Definition (7.1)

Sei G eine Gruppe und X eine Menge. Eine Gruppenoperation von G auf X ist eine Abbildung $\alpha : G \times X \longrightarrow X$ mit den Eigenschaften

$$\alpha(e_G, x) = x \qquad \text{und} \qquad \alpha(g, \alpha(h, x)) = \alpha(gh, x)$$

für alle $g, h \in G$ und $x \in X$, wobei e_G das Neutralelement der Gruppe bezeichnet.

An Stelle von $\alpha(g, x)$ verwendet man häufig auch die Infix-Schreibweise $g \cdot x$, wobei dann $\cdot$ das Symbol für die Gruppenoperation ist.

Zerlegung einer Menge in Bahnen

Proposition (7.3)

Sei G eine Gruppe, X eine Menge und $G \times X \to X$, $(g, x) \mapsto g \cdot x$ eine Gruppenoperation. Dann gilt

(i) Die Menge $\mathcal{B} = \{G(x) \mid x \in X\}$ der Bahnen ist eine Zerlegung von X.

(ii) Eine Teilmenge $Y \subseteq X$ ist genau dann G-invariant, wenn Y eine Vereinigung von Bahnen der Operation ist.

Der Stabilisator eines Elements

Satz (7.4)

Sei G eine Gruppe, die auf einer Menge X operiert, und $x \in X$. Dann ist die Teilmenge $G_x = \{g \in G \mid g \cdot x = x\}$ eine Untergruppe von G. Man nennt sie den Stabilisator von x.

Bahnlänge und Ordnung des Stabilsators

Satz (7.6)

Sei G eine Gruppe, die auf einer Menge X operiert, und sei $x \in X$. Dann gibt es eine Bijektion

$$\phi_x : G/G_x \to G(x)$$

mit $\phi_x(gG_x) = g \cdot x$ für alle $g \in G$. Ist insbesondere X endlich, dann ist auch der Index $(G : G_x)$ endlich, und es gilt $(G : G_x) = |G(x)|$.

Repräsentantensysteme der Bahnen

Definition (7.10)

Sei G eine Gruppe, die auf einer Menge X operiert, $\mathcal{B}$ die Menge der Bahnen dieser Operation und $\mathcal{S} \subseteq \mathcal{B}$ eine Teilmenge. Eine Teilmenge $R \subseteq X$ wird Repräsentantensystem von $\mathcal{S}$ genannt, wenn $G(x) \in \mathcal{S}$ für alle $x \in R$ gilt und die Abbildung $R \to \mathcal{S}$, $x \mapsto G(x)$ bijektiv ist.

Die Bahngleichung

Satz (7.11)

Sei G eine Gruppe, die auf einer endlichen Menge X operiert. Sei $F \subseteq X$ die Fixmpunktmenge der Operation und $R \subseteq X$ ein Repräsentantensystem der Menge aller Bahnen $G(x)$ mit mindestens zwei Elementen. Dann gilt

$$|X| = |F| + \sum_{x \in R} (G : G_x)$$

und $(G : G_x) > 1$ für alle $x \in R$.

Beweis der Bahngleichung

G eine Gruppe, X eine endliche Menge, auf der G operiert, $F \subseteq X$ Fixpunktmenge

$\mathcal{B} = \{G(x) \mid x \in X\}$ Menge der Bahnen

$\mathcal{S}$ = Menge der Bahnen B mit $|B| > 1$

Es gilt $|X| = \sum_{B \in \mathcal{B}} |B| = |F| + \sum_{B \in \mathcal{S}} |B| =$

Bahnen bilden Zerlegung von X

Für jedes $x \in F$ ist $\{x\}$ eine Bahn.

R ist Repräsentantensystem

$|F| + \sum_{x \in R} |G(x)| = |F| + \sum_{x \in R} (G : G_x)$.

$\square$

Anwendung: Disjunkte Zykelzerlegung der Permutationen

Satz (7.12)

Sei $n \in \mathbb{N}$. Dann besitzt jedes $\sigma \in S_n$ eine Darstellung $\sigma = \tau_1 \circ ... \circ \tau_r$ als Produkt paarweise disjunkter Zykel τ_j, und diese Darstellung ist bis auf die Reihenfolge der Faktoren eindeutig bestimmt.

