<u>Noch zu A4:</u> $G$, UG $N \subseteq G$ heißt NT $:\Leftrightarrow \forall a \in G: aNa^{-1} = N$ („$\subseteq$" „$\supseteq$")

$\Leftrightarrow \forall a \in G: aNa^{-1} \subseteq N$

$$\boxed{\Leftrightarrow \underbrace{a^{-1}aNa^{-1}a}_{N} \subseteq a^{-1}Na}$$

4.21. **Homomorphiesatz:**

Vor.: $G$ Gr., $N \trianglelefteq G$ NT

Beh.: (i) $\pi: G \to G/N$

$a \mapsto aN$ "Proj." zu $N$

ist surj. Gr.hom., $\ker \pi = N$

(ii) „univ. Eigensch.":

$\forall \varphi \in \mathrm{Hom}(G,H)$, $H$ Gr., $N \subseteq \ker\varphi$

$\exists!\, \bar\varphi : \mathrm{Hom}(G/N, H): \bar\varphi \circ \pi = \varphi.$

$$\begin{tikzcd}
N \subseteq \ker\varphi \trianglelefteq G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & H \\
G/N \arrow[ur, dashed, "\bar\varphi"'] &
\end{tikzcd}$$

$G/N \ni \left(\begin{array}{c} eN = N \\ \text{neutr. El.} \end{array}\right)$ $\qquad \varphi = \bar\varphi \circ \pi$

<u>Zusatz:</u> $(\alpha)$ $\mathrm{im}\,\bar\varphi = \mathrm{im}\,\varphi$

$(\beta)$ $\bar\varphi$ inj. $\Leftrightarrow \ker\varphi = N$

$(\gamma)$: $(\alpha) \wedge (\beta) \Rightarrow$

$$\boxed{\mathrm{im}\,\varphi \cong G/\ker\varphi = G/N}$$

<u>Bew.:</u> (i) $\pi$ Hom.: $\pi(ab) = (ab)N = (aN)(bN) = \pi(a)\pi(b)$ ✓, surj. ✓

$\ker\pi = N$: $aN = \pi(a) = e = eN \Leftrightarrow a \in N$ ✓

(ii) Sei $\varphi \in \mathrm{Hom}(G,H)$, $N \subseteq \ker\varphi$. $\to \forall a \in N: \varphi(a) = e_H$.

Def. $\bar\varphi(aN) := \varphi(a)$, dann $\bar\varphi \circ \pi = \varphi$. ✓

* wohldef.: $aN = bN \Rightarrow a^{-1}b \in N \subseteq \ker\varphi$

$\Rightarrow e = \varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b) \Rightarrow \varphi(a) = \varphi(b)$.

* eind.: nach Def. ✓

* Hom.: $\bar\varphi((aN)(bN)) = \bar\varphi((ab)N) = \varphi(ab) = \varphi(a)\varphi(b) = \bar\varphi(aN)\bar\varphi(bN)$.

$(\alpha)$ $\mathrm{im}\,\varphi = \mathrm{im}\,\bar\varphi$ nach Def. ✓, da $\pi$ surj.

$(\beta)$ „$\Rightarrow$" $\bar\varphi$ inj. z.z. $\ker\varphi \subseteq N$. Dazu: $a \in \ker\varphi \Leftrightarrow e = \varphi(a) = \bar\varphi \circ \pi(a) = \bar\varphi(aN)$

$\overset{\bar\varphi \text{ inj.}}{\Leftrightarrow} aN = N \Rightarrow a \in N$.

„$\Leftarrow$": $e_H = \bar\varphi(aN) = \bar\varphi(\pi a) = \varphi(a) \Rightarrow a \in N \Rightarrow aN = N \Rightarrow \bar\varphi$ inj.

