

Algebra

N. Perrin

Düsseldorf
Sommersemester 2014

Inhaltsverzeichnis

1	Gruppen	4
1.1	Wiederholung	4
1.1.1	Gruppen, Untergruppen	4
1.1.2	Gruppenhomomorphismen	5
1.1.3	Recht und Links Klassen	6
1.2	Normalteiler	8
1.3	Zentrum	12
1.4	Erzeuger und Zyklische Gruppe	13
1.5	Ordnung eines Elements	15
1.6	Derivierte Untergruppe	16
1.7	Semidirekte Produkte	17
1.8	Operation einer Gruppe auf einer Menge	19
1.9	Symmetrische Gruppe	24
1.10	Sylow Sätze	27
1.11	Auflösbare Gruppen	32
2	Ringe	35
2.1	Grundbegriffe	35
2.1.1	Definition	35
2.1.2	Ringhomomorphismus	37
2.1.3	Unterringe und Ideale	37
2.1.4	Quotienten	39
2.1.5	Erzeuger	40

1 Gruppen

1.1 Wiederholung

1.1.1 Gruppen, Untergruppen

Definition 1.1.1 Eine **Gruppe** ist eine Menge G mit einer Verknüpfung $G \times G \rightarrow G$, $(x, y) \mapsto x \cdot y$ so, dass

1. Es existiert ein **neutrales Element** e in G mit $e \cdot x = x \cdot e = x$ für alle $x \in G$.
2. Die Verknüpfung ist **assoziativ** i.e. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ für alle $x, y, z \in G$.
3. jedes $x \in G$ hat ein **inverses Element** $y \in G$ mit $x \cdot y = y \cdot x = e$.

Definition 1.1.2 Eine Gruppe G heißt **kommutativ** oder **abelsch** falls $x \cdot y = y \cdot x$ gilt für alle $x, y \in G$.

Beispiel 1.1.3 1. \mathbb{Z} mit $+$ ist eine Gruppe.

2. Sei $n \in \mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z} = \{\text{Restklassen modulo } n\}$. Dann ist $\mathbb{Z}/n\mathbb{Z}$ mit $+$ eine Gruppe.

3. Sei K ein Körper. Dann ist $\text{GL}_n(K)$ mit Matrixmultiplikation eine Gruppe.

4. S_n die Permutationsgruppe mit \circ der Komposition von Abbildungen als Verknüpfung ist eine Gruppe.

Lemma 1.1.4 Sei G eine Gruppe und seien x, y, z Elemente in G .

1. Das neutrale Element e_G ist eindeutig bestimmt.
2. Das inverse Element x^{-1} von x ist eindeutig bestimmt.
3. $xy = xz \Rightarrow y = z$ und $yx = zx \Rightarrow y = z$,
4. $(x^{-1})^{-1} = x$.
5. $(xy)^{-1} = y^{-1}x^{-1}$. □

Beweis. Siehe LAI. ■

Bemerkung 1.1.5 Sei $n \geq 0$ eine ganze Zahl. Aus 5. folgt per Induktion, dass $(x^n)^{-1} = (x^{-1})^n$. Wir schreiben x^{-n} für $(x^n)^{-1} = (x^{-1})^n$ also ist x^n für alle $n \in \mathbb{Z}$ definiert und es gilt $x^n x^m = x^{n+m}$ für alle $n, m \in \mathbb{Z}$.

Lemma 1.1.6 Seien G und G' zwei Gruppen und sei $(a, b) \cdot (a', b') = (aa', bb')$. Dann ist $G \times G'$ mit diesem Produkt eine Gruppe. \square

Beweis. Übung. \blacksquare

Definition 1.1.7 Seien G und G' zwei Gruppen. Das Produkt $G \times G'$ mit Verknüpfung $(a, b) \cdot (a', b') = (aa', bb')$ heißt **Produkt-Gruppe** von G und G' .

Definition 1.1.8 Sei G eine Gruppe. Eine Teilmenge $H \subset G$ heißt **Untergruppe** von G falls gilt:

1. $1 \in H$,
2. $x, y \in H \Rightarrow x \cdot y^{-1} \in H$.

Lemma 1.1.9 Eine Untergruppe ist eine Gruppe. \square

Beweis. Siehe LAI. \blacksquare

Beispiel 1.1.10 1. Sei G eine Gruppe. Dann ist $H = \{e_G\}$ die **Trivialuntergruppe** eine Untergruppe von G .

2. Sei $n \in \mathbb{Z}$. Dann ist $n\mathbb{Z} = \{m \in \mathbb{Z} \mid n \text{ teilt } m\}$ eine Untergruppe von $(\mathbb{Z}, +)$.

3. Sei K ein Körper. Dann ist $\text{SL}_n(K)$ eine Untergruppe von $\text{GL}_n(K)$.

1.1.2 Gruppenhomomorphismen

Definition 1.1.11 Seien G und G' zwei Gruppen. Eine Abbildung $f : G \rightarrow G'$ heißt **Gruppenhomomorphismus** falls für alle $x, y \in G$ gilt $f(xy) = f(x)f(y)$.

Beispiel 1.1.12 1. die Abbildung $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}_{>0}, \times)$ ist ein Gruppenhomomorphismus.

2. Sei K ein Körper. Dann ist $\det : \text{GL}_n(K) \rightarrow (K^\times, \times) = (K \setminus \{0\}, \times)$ ein Gruppenhomomorphismus.

Lemma 1.1.13 Sei $f : G \rightarrow G'$ ein Gruppenhomomorphismus dann gilt für alle $x \in G$

$$f(e_G) = e_{G'} \text{ und } f(x^{-1}) = f(x)^{-1}.$$

Beweis. Siehe LAI. \blacksquare

Definition 1.1.14 Sei $f : G \rightarrow G'$ ein Gruppenhomomorphismus, dann heißt die Teilmenge $\text{Ker}(f) = \{x \in G \mid f(x) = e_{G'}\}$ von G der **Kern** von f .

Lemma 1.1.15 Sei $f : G \rightarrow G'$ ein Gruppenhomomorphismus. Sei H eine Untergruppe von G und H' eine Untergruppe von G' .

1. Dann sind $f(H)$ und $f^{-1}(H')$ Untergruppen von G' und G .
2. Für $H' = \{e_{G'}\}$ ist $\text{Ker}(f) = f^{-1}(H')$ eine Untergruppe von G .
3. Für $H = G$ ist das Bild $f(G)$ von f eine Untergruppe von G' □

Beweis. Siehe Übungsblatt 0. ■

Beispiel 1.1.16 Die Signatur $\varepsilon : S_n \rightarrow \{\pm 1\}$ ist ein Gruppenhomomorphismus. Wir schreiben $A_n = \text{Ker}\varepsilon$ für die **Alternierende Gruppe**. Die Gruppe A_n ist eine Untergruppe von S_n .

Lemma 1.1.17 Sei $f : G \rightarrow G'$ ein Gruppenhomomorphismus. Die Abbildung f ist genau dann injektiv, wenn $\text{Ker}(f) = \{e_G\}$. □

Beweis. Siehe LAI. ■

Definition 1.1.18 Ein bijektiver Gruppenhomomorphismus $f : G \rightarrow G'$ heißt **Isomorphismus** oder **Gruppenisomorphismus**. Wenn $G' = G$ heißt ein Gruppenisomorphismus **Gruppenautomorphismus** oder **Automorphismus**.

Lemma 1.1.19 Sei G eine Gruppe und $g \in G$. Dann ist $\text{Int}_g : G \rightarrow G$ definiert durch $\text{Int}_g(h) = ghg^{-1}$ ein Gruppenautomorphismus. □

Beweis. Siehe Übungsblatt 0. ■

Definition 1.1.20 Sei G eine Gruppe und $g \in G$. Dann heißt Int_g **innerer Gruppenhomomorphismus** oder **Konjugation mit g** . Gruppenautomorphismen, die nicht dieser Form sind heißen **äußere Automorphismen**.

1.1.3 Recht und Links Klassen

Definition 1.1.21 Sei G eine Gruppe und H eine Untergruppe. Man definiert die Relation \sim durch

$$g' \sim g \Leftrightarrow \exists h \in H \text{ mit } g' = gh.$$

Lemma 1.1.22 Die Relation \sim ist eine Äquivalenzrelation und die Klasse eines Element $g \in G$ ist die Teilmenge $\bar{g} = [g] = gH = \{gh \in G \mid h \in H\}$. Die Äquivalenzklassen heißen **Linksklassen**. □

Beweis. Siehe Übungsblatt 0. ■

Definition 1.1.23 Sei G eine Gruppe und H eine Untergruppe.

1. Die Menge aller Äquivalenzklassen heißt **Quotient von G nach H** und ist G/H bezeichnet.
2. Die **kanonische Projektion** ist die Abbildung $G \rightarrow G/H$ definiert durch $g \mapsto \bar{g} = [g] = gH$.

Bemerkung 1.1.24 Analog kann man die Äquivalenzrelation $g' \sim_R g \Leftrightarrow \exists h \in H$ mit $g' = hg$ definieren. Die Äquivalenzklassen heißen **Rechtsklassen** $Hg = \{hg \in G \mid h \in H\}$ und die Menge aller Rechtsklassen ist $H \backslash G$. Man kann auch die kanonische Projektion $G \rightarrow H \backslash G$ durch $g \mapsto Hg$ definieren.

Satz 1.1.25 Sei G eine Gruppe und H eine Untergruppe von G .

1. Es gilt $gH \cap g'H' \neq \emptyset \Rightarrow gH = g'H$ (m.a.W. $gH \neq g'H \Rightarrow gH \cap g'H' = \emptyset$).
2. Es gilt $G = \bigcup_{gH \in G/H} gH$. □

Beweis. Siehe LAI. Wir geben trotzdem einen Beweis.

1. Sei $gh \in gH \cap g'H$. Dann gibt es $h' \in H$ mit $gh = g'h'$. Sei $gh'' \in gH$. Dann gilt $gh'' = gh h^{-1} h'' = g'h' h^{-1} h'' \in g'H$ also $gH \subset g'H$. Analog gilt $g'H \subset gH$.
2. Sei $g \in G$. Dann gilt $g \in gH$. Umgekehrt gilt $gH \subset G$. ■

Korollar 1.1.26 (Satz von Lagrange) Es gilt $|G| = |G/H||H|$.

Beweis. Die Gruppe G ist die disjunkte Vereinigung aller gH für $gH = \bar{g} \in G/H$ also gilt

$$|G| = \sum_{\bar{g} \in G/H} |gH|.$$

Aber die Abbildungen $gH \rightarrow g'H$ und $g'H \rightarrow gH$ definiert durch $a \mapsto g'g^{-1}a$ und $a \mapsto gg'^{-1}a$ sind inverse von einander. Es gilt also $|gH| = |g'H|$ für alle $g, g' \in G$ und insbesondere für $g' = e_G$ gilt $|gH| = |H|$. Daraus folgt $|G| = \sum_{\bar{g} \in G/H} |gH| = \sum_{\bar{g} \in G/H} |H| = |G/H||H|$. ■

Definition 1.1.27 Sei G eine Gruppe und H eine Untergruppe von G .

1. Die **Ordnung** von G ist $|G|$ die Anzahl aller Elementen in G (die **Mächtigkeit** von G).
2. Der **Index** von H in G ist $[G : H] = |G/H|$.

Korollar 1.1.28 Sei G eine endliche Gruppe und H eine Untergruppe. Dann sind die Ordnung $|H|$ und der Index $[G : H]$ von H Teiler der Ordnung $|G|$ von G .

1.2 Normalteiler

Definition 1.2.1 Sei G eine Gruppe. Eine Untergruppe H von G heißt **Normalteiler** falls für alle $g \in G$ gilt $gHg^{-1} \subset H$. Man schreibt $H \triangleleft G$.

Bemerkung 1.2.2 Eine Untergruppe H ist genau dann ein Normalteiler wenn gilt $ghg^{-1} \in H$ für alle $g \in G$ und alle $h \in H$.

Lemma 1.2.3 Jede Untergruppe einer abelschen Gruppe G ist normal. □

Beweis. Klar. ■

Lemma 1.2.4 Eine Untergruppe H ist genau dann Normalteiler, wenn $gH = Hg$ für alle $g \in G$. □

Beweis. Siehe Übungsblatt 0. ■

Beispiel 1.2.5 1. Die triviale Untergruppe $\{e_G\}$ und die Gruppe G sind Normalteiler von G : $\{e_G\} \triangleleft G$ und $G \triangleleft G$.

2. $n\mathbb{Z} \triangleleft \mathbb{Z}$.

3. $SL_n(K) \triangleleft GL_n(K)$ aber $SO_n(K) \not\triangleleft GL_n(K)$.

Lemma 1.2.6 Sei $f : G \rightarrow G'$ ein Gruppenhomomorphismus und seien $H \triangleleft G$ und $H' \triangleleft G'$.

1. Dann ist $f^{-1}(H') \triangleleft G$. Insbesondere gilt $\text{Ker } f \triangleleft G$.

2. Falls f surjektiv ist, gilt $f(H) \triangleleft G'$. □

Beweis. 1. Sei $g \in G$ und $h \in f^{-1}(H')$. Dann gilt $f(ghg^{-1}) = f(g)f(h)f(g)^{-1} \in H'$ also $ghg^{-1} \in f^{-1}(H')$.

2. Sei $g' \in G'$ und $h' \in f(H)$. Dann gibt es ein $h \in H$ mit $h' = f(h)$. Da f surjektiv ist gibt es ein $g \in G$ mit $f(g) = g'$. Dann gilt $g'h'g'^{-1} = f(g)f(h)f(g)^{-1} = f(ghg^{-1}) \in f(H)$. ■

Satz 1.2.7 Sei $H \triangleleft G$. Dann ist die Verknüpfung $G/H \times G/H \rightarrow G/H$, $(\bar{g}, \bar{g}') \mapsto \overline{gg'}$ wohl definiert und G/H ist mit dieser Verknüpfung eine Gruppe. Außerdem ist die kanonische Projektion $G \rightarrow G/H$ ein Gruppenhomomorphismus. □

Beweis. Seien $a, b \in G$ mit $\bar{a} = \bar{g}$ und $\bar{b} = \bar{g}'$. Wir zeigen, dass $\overline{ab} = \overline{gg'}$. Sei $h \in H$ mit $a = gh$ und $h' \in H$ mit $b = g'h'$. Da $g'H = Hg'$ gibt es $h'' \in H$ mit $hg' = gh''$. Es gilt

$$\overline{ab} = abH = ghg'h'H = gg'h''h'H = gg'H = \overline{gg'}.$$

Die Verknüpfung ist also wohl definiert.

Es gilt $\bar{g}\bar{e}_G = \overline{ge_G} = \bar{g}$ und analog gilt $\bar{e}_G\bar{g} = \bar{g}$ also gilt $\bar{e}_G = e_{G/H}$. Es gilt $\bar{g}(\bar{g}'\bar{g}'') = \overline{gg'g''} = \overline{g(g'g'')} = \overline{(gg')g''} = \overline{gg'g''} = (\bar{g}\bar{g}')\bar{g}''$. Es gilt $\bar{g}\bar{g}^{-1} = \overline{gg^{-1}} = \bar{e}_G$ und analog $\bar{g}^{-1}\bar{g} = \bar{e}_G$. Daraus folgt auch, dass die kanonische Projektion ein Gruppenhomomorphismus ist. ■

Definition 1.2.8 Sei H ein Normalteiler von G . Die Gruppe G/H heißt **Quotientgruppe** von G nach H .

Beispiel 1.2.9 Die Gruppe $\mathbb{Z}/n\mathbb{Z}$ ist die Quotientgruppe von \mathbb{Z} nach $n\mathbb{Z}$.

