

Mitschrieb der Vorlesung

# **Darstellungstheorie I**

Wintersemester 2009/10  
Prof. Dr. Richard Dipper

8. Dezember 2009

Mitgeschrieben von Stefan Bühler

# Inhaltsverzeichnis

<b>I Unknown</b>	<b>3</b>
<b>II Gruppenkonstruktionen und Automorphismen</b>	<b>4</b>
<b>III Operationen von Gruppen auf Mengen</b>	<b>9</b>
<b>IV Basics und Bruhat-Zerlegung</b>	<b>18</b>
<b>V Die spezielle und projektive lineare Gruppen</b>	<b>24</b>
<b>VI Normalteilerstruktur</b>	<b>31</b>
Aufsatz von Jordan-Hölder . . . . .	31

# I Unknown

# II Gruppenkonstruktionen und Automorphismen

**Definition:** Sei  $X$  eine Menge. Die Freie Gruppe  $\mathbb{F}X$  über  $X$  wird wie folgt konstruiert:  
Ein Wort in  $\mathbb{F}X$  besteht aus einer endlichen Folge

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_k^{\varepsilon_k}, k \geq 0, \varepsilon_i \in \{-1, 1\}, x_i \in X$$

Das leere Wort ( $k = 0$ ) wird als 1 notiert.

Ist für ein  $1 \leq i < k$  in einem Wort  $x_i = x_{i+1}$  und  $\varepsilon_i = -\varepsilon_{i+1}$ , so können wir dieses Wort verkürzen, in dem wir  $x_i^{\varepsilon_i} x_{i+1}^{\varepsilon_{i+1}}$  entfernen.

Wörter, die nicht mehr verkürzt werden können, heißen unverkürzbar.

Der transitive, symmetrische und reflexive Abschluss des „Kürzens“ definiert eine Äquivalenzrelation;  $\mathbb{F}X$  ist als die Gruppe mit der Menge der Äquivalenzklassen dieser Relation definiert, wobei die Multiplikation durch Konkatenation der Vertreter definiert wird.

Zwei Wörter sind also äquivalent, wenn man durch Kürzen und Erweitern des einen Wortes das andere erhält.

$\mathbb{F}X$  ist Gruppe mit folgender universeller Eigenschaft:

$$\begin{array}{ccc} X & \xrightarrow{i} & \mathbb{F}X \\ & \searrow \forall f & \downarrow \exists! \hat{f} \\ & & G \end{array} \quad , \text{ so dass } \hat{f} \circ i = f \text{ und } \hat{f} \text{ Gruppenhomomorphismus.}$$

**Definition:** Man kann das freie Produkt  $G * H$  über den Gruppen  $G$  und  $H$  als Wörter über dem Alphabet  $G \cup H$  definieren.

Das freie Produkt hat folgende universelle Eigenschaft:

Sei  $\varphi : G \times H \rightarrow A$ ,  $G, H, A$  Gruppen,  $\varphi|_{G \times \{1_H\}}$  und  $\varphi|_{\{1_G\} \times H}$  jeweils ein Gruppenhomomorphismus,  $i : (g, h) \mapsto gh$ :

$$\begin{array}{ccc} G \times H & \xrightarrow{i} & G * H \\ & \searrow \forall \varphi & \downarrow \exists! \hat{\varphi} \\ & & A \end{array} \quad , \text{ so dass } \hat{\varphi} \circ i = \varphi \text{ und } \hat{\varphi} \text{ Gruppenhomomorphismus.}$$

**Definition:** Gruppen mit Erzeugenden und Relationen:  $X$  eine Menge,  $S \subseteq \mathbb{F}X$  „Relationen“.

Dann ist  $N := \langle \mathbb{F}X S \rangle$  die normale Hülle von  $S$ .

$G = \mathbb{F}X/N$  die Gruppe, die von  $X$  mit den Relationen  $S$  erzeugt wird;  $G := \langle X \mid S \rangle$ .

Beispiele:

i) Sei  $n \in \mathbb{N}, C_n = \{1, g, \dots, g^{n-1}\} = \langle x \mid x^n = 1 \rangle$

Bem:  $|X| \leq 1 \Leftrightarrow \mathbb{F}X$  ist kommutativ;  $\mathbb{F}X \cong \mathbb{Z} \Leftrightarrow |X| = 1$

ii)  $\sigma_n = \langle \{s_i \mid 1 \leq i < n\} \mid s_i s_j = s_j s_i \text{ für } |i - j| \leq 2, s_i^2 = 1, s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} \rangle$

Beachte:

$T \leq S \leq \mathbb{F}X \Rightarrow U := \langle \mathbb{F}X T \rangle \leq \langle \mathbb{F}X S \rangle =: V$

$\Rightarrow$  1. Iso Satz  $\exists$  Epimorphismus  $\mathbb{F}X/U \rightarrow \mathbb{F}X/v$

iii) Die endlichen einfachen Gruppen sind (durchweg?) von 2 Elementen erzeugt.

iv) Sei  $G$  Gruppe. Wähle  $X = G$ , nach universeller Eigenschaft  $\exists!$  Epimorphismus  $\mathbb{F}G \rightarrow G$  mit Kern  $N \Rightarrow G = \mathbb{F}G/N$

**Definition:** Seien  $G, H$  Gruppen. Das direkte Produkt  $G \times H$  ist das kartesische Produkt mit komponentenweiser Multiplikation.

$G \cong \tilde{G} := G \times \{1_H\} \trianglelefteq G \times H \trianglerighteq \{1_G\} \times H =: \tilde{H} \cong H$

for all  $g \in \tilde{G}, h \in \tilde{H} : gh = hg \Rightarrow \tilde{G}\tilde{H} = \tilde{H}\tilde{G} = G \times H, \tilde{G} \cap \tilde{H} = \{1_{G \times H}\}$

$\Rightarrow$  Wir müssen nicht zwischen externem und internem Produkt unterscheiden.

$|G \times H| = |G||H|$

Betrachte  $H, N \leq G, N \trianglelefteq G \Rightarrow HN = NH, HN \leq G$

Sei zusätzlich  $HN = G, H \cap N = \{1\}$

Sei  $n \in N$ . Wegen  $nHn^{-1} = H$  ist  $c_n : H \rightarrow H : h \mapsto {}^n h = nhn^{-1}$  ein Automorphismus von  $H$ .

$n \mapsto c_n$  ist Gruppenhomomorphismus  $N \rightarrow \text{Aut}(H)$ .

**Satz 1.2.1:** Sei  $g \in G, c_g : G \rightarrow G : h \mapsto {}^g h$  Automorphismus von  $G$ . Die Menge  $\text{Inn}(G) := \{c_g \mid g \in G\} \subseteq \text{Aut}(G)$  ist Normalteiler von  $\text{Aut}(G)$ .

$\text{Out}(G) := \text{Aut}(G)/\text{Inn}(G)$  (Gruppe der äußeren Automorphismen von  $G$ )

Die Abbildung  $c : G \rightarrow \text{Aut}(G) : g \mapsto c_g$  ist Gruppenhomomorphismus mit Bild  $\text{Inn}(G)$

(klar) und  $\ker c = Z(G) := \{g \in G \mid gh = hg \forall h \in G\}$

Also ist  $G/Z(G) \cong \text{Inn}(G)$

*Beweis.* Sei  $g, h_1, h_2 \in G$

$c_g(h_1 h_2) = gh_1 h_2 g^{-1} = gh_1 g^{-1} g h_2 g^{-1} = c_g(h_1) c_g(h_2)$

$c_{g^{-1}} \circ c_g(h) = g^{-1} g h g^{-1} g = 1 h 1^{-1} = c_1(h) = \text{id}_H$

Also ist  $c_g$  bijektiv und daher Automorphismus von  $G$ .

$c : g \rightarrow \text{Aut}(G)$  ist Homomorphismus:

$$c_{g_1} \circ c_{g_2}(h) = g_1 g_2 h g_2^{-1} g_1^{-1} = g_1 g_2 h (g_1 g_2)^{-1} = c_{g_1 g_2}(h)$$

$$\begin{aligned} c_g = id_G &\Leftrightarrow c_g(h) = h \forall h \\ &\Leftrightarrow ghg^{-1} = h \forall h \\ &\Leftrightarrow gh = hg \forall h \\ &\Leftrightarrow g \in Z(G) \\ &\Rightarrow \ker c = Z(G) \end{aligned}$$

Da im  $c = \text{Inn}(G)$  ist  $\text{Inn}(G) \leq \text{Aut}(G)$ .

Sei  $\varphi \in \text{Aut}(G), g \in G$ : Zu zeigen:  $\varphi \text{Inn}(G) \varphi^{-1} = \text{Inn}(G) \Leftrightarrow \varphi c_g \varphi^{-1} \in \text{Inn}(G) \forall g, \varphi$

$$(\varphi c_g \varphi^{-1})(h) = \varphi(g \varphi^{-1}(h) g^{-1}) = \varphi(g) h \varphi^{-1}(g) = \varphi(g) h \varphi(g)^{-1} = c_{\varphi(g)}(h) \forall h \in G$$

$$\Rightarrow \varphi c_g \varphi^{-1} = c_{\varphi(g)} \in \text{Inn}(G)$$

Also ist  $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$  □

Beachte: Sei  $N \leq G$ . Dann ist  $N \trianglelefteq G \Leftrightarrow c_g(N) = N \forall g \in G$

$$(\Rightarrow c_{g|_N} \in \text{Aut}(N). c_g \text{ ist } \in \text{Inn}(N) \Leftrightarrow \exists n \in N : c_g = c_n)$$

**Definition:** Sei  $H < G$ . Dann ist  $H$  charakteristisch in  $G$ , falls  $\varphi(H) = H \forall \varphi \in \text{Aut}(G)$ .

Klar:  $H$  char. in  $G \Rightarrow H \trianglelefteq G$ .

Beispiel:

$Z(G)$  ist char. in  $G$ :

$$\forall z \in Z(G), g \in G : \varphi(g) \varphi(z) = \varphi(gz) = \varphi(zg) = \varphi(z) \varphi(g)$$

$$\Rightarrow \varphi(z)G = G\varphi(z)$$

$$\Rightarrow \varphi(z) \in Z(G)$$

**Satz 1.2.2:** Seien  $K \leq H \leq G$ ,  $K$  charakteristisch in  $H$ ,  $H$  char. in  $G$ . Dann ist  $K$  char. in  $G$ .

*Beweis.* Sei  $\varphi \in \text{Aut}(G)$ . Zu zeigen:  $\varphi(K) = K$ .

$\varphi \in \text{Aut}(G) \Rightarrow H$  char. in  $G \Rightarrow \varphi(H) = H \Rightarrow \varphi|_H \in \text{Aut}(H) \Rightarrow \varphi(K) = \varphi|_K = K$ , da  $K$  char. in  $H$  ist. Also ist  $K$  char. in  $G$ . □

*Bemerkung.* Sei  $S \subseteq G$  mit  $S^{-1} = S$  und  $\varphi(S) = \{\varphi(s) \mid s \in S\} = S$  für alle  $\varphi$  in  $\text{Aut}(G)$  ( $\text{Inn}(G)$ ). Dann ist  $\langle S \rangle \leq G$  char. (normal) in  $G$ .

**Definition:** Sei  $G$  Gruppe,  $a, b \in G$ . Dann ist  $[a, b] = aba^{-1}b^{-1}$  der Kommutator von  $a$  und  $b$  ( $[a, b]ba = aba^{-1}b^{-1}ba = ab$ ).

Die Untergruppe  $G' := \langle [a, b] \mid a, b \in G \rangle \leq G$  heißt Kommutatoruntergruppe von  $G$ .

**Satz 1.2.3:** Sei  $G$  Gruppe. Dann ist  $G'$  char. in  $G$  (weil  $\varphi[a, b] = [\varphi[a], \varphi[b]] \forall \varphi \in \text{Aut}(G)$  ebenfalls Kommutator ist, und  $[a, b]^{-1} = [b, a]$ ).

$G'$  ist der kleinste Normalteiler von  $G$ , so dass  $G/G'$  abelsch ist (d.h. ist  $N \trianglelefteq G, G/N$  abelsch  $\Rightarrow N \supseteq G'$ ).

*Beweis.* Siehe Algebra. ( $\pi : G \rightarrow G/N : g \mapsto gN, \pi[a, b] = [\pi(a), \pi(b)] = \dots dG/N = N$ ), □

**Definition:** Seien  $N, H \leq G, N \trianglelefteq G, G = NH = HN, H \cap N = \{1\}$ . dann heißt  $G$  (internes) semidirektes Produkt von  $N$  mit  $H$ . Wir schreiben  $G = N \rtimes H$ .

Beobachtungen:

a)  $G/N = NH/N \cong H/N \cap H \cong H$ . Also ist  $G/N \cong H$ . Daher ist  $|G| = |N||G/N| = |N|absH = |N \times H|$

b)  $G = N \cdot H \Rightarrow \forall x \in G \exists n \in N \exists h \in H : x = n \cdot h$ . Diese Darstellung ist eindeutig: denn seien  $n_1, n_2 \in N, h_1, h_2 \in H$  und sei  $n_1 h_1 = n_2 h_2$ , so folgt  $n_2^{-1} n_1 = h_2 h_1^{-1} \in N \cap H \Rightarrow n_2^{-1} n_1 = h_2 h_1^{-1} = 1 \Rightarrow n_1 = n_2, h_1 = h_2$

c) Allgemein gilt:  $H, N \trianglelefteq G, H \cap N = \{1\} \Rightarrow hn = nh \forall n \in N, h \in H$ , denn seien  $h \in H, n \in N \Rightarrow [n, h] = nhn^{-1}h^{-1} = (nhn^{-1})h^{-1} \in H \cap N = \{1\}$  (die Klammerung analog für  $N$ )

Daher: Ist  $G = N \rtimes H$  und zusätzlich  $H \trianglelefteq G \Rightarrow G = H \times N$  (da  $n_1 h_1 n_2 h_2 = n_1 n_2 h_1 h_2$ )

d)  $G = N \rtimes H, x = n_1 h_1, y = n_2 h_2 \in G \Rightarrow x \cdot y = n_1 h_1 n_2 h_2 = n_1 (h_1 n_2 h_1^{-1}) h_1 h_2 =$

$(n_1^{h_1} n_2)(h_1 h_2) = n' h'$  die eindeutige Darstellung vom Produkt  $x \cdot y$  als Produkt eines Elementes aus  $N$  mit einem Element aus  $H$ .

Die Abb.  $\varphi : H \rightarrow \text{Aut}(N) : h \mapsto \varphi(h) = \lambda_n. {}^h n = \varphi_n = c_{n|_N} \in \text{Aut}(N)$  ist Gruppenhomomorphismus.

e) Multiplikation in  $G$  wird vollständig auf die Multiplikation in  $N$  und Multiplikation in  $H$  und auf  $\varphi$  zurückgeführt:  $n_1 h_1 n_2 h_2 = n_1 \varphi_{h_1}(n_2) h_1 h_2$

f) Ist  $\varphi : H \rightarrow \text{Aut}(N)$  der triviale Homomorphismus, so ist  $\varphi_n = c_{n|_N} = id_N$  für alle  $h \in H$ , d.h.  $\varphi_h(n) = hnh^{-1} = n \Leftrightarrow hn = nh$ . Dann ist  $H \trianglelefteq G$  und  $G \cong H \times N$ .

