3. Operationen von Gruppen auf Mengen

In diesem Kapitel betrachten wir Operationen von Gruppen G auf Mengen M (auch Gruppenwirkungen genannt), wobei die Menge M auch die Menge der Elemente von G (oder einer anderen Gruppe) sein kann.

__Def.__ Sei G eine Gruppe und M eine Menge. Dann ist die Abbildung

$$G \times M \to M$$
$$(a, x) \mapsto a \circ x$$

eine __Operation von G auf M__ (kurz "Operation") falls gilt:

(i) $\forall x \in M \; (e_G \circ x = x)$

(ii) $\forall a, b \in G \; \forall x \in M \; (\underbrace{(ab)}_{\in G} \circ x = a \circ \underbrace{(b \circ x)}_{\in M})$

__Notation:__ Wir schreiben $G \curvearrowright M$

Transformationsgruppe

G-Menge

Um Operationen von Gruppen auf Gruppen zu untersuchen, brauchen wir den Begriff "Homomorphismus":

__Def.__ Seien $(G, \circ)$ und $(H, \cdot)$ Gruppen und sei $\varphi: G \to H$ eine Abbildung der Menge G in die Menge H. Dann ist φ ein __Homomorphismus__ falls für alle $x, y \in G$ gilt:

homos ≙ ähnlich, gleich
morph ≙ Gestalt
(z.B. amorph)

$$\varphi(\underbrace{x \circ y}_{\in G}) = \underbrace{\varphi(x)}_{\in H} \cdot \underbrace{\varphi(y)}_{\in H}$$

Faktum einfügen →

Faktum: $\varphi: G \to H$ Homom.
- $\varphi(e_G) = e_H$
- $\varphi(x^{-1}) = \varphi(x)^{-1}$

__Def.__ Analog zu S_n für die Gruppe der Bijektionen $\{1, \dots, n\} \to \{1, \dots, n\}$ definieren wir die __Symmetriegruppe der Menge M__ $S(M)$ als die Gruppe der Bijektionen $M \to M$.

Theorem 3.1 (a) $G \times M \to M$ eine Operation
$$(a, x) \mapsto a \circ x$$
so ist
$$\varphi : G \to S(M)$$
$$a \mapsto \varphi_a \quad \text{mit } \varphi_a(x) := a \circ x$$
ein Homomorphismus.

(b) Ist $G \to S(M)$ ein Homomorphismus
$$a \mapsto \varphi_a$$
so ist
$$G \times M \to M$$
$$(a, x) \mapsto a \circ x := \varphi_a(x)$$
eine Operation.

Beweis: (a) $\varphi_a \in S(M)$: φ_a ist bijektiv, denn es ex. eine Umkehrabbildung $\varphi_{a^{-1}}$ für die gilt:
$$\forall x \in M \, (\underbrace{(\varphi_{a^{-1}} \circ \varphi_a)(x)}_{a^{-1} \circ (a \circ x) \underset{G \curvearrowright M}{=} (a^{-1} a)(x) = x} = x \,)$$

φ Homom.: $\varphi(ab)(x) = \varphi_{ab}(x) \underset{\text{Def.}}{=} (ab) \circ x$
$$\underset{G \curvearrowright M}{=} a \circ (b \circ x) \underset{\text{Def.}}{=} \varphi_a(\varphi_b(x))$$
$$= (\varphi_a \circ \varphi_b)(x).$$

(b) $G \curvearrowright M$: (i) $e \circ x \underset{\text{Def.}}{=} \varphi_e(x) \underset{\varphi \text{ Hom.}}{=} \overset{\varphi_e}{\widetilde{\iota}}(x) = x$

(ii) $(ab) \circ x \underset{\text{Def.}}{=} \varphi_{ab}(x) \underset{\varphi \text{ Hom.}}{=} \varphi_a(\varphi_b(x)) \underset{\text{Def.}}{=} a \circ (b \circ x)$

Bem. Jeder Operation $G \curvearrowright M$ entspricht ein Homom. $G \to S(M)$ und umgekehrt.

