Zusammenhang zwischen Gruppenoperationen und Homomorphismen:

Sei G eine Gruppe, X eine Menge.

- Ist $\cdot : G \times X \to X$ eine Gruppenop., dann ist die Abb. $\tau_g : X \to X$, $x \mapsto g \cdot x$ für jedes $g \in G$ ein Element von $\mathrm{Bij}(X)$, und $\phi : G \to \mathrm{Bij}(X)$, $g \mapsto \tau_g$ ist ein Gruppenhomomorphismus. (Ist $n = |X|$, $n \in \mathbb{N}$, dann erhält man so einen Hom $G \to S_n$.)

- Ist $\phi : G \to \mathrm{Per}(X)$ ein Homomorphismus, dann ist $\circ : G \times X \to X, (g, x) \mapsto \phi(g)(x)$ eine Gruppenoperation.

Anwendungen:

(1) Satz von Cayley

(2) im Zusammenhang mit den Sylowsätze (betrachte die Op. von G auf der Menge X ihrer Sylowgruppen)

Bahngleichung

X endliche Menge, G Gruppe, $\cdot$ Operation von G auf X, $F \subseteq X$ Fixpunktmenge der Operation, $R \subseteq X$ Repr.-system der Bahnen mit mehr als einem Element

Dann gilt $|X| = |F| + \sum_{x \in R} \underbrace{(G : G_x)}_{= |G(x)|}$.

(Beweis beruht auf der Zerlegung von X in die Bahnen der Operation)

wichtiger Spezialfall (kommt zu Stande durch Anwendung der Bahngleichung auf die Operation von G auf sich selbst durch Konjugation)

Klassengleichung G endliche Gruppe, $Z(G)$ = Zentrum von G, $R \subseteq G$ Repräsentantensystem der Konjugationsklassen mit mehr als einem Element. Dann gilt

$$|G| = |Z(G)| + \sum_{g \in R} (G : C_G(g))$$

$C_G(g)$: Zentralisator von g in G

Beispiel: Klassengleichung von S_4

$$|S_4| = |\{id\}| + 6 + 8 + 6 + 3$$

2-Zykel, 3-Zykel, 4-Zykel, Doppeltransp.

Anwendungen:

- Einfachheit von A_5 (und von A_n für $n \geq 6$)
- p-Gruppen haben ein nichttriviales Zentrum

$\Rightarrow$ p-Gruppen sind auflösbar, Gruppen von Primzahlquadratordnung sind abelsch)

- nullter Sylowsatz, Lemma von Cauchy.
  (G endl. Gruppe, p Primzahl, $k \in \mathbb{N}_0$, $p^k \mid |G|$
  $\Rightarrow \exists\, U \leq G$ mit $|U| = p^k$ Ist p Primteiler von $|G|$, dann existiert ein $g \in G$ mit $\mathrm{ord}(g) = p$)

F2ST1A4 Sei G eine endliche Gruppe und p eine Primzahl mit $p \mid |G|$. Es sei $M = \{g \in G \mid \mathrm{ord}(g) = p\}$

(a) Zeigen Sie: Es gibt eine Gruppenoperation
- von $\mathbb{F}_p^\times$ auf M mit der Eigenschaft
  $(a + p\mathbb{Z}) \cdot g = g^a \quad \forall a \in \mathbb{Z}$ mit $p \nmid a$.

Definiere eine Abbildung $\cdot : (\mathbb{Z}/p\mathbb{Z})^\times \times M \to G$ durch $(a+p\mathbb{Z}) \cdot g = g^a$ für alle $a \in \{1, \dots, p-1\}$ und $g \in M$ (Diese Abb. ist wohldefiniert, weil $\{1, \dots, p-1\}$ ein Repräsentantensystem von $\mathbb{Z}/p\mathbb{Z}$ ist.)

Beh.: $(a+p\mathbb{Z}) \cdot g = g^a$ $a \in \mathbb{Z}$, $p \nmid a$, $g \in M$

Sei $a \in \mathbb{Z}$ mit $p \nmid a$ und $g \in M$. $\operatorname{ord}(g) = p \Rightarrow$

$g^p = e$. Division mit Rest $\Rightarrow \exists\, q, r \in \mathbb{Z}$

mit $a = qp + r$, $r \in \{1, \dots, p-1\}$ (wg $p \nmid a$)

$a \equiv r \bmod p \Rightarrow a + p\mathbb{Z} = r + p\mathbb{Z}$

$\Rightarrow (a+p\mathbb{Z}) \cdot g = (r+p\mathbb{Z}) \cdot g = g^r = g^{a-qp}$

$= g^a \cdot (g^p)^{-q} = g^a \cdot e^{-q} = g^a$ ($\Rightarrow$ Beh) (*1)

