Geometrie WS 19/20

Dozent: Prof. Dr. Ulrich Krähmer

28. Januar 2020

Inhaltsverzeichnis

Vorwort

Kapitel I
Gruppen

1. Wiederholung

Definition 1.1 (Halbgruppe, Monoid, Gruppe)
Eine Halbgruppe ist eine Menge G mit einem assoziativen Produkt

$$\cdot : G \times G \to G.$$

Ein Monoid ist eine Halbgruppe, in der ein Element $1 \in G$ existiert mit

$$1 \cdot x = x \cdot 1 = x \quad \forall x \in G.$$

Eine Gruppe ist ein Monoid, in dem für jedes $x \in G$ ein $y \in G$ existiert mit

$$xy = yx = 1.$$

▶ **Bemerkung 1.2**
1 ist eindeutig, wenn es existiert. y ist durch x eindeutig bestimmt: $x^{-1} = y$.

Definition 1.3 (Morphismus)
Ein Morphismus zwischen zwei Gruppen G und H ist eine Abbildung

$$f : G \to H \quad \text{mit} \quad f(xy) = f(x)f(y) \quad \forall x, y \in G.$$

Satz 1.4
Ist $f : G \to H$ ein Morphismus von Gruppen, so gilt

- $f(1) = 1$ und
- $f(x^{-1}) = f(x)^{-1}$ $\forall x \in G$.

Beweis. Für alle $x \in G$ gilt

$$f(x) = f(1 \cdot x) = f(1)f(x).$$

Gilt in einer beliebigen Gruppe jedoch $ab = b$ für zwei Elemente a, b, so folgt

$$(ab) \cdot b^{-1} = a\left(bb^{-1}\right) = a \cdot 1 = a \quad \text{mit} \quad bb^{-1} = 1.$$

Ferner gilt

$$f(x) \cdot f\left(x^{-1}\right) = f\left(x \cdot x^{-1}\right) = f(1) = 1$$

wie schon gezeigt (und analog $f(x^{-1})f(x) = 1$). Also ist $f(x^{-1}) = f(x)^{-1}$). □

■ **Beispiel 1.5**

1) Sei X eine beliebige Menge. $S_X = \{f : X \to X \mid f \text{ bijektiv}\}$ ist eine Gruppe bezüglich Komposition mit $1 = \mathrm{id}_X$. Insbesondere ist $S_n = S_{\{1,\dots,n\}}$ die symmetrische Gruppe und ein Element $f \in S_n$ ist eine Permutation.
2) $\mathrm{GL}(V) = \{f \in S_V \mid f \text{ linear}\}$, wobei V ein R-Modul ist mit kommutativen assoziativen Ring mit 1.

3) $\mathbb{Z}, \mathbb{Z}_n$ unter Addition

$$U_n = \mathbb{Z}_n^\times = \{m \in \{0, \dots, n-1\} \mid \text{ggT}(m,n) = 1\}$$

Beide Gruppen sind abelsch, d.h.

$$\forall x, y \in G : xy = yx.$$

4) $G = U(1) = \{z \in C \mid |z| = 1\} = \{e^{it} \mid t \in [0, 2\pi]\}$

5) $G = U(1) \times \text{SU}(2) \times \text{SU}(3)$, die Eichgruppe im Standardmodell der Elementarteilchen

Definition 1.6 (Ordnung)

- Ist G endlich, so nennt man $|G|$ die Ordnung von G.
- die Ordnung eines Elements, ist einfach die wiederholt aufeinander Ausführung des Elements, bis sich wieder die Identität ergibt.

■ **Beispiel 1.7**
$|S_n| = n!$

Definition 1.8 (p-Gruppe)
Ist $|G| = p^n$ für eine Primzahl p und ein $n \in \mathbb{N}$, so nennt man G eine p-Gruppe

Definition 1.9 (Untergruppe)
Sei G Gruppe. Eine Teilmenge $H \leq G$ ist eine Untergruppe $H < G$, wenn

(i) Für alle $x, y \in H$: $xy \in H$

(ii) $1 \in H$

(iii) Für alle $x \in H$: $x^{-1} \in H$

Satz 1.10
Ist $|G| < \infty$, so folgen Definitionen 1.9 (ii) und 1.9 (iii) bereits aus Definition 1.9 (i) und $H \neq \varnothing$.

Beweis. Sei $x \in H$ ein beliebiges Element. Aus 1.9 (i) folgt $x^n \in H$ für alle $n \in \mathbb{N}_+$. Da $|G| < \infty$ existiert $n \neq m$ mit $x^n = x^m$. O.E. sei $n > m$

$\Rightarrow x^{n-m}x^m = x^n$

$\Rightarrow x^{n-m} = 1$

$\Rightarrow$ 1.9 (ii)

Ferner impliziert die Existenz der inversen Elemente, dass die Linkstranslation

$$t_x \colon G \to G, y \mapsto xy \quad (x \in G \text{ fest})$$

injektiv ist, denn $(t_x)^{-1} = t_{x^{-1}}$. Ist $x \in H$, so heißt 1.9 (i) gerade $t_x(H) \subseteq H$, sprich t_x kann zu $t_x\big|_H \colon H \to H$ eingeschränkt werden. Die Einschränkung einer injektiven Abbildung ist injektiv. Da $|H| \leq |G| < \infty$, folgt $t_x\big|_H \colon H \to H$ ist surjektiv. Also existiert $y \in H$ mit $t_x(y) = 1$. Eindeutigkeit von x^{-1} heißt $y = x^{-1} \in H$. □

Definition 1.11 (Erzeugendensystem)
Ist $X \subseteq G$, so ist

$$\langle X \rangle = \bigcap_{\substack{H < G \\ X \subset H}} H$$

die von X erzeugte Untergruppe. Ist $\langle X \rangle = G$, nennen wir X ein Erzeugendensystem.

■

Definition 1.12 (Konjugation)
Ist $H < G$ und $x \in G$, so ist

$$x^{-1}Hx = \left\{x^{-1}Hx \mid y \in H\right\}$$

eine Untergruppe („$x^{-1}yx$“ y ist konjugiert mit x). Wir nennen diese zu H konjugiert.

Definition 1.13 (Konjugationsklasse)
Die Menge $\left\{x^{-1}yx \mid x \in G\right\}$ ist i.A. keine Untergruppe und diese nennt man Konjugationsklassen von y.

Definition 1.14 (Zentralisator, Zentrum)
Der Zentralisator von $y \in G$ ist

$$\{x \in G \mid xy = yx\} =: Z_G(y).$$

Das Zentrum von G ist

$$Z(G) = \bigcap_{y \in G} Z_G(y) = \{x \in G \mid \forall y \in G xy = yx\}.$$

■ **Beispiel 1.15**
Sei $G = S_n \ni f$ Permutation, z.B.

$$S_6 \in \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 1 & 2 & 3 \end{pmatrix} = (1524)(36)$$

letzteres nennt man Zykelnotation. 1-Zykeln, d.h. $i \in \{1, \ldots, n\}$ mit $f(i) = i$ werden meist nicht notiert, z.B.:

$$S_4 \in \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (12)$$

▶ **Bemerkung 1.16**
Ein k-Zykel ist ein Produkt von $k-1$ Transpositionen (2-Zykel), z.B.

$$(12345) = (15)(14)(13)(12)$$

ist das Produkt in S_5, d.h. Komposition! Also erzeugt $\{(i,j)\}$ die S_n. Jede Permutation kann also als Produkt von Transpositionen geschrieben werden. Diese Darstellung ist nicht eindeutig! (z.B. $(12)(23)(12) = (23)(12)(23)$) (“Braid relation”) und $(12)(12) = ()$. Allerdings kommen in jeder solcher Darstellungen entweder eine gerade oder ungerade Anzahl von Transpositionen vor ($\to$ Fehlstände). Insbesondere bilden gerade Permutationen (gerade Anzahl an Fehlständen $\Leftrightarrow$ Produkte von zu Transpositionen) eine Untergruppe $A_n < S_n$, die sogenannte alternierende Gruppe.

■ **Beispiel 1.17**
Sei $G = \mathrm{GL}(n, R)$ die invertierbare Matrizen mit Einträgen in R (nur endliche, wenn $R^\times$ *endlich*!). Untergruppen sind

- $\mathrm{SL}(n, R) = \{g \in \mathrm{GL}(n, R) \mid \det g = 1\}$
- $O(n, R) = \left\{g \in G \mid gg^T = g^T g = 1\right\}$ mit dem Skalarprodukt $\langle gv, gw\rangle = \langle v, w\rangle \quad \forall v, w \in R^n$
- $\mathrm{SO}(n, R) = \mathrm{SL}(n, R) \cap \mathrm{O}(n, R)$.

Ist R Ring mit Involuten (z.B. $R = \mathbb{C}, z = \bar{z}$)

- $U(n,R) = \{g \in \mathrm{GL}(n,R) \mid gg^* = g^*g = 1\}$
- $\mathrm{SU}(n,R) = \mathrm{SL}(n,R) \cap U(n,R)$

■ **Beispiel 1.18**
Sei D_n definiert durch

$$D_n = \{f\colon \mathbb{R}^2 \to \mathbb{R}^2 \text{ linear, bjektiv} \mid f(P_n) = P_n\},$$

wobei $P_n \subset \mathbb{R}^2$ das regulär n-gen ist, z.B. das Hexagon P_6. Alternativ ist $D_n \subseteq S_n$, wobei $\{1,\dots,n\}$ mit der Menge der Ecken von P_n identifiziert wird und man erhält alle Permutationen, die benachbarte Ecken auf benachbarte abbilden:

- r: Rotation um $2\pi/n$ im mathematische positiven Sinn
- s: eine beliebige Spiegelung in D_n

Also hat man

$$\langle\{s,r\}\rangle = D_n = \{s^i r^j \mid i = 0,1, j = 0,\dots,n-1\}$$

und der Mächtigkeit $|D_n| = 2n$.

Für die erzeugenden Elemente $D_n = \langle\{s,r\}\rangle$ gilt:

- $srs = r^{n-1}$,
- $r^{n-1} = r^{-1}$,
- $r^n = 1$,
- $s^2 = 1$.

Im unendlichen Fall $D_\infty \subset S_\mathbb{Z}$ gilt z.B. $r(z) = z+1$, $s(z) = -z$, wobei r, $s\colon \mathbb{Z} \to \mathbb{Z}$ sind und D_∞ erzeugen: $D_\infty = \langle\{r,s\}\rangle$.

2. Nebenklassen, Normalteiler, Isomorphiesätze

Definition 2.1
$A, B \subseteq G$ Teilmengen (nicht unbedingt Untergruppen!), dann:

- $AB = \{xy \in G \mid x \in A, y \in B\}$
- $A^{-1} = \{x^{-1} \in G \mid x \in A\}$

▶ **Bemerkung 2.2**
$\varnothing \neq H \subseteq G$ ist Untergruppe $\Leftrightarrow HH = H$, $H^{-1} = H$

Definition 2.3
Ist $x \in G$, so nennen wir

$$f_x\colon G \to G \text{ mit } y \mapsto x^{-1}yx$$

den durch x definierten inneren Automorphismus. Ist $H < G$, so nennen wir $f(H) = x^{-1}Hx$ eine zu H konjugierte Untergruppe.

Satz 2.4
- f_x ist ein Endomorphismus von G (d.h. ein Morphismus $G \to G$)
- Das Bild $\mathrm{Im}\, f$ eines beliebigen Gruppenmorphismus $f\colon K \to L$ ist eine Untergruppe: $\mathrm{Im}\, f < L$

Beweis.
- $f_x(yz) = x^{-1}yzx = x^{-1}y(xx^{-1})zx = (x^{-1}yx)(x^{-1}zx) = f_x(y)f_x(z)\ \forall y, z \in G$
- Wir untersuchen die drei Eigenschaften:
  - $\operatorname{Im} f$ ist abgeschlossen: seien $f(y), f(z) \in \operatorname{Im} f$. Dann gilt:
    $$f(y)f(z) = f(yz) \in \operatorname{Im} f$$
  - $f(1) = 1 \Rightarrow 1 \in \operatorname{Im} f$
  - $f(x)^{-1} = f(x^{-1}) \Rightarrow (\operatorname{Im} f)^{-1} = \operatorname{Im} f$ □

Definition 2.5
Ist $H < G, x \in G$, so nennt man

$$G \supseteq xH = \{x\}H = \{xy \in G \mid y \in H\} \quad \text{linke Nebenklasse}$$
$$G \supseteq Hx = \{yx \in G \mid y \in H\} \quad \text{rechte Nebenklasse}$$

■ **Beispiel 2.6**
Sei $G = V$ Vektorraum über Körper K mit $+$ als Gruppenstruktur, dann ist $H = W < V$ ein Untervektorraum und $xH = x + W \subseteq V$ affiner Unterraum, Element von V/W

Dies verallgemeinert sich zu

Definition 2.7
Sei $H < G$, $G/H = \{xH \mid x \in G\} \subseteq \mathcal{P}(G)$

▶ **Bemerkung 2.8**
$xH = yH \Leftrightarrow x \sim y$ definiert eine Äquivalenzrelation und das ist äquivalent zu

$$\exists h \in H : x = yh \Leftrightarrow y^{-1}y \in H.$$

Beachte dabei $G/H = G/N$ ist die Menge aller Äquivalenzklassen $xH = [x]$. Desweiteren gibt es die kanonische Projektion $\pi\colon G \to G/H, x \mapsto xH$.

Insbesondere ist G die disjunkte Vereinigung aller Äquivalenzklassen. Speziell ist für jedes $x \in G$ definiert:

$$t_x\colon G \to G, y \mapsto xy \text{ eine Bijektion}, \quad H = 1H = [x] \to xH = [x].$$

Definition 2.9 (Index)
Sei $H < G$, dann ist $[G : H] := |G/H|$ der Index von H in G.

Folgerung 2.10
Sei $K < H < G$ und $|G| < \infty$, dann

$$[G : K] = |G/K| = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = [G : H][H : K].$$

Alle xH haben also die gleiche Kardinalität und wir erhalten:

Satz 2.11 (Lagrange, Klausur!)
Sei $|G| < \infty$ und $H < G$. Dann gilt $|G| = |G/H| \cdot |H|$. Insbesondere ist $|G|$ durch $|H|$ teilbar.

Beweis. • Beweisskizze: Äquivalenzrelation und Bijektion $xH \cong yH$.
Let $H < G$ a subgroup of G and $xH := \{xy \mid y \in H\} \leq G$ the coset of H in G. Then we have $G/$

$H = \{xH \mid x \in G\} \subseteq \mathcal{P}(G)$. Then

$$xH = \tilde{x}H \Leftrightarrow \exists y \in H \quad x = \tilde{x}y \Leftrightarrow \tilde{x}^{-1}x \in H$$
$$G = \bigcup_{xH \in G/H} xH \Rightarrow |G| = |G/H| \cdot |H|$$
$$|xH| = |H| \quad \forall x \in G.$$

- Wikipedia: This can be shown using the concept of left cosets of H in G. The left cosets are the equivalence classes of a certain equivalence relation on G and therefore form a partition of G. Specifically, x and y in G are related iff there exists h in H such that $x = yh$. If we can show that all cosets of H have the same number of elements, then each coset of H has precisely $|H|$ elements. We are then done since the order of H times the number of cosets is equal to the number of elements in G, thereby proving that the order of H divides the order of G.

  To show any two left cosets have the same cardinality, it suffices to demonstrate a bijection between them. Suppose aH and bH are two left cosets of H. Then define a map $f\colon aH \to bH$ by setting $f(x) = ba^{-1}x$. This map is bijective because it has an inverse given by $f^{-1}(y) = ab^{-1}y$. □

▶ **Bemerkung**
This proof also shows that the quotient of the orders $|G|/|H|$ is equal to the index $[G\colon H]$ (the number of left cosets of H in G). If we allow G and H to be infinite, and write this statement as

$$|G| = [G\colon H] \cdot |H|$$

then, seen as a statement about cardinal numbers, it is equivalent to the axiom of choice.

