt es $a \in I$ und $b \in J$ mit $a + b = 1$. Also ist

$$(ay + bx) + I = bx + I = (ax + bx) + I = x + I$$

und ebenso $(ay + bx) + J = x + J$. Also gilt $\varphi(bx + ay) = (x + I, x + J)$ und φ is surjektiv. □

Man kann den chinesischen Restsatz auch auf mehrere Faktoren ausdehnen.

Theorem 3.11.2 (Chinesischer Restsatz)**.** *Seien $I_1, \ldots, I_n$ paarweise teilerfremde Ideale in R. Dann ist jedes Ideal I_j teilerfremd zu $\prod_{i \neq j} I_i$ und*

es gilt $\prod_{i=1}^{n} I_i = \cap_{i=1}^{n} I_i$. *Die Zuordnung* $x \mapsto (x + I_1, \ldots, x + I_n)$ *definiert einen Ringhomomorphismus* $\varphi\colon R \to R/I_1 \times \cdots \times R/I_n$, *der einen Ringisomorphismus*

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

induziert.

Korollar 3.11.3. *Seien* $m_1, \ldots m_n$ *paarweise teilerfremde Zahlen und sei* $m := m_1 \cdots m_n$. *Dann erhalten wir einen Ringisomorphismus*

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}.$$

Sind $x_1, \ldots x_n \in \mathbb{Z}$, *dann hat das System von Kongruenzen* $x \equiv x_j \bmod m_j$ *für* $j = 1, 2, \ldots, n$ *genau eine Lösung modulo* m.

Beweis. Der Ringisomorphismus folgt direkt aus dem Theorem. Die Lösbarkeit der simultanen Kongruenzen bedeutet genau, dass die Abbildung $\varphi\colon \mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$ surjektiv ist. Also gibt es eine Lösung $x \in \mathbb{Z}$ und die Menge aller Lösungen ist durch die zugehörige Nebenklasse $x + \cap_{i=1}^{n} m_i\mathbb{Z} = x + m\mathbb{Z}$ gegeben. Man kann eine Lösung x aus dem Beweis der Surjektivität von φ explizit konstruieren. Für alle j setze man $m'_j = \frac{m}{m_j}$. Nach Voraussetzung sind m_j und m'_j teilerfremd. Deshalb ist $m_j\mathbb{Z} + m'_j\mathbb{Z} = 1$ und man kann (auch mit dem Euklidischen Algorithmus) ganze Zahlen a_j und b_j finden mit $a_j m_j + b_j m'_j = 1$. Dann ist

$$x = \sum_{j=1}^{n} x_j b_j m'_j$$

die gesuchte Lösung, die eindeutig ist modulo m. □

Beispiel 3.11.4. *Das System von Kongruenzen* $x \equiv 1 \bmod 2$, $x \equiv 2 \bmod 3$ *und* $x \equiv 3 \bmod 5$ *hat genau die ganzzahligen Lösungen* $x \in S = 23 + 30\mathbb{Z}$.

Man hat

$$\begin{aligned} m_1 = 2, m_2 = 3, m_3 = 5, \\ x_1 = 1, x_2 = 2, x_3 = 3, \\ m'_1 = 15, m'_2 = 10, m'_3 = 6. \end{aligned}$$

Wegen

$$\begin{aligned} 1 &= -7 \cdot m_1 + 1 \cdot m_1', \\ 1 &= -3 \cdot m_2 + 1 \cdot m_2' \\ 1 &= -1 \cdot m_3 + 1 \cdot m_3' \end{aligned}$$

können wir $b_1 = b_2 = b_3 = 1$ wählen. Dann ist

$$\begin{aligned} x &= x_1 b_1 m_1' + x_2 b_2 m_2' + x_3 b_3 m_3' \\ &= 1 \cdot 1 \cdot 15 + 2 \cdot 1 \cdot 10 + 3 \cdot 1 \cdot 6 \\ &= 53 \equiv 23 \bmod 30. \end{aligned}$$

Sei $U(n)$ die prime Restklassengruppe, also die Gruppe der Einheiten des Ringes $\mathbb{Z}/n\mathbb{Z}$, siehe Bemerkung 2.3.4. Dann erhalten wir folgendes Resultat.

Korollar 3.11.5. *Seien $m_1, \dots m_n$ paarweise teilerfremde Zahlen und sei $m := m_1 \cdots m_n$. Dann erhalten wir einen Gruppenisomorphismus*

$$U(m) \cong U(m_1) \times \cdots \times U(m_n).$$

Beweis. Ist $R \cong R_1 \times \cdots \times R_n$ ein Ringisomorphismus, dann erhält man einen induzierten Gruppenisomorphismus der Einheitengruppen $U(R) \cong U(R_1) \times \cdots \times U(R_n)$. Daher folgt die Aussage aus Korollar 3.11.3. □

Da $|U(m)| = \varphi(m)$ und $|U(m_1) \times \cdots \times U(m_n)| = \varphi(m_1) \cdots \varphi(m_n)$, so folgt

$$\varphi(m_1 \cdots m_n) = \varphi(m_1) \cdots \varphi(m_n)$$

für paarweise teilerfremde Zahlen m_i. Die Eulersche φ-Funktion ist also *multiplikativ*. Wir haben

$$\varphi(n) = |U(n)| = \sum_{\substack{1 \le d \le n \\ (n,d)=1}} 1.$$

Für Primzahlen p gilt $\varphi(p) = p - 1$, und für Primzahlpotenzen gilt $\varphi(p^e) = p^e(1 - \frac{1}{p})$, mit $e \ge 1$. In der Tat,

$$p^e - \varphi(p^e) = |d \colon 1 \le d \le n, \gcd(n, p^e) > 1|,$$

was genau der Anzahl der Vielfachen von p, zwischen 1 und p^e, entspricht, und das sind genau $p^e - p^{e-1} = p^e(1 - \frac{1}{p})$ Vielfache.

Korollar 3.11.6. *Für eine natürliche Zahl $n \geq 1$ gilt*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Beweis. Sei $n = p_1^{e_1} \cdots p_k^{e_k}$ die Primfaktorzerlegung von n. Da φ multiplikativ ist, gilt

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{e_1}) \cdots \varphi(p_k^{e_k}) \\
&= p_1^{e_1} \left(1 - \frac{1}{p_1}\right) \cdots p_k^{e_k} \left(1 - \frac{1}{p_k}\right) \\
&= p_1^{e_1} \cdots p_k^{e_k} \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\
&= n \prod_{p|n} \left(1 - \frac{1}{p}\right).
\end{aligned}$$

□

Definition 3.26. Sei d eine ganze Zahl, die teilerfremd zu n ist. Sei $\mathrm{ord}_n(d)$ die Ordnung von d als Element in $U(n)$. Dann heißt d eine *Primitivwurzel modulo n*, falls $\mathrm{ord}_n(d) = \varphi(n)$ gilt, also $U(n)$ zyklisch ist.

