Gruppen

<u>Gruppe</u> G: Monoid mit $G^\times = G$

<u>Bsp</u>: $(\mathbb{Z}, +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$, $(\mathrm{Sym}(M), \circ)$

<u>Untergruppe</u> U von G: $1 \in U \subseteq G$, $(U, \cdot)$ Gruppe

$\Leftrightarrow$ Untermagma, abgeschlossen unter Inversenbildung

$\Leftrightarrow$ $U \neq \emptyset$ und $x, y \in U \Rightarrow xy^{-1} \in U$

$$\langle M \rangle := \bigcap_{\substack{M \subseteq U \\ U \leq G \text{ UG}}} U = \{x_1 \cdots x_n : n \in \mathbb{N}_0,\ x_i \in M \text{ oder } x_i^{-1} \in M\}$$

↳ kleinste UG von G, die M enthält

<u>Direktes Produkt</u> $G \times H$ mit

$(g, h)(\tilde{g}, \tilde{h}) := (g\tilde{g}, h\tilde{h})$

$\leadsto$ $1 = (1_G, 1_H)$, $(g,h)^{-1} = (g^{-1}, h^{-1})$, ...

G <u>einfach</u>: einzige UGen $\{1\}$, G

<u>Ordnung</u> von G: ~~#G~~ $\mathrm{ord}(G) := \#G$

von $g \in G$: $\mathrm{ord}(g) := \# \langle g \rangle$

$= \min\{k \in \mathbb{N} : g^k = 1\} \in \mathbb{N} \cup \{\infty\}$

<u>Satz von Lagrange</u>: $H \leq G$ UGe, G endlich

$\Rightarrow \mathrm{ord}(H) \mid \mathrm{ord}(G)$

<u>Bem</u>: $g^n = 1 \Rightarrow \mathrm{ord}(g) \mid n$ (Euklids Algo)

<u>Homomorphismus</u> $\Phi : G \to H$:

$$\Phi(xy) = \Phi(x)\,\Phi(y) \qquad (\forall x, y \in G)$$

$\rightsquigarrow$ $\Phi(1) = 1$, $\Phi(x)^{-1} = \Phi(x^{-1})$, $\Phi(G) \subseteq H$ UGe,

$\Phi^{-1}(U) \subseteq G$ UG falls $U \leq H$ UGe

<u>Hom</u>(G,H), <u>End</u>(G), <u>Iso</u>(G,H), <u>Aut</u>(G)

<u>A4</u>: $\Phi \in \mathrm{Iso}(G,H) \implies \mathrm{ord}(x) = \mathrm{ord}(\Phi(x)) \quad (\forall x \in G)$

<u>Beweis</u>:

$$x^n = 1 \implies \Phi(x)^n = \Phi(x^n) = \Phi(1) = 1$$

$\implies \mathrm{ord}(\Phi(x)) \mid \mathrm{ord}(x)$ und

$$\mathrm{ord}(\underbrace{\Phi^{-1}(\Phi(x))}_{=x}) \mid \mathrm{ord}(\Phi(x))$$

$\square$

~~Bsp~~:

<u>Kern</u>: $\ker(\Phi) := \{ g \in G : \Phi(g) = 1 \}$

$\rightsquigarrow$ Φ inj $\iff \ker(\Phi) = \{1\}$

Zyklische Gruppen

G <u>zyklisch</u>: $G = \langle x \rangle$ für ein $x \in G$ $\boxed{\leadsto \text{abelsch}}$

<u>A2</u>: G zyklisch $\Rightarrow$ $G \cong \mathbb{Z}$ oder $G \cong \mathbb{Z}/n\mathbb{Z}$ (für ein n)

<u>Bew</u>: $G = \langle x \rangle$

<u>1. Fall</u>: $\#G = \infty$. Betrachte

$$\Phi : \mathbb{Z} \longrightarrow G, \quad n \longmapsto x^n$$

$\leadsto$ Hom., surjektiv; injektiv, <u>denn</u>:

$x^n = 1$ für $n \neq 0$; o.E. $n > 0$ $\Rightarrow$ $\underset{\#G}{\overset{}{\underset{\shortparallel}{\mathrm{ord}}}}(x) = n < \infty$ ↯

