Algebra

Anton Deitmar

Sommer 2026

Inhaltsverzeichnis

1 Gruppen

1.1 Gruppenordnung

Definition 1.1.1. Sei G eine Gruppe und $S \subset G$ eine Teilmenge. Wir schreiben

$$\langle S \rangle$$

für die von S **erzeugte Untergruppe**, also

$$\langle S \rangle = \bigcap_{\substack{H \supset S \\ H \text{ Untergruppe von } G}} H.$$

Lemma 1.1.2. *Die Gruppe $\langle S \rangle$ besteht genau aus allen Gruppenelementen der Form $s_1 s_2 \cdots s_k$ wobei $k \in \mathbb{N}$ und für jedes j gilt*

$$s_j \in S \quad \textit{oder} \quad s_j^{-1} \in S.$$

Beweis. Sei $\widehat{S}$ die Menge all dieser Produkte in G. Dann gilt $\widehat{S} \subset \langle S \rangle$. Da aber $\widehat{S}$ selbst schon eine Gruppe ist, tritt $\widehat{S}$ in dem Schnitt auf und daher folgt Gleichheit. □

Definition 1.1.3. Ist G eine endliche Gruppe, so nennt man die Anzahl $|G|$ der Elemente die **Ordnung** der Gruppe G,

$$\operatorname{ord}(G) = |G|.$$

Wir schreiben auch 1 für das neutrale Element e einer Gruppe.

Ist $a \in G$, so bezeichnet $\langle a \rangle$ die von a **erzeugte Gruppe**, also die kleinste Untergruppe von G, die a enthält. Diese beschreibt man einmal als

$$\langle a \rangle = \bigcap_{\substack{H \text{ Untergruppe} \\ H \ni a}} H,$$

wobei man sich klarmachen muss, dass dies wieder eine Untergruppe ist. Andererseits kann man $\langle a \rangle$ konstruktiv beschreiben:

$$\langle a \rangle = \left\{ a^k : k \in \mathbb{Z} \right\}.$$

Ist $\langle a \rangle$ eine endliche Gruppe, so nennt man die Ordnung von $\langle a \rangle$ auch die **Ordnung** des Elements a und man schreibt

$$\operatorname{ord}(a) = \operatorname{ord}(\langle a \rangle) = |\langle a \rangle|.$$

Ist $\langle a \rangle$ nicht endlich, so setzt man $\operatorname{ord}(a) = \infty$.

Beispiele 1.1.4. (a) $\operatorname{Per}(n)$ ist die Gruppe der **Permutationen** der Menge $\{1, \ldots, n\}$. Sie hat die Ordnung

$$|\operatorname{Per}(n)| = n! = n(n-1)(n-2)\cdots 1.$$

(b) $\mathrm{Per}^+(n)$ ist die Untergruppe der **geraden Permutationen**, also

$$\begin{aligned}\mathrm{Per}^+(n) &= \{\sigma \in \mathrm{Per}(n) : \mathrm{sign}(\sigma) = 1\}\\ &= \{\tau_1\tau_2\cdots\tau_{2k} : \tau_1,\dots,\tau_{2k} \text{ Transpositionen}\}\end{aligned}$$

(c) Seien $n \in \mathbb{N}$, p eine Primzahl und $\mathbb{F}_p = \mathbb{Z}/p$ der Körper mit p Elementen. Die Gruppe $\mathrm{GL}_n(\mathbb{F}_p)$ aller invertierbaren $n \times n$ Matrizen hat die Ordnung

$$\begin{aligned}|\mathrm{GL}_n(\mathbb{F}_p)| &= (p^n-1)(p^n-p)\cdots(p^n-p^{n-1})\\ &= p^{1+2+\cdots+(n-1)}\,(p^n-1)(p^{n-1}-1)\cdots(p-1)\\ &= p^{\frac{n(n-1)}{2}}\,(p^n-1)(p^{n-1}-1)\cdots(p-1).\end{aligned}$$

Begründung: Die erste Spalte kann alle Elemente von $\mathbb{F}_p^n$ enthalten, außer ohne den Nullvektor, es gibt also p^n-1 mögliche erste Spalten. Die zweite Spalte kann alle Vektoren enthalten, außer den Vielfachen der ersten Spalte, also $p^n - p$ Vektoren und so weiter.

(d) Die Gruppe B_n aller oberen Dreiecksmatrizen in $\mathrm{GL}_n(\mathbb{F}_p)$ hat

$$|B_n| = (p-1)^n\, p^{\frac{n(n-1)}{2}}$$

Elemente.

(e) Sei $n \in \mathbb{N}$ dann ist

$$\begin{aligned}\mu_n &= \{e^{2\pi ik/n} : 0 \le k \le n-1\}\\ &= \{z \in \mathbb{C} : z^n = 1\}\end{aligned}$$

eine Untergruppe von $\mathbb{C}^\times$, die Gruppe der **n-ten Einheitswurzeln**. Sie hat die Ordnung n.

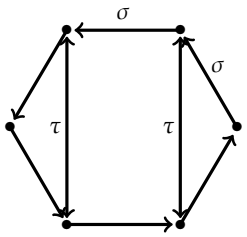
(f) Sei $n \in \mathbb{N}$ die **Diedergruppe** D_n, $n \ge 3$ der Ordnung $2n$ ist eine Gruppe erzeugt von zwei Elementen σ, τ mit den Relationen

$$\sigma^n = 1 = \tau^2 \quad \text{und} \quad \tau\sigma\tau^{-1} = \sigma^{-1}.$$

Insbesondere soll σ die Ordnung n haben und τ die Ordnung 2.
Das bedeutet, D_n besteht genau aus den Elementen

$$1, \sigma, \sigma^2, \dots, \sigma^{n-1}, \tau, \tau\sigma, \dots, \tau\sigma^{n-1}$$

und die Produkte dieser Elemente rechnet man mit den Relationen aus.
Man kann sie als Untergruppe von $\mathrm{Per}(n)$ wie folgt darstellen. Stellen wir uns die Elemente von $\{1, 2, \dots, n\}$ auf einem Kreis in gleichen Abständen angeordnet vor. Dann ist σ die Rotation um den Winkel $2\pi/n$ und τ ist irgendeine Spiegelung an einer Geraden, die die Menge $\{1, \dots, n\}$ in sich abbildet.



Es gilt $D_2 \cong \mathbb{Z}/2$, sowie $D_4 \cong (\mathbb{Z}/2) \times (\mathbb{Z}/2)$ und schliesslich

$$D_6 \cong \mathrm{Per}(3).$$

Lemma 1.1.5. *Sei a ein Element der Gruppe G. Die von a erzeugte Gruppe $\langle a\rangle$ ist genau dann endlich, wenn es ein $n \in \mathbb{N}$ gibt mit $a^n = 1$. Es gilt*

$$\mathrm{ord}(a) = \min\left\{n \in \mathbb{N} : a^n = 1\right\}.$$

Ist k die Ordnung von a so gilt für jedes $n \in \mathbb{N}$

$$a^n = 1 \quad \Leftrightarrow \quad k \mid n.$$

Definition 1.1.6. Eine Gruppe, die von einem Element erzeugt wird, nennen wir eine **zyklische Gruppe**.

Sind G, H zwei Gruppen, so wird das Produkt $G \times H$ durch die Vorschrift

$$(g,h)(g',h') = (gg',hh')$$

eine Gruppe. Das neutrale Element ist $(1,1)$. Das Inverse zu (g,h) ist (g^{-1},h^{-1}). Für die Ordnungen gilt

$$\operatorname{ord}(G \times H) = \operatorname{ord}(G)\operatorname{ord}(H).$$

Beispiel 1.1.7. Wir bezeichnen mit $\mathbb{Z}/m\mathbb{Z}$ oder auch $\mathbb{Z}/m$ die **zyklische Gruppe** mit m Elementen, $m \in \mathbb{N}$, also die Gruppe $\{0,1,2,\ldots,m-1\}$ mit Verknüpfung: $a \boxplus b$ = Rest von $a+b$ modulo m.

1.2 Nebenklassen

Definition 1.2.1. Sei G eine Gruppe und sei $H \subset G$ eine Untergruppe. Ist $a \in G$, so ist die **Linksnebenklasse** von a nach H gleich der Menge

$$aH = \{ah : h \in H\}.$$

Da H eine Gruppe ist, gilt für $h \in H$ schon

$$hH = H.$$

Wir schreiben

$$G/H$$

für die Menge der H-Nebenklasen in G.

Beispiele 1.2.2. (a) Ist V ein Vektorraum und $U \subset V$ ein Unterraum, dann sind die Nebenklassen nach U genau die affinen Räume $v+U$, die U als linearen Teil haben.

(b) Sei $G = D_n$ die Diedergruppe und sei $H = \langle\tau\rangle$ die von τ erzeugte Untergruppe, dann ist $H = \{1,\tau\}$ und die H-Linksnebenklassen sind

$$\underbrace{\{1,\tau\}}_{=H}, \underbrace{\{\sigma,\sigma\tau\}}_{=\sigma H}, \ldots, \underbrace{\{\sigma^{n-1},\sigma^{n-1}\tau\}}_{=\sigma^{n-1}H}.$$

(c) Seien $G = \mathrm{GL}_n(\mathbb{F}_p)$ und $H = B_n$, dann gibt es $p^{\frac{n(n-1)}{2}}$ Nebenklassen, also

$$|G/H| = p^{\frac{n(n-1)}{2}}$$

Begründung: Sei U die Untergruppe von $\mathrm{GL}_n(\mathbb{F}_p)$ bestehend aus allen unteren Dreiecksmatrizen mit Einsen auf der Diagonalen. Wir behaupten

$$G/H = \bigsqcup_{u \in U} uH.$$

In LinA beweist man $G = UH = \{uh : u \in U,\ h \in H\}$, so dass jede Nebenklasse in der Form uH geschrieben werden kann. Es bleibt zu zeigen, dass zwei verschiedene $u, u' \in U$ zwei verschiedene Nebenklassen liefen. Es gelte also $uH = u'H$. Dann ist $u^{-1}u' \in H$ aber gleichzeitig ist $u^{-1}u' \in U$ und damit $u^{-1}u' = I$ also $u = u'$ wie gewünscht.

Lemma 1.2.3. *Sei G eine Gruppe und H eine Untergruppe. Die Anzahl der Nebenklassen $|G/H| \in \mathbb{N} \cup \{\infty\}$ wird der* **Index** *von H in G genannt. Zwei Linksnebenklassen sind entweder gleich oder disjunkt, daher kann man G disjunkt in seine Nebenklassen zerlegen, es gibt also eine Familie $(x_i)_{i\in I}$ in G so dass*

$$G = \bigsqcup_{i\in I} x_i H.$$

Beweis. Sei $xH \cap yH \neq \emptyset$. Wir zeigen $xH \subset yH$. Aus Symmetrie folgt dann die andere Richtung. Sei also $z \in xH \cap yH$, dann existieren $h_1, h_2 \in H$ so dass $z = xh_1 = yh_2$. Es folgt $x = yh_2h_1^{-1} \in yH$ und ist $u \in xH$, also $u = xh_3$, so folgt $u = xh_3 = y\underbrace{h_2h_1^{-1}h_3}_{\in H} \in yH$. □

Beispiele 1.2.4. (a) Sei $G = D_n$ die Diedergruppe und sei $H = \langle\tau\rangle$ die von τ erzeugte Untergruppe, dann ist $|G/H| = n$.

(b) Seien $G = \mathrm{GL}_n(\mathbb{F}_p)$ und $H = B_n$, dann ist der Index $|G/H| = p^{\frac{n(n-1)}{2}}$.

Proposition 1.2.5. *Sei G eine endliche Gruppe. Ist H eine Untergruppe, dann ist die Ordnung $|H|$ ein Teiler der Ordnung $|G|$ von G. Genauer gilt*

$$|G| = |H||G/H|,$$

wobei G/H die Menge aller Nebenklassen aH ist.

Insbesondere gilt für jedes Element x

$$\mathrm{ord}(x) \mid \mathrm{ord}(G),$$

d.h., die Ordnung von x teilt die Gruppenordnung. Insbesondere folgt

$$x^{\mathrm{ord}(G)} = 1.$$

Beweis. Wir haben $G = \bigsqcup_{i\in I} x_iH$, und da G endlich ist, muss I endlich sein, wir finden also $x_1, \ldots, x_n \in G$ so dass $G = \bigsqcup_{j=1}^{n} x_jH$. Also folgt

$$\mathrm{ord}(G) = \sum_{j=1}^{n} |x_jH|.$$

Die Untergruppe H bildet selbst eine Nebenklasse, wir können also $x_1 = e$ annehmen. Die Abbildung $h \mapsto x_jH$ ist eine Bijektion von H nach x_jH, also haben alle Nebenklassen gleich viele Elemente, nämlich $\mathrm{ord}(H)$ viele, es ist also

$$\mathrm{ord}(G) = \sum_{j=1}^{n} \mathrm{ord}(H) = n\,\mathrm{ord}(H).$$

Ist $a \in G$ ein beliebiges Element und ist $H = \langle a\rangle$ die von a erzeugte Untergruppe, dann ist $\mathrm{ord}(a) = \mathrm{ord}(H)$ ein Teiler von $\mathrm{ord}(G)$. □

Lemma 1.2.6. *Ist G eine abelsche Gruppe und $a, b \in G$ von endlichen Ordnungen m, n. Sind m und n teilerfremd, dann ist $\langle ab\rangle = \langle a, b\rangle$ und hat die Ordnung mn.*

Beweis. Wegen $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = 1$ hat ab endliche Ordnung k und diese ist ein Teiler von mn. Es gilt dann $1 = (ab)^k = a^k b^k$, also $a^k = b^{-k}$. Die Ordnung von a^k ist ein Teiler von m, die Ordnung von b^{-k} ist ein Teiler von n, daher müssen beide Ordnungen gleich 1 sein, also $a^k = 1 = b^k$. Damit ist k ein Vielfaches von m und von n, die Ordnung von ab ist also mn.