Satz 1.2.10 Sei $f : G \rightarrow G'$ ein Gruppenhomomorphismus, sei H ein Normalteiler von G und sei $p : G \rightarrow G/H$ die kanonische Projektion.

1. Es gibt ein eindeutig bestimmter Gruppenhomomorphismus $\bar{f} : G/H \rightarrow G'$ so, dass das Diagramm

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ p \downarrow & \nearrow \bar{f} & \\ G/H & & \end{array}$$

kommutiert, genau dann wenn $H \subset \text{Ker} f$.

Angenommen $H \subset \text{Ker} f$ und sei \bar{f} wie in 1.

2. Die Abbildung \bar{f} ist genau dann injektiv, wenn $H = \text{Ker} f$.

3. Die Abbildung \bar{f} ist genau dann surjektiv, wenn f surjektiv ist. □

Beweis. 1. Sei \bar{f} wie oben und sei $h \in H$. Dann gilt $f(h) = \bar{f} \circ p(h)$. Aber $p(h) = [h] = hH = H = [e_G] = e_{G/H}$. Daraus folgt $f(h) = \bar{f}(e_{G/H}) = e_{G'}$ da \bar{f} ein Gruppenhomomorphismus ist. Es folgt $H \subset \text{Ker} f$.

Umgekehrt sei $H \subset \text{Ker} f$. Sei $g \in G$, wir setzen $\bar{f}([g]) = f(g)$ (die ist die einzige Möglichkeit so, dass das Diagramm kommutiert, dies zeigt, dass \bar{f} eindeutig bestimmt ist). Sei g' mit $[g'] = [g]$. Es gibt $h \in H$ mit $g' = gh$ und es gilt $f(g') = f(gh) = f(g)f(h) = f(g)e_{G'} = f(g)$. Also ist die Abbildung \bar{f} wohl definiert. Außerdem gilt $\bar{f}([g][g']) = \bar{f}([gg']) = f(gg') = f(g)f(g') = \bar{f}([g])\bar{f}([g'])$ und \bar{f} ist ein Gruppenhomomorphismus. Darüber hinaus gilt $\bar{f} \circ p(g) = \bar{f}([g]) = f(g)$ und das Diagramm ist kommutativ.

2. Sei \bar{f} injektiv. Dann gilt $\text{Ker} \bar{f} = \{e_{G/H}\}$. Sei $g \in \text{Ker} f$. Es gilt $\bar{f}([g]) = e_{G'}$ also $[g] \in \text{Ker} \bar{f}$ und da \bar{f} injektiv ist, gilt $[g] = e_{G/H}$. Es folgt $gH = [g] = e_{G/H} = H$ und $g \in H$. Also $\text{Ker} f \subset H$ und da $H \subset \text{Ker} f$ folgt $H = \text{Ker} f$.

Umgekehrt sei $H = \text{Ker} f$ und sei $[g] \in \text{Ker} \bar{f}$. Es gilt $f(g) = \bar{f}([g]) = e_{G'}$ also $g \in \text{Ker} f = H$. Es folgt $[g] = H = e_{G/H}$ und \bar{f} ist injektiv.

3. Sei f surjektiv und sei $g' \in G'$. Dann gibt es $g \in G$ mit $f(g) = g'$. Es gilt $\bar{f}([g]) = f(g) = g'$ also ist \bar{f} auch surjektiv.

Umgekehrt, sei \bar{f} surjektiv und sei $g' \in G'$. Es gibt $[g] \in G/H$ mit $\bar{f}([g]) = g'$. Daraus folgt $f(g) = \bar{f}([g]) = g'$ und f ist surjektiv. ■

Korollar 1.2.11 Sei $f : G \rightarrow G'$ ein surjektiver Gruppenhomomorphismus. Dann gilt $G/\text{Ker } f \simeq G'$.

Beispiel 1.2.12 1. Es gilt $\text{GL}_n(k)/\text{SL}_n(k) \simeq k^\times$ (der Kernel des surjektiven Gruppenhomomorphismus $\det : \text{GL}_n(k) \rightarrow k^\times$ ist $\text{SL}_n(k)$).

2. Es gilt $\mathbb{C}^\times/S^1 \simeq \mathbb{R}_{>0}$ (der Kernel des surjektiven Gruppenhomomorphismus $|\cdot| : \mathbb{C}^\times \rightarrow \mathbb{R}_{>0}$ ist S^1).

3. Es gilt $\mathbb{R}/\mathbb{Z} \simeq S^1$ (der Kernel des surjektiven Gruppenhomomorphismus $r \mapsto e^{2i\pi r}$ ist \mathbb{Z}).

4. Es gilt $S_n/A_n \simeq \{\pm 1\}$ (der Kernel des surjektiven Gruppenhomomorphismus $\varepsilon : S_n \rightarrow \{\pm 1\}$ ist A_n).

Definition 1.2.13 Ein Diagramm $1 \longrightarrow H \xrightarrow{i} G \xrightarrow{f} G' \longrightarrow 1$ heißt **exakte Sequenz**,

- wenn alle Abbildungen Gruppenhomomorphismen sind,
- wenn i injektiv ist,
- wenn f surjektiv ist und
- wenn $i(H) = \text{Ker } f$.

Bemerkung 1.2.14 Falls $1 \longrightarrow H \xrightarrow{i} G \xrightarrow{f} G' \longrightarrow 1$ eine exakte Sequenz ist, gilt $G' \simeq G/H$.

Beispiel 1.2.15 Es gibt (Siehe Übungsblatt 1) eine exakte Sequenz

$$1 \rightarrow A_3 \simeq \mathbb{Z}/3\mathbb{Z} \rightarrow S_3 \rightarrow \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z} \rightarrow 1.$$

Definition 1.2.16 Eine Gruppe G heißt **einfach** falls G und $\{e_G\}$ die einzigen Normalteiler von G sind.

Beispiel 1.2.17 1. Die Gruppe $\mathbb{Z}/n\mathbb{Z}$ ist genau dann einfach, wenn p eine Primzahl ist (Siehe Übungsblatt 1).

2. Später zeigen wir, dass die Gruppe $A_n = \text{Ker}(\varepsilon : S_n \rightarrow \{\pm 1\})$ einfach für $n \geq 5$ ist.

Definition 1.2.18 Sei G eine Gruppe und H eine Untergruppe. Der **Normalisator** $N_G(H)$ von H in G ist

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

Lemma 1.2.19 Sei G eine Gruppe und H eine Untergruppe.

1. Der Normalisator $N_G(H)$ ist eine Untergruppe von G .
2. Es gilt $H \triangleleft N_G(H)$ (also H ist Normalteiler in $N_G(H)$).
3. Sei K eine Untergruppe von G mit $H \triangleleft K$. Dann gilt $K \subset N_G(H)$ (i.e. $N_G(H)$ ist die größte Untergruppe von G mit $H \triangleleft N_G(H)$). \square

Beweis. 1. Es gilt $e_G H e_G^{-1} = e_G H e_G = H$ also $e_G \in N_G(H)$. Seien $a, b \in N_G(H)$. Dann gilt $a H a^{-1} = H$ und $b H b^{-1} = H$ also $b^{-1} H b = H$. Daraus folgt

$$(ab^{-1})H(ab^{-1})^{-1} = ab^{-1}Hba^{-1} = aHa^{-1} = H$$

und $ab^{-1} \in N_G(H)$ und $N_G(H)$ ist eine Untergruppe von G .

2. Klar.

3. Sei K eine Untergruppe mit $H \triangleleft K$. Sei $k \in K$. Dann gilt $kH^{-1} \subset K$. Da K eine Gruppe ist gilt auch $k^{-1} \in K$ also $k^{-1}Hk \subset H$ und mit Linksmultiplikation mit k und Rechtsmultiplikation mit k^{-1} folgt $H \subset kHk^{-1}$. Daraus folgt $kHk^{-1} = H$ und $k \in N_G(H)$. \blacksquare

Beispiel 1.2.20 Sei $G = S_3$ und sei $H = \{(123) = \text{Id}, (213)\}$ und $A_3 = \{(123) = \text{Id}, (231), (312)\}$. Dann sind H und A_3 Untergruppe von G und es gilt (siehe Übungsblatt 1)

$$N_G(H) = H \text{ und } N_G(A_3) = S_3.$$

Satz 1.2.21 (Erster Isomorphiesatz) Sei G eine Gruppe, $H \triangleleft G$ ein Normalteiler von G und $K \subset G$ eine Untergruppe von G .

1. Dann gilt $HK = KH$, $KH \subset G$ ist eine Untergruppe, $H \triangleleft KH$ und $K \cap H \triangleleft K$.
2. Die Abbildung $f : K/(K \cap H) \rightarrow KH/H$ definiert durch $k(K \cap H) \mapsto kH$ ist ein Isomorphismus also

$$K/(K \cap H) \simeq KH/H.$$

Beweis. 1. Sei $h \in H$ und $k \in K$. Da H ein Normalteiler ist, gilt $khk^{-1} \in H$ und es folgt $kh \in Hk \subset HK$. Daraus folgt $KH \subset HK$. Analog gilt $k^{-1}hk \in H$ und $hk \in kH \subset KH$. Daraus folgt $HK \subset KH$ und $KH = HK$.

Da $e_G \in H$ und $e_G \in K$ gilt $e_G \in KH$. Seien $k, k' \in K$ und $h, h' \in H$ so, dass $kh, k'h' \in KH$. Es gilt $kh(k'h')^{-1} = kh h'^{-1} k'^{-1} \in KHK = KKH = KH$. Daraus folgt, dass KH eine Untergruppe ist.

Da H ein Normalteiler ist, gilt $gHg^{-1} \subset H$ für alle $g \in G$. Insbesondere für alle $g \in KH$ und es folgt $H \triangleleft KH$.

Sei $g \in H \cap K$ und $k \in K$. Es gilt $kgk^{-1} \in K$ und da H ein Normalteiler ist, gilt auch $kgk^{-1} \in H$. Also $kgk^{-1} \in H \cap K$ und $H \cap K \triangleleft K$.

2. Sei $f : K \rightarrow KH/H$ die Abbildung definiert durch $f(k) = kH$. Seien $k, k' \in K$. Es gilt $f(kk') = kH \cdot k'H = kk'H = f(kk')$ also ist f ein Gruppenhomomorphismus. Seien $k \in K$ und $h \in H$. Dann gilt $f(k) = kH = khH$ und f ist surjektiv. Sei $k \in K \cap H$. Dann gilt $f(k) = kH = H = e_{KH/H}$ also $H \cap K \subset \text{Ker} f$. Sei $k \in K \cap \text{Ker} f$. Dann gilt $kH = f(k) = H$ und $k \in H$ also $k \in H \cap K$. Es folgt $H \cap K = \text{Ker} f$. Nach Korollar 1.2.11 folgt, dass $K/(H \cap K) \simeq KH/H$. ■

Satz 1.2.22 (Zweiter Isomorphiesatz) Sei G eine Gruppe und seien $H \triangleleft G$ und $K \triangleleft G$ mit $K \subset H$.

1. Dann gilt $K \triangleleft H$ und $H/K \triangleleft G/K$.

2. Die Abbildung $f : (G/K)/(H/K) \rightarrow G/H$ definiert durch $gK \cdot H/K \mapsto gH$ ist ein Isomorphismus also

$$(G/K)/(H/K) \simeq G/H.$$

Beweis. 1. Sei $h \in H \subset G$. Da $K \triangleleft G$ gilt $hKh^{-1} = K$ und $K \triangleleft H$.

Die Teilmenge $H/K \subset G/K$ ist $\pi_K(H)$, wobei $\pi : G \rightarrow G/K$ die kanonische Projektion ist. Da $H \triangleleft G$ und π surjektiv folgt, dass $H/K \triangleleft G/K$.

2. Die kanonische Projektion $\pi_H : G \rightarrow G/H$ ist ein surjektiver Gruppenhomomorphismus und es gilt $K \subset H = \text{Ker} \pi_H$. Daraus folgt, dass es ein surjektiver Gruppenhomomorphismus $F = \bar{\pi}_H : G/K \rightarrow G/H$ gibt mit $\pi_H = \pi_K \circ F$ also $F([g]_K) = [g]_H$.

Wir zeigen, dass $\text{Ker} F = H/K$. Daraus folgt, dass es ein Gruppenisomorphismus $\bar{F} : (G/K)/(H/K) \rightarrow G/H$ gibt mit $\bar{F}([g]_K)_{H/K} = [g]_H$. Sei $[g]_K \in \text{Ker} F$. Dann gilt $[e_G]_H = F([g]_K) = [g]_H$ also $g \in H$ und $[g]_K \in H/K$. Umgekehrt, sei $[g]_K \in H/K$ also $[g]_K = [h]_K$ für ein $h \in H$ i.e. es gibt ein $k \in K$ mit $g = hk$. Da $K \subset H$ gilt $g \in H$. Daraus folgt $[g]_H = [e_G]_H$ und $F([g]_K) = [g]_H = [e_G]_H$ also $[g]_K \in \text{Ker} F$. Umgekehrt, sei $[g]_K \in \text{Ker} F$. Es gilt $[g]_H = F([g]_K) = [e_G]_H$ also $g \in H$. Daraus folgt $[g]_K \in H/K$. ■

1.3 Zentrum

Definition 1.3.1 Sei G eine Gruppe.

1. **Das Zentrum** einer Gruppe G ist die Menge

$$Z(G) = \{g \in G \mid gh = hg \text{ für alle } h \in G\}.$$

2. Sei $X \subset G$ eine Teilmenge. Der **Zentralisator** von G ist die Teilmenge

$$Z_G(X) = \{g \in G \mid gx = xg \text{ für alle } x \in X\}.$$

Bemerkung 1.3.2 Es gilt $Z(G) = Z_G(G)$.

Beispiel 1.3.3 1. Sei G eine kommutative Gruppe. Dann gilt $Z(G) = G$.

2. Sei $G = S_n$. Dann gilt $Z(S_n) = \{\text{Id}\}$ (Siehe Übungsblatt 2) für $n \geq 3$.

Lemma 1.3.4 Sei G eine Gruppe und $X \subset G$ eine Teilmenge.

1. Der Zentralisator $Z_G(X)$ ist eine Untergruppe.
2. Das Zentrum $Z(G)$ ist ein Normalteiler von G und $Z_G(X)$ und ist abelsch.
3. Es gilt $G/Z(G) \simeq \{\text{innere Automorphismen}\}$.
4. Falls $G/Z(G)$ zyklisch ist (siehe Definition 1.4.2 unten), gilt $G = Z(G)$ also G ist abelsch. \square

Beweis. 1. Es gilt $e_G x = x e_G$ für alle $x \in G$ also ist $e_G \in Z_G(X)$. Seien $g, h \in Z_G(X)$. Es gilt $gx0xg$ und $hx = xh$ für alle $x \in X$. Daraus folgt $xh^{-1} = h^{-1}x$ für alle $x \in X$ und $xgh^{-1} = gxh^{-1} = gh^{-1}x$ i.e. $gh^{-1} \in Z_G(X)$.

2. Nach der Definition gilt $Z(G) \subset Z_G(X)$. Sei $z \in Z(G)$ und $g \in G$. Es gilt $gzg^{-1} = gg^{-1}z = z$ also $gzg^{-1} \in Z(G)$. Daraus folgt, dass $Z(G)$ ein Normalteiler in G und $Z_G(X)$ ist. Seien $z, z' \in Z(G)$. Es gilt $zz' = z'z$ also $Z(G)$ ist abelsch.