Daher: Ist  $\varphi : H \rightarrow \text{Aut}(N)$  nicht trivial, so kann  $G$  nicht abelsch sein. ( $\varphi(h) = \varphi_h \neq id_N, h \in H, \Rightarrow n \in N : \varphi_h(n) = hnh^{-1} \neq n \Rightarrow hn \neq nh$ )

**Definition:** Seien  $H, N$  Gruppen, und sei  $\varphi : H \rightarrow \text{Aut}(N) : j \mapsto \varphi(h) = \varphi_h \in \text{Aut}(N)$  ein Homomorphismus.

Wir definieren das (äußere) semidirekte Produkt  $G = N \rtimes H$  wie folgt:

Als Menge ist  $G$  einfach das kartesische Produkt  $N \times H$ .

Sei  $n_1, n_2 \in N, h_1, h_2 \in H :$

$$(n_1, h_1) \cdot (n_2, h_2) := (n_1 \cdot \varphi_{h_1}(n_2), h_1 \cdot h_2)$$

**Satz 1.2.4:** Mit obiger Multiplikation wird  $G = N \times H$  zur Gruppe  $N \rtimes H$  mit Einselement  $1_G = (1_N, 1_H)$  und Inverser  $(n, h)^{-1} = (\varphi_{h^{-1}}(n^{-1}), h^{-1})$

Seien  $\tilde{N} = N \times \{1_H\} \subseteq N \times H$  und  $\tilde{H} = \{1_N\} \times H \subseteq N \times H$ .

Dann ist  $\tilde{N} \trianglelefteq G, \tilde{H} \leq G, \tilde{N} \cong N, \tilde{H} \cong H$  und  $G = \tilde{N} \rtimes \tilde{H}$  (intern). Für  $\tilde{h} = (1_N, h) \in \tilde{H}, \tilde{n} = (n, 1_H) \in \tilde{N}, h \in H, n \in N$  ist  $\tilde{h}^{-1}\tilde{n}\tilde{h} = (\varphi_h(n), 1_H)$ , d.h.  $c_{\tilde{n}^{-1}|_{\tilde{N}}} \leftrightarrow \varphi_h \in \text{Aut}(N)$

*Beweis.* Übung. □

*Bemerkung.* Sind  $\varphi, \psi$  verschiedene Homomorphismen von  $H \rightarrow \text{Aut}(N)$ , so können  $N \rtimes_{\varphi} H, N \rtimes_{\psi} H$  isomorph oder nicht isomorph sein.

*Beispiel.*  $C_n (\cong (\mathbb{Z}/n\mathbb{Z}, +)) = N, H = C_2 = \{1, h\}$

$\varphi : H \in \text{Aut}(C_n)$  durch  $\varphi(1) = id_{C_n}, \varphi_h(x) = x^{-1}$

Die Gruppe  $D_{2n} := C_n \rtimes_{\varphi} C_2$  heißt Diedergruppe der Ordnung  $2n$ .

$D_{2n}$  ist die Gruppe der Symmetrien eines regelmäßigen  $n$ -Ecks;  $C_n \trianglelefteq D_{2n}$  ist die Gruppe der Rotationen,  $C_2 = D_{2n}/C_n$  sind die Spiegelungen.

$D_{2n} = \langle x, y \mid x^n = y^2 = 1, yxy = x^{-1} \rangle$



# III Operationen von Gruppen auf Mengen

Im folgenden sei:  $G =$  Gruppe,  $X =$  Menge,  $\sigma_X = \{f : X \rightarrow X \mid f \text{ bij. Abb.}\} =$  „symmetrische Gruppe auf  $X$ “.

**Definition:** Eine (Links-)Operation von  $G$  auf  $X$  ist eine (externe) Verknüpfung

$$G \times X \rightarrow X : (g, x) \mapsto gx$$

so dass gilt:

- i)  $1_G \cdot x = x \forall x \in X$
- ii)  $(gh) \cdot x = g \cdot (h \cdot x)$

Wir sagen: „ $G$  operiert auf  $X$ “ (durch Permutationen) oder kurz: „ $X$  ist  $G$ -Menge“. (Analog: Rechtsoperation:  $X \times G \rightarrow X$ )

*Bemerkung.* Ist  $X$   $G$ -Menge,  $\sigma_X =$  symmetrische Gruppe auf  $X$ , so wird durch  $\lambda : G \rightarrow \sigma_X : g \mapsto \lambda_g \in \sigma_X$  ein Gruppenhomomorphismus  $\lambda$  definiert, wobei  $\lambda_g : X \rightarrow X : x \mapsto g \cdot x$ ; denn: Sei  $g \in G : \lambda_g \lambda_{g^{-1}} : x \mapsto g(g^{-1}x) = (gg^{-1})x = 1_G x = x \forall x \in X$ , also ist  $\lambda_g$  bijektiv und  $\in \sigma_X$ .

Seien  $g, h \in G \Rightarrow \lambda_g \circ \lambda_h(x) = \lambda_g(\lambda_h(x)) = g \cdot (h \cdot x) = (g \cdot h) \cdot x = \lambda_{gh}(x) \forall x \in X \Rightarrow \lambda_g \lambda_h = \lambda_{gh}$ , d.h.  $\lambda$  ist Homomorphismus.

Umgekehrt: Sei  $\varphi : G \rightarrow \sigma_X$  homomorph. Dann wird durch  $g \cdot x := (\varphi(g))(x)$  eine Operation von  $G$  auf  $X$  definiert, mit  $\lambda = \varphi$  (Beweis: Übung).

$\lambda$  heißt „die zur  $G$ -Menge  $X$  gehörende Darstellung von  $G$ “.

Also: Das Konzept der  $G$ -Mengen  $X$  ist äquivalent zum Konzept der Homomorphismen  $G \rightarrow \sigma_X$ .

(Im Falle der Rechtsoperation: Entweder  $\text{op } \sigma_X$  auch von rechts, oder die zug. Darst.  $\rho : G \rightarrow \sigma_X$  ist ein Antihomomorphismus)

*Beispiele:* (Running Gag)

1.)  $\sigma_X$  operiert auf  $X$  mit Darstellung  $id_{\sigma_X} : \sigma_X \rightarrow \sigma_X : \pi \mapsto \pi \in \sigma_X, \pi x = \pi(x) \forall x \in X$

2.)  $G$  operiert auf der Menge  $G$  durch Linkstranslation  $g \cdot h = gh$ .

Darstellung:  $\lambda G \rightarrow \sigma_G : g \mapsto \lambda_g; \lambda_g : h \mapsto gh \forall h \in G$

( $|\sigma_G| = |G|!$ )

3.)  $G$  operiert auf  $G$  durch Konjugation:

$$g \cdot h = {}^g h = ghg^{-1} [= c_g(h)]$$

4.) Sei  $H \leq G$ ,  $G = \bigcup_{i \in I} g_i H$

Wir definieren eine Operation von  $G$  auf der Menge  $G/H$  der Nebenklassen von  $H$  in  $G$  durch:  $g(g_i H) = g_j H$  (bzw. auf  $I : g_i = j$ )

(Linkstranslation auf  $G/H$ , Rechtsnebenklassen  $H \backslash G$  durch Rechtstranslation)

Spezialfall:  $H = (I) \Rightarrow$  Operation von  $G$  auf  $G/H = G/(I) = G$  aus 2.)

4.) ist die Mutter aller  $G$ -Operationen auf Mengen.

**Definition:** Eine Operation von  $G$  auf  $X$  heißt treu, falls gilt: Ist  $gx = x \forall x \in X \Rightarrow g = 1$ .

Offensichtlich heißt dies für die zugehörige Darstellung  $\varphi : G \rightarrow \sigma_X$ , dass  $\varphi$  injektiv ist; denn

$$gx = x \forall x \in X \Leftrightarrow (\varphi(g))(x) = x \forall x \in X \Leftrightarrow \varphi(g) = id_X \Leftrightarrow g \in \ker \varphi$$

So:  $\ker \varphi = \{g \in G \mid gx = x \forall x \in X\}$ .

*Beispiele:* 1.), 2.) treu, da  $g \cdot h = h \forall h \in G \Leftrightarrow g = 1$

3.) (i.A.) nicht treu. Genauer:  $\ker \varphi = \ker c_g = \{g \in G \mid c_g = id_G\} = \{g \in G \mid c_g(h) = h \forall h \in G\} = \{g \in G \mid ghg^{-1} = h \forall h \in G\} = Z(G)$  Zentrum von  $G$ .

Klar:  $X$  treue  $G$ -Menge, so enthält  $\sigma_X$  durch die zugehörige Darstellung  $\varphi : G \rightarrow \sigma_X$  eine zu  $G$  isomorphe Untergruppe.

**Definition:** Seien  $X, Y$   $G$ -Mengen. Eine Abbildung  $\varphi : X \rightarrow Y$  heißt  $G$ -Homomorphismus (auch  $G$ -equivariant) falls gilt:

$$\forall x \in X, g \in G : \varphi(g, x) = g\varphi(x)$$

Wie üblich: Epi-, Mono- und Isomorphismen.

Komposition (und Inversen falls bijektiv) sind wieder Homomorphismen.

Isosätze etc.

Also: Kategorie der  $G$ -Mengen.

Übersetzung für Darstellungen:

Seien  $\varphi : G \rightarrow \sigma_X, \psi : G \rightarrow \sigma_Y$  ( $X, Y$  Mengen) Darstellungen.

Ein Morphismus von  $\varphi$  nach  $\psi$  ist eine Mengenabbildung  $f : X \rightarrow Y$ , so dass  $\forall g \in G$  das folgende Diagramm kommutiert:

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

d.h.  $f \circ \varphi(g) = \psi(g) \circ f \Leftrightarrow \psi(g) \circ f \circ \varphi(g)^{-1} = f \forall g \in G$

Dies macht die Klasse der (Permutations-) Darstellungen zu einer Kategorie. Diese ist isomorph zur Kategorie der  $G$ -Mengen (Beweis: Übung).

Ziel: Klassifikation von  $G$ -Mengen.

**Definition:**  $X, Y$   $G$ -Mengen:

- a) Die disjunkte Vereinigung  $X \dot{\cup} Y$  wird zur  $G$ -Menge durch  $g \cdot z = \begin{cases} gx & \text{für } z = x \in X \\ gy & \text{für } z = y \in Y \end{cases}$   
 („direkte Summe“, „Koprodukt“ in Kategorie der  $G$ -Mengen)
- b) Das kartesische Produkt  $X \times Y$  wird zu  $G$ -Menge durch  $g \cdot (x, y) = (gx, gy) \forall x \in X, y \in Y, g \in G$
- c)  $\sigma_X$  wird  $G$ -Menge durch  $gZ = \{gz \mid z \in Z\}$  für  $Z \subseteq X$

**Definition:** Sei  $X$  eine  $G$ -Menge,  $x \in X$ . Die Bahn (Orbit)  $Gx$  ( ${}^Gx$ ) ist  $\{gx \mid g \in G\} \subseteq X$ , und der Stabilisator  $Stab_G(x)$  in  $G$  von  $x$  ist  $\{g \in G \mid gx = x\} \subseteq G$ .

Für  $S \subseteq G$  ist der  $Stab_G(S) = \{g \in G \mid gs = s \forall s \in S\}$

Der Punktstabilisator von  $S$  in  $G$  ist  $PStab_G(S) = \{g \in G \mid gs = s \forall s \in S\} = \bigcap_{s \in S} Stab_G(s)$

Klar:

1.  $Stab_G(x), Stab_G(S), PStab_G(S)$  sind Untergruppen von  $G$ .
2. Die Einschränkung von der  $G$ -Operation auf die Bahn  $Gx$  macht die Bahn  $Gx$  von  $x$  zur  $G$ -Menge.  
 Wir definieren eine Äquivalenzrelation  $\sim_G$  auf  $X$  durch  $x \sim_G y \Leftrightarrow \exists g \in G : y = gx$   
 Die Äquivalenzklasse von  $x \in X$  ist die Bahn  $Gx$ .  
 Konsequenz:  $X$  ist die direkte Summe der Bahnen von  $G$  auf  $X$ .

**Definition:**  $G$  operiert (einfach) transitiv auf  $X$ , falls nur eine Bahn existiert, d.h.  $\forall x, y \in X : \exists g \in G : x = gy$ .

*Beispiele:* von 1.3.1

A) Bahnen:

- 1.)  $G$  ist die einzige Bahn.
- 2.)  $\forall h_1, h_2 \in G \exists g \in G : h_2 = gh_1 : g := h_2 h_1^{-1}$ , also:  $G$  ist die einzige Bahn.
- 3.)  $g \sim_G h \Leftrightarrow \exists x \in G : h = xgx^{-1} \Leftrightarrow g$  und  $h$  sind konjugiert  $\Leftrightarrow$  Bahnen sind Konjugationsklassen.
- 4.) Eine Bahn.  $g, h \in G \Rightarrow \exists x \in G : h = xg \Rightarrow hH = xgH$

B) Stabilisatoren:

- 1.)  $x \in X : Stab_{\sigma_X}(x) = \{\pi \in \sigma_X \mid \pi(x) = x\} = \sigma_{X \setminus \{x\}}$ , z.Bsp.  $Stab_{\sigma_n}(n) = \sigma_{n-1}$   
 $Stab_{\sigma_n}(\{1, \dots, i\}) = \{\pi \in \sigma_n \mid 1 \leq \pi(j) \leq i \forall 1 \leq j \leq i\} = \sigma_{\{1, \dots, i\}} \times \sigma_{\{i+1, \dots, n\}}$
- 2.)  $h \in G : Stab_G(h) = \{g \in G \mid gh = h\} = \{1\}$

3.)  $h \in G : Stab_G(h) = \{g \in G \mid {}^g h = h\} = \{g \in G \mid ghg^{-1} = h\} = \{g \in G \mid gh = hg\} =$   
 Zentralisator von  $h$  in  $G$ .