Es bleibt zu zeigen, dass $a, b \in \langle ab\rangle$. Da m un n teilerfremd sind, gibt es $x, y \in \mathbb{Z}$ mit $1 = mx + ny$. Daher ist $a = a^1 = a^{mx}a^{ny} = (a^n)^y$. Damit folgt $(ab)^{ny} = a^{ny}b^{ny} = a^{ny} = a$ und daher liegt a in der von ab erzeugten Gruppe. Aus Symmetriegründen gilt dasselbe für b. □

1.3 Homomorphismen und Operationen

Definition 1.3.1. Eine Abbildung $\phi : G \to H$ zwischen zwei Gruppen heisst **Gruppenhomomorphismus**, falls

$$\phi(ab) = \phi(a)\phi(b)$$

für alle $a, b \in G$ gilt.

Beispiele 1.3.2. (a) Die aus der LinA bekannt Signum-Abbildung sign : $\mathrm{Per}(n) \to \{\pm 1\}$ ist ein Gruppenhomomorphismus.

(b) Ist G eine abelsche Gruppe und ist $n \in \mathbb{N}$, dann ist

$$x \mapsto x^n$$

ein Gruppenhomomorphismus $G \to G$, denn $(ab)^n = a^n b^n$.

(c) Die natürliche Abbildung $\phi : \mathrm{Per}(n) \to \mathrm{Per}(n+1)$ ist ein Gruppenhomomorphismus.

(d) Die Determinante $\det : \mathrm{GL}_n(\mathbb{F}_p) \to \mathbb{F}_p^\times$ ist ein Gruppenhomomorphismus.

(e) Die Abbildung $\mathrm{GL}_n(\mathbb{F}_p) \to \mathrm{GL}_{n+1}(\mathbb{F}_p)$, $A \mapsto \begin{pmatrix} A & \\ & 1 \end{pmatrix}$ ist ein Gruppenhomomorphismus.

(f) Ist G eine Gruppe und ist $a \in G$, dann ist die Abbildung

$$\phi : x \mapsto axa^{-1}$$

Ein Homomorphismus von G nach G. Wir nenne diesen Homomorphismus die **Konjugation** mit a.

Beweis. Für $x, y \in G$ gilt $\phi(xy) = axya^{-1} = axa^{-1}aya^{-1} = \phi(x)\phi(y)$. □

(g) Sei G die Gruppe $\mathrm{GL}_n(K)$ aller invertierbarer $n \times n$ Matrizen über dem Körper K. Dann ist die Abbildung $\psi : G \to G$,

$$\psi(A) = A^{-t} = (A^t)^{-1} = (A^{-1})^t$$

ein Gruppenhomomorphismus.

Definition 1.3.3. Ein Gruppenhomomorphismus $f : G \to H$ heisst **Isomorphismus**, wenn es einen Gruppenhomomorphismus $g : H \to G$ gibt so dass $f \circ g = \mathrm{Id}_H$ und $g \circ f = \mathrm{Id}_G$ ist.
Zwei Grupen G, H heißen **isomorph**, falls es einen Isomorphismus zwischen Ihnen gibt. Wir schreiben in diesem Fall $G \cong H$.

Lemma 1.3.4. *Ein Gruppenhomomorphismus $f : G \to H$ ist genau dann ein Isomorphismus, wenn die Abbildung f bijektiv ist.*

Beweis. Die Abbildung f ist genau dann bijektiv, wenn es eine Umkehrabbildung gibt. Die Aussage des Lemmas ist also die, dass die Umkehrabbildung automatisch ein Gruppenhomomorphismus ist. Sei hierzu $g : H \to G$ die Umkehrabbildung. Für $x, y \in H$ gilt

$$f(g(xy)) = xy = f(g(x))f(g(y)) = f(g(x)g(y))$$

und da f injektiv ist, folgt $g(xy) = g(x)g(y)$, also ist g ein Gruppenhomomorphismus. □

Lemma 1.3.5. *Ist $\phi : G \to H$ ein Gruppenhomomorphismus, dann gilt $\phi(1) = 1$ und $\phi(a^{-1}) = \phi(a)^{-1}$.*

Beweis. Übungsaufgabe Blatt 1. □

Definition 1.3.6. Sei G eine Gruppe und M eine Menge. Eine **Operation** von G auf M ist eine Abbildung

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

mit den Eigenschaften

- $1.m = m$ (das neutrale Element operiert neutral)
- $(ab).m = a.(b.m)$ (Operation und Multiplikation sind kompatibel)

Beispiele 1.3.7. (a) Sei G eine Gruppe. Dann definiert die Vorschrift

$$g.m = gm$$

eine Operation der Gruppe auf sich selbst, die **Linkstranslationsoperation**.

Beweis. Es gilt $1.m = 1m = m$ und $(ab).m = (ab)m = a(bm) = a.(b.m)$. □

(b) Sei G eine Gruppe, dann operiert G durch

$$g.m = mg^{-1}$$

auf sich selbst, dies ist die **Rechtstranslationsoperation**.

Beweis. Es gilt $1.m = m1^{-1} = m1 = m$ und $(ab).m = m(ab)^{-1} = (mb^{-1})a^{-1} = a.(b.m)$. □

(c) Sei G eine Gruppe, dann operiert G auf sich selbst durch die Vorschrift

$$g.m = gmg^{-1}$$

dies ist die **Konjugationsoperation**.

Beweis. Es gilt $1.m = 1m1^{-1} = m$ und $(ab).m = abm(ab)^{-1} = abmb^{-1}a^{-1} = a.(b.m)$. □

(d) (Abgeleitete Operationen.) Operiert die Gruppe G auf der Menge M und ist S eine weitere Menge, dann operiert G auf der Menge $A = \mathrm{Abb}(M, S)$ aller Abbildungen von M nach S durch

$$g.\phi(m) = \phi(g^{-1}.m).$$

Beweis. Es ist $e.\phi(m) = \phi(e^{-1}.m) = \phi(m)$ und $(ab).\phi(m) = \phi((ab)^{-1}.m) = \phi(b^{-1}.a^{-1}.m) = b.\phi(a^{-1}.m) = a.(b.\phi)(m)$. □

(e) Die Gruppe $\mathrm{GL}_n(\mathbb{F}_p)$ operiert durch Matrixmultiplikation auf $\mathbb{F}_p^n$. Dies folgt aus der Assoziativität der Matrixmultiplikation.

(f) Die Gruppe $\mathrm{GL}_n(\mathbb{F}_p)$ operiert auf $\mathrm{M}_n(\mathbb{F}_p)$ durch

$$x.a \coloneqq xax^t,$$

wobei x^t die transponierte Matrix ist.

Lemma 1.3.8. *Sei $M \neq \emptyset$ eine Menge. Operiert die Gruppe G auf der Menge M, dann ist die Abbildung $\phi : G \to \mathrm{Per}(M)$, $g \mapsto (m \mapsto gm)$ ein Gruppenhomomorphismus. Ist umgekehrt $\phi : G \to \mathrm{Per}(M)$ ein Gruppenhomomorphismus, dann definiert*

$$gm = \phi(g)(m)$$

eine Operation. Diese Zuordnungen (Operation)↦(Gruppenhomomorphismus) und umgekehrt sind invers zueinander. Also ist eine Operation dasselbe wie ein Gruppenhomomorphismus nach $\mathrm{Per}(M)$.

Beweis. Die Gruppe G operiere auf M. Für $g \in G$ sei $\phi(g) : M \to M$, $m \mapsto gm$. Zunächst müssen wir zeigen, dass $\phi(g)$ bijektiv ist, wir also wirklich in $\mathrm{Per}(M)$ landen. Wir behaupten, dass $\phi(g^{-1})$ eine Umkehrabbildung zu $\phi(g)$ ist. Dies folgt aus

$$\phi(g)(\phi(g^{-1})(m)) = \phi(g)(g^{-1}m) = gg^{-1}m = 1m = m$$

und

$$\phi(g^{-1})(\phi(g)(m)) = \phi(g^{-1})(gm) = g^{-1}gm = 1m = m.$$

Wir haben also in der Tat eine Abbildung $\phi : G \to \mathrm{Per}(M)$. Wir rechnen nun nach, dass dies ein Gruppenhomomorphismus ist. Für $g, h \in G$ gilt

$$\phi(gh)(m) = (gh)m = g(hm) = \phi(g)(hm) = \phi(g)(\phi(h)(m)) = \phi(g)\phi(h)(m).$$

Also ist ϕ ein Gruppenhomomorphismus. Die Umgekehrte Richtung ist leicht nachzurechnen und die Tatsache, dass diese Zuordnungen invers zueinander sind, auch. □

Definition 1.3.9. Die Gruppe G operiere auf der Menge M. Für gegebenes $m \in M$ ist die Menge

$$Gm = \left\{gm : g \in G\right\}$$

die **Bahn** oder das **Orbit** von m. Ferner ist

$$G_m = \left\{g \in G : gm = m\right\}$$

der **Stabilisator** von m.

Beispiele 1.3.10. (a) Sei G eine Gruppe. Operiert die Gruppe durch Linkstranslation auf sich selbst, also $g.x = gx$, dann ist der Stabilisator immer gleich $\{1\}$.

(b) In der Operation von $\mathrm{GL}_n(\mathbb{F}_p)$ auf $\mathbb{F}_p^n$ ist etwa der Stabilisator von $e_1 = (1, 0, \ldots, 0)$ gleich der Menge aller Martizen mit erster Spalte e_1.

Satz 1.3.11. *Die Gruppe G operiere auf der Menge M.*

(a) *Der Stabilisator eines Punktes $m \in M$ ist eine Untergruppe von G. Er wird auch die* **Standgruppe** *von m genannt.*

(b) *Sei $H = G_m$ die Standgruppe von m. Die Abbildung $gH \mapsto gm$ ist eine Bijektion von G/H zum Orbit von m.*

(c) *Die Orbiten zweier Punkte sind entweder gleich oder disjunkt, man kann deshalb M disjunkt in seine Orbiten zerlegen. Man schreibt $G\backslash M$ für die Menge aller Orbiten.*

(d) *(Bahnengleichung) Sind G und M endliche Mengen, so gilt*

$$|M| = \sum_{Gm \in G\backslash M} \frac{|G|}{|G_m|}.$$

Man kann Teil (c) auch so ausdrücken, dass man sagt: die Operation von G definiert eine Äquivalenzrelation auf M, wobei m und m' äquivalent heissen, falls sie in demselben Orbit liegen. Der Quotient nach dieser Äquivalenzrelation wird dann mit $G\backslash M$ bezeichnet.

Beweis. (a) Sei $H = G_m$, dann gilt offensichtlich $e \in H$. Sind $a, b \in H$, dann ist

$$(ab)m = a(bm) = am = m,$$

also liegt auch ab wieder in H. Ferner folgt aus $am = m$ durch Anwenden von a^{-1} schon $m = a^{-1}m$, so dass auch $a^{-1} \in H$ folgt. Also ist H eine Untergruppe.

(b) Sei $\psi : G/H \to Gm$ diese Abbildung. Zunächst ist festzustellen, dass sie überhaupt wohldefiniert ist, ist also $gH = g'H$, dann ist $g' = gh$ für ein $h \in H$ und damit ist $g'm = g(hm) = gm$, somit ist ψ wohldefiniert.
Injektivität. Sei $\psi(aH) = \psi(bH)$, dann ist $am = bm$ also $a^{-1}bm = m$, was soviel heisst wie $a^{-1}b \in H$ und somit $bH = aH$.
Surjektivität. Sei $z \in Gm$, also $z = gm$ für ein $g \in G$, dann folgt $z = \phi(gH)$.

(c) Sei $Gm \cap Gm' \neq \emptyset$, dann ist zu zeigen, dass $Gm = Gm'$ gilt. Sei $z \in Gm \cap Gm'$ dann existieren also $g, g' \in G$ so dass $gm = z = g'm'$. Es folgt $m' = (g')^{-1}gm$ so dass $m' \in Gm$ und damit $hm' \in Gm$ für jedes $h \in G$, was soviel heisst wie $Gm' \subset Gm$. Aus Symmetrie folgt die umgekehrte Inklusion.

(d) folgt aus (b) und (c). □

Definition 1.3.12. Sei G eine Gruppe. Das **Zentrum** $Z = Z(G)$ von G ist die Menge aller $x \in G$, die mit allen Elementen vertauschen, also

$$Z(G) = \left\{x \in G : xy = yx \ \forall_{y \in G}\right\}.$$

Beispiele 1.3.13. (a) Ist G abelsch, so gilt $Z(G) = G$ und umgekehrt.

(b) Ist $G = \mathrm{GL}_n(\mathbb{F}_p)$, dann besteht das Zentrum aus die Matrizen der Form λI, wobei $\lambda \in \mathbb{F}_p^\times$. Dies ist eine Übungsaufgabe der Linearen Algebra. (Man löse zuerst den Fall $n = 2$, dann sieht man auch den allgemeinen Beweis.)

(c) Ist $n \geq 3$, dann ist das Zentrum von $G = \mathrm{Per}(n)$ die triviale Gruppe.