(γ): $(\alpha)\wedge(\beta)$

$$\begin{tikzcd} G \arrow[r, two heads, "\varphi"] \arrow[d, two heads, "\pi"'] & \operatorname{im}\varphi \subseteq H \\ \underbrace{G/\ker\varphi}_{N} \arrow[ur, dashed, "\bar\varphi"', "\cong"] & \end{tikzcd}$$

$\left.\begin{array}{l} (\alpha) \rightsquigarrow \bar\varphi \text{ surj., da } \varphi \text{ surj.} \\ (\beta) \rightsquigarrow \bar\varphi \text{ inj., da } \ker\varphi = N \end{array}\right\} \Rightarrow \bar\varphi$ bij., also Isom.

$$\underline{\operatorname{im}\varphi \cong G/\ker\varphi.}$$ □

4.22 → 2. Isomorphiesatz:

$(N \trianglelefteq G,\ \pi: G \to G/N,\ a \mapsto aN)$

$$G/M \cong \underbrace{(G/N)}_{\bar G} / \underbrace{(M/N)}_{\bar M}$$

| $\mathcal{U}$: | $\bar{\mathcal{U}}$: |
|---|---|
| $G$ | $\bar G = G/N$ |
| $\cup\!\mid$ | $\cup\!\mid$ |
| $M$ | $\bar M = M/N$ |
| $\cup\!\mid$ | |
| $N$ | |

4.23 <u>Satz</u>: $G$ zyklische Gr. Dann: $\begin{cases} G \cong \mathbb{Z}, & \#G = \infty \\ G \cong \mathbb{Z}/\mathbb{Z}r, & \#G = r \in \mathbb{N} \end{cases}$

<u>Bew.</u>: Sei $G = \langle a \rangle$, dann: $\varphi: \mathbb{Z} \twoheadrightarrow G$, $n \mapsto a^n$ surj. Gruppenhom.

$\boxed{\text{Hom.satz} \overset{}{\Rightarrow} 4.21}$ $\underline{\underline{G \cong \mathbb{Z}/\ker\varphi}} \begin{cases} = \mathbb{Z}/\mathbb{Z}r, & \text{falls } \ker\varphi = \mathbb{Z}r,\ r = \#G \in \mathbb{N} \\ \cong \mathbb{Z}, & \text{sonst } \ker\varphi = \{0\} \text{ mit } \#G = \infty \end{cases}$

$\left\{ \begin{array}{l} \text{alle UG von } \mathbb{Z}: \\ \underline{\underline{r\mathbb{Z}}} \text{ bzw. } \underline{\underline{\{0\}}} \end{array} \right\} \Leftarrow$ Bsp. 2.6 ! □

4.24 <u>Satz (UG von zykl. Gruppen):</u>

(i) $\mathbb{Z}$: UG von $\mathbb{Z}$ sind $\mathbb{Z}r$, $r \in \mathbb{N}_0$, alle zykl.

Es gilt: $\underline{\mathbb{Z}r \subseteq \mathbb{Z}s} \Leftrightarrow r \in \mathbb{Z}s \Leftrightarrow \underline{s \mid r}$

(ii) $\mathbb{Z}/\mathbb{Z}r$: Sei $H \subseteq \mathbb{Z}/\mathbb{Z}r$ eine UG. Bet. $\pi: \mathbb{Z} \to \mathbb{Z}/\mathbb{Z}r$,

$\Rightarrow \pi^{-1}(H)$ UG von $\mathbb{Z}$, d.h. zykl., also $\pi^{-1}(H) = \mathbb{Z}s$, $s \in \mathbb{N}_0$

$\Rightarrow H = \pi(\pi^{-1}(H)) = \pi(\mathbb{Z}s) = \mathbb{Z}s/\mathbb{Z}r$ zyklisch

also: $H \cong \underline{\underline{\mathbb{Z}/\mathbb{Z}t}}$, $t \in \mathbb{N}_0$, dabei $\underline{t \mid r}$, denn $H = \langle s + \mathbb{Z}r \rangle$, $t = \#H = \operatorname{ord}(s+\mathbb{Z}r) \mid r$.

# A5: Die symmetrischen Gruppen $S_n$

5.1. $S_n$, $A_n$, $A_n$ ist für $n \geq 5$ einfach

5.2. **Lemma:** Für $S_n := \{ \sigma : \{1,\dots,n\} \to \{1,\dots,n\};\ \sigma \text{ bij.} \}$ gilt: $\# S_n = n!$

5.3. **Def.:** Sei $r \geq 1$. $\sigma \in S_n$ heißt r-Zyklus $:\Leftrightarrow$
$\exists$ pwv $i_1,\dots,i_r \in \{1,\dots,n\}$: $\sigma(i_\nu) = \begin{cases} i_{\nu+1}, & 1 \leq \nu < r \\ i_1, & \nu = r \end{cases}$

und $\sigma(i) = i$ für $i \notin \{i_1,\dots,i_r\}$.