4.) Spezialfall  $Stab_G(1 \cdot H) = \{g \in G \mid gH = H\} = H$

**Lemma 1.3.5:** Sei  $X$   $G$ -Menge,  $x \in X, g \in G$ : Dann ist  $Stab_G(gx) = g \cdot Stab_G(x) \cdot g^{-1}$   
 („konjugierte Untergruppe“)

*Beweis.* „ $\supseteq$ “ Sei  $h = gfg^{-1} \in$  rechte Seite  $\Rightarrow h(gx) = gfg^{-1}gx = gfx = gx \Rightarrow h \in$  linke  
 Seite. „ $\subseteq$ “ Sei  $h \in Stab_G(gx)$ , d.h.  $h(gx) = gx \Rightarrow g^{-1}hgx = x \Rightarrow g^{-1}hx = f \in Stab_G(x) \Rightarrow$   
 $h = gfg^{-1} \in gStab_G(x)g^{-1}$  □

*Beispiele:* von 1.3.1, Stabilisator für 4.):  
 $Stab_G(xH) = xHx^{-1}$

Neues Beispiel für 1.3.1:

5.) Sei  $X = \{H \leq G\}$ . Dann operiert  $G$  auf  $X$  durch Konjugation  $l \text{sup} gH = gHg^{-1}$   
 $Stab_G(H) = \{g \in G \mid gHg^{-1} = H\} = N_G(H)$  der Normalisator von  $H$  in  $G$  (die größte  
 Untergruppe von  $G$  in der  $H$  normal ist,  $H \trianglelefteq N_G(H) \leq G$ )

*Bemerkung.* Bahnen sind in 5.) Konjugationsklassen von Untergruppen.  
 Beachte:  $|c_g(H)| = |gHg^{-1}| = |H|$

**Satz 1.3.6:** Jede  $G$ -Menge ist (eindeutig) disjunkte Vereinigung (direkte Summe) von transi-  
 tiven  $G$ -Mengen, nämlich der Bahnen von  $G$  auf der Menge.

**Satz 1.3.7:** Sei  $X$  transitive  $G$ -Menge und  $x \in X, H = Stab_G(x)$ . Dann ist  $X \cong G/H$   
 (=  $G$ -Menge der Nebenklassen von  $H$  in  $G$  durch Linkstranslation, siehe Beispiel 4. aus  
 1.3.1)

*Beweis.* Definiere  $\varphi : G/H \rightarrow X : gH \mapsto gx$  für  $g \in G$ .

- 1.)  $\varphi$  ist wohldefiniert: Denn sei  $gH = fH \Rightarrow f^{-1}g \in H \Rightarrow f^{-1}gx = x$ , da  $H = Stab_G(x)$   
 ist  $\Rightarrow gx = fx$
- 2.) Umgekehrt gehts auch: Sei  $fx = gx$  ( $f, g \in G$ )  $\Rightarrow x = f^{-1}gx \Rightarrow f^{-1}g \in H \Rightarrow gH = fH$   
 Also ist  $\varphi$  injektiv.
- 3.) Wegen  $G \cdot x = X$  ist  $\varphi$  surjektiv.
- 4.) Seien  $a, g \in G$ : Dann ist  $a\varphi(gH) = a(gx) = (ag)x = \varphi(agH)$ , also ist  $\varphi$  ein Isomorphis-  
 mus von  $G$ -Mengen.

□

**Korrolar 1.3.8:**  $|X| = |G/H| = [G : H]$

Allgemein: Sei  $X$   $G$ -Menge,  $x \in X \Rightarrow |Gx| = |G : Sta_G(x)|$  (Bahngleichung)

Wir haben jetzt isomorphe alle  $G$ -Mengen konstruiert, nämlich als disjunkte Vereinigung (direkte Summen) von  $G$ -Mengen der Form  $G/H$  mit  $H \leq G$ .

Frage: Sind  $H, K \leq G$ . Wann ist  $G/H \cong G/K$  als  $G$ -Menge (unter Linkstranslation)?

**Lemma 1.3.9:** Seien  $X, Y$   $G$ -Mengen,  $\varphi : X \rightarrow Y$  Homomorphismus, und sei  $x \in X$ . Dann ist  $\text{Stab}_G(x) \leq \text{Stab}_G(\varphi(x))$

Insbesondere: ist  $\varphi$  ein Isomorphismus, so ist  $\text{Stab}_G(x) = \text{Stab}_G(\varphi(x))$ .

*Beweis.*  $g \in G : gx = x \Rightarrow g(\varphi(x)) = \varphi(gx) = \varphi(x) \Rightarrow g \in \text{Stab}_G(\varphi(x)) \quad \square$

**Satz 1.3.10:** Seien  $H, K \leq G$ . Dann ist  $G/H \cong G/K \Leftrightarrow H =_G K$  (d.h.  $\exists g \in G : gKg^{-1} = H$ ).

Bemerkung: 1.3.6 + 1.3.9 liefert die Klassifikation der  $G$ -Mengen.

*Beweis.* Sei  $\varphi : G/H \rightarrow G/K$  ein Isomorphismus von  $G$ -Mengen,  $(\exists x \in G) : \varphi(1 \cdot H) = xK \Rightarrow \text{Stab}_G(1 \cdot H) = H = \text{Stab}_G(xK) = x \text{Stab}_G(1 \cdot K)x^{-1} = xKx^{-1}$ . Also ist  $H =_G K$ . Umgekehrt ist  $H =_G K$ , etwa  $K = xHx^{-1}$ . Dann ist (nach 1.3.4)  $K = \text{Stab}_G(xH)$ , und  $G/K \cong G/H$  nach 1.3.6  $\square$

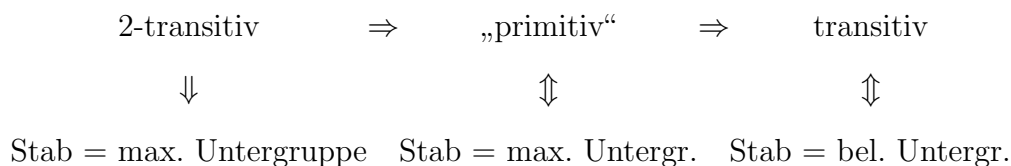
**Definition:** Sei  $k \in \mathbb{N}$ ,  $X$   $G$ -Menge. Dann heißt  $X$   $k$ -fach transitiv ( $k$ -trans.) falls gilt: Sind  $x_1, \dots, x_k \in X$  und  $y_1, \dots, y_k \in X$  jeweils beliebige aber paarweise verschieden, so gibt es  $g \in G : y_i = gx_i \forall 1 \leq i \leq k$

(Klar:  $G$  operiert auf  $X^{\times k} = X \times \dots \times X$   $k$ -trans.  $\Leftrightarrow G$  operiert auf  $\{(x_1, \dots, x_k) \in X^{\times k} \mid x_i \text{ paarweise verschieden}\}$  transitiv. 1-transitiv = transitiv)

**Satz 1.3.11:** Sei  $X$  2-transitive  $G$ -Menge,  $x \in X$ . Dann ist  $\text{Stab}_G(x)$  maximale Untergruppe von  $G$ .

*Beweis.* 2-transitiv  $\Rightarrow X$  ist transitiv  $\Rightarrow X \cong G/H$  für  $H = \text{Stab}_G(X)$ . Angenommen,  $H$  ist nicht maximal in  $G$ . Sei  $H < K < G, g \in G, g \notin K, k \in K, k \notin H$ . Dann ist  $kH \neq H, gH \neq H$ . Wir haben also zwei Paare  $(H, kH)$  und  $(H, gH)$ . 2-transitiv  $\Rightarrow \exists f \in G : f \cdot (1H) = (1H), f(kH) = gH \Rightarrow f \in H \Rightarrow fk \in K \Rightarrow \exists h \in H : fk = gh \Rightarrow K = fK = ghK = gK \Rightarrow g \in K$  Widerspruch!  $\square$

**Definition:** Eine transitive  $G$ -Menge  $X$  heißt primitiv  $\Leftrightarrow \forall x \in X : \text{Stab}_G(x)$  maximale Untergruppe von  $G$  ist.



**Satz 1.3.12:** Eine transitive  $G$ -Menge  $X$  ist primitiv  $\Leftrightarrow$  wenn gilt: Sei  $Y \subsetneq X, |Y| \geq 2$ . Dann gibt es für alle  $g \in G$  Elemente  $y, z \in Y$  mit  $gy \in Y, gz \notin Y$ .

Anwendungen:

**Satz 1.3.13:** Sei  $G$  endlich,  $H, K \leq G$ . Es gilt:

$$|H \cdot K| = \frac{|H| \cdot |K|}{|H \cap K|}$$

*Beweis.* Sei  $X = G/K$  eine  $G$ -Menge. Durch Einschränken ist  $G/K$  auch  $H$ -Menge.

Sei  $H_K$  die Bahn von  $K = 1 \cdot K$  unter dieser  $H$ -Operation.

Klar:  $H_K = \{hK \mid h \in H\}, HK = \bigcup_{h \in H} hK$ .

Also ist  $HK$  die Vereinigung von  $K$ -Nebenklassen von  $G$  mit Vertretern aus  $H$ .

Also ist  $|HK| = |{}^H K| \cdot |K|$ . Nach 1.3.7 ist  $|{}^H K| = |H : \text{Stab}_H(K)|$

$\text{Stab}_H(K) = \{h \in H \mid hK = K\} = K \cap H$ .

Also ist  $|HK| = |K| \cdot |{}^H K| = |K| \cdot |H : \text{Stab}_H(K)| = |K| \cdot |H : (H \cap K)| = |K| \cdot \frac{|H|}{|H \cap K|}$   $\square$

Konjugationsop:  $|G| = n \in \mathbb{N}, 1 = g_1, g_2, \dots, g_k$  seien Vertreter der Konjugationsklassen von  $G$ .

$\mathcal{C}_i := {}^G g_i = \{gg_i g^{-1} \mid g \in G\}$  Bahn

$C_i = \text{Stab}_G(g_i) = C_G(g_i) = \{h \in G \mid hg_i = g_i h\} \leq G$

**Satz 1.3.14:** Klassengleichung: Sei  $|G| = n$ .

$$n = 1 + \sum_{i=2}^k |G : C_i| = |Z(G)| + \sum_{i=1, \dots, k, g_i \notin Z(G)} |G : C_i|$$

*Beweis.* Ohne Einschränkung:  $Z(G) = \{g_1, \dots, g_l\}, 1 \leq l \leq k \Rightarrow C_i = G \forall i = 1, \dots, l, C_i = \{g_i\}$

Mit 1.3.7  $\Rightarrow \sum_{i=1, \dots, k} |{}^G g_i| = |\mathcal{C}_i| = [G : C_i] = [G : \text{Stab}_G(g_i)]$   $\square$

**Definition:** Sei  $G$  endliche Gruppe,  $G^1 = [G, G]$ . Definiere  $D^i(G) (i \in \mathbb{N})$  durch

1.  $D^1(G) = G^1$
2.  $i > 1 : D^i(G) = [D^{i-1}(G), D^{i-1}(G)]$

Klar:  $D^i(G) \trianglelefteq D^{i-1}(G)$  und  $D^{i-1}(G)/D^i(G)$  abelsch.

$G$  heißt auflösbar, falls  $D^k(G) = (1)$  für ein  $k \in \mathbb{N} \Leftrightarrow \exists (1) = N_1 \leq N_2 \leq \dots \leq N_m = G$  mit  $N_i \trianglelefteq N_{i+1}$  und  $N_{i+1}/N_i$  abelsch (zyklisch, zyklisch von Primzahlordnung nach Korrespondenzsatz).

Kann man zusätzlich  $N_i$  so wählen, dass  $N_i \trianglelefteq G$  ist, so heißt  $G$  Überauflösbar („supersolvable“).

$N \trianglelefteq G$ : mit  $N$  auflösbar,  $G/N$  auflösbar  $\Leftrightarrow G$  auflösbar.

Sei  $Z_i(G)$  induktiv durch folgendes definiert:

- i)  $Z_1(G) = Z(G) \trianglelefteq G$  (charakteristisch)
- ii)  $Z_2(G)$  ist volles Urbild von  $Z(G/Z(G))$  in  $G$  unter natürlicher Projektion  $G \rightarrow G/Z(G)$ .  
Beachte: Nach Korrespondenzsatz (1.2.10) gilt:  $Z_2(G) \trianglelefteq G$ .  
( $Z_2(G) = \{g \in G \mid gZ(G) \in Z(G/Z(G))\}$ )
- iii)  $i > 1$ :  $Z_i(G)$  ist volles Urbild von  $Z(G/Z_{i-1})$  in  $G$ ,  $Z_i(G) \trianglelefteq G$ .

Haben: (1) =  $Z_1(G) \trianglelefteq Z_2(G) \trianglelefteq \dots \trianglelefteq Z_i(G) \trianglelefteq \dots$   
 $Z_i(G)/Z_{i-1}(G)$  abelsch,  $Z_i(G) \trianglelefteq G$ . (Beweis: Übung)  
 $G$  heißt nilpotent, falls  $\exists k \in \mathbb{N} : Z_k(G) = G$ .

Beachte: nilpotent  $\Rightarrow$  überauflösbar  $\Rightarrow$  auflösbar

**Korollar 1.3.15:** Sei  $G$  eine  $p$ -Gruppe,  $p$  Primzahl (d.h.  $\exists t \in \mathbb{N} : |G| = p^t$ ), Dann ist  $|Z(G)| > 1$ .

Insbesondere ist  $G$  nilpotent.

*Beweis.*  $x \in G, x \notin Z(G) \Rightarrow C_G(x) \subsetneq G \Rightarrow [G : C_G(x)]$  wird von  $p$  geteilt.

Klassengleichung:  $|G| = p^t = |Z(G)| + \sum_{i=1}^k |G : C_G(g_i)|$

$p$  teilt  $|G : C_G(g_i)| \Rightarrow p$  teilt die Summe  $\Rightarrow p$  teilt  $|Z(G)|$ .

Rest: Übung. □

*Bemerkung.* Berühmte Ergebnisse:

- I) Burnside's  $pq$ -Theorem: Seien  $p, q$  Primzahlen,  $|G| = p^a \cdot q^b, a, b \in \mathbb{N} \Rightarrow G$  ist auflösbar.
- II) Feit-Thompson: Ist  $2 \nmid |G| \Rightarrow G$  ist auflösbar.

Beachte: Sei  $H \leq G$ . Dann ist  $H \trianglelefteq G \Leftrightarrow H$  ist Vereinigung von (disjunkten) Konjugationsklassen von  $G$ ; denn  $gHg^{-1} = H \forall g \in G$  gilt genau dann, wenn  $\forall h \in H, g \in G : c_g(h) = ghg^{-1} \in H$ , d.h.  ${}^G h \subseteq H$ . Daher ist  $|H| = \sum_{g_i \in H} |C_i|$

Erinnerung: Sei  $H \leq G$ . Dann ist  $N_g(H) = \{g \in G \mid gHg^{-1} = H\} \leq G$  und  $H \trianglelefteq N_G(H) =$  die eindeutig bestimmte größte Untergruppe von  $N$ , in der  $H$  normal ist.  $H \trianglelefteq G \Leftrightarrow N_G(H) = G$ .

**Satz 1.3.16:** Sei  $|G| = n < \infty$ , und sei  $H \leq G$ . Sei  $\mathcal{A} = \{gHg^{-1} \mid g \in G\}$ . Dann ist  $|\mathcal{A}| = |G : N_G(H)|$ .

*Beweis.*  $G$  operiert auf  $\sigma(G)$  ( $\{K \leq G\}$ ) per Konjugation, und  $\mathcal{A}$  ist gerade die Bahn  ${}^G H$  von  $H$  unter dieser Operation.  $N_G(H) = \text{Stab}_G(H)$ . So folgt die Behauptung aus 1.3.7. □

**Definition:**  $H, K \leq G, z \in G$ . Dann heißt  $H z K = \{h z k \mid h \in H, k \in K\}$  die  $H$ - $K$ -Doppelnebenklasse von  $z$ .

