Vorträge 1 + 2 — Grundlagen

Begriff Gruppe.

Seien G und H Gruppen.

Eine Abbildung $G \xrightarrow{f} H$ heißt *(Gruppen-)Morphismus,* falls $f(xy) = f(x)f(y)$ für $x,\, y \in G$. Dann ist auch $f(1) = 1$.

Ist f zudem bijektiv, so heißt f *Isomorphismus.* Dann ist auch f^{-1} Isomorphismus.

Ein Isomorphismus von G nach G heißt auch *Automorphismus* von G.

Die Automorphismen von G bilden mit der Komposition eine Gruppe, geschrieben $\operatorname{Aut} G$, die *Automorphismengruppe* von G.

Beispiel. Sei $g \in G$. Schreibe ${}^g x := gxg^{-1}$ für die *Konjugation* von x mit g von links. Es ist $G \longrightarrow G$, $x \longmapsto {}^g x$ ein Automorphismus. Automorphismen dieser Form heißen *inner,* Automorphismen nicht von dieser Form *äußer.*

Eine Teilmenge $U \subseteq G$ heißt *Untergruppe,* falls $1 \in U$ und falls für alle $u,\, v \in U$ auch $uv^{-1} \in U$. Schreibe $U \leqslant G$.

Eine Untergruppe $U \leqslant G$ heißt *Normalteiler,* falls für alle $u \in U$ und alle $g \in G$ auch ${}^g u := gug^{-1}$ in U liegt. Schreibe $U \trianglelefteqslant G$.

Bemerkung. Untergruppe mit vererbter Multiplikation wieder Gruppe.

Beispiel. Ist $G \xrightarrow{f} H$ ein Gruppenmorphismus, so ist $f(G) \leqslant H$ und $\operatorname{Kern} f := f^{-1}(1) \trianglelefteqslant G$.

Bemerkung. *Ein Gruppenmorphismus $G \xrightarrow{f} H$ ist injektiv genau dann, wenn* $\operatorname{Kern} f = \{1\}$.

Beispiel. Zykelschreibweise in $\mathcal{S}_n$. Eine Untergruppe in $\mathcal{S}_3$, die Normalteiler ist. Eine, die es nicht ist.

Lemma (Lagrange). *Ist G endlich, so ist $|U|$ Teiler von $|G|$.*

Beweis. Es ist $G = \bigsqcup_{g \in T} gU$ eine disjunkte Vereinigung für eine Teilmenge $T \subseteq G$. Alle *Nebenklassen* gU haben Kardinalität $|U|$. □

Beispiel. Untergruppe $\langle g \rangle := \{g^z \;:\; z \in \mathbf{Z}\}$. *Ordnung* eines Elements ist $|\langle g \rangle|$, ggf. gleich ∞. Ist G endlich, dann ist $|\langle g \rangle|$ Teiler von $|G|$ (Lagrange). Zusammenhang $|\langle g \rangle|$ und $|\langle g^k \rangle|$ für $k \geqslant 1$: $|\langle g^k \rangle| = |\langle g \rangle| / \operatorname{ggT}(|\langle g \rangle|, k)$.

Sei $N \trianglelefteqslant G$. Sei $G/N := \{gN \;:\; g \in G\}$ die *Faktorgruppe G modulo N.* Setze $gN \cdot hN := (gh)N$.

Lemma. *Es ist G/N eine Gruppe, und $G \longrightarrow G/N$ Gruppenmorphismus mit Kern N.*

Beispiel. $\mathcal{S}_3/\langle (1,2,3) \rangle \simeq \mathcal{C}_2$.

Lemma (Homomorphiesatz). *Sei $G \xrightarrow{f} H$ ein Gruppenmorphismus. Dann ist*

$$\begin{array}{rcl} G/\operatorname{Kern} f & \longrightarrow & f(G) \\ g \operatorname{Kern} f & \longmapsto & f(g) \end{array}$$

ein Isomorphismus.

Beweis. Wohldefiniert. Surjektiv und Morphismus nach Konstruktion. Injektiv, da Kern dieses Morphismus gleich $\{1\}$. ▫

Beispiel. Wir haben einen Gruppenmorphismus $G \longrightarrow \operatorname{Aut} G$, $g \longmapsto (x \mapsto {}^g x)$. Sein Kern ist das *Zentrum*

$$\mathrm{Z}(G) \;:=\; \{g \in G \;:\; gx = xg \text{ für alle } x \in G\}\;.$$

Sein Bild, geschrieben $\operatorname{Inn} G$, ist normal in $\operatorname{Aut} G$. Wir haben $\operatorname{Inn} G \simeq G/\mathrm{Z}(G)$. Schreibe noch $\operatorname{Out} G := \operatorname{Aut} G/\operatorname{Inn} G$.

Sei X eine Menge. Sei $G \times X \longrightarrow X$, $(g,x) \longmapsto g \cdot x = gx$ eine Abbildung so, daß $1 \cdot x = x$ für $x \in X$, und so, daß $g(hx) = (gh)x$. Diese Abbildung heißt auch *Operation* von G auf X.

Beispiel. $\mathcal{S}_n$ operiert auf $\{1, \ldots, n\}$. G operiert auf G via $g * x := g \cdot x$ für $g,\, x \in G$ (Operation hier $(*)$ geschrieben). G operiert auf G via $g * x := gxg^{-1} = {}^g x$ für $g,\, x \in G$ (Operation hier $(*)$ geschrieben).

Sei $\mathrm{C}_G(x) := \{g \in G \;:\; gx = x\} \leqslant G$ für $x \in X$ der *Stabilisator* von x in G.

Beispiel. Stabilisator in obigen drei Beispielen.

Lemma (Bahnenlemma). *Sei $x \in X$. Es ist $|Gx| = \dfrac{|G|}{|\mathrm{C}_G(x)|}$.*

Beweis. Die Abbildung $G/\mathrm{C}_G(x) \longrightarrow Gx$, $g\mathrm{C}_G(x) \longmapsto gx$ ist wohldefiniert und bijektiv. ▫

Beispiel. Operation von $\mathcal{S}_n$ auf $\{1, \ldots, n\}$, $x = 1$.