3. Sei $f : G \rightarrow \{\text{innere Automorphismen}\}$ definiert durch $f(g) = \text{Int}_g$. Diese Abbildung ist surjektiv und es gilt $f(gh) = \text{Int}_{gh} = \text{Int}_g \circ \text{Int}_h$ (es gilt $\text{Int}_g \circ \text{Int}_h(g') = \text{Int}_g(hg'h^{-1}) = ghg'h^{-1}g^{-1} = (gh)g'(gh)^{-1} = \text{Int}_{gh}(g')$). Die Abbildung ist also ein surjektiver Gruppenhomomorphismus. Sei $g \in \text{Ker}(f)$. Es gilt $\text{Int}_g = \text{Id}$ also $\text{Int}_g(h) = h$ für alle $h \in G$. Dies ist äquivalent zu $ghg^{-1} = h$ für alle $h \in H$ und auch zu $gh = hg$ für alle $h \in G$. Also $\text{Ker}(f) = Z(G)$.

4. Seien $g, h \in G$ und sei $\pi : G \rightarrow G/Z(G)$ die kanonische Projektion. Da $G/Z(G)$ zyklisch ist gibt es ein $a \in G$ mit $G/Z(G) = \langle [a] \rangle$. Insbesondere gibt es $n, m \in \mathbb{Z}$ mit $[g] = [a]^n$ und $[h] = [a]^m$. Es gibt also $z, z' \in Z(G)$ mit $g = a^n z$ und $h = a^m z'$. Daraus folgt $gh = a^n z a^m z' = a^m z' a^n z = hg$ und G ist kommutativ. \blacksquare

1.4 Erzeuger und Zyklische Gruppe

Lemma 1.4.1 Sei G eine Gruppe.

1. Sei $(H_i)_{i \in I}$ eine Familie von Untergruppen von G . Dann ist $\bigcap_{i \in I} H_i$ eine Untergruppe von G .
2. Sei A eine Teilmenge von G . Dann gibt es eine kleinste Untergruppe H mit $A \subset H$. \square

Beweis. 1. Siehe Übungsblatt 1.

2. Sei $(H_i)_i$ die Familie aller Untergruppen von G die A enthalten (diese Familie ist nicht leer da G eine solche Gruppe ist). Dann ist $H = \bigcap_{i \in I} H_i$ die minimale Untergruppe die A enthält ■

Definition 1.4.2 1. Sei G eine Gruppe und A eine Teilmenge von G . Die kleinste Untergruppe die A enthält heißt **die von A erzeugte Untergruppe** und ist $\langle A \rangle$ geschrieben. Falls A nur einelementig ist: $A = \{g\}$ schreibt man $\langle A \rangle = \langle g \rangle$.

2. Eine Teilmenge A einer Gruppe G heißt **erzeugend** (man sagt auch A **erzeugt** G) falls $G = \langle A \rangle$.

3. Eine Gruppe G heißt **zyklisch** falls es ein Element $g \in G$ gibt mit $G = \langle g \rangle$.

Beispiel 1.4.3 1. Die Gruppe $(\mathbb{Z}, +)$ ist zyklisch und 1 erzeugt \mathbb{Z} .

2. Sei $n \in \mathbb{Z}$. Die Gruppe $(\mathbb{Z}/n, +)$ ist zyklisch und $\bar{1}$ erzeugt $\mathbb{Z}/n\mathbb{Z}$.

3. Die einfache Transpositionen $(s_i)_{i \in [1, n-1]}$ definiert durch

$$s_i(k) = \begin{cases} k & \text{für } k \notin \{i, i+1\} \\ i+1 & \text{für } k = i \\ i & \text{für } k = i+1 \end{cases}$$

erzeugen S_n i.e. $S_n = \langle s_i \mid i \in [1, n-1] \rangle$ (Siehe LAII).

Lemma 1.4.4 Sei G eine Gruppe und $g \in G$. Es gilt $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$. □

Beweis. Sei $n \in \mathbb{Z}$. Da $\langle g \rangle$ eine Gruppe ist und enthält g , gilt $g^{-1} \in \langle g \rangle$ und $g^n \in \langle g \rangle$ also $\{g^n \mid n \in \mathbb{Z}\} \subset \langle g \rangle$.

Umgekehrt, seien $n, m \in \mathbb{Z}$. Dann ist $(g^n)(g^m)^{-1} = g^{n-m} \in \{g^n \mid n \in \mathbb{Z}\}$ und $e_G = g^0 \in \{g^n \mid n \in \mathbb{Z}\}$. Daraus folgt, dass $\{g^n \mid n \in \mathbb{Z}\}$ eine Untergruppe von G ist und enthält g . Also $\langle g \rangle \subset \{g^n \mid n \in \mathbb{Z}\}$. ■

Satz 1.4.5 Sei G eine zyklische Gruppe. Dann ist G isomorph zu \mathbb{Z} oder $\mathbb{Z}/n\mathbb{Z}$. □

Beweis. Sei $g \in G$ so, dass $G = \langle g \rangle$. Sei $f : \mathbb{Z} \rightarrow G$ definiert durch $f(n) = g^n$. Dies ist ein Gruppenhomomorphismus und nach dem obigen Lemma folgt $f(\mathbb{Z}) = G$. Falls f injektiv ist, ist f ein Isomorphismus und $G \simeq \mathbb{Z}$. Sonst sei $N = \text{Ker } f$. Dann ist N eine Untergruppe von \mathbb{Z} und es folgt $N = n\mathbb{Z}$ für eine $n \in \mathbb{Z}$ (Siehe Übungsblatt 0 oder im Beweis von Korollar 1.4.7). Es folgt (nach Korollar 1.2.11) $G = \mathbb{Z}/N = \mathbb{Z}/n\mathbb{Z}$. ■

Korollar 1.4.6 Sei p eine Primzahl und G eine Gruppe mit $|G| = p$.

1. Sei $g \in G$ mit $g \neq e_G$. Dann gilt $G \simeq \langle g \rangle$.

2. Es gilt $G \simeq \mathbb{Z}/p\mathbb{Z}$.

Beweis. 1. Sei $H = \langle g \rangle$. Dann gilt $e_G, g \in H$ also $|H| \geq 2$. Nach dem Satz von Lagrange gilt $|H|$ teilt p also $|H| = p = |G|$ und $H = G$.

2. Folgt vom obigen Satz. ■

Korollar 1.4.7 Jede Untergruppe einer zyklischen Gruppe ist zyklisch.

Beweis. Die Gruppe G ist isomorph zu \mathbb{Z} oder $\mathbb{Z}/n\mathbb{Z}$. Es wurde im Übungsblatt 0 gezeigt, dass die Untergruppen zyklisch sind. Wir geben dennoch einen Beweis.

Angenommen $G = \mathbb{Z}$. Sei H eine Untergruppe von \mathbb{Z} . Falls $H = \{0\}$ sind wir fertig. Sonst ist $H \cap \mathbb{Z}_{>0} \neq \emptyset$. Sei $m = \min\{r \in H \mid r > 0\}$. Sei $n \in H$. Dann gibt es $k \in \mathbb{Z}$ und $r \in [0, m-1]$ mit $n = km + r$. Da H eine Gruppe ist gilt $r = n - km \in H$ und da m minimal war, gilt $r = 0$. Daraus folgt $H = m\mathbb{Z}$.

Sei $G = \mathbb{Z}/n\mathbb{Z}$ und sei H eine Untergruppe von G . Sei $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} = G$ die kanonische Projektion. Dann ist $\pi^{-1}(H)$ eine Untergruppe von \mathbb{Z} also gibt es ein $m \in \mathbb{Z}$ mit $\pi^{-1}(H) = m\mathbb{Z}$. Da die kanonische Projektion surjektiv ist, folgt $H = \pi(\pi^{-1}(H)) = \pi(m\mathbb{Z}) = \{k[m] = [mk] \in \mathbb{Z}/n\mathbb{Z}\}$. ■

1.5 Ordnung eines Elements

Definition 1.5.1 Sei G eine Gruppe und $g \in G$. Die **Ordnung** $\text{ord}(g)$ von g ist die Ordnung der Gruppe $\langle g \rangle$.

Lemma 1.5.2 Es gilt $\{k \in \mathbb{Z}_{\geq 0} \mid g^k = e_G\} = \text{ord}(g)\mathbb{Z}$ (wir setzen $\infty\mathbb{Z} = \{0\}$). □

Beweis. Nach Satz 1.4.5 ist die Gruppe $\langle g \rangle$ isomorph zu \mathbb{Z} oder $\mathbb{Z}/n\mathbb{Z}$.

Im ersten Fall gilt $\text{ord}(g) = \infty$ und im zweiten Fall gilt $\text{ord}(g) = n$. Außerdem ist die Abbildung $\mathbb{Z} \rightarrow \langle g \rangle$ bzw. $\mathbb{Z}/n\mathbb{Z} \rightarrow \langle g \rangle$ definiert durch $k \mapsto g^k$ bzw. $[k] \mapsto g^k$ ein Isomorphismus.

Im ersten Fall gilt $\{k \in \mathbb{Z}_{\geq 0} \mid g^k = e_G\} = \{0\}$. Im zweiten Fall gilt $\{k \in \mathbb{Z} \mid g^k = e_G\} = \{k \in \mathbb{Z} \mid [k] = 0 \in \mathbb{Z}/n\mathbb{Z}\} = n\mathbb{Z}$. ■

Lemma 1.5.3 Sei G eine Gruppe und $g \in G$ mit $\text{ord}(g) = n < \infty$. Dann gilt

$$\text{ord}(g^m) = \frac{n}{\text{ggT}(m, n)}$$

für alle $m \in \mathbb{Z}$. □

Beweis. Seien $d = \text{ggT}(m, n)$, $m' = \frac{m}{d} \in \mathbb{Z}$ und $n' = \frac{n}{d} \in \mathbb{Z}$. Sei $s = \text{ord}(g^m)$. Es gilt $g^{ms} = (g^m)^s = e_G$. Also gibt es $k \in \mathbb{Z}$ mit $ms = kn$. Es folgt $m's = n'k$. Da $\text{ggT}(m', n') = 1$ folgt $n' \mid s$.

Es gilt $(g^m)^{n'} = g^{mn'} = g^{m'dn'} = g^{m'n} = (g^n)^{m'} = e_G$. Daraus folgt $s \mid n'$. Insgesamt folgt $s = n'$. ■

Korollar 1.5.4 Die erzeugende Elemente von $\mathbb{Z}/n\mathbb{Z}$ sind die Klassen $[m] \in \mathbb{Z}/n\mathbb{Z}$ mit $\text{ggT}(m, n) = 1$.

Beweis. Sei $[m] \in \mathbb{Z}/n\mathbb{Z}$ mit $\mathbb{Z}/n\mathbb{Z} = \langle [m] \rangle$. Dann gilt $[m] = m[1]$ und $\text{ord}([1]) = n$. Daraus folgt $\text{ord}(m) = n/\text{ggT}(m, n)$.

Die Klasse $[m]$ ist aber genau dann erzeugend, wenn $\text{ord}([m]) = n$ also $n/\text{ggT}(m, n) = n$ i.e. $\text{ggT}(m, n) = 1$. ■

Beispiel 1.5.5 Die erzeugende Klassen in $\mathbb{Z}/4\mathbb{Z}$ sind $[1]$ und $[3]$.

Korollar 1.5.6 Sei $n \in \mathbb{Z}$. Die Gruppe $\mathbb{Z}/n\mathbb{Z}$ hat für jedes $m|n$ genau eine Untergruppe der Ordnung m : die Gruppe

$$m\mathbb{Z}/n\mathbb{Z} = \{[km] \in \mathbb{Z}/n\mathbb{Z} \mid k \in \mathbb{Z}\}.$$

Beweis. Dies wurde im Übungsblatt 0 bewiesen. Wir geben dennoch einen Beweis. Sei H eine Untergruppe von $\mathbb{Z}/n\mathbb{Z}$ und sei $d = \min\{k \in \mathbb{Z}_{>0} \mid [k] \in H\}$. Da $[0] = [n] \in H$ gilt $0 < d \leq n$. Sei $[k] \in H$. Wir schreiben $k = da + b$ mit $a, b \in \mathbb{Z}$ und $b \in [0, d-1]$. Es gilt $[k], [d] \in H$ also $[b] = [k] - a[d] \in H$. Da d minimal ist, folgt $b = 0$ und $k \in d\mathbb{Z}$. Es folgt $H = d\mathbb{Z}/n\mathbb{Z} = \{[kd] \in \mathbb{Z}/n\mathbb{Z} \mid k \in \mathbb{Z}\} = \langle [d] \rangle$. Außerdem gilt $\text{ord}([d]) = \frac{n}{\text{ggT}(n, d)} = \frac{n}{d} := m$. ■

1.6 Derivierte Untergruppe

Definition 1.6.1 Sei G eine Gruppe, seien $g, h \in G$ und seien $H, K \subset G$ Untergruppen.

1. Der **Kommutator** von g und h ist $[g, h] = ghg^{-1}h^{-1}$.
2. Der **Kommutator** $[H, K]$ von H und K ist die Gruppe $[H, K] = \langle [h, k] \mid h \in H \text{ und } k \in K \rangle$.
3. Die **derivierte Gruppe** $D(G)$ von G ist die Gruppe $D(G) = [G, G]$ (manchmal wird $D(G)$ auch (G, G) bezeichnet).

Lemma 1.6.2 Sei G eine Gruppe.

1. $D(G) = \{[g_1, h_1] \cdots [g_n, h_n] \mid n \in \mathbb{Z}_{\geq 0} \text{ und } g_i, h_i \in G\}$.
2. $D(G)$ ist eine Normalteiler in G .
3. $G/D(G)$ ist abelsch.
4. Sei $N \triangleleft G$ mit G/N abelsch. Dann gilt $D(G) \subset N$. Also ist $D(G)$ die kleinste Untergruppe so, dass $G/D(G)$ abelsch ist. □

Beweis. 1. Sei $H = \{[g_1, h_1] \cdots [g_n, h_n] \mid n \in \mathbb{Z}_{\geq 0} \text{ und } g_i, h_i \in G\}$. Es gilt $H \subset D(G)$. Wir zeigen, dass H eine Untergruppe ist. Alle Produkte von Elementen aus H sind noch in H . Es gilt $[g, h]^{-1} = [h, g]$ also ist das Inverses jedes Element aus H noch in H und H ist eine Untergruppe. Daraus folgt $D(G) \subset H$ da $D(G)$ die kleinste Untergruppe die alle Kommutatoren enthält ist.

2. Seien $g, h, k \in G$. Es gilt $k[g, h]k^{-1} = [kgk^{-1}, khk^{-1}]$. Daraus folgt $k[g, h]k^{-1} \in D(G)$ und nach 1. $kD(G)k^{-1} \subset D(G)$.

3. Seien $g, h \in G$. Dann gilt $[ghg^{-1}h^{-1}] = e$ in $G/D(G)$ also $[g][h] = [h][g]$ und $G/D(G)$ ist abelsch.

4. Seien $g, h \in G$. Es gilt $[ghg^{-1}h^{-1}]_N = [g]_N[h]_N[g]_N^{-1}[h]_N^{-1} = [e_G]_N$ da G/N abelsch ist. Daraus folgt $ghg^{-1}h^{-1} \in N$ und $D(G) \subset N$. ■

1.7 Semidirekte Produkte

Lemma 1.7.1 Seien N und H zwei Gruppen und sei $\Phi : H \rightarrow \text{Aut}(N), h \mapsto \Phi_h$ ein Gruppen homomorphismus (wobei $\text{Aut}(N)$ die Gruppe aller Automorphismen von N ist).