Beweis von Satz 7.12 (Skizze)

geg: $\sigma \in S_n$, zzg: Existenz und Eindeutigkeit einer Produktzerlegung in disjunkte Zykel

Existenz: Setze $G = \langle \sigma \rangle$. Seien $B_1, \dots, B_r$ die Bahnen der Operation von G auf $M_n = \{1, 2, \dots, n\}$ mit mehr als einem Element. Definiere $\tau_j(k) = \begin{cases} \sigma(k) & \text{falls } k \in B_j \\ k & \text{sonst} \end{cases}$ für $1 \leq k \leq r$. ($\Rightarrow \tau_j|_{B_j} = \sigma|_{B_j}$) Überprüfe: τ_j ist jeweils ein k_j-Zykel, wobei $k_j = |B_j|$, und es gilt $\sigma = \tau_1 \circ \dots \circ \tau_r$.

Eindeutigkeit: Ist $\sigma = \sigma_1 \circ \dots \circ \sigma_s$ eine beliebige disjunkte Zykelzerlegung, dann entspricht jeder Faktor σ_i einer Bahn der Operation von $G = \langle \sigma \rangle$. Leite daraus ab, dass die σ_i bis auf Reihenfolge mit den τ_j übereinstimmen. $\square$

Merkmale der Operation durch Konjugation

Proposition (7.13)

Der Stabilisator eines Elements $h \in G$ unter der Operation durch Konjugation ist gegeben durch $C_G(h) = \{g \in G \mid gh = hg\}$. Die Fixpunkte der Operation sind die Elemente der Menge

$$Z(G) \quad = \quad \{g \in G \mid gh = hg \ \forall\ h \in G\} \quad ,$$

dem sogenannten Zentrum. Auch $Z(G)$ ist eine Untergruppe, darüber hinaus sogar ein Normalteiler von G.

Erinnerung: Operation einer Gruppe G auf sich selbst durch Konjugation

$$\boxed{g \cdot h = g h g^{-1} \quad \forall g, h \in G}$$

Fixpunktmenge = Zentrum $Z(G)$

Stabilisator von $h \in G$ = Zentralisator $C_G(h) = \{g \in G \mid gh = hg\}$

Die Bahn eines Elements h ist die sog. Konjugationsklasse $\{ghg^{-1} \mid g \in G\}$.

h, h' konjugiert in $G \Leftrightarrow \exists g \in G : h' = g h g^{-1}$

(ii)

(2-

(3-

(4-1

Die Klassengleichung

Satz (7.14)

Sei G eine endliche Gruppe, die durch Konjugation auf sich selbst operiert. Sei R ein Repräsentantensystem der Konjugationsklassen mit mehr als einem Element. Dann gilt

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

Diese Gleichung erhält man durch Anwendung der Bahngleichung auf die Operation durch Konjugation der Gruppe G auf der Menge ihrer Elemente.

Beispiele für die Klassengleichung: S_n

Proposition (7.15)

Sei $n \in \mathbb{N}$, und seien $\sigma, \sigma' \in S_n$ zwei nicht-triviale Elemente. Genau dann sind σ, σ' zueinander konjugiert, wenn sie denselben Zerlegungstyp besitzen.

Daraus folgt, dass die Konjugationsklassen in S_n genau den Zerlegungstypen der Elemente entsprechen.

Beispiel für Prop. 7.15:

Für jedes $\sigma \in S_5$ gilt

$$\sigma \circ (1\,2\,3)(4\,5) \circ \sigma^{-1} = (\sigma(1)\,\sigma(2)\,\sigma(3))(\sigma(4)\,\sigma(5))$$

(denn: Sei $k \in M_n$. σ bijektiv $\Rightarrow \exists\, l \in M_n$ mit $\sigma(l) = k$. Überprüfe für $l = 1, 2, \dots, 5$, dass die linke und rechte Seite $l = \sigma(k)$ gleich abbilden.)

