Satz: Für jede Ugr. H einer Gr. G sind äquiv.: (1) $G' \subseteq H$;
(2) $H \trianglelefteq G$ & G/H ab.

Bew: (1) $\Rightarrow$ (2): Sei $G' \subseteq H$. Dann: $ghg^{-1} = \underbrace{[g,h]}_{\in G' \subseteq H} h^{-1} \in H$ $(g \in G,\ h \in H)$.
Folglich: $H \trianglelefteq G$. Für $x, y \in G$ ist ferner $[xH, yH] = [x,y]H = 1$,
d.h. $(xH)(yH) = (yH)(xH)$.

(2) $\Rightarrow$ (1): Sei (2) erfüllt. Für $x, y \in G$ ist dann $[x,y]H = [xH, yH] = 1$,
d.h. $[x,y] \in H$. Folglich: $G' \subseteq H$.

Bsp: Wir werden später zeigen, dass "meist" $GL(n,K)' = SL(n,K)$ gilt.

8.6 Def: Die höheren Kommutatorgruppen einer Gr. G def. man induktiv:
$G^{(0)} := G$, $G^{(1)} := G'$, $G^{(2)} := G'' := (G')' = [G', G']$,
$G^{(i+1)} := (G^{(i)})'$ $(i \in \mathbb{N})$.

Bem: (i) Für jeden Gr.-Hom. $f: G \longrightarrow H$ & $i \in \mathbb{N}$ ist $f(G^{(i)}) = f(G)^{(i)} \leq H^{(i)}$; insbes. ist $G^{(i)} \leq G$ vollinv.

(ii) $U \leq G \wedge i \in \mathbb{N}_0 \Rightarrow U^{(i)} \leq G^{(i)}$.

(iii) Offenbar ist $G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \ldots$; setze $G^{(\infty)} := \bigcap_{i \in \mathbb{N}} G^{(i)}$.

8.7 Def: Eine Gr. G mit $G^{(n)} = 1$ für ein $n \in \mathbb{N}_0$ heißt auflösbar. Ggf. heißt das kleinste $s \in \mathbb{N}_0$ mit $G^{(s)} = 1$ (Auflösbarkeits-) Stufe von G.

Bem: (i) $s = 0 \iff G = 1$
$s \leq 1 \iff G' = 1 \iff G$ ab.
$s \leq 2 \iff G'' = 1 \iff G$ metabelsch.

(ii) Ugrn. & Faktorgrn. von auflösb. Grn. sind auflösb.

(iii) Für auflösb. Grn. G, H ist auch $G \times H$ auflösb.; denn $(G \times H)^{(i)} = G^{(i)} \times H^{(i)}$ für $i \in \mathbb{N}_0$.

(iv) Sind $M, N \trianglelefteq G$ & sind $G/M, G/N$ auflösb., so ist auch $G/M \cap N$ auflösb.; denn nach Bem. 4.6 ist $G/M \cap N$ zu einer Ugr. von $G/M \times G/N$ isom.

(v) Ist G auflösb. der Stufe s, so ist $G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq \ldots \trianglerighteq G^{(s)} = 1$ eine Normalreihe mit ab. Faktoren.

Satz: Für jede Gr. G sind äquiv.: (1) G auflösb.
(2) G hat eine Normalreihe mit ab. Faktoren.
(3) G hat eine Subnormalreihe $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_t = 1$ mit ab. Faktoren.

Bew: (1) $\Rightarrow$ (2): obige Bem.

(2) $\Rightarrow$ (3): trivial

(3) $\Rightarrow$ (1): Sei (3) erfüllt. Wir zeigen induktiv: $G^{(i)} \subseteq G_i$ für $i \in \mathbb{N}_0$. Für $i=0$ ist das klar. Sei also $i>0$ & $G^{(i-1)} \subseteq G_{i-1}$. Da $G_i \trianglelefteq G_{i-1}$ & G_{i-1}/G_i ab. ist, folgt aus Satz 8.5: $G^{(i)} = (G^{(i-1)})' \subseteq G_{i-1}' \subseteq G_i$. Am Schluss ist also $G^{(t)} \subseteq G_t = 1$.

Bsp: Für $n \in \mathbb{N}$ & jeden Körper K ist die Gr. $B(n,K)$ aller oberen Dreiecksmatrizen

$$\begin{pmatrix} * & \cdots & * \\ & \ddots & \vdots \\ 0 & & * \end{pmatrix}$$

in $GL(n,K)$ auflösb., vgl. Übungen.

8.8 Satz: Für jede Gr. G & $N \trianglelefteq G$ gilt: G auflösb. $\Leftrightarrow$ $N, G/N$ auflösb.

Bew: „$\Rightarrow$": Bem. 8.7 (ii).

„$\Leftarrow$": Seien $N, G/N$ auflösb. Dann ex. $s, t \in \mathbb{N}_0$ mit $N^{(s)} = 1$ & $1 = (G/N)^{(t)} = G^{(t)}N/N$. Folglich: $G^{(t)} \subseteq N$ & $G^{(t+s)} \subseteq N^{(s)} = 1$.