Beweis. Sei σ im Zentrum von $\mathrm{Per}(n)$ und $n \geq 3$. Sei $1 \leq i \leq n$ und sei $1 \leq j \leq n$ von i und von $\sigma(i)$ verschieden. Dann vertauscht σ mit der Transposition $\tau = \tau_{i,j}$, die man als Zykel in der Form (i, j) schreibt. Es gilt also $\sigma(j) = \sigma(\tau(i)) = \tau(\sigma(i))$. Waere nun $\sigma(i)$ von i und j verschieden, dann waere $\sigma(j) = \tau(\sigma(i)) = \sigma(i)$, was der Injektivitaet von σ widerspricht! Damit muss $\sigma(i)$ gleich i oder j sein, der Fall j ist aber in der Annahme ausgeschlossen. Es folgt $\sigma(i) = i$ und also $\sigma = \mathrm{Id}$. □

(d) Das Zentrum der Gruppe B_n der oberen Dreiecksmatrizen ist $\mathbb{F}_p^\times I$ falls $p \neq 2$ und im Fall $p = 2$ ist es die Menge aller Matrizen der Form

$$\begin{pmatrix} 1 & & * \\ & \ddots & \\ & & 1 \end{pmatrix}$$

also rechts oben in der Ecke kann ein beliebiger Eintrag sein, ansonsten ist es die Einheitsmatrix.
Begründung: Sei A im Zentrum. Für $i < j$ ist $I + E(i, j) \in B_n$ und da A mit I vertauscht, vertauscht es auch mit $E = E(i, j)$. Für $z < s$ folgt

$$\sum_{k=1}^{n} E_{z,k}A_{k,s} = \big(EA\big)_{z,s} = \big(AE\big)_{z,s} = \sum_{k=1}^{n} A_{z,k}E_{k,s}. \qquad (*)$$

Ist $i \neq z$ und $j \neq s$, sind beide Seiten Null. Für $i = z < j \leq s$ folgt

$$A_{j,s} = \begin{cases} 0 & j \neq s, \\ A_{i,i} & j = s. \end{cases}$$

Der Fall $j = s$ ergibt $A_{j,j} = A_{i,i}$, so dass alle Diagonaleinträge gleich sind. Der Fall $j < s$ liefert $A_{j,s} = 0$ und da j alle Werte $> z \geq 1$ annahmen kann, folgt $A_{z,s} = 0$, falls $z > 1$, das heißt, wir haben die behauptete Gestalt unterhalb der ersten Zeile.
Werten wir $(*)$ für $j = s$ und $z \neq i$ aus, so erhalten wir $0 = A_{z,i}$. Diese Gleichung enthält nur dann neue Informationen, wenn $z < i$. Uns fehlt aber nur der Fall $z = 1$ und in diesem Fall ist wegen $i < j$ die erste Zeile Null bis auf die letzte Position, damit haben wir A in der Gestalt

$$\begin{pmatrix} \lambda & & * \\ & \ddots & \\ & & \lambda \end{pmatrix}$$

mit einem $\lambda \in \mathbb{F}_p^\times$. Im Fall $p = 2$ muss $\lambda = 1$ sein und es muss nur noch gezeigt werden, dass jede Matrix dieser Form zentral ist, was man schnell nachrechnet. Im Fall $p \neq 2$ sei $\mu \in \mathbb{F}_p^\times$ und $M = \mathrm{diag}(\mu, 1, \ldots, 1)$ die Diagonalmatrix mit den Eintägen $\mu, 1, \ldots, 1$. Dann gilt $AM = MA$ und wir folgern

$$A_{1,n} = (AM)_{1,n} = (MA)_{1,n} = \mu A_{1,n}.$$

da dies fu4r jedes μ gilt und es wegen $p > 2$ ein $\mu \neq 1$ gibt, folgt $A_{1,n} = 0$.

(e) Das Zentrum der Diedergruppe D_n, $n \geq 3$ ist trivial, wenn n ungerade ist und es ist $\{1, \sigma^{n/2}\}$, wenn n gerade ist.
Begründung: Sei zunächst n ungerade, wegen $\tau\sigma\tau^{-1} = \sigma^{-1}$ folgt $\tau\sigma^k\tau^{-1} = \sigma^{-k}$ für jedes $k \in \mathbb{Z}$. Eine Potenz σ^k wird also nur dann im Zentrum liegen, wenn $\sigma^k = \sigma^{-k}$, oder $\sigma^{2k} = 1$. Da die Ordnung von σ gleich n ist, passiert das genau dann, wenn n gerade ist und $k = n/2$. Das bedeutet, für gerades n ist $\sigma^{n/2}$ ist die einzige Potenz $\neq 1$ von σ, die im Zentrum liegt und für ungerades n liegt keine im Zentrum. Die verbleibenden Elemente sind von der Form $\tau\sigma^k$ und wenn so eines im Zentrum liegt, gilt

$$\tau\sigma^k = \tau\big(\tau\sigma^k\big)\tau^{-1} = \tau\big(\tau\sigma^k\tau^{-1}\big),$$

so dass dann σ^k im Zentrum liegen muss. Es gilt dann aber

$$\begin{aligned} \tau\sigma^k &= \sigma\big(\tau\sigma^k\big)\sigma^{-1} \\ &= \tau\sigma^{-1}\sigma^k\sigma^{-1} = \tau\sigma^{k-2}. \end{aligned}$$

Da aber $n \geq 3$ folgt $k - 2 \not\equiv k$ modulo n und daher liegt $\tau\sigma^k$ nicht im Zentrum. □

Definition 1.3.14. Wir lassen nun die endliche Gruppe G durch Konjugation auf sich selbst operieren und wenden die Bahnengleichung an. Die Orbiten unter der Konjugation heissen auch **Konjugationsklassen**. Die Konjugationsklasse des Elementes $x \in G$ ist also die Menge

$$[x] = \left\{ yxy^{-1} : y \in G \right\}.$$

Satz 1.3.15 (Klassengleichung)**.** *Sei G eine endliche Gruppe mit Zentrum Z und sei $x_1, \ldots, x_n$ ein Vertretersystem der Konjugationsklassen von $G \setminus Z$. Dann gilt*

$$\operatorname{ord}(G) = \operatorname{ord}(Z) + \sum_{j=1}^{n} \frac{|G|}{|G_{x_j}|},$$

wobei G_{x_j} der **Zentralisator** *von x_j ist:*

$$G_{x_j} = \left\{ y \in G : yx_j = x_j y \right\}.$$

Beweis. Dies ist die Bahnengleichung auf die Konjugationsoperation angewendet. □

Beispiele 1.3.16. (a) Die Konjugationsklassen in Per(n) sind gut zu beschreiben: Man schreibt ein gegebenes Element σ als Produkt disjunkter Zykel $\sigma = Z_1 \cdots Z_k$. Da diese Zykel disjunkt sind, vertauschen sie miteinander und man kann sie so anordnen, dass für die Längen gilt $\ell(Z_1) \geq \cdots \geq \ell(Z_k)$. Zwei Elemente σ und τ sind genau dann konjugiert, wenn für ihre so normalisierten Zykeldarstellungen $\sigma = Z_1 \cdots Z_k$ und $\tau = W_1 \cdots W_l$ gilt $k = l$ und $\ell(Z_j) = \ell(W_j)$ für alle $1 \leq j \leq k$. Das bedeutet, dass diese Zahlentupel genau die Konjugationsklassen liefern. Sei also $\mathcal{Z}$ die Menge aller Tupel $\langle m_1, \ldots, m_k \rangle$ mit $m_1 \geq m_2 \geq \cdots \geq m_k \geq 2$ und $m_1 + \cdots + m_k \leq n$. Dann steht $\mathcal{Z}$ in Bijektion zur Menge aller nichttrivialen Konjugationsklassen in Per(n). Die Klassen in Per(3) sind dann gegeben durch

$$\langle 2 \rangle, \langle 3 \rangle,$$

es gibt also zwei Konjugationsklassen in Per(3). Für G = Per(4) gibt es

$$\langle 2 \rangle, \langle 2, 2 \rangle, \langle 3 \rangle, \langle 4 \rangle$$

also gibt es 4 Konjugationsklassen. Repräsentanten für diese Klassen sind (in Zykelschreibweise)

$$(1,2) \quad (1,2)(3,4) \quad (1,2,3) \quad (1,2,3,4)$$

Der Zentralisator von $(1,2)$ ist die disjunkte Vereinigung zweier Nebenklassen H, $(1,2)H$, wobei H die Gruppe aller Permutationen ist, die $\{1,2\}$ punktweise festhalten. Daher permutiert H nur 3 und 4, so dass $|H| = 2$ und daher hat der Zentralisator $G_{(1,2)}$ zusammen 4 Elemente. Ebenso bestimmt man die Ordnungen der anderen Zentralisatoren

$$|G_{(1,2)(3,4)}| = 4, \quad |G_{(1,2,3)}| = 3, \quad |G_{(1,2,3,4)}| = 8.$$

die Klassengleichung liest sich dann

$$24 = 1 + \frac{24}{4} + \frac{24}{4} + \frac{24}{3} + \frac{24}{8} = 1 + 6 + 6 + 8 + 3$$

(b) Die Konjugationsklassen von $G = \mathrm{GL}_n(\mathbb{F}_p)$ zu bestimmen, ist aufwändiger. Ersetzt man $\mathbb{F}_p$ durch einen algebraisch abgeschlossenen Körper, so liefert der Jordan-Normalform-Satz das Gewünschte.

1.4 Zyklische Gruppen

Eine Gruppe G heisst **zyklisch**, wenn G von einem Element erzeugt ist.

Beispiele 1.4.1.
- Die Gruppe $(\mathbb{Z}, +)$ ist zyklisch von unendlicher Ordnung.
- Für jedes $n \in \mathbb{N}$ gibt es eine zyklische Gruppe der Ordnung n, nämlich $\mathbb{Z}/n$.

Proposition 1.4.2. *Ist G zyklisch, dann ist G isomorph zu $\mathbb{Z}$ oder zu $\mathbb{Z}/n$, wobei $n = \mathrm{ord}(G)$.*

Mit anderen Worten, alle unendlichen zyklischen Gruppen sind isomorph und eine endliche zyklische Gruppe ist durch ihre Ordnung festgelegt.

Beweis. Sei G zyklisch und sei τ ein Erzeuger.

1. Fall. τ hat endliche Ordnung $n \in \mathbb{N}$. Dann ist die Abbildung $\mathbb{Z}/n \to G$, $k \mapsto \tau^k$ ein Gruppenisomorphismus.
2. Fall. τ hat keine endliche Ordnung. Dann ist die Abbildung $\mathbb{Z} \to G$, $k \mapsto \tau^k$ ein Isomorphismus. □

Fangen wir an mit Gruppen der Ordnung 1. Diese sind alle isomorph zu $\{1\}$, damit ist dieser erste Schritt abgeschlossen. Bevor wir uns mit den Ordnungen 2 und 3 herumschlagen, beweisen wir lieber einen Satz.

Satz 1.4.3. *Sei p eine Primzahl. Jede Gruppe der Ordnung p ist zyklisch, also isomorph zu der Gruppe $\mathbb{Z}/p$.*

Beweis. Sei G eine Gruppe der Ordnung p. Sei $e \neq \tau \in G$. Dann muss $\mathrm{ord}(\tau)$ ein Teiler von p sein. Da $\tau \neq e$, ist die Ordnung $\neq 1$, also ist $\mathrm{ord}(\tau) = p$, damit hat die zyklische Untergruppe $\langle\tau\rangle$, die von τ erzeugt wird, die Ordnung p, ist also gleich G. □

Satz 1.4.4. *Es gibt bis auf Isomorphie zwei Gruppen der Ordnung 4, die zyklische $\mathbb{Z}/4$ und die* **Kleinsche Vierergruppe** $(\mathbb{Z}/2) \times (\mathbb{Z}/2)$.

Beweis. Sei G eine Gruppe der Ordnung 4, die nicht zyklisch ist. Das bedeutet, dass jedes Element $\neq e$ die Ordnung 2 haben muss. Sei also a ein nichttriviales Element. Die Untergruppe $H = \langle a\rangle$ hat Index 2, ist also normal. sei $b \in G$, so folgt $bHb^{-1} = H$, da H nur aus zwei Elementen, e und a besteht, folgt $bab^{-1} = a$, also ist G abelsch. Seien nun a, b zwei verschiedene Elemente von $G \setminus \{e\}$. Dann liefert die Abbildung $(\mathbb{Z}/2) \times (\mathbb{Z}/2) \to G$, $(i, j) \mapsto a^i b^j$ einen injektiven Gruppenhomomorphismus. Das Bild hat Ordnung 4, ist also G und G damit isomorph zur Vierergruppe. □

1.5 Normalteiler

Definition 1.5.1. Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Der **Kern** von ϕ ist die Menge

$$\ker(\phi) = \{g \in G : \phi(g) = 1\}.$$

Lemma 1.5.2. *Ein Gruppenhomomorphismus $\phi : G \to H$ ist genau dann injektiv, wenn der Kern trivial ist.*

Proof. Ist ϕ injektiv und ist x im Kern, dann ist $\phi(x) = \phi(1)$, also $x = 1$, d.h., der Kern ist trivial. Ist umgekehrt der Kern trivial und ist $\phi(x) = \phi(y)$, dann ist $\phi(y^{-1}x = \phi(y)^{-1}\phi(x) = \phi(x)^{-1}\phi(x) = 1$, also ist $y^{-1}x = 1$, d.h., $x = y$. □

Lemma 1.5.3. *Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Dann ist der Kern N eine Untergruppe von G mit der Eigenschaft, dass*

$$gNg^{-1} = N$$

für alle $g \in G$ gilt.

Definition 1.5.4. Eine Untergruppe $N \subset G$ mit der Eigenschaft aus dem Lemma heisst **Normalteiler** von G.