Bsp. 1) $G \curvearrowright G$

(a) $(a,x) \mapsto ax$ Linkstranslation

(b) $(a,x) \mapsto xa^{-1}$ Rechtstranslation

(c) $(a,x) \to axa^{-1}$ Konjugation

2) M Menge der UG von G
$$G \times M \longrightarrow M$$
$$(a, H) \longmapsto aHa^{-1}$$

Def. Sei $G \curvearrowright M$ eine Operation und $x \in M$.

(i) $Gx := \{a \circ x : a \in G\} \subseteq M$ heisst "Bahn von x" oder "Orbit von x".

(ii) $St_G(x) := \{a \in G : a \circ x = x\}$ heisst "Stabilisatorgruppe von x in G".

(iii) $M/G := \{Gx : x \in M\}$ ist die "Menge der G-Bahnen in M".

Theorem 3.2 (a) $\forall x \in M \; (St_G(x) \leq G)$

(b) $M = \dot{\bigcup}_{N \in M/G} N$ (disj. Vereinigung)

(c) $\forall x \in M \; \forall a \in G \; (St_G(a \circ x) = a\, St_G(x)\, a^{-1})$

(d) $\forall x \in M \; ([G : St_G(x)] = |Gx|)$

Beweis: (a) Seien $a, b \in St_G(x)$, d.h. $a \circ x = x = b \circ x$.

Dann ist $(ab^{-1}) \circ x = (ab^{-1}) \circ \underbrace{(b \circ x)}_{=x \text{ weil } b \in St_G(x)} = a \circ ((bb^{-1}) \circ x)$

$= a \circ (e \circ x) = a \circ x = x$, weil $a \in St_G(x)$

also ist mit $a, b \in St_G(x)$ auch $ab^{-1} \in St_G(x)$.

(b) Seien $Gx, Gx' \in M/G$ und $y \in Gx \cap Gx'$.

a' durch ā ersetzen

Dann ex. $a, \bar{a} \in G$ mit $a \circ x = y = \bar{a} \circ x'$ und somit ist $x = (a^{-1}\bar{a}) \circ x' \in Gx'$ und $x' = (\bar{a}^{-1} a) \circ x \in Gx$, d.h. $Gx = Gx'$. [es gilt immer $x \in Gx$]

(c) Ist $b \in St_G(x)$, dann ist $\overbrace{(aba^{-1}) \circ (a \circ x)}^{=x} = \underbrace{(ab) \circ x}_{=e}$

$= a \circ \underbrace{(b \circ x)}_{=x \text{ weil } b \in St_G(x)} = a \circ x$,

also ist $(aba^{-1}) \in St_G(a \circ x)$, bzw. weil $b \in St_G(x)$ beliebig war, $a\, St_G(x)\, a^{-1} \leq St_G(a \circ x)$.

Ist andererseits $c \in St_G(a \circ x)$, so ist

$$c \circ (a \circ x) = a \circ x$$

$$\Leftrightarrow (a^{-1}c) \circ (a \circ x) = (a^{-1}a) \circ x = x$$

d.h. $(a^{-1}c\,a) \circ x = x$

und somit ist $a^{-1}c\,a \in St_G(x)$, bzw. $c \in a\,St_G(x)a^{-1}$, und weil $c \in St_G(a \circ x)$ beliebig war folgt $St_G(a \circ x) \leq a\,St_G(x)a^{-1}$.

(d) Sei $x \in M$ und $a \circ x, b \circ x \in Gx$.

Dann gilt $a \circ x = b \circ x \Leftrightarrow (b^{-1}a) \circ x = x \Leftrightarrow b^{-1}a \in St_G(x)$

$\underset{\text{Lem. 2.4 (d)}}{\Leftrightarrow} a\,St_G(x) = b\,St_G(x)$

also: $a \circ x \neq b \circ x \Leftrightarrow a\,St_G(x) \neq b\,St_G(x)$

D.h. wir haben gleich viele Elemente in Gx wie wir Nebenklassen von $St_G(x)$ haben und somit gilt

$[G : St_G(x)] = |Gx|$.

$\dashv$

Def. Sei $G \curvearrowright M$ eine Operation. Ist $|Gx| = 1$, d.h. $G = St_G(x)$, so heisst x <u>Fixpunkt</u>.