Beispiel 3.11.7. *Die Zahl 3 ist eine Primitivwurzel modulo 7. Für $n = 8$ existiert gar keine Primitivwurzel.*

In der Tat, modulo 7 gilt

$$3^1 \equiv 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5,\ 3^6 \equiv 1.$$

Also hat 3 die Ordnung $\varphi(7) = 6$, und $U(7)$ is zyklisch, mit Erzeuger 3. Allerdings ist auch 5 eine Primitivwurzel modulo 7. Für $n = 8$ ist $U(8) = \{1, 3, 5, 7\}$ und $\varphi(8) = 4$. Allerdings ist $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \bmod 8$. Also gibt es keine Primitivwurzel modulo 8. Die Gruppe $U(8)$ ist nicht zyklisch. Sie ist isomorph zur Kleinschen Vierergruppe $C_2 \times C_2$.

Satz 3.11.8. *Ist $U(n)$ zyklisch, so gibt es genau $\varphi(\varphi(n))$ Primitivwurzeln modulo n.*

Beweis. Sei g ein erzeugendes Element von $U(n)$. Dann hat g^k genau dann die Ordung $|U(n)| = \varphi(n)$, wenn $\gcd(k, |U(n)|) = 1$ gilt. Schreibt man $U(n) = \{g^0, g^1, \ldots, g^{\varphi(n)-1}\}$, so trifft diese Bedingung genau für

$$\varphi(|U(n)|) = \varphi(\varphi(n))$$

der auftretenden Exponenten k zu. □

Korollar 3.11.9. *Sei p eine Primzahl. Dann ist $U(p)$ zyklisch und es gibt $\varphi(\varphi(p)) = \varphi(p-1)$ viele Primitivwurzeln modulo p.*

Beweis. Die multiplikative Gruppe des endlichen Körpers $\mathbb{F}_p$ ist zyklisch, siehe Satz 4.1.4. Das ist aber gerade die Gruppe $U(p) \cong C_{p-1}$. Nach Satz 3.11.8 gibt es also $\varphi(\varphi(p))$ viele Primitivwurzeln modulo p. □

Eine natürliche Frage ist, ob auch die Gruppen $U(p^e)$ zyklisch sind, für Primzahlpotenzen. Allerdings wissen wir schon, dass $U(8) = U(2^3)$ nicht zyklisch ist, siehe Beispiel 3.11.7. Doch wir werden sehen, dass die Primzahl 2 hier eine Sonderrolle spielt. Für $p > 2$ sind tatsächlich alle Gruppen $U(p^e)$ mit $e \geq 1$ zyklisch. Zum Beweis brauchen wir einige Hilfsresultate.

Lemma 3.11.10. *Sei p eine Primzahl und g eine Primitivwurzel modulo p. Dann gilt entweder $g^{p-1} \not\equiv 1 \bmod p^2$ oder $(g+p)^{p-1} \not\equiv 1 \bmod p^2$.*

Beweis. Angenommen, die Aussage wäre falsch, d.h., wir hätten

$$g^{p-1} \equiv 1 \equiv (g+p)^{p-1} \bmod p^2.$$

Dann folgt aus dem binomischen Lehrsatz

$$\begin{aligned}(g+p)^{p-1} &\equiv g^{p-1} + p(p-1)g^{p-2} + \sum_{i=2}^{p-1} \binom{p-1}{i} p^i g^{p-1-i} \bmod p^2 \\ &\equiv g^{p-1} + p(p-1)g^{p-2} \bmod p^2,\end{aligned}$$

da alle Terme in der letzten Summe durch p^2 teilbar sind. Zusammen mit der Voraussetzung folgt, dass

$$p(p-1)g^{p-2} \equiv 0 \bmod p^2,$$

und somit $(p-1)g^{p-2} \equiv 0 \bmod p$, also $p \mid g^{p-2}$. Das ist ein Widerspruch, da g^{p-2} eine Primitivwurzel modulo p ist. Also ist die Aussage des Lemmas wahr. □

Beispiel 3.11.11. *Für $p = 7$ ist $g = 3$ eine Primitivwurzel modulo p mit $g^{p-1} \equiv 43 \not\equiv 1 \mod p^2$. Für $p = 29$ ist $g = 14$ eine Primitivwurzel modulo p mit $g^{p-1} \equiv 1 \mod p^2$, aber $(g+p)^{p-1} = 43^{28} \equiv 59 \not\equiv 1 \mod p^2$.*

Satz 3.11.12. *Sei $p > 2$ eine Primzahl, g eine Primitivwurzel modulo p mit $g^{p-1} \not\equiv 1 \mod p^2$. Dann ist g eine Primitivwurzel modulo p^e für alle $e \geq 1$.*

Beweis. Wir zeigen zunächst durch Induktion nach $e \geq 2$, dass gilt

$$g^{(p-1)p^{e-2}} \not\equiv 1 \mod p^e.$$

Für $e = 2$ ist das gerade die Voraussetzung des Satzes. Also ist der Induktionsanfang gezeigt. Nach Induktionsvoraussetzung gilt $g^{(p-1)p^{e-2}} \not\equiv 1 \mod p^e$. Dann ist $g^{(p-1)p^{e-2}} = 1 + ap^{e-1}$ für ein $a \in \mathbb{Z}$ mit $\gcd(a, p) = 1$, weil $g^{(p-1)p^{e-2}} = g^{\varphi(p^{e-1})} \equiv 1 \mod p^{e-1}$ nach Euler. Dann gilt

$$\begin{aligned} g^{(p-1)p^{e-1}} &= (1 + ap^{e-1})^p \\ &= 1 + pap^{e-1} + \binom{p}{2} a^2 p^{2e-2} + \sum_{i=3}^{p-1} \binom{p}{i} a^i p^{(e-1)i} \\ &\equiv 1 + ap^e + \frac{p-1}{2} a^2 p^{2e-1} \mod p^{e+1} \\ &\equiv 1 + ap^e, \end{aligned}$$

denn $(e-1)i \geq 3e - 3 \geq e - 1$ für $i \geq 3$, so dass die letzte Summe durch p^{e+1} teilbar ist, und weiterhin $p^{2e-1} \equiv 0 \mod p^{e+1}$ gilt, wegen $e \geq 2$. Aber das zeigt wegen $\gcd(p, a) = 1$ den Induktionsschluss, nämlich

$$g^{(p-1)p^{e-1}} \not\equiv 1 \mod p^{e+1}.$$

Sei nun $r = \operatorname{ord}_{p^e}(g)$. Nach Definition ist $g^r \equiv 1 \mod p^e$, also insbesondere auch $g^r \equiv 1 \mod p$. Daher ist r einerseits ein Teiler von $\varphi(p^e) = (p-1)p^{e-1}$ nach Euler, und andererseits $p - 1$ ein Teiler von r wegen $g^{p-1} \equiv 1 \mod p$ nach dem kleinen Fermat (der aus Euler folgt). Insgesamt gilt daher