Sei $N \rtimes H := N \times_{\Phi} H := (N \times H, \star)$ mit

$$(n, h) \star (n', h') = (n\Phi_h(n'), hh').$$

Dann ist $N \rtimes H$ eine Gruppe mit neutralem Element (e_N, e_H) und Inverse $(n, h)^{-1} = (\Phi_{h^{-1}}(n^{-1}), h^{-1})$. □

Beweis. Es gilt $(e_N, e_H) \star (n, h) = (e_N \Phi_{e_H}(n), e_H h) = (\text{Id}_N(n), h) = (n, h)$ und $(n, h) \star (e_N, e_H) = (n \Phi_h(e_N), h e_H) = (n, h)$.

Es gilt $(n, h) \star (\Phi_{h^{-1}}(n^{-1}), h^{-1}) = (n \Phi_h(\Phi_{h^{-1}}(n^{-1})), hh^{-1}) = (n \Phi_{hh^{-1}}(n^{-1}), e_H) = (n \text{Id}_N(n^{-1}), e_H) = (nn^{-1}, e_H) = (e_N, e_H)$. Es gilt auch $(\Phi_{h^{-1}}(n^{-1}), h^{-1}) \star (n, h) = (\Phi_{h^{-1}}(n^{-1}) \Phi_{h^{-1}}(n), h^{-1}h) = (\Phi_{h^{-1}}(n^{-1}n), e_H) = (\Phi_{h^{-1}}(e_G), e_H) = (e_N, e_H)$.

Es gilt

$$\begin{aligned} (n, h) \star ((n', h') \star (n'', h'')) &= (n, h) \star (n' \Phi_{h'}(n''), h' h'') \\ &= (n \Phi_h(n' \Phi_{h'}(n'')), hh' h'') \\ &= (n \Phi_h(n') \Phi_{hh'}(n''), hh' h'') \\ &= (n \Phi_h(n'), hh') \star (n'', h'') \\ &= ((n, h) \star (n', h')) \star (n'', h'') \end{aligned}$$

Daraus folgt, dass $N \rtimes H$ eine Gruppe ist. ■

Definition 1.7.2 Seien N und H zwei Gruppen und sei $\Phi : H \rightarrow \text{Aut}(N), h \mapsto \Phi_h$ ein Gruppen homomorphismus. Das heißt die Gruppe $N \rtimes H := N \times_{\Phi} H := (N \times H, \star)$ mit Produkt $(n, h) \star (n', h') = (n \Phi_h(n'), hh')$ **semidirektes Produkt von N und H bzgl. Φ** .

Beispiel 1.7.3 Sei $\Phi : H \rightarrow \text{Aut}(N)$ definiert durch $\Phi_h = \text{Id}_N$ für alle $h \in H$. Dann gilt

$$(n, h) \star (n', h') = (n\Phi_h(n'), hh') = (n\text{Id}_N(n'), hh') = (nn', hh')$$

und das semidirekte Produkt ist die Produktgruppe.

Lemma 1.7.4 Sei $G = N \rtimes H$ und seien $N' = \{(n, e_H) \mid n \in N\}$ und $H' = \{(e_N, h) \mid h \in H\}$.

1. Dann ist H' eine Untergruppe von G und $N' \triangleleft G$.
2. Es gibt Isomorphismen $N \simeq N'$ und $H \simeq H'$ definiert durch $n \mapsto (n, e_H)$ und $h \mapsto (e_N, h)$.
3. Es gilt $N' \cap H' = \{e_G\}$ und $G = N'H'$. □

Beweis. 1. Die Abbildung $\pi : G \rightarrow H$ definiert durch $\pi(h)$ ist ein Gruppenhomomorphismus und $\text{Ker}\pi = N'$ also $N' \triangleleft G$. Es gilt $e_G \in H'$ und $(e_N, h) \star (e_N, h') = (e_N, hh')$ also H' ist eine Untergruppe von G .

2. Man überprüft leicht, dass diese Abbildungen injektive Gruppenhomomorphismen sind. Per Definition sind diese Abbildungen surjektiv.

3. Es gilt $N' \cap H' = \{(e_n, e_H)\} = \{e_G\}$ und $(n, h) = (n, e_H) \star (e_N, h)$ also $G = N'H'$. ■

Satz 1.7.5 Sei G eine Gruppe, H eine Untergruppe und $N \triangleleft G$.

1. Falls gilt $N \cap H = \{e_G\}$ und $G = NH$. Dann ist für $\Phi : H \rightarrow \text{Aut}(N)$ definiert durch $\Phi_h(n) = hnh^{-1}$ die Abbildung

$$f : N \times_\Phi H \rightarrow G, (n, h) \mapsto nh$$

ein Isomorphismus.

2. Falls zusätzlich gilt $H \triangleleft G$, so wird der Isomorphismus zu $f : N \times H \rightarrow G$. □

Beweis. 1. Es gilt

$$f((n, h) \star (n', h')) = f(n\Phi_h(n'), hh') = nhn'h^{-1}hh' = nhn'h' = f(n, h)f(n', h').$$

Daraus folgt, dass f ein Gruppenhomomorphismus ist. Da $G = NH$ ist diese Abbildung surjektiv. Sei $(n, h) \in \text{Ker}f$. Es gilt $nh = e_G$ also $n = h^{-1}$ und $n \in N \cap H$ also $n = e_G$. Daraus folgt $h = e_G$ und f ist injektiv also ein Isomorphismus.

2. Seien $h \in H$ und $n \in N$. Es gilt $N \ni n^{-1}(hnh^{-1}) = (n^{-1}hn)h^{-1} \in H$ also $n^{-1}hnh^{-1} = e_G$. Es folgt $hn = nh$ und $\Phi_h(n) = n$ und $N \rtimes H = N \times H$. ■

Beispiel 1.7.6 1. Sei $c = (231)$, sei $s = (213)$ und seien $N = A_3 = \{\text{Id}, c, c^2\}$ und $H = \{\text{Id}, s\}$. Da A_3 ein Normalteiler ist, sind $\text{Int}_s : A_3 \rightarrow A_3$ und $\text{Int}_{\text{Id}} : A_3 \rightarrow A_3$ Gruppenautomorphismen und die Abbildung $\Phi : H \rightarrow \text{Aut}(A_3)$, $\Phi_h = \text{Int}_h$ ist ein Gruppenhomomorphismus.

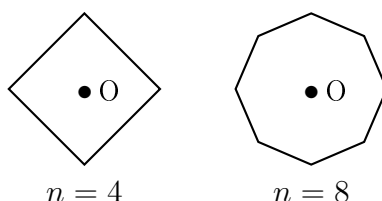
Dank dem obigen Satz zeigt man, dass die Abbildung

$$A_3 \rtimes H \rightarrow S_3, (n, h) \mapsto nh$$

ein Gruppenisomorphismus ist.

2. Allgemeiner gilt $S_n \simeq A_n \rtimes \{\pm 1\}$.

2. Diedergruppe. Sei R_n ein regelmäßiges Polygon. Zum Beispiel $R_n = \{e^{\frac{2ik\pi}{n}} \mid k \in [0, n-1]\}$.



Sei D_{2n} die Gruppe aller Isometrie die R_n erhalten. Man zeigt, dass D_{2n} genau $2n$ elemente hat. Sei O das Zentrum von R_n und seien D_1, \dots, D_n die Geraden die durch O und eine Ecke laufen oder die durch O und die Mitte einer Kante laufen. Sei R die Drehung um O von $\frac{2\pi}{n}$ und seien S_1, \dots, S_n die Spiegelungen an den Geraden D_1, \dots, D_n . Dann gilt

$$D_{2n} = \{\text{Id}, R, \dots, R^n, S_1, \dots, S_n\}.$$

Die Gruppe D_{2n} enthält $N = \{\text{Id}, R, \dots, R^n\}$ und man überprüft leicht, dass $N \triangleleft D_{2n}$. Sei $H = \{\text{Id}, S_1\}$. Dann ist H eine Untergruppe von G . Dank dem obigen Satz zeigt man, dass die Abbildung

$$N \rtimes H \rightarrow G, (n, h) \mapsto nh$$

ein Gruppenisomorphismus ist.

1.8 Operation einer Gruppe auf einer Menge

Definition 1.8.1 Sei G eine Gruppe und X eine Menge. Eine **Operation von G auf X** ist eine Abbildung $G \times X \rightarrow X$, $(g, x) \mapsto g \cdot x$ mit den Eigenschaften:

1. Für alle $x \in X$ gilt $e_G \cdot x = x$.
2. Für alle $g, h \in G$ und alle $x \in X$ gilt $(gh) \cdot x = g \cdot (h \cdot x)$.

Beispiel 1.8.2 1. Die **triviale Operation** $G \times X \rightarrow X$ definiert durch $g \cdot x = x$ für alle $g \in G$ und $x \in X$.

2. Die **Linkstranslation** $G \times G \rightarrow G$ definiert durch $g \cdot h = gh$ (hier ist $X = G$).

2. Die **Linkstranslation auf einem Quotient** $G \times G/H \rightarrow G/H$ definiert durch $g \cdot [g']_H = [gh]_H$ (hier ist $X = G/H$ wobei H eine Untergruppe ist).

3. Die **Konjugation** $G \times G \rightarrow G$ definiert durch $g \cdot h = ghg^{-1}$ (hier ist $X = G$).

4. $S_n \times [1, n] \rightarrow [1, n]$ definiert durch $\sigma \cdot i = \sigma(i)$.

4. $\text{GL}_n(K) \times K^n \rightarrow K^n$ definiert durch $A \cdot v = Av$.

Lemma 1.8.3 Sei $G \times X \rightarrow X$, $(g, x) \mapsto g \cdot x$ eine Operation.

1. Dann ist die Abbildung $\Phi(g) : X \rightarrow X$ definiert durch $\Phi(g)(x) = g \cdot x$ eine Bijektion von X und die Abbildung

$$\Phi : G \rightarrow \text{Bij}(X)$$

definiert durch $g \mapsto \Phi(g)$ ein Gruppenhomomorphismus.

2. Umgekehrt, sei $\Phi : G \rightarrow \text{Bij}(X)$ ein Gruppenhomomorphismus. Dann ist $G \times X \rightarrow X$ definiert durch $(g, x) \mapsto g \cdot x = \Phi(g)(x)$ eine Operation. \square

Beweis. 1. Wir zeigen, dass $\Phi(gh) = \Phi(g) \circ \Phi(h)$. Es gilt

$$\Phi(gh)(x) = (gh) \cdot x = g \cdot (h \cdot x) = \Phi(g)(h \cdot x) = \Phi(g)(\Phi(h)(x)) = (\Phi(g) \circ \Phi(h))(x).$$

Daraus folgt, dass $\Phi(g) \circ \Phi(g^{-1}) = \text{Id}_X = \Phi(g^{-1}) \circ \Phi(g)$ also ist $\Phi(g)$ bijektiv mit $\Phi(g)^{-1} = \Phi(g^{-1})$ und Φ ist ein Gruppenhomomorphismus.

2. Es gilt $e_G \cdot x = \Phi(e_G)(x) = \text{Id}_X(x) = x$ und $g \cdot (h \cdot x) = \Phi(g)(\Phi(h)(x)) = (\Phi(g) \circ \Phi(h))(x) = \Phi(gh)(x) = (gh) \cdot x$. \blacksquare

Definition 1.8.4 Sei $G \times X \rightarrow X$, $(g, x) \mapsto g \cdot x$ eine Operation von G auf X .

1. Die Operation heißt **transitiv**, falls es für alle $x, y \in X$ ein $g \in G$ gibt mit $g \cdot x = y$.

2. Eine Operation heißt **treu** falls $(g \cdot x = x \text{ für alle } x \in X) \Rightarrow (g = e_G)$.

3. Sei $x \in X$. Die Menge $G \cdot x = \{g \cdot x \in X \mid g \in G\}$ heißt **Orbit** oder **Bahn** von $x \in X$.

Man schreibt $X/G = \{G \cdot x \mid x \in X\}$ für die Menge aller Bahnen. Diese Menge heisst **Quotient von X nach G** .

4. Ein $x \in X$ heißt **Fixpunkt** falls $g \cdot x = x$ für alle $g \in G$. Die Menge aller Fixpunkte ist X^G geschrieben.

5. Für $x \in X$ heißt $G_x = \{g \in G \mid g \cdot x = x\}$ der **Stabilisator von x** .

6. Allgemeiner heißt für $Y \subset X$ eine Teilmenge $G_Y = \{g \in G \mid g \cdot Y = Y\}$ der **Stabilisator von Y** .

Bemerkung 1.8.5 Die Operation $G \times X \rightarrow X$ ist genau dann treu, wenn der Gruppenhomomorphismus $\Phi : G \rightarrow \text{Bij}(X)$ (siehe Lemma 1.8.3) injektiv ist.

Beispiel 1.8.6 1. Sei $G \times G \rightarrow G$ die Linkstranslation. Dann ist die Operation transitiv und treu. Daraus folgt

Satz 1.8.7 (Satz von Cayley) Sei G eine Gruppe der Ordnung n . Dann ist G eine Untergruppe von S_n . \square

Beweis. Sei $L : G \rightarrow \text{Bij}(G) \simeq S_n$ definiert durch $g \mapsto (L_g : G \rightarrow G, h \mapsto gh)$. Wir zeigen, dass L injektiv ist also dass die Operation treu ist. Sei $g \in \text{Ker} L$. Es gilt $L_g = \text{Id}_G$ also $L_g(h) = h$ für alle $h \in G$. Daraus folgt $gh = h$ und $g = e_G$. \blacksquare

2. Sei $G \times G/H \rightarrow G/H$ die Linkstranslation auf dem Quotient G/H . Dann ist die Operation transitiv und G_{e_G} der Stabilisator des neutrales Elements ist H .

3. Sei $G \times G \rightarrow G$ die Konjugation. Sei $h \in G$. Dann ist der Stabilisator von h der Zentralisator von h :

$$G_h = \{g \in G \mid ghg^{-1} = h\} = \{g \in G \mid gh = hg\} = Z_G(h).$$

4. Sei $X = \{H \subset G \mid H \text{ ist eine Untergruppe}\}$. Dann ist $G \times X \rightarrow X$ definiert durch $g \cdot H = gHg^{-1}$ eine Operation. Es gilt

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

Es gilt auch

$$X^G = \{H \in X \mid gHg^{-1} = H \text{ für alle } g \in G\} = \{H \in X \mid H \triangleleft G\}.$$

Definition 1.8.8 Sei $G \times X \rightarrow X$ eine Operation. Wir definieren auf X die Relation $x \sim y \Leftrightarrow y \in G \cdot x$.

Proposition 1.8.9 Sei $G \times X \rightarrow X$ eine Operation.

1. Die Relation $x \sim y$ ist eine Äquivalenzrelation.
2. Die Äquivalenzklassen sind die Bahnen.
3. Sei $x \in X$. Die Abbildung $G/G_x \rightarrow G \cdot x$ definiert durch $[g] \mapsto g \cdot x$ ist wohl definiert und bijektiv.

Beweis. 1. Es gilt $x = e_G \cdot x$ also $x \sim x$ und \sim ist reflexiv.

Seien $x, y \in X$ mit $x \sim y$. Dann gilt $y \in G \cdot x$ also gibt es ein $g \in G$ mit $y = g \cdot x$. Dann gilt $x = g^{-1} \cdot y$ und $x \in G \cdot y$ also $y \sim x$ und \sim ist symmetrisch.

Seien $x, y, z \in X$ mit $x \sim y$ und $y \sim z$. Dann gibt es $g, g' \in G$ mit $y = g \cdot x$ und $z = g' \cdot y$. Daraus folgt $z = g'g \cdot x$ und $x \sim z$ also \sim ist transitiv.

2. Sei $x \in X$. Die Äquivalenzklasse von x ist $\{y \in X \mid x \sim y\} = \{y \in X \mid y \in G \cdot x\} = G \cdot x$.

