Geometrie WS2018/19

Dozent: Prof. Dr. Arno Fehm

8. Dezember 2018

Inhaltsverzeichnis

Vorwort

Wir freuen uns, dass du unser Skript für die Vorlesung *Geometrie* bei Prof. Dr. Arno Fehm im WS2018/19 gefunden hast. Da du ja offensichtlich seit einem Jahr Mathematik studierst, kannst du dich glücklich schätzen zu dem einen Drittel zu gehören, dass nicht bis zum zweiten Semester abgebrochen hat.

Wenn du schon das Vorwort zu *Lineare Algebra und analytische Geometrie 1+2* gelesen hast, weißt du sicherlich, dass Prof. Fehm ein Freud der Algebra ist.[1] Auf die Frage eines Kommilitonen, wo in seinem Inhaltsverzeichnis (Gruppen, Ringe, Körper) die Geometrie vorkomme, antwortete er:

> *Die Frage ist nicht, wieso wir in dieser Vorlesung Algebra statt Geometrie machen, sondern warum hier seit 20 Jahren Geometrie unterrichtet wird.*

Wie auch im letzten Vorwort können wir dir nur empfehlen die Vorlesung immer zu besuchen, denn dieses Skript ist kein Ersatz dafür. Es soll aber ein Ersatz für deine unleserlichen und (hoffentlich nicht) unvollständigen Mitschriften sein und damit die Prüfungsvorbereitung einfacher machen. Im Gegensatz zu letztem Semester veröffentlicht Prof. Fehm auf seiner Homepage (`http://www.math.tu-dresden.de/~afehm/lehre.html`) kein vollständiges Skript mehr, sondern nur noch eine Zusammenfassung.

Der Quelltext dieses Skriptes ist bei Github (`https://github.com/henrydatei/TUD_MATH_BA`) gehostet; du kannst ihn dir herunterladen, anschauen, verändern, neu kompilieren, ... Auch wenn wir das Skript immer wieder durchlesen und Fehler beheben, können wir leider keine Garantie auf Richtigkeit geben. Wenn du Fehler finden solltest, wären wir froh, wenn du ein neues Issue auf Github erstellst und dort beschreibst, was falsch ist. Damit wird vielen (und besonders nachfolgenden) Studenten geholfen.

Und jetzt viel Spaß bei *Geometrie*!

[1] In Zukunft wird sich Prof. Fehm richtig freuen dürfen, denn im Zuge einer neuen Studienordnung, die am 1.4.2019 in Kraft tritt, kommt so gut wie keine Geometrie im *Bachelor Mathematik* vor.

Kapitel I

Endliche Gruppen

1. Erinnerung und Beispiele

▶ **Erinnerung 1.1**

Eine Gruppe ist ein Paar $(G, *)$ bestehend aus einer Menge G und einer Verknüpfung $* : G \times G \to G$, dass die Axiome Assoziativität, Existenz eines neutralen Elements und Existenz von Inversen erfüllt, und wir schreiben auch G für die Gruppe $(G, *)$. Die Gruppe G ist abelsch , wenn $g * h = h * g$ für alle $g, h \in G$. Eine allgemeine Gruppe schreiben wir multiplikativ mit neutralem Element 1, abelsche Gruppen auch additiv mit neutralem Element 0.

Eine Teilmenge $H \subseteq G$ ist eine Untergruppe von G, in Zeichen $H \leq G$, wenn $H \neq \emptyset$ und H abgeschlossen ist unter der Verknüpfung und den Bilden von Inversen. Wir schreiben 1 (bzw. 0) auch für die triviale Untergruppe $\{1\}$ (bzw. $\{0\}$) von G.

Eine Abbildung $\varphi : G \to G'$ zwischen Gruppen ist ein Gruppenhomomorphismus , wenn

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2) \quad \forall g_1, g_2 \in G$$

und in diesem Fall ist

$$\mathrm{Ker}(\varphi) = \varphi^{-1}(\{1\})$$

der Kern von φ. Wir schreiben $\mathrm{Hom}(G, G')$ für die Menge der Gruppenhomomorphismen $\varphi : G \to G'$.

■ **Beispiel 1.2**

Sei $n \in \mathbb{N}$, K ein Körper und X eine Menge.

(a) $\mathrm{Sym}(X)$, die symmetrische Gruppe aller Permutationen der Menge X mit $f \cdot g = g \circ f$, insbesondere $S_n = \mathrm{Sym}(\{1, ..., n\})$

(b) $\mathbb{Z}$ sowie $\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\}$ mit der Addition

(c) $\mathrm{GL}_n(K)$ mit der Matrizenmultiplikation, Spezialfall $\mathrm{GL}_1(K) = K^\times = K \backslash \{0\}$

(d) Für jeden Ring R bilden die Einheiten $R^\times$ eine Gruppe unter der Multiplikation, zum Beispiel $\mathrm{Mat}_n(K)^\times = \mathrm{GL}_n(K)$, $\mathbb{Z}^\times = \mu_2 = \{1, -1\}$

■ **Beispiel 1.3**

Ist $(G, \cdot)$ eine Gruppe, so ist auch $(G^{op}, \cdot^{op})$ mit $G = G^{op}$ und $g \cdot^{op} h = h \cdot g$ eine Gruppe.

▶ **Bemerkung 1.4**
Ist G eine Gruppe und $h \in G$, so ist die Abbildung

$$\tau_h = \begin{cases} G \to G \\ g \mapsto gh \end{cases}$$

eine Bijektion (also $\tau_h \in \mathrm{Sym}(G)$) mit Umkehrabbildung $\tau_{h^{-1}}$.

Satz 1.5
Sei G eine Gruppe. Zu jeder Menge $X \subseteq G$ gibt es eine kleinste Untergruppe $\langle X \rangle$ von G, die X enthält, nämlich

$$\langle X \rangle = \bigcap_{X \subseteq H \leq G} H$$

▶ **Bemerkung 1.6**
Man nennt $\langle X \rangle$ die von X erzeugte von G. Die Gruppe G heißt endlich erzeugt, wenn $G = \langle X \rangle$ für eine endliche Menge $X \subseteq G$.

Satz 1.7
Ein Gruppenhomomorphismus $\varphi : G \to G'$ ist genau dann ein Isomorphismus, wenn es einen Gruppenhomomorphismus $\varphi' : G' \to G$ mit $\varphi' \circ \varphi = \mathrm{id}_G$ und $\varphi \circ \varphi' = \mathrm{id}_{G'}$ gibt.

■ **Beispiel 1.8**
Ist G eine Gruppe, so bilden die Automorphismen $\mathrm{Aut}(G) \subseteq \mathrm{Hom}(G, G)$ eine Gruppe unter $\varphi \circ \varphi' = \varphi' \circ \varphi$. Für $\varphi \in \mathrm{Aut}(G)$ und $g \in G$ schreiben wir $g^\varphi = \varphi(g)$.

Satz 1.9
Einen Gruppenhomomorphismus $\varphi : G \to G'$ ist genau dann injektiv, wenn $\mathrm{Ker}(\varphi) = 1$.

■ **Beispiel 1.10**
Sei $n \in \mathbb{N}$, K ein Körper.

(a) $\mathrm{sgn} : S_n \to \mu_2$ ist ein Gruppenhomomorphismus mit Kern die alternierende Gruppe A_n.

(b) $\det : \mathrm{GL}_n(K) \to K^\times$ ist ein Gruppenhomomorphismus mit Kern $\mathrm{SL}_n(K)$.

(c) $\pi_{n\mathbb{Z}} : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a \mapsto a + n\mathbb{Z}$ ist ein Gruppenhomomorphismus mit Kern $n\mathbb{Z}$

(d) Ist A eine abelsche Gruppe, so ist

$$[n] : \begin{cases} A \to A \\ x \to nx \end{cases}$$

ein Gruppenhomomorphismus mit Kern $A[n]$, die n-Torsion von A und Bild nA.

(e) Ist G eine Gruppe, so ist

$$\begin{cases} G \to G^{op} \\ g \mapsto g^{-1} \end{cases}$$

ein Isomorphismus.

Definition 1.11 (Zykel, disjunkte Zykel)
Seien $n, k \in \mathbb{N}$. Für paarweise verschiedene Elemente $i_1, ..., i_k \in \{1, ..., n\}$ bezeichnen wir mit $(i_1 ... i_k)$ das $\sigma \in S_n$ gegeben durch

$$\begin{aligned} \sigma(i_j) &= i_{j+1} \quad \text{für } j = 1, ..., k-1 \\ \sigma(i_k) &= i_1 \\ \sigma(i) &= i \quad \text{für } i \in \{1, ..., n\} \setminus \{i_1, ..., i_k\} \end{aligned}$$

Wir nennen $(i_1 ... i_k)$ eine k-Zykel . Zwei Zykel $(i_1 ... i_k)$ und $(j_1 ... j_l) \in S_n$ heißen disjunkt , wenn $\{i_1, ..., i_k\} \cap \{j_1, ..., j_l\} = \emptyset$.

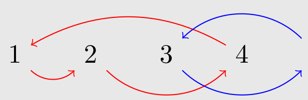
Satz 1.12
Jedes $\sigma \in S_n$ ist das Produkt von Transpositionen (das heißt 2-Zykeln).

Lemma 1.13
Disjunkte Zykel kommutieren, das heißt sind $\tau_1, \tau_2 \in S_n$ disjunkte Zykel, so ist $\tau_1 \tau_2 = \tau_2 \tau_1$.

Beweis. Sind $\tau_1 = (i_1 ... i_k)$ und $\tau_2 = (j_1 ... j_l)$ so ist

$$\tau_1 \tau_2(i) = \tau_2 \tau_1(i) = \begin{cases} \tau_1(i) & i \in \{i_1 ... i_k\} \\ \tau_2(i) & i \in \{j_1 ... j_l\} \\ i & \text{sonst} \end{cases}$$ □

Satz 1.14
Jedes $\sigma \in S_n$ ist ein Produkt von paarweise disjunkten k-Zykeln mit $k \geq 2$ eindeutig bis auf Reihenfolge (sogenannte Zykelzerlegung von σ).



Also ein 3-Zykel und ein 2-Zykel.

Beweis. Induktion nach $N = |\{i \mid \sigma(i) \neq i\}|$.
$N = 0$: $\sigma = \mathrm{id}$
$N > 0$: Wähle i_1 mit $\sigma(i_1) \neq i_1$, betrachte $i_1, \sigma(i_1), \sigma^2(i_1), ...$ Da $\{1, ..., n\}$ endlich und σ bijektiv ist, existiert ein minimales $k \geq 2$ mit $\sigma^k(i_1) = i_1$. Setze $\tau_1 = (i_1\, \sigma(i_1) ... \sigma^{k-1}(i_1))$. Dann ist $\sigma = \tau_1 \circ \tau_1^{-1} \sigma$, und nach Induktionshypothese ist $\tau_1^{-1} \sigma = \tau_2 \circ ... \circ \tau_m$ mit disjunkten Zyklen $\tau_2, ..., \tau_m$.
Eindeutigkeit ist klar, denn jedes i kann nur in einem Zykel $(i\, \sigma(i) ... \sigma^{k-1}(i))$ vorkommen. □

■ **Beispiel**

$(1\,2\,3\,4\,5)(2\,4) = (1\,4\,5)(2\,3) = (2\,3)(1\,4\,5) = (3\,2)(1\,4\,5) = (3\,2)(4\,5\,1) \neq (3\,2)(1\,5\,4)$

2. Ordnung und Index

Sei G eine Gruppe, $g \in G$.

Definition 2.1 (Ordnung)

(a) $\#G = |G| \in \mathbb{N} \cup \{\infty\}$, die Ordnung von G.

(b) $\operatorname{ord}(g) = \#\langle g \rangle$, die Ordnung von g.

Beispiel 2.2

(a) $\#S_n = n!$

(b) $\#A_n = \frac{1}{2}n!$ für $n \geq 2$

(c) $\#\mathbb{Z}/n\mathbb{Z} = n$

Lemma 2.3
Für $X \subseteq G$ ist

$$\langle X \rangle = \{g_1^{\varepsilon_1} \cdot \dots \cdot g_r^{\varepsilon_r} \mid r \in \mathbb{N}_0, g_1, ..., g_r \in X, \varepsilon_1, ..., \varepsilon_r \in \{-1, 1\}\}$$

Beweis. klar, rechte Seite ist Untergruppe, die X enthält, und jede solche enthält alle Ausdrücke der Form $g_1^{\varepsilon_1} \cdot \dots \cdot g_r^{\varepsilon_r}$. □

Satz 2.4

(a) Ist $\operatorname{ord}(g) = \infty$, so ist $\langle g \rangle = \{..., g^{-2}, g^{-1}, 1, g^1, g^2, ...\}$

(b) Ist $\operatorname{ord}(g) = n$, so ist $\langle g \rangle = \{1, g, g^2, ..., g^{n-1}\}$

(c) Es ist $\operatorname{ord}(g) = \inf\{k \in \mathbb{N} \mid g^k = 1\}$

Beweis. Nach Lemma 2.3 ist $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$. Sei $m = \inf\{k \in \mathbb{N} \mid g^k = 1\}$.

- $|\{k \in \mathbb{N} \mid g^k = 1\}| = m$: Sind $g^a = g^b$ mit $0 \leq a < b < m$, so ist $g^{b-a} = 1$, aber $0 < b - a < m$, was ein Widerspruch zur Minimalität von m ist.
- $m = \infty \Rightarrow \operatorname{ord}(g) = \infty$: klar
- $m < \infty \Rightarrow \langle g \rangle = \{g^k \mid 0 \leq k < m\}$: Für $k \in \mathbb{Z}$ schreibe $k = qm + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < m$

$$g^k = g^{qm+r} = (\underbrace{g^m}_{=1})^q \cdot g^r = g^r \in \{1, g, ..., g^{m-1}\}$$ □

Beispiel 2.5

(a) Ist $\sigma \in S_n$ ein k-Zykel, so ist $\operatorname{ord}(\sigma) = k$.

(b) Für $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$ ist $\operatorname{ord}(\overline{1}) = n$.

Definition 2.6 (Komplexprodukt, Nebenklasse)
Seien $A, B \subseteq G$, $H \leq G$

(a) $AB := A \cdot B := \{ab \mid a \in A, b \in B\}$ das Komplexprodukt von A und B.

(b) $gH := \{g\} \cdot H = \{gh \mid h \in H\}$ die Linksnebenklasse von H bezüglich g.
$Hg := H \cdot \{g\} = \{hg \mid h \in H\}$ die Rechtsnebenklasse von H bezüglich g.

(c) ${}^{G}/_{H} := \{gH \mid g \in G\}$ die Menge der Linksnebenklassen.
${}_{H}\backslash^{G} := \{Hg \mid g \in G\}$ die Menge der Rechtsnebenklassen.

Beispiel 2.7
Für $h \in H$ ist $hH = H = Hh$.

Lemma 2.8
Seien $H \leq G$, $g, g' \in G$.

(a) $gH = g'H \Leftrightarrow g' = gh$ für ein $h \in H$
$Hg = Hg' \Leftrightarrow g' = gh$ für ein $h \in H$

(b) Es ist $gH = g'H$ oder $gH \cap g'H = \emptyset$ und $Hg = Hg'$ oder $Hg \cap Hg' = \emptyset$.

(c) Durch $gH \mapsto Hg^{-1}$ wird eine wohldefinierte Bijektion ${}^{G}/_{H} \to {}_{H}\backslash^{G}$ gegeben.