$$\frac{r}{p-1} \mid p^{e-1},$$

so dass $\frac{r}{p-1} = p^k$ ist für ein $k < e$. Wir zeigen, dass $k = e - 1$ gilt. Angenommen, $k < e - 1$. Nach Euler ist

$$g^r = g^{p^k(p-1)} = g^{\varphi(p^{k+1})} \equiv 1 \mod p^{k+1}.$$

Wegen $k < e-1$ gilt diese Kongruenz auch modulo p^e. Wir können $g^{p^k(p-1)}$ dann noch zur Potenz mit p^{e-2-k} erheben und erhalten

$$g^{(p-1)p^{e-2}} \equiv 1 \bmod p^e.$$

Das steht im Widerspruch zu unserer ersten Formel, die wir mit Induktion bewiesen haben. Also folgt $k = e-1$ und somit

$$\mathrm{ord}_{p^e}(g) = r = (p-1)p^{e-1} = \varphi(p^e).$$

Somit ist g eine Primitivwurzel modulo p^e. □

Korollar 3.11.13. *Sei $p > 2$ eine Primzahl und $e \geq 1$. Dann ist $U(p^e)$ zyklisch.*

Beweis. Es ist g eine Primitvwurzel modulo p genau dann, wenn $g+p$ eine ist. Für eine der beiden ist aber, wegen Lemma 3.11.10, die Voraussetzung von Satz 3.11.12 erfüllt. Also ist $U(p^e)$ zyklisch, mit entweder g oder $g+p$ als erzeugendes Element. □

Korollar 3.11.14. *Sei $p > 2$ eine Primzahl und $e \geq 1$. Dann ist $U(2p^e)$ zyklisch.*

Beweis. Nach Korollar 3.11.5 ist

$$U(2p^e) \cong U(2) \times U(p^e) \cong U(p^e)$$

zyklisch. □

Der Fall $p = 2$ ist wesentlich komplizierter. Wir stellen hier nur die Beweisideen zusammen, geben aber keinen vollständigen Beweis. Die Gruppen $U(1)$ und $U(2)$ sind trivial, wegen $\varphi(1) = \varphi(2) = 1$, und $U(4) \cong C_2$ ist zyklisch wegen $\varphi(4) = 2$.

Satz 3.11.15. *Für alle $e \geq 3$ ist die Gruppe $U(2^e)$ nicht zyklisch. Genauer gilt, dass*

$$U(2^e) \cong C_2 \times C_{2^{e-2}}.$$

Wir können nun unser Hauptresultat formulieren.

Theorem 3.11.16 (Gauß)**.** *Die Gruppe $U(n)$ ist genau dann zyklisch, wenn n von der Form p^e oder $2p^e$ ist, mit $p > 2$ prim und $e \geq 1$, oder $n = 1, 2, 4$ ist.*

Beweis. Ist $n = p_1^{e_1} \cdots p_k^{e_k}$ die Primfaktorzerlegung von n, dann gilt nach Korollar 3.11.5, dass

$$U(n) \cong U(p_1^{e_1}) \times \cdots \times U(p_k^{e_k}).$$

Diese Gruppe ist genau dann zyklisch, wenn n nicht durch 8 teilbar ist (ansonsten wäre $U(8)$ eine nicht-zylische Untergruppe), und die Zahlen $\varphi(p_1^{e_1}), \ldots, \varphi(p_k^{e_k})$ paarweise teilerfremd sind. Da $\varphi(p^e)$ gerade ist für alle ungeraden Primzahlen p, folgt die Behauptung, mit Korollar 3.11.13 und 3.11.14.. □

Beispiel 3.11.17. *Die Gruppe*

$$\begin{aligned} U(360) &= U(2^3 \cdot 3^2 \cdot 5) \\ &\cong U(2^3) \times U(3^2) \times U(5) \\ &\cong C_2 \times C_2 \times C_6 \times C_4 \end{aligned}$$

ist nicht zyklisch.

In der Tat, 360 ist durch 8 teilbar. Auch die Gruppe

$$U(45) \cong U(3^2) \times U(5) \cong C_6 \times C_4$$

ist nicht zyklisch, da $\varphi(3^2) = 6$ und $\varphi(5) = 4$ beide gerade sind, also $\gcd(6, 4) > 1$ gilt.

Nun wollen wir auf quadratische Reste und das quadratische Reziprozitätsgesetz von Gauß eingehen, das zur Allgemeinbildung gehören sollte. Als Motivation können wir uns folgende Frage stellen:

Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$. Wie stellt man fest, ob die Kongruenz $x^2 \equiv a \bmod p$ in $\mathbb{Z}$ lösbar ist?

Anders gefragt, wann ist a ein Quadrat in $\mathbb{Z}/p\mathbb{Z}$?

Definition 3.27. Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$ mit $p \nmid a$. Dann heißt a ein QR (quadratischer Rest) modulo p, wenn $x^2 \equiv a \bmod p$ in $\mathbb{Z}$ lösbar ist, und andernfalls ein QNR (quadratischer Nichtrest).
Für ein beliebiges $a \in \mathbb{Z}$ definieren wir das *Legendre-Symbol* wie folgt:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{falls } p \mid a, \\ 1 & \text{falls } a \text{ ein QR modulo } p \text{ ist}, \\ -1 & \text{falls } a \text{ ein QNR modulo } p \text{ ist}. \end{cases}$$

Ist $a \equiv b \bmod p$, so folgt offensichtlich

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

Beispiel 3.11.18. *Die QR modulo $p = 11$ sind $a = 1, 3, 4, 5, 9$, und die QNR modulo 11 sind $a = 2, 6, 7, 8, 10$.*

Dazu berechnet man einfach die Restklassen der Quadrate

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

modulo p. Für $p = 11$ hat man $\frac{p-1}{2}$ QR und $\frac{p-1}{2}$ QNR. Das gilt immer:

Lemma 3.11.19. *Sei $p > 2$ eine Primzahl. Unter den Zahlen $1, 2, \ldots, p-1$ gibt es genau $\frac{p-1}{2}$ quadratische Reste und $\frac{p-1}{2}$ quadratische Nichtreste.*

Beweis. Die Aussage ist equivalent dazu, dass es in $\mathbb{F}_p^\times$ genauso viele Quadrate wie Nichtquadrate gibt. Dazu betrachten wir die Abbildung

$$q \colon \mathbb{F}_p^\times \to \mathbb{F}_p^\times,\ a \mapsto a^2.$$

Ihre "Fasern"$q^{-1}(\{c\})$ haben entweder null oder zwei Elemente: da $\mathbb{F}_p$ nullteilerfrei ist, also $a^2 = b^2$ gleichwertig mit $(a+b)(a-b) = 0$ ist, also $b = \pm a$. Ist $a \neq 0$, so gilt $a \neq -a$ wegen $p \neq 2$. Also haben die nichtleeren Fasern stets zwei Elemente a und $-a$. Deshalb ist

$$|\mathrm{im}(q)| = \frac{|\mathbb{F}_p^\times|}{2} = \frac{p-1}{2}.$$

Daraus folgt die Behauptung. □

Bemerkung 3.11.20. Eine kurze und schöne Zusammenfassung der obigen Aussage ist folgende Formel:

$$\sum_{a=0}^{p-1} \left(\frac{a}{p}\right) = 0.$$

Satz 3.11.21 (Euler)**.** *Sei p eine ungerade Primzahl. Dann gilt für $a \in \mathbb{Z}$*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

Diese Kongruenz bestimmt das Legendre-Symbol eindeutig.