Definiere  $\sim$  auf  $G$  durch  $, y \in G$ , so ist  $x \sim y \Leftrightarrow \exists h \in H, k \in K : y = h x k$

- i)  $x = 1_H x 1_K \Rightarrow x \sim x \forall x \in G$
- ii)  $y = h x k \Rightarrow x = h^{-1} y k^{-1} \Rightarrow$  Symmetrie
- iii)  $y = h_1 x k_1, z = h_2 y k_2 \Rightarrow z = h_2 h_1 x k_1 k_2 \Rightarrow x \sim z$

Also ist  $G$  disjunkte Vereinigung der  $H$ - $K$ -Doppelnebenklassen.

Klar:  $H z K = \bigcup_{h \in H} h z K = \bigcup_{k \in K} H z k$  ist (disjunkte) Vereinigung von  $K$ -Links- bzw  $H$ -Rechtsnebenklassen in  $G$ .

**Satz 1.3.17:** Sei  $|G| = n < \infty, H, K \leq G$  und  $z \in G$ . Dann gilt:

$$|H z K| = \frac{|H| \cdot |K|}{|H \cap z K z^{-1}|} = \frac{|H| \cdot |K|}{|z^{-1} H z \cap K|} = [H : (H \cap z K z^{-1})] \cdot |K| = |H| \cdot [K : (z^{-1} H z \cap K)]$$

Das kommt nicht von ungefähr: Ist  $h_1 = 1, h_2, \dots, h_l \in H$  ein Vertretersystem der Linksnebenklassen von  $H \cap z K z^{-1}$  in  $H$ , d.h.  $H = \dot{\bigcup}_{i=1, \dots, l} h_i (H \cap z K z^{-1})$ , so ist  $H z K = \dot{\bigcup}_{j=1, \dots, l} h_j z K$ .

Analog  $K = \dot{\bigcup}_{j=1, \dots, m} (z^{-1} H z \cap K) \cdot k_j, H z K = \dot{\bigcup}_{j=1, \dots, m} H z k_j$

Beweisidee:  $h \in H \cap z K z^{-1} \Leftrightarrow \exists k \in K : h = z k z^{-1} \Leftrightarrow h z K = z k z^{-1} z K = z k K = z K \Rightarrow h_i (z^{-1} H \cap K) z K = h_i z K$ , Details Übung.

*Beweis.* a)  $|H z K| = |H z K z^{-1}| \stackrel{1.3.12}{=} \frac{|H| \cdot |z K z^{-1}|}{|H \cap z K z^{-1}|} = \frac{|H| \cdot |K|}{|H \cap z K z^{-1}|} = \frac{|H| \cdot |K|}{|z^{-1} H z \cap K|}$

b) 2. Beweis:  $G$  operiert auf  $G/K$  wie üblich, also auch  $H$  durch Einschränkung.  $H z K$  ist die Vereinigung der Nebenklassen, die in  ${}^H z K$  liegen. Daher ist  $|H z K| = |K| \cdot$  Bahnlänge  $|{}^H z K|$ . Nun ist  $\text{Stab}_H(zK) = \{h \in H \mid h z K = z K\}$ . Aber  $h z K = z K \Leftrightarrow z^{-1} h z = k \in K \Leftrightarrow h = z k z^{-1}$  ist  $\exists k \in K$ .

Also ist  $\text{Stab}_H(zK) = H \cap z K z^{-1} \stackrel{1.3.7}{\Rightarrow} |H z K| = |K| [H : H \cap z K z^{-1}] = \frac{|H| \cdot |K|}{|H \cap z K z^{-1}|}$

□

$F$  ist ein Körper,  $n \in \mathbb{N}, G = \text{GL}_n(F) \cong \text{Aut}_F(V), v = F$ -Vektorraum mit  $\dim_F(V) = n$   
 $G = \{A \in F^{n \times n} \mid \det A \neq 0\} =$  volle lineare Gruppe.  
 $SL_n(F) = \{A \in F^{n \times n} \mid \det A = 1\} =$  spezielle lineare Gruppe.  
 $Z(G) = \{\alpha \cdot E_{n \times n} \mid 0 \neq \alpha \in F\}$



$$Z(\mathrm{SL}_n(F)) = Z(G) \cap \mathrm{SL}_n(G), \text{ da } G = \mathrm{SL}_n(F) \cdot \left\{ \begin{pmatrix} \alpha & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} \right\}$$

$$Z(\mathrm{SL}_n(F)) = \{\alpha \cdot 1_G \mid 0 \neq \alpha \in F, \alpha^n = 1\}$$

$$\mathrm{PSL}_n(F) = \mathrm{SL}_n(F)/Z(\mathrm{SL}_n(F)) = \text{„projektive spezielle lineare Gruppe“}$$

Ziel:  $\Gamma = \mathrm{PSL}_n(F), \Gamma \neq \mathrm{PSL}_n(\mathrm{GF}(q))$  für  $n = 2, q = 2, 3$  und  $n = 3, q = 2$ , dann ist  $\mathrm{PSL}_n(F)$  einfach.

Notation:  $|F| = \mathrm{GF}(q) = \mathbb{F}_q$  Körper mit  $q$  Elementen,  $q = p^a, p$  Primzahl,  $a \in \mathbb{N}$ .

$$G = \mathrm{GL}_n(q), \mathrm{SL}_n(F) = \mathrm{SL}_n(q), \mathrm{PSL}_n(F) = \mathrm{PSL}_n(q)$$

$$|G| = \prod_{k=1}^n (q^n - q^{k-1}) = (q^n - 1)(q^n - q)(q^n - q^2) \dots = q^{\frac{n(n-1)}{2}} (q^n - 1)(q^{n-1} - 1) \dots (q - 1)$$

$$|\mathrm{SL}_n(q)| = \frac{|\mathrm{GL}_n(q)|}{q-1}, |\mathrm{PSL}_n(q)| = \frac{|\mathrm{SL}_n(q)|}{|\{\alpha \mid \alpha^n = 1 \in F\}|}$$

# IV Basics und Bruhat-Zerlegung

**Satz 1.4.18:**  $|\mathrm{GL}_n(q)| = \text{oben (Algebra)}$

**Definition:**  $T := \{\text{Diagonalmatrizen in } G = \text{diag}(\alpha_1, \dots, \alpha_n) \mid 0 \neq \alpha_i \in \mathbb{F}_q\}$ ,  $|T| = (q-1)^n$ , Standard (Split) „Torus“

$B := \{A = \text{obere Dreiecksmatrizen in } G \mid \det A = \prod \alpha_i \neq 0\}$ , Standard „Boreluntergruppe“ von  $G$

Klar:  $T \leq B \leq G$  „Borus“, „Torel“;  $A \in B \Rightarrow A^{-1} \in B$ ;  $X, Y \in B \Rightarrow XY \in B$ , also  $B \leq G$ .

$U = \{A \in B \mid \text{Diagonaleinträge von } A \text{ sind } 1\} \leq B$

$A \in B, X \in U : AXA^{-1} \in U \Rightarrow U \trianglelefteq B$

Klar:  $U \cap T = (1_G)$ .

Sei  $A \in B \Rightarrow A \cdot \begin{pmatrix} A_{11}^{-1} & & 0 \\ & \ddots & \\ & & A_{nn}^{-1} \end{pmatrix} \in U$

d.h.  $Y \in T, A \cdot Y = X \Rightarrow A = X \cdot Y^{-1}$ . Also ist  $B = U \cdot T$ .

**Definition:** i) Eine Untergruppe von  $G$ , die konjugiert zu  $B$  ist, heißt Boreluntergruppe von  $G$ .

ii) Sei  $\xi = (e_1, \dots, e_n)$  natürliche Basis von  $\mathbb{F}_q^n$ , Für  $\pi \in \sigma_n$  sei  $\xi_\pi = (e_{\pi(1)}, \dots, e_{\pi(n)})$ . Sei  $E_\pi = m_{\text{id}}(\xi, \xi_\pi)$  Basiswechselmatrix von  $\xi$  nach  $\xi_\pi$

Beispiel:  $\pi = (2, 3, 1) : E_\pi = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \text{Permutationsmatrix zu } \pi$ .

Beachte: Matrix-Einheit:  $e_{ij} = (\delta_{rs}) \in M_{n \times n}(\mathbb{F}_q)$

$$E_\pi = \sum_{i=1}^n e_{\pi(i)i}$$

**Definition:** Eine Permutationsmatrix  $A \in M_{n \times n}(F)$  ist eine Matrix, die in jeder Spalte und Zeile genau einen von 0 verschiedenen Eintrag hat, der 1 ist.

Sei  $A$  Permutationsmatrix. Definiere  $\pi : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$  durch  $\pi(i) = j \Leftrightarrow A_{\pi(i)j} = 1$ .

Also ist  $\pi \mapsto E_\pi$  eine Bijektion von  $\sigma_n$  in  $W := \{\text{Permutationsmatrizen}\}$ .

Seien  $\sigma, \pi \in \sigma_n$ . Dann ist  $E_\pi \cdot E_\sigma = (\sum_{i=1}^n e_{\pi(i)i}) (\sum_{j=1}^n e_{\sigma(j)j}) = \sum_{i,j} \sigma_{i,j} e_{\pi(i)i} e_{\sigma(j)j} = \sum_{j=1}^n e_{\pi\sigma(j)j} = E_{\pi\sigma}$ .

Also ist  $\pi \mapsto E_\pi$  ein Isomorphismus von  $\sigma_n$  in  $W$ , insbesondere ist  $W \leq G$ ,  $W$  heißt „Weylgruppe“ von  $G$ .

**Satz 1.4.19:** Die Menge  $W$  der Permutationsmatrizen in  $G = \text{GL}_n(F)$  ist Untergruppe von  $G$  und isomorph zu  $\sigma_n$ .

Beachte: Sei  $\pi \in W \Rightarrow \det \pi = \text{sign } \pi \in \{-1, +1\}$

*Bemerkung.* Ist  $E_\pi$  Permutationsmatrix zu  $\pi \in \sigma_n, M \in F^{n \times n}$ , so entsteht  $\pi \cdot M = E_\pi M$  aus  $M$  durch entsprechende Zeilenpermutationen und  $M\pi$  durch entsprechende Spaltenpermutationen.

$\sigma_n$  operiert auf der natürlichen Basis  $\xi \rightsquigarrow \xi_\pi = (e_{\pi(1)}, \dots, e_{\pi(n)})$ .

**Definition:** Sei  $1 \leq i, j \leq n, i \neq j$ , und sei  $\alpha \in F$ . Dan sei  $x_{ij}(\alpha) \in F^{n \times n}$  die entsprechende

Elementarmatrix  $A = (\alpha_{st})$  mit  $\alpha_{st} = \begin{cases} 1 & \text{für } s = t \\ \alpha & \text{für } s = i, t = j \\ 0 & \text{sonst} \end{cases}$

$$x_{ij}(\alpha) = \begin{pmatrix} 1 & & & \alpha \\ & \ddots & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}, \alpha \text{ an Position } i, j$$

Die Matrizen  $x_{ij}(\alpha)$  und ihre  $G$ -konjugierten heißen Transvektionen.

Beachte:  $x_{ij}(\alpha) \cdot M$  entsteht aus  $M$  durch Addition von Reihe (Spalte)  $j$  mal  $\alpha$  zu Zeile (Spalte)  $i$  ( $M \cdot x_{ij}(\alpha)$ ).

**Lemma 1.4.20:** Seien  $\alpha, \beta \in F, i \neq j, \pi \in W$

- i)  $\det(x_{ij}(\alpha)) = 1$ , also ist  $x_{ij}(\alpha) \in \Omega_n(F) \leq \text{GL}_n(F)$ .
- ii) Ist  $\alpha \neq 0$ , so ist  $x_{ij}(\alpha) \in B \Leftrightarrow i < j$ . ( $U \leq B$ )
- iii)  $x_{ij}(\alpha)x_{ij}(\beta) = x_{ij}(\alpha + \beta), x_{ij}(\alpha)^{-1} = x_{ij}(-\alpha)$ . So ist  $X_{ij} = \{x_{ij}(\alpha) \mid \alpha \in F\} \leq G$  die sogenannte Wurzeluntergruppe zur Wurzel  $(j - i)$ ;  $X_{ij} \cong (F, +)$
- iv) Sind  $i, j, k \in \{1, \dots, n\}$  paarweise verschieden, so ist  $[x_{ij}(\alpha), x_{jk}(\beta)] = x_{ik}(\alpha\beta)$
- v) Ist  $\pi \in \sigma_n$ , so ist  $\pi x_{ij}(\alpha) \pi^{-1} = x_{\pi(i)\pi(j)}(\alpha)$
- vi) Bemerkung von oben.

*Beweis.* i),ii) trivial.

iii) Beachte:  $x_{ij}(\alpha) = E + \alpha e_{ij}$

$$(E + \alpha e_{ij})(E + \beta e_{ij}) = E + (\alpha + \beta)e_{ij} + \alpha\beta e_{ij}e_{ij} = E + (\alpha + \beta)e_{ij} = x_{ij}(\alpha + \beta).$$

$$\Rightarrow x_{ij}(\alpha) \cdot x_{ij}(-\alpha) = x_{ij}(0) = E = 1 \Rightarrow x_{ij}(\alpha)^{-1} = x_{ij}(-\alpha)$$

iv)  $[x_{ij}(\alpha), x_{jk}(\beta)] = (E + \alpha e_{ij})(E + \beta e_{jk})(E - \alpha e_{ij})(E - \beta e_{jk})$

$$= (E + \alpha e_{ij} + \beta e_{jk} + \alpha\beta e_{ik}) \cdot (E - \alpha e_{ij} - \beta e_{jk} + \alpha\beta e_{ik})$$

$$= E - \alpha e_{ij} - \beta e_{jk} + \alpha\beta e_{ik} + \alpha e_{ij} - 0 - \alpha\beta e_{ik} + 0 + \beta e_{jk} - 0 + 0 + \alpha\beta e_{ik} - 0 - 0 + 0$$

$$= E + \alpha\beta e_{ik} = x_{ik}(\alpha \cdot \beta)$$

v) Beachte:  $\pi e_{ij} = e_{\pi(i)j}$  wegen vi).  $e_{ij}\pi^{-1} = e_{i\pi(j)}$ ; denn  $E_\pi = \sum_{s=1}^n e_{\pi(s)s}$   
 $\Rightarrow E_\pi e_{ij} = \sum_{s=1}^n e_{\pi(s)s} e_{ij} = e_{\pi(s)j}, e_{ij} E_{\pi^{-1}} = \sum e_{ij} e_{\pi^{-1}(s)s} = e_{i\pi(j)}$   
 $\Rightarrow \pi x_{ij}(\alpha)\pi^{-1} = \pi(E + \alpha e_{ij})\pi^{-1} = \pi E \pi^{-1} + \alpha \pi e_{ij} \pi^{-1} = E + \alpha e_{\pi(i)\pi(j)} = x_{\pi(i)\pi(j)}(\alpha)$

□

Ziel:  $G = \bigcup_{w \in W} BwB$ , insbesondere: es gibt  $n!$  viele  $B$ - $B$ -Doppelnebenklassen in  $G$  ( $U$ - $B$ -,  $B$ - $U$ -). „Bruhat-Zerlegung“

**Lemma 1.4.21:** Sei  $M \in G$ . Dann gibt es ein  $b \in B(U)$  so, dass gilt:

Für  $1 \leq i \leq n$  gibt es eine eindeutig bestimmte Zeile  $k_i$  in  $b \cdot M$  so, dass der  $i$ -te Eintrag in dieser Zeile der erste von 0 verschiedene Eintrag in ihr ist, und  $\{k_1, \dots, k_n\} = \{1, \dots, n\}$ ;  $i \mapsto k_i \in \sigma_n$ .