Bem: Für auflösb. Normalt. M, N einer Gr. G ist auch MN ein auflösb. Normalt. von G; dies folgt aus dem Satz wg. $MN/N \cong M/M \cap N$. Ist G endl., so ist also das Produkt aller auflösb. Normalt. ein auflösb. Normalt. von G; dieser heißt auflösbares Radikal von G.

8.9 Satz: Für jede endl. Gr. G sind äquiv.:

(1) G auflösb.

(2) Jeder Komp.-Faktor von G ist zu $\mathbb{Z}/p\mathbb{Z}$ für ein $p \in \mathbb{P}$ isom.

(3) Jeder Hauptfaktor von G ist zu $(\mathbb{Z}/p\mathbb{Z})^n$ für geeignete $p \in \mathbb{P}, n \in \mathbb{N}$ isom.

Bew: (2) $\Rightarrow$ (1), (3) $\Rightarrow$ (1): Satz 8.7.

(1) $\Rightarrow$ (2): Sei G auflösb. mit Komp.-Reihe $G = G_0 \trianglerighteq G_1 \trianglerighteq \dots \trianglerighteq G_l = 1$. Für $i = 1, \dots, l$ ist dann $S_i := G_{i-1}/G_i$ auflösb. & einf. Daher: $S_i' \triangleleft S_i$ (denn sonst wäre $S_i'' = S_i' = S_i$ usw.), also $S_i' = 1$, d.h. S_i ab. Sei $1 \neq x \in S_i$. Dann: $1 \neq \langle x \rangle \trianglelefteq S_i$, also $S_i = \langle x \rangle$ zykl. Da S_i einf. ist, folgt $p_i := |S_i| \in \mathbb{P}$. Folglich: $S_i \cong \mathbb{Z}/p_i\mathbb{Z}$.

(1) $\Rightarrow$ (3): Sei G auflösb. mit Hauptreihe $G = G_0 \trianglerighteq G_1 \trianglerighteq \dots \trianglerighteq G_l = 1$. Für $i = 1, \dots, l$ ist dann $T_i := G_{i-1}/G_i$ auflösb. & char. einf. Nach Satz 6.3 ist $T_i \cong S_i^{n_i}$ für eine auflösb. einf. Gr. S_i & ein $n_i \in \mathbb{N}$. Wie oben ist $S_i \cong \mathbb{Z}/p_i\mathbb{Z}$ für ein $p_i \in \mathbb{P}$.

Bem: Man hat die folgenden Auflösbarkeitskriterien:

(i) (Burnsides $p^a q^b$-Satz, 1904)

Für $p, q \in \mathbb{P}$, $a, b \in \mathbb{N}_0$ ist jede Gr. der Ordnung $p^a q^b$ auflösb.

(ii) (Feit-Thompson 1963, Odd-Order-Theorem)

Gruppen ungerader Ordnung sind stets auflösb. (Bew. ca. 250 Seiten)

9. Nilpotente Gruppen

9.1 Def: Für $n \in \mathbb{N}$ & jede Gr. G def. man induktiv:

$$G^1 := G, \quad G^2 := [G,G], \quad G^{n+1} := [G, G^n].$$

Bem: (i) $n \in \mathbb{N} \Rightarrow G^n = [\underbrace{G, \dots, G}_{n}]$.

(ii) $n \in \mathbb{N} \wedge U \le G \Rightarrow U^n \le G^n$.

(iii) $n \in \mathbb{N} \wedge f: G \longrightarrow H$ Gr.-Hom. $\Rightarrow f(G^n) = f(G)^n \le H^n$; insbes. ist G^n vollinv. in G.

(iv) Nach (iii) ist jeweils $G^n \trianglelefteq G$, also $G^{n+1} \le G^n$ nach Satz 8.3. Wir erhalten so eine Folge vollinv. Ugr. $G = G^1 \ge G^2 \ge G^3 \ge \dots$, die absteigende Zentralfolge von G. Setze $G^\omega := \bigcap_{i \in \mathbb{N}} G^i$.

(v) $n \in \mathbb{N} \Rightarrow [G/G^{n+1}, G^n/G^{n+1}] = [G, G^n]G^{n+1}/G^{n+1} = G^{n+1}/G^{n+1} = 1$
$\Rightarrow G^n/G^{n+1} \subseteq Z(G/G^{n+1})$. Das erklärt den Begriff "Zentralfolge".

Satz: Für $1 \ne n \in \mathbb{N}$ & jede Gr. G gilt: $G^n = \langle [g_1, \dots, g_n] : g_1, \dots, g_n \in G \rangle$.

