Weitere Beispiele für Gruppenoperationen

(i) Jede Gruppe G operiert auf sich selbst durch Linkstranslation, d.h. durch die Abbildung $\bullet : G \times G \to G$, $g \bullet h = gh$

Diese Operation ist transitiv: Es gilt

$$G(e) = \{g \bullet e \mid g \in G\} = \{ge \mid g \in G\}$$
$$= \{g \mid g \in G\} = G.$$

Anwendung: Satz von Cayley (Ist $n \in \mathbb{N}$ und G eine Gruppe der Ordnung n, dann

Anwen
gleich
Teiler
poten
(„Nul
Poten
ord
(iii)
U
g
(A

ist G isomorph zu einer Untergr. von S_n.)

Bsp. $|G| = 4 \Rightarrow G \cong \mathbb{Z}/4\mathbb{Z}$ oder $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Die Gruppe $\mathbb{Z}/4\mathbb{Z}$ ist isomorph zur Untergruppe $\langle (1234) \rangle$ von S_4, und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ist isomorph zur Kleinschen Vierergruppe $V_4 \leq S_4$.

(ii) Jede Gruppe G operiert auf sich selbst durch <u>Konjugation</u>, d.h. durch $g \circ h = ghg^{-1}$.

Diese Operation ist im Fall $G \neq \{e\}$ <u>nicht</u> transitiv, wegen $G(e) = \{g \circ e \mid g \in G\} = \{geg^{-1} \mid g \in G\} = \{e\} \subsetneq G$

Sa

(i)

(ii)

Sem

ein

gleich

Anwendung: Klassengleichung (Spezialfall der Bahngleichung, s.u.), Folgerungen daraus: Zu jedem Teiler d der Ordnung einer endlichen Gruppe G von Primzahlpotenzordnung gibt es eine Untergruppe $U \leq G$ mit $|U| = d$ („Nullter Sylowsatz"), Lemma von Cauchy, Gruppen von p-Potenzordnung sind auflösbar, Gruppen von Primzahlquadratordnung sind abelsch

(iii) Jede Gruppe G operiert auf der Menge $\mathcal{U}$ ihrer Untergruppen durch Konjugation, d.h. durch

$$g \cdot U = gUg^{-1} \text{ für } g \in G,\ U \in \mathcal{U}$$

(Anwendung: Sylowsätze)

gleichung, s.u.); Folgerungen daraus; Zu jedem Teiler d der Ordnung einer endlichen Gruppe G ... Primzahl-

<u>Satz</u>: Sei G eine Gruppe, die auf einer Menge X operiert.

(i) Zusammenhang zwischen Bahnen und Stabilisatoren: Für jedes $x \in X$ sind $G(x)$ und G/G_x gleichmächtig. (insb.: Ist $(G:G_x)$ endlich, dann gilt $(G:G_x) = |G(x)|$.)

(ii) Bahngleichung: Sei $F \subseteq X$ die <u>Fixpunktmenge</u> der Operation, also $F = \{x \in X \mid g \cdot x = x \ \forall g \in G\}$ und $R \subseteq X$ ein Repräsentantensystem der Bahnen der Operation mit mehr als einem Element. Dann gilt
$$|X| = |F| + \sum_{x \in R} (G:G_x)$$

H25T3A2 Übung: H20T2A2, F19T3A3

Sei G eine Gruppe, Ω eine Menge und $\circ$ eine Operation von G auf Ω. Man nennt $K = \{g \in G \mid g \circ x = x \ \forall x \in X\}$ den Kern der Operation. Ist $K = \{e\}$, dann bezeichnet man die Operation als treu.

(a) Wir setzen voraus, dass G abelsch ist und treu und transitiv auf Ω operiert. Zeigen Sie, dass der Stabilisator G_x von x für jedes $x \in \Omega$ mit K übereinstimmt.

Da die Operation treu ist, gilt $K = \{e\}$.