Bestimmung der Klassengleichung für S_n

Lemma (7.16)

Sei $n \in \mathbb{N}$ und $2 \leq k \leq n$. Ist $A \subseteq M_n$ eine k-elementige Teilmenge, so beträgt die Anzahl der k-Zykel σ mit $\mathrm{supp}\sigma = A$ genau $(k-1)!$.

Folgerung (7.17)

Für $n \in \mathbb{N}$ und $k \in \{2, ..., n\}$ gibt es jeweils genau $(k-1)!\binom{n}{k}$ Zykel der Länge k.

Beispiele für die Klassengleichung

(i) $G = S_3$

$$\underset{|S_3|}{\overset{\|}{6}} = \underset{\text{Zentrum } \{id\}}{1} + \underset{\text{2-Zykel}}{3} + \underset{\text{3-Zykel}}{2}$$

(ii) $G = S_4$

$$\underset{|S_4|}{\overset{\|}{24}} = \underset{Z(S_4)}{1} + \underset{\text{2-Zykel}}{6} + \underset{\text{3-Zykel}}{8} + \underset{\text{4-Zykel}}{6} + \underset{\text{Doppeltranspositionen}}{3}$$

$$(2-1)!\binom{4}{2} = 1 \cdot 6 = 6$$

$$(3-1)!\binom{4}{3} = 2 \cdot 4 = 8$$

$$(4-1)!\binom{4}{4} = 6 \cdot 1 = 6$$

Weitere Ergänzungen

- Man kann auch Formeln für die Anzahl der Elemente eines beliebigen Zerlegungstyps angeben (siehe Skript).
- Im Skript wird auch ausgeführt, wie man die Klassengleichungen der alternierenden Gruppen A_n bestimmt.
- Desweiteren kann aus der Klassengleichung die Einfachheit der alternierenden Gruppen für $n \geq 5$ abgeleitet werden.

Beweis der Einfachheit von A_n für $n \geq 5$
(nur Skizze)

Klassengleichung für A_5:

$$\underset{|A_5|}{\underset{\|}{60}} = \underset{Z(A_5)}{1} + \underset{3\text{-Zykel}}{20} + \underbrace{12 + 12}_{5\text{-Zykel}} + \underset{\text{Doppeltransp.}}{15}$$

wichtige Beobachtung: Ist $N \trianglelefteq A_5$, dann gilt auf Grund der Eigenschaft $\sigma \circ N \circ \sigma^{-1} = N \ \forall \sigma \in A_5$, dass jede Konjugationsklasse von A_5 <u>entweder</u> in N liegt, oder zu N disjunkt ist. Mit anderen Worten,

A_5 ist Vereinigung von Konjugationsklassen der A_5

Eine Klasse, die auf jeden Fall in N liegt ist $\{id\}$.

<u>aber</u>: Es ist nicht möglich, einen echten Teiler von 60 als Summe von 1 und den Zahlen 12, 12, 15, 20 darzustellen.

Also existiert kein $N \trianglelefteq A_5$ mit $N \neq \{id\}, A_5$ (denn $|N|$ wäre ein echter Teiler von $|A_5| = 60$).

Die allgemeine Aussage erhält man durch vollständige Induktion über $n \geq 5$. <u>Ansatz</u>: Betrachte in S_{n+1} die Stabilisatorgruppen $G_i = (S_{n+1})_i$ für $1 \leq i \leq n+1$, und darin die Untergruppen $H_i = G_i \cap A_{n+1}$ ($H_i \cong A_n$)

Betrachte den Durchschnitt eines hypothetischen Normalteilers $N \trianglelefteq A_{n+1}$ mit H_i, also $H_i \cap N$. (siehe Skript) $\square$

Das nichttriviale Zentrum der p-Gruppen

Definition (7.20)

Sei p eine Primzahl. Eine endliche Gruppe G wird als p-Gruppe bezeichnet, wenn sie von p-Potenzordnung ist, also $|G| = p^e$ für ein $e \in \mathbb{N}_0$ erfüllt ist.

Satz (7.21)

Sei G eine nichttriviale p-Gruppe. Dann ist das Zentrum $Z(G)$ von G ebenfalls nichttrivial, besteht also aus mindestens p Elementen.