Bew: (Induktion nach n)

OE $n \ge 3$. Offenbar $N := \langle [g_1, \dots, g_n] : g_1, \dots, g_n \in G \rangle \trianglelefteq G$ & $N \subseteq G^n$. Nach Induktion dürfen wir $G^{n-1} = \langle [g_2, \dots, g_n] : g_2, \dots, g_n \in G \rangle$ voraussetzen. Dann: $G^{n-1}/N = \langle [g_2, \dots, g_n]N : g_2, \dots, g_n \in G \rangle$, & für $g_1, \dots, g_n \in G$ gilt: $[g_1 N, [g_2, \dots, g_n]N] = [g_1, [g_2, \dots, g_n]]N = 1$. Folglich: $G^{n-1}/N \subseteq Z(G/N)$ & $G^n/N = [G, G^{n-1}]/N = [G/N, G^{n-1}/N] = 1$, d.h. $G^n \subseteq N$.

9.2 Satz: Für $m, n \in \mathbb{N}$ & jede Gr. G gilt:

(i) $[G^m, G^n] \subseteq G^{m+n}$ (ii) $G^{(n)} \subseteq G^{2^n}$.

Bew: (i) (Induktion nach n)

Für $n = 1$ ist $[G^m, G] = [G, G^m] = G^{m+1}$. Sei also $n \ge 2$ & die Aussage für $n-1$ schon bewiesen. Mit $H := G/G^{m+n}$ gilt dann:

$$[G^m, G^n]G^{m+n}/G^{m+n} = [G^m/G^{m+n}, G^n/G^{m+n}] = [H^m, H^n]$$
$$= [H^m, [H, H^{n-1}]] = 1$$

wg.

$$[H, [H^{n-1}, H^m]] = [H, [H^m, H^{n-1}]] \overset{\text{Ind.}}{\subseteq} [H, H^{m+n-1}]$$
$$= H^{m+n} = G^{m+n}/G^{m+n} = 1$$

$$[H^{n-1},[H^m,H]] = [[H^m,H],H^{n-1}] = [[H,H^m],H^{n-1}] = [H^{m+1},H^{n-1}]$$
$$\overset{\text{Ind.}}{\subseteq} H^{m+n} = 1$$

(3-Ugm.-Lemma). Also: $[G^m,G^n] \subseteq G^{m+n}$.

(ii) (Induktion nach n)

Offenbar: $G^{(0)} = G = G^1 = G^{2^0}$. Sei also $n\in\mathbb{N}$ & bereits gezeigt: $G^{(n-1)} \subseteq G^{2^{n-1}}$.

Dann folgt aus (i): $G^{(n)} = [G^{(n-1)},G^{(n-1)}] \subseteq [G^{2^{n-1}},G^{2^{n-1}}] \subseteq G^{2^n}$.

9.3 Def: Für jede Gr. G def. man die *aufsteigende Zentralfolge* induktiv durch

$Z_0(G) := 1$, $Z_1(G) := Z(G)$, $Z_i(G)/Z_{i-1}(G) := Z(G/Z_{i-1}(G))$ $\quad (i\in\mathbb{N})$.

Bem: (i) Für $i\in\mathbb{N}_0$ ist $Z_i(G) \subseteq G$ char.; dies ist klar für $i=0,1$. Ist $Z_{i-1}(G) \subseteq G$ char. für ein $i\in\mathbb{N}_0$, so induziert jedes $\alpha\in\mathrm{Aut}\,G$ ein $\bar\alpha \in \mathrm{Aut}(G/Z_{i-1}(G))$ mit $\bar\alpha(g Z_{i-1}(G)) := \alpha(g) Z_{i-1}(G)$ für $g\in G$. Da $Z(G/Z_{i-1}(G)) \subseteq G/Z_{i-1}(G)$ char. ist, folgt: $\bar\alpha(Z_i(G)/Z_{i-1}(G)) = Z_i(G)/Z_{i-1}(G)$. Folglich: $\alpha(g)\in Z_i(G)$ für $g\in Z_i(G)$.

(ii) $1 = Z_0(G) \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \dots$; $Z_\infty(G) := \bigcup_{i\in\mathbb{N}} Z_i(G)$ heißt *Hyperzentrum* von G. Dann: $Z_\infty(G) \subseteq G$ char. Ugr.

9.4 Def: Eine Gr. G mit $Z_c(G) = G$ für ein $c\in\mathbb{N}_0$ heißt *nilpotent*; ggf. heißt das kleinste $c\in\mathbb{N}_0$ mit $Z_c(G) = G$ *(Nilpotenz-) Klasse* von G.

Bem: $c = 0 \iff G = 1$; $c \le 1 \iff G$ ab.

9.5 Def: Eine Normalreihe $G = G_0 \trianglerighteq G_1 \trianglerighteq \dots \trianglerighteq G_r = 1$ einer Gr. G mit $G_{i-1}/G_i \subseteq Z(G/G_i)$ für alle i heißt *Zentralreihe*.