Beweis des Lemmas. Es reicht zu zeigen, dass $gNg^{-1} \subset N$ ist, denn dies gilt dann ja für jedes g, also auch für g^{-1}, also $g^{-1}Ng \subset N$. Daraus folgt durch Rechtsmultiplikation mit g, dass $Ng \subset gN$ und hieraus $N \subset gNg^{-1}$.

Sei also $n \in N$, d.h., $\phi(n) = 1$. Dann gilt für beliebiges $g \in G$:

$$\phi(gng^{-1}) = \phi(g)\phi(n)\phi(g)^{-1} = \phi(g)1\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = 1,$$

also ist $gng^{-1} \in N$ wie verlangt. □

Beispiele 1.5.5. (a) Ist G abelsch, dann ist jede Untergruppe ein Normalteiler.

(b) Sei $G = \mathrm{Per}(n)$. Dann ist $\mathrm{Per}^+(n)$ ein Normalteiler und dies ist der Einzige. Dies kann man anhand der Klassifikation der Konjugationsklassen durch die Zykelstruktur beweisen.

(c) Ist H eine Untergruppe von $\mathbb{F}_p^\times$, dann ist $\det^{-1}(H)$ ein Normalteiler von $\mathrm{GL}_n(\mathbb{F}_p)$.

(d) Die Abbildung $B_n \to \left(\mathbb{F}_p^\times\right)^n$, $\begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ & & \lambda_n \end{pmatrix} \mapsto (\lambda_1, \ldots, \lambda_n)$ ist ein Gruppenhomomorphismus. Ist H eine Untergrupe von $\left(\mathbb{F}_p^\times\right)^n$, dann ist das Urbild von H ein Normalteiler.

(e) Ist $D_n = \langle \sigma, \tau \rangle$ die Diedergruppe, dann ist jede Untergruppe $N \subset \langle \sigma \rangle$ ein Normalteiler, denn ist $\sigma^k \in N$, dann folgt $\tau\sigma^k\tau^{-1} = \sigma^{-k} \in N$.

(f) Ist G irgendeine Gruppe, dann ist das Zentrum Z von G stets ein Normalteiler.

Beweis. Sei $z \in Z$ und $g \in G$. Dann ist

$$gzg^{-1} = zgg^{-1} = z \in Z,$$

also folgt $gZg^{-1} = Z$. □

(g) Ist G eine Gruppe und H eine Untergruppe vom Index 2, dann ist H ein Normalteiler.

Beweis. Es gibt genau zwei Linksnebenklassen $G = H \sqcup sH$ mit einem beliebigen $s \in G \setminus H$, also ist $sH = G \setminus H$ und ebenso fuer Rechtsnebenklassen: $G = H \sqcup Hs$, also $sH = G \setminus H = Hs$, oder $sHs^{-1} = H$. Dies gilt fuer jedes $s \notin H$ und fuer $s \in H$ gilt es sowieso. □

Satz 1.5.6. *Ist $N \subset G$ ein Normalteiler, so lässt sich auf der Menge der Nebenklassen G/N genau eine Gruppenstruktur installieren, so dass die Projektion $G \to G/N$ ein Gruppenhomomorphismus ist.*

Ist umgekehrt $H \subset G$ eine Untergruppe mit einer Gruppenstruktur auf dem Nebenklassenraum G/H so dass die Projektion $G \to G/H$ ein Homomorphismus ist, dann ist H ein Normalteiler.

Insbesondere folgt, dass die Normalteiler genau die Kerne von Homomorphismen sind.

Beweis. Die zweite Aussage folgt sofort aus Lemma 1.5.3, beweisen wir also die erste. Sei N ein Normalteiler in G. Wir wollen eine Gruppenstruktur auf dem Nebenklassenraum G/N definieren durch

$$(aN)(bN) := abN.$$

Wir zeigen die Wohldefiniertheit: Sei $aN = a'N$ und $bN = b'N$, so ist zu zeigen, dass $abN = a'b'N$ gilt. Es gibt $n_1, n_2 \in N$ mit $a' = an_1$ und $b' = bn_2$. Da N ein Normalteiler ist, gilt

$$a'b' = an_1bn_2 = ab\underbrace{(b^{-1}n_1b)}_{\in N}n_2 \in abN,$$

also folgt $a'b'N \subset abN$ und aus Symmetriegründen folgt auch die umgekehrte Inklusion. Die so definierte Multiplikation definiert eine Gruppenstruktur auf G/N so dass die Projektion $G \to G/N$ ein Homomorphismus ist. Da dieser surjektiv ist, ist die Gruppenstruktur eindeutig bestimmt. □

Beispiele 1.5.7. (a) Sei $G = \mathbb{Z}$ und $N = m\mathbb{Z}$ für ein gegebenes $m \in \mathbb{N}$. Da G abelsch ist, ist die Untergruppe N normal. Der Quotient $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m$ ist eine endliche Gruppe der Ordnung m, die von einem Element, der 1, erzeugt wird.

(b) Die Gruppe $\mathrm{Per}(n)/\mathrm{Per}^+(n)$ hat zwei Elemente, ist also Isomorph zu $\{\pm 1\} \cong \mathbb{Z}/2$.

(c) Die Gruppe $\mathrm{GL}_n(\mathbb{F}_p)/\mathrm{SL}_n(\mathbb{F}_p)$ ist isomorph zu $\mathbb{F}_p^\times$. (Hierzu muss man nur zeigen, dass $\det : \mathrm{GL}_n(\mathbb{F}_p) \to \mathbb{F}_p^\times$ surjektiv ist, was aber aus $\det\begin{pmatrix} x & \\ & 1 \end{pmatrix} = x$ folgt.)

(d) Ist $G = D_n = \langle \sigma, \tau \rangle$ die Diedergruppe und ist $N = \langle \sigma \rangle$, dann ist G/N eine Gruppe der Ordnung 2, also isomorph zu $\mathbb{Z}/2$.

Proposition 1.5.8. *Sei G eine Gruppe mit Zentrum Z. Ist G/Z zyklisch, dann ist G abelsch, also $G = Z$ und G/Z ist trivial.*

Beweis. Sei $a \in G$, so dass G/Z von der Restklasse $[a]$ erzeugt wird. Sind dann $b, c \in G$ mit Restklassen $[b] = [a]^m$ und $[c] = [a]^n$, dann ist $b = a^m z$ und $c = a^n w$ mit $z, w \in Z$. Es folgt

$$bc = a^m z a^n w = a^n w a^m z = cb$$

und damit $[b][c] = [bc] = [cb] = [c][b]$ und G/Z ist abelsch. □

Korollar 1.5.9. *Sei G eine Gruppe und Z ihr Zentrum. Dann kann die Ordnung von G/Z keine Primzahl sein.*

Beweis. Wäre $\operatorname{ord}(G/Z)$ eine Primzahl, dann wäre G/Z nach Satz 1.4.3 zyklisch und damit nach Proposition 1.5.8 $G/Z = \{e\}$, Widerspruch! □

1.6 Homomorphiesätze

Lemma 1.6.1. *Sei $N \subset G$ ein Normalteiler und sei $\alpha : G \to H$ ein Gruppenhomomorphismus mit $\alpha(N) = \{1\}$. Dann ist die Abbildung $\beta : G/N \to H$, $\beta(xN) = \alpha(x)$ ein wohhldefinierter Gruppenhomomorphismus. Das Diagramm*

$$\begin{array}{ccc} G & \xrightarrow{p} & G/N \\ & \searrow^{\alpha} & \downarrow{\scriptstyle \beta} \\ & & H \end{array}$$

kommutiert, d.h., $\alpha = \beta p$, wobei p die Projektion ist.

Proof. Zur Wohldefiniertheit sei $xN = yN$, also $x = yn$ für ein $n \in N$, dann folgt $\alpha(x) = \alpha(yn) = \alpha(y)\alpha(n) = \alpha(y)$, also ist β wohldefiniert. Schliesslich ist wegen $\beta\Big((xN)(yN)\Big) = \beta(xyN) = \alpha(xy) = \alpha(x)\alpha(y) = \beta(xN)\beta(yN)$ die Abbildung β ein Gruppenhomomorphismus. □

Satz 1.6.2. *Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann ist das Bild eine Untergruppe und f induziert einen Isomorphismus*

$$\mu : G/\ker(f) \xrightarrow{\cong} \operatorname{Bild}(f).$$

Beweis. Die Existenz von μ folgt aus Lemma 1.6.1. Die Surjektivität ist klar, da $\mu(x\ker(f)) = f(x)$ mit beliebigem x. Zur Injektivität sei $x\Big(\ker(f)\Big)$ im Kern von ϕ. Das bedeutet $1 = \phi\Big(x\Big(\ker(f)\Big) = f(x)$, also $x \in \ker(f)$, also $x\ker(f) = \ker(f)$. Das bedeutet, $x\ker(f)$ ist die triviale Klasse, also ist μ injektiv. □

Satz 1.6.3. (a) *Sind M, N Normalteiler in G so dass $M \subset N$, dann ist N/M ein Normalteiler in G/M und die Projektion induziert einen Isomorphismus*

$$(G/M)\Big/(N/M) \xrightarrow{\cong} G/N.$$

(b) *Sind M, N Normalteiler in G, dann ist auch $N \cap M$ ein Normalteiler in G, ferner ist*

$$MN = \Big\{mn : m \in M,\ n \in N\Big\}$$

eine Untergruppe von G und die Abbildung $m(M \cap N) \mapsto mN$ ist ein Isomorphismus

$$M\Big/M \cap N \xrightarrow{\cong} MN\Big/N.$$

Beweis. (a) Nach Lemma 1.6.1 ist

$$\begin{aligned} \phi : G/M &\to G/N, \\ xM &\mapsto xN. \end{aligned}$$

ein wohldefinierter Gruppenhomomorphismus. Wenn wir zeigen, dass der Kern gerade die Gruppe $N/M \subset G/M$ ist, folgt die Aussage (a) aus Satz 1.6.2. Es gilt

$$\begin{aligned} xM \in \ker(\phi) &\Leftrightarrow 1 = \phi\Big(xM\Big) = xN \\ &\Leftrightarrow x \in N \Leftrightarrow xM \in MN/M. \end{aligned}$$

(b) Sei $a \in N \cap M$ und sei $x \in G$. Dann ist xax^{-1} in N, da N normal ist und auch in M, da M normal ist, also liegt xax^{-1} in $N \cap M$. Damit ist $N \cap M$ normal.

Seien $a, a_1 \in MN$, also etwa $a = mn$, $a_1 = m_1 n_1$. Dann gilt

$$a^{-1}a_1 = (mn)^{-1}m_1n_1 = n^{-1}m^{-1}m_1n_1 = \underbrace{\Big(m^{-1}m_1\Big)}_{\in M}\underbrace{\Big(m^{-1}m_1\Big)^{-1}n^{-1}m^{-1}m_1}_{\in N}\underbrace{n_1}_{\in N}$$

Daher ist $a^{-1}a_1 \in MN$, diese Menge also eine Untergruppe, da sie außerdem nicht leer ist.

Die Abbildung $\phi : M \to MN/N$, $m \mapsto mN$ ist ein surjektiver Gruppenhomomorphismus mit Kern $M \cap N$, so dass die Behauptung aus Satz 1.6.2 folgt. □

Korollar 1.6.4. *Allgemeiner gilt: Sind M, N Untergruppen von G und wird N von M normalisiert, d.h. gilt*

$$mNm^{-1} = N$$

für alle $m \in M$, dann ist MN eine Untergruppe von G.

Beweis. Klar. □

Man kann statt Linksnebenklassen natürlich auch **Rechtsnebenklassen** betrachten, sei also $H \subset G$ eine Untergruppe und $a \in G$ dann ist

$$Ha = \left\{ha : h \in H\right\}$$

die Rechtsnebenklasse von a. Genau wie bei den Linksnebenklassen zerfällt G in disjunkte Klassen.

Satz 1.6.5. (a) *Eine Untergruppe H von G ist genau dann ein Normalteiler, wenn die Rechts- und Linksnebenklassen übereinstimmen, wenn also für jedes $a \in G$ gilt*

$$aH = Ha.$$

(b) *Sei H eine Untergruppe von G vom Index 2, d.h. die Nebenklassenmenge G/H hat zwei Elemente. Dann ist H ein Normalteiler.*

Beweis. (a) Ist H ein Normalteiler, dann gilt $aHa^{-1} = H$, woraus durch Multiplikation von rechts mit a folgt $aH = Ha$. Die Umkehrung geht umgekehrt.

(b) Sei H eine Untergruppe vom Index 2. Die Gruppe G zerfällt in zwei Linksnebenklassen, H und der Rest, der dann $G \setminus H$ ist. Ebenso zerfällt G in zwei Rechtsnebenklasse H und $G \setminus H$. Also stimmen die Rechts- und Linksnebenklassen überein. □

1.7 Freie Gruppen

Definition 1.7.1. Sei S eine Menge.Sei $T = S \times \{1, -1\}$. Wir Schreiben $(s, \pm 1)$ als $s^{\pm 1}$, wobei wir den Exponenten 1 auch weglassen, also $s^1 = s$ schreiben. Ein **Wort** in T ist ein Element von T^n für ein $n \in \mathbb{N}_0$. Auf der Menge der Wörter $\mathcal{W}(T)$ gibt es eine Multiplikation durch "Hintereinanderschreiben", das Produkt von $(t_1, \dots, t_n)$ und $(t'_1, \dots, t'_k)$ ist $(t_1, \dots, t_n, t'_1, \dots, t'_k)$. Diese Multiplikation ist Assoziativ und das leere Wort ist neutral. Wir betrachten die Äquivalenzrelation erzeugt durch

$$(\dots, x, t, t^{-1}, z, \dots) \sim (\dots, x, z, \dots).$$

Dann ist $\mathcal{W}(T)/\sim$ eine Gruppe mit dem leeren Wort als neutralem Element, das wir auch als 1 schreiben. Dies ist die **freie Gruppe** $F(S)$ in der Erzeugermenge S. Wir schreiben $t_1 \cdots t_n$ statt $(t_1, \dots, t_n)$ Jedes Element $\neq 1$ von $F(S)$ lässt sich eindeutig in der Form

$$s_1^{k_1} s_2^{k_2} \cdots s_n^{k_n}$$

schreiben, wobei $n \in \mathbb{N}$ und $k_1, \dots, k_n \in \mathbb{Z} \setminus \{0\}$.