Beweis. Für $p \mid a$ sind beide Seiten Null. Wir können also $p \nmid a$ annehmen. Nach dem kleinen Satz von Fermat gilt $a^{p-1} \equiv 1 \bmod p$. Mit anderen Worten, es gilt

$$p \mid (a^{p-1} - 1) = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1).$$

Da p prim ist, folgt $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$. Ist a ein QR modulo p, dann gibt es ein $b \in \mathbb{Z}$ mit $a \equiv b^2 \bmod p$, und es folgt $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) \bmod p$, und was die Behauptung ist. Das Polynom $f(x) = x^{\frac{p-1}{2}} - 1$ hat in $\mathbb{F}_p$ höchtens $\frac{p-1}{2}$ Nullstellen. Die Restklassen $[a]$ für QR a tragen aber nach Lemma 3.11.19 schon $\frac{p-1}{2}$ Nullstellen bei. Also folgt für jeden QNR a modulo p, dass $a^{\frac{p-1}{2}} \not\equiv 1 \bmod p$ ist, also $a^{\frac{p-1}{2}} \equiv -1 \bmod p$ gilt. Wegen $\left(\frac{a}{p}\right) = -1$ liefert das die Behauptung.
Die Eindeutigkeit des Legendre-Symbols folgt daraus, dass $0, 1, -1$ wegen $p > 2$ in verschiedenen Restklassen modulo p liegen. □

Korollar 3.11.22. *Sei p eine ungerade Primzahl. Für $a, b \in \mathbb{Z}$ gilt*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Beweis. Nach Satz 3.11.21 gilt

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p.$$

□

Also ist die Abbildung $\chi\colon U(p) \to \{1, -1\}$, $a \mapsto \left(\frac{a}{p}\right)$ ein Gruppenhomomorphismus. Man kann dieses Resultat zum Beispiel auch benutzen, um zu zeigen, dass das Produkt von zwei QNR ein QR ist.

Korollar 3.11.23. *Sei p eine ungerade Primzahl. Dann gilt*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{falls } p \equiv 1 \bmod 4, \\ -1 & \text{falls } p \equiv 3 \bmod 4. \end{cases}$$

Beweis. Nach Satz 3.11.21 gilt

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \bmod p.$$

Da aber beide Seiten den Wert ± 1 haben, folgt die Gleichheit. □

Diese Aussage wird auch oft als *Erster Ergänzungssatz zum Quadratischen Reziprozitätsgesetz* bezeichnet. Der zweite Ergänzungssatz besagt das folgende.

Satz 3.11.24. *Sei p eine ungerade Primzahl. Dann gilt*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{falls } p \equiv \pm 1 \bmod 8, \\ -1 & \text{falls } p \equiv \pm 3 \bmod 8. \end{cases}$$

Das *Quadratische Reziprozitätsgesetz* besagt folgendes.

Theorem 3.11.25 (QRG)**.** *Seien p und q verschiedene ungerade Primzahlen. Dann gilt*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right).$$

Falls $p \equiv 1 \bmod 4$ oder $q \equiv 1 \bmod 4$ gilt also $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, und falls $p \equiv q \equiv 3 \bmod 4$ gilt $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.

Gauß hat für dieses Theorem als Erster einen vollständigen Beweis gegeben. Er findet sich in seiner Schrift Disquisitiones Arithmeticae von 1801. Insgesamt fand er acht verschiedene Beweise. Sei p eine ungerade Primzahl. Wir setzen zur Abkürzung

$$p^* = \left(\frac{-1}{p}\right) \cdot p.$$

Dann gilt stets $p^* \equiv 1 \bmod 4$, und das QRG is äquivalent zu der Aussage

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right).$$

Definition 3.28. Sei p eine ungerade Primzahl und $\zeta = e^{\frac{2\pi i}{p}}$. Für $a \in \mathbb{Z}$ heißt

$$g_a = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) \zeta^{aj} \in \mathbb{Z}[\zeta]$$

eine *Gauß-Summe* zur Primzahl p. Sie ist ein Element in dem Ring $\mathbb{Z}[\zeta]$.

Für $a = 1$ schreiben wir $g_1 = g$.

Lemma 3.11.26. *Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$.*

(1) *Es gilt*

$$\sum_{j=0}^{p-1} \zeta^{aj} = \begin{cases} 0 & \text{falls } p \nmid a, \\ p & \text{falls } p \mid a. \end{cases}$$

(2) $g_a = \left(\frac{a}{p}\right) g$.

(3) $g^2 = p^*$.

Beweis. (1): Für $p \mid a$ gilt $\zeta^a = 1$, also ist die Summe gleich $p \cdot 1 = p$. Für $p \nmid a$ ist $\zeta^a \neq 1$ und es folgt

$$\sum_{j=0}^{p-1} \zeta^{aj} = \sum_{j=1}^{p} \zeta^{aj} = \zeta^a \sum_{j=0}^{p-1} \zeta^{aj},$$

also

$$(1 - \zeta^a) \left(\sum_{j=0}^{p-1} \zeta^{aj} \right) = 0.$$

Da der erste Faktor nicht Null ist, muss es der zweite sein.

(2): Für $p \mid a$ ist

$$g_a = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) = 0$$

nach Bemerkung 3.11.20. Da dann auch $\left(\frac{a}{p}\right) = 0$ gilt, folgt die Behauptung. Wir können also $p \nmid a$ annehmen. Also gibt es ein $b \in \mathbb{Z}$ mit $ab \equiv 1 \bmod p$, also ein inverses Element zu a in der Gruppe $U(p)$. Also ist

$$1 = \left(\frac{1}{p}\right) = \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$

aber in $\mathbb{Z}$ kann man nur $1 = 1 \cdot 1$ oder $1 = (-1) \cdot (-1)$ haben. Also gilt $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. Mit j durchläuft auch bj alle Restklassen modulo p, also erhalten wir

$$g_a = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) \zeta^{aj} = \sum_{j=0}^{p-1} \left(\frac{bj}{p}\right) \zeta^j = \left(\frac{b}{p}\right) \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) \zeta^j = \left(\frac{a}{p}\right) g.$$

