Mathematik für InformatikerInnen 2

Frank-Olaf Schreyer

Universität des Saarlandes, SS 2020

Gruppen und Symmetrie

Die Themen heute sind

- Beispiele von Gruppen
- Grundbegriffe: Untergruppen, Gruppenhomomorphismen
- S_n: die Gruppe der Permutationen von $\{1, \ldots, n\}$
- Signum einer Permutation

In der letzten Vorlesung hatten wir die Gruppe $\mathrm{GL}(n, K)$ eingeführt. In dieser Vorlesung werden wir Gruppen als fundamentales Konzept kennenlernen. Die Symmetriegruppen erfassen das Konzept der Symmetrie mathematisch.

Nochmal die Gruppenaxiome

Definition. Eine **Gruppe** $(G, \cdot)$ ist eine Menge G zusammen mit einer Verknüpfung $\cdot$, das heißt einer Abbildung

$$\cdot : G \times G \to G, \quad (a, b) \mapsto a \cdot b,$$

die folgenden Axiomen genügen:

G1) (Assoziativgesetz) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in G$.

G2) (Existenz des neutralen Elements)
$\exists\, e \in G$ mit $e \cdot a = a \quad \forall a \in G$.

G3) (Existenz von Inversen) $\forall a \in G, \exists a' \in G,$ so dass $a' \cdot a = e$.

Beispiele.

1. $(\mathbb{Z}, +)$, $(K, +)$, $(K^*, \cdot) = (K \setminus \{0\}, \cdot)$ sind Gruppen.
2. K Körper. $GL(n, K) = \{A \in K^{n \times n} \mid A \text{ ist invertierbar}\}$ ist eine Gruppe bezüglich des Matrizenprodukts.
3. Für $n \in \mathbb{Z}$ ist $\mathbb{Z}/n = \{\overline{0}, \ldots \overline{n-1}\}$ bzgl. der Addition eine Gruppe $(\mathbb{Z}/n, +)$ mit neutralem Element $\overline{0}$.

Orthogonale Abbildungen

Beispiele.

4. Eine Abbildung $f : \mathbb{R}^n \to \mathbb{R}^n$ mit

$$\|f(x) - f(y)\| = \|x - y\| \ \forall x, y \in \mathbb{R}^n \ \text{ und } \ f(0) = 0$$

heißt **orthogonal**. Man kann zeigen: f ist linear und bijektiv, das heißt,

$$f(x) = Ax \ \text{ für ein gewisses } \ A \in \mathrm{GL}(n, \mathbb{R}).$$

Die Menge der orthogonalen Abbildungen auf dem $\mathbb{R}^n$ bilden eine Gruppe, die sogenannte **Orthogonale Gruppe** $\mathrm{O}(n)$. Man kann zeigen, dass die zugehörigen Matrizen genau jene sind mit der Eigenschaft $A^t A = E$, wobei A^t die **transponierte Matrix** bezeichnet. Es bezeichne a_j die j-te Spalte von A. Dann ist

$$A^t A = E \iff \langle a_i, a_j \rangle = \delta_{ij} \ \forall i, j \in \{1, \ldots, n\}$$

Mit anderen Worten, die Spaltenvektoren von A stehen senkrecht aufeinander und haben die Länge 1.

5. Die Menge der Drehungen im $\mathbb{R}^2$ (um den Nullpunkt) ist $\mathrm{SO}(2)$, eine Untergruppe von $\mathrm{O}(2)$.

$$\mathrm{O}(2) \supset \mathrm{SO}(2) = \left\{ \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \mid \alpha \in [0, 2\pi] \right\}.$$

6. Sei $M \subset \mathbb{R}^n$ mit $0 \in \mathbb{R}^n$ als Schwerpunkt. Dann ist die Symmetriegruppe von M definiert durch

$$S(M) = \{A \in \mathrm{O}(n) \mid Ax \in M \ \forall x \in M\} \subset \mathrm{O}(n).$$

Zum Beispiel für den Tetraeder $M \subset \mathbb{R}^3$ besteht die Symmetriegruppe $T = S(M)$ aus 24 Elementen.

Eindeutigkeit des neutralen und der inversen Elemente

Satz. *In jeder Gruppe G mit neutralem Element e gilt:*

1. *Das neutrale Element e erfüllt auch: $a \cdot e = a \quad \forall a \in G$.*
2. *e ist eindeutig durch die Eigenschaft $e \cdot a = a \quad \forall a \in G$ charakterisiert.*
3. *Das Inverse a' zu $a \in G$ erfüllt auch $a \cdot a' = e$.*
4. *Für festes a ist $a' \in G$ durch die Eigenschaft $a' \cdot a = e$ eindeutig bestimmt.*

Beweis.