Folgerung 2.12
Sei $|G| < \infty$, dann gilt $|x| \mid |G|$ für alle $x \in G$. Dabei ist $|x| = |\langle\{x\}\rangle| = \min\{n \mid x^n = 1\}$. Also z.B. $\langle\{x\}\rangle \cong (\mathbb{Z}_{|x|}, +)$. Insbesondere gilt für alle $x \in G$: $x^{|G|} = 1$

Folgerung 2.13 (Eulers Theorem)
$|U_n| = \varphi(n) = |\{m \in \{1, \dots, n\} \mid \mathrm{ggT}(n, m) = 1\}| = |\{(\mathbb{Z}_n^\times, \cdot) \mid \mathrm{ggT}(n, m) = 1\}|$ mit $n \in \mathbb{N}$. Also ist $m^{\varphi(n)} = 1 \mod n$.

3. Morphismen

Definition 3.1
Ein injektiver Morphismus $f\colon G \to H$ wird auch Einbettung genannt. Ein Isomorphismus ist ein bijektiver Morphismus.

▶ **Bemerkung**
Ein injektiver Morphismus wird auch Monomorphismus genannt und ein surjektiver Morphismus Epimorphismus.

■ **Beispiel 3.2**

1) Betrachte die Determinate $\det\colon \mathrm{GL}(n, R) \to R^\times$, diese ist ein surjektiver Morphismus von Gruppen mit

$$\det(gh) = \det(g)\det(h)$$

2) Die Wahl einer Basis B in einem endlich erzeugten freien Modul V ist ein Isomorphismus von Moduln $s_B\colon R^{|B|} \to V$. Dieser induziert einen Gruppenisomorphismus

$$\mathrm{GL}(n, R) \to \mathrm{GL}(V), g \mapsto s_B \circ M_g \circ s_B^{-1}$$

3) Die Linkstranslation $t\colon G \to S_G$ mit $x \mapsto t_x$ (mit $t_x(y) = xy$) ist ein injektiver Gruppenho-

momorphismus

$$(t_x \circ t_z)(y) = t_x(t_z(y)) = t_x(zy) = xzy = t_{xz}(y)$$

also

$$t_x \circ t_y = t_{xy} \quad \forall x, y \in G$$

Ist $t_x = t_z$, so gilt $t_x(1) = t_z(1)$ und daraus $x1 = z1$, also $x = z$

Also kann jede endliche Gruppe als Untergruppe der S_n verstanden werden ($n = |G|$)!

■ **Beispiel 3.3**

1) $y \mapsto f_{x^{-1}} : G \to G$, $y \mapsto xyx^{-1}$ ist ein Morphismus $G \to \operatorname{Aut} G$ mit

$$f_x(y) = x^{-1}yx, \quad f_z(f_x(y)) = z^{-1}(x^{-1}yx)z = (xz)^{-1}y(xz) = f_{xz},$$

und ist i.A. nicht injektiv! Denke an G abelsch $\Leftrightarrow f_x = \mathrm{id}_G \ \forall x \in G$

2) $\operatorname{sgn} : S_n \to \mathbb{Z}_2 = \{-1, 1\}$

4. Normalteiler

Definition 4.1 (normale Untergruppe)
Eine Untergruppe $H < G$ ist normal $\Leftrightarrow \forall x \in G : xH = Hx$. Notation: $H \triangleleft G$.

Satz 4.2

$$H < G \text{ ist normal } \Leftrightarrow \forall x \in G x^{-1}Hx = H \Leftrightarrow AH = HA \quad \forall A \subseteq G$$

Beweis. Sei H normal und $x \in G$. Dann gilt $xH = Hx \Rightarrow x^{-1}xH = x^{-1}Hx$. Hier verwende $A, B \subseteq G, AB = \{ab \mid a \in A, b \in B\}$ definiert ein assoziatives Produkt $u \in \mathcal{P}(G)$, angewendet auf $A(BH) = (AB)H, A = \left\{x^{-1}\right\}, B = \{x\}$. Umgekehrt genauso $xH = Hx \Rightarrow x^{-1}xH = x^{-1}Hx$. Weiter gilt:

$$AH = \bigcup_{x \in A} xH, \quad HA = \bigcup_{x \in A} Hx$$

Also $xH = Hx \quad \forall x \in G \Rightarrow AH = HA \forall A \subseteq G$. Umgekehrt: Nimm $A = \{x\}$. □

Warum relevant?
Weil G/H eine Gruppenstruktur von G erbt $\Leftrightarrow H \triangleleft G$

Satz 4.3
Sei $H \triangleleft G$. Dann definiert

$$xH \cdot yH = (xy)H$$

eine Gruppenstruktur auf G/H und $\pi : G \to G$ mit $x \mapsto xH$ ist eine surjektiver Morphismus von Gruppen.

Beweis. $xH \cdot yH$ kann ich in $\mathcal{P}(G)$ immer bilden. Ist $H \triangleleft G$, gilt $xH = Hx$, also $xH \cdot yH = HxyH = xyHH = xyH$. (oder $A = \{x\}, B = \{y\}, C, D = H$). Anders gedacht: $H \triangleleft G$ heißt: $H \in Z(\mathcal{P}(G))$. Sprich: $G/H \subseteq \mathcal{P}(G)$ ist eine Unterhalbgruppe, d.h. abgeschlossen unter $\cdot$. Ferner gilt: $H = 1H$ ist ein Einselement $(xH)H = x(HH) = xH, H(xH) = (Hx)H = xH = (Hx)H = (xH)H$. Ausserdem ist G/H Gruppe

$$xH \cdot x^{-1}H = Hx \cdot x^{-1}H = H1H = HH = H$$

und genauso $x^{-1}HxH = H$. Sei $\pi : G \to G/H$ mit $x \mapsto xH$ also $\pi(xy) = \pi(x)\pi(y)$ mit $xyH = xH \cdot yH$. □

Definition 4.4 (Kern einer Gruppe)
Ist $f : G \to K$ ein Morphismus von Gruppen, so definieren wir den Kern $\ker f = \{x \in G \mid f(x) = 1_K\}$

▶ **Bemerkung**
Ist K eine abelsche Gruppe, so schreibt man die Gruppenoperation oft als $+$ und 1 oft als 0.

Satz 4.5
Es gilt $\ker(f) \triangleleft G$.

Beweis.
1. Sind $x, y \in \ker f$, so gilt $f(x)f(y) = f(xy)$ (und $11 = 1$), also ist $kerf$ abgeschlossen unter $\cdot$.
2. Ferner $f(1) = 1$, da f Morphismus $\Rightarrow G \ni 1 \in \ker f$.
3. Zuletzt: $f(x)^{-1} = f(x^{-1})$, dann
$$x \in \ker f \Rightarrow f(x) = 1 \Rightarrow f(x^{-1}) = f(x)^{-1} \Rightarrow x^{-1} \in \ker f$$
4. Ferner gilt für $x \in G, y \in \ker f$:
$$f(x^{-1}yx) = f(x^{-1}f(y)f(x)) = f(x^{-1}) \cdot 1f(x) = f(x^{-1}x) = f(1) = 1 \text{ also}$$
$$x^{-1} \in \ker f \subseteq \ker f \text{ also}$$
$$(x^{-1})^{-1} \ker f(x^{-1}) \subseteq \ker f \Rightarrow \ker f \subseteq x^{-1} \ker fx$$
5. $\ker f \triangleleft G$.

also 1. 2. 3. : $\ker f < G$. □

▶ **Bemerkung**
Ist $H \triangleleft G$, so gilt: $H = \ker \pi$ mit $\pi : G \to G/H$. (denn $\pi(x) = xH$, also $\ker \pi = \{x \mid xH = H\} = H$).
Normalerteiler sind also die Kerne von Morphismen.

Satz 4.6 (1. Isomorphiesatz, Klausur)
Ein Morphismus $f : G \to K$ von Gruppen induziert einen Isomorphismus:
$$\bar{f} : G/\ker f \to \operatorname{Im} f \text{ mit } [x] = x \ker f \mapsto f(x)$$

Beweis. Der einzig schwere Teil ist $\bar{f}$ ist wohldefiniert. $f(xH) := f(x) \in \operatorname{Im} f$, also landet $\bar{f}$ in $\operatorname{Im} f$. Ferner gilt: Ist $x \ker f = y \ker f$, so ist $y^{-1}x \in \ker f$ (allgemein: $xH = yH \Leftrightarrow y^{-1}xH) \Leftrightarrow f(y^{-1}x) = 1 \Leftrightarrow f(y^{-1})f(x) = 1 \Leftrightarrow f(y)^{-1}f(x) = 1 \Leftrightarrow f(x) = f(y)$. Also ist $\bar{f}$ wohldefiniert und injektiv. Surjektiv ist $\bar{f}$ per Definition.
Letzter Schritt: $\bar{f}(x \ker f \cdot y \ker f) = \bar{f}(xy \cdot \ker f)$ (**???**). $\bar{f}(x \ker f)\bar{f}(y \ker f) = f(x)f(y) = f(xy)$. Also ist $\bar{f}$ ein Morphismus von Gruppen. □

■ **Beispiel 4.7**
Sei $G = (\mathbb{R}, +)$, $K = (\mathbb{C} \setminus \{0\}, \cdot)$ und $f(t) = \exp(2\pi it)$, dann $f(x + y) = \exp(x) + \exp(y)$ also ein Gruppenmorphismus $G \to K$. Dann $\operatorname{Im} f = U(1) = S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ und $\ker f = \mathbb{Z}$. Also ist $\mathbb{R}/\mathbb{Z} \cong S^1$ ($\mathbb{R}^2/\mathbb{Z}^2 \cong T$ ist dann der Torus T, $U(n) = \left\{A \in \operatorname{Mat}(n, \mathbb{C}) \mid AA^T = 1\right\}$ unitäre Gruppe)

Definition 4.8 (einfache Gruppe)
Eine Gruppe G ist einfach, wenn $H \triangleleft G \Rightarrow H = G$ und $H = \{1\}$.

▶ **Bemerkung**
D.h.: Ist $f : G \to K$ irgendein Morphismus, so ist $G \cong \operatorname{Im} f$ ($\ker f = \{1\}$) oder $\operatorname{Im} f = \{1\}$ ($\ker f = G$).

Die endlichen einfachen Gruppen sind klassifiziert!

■ **Beispiel 4.9**

1. Sei $G = \mathbb{Z}_p, p$ prim hat nach LAGRANGE (Satz 2.11) noch nicht mal irgendeine echte Untergruppe, ist also einfach.
2. $\mathrm{SL}(n, \mathbb{Z}_p)/Z(\mathrm{SL}(n, \mathbb{Z}_p)) = \mathrm{PSL}(n, \mathbb{Z}_p)$ (projective linear group)

Satz 4.10 (Korrespondenztheorem)
Ist $H \triangleleft G$, so induziert (definiert) $\pi : G \to G/H$ einen Isomorphismus von teilgeordneten Mengen (partial ordered sets)

$$\{L < G \mid H < L\} \to \{K < G/H\} \text{ mit } L \mapsto \pi(L)$$

Dieser erhält und reflektiert Normalität und auch Unterquotienten.

Satz 4.11 (2. Isomorphiesatz, Klausur)
Let $H < G$, $K \triangleleft G \Rightarrow H \cap K \triangleleft H, K \triangleleft H, K < G$ und

$$H/H \cap K \to HK/K \text{ with } x(H \cap K) \mapsto xK$$

ist ein Isomorphismus.

Beweis. 1. Durchschnitte von Untergruppen sind Untergruppen, also $H \cap K < H$. Ist ferner $x \in H$ und $y \in H \cap K$, so gilt $xyx^{-1} \in H$ (da H Untergruppe) und $xyx^{-1} \in K$, da $x \in G$ und $y \in K$ und auch $K \triangleleft G$. Also gilt $xyx^{-1} \in H \cap K$.

2. Auch klar, da $(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK$ (wobei $K \triangleleft G$), Bemerkung: $H, K < G$ reicht nicht, HK ist i.A. keine Untergruppe von G. Klar das $1 = 1 \cdot 1 \in HK, 1 \in H, 1 \in K$ (da $H, K < G$).

   $$x \in H, y \in K \quad (xy)^{-1} = y^{-1}x^{-1} \Rightarrow (HK)^{-1} = K^{-1}H^{-1} = KH = KH, \text{ da } K \triangleleft G.$$

   Also gilt $HK < G$. $K \triangleleft HK$, wie im ersten Punkt des Beweises.

3. $$\varphi : H/H \cap K \to HK/K \text{ mit } (H \cap K) \mapsto xK$$

   wohldefiniert? Natürlich: Ist $x(H \cap K) = y(H \cap K)$ $x, y \in H$, so folgt $x = yz$ mit $z \in H \cap K$, also $yK = xK$, da 2. eben insbesondere in K ist. Gruppenhomomorphismus auch klar, da

   $$\varphi(x(H \cap K) \cdot y(H \cap K) = \varphi(xy(H \cap K)) = xyK$$
   $$\varphi(x(H \cap K))\varphi(y(H \cap K)) = xKyK$$ □

Lemma 4.12
$\varphi : G \to H$ ist injektiv genau, dann wenn $\ker \varphi = \{1\}$.

Beweis. Auf diesen Fall angewendet:

$$\ker \varphi = \{x(H \cap K) \subset H/H \cap K \mid xK = K\}$$

$xK = K$ heisst aber nichts anderes als $x \in K$, d.h.

$$\ker \varphi = \{x(H \cap K) \mid x \in H \cap K\} = H \cap K = 1$$

(in der Gruppe $H/H \cap K$) und surjektiv ist klar, da $xyK = xK$ für $x \in H, y \in K$. □

Satz 4.13 (3. Isomorphiesatz)
Sei $H \triangleleft G, K \triangleleft G, K < H$ impliziert $H/K \triangleleft G/H$ und es gilt

$$G/K \to H/H/H/K \text{ mit } xK \mapsto (xH) \cdot H/K$$

ist ein Isomorphismus.

Beweis.

$$\frac{|G|}{|K|} = |G/K||G/H/K/H| = \frac{|G/H|}{|K/H|} = \frac{\frac{|G|}{|K|}}{\frac{|K|}{|H|}}$$

Der Isomorphismus ist durch

$$xK \mapsto xH(K/H)$$

woldefiniert ist. Ist $xK = yK$ für $x, y \in G$, so ist $y^{-1}x \in K$. Zu zeigen ist

$$xH(K/H) = yH(K/H)$$
$$\Leftrightarrow Hx(K/H) = Hy(K/H) \quad \text{denn } H \text{ ist normal!}$$

aus $xK = yK$ folgt aber $xK/H = yK/H$. Was war $K/H \subseteq \mathcal{P}(K)$, also macht das keinen Sinn. Besser:

$$xH(K/H) = yH(K/H)$$

heisst $xH \cdot zH \in yHK/H$ (und umgekehrt) für alle $z \in K$. Sprich für alle $z \in K$ existiert ein $t \in K$

$$xHzH = yHtH \Leftrightarrow xzHH = ytHH \Leftrightarrow xzH = ytH$$

Dies folgt aber aus $a := y^{-1}x \in K$, nimm $\forall z \in K \exists t \in K\ t := y^{-1}xz = az \in K$ und $y^{-1}xt = t$. (Alternative ein Lemma zeigen: $\varphi\colon G/K \to N$ wohldefiniert, dann $x \in K$ und durch die Vorschrift auf $1 \in N$ abgebildet. Dann ist der Beweis kürzer.) □

5. Einfache Gruppen

Definition 5.1
G ist einfach, genau dann wenn $\{1\}, G$ sind die einzigen Normalteiler.

$$\varphi : G \to H \text{ mit } \operatorname{Im}\varphi = G/G/\ker\varphi$$
$$\operatorname{Im}\varphi \cong G \text{ oder } \operatorname{Im}\varphi = \{1\}$$

■ **Beispiel**
$G = \mathbb{Z}_p, p$ prim.