(G

2

S

N

(G

(c) Fü

nicht-a

endlich

wobei

zu (i) Se

Operation

Zu zeigen ist also $G_x = \{e\}$ für alle $x \in X$.

Angenommen, es gibt ein $x \in X$ mit $G_x \neq \{e\}$.

Sei $g \in G_x \setminus \{e\}$. Beh: $g \in K$

(Aus der Beh folgt dann $K \neq \{e\}$, im Widerspruch zu den Voraussetzungen.)

z.zg. $g \cdot y = y \ \forall y \in X$. Sei also $y \in X$.

Da die Operation transitiv ist, gilt

$G(x) = X \Rightarrow y \in G(x) \Rightarrow \exists h \in G : h \cdot x = y$

$$\Rightarrow g \cdot y = g \cdot (h \cdot x) = (gh) \cdot x \underset{G \text{ abelsch}}{=}$$

$$(hg) \cdot x = h \cdot (g \cdot x) \underset{g \in G_x}{=} h \cdot x = y$$

Damit ist die Beh bewiesen.

A3

(b) Wir setzen voraus, dass G endlich und abelsch ist, und treu und transitiv auf Ω operiert.
Zeigen Sie: $|G| = |\Omega|$

Sei $x \in X$. Da die Operation transitiv ist, gilt $G(x) = \Omega$.
Nach Teil (a) gilt $G_x = \{e\}$. $\Rightarrow |G| = \frac{|G|}{|G_x|} =$
$(G : G_x) = |G(x)| = |\Omega|$.

(c) Finden Sie Beispiele für Operationen einer nicht-abelschen endlichen Gruppe G auf einer endlichen Menge Ω, die treu und transitiv ist, wobei (i) $|G| = |\Omega|$ bzw. (ii) $|G| \neq |\Omega|$

zu (i) Setze $G = \Omega = S_3$, betrachte die Operation $\bullet$ von S_3 auf sich selbst durch Links-

X.

$\neq \{e\}$.

m

)

$\in X$.

}

$h \cdot x = y$

$x =$

↑ G abelsch

$= y$

translation. Diese Operation ist bekanntermaßen immer transitiv, und S_3 ist nicht abelsch.

noch zu überprüfen: $\circ$ ist treu, d.h. der Kern K der Operation ist gleich $\{id\}$.

Sei also $g \in K$. $\Rightarrow \forall h \in S_3 : g \circ h = h$

$\Rightarrow g \circ e = e \Rightarrow ge = e \Rightarrow g = e$

Also ist $K = \{e\}$.

zu (ii) Setze $G = S_3$, $\Omega = M_3 = \{1, 2, 3\}$

Laut VL ist für jedes $n \in \mathbb{N}$ die Operation von S_n auf M_n transitiv. (Für $n = 1$ ist das wegen $M_1 = \{1\}$ offensichtlich, und für $n \geq 2$ folgt es aus $k = (1\ k) \circ 1 \in S_n(1)$ für $1 \leq k \leq n$.)

s.o. $\Rightarrow S_3$ ist nicht abelsch, außerdem:

$|M_3| = 3 \neq 6 = |S_3|$. Schließlich ist die Opevation auch treu, denn: Sei σ ein Element des Kerns. Dann gilt $\sigma \cdot k = k$ für $1 \le k \le n$. nach Def. der Operation also $\sigma(k) = k \;\forall\, k \in M_n$, d.h. $\sigma = id$ $\square$

F23T1A4

(a) Zeigen Sie, dass die Charakteristik eines endlichen Körpers eine Primzahl ist.

Sei K ein endl. Körper und $n = \mathrm{char}(K)$. Da K endlich ist, muss $n \neq 0$ gelten, denn im Fall $n = 0$ wäre 1_K ein Element unendlicher Ordnung in $(K,+)$. Ang., n ist keine Primzahl.

