Die Struktur endlicher abelscher Gruppen

Satz (*Hauptsatz über endliche abelsche Gruppen*)

Jede endliche abelsche Gruppe G ist isomorph zu einem direkten Produkt zyklischer Gruppen. Es gibt also ein $r \in \mathbb{N}_0$ und $m_1, ..., m_r \in \mathbb{N}$ mit

$$G \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times ... \times \mathbb{Z}/m_r\mathbb{Z}.$$

Dabei können die Zahlen m_j so gewählt werden, dass

- es sich um Primzahlpotenzen handelt oder
- für $1 \leq j \leq r-1$ jeweils $m_j \mid m_{j+1}$ gilt.

Ergänzung:

Auch jede endlich erzeugte abelsche Gruppe ist Produkt zyklischer Gruppen, also isomorph zu einer Gruppe der Form

$$\mathbb{Z}^s \times \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_r\mathbb{Z}.$$

Elementordnungen in den symmetrischen Gruppen

Satz

Sei $n \in \mathbb{N}$ und $\sigma \in S_n$.

(i) Ist σ ein k-Zykel ($2 \leq k \leq n$), dann gilt $\mathrm{ord}(\sigma) = k$.

(ii) Die Anzahl der k-Zykel in S_n ist gegeben durch

$$(k-1)!\binom{n}{k}.$$

(iii) Ist σ ein Element vom Zerlegungtyp $(k_1, ..., k_r)$, dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(k_1, ..., k_r)$.

Ergänzung:

Zwei Elemente $\rho, \sigma \in S_n$ haben genau dann denselben Zerlegungstyp, wenn sie konjugiert zueinander sind, d.h. wenn ein $\tau \in S_n$ mit $\sigma = \tau \circ \rho \circ \tau^{-1}$ existiert.

Beispiel: Elemente von S_5, sortiert nach Zerlegungstypen $\square$ = Zerlegungstypen in A_5

Zerlegungstyp	$\square$ (1)	(2)	$\square$ (3)	(4)	$\square$ (5)	$\square$ (2,2)	(3,2)
Beispielelement	id	(12)	(145)	(1352)	(13524)	(13)(45)	(124)(35)
Anzahl	1	10	20	30	24	15	20
Elementordnung	1	2	3	4	5	2	6

Anzahl 3-Zykel: $2! \cdot \binom{5}{3} = 2 \cdot 10 = 20$

Anzahl der Elemente von Zerlegungstyp (3,2):

Möglichkeiten für den 3-Zykel: 20
Nach Wahl des 3-Zykels liegt die Transposition fest.
$\Rightarrow$ 20 Elemente vom Typ (3,2)

Anzahl der Elemente vom Typ (2,2):
Möglichkeiten für die 1. Transp.: 10
verbleibende Anzahl Mögl. für die 2. Transp.: $\binom{3}{2} \cdot (2-1)! = 3$
Da die Reihenfolge der Transpositionen keine Rolle spielt,
muss noch $\frac{1}{2!} = \frac{1}{2}$ multipliziert werden. $\Rightarrow \frac{1}{2} \cdot 10 \cdot 3 = 15$
Elemente vom Typ (2,2)
(Aus demselben Grund ist die Anzahl der Elemente vom Typ (2,2,2)
in S_6 gleich $\frac{1}{3!} \cdot \binom{6}{4} \cdot \binom{4}{2}$.)

H26T3A1 (a) Geben Sie alle abelschen Gruppen der Ordnung 40 bis auf Isomorphie an (und jeden Isomorphietyp nur einmal).

1. Möglichkeit: Darstellungen von 40 als Produkt von Primzahlpotenzen > 1

$40 = 2^3 \cdot 5 = 2^2 \cdot 2 \cdot 5 = 2 \cdot 2 \cdot 2 \cdot 5$

$\Rightarrow$ Es gibt drei Isomorphietypen, repräsentiert durch $G_1 = \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, $G_2 = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ und $(\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/5\mathbb{Z}$

2. Möglichkeit: Zur Zahl 40 gibt es die Elementarteilerketten (40), $(2, 20)$, $(2, 2, 10)$ $\Rightarrow$ Es gibt drei Isomorphietypen, repräsentiert durch $H_1 = \mathbb{Z}/40\mathbb{Z}$, $H_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$ und $H_3 = (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/10\mathbb{Z}$. □

H2 6 T3 A3 (R)

Gibt es in A_5 eine Untergruppe der Ordnung 15?