(3): Wegen (2) gilt

$$\sum_{a=0}^{p-1} g_a^2 = \sum_{a=0}^{p-1} \left(\frac{a}{p}\right)^2 g^2 = g^2 \sum_{a=0}^{p-1} \left(\frac{a}{p}\right)^2 = g^2(p-1).$$

Andererseits ist wegen (1)

$$\sum_{a=0}^{p-1} \zeta^{a(j+k)} = \begin{cases} 0 & \text{falls } p \nmid j+k, \\ p & \text{falls } p \mid j+k. \end{cases}$$

Deshalb gilt auch

$$\begin{aligned} \sum_{a=0}^{p-1} g_a^2 &= \sum_{a=0}^{p-1} \sum_{j,k=0}^{p-1} \left(\frac{j}{p}\right)\left(\frac{k}{p}\right) \zeta^{aj+ak} \\ &= \sum_{j,k=0}^{p-1} \left(\frac{jk}{p}\right) \sum_{a=0}^{p-1} \zeta^{a(j+k)} \\ &= \sum_{j=0}^{p-1} \left(\frac{-j^2}{p}\right) p \\ &= (p-1)\left(\frac{-1}{p}\right) p. \end{aligned}$$

Zusammen folgt

$$g^2(p-1) = (p-1)p^*,$$

und somit $g^2 = p^*$. □

Nun können wir das QRG beweisen:

Beweis von Theorem 3.11.25*:* Sei $I = (q)$ das von q erzeugte Ideal in $\mathbb{Z}[\zeta]$. Mit (3) gilt dann modulo I

$$g^q = (g^2)^{\frac{q-1}{2}} \cdot g = (p^*)^{\frac{q-1}{2}} g \equiv \left(\frac{p^*}{q}\right) g.$$

Andererseits haben wir wegen (2) auch

$$g^q \equiv \sum_{j=0}^{p-1} \left(\frac{j}{p}\right)^q \zeta^{aj} = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) \zeta^{aj} = g_q = \left(\frac{q}{p}\right) g.$$

Zusammen folgt $\left(\frac{p^*}{q}\right) g \equiv \left(\frac{q}{p}\right) g \mod I$. Nach Multiplikation mit g und wegen $g^2 = p^*$, was wir kürzen können, da p und q teilerfremd sind, erhalten wir

$$\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) \mod (q).$$

Da aber q keine Einheit ist in $\mathbb{Z}[\zeta]$ und zudem $2 \notin (q)$, da q ungerade ist, folgt daraus die sogar Gleichheit in $\mathbb{Z}$. □

Mit dem QRG kann man nun das Legendre-Symbol leicht ausrechnen.

Beispiel 3.11.27. *Es gilt* $\left(\frac{67}{109}\right) = -1$.

Wir haben nämlich, da $109 \equiv 1 \bmod 4$ ist,

$$\left(\frac{67}{109}\right) = \left(\frac{109}{67}\right) = \left(\frac{-25}{67}\right) = \left(\frac{-1}{67}\right)\left(\frac{5}{67}\right)^2 = -1.$$

Eine weiteres Thema der Zahlentheorie sind *Summen von Quadraten*. Mit den Eigenschaften des Ringes $\mathbb{Z}[i]$, der ganzen Gausschen Zahlen, können wir genau beschreiben, wann eine natürliche Zahl die Summe von zwei Quadratzahlen ist. Den folgenden Satz haben wir in den Übungen bewiesen:

Satz 3.11.28. *Der Ring $\mathbb{Z}[i]$ ist ein Euklidischer Ring mit der Normfunktion*

$$N(a+bi) = (a+bi)(a-bi) = a^2 + b^2.$$

Für $\alpha, \beta \in \mathbb{Z}[i]$ gilt $N(\alpha\beta) = N(\alpha)N(\beta)$. Folglich ist $\mathbb{Z}[i]$ auch ein Hauptidealring und ein faktorieller Ring.

Mit dem Euklidischen Algorithmus kann man daher einen ggT berechen. Zum Beispiel ist $5+4i$ ein größter gemeinsamer Teiler von 41 und $32+i$. Wegen $N(5+4i) = 5^2+4^2 = 41$ ist die Primzahl 41 also die Summe zweier Quadratzahlen. Wir wissen auch schon, dass

$$\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$$

die Einheiten des Ringes $\mathbb{Z}[i]$ sind. Hier ist $\varepsilon \in \mathbb{Z}[i]$ genau dann eine Einheit, wenn $N(\varepsilon) = 1$ gilt. Das folgende Lemma behandelt Primelemente in $\mathbb{Z}[i]$.

Lemma 3.11.29. *Sei $\pi \in \mathbb{Z}[i]$. Ist $N(\pi)$ eine Primzahl, dann ist π ein Primelement in $\mathbb{Z}[i]$. Ist umgekehrt π ein Primelement, so gibt es eine Primzahl p mit $p \mid \pi$ und $N(\pi)$ ist p oder p^2. In letzterem Fall gilt $\pi \sim p$ in $\mathbb{Z}[i]$ und es gibt keine Elemente der Norm p in $\mathbb{Z}[i]$.*

Beweis. Ist $N(\pi)$ eine Primzahl, so ist die Norm nicht 1. Also ist π keine Einheit und von Null verschieden. Da $\mathbb{Z}[i]$ ein Hauptidealring ist, ist π prim genau dann wenn es irreduzibel ist. Wir zeigen, dass π irreduzibel ist. Dazu sei $\pi = \alpha\beta$ eine Faktorisierung in $\mathbb{Z}[i]$. Dann folgt $N(\pi) = \mathbb{N}(\alpha)N(\beta)$. Da $N(\pi)$ eine Primzahl ist, muss entweder $N(\alpha) = 1$ oder $N(\beta) = 1$ gelten. Also ist entweder α oder β eine Einheit und π ist irreduzibel, beziehungsweise prim.

Sei umgekehrt π ein Primelement in $\mathbb{Z}[i]$. Dann ist $\pi \neq 0$ und keine Einheit, so dass $n = \pi\overline{\pi} = N(\pi) > 1$ ist. Dann ist n ein nicht-leeres Produkt von Primzahlen in $\mathbb{Z}$. Da π prim ist, muss π einen der Primfaktoren von n teilen. Sei p dieser Primfaktor, also $\pi \mid p$. Es folgt $N(\pi) \mid N(p) = p^2$, und somit gibt es zwei Möglichkeiten. Entweder ist $N(\pi) = p$ oder $N(\pi) = p^2$. Im zweiten Fall schreibe man $p = \pi\alpha$ mit einem $\alpha \in \mathbb{Z}[i]$. Dann folgt

$$p^2 = N(p) = N(\pi)N(\alpha) = p^2N(\alpha),$$

also $N(\alpha) = 1$. Also ist α eine Einheit und deshalb $\pi \sim p$. Angenommen, es gibt ein $\sigma \in \mathbb{Z}[i]$ mit $N(\sigma) = p$. Dann folgt auch $\sigma \mid p$, so dass p nicht irreduzibel, also auch nicht prim ist. Das ist ein Widerspruch, denn mit π ist auch p prim in $\mathbb{Z}[i]$. Also gibt es kein Element der Norm p in $\mathbb{Z}[i]$ im zweiten Fall. □

Bevor wir die Primelemente von $\mathbb{Z}[i]$ genau beschreiben können, brauchen wir noch ein Lemma.