Beweis. (a) Hinrichtung: $gH = g'H \Rightarrow g' = g' \cdot 1 \in g'H = gH \Rightarrow$ es existiert $h \in H$ mit $g' = gh$
Rückrichtung: $g' = gh \Rightarrow g'H = ghH = gH$

(b) Ist $gH \cap g'H \neq \emptyset$, so existieren $h, h' \in H$ mit $gh = g'h' \Rightarrow gH = ghH = g'h'H = g'H$

(c) wohldefiniert: $gH = g'H \overset{a)}{\Rightarrow} g' = gh$ mit $h \in H \Rightarrow H(g')^{-1} = Hh^{-1}g^{-1} = Hg^{-1}$
bijektiv: klar, Umkehrabbildung: $Hg \mapsto g^{-1}H$ □

Definition 2.9 (Index)
Für $H \subseteq G$ ist

$$(G : H) := |{}^{G}/_{H}| + |{}_{H}\backslash^{G}| \in \mathbb{N} \cup \{\infty\}$$

der Index von H in G.

Beispiel 2.10

(a) $(S_n : A_n) = 2$ für $n \geq 2$

(b) $(\mathbb{Z} : n\mathbb{Z}) = n$

Satz 2.11
Der Index ist multiplikativ: Sind $K \leq H \leq G$, so ist

$$(G : K) = (G : H) \cdot (H : K)$$

Beweis. Nach Lemma 2.8 bilden die Nebenklassen von H eine Partition von G, das heißt es gibt $(g_i)_{i \in I}$ in G

mit $G = \biguplus_{i \in I} g_i H$. Analog ist $H = \biguplus_{j \in J} h_j K$ mit $h_j \in H$. Dann gilt:

$$H = \biguplus_{j \in J} h_j K \overset{1.4}{\Rightarrow} gH = \biguplus_{j \in J} g h_j K \text{ für jedes } g \in G$$
$$G = \biguplus_{i \in I} g_i H = \biguplus_{i \in I} \biguplus_{j \in J} g_i h_j K = \biguplus_{(i,j) \in I \times J} g_i h_j K$$

Somit ist $(G : K) = |I \times J| = |I| \cdot |J| = (G : H) \cdot (H : K)$. □

Folgerung 2.12 (Satz von Lagrange)
Ist G endlich und $H \leq G$, so ist

$$\#G = \#H \cdot (G : H)$$

Insbesondere gilt $\#H | \#G$ und $(G : H) | \#G$.

Beweis. $\#G = (G : 1) \overset{2.11}{=} (G : H)(H : 1) = (G : H) \cdot \#H$. □

Folgerung 2.13 (kleiner Satz von Fermat)
Ist G endlich und $n = \#G$, so ist $g^n = 1$ für jedes $g \in G$.

Beweis. Nach Folgerung 2.12 gilt: $\mathrm{ord}(g) = \#\langle g \rangle | \#G = n$. Nach Satz 2.4 ist $g^{\mathrm{ord}(g)} = 1$, somit auch

$$g^n = (\underbrace{g^{\mathrm{ord}(g)}}_{=1})^{\frac{n}{\mathrm{ord}(g)}} = 1$$ □

▶ Bemerkung 2.14
Nach Folgerung 2.12 ist die Ordnung jeder Untergruppe von G ein Teiler der Gruppenordnung $\#G$. Umgekehrt gibt es im Allgemeinen aber nicht zu jedem Teiler d von $\#G$ eine Untergruppe H von G mit $\#H = d$.

3. Normalteiler und Quotientengruppen

Sei G eine Gruppe.

Definition 3.1 (normal, Normalteiler)
Eine Untergruppe $H \leq G$ ist normal (in Zeichen $H \trianglelefteq G$), wenn $g^{-1}hg \in H$ für alle $h \in H$ und $g \in G$. Ein Normalteiler von G ist eine normale Untergruppe von G.

■ **Beispiel 3.2**

(a) Ist G abelsch, so ist jede Untergruppe von G ein Normalteiler.

(b) Ist $\varphi : G \to H$ ein Gruppenhomomorphismus, so ist $\mathrm{Ker}(\varphi) \trianglelefteq G$, denn $\varphi(h) = 1 \Rightarrow \varphi(g^{-1}hg) = \varphi(g)^{-1}\varphi(h)\varphi(g) = 1 \ \forall g \in G$.

(c) Jede Gruppe G hat die trivialen Normalteiler $1 \trianglelefteq G$ und $G \trianglelefteq G$.

Lemma 3.3
Sei $H \leq G$ und $N \trianglelefteq G$.

(a) $H \trianglelefteq G \Leftrightarrow gH = Hg$ für alle $g \in G$

(b) $HN = NH$, $HN \leq G$, $N \trianglelefteq HN$, $H \cap N \leq N$, $H \cap N \trianglelefteq H$

(c) Sind $N, H \trianglelefteq G$, so ist $H \cap N \trianglelefteq G$, $HN \trianglelefteq G$

(d) Für $g, g' \in G$ ist $gN \cdot g'N = gg'N$

Beweis. (a) Hinrichtung: $\forall g \in G$, $\forall h \in H$: $g^{-1}hg \in H \Rightarrow gHg^{-1} \subseteq H \Rightarrow Hg = gH$ und $g^{-1}H \subseteq Hg^{-1} \Rightarrow gH = Hg$
Rückrichtung: $\forall g \in G$: $gH = Hg \Rightarrow \exists h' \in H$: $gh' = hg \Rightarrow g^{-1}hg = h \in H$

(b)
- $HN = \bigcup_{n \in \mathbb{N}} hN = \bigcup_{n \in \mathbb{N}} Nh = NH$
- $HN \cdot NH = H \cdot NH \cdot N = H \cdot HN \cdot N = HN$
  $(HN)^{-1} = N^{-1}H^{-1} = NH = HN$
- $N \trianglelefteq HN$: klar
- $H \cap N \leq N$: klar
- $H \cap N \trianglelefteq H$: $n \in H \cap N$, $h \in H \Rightarrow h^{-1}nh \in H \cap N$

(c)
- $H \cap N \trianglelefteq G$: $h \in H \cap N$, $g \in G \Rightarrow g^{-1}hg \in H \cap N$
- $HN \trianglelefteq G$: $g \in G \Rightarrow gHN \overset{a)}{=} Hg \cdot N = H \cdot gN \overset{a)}{=} H \cdot Ng = HNg$

(d) $gN \cdot g'N = g \cdot Ng' \cdot N \overset{a)}{=} g \cdot g'N = gg'N$ □

Satz 3.4
Sei $N \trianglelefteq G$. Dann ist G/N mit dem Komplexprodukt als Verknüpfung eine Gruppe, und $\pi_N : G \to G/N$, $g \mapsto gN$ ein Gruppenhomomorphismus mit Kern N.

Beweis.
- Komplexprodukt ist Verknüpfung auf G/N: Lemma 3.3
- Gruppenaxiome übertragen sich von G auf G/N: klar
- π_N ist ein Homomorphismus: Lemma 3.3
- $\mathrm{Ker}(\pi_N) = N$: Lemma 2.8 □

Folgerung 3.5
Die Normalteiler sind genau die Gruppenhomomorphismen.

Definition 3.6 (Quotientengruppe)
Für $N \trianglelefteq G$ heißt ${}^{G}\!/\!{}_{N}$ zusammen mit dem Komplexprodukt als Verknüpfung die <u>Quotientengruppe</u> von G nach N (oder G modulo N).

Lemma 3.7
Sei $N \trianglelefteq G$. Für $H \leq G$ ist $\pi_N(H) = {}^{HN}\!/\!{}_{N} \leq {}^{G}\!/\!{}_{N}$, und $H \mapsto \pi(H)$ liefert eine Bijektion zwischen

- den $H \leq G$ mit $N \leq H$ und
- den $H \leq {}^{G}\!/\!{}_{N}$

Beweis.

- $\pi_N(H) = \{hN \mid h \in H\} = \{hnN \mid h \in H, n \in N\} = {}^{HN}\!/\!{}_{N}$
- Umkehrabbildung: $H \mapsto \pi_N^{-1}(H)$:
  $H \leq {}^{G}\!/\!{}_{N}$: $\pi_N(\pi_N^{-1}(H)) = H$, da π_N surjektiv
  $N \leq H \leq G$: $\pi_N^{-1}(\pi_N(H)) = \pi_N^{-1}({}^{HN}\!/\!{}_{N}) = HN \subseteq H \cdot H = H$ □

Satz 3.8 (Homomorphiesatz)
Sei $\varphi : G \to H$ ein Gruppenhomomorphismus und $N \trianglelefteq G$ mit $N \leq \operatorname{Ker}(\varphi)$. Dann gibt es genau einen Gruppenhomomorphismus $\overline{\varphi} : {}^{G}\!/\!{}_{N} \to H$ mit $\overline{\varphi} \circ \pi_N = \varphi$.

$$\begin{tikzcd} G \arrow[rr, "\varphi"] \arrow[dr, "\pi_N"'] & & H \\ & {}^{G}\!/\!{}_{N} \arrow[ur, dashed, "\overline{\varphi}"'] & \end{tikzcd}$$

Beweis. Existiert so ein $\overline{\varphi}$, so ist $\overline{\varphi}(gN) = (\overline{\varphi} \circ \pi_N)(g) = \varphi(g)$ eindeutig bestimmt. Definiere $\overline{\varphi}$ nun so.

- $\overline{\varphi}$ ist wohldefiniert: $gN = g'N \overset{2.8}{\Rightarrow} \exists g' = gn$ für ein $n \in N \Rightarrow \varphi(g') = \varphi(g) \cdot \underbrace{\varphi(n)}_{=1} = \varphi(g)$, da $n \in \operatorname{Ker}(\varphi)$
- $\overline{\varphi}$ ist Homomorphismus: $\overline{\varphi}(gN \cdot g'N) = \overline{\varphi}(gg'N) = \varphi(gg') = \varphi(g) \cdot \varphi(g') = \overline{\varphi}(gN) \cdot \overline{\varphi}(g'N)$ □

Folgerung 3.9
Ein Gruppenhomomorphismus $\varphi : G \to H$ liefert einen Isomorphismus

$$\bar{\varphi} : {}^{G}\!/\!{}_{\operatorname{Ker}(\varphi)} \xrightarrow{\cong} \operatorname{Im}(\varphi) \leq H$$

Folgerung 3.10 (1. Homomorphiesatz)
Seien $H \leq G$ und $N \trianglelefteq G$. Der Homomorphismus

$$\varphi : H \overset{i}{\hookrightarrow} HN \xrightarrow{\pi_N} {}^{HN}\!/\!{}_{N}$$

induziert einen Isomorphismus

$$\bar{\varphi} : {}^{H}\!/\!{}_{H \cap N} \xrightarrow{\cong} {}^{HN}\!/\!{}_{N}$$

Beweis.

- φ ist surjektiv: Für $h \in H$ und $n \in N$ ist

$$hnN = hN = \varphi(h) \in \varphi(H) = \mathrm{Im}(\varphi)$$

- $\mathrm{Ker}(\varphi) = H \cap \mathrm{Ker}(\pi_N) = H \cap N$

Mit Folgerung 3.9 folgt die Behauptung. □

Folgerung 3.11 (2. Homomorphiesatz)
Seien $N \trianglelefteq G$ und $N \leq H \trianglelefteq G$. Der Homomorphismus $\pi_H : G \to {}^{G}/_{H}$ induziert einen Isomorphismus

$$({}^{G}/_{N})/({}^{H}/_{N}) \xrightarrow{\cong} {}^{G}/_{H}$$

Beweis. Da $N \leq H$ liefert π_H einen Epimorphismus (mit Satz 3.8) $\overline{\pi_H} : {}^{G}/_{N} \to {}^{G}/_{H}$.

$$\begin{tikzcd}
G \arrow[rr, "\pi_H"] \arrow[dr, "\pi_N"'] & & {}^{G}/_{H} \\
& {}^{G}/_{N} \arrow[ur, dashed, "\overline{\pi_H}"'] &
\end{tikzcd}$$

Dieser hat Kern $\mathrm{Ker}(\overline{\pi_H}) = {}^{H}/_{N}$, induziert nach Folgerung 3.9 einen Isomorphismus

$$({}^{G}/_{N})/\mathrm{Ker}(\overline{\pi_H}) \xrightarrow{\cong} \mathrm{Im}(\overline{\pi_H}) = {}^{G}/_{H}$$ □

Definition 3.12 (Konjugation)
Seien $x, x', g \in G$ und $H, H' \leq G$.

(a) $x^g := g^{-1}xg$, Konjugation von x mit g

(b) x und x' sind konjugiert (in G)$\Leftrightarrow \exists g \in G$: $x' = x^g$

(c) H und H' heißen konjugiert (in G)$\Leftrightarrow \exists g \in G$: $H' = H^g = \{h^g \mid h \in H\}$

Lemma 3.13
Die Abbildung

$$\mathrm{int} : \begin{cases} G \to \mathrm{Aut}(G) \\ g \mapsto (x \mapsto x^g) \end{cases}$$

ist ein Gruppenhomomorphismus.

Beweis.

- $\mathrm{int}(g) \in \mathrm{Hom}(G, G)$: $(xy)^g = g^{-1}xyg = g^{-1}xgg^{-1}yg = x^g \cdot y^g$
- $(x^g)^h = h^{-1}g^{-1}xgh = (gh)^{-1}x(gh) = x^{gh}$
- $\mathrm{int}(g) \in \mathrm{Aut}(G)$: Umkehrabbildung zu $\mathrm{int}(g)$ ist $\mathrm{int}(g^{-1})$
- $\mathrm{int}(g) \in \mathrm{Hom}(G, \mathrm{Aut}(G))$:

$$\mathrm{int}(gh) = \mathrm{int}(h) \circ \mathrm{int}(g) = \mathrm{int}(g) \cdot \mathrm{int}(h)$$ □

Definition 3.14 (innere Automorphismen, Zentrum, charakteristische Gruppe)

(a) $\mathrm{Inn}(G) = \mathrm{Im}(\mathrm{int}) \leq \mathrm{Aut}(G)$, die Gruppe der inneren Automorphismen von G

(b) $\mathrm{Z}(G) = \mathrm{Ker}(\mathrm{int}) = \{g \in G \mid xg = gx \quad \forall x \in G\}$, das Zentrum von G

(c) $H \leq G$ ist charakteristisch $\Leftrightarrow \forall \sigma \in \mathrm{Aut}(G)$: $H = H^\sigma$

▶ **Bemerkung 3.15**

(a) Konjugation ist eine Äquivalenzrelation

(b) $H \leq G$ ist normal $\Leftrightarrow H = H^\sigma \quad \forall \sigma \in \mathrm{Inn}(G)$

(c) Deshalb gilt für $H \leq G$: H ist charakteristisch $\Rightarrow$ H ist normal

■ **Beispiel 3.16**

$\mathrm{Z}(G)$ ist charakteristisch in G

4. Abelsche Gruppen

Sei G ein Gruppe.

Definition 4.1 (zyklische Gruppe)
Eine Gruppe G ist zyklisch $\Leftrightarrow G = \langle g \rangle$ für ein $g \in G$.