Bsp: Ist G nilp. der Kl. c, so ist $G = Z_c(G) \trianglerighteq Z_{c-1}(G) \trianglerighteq \dots \trianglerighteq Z_1(G) \trianglerighteq Z_0(G) = 1$ eine Zentralreihe, die *aufsteigende* (*obere*) *Zentralreihe* von G.

Satz: Für Ugrn. $G_0,\dots,G_r$ einer Gr. G mit $G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_r = 1$ sind äquiv.:

(1) $G = G_0 \trianglerighteq G_1 \trianglerighteq \dots \trianglerighteq G_r = 1$ ist eine Zentralreihe.

(2) $[G, G_{i-1}] \subseteq G_i$ für $i = 1,\dots,r$.

Bew: (1) $\Rightarrow$ (2): Ist (1) erfüllt, so gilt für alle i: $[G,G_{i-1}]G_i/G_i = [G/G_i, G_{i-1}/G_i] = 1$, d.h. $[G,G_{i-1}] \subseteq G_i$.

(2) ⇒ (1): Für $i = 1, \dots, r$ sei $[G, G_{i-1}] \le G_i \le G_{i-1}$. Nach Satz 8.3 (ii) ist dann $G_{i-1} \trianglelefteq G$, d.h. wir haben eine Normalreihe. Ferner ist $[G/G_i, G_{i-1}/G_i] = [G, G_{i-1}]G_i/G_i = 1$, d.h. $G_{i-1}/G_i \le Z(G/G_i)$.

Bem: Wg. (2) ist jede Verfeinerung einer Zentralreihe wieder eine.

9.6 Satz: Sei $G = G_0 \trianglerighteq G_1 \trianglerighteq \dots \trianglerighteq G_r = 1$ eine Zentralreihe einer Gr. G. Für $i = 0, \dots, r$ ist dann $G_{r-i} \le Z_i(G)$ & $G^{i+1} \le G_i$, insbes. ist $Z_r(G) = G$ & $G^{r+1} = 1$, d.h. G ist nilp., und die Kl. von G ist höchstens r.

Bew: (Induktion nach i)
Offenbar ist $G_r = 1 = Z_0(G)$ & $G^1 = G = G_0$. Sei also $i > 0$ & bereits $G_{r-i+1} \le Z_{i-1}(G)$ & $G^i \le G_{i-1}$ bewiesen. Dann ist:

$$[G/Z_{i-1}(G), G_{r-i}Z_{i-1}(G)/Z_{i-1}(G)] = [G, G_{r-i}]Z_{i-1}(G)/Z_{i-1}(G) \le G_{r-i+1}Z_{i-1}(G)/Z_{i-1}(G) = 1,$$

also $G_{r-i}Z_{i-1}(G)/Z_{i-1}(G) \le Z(G/Z_{i-1}(G)) = Z_i(G)/Z_i(G)$. Folglich: $G_{r-i} \le Z_i(G)$ & $G^{i+1} = [G, G^i] \le [G, G_{i-1}] \le G_i$.

Bem: (i) Nach 9.5, 9.6 ist eine Gr. G genau dann nilp., wenn sie eine Zentralreihe hat. Ggf. ist die Kl. von G durch die Länge einer Zentralreihe beschränkt.

(ii) Für jede nilp. Gr. G der Kl. c ist $G^{c+1} = 1$. Daher ist $G = G^1 \trianglerighteq G^2 \trianglerighteq \dots \trianglerighteq G^{c+1} = 1$ eine Zentralreihe, die <u>absteigende</u> (<u>untere</u>) <u>Zentralreihe</u> von G. Nach (i) ist ferner $G^c \ne 1$.

(iii) Eine Gr. G ist also genau dann nilp., wenn $G^s = 1$ für ein $s \in \mathbb{N}$ ist.

(iv) Ugrn. & Faktorgrn. einer nilp. Gr. G sind nilp.; ihre Kl. ist jeweils durch die Kl. von G beschränkt.

(v) Jede nilp. Gr. ist auflösb.

(vi) Die Hauptfaktoren einer endl. nilp. Gr. G haben Primzahlordnung; durch Verfeinerung der oberen Zentralreihe erhält man nämlich eine Komp.-Reihe, die gleichzeitig Zentralreihe ist. Diese ist also insbes. eine Normalreihe & damit eine Hauptreihe von G. Da G auflösb. ist, haben ihre Faktoren Primzahlordnung.

Bsp: (i) $\mathrm{Sym}(3)$ ist auflösb., aber wg. $Z(\mathrm{Sym}(3)) = 1$ nicht nilp.

(ii) Eine typische nilp. Gr. ist die Ugr. von $GL(n, K)$, ($n \in \mathbb{N}$, K Körper), die aus allen Matrizen der folgenden Form besteht:

$$\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}.$$ (siehe Übungen!)

9.7 Bem: Für jede Teilmenge X einer Gr. G ist der Normalisator

$$N_G(X) := \{g \in G : gXg^{-1} = X\}$$

eine Ugr. von G; dies rechnet man leicht nach. Ist $X \leq G$, so ist $X \trianglelefteq N_G(X)$.