Schreibweise: $(i_1, i_2, \dots, i_r)$ für $\sigma$

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 3 & 1 & 2 \end{pmatrix}$

$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $1 \to 2 \to 3 \to 1$

Bsp.: $\sigma = (1\ 2\ 3) \in S_3$

$\tau = (2\ 4\ 1\ 3) \in S_5$
$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix}$
$= (4\ 1\ 3\ 2)$

5.4. **Bem.:** $(i_1, \dots, i_r) = (i_2, \dots, i_r, i_1)$

5.5. **Def.:** 2-Zyklen $(ij)$ heißen Transpositionen.

Bsp.: $S_4 \ni (1\ 2)(3\ 4\ 1) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1\ 3\ 4\ 2)$

$(1\ 2)(1\ 2\ 3) = (2\ 3)$

$(3\ 4\ 1)(1\ 3)(2\ 4) = (1\ 4\ 2)$

$(1\ 2)(3\ 1) = (1\ 3\ 2)$

$\underbrace{(1\ 4\ 5)}_{\tau} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix}$, $\sigma$

$(1\ 4\ 5)(1\ 2) = \tau \circ \sigma$

5.6. **Lemma:** Jeder r-Zyklus ist Produkt von $r-1$ Transpositionen.

Bew.: VI nach $r \geq 2$: $r = 2$: $(i_1, i_2)$ ✓

$r \rightsquigarrow r+1$: $(i_1, \dots, i_r, i_{r+1}) = (i_r\ i_{r+1}) \underbrace{(i_1, \dots, i_r)}_{IV}$

$\square$

5.7. **Lemma:** Elementfremde Zyklen kommutieren. Bsp.: $(1\ 2)(4\ 5) = (4\ 5)(1\ 2)$

Bew.: Sei $\sigma = (i_1, \dots, i_r)$, $\tau = (j_1, \dots, j_s)$, $\forall k, l: i_k \neq j_l$

$\Rightarrow \sigma\tau = \sigma \circ \tau = (i_1 \dots i_r) \circ (j_1 \dots j_s) = (j_1 \dots j_s)(i_1 \dots i_r) = \tau\sigma$. $\square$

5.8. **Satz:** Jedes $\sigma \in S_n$ ist Produkt elementfremder Zyklen (der Länge $\geq 2$):
$\sigma = \rho_1 \cdots \rho_r$, die $\{\rho_1, \dots, \rho_s\}$ eind. best.

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

**Bew.:** Sei OE $\sigma \neq id$.
Ex.: $G = \langle \sigma \rangle = \{\sigma, \sigma^2, \dots\} \leq S_n$.
$G$ op. auf $X = \{1, \dots, n\}$, $G \times X \to X$
$(\sigma, i) \mapsto \sigma(i)$

Sei $X = X_1 \dot\cup \dots \dot\cup X_t$ die Bahnzerl. von $X$,
dabei OE $\# X_i \geq 2 \Leftrightarrow 1 \leq i \leq s$.
Sei $1 \leq j \leq s$, $X_j = Gi$, $\# X_j =: r$, $H := Iso(i) \leq G$ UG.
Dann (A 3.14): Bij. $G/H \longrightarrow X_j = Gi$
$\sigma^\ell H \longmapsto \sigma^\ell(i)$.
⌐$G$ ab. $\overset{A\,2.23}{\Rightarrow} H$ NT, also $G/H$ Gruppe, $\# G/H = r$,
also: $G/H = \{H, \sigma H, \sigma^2 H, \dots, \sigma^{r-1} H\}$⌐
$\Rightarrow X_j = \{i, \sigma i, \sigma^2 i, \dots, \sigma^{r-1} i\}$ und $\sigma \restriction X_j = \rho_j \restriction X_j$,

$\rho_j := (i, \sigma i, \sigma^2 i, \dots, \sigma^{r-1} i)$. Somit: $\sigma = \rho_1 \cdot \ldots \cdot \rho_s$.
steht für "$\circ$".