Wir fassen S als Teilmenge von $F(S)$ auf

Satz 1.7.2 (Universelle Eigenschaft)**.** *Jede Abbildung $\phi : S \to G$ in eine Gruppe G lässt sich eindeutig zu einem Gruppenhomomorphismus $\tilde{\phi} : F(S) \to G$ fortsetzen. Die Zuordnung $\phi \mapsto \tilde{\phi}$ ist eine Bijektion*

$$\mathcal{Z} : \mathrm{Abb}(S, G) \to \mathrm{Hom}(F(S), G).$$

Proof. Wir definieren die Fortsetzung durch

$$\tilde{\phi}(s_1^{k_1} \cdots s_n^{k_n}) := \phi(s_1)^{k_1} \cdots \phi(s_n)^{k_n},$$

wobei rechts das Produkt in G steht. Die Homomorphismuseigenschaft ist klar und ist $\psi : F(S) \to G$ eine weitere Fortsetzung von ϕ, so gilt

$$\begin{aligned} \psi(s_1^{k_1} \cdots s_n^{k_n}) &= \psi(s_1)^{k_1} \cdots \psi(s_n)^{k_n} \\ &= \phi(s_1)^{k_1} \cdots \phi(s_n)^{k_n} \\ &= \tilde{\phi}(s_1^{k_1} \cdots s_n^{k_n}), \end{aligned}$$

also $\psi = \tilde{\phi}$. Da die Einschränkung von $\tilde{\phi}$ auf die Teilmenge S gleich ϕ ist, ist die Zuordnung $\mathcal{Z}$ injektiv. Ist $\alpha : F(S) \to G$ ein Gruppenhomomorphismus, dann ist α eine Frotsetzung von $\phi := \alpha|_S : S \to G$ und nach der Eindeutigkeit folgt $\alpha = \tilde{\phi} = \mathcal{Z}(\phi)$ und $\mathcal{Z}$ ist demnach auch surjektiv. □

Korollar 1.7.3. *Jede Gruppe ist Quotient einer freien Gruppe, also von der Form $F(S)/N$ für einen Normalteiler $N \subset F(S)$.*

Proof. Sei G eine Gruppe und sei $S = G$ als Menge aufgefasst. Die Identität $G \to G$ setzt dann fort zu einem surjektiven Gruppenhomomorphismus $\alpha : F(S) \to G$, mit $N = \ker(\alpha)$ folgt dann also $G \cong F(S)/N$. □

1.8 Sylow-Gruppen

Definition 1.8.1. Sei G eine endliche Gruppe und p eine Primzahl. G heisst **p-Gruppe**, wenn die Ordnung von G eine p-Potenz ist.

Eine Untergruppe H von G heisst **p-Sylow-Gruppe**, wenn $\mathrm{ord}(H) = p^k$, $k \in \mathbb{N}$ und $\mathrm{ord}(G) = p^k m$ wobei m teilerfremd zu p ist. Das heisst, die Ordnung von H ist die maximale p-Potenz, die überhaupt in G auftreten kann.

Beispiel 1.8.2. Ist $G = \mathbb{Z}/n$ zyklisch und $n = p^k m$ mit $k \in \mathbb{N}$ und $p \nmid m$. Dann ist $m\mathbb{Z}/n \cong \mathbb{Z}/p^k$ die einzige p-Sylow-Gruppe von G.

Satz 1.8.3. *Sei G eine Gruppe der Ordnung p^k mit einer Primzahl p und $k \in \mathbb{N}$. Dann ist das Zentrum von G nichttrivial.*

Beweis. Betrachte die Klassengleichung

$$\operatorname{ord}(G) = \operatorname{ord}(Z) + \sum_{j=1}^{n} \frac{|G|}{|G_{x_j}|}.$$

Ist einer der Summanden $\frac{|G|}{|G_{x_j}|}$ gleich 1, dann ist für das betreffende x_j der Zentralisator $G_{x_j} = G$, was soviel bedeutet, dass x_j mit jedem $x \in G$ vertauscht, also ist x_j im Zentrum und das Zentrum ist damit nichttrivial. Wir koennen also annehmen, dass die Summanden $\frac{|G|}{|G_{x_j}|}$ ungleich 1. Da sie die Gruppenordnung teilen müssen, sind sie alle p-Potenzen, also folgt dass p die Summe $\sum_{j=1}^{n} \frac{|G|}{|G_{x_j}|}$ teilt. Daher muss p auch $\operatorname{ord}(Z)$ teilen. □

Beispiel 1.8.4. Sei $G = D_4$ die Diedergruppe mit 8 Elementen, also Erzeugern σ, τ und Relationen $\sigma^4 = 1 = \tau^2$ und $\tau\sigma\tau^{-1} = \sigma^{-1}$. Für $g = \sigma^2$ gilt dann $g^2 = 1$,sowie

$$g\sigma = \sigma g \qquad \text{und} \qquad \tau g \tau^{-1} = \tau\sigma^2\tau^{-1} = \sigma^{-2} = g^{-1} = g.$$

Damit vertauscht g mit beiden Erzeugern σ und τ, ist also zentral.

Korollar 1.8.5. *Sei p eine Primzahl und G eine Gruppe der Ordnung p^k für ein $k \in \mathbb{N}$. Dann gibt es eine Kette von normalen Untergruppen*

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_k = G,$$

so dass $\operatorname{ord}(G_j) = p^j$ *gilt. Also ist $G_j/G_{j-1} \cong \mathbb{Z}/p$ eine abelsche Gruppe.*

Insbesondere hat G für jedes $1 \leq j \leq k$ eine Untergruppe H der Ordnung p^j und es gibt ein Element der Ordnung p in G.

Beweis. Induktion nach k. Der Fall $k = 1$ ist klar.
$k \to k+1$: Wir wissen, dass G nicht-triviales Zentrum Z hat. Sei also $z_0 \in Z \setminus \{1\}$. Dann hat z_0 Ordnung p^l fuer ein $1 \leq l \leq k$ und damit hat $a := z_0^{p^{l-1}}$ die Ordnung p, also ist $G_1 := \langle a \rangle$ eine zentrale Untergruppe der Ordnung p. Nach Induktionsvoraussetzung hat G/G_1 eine solche Kette

$$1 = \overline{G}_1 \subset \overline{G}_2 \subset \cdots \subset \overline{G}_k = G/G_1$$

und wir definieren G_j als das Urbild von $\overline{G}_j$ unter der Projektion $G \mapsto G/G_1$. Dann ist $G_j \subset G$ der Kern von $G \to G/G_1 = \overline{G}_k \to \overline{G}_k/\overline{G}_j$ also normal und es gilt
$G_{j+1}/G_j \cong \left(G_{j+1}/G_1\right)\Big/\left(G_j/G_1\right) = \overline{G}_{j+1}/\overline{G}_j \cong \mathbb{Z}/p$. □

Satz 1.8.6. *Sei p eine Primzahl und G eine Gruppe der Ordnung p^2. Dann ist G abelsch, genauer ist*

$$G \cong \mathbb{Z}/p^2 \quad \textit{oder} \quad G \cong \mathbb{Z}/p \times \mathbb{Z}/p.$$

Beweis. Das Zentrum Z ist nichttrivial, also ist die Ordnung von G/Z gleich 1 oder p. Das zweite ist nach Korollar 1.5.9 (Die Ordnung von $G/Z(G)$ kann keine Primzahl sein) ausgeschlossen, also $G = Z$ und damit ist G abelsch.

Hat G ein Element der Ordnung p^2, dann ist G zyklisch und wir sind fertig. Andernfalls haben alle Elemente $\neq 1$ die Ordnung p. Sei dann $x \neq 1$ irgendein Element und y ein Element von $G \setminus \langle x \rangle$. Wir behaupten, dass die Abbildung

$$\begin{aligned} f : \mathbb{Z}/p \times \mathbb{Z}/p &\to G, \\ (i, j) &\mapsto x^i y^j \end{aligned}$$

ein Isomorphismus ist. Es ist nun allerdings ein Homomorphismus und das Bild enthält x und y und damit ist die Ordnung des Bildes größer als $\mathrm{ord}(\langle x \rangle) = p$. Da die Ordnung des Bildes aber p^2 teilen muss, ist sie gleich p^2 und damit ist f surjektiv. Da die Gruppen G und $(\mathbb{Z}/p)^2$ die gleiche Ordnung haben, ist f auch injektiv. □

Definition 1.8.7. Sei G eine Gruppe. Es gebe eine natürliche Zahl N so dass $x^N = 1$ für jedes $x \in G$ gilt. Dies ist zum Beispiel der Fall wenn G endlich ist. Die kleinste natuerliche Zahl N, fuer die dies der Fall ist, heisst der **Exponent** von G.

Beispiel 1.8.8. Die Gruppe $G = \prod_{j=1}^{\infty} \mathbb{Z}/2$ ist eine unendliche Gruppe vom Exponenten 2.

Lemma 1.8.9. (a) *Sei G eine endliche abelsche Gruppe vom Exponenten N. Dann teilt die Gruppenordnung eine Potenz von N.*

(b) *Sei G eine endliche abelsche Gruppe und p eine Primzahl, die die Gruppenordnung teilt. Dann enthält G ein Element der Ordnung p.*

Beweis. (a) Induktion nach der Gruppenordnung. Fuer die triviale Gruppe ist die Behauptung erfuellt.

Sei $b \in G$ ein nichttriviales Element und sei H die zyklische Gruppe erzeugt von b. Wegen $b^N = 1$ ist die Ordnung k von b ein Teiler von N und N ist auch ein Exponent von G/H. Nach Induktion teilt die Ordnung von G/H eine Potenz von N und wegen $|G| = |H|\,|G/H|$ gilt das auch für die Ordnung von G.

(b) Wir folgern nun, dass die abelsche Gruppe G mit $|G| = mp^k$, $k \geq 1$ ein Element x haben muss mit Ordnung np^l für ein $l \geq 1$. Waere dies nicht der Fall, waere m ein Exponent von G, was Teil (a) widerspricht.

Habe also das Element x die Ordnung np^l mit $l \geq 1$. Dann hat $y = x^{np^{l-1}}$ die Ordnung p. □

Satz 1.8.10 (Sylow)**.** *Sei G eine endliche Gruppe und p eine Primzahl.*

(a) *G enthält eine p-Sylow-Gruppe. Genauer ist jede p-Untergruppe H von G in einer p-Sylowgruppe enthalten.*

(b) *Alle p-Sylow-Gruppen von G sind zueinander konjugiert.*

(c) *Für die Anzahl s der p-Sylow-Gruppen gilt*

$$s \mid \mathrm{ord}(G), \quad s \equiv 1 \mod (p).$$

Beweis. (a): Wir zeigen die Existenz einer p-Sylowgruppe durch Induktion nach der Ordnung von G. Ist $p = |G|$ sind wir fertig. Sei also $|G| = p^k m$ mit $p \nmid m$. Ist H eine Untergruppe mit Index $|G/H|$ teilerfremd zu p, dann ist jede p-Sylow-Gruppe von H schon eine von G und wir sind fertig nach Induktion. Wir können also annehmen, dass jede echte Untergruppe einen Index hat, der von p geteilt wird. Die Klassengleichung sagt

$$p^k m = \mathrm{ord}(Z) + \sum_{j=1}^{n} |G/G_{x_j}|,$$

wobei Z das Zentrum von G ist und die x_j Vertreter der nichttrivialen Konjgationsklassen. Die Summanden rechts werden nach Voraussetzung alle von p geteilt, damit auch $\mathrm{ord}(Z)$. Nach Lemma 1.8.9 enthält Z ein Element z der Ordnung p. Sei dann S eine p-Sylow-Gruppe von $G/\langle z\rangle$ und sei $P : G \to G/\langle z\rangle$ die Projektion. Dann ist $P^{-1}(S)$ eine p-Sylow-Gruppe von G. Es gibt also eine p-Sylow-Gruppe.