Lemma 3.11.30. *Sei p eine Primzahl der Form $p = 4k + 1$. Dann gibt es ein $u \in \mathbb{Z}$ mit $p \mid u^2 + 1$.*

Beweis. Wegen Korollar 3.11.23 ist -1 genau dann ein quadratischer Rest modulo p, wenn $p \equiv 1 \bmod 4$ gilt. Das ist hier der Fall. Also gibt es ein $u \in \mathbb{Z}$ mit $u^2 \equiv -1 \bmod p$, also mit $p \mid u^2 + 1$. □

Der folgende Satz beschreibt alle Primelemente des Ringes $\mathbb{Z}[i]$.

Satz 3.11.31. *Ein Repräsentantensystem der Primelemente in $\mathbb{Z}[i]$ bis auf Assoziierte ist gegeben durch folgende Elemente:*

(1) $1+i$,

(2) q, *für jede Primzahl* $q \equiv 3 \bmod 4$,

(3) $\pi = a+bi$ *und* $\overline{\pi} = a-bi$, *für jede Primzahl* $p \equiv 1 \bmod 4$ *mit* $p = a^2+b^2$ *und* $0 < a < b$.

Beweis. Nach Lemma 3.11.29 teilt jedes Primelement π von $\mathbb{Z}[i]$ eine Primzahl p, und es gilt dann entweder $N(\pi) = p$ oder $\pi \sim p$. Wir betrachten die möglichen Primzahlen p je nach ihrem Rest bei Division durch 4.

1. Fall: $p \equiv 2 \mod 4$. Das bedeutet $p = 2$. Der zweite Fall von Lemma 3.11.29 kann nicht auftreten, da es Elemente der Norm 2 gibt, nämlich genau die vier Elemente $\pi = \pm 1 \pm i$. Sie sind alle zueinander assoziiert, und wir können eines als Repräsentant auswählen. Man beachte, dass $2 = (1+i)(1-i)$ eine echte Faktorisierung ist, und daher 2 nicht prim und nicht irreduzibel ist.

2. Fall: $q \equiv 3 \mod 4$. Es gibt in $\mathbb{Z}[i]$ keine Elemente der Norm q, weil die Norm die Summe zweier Quadrate ist, also kongruent $0, 1, 2$ modulo 4 ist, aber nicht kongruent 3 modulo 4. Da ein nicht-trivialer Teiler von q in $\mathbb{Z}[i]$, also keine Einheit und nicht zu q assoziiert, die Norm q haben müsste, ist q irreduzibel und damit prim. Nach Lemma 3.11.30 sind alle Primteiler von q in $\mathbb{Z}[i]$ zu q assoziiert.

3. Fall: $p \equiv 1 \mod 4$. Nach Lemma 3.11.30 gibt es ein $u \in \mathbb{Z}$ mit $p \mid u^2+1$. Da p ein Teiler von $u^2+1 = (u+i)(u-i)$, aber nicht von $u \pm i$, kann p nicht prim in $\mathbb{Z}[i]$ sein. Also gibt es einen Primteiler $\pi = a+bi$ von p, und nach Lemma 3.11.29 gilt $p = N(\pi) = a^2+b^2$, also $p = (a+bi)(a-bi) = \pi\overline{\pi}$. Durch eventuelles Ändern der Vorzeichen oder Vertauschen von a und b können wir $0 < a < a$ erreichen. Da p ungerade ist, ist $|a| \neq |b|$. Da $N(\pi) = N(\overline{\pi}) = p$ prim ist, sind π und $\overline{\pi}$ beide prim in $\mathbb{Z}[i]$. Wegen $p = \pi\overline{\pi}$ sind alle Primteiler von p entweder zu π oder zu $\overline{\pi}$ assoziiert, die wiederum nicht zueinander assoziiert sind (die Assoziierten von π sind $a+bi$, $-b+ai$, $-a-bi$, $b-ai$).

Ist also π ein Primelement in $\mathbb{Z}[i]$, dann ist π ein Teiler einer Primzahl p, und

jeder Primteiler in $\mathbb{Z}[i]$ einer Primzahl ist zu genau einem der aufgelisteten Primelemente assoziiert. Damit sind wir fertig. □

Der Satz hat ein schönes Korollar über die Summe von zwei Quadratzahlen.

Korollar 3.11.32. *Sei p eine Primzahl mit $p \equiv 1 \bmod 4$. Dann gibt es eindeutig bestimmte $a, b \in \mathbb{Z}$ mit $0 < a < b$, und $p = a^2 + b^2$.*

Beweis. Die Existenz von ganzen Zahlen a, b mit $p = a^2 + b^2$ folgt aus $p = N(\pi) = a^2 + b^2$ wie oben im Satz. Wir zeigen noch die Eindeutigkeit. Es gelte auch $p = c^2+d^2$ mit $0 < c < d$. Mit $\pi = c+di$ gilt dann $\pi \mid p$. Dann hat man $\pi \sim a + bi$ oder $\pi \sim a - bi$ aus dem obigen Satz. Das bedeutet, dass sich c, d von a, b nur durch Vorzeichen oder Reihenfolge unterscheiden können. Durch die Bedingung $0 < c < d$ werden aber sowohl die Vorzeichen als auch die Reihenfolge eindeutig festgelegt. Also folgt $(c, d) = (a, b)$. □

So ist etwa $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, oder $17 = 1^2 + 4^2$. Allerdings ist $p = 7$ nicht die Summe zweier Quadratzahlen, und noch nicht einmal die Summe dreier Quadratzahlen. Dann braucht man 4 Quadrate, nämlich $7 = 1^2 + 1^2 + 1^2 + 2^2$. Das Korollar heißt auch *Zwei-Quadratesatz* für Primzahlen, und wurde von Pierre de Fermat formuliert und bewiesen. Der *allgemeine* Zwei-Quadratesatz lautet wie folgt.

Theorem 3.11.33 (Zwei-Quadratesatz)**.** *Eine natürliche Zahl $n \geq 1$ ist genau dann die Summe zweier Quadratzahlen, wenn in ihrer Primfaktorzerlegung jede Primzahl q der Form $4k + 3$ mit geradem Exponenten (auch der Exponent Null ist gerade) auftritt.*

Beweis. Wegen $N(a + bi) = a^2 + b^2$ ist die Menge der darstellbaren Zahlen n gerade $\{N(\alpha) \mid 0 \neq \alpha \in \mathbb{Z}[i]\}$. Wegen der Multiplikativität der Norm und weil $\mathbb{Z}[i]$ faktoriell ist, erhalten wir als Werte gerade alle Produkte von Normen $N(\pi)$ von Primelementen π. Diese Normen sind 2, und p für alle Primzahlen $p \equiv 1 \bmod 4$ und q^2 für alle Primzahlen $q \equiv 3 \bmod 4$. Aber n ist genau dann ein Produkt solcher Normen, wenn die Primzahlen q in der Primfaktorzerlegung von n mit geradem Exponenten vorkommen. □

Demnach ist 7 nicht die Summe zweier Quadratzahlen, 49 aber schon, nämlich $49 = 0^2 + 7^2$. In diesem Zusammenhang wollen wir die sogenannte *Brahmagupta-Identität* erwähnen.