■ **Beispiel 4.2**

(a) $\mathbb{Z} = \langle 1 \rangle$

(b) $\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \rangle$

(c) $C_n = \langle (1\,2\,...\,n) \rangle \leq S_n$

(d) Ist $\#G = p$ eine Primzahl, so ist G zyklisch (Übung 6)

Lemma 4.3
Die Untergruppen von $(\mathbb{Z}, +)$ sind genau die $\langle k \rangle = \mathbb{Z}k$ mit $k \in \mathbb{N}_0$ und für $k_1, ..., k_r \in \mathbb{Z}$ ist $\langle k_1, ..., k_r \rangle = \langle k \rangle$ mit

$$k = \mathrm{ggT}(k_1, ..., k_r)$$

Beweis. Zwei Beweise sind möglich:

1. Jede Untergruppe von $\mathbb{Z}$ ist ein Ideal von $(\mathbb{Z}, +, \cdot)$ und $\mathbb{Z}$ ist ein Hauptidealring.
2. Sei $H \leq \mathbb{Z}$. Setze $k = \min\{H \cap N\}$, ohne Einschränkung $H \neq \{0\}$.
   - $H = \langle k \rangle$: $n \in H \Rightarrow n = qk + r$ mit $q, r \in \mathbb{Z}$, $0 \leq r < k \Rightarrow r = n - \underbrace{qk}_{k+...+k} \in H \xRightarrow[\text{mal}]{k \text{ mini-}} r = 0 \Rightarrow n \in \langle k \rangle$
   - $\langle k_1, ..., k_r \rangle = \langle k \rangle \Rightarrow k = \mathrm{ggT}(k_1, ..., k_r)$:
     $k_i \in \langle k \rangle \Rightarrow k | k_i \quad \forall i$
     $k \in \langle k_1, ..., k_r \rangle \Rightarrow k = n_1 k_1 + ... + n_r k_r$ mit $n_i \in \mathbb{Z}$ $\exists d | k_i \Rightarrow d | k \Rightarrow k = \mathrm{ggT}(k_1, ..., k_r)$ □

Satz 4.4 (Klassifikation von zyklischen Gruppen)
Sei $G = \langle g \rangle$ zyklisch. Dann ist G abelsch und

(a) $G \cong (\mathbb{Z}, +)$ oder

(b) $G \cong (\mathbb{Z}/n\mathbb{Z}, +)$ mit $n = \#G < \infty$

Beweis. Betrachte

$$\varphi : \begin{cases} \mathbb{Z} \to G \\ k \mapsto g^k \end{cases}$$

φ ist ein Homomorphismus und surjektiv, da $G = \langle g \rangle$. Nach Folgerung 3.9 ist $G = \mathrm{Im}(\varphi) \cong {}^{\mathbb{Z}}/_{\mathrm{Ker}(\varphi)}$. Nach Lemma 4.3 ist $\mathrm{Ker}(\varphi) = \langle n \rangle$ für ein $n \in \mathbb{N}_0$.

- $n = 0$, so ist $\mathrm{Ker}(\varphi) = \langle 0 \rangle$, also φ injektiv und $G \cong \mathbb{Z}$.
- $n > 0$, so ist $G \cong \mathbb{Z}/n\mathbb{Z}$ und $n = \#\mathbb{Z}/n\mathbb{Z} = \#G$. □

Satz 4.5
Sei $G = (G, +) = \langle g \rangle$ zyklisch der Ordnung $n \in \mathbb{N}$.

(a) Zu jedem $d \in \mathbb{N}$ mit $d \mid n$ hat G genau eine Untergruppe der Ordnung d, nämlich $U_d = \langle \frac{n}{d} g \rangle$

(b) Für $d \mid n$ und $d' \mid n$ ist $U_d \leq U_{d'} \Leftrightarrow d \mid d'$

(c) Für $k_1, \ldots, k_k \in \mathbb{Z}$ ist $\langle k_1 g, \ldots, k_r g \rangle = \langle eg \rangle = U_{n/e}$ mit $e = \text{ggT}(k_1, \ldots, k_r, n)$

(d) Für $k \in \mathbb{Z}$ ist $\text{ord}(kg) = \frac{n}{\text{ggT}(k,n)}$

Beweis. Betrachte wieder

$$\varphi : \begin{cases} \bar{k} \to G \\ k \mapsto kg \end{cases}$$

(a) Nach Lemma 3.7 und Lemma 4.3 liefert φ Bijektion

$$\{e \in \mathbb{N} \mid n\mathbb{Z} \leq e\mathbb{Z}\} \xrightarrow{1.1} \{H \leq G\}$$

und $n\mathbb{Z} \leq e\mathbb{Z} \Leftrightarrow e \mid n$. Ist $H = \varphi(e\mathbb{Z}) = \langle eg \rangle$, so ist $H \cong {}^{e\mathbb{Z}}/{}_{n\mathbb{Z}}$, also $n = (\mathbb{Z} : n\mathbb{Z}) = (\mathbb{Z} : e\mathbb{Z}) \cdot (e\mathbb{Z} : n\mathbb{Z}) = e \cdot \#H$

(b) $U_d \leq U_{d'} \Leftrightarrow \langle \frac{n}{d} g \rangle \leq \langle \frac{n}{d'} g \rangle \Leftrightarrow \frac{n}{d}\mathbb{Z} \leq \frac{n}{d'}\mathbb{Z} \Leftrightarrow \frac{n}{d'} \mid \frac{n}{d} \Leftrightarrow d \mid d'$

(c) Mit $H = \langle k_1, \ldots, k_r, n \rangle \leq \mathbb{Z}$ ist $n\mathbb{Z} \leq H$, $\varphi(H) = \langle k_1 g, \ldots, k_r g \rangle$. Nach Lemma 4.3 ist $H = \langle e \rangle$ mit $e = \text{ggT}(k_1, \ldots, k_r, n)$, somit $\langle k_1 g, \ldots, k_r g \rangle = \varphi(e\mathbb{Z}) = U_{n/e}$

(d) $\text{ord}(kg) = \#\langle kg \rangle \overset{c)}{=} \#U_{n/e}$ mit $e = \text{ggT}(k, n)$ □

Lemma 4.6
Seien $a, b \in G$. Kommutieren a und b und sind $\text{ord}(a)$ und $\text{ord}(b)$ teilerfremd, so ist

$$\text{ord}(a, b) = \text{ord}(a) \cdot \text{ord}(b)$$

Beweis. Nach Folgerung 2.12 ist $\langle a \rangle \cap \langle b \rangle = 1$. Ist $(ab)^k = 1 = a^k b^k$, so ist $a^k = b^{-k} \in \langle a \rangle \cap \langle b \rangle = 1$, also $a^k = b^k = 1$. Somit ist $(ab)^k = 1 \Leftrightarrow a^k = 1$ und $b^k = 1$ und damit $\text{ord}(ab) = \text{kgV}(\text{ord}(a), \text{ord}(b)) = \text{ord}(a) \cdot \text{ord}(b)$ □

Folgerung 4.7
Ist G abelsch und sind $a, b \in G$ mit $\text{ord}(a) = m < \infty$, $\text{ord}(b) = n < \infty$, so existiert $c \in G$ mit

$$\text{ord}(c) = \text{kgV}(\text{ord}(a), \text{ord}(b))$$

Beweis. Schreibe $m = m_0 m'$ und $n = n_0 n'$ mit $m_0 n_0 = \text{kgV}(m, n)$ und $\text{ggT}(m_0, n_0) = 1 \Rightarrow \text{ord}(a^{m'}) = m_0$, $\text{ord}(b^{n'}) = n_0 \Rightarrow \text{ord}(b^{n'} \cdot a^{m'}) \overset{4.6}{=} m_0 \cdot n_0 = \text{kgV}(m, n)$. □

Theorem 4.8 (Struktursatz für endlich erzeugte abelsche Gruppen)
Jede endliche erzeugte abelsche Gruppe G ist eine direkte Summe zyklischer Gruppen

$$G \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^{k} \mathbb{Z}/d_i\mathbb{Z}$$

mit eindeutig bestimmten $d_1, \ldots, d_k > 1$ die $d_i \mid d_{i+1}$ für alle i erfüllen.

Beweis.
- Existenz: LAAG 2: VIII. 6.14
- Eindeutigkeit: Für $d \in \mathbb{N}$ ist

$$\begin{aligned}\# G/dG &= \# \left(\mathbb{Z}/d\mathbb{Z}\right)^r \oplus \bigoplus_{i=1}^{k} (\mathbb{Z}/d_i\mathbb{Z})/d\cdot(\mathbb{Z}/d_i\mathbb{Z}) \\ &\overset{4.5}{=} d^r \cdot \prod_{i=1}^{n} \frac{d_i}{\mathrm{ggT}(d, d_i)}\end{aligned}$$

und daraus kann man $r, k, d_1, \ldots, d_k$ erhalten. □

Lemma 4.9
Sei $G = (G, +) = \langle g \rangle$ zyklisch der Ordnung $n \in \mathbb{N}$. Die Endomorphismen von G sind genau die

$$\varphi_{\overline{k}} : \begin{cases} G \to G \\ x \mapsto kx \end{cases} \quad \text{für } \overline{k} = k + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$$

Dabei ist $\varphi_{\overline{l}} \circ \varphi_{\overline{k}} = \varphi_{\overline{kl}}$.

Beweis.
- $\varphi_{\overline{k}}$ wohldefiniert $\overline{k_1} = \overline{k_2} \Rightarrow k_2 = k_1 + an$ mit $a \in \mathbb{Z} \Rightarrow k_2x = k_1x + an \cdot x$, aber $nx = 0$.
- $\varphi_{\overline{k}} \in \mathrm{Hom}(G, G)$: klar, da G abelsch
- $\overline{k} = \overline{l} \Leftrightarrow \varphi_{\overline{k}} = \varphi_{\overline{l}}$: $\varphi_{\overline{k}}(g) = \varphi_{\overline{l}}(g) \Rightarrow (k - l)g = 0 \xRightarrow[=n]{\mathrm{ord}(g)} n \mid (k - l) \Rightarrow \overline{k} = \overline{l}$
- $\varphi \in \mathrm{Hom}(G, G) \Rightarrow \varphi = \varphi_{\overline{k}}$ für ein $k \in \mathbb{Z}$: $\varphi(g) = kg$ für ein $k \Rightarrow \varphi = \varphi_{\overline{k}}$
- $\varphi_{\overline{k}} \circ \varphi_{\overline{l}} = \varphi_{\overline{kl}}$: $l(kx) = (lk)x$ □

Satz 4.10
Ist G zyklisch von Ordnung $n \in \mathbb{N}$, so ist

$$\mathrm{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

Beweis. $\mathrm{Aut}(G) \subseteq \mathrm{Hom}(G, G) = \{\varphi_{\overline{k}} \mid \overline{k} \in \mathbb{Z}/n\mathbb{Z}\}$, $\varphi_{\overline{k}} \in \mathrm{Aut}(G) \Leftrightarrow$ es existiert ein $\overline{l} \in \mathbb{Z}/n\mathbb{Z}$ mit $\varphi_{\overline{l}} \circ \varphi_{\overline{k}} = \varphi_{\overline{1}}$ also existiert ein $\overline{l} \in \mathbb{Z}/n\mathbb{Z}$ mit $\overline{kl} = 1 \Leftrightarrow \overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$ und

$$\begin{cases} (\mathbb{Z}/n\mathbb{Z})^\times & \to \mathrm{Aut}(G) \\ \overline{k} & \mapsto \varphi_{\overline{k}} \end{cases}$$

ist ein Isomorphismus. □

Definition 4.11 (Euler'sche Phi-Funktion)

$$\Phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$$

ist die <u>EULER'sche Phi-Funktion</u> .

Beispiel 4.12

p prim $\Rightarrow \varphi(p) = p - 1$, da $\mathbb{Z}/p\mathbb{Z}$ Körper ist.

Satz 4.13

Ist K ein Körper und $H \leq K^\times$ abelsch, so ist H zyklisch.

Beweis. Setze $m = \max\{\mathrm{ord}(h) \colon h \in H\}$. Nach Folgerung 4.7 gilt $\mathrm{ord}(h) \mid m \quad \forall h \in H$. $\Rightarrow$ Jedes $h \in H$ ist Nullstelle von $f = x^m - 1 \in K[x]$. $\Rightarrow \#H \leq \deg f = m \leq \#H \Rightarrow \#H = m$. Ist $h \in H$ mit $m = \mathrm{ord}(h)$, so ist dann $H = \langle h \rangle$. □

Folgerung 4.14

Für $p \in \mathbb{N}$ prim ist

$$\mathrm{Aut}(C_p) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$$

5. Direkte und semidirekte Produkte

Sei G eine Gruppe und $n \in \mathbb{N}$.

Definition 5.1 (direktes Produkt)
Das direkte Produkt von Gruppen $G_1, ..., G_n$ ist das kartesische Produkt

$$G = \prod_{i=1}^{n} G_1 = G_1 \times ... \times G_n = \bigtimes_{i=1}^{n} G_1$$

mit komponentenweiser Multiplikation.

▶ **Bemerkung 5.2**

(a) Wir identifizieren G_j mit der Untergruppe

$$G_j = \prod_{i \neq j} 1 = 1 \times ... \times 1 \times G_j \times 1 \times ... \times 1$$

von $\prod_{i=1}^{n} G_j$.

(b) Für $i \neq j$, $g_i \in G_i$, $g_j \in G_j$ gilt dann

$$g_i g_j = g_j g_i \tag{1}$$

Definition 5.3 (internes direktes Produkt)
Seien $H_1, ..., H_n \leq G$. Dann ist G das interne direkte Produkt von $H_1, ..., H_n$, in Zeichen

$$G = \prod_{i=1}^{n} H_i = H_1 \times ... \times H_n = \bigtimes_{i=1}^{n} H_i$$

wenn

$$\begin{cases} H_1 \times ... \times H_n & \to G \\ (g_1, ..., g_n) & \mapsto g_1 \cdot ... \cdot g_n \end{cases}$$

ein Gruppenisomorphismus ist.

Satz 5.4
Seien $U, V \leq G$. Dann sind äquivalent:

(i) $G = U \times V$

(ii) $U \trianglelefteq G$, $V \trianglelefteq G$, $U \cap V = 1$, $UV = G$

Beweis.
- $(i) \Rightarrow (ii)$: Im externen direkten Produkt $U \times V$ gilt:
  - $UV = U \times V$: Für $u \in U$, $v \in V$ ist $(u, v) = (u, 1) \cdot (1, v) \in UV$
  - $U \cap V = 1$: klar
  - $U \trianglelefteq U \times V$: Für $g = (u, v) \in U \times V$ und $u_0 = (u_0, 1) \in U$ ist

$$u_0^g = g^{-1} u_0 g = (u^{-1}, v^{-1})(u_0, 1)(u, v) = (u_0^u, 1) \in U$$

- $(ii) \Rightarrow (i)$: betrachte

$$\varphi : \begin{cases} U \times V \to G \\ (u,v) \mapsto w \end{cases}$$

  - Gleichung (1) gilt: Für $u \in U$, $v \in V$ gilt in G:

$$u^{-1}v^{-1}uv = \underbrace{(v^{-1})^u v}_{\in V} = \underbrace{u^{-1}u^v}_{\in U} \cap V = 1 \Rightarrow uv = vu$$

  - φ ist Homomorphismus: $\varphi((u_1,v_1)(u_2,v_2)) = \varphi(u_1u_2, v_1v_2) = u_1u_2v_1v2 \overset{(1)}{=} u_1v_1u_2v_2 = \varphi(u_1,v_1) \cdot \varphi(u_2,v_2)$
  - φ surjektiv: $\mathrm{Im}(\varphi) = UV = G$
  - φ injektiv: $1 = \varphi(u,v) = uv \Rightarrow u = v^{-1} \in U \cap V = 1 \Rightarrow (u,v) = (1,1)$ □

Folgerung 5.5
Seien $H_1, ..., H_n \leq G$. Dann sind äquivalent:

(i) $G = H_1 \times ... \times H_n$

(ii) $G = H_1...H_n$ und $\forall i$: $H_i \trianglelefteq G$ und $H_{i-1} \cap H_i = 1$

Beweis. Induktion nach n.
$n = 1$: trivial
$n > 1$: Setze $U = H_1...H_{n-1}$ und $V = H_n$. Dann ist $U \trianglelefteq G$ (Lemma 3.3 c) und $V \trianglelefteq G$, $UV = H_1...H_n = G$, $U \cap V = 1$. Somit ist $\varphi : U \times V \to G$ ein Isomorphismus nach Satz 5.4. Da $H_i \trianglelefteq U$ für $i < n$ folgt nach Induktionshypothese, dass

$$\varphi' : \begin{cases} H_1...H_{n-1} & \to U \\ (h_1, ..., h_{n-1}) & \mapsto h_1...h_{n-1} \end{cases}$$

Somit ist

$$\varphi \circ (\varphi' \times \mathrm{id}_{H_n}) : \begin{cases} H_1...H_n & \to G \\ (h_1...h_n) & \mapsto \varphi(\varphi'((h_1, ..., h_{n-1}), h)) = h_1...h_n \end{cases}$$

ein Isomorphismus. □

Definition 5.6 (internes semidirektes Produkt)
Seien $H, N \leq G$. Dann ist G das <u>interne semidirekte Produkt</u> von H und N, in Zeichen

$$G = H \ltimes N = N \rtimes H$$

wenn $N \trianglelefteq G$, $H \cap N = 1$ und $NH = G$.