(b): Sei nun $\mathcal{S}$ die Menge aller p-Sylow-Gruppen in G. Dann operiert G durch Konjugation auf $\mathcal{S}$. Sei $P \in \mathcal{S}$ und sei G_P der Stabilisator von P in G. Sei $\mathcal{S}_0 = G.P$ das Orbit von P und sei $H \subset G$ eine nichttriviale p-Gruppe. Dann operiert H auf dem Orbit $\mathcal{S}_0$ durch Konjugation und die Bahnengleichung sagt

$$\frac{|G|}{|G_P|} = |\mathcal{S}_0| = \sum_{\nu=1}^{N} \frac{|H|}{|H_{P_\nu}|},$$

wobei die P_ν durch ein Vertretersystem der H-Orbiten laufen. Da $P \subset G_P$, wird der Index $|G/G_P|$ nicht von p geteilt. Da $|H|$ eine p-Potenz ist, sind alle $\frac{|H|}{|H_{P_\nu}|}$ Potenzen von p, also muss für ein ν schon $H = H_{P_\nu}$ gelten. Also normalisiert H schon P_ν. Daher ist dann HP_ν eine Untergruppe von G mit P_ν als Normalteiler. Nach dem Homomorphiesatz folgt $HP_\nu/P_\nu \cong H/H \cap P_\nu$ so dass

$$|HP_\nu| = |P_\nu|\,|HP_\nu/P_\nu| = |P_\nu|\,|H/H \cap P_\nu|$$

eine p-Potenz ist. Da aber $|P_\nu|$ schon die maximal mögliche p-Potenz ist, folgt $HP_\nu = P_\nu$, also $H \subset P_\nu$. Damit ist (a) gezeigt. Wendet man dies auf $H = Q$ eine andere p-Sylow-Gruppe an, folgt wegen der Maximalität von Q, dass $Q = P_\nu$ sein muss, also sind alle p-Sylow-Gruppen in einem Orbit, sind also alle zueinander konjugiert und damit folgt (b).

(c): Die Anzahl s der p-Sylow-Gruppen ist dann gleich $|G/G_P|$ und damit ein Teiler von $\mathrm{ord}(G)$.

Zum Schluss liefert die Bahnengleichung für $H = P$

$$s = |\mathcal{S}| = \frac{|P|}{|P|} + \sum_{P.P_v \neq P.P} \frac{|P|}{|P_{P_v}|}$$

Jedes P_{P_v} rechts muss eine echte Untergruppe von P sein, denn sonst wäre $P \subset P_v$ nach obiger Argumentation. Also ist jeder Index $\frac{|P|}{|P_{P_v}|}$ durch p teilbar , somit also $s \equiv \frac{|P|}{|P|} = 1 \mod p$. □

Definition 1.8.11. Eine Gruppe G heisst **einfach**, wenn sie keinen echten Normalteiler hat, also keinenNormalteiler ausser $\{1\}$ und G.

Beispiele 1.8.12.
- $\mathbb{Z}/p$ ist einfach, wenn p eine Primzahl ist, denn diese Gruppe hat nicht einmal eine echte Untergruppe.
- Die Gruppe A_n der geraden Permutationen in Per(n) ist einfach, falls $n \geq 5$.

Korollar 1.8.13. *Sei G eine Gruppe der Ordnung pq für Primzahlen $p > q$. Dann ist die p-Sylow-Gruppe ein Normalteiler, die Gruppe G also nicht einfach.*

Beweis. Die Anzahl der p-Sylow-Gruppen s teilt die Gruppenordnung, also ist $p = 1, q, p, pq$ und es gilt $s \equiv 1(p)$, so dass nur noch $s = 1$ in Frage kommt. Daher gibt es nur eine p-Sylow-Gruppe P. Da für $g \in G$ auch gPg^{-1} eine p-Sylow-Gruppe ist, folgt $gPg^{-1} = P$, also ist P ein Normalteiler. □

Beispiele 1.8.14.
(a) Die Gruppe Per(3) hat Ordnung $6 = 2 \cdot 3$, daher gibt es 2 und 3 Sylow-Gruppen, beide sind zyklisch.

(b) $|\text{Per}(4)| = 24 = 2^3 \cdot 3$. Die 3-Sylow ist zyklisch und die 2-Sylow ist die Diedergruppe D_4, die ja auch vier Punkte permutiert.

(c) Die Gruppe $\text{GL}_n(\mathbb{F}_p)$ hat die Ordnung $p^{\frac{n(n-1)}{2}}(p^n - 1)(p^{n-1} - 1) \cdots (p - 1)$. Daher hat jede p-Sylow die Ordnung $p^{\frac{n(n-1)}{2}}$. Ist $p \geq n$, dann ist die Gruppe S der oberen Dreiecksmatrizen mit Einsen auf der Diagonale

$$S = \begin{pmatrix} 1 & & * \\ & \ddots & \\ & & 1 \end{pmatrix}$$

eine p-Sylow-Gruppe. Dasselbe gilt für B_n.

(d) Die Diedergruppe $D_{2p} = \langle \sigma, \tau \rangle$ hat $\langle \sigma \rangle$ als p-Sylow und $\langle \tau \rangle$ als 2-Sylowgruppe.

1.9 Kommutatoren

Definition 1.9.1. Sind a, b Elemente einer Gruppe G, so sei

$$[a, b] = aba^{-1}b^{-1}$$

der **Kommutator** von a und b. Sei $[G, G]$ die Gruppe, die von allen Kommutatoren erzeugt wird, sie wird die **Kommutatorgruppe** genannt.

Die Kommutatorgruppe ist genau dann trivial, wenn die Gruppe G abelsch ist.

Proposition 1.9.2. *Die Kommutatorgruppe* $[G,G]$ *ist ein Normalteiler von G. Der Quotient* $G/[G,G]$ *is abelsch und* $[G,G]$ *ist der kleinste Normalteiler mit abelschem Quotienten. Andersherum ist* $G/[G,G]$ *der groesste abelsche Quotient von G und wird daher die* **Abelisierung** *der Gruppe G genannt und* G^{ab} *geschrieben.*

Beweis. Sind $a,b \in G$ und ist $\phi : G \to H$ irgendein Gruppenhomomorphismus, so ist das Bild

$$\phi([a,b]) = \phi(aba^{-1}b^{-1}) = \phi(a)\phi(b)\phi(a)^{-1}\phi(b)^{-1} = [\phi(a),\phi(b)]$$

wieder ein Kommutator. Ist daher $\phi : G \to G$, $x \mapsto gxg^{-1}$, so folgt, dass $g[G,G]g^{-1} \subset [G,G]$ und damit ist $[G,G]$ normal. Ist N irgendein Normalteiler mit abelschem Quotienten G/N uns sei $\phi : G \to G/N$ der entsprechende Gruppenhomomorphismus. Dann ist, da G/N abelsch ist, $\phi([a,b]0 = [\phi(a),\phi(b)] = 1$, also liegt $[G,G]$ im Kern von ϕ, mit anderen Worten $[G,G] \subset N$, wie verlangt. □

Definition 1.9.3. Sei G eine Gruppe. Fuer beliebige Teilmengen $A,B \subset G$ sei $[A,B]$ die Untergruppe erzeugt von allen Kommutatoren $[a,b]$ mit $a \in A$ und $b \in B$.

Lemma 1.9.4. *Sei G eine Gruppe,* $G_0 = G$ *und* $G_{j+1} = [G,G_j]$ *fuer* $j = 0,1,\ldots$ *So folgt* $G_0 \supset G_1 \supset \ldots$ *und jede Gruppe* G_j *ist ein Normalteiler in G. Die Gruppe* G_j/G_{j+1} *liegt im Zentrum von* G/G_{j+1}.

Eine Gruppe G heisst **nilpotent**, *falls* $G_n = \{1\}$ *fuer ein* $n \in \mathbb{N}$ *gilt.*

Beweis. Es gilt $G_0 \supset G_1$ und induktiv folgt aus $G_{j-1} \supset G_j$ schon $G_j = [G,G_{j-1}] \supset [G,G_j] = G_{j+1}$. Ferner ist G_0 ein Normalteiler und ist G_j ein Normalteiler, so gilt fuer $g \in G$, dass

$$gG_{j+1}g^{-1} = g[G,G_j]g^{-1} = [G,gG_jg^{-1}] = [G,G_j] = G_{j+1},$$

also ist auch G_{j+1} ein Normalteiler und induktiv sind's dann alle. Wegen $[G,G_j \subset G_{j+1}$ ist G_j zentral modulo G_{j+1}. □

Lemma 1.9.5. *Ist Z eine zentrale Untergruppe von G, dann gilt*

$$G \text{ nilpotent} \quad \Leftrightarrow \quad G/Z \text{ nilpotent}.$$

Proof. Homomorphe Bilder von nilpotenten Gruppen sind immer nilpotent, daher folgt "⇒". Sei also G/Z nilpotent. Da ϕ surjektiv ist, folgt $\phi(G_j) = (G/Z)_j$. Ist nun etwa $(G/Z)_n = \{1\}$, so folgt $\phi(G_n) = 1$, also $G_n \subset Z$ und da Z zentral ist $G_{n+1} = [G,G_n] \subset [G,Z] = 1$, so dass auch G nilpotent ist. □

Beispiele 1.9.6.

Abelsche Gruppen sind nilpotent.

Sei K ein Koerper, sei $n \in \mathbb{N}$ und sei G die Gruppe aller oberen Dreieckmatrizen in $\mathrm{M}_n(K)$ mit Einsen auf der Diagonale. Dann ist G nilpotent, denn G_j ist genau die Untergruppe aller Matrizen mit Nullen auf den ersten j Nebendiagonalen (Uebungsaufgabe).

Proposition 1.9.7. *Sei p eine Primzahl. Dann ist jede endliche p-Gruppe nilpotent.*

Beweis. Induktion nach der Ordnung. Ist $|G| = 1$ dann ist G abelsch also nilpotent. Ist $|G| = p^{k+1}$, dann hat G ein nichttriviales Zentrum Z, also $|Z| = p^j$ fuer ein $j \in \mathbb{N}$. Damit ist G/Z eine Gruppe der Ordnung p^{k+1-j} und nach Induktionsvoraussetzung koennen wir G/Z als nilpotent voraussetzen, so dass nach Lemma 1.9.5 auch G nilpotent ist. □

2 Ringe

2.1 Definition

Definition 2.1.1. Wenn wir in dieser Vorlesung **Ring** sagen, werden wir stets einen **kommutativen Ring mit Eins** meinen, also eine abelsche Gruppe $(R, +)$ mit einer weiteren Verknüpfung $(a, b) \mapsto ab$, so dass
Assoziativität: $(ab)c = a(bc)$ und
Kommutativität: $ab = ba$ sowie
Distribitivität: $a(b + c) = ab + ac$ gelten und es ein Element $1 = 1_R$ gibt mir $a \cdot 1 = a$.

Definition 2.1.2. Ein **Ringhomomorphismus** $\phi : R \to S$ ist eine Abbildung zwischen Ringen, so dass

$$\phi(a + b) = \phi(a) + \phi(b), \qquad \phi(ab) = \phi(a)\phi(b), \qquad \phi(1) = 1$$

gelten.

Beispiele 2.1.3. (a) Jeder Körper ist ein Ring.

(b) $\mathbb{Z}$ ist ein Ring, der kein Körper ist.

(c) Der einfachste Ring ist der **Nullring** $N = \{0\}$. In diesem Ring gilt $0 = 1$. Ist R ein Ring, in dem $0 = 1$ gilt, dann ist R der Nullring, denn für $a \in R$ gilt

$$a = 1a = 0a = (1 - 1)a = a - a = 0.$$

(d) Sei $\alpha = \sqrt{2} \in \mathbb{R}$. Dann gilt $\alpha^2 = 2$. Wir definieren

$$\mathbb{Z}[\sqrt{2}] = \left\{k + l\alpha : k, l \in \mathbb{Z}\right\}.$$

Wegen $(k + l\alpha)(m + n\alpha) = km + 2ln + (kn + lm)\alpha$ ist $\mathbb{Z}[\sqrt{2}]$ ein Unterring von $\mathbb{R}$.

(e) Der **Gaußsche Zahlring** ist definiert als

$$\mathbb{Z}[i] = \left\{a + bi : a, b \in \mathbb{Z}\right\} \subset \mathbb{C}.$$

(f) Ist R ein Ring, dann definiert man den Polynomring $R[x]$ genau wie im Körperfall. Elemente sind formale Ausdrücke der Form

$$a_0 + \cdots + a_n x^n$$

und die Multiplikation ist definiert durch

$$(a_0 + \cdots + a_n x^n)(b_0 + \cdots + b_m x^m) = c_0 + \cdots + c_{m+n} x^{m+n},$$

wobei $c_k = \sum_{i+j=k} a_i b_j$. Insbesondere kann man also den Übergang von einem Ring zum Polynomring wiederholen und erhält den **Polynomring in mehreren Variablen**,

$$R[X_1, \ldots, X_r].$$

Die Elemente dieses Rings sind formale Ausdrücke der Form

$$\sum_{\alpha} c_\alpha X^\alpha,$$

wobei α durch $\mathbb{N}_0^r$ läuft, $c_\alpha \in R$ ein Koeffizient ist, der nur für endlich viele α nicht Null ist und

$$X^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_r^{\alpha_r}$$

ist.

(g) Es gibt auch den **Polynomring in unendlich vielen Variablen**: Ist $(T_i)_{i\in I}$ eine Familie von Variablen, so definiert man

$$R[T_i, i \in I] \coloneqq \bigcup_{\substack{E\subset I \\ E \text{ endlich}}} R[T_i : i \in E].$$

Die Elemente sind also endliche Linearkombinationen von endlichen Produkten der T_i.

(h) Sei p eine Primzahl und sei $\mathbb{Z}_{(p)}$ die Menge aller rationalen Zahlen $\frac{a}{b} \in \mathbb{Q}$ für die der Nenner b zur Primzahl p teilerfremd ist, also von p nicht geteilt wird. Dies ist ein Unterring von $\mathbb{Q}$.

(i) Für $m \in \mathbb{N}$ ist die Menge $\mathbb{Z}/m$ der Restklassen $\{0, 1, 2, \ldots, m-1\}$ mit Addition und Multiplikation

$$a \boxplus b = \text{Rest von } a + b \text{ modulo } m,$$
$$a \cdot b = \text{Rest von } ab \text{ modulo } m$$

ein Ring, den wir ebenfalls mit $\mathbb{Z}/m$ bezeichnen.