Satz: Für jede echte Ugr. U einer nilp. Gr. G ist $U < N_G(U)$.

Bew: Da G nilp. ist, ex. ein $n \in \mathbb{N}$ mit $G^n = 1 \subseteq U$. Sei $m \in \mathbb{N}$ min. mit $G^m \subseteq U$. Wg. $G^1 = G \not\subseteq U$ ist $m \geq 2$. Wg. $[U, G^{m-1}] \subseteq [G, G^{m-1}] = G^m \subseteq U$ ist $G^{m-1} \subseteq N_G(U)$ nach Satz 8.3 (ii), aber $G^{m-1} \not\subseteq U$.

9.8 Satz: Für jeden Normalt. $N \neq 1$ einer nilp. Gr. G ist $[G,N] < N$ & $Z(G) \cap N \neq 1$; insbes. liegt jeder min. Normalt. einer nilp. Gr. im Zentrum.

Bew: Def. $N_1 := N$ & $N_{i+1} := [G, N_i]$ $(i \in \mathbb{N})$. Dann: $N_i \trianglelefteq G$, $N_i \trianglelefteq N$ & $N_i \subseteq G^i$ $(i \in \mathbb{N})$. Da G nilp. ist, ex. ein $m \in \mathbb{N}$ mit $1 = G^m = N_m$. Dann: $N_2 = [G,N] < N$; denn im Fall $N_2 = N$ wäre auch $N_3 = [G, N_2] = [G,N] = N_2 = N$, usw. ↯ Sei $n \in \mathbb{N}$ mit $N_n = 1 \neq N_{n-1}$. Dann: $[G, N_{n-1}] = N_n = 1$, also $N_{n-1} \subseteq Z(G) \cap N$.

9.9 Satz: Für nilp. Normalt. A, B einer Gr. G ist auch AB ein nilp. Normalt. von G. Hat A die Kl. a & B die Kl. b, so hat AB höchstens die Kl. $a+b$.

Bew: Nach Satz 8.4 (i) gilt für $L, M, N \trianglelefteq G$:

$$[L, MN] = [L,M][L,N] \quad \& \quad [LM, N] = [L,N][M,N].$$

Daraus folgt, dass $(AB)^{a+b+1}$ ein Produkt von Grn. der Form $[H_0, \ldots, H_{a+b}]$ $(H_0, \ldots, H_{a+b} \in \{A, B\})$ ist. Wg. Bem. 9.6 (i) genügt zu zeigen, dass jede dieser Grn. trivial ist. Sei also $m := |\{i : H_i = A\}|$, $n := |\{i : H_i = B\}|$. Dann: $a+b+1 = m+n$, also $m > a$ oder $n > b$, OE $m > a$. Dann: $[H_0, \ldots, H_{a+b}] \subseteq A^m \subseteq A^{a+1} = \underline{1}.$

Bem: I.a. ist eine Gr. G, die einen nilp. Normalt. N mit einer nilp. Faktorgr. G/N hat, nicht selbst nilp.

Bsp: $G = \mathrm{Sym}(3)$, $N = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\rangle$.

10. Gruppenoperationen

10.1 Def.: Eine (<u>Links-</u>) <u>Operation</u> (action) einer Gr. G auf einer Menge Ω ist eine Abb.

$$G \times \Omega \longrightarrow \Omega,\ (g,\omega) \longmapsto {}^g\omega,$$ mit folgenden Eigenschaften:

- ${}^1\omega = \omega$ & ${}^a({}^b\omega) = {}^{ab}\omega$ für alle ~~an~~ $\omega \in \Omega$, $a, b \in G$.

Man sagt auch: "G <u>operiert</u> auf Ω" oder "Ω ist eine G-<u>Menge</u>".

<u>Bem:</u> (i) Rechtsoperationen def. man analog als Abbn. $\Omega \times G \longrightarrow \Omega$, $(\omega, g) \longmapsto \omega^g$.

(ii) Man beachte die Analogie zur Mult. von Vektoren eines Vr. mit Skalaren aus einem Körper.

<u>Bsp:</u> (i) Für jede Menge Ω op. $\mathrm{Sym}(\Omega)$ auf Ω durch ${}^g\omega := g(\omega)$ ~~für~~ ($g \in \mathrm{Sym}(\Omega)$, $\omega \in \Omega$).

(ii) Für jeden Körper K ~~und~~ & jeden K-Vr. V op.

$$GL(V) = \{ f : V \longrightarrow V \mid f \text{ lin. \& bij.} \}$$

auf V durch ${}^g v := g(v)$ ~~für~~ ($g \in GL(V)$, $v \in V$).