Satz 5.2
A_n ist einfach für $n > 4$.

▶ **Bemerkung**
$A_4 \triangleright \{(), (12)(34), (13)(24), (14)(23)\}$, d.h. A_4 ist nicht einfach.

Lemma 5.3
1. $S_n = \langle (ii+1) \rangle$ für $i = 1, \ldots, n-1$
2. $A_n = \langle (ijk) \rangle$

Beweis. 1. Betrachte $(23)(12)(23) = (13)$ und $(34)(13)(34) = (14)$, per Induktion folgt

$$(1i) \in \langle (ii+1) \rangle \text{ und } (1i)(1j)(1i) = (ij) \quad (i \neq j) \Rightarrow (ij) = \langle (rr+1) \rangle \quad r = 1, \ldots n-1$$

damit folgt 1.

2.

$$(ij)(jk) = (ijk) \text{ und } (ij)(kr) = (ijk)(jkr)$$

also folgt 2. □

Beweis (Satz 5.2). Sei $N \neq \{1\}$ Normalteiler von $A_n, n > 4$

1. Ist $(yk) \in N$, so gilt $(abc) \in N$ für alle a, b, c. Ist $\sigma \in S_n$, so gilt $\sigma(ijk)\sigma^{-1} = (\sigma(i)\sigma(j)\sigma(k))$ (siehe ÜA 5, 1. Blatt) Sei $\sigma \in S_n$so, dass $\sigma(i) = a$, $\sigma(j) = b$ und natürlich $\sigma(k) = c$. Ist $\sigma \in A_n$ so folgt (da $N \triangleleft A_n$, $(abc) \in N$). Wenn nicht wähle r, s ungleich und setze $\tilde{\sigma} := \sigma(rs) \in A_n$. Dann ist $\tilde{\sigma}(ijk)\tilde{\sigma}^{-1} = \sigma(rs)(ijk)(rs)\sigma^{-1} = (abc)$.
2. Bleibt zu zeigen: $\exists(ijk) \in N$. Sei

   $$1 \neq \sigma = \gamma_1\gamma_2 \dots \gamma_r \in N \text{ beliebig,}$$

   wobei γ_i Zykel ist und die Länge der Zykel γ_i nicht wachse also $l(\gamma_i) \geq l(\gamma_{i+1})$. Fallunterscheidung: (Ziel ist in jedem Fall gibt es ein $(ijk) \in N$.)
   (a) $l(\gamma_i) \geq 4$:
   Sei $\gamma_1 = (i_1, \dots, i_k)$ und $\pi(i_1 i_2 i_3)$

   $$\Rightarrow \pi_{\gamma_j} = \gamma_j \pi \quad \forall j > 1 \sigma^{-1} \underbrace{\pi^{-1}\sigma\pi}_{\in N, \text{ da } N \triangleleft A_n} = (i_1 i_2 i_4) \subset N$$

   also einfach Nachrechnen.
   (b) $l(\gamma_1) - l(\gamma_2) = 3$:
   Sei $\gamma_1 = (ijk), \gamma_2 = (pqs)$. Nimm $\pi = (kpq)$ und daraus folgt $\sigma^{-1}\pi^{-1}\sigma\pi = (isk)$
   (c) $l(\gamma_1) = 3, l(\gamma_2) = 2$:
   $\gamma_1 = (ijk) \Rightarrow \sigma^2 = (ikj)$
   (d) $l(\gamma_1) = l(\gamma_2) = 2, r = 2$:
   Sei $\gamma_1 = (ij)$, $\gamma_2 = (kl)$ $n \geq 5 \Rightarrow \exists m \notin \{i, j, k, l\}$ und $\pi = (ijm)$
   $\sigma\pi^{-1}\sigma\pi = (imj) \in N$
   (e) $l(\gamma_i) = 2 \forall i, r > 2$:
   $\sigma \in A_n$, $\gamma_1 = (ij)$, $\gamma_2 = (kl)$, sowie $\gamma_3 = (pq)$, $\gamma_4 = (st)$, setze $\pi = (ip)(jk)$ und $\sigma\pi\sigma\pi = (ipl)(jkq)$ und benutze Fall 2. □

Definition 5.4
Eine kurze Sequence von Gruppen ist ein Paar von Morphismen $f : H \to G$ mit $g : G \to K$ und dann

1. f ist injectiv
2. g ist surjektiv
3. $\operatorname{Im} f = \ker g$

Man schreibt auch:

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

Sprich: H ist (isomorph zu einer) normalen Untergruppe von G und K ist (isomorph zu) G/H
Allgemeiner: exakte Folgen:

$$\dots \xrightarrow{f_i} G_{i-1} \xrightarrow{f_{i-1}} G_{i-2} \longrightarrow \dots \qquad \operatorname{Im} f_i = \ker f_{i-1}$$

Einfachster Fall (⇒ langweiliger) Fall: Direkte Produkte

Definition 5.5 (äußeres direktes Produkt)
Seien H, K Gruppen. Auf der Menge $G := H \times K$ (Wenn sowas im Buch steht ist es direktes Produkt gemeint) erhalten von einer Gruppenstruktur durch

$$(a, b)(x, y) := (ax, by) \text{ mit } a, b \in H, x, y \in K$$

Definition 5.6 (inneres direktes Produkt)
Sei G Gruppe und $H, K \triangleleft G$ mit

1. $H \cap K = \{1\}$
2. $HK = G$

Dann nennen wir G das innere direkte Produkt von H und K.

Satz 5.7
Ist G das innere direkte Produkt von $H, K \triangleleft G$, so gilt

$$G \cong H \times K$$

als Gruppe.

Beweis. Wir zeigen, dass $\varphi : H \times K \to G$ mit $(a, b) \mapsto ab$ ein Isomorphismus von Gruppen ist. Es gilt für alle $a, x \in H, b, y \in K$.

$$\varphi((a,b)) \cdot \varphi((x,y)) = abxy = axx^{-1}bxb^{-1}by = axby = \varphi((ax, by))$$

denn der Kommutator $x^{-1}bxb^{-1}$ liegt in $H \cap K = \{1\}$. (denn $x^{-1}bx \in K$, da $K \triangleleft G$, also $x^{-1}bxb^{-1} \in K$, genauso $bxb^{-1} \in H$, da $H \triangleleft G$, also $x^{-1}bxb^{-1} \in H$) Nach Annahme 1. ist φ surjektiv. Die Abbildung ist injektiv, denn

$$ab = xy \Rightarrow x^{-1}a = yb^{-1} \in G \cap K = \{1\} \Rightarrow x = a, y = b \quad \forall y, x \in H, b, y \in K.$$ □

▶ **Bemerkung**
In diesem Fall ist $G/H \cong K, G/K \cong H$

$$1 \longrightarrow H \longrightarrow G \longrightarrow K \longrightarrow 1$$

$$1 \longrightarrow K \longrightarrow G \longrightarrow H \longrightarrow 1$$

■ **Beispiel**
Sei $G = D_6$, also die Sachen, die man mit einem Hexagon machen kann.

$$H = \left\{1, r^3\right\} \cong \mathbb{Z}_2 \text{ und } K = \left\{s^j r^{2i} \mid i = 0, 1, 2, j = 0, 1\right\} \cong D_3$$
$$D_6 \cong \mathbb{Z}_2 \times D_3$$

Kompositionsreihen und Jordan-Hölder.

Definition 5.8 (Kette,Subnormale Reihe,einfache Kompositionsreihe)
Eine Reihe in G ist eine Kette von Untergruppen

$$G = G_0 > G_1 > G_2 > \cdots > G_d = \{1\} \text{ mit } G_{i+1} \neq G,$$

Eine subnormale Reihe ist eine in der $G_{i+1} \triangleleft G_i$ gilt ($G_i \triangleleft G$ für alle $i \Leftrightarrow$ "normale Reihe"). Eine Kompositionsreihe ist eine solche mit G_i/G_{i+1} einfach.

▶ **Bemerkung**
Nach dem Korrespondenztheorem heisst G_i/G_{i+1} einfach genau, dass $G_{i+1} \triangleleft G_i$ eine maximale normale Untergruppe ist.

$$\{L < G_i \mid G_{i+1} < L\} \xrightarrow{\pi} \{P < G_i/G_{i+1}\}$$

■ **Beispiel 5.9**
Sei $G = G_0 = S_4, G_1 = A_4, S_4/A_4 \cong \mathbb{Z}_2$ (nach 1. Isomorphiesatz, $A_4 = \ker \operatorname{sgn}$ mit $\operatorname{sgn} : S_4 \to \mathbb{Z}_2$).

Und die $G_2 = N = \{(12)(34), (13)(24), (14)(23), 1\}$ KLEINsche Vierergruppe. Dann

$$|A_4/N| = \frac{|A_4|}{|N|} = \frac{12}{4} = 3 \quad \text{Lagrange Theorem}$$
$$\Rightarrow A_4/N \cong \mathbb{Z}_3 = \mathbb{Z}/3\mathbb{Z} \text{ einfach.}$$

$$G_3 := \{1\}$$

$\{1\} \triangleleft H \triangleleft A_4 \triangleleft S_4$ ist Kompositionsreihe

$$\{1\} \longrightarrow N \longrightarrow A_4 \longrightarrow \mathbb{Z}_3 \longrightarrow \{1\}$$

$$\{1\} \longrightarrow A_4 \longrightarrow S_4 \longrightarrow \mathbb{Z}_2 \longrightarrow \{1\}$$

wobei $N, \mathbb{Z}_3, \mathbb{Z}_2$ einfach ist und A_4 gerade gebaut.

Satz 5.10
Ist G endliche Gruppe, so besitzt G eine Kompositionsreihe.

Beweis. Induktion nach $|G|$. Also $G = G_0$ gegeben

1. G einfach, dann $G_1 = \{1\}$ und ✓$G = G_0 \triangleright \{1\} = G_1$, also $G_0/G_1 = G$
2. G nicht einfach dann G_1 maximale normale Untergruppe, gibts da $|G| < \infty$. Dann $|G_1| < |G|$, also existiert nach Induktion Kompositionsreihe

   $$G_1 \triangleright G_2 \triangleright G_3 \triangleright \cdots \triangleright G_d \triangleright \{1\}$$

   Also $G_0 \triangleright G_1 \triangleright \ldots$ "tuts". □

■ **Beispiel**

- $G = \mathbb{Z}$ hat keine Kompositionsreihe, denn

  $$\mathbb{Z} = G_0 \triangleright G_1 \Rightarrow G_1 \cong \mathbb{Z}$$

- $$S_4 \triangleright A_4 \triangleright N \triangleright \{(), (12)(34)\} \cong \mathbb{Z}_2 \triangleright 1$$

mit $S_4/A_4 \cong \mathbb{Z}_2, N = \{(), (12)(34), (13)(24), (14)(23)\}, N/\{(), (12)(34)\} \cong \mathbb{Z}_2$

Satz 5.11 (Jordan-Hölder)
Sei G endliche Gruppe und seien $\{H_i\}_{i=0,\ldots,p}$ und $\{G_j\}_{j=0,\ldots,n}$ zwei Kompositionsreihe der Länge p. Dann gilt $p = n$ und ex existiert $\sigma \in S_{0,\ldots,n-1}$ mit

$$G_i/G_{i+1} \cong H_{\sigma(i)}/H_{\sigma(i)+1}$$

Beweis.

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{1\}$$
$$G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_p = \{1\}$$

Beweis erfolgt durch Induktion nach $m = \min(n, p)$

- $n = 1$ klar ✓, da

  $$G = G_1 \triangleright G_1 = 1, \text{ da } G = G_0/G_1 \text{ einfach}$$

  sei nun der Satz für alle Kompositionsreihen von Gruppen kürzer Länge bewiesen. Wäre $G_1 = H_1$, so könnten wir die Induktionsannahme direkt auf $G_1 = H_1$ anwenden und wir wären fertig. Annahme $G_1 \neq H_1$, so gilt auch $H_1 \not\lhd G_1, G_1 \not\lhd H_1$ (mit Korrespondenztheorem, $G/G_1, G/H_1$ einfach). Also ist $H_1 \cap G_1 \lhd G_1, H_1 \cap G_1 \lhd H_1$ echte Normalteiler. ($y \in H \cap K, x \in G, dann xyx^{-1} \in H, xyx^{-1} \in K, daH, K \triangleright G$). Betrachte eine Kompositionsreihe

  $$G_1 \cap H_1 = K_2 > K_3 > \cdots > K_n = 1 \text{ von } K_2 := G_1 \cap H_1$$

  Behauptung:

  $$G_1 > K_2 > ... > K_t = 1$$
  $$H_1 > K_2 > ... > K_t = 1$$

  sind Komposition, d.h. $G_1/K_2, H_1/K_2$ sind einfach. Mit 2. Isomorphiesatz folgt:

  $$G_1/G_1 \cap H_1 \cong G_1H_1/H_1 = H_1 = G/H_1$$

  denn aus $H_1, G_1 \lhd G$ folgt $H_1G_1 \lhd G$ und H_1, G_1 wären ja maximale normale Untergruppen H_0/H_1 ist aber einfach. Genauer $H_1/G_1 \cap H_1$ einfach also isomorph zu G_0/G_1. Vergleiche nun die Kompositionsreihen

  $$G_1 > G_2 > ... > G_n = 1$$
  $$G_1 > K_2 > ... > K_t = 1$$

  mit Induktion folgt $t = n$ und alles weitere. Sei $n = m$ oBdA. Genauso mit

  $$H_1 < H_2 ... H_1 < K_2 ...$$

Beweise zuerst folgende Behauptung:
Ist $G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_1 = 1$ Kompositionsreihe und $N \lhd G$, so ist $N = N \cap G_0 \triangleright N \cap N_1 \triangleright \ldots, \triangleright N \cap 1 = 1$ Kompositionsreihe (gegebenenfalls nach Auslassen von $N \cap G_1 = N \cap G_{i+1}$)

Beweis.

$$N \cap G_i/N \cap G_{i+1} = N \cap G_i/(N \cap G_i) \cap G_{i+1} \text{ mit } (G_{i+1} < G_1!)$$
$$\cong (N \cap G_1)G_{i+1}/G_{i+1} \lhd G_i/G_{i+1} \text{ einfach } \cong \text{ da 2. Isomorphiesatz}$$

Also $N \cap G_i/N \cap G_{i+1} \cong G_i/G_{i+1}$ oder $N \cap G_i/N \cap G_{i+1} \Leftrightarrow N \cap G_i = N \cap G_{i+1}$. □

1. Fall 1: $G_1 = H_1$ folgt mit Induktion

   $$G_i = H_1 \triangleright G_2 \triangleright \ldots \triangleright G_n = \{1\}$$
   $$G_i = H_1 \triangleright G_2 \triangleright \ldots \triangleright H_p = \{1\}$$

2. Fall 2: $G_1 \neq H_1$. Dann ist $G \cap H_1 \lhd G_1$ (nicht gleich!). Beachte Nach Korrespondenztheorem ist $H_1 \leq ...$ □

Letztes Mal: äusseres Produkt $\cong$ inneres Produkt $G = K \times L$, brauchte dazu

$$K, L \lhd G, K \cap L = \{1\}, KL = G \Leftrightarrow K \times L \to G \text{ mit } (a, b) \mapsto ab \text{ ist bijektiv}$$

Allgemeiner: Ist G Gruppe, $K \lhd G, L < G$ (nicht normal), so definiert jedes $x \in L$ einen Automorphismus von K:

$$\rho\colon L \to \mathrm{Aut}(K) \text{ mit } x \mapsto \rho_x, \rho_x(y) = xyx^{-1}, y \in K$$

Ist $K \cap L = \{1\}$, so ist $KL < G$ vollständig durch K, L, ρ gegeben.