3. Seien $g, g' \in G$ mit $[g] = [g']$. Dann gibt es ein $h \in G_x$ mit $g' = gh$. Daraus folgt $g' \cdot x = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot x$ und die Abbildung ist wohl definiert. Per Definition einer Bahn ist diese Abbildung surjektiv. Seien $g, g' \in G$ mit $g \cdot x = g' \cdot x$. Dann gilt $x = (g^{-1}g') \cdot x$ und $g^{-1}g' = h \in G_x$. Daraus folgt $g' = gh$ und $[g] = [g']$. Die Abbildung ist injektiv. ■

Korollar 1.8.10 (Bahnformel) Sei $G \times X \rightarrow X$ eine Operation mit G endlich. Es gilt

$$|G \cdot x| = [G : G_x] = \frac{|G|}{|G_x|}.$$

Beweis. Nach 3. im obigen Proposition gilt $|G/G_x| = |G \cdot x|$. Nach dem Satz von Lagrange gilt $|G/G_x| = [G : G_x] = |G|/|G_x|$. ■

Satz 1.8.11 (Bahngleichung) Sei $G \times X \rightarrow X$ eine Operation mit X endlich. Dann gilt

$$|X| = \sum_{[x] \in X/G} |G \cdot x| = \sum_{[x] \in X/G} [G : G_x].$$

Beweis. Da die Bahnen die Äquivalenzklassen einer Äquivalenzrelation sind gilt

$$X = \coprod_{[x] \in X/G} G \cdot x.$$

Daraus folgt die Behauptung. ■

Korollar 1.8.12 Sei G eine endliche Gruppe und H eine Untergruppe. Der kleinste Primteiler von $|H|$ sei größer gleich $[G : H]$. Dann ist $H \triangleleft G$

Beweis. Sei p der kleinste Primteiler von $|H|$ und sei $X = G/H$. Sei $H \times X \rightarrow X$ die Linksoperation: $h \cdot gH = hgH$. Sei $x \in X$. Nach der Bahnformel ist $|H \cdot x|$ ein Teiler von $|H|$ also $|H \cdot x| = 1$ oder $|H \cdot x| \geq p$. Nach der Bahngleichung gilt

$$p \geq [G : H] = |X| = \sum_{[x] \in X/H} |G \cdot x|.$$

Sei $x = [e_G] \in X$. Dann ist x ein Fixpunkt $|H \cdot x| = |\{x\}| = 1$. Daraus folgt

$$p - 1 \geq \sum_{[x] \in X/H, x \neq [e_G]} |G \cdot x|.$$

Da $|G \cdot x| = 1$ oder $|G \cdot x| \geq p$ muss $|G \cdot x| = 1$ für alle $x \in X$ gelten. Also für alle $[g] \in G/H$ gilt $[hg] = [g]$ für alle $h \in G$ i.e. $g^{-1}hg \in H$ für alle $g \in G$ und $h \in H$ i.e. $H \triangleleft G$. ■

Beispiel 1.8.13 1. Wenn $[G : H]$ der kleinste Primteiler von $|G|$ ist, ist die Bedingung erfüllt.

2. Insbesondere wenn $[G : H] = 2$ ist die Bedingung erfüllt und $H \triangleleft G$.

Definition 1.8.14 Sei p eine Primzahl. Eine endliche Gruppe G heißt **p -Gruppe** falls $|G| = p^k$ eine Potenz von p ist.

Korollar 1.8.15 Sei G eine p -Gruppe. Dann gilt $|Z(G)| > 1$.

Beweis. Sei $|G| = p^k$. Sei $X = G$ und $G \times X \rightarrow X$ die Konjugation. Es gilt $X^G = Z(G)$: sei $z \in Z(G)$. Dann gilt $g \cdot z = gzg^{-1} = z$. Umgekehrt, sei $z \in X^G$. Dann gilt $g \cdot z = z$ für alle $g \in G$ also $gzg^{-1} = z$ für alle $g \in G$ i.e. $gz = zg$ für alle $g \in G$. Insbesondere gilt

$$z \in Z(G) \Leftrightarrow |G \cdot x| = 1.$$

Nach der Bahnformel folgt

$$z \in Z(G) \Leftrightarrow p \nmid |G \cdot x|.$$

Nach der Bahngleichung gilt

$$p^k = |X| = \sum_{[x] \in X/H} |G \cdot x| = \sum_{[x] \in X/G, x \in Z(G)} |G \cdot x| + \sum_{[x] \in X/G, x \notin Z(G)} |G \cdot x|$$

also $p^k = |Z(G)| + \sum_{[x] \in X/G, x \notin Z(G)} |G \cdot x|$. Alle Terme in der Zweite Summe sind durch p teilbar also muss $|Z(G)|$ durch p teilbar sein. Daraus folgt $|Z(G)| > 1$. ■

Satz 1.8.16 Sei p eine Primzahl und sei G eine Gruppe der Ordnung p^2 . Dann gilt $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ oder $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. □

Beweis. Fall 1: Es gebe $g \in G$ mit $\text{ord}(g) = p^2$. Dann gilt $\mathbb{Z}/p^2\mathbb{Z} \simeq \langle g \rangle = G$.

Fall 2: Für alle $g \in G$ mit $g \neq e_G$ gilt $\text{ord}(g) = p$. Sei $g \in G \setminus \{e_G\}$. Dann gilt $|\langle g \rangle| = p$ also es gibt $h \in G \setminus \langle g \rangle$. Sei $N = \langle g \rangle$ und $H = \langle h \rangle$. Dann $p = |N| = |H|$ der kleinste Primteiler von $|N|$ und $|H|$ ist und $p \geq p = [G : N] = [G : H]$ gilt nach Korollar 1.8.12: $N \triangleleft G$ und $H \triangleleft G$. Der Durchschnitt $H \cap N$ ist eine echte Untergruppe von H da $h \in H \setminus N$. Also gilt $|H \cap N| < p$ und $|H \cap N| < p$. Daraus folgt $|N \cap H| = 1$ und $N \cap H = \{e_G\}$. Da N und H normal sind gilt $\langle N, H \rangle = NH = HN$. Dies ist eine Untergruppe von G die $N \cup \{h\}$ enthält also $|NH| \geq p + 1$ und $|NH|$ teilt p^2 . Daraus folgt $|NH| = p^2$ und $NH = G$. Nach dem Satz 1.7.5 folgt $G \simeq N \times H$ also $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. ■

Bemerkung 1.8.17 Für Gruppen G der Ordnung $|G| = p^3$ ist die Klassifikation schon schwieriger: siehe Übungsblatt 3 für den Fall $|G| = 8 = 2^3$. Die Gruppen der Ordnung 8 sind isomorph zu

$$\mathbb{Z}/8\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad D_8, \quad \mathbb{H}.$$

1.9 Symmetrische Gruppe

Definition 1.9.1 1. Ein Element $\sigma \in S_n$ heißt **r -Zykel** falls es paarweise verschiedene Elemente $x_1, \dots, x_r \in [1, n]$ mit

$$\begin{aligned}\sigma(x_k) &= x_{k+1} \text{ für alle } k \in [1, r-1], \\ \sigma(x_r) &= x_1 \text{ und} \\ \sigma(x) &= x \text{ für alle } x \in [1, n] \setminus \{x_1, \dots, x_r\}.\end{aligned}$$

2. Die Menge $\text{Supp}(\sigma) = \{x_1, \dots, x_r\}$ heißt **Träger des Zyklus**. Die Zahl r ist die **Länge des Zyklus**. Wir schreiben $[x_1, \dots, x_r]$ für den Zykel der Länge r mit Träger $\{x_1, \dots, x_r\}$.

3. Zwei Zykel σ, σ' heißen **fremd** falls $\text{Supp}(\sigma) \cap \text{Supp}(\sigma') = \emptyset$.

Bemerkung 1.9.2 Eine Transposition ist ein 2-Zykel.

Satz 1.9.3 1. Fremde Zykeln kommutieren.

2. Jedes $\gamma \in S_n$ ist ein Produkt fremder Zykeln. Diese sind eindeutig bis auf Reihenfolge. \square

Beweis. 1. Seien σ, σ' fremde Zykeln und sei $x \in [1, n]$. Es gilt

$$\sigma(\sigma'(x)) = \begin{cases} x & \text{für } x \notin \text{Supp}(\sigma) \cup \text{Supp}(\sigma') \\ \sigma(x) & \text{für } x \in \text{Supp}(\sigma) \setminus \text{Supp}(\sigma') \\ \sigma'(x) & \text{für } x \notin \text{Supp}(\sigma') \setminus \text{Supp}(\sigma) \end{cases} = \sigma'(\sigma(x)).$$

2. Sei $H = \langle \gamma \rangle$ die von γ erzeugte Untergruppe. Wir lassen H operieren auf $[1, n]$ durch $\gamma^n \cdot x = \gamma^n(x)$. Seien B eine Bahn, sei $r = |B|$ und sei $x_1 \in B$. Es gilt

$$B = \{x_1, x_2 = \gamma(x_1), \dots, x_r = \gamma^{r-1}(x_1)\}.$$

Sei $\sigma_B = [x_1, \dots, x_r]$. Es gilt

$$\gamma = \prod_{B \in [1, n]/H} \sigma_B.$$

Umgekehrt zerlegt jede Faktorisierung $\gamma = \prod_k \sigma_k$ die Menge X in Bahnen gegeben durch die Träger von σ_k . Diese Bahnen und also die Zerlegung ist bis auf Reihenfolge eindeutig bestimmt. \blacksquare

Beispiel 1.9.4 Sei $\gamma = (36451872) \in S_8$. Die Bahnen von γ sind $\{1, 2, 4, 5\}$, $\{2, 6, 8\}$ und $\{7\}$. Es gilt also

$$\gamma = [1345][268][7] = [1345][268].$$

Korollar 1.9.5 Sei $\gamma = \sigma_1 \cdots \sigma_k$ die Zerlegung von γ als Produkt fremder Zyklen und sei $r_i = \text{ord}(\sigma_i)$. Dann gilt $\text{ord}(\gamma) = \text{kgV}(r_1, \dots, r_k)$.

Beweis. Sei $d = \text{kgV}(r_1, \dots, r_k)$. Es gilt $\gamma^d = \sigma_1^d \cdots \sigma_k^d = \text{Id}$ also $\text{ord}(\gamma) | d$. Umgekehrt für a mit $\gamma^a = \text{Id}$ gilt $\text{Id} = \gamma^a = \sigma_1^a \cdots \sigma_k^a$ und da die Träger disjunkt sind gilt $\sigma_i^a = \text{Id}$ für alle $i \in [1, k]$ also $r_i | a$. Daraus folgt $\text{kgV}(r_1, \dots, r_k) | a$. ■

Lemma 1.9.6 (Konjugationsprinzip) Sei $\sigma = [x_1, \dots, x_r]$ ein r -Zykel und sei $\gamma \in S_n$. Dann gilt

$$\gamma \sigma \gamma^{-1} = [\gamma(x_1), \dots, \gamma(x_r)].$$

Beweis. Siehe Übungsblatt 4. ■

Korollar 1.9.7 Sei $n \geq 0$. Es gilt $S_n = \langle [1, 2], [1, 2, \dots, n] \rangle$.

Beweis. Sei $H = \langle [1, 2], [1, 2, \dots, n] \rangle$. Sei $\sigma = [1, 2, \dots, n]$. Es gilt $H \ni \sigma^k [1, 2] \sigma^{-k} = [\sigma^k(1), \sigma^k(2)] = [k+1, k+2]$. Da die einfachen Transpositionen $[i, i+1]$ die Gruppe S_n erzeugen, gilt $H = S_n$. ■

Definition 1.9.8 Sei $k \geq 0$. Eine Operation $G \times X \rightarrow X$ heißt **k -transitiv** falls für $x_1, \dots, x_k \in X$ paarweise verschiedene Elemente und $y_1, \dots, y_k \in X$ paarweise verschiedene Elemente es ein $g \in G$ gibt mit

$$g \cdot x_i = y_i \text{ für alle } i \in [1, k].$$

Beispiel 1.9.9 Sei $S_n \times [1, n] \rightarrow [1, n]$ die Operation $\gamma \cdot x = \gamma(x)$. Dann ist diese Operation n -transitiv.

Lemma 1.9.10 Sei $A_n \times [1, n] \rightarrow [1, n]$ die Operation gegeben durch $\gamma \cdot x = \gamma(x)$. Dann ist diese Operation $(n-2)$ -transitiv. □

Beweis. Seien $x_1, \dots, x_{n-2} \in [1, n]$ paarweise verschieden und $y_1, \dots, y_{n-2} \in [1, n]$ paarweise verschieden. Seien $x_{n-1}, x_n, y_{n-1}, y_n$ so, dass

$$\{x_1, \dots, x_n\} = [1, n] = \{y_1, \dots, y_n\}.$$

Da S_n n -transitiv operiert gibt es $\gamma \in S_n$ mit $\gamma(x_i) = y_i$ für alle $i \in [1, n]$. Fall $\gamma \in A_n$ sind wir fertig. Sonst, sei $\gamma' = \gamma \circ [x_{n-1}, x_n]$. Dann gilt $\gamma' \in A_n$ und $\gamma'(x_i) = y_i$ für alle $i \in [1, n-2]$.

ment es ein $g \in G$ gibt mit

$$g \cdot x_i = y_i \text{ für alle } i \in [1, k].$$

Satz 1.9.11 1. In S_n sind alle r -Zykel konjugiert.

2. Für $n \geq 5$ sind alle 3-Zykel konjugiert in A_n .

3. Jedes Element in A_n ist ein Produkt gerader Anzahl von Transpositionen.

4. Ein r -Zyklus ist genau dann in A_n , wenn r ungerade ist.

5. Die Menge aller 3-Zykel erzeugt A_n . □

Beweis. 1. Seien $\sigma = [x_1, \dots, x_r]$ und $\sigma' = [y_1, \dots, y_r]$ zwei r -Zykel. Da S_n n -transitiv operiert, gibt es $\gamma \in S_n$ mit $\gamma(x_i) = y_i$ für alle $i \in [1, r]$. Daraus folgt $\gamma\sigma\gamma^{-1} = \sigma'$.

2. Sei $\sigma = [x_1, x_2, x_3]$ und $\sigma' = [y_1, y_2, y_3]$. Da $n \geq 5$ gilt $n - 2 \geq 3$. Da A_n $n - 2$ -transitiv operiert gibt es $\gamma \in A_n$ mit $\gamma(x_i) = y_i$ für alle $i \in [1, 3]$. Daraus folgt $\gamma\sigma\gamma^{-1} = \sigma'$.

3. Jede Permutation ist ein Produkt von Transpositionen und per Definition von A_n sind Element in A_n Produkt gerader Anzahl von Transpositionen.

4. Sei $\sigma = [x_1, \dots, x_r]$. Es gilt $\sigma = [x_1, x_2][x_2, x_3] \cdots [x_{r-1}, x_r]$ also ist σ ein Produkt von $r - 1$ Transpositionen und es gilt $\varepsilon(\sigma) = (-1)^r$.

4. Sei $[x_1, x_2][x_3, x_4]$ oder $[x_1, x_2][x_2, x_3]$ ein Produkt von 2 Transpositionen mit x_1, x_2, x_3, x_4 paarweise verschieden. Es gilt

$$[x_1, x_2][x_3, x_4] = [x_1, x_3, x_2][x_1, x_3, x_4] \text{ und } [x_1, x_2][x_2, x_3] = [x_1, x_2, x_3]$$

und daraus folgt, dass alle Element in A_n Produkte von 3-Zykel sind. ■

Korollar 1.9.12 Sei $n \geq 2$.

1. Es gilt $D(S_n) = A_n$.

2. Es gilt

$$D(A_n) = \begin{cases} \{\text{Id}\} & \text{für } n = 2, 3 \\ V_4 & \text{für } n = 4 \\ A_n & \text{für } n \geq 5 \end{cases}$$

wobei $V_4 = \{\text{Id}, [12][34], [13][24], [14][23]\}$.