*Beweis.* Die 1. Spalte von  $M$  kann nicht die 0-Spalte sein  $\Rightarrow \exists k_1$  so, dass Eintrag  $k_i$  in  $M = (\alpha_{rs})$  ungleich 0 aber  $\alpha_{r1} = 0$  für  $r > k_1$  ist. (Der letzte von 0 verschiedene Eintrag in der Spalte).

Durch elementare Zeilentransformationen  $(x_{1,l}(\frac{-\alpha_{l,1}}{\alpha_{k_1,1}}), l < k_1)$  aus  $U$  kann man  $M'$  erhalten, in der  $k_i$  der einzige von 0 verschiedene Eintrag in der 1. Spalte ist.

Streiche 1. Spalte und  $k_1$ -te Zeile und arbeite induktiv weiter. □

**Satz 1.4.22:**  $G = BWB = \bigcup_{w \in W} BwB$  (bzw.  $UwB$  oder  $BwU$ ).

*Beweis.*  $M \in G, b \in B, k_i$  wie in 2.1.5 gewählt. Die Abbildung  $i \mapsto k_i$  ist Permutation  $\pi = \pi_M \in \sigma_n$ .

Sei  $w = \pi^{-1}$ . Dann ist  $wbM = \tilde{b} \in B \Rightarrow M = b^{-1}\pi\tilde{b} \in B\pi B$ .

Beachte: 2.1.5 konstruiert  $\pi_M$  für  $M$ . □

**Lemma 1.4.23:** Seien  $w_1, w_2 \in W$  und  $b \in B$ , so dass  $w_1bw_2 \in B$  ist, dann ist  $w_1^{-1} = w_2$ .

*Beweis.* Sei  $1 \leq j \leq n$  beliebig und sei  $i = w_1^{-1}(j)$ , also  $w_1(i) = j$ .

Sei wieder  $E = (e_1, \dots, e_n)$  natürliche Basis von  $F^n$ , so ist  $w_1^{-1}(e_j) = e_i$ .

Dann ist Zeile  $j$  von  $w_1b$  gleich Zeile  $i$  von  $b$ .

Sei  $k = w_2^{-1}(i)$ , d.h.  $w_2(k) = i$ , dann ist Spalte  $k$  von  $w_1bw_2$  gleich Spalte  $i$  von  $w_1b$ .

Es sei  $\beta = (b)_{ii} \in F$ .  $\beta \neq 0$  ( $b \in B$ );  $\beta$  ist auch  $(w_1b)_{ji}$  und  $(w_1bw_2)_{jk}$  (und immer noch  $\neq 0$ )  
 $\Rightarrow j \leq k$ , da  $w_1bw_2 \in B$

Wir haben  $w_2^{-1}w_1^{-1}(j) = w_2^{-1}(i) = k \geq j \Rightarrow w_2^{-1}w_1^{-1} = 1 \Rightarrow w_1 = w_2^{-1}$  □

**Korollar 1.4.24:** Seien  $w, w' \in W, w \neq w'$ . Dann ist  $BwB \cup Bw'B = \emptyset$ , und daher  $G =$

$\bigcup_{\pi \in W} B\pi B$ .

*Beweis.* Sei  $BwB \cap Bw'B \neq \emptyset \Rightarrow BwB = Bw'B \Rightarrow \exists b, b' : w' = bwb' \Rightarrow w^{-1}b^{-1}w' = b' \in B \Rightarrow w^{-1} = (w')^{-1} \Rightarrow w = w'$   $\square$

*Bemerkung.* In 2.1.5 wird das eindeutig bestimmte  $w \in W$  für  $M \in G$  konstruiert so, dass  $M \in BwB$  ist.

**Lemma 1.4.25:** Sei  $b \in B$ . Dann gibt es ein Produkt  $t$  von Transvektionen so, dass  $t \cdot b$  Diagonalmatrix ist, die dieselben Diagonaleinträge wie  $b$  hat.

Beweis klar.

**Satz 1.4.26:**  $G$  wird von  $T \leq G$  und der Menge der Transvektionen erzeugt.

*Beweis.* Sei  $H$  die Untergruppe von  $G$ , die von diesen Matrizen erzeugt wird.

Zu zeigen:  $H = G$

Wegen 2.1.10 ist  $B \leq H$ , und daher genügt es wegen der Bruhat-Zerlegung 2.1.8 zu zeigen, dass  $w \in H \forall w \in W$ .

Dafür genügt es zu zeigen:  $\tau_{i,j} \in \sigma_n$  ist in  $H$  enthalten:

$E_{\tau_{i,j}} = \sum_{s \neq i, s \neq j} e_s s + e_i j + e_j i = x_{ji}(1)x_{ij}(-1)x_{ji}(1) \cdot D, D$  Diagonalmatrix.

$$w = x_{ji}(1)x_{ij}(-1)x_{ji}(1), we_k = \begin{cases} e_n & \text{für } k \neq i, k \neq j \\ e_j & \text{für } k = i \\ -e_i & \text{für } k = j \end{cases} \quad \square$$

Missing: 17.11.2009

$$P_f = U_f \rtimes L_f$$

Beispiele:  $V = F^n, \xi = (e_i, \dots, e_n), V_i = \langle e_i, \dots, e_{n_i} \rangle, 0 < n_1 < \dots < n_k = n, f = (V_1, \dots, v_n)$

Beachte:  $V_i = V_{i-1} \oplus y_i, y_i := \langle e_{n_{i-1}+1}, \dots, e_{n_i} \rangle$

$v_i = n_i, v_2 = n_2 - n_1, v_3 = n_3 - n_2, \dots, v_k = n_k - n_{k-1}, v_i = \dim_F(y_i)$

$L_f = \{\text{Matrix mit von } 0 \text{ verschiedenen Blöcken der Größen } v_i \times v_i \text{ auf der Diagonale aus } G\}$

...

$v = (v_1, \dots, v_k) \models n$  Wir schreiben  $P_v = U_v \rtimes L_v$  anstatt  $P_f, L_f, U_f$ . ( $\nu = (n) \Rightarrow P_{(n)} = G = L_{(n)}, U_{(n)} = (1)$ )

Sonderfall:  $v = (1^n) = (1, \dots, 1) \models n, P_v = B = u \cdot T$ , Borus.

**Definition:** Eine  $n \times m$ -Matrix  $A$  heißt (untere) unitriangulär, falls folgendes gilt:  $A_{ii} = 1, A_{ij} = 0 \forall i < j$  (allgemeine untere Dreiecksmatrix mit 1 auf der Diagonale), analog obere.

**Lemma 1.4.27:** Sei  $V = F^n, f = (W_1, \dots, W_n)$  mit  $W_i = \langle e_1, \dots, e_i \rangle, \xi = (e_1, \dots, e_n)$  natürliche Basis von  $V$ .

Sei  $X$  ein  $B$ -invarianter Unterraum von  $V$ , d.h.  $bx \in X \forall b \in B, x \in X (\Rightarrow bX = X)$ .

Dann ist  $W = W_i$  für ein  $1 \leq i \leq n$ .

*Beweis.* Sei  $1 \leq k \leq n$  minimal mit  $X \subseteq W_k$ . Wir zeigen:  $X = W_k$ .

Dann existiert ein  $x = \sum_{i=1}^k \alpha_i e_i$  mit  $\alpha_k \neq 0$  (da  $k$  minimal).

...  $\exists b \in B : b \cdot x = e_k \Rightarrow e_k \in X$

Nun ist  $(E + e_{k-1,k})e_k = e_k + e_{k-1} \in X \Rightarrow e_{k-1} \in X$ , analog  $\forall i \leq k : e_i \in X \Rightarrow W_k \subseteq X \Rightarrow W_k = X$ .  $\square$

**Satz 1.4.28:** Sei  $B \leq H \leq G$ . Dann ist  $H$  eine Standardparabolische Untergruppe, d.h.  $\exists \nu \models n, H = P_\nu$

*Beweis.* Sei  $X$  ein  $H$ -invarianter Unterraum von  $V$ . Dann ist  $X$  auch  $B$ -invariant, weil  $B \subseteq H$ . Also gibt es ein  $1 \leq i \leq n : X = W_i = \langle e_1, \dots, e_i \rangle, \xi = (e_1, \dots, e_n)$  natürliche Basis wegen 2.2.5.

Seien  $W_{\alpha_1}, \dots, W_{\alpha_r}$  mit  $1 \leq \alpha_1 < \alpha_2 < \dots < \alpha_r = n$  genau die  $H$ -invarianten Unterräume von  $V$ .  $\underline{\alpha} = (\alpha_1, \dots, \alpha_r), W_{\alpha_i} = \langle e_1, \dots, e_{\alpha_i} \rangle, F_{\underline{\alpha}} = (W_{\alpha_1}, \dots, W_{\alpha_r})$  ist  $H$ -invariante Fahne von Dimensionstyp  $\underline{\alpha}$ .

Sei  $\mu_1 = \alpha_1, \mu_2 = \alpha_2 - \alpha_1, \dots, \mu_r = \alpha_r - \alpha_{r-1} \Rightarrow \mu = (\mu_1, \dots, \mu_r) \models n$ .

$\text{Stab}_G(F_{\underline{\alpha}}) = P_\mu, H \leq P_\mu$

Zu zeigen:  $H = P_\mu$ .

Spezialfälle

1.)  $r = 1, \mu = (n), P_\mu = G$

Zu zeigen:  $H = G$

$\langle He_1 \rangle = H$ -invarianter Unterraum  $\Rightarrow V = \langle He_1 \rangle \Rightarrow \exists h \in H : he_1 = \alpha_1 e_1 + \dots + \alpha_n e_n$  mit  $\alpha_n \neq 0$

Bruhat-Zerlegung:  $h \in BwB, \exists w \in W$

2.1.9 und 2.1.5  $\Rightarrow$  Für  $g \in BwB$  hat  $g$  als Matrix die Form ...

d.h. hier für  $h \in BwB : w(1) = n$

Beachte: Wegen  $B \subseteq H$  ist  $h = b_1 w b_2 \Rightarrow w = b_1^{-1} h b_2^{-1} \in H$

Sei  $1 < j \leq n$  mit  $w(j) = 1$  (Ohne Einschränkung  $n \geq 2$ )

Dann ist  $X_{1j} = \{x_{1j}(\alpha) | \alpha \in F\} \subseteq B \subseteq H$

$X_{n1} = X_{w(1)w(j)} = w X_{1j} w^{-1} \in H$  (mit 2.1.4)

Sei  $1 \leq i < m < n \Rightarrow X_{im} \subseteq B \subseteq H$

Dann ist  $X_{nm}(\alpha) = [x_{n1}(\alpha), x_{1m}(1)] \in H \forall \alpha \in F$  (mit 2.1.4)

$\Rightarrow X_{nm} \subseteq H$

$\forall 1 \leq i < n : x_{i1}(\alpha) = [x_{in}(\alpha), x_{n1}(1)] \in H \Rightarrow X_{i1} \subseteq H$

$\forall 1 < i, m \leq n, i \neq m : x_{im}(\alpha) = [x_{i1}(\alpha), x_{1m}(1)] \in H \Rightarrow X_{im} \subseteq H$

Wir haben gezeigt  $X_{ij} \subseteq H \forall 1 \leq i, j \leq n, i \neq j$

Da  $T \subseteq B \subseteq H \Rightarrow H = G$ .

2.)  $r = 2, I_{\underline{\alpha}} = W_m \leq V = W_n$

Wir wissen schon:  $H \leq P_\mu, \mu = (m, n - m) \models n$

Klar:  $U_\mu \subseteq B \subseteq H, P_\mu = U_\mu \rtimes L_\mu$ , es genügt also zu zeigen:  $L_\mu \subseteq H$ .

$L \cong \text{GL}_m(F) \times \text{GL}_{n-m}(F)$

$GL_m(F) = \langle \text{Diagonalmatrizen in } GL_m(F) \text{ und } x_{ij}(\alpha) \rangle$ , analog  $GL_{n-m}$

Es genügt also zu zeigen:  $X_{ij} \in H \forall 1 \leq i, j \leq m, i$  und  $m+1 \leq i, j \leq n$

Sei  $X_1 = \langle He_1 \rangle = H$ -invarianter Unterraum von  $W_m \Rightarrow X_1 = W_m$

D.h.  $\exists h \in H, he_1 = \alpha e_1 + \dots + \alpha_m e_m$  mit  $\alpha_m \neq 0$ .

Sei  $w \in W$  mit  $h \in BWB$ . Wie oben folgt aus 2.1.9 und 2.1.5  $w(1) = m$  und daher  $X_{m1} \subseteq H$ .

Beachte:  $w \in H \Rightarrow w^{-1}(1) = j \leq m$

$X_{m1} = X_{w(1)w(j)} = wX_{1j}w^{-1} \in H$ .

Kommutatoren wie im ersten Spezialfall  $\Rightarrow X_{ij} \subseteq H \forall 1 \leq i, j \leq m \Rightarrow GL_m(F) \subseteq H$ .

$\langle Hem+1 \rangle$  ebenfalls  $H$ -invariant  $\Rightarrow \exists h \in H : he_{m+1} = \alpha_{m+1}e_{m+1} + \dots + \alpha_n e_n$  mit  $\alpha_n \neq 0$ .

Es folgt analog wie eben  $X_{ij} \subseteq H \forall m+1 \leq i, j \leq n \Rightarrow GL_{n-m}(F) \subseteq H$ .

$\Rightarrow P_\mu \subseteq H \Rightarrow H = P_\mu$

Übung: Allgemeiner Fall.

□

# V Die spezielle und projektive lineare Gruppen

Ziel:  $\text{PSL}_n(F)$  ist einfach, falls  $n > 2$  oder  $n = 2$  und  $F \neq \text{GF}(2)$  oder  $\text{GF}(3)$  ist.

2.3.1 Erinnerung:  $\det : \text{GL}_n(F) \rightarrow F^* : g \mapsto \det g$  ist Gruppenhomomorphismus mit Kern  $\text{SL}_n(F) \trianglelefteq G, \text{SL}_n(F) = \{g \in \text{GL}_n(F) \mid \det g = 1\}$ .