Seien nun $a, b \in \mathbb{Z}$ mit $p \nmid a, b$, und $g \in M$.

zu überprüfen: (1) $(1+p\mathbb{Z}) \circ g = g$

(2) $(a+p\mathbb{Z}) \circ ((b+p\mathbb{Z}) \circ g) = ((a+p\mathbb{Z}) \cdot (b+p\mathbb{Z})) \circ g$

zu (1) $(1+p\mathbb{Z}) \circ g = g^1 = g$

zu (2) $(a+p\mathbb{Z}) \circ ((b+p\mathbb{Z}) \circ g) =$

$(a+p\mathbb{Z}) \circ g^b = (g^b)^a = g^{ab} =$

$(ab+p\mathbb{Z}) \circ g = ((a+p\mathbb{Z}) \cdot (b+p\mathbb{Z})) \circ g$

Nachtrag (*1):

Wir zeigen nun, dass $\mathbb{F}_p^\times \times M \to G$,

$(a+p\mathbb{Z}, g) \mapsto g^a$ eine Abbildung $\mathbb{F}_p^\times \times M \to M$

$(\mathbb{Z}/p\mathbb{Z})^\times$ M

für alle

(Diese Abb.

$\mathbb{Z}$ ein Re-

ist.)

$p \nmid a$ $g \in M$

$\operatorname{ord}(g) = p \Rightarrow$

$\exists\, q, r \in \mathbb{Z}$

$-1 = q \cdot p + r$ (wg $p \nmid a$)

$a = r + p\mathbb{Z}$

$g^a = g^r = g^{a-qp}$

ist. Sei $a \in \mathbb{Z}$ mit $p \nmid a$, und $g \in M$.

z.z.: $g^a \in M$, d.h. $\operatorname{ord}(g^a) = p$

$g \in M \Rightarrow \operatorname{ord}(g) = p$. Wegen $p \nmid a$ (und p Primzahl) gilt $\operatorname{ggT}(a, p) = 1$. Daraus folgt $\operatorname{ord}(g^a) = \operatorname{ord}(g) = p$.

(b) Sei $g \in M$. Zeigen Sie, dass der Stabilisator $(\mathbb{F}_p^\times)_g$ trivial ist.

Sei $a \in \mathbb{Z}$ mit $p \nmid a$ und $a + p\mathbb{Z} \in (\mathbb{F}_p^\times)_g$

z.z.: $a + p\mathbb{Z} = 1 + p\mathbb{Z}$

$a + p\mathbb{Z} \in (\mathbb{F}_p^\times)_g \Rightarrow (a + p\mathbb{Z}) \cdot g = g$

$\rightarrow g^a = g \Rightarrow g^{a-1} = e \overset{\operatorname{ord}(g) = p}{\Longrightarrow} p \mid (a-1)$

$\rightarrow a \equiv 1 \bmod p \Rightarrow a + p\mathbb{Z} = 1 + p\mathbb{Z}$

(c) Folgern Sie aus Teil (b), dass $p-1$ ein Teiler von $|M|$ ist.

Für jedes $g \in M$ gilt $|\mathbb{F}_p^\times(g)| = (\mathbb{F}_p^\times : (\mathbb{F}_p^\times)_g)$

$= \frac{|\mathbb{F}_p^\times|}{|(\mathbb{F}_p^\times)_g|} \overset{(b)}{=} \frac{|\mathbb{F}_p^\times|}{1} = p-1$. Alle Bahnen der Operation haben also die Länge $p-1$. Ist $p=2$, dann ist $p-1=1$ auf jeden Fall ein Teiler von M. Andernfalls ($p \neq 2$) gibt es keine Bahnen der Länge 1, d.h. die Fixpunktmenge ist $F = \emptyset$. Sei R ein Repräsentantensystem der Bahnen mit mehr als einem Element.

Bahngleichung $\Rightarrow |M| = |F| +$

$$\sum_{g \in R} (\mathbb{F}_p^\times : (\mathbb{F}_p^\times)_g) = 0 + \sum_{g \in R} (p-1) =$$

$|R| \cdot (p-1) \Rightarrow (p-1)$ teilt $|M|$ $\square$

Übung: H13T3A4

H25T3A2 Sei G eine Gruppe, Ω eine Menge und $\circ$ eine Operation von G auf Ω. Der Kern von $\circ$ ist gegeben durch $K = \{g \in G \mid g \circ \omega = \omega \ \forall \omega \in \Omega\}$. Man bezeichnet die Operation als treu, wenn $K = \{e\}$ ist.

(a) Zeigen Sie: Ist G abelsch und operiert G treu und transitiv auf Ω, dann gilt $G_\omega = K \ \forall \omega \in \Omega$, d.h. der Kern der Operation stimmt mit jedem Stabilisator überein.