Definition 5.12 (semidirekte Produkt)
Das semidirekte Produkt (äussere) zweier Gruppen K, L bezüglich eines Homomorphismus

$$\rho\colon L \to \mathrm{Aut}(K)$$

ist die Gruppe $G = K \rtimes_\rho L$, die $K \times L$ als Menge ist

$$(a, x)(b, y) = (a\rho_x(b), xy) \text{ mit } a, b \in K, x, y \in L$$

■ **Beispiel 5.13**
Sei $G = D_n$

$$\begin{aligned} K = \mathbb{Z}_n &= \left\{1, r, r^2, ..., r^{n-1}\right\} \text{ (Rotationen)} \\ L = \mathbb{Z}_2 &= \{1, s\} \ (s \text{ irgendeine Spiegelung}) \\ KL = D_n &= \left\{r^i, s^j \mid i = 0, ..., n-1, j = 0, 1\right\} = \mathbb{Z}_n \times \mathbb{Z}_2 \end{aligned}$$

als Menge.

Noch allgemeiner:
G Gruppe, $G = KL, K \cap L = \{1\}$, d.h. alle $g \in G$ können eindeutig als $xy = y$ mit $x \in K, y \in L$ geschrieben werden, aber $K \not\trianglelefteq G, L \not\trianglelefteq G$. G nennt man dann ein Bieressprodukt (Zappa-Zsep-Produkt, exakt Faktorisierung) (innere Version). K, L matched pair of groups (äussere Version).

■ **Beispiel 5.14 (Iwasawazerlegung)**

$$G = \mathrm{SL}(n, \mathbb{C}) \quad K = \mathrm{SU}(n)L = \left\{ \begin{pmatrix} \lambda_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & \lambda_n \end{pmatrix} \in \mathrm{SL}(n, \mathbb{C}) \mid \lambda_1, ..., \lambda_n \in (0, \infty) \right\}$$

Ausblick: Gruppentheorie = Studium von Symmetrie, z.B. $G < S_X$ (allgemeiner $G < \mathrm{Aut}(X)$, X könnte zum Beispiel topologischer Raum sein). Im 19. Jh. gab es nur die Transformationsgruppen G, mit $g \in G$ mit $g : X \to X$ Abbildung. Zum Beispiel $X = \mathbb{R}^3$ und $G = \mathrm{SO}(3)$ = Rotationen im Euklidischen Raum. Abstraktion $\to$ Algebra $\supseteq$ Gruppentheorie mit Definition wie in VL1.

Definition 5.15
Eine Wirkung einer Gruppe G auf eine Menge X ist ein Gruppenhomomorphismus

$$\rho \colon G \to S_X = \{f \colon X \to X \mid f \text{ bijektiv}\} \text{ mit } g \mapsto \rho_g \colon X \to X$$

d.h. eine Abbildung $G \times X \to X$ mit $(g, x) \to gx = \rho_g(x)$ mit $1x = x \forall x \in X, g(hx) = (gh)x \forall g, h \in G, x \in X$. (zb. Vektor und Matrix).

6. Permutationsdarstellungen und Gruppenoperationen

Allgemeines

Motivation: $H < G \Rightarrow G/H$
Notation: $x, y \in G$ konjugiert $\Leftrightarrow \exists g \in G \colon g^{-1}yg \Leftrightarrow \exists h \in G \colon x = hyh^{-1}$

Definition 6.1
Sei G Gruppe, $X \neq \varnothing$ Menge, S_X Permutationsgruppe von X. Dann

1. Eine Permutationsdarstellung ist ein Gruppenmorphismus

$$\theta \colon G \to S_X$$

2. Eine (linke) Operation von G auf X ist eine Abbildung

$$G \times X \to X \text{ mit } (g, x) \mapsto g \cdot x$$

so dass: $(\forall x \in X, \forall g, h \in G)$

- $g \cdot x = x$
- $(g \cdot h) \cdot x = g \cdot (h \cdot x)$

Satz 6.2
Es gibt eine bijektive Korrespondenz zwischen den Operationen von G auf X und den Darstellungen von G als Permutationen von X.

Beweis.

- Sei $\theta\colon G \to S_X$ eine Permutationsdarstellung. Definiere $G \times G \to X$, wobei $g \cdot x := \theta(g)(x)$

$$1 \cdot x = \theta(1)(x) = \mathrm{id}_X(x) = x$$
$$(gh) \cdot x = \theta(gh)(x) = \theta(g) \cdot \theta(h)(x) = \theta(g)(h \cdot x) = g(h \cdot x) \quad g, h \in G$$

ist Operation von G auf X.

- Sei $G \times X \to X$ mit $(g, x) \mapsto gx$ eine Operation. Für jedes $g \in G$: $\theta(g) := x \mapsto g \cdot x$ und damit haben wir $\theta\colon G \to \mathrm{Set}(X, X)$. Sei $g, h \in G$ und $x \in X$

$$\begin{aligned}\theta(gh)(x) &= (gh) \cdot x \\ &= g \cdot (h \cdot x) \\ &= g \cdot (\theta(g)(x)) \\ &= \theta(g)(\theta(h)(x)) \\ &= \theta(g) \cdot \theta(h)(x)\end{aligned}$$

also gilt $\theta(gh) = \theta(g) \cdot \theta(h)$.

$$\theta(1)(x) = 1 \cdot x = x \quad \forall x \in X \Rightarrow \theta(1) = \mathrm{id}_X$$

also θ Morphismus von Monoide.

$$\forall g \in G\colon \theta(g) \cdot \theta(g^{-1}) = \theta(g \cdot g^{-1}) = \theta(1) = \mathrm{id}_X = \theta(g^{-1}) \cdot \theta(g^{-1})$$

und wir haben $\theta(g)$ bijektiv mit Inverse $\theta(g^{-1})$ und damit $\theta\colon G \to S_X$ □

■ **Beispiel**
Setze Notation: $G \underset{\curvearrowright}{} X$ G operiert auf X.

1. $X \neq \varnothing$ Menge $\forall G < S_X \Rightarrow G$ operiert natürlich auf X.
2. D_n operiert auf P_n (reguläre Polygone mit n Seiten)
3. V Vektorraum $\Rightarrow \mathrm{GL}(V)$ operiert auf V
4. $G \underset{\curvearrowright}{} X \Rightarrow$
   - $G \underset{\curvearrowright}{} X^n$ mit $(x_1, \ldots, x_n) \in X^n$ und $g\colon (x_1, \ldots, x_n) := (g \cdot x_1, \ldots, g \cdot x_n)$
   - $G \underset{\curvearrowright}{} \mathcal{P}(X)$ und $A \subseteq X$, sowie $g \cdot A = \{g \cdot a \mid a \in A\}$
5. $H < G \Rightarrow G \underset{\curvearrowright}{} G/H$ und aH mit $g(aH) = (ga)H$

Morphismen

Definition 6.3
Ein Morphismus zwischen zwei Operationen (G, X) und (H, Y) ist ein Paar (φ, α), wobei

- $\varphi\colon G \to H$ Gruppenhomomorphismus

- $\alpha\colon X \to Y$ Abbildung
- $\forall g \in G$ und $x \in X\colon\ \alpha(g \cdot x) = \varphi(g) \cdot \alpha(x)$

$$\begin{array}{ccc} X & \xrightarrow{\alpha} & Y \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle \varphi(g)} \\ X & \xrightarrow{\alpha} & Y \end{array}$$

■ **Beispiel**
Sei $G = \mathbb{Z} \curvearrowright_{\mathbb{Q}} \mathbb{Z}_n = X, n \neq 0, \forall g \in \mathbb{Z}, \overline{x} \in \mathbb{Z}_n\colon g \cdot \overline{x} = \overline{g + x}$ ist nicht treu, da $\forall g \in \mathbb{Z}\colon (g + n) \cdot \overline{x} = \overline{g + n + x} = g \cdot \overline{x}$

$$\begin{array}{ccc} G & \xrightarrow{\theta} & S_X \\ \downarrow & \nearrow_{\overline{\theta}} & \\ G/\ker\theta & & \end{array}$$

also $\overline{\theta}$ injektiv $\Rightarrow G/\ker\theta \curvearrowright_{\mathbb{Q}} X$ treu.
Für $\mathbb{Z} \curvearrowright_{\mathbb{Q}} \mathbb{Z}_n\colon \ker\theta = n\mathbb{Z} \Rightarrow \mathbb{Z}_n \curvearrowright_{\mathbb{Q}} \mathbb{Z}_n$ treu, da

$$\begin{aligned} \overline{x}, \overline{y} \in \mathbb{Z}_n \quad k \in \mathbb{Z},\ \text{so dass } \overline{k} = \overline{x - y} \in \mathbb{Z}_n \\ k \cdot \overline{y} = \overline{k + y} = \overline{x - y + y} = \overline{x} \end{aligned}$$

Sei $n \in \mathbb{N}, n \geq 1$ und $\mathbb{Z} \curvearrowright_{\mathbb{Q}} \mathbb{Z}_n := \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}$, also $D_n \curvearrowright_{\mathbb{Q}} P_n$.

$$\begin{aligned} x \in \mathbb{Z}\colon x \cdot \overline{y} &:= \overline{x + y} \\ \alpha\colon \mathbb{Z}_n &\to P_n \\ \varphi\colon \mathbb{Z} &\to D_n \end{aligned}$$

(Als Beispiel kann man sich die P_5 nehmen und aufmalen ;)) Definiere $\varphi(1)$. Drehung von Zentrum Z um den Winkel $2\pi/n$.

$$\begin{aligned} \alpha(1 \cdot \overline{0}) &= \alpha(\overline{1}) \\ \varphi(1) \cdot \alpha(\overline{0}) &= \alpha(\overline{1}) \\ \Rightarrow (\varphi, \alpha)\colon&\ \text{Morphismus} \end{aligned}$$

Definition 6.4
- $H = G, \varphi = \mathrm{id}_G$, also ist G-Morphismus
- (φ, α) ist ein Isomorphismus, wenn φ Gruppenmorphismus und α Bijektion

Bahnen

Lemma 6.5
Sei $G \curvearrowright_{\mathbb{Q}} X$. Definiere eine Relation $\sim$ auf X:

$$\forall x, y \in X\colon x \sim y \Leftrightarrow \exists g \in G\colon y = y \cdot x$$

Dann ist $\sim$ eine Äquivalenzrelation.

Beweis.
- $x \sim x$, da $x = 1 \cdot x$

- $x \sim y \Rightarrow y \sim x$, da
$$\begin{aligned} y = y \cdot x &\Rightarrow g^{-1}y = y^{-1}(gx) \\ &\Rightarrow g^{-1}y = (g^{-1}y)x \\ &\Rightarrow g^{-1}y = x \end{aligned}$$
- $x \sim y$ und $y \sim z \Rightarrow x \sim z$, da
$$y = g \cdot x \text{ und } z = h \cdot y \Rightarrow z = h(g \cdot x) = (hg) \cdot x$$ □

Definition 6.6
- Für alle $x \in X$ Äquivalenzklassen von X: $G \cdot x := \{gx \mid g \in G\}$.
- Gx wird Bahn von x genannt und $|Gx|$ die Länge von Gx.
- $\forall x, y \in X$ entweder $Gx = Gy$ oder $Gx \cap Gy = \varnothing$:
$$X = \bigcup_{x \in X} G \cdot x$$

■ **Beispiel**
Sei $G = (\mathbb{R}, +)$ und $X = \mathbb{C}$:

1. Translation: $a \in \mathbb{C} \setminus \{0\}$ und $\forall \lambda \in \mathbb{R}, z \in \mathbb{C}$: $\lambda \cdot z := z + \lambda a$ (nicht transitiv). Ist treu, da
$$\begin{aligned} \forall \lambda_1, \lambda_2 \in \mathbb{R}, z \in \mathbb{C}\colon z + \lambda_1 a &= z + \lambda_2 a \\ &\Leftrightarrow z + \lambda_1 a = z + \lambda_2 a \\ &\Leftrightarrow (\lambda_1 - \lambda_2)a = 0 \\ &\Leftrightarrow \lambda_1 = \lambda_2 \end{aligned}$$

2. Drehungen: $\forall \lambda \in \mathbb{R}, z \in \mathbb{C}$ und damit $\lambda \cdot z = e^{2\pi i \lambda} z$ (nicht transitiv). Ist nicht treu, da
$$\begin{aligned} &\forall \lambda \in \mathbb{R}, \forall k \in \mathbb{Z}\colon \lambda \cdot z = (\lambda + k) \cdot z, \\ &\ker \theta = \mathbb{Z} \Rightarrow S^1 = \mathbb{R}/\mathbb{Z} \curvearrowright_{Q} \mathbb{C} \end{aligned}$$

Stabilisator

Sei $G \curvearrowright_{Q} X$ und $x \in X$.

Definition 6.7
Definiere $G_x := \{g \in G \mid g \cdot x = x\}$ als Stabilisator von x.

Lemma 6.8
Es gilt $G_x < G$.

Beweis.
- $1 \in G_x$: $1 \cdot x = x$
- $\forall g, h \in G_x \Rightarrow h \in G_x$ und $(gh)x = g(hx) = gx = x$
- Sei $g \in G_x \Rightarrow g^{-1} \in G_x$: $gx = x \Rightarrow g^{-1}(gx) = g^{-1}x$ und damit $x = 1x = (g^{-1}g)x$ □

... additions to previous example is missing, get from florian :(

Lemma 6.9
$G \curvearrowright_{Q} X$ und $\theta\colon G \to G_X$ assozierte Permutationsdarstellung. Dann
$$\ker \theta = \bigcup_{x \in X} G_x$$

Beweis.

$$\begin{aligned} g \in \ker\theta &\Leftrightarrow \theta(x) = \mathrm{id}_X \\ &\Leftrightarrow gx = x \quad \forall x \in X \\ &\Leftrightarrow g \in G_x \quad \forall x \in X \end{aligned}$$

□

Definition 6.10
$G \curvearrowright X$ ist treu genau dann, wenn

$$\theta\colon G \to S_X \text{ injektiv}$$
$$\forall g, h \in G\ (\forall x \in X\colon gx = hx) \Rightarrow g = h$$

Transitive Operationen

Definition 6.11

$G \curvearrowright X$ transitiv $\Leftrightarrow$ gibt genau eine Bahn

$$\Leftrightarrow x_0 \in X \quad X = G \cdot x_0$$
$$\Leftrightarrow \forall x, y \in X\colon \exists g \in G\colon y = gx$$

■ **Beispiel**
Betrachte

$$O(n) = \left\{A \in \mathrm{Mat}(n, \mathbb{R}) \mid A^T A = 1_n\right\} = \{A \in \mathrm{Mat}(n\mathbb{R}) \mid \|Ax\| = \|x\| \forall x \in \mathbb{R}^n\}$$

also $O(n) \curvearrowright S^{n-1} = \{x \in \mathbb{R}^n \mid \|x\| = 1\}$ (Drehungen und Spiegelungen in der S^2 zum Beispiel) ist transitiv.

Lemma 6.12
$G \curvearrowright G/H$ transitiv

Beweis. $g, h \in G$, dann $gH = gh^{-1} \cdot hH$ □

Theorem 6.13 (Die Struktur von Gruppenoperationen)

1. $G \curvearrowright X \Rightarrow \exists H < G$ und ein G-Isomorphismus durch $(G, X) \cong (G, G/H)$ ist transitiv. (H muss nicht eindeutig sein)
2. $H, K < G$, dann

   $$(G, G/H) \cong (G, G/K) \Leftrightarrow H \text{ und } K \text{ konjugiert}$$

   also linke Seite G-Isomorph und bei der rechten Seite: $\exists g_0 \in G\colon H = g_0 K g_0^{-1}$.