Definition 2.1.4. Ein Element $0 \neq a \in R$ eines Rings heißt **invertierbar** oder **Einheit** des Rings, wenn es ein $b \in R$ gibt mit $ab = 1$. Die Menge $R^\times$ der invertierbaren Elemente ist eine abelsche Gruppe bzgl. der Multiplikation. Ein Ring R ist genau dann ein Körper, wenn $R^\times = R \setminus \{0\}$ gilt.

Beispiele 2.1.5.

- Die Einheiten von $\mathbb{Z}$ sind ± 1.
- Sei K ein Körper und sei $R = K[x]$ der Polynomring. Die Einheiten von R sind genau die konstanten Polynome $\neq 0$.
- Die Einheiten des Rings $R = \mathbb{Z}[\sqrt{-5}]$ sind genau die Zahlen 1 und -1.

  Beweis. Seien $a, b \in R$ mit $ab = 1$. Da $a, b \in \mathbb{C}$ ist, gilt diese Gleichung auch dort, also ist auch $1 = |ab|^2 = |a|^2|b|^2$. Damit gilt $|a|^2 \leq 1$ oder $|b|^2 \leq 1$. Nehmen wir $|a|^2 \leq 1$ an. Sei $a = k + il\sqrt{5}$, dann ist $|a|^2 = k^2 + 5l^2$ und da $k, l \in \mathbb{Z}$, folgt $l = 0$ und $a = k = \pm 1$. Damit ist auch $b = \pm 1$ und die Behauptung ist gezeigt. □

- Die Einheiten des Rings $\mathbb{Z}/m$ sind genau die Zahlen $1 \leq x \leq m-1$, die zu m teilerfremd sind. Dies zeigt man mit Hilfe der Division mit Rest (Übungsaufgabe!)

Definition 2.1.6. Ein Element $a \neq 0$ eines Rings R heißt **Nullteiler**, falls es ein $b \neq 0$ gibt mit $ab = 0$.

Ein Ring R mit $0 \neq 1$ heißt **nullteilerfrei**, oder **integer**, oder auch **Integritätsring**, falls gilt

$$ab = 0 \quad \Rightarrow \quad a = 0 \text{ oder } b = 0.$$

Beispiele 2.1.7.

- Der Nullring ist kein Integritätsring.
- Körper sind Integritätsringe.
- Jeder Unterring eines Integritätsrings ist ein Integritätsring. So ist zum Beispiel $\mathbb{Z}[\sqrt{-5}]$ ein Integritätsring, da er ein Unterring des Körpers $\mathbb{C}$ ist.
- $\mathbb{Z}$ ist ein Integritätsring.
- $\mathbb{Z}/m$ ist genau dann ein Integrigtätsring, wenn m eine Primzahl ist.
- Sind R, S Ringe, dann ist auch das kartesische Produkt $R \times S$ ein Ring, indem man die Operationen Komponentenweise definiert. Das Nullelement ist $(0, 0)$ und die Eins ist $(1, 1)$. Dieser Ring ist kein Integritätsring, auch wenn R und S welche sind, denn es gilt

$$(0, 1) \cdot (1, 0) = (0, 0).$$

Satz 2.1.8. *Ist R ein Integritätsring, dann auch der Polynomring $R[x]$.*

Beweis. Seien $f, g \in R[x]$, beide $\neq 0$. Wir zeigen $fg \neq 0$. Sei dazu

$$f(x) = a_0 + \cdots + a_n x^n,$$
$$g(x) = b_0 + \cdots + b_m x^m$$

mit $a_n \neq 0 \neq b_m$. Dann gilt

$$f(x)g(x) = c_0 + \cdots + c_{m+n} x^{m+n},$$

wobei $c_k = \sum_{i+j=k} a_i b_j$. Insbesondere ist dann $c_{m+n} = a_n b_m \neq 0$, da R ein Integritätsring ist. □

Beispiele 2.1.9.
- Die Inklusionen $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$ sind Ringhomomorphismen.
- Sei $m \in \mathbb{N}$. Die Projektion $\mathbb{Z} \to \mathbb{Z}/m$, die $a \in \mathbb{Z}$ auf den Rest modulo m wirft, ist ein Ringhomomorphismus.
- Ist $R = K[x]$ ein Polynomring und ist $\alpha \in K$. Dann ist die **Auswertungsabbildung** $\delta_\alpha : K[x] \to K$, die $f(x)$ auf $f(\alpha)$ schickt, ein Ringhomomorphismus.

2.2 Ideale

Definition 2.2.1. Sei R ein Ring (kommutativ mit Eins). Ein **Ideal** in R ist eine additive Untergruppe $I \subset R$ so dass $RI \subset I$.

Proposition 2.2.2. (a) *Ist $\phi : R \to S$ ein Ringhomomorphismus und ist $I \subset S$ ein Ideal, dann ist das Urbild $\phi^{-1}(I)$ ein Ideal. Insbesondere ist* $\ker(\phi) = \left\{x \in R : \phi(x) = 0\right\}$ *ein Ideal.*

(b) *Ist K ein Körper und ist R ein Ring, der nicht der Nullring ist, dann ist jeder Ringhomomorphismus $\phi : K \to R$ injektiv. Insbesondere ist jeder Homomorphismus zwischen Körpern injektiv.*

Beweis. (a) Da ϕ ein additiver Gruppenhomomorphismus ist, ist das Urbild eine Untergruppe. Sei also $a \in \phi^{-1}(I)$ und $r \in R$. Dann folgt $\phi(ra) = \phi(r) \underbrace{\phi(a)}_{\in I} \in I$, also ist $ra \in \phi^{-1}(I)$.

(b) Da R nicht der Nullring ist, gilt $\phi(1) = 1 \neq 0$ und daher ist der Kern von ϕ nicht ganz K. Das einzige andere Ideal, das K hat, ist $\{0\}$. Damit ist ϕ injektiv. □

Beispiele 2.2.3.
- 0 und der ganze Ring R sind Ideale.
- Sei $I \subset R$ ein Ideal. Enthält I ein invertierbares Element, so ist $I = R$.
- Ist $r \in R$, so ist die Menge
$$rR = \left\{rx : x \in R\right\}$$
ein Ideal. Ein solches Ideal nennt man **Hauptideal**. Manche Autoren schreiben auch (a) für aR.

Definition 2.2.4. In der Regel ist nicht jedes Ideal ein Hauptideal. Ein **Hauptidealring** ist ein Ring R, der

(a) integer ist und in dem

(b) jedes Ideal ein Hauptideal ist.

Beispiele 2.2.5.

- Jeder Körper K ist ein Hauptidealring, denn er hat nur zwei Ideale, $\{0\} = 0K$ und $K = 1K$.
- $\mathbb{Z}$ ist ein Hauptidealring.

  Beweis. Sei $I \subset \mathbb{Z}$ ein Ideal. Ist $I \cap \mathbb{N} = \emptyset$, dann ist auch $I \cap (-\mathbb{N}) = \emptyset$ und daher $I = \{0\} = 0\mathbb{Z}$. Ist $I \cap \mathbb{N} \neq \emptyset$, dann gibt es eine kleinste natürliche Zahl $m \in I$. Wir behaupten, dass $I = m\mathbb{Z}$. Klar ist $m\mathbb{Z} \subset I$. Sei also $k \in I$, dann existiert ein $p \in m\mathbb{Z}$ so dass $0 \leq k - p < m$. Da m minimal in $I \cap \mathbb{N}$ ist, folgt $k - p = 0$, also $k = p \in m\mathbb{Z}$. □

- Ist K ein Körper, so ist der Polynomring $R = K[x]$ ein Hauptidealring.

  Beweis. Sei $I \neq 0$ ein Ideal und sei $g \in I \setminus \{0\}$ ein Polynom von minimalem Grad. Sei $f \in I$ beliebig, dann ist $\text{grad}(f) \geq \text{grad}(g)$, also existieren nach der **Division mit Rest** Polynome q, r mit

  $$f = qg + r$$

  und $\text{grad}(r) < \text{grad}(g)$. Dann ist $r = f - qg \in I$ und da der Grad von g minimal war, ist $r = 0$, also $f = gq \in gR$. □

- Sei K ein Körper. Der Polynomring $R = K[x, y]$ ist kein Hauptidealring.

  Beweis. Betrachte das Ideal

  $$I = xR + yR.$$

  Erstens ist $I \neq R$, denn kein Polynom in I hat einen konstanten Term. Angenommen: I ist ein Hauptideal, also etwa $I = fR$, dann gibt es g mit $fg = x$, woraus $f \in K[x]$ folgt, da die Variable y nicht vorkommt. Ebenso gibt es h mit $fh = y$, also $f \in K[y]$, so dass $f \in K[x] \cap K[y] = K$, also muss f konstant sein. Da $I \neq 0$ ist $f \in K \setminus \{0\} = K^\times$, es gibt also ein f' mit $ff' = 1$, also ist $1 \in I$ und somit $I = R$, ein Widerspruch! □

- Der Ring $R = \mathbb{Z}[\sqrt{-5}]$ ist kein Hauptidealring. Der Beweis hierzu wird auf später verschoben.

Definition 2.2.6. Sei R ein Hauptidealring und seien $a, b \in R$. Ein **größter gemeinsamer Teiler** $\text{ggT}(a, b)$ ist ein Erzeuger des Ideals $aR + bR$. Ein ggT ist bis auf Multiplikation mit einer Einheit eindeutig festgelegt.

Beispiel 2.2.7. In $R = \mathbb{Z}$ ist 5 ein ggT von 10 und 15.

Beweis. 5 teilt 10 und 15, also folgt $10\mathbb{Z} + 15\mathbb{Z} \subset 5\mathbb{Z}$. Andererseits ist $5 = 15 - 10$, liegt also in $10\mathbb{Z} + 15\mathbb{Z}$. □

Definition 2.2.8. Sei R ein Ring und $I \subset R$ ein Ideal. Dann ist I eine Untergruppe von $(R, +)$ und wir können die Menge R/I der Nebenklassen betrachten.

Satz 2.2.9. *Auf der Menge R/I gibt es genau eine Ringstruktur, so dass die Projektion $\pi : R \to R/I$ ein Ringhomomorphismus ist. Für diesen Ringhomomorphismus gilt $I = \ker(\pi)$, also ist jedes Ideal der Kern eines Ringhomomorphismus.*

Beweis. Wir machen uns zunächst klar, dass für $a, b \in R$ die Bedingung $a + I = b + I$ gleichwertig ist zu $a - b \in I$.

Wir definieren Addition und Multiplikation durch $(a + I) + (b + I) = (a + b) + I$ und $(a + I)(b + I) = ab + I$. Hier ist Wohldefiniertheit zu prüfen. Seien $a_I = a' + I$ und $b + I = b'I$, also $a - a', b - b' \in I$, dann folgt

$$(a + b) - (a' + b') = (a - a') + (b - b') \in I$$

also folgt $(a + b) + I = (a' + b') + I$ und damit die Wohldefiniertheit der Addition. Für die Multiplikation rechne

$$\begin{aligned} ab - a'b' &= ab - ab' + ab' - a'b' \\ &= a(b - b') + (a - a')b' \in I. \end{aligned}$$

Die Eindeutigkeit der Ringstruktur ist wegen der Surjektivität von π klar und der Kern der Projektion $R \to R/I$ ist die triviale Nebenklasse, also I. □

Beispiel 2.2.10. Der Ring $\mathbb{Z}/m$.

Ein Ideal $\mathfrak{m}$ eines Rings R heisst **maximales Ideal**, wenn $\mathfrak{m} \neq R$ und $\mathfrak{m}$ ist maximal in der Menge aller Ideale $I \neq R$, also mit anderen Worten:

(a) $1 \notin \mathfrak{m}$ und

(b) ist I ein Ideal mit $\mathfrak{m} \subset I$ und $I \neq R$, dann ist $\mathfrak{m} = I$.

Satz 2.2.11.

(a) *Jedes Ideal $I \neq R$ liegt in einem maximalen Ideal.*

(b) *Jedes Element von $R \setminus R^\times$ liegt in einem maximalen Ideal.*

(c) *Ein Ideal J ist genau dann maximal, wenn R/J ein Körper ist.*

Beweis. (a) Sei $I \neq R$ ein Ideal und sei S die Menge aller Ideale J mit $1 \notin J$ und $J \supset I$. Dann ist S mit der Inklusion partiell geordnet und die Kettenbedingung ist erfüllt, denn sei $\emptyset \neq K \subset S$ eine Kette, also eine linear geordnete Teilmenge und sei $\mathfrak{a} = \bigcup_{J \in K} J$, dann ist $\mathfrak{a}$ wieder ein Ideal und es gilt $I \subset \mathfrak{a}$, sowie $1 \notin \mathfrak{a}$. Dieses $\mathfrak{a}$ ist dann eine obere Schranke zu K. Nach dem Lemma von Zorn gibt es ein maximales Element $\mathfrak{m}$ in S, also liegt I in einem maximalen Ideal.

(b) Sei $r \in R \setminus R^\times$ eine Nichteinheit und sei $I = (r) = rR$ das Hauptideal. Dann gilt $1 \notin I$, da r nicht invertierbar ist. Also gibt es nach Teil (a) ein maximales Ideal, das I und damit auch r enthält.

(c) Sei J ein maximales Ideal und sei $r \in R \setminus J$. Wegen der Maximalität von J muss das Ideal $\langle r, J \rangle = rR + J$ gleich dem ganzen Ring sein, also auch die Eins enthalten, es gibt also $r' \in R$ und ein $\alpha \in J$ mit $rr' + \alpha = 1$ oder $rr' \in 1 + J$, so dass in R/J gilt

$(r + J)(r' + J) = rr' + J = 1 + J$, das heisst, dass r im Quotienten R/J invertierbar ist, also ist in R/J jedes Element $\neq 0$ invertierbar, d.h., R/J ist ein Körper.