Beweis. 1. Da $S_n/A_n \simeq \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$ abelsch ist, gilt $D(S_n) \subset A_n$ (Lemma 1.6.2). Für $n = 2$ gilt $A_n = \{\text{Id}\}$ also $A_n \subset D(S_n)$. Für $n \geq 3$ gilt

$$[a, b, c] = [b, c][a, b][b, c][a, b] = [b, c][a, b][b, c]^{-1}[a, b]^{-1} = [[b, c], [a, b]] \in D(S_n).$$

Da A_n von den 3-Zykeln erzeugt ist, gilt $A_n \subset D(S_n)$.

2. Für $n = 2, 3$ ist A_n abelsch also gilt $D(A_n) = \{\text{Id}\}$. Für $n = 4$ gilt $V_4 \triangleleft A_4$ (Siehe Übungsblatt 3) und $A_4/V_4 \simeq \mathbb{Z}/3\mathbb{Z}$ ist abelsch. Nach Lemma 1.6.2 gilt $D(A_4) \subset V_4$. Umgekehrt gilt für $a, b, c, d \in [1, 4]$ paarweise verschieden:

$$\begin{aligned} [a, b][c, d] &= [a, b, c][a, b, d][a, c, b][a, d, b] \\ &= [a, b, c][a, b, d][a, b, c]^{-1}[a, b, d]^{-1} = [[a, b, c], [a, b, d]] \in D(A_4). \end{aligned}$$

Daraus folgt $V_4 \subset D(A_4)$.

Sei $n \geq 5$, seien $a, b, c \in [1, n]$ paarweise verschieden und seien $x, y \in [1, n] \setminus \{a, b, c\}$. Es gilt

$$\begin{aligned} [a, b, c] &= [a, b, x][a, c, y][a, x, b][a, y, c] \\ &= [a, b, x][a, c, y][a, b, x]^{-1}[a, c, y]^{-1} = [[a, b, x], [a, c, y]] \in D(A_n). \end{aligned}$$

Es folgt $A_n \subset D(A_n)$ und da $D(A_n) \subset A_n$ ist die Behauptung bewiesen. ■

Man kann eigentlich das folgende Resultat zeigen (Siehe Übungsblatt 4 für den Fall $n = 5$).

Theorem 1.9.13 Die Gruppe A_n ist einfach für $n \geq 5$. □

1.10 Sylow Sätze

Definition 1.10.1 Sei G eine Gruppe und sei p ein Primteiler von $|G|$ so, dass

$$|G| = p^\alpha m \text{ wobei } p \nmid m.$$

Eine Untergruppe von G der Ordnung p^α heißt **p -Sylowuntergruppe**.

Bemerkung 1.10.2 Sei G eine Gruppe und p eine Primzahl. Eine Untergruppe H ist genau dann eine Untergruppe, wenn H eine p -Gruppe ist und $[G : H]$ und p teilerfremd sind.

Beispiel 1.10.3 Sei p eine Primzahl, sei $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ und sei $G = \text{GL}_n(\mathbb{F}_p)$. Es gilt

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

Um es zu zeigen, zählen wir die Basen von \mathbb{F}_p^n ab. In \mathbb{F}_p^n gibt es p^n Elemente. Eine Basis ist der Form (v_1, \dots, v_n) . Der erste Basisvektor v_1 kann beliebig in $\mathbb{F}_p^n \setminus \{0\}$ gewählt werden also $p^n - 1$ Möglichkeiten. Der zweite Basisvektor v_2 kann beliebig in $\mathbb{F}_p^n \setminus \langle v_1 \rangle$ gewählt werden also $p^n - p$ Möglichkeiten. Nach Induktion kann v_{k+1} beliebig in $\mathbb{F}_p^n \setminus \langle v_1, \dots, v_k \rangle$ gewählt werden also $p^n - p^k$ Möglichkeiten.

Sei H die Untergruppe von G , welche von oberen Dreiecksmatrizen mit 1 auf der Diagonal besteht. Dann gilt

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

und H ist eine Sylowuntergruppe von G .

Lemma 1.10.4 Sei G eine Gruppe mit $|G| = n = p^\alpha m$ mit $p \nmid m$. Sei H eine Untergruppe von G und sei S eine p -Sylowuntergruppe von G . Dann gibt es ein $g \in G$ so, dass $gSg^{-1} \cap H$ eine p -Sylowuntergruppe von H ist. Insbesondere hat H auch eine p -Sylowuntergruppe. \square

Beweis. Sei $X = G/S$. Sei $G \times X \rightarrow X$ die Linkstranslation auf dem Quotient $X = G/S$ definiert durch $g \cdot [g'] = [gg']$. Der Stabilisator von $[g] = gS$ ist gSg^{-1} (Siehe Übungsblatt 4).

Per Einschränkung operiert H auf X durch $H \times X \rightarrow X$ mit $h \cdot [g'] = [hg']$. Der Stabilisator $H_{[g]}$ von $[g] = gS$ ist $gSg^{-1} \cap H$ (Siehe Übungsblatt 4).

Die Gruppen $gSg^{-1} \cap H$ sind p -Gruppen, da $|gSg^{-1} \cap H|$ die Ordnung $|S| = p^\alpha$ teilt. Wir zeigen, dass es ein g gibt so, dass $|H/(gSg^{-1} \cap H)| = [H : gSg^{-1} \cap H]$ und p teilerfremd sind.

Falls es nicht der Fall ist gilt nach der Bahnformel $|H \cdot [g]| = |H|/|H_{[g]}| = |H/(gSg^{-1} \cap H)| = [H : gSg^{-1} \cap H]$ und teilt p die Zahl $|H \cdot x|$ für alle $x = [g] \in X$. Nach der Bahngleichung

$$m = |G/S| = |X| = \sum_{[x] \in X/H} |H \cdot x|$$

würde m durch p teilbar sein. Ein Widerspruch. \blacksquare

Satz 1.10.5 (Erster Sylowsatz) Sei G eine Gruppe und p ein Primteiler von $|G|$. Dann hat G mindestens eine p -Sylowuntergruppe. \square

Beweis. Sei G eine Gruppe und p ein Primteiler von $n = |G|$. Nach dem Satz von Cayley ist G isomorph zu einer Untergruppe von S_n . Die Gruppe S_n ist aber eine Untergruppe von $\text{GL}_n(K)$ für jeden Körper K dank der Abbildung

$$\sigma \mapsto P_\sigma$$

wobei P_σ die Permutationsmatrix ist: $P_\sigma = (a_{i,j})_{i,j \in [1,n]}$ mit $a_{i,j} = \delta_{\sigma(i),j}$. Also für $K = \mathbb{F}_p$ ist G eine Untergruppe von $\text{GL}_n(\mathbb{F}_p)$. Da $\text{GL}_n(\mathbb{F}_p)$ eine p -Sylowuntergruppe hat, hat G auch eine p -Sylowuntergruppe nach dem obigen Lemma. \blacksquare

Korollar 1.10.6 (Satz von Cauchy) Sei G eine Gruppe und p ein Primteiler von p . Dann gibt es ein Element der Ordnung p .

Beweis. Sei $|G| = p^\alpha m$ mit $p \nmid m$ und sei S eine p -Sylowuntergruppe von G . Sei $g \in S \setminus \{e_G\}$. Dann gilt $\text{ord}(g) \neq 0$ und $\text{ord}(g) | p^\alpha$ also $\text{ord}(g) = p^k$ für $k \geq 1$. Dann gilt $\text{ord}(g^{p^{k-1}}) = \frac{p^k}{\text{ggT}(p^k, p^{k-1})} = \frac{p^k}{p^{k-1}} = p$. \blacksquare

Korollar 1.10.7 Eine Gruppe G ist genau dann eine p -Gruppe, wenn $\text{ord}(g)$ eine Potenz von p ist für jedes $g \in G$.

Beweis. Sei G eine p -Gruppe. Nach dem Satz von Lagrange ist die Ordnung jedes Element einen Teiler von $|G|$ also eine Potenz von p .

Umgekehrt, sei G eine Gruppe die keine p -Gruppe ist. Dann gibt es einen Primteiler q von $|G|$ mit $p \neq q$ und G hat ein Element der Ordnung q . ■

Korollar 1.10.8 Sei p eine Primzahl und G eine Untergruppe von S_p so, dass p ein Teiler von $|G|$ ist und G eine Transposition enthält. Dann gilt $G = S_p$.

Beweis. Es gilt $|S_p| = p! = pm$ mit $p \nmid m$. Da p die Ordnung $|G|$ teilt gilt $|G| = pm'$ mit $p \nmid m'$. Sei $\sigma \in G$ der Ordnung p . Wir zeigen, dass σ ein p -Zykel ist. Sei $\sigma = c_1 \cdots c_k$ die Zerlegung von σ in Produkt von r -Zykeln mit disjunkten Träger. Es gilt $\text{ord}(\sigma) = \text{kgV}(\text{ord}(c_1), \dots, \text{ord}(c_k))$ nach Korollar 1.9.5. Insbesondere muss p die Ordnung $\text{ord}(c_i)$ für ein i teilen. Für so ein i gilt $\text{ord}(c_i) = p$ und c_i ist ein p -Zykel. Also enthält G eine Transposition τ und ein p -Zykel σ' .

Sei $\tau = [a, b]$. Es gibt ein $\gamma \in S_n$ so, dass $\gamma\tau\gamma^{-1} = [1, 2]$ (wähle γ mit $\gamma(a) = 1$ und $\gamma(b) = 2$). Es genügt zu zeigen, dass $G' = \gamma G \gamma^{-1} = S_n$ und es gilt $\gamma G \gamma^{-1} \ni [1, 2], \sigma = \gamma\sigma'\gamma^{-1}$ wobei σ ein p -Zykel ist. Da σ ein p -Zykel ist gibt es ein k mit $\sigma^k(1) = 2$. Außerdem gilt $\sigma^k \in \langle \sigma \rangle \setminus \{\text{Id}\}$ also $1 < \text{ord}(\sigma^k) | \text{ord}(\sigma) = p$. Es gilt also $\text{ord}(\sigma^k) = p$ und $\sigma^k = [1, 2, x_3, \dots, x_p]$. Sei $\delta \in S_n$ mit $\delta(1) = 1$, $\delta(2) = 2$ und $\delta(x_i) = i$ für alle $i \geq 3$. Dann gilt $\delta[1, 2]\delta^{-1} = [1, 2]$ und $\delta\sigma^k\delta^{-1} = [1, 2, \dots, p]$. Die Gruppe $G'' = \delta G' \delta^{-1}$ enthält $[1, 2]$ und $[1, 2, \dots, p]$ also nach Korollar 1.9.7 gilt $G'' = S_p$. Daraus folgt $G' = S_p$ und $G = S_p$. ■

Korollar 1.10.9 Seien p und q Primzahlen und G eine Gruppe der Ordnung $|G| = p^k q^l$ mit $k, l \geq 1$ so, dass $q > p^k$. Dann gilt $G \simeq K_q \rtimes K_p$ wobei K_p und K_q beliebige p - und q -Sylowuntergruppen sind.

Beweis. Nach Korollar 1.8.12 gilt $K_q \triangleleft G$. Sei $H = K_p \cap K_q$. Dann ist $|H|$ ein Teiler von $p^k = |K_p|$ und $q^l = |K_q|$ also $|H| = 1$ und $K_q \cap K_p = \{e_G\}$. Daraus folgt, dass die Abbildung $K_q \times K_p \rightarrow G$, $(a, b) \mapsto ab$ injektiv ist. Da $|K_p \times K_q| = p^k q^l = |G|$, folgt, dass diese Abbildung eine Bijektion ist also $G = K_q K_p$. Nach dem Satz 1.7.5 folgt $G \simeq K_q \rtimes K_p$. ■

Satz 1.10.10 (Zweiter Sylowsatz) Sei p eine Primzahl und G eine Gruppe der Ordnung $|G| = p^\alpha m$ mit $p \nmid m$.

1. Sei H eine Untergruppe von G die eine p -Gruppe ist. Dann gibt es S eine p -Sylowuntergruppe von G mit $H \subset S$.

Sei k die Anzahl aller p -Sylowuntergruppen

2. Alle p -Sylowuntergruppe sind zueinander konjugiert.

3. Es gilt $k \mid |G|$.

4. Es gilt $k \equiv 1 \pmod{p}$ (also k teilt m). □

Korollar 1.10.11 (Vom Satz 1.10.10.2) Sei G eine Gruppe und S eine p -Sylowuntergruppe. Dann gilt

$$S \triangleleft G \Leftrightarrow S \text{ ist die einzige } p\text{-Sylowuntergruppe von } G \Leftrightarrow k = 1.$$

Beweis. Die letzte Äquivalenz ist klar da k die Anzahl von p -Sylowuntergruppen ist.

(\Rightarrow). Sei S eine p -Sylowuntergruppe mit $S \triangleleft G$. Sei T eine weitere p -Sylowuntergruppe. Nach Satz 1.10.10.2 gibt es ein $g \in G$ mit $gSg^{-1} = T$. Da aber $S \triangleleft G$, folgt $S = gSg^{-1} = T$.

(\Leftarrow). Sei S eine p -Sylowuntergruppe und sei $g \in G$. Dann ist gSg^{-1} auch eine p -Sylowuntergruppe. Daraus folgt nach Annahme, dass $gSg^{-1} = S$ und $S \triangleleft G$. ■

Beispiel 1.10.12 Sei G eine Gruppe der Ordnung 255. Dann ist G nicht einfach. Tatsächlich gilt $255 = 3 \times 5 \times 17$. Sei $p = 17$. Es gilt $|G| = p^\alpha m$ mit $\alpha = 1$ und $m = 3 \times 5 = 15$. Sei k die Anzahl von p -Sylowuntergruppen. Es gilt $k \equiv 1 \pmod{p}$ und $k|m$. Die Teiler von 15 sind 1, 3, 5 und 15. Da $3, 5, 15 \not\equiv 1 \pmod{p}$ gilt $k = 1$. Also ist K_{17} die einzige 17-Sylowuntergruppe und also ein Normalteiler. Es folgt, dass G nicht einfach ist.

Beweis vom Satz 1.10.10. Wir zeigen 1. und 2. Sei H eine Untergruppe von G die eine p -Gruppe ist und sei S eine p -Sylowuntergruppe. Nach Lemma 1.10.4 gibt es ein $g \in G$ so, dass $gSg^{-1} \cap H$ eine p -Sylowuntergruppe von H ist. Da H eine p -Gruppe ist, ist eine p -Sylowuntergruppe die ganze Gruppe also $gSg^{-1} \cap H = H$ i.e. $H \subset gSg^{-1}$. Die Untergruppe gSg^{-1} hat Ordnung $|S| = p^\alpha$ und ist also eine p -Sylowuntergruppe. Daraus folgt 1.

Falls H eine p -Sylowuntergruppe ist gilt $H \subset gSg^{-1}$ und $|H| = p^\alpha = |gSg^{-1}|$ und es folgt $H = gSg^{-1}$. Dies zeigt 2.

3. Wir betrachten $X = \{p\text{-Sylowuntergruppen}\}$ und die Operation $G \times X \rightarrow X$ definiert durch $g \cdot S = gSg^{-1}$. Nach 2. ist diese Operation Transitiv also gilt $G \cdot S = X$. Nach der Bahnformel folgt, dass $k = |X| = |G \cdot S|$ ein Teiler von $|G|$ ist.