Bsp. (1) Sei $M = G$ und $G \curvearrowright G$ definiert durch

$$G \times G \to G$$
$$(a, x) \mapsto axa^{-1}$$

Für $x \in G$ sei $[x] := \{axa^{-1} : a \in G\}$ die <u>Konjugationsklasse</u> von x (in G), bzw. der Orbit von x.

Es gilt mit Thm. 3.2: $|[x]| = [G : St_G(x)]$ wobei $St_G(x) = Z_G(x)$.

[beachte: $axa^{-1} = x \Leftrightarrow ax = xa$]

Weiter gilt: $|[x]| = 1 \Leftrightarrow x \in Z(G)$.

[beachte: Ist $St_G(x) = Z_G(x) = G$, so gilt für alle $a \in G$:

$axa^{-1} = x$, d.h. $\forall a \in G\,(ax = xa)$, also $x \in Z(G)$.]

(2) Sei $M = UGr(G)$, d.h. M ist die Menge aller Untergruppen von G. $G \curvearrowright UGr(G)$ sei definiert durch

$$G \times UGr(G) \longrightarrow UGr(G)$$
$$(a, H) \longmapsto aHa^{-1}$$

Für $H \leq G$ sei $[H] := \{aHa^{-1} : a \in G\}$ die <u>Konjugationsklasse</u> von H in G, bzw. der Orbit von H.

Es gilt:
- $H \leq G$ ist Fixpunkt gdw. $H \trianglelefteq G$.
- $St_G(H) = \{a \in G : aHa^{-1} = H\}$ ist der <u>Normalisator</u> von H in G, bezeichnet mit $N(H)$.
- $G = N(H) \iff H \trianglelefteq G$
- $|[H]| = [G : N(H)]$
- $H \trianglelefteq N(G)$

<u>Lemma 3.3</u> Sei G eine Gruppe und seien $A, B \leq G$.
Dann gilt $[A, B] \leq A$ genau dann wenn $B \leq N(A)$.

<u>Beweis:</u> Für $a \in A$ und $b \in B$ gilt:

$$[a, b] = aba^{-1}b^{-1} \in A \iff ba^{-1}b^{-1} \in a^{-1}A = A \iff b \in N(A).$$

Weil a und b beliebig waren gilt $B \leq N(A)$. ⊣

Sei $G \curvearrowright G$ durch Konjugation definiert, d.h. $G \times G \longrightarrow G$
$$(a, x) \longmapsto axa^{-1}$$

<u>Faktum 3.4</u> Seien $[x_1], \dots, [x_n]$ die n verschiedenen Konjugationsklassen mit mehr als einem Element.
Dann ist

$$|G| = \underbrace{|Z(G)|}_{\substack{\text{Vereinigung der} \\ \text{1-elem. Konj.-Klassen}}} + \sum_{i=1}^{n} |[x_i]| = |Z(G)| + \sum_{i=1}^{n} [G : Z_G(x_i)].$$

Beweis: Es gilt $a \in Z(G) \iff |[a]| = 1$. Zudem zerfällt G in paarweise disjunkte Konjugationsklassen.

$\dashv$

Proposition 3.5 Ist G eine Gruppe mit $|G| = p^2$ und p prim, so ist G abelsch.

Beweis: Wir nehmen an, dass G nicht abelsch ist und führen diese Annahme zu einem Widerspruch.

- Ist G nicht abelsch, so ist $Z(G) \neq G$, d.h. $Z(G) < G$ und es gilt: $|Z(G)| \in \{1, p\}$.
- Mit Faktum 3.4 ex. $x_1, \dots, x_n \in G$ mit $|[x_i]| > 1$ und $p^2 = |G| = \underbrace{|Z(G)|}_{1 \text{ oder } p} + \underbrace{\sum_{i=1}^{n} [G : Z_G(x_i)]}_{< p^2}$.

  Weil $\underset{1 < |[x_i]|}{1 <} [G : Z_G(x_i)] < p^2$ muss gelten $|Z_G(x_i)| = p$.
- Somit ist $p^2 = |Z(G)| + n \cdot p$ und damit $|Z(G)| = p = |Z_G(x_i)|$
- Mit $Z(G) \leq Z_G(x_i)$ folgt $Z(G) = Z_G(x_i)$
- Sei $x_0 \in G \setminus Z(G)$. Dann ist $x_0 \in [x_i]$ (für ein i), $|Z_G(x_0)| = |Z_G(x_i)| = p$, und mit $Z(G) \leq Z_G(x_0)$ folgt $Z(G) = Z_G(x_0)$. Das ist aber ein Widerspruch, denn $x_0 \in Z_G(x_0) \setminus Z(G)$.