Satz 3.11.34. *Für $a, b, c, d \in \mathbb{Z}$ gilt die Identität*

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

Beweis. In $\mathbb{Z}[i]$ gilt

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Nimmt man die Norm auf beiden Seiten, und wendet die Multiplikativität der Norm an, so erhält man die Identität. □

Zum Beispiel ist $(1^2 + 4^2)(2^2 + 7^2) = 26^2 + 15^2$.

Wie steht es mit der Darstellbarkeit von n als Summe von mehr als zwei Quadraten? Hier gibt es einen berühmten Satz von Lagrange. Er besagt, dass man jede natürliche Zahl n als Summe von *vier* Quadraten schreiben kann, also $n = a^2 + b^2 + c^2 + d^2$ gilt. Für den Beweis sind einige Vorbereitungen nötig. Zunächst sei

$$S := \{a^2 + b^2 + c^2 + d^2 \mid a, b, c, d \in \mathbb{Z}\}.$$

Wir brauchen nun den Ring $\mathbb{H}$ der *Quaternionen*, den Hamilton entdeckt hat. Dieser ist ein 4-dimensionaler $\mathbb{R}$-Vektoraum mit Basis $\{1, i, j, k\}$, der mit einem Algebraprodukt (Ringprodukt) versehen ist, das man nur auf der Basis definieren muss. Die Multiplikation $\mathbb{H} \times \mathbb{H} \to \mathbb{H}$, $(x, y) \mapsto xy$ ist $\mathbb{R}$-bilinear und erfüllt die Distributivgesetze. Die 1 ist das Einselements des Ringes, und die restlichen Produkte auf der Basis sind gegeben durch

$$\begin{aligned} &i^2 = j^2 = k^2 = -1, \\ &ij = k,\ jk = i,\ ki = j, \\ &ji = -k,\ kj = -i,\ ik = -j. \end{aligned}$$

Für eine Quaternion $\alpha = a + bi + cj + dk$ denifiert man die *konjugierte* Quaternion durch

$$\overline{\alpha} = a - bi - cj - dk.$$

Definition 3.29. Die *Norm* einer Quaternion $\alpha = a + bi + cj + dk$ is definiert als

$$N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2 + c^2 + d^2.$$

Die Konjugation ist ein bijektiver Anti-Ringhomomorphismus, d.h., es gilt $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$. Die Norm ist multiplikativ, wegen

$$N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\overline{\beta}\overline{\alpha} = \alpha N(\beta)\overline{\alpha} = \alpha\overline{\alpha}N(\beta) = N(\alpha)N(\beta).$$

Es ist leicht zu sehen, dass $U(\mathbb{H}) = \mathbb{H} \setminus 0$ ist. In der Tat, für $\alpha \neq 0$ gilt

$$\alpha^{-1} = \frac{1}{N(\alpha)}\overline{\alpha}.$$

Damit ist $\mathbb{H}$ fast ein Körper, wie $\mathbb{C}$. Allerdings ist die Gruppe $(\mathbb{H}^\times, \cdot)$ nicht kommutativ (wegen $ij = -ji$ etc.).

Definition 3.30. Der Unterring $\mathbb{Z}_\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z}\}$ von $\mathbb{H}$ heißt der *Ring der ganzzahligen Quaternionen.*

Es gilt $S = N(\mathbb{Z}_H)$. Nun können wir folgendes Lemma beweisen.

Lemma 3.11.35. *Die Menge S ist multiplikativ abgeschlossen. Das bedeutet, für $m, n \in S$ gilt auch $mn \in S$.*

Beweis. Seien $m, n \in S$. Dann gibt es $\alpha, \beta \in \mathbb{Z}_\mathbb{H}$ mit $N(\alpha) = m$ und $N(\beta) = n$. Also ist $mn = N(\alpha)N(\beta) = N(\alpha\beta) \in S$. □

Damit reduziert sich der Beweis, dass alle $n \in \mathbb{N}$ sich als Summe von vier Quadraten darstellen lassen auf Primzahlen. Wir können für das Lemma auch eine explizite Formel ableiten, nämlich aus der Gleichung $N(\alpha)N(\beta) = N(\alpha\beta)$.

Korollar 3.11.36. *Für $a, b, c, d \in \mathbb{Z}$ und $w, x, y, z \in \mathbb{Z}$ gilt*

$$\begin{aligned}(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) = {} & (aw + bx + cy + dz)^2 \\ & + (-ax + bw - cz + dy)^2 \\ & + (-ay + bz + cw - dx)^2 \\ & + (-az - by + cx + dw)^2.\end{aligned}$$

Wir brauchen ein Lemma, analog zum Lemma 3.11.30 für den Beweis des Zwei-Quadratesatz.

Lemma 3.11.37. *Sei p eine Primzahl. Dann gibt es $u, v \in \mathbb{Z}$ mit $u^2 + v^2 \equiv -1 \bmod p$ und $|u|, |v| \leq \frac{p}{2}$.*

Beweis. Für $p = 2$ können wir $u = 0$ und $v = 1$ nehmen. Sei also $p > 2$. Wir wollen $u, v \in \mathbb{F}_p$ finden mit $u^2 + v^2 = -1$, also mit $u^2 = -1 - v^2$. Die Menge $\{u^2 \mid u \in \mathbb{F}_p\}$ hat genau $\frac{p+1}{2}$ Elemente. Um das einzusehen, betrachten wir die Abbildung $q\colon \mathbb{F}_p \to \mathbb{F}_p$, $u \mapsto u^2$. Ihre Fasern sind entweder leer, haben ein Element (das passiert genau für 0), oder zwei Elemente u und $-u$ (denn $x^2 = a^2$ impliziert $x = \pm a$ in $\mathbb{F}_p$). Hier sind u und $-u$ verschieden, da $p > 2$ ist. Also werden die $p - 1$ Elemente von $\mathbb{F}_p^\times$ auf $\frac{p-1}{2}$ Werte abgebildet werden. Zusammen mit dem Wert 0 folgt also, dass die obige Menge genau $\frac{p+1}{2}$ Elemente hat. Da $a \mapsto -1 - a$ eine Bijektion ist, hat auch die Menge $\{-1 - v^2 \mid v \in \mathbb{F}_p\}$, genau $\frac{p+1}{2}$ Elemente. Da aber $\frac{p+1}{2} + \frac{p+1}{2} > p$, und $\mathbb{F}_p$ nur p Elemente hat, gilt nach dem Schubfachprinzip, dass

$$\{u^2 \mid u \in \mathbb{F}_p\} \cap \{-1 - v^2 \mid v \in \mathbb{F}_p\} \neq \emptyset$$