Sei P

Dann

laut

zu P

$|\mathbb{F}_p$

K^m

(c)

W

C

M

Dann gilt entweder $n = 1$ oder es gibt $r, s \in \mathbb{N}$ mit $rs = n$ und $1 < r, s < n$. Ang. $n = 1$. $\Rightarrow 1_{\mathbb{K}} = 1 \cdot 1_{\mathbb{K}} = 0_{\mathbb{K}}$. Aber in Körpern gilt $1_{\mathbb{K}} \neq 0_{\mathbb{K}}$.

Ang., es gibt $r, s \in \mathbb{N}$ wie oben. $r, s \in \mathbb{N}$ mit $r, s < \operatorname{char}(\mathbb{K}) \Rightarrow r \cdot 1_{\mathbb{K}} \neq 0_{\mathbb{K}}$, $s \cdot 1_{\mathbb{K}} \neq 0_{\mathbb{K}}$

andererseits: $(r \cdot 1_{\mathbb{K}}) \cdot (s \cdot 1_{\mathbb{K}}) = (rs) \cdot 1_{\mathbb{K}} = n \cdot 1_{\mathbb{K}} = 0_{\mathbb{K}} \overset{\mathbb{K} \text{ Körper}}{\Longrightarrow} r \cdot 1_{\mathbb{K}} = 0_{\mathbb{K}}$ oder $s \cdot 1_{\mathbb{K}} = 0_{\mathbb{K}}$ ↯

(b) Sei V ein Vektorraum über einem endl. Körper $\mathbb{K}$ von endlicher Dimension. Zeigen Sie, dass $|V|$ eine Potenz von $\operatorname{char}(\mathbb{K})$ ist.

…ons.

…r

$\square$

…l –

…l.

Sei P der Primkörper von K und $p = \mathrm{char}(K)$.
Dann ist K ein endl-dim. P-Vektorraum und $P \cong \mathbb{F}_p$ laut Vorlesung. Sei $d = \dim_P K$. Dann ist K isomorph zu P^d als P-Vektorraum $\Rightarrow |K| = |P^d| = |P|^d = |\mathbb{F}_p|^d = p^d$. Sei $m = \dim_K V$. Dann ist V isomorph zu K^m als K-Vektorraum. $\Rightarrow |V| = |K^m| = |K|^m = (p^d)^m = p^{dm}$.

(c) Sei K ein endlicher Körper und $q = |K|$, $\mathrm{char}(K) \neq 2$.
Weiter sei $\circ$ die Operation durch Konjugation von $G = Gl_2(K)$ auf $X = \mathcal{M}_{2,K}$. Bestimmen Sie die Mächtigkeit der Bahn $G(A)$ für $A = \begin{pmatrix} 0_K & 1_K \\ 1_K & 0_K \end{pmatrix}$.

Sei $G_A \leq G$ der Stabilisator von A. Laut Vl. gilt

$$|G(A)| = (G : G_A) = \frac{|G|}{|G_A|}$$

<u>Beh.</u>: $|G| = (q^2-1)(q^2-q)$ (bereits früher erledigt, wird hier weggelassen)

Nach Def. gilt $G_A = \{T \in GL_2(K) \mid TAT^{-1} = A\}$

Es ist $\chi_A = \det(xE - A) = \det\begin{pmatrix} x & -1_K \\ -1_K & x \end{pmatrix} = x^2 - 1_K = (x-1_K)(x+1_K)$

char $K \neq 2 \Rightarrow$ A hat zwei verschiedene Eigenwerte, nämlich ± 1. außerdem: χ_A zerfällt über K in Linearfaktoren, für die beiden Eigenwerte gilt $\mu_a(A, 1_K) = \mu_a(A, -1_K) = 1 \Rightarrow \mu_g(A, \lambda) = 1$ für $\lambda \in \{\pm 1_K\}$

Mächtigkeit der Bahn $G(A)$ für $A =$

$\Rightarrow$ A ist diagonalisierbar und ähnlich zur Matrix $D = \begin{pmatrix} 1_K & 0_K \\ 0_K & -1_K \end{pmatrix}$, d.h. $A = T_0 D T_0^{-1}$ für eine Matrix $T_0 \in GL_2(K)$.