▶ **Bemerkung 5.7**
Ist $G = H \ltimes N$, so ist

$$\alpha : \begin{cases} H \to \mathrm{Aut}(N) \\ h \mapsto \mathrm{int}(h)|_N \end{cases}$$

ein Gruppenhomomorphismus. Im Fall $G = H \times N$ ist $\alpha(h) = \mathrm{id}_N$ für alle $h \in H$. Für $h_1, h_2 \in H$ und $n_1, n_2 \in N$ ist

$$\begin{aligned} h_1 n_1 \cdot h_2 n_2 &= h_1 h_2 h_2^{-1} n_1 h_2 n_2 \\ &= h_1 h_2 \cdot \underbrace{n_1^{h_2}}_{\in N} \cdot n_2 \\ &= h_1 h_2 \cdot n_1^{\alpha(h_2)} \cdot n_2 \end{aligned} \tag{2}$$

Definition 5.8 (semidirektes Produkt)
Seien H, N Gruppen und $\alpha \in \mathrm{Hom}(H, \mathrm{Aut}(N))$. Das semidirekte Produkt $H \ltimes_\alpha N$ von H und N bezüglich α ist das kartesische Produkt $H \times N$ mit der Multiplikation

$$(h_1, n_1) \cdot (h_2, n_2) = (h_1 h_2, n_1^{\alpha(h_2)} n_2)$$

▶ **Bemerkung 5.9**

(a) Wir identifizieren H, N mit der Teilmenge $H \times 1$ bzw. $N \times 1$ von $H \ltimes_\alpha N$.

(b) Ist $\alpha \in \mathrm{Hom}(H, \mathrm{Aut}(N))$ trivial, also $\alpha(h) = \mathrm{id}_N$ für alle $h \in H$, so ist $H \ltimes_\alpha N = H \times N$, das direkte Produkt.

Satz 5.10
Seien H, N Gruppen, $\alpha \in \mathrm{Hom}(H, \mathrm{Aut}(N))$. Dann ist $G = H \ltimes_\alpha N$ eine Gruppe, und diese ist das interne semidirekte Produkt von $H \leq G$ und $N \trianglelefteq G$, wobei

$$\mathrm{int}(h)|_N = \alpha(h) \quad \forall h \in H$$

Beweis. Seien h_1, h_2, h_3, $h \in H$ und n_0, n_1, n_2, n_3, $n \in N$.

- neutrales Element:

$$\begin{aligned} (1_H, 1_N)(h, n) &= (h, 1_N^{\alpha(h)} n) = (h, n) \\ (h, n)(1_H, 1_N) &= (h, n^{\alpha(1_H)} 1_H) \overset{(*)}{=} (h, n) \end{aligned}$$

  $(*)$: $\alpha(1_H) = \mathrm{id}$

- Assoziativität:

$$\begin{aligned} &[(h_1, n_1)(h_2, n_2)](h_3, n_3) = (h_1 h_2, n_1^{\alpha(h_2)} n_2)(h_3, n_3) = (h_1 h_2 h_3, (n_1^{\alpha(h_2)} n_2)^{\alpha(h_3)} n_3) \overset{(*)}{=} (h_1 h_2 h_3, n_1^{\alpha(h_2)\alpha(3)} n_2^{\alpha(h_3)} n_3) \\ &(h_1, n_1)[(h_2, n_2)(h_3, n_3)] = (h_1, n_1)(h_2 h_2, n_2^{\alpha(h_3)} n_3) = (h_1 h_2 h_3, n_1^{\alpha(h_2)\alpha(3)} n_2^{\alpha(h_3)} n_3) \end{aligned}$$

  $(*)$: $\alpha(h_3)$ ist ein Automorphismus und α ist ein Homomorphismus

- Inverses: $(h, n)^{-1} = (h^{-1}, (n^{-1})^{\alpha(h^{-1})})$
- $H \leq G$:

$$\begin{aligned} (h_1, 1)(h_2, 1) &= (h_1 h_2, 1^{\alpha(h_2)} 1) = (h_1 h_2, 1) \in H \\ (h, 1)^{-1} &= (h^{-1}, 1) \in H \end{aligned}$$

- $N \leq G$:

$$(1, n_1)(1, n_2) = (1, n_1^{\alpha(1)} n_2) = (1, n_1 n_2) \in N$$
$$(1, n)^{-1} = (1, (n^{-1})^{\alpha(1^{-1})}) = (1, n^{-1}) \in N$$

- $H \cap N = 1$: klar
- $HN = G$: $(h, 1)(1, n) = (h, 1^{\alpha(1)} n) = (h, n) \in G$
- $N \trianglelefteq G$: $(h, n)^{-1}(1, n_0)(h, n) = (h^{-1}, (n^{-1})^{\alpha(h^{-1})})(h, n_0^{\alpha(h)} n) = (1, ...) \in N$
- $\mathrm{int}(h)|_N = \alpha(h)$:

$$\begin{aligned} n^{\mathrm{int}(h)|_N} &= (h, 1)^{-1}(1, n)(h, 1) \\ &= (h^{-1}, 1)(h, n^{\alpha(h)} 1) \\ &= (1, 1^{\alpha(h)} n^{\alpha(h)}) \\ &= (1, n^{\alpha(h)}) \\ &= n^{\alpha(h)} \end{aligned}$$

□

Folgerung 5.11
Sei $G = H \ltimes N$ und α wie inBemerkung 5.7. Dann ist

$$\varphi : \begin{cases} H \ltimes_\alpha N & \to G \\ (h, n) & \mapsto hn \end{cases}$$

ein Isomorphismus. Insbesondere ist G durch H, N und α bis auf Isomorphie eindeutig bestimmt.

Beweis.

- φ ist Homomorphismus: $\varphi((h_1, n_1) \cdot (h_2, n_2)) = \varphi(h_1 h_2, n_1^{\alpha(h_2)} n_2) = h_1 h_2 n_1^{\alpha(h_2)} n_2 \overset{(2)}{=} h_1 h_2 n_1 n_2 = \varphi(h_1, n_1) \cdot \varphi(h_2, n_2)$
- φ ist surjektiv: $\mathrm{Im}(\varphi) = HN = G$
- φ ist injektiv: $H \cap N = 1$

□

■ **Beispiel 5.12**
Sei $G = H \ltimes N$.

(a) $H = N = C_2$: $\mathrm{Aut}(N) = \{\mathrm{id}_{C_2}\} \Rightarrow \alpha \in \mathrm{Hom}(C_2, \mathrm{Aut}(C_2)) = 1$ (konstante Abbildung) $\Rightarrow G = H \ltimes_\alpha N = H \times N \cong C_2 \times C_2 \cong V_4$

(b) $H = C_2$, $N = C_3$: $\mathrm{Aut}(N) \cong (\mathbb{Z}/3\mathbb{Z})^\times \cong C_2 \Rightarrow \alpha \in \mathrm{Hom}(C_2, \mathrm{Aut}(C_3)) = \{\mathrm{id}_{C_2}, 1\} \Rightarrow H \ltimes_\alpha N = H \times N \cong C_6$ oder $H \ltimes_{\mathrm{id}_{C_2}} N \cong S_3$

6. Gruppenwirkungen

Sei G eine Gruppe und X eine Menge.

Definition 6.1 (Wirkung, G-Menge)
Eine (rechts-)Wirkung von G auf X ist eine Abbildung

$$\begin{cases} X \times G \to X \\ (x, g) \mapsto x^g \end{cases}$$

mit $x \in X$ und $h, g \in G$, wobei

- (W1): $x^{1_G} = x$
- (W2): $(x^g)^h = x^{gh}$

Eine G-Menge ist eine Menge X zusammen mit einer Wirkung von G auf X.

Beispiel 6.2

(a) Die symmetrische Gruppe $G = \mathrm{Sym}(X)$ wirkt auf X durch $x^\sigma = \sigma(x)$ mit $x \in X$, $\sigma \in G$. So wirkt zum Beispiel S_n auf $X = \{1, ..., n\}$.

(b) G wirkt auf $X = G$ durch Multiplikation $x^g = xg$, die sogenannte reguläre Darstellung von G.

(c) G wirkt auf $X = G$ durch Konjugation: $x^g = g^{-1}xg$.

(d) G wirkt auf der Menge $\mathrm{UG}(G)$ der Untergruppen von G durch Konjugation $H^g = \{h^g \mid h \in H\}$ mit $H \leq G$.

(e) Sind H, N Gruppen, so liefert jedes $\alpha \in \mathrm{Hom}(H, \mathrm{Aut}(N))$ eine Wirkung von H auf N durch $n^h = n^{\alpha(h)}$.

(f) Ist K ein Körper, so wirkt $K^\times$ auf K durch $x^y = xy$ mit $x \in K$ und $y \in K^\times$.

(g) Ist K ein Körper, $n \in \mathbb{N}$, so wirkt $\mathrm{GL}_n(K)^{op}$ auf K^n durch Multiplikation $x^A = Ax$

Anmerkung
^{op} ist nötig, weil die Multiplikation “falsch herum“ definiert wurde. g) wäre ein Beispiel für eine Linkswirkung, also ist es dann mit ^{op} eine Rechtswirkung.

Beispiel

The additive group of the real numbers $(\mathbb{R}, +)$ acts on the phase space $V = \mathbb{R}^3$ of “well-behaved” systems in classical mechanics (and in more general dynamical systems) by time translation: if t is in $\mathbb{R}$ and x is in the phase space, then x describes a state of the system, and $t + x$ is defined to be the state of the system t seconds later if t is positive or $-t$ seconds ago if t is negative.

▶ **Bemerkung 6.3**
Wirkt G auf X, so ist für jedes $g \in G$ die Abbildung

$$\sigma_g : \begin{cases} X \to X \\ x \mapsto x^g \end{cases}$$

bijektiv, da $\sigma_g \circ \sigma_{g^{-1}} = \sigma_{g^{-1}} \sigma_g = \sigma_1 = \mathrm{id}_X$, also $\sigma_g \in \mathrm{Sym}(X)$ und

$$\begin{cases} G \to \mathrm{Sym}(G) \\ g \mapsto \sigma_g \end{cases}$$

ist ein Gruppenhomomorphismus. Umgekehrt liefert jeder Homomorphismus $\sigma : G \to \mathrm{Sym}(G)$ eine Wirkung von G auf X durch $x^g = x^{\sigma(g)}$. Somit steht die Menge der Wirkungen von G auf X in natürlicher Bijektion zu $\mathrm{Hom}(G, \mathrm{Sym}(X))$.

Definition 6.4 (Fixpunkt, Stabilisator, Bahn, Bahnraum, G-invariant, treu, transitiv, frei)
Sei X eine G-Menge, $g_0 \in G$, $x_0 \in X$

(a) x_0 ist ein Fixpunkt von $g_0 \Leftrightarrow x_0^{g_0} = x_0$

(b) $\mathrm{Fix}(G) = X^G = \{x \in X \mid x^g = x \quad \forall g \in G\}$, die Menge der Fixpunkte von X unter G

(c) $G_{x_0} = \mathrm{Stab}(x_0) = \{g \in G \mid x_0^g = x\}$ der Stabilisator von x_0 in G

(d) $x_0^G = \{x_0^g \mid g \in G\}$, die Bahn von x_0 unter G

(e) $X/G = \{x^G \mid x \in X\}$, der Bahnenraum

(f) $Y \leq X$ ist G-invariant $\Leftrightarrow Y^g = \{y^g \mid y \in Y\} \leq Y$

(g) Die Wirkung von G auf X ist

- treu, wenn $\bigcap_{x \in X} G_x = 1$
- transitiv, wenn gilt: $\forall x, y \in X \exists g \in G$: $x^g = y$
- frei, wenn $G_x = 1$ für alle $x \in X$

▶ **Bemerkung 6.5**

(a) Der Stabilisator G_{x_0} besteht aus den $g \in G$, die x_0 als Fixpunkt haben.

(b) Die Wirkung von G auf X ist

- transitiv, wenn es nur eine Bahn gibt, also $|X/G| = 1$
- frei, wenn kein $1 \neq g \in G$ einen Fixpunkt hat
- treu, wenn kein $1 \neq g \in G$ alle $x \in X$ als fixiert

■ **Beispiel 6.6**
Für $n > 1$ wirkt $G = S_n$ auf $X = \{1, ..., n\}$ transitiv, treu, aber für $n \geq 3$ nicht frei. Der Stabilisator G_n von $n \in X$ ist eine Untergruppe von S_n isomorph zu S_{n-1}.

■ **Beispiel 6.7**

Die reguläre Darstellung von G auf $X = G$ ist frei und transitiv:

- frei: $x^g = x \Rightarrow xg = x \Rightarrow g = 1$
- transitiv: $x, y \in X = G \Rightarrow$ für $g = x^{-1}y$ ist $x^g = y$

Lemma 6.8

Sei X eine G-Menge.

(a) Für $x \in X$ ist $G_x \leq G$.

(b) Für $x, y \in X$ ist $x^G = y^G$ oder $x^G \cap y^G = \emptyset$.

(c) $\bigcap_{x\in X} = \mathrm{Ker}(\sigma)$, $\sigma : G \to \mathrm{Sym}(X)$ wie in Bemerkung 6.3

(d) Für $x \in X$ und $g \in G$ ist $G_{x^g} = (G_x)^g$

Beweis. Seien $x, y \in X$, $g, h \in G$

(a) Sei $x^g = x$ und $x^h = x$. Dann

$$\begin{aligned} x^{g^h} &= (x^g)^h = x^h = x \Rightarrow gh \in G_x \\ x^{g^{-1}} &= (x^g)^{g^{-1}} = x^1 = x' g^{-1} \in G_x \end{aligned}$$

(b) $x^g = y^h \Rightarrow x^G = (x^g)^G = (y^h)^H = y^H$

(c) $g \in \bigcap_{x\in X} G_x \Rightarrow \forall x \in X$: $x^g = x \Leftrightarrow \sigma_g = \sigma(g)\,\mathrm{id}_X$

(d) $h \in G_{x^g} \Leftrightarrow (x^g)^h = x^g \Leftrightarrow x^{ghg^{-1}} = x \Leftrightarrow h^{g^{-1}} \in G_x \Leftrightarrow h \in (G_x)^g$ □

Satz 6.9 (Cayley)

Ist $n = \#G < \infty$, so ist G isomorph zu einer Untergruppe der S_n.