Beweis. 1.
- $\Leftarrow$: $H < G$: $G \curvearrowright G/H$ transitiv.
- $\Rightarrow$: Sei $G \curvearrowright X$ transitiv $x \in X$ beliebig und $X = Gx$. Definiere

  $$H := G_x \text{ und } \alpha : X \to G/H \text{ mit } gx \mapsto gH$$

  – Ist α wohldefiniert? Ja, da $\forall g, h \in G$ haben wir

  $$\begin{aligned} gx = hx &\Leftrightarrow h^{-1}gx = x \\ &\Leftrightarrow h^{-1}g \in G_x = H \text{ (siehe HA1.1 gilt)} \\ &\Leftrightarrow gH = hH. \end{aligned}$$

- α injektiv? $\forall g, h \in G\colon \alpha(gx) = \alpha(hx)$. (Gehe die Wohldefiniertheit rückwärts).
- α surjektiv? $\forall g \in G\colon gH = \alpha(gx)$
- Betrachte

$$\begin{array}{ccc} X & \xrightarrow{\alpha} & G/H \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g} \\ X & \xrightarrow{\alpha} & G/H \end{array}$$

$$\begin{aligned} \forall g \in G, y \in X g\alpha(y) &\stackrel{?}{=} \alpha(gy) \exists h \in G, y = hx \\ \alpha(gy) = \alpha(g(hx)) &= \alpha(ghx) \\ &= ghH = ghH = g\alpha(hx) \\ &= g\alpha(y) \end{aligned}$$

Also ist α G-Isomorphismus.

- Wir müssen zuerst ein Lemma zeigen:

> **Lemma 6.14**
> Sei $\alpha\colon X \to Y$ G-Isomorphismus, dann $\forall x \in X\colon G_x = G_{\alpha(x)}$

Beweis. α G-Isomorphismus gdw α bijektiv und $\forall x \in X\colon g\alpha(x) = \alpha(gx)$ und $\forall g \in G$

$$\begin{aligned} gx = x &\Leftrightarrow g\alpha(x) = \alpha(gx) = \alpha(x) \\ &\Rightarrow g \in G_x \Leftrightarrow g \in G_{\alpha(x)} \end{aligned}$$

□

- $\Rightarrow$: Sei $\alpha\colon G/H \to G/K$ ein G-Isomorphismus. Sei $g_0 \in G$, so dass $\alpha(H) = g_0K$. Wir haben Stabilisator von H in G

$$\{g \in G \mid gH = H\} = H$$

und der Stabilisator von gK in G

$$\{g \in G \mid g \cdot g_0K = g_0K\} = g_0Kg_0^{-1}$$

dann haben wir

$$\begin{aligned} gg_0K = g_0K &\Leftrightarrow g_0^{-1}gg_0K = K \\ &\Leftrightarrow g^{-1}gg_0 \in K \\ &\Leftrightarrow g \in g_0Kg_0^{-1} \end{aligned}$$

nun nutze das Lemma und es folgt $H = g_0Kg_0^{-1}$.

- $\Leftarrow$: Sei $g_0 \in G$ und nehme an $H = g_0Kg^{-1}$. Definiere $\alpha : G/H \to G/K$ mit $gH \mapsto gg_0K$.
  - α wohldefiniert: $\forall h, g \in G$

$$\begin{aligned} gH = gH &\Leftrightarrow h^{-1}g \in H = g_0Kg_0^{-1} \\ &\Leftrightarrow g_0^{-1}h^{\cdot 1}gg_0 \in K \\ &\Leftrightarrow (hg_0)^{-1}gg_0 \in K \\ &\Leftrightarrow gg_0K = hg_0K \end{aligned}$$

  - α injektiv
  - α surjektiv $\forall g \in G\colon\ gK = \alpha(gg_0^{-1}H)$.
  - $\forall g, h \in G\colon h\alpha(gH) = hgg_0K = \alpha(hgH)$.

  Also haben wir, dass α G-Isomorphismus ist. □

2.

Theorem 6.15 (Bahnen.Stabilisator-Satz)

$$G \curvearrowright_Q X \Rightarrow \forall x \in X \colon |Gx| = [G \colon G_x]$$

Beweis. Für alle $x \in X$ gilt $G \curvearrowright_Q Gx$ transitiv

$$\begin{aligned}(G, G_x) &\cong (G, G/G_x) \quad G\text{-Isomorph} \\ &\Rightarrow |Gx| = |G/G_x| = [G \colon G_x].\end{aligned}$$

□

Ausblick:

1. $G \curvearrowright_Q G$ durch Linksmultiplikation gegeben $\forall g, h \in G \colon g \cdot h = gh$
2. $H < G$, $G \curvearrowright_Q G/H$ durch Linksmultiplikation
3. $G \curvearrowright_Q G$ durch Konjugation $\forall g, x \in G \colon x^g := gxg^{-1}$
4. $G \curvearrowright_Q \mathcal{P}(G)$ durch Konjugation

Theorem 6.16
As G-Space, we have $G_x \cong G/G_x$.

■ **Beispiel**

- $G = \mathrm{SO}(3)$ Rotation im $\mathbb{R}^3$, dann $A \in \mathrm{SO}(3) \ni \mathrm{Mat}(3, \mathbb{R})$, $AA^T = 1$, $\det A = 1$, dann kann man sich das Skalarprodukt anschaun
  - (Wirkung durch Multiplikation) und nehme $x = (001)^T, G_x = S^2$ (Bahn, Orbit dieses Punkte ist S^2), Stabilisator $G_x = \mathrm{SO}(2)$
  - Allgemeiner: eingebettet in SO(3) durch

    $$\gamma \colon \mathrm{SO}(2) \to \mathrm{SO}(3) \text{ mit } B \mapsto \begin{pmatrix} B & 0 \\ 0 & 1 \end{pmatrix}$$

    ist Gruppenhomo. (also $S^2 \cong \mathrm{SO}(3)/\mathrm{SO}(2)$ und Erlangen Programm ...)
- Cayleys Satz $X = G$, α ist Gruppenstruktur. Hier gilt:

  $$G = \{1\} \forall x \in X = G \text{ mit } gx = x \Rightarrow g = 1$$

  durch Multiplikation von rechts mit x^{-1}. (Spezielle Situation, i.A. gibts kein xy für $x, y \in X$!) Insbesondere ist die Wirkung treu, also ρ injektiv und wir erhalten

  $$G \cong \rho(G) < S_G$$

- G Gruppe, $H < G$, $X = G/H$ mit Wirkung $g(hH) := (gh)H, g, h \in G$, transitiv, da $x = hH, y = tH$ ($x, y \in X$ beliebig), dann wähle $g := tH^{-1}$ meine Wahl ($\exists g \in G \; th^{-1}hH = gx =$

$y = tH$)

$G_x = \{g \in G \mid gx = x\}$ und $x = hH \quad gx = x \Leftrightarrow ghH = hH \Rightarrow h^{-1}gh \in H \Rightarrow g \in hHH^{-1} \in H$

Insbesondere $\ker \rho = \bigcap_{x \in X} G_x = \bigcap_{H \in H} hHh^{-1} \triangleleft G$

Dies ist $= H \Leftrightarrow H \triangleleft G$

- Adjungierte Wirkung: $X = G$ (wie oben) aber

  $g \triangleright x \cdot gxg^{-1}$

  ($\triangleright$ neues Symbol zum unterscheiden). $G_x =$ Konjugationsklassen von $x \in X = C(x)$ und

  $G_x = \{g \in G \colon gxg^{-1} = x \Leftrightarrow gx = xg\} = Z(x)$ Zentralisator

  Nutze Orbit-Stabiliser-Theorem:

  $$G/Z(x) \cong C(x) \text{ und } |C(x)| = \frac{|G|}{|Z(x)|}$$

  Die Konjugationsklassen mit nur einem Element bilden das Zentrum von G. Also gilt

  $$G = Z(G) \cup C(x_1) \cup \dots C(x_d)$$

  für geeignete $x_1, \dots, x_d \in G$

  $$|G| = |Z(G)| + \sum_{i=1}^{d} \frac{|G|}{|Z(x_i)|} \qquad \text{(class-equation)}$$

  (wobei die Vereinigung disjunkt sind)

Satz 6.17
Eine endliche p-Gruppe hat nichttriviales Zentrum.

Beweis. $|G| = p^n$ mit $p =$prim und dann

$$\begin{aligned} p^n &= |Z(G)| + \sum_{i=1}^{d} \frac{|G|}{|Z(x_i)|} \\ &= |Z(G)| + p^{n_1} + \dots + p^{n_d} \quad n > 0 \end{aligned}$$

Also ist $|Z(G)| \geq 1$ denn $1 \in Z(G)$ und $|Z(G)|$ ist teilbar durch p und damit ist $|Z(G)| \geq p$ □

Insbesondere ist G nicht einfach! ($Z(G) \triangleleft G$)

7. Die Sylow-Sätze

Sei G eine endliche Gruppe.

Definition 7.1
Eine Untergruppe von G ist eine maximale p-Untergruppe (für eine Primzahl p), d.h. $H < G$ und $\exists p$ prim, $n \in \mathbb{N}$: $|H| = p^{n+1} \nmid G$ (teil nicht).

Also $|G| = p^n \cdot m$ und $p \nmid m$.

Theorem 7.2 (alle Sylow-Sätze)
Mit der wie oben gilt:

1. Die Zahl r der Sylowschen Untergruppen von G ist 1 modulo p ($\exists s\colon r = 1+sp$). Insbesondere ist $r \neq 0$!
2. Jede p-Untergruppe von G ist in einer Sylowschen enthalten
3. Alle Sylowschen Untegruppen sind konjugiert zueinander. Insbesondere gilt: $r \mid m$. Also

$$H < G \quad |H| = p^n \quad N_G = N := \left\{g \in G \mid gHg^{-1} = H\right\} \quad |G/N| = r = \frac{p^n \cdot m}{p^n \cdot N/H}$$

da $m = r \cdot |N/H|$ und $|N| = |N/H| \cdot p^n$

Beweis. 1. Sei $X := \{P \subseteq G \mid |P| = p^n\} \ni \{x_1, \ldots, x_{p^n} \mid x_j \in G\}$. G wirkt auf X durch Multiplikation von links.

$$g\{x_1, \ldots, x_{p^n}\} = \{gx_1, \ldots, gx_{p^n}\}$$

Gesucht ist $H \subset X$ mit $H < G$. Für ein solches H ist dann $G/H \subseteq X$ eine Bahn der G-Wirkung mit der Länge $m = |G/H| = \frac{|G|}{|H|} = \frac{p^n m}{p^n}$
Behauptung 1: Alle Bahnen in X der Länge m sind von dieser Form.

Beweis (Beweis der Behauptung). Sei $GP \subseteq X$ eine Bahn mit $|GP| = m$. WLOG ist $1 \in P$ (wenn nicht, wähle $x \in P$ beliebig und ersetze P durch $x^{-1}P$)

$$G_P = \{g \in G \mid gP = P\} \quad P = \{1, x_2, \ldots, x_{p^n}\}$$
$$\text{und } gP = \{g1, gx_2, \ldots, gx_{p^n}\}$$

Also $1 \in P \Rightarrow G_P \subset P$ und daraus $|G_P| \leq |P| = p^n$. Aber wir wissen auch:

$$m = |GP| = |G/G_P| = \frac{|G|}{|G_P|} = \frac{p^n m}{G_P} \Rightarrow |G_P| = p^n. \qquad (*)$$

Also ist $G_P = P$. Damit folgt die Behauptung $G_p < G$.
Behauptung ($*$): Alle Bahnen in X, deren Länge nicht durch p teilbar ist, sind von der Form G/H □

Damit folgt 1.
Behauptung 2: Die einzige Nebenklasse gH, die eine Untergruppe von G ist, ist H selbst (H wie oben Sylowsche Untergruppe)

Beweis. gH Untergruppe $\Rightarrow 1 \in gH \Rightarrow g^{-1} \in H$ und daraus $g \in H$ und schließlich $gH = H$ □

Also existiert eine Bijektion zwischen den Sylowschen p-Untergruppen $H < G$ und den Bahnen $GP \subseteq X$ mit $|GP|$ nicht durch p teilbar.
Behauptung: Ist $[n] \in \mathbb{Z}_p$ die Klasse von $n \in \mathbb{Z}$ in $\mathbb{Z}_p$, so gilt

$$[r] = \frac{1}{[m]} \binom{|G|}{p^n}$$

▶ **Bemerkung**
$|X| = \binom{|G|}{p^n}$ per Definition von X als $\{P \subseteq G \mid |P| = p^n\}$

Nach Behauptung 1 und Behauptung 2 gilt $rm = \binom{|G|}{p^n}$ modulo p, denn X zerfällt in Bahnen, da G-Wirkung und die Bahnen deren Länge nicht durch p teilbar sind. Die Bahnen sind von der Form G/H für eine eindeutige, bestimmte Sylow p-Untergruppe H, haben die Länge m und es gibt r davon. Damit ist der erste Sylow-Satz bewiesen.
Yeah its scrambled again :/

▶ **Bemerkung**
Only $|G|$ enters here, we can compute r modulo p using any group G of the size $|G|$, z.B. können wir $G = \mathbb{Z}_{|G|}$, und in $\mathbb{Z}_{p^i m}$ gibt es genau eine Sylow p-Untergruppe, nämlich $\langle [m] \rangle = \{[e], [m], [2m], \dots, [(p^i - 1)m]\}$ (Erinnerung 1. Semester: $H \leq \mathbb{Z} \Leftrightarrow H = a\mathbb{Z} \dots$) $\Rightarrow$ 1.

2. Betrachte die Konjugationswirkung von G auf X

$$\mathrm{Ad}(g)P := \{gx^{-1}g, \dots, gx_{p^i}g^{-1}\}$$

Behauptung 3: Ist $P \leq G$ Sylow p-Untergruppe und $Q \leq P$ eine p-Untergruppe, so existiert $R = gPg^{-1}$ mit $aRa^{-1} \quad \forall a \in G$ $(N_G R \geq Q)$

Beweis. Betrachte den Orbit von P unter der adjungierten Wirkung

$$\mathrm{Ad}(G)P := \{gPg^{-1} \mid g \in G\} \cong G/N_G P \quad \text{orbit stabilizer}$$
$$(g \in N_G P \Leftrightarrow gPg^{-1} = P)$$

Dann gilt noch

$$p^i n = |N_G P| \Rightarrow |\mathrm{Ad}(G)P| = \frac{m}{n} \tag{$**$}$$

nicht durch p teilbar ($P \leq N_G P$). Jetzt wirken nur mit Q durch Konjugation auf diesen einen Orbit $\mathrm{Ad}(G)P$. $Q \leq G$, der eine Orbit zerfällt gegebenenfalls in mehrere. Jeder Teil ist von der Form

$$\{aRa^{-1} \mid a \in Q\} \quad \text{für ein } R \text{ von der Form} \quad R = gPg^{-1} \tag{$***$}$$

für ein $g \in G$

$$\mathrm{Ad}(G)R \cong Q/Q \cap N_G R$$

$\cong$ folgt aus orbit-stabilizer wieder und $N_G R$ sind die $a \in Q$ mit $aRa^{-1} = R$

$$|\mathrm{Ad}(Q)R| = \frac{|Q|}{|Q \cap N_G R|} = p^s$$

für ein s, denn Q war p-Untergruppe nach Annahme. Wegen ($**$) muss ein P existieren mit $s = 0$, d.h. $Q \subseteq N_G R$ □

Behauptung 5: R wie im Behauptung 4 ist eine Sylowsche Untergruppe und $Q \leq R$

Beweis. R ist Bild von P unter dem (inneren) Automorphismus $x \mapsto gxg^{-1}$ mit g aus ($***$) also ist R eine Sylowuntergruppe, da $Q \leq N_G R$ ist

$\{ab \in G \mid a \in Q, b \in R\} = QR \leq G$ eine Untergruppe
$a, a' \in Q, b, b' \in R \; ab \cdot a'b' =$ ... need to add still!