$\#\emptyset$

<u>2. Fall</u>: $\#G = n < \infty$. Betrachte

$$\Phi : \mathbb{Z}/n\mathbb{Z} \longrightarrow G, \quad [m] \longmapsto x^m$$

$\leadsto$ wohldef.: $[m] = [\tilde{m}] \Rightarrow m = \tilde{m} + k \cdot n$

$$\Rightarrow x^m = x^{\tilde{m}} \underbrace{(x^n)}_{=1}{}^k = x^{\tilde{m}}$$

Hom, surjektiv: klar $\overset{\#=\#}{\underset{\text{endl}}{\Longrightarrow}}$ auch injektiv

[oder, nachrechnen (explizit): ~~injektiv~~: $x^m = 1 \Rightarrow \mathrm{ord}(x) \mid m \Rightarrow n \mid m \Rightarrow [m] = 0$] $\square$

<u>A3</u>: $\#G$ prim $\Rightarrow$ G zyklisch

<u>Bew</u>. Wähle $x \in G \setminus \{1\}$

$$\Rightarrow \left.\begin{array}{l} \mathrm{ord}(x) \neq 1 \\ \mathrm{ord}(x) \mid \#G \end{array}\right\} \Rightarrow \left.\begin{array}{l} \mathrm{ord}(x) = \#G \\ \langle x \rangle \subseteq G \end{array}\right\} \Rightarrow \langle x \rangle = G. \qquad \square$$

$\leadsto$ wird sogar von <u>jedem</u> $x \neq 1$ erzeugt

$\leadsto$ kennen die Gp. d.O. 2, 3, 5, 7, ...

A4: $U, V \leq G$ UGen, $\#U = p$, $\#V = q$ prim

$\Rightarrow U = V$ oder $U \cap V = \{1\}$

Bew: $1 \neq x \in U \cap V$

$\overset{A3}{\underset{Bem}{\Longrightarrow}} \langle x \rangle = U = V$. $\square$

A5: Zeige:

(1) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \not\cong \mathbb{Z}/4\mathbb{Z}$

(2) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$

Bew: (1) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ hat kein Element d. O. 4 (vgl. A1)

(2) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \langle ([1]_2, [1]_3) \rangle \rightsquigarrow$ A2. $\square$

Abelsche Gruppen

A6: Zeige:

G abelsch

$\Leftrightarrow (\cdot)^{-1}$ Automorphismus

Dann gilt auch: $\prod_{g \in G} g^2 = 1$
falls G endlich

Bew: ($\Rightarrow$) $(ab)^{-1} = b^{-1}a^{-1} \overset{ab.}{=} a^{-1}b^{-1}$. Also Hom, bijektiv ist klar ($a^{-1} = b^{-1} \Rightarrow a = b$, $a = (a^{-1})^{-1}$)

($\Leftarrow$) $(ab)^{-1} = a^{-1}b^{-1} \Rightarrow ab = (a^{-1}b^{-1})^{-1} = ba$.

Und dann:

$$1 = \Big(\prod_{g \in G} g\Big)\Big(\prod_{g \in G} g\Big)^{-1} \overset{Hom}{=} \Big(\prod_{g \in G} g\Big)\Big(\prod_{g \in G} g^{-1}\Big) \overset{bij.}{=} \Big(\prod_{g \in G} g\Big)\Big(\prod_{g \in G} g\Big) \overset{ab.}{=} \prod_{g \in G} g^2$$

$\square$

Gruppentafeln

$G = \{g_1, \dots, g_n\}$, $n = \# G$

Gruppentafel:

$\cdot$	g_1 ...	g_j ...	g_n
g_1			
$\vdots$			
g_i		$g_i \cdot g_j$	
$\vdots$			
g_n			

Kleinsche Vierergruppe: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{\underbrace{([0],[0])}_{=0}, \underbrace{([1],[0])}_{=a}, \underbrace{([0],[1])}_{=b}, \underbrace{([1],[1])}_{=c}\}$

$+$	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

$\leftarrow$ (neutr. El.)

$\uparrow$ (neutr. El.)

alle Elemente haben Ordnung 2

Bem: • Jedes Element genau einmal pro Zeile & Spalte.

$[x_1 \cdot y = x_2 \cdot y \implies x_1 = x_2]$

• G abelsch $\iff$ Gruppentafel symmetrisch

• $G_1 \cong G_2 \iff$ gleiche Gruppentafel (bis auf Umbenennen & Vertauschen)

A7: Bestimme alle Gruppen d. Ordnung 4.