Eind.: Für $\sigma \in S_n$ sei $\sigma = \underbrace{\rho_1 \cdots \rho_s}_{\text{el. fremde Zyklen}} = \underbrace{\rho_1' \cdots \rho_{s'}'}_{\text{el. fremde Zyklen}}$, die $\rho_n$ wie oben konstruiert

zeige: $\forall i\ \exists j: \rho_i' = \rho_j$
OE $i = 1$, $\rho_1' = (\ell_1, \dots, \ell_r)$, $r \geq 2$ $\rightsquigarrow \sigma(\ell_1) = \ell_2, \sigma(\ell_2) = \ell_3, \dots, \sigma(\ell_r) = \ell_1$
$\Rightarrow \{\ell_1, \dots, \ell_r\}$ ist Bahn, also $X_j = \{\ell_1, \dots, \ell_r\}$
und $\ell_\nu = \sigma^{\nu - 1}(\ell_1)$, $\ell_1 = \sigma(\ell_r) = \sigma^r(\ell_1)$
$\Rightarrow \exists j: \rho_j = (\ell_1, \dots, \ell_r) = \rho_1'$. □

5.9. **Kor.:** Jede Permutation ist Produkt von Transpositionen.

5.10 **Bem.:** Sei $\rho = (i_1 \dots i_r)$ $r$-Zykl., $\tau \in S_n$ $\Rightarrow$ $\tau \rho \tau^{-1} = (\tau i_1, \dots, \tau i_r)$ wieder $r$-Zyklus

**Bsp.:** $\underbrace{(1\,4\,5)}_{\tau =}(1\,2\,3)\underbrace{(5\,4\,1)}_{=(145)^{-1}} = (2\,3\,4) = (\underset{\tau(1)}{4}\;\underset{\tau(2)}{2}\;\underset{\tau(3)}{3})$

**Bew.:**

$\tau(i_\nu) \xmapsto{\tau^{-1}} i_\nu \xmapsto{\rho} i_{\nu+1} \xmapsto{\tau} \tau(i_{\nu+1})$, $\quad 1 \leq \nu \leq r-1$,

$j \mapsto \tau^{-1}(j) \longmapsto \tau^{-1}(j) \mapsto j$, $\quad j \in \{\tau(i_\nu);\ \nu \in \{1, \dots, r\}\}$

$\tau(i_r) \mapsto i_r \longmapsto i_1 \longmapsto \tau(i_1)$

□

5.11 **Def.:** Sei $\sigma \in S_n$, $\sigma \neq e$.
Sei $\sigma = \rho_1 \cdot \ldots \cdot \rho_m$ Darst. als Prod. d. fr. Zyklen, $r_i := \text{Länge } \rho_i \geq 2$
mit $r_1 \geq r_2 \geq \ldots \geq r_s$.
Die Folge $[r_1, r_2, \dots, r_s]$ heißt Zyklentyp von $\sigma$.

Bsp.: Z.T. von $(1\,2)(4\,5\,6)(7\,8\,9\,10)$ ist $[4, 3, 2]$
" von $(1\,2)(3\,4)$ ist $[2, 2]$
" von $(1\,2\,3)(4\,5)$ ist $[3, 2]$

5.12 **Bem.:** $\sigma, \sigma' \in S_n \setminus \{id\}$ konj. (d.h. $\exists \tau \in S_n : \sigma' = \tau \sigma \tau^{-1}$)
$\Leftrightarrow$ $\sigma, \sigma'$ gleichen Zyklentyp

**Bew.:** "$\Rightarrow$": Sei $\sigma = \rho_1 \cdot \ldots \cdot \rho_s$, $\sigma' = \tau \sigma \tau^{-1}$
$\Rightarrow \sigma' = \tau \sigma \tau^{-1} = (\tau \rho_1 \tau^{-1})(\tau \rho_2 \tau^{-1})(\tau \rho_3 \tau^{-1}) \dots (\tau \rho_s \tau^{-1})$
nach Bem. 5.10

"$\Leftarrow$": Sei $\sigma = \rho_1 \cdots \rho_s$, $\sigma' = \rho_1' \cdots \rho_s'$ mit Länge $\rho_i$ = Länge $\rho_i' \geq 2$
Wähle $\tau \in S_n$ mit $\tau \rho_i \tau^{-1} = \rho_i'$ (geht, da dieselbe Länge, mit Bem. 5.10)

$\Rightarrow \tau \sigma \tau^{-1} = (\underbrace{\tau \rho_1 \tau^{-1}}_{\rho_1'}) \cdots (\underbrace{\tau \rho_s \tau^{-1}}_{\rho_s'}) = \sigma'$.

□