Klar:  $\det$  ist surjektiv

Isosätze:  $q - 1 = \frac{|\text{GL}_n(q)|}{|\text{SL}_n(q)|} \Rightarrow |\text{SL}_n(q)| = \prod_{k=1}^n \frac{q^k - q^{k-1}}{q-1} = \prod_{k=1}^{n-1} \frac{q^{k+1} - q^k = q^{\frac{n(n+1)}{2}} (q^n - 1)(q^{n-1} - 1) \dots (q^2 - 1)}{q-1}$

2.3.2 Satz:  $\text{SL}_n(F)$  wird von den Wurzeluntergruppen (d.h. von den Transvektionen) in  $G$  erzeugt.

Beweis: Für  $1 \leq i, j \leq n, i \neq j$ , und für  $\alpha \in F$  ist  $x_{ij}(\alpha) \in \text{SL}_n(F)$  nach 2.1.4.

In 2.1.5 haben wir gezeigt: Ist  $g = (\alpha_{ij}) \in \text{SL}_n(F) \subseteq G$ , so gibt es ein  $u \in U$  (Produkt von Transvektionen) so, dass gilt: Für  $1 \leq i \leq n$  gibt es eine eindeutig bestimmte Zeile  $k_i$  in  $ug$  so, dass der  $i$ -te Eintrag in dieser Zeile der erste von 0 verschiedene ist. Die Abbildung  $\pi : i \mapsto k_i$  ist Element von  $\sigma_n = W$ .

Wir können diese Zeilen nach 2.1.11 durch ein Produkt  $\tilde{\pi}$  von Transvektionen  $(i, \tilde{j}) = x_{ij}(1)x_{ji}(-1)x_{ij}(1)$  ( $(i, j) \in \sigma_n$  Transposition) bis aufs Vorzeichen ordnen. ( $(i, \tilde{j}) = \text{diag}(1, \dots, 1, -1, 1, \dots, (i, j))$ ). Daraus folgt: durch ein Produkt  $b \in \text{SL}_n(F)$  von Transvektionen wird  $b \cdot g$  eine obere Dreiecksmatrix  $\tilde{g}$ .

Also  $bg = \tilde{g} = \begin{pmatrix} \lambda_1 & & & A \\ & \ddots & & \\ 0 & & & \lambda_n \end{pmatrix}$ . Beachte:  $\det \tilde{g} = \det b \cdot \det g = 1$ , d.h.  $\tilde{g} \in \text{SL}_n(F)$ .  
 $\Rightarrow \det \tilde{g} = \lambda_1 \cdot \dots \cdot \lambda_n = 1$ .

Beachte: Seien  $\alpha, \beta, \gamma \in F$  mit  $\alpha\gamma \neq 0$ .

$$\begin{aligned} x_{21}(-1)x_{12}(1-\gamma^{-1})x_{21}(\gamma) \cdot \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1-\gamma^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1-\gamma^{-1} \\ -1 & \gamma^{-1} \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \alpha\gamma & \gamma\beta + \gamma \end{pmatrix} = \begin{pmatrix} \alpha + \alpha\gamma - \alpha & \beta + \gamma\beta + \gamma - \beta - 1 \\ -\alpha + \alpha & -\beta + \beta + 1 \end{pmatrix} = \begin{pmatrix} \alpha\gamma & \gamma\beta - \beta - 1 \\ 0 & 1 \end{pmatrix} \end{aligned}$$



Auf alle Zeilen von  $\tilde{g}$  anwenden.

$\Rightarrow$  Man kann  $\tilde{g}$  durch Premultiplikation mit einem Produkt von Transvektionen auf die

$$\text{Gestalt } \tilde{g}' = \begin{pmatrix} \lambda_1 \cdots \lambda_n & & & * \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} = \begin{pmatrix} 1 & & & * \\ & \ddots & & \\ 0 & & & 1 \end{pmatrix} \in U \text{ bringen. Jedes Element von } U$$

ist aber Produkt von Transvektionen (elementare Zeilenoperationen:  $\tilde{g}' \rightsquigarrow 1$ ). Also ist  $\tilde{g}'$  Produkt von Transvektionen. Also ist  $g$  Produkt von Transvektionen.

2.3.3 Satz: Die Wurzeluntergruppen  $X_{ij}, 1 \leq i, j \leq n, i \neq j$ , sind in  $\text{SL}_n(F)$  konjugiert.

Beweis: Seien  $1 \leq i, j \leq n, 1 \leq k, l \leq n, i \neq j, k \neq l$ .

$\sigma_n$  ist  $n$ -fach transitiv auf  $\{1, \dots, n\}$ , also zweifach transitiv  $\Rightarrow \exists w \in W = \sigma_n : w(i) = k, w(j) = l$ .

Haben gesehen:  $wX_{ij}w^{-1} = X_{w(i),w(j)} = X_{kl}$ . Ist  $w$  gerade Permutation, d.h.  $\text{sign } w = \det w = 1 \Rightarrow w \in \text{SL}_n(F)$  und wir sind fertig.

Sei also  $\text{sign } w = \det w = -1$  und  $\alpha \in F$ . Sei  $d = d^{-1} = \begin{pmatrix} -1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} \in \text{GL}_n(F)$ . Dann

ist  $\det(dw) = \det d \cdot \det w = -\det w = 1$ , d.h.  $dw \in \text{SL}_n(F)$ .

$$dwX_{ij}(dw)^{-1} = d(wX_{ij}w^{-1})d = dX_{kl}d = d(E + \alpha e_{kl})d = dEd + \alpha de_{kl}d = \begin{cases} X_{kl}(\alpha) & \text{für } k, l \neq 1 \\ X_{kl}(-\alpha) & \text{sonst, } (k \neq l) \end{cases}$$

In jedem Fall ist  $(dw)X_{ij}(dw)^{-1} = X_{kl}$ .

Definition: Sei  $Z = \{\alpha E \mid \alpha \in F^*\}, E = 1$ . Dann ist  $Z \leq G, G \subseteq Z(G) = \text{Zentrum von } G$ .

2.3.4 Satz:  $Z = Z(G)$  und  $Z \cap \text{SL}_n(F) = Z(\text{SL}_n(F))$ .

Es genügt zu zeigen: Jedes Element von  $\text{GL}_n(F)$  (bew.  $\text{SL}_n(F)$ ), das mit allen Transvektionen  $x_{ij}(1)$  ( $1 \leq i, j \leq n, i \neq j$ ) vertauscht, liegt schon in  $Z$ .

$$\text{Sei } g = (\alpha_{ij}) = \sum_{i,j} \alpha_{ij} e_{ij} \in Z(G) \Rightarrow g \cdot x_{rs}(1) = x_{rs}(1) \cdot g \forall 1 \leq r, s \leq n, r \neq s \Leftrightarrow g(E + e_{rs}) = (E + e_{rs})g \Leftrightarrow \sum_{i,j} \alpha_{ij} e_{ij} e_{rs} = \sum_{kl} \alpha_{kl} e_{rs} e_{kl} \Leftrightarrow \sigma_i \alpha_{ir} e_{is} = \sum_l \alpha_{sl} e_{rl}$$

d.h.  $e_{is} = e_{rl} \Leftrightarrow i = r, l = s, \alpha_{rr} = \alpha_{ss}, r \neq s, \alpha_{ij} = 0$  sonst.

$\Rightarrow g = \alpha \cdot E \in Z$ . (Für  $\text{SL}_n(F) : \alpha^n = \det \alpha E = 1$ )

Definition:  $\text{GL}_n(F)/Z = \text{PGL}_n(F) = \text{„projektive allgemeine lineare Gruppe“}$

$\text{SL}_n(F)/Z(\text{SL}_n(F)) = \text{PSL}_n(F) = \text{„projektive spezielle lineare Gruppe“}$

2. Isosatz:  $\text{PSL}_n(F) \cong \text{SL}_n(F)/(Z \cap \text{SL}_n(F)) = Z \cdot \text{SL}_n(F)/Z \leq \text{GL}_n(F)/Z = \text{PGL}_n(F)$

$$\text{Für } F = \text{GF}(q) = (F)_q : |\text{PGL}_n(q)| = \frac{|\text{GL}_n(q)|}{Z} = \frac{|\text{GL}_n(q)|}{q-1} = |\text{SL}_n(q)|$$

Bemerkung:

$$1) \text{ GL}_n(F) = \text{SL}_n(F) \rtimes \left\{ \begin{pmatrix} \alpha & & 0 \\ & 1 & \\ & & \ddots \\ 0 & & & 1 \end{pmatrix} \mid \alpha \in F^* \right\}$$

2)  $F$  algebraisch abgeschlossen  $\Rightarrow z := (\sqrt[n]{\det g}^{-1} E) \in Z, g \cdot z \in \text{SL}_n(F)$ , es folgt:  $\text{PSL}_n(F) \cong \text{PGL}_n(F)$ .

3)  $\text{PSL}_2(2) \cong \sigma_3 \supseteq A_3$ , da  $\text{PSL}_2(2) \cong \text{GL}_2(2)$   
 $\text{PSL}_2(3) \cong A_4 \supseteq V_4 \cong G_2 \times G_2$

2.3.6 Lemma: Sei  $n \geq 2$ ; und  $|F| \neq 2, 3$  für  $n = 2$ . Dann ist jede Tranvektion  $x_{ij}(\alpha)$  ( $1 \leq i, j \leq n, i \neq j, \alpha \in F$ ) ein Kommutator von Elementen in  $\text{SL}_n(F)$ .

Beweis: Ist  $n > 2$ , dann ist  $x_{ij}(\alpha) = [x_{ij}(\alpha), x_{kj}(\alpha)]$  mit  $1 \leq k \leq n, k \neq i, k \neq j$ .

Sei  $n = 2, \beta, \gamma \in F$  mit  $\beta \neq 0$ .

$$\left[ \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}, \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & (\beta^2 - 1)\gamma \\ 0 & 1 \end{pmatrix}$$

$\Rightarrow x_{12}(\alpha)$  ist Kommutator dieser Elemente aus  $\text{SL}_2(F)$ , falls es  $\beta, \gamma \in F$  mit  $\beta \neq 0$  gibt, so dass  $\alpha = (\beta^2 - 1)\gamma$  ist.

Sei  $|F| > 3$ , dann gibt es immer ein  $\beta \in F^*$  mit  $\beta^2 \neq 1$  und  $\gamma = \alpha(\beta^2 - 1)^{-1}$ .

$x_{21}(\alpha)$  ähnlich bzw. ist konjugiert in  $\text{SL}_2(F)$  zu einem Element aus  $X_{12}$ .

2.3.7 Korollar: Sei  $n > 2$  oder  $|F| > 3$  für  $n = 2$ . Dann ist  $\text{SL}_n(F) = [\text{SL}_n(F), \text{SL}_n(F)]$ .

2.3.8 Lemma: Sei  $n \leq 2$   $\text{SL}_n(F)$  operiert auf der  $\{Fv \mid 0 \neq v \in F^n\}$  durch  $g(Fv) := F(gv)$  (Kern ist das Zentrum).

Diese Operation ist 2-fach transitiv.

Beweis: Seien  $c_1, c_2, d_1, d_2 \in F^n \setminus \{0\}$  und  $c_1, c_2$  bzw.  $d_1, d_2$  linear unabhängig, d.h.  $Fc_1 \neq Fc_2, Fd_1 \neq Fd_2$ .

Ergänze  $c_1, c_2$  bzw.  $d_1, d_2$  zu Basen  $\tilde{C} = (c_1, c_2, \dots, c_n)$  und  $\tilde{D} = (d_1, d_2, \dots, d_n)$  von  $F^n$ . Sei  $C = m_{\text{id}}(\xi, \tilde{C}) = m_f(\xi, \xi)$  mit  $f(e_i) = c_i$ .

$D = m_{\text{id}}(\xi, \tilde{D}) = m_g(\xi, \xi)$  mit  $g(e_i) = d_i$

Dann sind  $C, D \in \text{GL}_n(F)$ . Sei  $\epsilon = \det D / \det C = \det(DC^{-1}), A = \begin{pmatrix} \epsilon & 0 \\ 0 & 1_{n-1} \end{pmatrix}, \det A =$

$\epsilon, B = DA^{-1}C^{-1}$ , so ist  $Bc_1 = \epsilon^{-1}d_1, Bc_i = d_i$  für  $i > 2$

$BFc_i = FBc_i = Fd_i$  für alle  $i$ . Klar:  $\det B = 1$ , d.h.  $B \in \text{SL}_n(F)$  □

Missing: 27.11.2009

$$|G| = p^a m, p \nmid m, |G|_p = p^a, |G|_{p'} = m$$

$\text{Syl}_p(G) \equiv 1 \pmod{p}$  Beweis:  $X = \{A \subseteq G \mid |A| = |G|_p = p^a\}$   $G$ -Menge

Bemerkung:  $P \in \text{Syl}_p(G) \Rightarrow P \in X$

$A \in X$  so gibt es ein  $g \in G : g \cdot A \ni 1$

$$|X| = \binom{p^a \cdot m}{p^a} = \sum_{O \in G\text{-Bahnen von } X} |O|$$

Sei  $A \in X, A \in O = \text{Orbit von } X$  so, dass  $1 \in A$ . Sei  $P = \text{Stab}_G(A) \leq G$ . Dann ist  $P \subseteq P \cdot A = A \Rightarrow |P| \leq |A| = p^a$

1.3.7  $\Rightarrow |O| = |G : P|$ .

Angenommen  $p$  teilt nicht  $|G : P|$ , so ist  $|G|_p$  Teiler von  $|P|$ . Also ist  $|G|_p = |P| = p^a$  und  $P \in \text{Syl}_p(G)$  und  $|O| = m$ .

Sei umgekehrt  $P \in \text{Syl}_p(G)$ . Dann ist die  $G$ -Menge  $G/P = \cup g_i P$  mit  $|g_i P| = |P| = p^a$ , d.h.  $G/P$  ist ein Orbit  $O$  in  $X$ :  $|O| = |G : P| = m$

Klar:  $\text{Stab}_G(1 \cdot P) = P$

Auf diese Weise erhalten wir eine Bijektion zwischen der Menge der  $G$ -Bahnen in  $X' := \{A \in X \mid p \nmid |G \cdot A|\}$

Also ist  $X' = \text{Vereinigung aller Bahnen } O \text{ von } X \text{ mit } p \nmid |O|$

$X \setminus X' = \text{Vereinigung aller Bahnen } O \text{ von } X \text{ mit } p \mid |O|$  und daher  $p \mid |X \setminus X'| = |X| - |X'|$

Also  $|X| \equiv |X'| \pmod{p}$

Sei  $r = |\text{Syl}_p(G)| = \text{Anzahl der } p\text{-Sylow Untergruppen von } G = |\{\text{Bahnen } O \text{ von } X \text{ mit } O \subseteq X'\}|$ .

Es gilt dann:  $r \cdot m = |X'| \equiv_p |X| \equiv_p \binom{p^a m}{p^a}$

$p \nmid m \Rightarrow r \pmod{p}$  ist nur von  $|G|$  und nicht von  $G$  selbst abhängig. Das heißt je zwei Gruppen  $G$  und  $H$  mit  $|G| = |H|$  haben  $\pmod{p}$  dieselbe Anzahl von  $p$ -Sylowgruppen.