(iii) Für $n \in \mathbb{N}$ ~~und~~ jeden Körper K op. $GL(n,K)$ auf $K^{n \times n}$ durch

$$^A B = A B A^{-1} \quad (A \in GL(n,K),\ B \in K^{n\times n})$$

(iv) Für $m, n \in \mathbb{N}$ & jeden Körper K op. $GL(m,K) \times GL(n,K)$ auf $K^{m \times n}$ durch ${}^{(A,B)}C = A C B^{-1}$ ($A \in GL(m,K)$, $B \in GL(n,K)$, $C \in K^{m\times n}$).

(v) Für $n \in \mathbb{N}$ op. die <u>orthogonale Gruppe</u>

$$O(n, \mathbb{R}) = \{ A \in \mathbb{R}^{n\times n} : A A^T = 1_n \}$$

des <u>Grades</u> n über $\mathbb{R}$ auf die Menge S aller <u>reellen symmetrischen</u> $n\times n$-Matrizen durch ${}^A B := A B A^T$ ($A \in O(n,\mathbb{R})$, $B \in S$).

(vi) Analog op. die <u>unitäre Gruppe</u>

$$U(n, \mathbb{C}) = \{ A \in \mathbb{C}^{n\times n} : A \bar{A}^T = 1_n \}$$

des Grades n über $\mathbb{C}$ auf die Menge H aller <u>hermitischen</u> $n\times n$-Matrizen $B = \bar{B}^T$ durch ${}^A B := A B \bar{A}^T$ ($A \in U(n,\mathbb{C})$, $B \in H$).

<u>Satz:</u> Für jede Gr. G, jede G-Menge Ω & $g \in G$ ist $\tau_g : \Omega \longrightarrow \Omega$, $\omega \longmapsto {}^g\omega$, bij., d.h. $\tau_g \in \mathrm{Sym}(\Omega)$. Außerdem ist $\tau : G \longrightarrow \mathrm{Sym}(\Omega)$, $g \longmapsto \tau_g$, ein Hom.

<u>Bew:</u> Für $a, b \in G$, $\omega \in \Omega$ ist $(\tau_a \circ \tau_b)(\omega) = {}^a({}^b\omega) = {}^{ab}\omega = \tau_{ab}(\omega)$ & $\tau_1(\omega) = {}^1\omega = \omega$. Daher ~~gilt~~ $\tau_a \circ \tau_b = \tau_{ab}$ & $\tau_1 = \mathrm{id}_\Omega$; insbes.: $\tau_a \circ \tau_{a^{-1}} = \tau_{aa^{-1}} = \tau_1 = \mathrm{id}_\Omega$ & analog $\tau_{a^{-1}} \circ \tau_a = \mathrm{id}_\Omega$. Folglich: τ_a bij.

Ferner ist τ ein Hom.

10.2 Bem: Nach Satz 10.1 induziert jede Op. einer Gr. G auf einer Menge Ω einen Hom. $G \longrightarrow \mathrm{Sym}(\Omega)$. Wir zeigen jetzt umgekehrt, dass jeder Hom. $G \longrightarrow \mathrm{Sym}(\Omega)$ eine Op. von G auf Ω induziert. Man sieht sofort, dass beide Prozesse zueinander invers sind.

Satz: Seien G eine Gr., Ω eine Menge & $\tau: G \longrightarrow \mathrm{Sym}(\Omega)$ ein Hom. Dann erhält man durch ${}^g\omega = (\tau(g))(\omega)$ $(g \in G, \omega \in \Omega)$ eine Op. von G auf Ω.

Bew: Da τ ein Hom. ist, ist $\tau(1) = 1_{\mathrm{Sym}(\Omega)} = \mathrm{id}_\Omega$. Daher: ${}^1\omega = (\tau(1))(\omega) = \mathrm{id}_\Omega(\omega) = \omega$ &

$${}^a({}^b\omega) = (\tau(a))\big((\tau(b))(\omega)\big) = (\tau(a)\circ\tau(b))(\omega) = (\tau(ab))(\omega) = {}^{ab}\omega$$

für $\omega \in \Omega$, $a, b \in G$.

Def: Seien G eine Gr., Ω eine G-Menge & $\tau: G \longrightarrow \mathrm{Sym}(\Omega)$ der entsprechende Hom. Dann heißt

$$\mathrm{Ker}(\tau) = \{g \in G : \tau(g) = \mathrm{id}_\Omega\} = \{g \in G : {}^g\omega = \omega \text{ für } \omega \in \Omega\}$$

Kern der Operation. Ist $\mathrm{Ker}\,\tau = G$, d.h. ${}^g\omega = \omega$ für alle $g \in G, \omega \in \Omega$, so heißt die Op. trivial. Ist $\mathrm{Ker}\,\tau = 1$, d.h. ist τ inj., so heißt die Op. treu. Ggf. gilt: $G \cong \tau(G) \leq \mathrm{Sym}(\Omega)$.