Dann $|QR| = |Q||R|/|Q \cap R| = \frac{p^j p^i}{Q \cap R}$, d.h. QR ist p-Untergruppe wegen $R \leq QR$ und R Sylow, also maximal, so folgt $QR = R \Rightarrow Q \leq R$ und das gibt uns den zweiten Sylow Satz. □

3. Ist der Spezialfall, in dem Q selbst eine Sylowuntergruppe war! Dann ist $Q = R$ im obigen Beweis, aber $R = gPg^{-1}$. □

Anwendungen

1. Cauchy's Satz: G endlich Gruppe $p \mid |G| \Rightarrow \exists g \in G$ mit $\mathrm{ord}(g) = p$ (p ist prim!)

Beweis. Sei $P \leq G$ eine Sylow p-Untergruppe, $|P| = p^i$. Für $x \in P$ gilt $\mathrm{ord}(x) \mid p^i$, d.h. $\mathrm{ord}(x) = p^s$, also hat $x^{p^{s-1}}$ die Ordnung p □

2. $|G| = pg$, $p \neq q$, p, q prim $\Rightarrow G$ nicht einfach.

Beweis. Sei $q < p$. Wieviele Sylow p-Untergruppen gibt es? Ist r diese Zahl, so ist $r = 1 \mod p$. jede davon hat p Elemente, d.h. ist isomorphic zu $\mathbb{Z}_p$. Sind P_1, P_2 zwei solche, so folgt $P_1 \cap P_2 = \{1\}$ (denn dies ist die einzige Untergruppe in $\mathbb{Z}_p$). Gäbe es mehr als eine Sylow p-Untergruppe, also mindestens $p+1$ Stück, wären deren Vereinigung eine Menge mit $1 \in \{1\} + (p+1)(p-1) = p^2$ Elementen und das ist ein Widerspruch also $|G| = pq < p^2$. □

Satz 7.3
Annahme wie oben, aber $q \nmid p-1$. Dann ist $G \cong \mathbb{Z}_{pq}$.

Beweis. Denke zusätzlich über Sylow q-Gruppen nach. Deren Zahl s ist 1 modulo q. Ausserdem teilt $\gamma, p \cdot q$, d.h. $\gamma = 1, \gamma = p, \gamma = q$ oder $s = pq$, damit die Sylowgruppen alle konjugiert sind zueinander sind. D.h. die Menge S_q der Sylow p-Untergruppe von G ist Orbit (eine Bahn) in $X = \{P \subseteq G \mid |p| = q\}$ unter Konjugation. Nach dem Stabilisator-Bahnen-Satz ist die Menge der Sylow q-Gruppen in einer Gruppe G also im Bijektion mit $G/N_G H$, wobei $H \leq G$ eine beliebige Sylow q-Untergruppe ist und $N_G H = \left\{x \in G \mid xHx^{-1} = H\right\}$ der Normalisator (Stabilisator von H unter der adjungierten Wirkung) von H in G ist. D.h. $G/N_G H$ ist die Menge der zu H konjugierten Untergruppen.

$$s = |G/N_G H| = \frac{|G|}{|N_G H|}$$

ist also die Zahl der zu H konjugierten Untergruppen. Insbesondere ist $H \leq N_G H$, also $|H||N_G H|$ und

$$s = \frac{G/H}{|N_G H|/|H|}$$

Wir haben in den Sylowsätzen 3. hinzugefügt, dass $\gamma \mid m$. Im unserer speziellen Situation heisst dies: s teilt p

$$|G| = pq \quad s = \#\text{ Sylow-}p\text{-Untergruppen}$$

$H \leq G$ beliebige solche Untegruppe, d.h. $|H| = q$, d.h. $H \cong \mathbb{Z}_q$ und $H \leq N_G H$

$$s = \frac{|G|/|H|}{|N_G H|/|H|} = \frac{(pq)/q}{n/q} = \frac{p}{n/q}$$

(n könnte pq ($s = 1$) oder q ($s = p$ sein). $s = \#$ Sylow q-Untergruppen in G mit $|G| = pq$ mit $p > q$. $S \mid p$ (nach Sylow 3.) folgt dann $s = 1$ oder $s = p$. $s = 1 \mod q$ (sylow 1.) folgt

$$s = 1, s = q+1, s = 2q+1, \ldots \qquad (*)$$

Wenn wir also noch annehmen $q \nmid p-1$, so fällt $s = p$ als Fall weg, wegen (∗). Also ist $s = 1$ und auch die Sylow q-Untergruppe ist eindeutig und somit normal.

$$\mathbb{Z}_p \cong \leq G \geq Q \cong \mathbb{Z}_q$$

Wir haben $H \cap Q = \{1\}$, also gilt $G \cong H \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ $G \cong R/I_1 \cap \ldots \cap I_d \cong \bigtimes_{i=1}^{d} R/I_i$. □

Satz 7.4
Sei H p-Sylow Untergruppe von G, H eindeutig, dann folgt damit H normal.

Beweis. Sei

$$\alpha \colon G \to G \text{ mit } y \mapsto yxy^{-1}$$

Automorphismus und $\alpha(H) \leq G$, $|\alpha(H)| = |H|$, dann folgt $\alpha(H) = H$ □

Satz 7.5
Ist $n = pq, p > q$ und $q \mid p-1$, so gibt es bis auf Isomorphie genau zwei Gruppen G der Ordnung n, die zyklische Gruppe $\mathbb{Z}_{pq}$ und eine nichtabelsche Gruppe, die ein semidirektes Produkt $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ ist.

Beweis. Wie oben gibt es eine eindeutige Sylow p-Untergruppe $H \cong \mathbb{Z}_p$. Wir haben oben gesehen, dass es entweder $s = 1$ oder $s = p$ Sylow q-Untergruppe gibt. Im Fall $s = 1$, gibt es eine eindeutige Sylow q-Untergruppe $Q = \mathbb{Z}_q$ und $G = \mathbb{Z}_p \times \mathbb{Z}_q$ (wie oben). Im Fall $s = p$ gibt es Sylow q-Untergruppen $Q_1, \ldots, Q_p$ und $Q_i \cong \mathbb{Z}_q \forall i \in [1, p]$ aber keine ist normal.

$Q_1 \cong \mathbb{Z}_q$ wirkt auf $H \cong \mathbb{Z}_p$ durch Konjugation und wie oben ist $Q_1 \cap H = \{1\}$. Also ist $HQ \leq G$ Untegruppe mit pq Elementen, also $HQ = G$ und dies ist ein internes semidirektes Produkt, $H \rtimes Q_1 = G$

$$G \cong \mathbb{Z}_p \times \mathbb{Z}_q = \mathbb{Z}_{pq}$$

Noch zu zeigen: 1. dieser Fall tritt auf, egal welche p, q wir betrachten.
2. und zwar auf eindeutige Weise bis auf Isomorphie. □

Satz 7.6 (Burnside)
Sei $|G| = p^i q^j$ (p, q Primzahlen). Dann G auflösbar (Auf jeden Fall nicht einfach!!!)

Beweis. to be done ... □

Definition 7.7
Ist G eine Gruppe und sind $(a, b) \in G^2$, so ist deren Kommutator

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

und die derivierte Gruppe G' also die von allem Kommutatoren erzeugte Untergruppe $G' \triangleleft G$

$$G \triangleright G' \triangleright G'' \triangleright ...$$

G auflösbar wenn n mit $G^{(n)} = \{1\}$

▶ **Bemerkung**
Sei $\alpha\colon G \to H$ Homomorphismus, also

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

Damit gilt $\alpha(G') \subseteq H'$. Insbesondere ($G = H$), G' ist eine charakteristische Untergruppe (invariant unter allen $\alpha \in \mathrm{Aut}(G)$) und $G' \triangleleft G$ ($\alpha(a) = xax^{-1}$)

■ **Beispiel**
Wenn G einfach ist, dann $G' = G$ oder $G' = 1 \Leftrightarrow G$ abelsch. Also einfach und äuflösbar $\Leftrightarrow G = \mathbb{Z}_p$.
$\mathrm{Aut}(G) = \{\alpha\colon G \to G \mid \alpha \text{ bijektiv}, \alpha(ab) = \alpha(a)\alpha(b) \forall (a, b) \in G\}$. Ist $x \in G$, so ist $\alpha_2(a) = xax^{-1}$ ein Automorphismus. Die Automorphismen dieser Form nennt man innere Automorphismen.

$$G \to \mathrm{Aut}(G) \text{ mit } x \mapsto \alpha_x$$

ist ein Gruppenhomomorphismus und es gilt

$$\begin{aligned}(\alpha_x \circ \alpha_y)(a) &= \alpha_x(\alpha_y(a)) = \alpha_x(gag^{-1}) \\ &= x(yay^{-1})x^{-1} = (xy)a(xy)^{-1} \\ &= \alpha_{xy}(a)\end{aligned}$$

für alle $a \in G$, also hat man $\alpha_x \circ \alpha_y = \alpha_{xy}$. Der Kern von $x \mapsto \alpha_x$ ist das Zentrum $Z(G)$ ($\alpha_x = \mathrm{id} \Leftrightarrow xa = ax \forall a \in G$). Das Bild von $x \mapsto \alpha_x$ ist die Gruppe $\mathrm{Inn}(G)$ der inneren Automorphismen. Diese ist normal: Ist $\beta \in \mathrm{Aut}(G)$, so gilt:

$$\begin{aligned}(\beta \circ \alpha_x \circ \beta^{-1})(a) &= \beta(\alpha_x(\beta^{-1}(a))) = \beta(x\beta^{-1}(a)x^{-1}) \\ &= \beta(x)a\beta^{-1}(x) \\ &= \alpha_{\beta(x)}(a)\end{aligned}$$

also $\beta \circ \alpha_x \circ \beta = \alpha_{\beta(x)}$ und es gilt $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$.

Definition 7.8
$\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ äussere Automorphismen.

Satz 7.9 (Klausur!!!)
G' ist die kleinste normale Untergruppe $N \triangleleft G$, für die G/N (G/G' abelsch) abelsch ist.

Beweis.
- $G \triangleleft G$ haben wir gesehen.
- G/G' abelsch

$$ab'bG' \cdot (aG')^{-1}(bG)^{-1} = [aG', bG']_{G/G'}$$
$$aba^{-1}b^{-1} = 1G'$$

nach Definition ($aba^{-1}b^{-1} \in G'$) (G abelsch $\Leftrightarrow \forall (ab) \in G^2 \colon aba^{-1}b^{-1} = 1$). Hier $a = aG', b = bG'$ und $1 = G'$.
- Ist umgekehrt G/N abelsch, so folgt $[aN, bN]_{G/N} = 1_{G/N} = 1N$, also $aba^{-1}b^{-1} \in N$; $\forall (a, b) \in G^2$. Also gilt $G' \leq N$. □

■ **Beispiel**
Sei $G = A_4$ und es gilt:

$$\begin{aligned}[(123), (234)] &= (123)(234)(123)^{-1}(234)^{-1} \\ &= (123)(234)(321)(432) \\ &= (14)(23) \in A_4'\end{aligned}$$

Ähnlich sieht man $(12)(34), (13)(24) \in A_4'$, d.h. $V \triangleleft A_4'$ und $A_4/V \cong \mathbb{Z}_3$ abelsch. Also ist $V = A_4'$, wobei $V = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ die kleinsche Vierergruppe ist.

▶ **Bemerkung**
$[a, b] \cdot [c, d]$ ist im Allgemeinen kein Kommutator, man muss G' schon echt erzeugen, passiert aber erst do ab $|G| = 90$.

■ **Beispiel**
$S_4' = A_4$, denn $A_4 \triangleleft S_4$, denn $A_4 = \ker \delta$ und $\delta \colon S_4 \to \mathbb{Z}_2$ mit $\delta(a) = \pm 1$ und $S_4/A_4 \cong \mathbb{Z}_2$ (mit ersten Isomorphiesatz $\mathrm{Inn}\, \delta = \mathbb{Z}_2$) ist abelsch:

$$S_4'' = A_4' = V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$
$$S_4''' = A_4'' = V' = 1$$

Also ist S_4 aufösbar. Aber: $n > 4 \colon S_n' = A_n$, doch A_n ist einfach, also $A_n' = A_n$, S_n also nicht auflösbar.

▶ **Bemerkung**
- $|G| = p^i q^j \Rightarrow G$ auflösbar (Burnside)
- $|G|$ ungerage $\Rightarrow G$ auflösbar (Feit-Thompson)

Satz 7.10 (Klausur!!!)
1. G auflösbar, $H \leq G \Rightarrow H$ auflösbar.
2. G auflösbar, $N \triangleleft G \Rightarrow G/N$ auflösbar
3. $N \triangleleft G$, N auflösbar, G/N auflösbar $\Rightarrow G$ auflösbar

Beweis.
1. $H' \leq G' \Rightarrow H'' \leq G'' \ldots H^{(n)} \leq 1 \Rightarrow H^{(n)} = 1$
2. $\pi \colon G \to G/N$ mit $a \mapsto aN$ surjektiver Gruppenhomomorphismus, da $\pi([a, b]) = [\pi(a), \pi(b)] \Rightarrow \pi(G') = \pi(G/N)'$. Nun verwende Induktion $\pi(G'') = (G/N)'' \ldots$

3. Umgekehrt: Wie in 2. projeziert die Reihe von G uf die von G/N, also

$$\begin{array}{ccccccc} G\triangleright & & G'\triangleright & & G''\triangleright & G'''\triangleright & \dots & G^{(n)} \\ \downarrow & & \downarrow & & \downarrow & \downarrow & \dots & \downarrow \\ G/N\triangleright & (G/N)'\triangleright & & (G/N)''\triangleright & & (G/N)'''\triangleright & \dots & (G/N)^n = 1 \end{array}$$

Also $(G/N)' = G'N/N$ (haben wir in 2.) ausgerechnet, nun anders geschrieben. Induktion: $G/N^{(n)} = G^{(n)}N/N$. Also $(G/N)^{(n)} = 1 \Leftrightarrow G^{(n)} \subset N$. Damit folgt aber, dass $G^{(n+1)} < N$ (wie in 1.) und $G^{(n+m)} < N^{(m)}$. Da N auflösbar, erhält man irgendwann 1. □

Satz 7.11
G auflösbar und endlich $\Leftarrow$ Alle Faktoren in einer Kompositionsreihe isnd abelsch und in der Form $\mathbb{Z}_n$ (zyklisch)

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_n = 1 \text{ und } G_i/G_{i+1} \text{ einfach}$$

Beweis.
- "$\Rightarrow$": Induktion nach der derivaten Länge $l := \min\{n \mid G^{(n)} = 1\}$
  - $l = 1$: G abelsch $\Rightarrow$ Behauptung
  - $l \to l+1$: Nach Korrespondenztheorem sind die Kompositionsfaktoren von G die von G/G' zusammen mit denen von G'
- Wieder Induktion, diesmal nach der Länge c einer Kompositionsreihe von G
  - $c = 1$: G abelsch und damit auflösbar
  - $c \to c+1$: Sei $G = H_1 \triangleright H_2 \triangleright \dots \triangleright H_c = 1$ eine Kompositionsreihe. Dann ist G/H_2 abelsch nach Annahme (denn $\cong \mathbb{Z}_n$) und $H_2 \triangleright \dots \triangleright H_c = 1$ ist eine kürzere Kompositionsreihe, also per Induktion H_2 auflösbar. Nach dem Satz ist G auflösbar ($H \triangleleft G$ auflösbar $\Rightarrow G$ auflösbar) G/H_2 auflösbar. □

8. nilpotente Gruppen

Definition 8.1
Zu einer Gruppe G definiert man die untere zentrale Reihe induktiv wie folgt

$$G = \Gamma_0(G) \triangleright \Gamma_1(G) \triangleright \Gamma_2(G) \triangleright \dots$$

durch $G = \Gamma_0$. Wobei $\Gamma_{i+1}(G)$ ist die durch alle Kommutatoren $[a,b]$, $a \in \Gamma_1(G), b \in G$ erzeugte Untergruppe.

▶ **Bemerkung**
$\Gamma_1(G) = G'$. G'' ist nur durch die $aba^{-1}b^{-1}$ mit $a, b \in G'$ erzeugt $\Gamma_2(G)$ enthält durch $aba^{-1}b^{-1}$ mit $b \notin G'$. Durch Induktion sehen wir: $G^{(n)} < \Gamma_n(G)$.