Sei umgekehrt R/J ein Körper und sei $r \in R \setminus J$, dann ist r modulo J invertierbar, also existiert ein $r' \in R$ mit $rr' \in 1 + J$, so dass $1 \in rR + J$, also ist J maximal. □

Definition 2.2.12. Ein Ideal $J \neq R$ eines Rings R heisst **Primideal**, wenn für $x, y \in R$ gilt

$$xy \in J \quad \Rightarrow \quad x \in J \text{ oder } y \in J.$$

Satz 2.2.13. *Ein Ideal $J \neq R$ ist genau dann ein Primideal, wenn R/J ein Integritätsring ist.*

Insbesondere ist jedes maximale Ideal ein Primideal.

Beweis. Sei J ein Primideal und seien $x, y \in R$ so dass für die Restklassen gilt $[x][y] = [0]$. Dann ist also $[xy] = [0]$, so dass $xy \in J$ folgt. Dann ist also $x \in J$ oder $y \in J$, was mit $[x] = [0]$ oder $[y] = [0]$ gleichbedeutend ist, das heisst, R/J ist ein Integritätsring. Für die Umkehrung liest man diesen Beweis rückwärts.

Der Zusatz folgt, da ein Ideal J genau dann maximal ist, wenn R/J ein Körper ist. □

2.3 Der chinesische Restsatz

Definition 2.3.1. Zwei Ideale I, J in einem Ring heißen **teilerfremd**, falls $I + J = R$ gilt.

Beispiel 2.3.2. In $R = \mathbb{Z}$ sind die Hauptideale $m\mathbb{Z}$ und $n\mathbb{Z}$ genau dann teilerfremd, wenn die Zahlen m und n keine echten gemeinsamen Teiler haben, wenn also m und n teilerfremd sind.

Beweis. Seien die Ideale teilerfremd, dann ist $1 \in m\mathbb{Z} + n\mathbb{Z}$, es gibt also $a, b \in \mathbb{Z}$ mit $am + bn = 1$. Würden nun m und n von einer Primzahl p geteilt, dann würde auch 1 von p geteilt, was ein Widerspruch ist.

Seien umgekehrt die Zahlen m und n teilerfremd. Das Ideal $m\mathbb{Z} + n\mathbb{Z}$ ist ein Hauptideal, also von der Form $g\mathbb{Z}$ für ein $g \in \mathbb{N}$. Dann ist $m \in g\mathbb{Z}$ also folgt $g \mid m$ und ebenso $g \mid n$ und daher ist $g = 1$, also sind die Ideale $m\mathbb{Z}$ und $n\mathbb{Z}$ teilerfremd. □

Definition 2.3.3. Sind I und J Ideale, so definieren wir das Ideal IJ als

$$IJ = \left\{ \sum_{j=1}^{n} a_j b_j : a_j \in I,\ b_j \in J \right\}.$$

Sind etwa beides Hauptideale, $I = aR$ und $J = bR$, dann ist auch IJ ein Hauptideal, nämlich $IJ = abR$.

Lemma 2.3.4. *Sind die Ideale I und J teilerfremd, dann gilt*

$$IJ = I \cap J.$$

Beweis. Die Inklusion "$\subset$" gilt auch ohne die Teilerfremdheit, da $IJ \subset IR = I$ und ebenso für J.

Zum Beweis von "$\supset$" seien also I und J teilerfremd, also gibt es Elemente $a \in I$ und $b \in J$ mit $1 = a + b$. Sei dann $x \in I \cap J$, dann ist $x = ax + bx$ und da ax und bx beide in IJ liegen, ist $x \in IJ$. □

Satz 2.3.5 (Chinesischer Restsatz)**.** *Sei R ein Ring und $I_1, \ldots, I_r$ seien paarweise teilerfremde Ideale. Sei $I = I_1 \cdots I_r = I_1 \cap \cdots \cap I_r$, dann liefern die kanonischen Projektionen einen Isomorphismus*

$$R/I \cong \prod_{\nu=1}^{r} R/I_\nu.$$

Beweis. Da $I_\nu \supset I$ für jedes ν, gibt es kanonische Projektionen $\pi_\nu : R/I \to R/I_\nu$, also einen Ringhomomorphismus

$$\pi : R/I \to \prod_{\nu=1}^{r} R/I_\nu.$$

Injektivität: Sei $\pi(\bar{x}) = 0$, und $x \in R$ ein Urbild von $\bar{x}$. Dann ist $x \in I_\nu$ für jedes ν. Nun sind die I_ν paarweise teilerfremd, also gibt es beispielsweise $a \in I_1$, $b \in I_2$ mit $a + b = 1$. Dann ist $x = 1 \cdot x = (a + b)x = ax + bx$. Da $x \in I_2$ und $a \in I_1$, ist $ax \in I_1 I_2$ und ebenso für bx, also ist $x \in I_1 I_2$. Nun ist $I_1 I_2$ immer noch teilerfremd zu $I_3, \ldots, I_r$, denn sind $a \in I_1$ und $b \in I_3$ mit $a + b = 1$ und $x \in I_2$ und $y \in I_3$ mit $x + y = 1$, so gilt

$$1 = (a + b)(x + y) = \underbrace{ax}_{\in I_1 I_2} + \underbrace{ay + bx + by}_{\in I_3}.$$

Also kann man induktiv fortfahren und erhält schließlich $x \in I_1 \cdots I_r = I$, d.h., π ist injektiv.

Surjektivität. Für die Surjektivität reicht es, zu zeigen, dass es Elemente $x_j \in R$ gibt, mit $\pi_j(x_j) = 1$ und $\pi_k(x_j) = 0$ für $k \neq j$. Modulo Umnummerierung reicht es, x_1 nachzuweisen. Seien $a \in I_1$ und $b \in I_2 \cdots I_r$ mit $a + b = 1$. Dann ist $x_1 = b$ das gewünschte Element. □

2.4 Teilbarkeit

Definition 2.4.1. Seien a, b Elemente eines Integritätsrings R.

(a) Man sagt a **teilt** b oder ist ein **Teiler** von b, falls es ein $c \in R$ gibt so dass $ac = b$. In diesem Fall schreibt man $a \mid b$. Ist a kein Teiler von b, so schreibt man $a \nmid b$.

(b) a und b heißen **assoziiert**, wenn es eine Einheit $u \in R^\times$ gibt mit $a = bu$.

Beispiele 2.4.2.
- Für zwei natürliche Zahlen m, n gilt m teilt n in $\mathbb{Z}$ genau dann, wenn m ein Teiler im üblichen Sinne ist.
- Zwei Elemente a, b in $\mathbb{Z}$ sind genau dann assoziiert, wenn $a = \pm b$ gilt.
- Jedes Element $a \in R$ teilt die Null, denn es gilt $a \cdot 0 = 0$. Die Null teilt nur sich selbst.

Lemma 2.4.3. *Für zwei Elemente a, b eines Integritätsrings R sind äquivalent*

(i) *$a \mid b$ und $b \mid a$,*

(ii) *$aR = bR$,*

(iii) *a und b sind assoziiert.*

Beweis. (i)⇒(iii): Es gelte $a = bc$ und $b = ad$. Wir nehmen an, dass $a \neq 0$, da sonst auch $b = 0$. Es ist $a = bc = acd$, also $a(1 - cd) = 0$ und da $a \neq 0$ und R integer ist, folgt $cd = 1$, also sind c, d Einheiten und a und b sind assoziiert.

(iii)⇒(ii) Es sei $a = bu$ mit einer Einheit u. Wegen $uR = R$ folgt dann $aR = buR = bR$.

(ii)⇒(i) Sei $aR = bR$, dann folgt $a \in bR$, also gibt es ein $c \in R$ mit $a = bc$, also $b \mid a$. Ebenso folgt $b \mid a$. □

Definition 2.4.4. Sei R ein Integritätsring und p ein Element, das weder Null noch eine Einheit ist.

(a) Das Element p heißt **irreduzibel**, falls aus der Gleichung $p = ab$ in R stets folgt, dass a oder b eine Einheit ist.

(b) Das Element p heißt **Primelement**, falls aus $p \mid ab$ stets folgt $p \mid a$ oder $p \mid b$.

Lemma 2.4.5. *Sei R ein Integritätsring. Ein Element $p \in R \setminus \{0\}$ ist genau dann ein Primelement, wenn pR ein Primideal ist.*

Beweis. Für $x \in R$ gilt $x \in pR \Leftrightarrow p \mid x$, so dass die Eigenschaft p prim oder pR prim direkte Umformulierungen voneinander sind. □

Beispiele 2.4.6.
- In $R = \mathbb{Z}$ sind die Primelemente genau die Elemente der Form $\pm p$, wobei p eine Primzahl ist.
- In $R = \mathbb{C}[x]$ sind die Primelemente genau die Elemente $c(x - a)$ mit $c \in \mathbb{C}^\times$, $a \in \mathbb{C}$.
- In $R = \mathbb{R}[x]$ sind die Primelemente genau die Polynome der Form $c(x - \alpha)$ für ein $\alpha \in \mathbb{R}$ oder $c(x^2 + ax + b)$, falls dieses Polynom keine reelle Nullstelle hat.

Proposition 2.4.7. *Sei R ein Integritätsring. Dann ist jedes Primelement von R auch irreduzibel.*

Beweis. Seien p ein Primelement und sei $p = ab$. Dann teilt p das Produkt ab also teilt p einen der Faktoren, sagen wir a. Das heißt $a = pc = abc$, also $a(1 - bc) = 0$, also $bc = 1$, so dass b eine Einheit ist. □

Satz 2.4.8. *Sei R ein Hauptidealring und sei $p \in R$. Dann sind äquivalent*

(a) *p irreduzibel,*

(b) *p ist ein Primelement.*

Beweis. Wir müssen nur (a)⇒(b) zeigen: Sei p irreduzibel und p teile ab und $p \nmid a$. Wir müssen zeigen, dass p das Element b teilt. Sei I das von p und a erzeugte Ideal, also $I = aR + pR$. Dann ist dies ein Hauptideal, also etwa $I = (c)$. Dann folgt $c \mid a$ und $c \mid p$, also etwa $cd = p$. Da p irreduzibel ist, ist c oder d eine Einheit. Ist d eine Einheit, so ist $(p) = (c) = I = aR + pR$, also ist $a \in (p)$, d.h. p teilt a, was der Voraussetzung widerspricht. Also ist c eine Einheit, d.h., $I = R$ und es gibt $r, s \in R$ mit $ar + ps = 1$, also $b = abr + psb = p(r'r + sb)$ fuer ein r', also $p \mid b$ wie verlangt. □

Korollar 2.4.9. *In einem Hauptidealring R lässt sich jedes Element von $R \setminus \{0\}$, das keine Einheit ist, als endliches Produkt von Primelementen schreiben.*

Beweis. Da jedes irreduzible Element prim ist, genügt es, eine Zerlegung in irreduzible zu konstruieren. Sei $a \in R$ ungleich Null und keine Einheit. *Angenommen*, a lässt sich nicht als Produkt von Irreduziblen schreiben. Dann ist a reduzibel und kann selbst als Produkt $a_1 a_1'$ von Nichteinheiten geschrieben werden. Da a kein Produkt von Irreduziblen ist, gilt dasselbe für mindestens einen der Faktoren, sagen wir a_1, und a_1 kann als Produkt $a_2 a_2'$ zweier Nichteinheiten geschrieben werden. Iteration liefert eine Folge von Elementen

$$a = a_0, a_1, \cdots \in R$$

so dass a_{j+1} ein Teiler von a_j, aber nicht assoziiert zu a_j ist. Also folgt für die Hauptideale

$$aR = a_0 R \subsetneq a_1 R \subsetneq a_2 R \subsetneq \dots$$

Man prüft leicht nach, dass die Vereinigung einer aufsteigenden Folge von Idealen wieder ein Ideal ist, also ist

$$\bigcup_{j \in \mathbb{N}} a_j R$$

wieder ein Ideal in R, also ein Hauptideal bR. Dann ist $b \in a_j R$ für ein j und daher

$$bR \subset a_j R \subset a_{j+1} R \subset bR,$$

woraus Gleichheit folgt, ein *Widerspruch!* Daher ist die Annahme falsch, also ist jedes Element als Produkt von Irreduziblen darstellbar. □

Lemma 2.4.10. *Gilt in einem Integritätsring R die Gleichung*

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

für Primelemente p_j und irreduzible Elemente q_i, dann ist $r = s$ und nach Umnummerierung ist jedes p_j assoziiert zu q_j.

Beweis. Da $p_1 \mid q_1 \cdots q_s$, gibt es ein j mit $p_1 \mid q_j$. Nach Umnummerierung können wir $p_1 \mid q_1$ annehmen. Es folgt $q_1 = \varepsilon_1 p_1$, wobei ε_1 auf Grund der Irreduzibilität von q_1 eine Einheit ist. Da wir uns in einem Integritätsring befinden, folgt

$$p_2 \cdots p_r = \varepsilon_1 q_2 \cdots q_s.$$

Wir iterieren diesen Vorgang und können die q_i so umnummerieren, dass p_j zu q_j assoziiert ist. Insbesondere folgt $r \leq s$. Ist $r < s$ erhalten wir

$$1 = \varepsilon q_{r+1} \cdots q_s,$$

woraus folgt, dass q_s eine Einheit ist, was ein Widerspruch ist, also ist $r = s$. □