Mathematik für InformatikerInnen 2

Frank-Olaf Schreyer

Universität des Saarlandes, SS 2020

Gruppen und Operationen

Die Themen heute sind

- Gruppenoperationen
- Bahnen und Quotienten $G\backslash M$
- Index einer Untergruppe
- Stabilisatoren und die Klassengleichung

In der letzten Vorlesung hatten wir Gruppen eingeführt und zum Beipiel die Operation von S_4 auf dem Tetraeder betrachtet. Heute wollen wir Gruppenoperationen auf Mengen allgemein definieren.

Gruppenoperationen

Definition. Sei G eine Gruppe und M eine Menge. Eine **Operation** von G auf M ist eine Abbildung

$$G \times M \to M, \quad (g, m) \mapsto g \cdot m,$$

die den folgenden Axiomen genügt:

O1) ('Assoziativgesetz')
$(a \cdot b) \cdot m = a \cdot (b \cdot m) \quad \forall a, b, \in G$ und $\forall m \in M$

O2) (Wirkung des neutralen Elements $e \in G$)
$e \cdot m = m \quad \forall m \in M.$

Beispiele.

1. $\mathrm{GL}(n, K)$ operiert auf K^n vermöge $(A, x) \mapsto Ax$.
2. Für $M \subset \mathbb{R}^3$ mit Schwerkpunkt im Nullpunkt operiert die Symmetriegruppe $S(M) \subset \mathrm{O}(3)$ auf M.
3. S_n operiert auf $\{1, \ldots, n\}$.

Bahnen

Bemerkung. Sei $G \times M \to M$ eine Operation. Dann ist

$$G \to \operatorname{Bij}(M), \quad g \mapsto (g \colon M \to M, \quad m \mapsto g \cdot m)$$

ein Gruppenhomomorphismus.

Definition. Seien $G \times M \to M$ eine Gruppenoperation und $m \in M$. Dann heißt die Menge

$$Gm := G \cdot m := \{g \cdot m \mid g \in G\}$$

die **Bahn** oder der **Orbit** von m (unter G).

Beispiel. Die Bahnen von $\mathrm{SO}(2)$ auf $\mathbb{R}^2$ sind Kreise:

Der Bahnenraum $G\backslash M$

Bemerkung. Sei $G \times M \to M$ eine Operation und $m, n \in M$.
Dann gilt entweder $Gm = Gn$ oder $Gm \cap Gn = \emptyset$.
Mit anderen Worten: *in der gleichen Bahn liegen* ist eine Äquivalenzrelation auf M.

Mit

$$G\backslash M := \{Gm \mid m \in M\} \subset 2^M$$

bezeichnen wie die **Menge der Bahnen** (oder den **Bahnenraum**).

$$\pi : M \to G\backslash M, m \mapsto Gm$$

bezeichnet die kanonische **Quotientenabbildung**.

Beispiele. 1. $SO(2)\backslash\mathbb{R}^2 \cong \mathbb{R}_{\geq 0}$.

2. Sei $\sigma \in S_n$ eine Permutation. Den Bahnen der Operation der Untergruppe $G = \langle\sigma\rangle$ auf $\{1,\ldots,n\}$ entsprechen die Faktoren in der Zykelschreibweise von σ.

3. Die Symmetriegruppe D_8 des Quadrats besteht aus 4 Drehungen und 4 Spiegelungen.

Ende Teil 1

Stabilisator

Definition. Sei $G \times M \to M$ eine Gruppenoperation und $m \in M$. Dann heißt

$$\mathrm{Stab}(m) = \{g \in G \mid g \cdot m = m\}$$

der **Stabilisator** von m. $\mathrm{Stab}(m) \subset G$ ist eine Untergruppe.

Beweis. Zu zeigen ist: $a, b \in Stab(m) \implies ab \in \mathrm{Stab}(m)$ und $a \in Stab(m) \implies a^{-1} \in \mathrm{Stab}(m)$.

Beispiel.