Das bedeutet, es gibt $u, v \in \mathbb{F}_p$ mit $u^2 = -1 - v^2$. Es gibt also ganze Zahlen $u, v \in \mathbb{Z}$ mit $u^2 + v^2 \equiv -1 \bmod p$. Wir können dabei u und v durch ihre betragsmässig kleinsten Reste modulo p erstetzen, ohne die Klasse modulo p zu ändern. Dann hat man auch $|u|, |v| \leq \frac{p}{2}$. □

Ein ganz ähnlicher Beweis zeigt auch, dass es für jedes $a \in \mathbb{F}_p$ Elemente $u, v \in \mathbb{F}_p$ gibt mit $u^2 + v^2 = a$. In $\mathbb{F}_p$ sind also alle Elemente die Summe zweier Quadrate. Nun können wir den Satz von Lagrange beweisen.

Satz 3.11.38 (Lagrange 1770)**.** *Jedes $n \in \mathbb{N}$ kann man in der Form*

$$n = a^2 + b^2 + c^2 + d^2$$

mit $a, b, c, d \in \mathbb{Z}$ schreiben.

Beweis. Da die Menge $S = N(\mathbb{Z}_{\mathbb{H}})$ multiplikativ ist, genügt es zu zeigen, dass jede Primzahl p in S liegt. Für $p = 2$ haben wir $2 = 0^2 + 0^2 + 1^2 + 1^2$. Sei also $p > 2$. Nach Lemma 3.11.37 gibt es $u, v \in \mathbb{Z}$ mit $|u|, |v| \leq \frac{p}{2}$ und $p \mid 1^2 + u^2 + v^2$. Also gibt es ein m mit $0^2 + 1^2 + u^2 + v^2 = mp \in S$, und

$$1 \leq m \leq \frac{1 + (p/2)^2 + (p/2)^2}{p} < p.$$

Wir können also jedenfalls ein Vielfaches von p als Summe von vier Quadraten schreiben. Sei nun $m \geq 1$ *minimal* mit $mp \in S$. Wir müssen $m = 1$

zeigen. Wir führen einen Beweis durch Widerspruch und nehmen an, dass $m > 1$ gilt. Sei $\alpha = a + bi + cj + dk \in \mathbb{Z}_{\mathbb{H}}$ mit $N(\alpha) = mp$. Wir betrachten $\beta = A + Bi + Cj + Dk$ modulo k, indem wir $A, B, C, D \in \mathbb{Z}$ wählen mit $|A|, |B|, |C|, |D| \leq \frac{m}{2}$, und mit $\beta \equiv \overline{\alpha} \bmod m$, also mit

$$A \equiv a,\ B \equiv -b,\ C \equiv -c,\ D \equiv -d \bmod m.$$

Dann haben wir

$$\begin{aligned} N(\beta) &= A^2 + B^2 + C^2 + D^2 \leq 4 \cdot (m/2)^2 = m^2, \\ N(\beta) &\equiv a^2 + b^2 + c^2 + d^2 = N(\alpha) \equiv 0 \bmod m. \end{aligned}$$

In der Ungleichung kann aber keine Gleichheit gelten. Denn sonst muss $m = 2r$ gerade sein, und $A, B, C, D = \pm r$. Dann ist auch $a, b, c, d \equiv r \bmod 2r$, und a, b, c, d sind alle durch r teilbar. Dann kann man

$$a = ra', b = rb', c = rc', d = rd'$$

schreiben, mit a', b', c', d' ungerade. Dann ist

$$mp = a^2 + b^2 + c^2 + d^2 = r^2((a')^2 + (b')^2 + (c')^2 + (d')^2)$$

durch $m^2 = 4r^2$ teilbar, weil $(a')^2, \ldots (d')^2$ ja kongruent 1 modulo 4 sind. Aber $m^2 \mid mp$ ist ein Widerspruch, da m wegen $1 < m < p$ kein Teiler von p ist, da p prim ist. Ebenso folgt, dass A, B, C, D nicht alle Null sein können. Die Kongruenz oben für $N(\beta)$ ist

$$A^2 + B^2 + C^2 + D^2 \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \bmod m,$$

und es gilt $A^2 + B^2 + C^2 + D^2 = mm'$ mit $0 < m' < m$. Die Fälle $m' = m$ und $m' = 0$ haben wir gerade ausgeschlossen. Nun ist

$$\begin{aligned} m^2 m' p &= (a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) \\ &= (aA - bB - cC - dD)^2 \\ &+ (aB + bA + cD - dC)^2 \\ &+ (aC + cA - bD + dB)^2 \\ &+ (aD + dA + bC - cB)^2. \end{aligned}$$

Die vier Quadrate auf der rechten Seite sind alle durch m^2 teilbar, weil der Ausdruck in jeder Klammer durch m teilbar ist. Also erhalten wir eine

Darstellung von $m'p$ als Summe von vier Quadraten, also $m' \in S$ mit $m' < m$. Das ist ein Widerspruch zur Minimalität von m. Also folgt $m = 1$ und wir sind fertig. □

Was kann man über ganze Zahlen n sagen, die als Summe von *drei* Quadraten darstellbar sind?

Theorem 3.11.39 (Gauß)**.** *Eine positive ganze Zahl n ist genau dann von der Form $n = a^2 + b^2 + c^2$ mit $a, b, c \in \mathbb{Z}$, wenn n nicht von der Form*

$$4^m(8k + 7)$$

mit ganzen Zahlen $k, m \geq 0$ ist.

Zum Beispiel ist $n = 15$ sehr wohl von der Form $8k + 7$, und $m = 0$. Und in der Tat, 15 ist nicht die Summe dreier Quadrate, wie man leicht nachprüft.

Der Satz ist viel schwerer zu beweisen, als der Zwei- und Vier-Quadrate Satz. Ein Grund ist, dass die Menge $S = \{a^2 + b^2 + c^2 \mid a, b, c \in \mathbb{Z}\}$ hier nicht multiplikativ abgeschlossen ist. Es ist $3, 5 \in S$, wegen $3 = 1^2 + 1^2 + 1^2$ und $5 = 0^2 + 1^2 + 2^2$, aber $15 = 3 \cdot 5 \notin S$. Weiterhin kann man erwähnen, dass nur eine Richtung schwierig ist. Wenn n von der Form $4^m(8k + 7)$ ist, zeigt eine Betrachtung modulo 8 recht schnell, dass n nicht die Summe von drei Quadraten sein kann. Für die anspruchsvolle Richtung kann man die Theorie binärer quadratischer Formen verwenden.