Definition 8.2
G nilpotent, genau dann wenn $\exists n \colon \Gamma_n(G) = 1$.

▶ **Bemerkung 8.3**
Es gilt die Hierarchie: Abelsche Gruppen $<$ nilpotente Gruppen $<$ auflösbare Gruppen

■ **Beispiel**
- S_3 ist auflösbar, aber nicht nilpotent, da

$$S_3' = A_3 = \{(), (123), (132)\} \cong \mathbb{Z}_3 \quad \text{abelsch} \quad S_3'' = A_3' = 1$$

Aber in $\Gamma_2(S_3)$ gibt es $(123)(12)(123)(12)^{-1} = (123)(12)(132)(132)(12) = (132)$ und somit $\Gamma_2(S_3) = \Gamma_1(S_3) = A_3$ und daraus folgt $\Gamma_n(S_3) \forall n \geq 1$, damit ist S_3 nicht nilpotent.
- $\mathbb{Z}_3 \times \mathbb{Z}_3, S_3 \cong D_3 \cong \mathbb{Z}_3 \times \mathbb{Z}_2$

Satz 8.4
Untergruppen und Quotienten von nilpotenten Gruppen sind wieder nilpotent.

Beweis. Siehe Beweis bei auflösbaren Gruppen. □

▶ **Bemerkung**
Es gilt NICHT: $N \triangleright G$ nilpotent, G/N nilpotent impliziert G nilpotent

Satz 8.5
$\Gamma_i(G \times H) = \Gamma_i(G) \times \Gamma_i(H)$ (impliziert G, H nilpotent $\Rightarrow G \times H$ nilpotent)

Beweis. Induktion nach $|G| = p^i$. Wir haben gesehen: Eine p-Gruppe hat $Z(G) \neq 1$. $|G| = 1$ trivial. Per Induktion ist $G/Z(G)$ nilpotent, da $G/Z(G) = \frac{|G|}{|Z(G)|} = \frac{p^i}{p^j} = p^s$. Also existiert $n \in \mathbb{N}$ mit $\Gamma_n(G/Z(G)) = 1$, d.h. $\Gamma_n(G) \subseteq Z(G)$. Schlussendlich haben wir $\Gamma_{n+1}(G) = 1$ und G ist nilpotent. □

Lemma 8.6
G nilpotent, $H \lneq G \Rightarrow H \lneq N_G(H)$.

Beweis. Sei i minimal mit $\Gamma_i(G) \leq H$. Da $H \neq G$, ist $i \geq 1$. Es gilt

$$[\Gamma_{i-1}(G), H] \leq [\Gamma_{i-1}, G] = \Gamma_i(G) \leq H$$

zum ersten Term in der Gleichung: von allen $aba^{-1}b^{-1}$ mit $a \in \Gamma_{i-1}(G), b \in H$ erzeugte Untergruppe, also ist $aba^{-1}b^{-1} \in H$ für $a \in \Gamma_{i-1}(G), b \in H$, d.h. $aba^{-1} \in H$ und $\Gamma_{i-1}(G) \leq N_G(H)$, $\Gamma_{i-1}(G) \gneq H$. □

■ **Beispiel**
Sei $B = \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \mid x, y, z \in K \right\}$, wobei $xz \neq 0$

$$\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} u & v \\ 0w & \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}^{-1} \begin{pmatrix} u & v \\ 0 & w \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} u & v \\ 0w & \end{pmatrix} \frac{1}{xz} \begin{pmatrix} z & -y \\ 0 & x \end{pmatrix} \frac{1}{uw} \begin{pmatrix} w & -v \\ 0 & v \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \frac{1}{xzuw}(xv + yw - zv - yu) \\ 0 & 1 \end{pmatrix}$$

damit ist dann

$$B' = \left\{ \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \mid s \in K \right\}$$

und $B'' = 1$, so B ist solvable. However ... if u need the pictures let me know, i have them, to bored to type it.

▶ **Erinnerung 8.7**
1. H, G nilpotent $\Rightarrow G \times H$ nilpotent

2. p-Gruppen nilpotent
3. G nilpotent, $H \leq G \Rightarrow H \lneq N_G(H) = \left\{x \in G \mid xyx^{-1} \in H \forall y \in H\right\} (H \triangleleft G \Rightarrow N_G(H) = G)$

Lemma 8.8
Sei G endliche Gruppe, $H \leq G$ Sylowgruppe. Dann gilt

$$N_G(N_G(H)) = N_G(H).$$

Beweis. Sei $x \in N_G(N_G(H))$, d.h. $xN_G(H)x^{-1} = N_G(H)$. Also gilt insbesondere

$$\tilde{H} := xHx^{\cdot 1} \subseteq N_G(H)$$

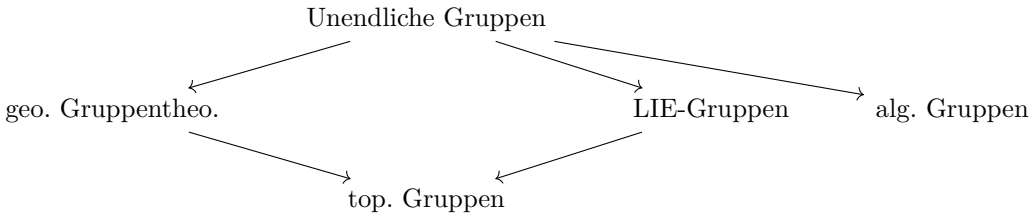
dann $H, \tilde{H}$ sind dann beides Sylowgruppen von $N_G(H)$. Also existiert nach Sylowsätzen ein $n \in N_G(H)$ mit $nHn^{-1} = \tilde{H}$. Aber $n \in N_G(H)$ heisst ja $nHn^{-1} = H$, also $H = \tilde{H}$. Also $x \in N_G(H)$. □

Satz 8.9
Eine endliche Gruppe ist nilpotent, genau dann wenn $G = \bigtimes_{i=1}^{d} H_i$, wobei die H_d ihre Syllowuntergruppe sind.

Beweis.
- $\Leftarrow$: folgt aus den Sätzen von VL 9.12.2019, bzw. aus den ersten beiden punkten der letzten Erinnerung.
- $\Rightarrow$ Sei $H \leq G$ eine Sylowuntergruppe. Ein Lemma sagt: $N_G(N_G(H)) = N_G(H)$. Also sagt dritte Punkt in der letzten Erinnerung, dass $N_G(H) = G$ gilt. Also gibt es für jedes $p \mid |G|$ genau eine Sylow p-Untergruppe, die normal ist. Sind H_1, H_2 zwei Sylowgruppen für verschiedene Primzahlen $p_1, p_2 \mid |G|$, folgt

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

  denn $H_1 \cap H_2 \leq H_1$, also (Lagrange) $(H_1 \cap H_2 = p_1^j)$, genau aber $H_1 \cap H_2 \leq H_2$, also $|H_1 \cap H_2| = p_2^k$, also $j = k = 0$, d.h. $H_1H_2 = H_1 \times H_2 \triangleleft G$ und jetzt Induktion nutzen. □



- Geometrische Gruppentheorie (Thom): Zunächst sind die Gruppen selbst nur Gruppen, aber man studiert durch ihre Wirkungen auf geometrische Objekte, z.B. Graphen, topologische Räume, HILBERT-Räume, Mannigfaltigkeiten, ...
  Die Gruppe G sind meist durch eine Repräsentation durch Erzeuger und Relatoren gegeben.

1. Freie Gruppen: Bei einem Vektorraum der Form $F(B) := k^B$ (frei über B) galt

   $$\mathrm{Hom}_{\mathrm{Vect}}(F(B), V) \cong \mathrm{Hom}_{\mathrm{Set}}(B, U(V))$$

   dann haben wir $F\colon$ Set $\to$ Vect Freie Funktor und $U\colon$ Vect $\to$ Set Vergissfunktor, $U(v)$ ist einfach die Menge V. Also bilden eine Adjunktion (siehe CAT-VL) $U \dashv F$.
   Genauer gibt es:

   $$F\colon \mathrm{Set} \to \mathrm{Grp}$$
   $$U\colon \mathrm{Grp} \to \mathrm{Set}$$

   mit $\mathrm{Hom}_{\mathrm{Grp}}(F(X), G) \cong \mathrm{Hom}_{\mathrm{Set}}(X, U(G))$. Die freie Gruppe $F(X)$ ist hierbei explizit konstruiert als die Menge aller Wörter $x_1, \ldots, x_d$ mit Buchstaben aus dem Alphabet $\left\{a, a^{-1} \mid a \in X\right\}$, die dann noch auf offenkundige Weise reduziert (gekürzt) werden.

■ **Beispiel**
$X = \{a, b\}$ $F(X)$ enthält z.B. $bab, b^3a, b^{-1}a^2, ...a^{-1}ab$ würde zu b gekürzt

Relationen sind vorgegebene Gleichung, die man festlegt um kleinere Gruppen als Quotienten von $F(X)$ zu definieren, also Präsentation einer Gruppe

$$\langle a, b \mid a^2, b^2, ababab \rangle$$

(Bemerkung: lässt man $ababab$ weg erhält man die Gruppe der Zöpfe (Braid groups)) $F(\{a, b\})/N$ wobei die kleinste normale Untergruppe ist, die $a^2, b^2, ababab$ enthält $a^2 = 1$ in $F(\{a, b\})/N$.
Übung $\langle a, b \mid a^2, b^2, ababab \rangle \cong S_3$

9. Exkurs: LIE-Algebra

i will add this, when there is some time left, but it was really extra and relevant for the exam ...

Kapitel II
Ringe

R sie kommutativer Ring mit 1-Element und V ein R-Modul.

▶ **Erinnerung 0.1**
Ist X eine Menge, so kann man ein

$$R^X = \{f\colon X \to R \mid f(x) = 0, \text{ für fast alle } x \in X\}$$

definieren Modul mit

$$+\colon R^X \times R^X \to R^X \text{ mit } (f+g)(x) = f(x) + g(x) \quad x \in X, f, g \in R^X$$
$$\cdot\colon R \times R^X \to R^X \text{ mit } (rf)(x) = r \cdot f(x)$$

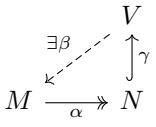
Ist V ein R-Modul und $X \subseteq V$ (X nicht unbedingt Untermodul), so erhält man einen Morphismus von R-Moduln (R-lineare Abbildungen)

$$S_x\colon R^X \to V \text{ mit } f \mapsto \sum_{x \in X} f(x) \cdot x$$

Also ist $\mathrm{Im}(S_X)$ die Menge aller Linearkombinationen von Elementen von X, d.h. $\mathrm{span}_R X$ bzw. der von X erzeugte Untermodul von V. X ist ein Erzeugendensystem von V, wenn $\mathrm{Im}(S_X) = V$ ist. Ein Modul heißt endlich erzeugt, wenn es ein $X \subseteq V$ mit $\mathrm{Im}(S_X) = V$ und $|X| < \infty$.
X ist linear unabhängig, wenn S_X injektiv ist, also $\ker S_X = 0$. Ist S_X bijektiv, also X ein linearer unabhängiges Erzeugendensystem, so nennt man X Basis von V. Ein Modul V der eine Basis enthält ist frei $V \cong R^X$. Also R Körper $\Rightarrow$ Jeder Modul (= VR) ist frei und $R^X \cong R^V \Leftrightarrow |X| = |Y| = \dim R^X$

■ **Beispiel 0.2**
Sei $R = \mathbb{Z}$, dann $\mathbb{Z}$-Moduln sind abelsche Gruppen, also ($4x = x + x + x + x$) durch $+$ in V festgelegt. $V = \mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}, X = \{1 + 2\mathbb{Z}\} = \{[1]\}$ ist Erzeugendensystem (sogar minimal). Aber X ist keine Basis, denn es ist nicht linear unabhängig, da $2 \cdot [1] = [0]$

Definition 0.3
Ein R-Modul V ist projektiv $\Leftrightarrow$ für jede Epimorphismus (surjektiv) $\alpha\colon M \to N$ von R-Moduln und jeden Morphismus $\gamma\colon V \to N$ gibt es einen Morphismus $\beta\colon V \to M$ mit $\alpha \circ \beta = \gamma$



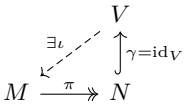
Satz 0.4
Für einen R-Modul V sind äquivalent

1. V ist projektiv
2. Jeder Epimorphismus $\pi\colon M \to N$ ist split, d.h. $\exists \iota\colon V \to M$ mit $\pi \circ \iota = \mathrm{id}$ (M R-Modul)
3. Es existiert ein R-Modul W mit $V \oplus W$, der frei ist

▶ **Bemerkung 0.5**
$W \subseteq V$ ist Komplement zu $U \subseteq V \Leftrightarrow \pi\colon V \to V/U$ ist isomorph und $\pi_{|W}\colon W \to V/U$

■ **Beispiel 0.6**
$\pi\colon \mathbb{Z} \to Z$ splittet nicht als $\mathbb{Z}$-Modulmorphismus. Also ist $\mathbb{Z}_2$ nicht projektiv.

Beweis (Satz 0.4). 1. $1 \Rightarrow 2$: Betrachte $(N = V,\ \gamma = \mathrm{id}_V,\ \alpha = \pi)$



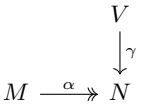
2. $2 \Rightarrow 3$: Jeder Modul V hat ein Erzeugendensystem, z.B. $V = X$ selbst. $S_X : R^X \to V$ ist ein Epimorphismus (R^X ist frei! X ist Basis bzw. $\{\delta_x\}_{x\in X}$ ist Basis ($f = \sum_{x\in X} f(x)\delta_x$)). V projektiv, existiert ein Splitting $\iota\colon V \to R^X$ mit $\pi \circ \iota = \mathrm{id}_X$, $\tilde{V} = \operatorname{Im}\iota$ ist dann ein Untermodul von R^X, der Isomorphismus zu V ist. Betrachte nun $\varepsilon = \iota \circ \pi\colon R^X \to R^X$. Dies ist ein idempotenter Morphismus, d.h.

$$\begin{aligned}\varepsilon \circ \varepsilon &= (\iota \circ \pi)(\iota\circ)\\ &= \iota \circ (\pi \circ \iota) \circ \pi\\ &= \iota \circ \mathrm{id} \circ \pi = \varepsilon.\end{aligned}$$

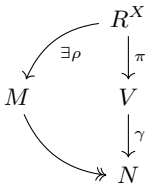
Somit gilt aber $R^X \cong \ker\varepsilon \oplus \operatorname{Im}\varepsilon$ mit $f \mapsto (f - \varepsilon(f), \varepsilon(f))$ und $\ker\varepsilon \cap \operatorname{Im}\varepsilon = 0$ $f = \varepsilon(g), \varepsilon(f) = 0$ heißt $\varepsilon(\varepsilon(g)) = \varepsilon(g) = f$. Also gilt $\operatorname{Im}\varepsilon = \operatorname{Im}\iota = \tilde{V} \cong V$. Denn $\varepsilon(f) = (\iota \circ \pi)(f) = \iota(\pi(f))$, also $\operatorname{Im}\varepsilon \subseteq \operatorname{Im}\iota$ und da π surjektiv ist gilt Gleichheit. $V = \tilde{V}$, da ι injekti ist, da $(\pi \circ \iota = \mathrm{id}_V)$ also $\ker\iota = 0$ und $V \cong V/\ker\iota \cong \operatorname{Im}\iota = \tilde{V}$. Also ist

$$V \oplus W \cong \tilde{V} \oplus W \text{ mit } W = \ker\varepsilon$$

3. $3 \Rightarrow 1$: Sei $V \oplus W \cong R^X$ frei und ein Diagramm der Form



folgt



(α Epimorphismus $R^X = V \oplus W$, $\pi\colon R^X \to V$, 1. Komponente $V \cong R^X/W$)
Für jedes Basiselement $\delta_x \in R^X (x \in X)$ existiert ein $m_x \in M$ mit $\alpha(m_x) = \gamma(\pi(\delta_x))$ (dann ist α surjektiv). Jetzt kommt die Freiheit: Jede Abbildung $\{\delta_x\}_{x\in X} \to M$ kann zu einer linearen Abbildung (eindeutig) $R^X \xrightarrow{\rho} M$ festgesetzt werden.