Sei  $G = C_{p^a m}$ , dann ist  $r \equiv 1 \pmod{p}$ , also ist  $|\text{Syl}_p(G)| \equiv 1 \pmod{p}$  für alle  $G$  mit  $G = p^a m$ . Insbesondere ist  $r \neq 0$ , d.h.  $G$  besitzt mindestens eine  $p$ -Sylow Untergruppe.

Dies zeigt 1) und 4).

Sei nun  $P \in \text{Syl}_p(G), G$  Gruppe der Ordnung  $p^a m, p^a = |G|_p, Q \leq G$   $p$ -Gruppe.

$Y = \{gPg^{-1} \mid g \in G\}$ .  $Q$  operiert auf  $Y$  durch Konjugation:

${}^x(yPy^{-1}) = xyP(xy)^{-1} \in Y$  für  $x \in X$ .

Sei  $O$  ein  $Q$ -Orbit von  $Y, P_1 \in O$ . Dann ist  $|O| = |Q : \text{Stab}_Q(P_1)| = \text{Potenz von } p \text{ (möglicherweise } p^0)$ .

Aber  $|Y| = |G : N_G(P)|$  Teiler von  $m$  (1.3.15)  $\Rightarrow p \nmid |Y|$ . Also muss es eine  $Q$ -Bahn  $O$  in  $Y$  geben mit  $p \nmid |O| \Rightarrow \exists Q$ -Bahn  $O$  in  $Y$  mit  $|O| = p^0 = 1 \Rightarrow O = \{P_1\}$ . Dann ist also  $xP_1x^{-1} = P_1 \forall x \in Q$ . Daher ist  $QP_1 = P_1Q$  und mit (1.1.4) ist  $QP_1 \leq G$

Klar ist:  $|P_1| \leq |QP_1|$ . Nach 1.3.12 ist  $|QP_1| = \frac{|Q||P_1|}{|Q \cap P_1|} = |P_1||Q : Q \cap P_1|$ . Also ist  $QP_1$  eine  $p$ -Untergruppe von  $G$ .

Also ist wegen  $|P_1| \leq |QP_1|$  die Ordnung  $|Q \cdot P_1|$  von  $QP_1$  gleich  $|P_1| = p^a$  und daher  $|Q \cap P_1| = |Q| \Rightarrow Q \subseteq P_1 \in \text{Syl}_p(G)$ . Dies zeigt 3).

Seien  $Q, P \in \text{Syl}_p(G) \Rightarrow$  (nach vorigem Schritt)  $\exists g \in G : Q \leq gPg^{-1}$ . Wegen  $|Q| = |P| = p^a$  ist  $Q = gPg^{-1}$ .  $\square$

2. Beweis für Existenz von  $p$ -Sylowuntergruppen:

Induktion über  $|G|$

$|G| = 1$  trivial

$p \nmid |G|$  trivial

$|G| = p^a m$  mit  $p \nmid m > 1$ , und sei die Behauptung beweisen für alle Gruppen  $|H|$  mit  $|H| < |G|$ .

Besitzt  $G$  eine echte Untergruppe  $H$  mit  $p \nmid [G : H]$ , so ist jede  $p$ -Sylowgruppe von  $H$  eine  $p$ -Sylowgruppe von  $G$  und wir sind fertig.

Ohne Einschränkung gelte  $H \leq G \Rightarrow p \mid [G : H]$

Klassengleichung 1.3.13:

$|G| = |Z(G)| + \sum_{i=1}^l [G : C_G(g_i)]$  mit  $\{g_1, \dots, g_l\}$  Repräsentanten von Konjugationsklassen von  $G$  der Größe  $> 1$ .

Für  $1 \leq i \leq l$  ist  $C_G(g_i) \leq G$  und daher  $p \mid [G : C_G(g_i)]$

Also teilt  $p \mid |Z(G)|$  = abelsche Gruppe. Also ist  $|Z(G)| > 1$ .

$\Rightarrow G$  besitzt eine normale Untergruppe  $N (\leq Z(G))$  der Ordnung  $p$ .  $|G/N| = p^{a-1}m < p^a m \Rightarrow \exists \bar{P} \in \text{Syl}_p(G/N)$

Sei  $P =$  volles Urbild von  $\bar{P}$  in  $G \Rightarrow N \trianglelefteq P, P/N = \bar{P} \Rightarrow |P| = p^a \Rightarrow P \in \text{Syl}_p(G)$ .

Korollar: Sei  $|G| = p^a m, p^a = |G|_p$ . Dann gibt es für  $1 \leq b \leq a$  eine Untergruppe  $H$  von  $G$  mit  $|H| = p^b$  (Weil  $P \in \text{Syl}_p(G)$  eine  $p$ -Gruppe, daher nilpotent und damit auflösbar ist. Wir können  $H \leq P$  wählen!).

3.1.3 Korollar:  $|\text{Syl}_p(G)|$  ist Teiler von  $|G|_{p'} = \frac{|G|}{|G|_p}$  ( $|G| = p^a m, p \nmid m$ )

Beweis:  $G$  operiert auf  $\text{Syl}_p(G)$  per Konjugation transitiv. Also ist  $P \in \text{Syl}_p(G)$ , so ist  $|\text{Syl}_p(G)| = [G : \text{Stab}_G(P)]$ . Wegen  $P \trianglelefteq N_G(P) \leq G$  ist daher  $|\text{Syl}_p(G)|$  Teiler von  $m$ .

3.1.4 Korollar: (Cauchy's Theorem)  $G$  hat ein Element der Ordnung  $p$  ( $p \mid |G|$ )

3.1.5 Satz: Sei  $N \trianglelefteq G (N \neq G)$ , und sei  $P \in \text{Syl}_p(G)$ . Dann ist  $PN/N \in \text{Syl}_p(G/N)$  und  $P \cap N \in \text{Syl}_p(N)$ .

Beweis:  $[G/N : PN/N] = [G : PN]$  wegen 3. Isosatz.  $PN/N \cong P/(P \cap N) \Rightarrow PN/N$  ist Gruppe.

$p \nmid [G : P] = |G|_{p'} \Rightarrow [G : PN]$  ist Teiler von  $m$ , wird nicht von  $p$  geteilt.

$\Rightarrow PN/N \in \text{Syl}_p(G/N)$ .

Nach 1.3.12 ist  $[PN : P] = \frac{|P| \cdot |N|}{|P \cap N| \cdot |P|} = \frac{|N|}{|P \cap N|} \Rightarrow$  (nach oben)  $P \cap N$  ist  $p$ -Untergruppe von  $N$  mit  $[N : P \cap N]$  wird nicht von  $p$  geteilt. Also ist  $P \cap N \in \text{Syl}_p(N)$ .  $\square$

Vorsicht:  $H \leq G \not\Rightarrow H \cap P \in \text{Syl}_p(H)$  für  $P \in \text{Syl}_p(G)$

3.1.6 Satz: Sei  $H \leq G, P \in \text{Syl}_p(G)$ . Dann gibt es  $g \in G$  so, dass  $gPg^{-1} \cap H \in \text{Syl}_p(H)$  ist.

Beweis: Sei  $Q \in \text{Syl}_p(H) \Rightarrow \exists P' \in \text{Syl}_p(G)$  mit  $Q \subseteq P' \Rightarrow \exists g \in G$  mit  $P' = gPg^{-1} \cap H \supseteq Q$

Klar:  $Q = P' \cap H$  (warum?)

Anwendungen:

3.1.7 Satz („ $pq$ -Theorem“): Seien  $p, q$  Primzahlen mit  $p > q$ . Sei  $G$  Gruppe mit  $|G| = p \cdot q$ . Dann ist  $G$  abelsch (und daher  $\cong C_{q \cdot p} \cong C_q \times C_p$ ) oder  $p \equiv 1 \pmod q$ . Ist dies so, dann gibt es bis auf Isomorphie genau eine nicht abelsche Gruppe der Ordnung  $p \cdot q$ .

Beweis: Sei  $P \in \text{Syl}_p(G), Q \in \text{Syl}_q(G) \Rightarrow |P| = p, |Q| = q \Rightarrow P \cong C_p \wedge Q \cong C_q$ . Wir haben  $P \cap Q = (1)$ , und daher ist  $G = P \cdot Q$  (1.3.12). Mit 3.1.3 folgt  $|\text{Syl}_p(G)| \mid [G : P]$  und mit 3.1.4  $|\text{Syl}_p(G)| \cong 1 \pmod p$   
 $\Rightarrow |\text{Syl}_p(G)| = 1 = [G : N_G(P)] \Rightarrow N_G(P) = G \Rightarrow P \trianglelefteq G$  ( $p > q \Rightarrow q \not\equiv 1 \pmod p$ ).

Ist  $p \not\equiv 1 \pmod q \Rightarrow$  (analog)  $Q \trianglelefteq G \Rightarrow G = P \times Q$

Sei also  $p \equiv 1 \pmod q$ . Sei  $G$  nicht abelsch,  $\varphi : Q \rightarrow \text{Aut}(P) : x \mapsto c_x, c_x : P \rightarrow P : y \mapsto xyx^{-1}$ .

$\ker \varphi \neq (1) \Rightarrow \ker \varphi = Q \Rightarrow \varphi Q \Rightarrow (1) \leq P$  und  $c_x = \text{id}_P \Rightarrow G = P \times Q$ ,  $G$  abelsch. Widerspruch!

Also ist  $\ker \varphi = (1)$ , d.h.  $\varphi$  ist injektiv. Sei  $P = \langle g \rangle$ . Leicht: Sei  $1 \leq i \leq p-1$ , so induziert  $g \mapsto g^i$  einen Automorphismus  $\sigma_i$  von  $P = C_p = \langle g \rangle$ , und  $\text{Aut}(P) = \{\sigma_i \mid 1 \leq i \leq p-1\}$  ist zyklisch der Ordnung  $p-1$ .

Nun ist  $q \mid p-1$ , also hat  $C_{p-1} \cong \text{Aut}(C_p)$  eine eindeutige Untergruppe der Ordnung  $q$ , und diese ist isomorph zu  $C_q \cong Q$ .

Also: Unter  $\varphi$  wird  $Q$  auf die eindeutig bestimmte Untergruppe der Ordnung  $q$  von  $\text{Aut}(P)$  abgebildet.

Beachte: Ist  $\psi : Q \rightarrow \text{Aut}(P)$  ein Monomorphismus, so ist  $\text{im } \varphi = \text{im } \psi$ , es gibt aber viele Monomorphismen von  $Q \rightarrow \text{Aut}(P)$ .

Für jeden solchen Monomorphismus  $\psi$  haben wir eine Gruppe  $P \rtimes_{\psi} Q$ .

Der nächste Satz zeigt: Alle diesen semidirekten Produkte sind isomorph. Also gibt es in diesem Fall ( $p \equiv 1 \pmod q$ ) genau eine nichtabelsche Gruppe der Ordnung  $p \cdot q$ .  $\square$

3.1.8 Satz: Sei  $H$  zyklische Gruppe,  $N$  Gruppe. Seien  $\varphi, \psi$  Monomorphismen von  $H \rightarrow \text{Aut}(N)$  mit  $\text{im } \varphi = \text{im } \psi$ . Dann ist  $N \rtimes_{\varphi} H \cong N \rtimes_{\psi} H$ .

Beweis: Sei  $H = \langle x \rangle$ . Wegen  $\varphi(H) = \psi(H)$  ist  $\langle \varphi(x) \rangle = \langle \psi(x) \rangle \leq \text{Aut}(N)$ . Es gibt also  $a, b \in \mathbb{Z}$  mit  $\varphi(x)^a = \psi(x)$  und  $\psi(x)^b = \varphi(x)$ . Für  $s \in \mathbb{Z}$  ist dann  $\varphi((x^s)^a) = \varphi(x)^{as} = \psi(x)^s = \psi(x^s)$ , d.h.  $\varphi(h^a) = \psi(h) \forall h \in H$ , analog  $\psi(h^b) = \varphi(h) \forall h \in H$ .

Definiere  $\tau : N \rtimes_{\psi} H \rightarrow N \rtimes_{\varphi} H$  durch  $\tau(n \cdot h) = n \cdot h^a$  und  $\lambda : N \rtimes_{\varphi} H \rightarrow N \rtimes_{\psi} H$  durch  $\lambda(n \cdot h) = n \cdot h^b$

$$\tau(n_1 h_1 n_2 h_2) = \tau(n_1 \psi(h_1)(n_2) h_1 h_2) = n_1 \psi(h_1)(n_2)(h_1 h_2)^a = n_1 \varphi(h_1^a)(n_2) h_1^a h_2^a = n_1 h_1^a n_2 h_2^a = \tau(n_1 h_1) \tau(n_2 h_2)$$

$\Rightarrow \tau$  (und analog  $\lambda$ ) ist Gruppenhomomorphismus.

Nun ist  $\tau \lambda : nh \mapsto \tau(n \cdot h^b) = n \cdot h^{ba}$ , aber  $\varphi(x) = \psi(x)^b = (\varphi(x^a))^b = \varphi(x^{ab})$  und  $\varphi$  ist injektiv. Also ist  $x = x^{ab}$  und daher  $h = h^{ab} \forall h \in H$ , also ist  $\tau \lambda = \text{id}_{N \rtimes_{\varphi} H}$ ,  $\lambda \tau = \text{id}_{N \rtimes_{\psi} H}$

Also sind  $\tau, \lambda$  Isomorphismen und  $N \rtimes_{\varphi} H \cong N \rtimes_{\psi} H$ ,  $\square$ .

Erinnerung:  $A_5$  ist einfach  $A_5 \leq \sigma_5$ ,  $|\sigma_5| = 5! = 120 \Rightarrow A_5 = 60 = 3 \cdot 5 \cdot 2^2$ .

3.1.9 Satz: Sei  $G$  einfach,  $|G| = 60$ . Dann ist  $G \cong A_5$ .

Beweis: Sei  $n \in \mathbb{N}$  und  $H \leq G$  mit  $[G : H] = n$ . Sei  $\rho : G \rightarrow \sigma_n$  die Darstellung, die zu der  $G$ -Menge  $G/H$  gehört.  $\Rightarrow \rho$  ist injektiv. Insbesondere ist  $|G| = 60 \leq n! \Rightarrow n \geq 5$ .

Beh:  $G$  besitzt eine Untergruppe von  $H$  mit  $[G : H] = 5$ .

Angenommen,  $G$  besitzt keine solche Untergruppe:  $|\text{Syl}_2(G)| \neq 1$  teilt  $3 \cdot 5 = 15$ , sonst wäre  $G$  nicht einfach. Sei  $P \in \text{Syl}_2(G)$ . Betrachte Möglichkeiten für  $|\text{Syl}_2(G)|$ :

3:  $[G : N_G(P)] = 3 < 5$  Widerspruch!