Beweis. Betrachte die reguläre Darstellung $\sigma : G \to \mathrm{Sym}(G)$. Da diese Wirkung frei ist (Beispiel 6.7), also insbesondere treu, ist σ injektiv (Lemma 6.8 c), somit $G \cong \mathrm{Im}(\sigma) \leq \mathrm{Sym}(G)$. Eine Aufzählung $G = \{g_1, ..., g_n\}$ liefert einen Isomorphismus

$$\varphi : \begin{cases} S_n \to \mathrm{Sym}(X) \\ \tau \mapsto (g_i \mapsto g_{\tau(i)}) \end{cases}$$

und somit ist $G \cong \varphi^{-1}(\mathrm{Im}(\sigma)) \leq S_n$. □

Lemma 6.10

Für eine G-Menge X und $x \in X$ ist

$$\varphi : \begin{cases} {}_{G_x}\backslash^{G} \to x^G \\ G_x g \mapsto x^g \end{cases}$$

eine Bijektion.

Beweis.
- φ wohldefiniert: $G_x g = G_x g' \Rightarrow g' = gh$ mit $h \in G_x \Rightarrow x^{g'} = x^{hg} = x^g$
- φ surjektiv: klar
- φ injektiv: $x^g = x^{g'} \Leftrightarrow x = x^{g' g^{-1}} \Leftrightarrow g' g^{-1} \in G_x \Leftrightarrow g' \in G_x g \Leftrightarrow G x'_g = G_x g$ □

Satz 6.11 (Bahn-Stabilisator-Satz)
Sei X eine G-Menge, $x \in X$. Dann ist

$$\# x^G = (G : G_x)$$

Beweis. Lemma 6.10 □

■ **Beispiel**

Da bei Prof Fehm, die Verbindung zwischen Algebra und Geometrie keine Beachtung geschenkt wird, hier mal ein sehr anschauliches Beispiel von Wikipedia.
One can use the orbit-stabilizer theorem Satz 6.11 to count the automorphisms of a graph. Consider the cubical graph, and let G denote its automorphism group. Then G acts on the set of vertices $\{1, 2, \ldots, 8\}$, and this action is transitive as can be seen by composing rotations about the center of the cube. Thus, by the orbit-stabilizer theorem, we have that $|G| = |G \cdot 1||G_1| = 8|G_1|$. Applying the theorem now to the stabilizer G_1, we obtain $|G_1| = |(G_1) \cdot 2||(G_1)_2|$. Any element of G that fixes 1 must send 2 to either 2, 4 or 5. There are such automorphisms; consider for example the map that transposes 2 and 4, transposes 6 and 8, and fixes the other vertices. Thus, $|(G_1) \cdot 2| = 3$. Applying the theorem a third time gives $|(G_1)_2| = |((G_1)_2) \cdot 3||((G_1)_2)_3|$. Any element of G that fixes 1 and 2 must send 3 to either 3 or 6, and one easily finds such automorphisms. Thus, $|((G_1)_2) \cdot 3| = 2$. One also sees that $((G_1)_2)_3$ consists only of the identity automorphism, as any element of G fixing 1, 2 and 3 must also fix 4 and consequently all other vertices. Combining the preceding calculations, we now obtain $|G| = 8 \cdot 3 \cdot 2 \cdot 1 = 48$.

Folgerung 6.12 (Bahngleichung)
Ist X eine G-Menge und $X = \biguplus_{i=1}^{n} x_i^G$ die Zerlegung von X in Bahnen (vgl. Lemma 6.8 c) so ist

$$\# X = \sum_{i=1}^{n} (G : G_i)$$

Definition 6.13 (Zentralisator, Normalisator)

(a) Für $h \in H$ ist

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

der Zentralisator von h.

(b) Für $H \leq G$ ist

$$N_G(h) = \{g \in G \mid gH = Hg\}$$

der Normalisator von H.

▶ **Bemerkung 6.14**

(a) Der Zentralisator von h ist der Stabilisator von h unter der Wirkung von G auf $X = G$ durch Konjugation (Beispiel 6.2 c). Es ist die größte Untergruppe H mit $h \in \mathrm{Z}(h)$.

(b) Der Normalisator von $H \leq G$ ist der Stabilisator von H unter der Wirkung von G auf $X = \mathrm{UG}(G)$ durch Konjugation (Beispiel 6.2 d). Dies ist die größte Untergruppe N von G mit $H \trianglelefteq N$.

Folgerung 6.15
Für $h \in G$ und $H \leq G$ ist $C_G(h) \leq G$ und $H \trianglelefteq N_G(H) \leq G$ und

(a) $(G : C_G(h))$ ist genau die Anzahl der zu h konjugierten Elemente von G

(b) $(G : N_G(H))$ ist genau die Anzahl der zu H konjugierten Untergruppen von G

Beweis. Satz 6.11 □

Folgerung 6.16 (Klassengleichung)
Sei G endlich mit Zentrum $Z = \mathrm{Z}(G)$ und sei $x_1, ..., x_n$ ein Repräsentantensystem der Konjugationsklassen in $G \setminus Z$. Dann ist

$$\#G = \#Z + \sum_{i=1}^{n} (G : C_G(x_i))$$

Beweis. aus Satz 6.11 und Folgerung 6.15, da $G = Z \uplus G \setminus Z = Z \uplus \biguplus_{i=1}^{n} x_i^G$. □

7. p-Gruppen

Sei G eine endliche Gruppe und p eine Primzahl.

Definition 7.1 (p-Gruppe)
G ist eine $\underline{p\text{-Gruppe}}$ $\Leftrightarrow \#G = p^n$ für ein $n \in \mathbb{N}_0$.

Satz 7.2
Sei G eine p-Gruppe und X eine endliche G-Menge. Dann ist

$$\#\operatorname{Fix}_X(G) \equiv \#X \mod p$$

Beweis. Sei $x \in X$.

- $x \in \operatorname{Fix}_X(G) \Rightarrow (G : G_x) = 1$
- $x \notin \operatorname{Fix}_X(G) \Rightarrow 1 \neq (G : G_x) \mid \#G = p^n \Rightarrow (G : G_x) \equiv 0 \mod p$
- Ist $X = \biguplus_{i=1}^n x_i^G$, so ist

$$\#X = \sum_{i=1}^n (G : G_i) \equiv \#\operatorname{Fix}_X(G) \mod p$$ □

Folgerung 7.3 (Satz von Cauchy)
Teilt p die Ordnung von G, so hat G ein Element der Ordnung p.

Beweis. Sei $X = \{g_1, ..., g_p \in G^p \mid g_1 \cdot ... \cdot g_p = 1\}$. Es ist $\#X = (\#P)^{p-1}$ und $C_p = \langle (1\,2 \ldots p) \rangle \leq S_p$ wird auf X durch $(g_1, ..., g_p)^\sigma = (g_{\sigma(1)}, ..., g_{\sigma(p)})$ beschrieben. Mit Satz 7.2 gilt:

$$\#\operatorname{Fix}_X(C_p) \equiv \#X \equiv (\#G)^{p-1} \equiv 0 \mod p$$

Da $(1, ..., 1) \in \operatorname{Fix}_X(C_p)$ folgt $\#\operatorname{Fix}_X(C_p) \geq p \geq 2$, es existiert also $1 \neq g \in G$ mit $(g, ..., g) \in X$, das heißt $\operatorname{ord}(g) = p$. □

Folgerung 7.4
Jede nicht-triviale p-Gruppe hat eine nicht-triviales Zentrum.

Beweis. Betrachte Wirkung von G auf $X = G$ durch Konjugation (Beispiel 6.2 c). Dann

$$\#\operatorname{Z}(G) \equiv \operatorname{Fix}_X(G) \overset{7.2}{\equiv} \#G \equiv 0 \mod p$$

insbesondere ist $\operatorname{Z}(G) \neq 1$. □

Lemma 7.5
$\#G = p \Rightarrow G$ ist zyklisch.

Beweis. Sei $1 \neq g \in G \Rightarrow 1 \neq \operatorname{ord}(g) \mid \#G \Rightarrow \operatorname{ord}(g) = p \Rightarrow G = \langle g \rangle$ ist zyklisch. □

Lemma 7.6
${}^{G}/_{\operatorname{Z}(G)}$ zyklisch $\Rightarrow G$ ist abelsch.

Beweis. Sei $a \in G$ mit ${}^{G}/_{\mathrm{Z}(G)} = \langle a\,\mathrm{Z}(G)\rangle$. Dann ist

$$G = \bigcup_{k\in\mathbb{Z}} a^k\,\mathrm{Z}(G).$$

Sind nun $x, y \in G$, so ist $x = a^k c$, $y = a^l d$ mit $k, l \in \mathbb{Z}, c, d \in \mathrm{Z}(G) \Rightarrow x \cdot y = a^k c \cdot a^l d = a^l d \cdot a^k c = y \cdot x$ □

Satz 7.7
Ist $\#G = p^2$, so ist G abelsch.

Beweis. Nach Folgerung 7.4 ist $\mathrm{Z}(G) \neq 1$. $\Rightarrow \#{}^{G}/_{\mathrm{Z}(G)} \mid p \overset{7.5}{\Longrightarrow} {}^{G}/_{\mathrm{Z}(G)}$ ist zyklisch $\overset{7.6}{\Longrightarrow} G$ ist abelsch. □

▶ Bemerkung 7.8

Mit dem Struktursatz Theorem 4.8 erhalten wir

$$\begin{aligned} \#G = p &\Rightarrow G \cong \mathbb{Z}/p\mathbb{Z} \\ \#G = p^2 &\Rightarrow G \cong \mathbb{Z}/p^2\mathbb{Z} \text{ oder } G \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \end{aligned}$$

Satz 7.9
Ist $\#G = p^k$ und $l \leq k$, so gibt es $H \leq G$ mit $\#H = p^l$.

Beweis. Induktion nach l:
$\underline{l = 0}$: trivial Untergruppe!
$\underline{l - 1 \to l}$: Nach 7.4 ist $\#\,\mathrm{Z}(G) = p^a, a > 0$, nach Folgerung 7.3 (Cauchy) existiert somit ein $g \in \mathrm{Z}(G)$ mit $\mathrm{ord}(g) = p$. Da $g \in \mathrm{Z}(G)$ ist $\langle g\rangle \trianglelefteq G$ und $\#{}^{G}/_{\langle g\rangle} = p^{k-1}$. Nach Induktionshypothese ist Untergruppe $H_0 \leq {}^{G}/_{\langle p\rangle}$ mit $\#H_0 = p^{l-1}$. Betrachte den hom $\pi_{\langle g\rangle} : G \to {}^{G}/_{\langle p\rangle} \Rightarrow H := \pi_{\langle g\rangle}^{-1}(H_0) \leq G$, $\#H = \#\,\mathrm{Ker}(\pi_{\langle g\rangle}) \cdot \#H_0 = p \cdot p^{l-1} = p^l$. □

8. Die Sylow-Sätze

Sei G eine endliche Gruppe und $p \in \mathbb{N}$ prim .

Definition 8.1 (p-Sylow-Untergruppe)
Sei $H \leq G$.

(a) H ist p-SYLOW-Untergruppe von G (oder p-SYLOWgruppe von G) $\Leftrightarrow$ H ist p-Gruppe und $p \nmid (G : H)$

(b) $\mathrm{Syl}_p(G) = \{H \leq G \mid H \text{ ist } p\text{-SYLOWgruppe von } G\}$

▶ **Bemerkung 8.2**
Schreibe $\#G = p^k \cdot m$ mit $p \nmid m$. Dann gilt für $H \leq G$. $H \in \mathrm{Syl}_p(G) \Leftrightarrow \#H = p^k$.

■ **Beispiel 8.3**

(a) $\mathrm{Syl}_3(S_3) = \{A_3\}$

(b) $\mathrm{Syl}_2(S_3) = \{\langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle\}$

(c) $\mathrm{Syl}_2(S_4) \ni D_4$

Satz 8.4
Es gilt $\mathrm{Syl}_p(G) \neq \emptyset$.

Beweis. Induktion nach $n := \#G = p^k \cdot m$, $p \nmid m$.
$\underline{n = 1}$: $1 \in \mathrm{Syl}_2(1)$!
$\underline{n > 1}$: Ist $p \nmid n$, so ist $1 \in \mathrm{Syl}_p(G)$. Sei also $k \geq 1$.

- **1. Fall:** Es existiert $H \lneqq G$ mit $p \nmid (G : H)$. Nach Induktionshypothese existiert $S \in \mathrm{Syl}_p(H)$. Da $p \nmid (G : S) = (G : H)(H : S)$ ist $S \in \mathrm{Syl}_p(G)$.
- **2. Fall:** Es ist $p \mid (G : H)$ für alle $H \lneqq G$. Nach Klassengleichung Folgerung 6.16 ist $0 \equiv n = \#\mathrm{Z}(G) + \sum_{i=1}^r (G : C_G(x_i)) = \mathrm{ord}\,\mathrm{Z}(G) \mod p$, wobei $G \setminus \mathrm{Z}(G) = \biguplus_{i=1}^r x_i^G$, also $p \mid \#\mathrm{Z}(G)$. Nach Folgerung 7.3 (CAUCHY) existiert ein $g \in \mathrm{Z}(G)$ mit $\mathrm{ord}(g) = p$. $\Rightarrow$ $N := \langle g \rangle \trianglelefteq G$, $\#N = p$, $\#G/N = p^{k-1}m$. Nach Induktionshypothese existiert $\overline{S} \in \mathrm{Syl}_p(G/N)$, das heißt $\overline{S} = p^{k-1}$. Setze $S := \pi_N^{-1}(\overline{S}) \leq G$. Dann ist $\#S = \#\mathrm{Ker}(\pi_N)\#\overline{S} = p \cdot p^{k-1} = p^k$, das heißt $S \in \mathrm{Syl}_p(G)$. □

Folgerung 8.5
Ist $k \in \mathbb{N}$ mit $p^k \mid \#G$, so existiert $H \leq G$ mit $\#H = p^k$.

Beweis. Satz 8.4 und Satz 7.9. □

Theorem 8.6 (Sylow-Sätze)
Sei G eine endliche Gruppe.

(a) Jede p-Gruppe $H \leq G$ ist in einer $p-$SYLOWgruppe von G enthalten.

(b) Je zwei p-SYLOWgruppen von G sind konjugiert.

(c) Für die Anzahl $s_p := \#\operatorname{Syl}_p(G)$ gilt

$$s_p = (G : N_G(S)) = 1 \mod p$$

wobei $S \in \operatorname{Syl}_p(G)$ beliebig.

Beweis. Fixiere $S_0 \in \operatorname{Syl}_p(G)$. Definiere $X = \{S_0^g \mid g \in G\} \subseteq \operatorname{Syl}_p(G)$.

- **Behauptung 1** $p \nmid \#X$: Wirkung von G auf X durch Konjugation ist transitiv und $G_{S_0} = N_G(S_0) \trianglelefteq S_0$. Dann

$$\#X = \#S_0^G \overset{6.11}{=} (G : G_{S_0}) \mid (G : S_0)$$

und $p \nmid (G : S_0)$, somit $p \nmid \#X$.