Sei $\omega \in \Omega$, z.Zg.: $G_\omega = K$

„$\supseteq$" Sei $g \in K \Rightarrow g \circ \omega' = \omega' \ \forall \omega' \in \Omega \Rightarrow$

insb. $g \circ \omega = \omega \Rightarrow g \in G_\omega$

„$\subseteq$" Sei $g \in G_\omega$. z.Zg.: $g \in K$

Sei $\omega' \in \Omega$. z.Zg.: $g \circ \omega' = \omega'$ Da die Operation transitiv ist, liegen ω und ω' in derselben

Bahn $\rightsquigarrow w' \in G(w) \Rightarrow \exists h \in G : w' = h \cdot w$

$\Rightarrow g \cdot w' = g \cdot (h \cdot w) = (gh) \cdot w = (hg) \cdot w$

$= h \cdot (g \cdot w) = h \cdot w = w'$

$\uparrow g \in G_w$

(b) Zeigen Sie, dass unter den Voraussetzungen von Teil (a) die Gleichung $|G| = |\Omega|$ gilt.

Sei $w \in \Omega$ beliebig gewählt. Betrachte die Abbildung $\varphi : G \to \Omega, g \mapsto g \cdot w$. Wenn φ bijektiv ist, folgt daraus $|G| = \Omega$. zzg. also:

(1) φ ist surjektiv (2) φ ist injektiv

zu (1) Sei $\omega' \in \Omega$, z.zg. $\exists g \in G$ mit $\varphi(g) = \omega'$, gleichbed.: $\exists g \in G$ mit $g \circ \omega = \omega'$. Da $\circ$ transitiv ist, gilt $G(\omega) = \Omega$ und $\omega' \in G(\omega)$. Also existiert tatsächlich ein $g \in G$ mit $g \circ \omega = \omega'$.

zu (2) Seien $g, h \in G$ mit $\varphi(g) = \varphi(h)$

z.zg. $g = h$ Vor. $\Rightarrow g \circ \omega = h \circ \omega$

$\Rightarrow (h^{-1} g) \circ \omega = h^{-1} \circ (g \circ \omega) = h^{-1} \circ (h \circ \omega)$

$= (h^{-1} h) \circ \omega = e \circ \omega = \omega \Rightarrow h^{-1} g \in G\omega$

$\overset{(a)}{\Rightarrow} h^{-1} g \in K \overset{\text{Op. ist treu}}{\underset{K = \{e\}}{\Rightarrow}} h^{-1} g = e \Rightarrow g = h$

(c) Geben Sie je ein Beispiel für eine nicht-abelsche Gruppe G und eine Menge Ω an, sowie eine treue und transitive Operation, so dass

(i) $|G| = |\Omega|$ (ii) $|G| \neq |\Omega|$

zu (i) Wähle $G = S_3$, $\Omega = S_3$. Betrachte die Operation von G auf Ω durch Linkstranslation.

zu (ii) Wähle $G = S_3$, $\Omega = M_3 = \{1, 2, 3\}$. Betrachte die Op. $G \times \Omega \to \Omega$, $(\sigma, k) \mapsto \sigma(k)$

Nachweise: siehe nächste Seite.

zu (i) Die Gruppe S_3 ist nicht-abelsch, da zum Beispiel $(1\ \ 2) \circ (1\ \ 3) \neq (1\ \ 3) \circ (1\ \ 2)$ gilt. Die Operation jeder Gruppe G auf sich selbst durch Linkstranslation ist immer transitiv. (Denn für jedes $g \in G$ gilt $g \cdot e_G = ge_G = g$, also $g \in G(e)$, und somit $G(e) = G$.) Eine solche Operation ist auch immer treu. Ist nämlich $g \in G$ im Kern K der Operation enthalten, dann folgt $g = ge_G = g \cdot e_G = e_G$, als $K = \{e_G\}$.

zu (ii) Auch hier ist die Operation transitiv, denn die Gleichungen $\mathrm{id} \cdot 1 = 1$, $(1\ \ 2) \cdot 1 = 2$ und $(1\ \ 3) \cdot 1 = 3$ zeigen, dass die Bahn $S_3(1)$ mit $M_3 = \{1, 2, 3\}$ übereinstimmt. Zum Nachweis, dass die Operation auch treu ist, sei σ ein Element des Kerns K der Operation. Dann gilt für alle $k \in M_3$ jeweils $\sigma(k) = \sigma \cdot k = k$, woraus $\sigma = \mathrm{id}$ folgt. Anderseits ist $|G| = |S_3| = 6$ und $|\Omega| = |M_3| = 3$, also $|G| \neq |\Omega|$.