5:  $[G : N_G(P)] = 5$  Widerspruch zur Annahme

Also ist  $[G : N_G(P)] = 15$  Seien  $S_1, S_2 \in \text{Syl}_2(G)$ ,  $S_1 \neq S_2$ . Sei  $1 \neq t \in S_1 \cap S_2$ .  $V_4 = C_2 \times C_2, C_4$  sind die einzigen Gruppen der Ordnung 4.  $\Rightarrow S_1$  und  $S_2$  sind abelsch  $\Rightarrow |C_G(t)| > 4$  und  $4 \mid |C_G(t)|$ , da  $S_1 \leq C_G(t)$ .  $\Rightarrow [G : C_G(t)] \in \{1, 3, 5\} \Rightarrow [C : C_G(t)] = 1 \Rightarrow t \in Z(G) \trianglelefteq G$  Widerspruch zur Einfachheit von  $G$ .

Also hat  $G : 15(4 - 1) = 45$  der Ordnung 2 oder 4. Da  $G$  einfach ist, gilt für  $P \in \text{Syl}_5(G) : 1 \neq [G : N_G(P)] \mid 4 \cdot 3$  und  $[G : N_G(P)] \equiv 1 \pmod{5}$ , also nicht  $\{1, 2, 3, 4, 12\}$  - also hat  $G$  genau 6 5-Sylowgruppen, und daher  $6(5 - 1) = 24$  Elemente der Ordnung 5. Also ist  $|G| \leq 45 + 24 > 60$  Widerspruch. Also hat  $G$  eine Untergruppe  $H$  mit  $[G : H] = 5$ .

Sei wieder  $\varphi : G \rightarrow \sigma_5$  die Darstellung auf  $G/H$ . Diese ist injektiv, so ist  $G$  ohne Einschränkung Untergruppe von  $\sigma_5$  vom Index 2, da die  $|G| = 60 = \frac{120}{2} = \frac{|\sigma_5|}{2}$ . Also ist  $G \trianglelefteq \sigma_5$ . Angenommen  $G \neq A_5 \Rightarrow |G \cdot A_5| > 60 \Rightarrow G \cdot A_5 = \sigma_5$ .

Nach 1.3.12:  $|G \cap A_5| = \frac{|G||A_5|}{|G \cdot A_5|} = 30$ . Also ist  $G \cap A_5$  Untergruppe von  $G$  vom Index 2 - Widerspruch. Also  $G = A_5$ .

3.1.10 Korollar:  $\text{PSL}_2(4) \cong \text{PSL}_2(5) \cong A_5$ , da  $\text{PSL}_2(4)$  und  $\text{PSL}_2(5)$  einfach mit Ordnung 60.

Bemerkung: Man kann zeigen: Alle anderen Gruppen  $\text{PSL}_n(q)$  sind paarweise verschieden (?).

Relativ leichte Übung: Ist  $G$  einfach und  $|G| < 60$  so folgt  $G \cong C_{|G|}$

3.1.11 Satz „Frattini Argument“: Sei  $G$  endliche Gruppe,  $N \trianglelefteq G$  und  $P \in \text{Syl}_p(N)$ ,  $p$  Primzahl. Dann ist  $G = N_G(P) \cdot N$ .

Beweis: Sei  $g \in G$ . Wegen  $gNg^{-1} = N \trianglelefteq G$  ist  $gPg^{-1} \subseteq N \Rightarrow gPg^{-1} \in \text{Syl}_p(N)$ . Also gibt es  $n \in N : n(gPg^{-1})n^{-1} = P = ngP(ng)^{-1} \Rightarrow ng \in N_G(P) \Rightarrow g \in n^{-1}N_G(P) \subseteq NN_G(P) = N_G(P)N$ .  $\square$

# VI Normalteilerstruktur

## Aufgabe 1 Satz von Jordan-Hölder

Sei im folgenden  $G$  eine beliebige Gruppe.

4.1.1 Definition: Sei  $\Omega$  eine Menge, dann heißt  $G$  Gruppe mit Operatorenbereich  $\Omega$  (kurz  $\Omega$ -Gruppe), falls es eine externe binäre Verknüpfung  $\Omega \times G \rightarrow G : (\alpha, g) \mapsto \alpha g \in G$  gibt mit  $\alpha(g_1 g_2) = (\alpha g_1)(\alpha g_2) \forall g_1, g_2 \in G, \alpha \in \Omega$ .

Äquivalente Formulierung: Es gibt eine Abbildung von  $\Omega \rightarrow \{\sigma : G \rightarrow G \mid \sigma \text{ ist Gruppenhom.}\}$ .

Eine Untergruppe  $H$  der  $\Omega$ -Gruppe  $G$  heißt zulässig ( $\Omega$ -Untergruppe,  $H \leq_{\Omega} G$ ), falls  $\alpha h \in H \forall h \in H, \alpha \in \Omega$ , und sie heißt zulässiger Normalteiler ( $\Omega$ -Normalteiler,  $H \trianglelefteq_{\Omega} G$ ), wenn  $H$  zusätzlich Normalteiler von  $G$  ist.

Klar: Homomorphismen von  $\Omega$ -Gruppen:  $F : G \rightarrow X$  Gruppenhomomorphismus mit  $f(\alpha g) = \alpha f(g)$ ,  $G, X$   $\Omega$ -Gruppen,  $g \in G, \alpha \in \Omega$

Es gelten Isosätze, Kerne von  $\Omega$ -Homomorphismen sind  $\Omega$ -Normalteiler, Bilder sind  $\Omega$ -Untergruppen.

Eine  $\Omega$ -Gruppe heißt einfach, falls sie keine nichttrivialen  $\Omega$ -Normalteiler hat.

4.1.2 Beispiele:  $G : \Omega$ -Gruppe

- i)  $\Omega = \emptyset$ : zulässigen Untergruppen = Untergruppe von  $G$ , zulässigen Normalteiler = Normalteiler von  $G$ .
- ii)  $\Omega = \text{Inn}(G)$  ( $\Omega = G$  operiert durch Konjugation auf  $G$ ): zulässigen Untergruppen = zulässigen Normalteiler = Normalteiler von  $G$ .
- iii)  $\Omega = \text{Aut}(G)$ : zulässigen Untergruppen = char. Untergruppen von  $G$ .
- iv)  $G = (R, +)$  = add. Gruppe eines Rings  $R$  mit 1 (alle Untergruppen sind Normalteiler)  
 $\Omega = R$  operiert auf  $G$  per Multiplikation von links (rechts). Die  $\Omega$ -Untergruppen von  $(R, +)$  sind genau die Linksideale (Rechtsideale) von  $R$ . Links-Rechts-Operation:  $\Omega \times G \times \Omega \rightarrow G : (\alpha, g, \beta) \mapsto \alpha g \beta$  mit  $(\alpha g) \beta = \alpha (g \beta)$ .  
Für  $(R, +)$  mit  $\Omega = R$  sind dann die zulässigen Untergruppen die Ideale von  $R$ .

v)  $M = G =$  additive abelsche Gruppe mit  $R$ -Modul,  $R = \text{Ring} \ni 1$ ,  $M$  ist eine  $R$ -Gruppe unter Linksmultiplikation mit Elementen von  $R$ .

Die zulässigen  $R$ -Untergruppen = zulässige  $R$ -Normalteiler = Untermoduln (analog für Rechtsmoduln).

Jetzt sei  $\Omega$  eine Menge und  $G$  eine  $\Omega$ -Gruppe.

Definition: Eine endliche Folge  $G = G_0 >_{\Omega} G_1 >_{\Omega} G_2 >_{\Omega} \dots >_{\Omega} G_r = (1)$  von  $\Omega$ -Untergruppen heißt Kompositionsreihe von  $G$ , falls  $G_{i+1} \trianglelefteq_{\Omega} G_i$  und  $G_i/G_{i+1}$  ist einfache  $\Omega$ -Gruppe.

Beispiel:  $\sigma_5 \supseteq A_5 \supseteq (1)$  ist eine Kompositionsreihe mit „Kompositionsfaktoren“  $\sigma_5/A_5 \cong C_2, A_5 = A_5/(1)$ .

Definition:  $N$  ist maximale normale  $\Omega$ -Untergruppe von  $G$ , falls  $G \neq N \trianglelefteq_{\Omega} G$  und kein  $\Omega$ -Normalteiler von  $G$  echt zwischen  $N$  und  $G$  existiert  $\Rightarrow G/N$  einfache  $\Omega$ -Gruppe.

Beachte: Für  $\Omega$ -Gruppen gelten die 3 Isomorphiesätze, und daher der Korrespondenzsatz 1.1.11.

4.1.3 Satz: Endliche Gruppen ( $\Omega = \emptyset$ ) besitzen Kompositionsreihen. Beweis klar.

4.1.4 Korollar: Sei  $G$  endliche Gruppe ( $\Omega = \emptyset$ ), und sei  $N \trianglelefteq G$ . Dann besitzt  $G$  eine Kompositionsreihe „durch“  $N$ , d.h.  $N$  kommt als eine der Untergruppen  $G_i$  vor.

Beweis: Sei  $N = N_0 > N_1 > N_2 > \dots > N_k = (1)$  Kompositionsreihe von  $N$  und  $G/N = H_0 > H_1 > \dots > H_r = (1)$  Kompositionsreihe von  $G/N$ ,  $G_i =$  volles Urbild von  $H_i$  in  $G/N$ , also  $G_i = \{g \in G \mid gN \in H_i\}$ .

1.1.11  $\Rightarrow G = G_0 > G_1 > \dots > G_{r-1} > N = N_0 > \dots > N_k = (1)$  Kompositionsreihe von  $G$  durch  $N$ .

4.1.5 Lemma: Sei  $G$  beliebige  $\Omega$ -Gruppe mit einer Kompositionsreihe. Sei  $N \trianglelefteq_{\Omega} G$ , dann besitzt  $N$  ebenfalls eine Kompositionsreihe.

Beweis: Sei  $G = G_0 > G_1 > \dots > G_r = (1)$  Kompositionsreihe von  $G$ . Sei  $N_i = N \cap G_i$ . Dann ist  $N = N_0 \geq N_1 \geq \dots \geq N_r = (1)$

Dann ist  $N_{i+1} = G_{i+1} \cap N \trianglelefteq N_i = G_i \cap N$  und  $N_i/N_{i+1} = (N \cap G_i)/(N \cap G_{i+1}) = (N \cap G_i)/((N \cap G_i) \cap (G_{i+1})) \cong (2. \text{ Isosatz}) ((N \cap G_i)G_{i+1})/G_{i+1} \trianglelefteq G_i/G_{i+1}$  (Korrespondenzsatz) Also ist, da  $G_i/G_{i+1}$  einfach ist, entweder  $N_i/N_{i+1} = (1)$  (d.h.  $N_i = N_{i+1}$ ), oder  $N_i/N_{i+1} \cong G_i/G_{i+1}$  einfach.

So erhalten wir eine Kompositionsreihe von  $N$  durch Streichung der Wiederholungen in  $N = N_0 \geq N_1 \geq \dots \geq N_r = (1)$ . □

Definition: Eine Kette  $G = G_0 > G_1 > \dots > G_r = (1)$  heißt  $\Omega$ -Subnormalkette, falls  $G_{i+1} \trianglelefteq_{\Omega} G$  ist, und  $\Omega$ -Normalkette, falls  $G_i \trianglelefteq_{\Omega} G$  ist.



Seien  $G = G_0 > G_1 > \dots > G_r = (1)$  und  $G = H_0 > H_1 > \dots > H_r = (1)$  zwei Subnormalketten derselben Länge  $r$ . Dann heißen diese äquivalent, falls es ein  $\rho \in \sigma_r$  gibt mit  $G_{i-1}/G_i \cong H_{\rho(i)-1}/H_{\rho(i)}$  für  $1 \leq i \leq r$ .

Klar: Dies ist eine Äquivalenzrelation auf der Menge der Subnormalketten der Länge  $r$  von  $G$ .

4.1.6 Satz (Jordan-Hölder): Sei  $G$  eine  $\Omega$ -Gruppe und besitze  $G$  eine Kompositionsreihe. Dann haben je zwei Kompositionsreihen von  $G$  dieselbe Länge und sind äquivalent.

Konsequenz: In einer Kompositionsreihe einer  $\Omega$ -Gruppe (= einfache  $\Omega$ -Gruppen), sind die vorkommenden einfachen Kompositionsfaktoren mit ihren Multiplizitäten eindeutig bestimmt (aber nicht die Reihenfolge).

Beweis: Seien  $G = G_0 > G_1 > \dots > G_r = (1)$  und  $G = H_0 > H_1 > \dots > H_s = (1)$  zwei Kompositionsreihen von  $G$ .

Induktion über  $r$ :

$r = 0$ :  $G = (1)$  trivial.

$r = 1$ :  $G \triangleright (1)$  ist Kompositionsreihe  $\Rightarrow G$  ist einfach  $\Rightarrow s = s, H_1 = (1)$ .

Sei  $r > 1$  und die Behauptung bewiesen für alle  $\Omega$ -Gruppen mit einer Kompositionsreihe der Länge  $< r$ .

Ist  $G_1 = H_1$ , so hat  $G_1 = H_1$  die Kompositionsreihe  $G_1 > G_2 > \dots > G_r = (1)$  der Länge  $r - 1$  und  $H_1 > H_2 > \dots > H_s = (1)$ , die nach Induktionsvoraussetzung äquivalent sind und  $r - 1 = s - 1$ , also  $r = s$  und mit  $G/G_1 = H/H_1$  fertig.

Sei also  $G_1 \neq H_1$ . Wegen  $G_1 \trianglelefteq G_0 = G, H_1 \trianglelefteq H_0 = G$  ist  $G_1 \not\leq G_1 H_1 \trianglelefteq G$ . Da  $G/G_1$  einfach ist, ist also  $G_1 H_1 = G$ .

Sei  $K = G_1 \cap H_1$ , dann ist  $G/G_1 \cong H_1/K$  und  $G/H_1 \cong G_1/K$ .

Also sind  $G_1/K$  und  $H_1/K$  einfache  $\Omega$ -Gruppen.

Beachte  $K \trianglelefteq G$ , also besitzt  $K$  eine Kompositionsreihe  $K = K_0 > K_1 > \dots > K_t = (1)$ .

$G_1 > K_0 > K_1 > \dots > K_t = (1)$  ist Kompositionsreihe von  $G$  der Länge  $t + 1$ , die nach Induktionsvoraussetzung äquivalent zu  $G_1 > G_2 > \dots > G_r$  ist, und  $t + 1 = r - 1$ , analog  $t + 1 = s - 1$ , also  $r = s$ .

Wegen  $G/G_1 \cong H_1/K$  und  $G/H_1 \cong G_1/K$  sind die ursprünglichen Kompositionsreihen äquivalent.

Beispiele:

- i)  $\Omega = \emptyset$ , Kompositionsreihen sind Subnormalketten  $G = G_0 > G_1 > \dots > G_r = (1)$  mit  $G_{i+1} \trianglelefteq G_i$  und  $G_i/G_{i+1}$  einfache Gruppe.
- ii)  $M$  ist  $R$ -Module,  $R = K$ -Algebra,  $\dim_K(M) < \infty \Rightarrow M$  hat Kompositionsreihe.
- iii)  $G$  ist  $\Omega$ -Gruppe mit  $\Omega = \text{Inn}(G)$  ( $\text{Aut}(G)$ ?)