4. Sei S eine p -Sylowuntergruppe. Wir betrachten die Einschränkungen der obigen Operation auf S i.e. $S \times X \rightarrow X$ definiert durch $s \cdot T = sTs^{-1}$. Sei $S \cdot T$ eine Bahn dieser Operation. Nach der Bahnformel teilt $|S \cdot T|$ die Ordnung $|S|$ also gilt

$$|S \cdot T| = \begin{cases} 1 & \text{für } S \cdot T = \{T\} \text{ i.e. } T \text{ Fixpunkt oder} \\ pa & \text{für ein } a \in \mathbb{N}. \end{cases}$$

Sei also X^S die Fixpunkte. Es gilt nach der Bahngleichung:

$$|X| = \sum_{[x] \in X/S} |S \cdot x| = \sum_{x \in X^S} |S \cdot x| + \sum_{[x] \in X/S, x \notin X^S} |S \cdot x| = |X^S| + pb.$$

Also gilt $k = |X| \equiv |X^S| \pmod{p}$. Es genügt zu zeigen, dass $X^S = \{S\}$ also $|X^S| = 1$. Sei $T \in X^S$. Also ist T eine p -Sylowuntergruppe mit $sTs^{-1} = T$ für alle $s \in S$. Sei

$H = \langle S, T \rangle$. Dann sind S und T p -Sylowuntergruppe von H (beide sind schon p -Sylowuntergruppe von G). Außerdem gilt $T \subset N_H(T)$ und weil $sTs^{-1} = T$ für alle $s \in S$ gilt auch $S \subset N_H(T)$. Also gilt $H = \langle S, T \rangle \subset N_H(T)$. Daraus folgt $H = N_H(T)$ i.e. $T \triangleleft H$. Nach Korollar 1.10.11 hat H genau eine p -Sylowuntergruppe. Es folgt $S = T$. ■

Korollar 1.10.13 (Primärzerlegung abelscher Gruppen) Sei G eine endliche abelsche Gruppe. Dann ist für jeder Primteiler p von G die p -Sylowuntergruppe K_p von G eindeutig durch

$$K_p = \{g \in G \mid \text{ord}(g) \text{ ist Potenz von } p\}$$

gegeben und es gilt

$$G = \prod_{p \text{ Primteiler von } |G|} K_p.$$

Beweis. Sei K_p eine p -Sylowuntergruppe. Da G abelsch ist K_p ein Normalteiler also ist K_p die einzige p -Sylowuntergruppe. Da $|K_p|$ eine Potenz von p ist gilt $K_p \subset \{g \in G \mid \text{ord}(g) \text{ ist Potenz von } p\}$. Umgekehrt, sei $g \in G$ so, dass $\text{ord}(g)$ eine Potenz von p ist. Dann ist $\langle g \rangle$ eine p -Gruppe und also in einer p -Sylowuntergruppe enthalten. Es folgt $g \in K_p$ da K_p die einzige p -Sylowuntergruppe ist.

Seien p_1, \dots, p_k die Primteiler von $|G|$ und sei $f : \prod_{i=1}^k K_{p_i} \rightarrow G$ definiert durch $f(x_1, \dots, x_k) = x_1 \cdots x_k$. Da G kommutativ ist ist f ein Gruppenhomomorphismus. Sei $(x_1, \dots, x_k) \in \text{Ker } f$. Dann gilt $x_1 x_2 \cdots x_k = e_G$. Sei $\text{ord}(x_i) = p_i^{\alpha_i}$. Es folgt

$$e_G = (x_1 \cdots x_k)^{p_2^{\alpha_2} \cdots p_k^{\alpha_k}} = x_1^{p_2^{\alpha_2} \cdots p_k^{\alpha_k}}.$$

Da $\text{ggT}(p_1^{\alpha_1}, p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = 1$ gibt es $a, b \in \mathbb{Z}$ mit $ap_1^{\alpha_1} + bp_2^{\alpha_2} \cdots p_k^{\alpha_k} = 1$. Es folgt

$$x_1 = x_1^{ap_1^{\alpha_1} + bp_2^{\alpha_2} \cdots p_k^{\alpha_k}} = e_G.$$

Analog gilt $x_i = e_G$ für alle i und f ist injektiv. Sei

$$|G| = p_1^{\beta_1} \cdots p_k^{\beta_k}.$$

Es gilt $|K_{p_i}| = p_i^{\beta_i}$ und $|\prod_{i=1}^k K_{p_i}| = |G|$. Daraus folgt, dass f bijektiv ist also ein Isomorphismus. ■

Beispiel 1.10.14 Sei G eine abelsche Gruppe der Ordnung $|G| = p_1 \cdots p_k$. Dann gilt

$$G \simeq \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k\mathbb{Z}.$$

Man kann sogar zeigen:

Theorem 1.10.15 Sei G eine endliche abelsche Gruppe. Dann gibt es Zahlen $a_1, \dots, a_k \in \mathbb{N}$ mit

$$G \simeq \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_k\mathbb{Z}.$$

1.11 Auflösbare Gruppen

Definition 1.11.1 Sei G eine Gruppe. Die k -te **derivierte Untergruppe** $D^k(G)$ ist definiert per Induktion durch

$$D^0(G) = G, \quad D^1(G) = D(G) \text{ und } D^{k+1}(G) = D(D^k(G)).$$

Beispiel 1.11.2 1. Für $n \geq 5$ gilt $D^0(S_n) = S_n$, $D^1(S_n) = D(S_n) = A_n$, $D^2(S_n) = D(D(S_n)) = D(A_n) = A_n$ und per Induktion $D^k(S_n) = A_n$ für alle $k \geq 1$.

2. Für $n = 4$ gilt $D^0(S_4) = S_4$, $D^1(S_4) = A_4$, $D^2(S_4) = D(A_4) = V_4$, $D^3(S_4) = D(V_4) = \{\text{Id}\}$ und $D^k(S_4) = \{\text{Id}\}$ für alle $k \geq 3$.

Bemerkung 1.11.3 Sei G eine Gruppe. Es gilt

$$G = D^0(G) \triangleright D^1(G) \triangleright \cdots \triangleright D^k(G) \triangleright D^{k+1}(G) \triangleright \cdots$$

und $D^k(G)/D^{k+1}(G)$ ist abelsch.

Definition 1.11.4 Eine Gruppe G heißt **auflösbar** wenn es eine Folge von Untergruppen $(G_i)_{i \in [1, m]}$ gibt mit

- $G_0 = G$ und $G_m = \{e_G\}$,
- $G_{i+1} \triangleleft G_i$ und
- G_i/G_{i+1} ist abelsch.

Beispiel 1.11.5 1. Sei G abelsch, dann ist G auflösbar mit $G_1 = \{e_G\} \triangleleft G_1 = G$.

2. Die Gruppen S_n und A_n sind für $n \leq 4$ auflösbar mit den Folgen

$$\{\text{Id}\} = A_1 = S_1, \quad \{\text{Id}\} = A_2 \triangleleft S_2, \quad \{\text{Id}\} \triangleleft A_3 \triangleleft S_3 \quad \text{und} \quad \{\text{Id}\} \triangleleft V_4 \triangleleft A_4 \triangleleft S_4.$$

Satz 1.11.6 Eine Gruppe G ist genau dann auflösbar, wenn es ein m gibt mit $D^m(G) = \{e_G\}$. □

Beweis. (\Leftarrow). Sei $G_i = D^i(G)$. Dann ist G_i eine Folge von Untergruppen, die die Definition der Auflösbarkeit erfüllt.

(\Rightarrow). Sei $(G_i)_{i \in [1, m]}$ eine Folge von Untergruppen mit $G_0 = G$, $G_r = \{e_G\}$, $G_{i+1} \triangleleft G_i$ und G_i/G_{i+1} ist abelsch. Wir zeigen, dass $D^i(G) \subset G_i$ per Induktion nach i . Daraus folgt, dass $D^m(G) \subset G_m = \{e_G\}$ also $D^m(G) = \{e_G\}$.

Es gilt $D^0(G) = G = G_0$. Angenommen gilt $D^i(G) \subset G_i$. Da G_i/G_{i+1} abelsch ist gilt $D(G_i) \subset G_{i+1}$. Daraus folgt

$$D^{i+1}(G) = D(D^i(G)) \subset D(G_i) \subset G_{i+1}.$$

Korollar 1.11.7 Die Gruppen S_n und A_n sind für $n \geq 5$ nicht auflösbar.

Beweis. Es gilt $D^k(S_n) = D^k(A_n) = A_n$ für $k \geq 2$ und $n \geq 5$. ■

Satz 1.11.8 Sei $f : G \rightarrow G'$ ein Gruppenhomomorphismus und sei H eine Untergruppe von G .

1. Es gilt $f(D(H)) = D(f(H))$.
2. Es gilt $f(D^k(G)) \subset D^k(G')$ für alle k .
3. Falls f surjektiv ist, gilt $f(D^k(G)) = D^k(G')$ für alle k . □

Beweis. 1. Folgt aus $f([a, b]) = [f(a), f(b)]$.

2. Per Induktion nach k . Es gilt $f(D^0(G)) = f(G) \subset G' = D^0(G')$. Angenommen gilt $f(D^k(G)) \subset D^k(G')$. Dann gilt nach 1. $f(D^{k+1}(G)) = f(D(D^k(G))) = D(f(D^k(G))) \subset D(D^k(G')) = D^{k+1}(G')$.

3. Per Induktion nach k . Es gilt $f(D^0(G)) = f(G) = G' = D^0(G')$. Angenommen gilt $f(D^k(G)) = D^k(G')$. Dann gilt nach 1. $f(D^{k+1}(G)) = f(D(D^k(G))) = D(f(D^k(G))) = D(D^k(G')) = D^{k+1}(G')$. ■

Korollar 1.11.9 Sei G eine Gruppe, H eine Untergruppe und N ein Normalteiler.

1. Falls G auflösbar ist gilt H , N und G/N sind auflösbar.
2. Die Gruppe G ist genau dann auflösbar, wenn N und G/N auflösbar sind.

Beweis. 1. Sei m mit $D^m(G) = \{e_G\}$. Es gilt $D^m(H) \subset D^m(G)$ also ist H auflösbar. Das gleiche gilt für N . Nach dem obigen Satz mit $f : G \rightarrow G/N$ die kanonische Projektion gilt $f(D^m(G)) = D^m(G/N)$ also $D^m(G/N) = \{e_{G/N}\}$.

2. (\Rightarrow). Folgt aus 1.

(\Leftarrow). Seien m und r mit $D^m(N) = \{e_G\}$ und $D^r(G/N) = \{e_{G/N}\}$. Sei $f : G \rightarrow G/N$ die kanonische Projektion. Nach dem obigen Satz gilt $f(D^r(G)) = D^r(G/N) = \{e_{G/N}\}$. Also gilt $D^r(G) \subset \text{Ker } f = N$. Daraus folgt $D^{m+r}(G) = D^m(D^r(G)) \subset D^m(N) = \{e_G\}$. ■

Korollar 1.11.10 Seien G_1, \dots, G_r , H und N Gruppen.

1. Das Produkt $G_1 \times \dots \times G_r$ ist genau dann auflösbar, wenn G_i für alle $i \in [1, r]$ auflösbar ist.
2. Das semidirekte Produkt $N \rtimes H$ ist genau dann auflösbar, wenn N und H auflösbar sind.

Beweis. Siehe Übungsblatt 5. ■

Korollar 1.11.11 Jede p -Gruppe ist auflösbar.

Beweis. Siehe Übungsblatt 5. ■

Satz 1.11.12 Sei G endlich auflösbar. Jede Folge von Untergruppen $(G_i)_{i \in [1, r]}$ mit $G_0 = G$, $G_r = \{e_G\}$, $G_{i+1} \triangleleft G_i$ und G_i/G_{i+1} abelsch lässt sich verfeinern in einer Folge von Untergruppen $(G'_i)_{i \in [1, r]}$ mit

- $G'_0 = G$ und $G'_r = \{e_G\}$,
- $G'_{i+1} \triangleleft G'_i$ und
- $G'_i/G'_{i+1} \simeq \mathbb{Z}/p_i\mathbb{Z}$ für eine Primzahl p_i . □

Beweis. Sei $(G_i)_{i \in [1, r]}$ eine Folge die sich nicht verfeinern lässt aber mit ein k so, dass G_k/G_{k+1} nicht von Primzahlordnung. Sei p ein Primteiler von G_k/G_{k+1} und $x \in G_k/G_{k+1}$ ein Element der Ordnung p ist (Satz von Cauchy). Dann gilt $\{e\} \subsetneq \langle x \rangle \subsetneq G_k/G_{k+1}$. Da G_k/G_{k+1} abelsch ist gilt $\langle x \rangle \triangleleft G_k/G_{k+1}$. Sei $\pi : G_k \rightarrow G_k/G_{k+1}$ die kanonische Projektion und $H = \pi^{-1}(\langle x \rangle)$. Es gilt $G_{k+1} \subsetneq H \subsetneq G_k$ und $G_{k+1} \triangleleft H \triangleleft G_k$. Ein Widerspruch zur nicht Verfeinbarkeit. ■

Beispiel 1.11.13 Es gilt $S_4 \overset{\mathbb{Z}/2\mathbb{Z}}{\triangleright} A_4 \overset{\mathbb{Z}/3\mathbb{Z}}{\triangleright} V_4 \overset{\mathbb{Z}/2\mathbb{Z}}{\triangleright} \{\text{Id}, [12][34]\} \overset{\mathbb{Z}/2\mathbb{Z}}{\triangleright} \{\text{Id}\}$.

2 Ringe

2.1 Grundbegriffe

2.1.1 Definition

Definition 2.1.1 1. Ein **Ring** ist eine Menge R mit zwei Verknüpfungen $+: R \times R \rightarrow R$, $(a, b) \mapsto a + b$ und $\times: R \times R \rightarrow R$, $(a, b) \mapsto ab$ so, dass

- $(R, +)$ ist eine kommutative Gruppe mit 0_R als neutrales Element,
- $(ab)c = a(bc)$ für alle $a, b, c \in R$,
- $a(b + c) = ab + ac$ und $ba + ca = (b + c)a$ für alle $a, b, c \in R$,
- es gibt ein $1_R \in R$ mit $a \cdot 1_R = 1_R \cdot a = a$ für alle $a \in R$.

2. Falls \times kommutativ ist *i.e.* $ab = ba$ für alle $a, b \in R$ heißt R **kommutativer Ring**.

Bemerkung 2.1.2 Sei R ein Ring.

1. Falls $1_R = 0_R$ gilt $R = \{0_R\}$. In diesem Fall heißt R der **Nullring**.

2. Für alle $a, b \in R$ gilt

- $0_R \cdot a = a \cdot 0_R = 0_R$
- $(-a)(-b) = ab$

Beispiel 2.1.3 1. $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ und $(\mathbb{C}, +, \times)$ sind Ringe.

2. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ ist ein Ring.

3. Sei K ein Körper. $(M_n(K), +, \times)$ ist ein Ring, wobei $+$ bzw. \times Matrixaddition bzw. Matrixmultiplikation sind.

4. Für $x \in \mathbb{C}$, sei $x \mapsto \bar{x}$ die komplexe Konjugation. Die Menge der Quaternionen

$$\mathbf{H} = \left\{ \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} \in M_2(\mathbb{C}) \mid x, y \in \mathbb{C} \right\}$$

mit Matrixaddition und Matrixmultiplikation ist ein nicht kommutativer Ring.

Definition 2.1.4 Seien R und R' zwei Ringe. Das Produkt $R \times R'$ mit $(a, a') + (b, b') = (a+b, a'+b')$ und $(a, a')(b, b') = (ab, a'b')$ ist ein Ring und heißt **Produkttring** von R und R' .

Definition 2.1.5 Sei R ein Ring.