- **Behauptung 2** $H \leq G$ p-Gruppe, $S \in \operatorname{Fix}_X(H) \Rightarrow H \leq S$: Sei $G_0 = N_G(S)$. Dann:
  - $S \trianglelefteq G_0$, $H \leq G_0 \Rightarrow S \trianglelefteq HS \leq G_0 \leq G$
  - ${}^{HS}/_{S} \cong {}^{H}/_{H\cap S}$ ist p-Gruppe, da H p-Gruppe und S p-Gruppe $\Rightarrow HS$ ist p-Gruppe
  - $p \nmid (G : S) \Rightarrow (HS : S) \mid (G : S) \Rightarrow p \nmid (HS : S) \Rightarrow (HS : S) = 1$, also $HS = S$ und damit $H \leq S$.

Jetzt zu den Beweisen der SYLOW-Sätze.

(a) Sei $H \leq G$ p-Gruppe.

$$\#\operatorname{Fix}_X(H) \overset{7.2}{\equiv} \#X \not\equiv 0 \mod p$$

Also existiert $S = S_0^g \in \operatorname{Fix}_X(H)$. Mit Behauptung 2 folgt $H \leq S \in \operatorname{Syl}_p(G)$.

(b) Sei $H \in \operatorname{Syl}_p(G)$. Nach dem Beweis von (a) ist $H \leq S_0^g$ für ein $g \in G$. Also $H = S_0^g$ ist konjugiert zu S_0.

(c) Nach (b) ist $\operatorname{Syl}_p(G) = X$, also

$$s_p = \#X = (G : N_G(S_0))$$

Es ist $S_0 \in \operatorname{Fix}_X(S_0)$ und für $S \in \operatorname{Fix}_X(S_0)$ ist $S_0 \leq S$, also $S_0 = S$ nach Behauptung 2, das heißt es gibt genau einen Fixpunkt. Es folgt $\#\operatorname{Fix}_X(S_0) = 1$ und deshalb

$$s_p = \#X \overset{7.2}{\equiv} \#\operatorname{Fix}_X(S_0) \equiv 1 \mod p$$

□

Folgerung 8.7
Sei $S \in \operatorname{Syl}_p(G)$. Genau dann ist $S \trianglelefteq G$, wenn $s_p = 1$.

■

Folgerung 8.8
Schreibe $\#G = p^k m$, $p \nmid m$. Dann gilt

$$s_p \mid m \text{ und } p \mid s_p - 1$$

■ **Beispiel 8.9**
Sei $\#G = pq$, mit Primzahlen $p < q$. Wähle $P \in \mathrm{Syl}_p(G)$, $Q \in \mathrm{Syl}_q(G)$.

- $s_q \mid p$ und $q \mid s_q - 1 \overset{p<q}{\Longrightarrow} s_q = 1 \overset{8.7}{\Longrightarrow} Q \trianglelefteq G. \Rightarrow G = P \ltimes Q$ (denn $P \cap Q = 1$ und $PQ = G$).
- $s_p \mid q$ und $q \mid s_q - 1 \Rightarrow s_p = 1$ oder ($s_p = q$ und $q \equiv 1 \mod p$)
  - **1. Fall** mit $q \neq 1 \mod p$: Dann ist $s_p = 1 \Rightarrow P \trianglelefteq G \Rightarrow G = P \times Q \cong C_p \times C_q \cong C_{pq}$
  - **2. Fall** mit $q = 1 \mod p$: $\mathrm{Aut}(Q) \cong \mathrm{Aut}(C_q) \overset{4.14}{\cong} C_{q-1}$ hat genau eine Untergruppe mit Ordnung p, also ist $\mathrm{Hom}(P, \mathrm{Aut}(Q)) \neq 1$. Es kann deshalb entweder $G = P \ltimes Q = P \times Q \cong C_{pq}$ abelsch oder $G = P \ltimes Q \cong C_p \ltimes_\alpha C_q$ mit $\alpha \neq 1$ nicht abelsch geben, z.B. $S_3 \cong C_2 \ltimes_\alpha C_3$.

9. Einfache Gruppen

Sei G eine Gruppe und $n \in \mathbb{N}$.

Definition 9.1 (Einfache Gruppe)
Eine Gruppe G heißt einfach , wenn $G \neq 1$ und es kein $1 \neq N \ntrianglelefteq G$ gibt.

► Bemerkung 9.2
Die einfachen Gruppen sind die grundlegenden "Bausteine" der Gruppen, siehe Kapitel 1.10.

■ Beispiel 9.3

(a) C_n ist einfach $\Leftrightarrow$ n ist prim, da dann $\# C_n$ keine weiteren Teiler hat, also auch keine Untergruppen

(b) Sei G endlich abelsch. Dann: G ist einfach $\Leftrightarrow G \cong C_p$, p prim

(c) Sei G eine p-Gruppe. Dann: G ist einfach $\overset{7.4}{\Longleftrightarrow} G \cong C_p$, p prim

(d) $A_2 = \{\mathrm{id}\}$ und damit einfach

(e) A_3 ist einfach, da $A_3 \cong C_3$

(f) A_4 ist nicht einfach (da $V_4 \trianglelefteq A_4$ gilt)

Definition 9.4 (Typ)
Sei $\sigma \in S_n$. Ist $\sigma = \sigma_1 \cdots \sigma_k$ eine Zerlegung in paarweise disjunkte Zykel σ_i mit $\mathrm{ord}(\sigma_i) = r_i$, wobei $r_1 \geq r_2 \geq \cdots \geq r_k \geq 2$, so heißt

$$\mathrm{Typ}(\sigma) := (r_1, \ldots, r_k, \underbrace{1, \ldots, 1}_{=\#\,\mathrm{Fix}(\sigma)})$$

der Typ von σ.

■ Beispiel 9.5
Sei $\sigma = (12)(25) \in S_5$. Die Zykelzerlegung ist $\sigma = (1\,5\,2)$. Also ist $\mathrm{Typ}(\sigma) = (3, 1, 1)$. Die beiden Fixpunkte sind 3 und 4.

Definition 9.6 (Partition)
Eine Partition von n ist eine endliche Folge $(r_1, \ldots, r_k)$ mit $r_1, \ldots, r_k \in \mathbb{N}$, $r_1 \geq \cdots \geq r_k$ und $n = \sum_{i=1}^k r_i$.

Lemma 9.7
$\{\mathrm{Typ}(\sigma) \mid \sigma \in S_n\}$ ist genau die Menge der Partitionen von n.

Beweis.

- Hinrichtung: klar
- Rückrichtung: Ist $(r_1, ..., r_k)$ eine Partition von n, so ist $(r_1, ..., r_k) = \mathrm{Typ}(\sigma)$ für

$$\sigma = (1 \ldots r_1)(r_1 + 1 \ldots r_1 + r_2)\ldots(1 + \sum_{i=1}^{k-1} r_i \ldots n)$$

□

Satz 9.8
Für $\sigma, \sigma' \in S_n$ sind äquivalent:

(a) σ, σ' sind konjugiert in S_n.

(b) $\mathrm{Typ}(\sigma) = \mathrm{Typ}(\sigma')$

Beweis. Schreibe $\sigma = \sigma_1 ... \sigma_k$ paarweise disjunkte Zykel, $r_\nu = \mathrm{ord}(\sigma_\nu)$, $r_1 \geq ... \geq r_k$, $\sigma_\nu = (i_{\nu,1} \dots i_{\nu,r_\nu})$, $\{1, ..., n\} = \{i_{\nu,\mu} \mid \nu, \mu\}$

- (a) $\Rightarrow$ (b): Ist $\sigma' = \sigma^\tau$ mit $\tau \in S_n$, so ist

$$\sigma^\tau = \sigma_1^\tau ... \sigma_k^\tau \quad \text{und} \quad \sigma_\nu^\tau = (i_{\nu,1}^\tau \dots i_{\nu,r_\nu}^\tau)$$

  Insbesondere $\mathrm{Typ}(\sigma) = \mathrm{Typ}(\sigma')$.

- (b) $\Rightarrow$ (a): Ist $\mathrm{Typ}(\sigma) = \mathrm{Typ}(\sigma')$, so ist $\sigma' = \sigma_1' ... \sigma_k'$ mit paarweise disjunkten Zykeln mit $\mathrm{ord}(\sigma_\nu') = r_\nu$ und $\sigma_\nu' = (i_{\nu,1}' \dots i_{\nu,r_\nu}')$ und deshalb wieder $\{1, ..., n\} = \{i_{\nu,\mu}' \mid \nu = 1, ..., k, \mu = 1, ..., r_\nu\}$. Mit $\tau \in S_n$ definiert durch

$$i_{\nu,\mu}^\tau = i_{\nu,\mu}'$$

  ist dann $\sigma^\tau = \sigma_1^\tau ... \sigma_k^\tau$ mit $\sigma_\nu^\tau = (i_{\nu,1}^\tau \dots i_{\nu,r_\nu}^\tau) = (i_{\nu,1}' \dots i_{\nu,r_\nu}') = \sigma_\nu'$. □

Lemma 9.9
Ist $n \geq 5$, so sind je zwei 3-Zykel konjugiert in A_n.

Beweis. Seien $\sigma = (i_1\, i_2\, i_3)$ und $\sigma' = (i_1'\, i_2'\, i_3')$. Nach Satz 9.8 existiert $\tau \in S_n$ mit $\sigma' = \sigma^\tau$. Ist $\tau \in A_n$, so sind wir fertig. Andernfalls gibt es wegen $n \geq 5$ $j_1 \neq j_2 \in \{1, ..., n\} \setminus \{i_1', i_2', i_3'\}$. Dann ist $\tau(j_1, j_2) \in A_n$ und

$$\sigma^{\tau(j_1,j_2)} = (\sigma^\tau)^{(j_1,j_2)} = (\sigma')^{(j_1,j_2)} = \sigma'$$

□

Lemma 9.10
Ist $n \geq 3$ wird A_n von den 3-Zykeln erzeugt.

Beweis. Sei $\sigma \in A_n$. Schreibe $\sigma = \tau_1 \dots \tau_{2r}$ mit Transpositionen $\tau_1, \dots, \tau_{2r} \in S_n$ (siehe Definition 1.11). Es genügt zu zeigen, dass $\tau_1\tau_2$ Produkt ist von 3-Zykeln. Ohne Einschränkung sei $\tau_1 = (1\,2)$.

- $\tau_2 = (1\,2) = \tau_1$: $\tau_1\tau_2 = (1\,2\,3)(2\,1\,3)$
- $\tau_2 = (1\,k)$ für ein $k > 2$: $\tau_1\tau_2 = (1\,2\,k)$
- $\tau_2 = (2\,k)$ für ein $k > 2$: analog
- $\tau_2 = (k\,l)$ für $l > k > 2$: $\tau_1\tau_2 = (1\,k\,l)(1\,k\,2)$ □

Theorem 9.11
Für $n \geq 5$ ist A_n einfach.

Beweis. Sei $1 \neq N \trianglelefteq A_n$. Enthält N ein 3-Zykel, somit nach Lemma 9.9 schon alle 3-Zykel, daraus folgt mit Lemma 9.10 $N = A_n$. Sei $1 \neq \sigma \in N$ ist mit Zykelzerlegung $\sigma = \sigma_1 \dots \sigma_k$.

- **Fall 1:** Zykelzerlegung enthält 2 Transpositionen, etwa $\sigma_1 = (1\,2)$, $\sigma_2 = (3\,4)$
  $\Rightarrow \sigma' := \sigma^{(1\,2\,3)} = (1\,2\,3)^{-1}(1\,2)(3\,4)\sigma_3 \dots \sigma_k(1\,2\,3) = (2\,3)(1\,4)\sigma_3 \dots \sigma_k \in N$
  $\Rightarrow \sigma' \cdot \sigma^{-1} = (1\,3)(2\,4) \in N$
  $\Rightarrow \sigma'' := (\sigma'\sigma^{-1})^{(1\,5\,3)} = (1\,5)(2\,4) \in N$
  $\Rightarrow \sigma'\sigma^{-1}\sigma'' = (1\,3\,5) \in N$
- **Fall 2:** Zykelzerlegung von σ enthält Zykel der Länge $m \geq 4$, etwa $\sigma_1 = (1 \dots m)$
  $\Rightarrow \sigma' := \sigma^{(1\,2\,3)} = (2\,3\,1\,4\,5\,\dots\,m)\sigma_2\sigma_k \in N$
  $\Rightarrow \sigma^{-1}\sigma' := (2\,4\,1) \in N$
- **Fall 3:** Zykelzerlegung besteht aus 3-Zykeln, etwa $\sigma_1 = (1\,2\,3)$, $\sigma_2 = (4\,5\,6)$ ($\sigma_1 \cap \sigma_2 = \emptyset$) (dieser Fall existiert nur für $n \geq 6$)
  $\Rightarrow \sigma' := \sigma^{(2\,3\,4)} = (1\,3\,4)(2\,5\,6)\sigma \dots \sigma_k \in N$
  $\Rightarrow \sigma^{-1}\sigma' = (1\,4\,2\,3\,5) \in N$
  $\Rightarrow$ Fertig nach Fall 2! □

Folgerung 9.12
Für $n \neq 4$ hat S_n nur die Normalteiler 1, A_n, S_n.

Beweis. Sei $N \trianglelefteq S_n$.

- $n \leq 3$: klar mit V5 + Satz 9.8
- $n \geq 5$: $N \cap A_n \trianglelefteq A_n \overset{9.11}{\Longrightarrow} N \cap A_n \in \{1, A_n\}$
  - $N \cap A_n = A_n$: $A_n \leq N \leq S_n \xRightarrow{(S_n:A_n)=2} N \in \{A_n, S_n\}$
  - $N \cap A_n = 1$: $NA_n = N \times A_n \Rightarrow \#N \leq 2$, denn $\#N : \#A_n = \#NA_n \leq \#S_n = 2\#A_n$. Wäre $N \neq 1$, so existiert $1 \neq \sigma \in N$ mit $\mathrm{ord}(\sigma) = 2$, also $\mathrm{Typ}(\sigma) = (2, \dots, 2, 1, \dots, 1)$ im Widerspruch zu Satz 9.8, denn es existiert $1 \neq \sigma' \neq \sigma$ konjugiert zu σ, insbesondere $\sigma' \in N$, also ist $\#N \geq 3$. □

▶ Bemerkung 9.13

- Man kann zeigen, dass es keine nicht zyklische einfachen Gruppen der Ordnung $\#G < \#A_5 = 60$ gibt! (Kann mit den SYLOW-Sätzen (Theorem 8.6) gezeigt werden oder mit BURNSIDE's Lemma, welches wir in dieser Vorlesung nicht behandelt haben.)
- Die endlichen einfachen Gruppen sind vollständig klassifiziert:
  (a) C_p mit p prim
  (b) A_n mit $n \geq 5$
  (c) Einfache Gruppen von LIE-Typ
  (d) 26 "sporadische" einfache Gruppen (z.B. Monster Gruppe mit Ordnung ca. 10^{53})

10. Auflösbare Gruppen

Sei G eine endliche Gruppe.

Definition 10.1 (Normalreihe, Faktoren, Verfeinerung, Kompositionsreihe)

(a) Eine Normalreihe von G ist eine Folge von Untergruppen

$$G = G_0 \gneq G_1 \gneq \dots \gneq G_n = 1 \qquad (*)$$

Dabei ist n die Länge der Normalreihe, und die Quotienten ${}^{G_{i-1}}/_{G_i}$ heißen die Faktoren der Normalreihe.

(b) Eine Normalreihe $G_0, \dots, G_n$ von G ist eine Verfeinerung einer Normalreihe $H_0, \dots, H_m$ von G, wenn $i_1, \dots, i_m$ mit $H_j = G_{i_j} \forall j$ gibt.

(c) Eine Kompositionsreihe ist eine Normalreihe, die maximal bezüglich Verfeinerung ist.