Sei T die Symmetriegruppe des Tetraeders mit Ecken $1, 2, 3, 4$. Dann hat Stab(4) sechs Elemente, nämlich die drei Drehungen, die die Ecke 4 festlassen, sowie drei Spiegelungen. Für den Mittelpunkt der Kante $\overline{12}$ hat der Stabilisator 4 Elemente.

Beispiel. Die Gruppe $G = \mathrm{GL}(m, K) \times \mathrm{GL}(n, K)$ operiert auf $K^{m\times n}$ von links durch

$$(T, S) \cdot A := TAS^{-1}.$$

Dies ist eine Operation: $(T_1, S_1)(T_2, S_2) = (T_1 T_2, S_1 S_2)$ ist die Verknüpfung in G, und

$$\begin{aligned}(T_1, S_1)((T_2, S_2)A) &= T_1(T_2 A S_2^{-1})S_1^{-1} = T_1 T_2 A S_2^{-1} S_1^{-1} \\ &= (T_1 T_2)A(S_1 S_2)^{-1} = (T_1 T_2, S_1 S_2)A\end{aligned}$$

da $(S_1 S_2)^{-1} = S_2^{-1} S_1^{-1}$ gilt.
Nach unserem Klassifikationssatz für lineare Abbildungen gilt:

$$GA = \{B \in K^{m\times n} \mid \operatorname{rang} B = \operatorname{rang} A\}.$$

Es gibt also genau $\min(m, n) + 1$ viele verschiedene Bahnen.
Bemerkung. Oben haben wir Operationen von links definiert. Man kann auch **Operationen von rechts**

$$M \times G \to M, (m, g) \mapsto mg$$

definieren. In dem Fall bezeichnen wir den Bahnenraum mit M/G.

Nebenklassen

Beispiel. Sei $H \subset G$ eine Untergruppe. Dann operiert H auf G von links vermöge:

$$H \times G \to G \quad (h, g) \mapsto h \cdot g = hg$$

und von rechts vermöge:

$$G \times H \to G, \quad (g, h) \mapsto g \cdot h = gh.$$

Definition. Sei $H \subset G$ eine Untergruppe.

$$H \backslash G := \{Hg \mid g \in G\} \subset 2^G$$

heißt Menge der **Rechtsnebenklassen** von H in G.
Entsprechend ist

$$G/H := \{gH \mid g \in G\} \subset 2^G$$

die Menge der **Linksnebenklassen** von H in G.

Beispiele.

1. Sei $U \subset V$ ein Untervektoraum. Dann ist $(U, +)$ eine Untergruppe von $(V, +)$. Die Linke und rechte Nebenklasse von $v \in V$ stimmen überein: $v + U = U + v$, da $(V, +)$ abelsch ist. Die Menge der Nebenklassen

$$V/U = \{v + U \mid v \in V\} \subset 2^V$$

ist die Menge der zu U parallelen Räume.

2. Für $H = \langle (12) \rangle \subset S_3 = G$ sind die Nebenklassen

$H\backslash G$	$\{e, (12)\}$	$\{(23), (123)\}$	$\{(13), (132)\}$
G/H	$\{e, (12)\}$	$\{(23), (132)\}$	$\{(13), (123)\}$

Insbesondere gilt $H(23) \neq (23)H$.
Die Linksnebenklasse gH, d.h., die Bahn von g unter Rechtsoperation von H auf G, und die Rechtsnebenklasse Hg können verschiedene Teilmengen von G sein.

Ende Teil 2

Index einer Untergruppe

Definition. Sei $H \subset G$ eine Untergruppe. Dann bezeichnet

$$[G : H] := |G/H| \overset{!}{=} |H \setminus G|$$

den **Index** von H in G.