Lsg: 1. Fall: Es ex. ein Element d. Ordnung 4

$\overset{\text{zyklisch}}{\Longrightarrow} G \cong \mathbb{Z}/4\mathbb{Z}$

2. Fall: Alle Elemente außer 1 haben Ordnung 2

$\rightsquigarrow$

$\cdot$	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

$\Rightarrow G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$\square$

Die Symm. Gruppen

$S_n := \mathrm{Sym}(\{1,\dots,n\})$

~~$\sigma \in S_n$ Permuta~~

Permutation: $\sigma \in S_n$, $\sigma = \begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix}$ („Wertetabelle")

Zykel: $\sigma = (a_1 \dots a_m) \in S_n$ def. durch

$$\begin{cases} \sigma(a_k) := a_{k+1} & (\forall k \in \{1,\dots,m-1\}) \\ \sigma(a_m) := a_1 & \\ \sigma(x) := x & (\text{sonst}) \end{cases}$$

Transposition: $(a\ b) \in S_n$ $(a \neq b)$

klar: $\boxed{\# S_n = n!}$

Bsp:

$S_3 = \{id, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$

nichtabelsch: $(1\ 2)(1\ 3) = (1\ 3\ 2) \neq (1\ 2\ 3) = (1\ 3)(1\ 2)$.

A8: Zeige: $\# G = 6 \Rightarrow$ es ex. Elemente d.O. 2 und 3

Bew. Lagrange $\Rightarrow \mathrm{ord}(x) \in \{1,2,3,6\}$ $(\forall x \in G)$

1. Fall: $\exists x: \mathrm{ord}(x) = 6 \Rightarrow \mathrm{ord}(x^2) = 3$, $\mathrm{ord}(x^3) = 2$

2. Fall: Ann: ~~Es gibt kei Element d. Ordnung~~ 2. $\mathrm{ord}(x) = 2$ $(\forall x \neq 1)$

$\overset{\text{ÜB}}{\underset{4(c)}{\Rightarrow}}$ G abelsch. Wähle $a \neq 1$, $b \in G \setminus \langle a \rangle$

$\Rightarrow \{1, a, b, ab\} \subseteq G$ UGe mit $\underline{\underline{4}}$ Elementen ↯

Ann: ~~Es gibt~~ $\mathrm{ord}(x) = 3$ $(\forall x \neq 1)$

$\Rightarrow$ Wähle $a \neq 1$, $b \in G \setminus \langle a \rangle$, $c \in G \setminus \langle a \rangle \setminus \langle b \rangle$

$\Rightarrow \langle a \rangle, \langle b \rangle, \langle c \rangle$ haben paarw. Schnitt $\{1\} \Rightarrow \underline{\underline{7}}$ Elemente ↯ □

$\underline{A9}$: Bestimme alle Gruppen der Ordnung 6.

$\underline{Lsg}$: ~~1. Fall~~ Wähle $a, b \in G$ mit $ord(a) = 2$, $ord(b) = 3$

$\Rightarrow G = \{1, b, b^2, a, ab, ab^2\} = \underbrace{\langle b \rangle \dot{\cup} a\langle b \rangle}_{\text{denn } a \notin \langle b \rangle \text{ ! (A4)}}$

~~(klar, denn $b^k = ab^l \Leftrightarrow a = b^{k-l} \in \langle a \rangle$ ... $\langle b \rangle$ ...)~~

$\underline{1. Fall}$: G abelsch

$$\Phi : \begin{cases} (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \longrightarrow G \\ ([k]_2, [l]_3) \longmapsto a^k b^l \end{cases}$$

• wohldef: $[k]_2 = [\tilde{k}]_2$, $[l]_3 = [\tilde{l}]_3$

$\Rightarrow 2 \mid k - \tilde{k}$, $3 \mid l - \tilde{l}$

$\Rightarrow a^k b^l = a^{\tilde{k}} \underbrace{a^{k-\tilde{k}}}_{=1} b^{\tilde{l}} \underbrace{b^{l-\tilde{l}}}_{=1} = a^{\tilde{k}} b^{\tilde{l}}$

$\left.\begin{array}{l} \bullet \text{ surjektiv} \\ \#_{..} = \# G \end{array}\right\} \Rightarrow$ bijektiv

• Hom: ✓ ~~abelsch~~ $a^{k+\tilde{k}} b^{l+\tilde{l}} = a^k b^l a^{\tilde{k}} b^{\tilde{l}}$ da abelsch.