▶ **Bemerkung 10.2**

(a) Für eine Normalreihe $(*)$ gilt nach Lemma 3.7 + Ü27: Genau dann ist ${}^{G_{i-1}}/_{G_i}$ einfach, wenn es kein $G_{i-1} \gneq N \gneq G_i$ mit $N \trianglerighteq G_{i-1}$ gibt. Das heißt, genau dann ist eine Normalreihe eine Kompositionsreihe, wenn alle ihre Faktoren einfach sind.

(b) Jede Normalreihe besitzt eine Verfeinerung, die eine Kompositionsreihe ist.

■ **Beispiel 10.3**

(a) S_3 hat eine Kompositionsreihe

$$S_3 > A_3 > 1$$

mit Faktoren ${}^{S_3}/_{A_3} \cong C_2$, ${}^{A_3}/_1 \cong C_3$.

(b) S_4 hat die Kompositionsreihe

$$S_4 > A_4 > V_4 > H = \langle (1\,2)(3\,4) \rangle > 1$$

mit Faktoren ${}^{S_4}/_{A_4} \cong C_2$, ${}^{A_4}/_{V_4} \cong C_3$, ${}^{V_4}/_H \cong C_2$ und ${}^H/_1 \cong C_2$.

(c) S_5 hat die Kompositionsreihe

$$S_5 > A_5 > 1$$

mit Faktoren ${}^{S_5}/_{A_5} \cong C_2$, ${}^{A_5}/_1 \cong A_5$ nach Theorem 9.11.

Theorem 10.4 (Jordan-Hölder)
Je zwei Kompositionsreihen von G haben die gleiche Länge und ihre Faktoren stimmen bis auf Isomorphie und Reihenfolge überein.

Beweis. Induktion über die minimale Länge n einer Kompositionsreihe: Seien

$$G = A_0 \gneq A_1 \gneq \cdots \gneq A_n = 1,$$
$$G = B_0 \gneq B_1 \gneq \cdots \gneq B_m = 1$$

$$\begin{tikzcd}
& A_1 \arrow[rr, no head] & & A_2 \arrow[rr, no head] & & \cdots \arrow[rr, no head] & & A_n \\
G \arrow[ur, no head] \arrow[dr, no head] & & N \arrow[ul, no head] \arrow[dl, no head] \arrow[rr, no head] & & N_1 \arrow[rr, no head] & & N_2 \arrow[rr, no head] & & \cdots \arrow[rr, no head] & & N_l \\
& B_1 \arrow[rr, no head] & & B_2 \arrow[rr, no head] & & \cdots \arrow[rr, no head] & & B_m
\end{tikzcd}$$

<u>$n = 0$:</u> $G = 1$ klar
<u>$n > 0$:</u> $G \neq 1 \Rightarrow m > 0$. Es ist $N = A_1 \cap B_1 \trianglelefteq G$, $A_1 B_1 \trianglelefteq G$

- **1. Fall:** $A_1 = B_1$: Behauptung aus Induktionshypothese für $N = A_1 = B_1$
- **2. Fall:** $A_1 \neq B_1$: Dann ist $A_1 \precneqq A_1 B_1 \trianglelefteq G$ und somit ist $A_1 B_1 = G$, denn G/A_1 ist einfach

$$G/A_1 = A_1B_1/A_1 \overset{3.10}{\cong} B_1/A_1 \cap B_1 = B_1/N$$
$$G/B_1 \cong A_1/N$$

Insbesondere sind A_1/N und B_1/N einfach. Sei $N = N_0 > N_1 > \cdots > N_l = 1$ Kompositionsreihe. Dann ist auch $A_1 > N > N_1 > \cdots > N_l$ ist Kompositionsreihe der Länge $l + 1$. Da $A_1 > A_2 > \cdots > A_n$ Kompositionsreihe minimaler Länge $n - 1$ ist. Es folgt aus der Induktionshypothese, dass $n - 1 = l + 1$ und dass die Faktoren übereinstimmen. Ebenso sind $B_1 > B_2 > \cdots > B_m$ und $B_1 > N_0 > N_1 > \cdots > N_l$ Kompositionsreihe mit Länge $m - 1$ und $l + 1$. Da $l + 1 = n - 1 < n$ folgt aus der Induktionshypothese, dass $l + 1 = m - 1$ und dass die Faktoren übereinstimmen. Also $m = l + 2 = n$ und $A_0 > \cdots > A_n$ und $B_0 > \cdots > B_n$ haben Faktoren $G/A_1 \cong B_1/N$, $A_1/N \cong G/B_2$, N/N_1, $N_1/N_2, \ldots, N_{l-1}/N_l$ □

Definition 10.5 (Kompositionsfaktoren, auflösbar)

(a) Die Faktoren einer Kompositionsreihe von G heißen die <u>Kompositionsfaktoren</u> von G.

(b) G ist <u>auflösbar</u>, wenn alle Kompositionsfaktoren von G zyklisch sind.

■ Beispiel 10.6

(a) S_3 hat Kompositionsfaktoren C_2, C_3: auflösbar

(b) S_4 hat Kompositionsfaktoren C_2, C_3, C_2, C_2: auflösbar

(c) S_n, $n \geq 5$ hat Kompositionsfaktoren C_2, A_n: nicht auflösbar

(d) G ist abelsch $\Longrightarrow G$ ist auflösbar (Beispiel 9.3c)

(e) G ist p-Gruppe $\Longrightarrow G$ ist auflösbar (Beispiel 9.3d))

(f) C_4 und V_4 haben Kompositionsfaktoren C_2 und C_2, aber $C_4 \ncong V_4$.

Lemma 10.7
Sei $N \trianglelefteq G$. Genau dann ist G auflösbar, wenn N und G/N auflösbar sind.

Beweis.
- Hinrichtung: Ist $N = N_0 > \cdots > N_l = 1$ Kompositionsreihe, so kann $G > N_0 > \cdots > N_l = 1$ zu einer Kompositionsreihe von G verfeinert werden, Kompositionsfaktoren von N sind die Kompositions-

faktoren von G. Somit ist N auflösbar. Ist ${}^{G}/_{H} = H_0 > \cdots > H_k$ Kompositionsreihe von ${}^{G}/_{N}$, so kann $G = \pi_N^{-1}(H_0) > \pi_N^{-1}(H_1) > \cdots > \pi_N^{-1}(H_k) = N > 1$ zu einer Kompositionsreihe verfeinert werden, die Kompositionsfaktoren von ${}^{G}/_{N}$ sind also Kompositionsfaktoren von G. Somit ist ${}^{G}/_{N}$ auflösbar.

- Rückrichtung: Sind $N = N_0 > \cdots > N_l$ und ${}^{G}/_{N} = H_0 > \cdots > H_k$ Kompositionsreihen, so ist $G = \pi_N^{-1}(H_0) > \cdots > \pi_N^{-1}(H_k) = N > N_1 > \cdots > N_l$ eine Kompositionsreihe von G und ist damit auflösbar. □

Satz 10.8
Für G sind äquivalent:

(a) G ist auflösbar.

(b) G hat eine Normalreihe mit zyklischen Faktoren.

(c) G hat eine Normalreihe mit abelschen Faktoren.

(d) G hat eine Normalreihe mit auflösbaren Faktoren.

Beweis.
- (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\overset{10.6}{\Longrightarrow}$ (d)
- (d) $\Rightarrow$ (a): Induktion über die Länge der Normalreihe mit Lemma 10.7 □

Definition 10.9 (Kommutator, Kommutatoruntergruppe)
Seien $x, y \in G$, $H, K \leq G$.

(a) $[x, y] := x^{-1}y^{-1}xy$, der Kommutator von x und y

(b) $[H, K] := \langle [h, k] \mid h \in H, k \in K \rangle$

(c) $G' := [G, G]$, die Kommutatoruntergruppe von G

▶ Bemerkung 10.10
Genau dann kommutieren x und y (also $xy = yx$), wenn $[x, y] = 1$. Es gilt $[x, y]^{-1} = [y, x]$.

Lemma 10.11
Ist $\varphi : G \to H$ ein Epimorphismus, so ist $\varphi(G') = H'$.

Beweis. Da $\varphi([x, y]) = [\varphi(x), \varphi(y)]$ ist

$$\begin{aligned}
\varphi(G') &= \varphi(\langle \{[x, y] \mid x, y \in H\} \rangle) \\
&= \langle \varphi(\{[x, y] \mid x, y \in G\}) \rangle \\
&= \langle \{[\varphi(x), \varphi(y)] \mid x, y \in G\} \rangle \\
&= \langle \{[x, y] \mid x, y \in H\} \rangle = H'
\end{aligned}$$ □

Lemma 10.12
G' ist der kleinste Normalteiler von G mit ${}^{G}/_{G'}$ abelsch.

Beweis.
- G' ist charakteristisch $\Rightarrow G' \trianglelefteq G$
- ${}^{G}/_{G'} = \pi_{G'}(G) \overset{10.11}{\Longrightarrow} ({}^{G}/_{G'})' = \pi_{G'}(G') = 1 \Rightarrow [x, y] = 1$ für alle $x, y \in {}^{G}/_{G'}$, das heißt ${}^{G}/_{G'}$ ist abelsch

- Sei $N \trianglelefteq G$ mit ${}^{G}/_{N}$ abelsch $\Rightarrow \pi_N(G') \overset{10.11}{=} ({}^{G}/_{N})' = 1 \Rightarrow G' \leq \mathrm{Ker}(\pi_N) = N$, das heißt G' ist der kleinste Normalteiler. □

Definition 10.13 (Kommutatorreihe)
Wir definieren die Kommutatorreihe

$$G = G^{(0)} \geq G^{(1)} \geq \dots$$

induktiv durch $G^{(0)} = G$ und $G^{(n+1)} = (G^{(n)})'$.

Satz 10.14
Ist $G_n \ntrianglelefteq \dots \ntrianglelefteq G_1 \ntrianglelefteq G_0 = G$ eine Normalreihe mit abelschen Faktoren (wir fordern ausnahmsweise nicht, dass $G_n = 1$), so ist $G^{(i)} \leq G_i$ für alle $i \leq n$. Insbesondere ist G genau dann auflösbar, wenn $G^{(n)} = 1$ für ein n.

Beweis. Induktion über n
$n = 0$: klar
$n - 1 \to n$: Nach Induktionshypothese ist $G^{(n-1)} \leq G_{n-1}$, ${}^{G_{n-1}}/_{G_n}$ abelsch $\Rightarrow G^{(n)} = (G^{(n-1)})' \leq (G_{n-1})' \overset{10.12}{\leq} G_n$.
Für den "Insbesondere"-Fall gilt:

- Hinrichtung: Kompositionsreihe $G = G_0 > G_1 > \dots G_n$ ist Normalreihe mit abelschen Faktoren $\Rightarrow G^{(n)} \leq G_n = 1 \Rightarrow G^{(n)} = 1$
- Rückrichtung: $G = G^{(0)} > G^{(1)} > \dots > G^{(n)} = 1$ mit n minimal ist Normalreihe mit abelschen Faktoren $\overset{10.8}{\Longrightarrow} G$ ist auflösbar. □

Folgerung 10.15
Ist G auflösbar und $H \leq G$, so ist auch H auflösbar.

Beweis. G auflösbar $\overset{10.14}{\Longrightarrow} G^{(n)} = 1$ für ein $n \Rightarrow H^{(n)} \leq G^{(n)} = 1 \Rightarrow H^{(n)} = 1 \overset{10.14}{\Longrightarrow} H$ auflösbar. □

▶ Bemerkung 10.16
Das kleinste n mit $G^{(n)} = 1$ heißt Stufe von G. (rank im englischen Sprachraum)

▶ Bemerkung 10.17
Es gelten die folgenden tiefen Sätze:

- Satz von Burnside: Ist $\#G = p^a q^b$ mit p, q prim, so ist G auflösbar.
- Satz von Feit-Thompson: Ist $\#G$ ungerade, so ist G auflösbar.

Kapitel II

Kommutative Ringe

1. Erinnerung und Beispiele

▶ **Erinnerung 1.1**

Ein Ring ist eine abelsche Gruppe $(R, +)$ zusammen mit einer Verknüpfung $\cdot : R \times R \to R$ die Assoziativität und Distributivität erfüllt. Eine Teilmenge $\emptyset \neq S \subseteq R$ ist ein Unterring oder Teilring von R, wenn S abgeschlossen unter Addition, Subtraktion und Multiplikation ist. Eine Abbildung $\varphi : R \to R^{'}$ zwischen Ringen ist ein Ringhomomorphismus , wenn $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$ und $\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$ und in diesem Fall ist

$$\ker(\varphi) = \varphi^{-1}(\{0\})$$

der Kern von φ.

▶ **Bemerkung 1.2**

In dieser Vorlesung bedeutet "Ring" immer kommutativer Ring mit Einselement, d.h. $(R, \cdot)$ bildet ein kommutativer Monoid mit Einselement 1_R. Wir fordern dann zusätzlich, dass Unterringe von R das Einselement von R enthalten und dass Ringhomomorphismen $\varphi : R \to R^{'}$ das Einselement von R auf das Einselement von $R^{'}$ abbilden.

■ **Beispiel 1.3**

1. Der Ring $\mathbb{Z}$ der ganzen Zahlen.
2. Der Restklassenring $\mathbb{Z}/n\mathbb{Z}$ für $n \in \mathbb{N}$.
3. Die Körper $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
4. Der Nullring $R = \{0\}$

Seien R, S Ringe. (Meisten Beweise sind LAAG1+2 Skript zu entnehmen!)

Satz 1.4

Ein Ringhomomorphismus $\varphi : R \to S$ ist ein Isomorphismus (d.h. bijektiv), wenn es einen Ringhomomorphismus $\psi : S \to R$ mit $\psi \circ \varphi = \mathrm{id}_R$ und $\varphi \circ \psi = \mathrm{id}_S$ gibt.

Satz 1.5

Ein Ringhomomorphismus $\varphi : R \to S$ ist genau dann injectiv, wenn $\ker(\varphi) = \{0\}$.

Definition 1.6
Für $x \in R$ heißt invertierbar oder eine Einheit, wenn es $y \in R$ mit $xy = 1$ gibt, und die $R^\times$ der Einheiten bildet eine Gruppe unter Multiplikation.
Für $x \in R$ ist eine Nullteiler, wenn es $0 \neq y \in R$ mit $xy = 0$ gibt, und R ist nullteilerfrei, wenn es keinen Nullteiler $0 \neq x \in R$ gibt.

Beispiel 1.7

1. $\mathbb{Z}$ ist nullteilerfrei, $\mathbb{Z}^\times = \mu_2 = \{\pm 1\}$.
2. $\mathbb{Z}/n\mathbb{Z}$ ist genau dann nullteilerfrei, wenn n prim ist.

Beispiel 1.8
Für eine Familie von Ringen $(R_i)_{i \in I}$ wird $\prod_{i\in\Lambda} R_i$ durch komponentenweise Addition und Multiplikation zu einem Ring, genannt das direkte Produkt der R_i. Bezeichnet 1_{R_i} das Einselement von R_i, so ist (1_{R_i}) das Einselement von $\prod_{i\in\Lambda} R_i$ und

$$\left(\prod_{i\in\Lambda} R_i\right)^\times = \prod_{i\in I} R_i$$

Beispiel 1.9
Der Polynomring eine Variablen x über R ist

$$R[x] = \left\{\sum_{i=0}^{\infty} a_i x^i \mid a_i \in R,\ \text{fast alle } a_i = 0\right\}$$

mit der Addition und Multiplikation

$$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$
$$\left(\sum_{i=0}^{\infty} a_i x^i\right) + \left(\sum_{j=0}^{\infty} b_j x^j\right) = \sum_{k=0}^{\infty} \left(\sum_{i+j=k}^{\infty} a_i b_j\right) x^k$$

Ist $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ mit $a_n \neq 0$, so ist $\deg(f) = n$ der Grad von f (mit $\deg(0) = -\infty$) und $\mathrm{LC}(f) = a_n$ der Leitkoeffizient von f, f heißt normiert, wenn $\mathrm{LC}(f) = 1$.