Laut Vl. ist jede Untergr. der Ordnung 15 zyklisch und enthält somit ein Element der Ordnung 15. Gäbe es in A_5 eine Untergruppe der Ordnung 15, dann müsste es auch ein Element $\sigma \in A_5$ mit $\operatorname{ord}(\sigma) = 15$ geben. Sei $(k_1, \dots, k_r)$ der Zerlegungstyp von σ (mit $r \in \mathbb{N}$, $k_1 \geq \dots \geq k_r \geq 2$)

$\Rightarrow \operatorname{kgV}(k_1, \dots, k_r) = \operatorname{ord}(\sigma) = 15$

$\Rightarrow \exists j : 15 \mid k_j$ oder $\exists i,j$ mit $i \neq j$, $3 \mid k_i$ und $5 \mid k_j$. In beiden Fällen wäre $\sum_{i=1}^{r} k_i \geq 8$, im Widerspruch zu $\sum_{i=1}^{r} k_i \leq 5$ wegen $\sigma \in S_5$. Es gibt also keine Untergr. der Ordnung 15 in S_5. □

H21T3A1

(a) Sei U eine Untergruppe von S_5 mit $|U| \in \{3, 5, 7\}$. Zeigen Sie: Dann ist U eine Untergruppe von A_5.

1. Fall: $|U| = 3$ Dann gibt es in U nur Elemente der Ordnung 1 und 3 (nach dem Satz v. Lagrange da 3 eine Primzahl ist.) Sei $\sigma \in U$, z.zg.: $\sigma \in A_5$

$\left(\frac{n-1}{2}\right)$

$(n-4)$

$\frac{a(n)}{n} = +\infty$

□

Ist $\text{ord}(\sigma) = 1$, dann folgt $\sigma = id \in A_5$.

Ist $\text{ord}(\sigma) = 3$, dann muss σ ein 3-Zykel sein, denn die einzigen Zerlegungstypen in S_5 sind $()$, (2), (3), (4), (5), $(2,2)$, $(3,2)$, und die Elemente vom Typ (3) sind die einzigen mit Ordnung 3. 3-Zykel haben Signum $1 \Rightarrow \sigma \in A_5$ auch in diesem Fall

2. Fall: $|U| = 5$ Übung

(6) Zeigen Sie, dass es in S_5 genau 10 Untergruppen der Ordnung 3 gibt.

Allgemein gilt: Ist G eine endliche Gruppe und $n \in \mathbb{N}$, dann ist die Anzahl der zyklischen Untergruppen der Ordnung n multipliziert mit $\varphi(n)$

das Ord-

ung 15

Element

As eine

dann müsste

mit ord(σ)

der Zerlegungs-

= 2)

= 15

gleich der Anzahl der Elemente der Ordnung n.
Da 3 eine Primzahl ist, ist jede Untergr. der Ordnung 3 zyklisch, und $\varphi(3) = 2$.
$\Rightarrow$ Die ges. Anzahl der Untergr. ist halb so groß wie die Anzahl der Elemente der Ordnung 3, also halb so groß wie die Anzahl der 3-Zykel (3.0). Ist $n \in \mathbb{N}$ und $k \in \{2, \dots, n\}$, dann gibt es in S_n genau $(k-1)!\binom{n}{k}$ k-Zykel in S_n, also $(3-1)!\binom{5}{3} = 20$ 3-Zykel in S_3. Die ges. Anzahl der Untergruppen ist also gleich $\frac{1}{2} \cdot 20 = 10$.

(c) Übung

H13T3A3 Sei $n \in \mathbb{N}$ und $\sigma \in S_n$.

(a) Sei σ das Produkt zweier disjunkter Zykel der Längen k und l, wobei k und l teilerfremd sind. Bestimmen Sie die Ordnung von σ. [kurze Lösung durch Verwendung der allgemeinen Regel für Elementordnungen: O.B.d.A. sei $k \geq l$. Dann ist (k, l) der Zerlegungstyp von σ, und somit $\operatorname{ord}(\sigma) = \operatorname{kgV}(k, l) = kl$, auf Grund der Teilerfremdheit und der allgemeinen Regel für Elementordn. in S_n]

Sei ρ der k-Zyklus und τ der dazu disjunkte l-Zyklus, so dass $\sigma = \rho \circ \tau$.