$\underline{2. Fall}$: G nicht abelsch

$\Rightarrow$ ~~ab~~ $ba \neq ab$ (sonst $a^k b^l a^{\tilde{k}} b^{\tilde{l}} = a^{\tilde{k}} b^{\tilde{l}} a^k b^l$)

$\Rightarrow$ ~~Außerdem~~ $ba \in \{1, b, b^2, b^2 a, ab\}$

1: sonst $b = a^{-1} = a$; b: sonst $a = 1$; b^2: sonst $a = b$; $b^2 a$: sonst $b = 1$; ab: s.o.

$\Rightarrow \boxed{ba = ab^2}$, und Verknüpfung $(a^k b^l) \cdot (a^{\tilde{k}} b^{\tilde{l}})$ ist eind. bestimmt

$\Rightarrow$ höchstens eine ~~solche~~ nichtab. Gruppe d.O. 6,

$\Rightarrow$ muss S_3 sein! $\square$

Isomorphieklassen der Gruppen d. Ordnung < 8

$\#G$	
1	$\{1\}$
2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/2\mathbb{Z})$ ← A7
5	$\mathbb{Z}/5\mathbb{Z}$
6	~~$\mathbb{Z}/6\mathbb{Z}$~~ $(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/3\mathbb{Z})$, S_3 ← A9 (noch ein Beweis, dass $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$)
7	$\mathbb{Z}/7\mathbb{Z}$

Konjugation

Konjugation mit g:

$k_g: G \longrightarrow G,\ x \longmapsto gxg^{-1} \quad \rightsquigarrow \quad k_g \in \mathrm{Aut}(G)$

x, y konjugiert $:\iff \exists g: \ x = gyg^{-1}$

$\rightsquigarrow$ ÄR, Konjugationsklassen

$k: G \to \mathrm{Aut}(G),\ g \mapsto k_g$

Innere Automorphismen: $\mathrm{Inn}(G) := k(G) \subseteq \mathrm{Aut}(G)$ UG

Zentrum: $Z(G) := \ker(k) = \{g \in G : k_g = \mathrm{id}\}$

$= \{g \in G : \forall x \in G \quad gx = xg\}$

↳ Elemente, die mit <u>allen</u> in G kommutieren!

Bsp: $\mathrm{Inn}(S_3) \cong S_3$.

~~Sogar~~ $\Rightarrow$ $\mathrm{Inn}(S_3) = \mathrm{Aut}(S_3)$, denn:

$\cancel{\Phi \in \mathrm{Aut}(S_3),\ S_3 = \langle (1\ 2), (2\ 3)\rangle}$

$$S_3 = \langle \underbrace{(1\ 2)}_{= \tau}, \underbrace{(1\ 2\ 3)}_{= \pi} \rangle$$

$\Phi \in \mathrm{Aut}(S_3)$

$\Rightarrow \mathrm{ord}(\Phi(\tau)) = 2, \quad \Rightarrow \Phi(\tau) \in \{(1\ 2), (1\ 3), (2\ 3)\}$

$\quad\ \mathrm{ord}(\Phi(\pi)) = 3 \quad \Rightarrow \Phi(\pi) \in \{(1\ 2\ 3), (1\ 3\ 2)\}$

$\Rightarrow 3 \cdot 2 = 6$ Möglichkeiten (höchstens)

$$\left.\begin{aligned} &\Rightarrow \#\mathrm{Aut}(S_3) \le 6 \\ &\#\mathrm{Inn}(S_3) = 6 \\ &\mathrm{Inn}(S_3) \le \mathrm{Aut}(S_3) \end{aligned}\right\} \Rightarrow \mathrm{Inn}(S_3) = \mathrm{Aut}(S_3).$$

$\square$

Normalteiler

$N \trianglelefteq G$: $N \le G$ UGe mit

$\quad gNg^{-1} \subseteq N \qquad (\forall g)$

$\Leftrightarrow gNg^{-1} = N \qquad (\forall g)$

$\Leftrightarrow gN = Ng \qquad (\forall g)$

Bem: $\#gNg^{-1} = ?$ $\rightsquigarrow$ ÜD, A1, Cd)