Für jedes $T \in GL_2(K)$ gilt die Äquivalenz $T \in G_A \iff T \cdot A = A \iff$
$TAT^{-1} = A \iff T T_0 D T_0^{-1} T^{-1} =$
$T_0 D T_0^{-1} \iff T_0^{-1} T T_0 D T_0^{-1} T^{-1} T_0 = D$
$\iff (T_0^{-1} T T_0) D (T_0^{-1} T T_0)^{-1} = D$
$\iff T_0^{-1} T T_0 \cdot D = D$. Durch $T \mapsto$
$T_0^{-1} \cdot T$ ist also Bijektion zwischen G_A und
G_D geg. $\Rightarrow |G_A| = |G_D|$

nicht-abelschen endlichen Gruppe G auf einer

Für $T \in GL_2(K)$ gilt außerdem die Äquivalenz

$$T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_D \Leftrightarrow TDT^{-1} = D \Leftrightarrow$$

$$TD = DT \Leftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\Leftrightarrow \begin{pmatrix} a & -b \\ c & -d \end{pmatrix} = \begin{pmatrix} a & b \\ -c & -d \end{pmatrix} \Leftrightarrow b = d = 0_K$$

und $a, b \in K^\times$

also: $|G_D| = |K^\times| \cdot |K^\times| = (q-1)\cdot(q-1)$

Anzahl Paare $(a,b) \in K^\times \times K^\times$

$$\Rightarrow |G(A)| = \frac{|G|}{|G_A|} = \frac{(q^2-q)(q^2-1)}{(q-1)^2} = \frac{(q-1)(q-1)\cdot q \cdot (q+1)}{(q-1)^2}$$

$$= q\cdot(q+1)$$

Übung: H22T1A1

Anmerkungen

- Allgemein gilt: Ist $\bullet : G \times X \to X$ eine Operation einer Gruppe G auf einer Menge X, und sind $x, y \in X$ Elemente derselben Bahn, dann sind die Stabilisatoren G_x und G_y isomorph. (Genauer: Es gilt $G_y = gG_xGg^{-1}$, wobei $g \in G$ ein Element mit der Eigenschaft $g \bullet x = y$ bezeichnet.) Dies ist der allgemeine Grund für die Gleichung $|G_A| = |G_D|$ in der Aufgabe.
- Man hätte Teil (c) auch ohne den Umweg über die Diagonalmatrix D lösen können. Allerdings wäre dadurch die nachfolgende Rechnung umständlicher geworden. Betrachtet man an Stelle der Gleichung $TD = DT$ die Gleichung $TA = AT$, dann erhält man

Anmerkungen

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0_K & 1_K \\ 1_K & 0_K \end{pmatrix} = \begin{pmatrix} 0_K & 1_K \\ 1_K & 0_K \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \Leftrightarrow \quad \begin{pmatrix} b & a \\ d & c \end{pmatrix} = \begin{pmatrix} c & d \\ a & b \end{pmatrix}$$
$$\Leftrightarrow \quad c = b, d = a$$

und somit

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

Weil T invertierbar ist, muss $a^2 - b^2 \neq 0_K$ gelten, was zu $b \notin \{\pm a\}$ äquivalent ist. Man kann nun die Anzahl der möglichen Paare (a, b) bestimmen. Im Fall $a = 0_K$ muss b ungleich null sein; es gibt also $q - 1$ Möglichkeiten für b. Im Fall $a \neq 0_K$ sind durch $\pm a$ zwei Möglichkeiten für b ausgeschlossen, so dass dieser Fall $(q-1)(q-2)$ mögliche Paare (a, b) liefert. Insgesamt kommen wir auch hier auf $(q-1) + (q-1)(q-2) = (q-1)^2$ Möglichkeiten für das Paar (a, b).