10.3 Satz: (Cayley)
Jede Gr. G ist zu einer Ugr. einer symm. Gr. isom.

Bew: G wird zu einer G-Menge durch ${}^g\omega := g\omega$ für $g, \omega \in G$. Diese ist treu; denn aus ${}^g\omega = \omega$ für alle $\omega \in \Omega$ folgt $g = 1$. Mit den obigen Bezeichnungen ist also $G \cong \tau(G) \leq \mathrm{Sym}(G)$.

10.4 Satz: Seien G eine Gr. & Ω eine G-Menge. Für $\alpha, \beta \in \Omega$ schreiben wir $\alpha \sim \beta$, falls ein $g \in G$ mit ${}^g\alpha = \beta$ ex. Dann ist $\sim$ eine Äquiv.-Rel. auf Ω, d.h. für $\alpha, \beta, \gamma \in \Omega$ gilt:

(i) (Reflexivität) $\alpha \sim \alpha$;

(ii) (Symmetrie) $\alpha \sim \beta \Rightarrow \beta \sim \alpha$;

(iii) (Transitivität) $\alpha \sim \beta \wedge \beta \sim \gamma \Rightarrow \alpha \sim \gamma$.

Bew: (i) ${}^1\alpha = \alpha$.

(ii) Ist $g \in G$ mit ${}^g\alpha = \beta$, so ist $g^{-1} \in G$ mit ${}^{g^{-1}}\beta = {}^{g^{-1}}({}^g\alpha) = {}^{g^{-1}g}\alpha = {}^1\alpha = \alpha$.

(iii) Sind $g, h \in G$ mit ${}^g\alpha = \beta$, ${}^h\beta = \gamma$, so ist $hg \in G$ mit ${}^{hg}\alpha = {}^h({}^g\alpha) = {}^h\beta = \gamma$.

Bem: Für $\alpha \in \Omega$ ist die Bahn $\mathrm{Orb}_G(\alpha) := \{ {}^g\alpha : g \in G \}$ (orbit) die Äquiv.-Kl. von α bzgl. $\sim$; $|\mathrm{Orb}_G(\alpha)|$ heißt Länge der Bahn von α. Aus allg. Tatsachen über Äquiv.-Rel. folgt, dass Ω die disjunkte Vereinigung der verschiedenen Bahnen von G auf Ω ist. Für jedes Repräsentantensystem R dieser Bahnen gilt also:

$$\Omega = \dot\bigcup_{\alpha \in R} \mathrm{Orb}_G(\alpha) \ \& \ |\Omega| = \sum_{\alpha \in R} |\mathrm{Orb}_G(\alpha)| \quad \text{(Bahnengleichung).}$$

Bsp: (i) Für $n \in \mathbb{N}$ & jeden Körper K liegen zwei Matrizen aus $K^{n\times n}$ genau dann in der gleichen Bahn unter der Op. von $GL(n,K)$ auf $K^{n\times n}$ durch ${}^AB := ABA^{-1}$ $(A \in GL(n,K),\ B \in K^{n\times n})$, wenn sie ähnlich im Sinn der Lin. Alg. sind.

(ii) Für $m, n \in \mathbb{N}$ & jeden Körper K liegen zwei Matrizen aus $K^{m\times n}$ genau dann in der gleichen Bahn unter der Op. von $GL(m,K) \times GL(n,K)$ auf $K^{m\times n}$ durch ${}^{(A,B)}C = ACB^{-1}$ $(A \in GL(m,K),\ B \in GL(n,K),\ C \in K^{m\times n})$, wenn sie äquivalent im Sinne der Lin. Alg. sind.

10.5 Def: Für jede Gr. G, jede G-Menge Ω & $\omega \in \Omega$ heißt $\mathrm{Stb}_G(\omega) := G_\omega := \{ g \in G : {}^g\omega = \omega \}$ Stabilisator von ω in G.

Satz: In dieser Situation gilt: (i) $\mathrm{Stb}_G(\omega) \leq G$.

(ii) $x \in G \Rightarrow \mathrm{Stb}_G({}^x\omega) = x\,\mathrm{Stb}_G(\omega)\,x^{-1}$.

(iii) Die Abb. $f : G/\mathrm{Stb}_G(\omega) \longrightarrow \mathrm{Orb}_G(\omega)$, $g\,\mathrm{Stb}_G(\omega) \longmapsto {}^g\omega$, ist bij.; insbes. ist $|\mathrm{Orb}_G(\omega)| = |G : \mathrm{Stb}_G(\omega)|$. Im Fall $|G| < \infty$ ist also jede Bahnlänge ein Teiler von $|G|$.

Bew: (i) Wg. ${}^1\omega = \omega$ ist $1 \in \mathrm{Stb}_G(\omega)$, & für $a, b \in \mathrm{Stb}_G(\omega)$ ist $ab^{-1} \in \mathrm{Stb}_G(\omega)$ wg ${}^{ab^{-1}}\omega = {}^{ab^{-1}}({}^b\omega) = {}^{ab^{-1}b}\omega = {}^a\omega = \omega$.