Satz (Indexformel). *Sei $H \subseteq G$ eine Untergruppe. Dann gilt:*

$$|G| = [G : H] \cdot |H|.$$

Beweis. Je zwei Nebenklassen g_1H, g_2H haben gleich viele Elemente, denn

$$g_1H \to g_2H, \quad x \mapsto g_2g_1^{-1}x$$

ist eine Bijektion, deren Umkehrabbildung ist die Multiplikation mit $g_1g_2^{-1}$. Da $G = \dot{\bigcup}_{gH \in G/H} gH$ die disjunkte Vereinigung der Bahnen ist, folgt:

$$|G| = \sum_{gH \in G/H} |gH| = \sum_{gH \in G/H} |H| = |G : H| \cdot |H|. \qquad \square$$

Bemerkungen.

1. Jede Gruppe G operiert auf sich selbst durch Translation
$$G \times G \to G, (g, h) \mapsto gh.$$
2. Eine weitere Operation ist die Operation durch **Konjugation**
$$G \times G \to G, (g, h) \mapsto ghg^{-1}.$$
(Dies ist eine Operation von links, da $(g_1 g_2)^{-1} = g_2^{-1} g_1^{-1}$ gilt.)
3. Unter Konjugation mit g wird die rechte Nebenklasse $Hg \subset G$ bijektiv auf die linke Nebenklasse gH abgebildet:
$$Hg \overset{g}{\mapsto} g(Hg)g^{-1} = gHe = gH,$$
was $|gH| = |Hg|$ zeigt.

Satz von Lagrange

Für eine Gruppe G nennt man $|G|$ auch die **Ordnung** von G.

Korollar. *Sei G eine Gruppe. Dann gilt:*

1. *Ist $H \subset G$ eine Untergruppe, $|G| < \infty$, dann gilt*
$$|H| \ \textit{teilt} \ |G|.$$
2. $|G| < \infty, g \in G \Rightarrow \mathrm{ord}(g)$ *teilt* $|G|$.

Beweis. Die erste Aussage folgt direkt aus der Indexformel, die zweite ebenfalls, weil $\langle g \rangle$ für jedes $g \in G$ eine Untergruppe von G ist. □

Beispiele.

1. A_4 ist eine Untergruppe von S_4, und es gilt:
$$|S_4| = 24, \ |A_4| = 12 \text{ und } [S_4 : A_4] = 2.$$
2. Für jede Primzahl p hat $(\mathbb{Z}/p\mathbb{Z}, +)$ nur die trivialen Untergruppen $\{0\}$ und $\mathbb{Z}/p\mathbb{Z}$ selbst.

Bahnen und Stabilisatoren

Lemma. *Sei $G \times M \to M$ eine Operation, $m \in M$, $H = \mathrm{Stab}(m)$. Dann ist die Abbildung*

$$G/H \to Gm, \quad gH \mapsto g \cdot m$$

eine wohldefinierte Bijektion. Insbesondere gilt für jedes $m \in M$:

$$[G : \mathrm{Stab}(m)] = |G/\,\mathrm{Stab}(m)| = |Gm|.$$

Beweis.
Wohldefiniert: Sei $g_1 \in gH$. Dann ist $gm = g_1 m$ zu zeigen. Gilt etwa $g_1 = gh$,so folgt $g_1 m = ghm = gm$.
Surjektiv: Ist klar.
Injektiv: Angenommen, $g_1 m = g_2 m$. Dann gilt:

$$g_2^{-1} g_1 m = m \Rightarrow g_2^{-1} g_1 \in \mathrm{Stab}(m) = H.$$

Das liefert: $g_2 H = g_2((g_2^{-1} g_1)H) = g_1 H$, was zu zeigen war. $\square$

Beispiel. Wir betrachten die Symmetriegruppe $T \cong S_4$ des Tetraeders mit Ecken e_1, e_2, e_3, e_4.