Beh.: $\operatorname{ord}(\sigma) = kl$

ρ k-Zyklus $\Rightarrow \rho^k = id$ $\quad \tau$ l-Zyklus $\Rightarrow \tau^l = id$

Als disjunkte Zyklen sind ρ und τ vertauschbar.

$\Rightarrow (\rho \circ \tau)^m = \rho^m \circ \tau^m \quad \forall\, m \in \mathbb{N}$. insg. sind:

$\sigma^{kl} = (\rho \circ \tau)^{kl} = \rho^{kl} \circ \tau^{kl} = (\rho^k)^l \circ (\tau^l)^k =$

$id^l \circ id^k = id \Rightarrow \operatorname{ord}(\sigma) \mid kl$

noch z.zg.: $\forall m \in \mathbb{Z}: \sigma^m = id \Rightarrow kl \mid m$

Sei $m \in \mathbb{Z}$ mit $\sigma^m = id$. $\Rightarrow \rho^m \circ \tau^m = id$

$\Rightarrow \rho^m \overset{(*)}{=} \tau^{-m}$ $\quad$ ρ k-Zykel $\Rightarrow ord(\rho) = |\langle\rho\rangle| = k$

τ l-Zykel $\Rightarrow ord(\tau) = |\langle\tau\rangle| = l$

$|\langle\rho\rangle|, |\langle\tau\rangle|$ teilerfremd $\Rightarrow \langle\rho\rangle \cap \langle\tau\rangle = \{id\}$

$(*) \Rightarrow \rho^m, \tau^{-m} \in \langle\rho\rangle \cap \langle\tau\rangle \Rightarrow \rho^m = \tau^{-m} = id$

$\rho^m = id$, $k = ord(\rho) \Rightarrow k \mid m$

$\tau^{-m} = id$, $l = ord(\tau) \Rightarrow l \mid (-m) \Rightarrow l \mid m$

$k \mid m$, $l \mid m$, k, l teilerfremd $\Rightarrow kl \mid m$

Insgesamt ist damit $ord(\sigma) = kl$ nachgewiesen.

(b) Für jedes $n \in \mathbb{N}$ sei $a(n)$ die größte in S_n vorkommende Elementordnung. [$a(2) = 2$, $a(3) = 3$, $a(4) = 4$, $a(5) = 6$, $a(6) = 6$, $a(7) = 12$, ...]

Zeigen Sie: $\lim_{n \to \infty} \frac{a(n)}{n} = +\infty$

Sei $n \in \mathbb{N}$ und $k = \lfloor \frac{n-1}{2} \rfloor$, $l = k + 1$.

$\Rightarrow k + l \leq \frac{n-1}{2} + \frac{n-1}{2} + 1 = (n-1) + 1 = n$

Es gibt also in S_n ein Produkt aus einem k-Zykel und einem dazu disjunkten l-Zykel. Außerdem gilt $ggT(k, l) = 1$, denn: Sei $d \in \mathbb{N}$ mit $d \mid k$, $d \mid l$.

$\Rightarrow d \mid (\ell - k) \Rightarrow d \mid n \Rightarrow d = 1.$

Teil (a) $\Rightarrow \operatorname{ord}(\sigma) = k\ell$

$\Rightarrow a(n) \geq \operatorname{ord}(\sigma) = k\ell \geq \left(\frac{n-1}{2} - 1\right)\left(\frac{n-1}{2}\right)$

$= \frac{1}{4}(n-3)(n-1) = \frac{1}{4}(n^2 - 4n + 3)$

$\Rightarrow \frac{a(n)}{n} \overset{(*)}{\geq} \frac{1}{4}\left(n - 4 + \frac{3}{n}\right) \geq \frac{1}{4}(n-4)$

$\lim_{n\to\infty} \frac{1}{4}(n-4) = +\infty \overset{(*1)}{\Rightarrow} \lim_{n\to\infty} \frac{a(n)}{n} = +\infty$

□