$$\mathrm{Mod}_R(R^X, M) \cong \mathrm{Set}(X, M)$$

Sprich $\exists!\rho\colon R^X \to M$ mit $\rho(\delta_x) = m_x$. Die Einschränkung von ρ auf das Untermodul $V \subseteq R^X$ (bzw. wenn man die Einbettung $V \to R^X$) mit ι bezeichnet $\rho \circ \iota$) liefert dies das gewünschte $\beta\colon V \to M$. □

■ **Beispiel 0.7**
$R \in C^\infty(\mathbb{R}, \mathbb{R})$ stetige Funktion von $\mathbb{R} \to \mathbb{R}$, $S \subseteq \mathbb{R}$ Teilmenge, z.B. $S = [0, 1]$,
$V = \{f \in C^\infty(\mathbb{R}, \mathbb{R}) \mid f(x) = \text{ für } x \notin S\}$ Untermodul von R selbst ist, d.h. $V \triangleleft R$ ist Ideal und

sogar Hauptideal.

$$V = p \cdot R, p = \chi_S, p(x) = \begin{cases} 0 & x \notin S \\ 1 & x \in S \end{cases}$$
$$p^2 = p, (1-p)^2 = (1-p) = \chi_{R \setminus S}$$

damit ergibt sich $R = p \cdot R \oplus (1-p)R = V \oplus W$

▶ **Erinnerung 0.8**

- Morphismus $R^n \to R^n$ ist gegeben durch Matrixmultiplikation. Die Projektion auf V ($\varepsilon \colon R^n = V \oplus W \to R^n$ with $(v, w) \mapsto v$) korrespondiert zu einer idempotenten Matrix. $e \in \mathrm{Mat}(n, R), e^2 = e$ und $V = e \cdot R = \{ex \mid x \in R\} = \mathrm{Im}(\varepsilon)$.
- projektiv gdw für alle Endomorphismen $M \xrightarrow{\pi} V$ split, also $M \cong V \oplus \ker(\pi)$ (V ist $\mathrm{Im}(\pi)$, Kern-Bild-Formel). Wenn V endlich erzeugt ist $V = \mathrm{span}\{x_1, \ldots, x_n\}$
- $\pi \colon V$ with $(v_1, \ldots, v_n)^T \mapsto \sum_{i=1}^n v_i x_i$ surjektiv. Also $V \cong R^n / ker(\pi)$

■ **Beispiel 0.9**
Sei $R = \mathbb{C}$, dann

1. $\mathbb{Z}$-Modul ist abelsche Gruppe
2. $\mathbb{C}(t)$-Modul ist $\mathbb{C}$-Vektorraum V und $\mathbb{C}$-lineare Abbildung $\pi \colon V \to V$

beide sind Hauptidealringe $(\mathbb{Z}, C(t))$ (HIR).

Definition 0.10
R ist ein HIR $\Leftrightarrow$ R ist Integritätsbereich (eng. integral domain, nullteilerfrei) (ID) und jedes Ideal $I \triangleleft R$ ist ein Hauptideal, d..h. es existiert $a \in R$ mit

$$I = R \cdot a = \{ra \mid r \in R\} = \{s \in R \mid a \mid s\}$$

($a \mid s$, entspricht a teilt s)

Ziel dabei ist: Endlich erzeugte Moduln über HIR haben eine Zerlegung (decompositon) $V = R \oplus T$ mit F frei und T Torsion.

Definition 0.11
Sei R ID, V R-Modul

1. $x \in V$ ist ein Torsionselement $\Leftrightarrow \exists r \in R, r \neq 0, r \cdot x = 0$
2. $T(V) = \{x \in V \mid x \text{ ist Torsionselement}\} \leq V$
3. V ist torsionsfrei, wenn $T(V) = 0$
4. Annihilator $\mathrm{Ann}_R(V) := \{r \in R \mid rx = 0 \forall x \in V\} \triangleleft R$

■ **Beispiel 0.12**

1. Da R ID ist, ist ein freier Modul torsionsfrei:
   $f \in R^\times, r \in R, r \neq 0, r \cdot f = 0$ heißt $(rf)(x) = r \cdot f(x) = 0 \forall x \in X \Leftrightarrow f(x) = 0 \forall x \in X$
2. Ist $R = \mathbb{Z}$ und V eine endliche abelsche Gruppe, so gilt $|V| \cdot x = 0 \quad \forall x \in V$ ($\mathrm{ord}(x) \mid \mathrm{ord}(V)$).
   Also ist $V = T(V)$.

▶ **Bemerkung**
$T(V) \leq V$ ist Untermodul (Übung!)

Lemma 0.13
$V/T(V)$ ist torsionsfrei. (R ID für den Rest der heutigen VL :S)

Beweis. Sei $X \in V/T$ Torsionselement x ist von der Form $X = [v] = v + T$ für ein $v \in V$. $T := T(V)$ x ist Torsionselement heißt: $\exists r \in R\backslash\{0\}\colon r \cdot x = 0$, d.h. $[rv] = [0]$, also $r \cdot v \in T$. Damit ergibt sich $\exists s \in R\backslash\{0\}\colon s(rv) = 0$ also $(sr)v = 0$. Da R ID ist, ist $t := sr \neq 0$, also ist $v \in T(V) = T$ und da bedeutet $[v] = x = 0$. □

Lemma 0.14
Sind $N \leq M$ Moduln, so gilt M ist Torsion ($(M = T(M))$) $\Leftrightarrow$ N ist Torsion ($N = T(N)$) und $M/n = T(M/N)$.

Beweis. Analog zu Lemma 0.13. □

Satz 0.15
Sei V endlich erzeugter, torsionsfreier R-Modul, $V = Span\{x_1, \ldots, x_n\}$ und $V \neq 0$.

1. $\exists i_1, \ldots, i_k\colon F = R\sum_{j=1}^{k} x_{i_j}$ ist frei mit Basis $\{x_{i_1}, \ldots, x_{i_k}\}$
2. V/F ist Torsionsmodul: $V/F = T(V/F)$
3. Existiert ein Morphismus, der injektiv ist $L\colon V \hookrightarrow F$

Beweis. Induktion nach n: (Beweis die ersten zwei Aussagen)

- $n = 1$: $V = R \cdot x \cong R$, da torsionsfrei, $V = Rx$ heißt es existiert ein Endomorphismus $\pi\colon R \to V$ mit $r \cdot x$ und wenn x kein Torsionselement ist, ist $\ker \pi = 0$ ($\nexists r \neq 0\colon rx = 0$, also ist π isomorph) und damit gilt Satz 0.15.
- $n-1 \to n$: OBdA ist $\{x_1, \ldots, x_n\}$ keine Basis, sonst wären wir fertig. (Mit $F = V$). Also existiert eine Linearkombination $0 = \sum_{i=1}^{n} r_i x_n$ oBdA mit $r \neq 0$, d.h. $\exists r = r_n \in R\backslash 0$ mit $r \cdot x_n \in \text{span}\{x_1, \ldots, x_{n-1}\} := W$. Behauptung: V/W ist Torsion: Denn ein Element in V/F ist von der Form: $[sx_n] = s[x_n]$ und $r[sx_n] = s[rx_n] = 0$, da $rx_n \in W$, also $[rx_n] = 0$ in V/W. Nach Induktionsannahme existiert Teilmenge $B \subseteq \{x_1, \ldots, x_{n-1}\}$, die einen freien Untermodul $G \subseteq W$ aufspannt und W/G ist Torsion. Nach dem 3. Isomorphiesatz gilt:

  $$V/G/W/G \cong V/W$$

  Also ist V/G ein Torsionsmodul (W/G Torsion, V/W und Lemma 0.13) und damit haben wir $F = V$.
- Nun zu der 3. Aussage: Da V/F Torsion ist existiert für jedes x_i ein $r_i \in R \setminus 0$ mit $r_i x_i \in F$, $r_i[x_i] = [r_i x_i] = [0] \Leftrightarrow r_i x_i \in F$. Sei $r := \prod_{j=i}^{n} r_j \neq 0$. Definiere $L\colon V \to F$ mit $x \mapsto rx$. Da R kommutativ ist, ist L R-linear. Da V torsionsfrei ist, ist L injektiv. Das Bild ist in F, da $V = \text{span}_R\{x_1, \ldots, x_n\}$ und

  $$r\left(\prod_{j=1}^{n} r_j x_j\right) = \prod_{j=1}^{n} r_j = a_1 r_2 \cdots r_n(\underbrace{r_1 x_1}_{\in F}) + a_2 r_1 r_3 \cdots r_n(\underbrace{r_2 x_2}_{\in F}) + \cdots \in F.$$

  □

Folgerung 0.16
Sei V endlich erzeugter R-Modul. Entweder ist V Torsion, $V = T(V)$ oder V enthält einen freien Untermodul F mit V/F Torsion.

Beweis. still TODO. □

three lectures missing :/

Theorem 0.17
$M(p) = M_1 \oplus \cdots \oplus M_k$ mit $M \cong R/Rp_i^n$ zyklisch und $\text{Ann}_R(x) = \{a \in R \mid ax = 0\} \lhd R$

▶ **Bemerkung**
Also sieht das so aus

$$M = R^s \oplus \left(\bigoplus_{i=1}^{n} R/Rp_i^{m_i} \right)$$

mit p prim und $m_i \geq 0$

Beweis. Induktion nach Zahl t der Erzeuger $m_1, \ldots, m_t$ von $M = M(p)$. Wir sind im Induktionsschritt und haben $n_1, \ldots, n_t$ gewählt mit $\mathrm{Ann}_R(m_i) = Rp^{n_i}$, d.h. $n_i = \min\{n \in \mathbb{N} \mid p^n m_i = 0, p^{n-1} m_i \neq 0\}$, also $n = \max\{n_1, \ldots, n_t\}$, oBdA $n = n_1$. Dann gilt insbesondere $p^n x = 0$ für alle $x \in M$.
Trick Betrachte M/Rm_1. Dies ist ein $t-1$ erzeugter p-primärer R-Modul, also zieht die Induktionsannahme. Also ist $M/Rm_i = R \cdot \bigoplus_{i=1}^{k} [x_i]$, wobei $[x_i] = x + Rm_i \subset M/Rm_i, x_i \in M$ und $\mathrm{Ann}_R([x_i]) = Rp^{s_i}$. Sei $a \in \mathrm{Ann}_R([x_i]) \Leftrightarrow a[x_i] = 0$ in $M/Rm_i \Leftrightarrow [ax_i = 0]$ in $M/Rm_i \Leftrightarrow ax_i \in Rm_i$. Also haben wir $p^{s_i} x_i = r_i m_1$ $(*)$ für irgendwelche $r_1, \ldots, r_k \in R$.
Erinnerung: $p^n x_i = 0$ (denn $p^n \in \mathrm{Ann}_R(M)$), daraus folgt $r_i = r_i' \cdot p^{s_i}$. Setze $y_i := x_i - r_i' m_1$. Dann ist $[x_i] = [y_i]$. Dann gilt $p^{s_i} y_i = p^{s_i} x_i - p^{s_i} r_i' m_1 = p^{s_i} x_i - r_i m_1 \overset{(*)}{=} p^{s_i} x_i - r_i m_1 = 0$. Betrachte $p^{s_i - 1} y_i = p^{s_i - 1} x_i - p^{s_i - 1} r_i' m_1 \neq 0$, denn ansonsten wäre $p^{s_i - 1} x_i \in Rm_1$, also $p^{s_i - 1} \in \mathrm{Ann}_R([x_i]) = Rp^{s_i}$. Also ist $\mathrm{Ann}_R(y_i) = \mathrm{Ann}_R([y_i]) = Rp^{s_i}$, wobei $\mathrm{Ann}_R(y_i)$ in M und $\mathrm{Ann}_R([y_i])$ in M/Rm_1 betrachtet wird. Es gilt nun

$$M/Rm_1 = R \bigoplus_{i=1}^{n} [y_i]$$

also

$$M = Rm_1 + Ry_1 + \cdots + Ry_k$$

Es blibt noch zu zeigen, das die Summe direkt ist! Setze $y_0 := m_1$. Sei $x \in Ry_i \cap \sum_{j \neq i} Ry_j$, dann ist zu zeigen, dass $x = 0$ ist. Also existiert $s_0, \ldots, s_k \in R$, sodass $x = (-s_i y_i) = \sum_{j \neq i} s_j y_j$, daraus folgt $\sum_{j=0}^{k} s_j y_j = 0$. Insbesondere gilt dies modulo Rm_1:

$$s_1[y_1] + \cdots + s_k[y_k] = 0 \quad ([y_0] = [m_1] = 0)$$
$$[s_1 y_1 + \cdots + s_k y_k] = 0$$

Aber:

$$M/Rm_1 = R \bigoplus_{i=1}^{k} [y_i]$$

hier eine direkte Summe. Also gilt schon $[s_j y_j] = 0$ für jedes $j = 1, \ldots, k$ allein. Also $s_j \in \mathrm{Ann}_R([b_j]) = \mathrm{Ann}_R(b_j)$ ("Das war der Witz!" $\Rightarrow x = 0$) und $s_j y_j = 0$ für $j \geq 1$. □

Satz 0.18
Ist M ein endlich erzeugter Modul über einem HIR R, so existieren $s, s_1, \ldots, s_k \in \mathbb{N}$ und $p_1, \ldots, p_k \in R$ prim mie

$$M \cong R^s \oplus \left(\bigoplus_{i=1}^{k} R/Rp_i^{s_i} \right)$$

Anders gesagt: Es existiert Erzeuger $e_1, \ldots, e_{s+k}$ in M mit $\sum_{i=1}^{s+k} r_i e_i = 0 \Leftrightarrow r_i e_i = 0$ für alle i genau, dann wenn $r_1 = \cdots = r_s = 0$ und $r_{s+j} \in Rp_j^{s_j}$ für $j = 1, \ldots, k$.

■ **Beispiel 0.19**

- $R = \mathbb{Z}$, dann folgt R-Moduln sind dasselbe wie abelsche Gruppen. Also erhalten wir eine Klassifikation der endlich erzeugten abelschen Gruppen. Hier ist $R^s = \mathbb{Z}^s, R/Rp_j^{s_j} = \mathbb{Z}_{p_j^{s_j}}$. Also $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ (Chinesischer Restsatz!). Insbesondere haben wir alle endlichen abelschen

Gruppen klassifiziert! (endlich $\Leftrightarrow s = 0 \Leftrightarrow M$ ist Torsion)

- Abelsche Gruppe der Ordnung 6. Gibt es nur eine $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, andererseits Ab. Gruppe der Ordnung 4. Gibt es zwei! $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$. Also

$$\left|\bigtimes_{i=1}^{k} \mathbb{Z}_{p_i^{s_i}}\right| = \left|\mathbb{Z}_{p_1^{s_1}}\right| \cdots \left|\mathbb{Z}_{p_n^{s_n}}\right| = p_1^{s_1} \cdots p_k^{s_k}$$

Anhang

Literaturverzeichnis

[1] Alperin, J. L., and Bell, R. B. Groups and representations. Springer, 2015.

[2] Artin, E. Galoissche Theorie. Deutsch, 1973.

[3] Bosch, S. Algebra. Springer Spektrum, 2013.

[4] Hungerford, T. W. Algebra. Springer, 1996.

[5] Jacobson, N. Lectures in abstract algebra. Springer, 1975.

[6] Lang, S. Algebra. Springer, 2008.

[7] Serre, J.-P. Linear representations of finite groups. Springer, 1977.

[8] Vinberg, E. B. A course in algebra. Universities Press, 2012.

Index