1. Ein Element $a \in R$ heißt **Einheit** oder **invertierbar** falls es ein $b \in R$ gibt mit $ab = ba = 1_R$. Mann schreibt R^\times für die Menge aller Einheiten:

$$R^\times = \{a \in R \mid a \text{ ist eine Einheit}\}.$$

2. Ein Element $a \in R$ heißt **Nullteiler** falls es ein $b \in R \setminus \{0_R\}$ gibt mit $ab = 0_R$ oder $ba = 0_R$.

Bemerkung 2.1.6 Sei R ein Ring.

1. Die Menge (R^\times, \times) ist eine Gruppe. Insbesondere ist für $a \in R^\times$ das Element $b \in R$ mit $ab = ba = 1_R$ ein Element in R^\times und ist eindeutig bestimmt. Wir schreiben $b = a^{-1}$.

2. Es gilt $R^\times \subset R \setminus \{\text{Nullteiler}\}$: sei $b \in R$ mit $ab = 0_R$ oder $ba = 0_R$. Es gilt $0_R = a^{-1}ab = b$ oder $0_R = baa^{-1} = b$.

Definition 2.1.7 Sei R ein Ring.

1. R heißt **Nullteilerfrei** falls $(a \in R \text{ Nullteiler} \Rightarrow a = 0)$.

2. R heißt **Integritätring** falls $R \neq \{0_R\}$, R kommutativ und Nullteilerfrei ist.

3. R heißt **Schiefkörper** falls $R^\times = R \setminus \{0_R\}$.

4. R heißt **Körper** falls R ein kommutativer Schiefkörper ist.

Beispiel 2.1.8 1. Der Ring \mathbb{Z} ist ein Integritätsring.

2. Der Ring $R = \mathbb{Z}/4\mathbb{Z}$ ist kein Integritätsring: Es gilt $[2] \neq 0_R$ aber $[2][2] = [4] = 0_R$.

3. Der Ring \mathbf{H} ist ein nicht kommutativer Schiefkörper.

Definition 2.1.9 Sei R ein Ring.

1. Der **Polynomring** zu R ist

$$R[X] = \left\{ \sum_{k=0}^{\infty} r_k X^k \mid r_k \neq 0 \text{ nur für endlich viele } k \right\}$$

mit

$$\left(\sum_{k=0}^{\infty} r_k X^k \right) + \left(\sum_{k=0}^{\infty} r'_k X^k \right) = \sum_{k=0}^{\infty} (r_k + r'_k) X^k$$

und

$$\left(\sum_{k=0}^{\infty} r_k X^k\right) \times \left(\sum_{k=0}^{\infty} r'_k X^k\right) = \sum_{k=0}^{\infty} \left(\sum_{a+b=k} r_a r'_b\right) X^k.$$

2. Per Induktion definiert man den **Polynomring mit n Unbekannten zu R** als

$$R[X_1, \dots, X_n] = (R[X_1, \dots, X_{n-1}])[X_n].$$

Bemerkung 2.1.10 Sei R ein Ring.

1. Sei P ein Polynom in $R[X]$. Dann definiert P eine polynomiale Abbildung $f_P : R \rightarrow R$ durch $f_P(r) = P(r)$.

2. Man sollte aber Polynome und polynomiale Abbildungen nicht verwechseln. Zum Beispiel für $R = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ sind die Polynome $P = 0$ und $Q = X + X^2$ verschieden aber die Abbildungen die sie definieren sind $f_P : \mathbb{F}_2 \rightarrow \mathbb{F}_2$ und $f_Q : \mathbb{F}_2 \rightarrow \mathbb{F}_2$ und es gilt $f_P(x) = 0 = f_Q(x)$ für alle $x \in \mathbb{F}_2$ also $f_P = f_Q$.

2.1.2 Ringhomomorphismus

Definition 2.1.11 Ein **Ringhomomorphismus** ist eine Abbildung $f : R \rightarrow R'$, wobei R und R' Ringe sind so, dass für alle $a, b \in R$ gilt

$$f(a + b) = f(a) + f(b), \quad f(ab) = f(a)f(b) \quad \text{und} \quad f(1_R) = 1_{R'}.$$

Lemma 2.1.12 Sei $f : R \rightarrow R'$ ein Ringhomomorphismus.

1. Dann gilt $f(R^\times) \subset R'^\times$.

2. Die induzierte Abbildung $f : R^\times \rightarrow R'^\times$ ist ein Gruppenhomomorphismus. □

Beweis. Übung. ■

2.1.3 Unterringe und Ideale

Definition 2.1.13 Sei R ein Ring.

1. Eine Untergruppe $R' \subset R$ heißt **Unterring** falls

- $1_R \in R'$ und
- $ab \in R'$ für alle $a, b \in R'$.

2. Eine Untergruppe $I \subset R$ heißt **Ideal** falls $ab, ba \in I$ für alle $a \in I$ und alle $b \in R$.

Lemma 2.1.14 Sei R ein Ring und I ein Ideal. Dann gilt

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

Beweis. Übung. ■

Beispiel 2.1.15 1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbf{H}$ sind Unterringe.

2. Sei R ein Ring. Die Menge $\{0_R\}$ ist ein Ideal und heißt **Nullideal**.

3. Sei R ein kommutativer Ring und $r \in R$. Dann ist $(r) = rR = \{ra \in R \mid a \in R\}$ ein Ideal.

4. Zum Beispiel ist $n\mathbb{Z} \subset \mathbb{Z}$ ein Ideal. Alle Ideale in \mathbb{Z} sind dieser Form (schon alle Untergruppen sind dieser Form!).

5. Sei K ein Körper und $R = K[X]$. Dann sind alle Ideale I in R der Form $I = (P)$ für ein $P \in K[X]$ (Siehe LAII Übungsblatt 8 Übung 1).

Lemma 2.1.16 Sei $f : R \rightarrow R'$ ein Ringhomomorphismus, seien $S \subset R$ und $S' \subset R'$ Unterringe und $I \subset R$ und $I' \subset R'$ Ideale.

1. Dann sind $f(S)$ und $f^{-1}(S')$ Unterringe von R' und R . Insbesondere ist $\text{im } f$ ein Unterring.

2. 1. Dann ist $f^{-1}(I')$ ein Ideal von R . Insbesondere ist $\text{Ker } f$ ein Ideal.

3. Falls f surjektiv ist, ist $f(I)$ ein Ideal in R' . □

Beweis. Bilder und Urbilder von Untergruppen sind Untergruppen.

1. Es gilt $1_R \in S$ also $1_{R'} = f(1_R) \in f(S)$. Seien $f(a), f(b) \in f(S)$ mit $a, b \in S$. Dann gilt $ab \in S$ und $f(a)f(b) = f(ab) \in f(S)$.

Es gilt $f(1_R) = 1_{R'} \in S'$ also $1_R \in f^{-1}(S')$. Seien $a, b \in f^{-1}(S')$ also $f(a), f(b) \in S'$. Dann gilt $f(ab) = f(a)f(b) \in S'$ also $ab \in f^{-1}(S')$.

2. Sei $a \in f^{-1}(I')$ und $b \in R$. Dann gilt $f(a) \in I'$ und $f(ab) = f(a)f(b) \in I'$ und $f(ba) = f(b)f(a) \in I'$.

3. Sei $f(a) \in f(I)$ mit $a \in I$ und sei $b' \in R'$. Da f surjektiv ist, gibt es ein $b \in R$ mit $f(b) = b'$. Es folgt $ab, ba \in I$ und $f(a)f(b) = f(ab) \in f(I)$ und $f(b)f(a) = f(ba) \in f(I)$. ■

2.1.4 Quotienten

Sei R ein Ring und I ein Ideal. Dann ist $(R/I, +)$ eine Gruppe und die kanonische Projektion $\pi : R \rightarrow R/I$ ist ein Gruppenhomomorphismus.

Lemma 2.1.17 Sei R ein Ring und I ein Ideal.

1. Dann ist die Verknüpfung $\times : R/I \times R/I \rightarrow R/I$, $([a], [b]) \mapsto [ab]$ wohl definiert.
2. $(R/I, +, \times)$ ist ein Ring und die kanonische Projektion $\pi : R \rightarrow R/I$ ist ein Ringhomomorphismus. \square

Beweis. 1. Seien $a', b' \in R$ mit $[a'] = [a]$ und $[b'] = [b]$. Es gibt $c, d \in I$ mit $a' = a + c$ und $b' = b + d$. Dann gilt $a'b' = ab + ad + cb + cd$ und da $ad, cb, cd \in I$ gilt $[a'b'] = [ab]$.

2. Übung. \blacksquare

Definition 2.1.18 Sei R ein Ring und I ein Ideal. Dann heißt R/I mit $[a] + [b] = [a + b]$ und $[a][b] = [ab]$ der **Quotientring**.

Bemerkung 2.1.19 Sei R ein Ring und I ein Ideal. Dann gilt $I = \text{Ker}\pi$, wobei $\pi : R \rightarrow R/I$ die kanonische Projektion. Also ist jeder Ideal der Kern eines Ringhomomorphismus.

Satz 2.1.20 Sei $f : R \rightarrow R'$ ein Ringhomomorphismus, sei I ein Ideal von R und sei $\pi : R \rightarrow R/I$ die kanonische Projektion.

1. Es gibt ein eindeutig bestimmter Ringhomomorphismus $\bar{f} : R/I \rightarrow R'$ so, dass das Diagramm

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ p \downarrow & \nearrow \bar{f} & \\ R/I & & \end{array}$$

kommutiert, genau dann wenn $I \subset \text{Ker}f$.

Angenommen $I \subset \text{Ker}f$ und sei \bar{f} wie in 1.

2. Die Abbildung \bar{f} ist genau dann injektiv, wenn $I = \text{Ker}f$.

3. Die Abbildung \bar{f} ist genau dann surjektiv, wenn f surjektiv ist. \square

Beweis. 1. Nach Satz 1.2.10.1 existiert ein eindeutig bestimmter Gruppenhomomorphismus \bar{f} wie oben genau dann, wenn $I \subset \text{Ker}f$. Wir zeigen, dass \bar{f} ein Ringhomomorphismus ist. Es gilt $\bar{f}([1_{R/I}]) = \bar{f}(\pi(1_R)) = f(1_R) = 1_{R'}$. Seien $a, b \in R$. Es gilt $\bar{f}([a][b]) = \bar{f}([ab]) = \bar{f}(\pi(ab)) = f(ab) = f(a)f(b) = \bar{f}([a])\bar{f}([b])$.

2. Folgt aus Satz 1.2.10.2.

3. Folgt aus Satz 1.2.10.3. \blacksquare

Korollar 2.1.21 Sei $f : R \rightarrow R'$ ein surjektiver Ringhomomorphismus. Dann gilt $R/\text{Ker } f \simeq R'$.

Beispiel 2.1.22 Es gilt $\mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C}$.

2.1.5 Erzeuger

Lemma 2.1.23 Sei R ein Ring. Sei $(R_a)_{a \in A}$ eine Familie von Unterringen und sei $(I_a)_{a \in A}$ eine Familie von Idealen. Seien I und J zwei Ideale.

1. Dann ist $\bigcap_{a \in A} R_a$ ein Unterring
2. Dann sind $\bigcap_{a \in A} I_a$, $I + J = \{a + b \in R \mid a \in I, b \in J\}$ Ideale.
3. Sei $A \subset R$ eine Teilmenge. Dann gibt es einen kleinsten Unterring S mit $A \subset S$.
4. Sei $A \subset R$ eine Teilmenge. Dann gibt es ein kleinstes Ideal I mit $A \subset I$. □

Beweis. 1 + 2 Übung.

3 + 4. Der kleinste Unterring bzw. das kleinste Ideal sind

$$\bigcap_{S \supset A, S \text{ Unterring}} S \text{ und } \bigcap_{I \supset A, I \text{ Ideal}} I.$$

Definition 2.1.24 Sei R ein Ring, A eine Teilmenge in R , S ein Unterring und I, J Ideale in R .

1. Der kleinste Unterring, der S und A enthält, heißt **der von S und A erzeugte Unterring**.

Man schreibt $S[A]$ für den von S und A erzeugten Unterring.

2. Das kleinste Ideal, das A enthält, heißt **das von A erzeugte Ideal**.

Man schreibt (A) für das von A erzeugte Ideal. Falls $A = \{a\}$ schreibt man $(A) = (a)$. Ein solches Ideal heißt **Hauptideal**.

2. **Die Summe von I und J** ist das Ideal $I + J = \{a + b \in R \mid a \in I, b \in J\}$.

3. **Das Produktideal von I und J** ist $IJ = (ab \mid a \in I, b \in J)$ i.e. das von Produkten ab mit $a \in I$ und $b \in J$ erzeugte Ideal.

Beispiel 2.1.25 1. $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ ist der von $\sqrt{2}$ erzeugte Unterring von \mathbb{R} .

2. Allgemeiner gilt für R kommutativ, $S \subset R$ Unterring und $r \in R$:

$$S[r] = \{P(r) \in R \mid P \in S[X]\}.$$

3. Sei R ein kommutativer Ring und $r \in R$. Dann gilt $(r) = \{ra \in R \mid a \in R\}$.

Bemerkung 2.1.26 Es gilt $IJ \subset I \cap J$.

Index

- $D^k(G)$, 32
- k -te derivierte Untergruppe, 32
- p -Gruppe, 23
- äußere Automorphismen, 6

- abelsch, 4
- Alternierende Gruppe, 6
- assoziativ, 4
- auflösbar, 32
- Automorphismus, 6

- Bahn, 20

- Derivierte Gruppe, 16

- erzeugte Untergruppe, 14
- exakte Sequenz, 10

- Fixpunkt, 20

- Gruppe, 4
 - einfach, 10
- Gruppenhomomorphismus, 5
 - Gruppenautomorphismus, 6
 - Gruppenisomorphismus, 6
- innerer, 6
- Kern, 6
- Konjugation mit g , 6

- Ideal, 37
 - erzeugtes Ideal, 40
 - Hauptideal, 40
 - Nullideal, 38
 - Produktideal, 40
 - Summe, 40
- inverses Element, 4
- invertierbares Element, 36
- Isomorphismus, 6

- Körper, 36

- kanonische Projektion, 7
- kommutativ, 4
- Kommutator, 16
- Kommutator Untergruppe, 16

- Linksklassen, 6

- Mächtigkeit, 7

- neutrales Element, 4
- Normalisator, 10
- Normalteiler, 8

- Operation, 19
 - k -transitiv, 25
 - Konjugation, 20
 - Linkstranslation, 20
 - transitiv, 20
 - treu, 20
 - Triviale Operation, 20
- Orbit, 20
- Ordnung, 7
 - Ordnung eines Elements, 15

- Polynomring, 36
- Polynomring mit n Unbekannten, 37
- Produkt-Gruppe, 5

- Quotient G/H , 7
- Quotient $H \backslash G$, 7
- Quotient einer Menge
 - nach einer Gruppe, 20
- Quotientgruppe, 9
- Quotientring, 39

- Rechtsklassen, 7
- Ring, 35
 - Einheit, 36
 - erzeugter Unterring, 40

- Integritätsring, [36](#)
- kommutativ, [35](#)
- Nullring, [35](#)
- Nullteiler, [36](#)
- Nullteilerfrei, [36](#)
- Produkt, [36](#)
- Schiefkörper, [36](#)

- Semidirektes Produkt, [17](#)
- Stabilisator, [20](#)
- Sylowuntergruppe, [27](#)

- Trivialeuntergruppe, [5](#)

- Untergruppe, [5](#)
 - Index, [7](#)
- Unterring, [37](#)

- Zentralisator, [12](#)
- Zentrum, [12](#)
- Zykel, [24](#)
 - fremd, [24](#)
 - Länge, [24](#)
 - Träger, [24](#)
- zyklische Gruppe, [14](#)