Satz 1.10
Seien $f, g \in R[x]$.

1. $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$
2. $\deg(f \cdot g) \leq \deg(f) + \deg(g)$
3. Ist $f \neq 0$ und $\mathrm{LC}(f)$ kein Nullteiler, so ist $\deg(fg) = \deg(f) + \deg(g)$.

Beweis. Siehe LAAG I.6.4. □

Folgerung 1.11
Ist R nullteilerfrei, so auch $R[x]$ und $(R[x])^\times = R^\times$.

Beweis.
- Ist $fg = 0$, so ist

$$-\infty = \deg(0) = \deg(fg) \overset{1.10}{=} \deg(f) + \deg(g)$$

folglich $f = 0$ oder $g = 0$.

- Ist $fg = 1$, so ist

$$0 = \deg(1) = \deg(fg) \overset{1.10}{=} \deg(f) + \deg(g)$$

folglich $\deg(f) = \deg(g) = 0$, d.h. $f, g \in R$. $\square$

Satz 1.12 (Universelle Eigenschaft des Polynomrings)
Ist $\varphi : R \to S$ ein Ringhomomorphismus und $s \in S$, so gibt es genau einen Ringhomomorphismus $\varphi_s : R[x] \to S$ mit

$$\varphi_s|_R = \varphi \text{ und } \varphi_s(x) = S$$

Beweis. Ist $R[x] \to S$ ein Ringhomomorphismus mit $\varphi_s|_R = \varphi$ und $\varphi_{s(x)} = S$, so ist

$$\varphi_s\left(\sum_{i\geq 0}^{\infty} a_i x^i\right) = \sum_{i=0}^{\infty} \varphi_s(a_i)\varphi_s(x^i) = \sum_{i\geq 0}^{\infty} \varphi(a_i)s^i$$

eindeutig bestimmt. Umgekehrt ist das so definierte φ_s ein Ringhomomorphismus (Übung), der $\varphi_s|_R$ und $\varphi_s(x) = s$ erfüllt. $\square$

▶ **Bemerkung 1.13**
Insbesondere hat man für $a \in R$ den Einsetzungshomomorphismus:

$$\varphi_a : \begin{cases} R[x] & \to R \\ f & \mapsto f(a) \end{cases}$$

gegeben durch $\varphi_a \mid_R = \mathrm{id}_R$ und $\varphi_a(x) = a$. Dies liefert eine Abbildung

$$\begin{cases} R[x] & \to \mathrm{Abb}(R, R) \\ f & \mapsto \tilde{f}, \tilde{f}(a) = \varphi_a(f) \end{cases}$$

Diese Abbildung ist im Allgemeinen <u>nicht injectiv</u>!!! Sei z.B. für $R = \mathbb{Z}/n\mathbb{Z}$ und $f = x^2 + x$ ist $f(0) = \bar{0}$, $f(\bar{1}) = \bar{0}$, aber $\tilde{f} = \tilde{0}$, aber $f \neq 0$.

Satz 1.14 (Polynomdivision)
Sei $0 \neq g \in R[x]$ mit $\mathrm{LC}(g) \in R^\times$. Zu jedem Polynom $f \in R[x]$ gibt es eindeutig bestimmte $q_1 r \in R[x]$ mit $f = qg + r$ und $\deg(r) < \deg(g)$.

Beweis. Wie im Falle $R = K$ ein Körper.

- **Eindeutigkeit:** Sei $f = q_1 g + r_1 = q_2 g + r_2$ und $\deg(r_1) < \deg(g) \Rightarrow r_1 - r_2 = (q_2 - q_1)g$. Da $\mathrm{LC}(g) \in R^\times$ ist $\mathrm{LC}(g)$ kein Nullteiler $\overset{1.10}{\Rightarrow} \deg(r_1 - r_2) < \deg(g) = \deg(q_2 - q_1) + \deg(g)$

$\Rightarrow \deg(q_2 - q_1) < 0 \Rightarrow q_1 = q_2$ und $r_1 = r_2$

- **Existenz:** Sei $f = \sum_{i=0}^{n} a_i x^i$, $a_n \neq 0$ und $g = \sum_{j=0}^{m} b_j x^j$ mit $b_m \neq 0$. Nach Vorraussetzung ist $b_m \in R^{\times}$ es existiert also $b_m^{-1} \in R$.
  Induktion nach $\deg(f) = n$:
  - $n < m$**:** $q = 0$, $r = f$
  - $n \geq m$**:** $f_i = f - a_n b_m^{-1} x^{n-m} \cdot g \Rightarrow \deg(f_1) < \deg(f)$ mit Induktionshypothese folgt $f_1 = q_1 \cdot g + r_1$ mit $\deg(r) < m \Rightarrow f = (q_1 + a_n b_m^{-1} x^{n-m})g + r$ □

Folgerung 1.15
Ist $f \in R[x]$ und $a \in R$, $f(a) = 0$, so ist

$$f(x) = (x - a) \cdot q(x) \text{ mit } q \in R[x].$$

Beweis. Sei $f = q(x-a) + r$, $\deg(r) < \deg(x-a)$, d.h. $\deg(1) \leq 0 \Rightarrow 0 = f(a) = q(a-a) + r(a) \Rightarrow r(a) = 0.$□

Folgerung 1.16
Ist R nullteilerfrei, so hat $0 = f \in R[x]$ höchstens $\deg(f)$ viele Nullstellen in R.

Definition 1.17 (Polynomring in kommutieren Variablen)
Für eine Menge I definieren wir den Monoid

$$\mathbb{N}_0^{(I)} := \left\{ (\mu_i)_{i \in I} \in \prod_{i \in I} \mathbb{N}_0 \colon \mu_i = 0 \text{ für fast alle } i \right\}$$

mit Addition

$$(\mu_i)_{i \in I} + (\nu_i)_{i \in I} := (\mu_i + \nu_i)_{i \in I},$$

sowie den Ring

$$R[x_i \colon i \in I] = \{(_\mu)_{\mu \in \mathbb{N}_0} \colon a_\mu \in R, \text{ fast alle gleich } 0\}$$

mit Addition und Multiplikation

$$(a_\mu)^{(I)}_{\mu \in \mathbb{N}_0} + (b_\mu)^{(I)}_{\mu \in \mathbb{N}_0} := (a_\mu + b_\mu)^{(I)}_{\mu \in \mathbb{N}_0}$$
$$(a_\lambda)_{\lambda \in \mathbb{N}_0^{(I)}} \cdot (b_\nu)_{\nu \in \mathbb{N}_0^{(I)}} := \left(\sum_{\lambda + \nu = \mu} a_\lambda b_\mu \right)^{(I)}_{\mu \in \mathbb{N}_0},$$

gennant Polynomring in kommutierenden Variablen $x_i, i \in I$. Wir identifizieren den Ring R mit den Unterring

$$\{(r\delta_{\mu,\underline{0}})^{(I)}_{\mu \in \mathbb{N}_0} \colon r \in R\}.$$

Wir schreiben $x_i := (\delta_{\mu\nu})^{(I)}_{\mu \in \mathbb{N}_0}$, $\mu := (\delta_{ij})_{i \in I}$ und $x^\mu := \prod_{i \in I} x_i^{\mu_i}$. Damit ist dann

$$(a_\mu)^{(I)}_{\mu \in \mathbb{N}_0} = \sum_{\mu \in \mathbb{N}_0^{(I)}} a_\mu x^\mu.$$

Weiter schreiben wir

$$R[x_1, \ldots, x_n] := R[x_i \colon i \in \{i, \ldots, n\}].$$

■ **Beispiel 1.18**
Sei $R = \mathbb{Z}$ und $I = \{1, 2\}$, dann

$$\left(x_1 x_2 + x_2^2\right)^2 = a_{(2,1)} x_1^2 x_2^2 + a_{(1,3)} x_1 x_2^2 + a_{(0,4)} x_2^4$$

mit $a_{(2,1)} = 1$, $a_{(1,3)} = 2$ und $a_{(0,4)} = 1$

▶ **Bemerkung 1.19**
Satz 1.10 und Satz 1.12 kann man allgemein für $R[x_i \colon i \in I]$ anstatt $R[x]$ formulieren. Für Satz 1.14 - Folgerung 1.16 gibt es keine Verallgeminerung. So hat z.B. $f = x_1 - x_2$ unendlich viele Nullstellen, da $f(a, a) = 0$ für alle $a \in \mathbb{Z}$.

2. Ideale

Sei R ein Ring. (Meisten Beweise finden sich wieder in LAAG1-2 Skript!)

Definition 2.1 (siehe LAAG II.3.9, VIII.2.13)
Ein ideal von R ist eine Untergruppe $I \leq (R,+)$ mit $a \in I$, $r \in R \to ra \in I$ (in Zeichen: $I \trianglelefteq R$).

Beispiel 2.2

1. Für $a \in R$ ist $(a) := Ra = \{ra \colon r \in R\}$ das von a erzeugte Hauptideal .
2. (0) das Nullideal
3. $(1) = R$ triviale Ideal (ein Ideal $I \trianglelefteq R$ mit $I \neq R$ ist ein echtes Ideal von R)

Bemerkung 2.3

1. $I \leq R$ ist Ideal von $R \Leftrightarrow I + I \subseteq, R \cdot I \subseteq I, 0 \in I$
2. Ein Ideal von R ist im Allgemeinen kein Unterring von R.
3. Für $I \trianglelefteq R$ ist $I = R \Leftrightarrow 1 \in I$
4. Für Hauptideal: $a \in R$ gilt $(a) = R \Leftrightarrow a \in R^\times$
   Insbesondere gilt: Genau dann ist R ein Körper, wenn $(0) \neq (1)$ die beiden einzigen Ideale von R sind.
5. Sind $I, J \trianglelefteq R$, so auch $I + J$ und $I \cap J$.
6. Der Schnitt einer Famile $(I_i)_{i \in \Lambda}$ von Idealen von R ist wieder ein Ideal von R. Insbesondere existiert zu jeder $A \subseteq R$ ein kleinstes Ideal $\langle A \rangle$ von R, das A enthält (das von A erzeugte Ideal). Es gilt

$$\langle A \rangle = \left\{ \sum_{i=1}^{n} r_i a_i \colon n \in \mathbb{N}, r \in R, a \in A \right\}$$

Wir schreiben $(a_1, \ldots, a_n)$ für $\langle \{a_1, \ldots, a_n\} \rangle$.

Beispiel 2.4
Ist $\varphi : R \to S$ ein Ringhomomorpismus, so ist $\ker \varphi \trianglelefteq R : \varphi(a) = 0, \varphi(b) = 0, r \in R \Rightarrow \varphi(a + b) = \varphi(a) + \varphi(b) = 0$
$\varphi(ra) = \varphi(r) \cdot \underbrace{\varphi(a)}_{=0} = 0$

Definition 2.5 (Quotientenring)
Sei $I \trianglelefteq R$. Der Quotientenring (QR) von R modulo I ist $R/I := \{x + I \colon x \in R\}$ mit $(x, y \in R)$

- $(x + I) +_{QR} (y + I) := (x + y) + I$
- $(x + I) \cdot_{QR} (y + I) := (xy) + I$

Satz 2.6
R/I ist ein Ring und $\pi_I : R \to R/I$ mit $x \mapsto x + I$ ist ein Ringepimorphismus mit Kern I.

Beweis. Siehe LA VIII.5.8. □

▶ **Bemerkung 2.7**

1. Die Ideale sind also genau die Kerne von Ringhomomorphismen.
2. Für $x, y \in R$ schreibt man

$$\begin{aligned} x \equiv y \mod I &\Leftrightarrow x - y \in I \\ &\Leftrightarrow x + I = y + I \\ &\Leftrightarrow \pi_I(x) = \pi_I(y) \end{aligned}$$

Satz 2.8 (Homomorphiesatz)
Sei $\varphi : R \to S$ ein Ringhomomorphismus und $I \trianglelefteq R$ ein Ideal mit $I \subseteq \ker \varphi$. Dann gibt es genau einen Ringhomomorphismus $\overline{\varphi} : R/I \to S$ mit $\varphi = \overline{\varphi} \circ \pi_I$

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "\pi_I"'] & & S \\ & R/I \arrow[ur, dashed, "\overline{\varphi}"'] & \end{tikzcd}$$

Insbesondere gilt: Ist φ surjektiv, so induziert φ ein Isomorphismus

$$R/\ker \varphi \cong S.$$

Beweis. Siehe LAAG VIII.5.9. □

Lemma 2.9

1. Für $J \trianglelefteq S$ ist $\varphi^{-1}(J) \trianglelefteq R$.
2. Ist φ surjektiv, so liefert $J \mapsto \varphi^{-1}(J)$ eine Bijektion Φ zwischen
   (a) Idealen von S, und
   (b) Idealen von R, die $\ker \varphi$ enthalten

Beweis. (vgl. LAAG VIII.5.5) Skizze:

1. $a \in \varphi^{-1}(J)$, $r \in R \Rightarrow \varphi(ra) = \underbrace{\varphi(r)}_{\in R}\underbrace{\varphi(a)}_{\in J} \in J$
2. Umkehrabbildung: $I \mapsto \varphi(I)$
   - $\varphi(\varphi^{-1}(J)) = J$: φ surjektiv
   - $\varphi^{-1}(\varphi(I)) = I$: **???**
   - $I \trianglelefteq R \Rightarrow \varphi(I) \trianglelefteq S : A \in I, s \in S \xRightarrow{\varphi \textbf{ surjektiv}} s = \varphi(r)$ **mit** $r \in R$
     $\Rightarrow s\varphi(a) = \varphi(r)\varphi(a) = \varphi(\underbrace{ra}_{\in I})$ **mit** $ra \in I$
     $\Rightarrow s\varphi(a) \in \varphi(I)$ □

Definition 2.10 (prim und maximal Ideal)

1. I ist prim $:\Leftrightarrow \dot{I} \neq R$ und für $a, b \in R$ gilt:

$$ab \in I \Rightarrow a \in I \vee b \in I$$

2. I ist maximal $:\Leftrightarrow I \neq R$ und $J \trianglelefteq R$ mit

$$I \subseteq J \subsetneq R, \text{ so ist } I = J. \tag{1}$$

Satz 2.11
Sei $I \not\trianglelefteq R$

1. I ist prim $\Leftrightarrow R/I$ ist nullteilerfrei
2. I ist maximal $\Leftrightarrow R/I$ ist Körper
3. I ist maximal $\Rightarrow I$ prim

Beweis. c) folgt aus a) + b), denn Körper sind nullteilerfrei!

1. finish proof later ... □

Beispiel 2.12 (Gegenbeispiel das die Umkehrung von Satz 2.11c) nicht gilt!)
In $R = \mathbb{Z}$: Ideale sind genau die Hauptideale

- $(n) = n\mathbb{Z}, n \in \mathbb{N}_0$
- (n) ist prim $\Rightarrow n$ Primzahl oder $n = 0$
- (n) ist maximal $\Rightarrow n$ Primzahl

Satz 2.13
Jedes echte Ideal Iu ...

Kapitel III

Körpererweiterungen

Anhang

Anhang A: Listen

A.1. Liste der Theoreme

A.2. Liste der benannten Sätze, Lemmata und Folgerungen