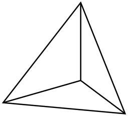
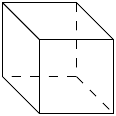
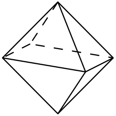
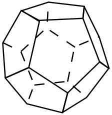
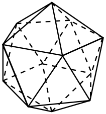
1. $\mathrm{Stab}(e_4) = S(\mathrm{Dreieck}(e_2, e_3, e_4)) \cong S_3$,
   $Te_4 = \{e_1, \dots, e_4\}$,
   $[T : Stab(e_4)] = |Te_4| \implies |T| = |Te_4| \cdot |\mathrm{Stab}(e_4| = 4 \cdot 6 = 24.$
2. Für den Mittelpunkt m_{12} der Kante $\overline{e_1 e_2}$ gilt: $|Tm_{12}| = 6$ und $\mathrm{Stab}(m_{12}) = \{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$. Also

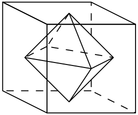
$$|T| = |Tm_{12}| \cdot |\mathrm{Stab}(m_{12})| = 6 \cdot 4.$$

Symmetriegruppe des Würfels

Welche Ordnung hat die Symmetriegruppe des Würfels?

Die Platonischen Körper

4	6	8	12	20
				
Tetraeder	Hexaeder (Würfel)	Oktaeder	Dodekaeder	Ikosaeder
24	48	48		

 $\Longrightarrow \quad S(\text{Oktaeder}) \cong S(\text{Würfel})$

Anwendung: Klassifikation von Graphen

Definition. Ein (**ungerichteter**) **Graph** ist ein Tupel

$$G = (V, E),$$

wobei V eine Menge (von **Ecken** bzw. **Knoten**, engl. vertex) und $E \subset V \times V$ (**Kanten**, engl. edge) eine Teilmenge ist, welche symmetrisch (ungerichtet!) und disjunkt von der Diagonalen (d.h. schleifenfrei) ist.

Isomorphie von Graphen

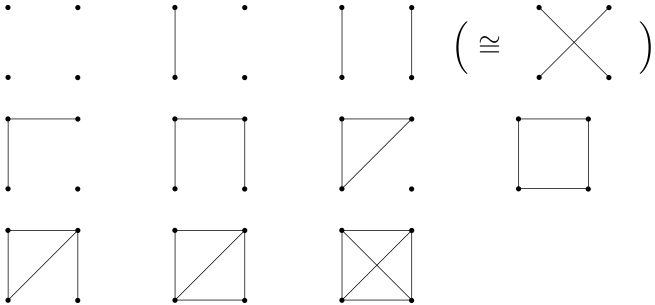
Definition. Zwei Graphen $G_1 = (V_1, E_1), G_2 = (V_2, E_2)$ heißen **isomorph**, wenn es eine bijektive Abbildung

$$\varphi : V_1 \to V_2$$

gibt, die Kanten in Kanten und Nichtkanten in Nichtkanten überführt. Das heißt:

$$(v, w) \in E_1 \Leftrightarrow (\varphi(v), \varphi(w)) \in E_2.$$

Wieviele Isormophieklassen von Graphen mit 4 Knoten gibt es?



Sei M die Menge der Graphen mit den 4 Ecken $\{1, \dots, 4\}$. Es gilt:

$$|M| = 2^6,$$

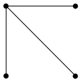
da es 6 mögliche Kanten gibt. S_4 operiert auf M. Wir fragen nach $|S_4 \backslash M|$. Dazu berechnen wir jeweils die Stabilisatoren $H = \mathrm{Stab}((V, E))$.

Wieviele Isormophieklassen von Graphen mit 4 Knoten gibt es?

Die Bahnengleichung liefert:

$$2^6 = 64 \stackrel{!}{=} 1 + 6 + 3 + 12 + 12 + 4 + 3 + 12 + 6 + 1 = 60.$$

Die Bahnengleichung ist also nicht erfüllt, d.h., es fehlt mindestens ein Graph. In der Tat, es fehlt der Graph G_{11}:



Es gilt: $\mathrm{Stab}(G_{11}) \cong S_3$; davon gibt es also $\frac{24}{6} = 4$ Stück. Damit ist die Bahnengleichung erfüllt.

$$\Longrightarrow \quad \text{Es gibt also genau 11 Isomorphietypen!}$$