(ii) $g \in \mathrm{Stb}_G({}^x\omega) \iff {}^{gx}\omega = {}^x\omega \iff {}^{x^{-1}gx}\omega = \omega \iff x^{-1}gx \in \mathrm{Stb}_G(\omega)$ $\iff g \in x\,\mathrm{Stb}_G(\omega)\,x^{-1}$.

(iii) Für $g, h \in G$ gilt: ${}^g\omega = {}^h\omega \iff {}^{g^{-1}h}\omega = \omega \iff g^{-1}h \in \mathrm{Stb}_G(\omega) \iff$ $g\,\mathrm{Stb}_G(\omega) = h\,\mathrm{Stb}_G(\omega)$.

10.6 Def: Seien G eine Gr. & $\Omega \neq \emptyset$ eine G-Menge mit einer einzigen Bahn. Dann heißt die Op. transitiv.

Bsp: Für jede Gr. G & $H \leq G$ op. G transitiv auf G/H durch ${}^x(gH) := xgH$ $(x, g \in G)$. Dabei gilt:

$xgH = gH \iff g^{-1}xgH = H \iff g^{-1}xg \in H \iff x \in gHg^{-1}$.

Daher: $\mathrm{Stb}_G(gH) = gHg^{-1}$; insbes.: $\mathrm{Stb}_G(H) = H$, & der Kern der Op. von G auf G/H ist $\bigcap_{g\in G}\mathrm{Stb}_G(gH) = \bigcap_{g\in G} gHg^{-1} =: \mathrm{Core}_G(H)$, der <u>Kern</u> von H in G. Offenbar ist $\mathrm{Core}_G(H)$ der größte Normalt. $N \trianglelefteq G$ mit $N \subseteq H$, & $G/\mathrm{Core}_G(H)$ ist zu einer Ugr. von $\mathrm{Sym}(G/H)$ isom. So kann man oft nichttriv. Normalt. von G konstruieren.

<u>Bem:</u> Eine G-Menge $\Omega \neq \emptyset$ ist genau dann transit., wenn zu je zwei $\alpha,\beta\in\Omega$ ein $g\in G$ mit ${}^g\alpha=\beta$ ex. Ggf. ist $|\Omega| = |G:\mathrm{Stb}_G(\omega)|$ für $\omega\in\Omega$. Ex. zu je zwei $\alpha,\beta\in\Omega$ <u>genau ein</u> $g\in G$ mit ${}^g\alpha=\beta$, so heißt die Op. <u>regulär</u>. Ggf. ist $|\Omega|=|G|$.

<u>Satz:</u> (Frattini-Argument)
Seien G eine Gr., $H\le G$ & $\Omega\neq\emptyset$ eine G-Menge. Op. H trans. auf Ω, so ist $G = \mathrm{Stb}_G(\omega)H$ für $\omega\in\Omega$.

<u>Bew:</u> Seien $\omega\in\Omega$, $g\in G$. Da H trans. op., ex. ein $h\in H$ mit ${}^h({}^g\omega)=\omega$. Folglich: $hg\in\mathrm{Stb}_G(\omega)$ & $g = h^{-1}\cdot hg \in H\,\mathrm{Stb}_G(\omega)$. Daher $G = H\cdot\mathrm{Stb}_G(\omega) = \mathrm{Stb}_G(\omega)H$.

<u>10.7 Def:</u> Seien G eine Gr., Ω eine G-Menge, $x\in G$ & $Y\subseteq G$. Dann heißen die El. in $\mathrm{Fix}_\Omega(x) := \{\omega\in\Omega : {}^x\omega=\omega\}$ bzw. $\mathrm{Fix}_\Omega(Y) := \{\omega\in\Omega : {}^y\omega=\omega \text{ für } y\in Y\}$
<u>Fixpunkte</u> von x bzw. Y.

<u>Satz:</u> (Burnsides Lemma)
Seien G eine endl. Gr. & Ω eine endl. G-Menge.

(i) Für die Anzahl n der Bahnen von G auf Ω gilt dann:
$$n = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}_\Omega(g)|.$$

(ii) Ist die Op. trans. & $\omega\in\Omega$, so gilt für die Anzahl m der Bahnen von $\mathrm{Stb}_G(\omega)$ auf Ω:
$$m = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}_\Omega(g)|^2$$

<u>Bew:</u> (i) Offenbar ist
$$\sum_{g\in G}|\mathrm{Fix}_\Omega(g)| = |\{(g,\omega)\in G\times\Omega : {}^g\omega=\omega\}| = \sum_{\omega\in\Omega}|\mathrm{Stb}_G(\omega)|.$$
Auf jeder Bahn ist $|\mathrm{Stb}_G(\omega)|$ konstant nach Satz 10.5 (ii), & die Bahn von $\omega\in\Omega$ enthält genau $|G:\mathrm{Stb}_G(\omega)|$ El. Mit Lagrange ergibt sich:
$$\sum_{\omega\in\Omega}|\mathrm{Stb}_G(\omega)| = n\cdot|G|.$$