Beweis von Satz 7.21:

<u>geg.</u>: p Primzahl, G eine p-Gruppe mit $|G| = p^e$, wobei $G \neq \{e_G\}$ $(e \in \mathbb{N})$.

z.zg.: $Z(G) \neq \{e_G\}$

Sei $R \subseteq G$ ein Repräsentantensystem der Konjugationsklassen mit mehr als einem Element. Klassengleichung $\rightarrow$

$$p^e \overset{(*)}{=} |Z(G)| + \sum_{h \in R} (G : C_G(h))$$

Für jedes $h \in R$ ist $(G : C_G(h))$ ein Teiler von $|G| = p^e$ größer als 1. $\Rightarrow p \mid (G : C_G(h))$ für alle $h \in R$ (*) $\Rightarrow p^e \equiv |Z(G)| \bmod p$

$\overset{e \geq 1}{\Rightarrow} |Z(G)| \equiv 0 \bmod p \Rightarrow p \mid |Z(G)|$

Daraus folgt, dass $Z(G)$ nicht nur das Neutralelement enthält (denn dann wäre $|Z(G)| = 1$ $\lightning$ da $p \nmid 1$.) $\square$

G
da
Seie
$a Z($
ebens
Sei g
$a Z(G$

Gruppen von Primzahlquadratordnung

Lemma (7.22)

Ist G eine Gruppe mit der Eigenschaft, dass die Faktorgruppe $G/Z(G)$ zyklisch ist, dann ist G selbst abelsch.

Satz (7.23)

Sei p eine Primzahl. Dann ist jede Gruppe der Ordnung p^2 abelsch. Bis auf Isomorphie sind also $\mathbb{Z}/p^2\mathbb{Z}$ und $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ die einzigen Gruppen der Ordnung p^2.

Beweis von Lemma 7.22:

P gegeben: G Gruppe mit der Eigenschaft, dass dass die Faktorgruppe $G/Z(G)$ zyklisch ist. z.zg.: G ist abelsch

$G/Z(G)$ zyklisch $\Rightarrow \exists \bar{g} \in G/Z(G)$, so dass $G/Z(G) = \langle \bar{g} \rangle$.

Seien $a, b \in G$. z.zg. $ab = ba$

$aZ(G) \in G/Z(G) \Rightarrow \exists k \in \mathbb{Z}: aZ(G) = \bar{g}^k$

ebenso: $\exists l \in \mathbb{Z}: bZ(G) = \bar{g}^l$

Sei $g \in G$ ein Element mit $gZ(G) = \bar{g}$.

$aZ(G) = g^k Z(G) \Rightarrow a \in g^k Z(G)$

$\Rightarrow \exists\, c \in Z(G)$ mit $a = g^k c$

genauso: $\exists\, d \in Z(G)$ mit $b = g^l d$.

$$\Rightarrow a \cdot b = g^k c\, g^l d \underset{\uparrow c \in Z(G)}{=} g^k g^l c\, d \underset{\uparrow d \in Z(G)}{=} g^{k+l} d c =$$

$$= g^l g^k d\, c = g^l d\, g^k c = b\, a. \qquad \square$$

$aZ(G) = gZ(G) \Rightarrow a \in g^k Z(G)$

Beweis von Satz 7.23:

geg.: p Primzahl, G Gruppe mit $|G| = p^2$

z. zg: G ist abelsch

Satz 7.21 $\Rightarrow Z(G) \neq \{e\} \underset{Z(G) \leq G}{\overset{\text{Lagrange}}{\Longrightarrow}} |Z(G)| \in \{p, p^2\}$

1. Fall: $|Z(G)| = p^2 \Rightarrow Z(G) = G$ Aus der Definition des Zentrums folgt dann, dass G abelsch ist.

2. Fall: $|Z(G)| = p$ Es gilt $|G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p$. Als Gruppe von Primzahlordnung ist $G/Z(G)$ zyklisch. Lemma 7.22 $\Rightarrow$ Die Gruppe G ist abelsch. $\square$