$\dashv$

Bem. Mit dem Hauptsatz über endl. erzeugte abelsche Gruppen werden wir später sehen, dass es (bis auf Isom.) nur jeweils zwei Gruppen der Ordnung p^2 gibt, nämlich C_{p^2} und $C_p \times C_p$

Def. Sei G eine Gruppe, M eine Menge und $G \curvearrowright M$ eine Operation. Dann sei, für $a \in G$:

$$^{a}M := \{x \in M : a \circ x = x\}$$

also diejenigen Elemente von M, die durch a festgehalten werden.

Als weitere Anwendung von Gruppenoperationen beweisen wir die folgende

Proposition 3.6 ("Burnside's Lemma") [bewiesen von Cauchy & Frobenius] Ist $G \curvearrowright M$ eine Operation, dann gilt:

$$\left| M/G \right| = \frac{1}{|G|} \cdot \sum_{a \in G} \left| {}^{a}M \right|$$

Beweis:
- Es gilt $\sum_{a \in G} |{}^{a}M| = \sum_{a \in G} |\{x \in M : a \circ x = x\}|$

$$= \sum_{x \in M} |\{a \in G : a \circ x = x\}| = \sum_{x \in M} |St_G(x)|.$$

- Weiter gilt: Ist $Y \in M/G$ und $y_0 \in Y$ beliebig, so ist $|Y| = |Gy_0| = |[G : St_G(y_0)]| = \frac{|G|}{|St_G(y_0)|}$

- $\sum_{x \in M} |St_G(x)| = \sum_{Y \in M/G} \sum_{y \in Y} |St_G(y)| = \sum_{Y \in M/G} |Y| \cdot |St_G(y_0)|$ für ein $y_0 \in Y$

$$= \sum_{Y \in M/G} \frac{|G|}{|St_G(y_0)|} \cdot |St_G(y_0)| = \sum_{Y \in M/G} |G| = |M/G| \cdot |G|$$

- Somit ist $\sum_{a \in G} |{}^{a}M| = \sum_{x \in M} |St_G(x)| = |M/G| \cdot |G|$

bzw. $\left| M/G \right| = \frac{1}{|G|} \cdot \sum_{a \in G} |{}^{a}M|$

$\dashv$

Beispiel: Wieviele wesentlich verschiedene Möglichkeiten gibt es, einen Würfel (d.h. die Würfelflächen) mit 3 verschiedenen Farben zu färben?
(wobei mit "wesentlich verschieden" gemeint ist, dass die Färbungen nicht durch Rotation des Würfels ineinander übergeführt werden können)

- Die Menge M ist die Menge aller möglichen Färbungen, also $|M| = 3^6$.
- Die Gruppe G ist die Würfelgruppe, also $|G| = 24$.
- $G \curvearrowright$ ist eine Operation und wir müssen $|M/G|$ bestimmen. Dafür bestimmen wir $|{}^aM|$ für jedes $a \in G$.

#1 • $a = 1$: $|{}^aM| = 3^6$

#6 • "Rotation um $\pm\frac{\pi}{2}$ um eine Achse durch Flächenmittelpunkte"; es gibt 3 solche Rotationen.
$|{}^aM| = 3^3$

#3 • "Rotationen um π um Achsen durch Flächenmittelpunkte"; $|{}^aM| = 3^4$

#8 • "Rotationen um $\pm\frac{2\pi}{3}$ um Achsen durch Würfeldiag."
$|{}^aM| = 3^2$

#6 • "Rotationen um π um Achsen durch Kantenmittelpunkte"; $|{}^aM| = 3^3$

#24

$$|M/G| = \frac{1}{24} \cdot \left(3^6 + 6 \cdot 3^3 + 3 \cdot 3^4 + 8 \cdot 3^2 + 6 \cdot 3^3\right)$$

$$= \underline{\underline{57}}$$