Zu 3.: Zu a' gibt $a'' \in G$, so dass $a'' \cdot a' = e$ nach (G3). Es folgt:

$$\begin{aligned} a \cdot a' &\overset{G2}{=} e \cdot (a \cdot a') = (a'' \cdot a') \cdot (a \cdot a') \\ &\overset{G1}{=} a'' \cdot (a' \cdot (a \cdot a')) \overset{G1}{=} a'' \cdot ((a' \cdot a) \cdot a') \\ &\overset{G3}{=} a'' \cdot (e \cdot a') \overset{G2}{=} a'' \cdot a' = e. \end{aligned}$$

Eindeutigkeit des neutralen und der inversen Elemente, 2

Zu 1.: Wir können nun 3. verwenden:

$$a \cdot e \overset{G3}{=} a \cdot (a' \cdot a) \overset{G1}{=} (a \cdot a') \cdot a \overset{3.}{=} e \cdot a \overset{G2}{=} a.$$

Zu 2.: Sei e' ein weiteres neutrales Element. Dann gilt

$$e \overset{G2}{=} e' \cdot e \overset{3.}{=} e'.$$

e ist nämlich ebenfalls neutrales Element.

Zu 4.: Sei $\tilde{a}$ ein weiteres Inverses Element zu a. Dann gilt:

$$\tilde{a} \cdot a \overset{G3}{=} e \overset{3.}{=} a \cdot \tilde{a}.$$

Es folgt:

$$\tilde{a} \overset{1.}{=} \tilde{a} \cdot e \overset{3.}{=} \tilde{a} \cdot (a \cdot a') \overset{G1}{=} (\tilde{a} \cdot a) \cdot a' \overset{G3}{=} e \cdot a' \overset{G1}{=} a'. \qquad \square$$

Bemerkung. Für das inverse Element zu $a \in G$ schreibt man meist $a^{-1} := a'$. Eine Ausnahme sind abelsche Gruppen mit $+$ als Verknüpfungszeichen. Dort bevorzugen wir $-a := a'$ und sprechen vom Negativen statt dem Inversen.

Ende Teil 1

Untergruppen

Definition. Eine nichtleere Teilmenge $U \subset G$ ist ein Untergruppe, falls folgendes gilt:

1. $u_1, u_2 \in U \implies u_1 \cdot u_2 \in U$
2. $u \in U \implies u^{-1} \in U$

$(U, \cdot)$ mit $\cdot : U \times U \to U \subset G$ ist dann ebenfalls eine Gruppe.
Bedingungen 1. und 2. lassen sich äquivalent zusammenfassen in

3. $u_1, u_2 \in U \implies u_1^{-1} \cdot u_2 \in U$.

Beispiele.

1. Die Symmetriegruppe T des Tetraeders ist per Definition eine Untergruppe von $\mathrm{O}(3)$.
2. Für $\Delta \subset \mathbb{R}^2$ ein reguläres Dreieck ist $S(\Delta)$ eine Untergruppe von $\mathrm{O}(2)$ und $S(\Delta) \cap \mathrm{SO}(2)$, die Gruppe der Drehungen ,ist eine Untergruppe.

Gruppenhomomorphismen

Definition. Ein **Gruppenhomomorphismus**

$$\varphi : G \to H$$

ist eine Abbildung zwischen Gruppen, die folgendes erfüllt:

$$\varphi(a \circ_G b) = \varphi(a) \circ_H \varphi(b) \quad \forall a, b \in G.$$

Dabei sind $\circ_G$ und $\circ_H$ die Verknüpfungen in G bzw. H. Es gilt:

$$\varphi(e_G) = e_H \text{ und } \varphi(a^{-1}) = (\varphi(a))^{-1}.$$

Einen injektiven bzw. surjektiven Gruppenhomomorphismus nennt man auch (Gruppen–)**Epimorphismus** bzw. **Monomorphismus**. Ein **Isomorphismus** zwischen Gruppen ist ein bijektiver Homomorphismus. Für $\varphi : G \to H$ ein Gruppenhomomorphismus ist der **Kern**

$$\ker \varphi = \{a \in G \mid \varphi(a) = e_H\}$$

eine Untergruppe von G. Das **Bild** von φ

$$\text{Bild}\, \varphi = \varphi(G) \subset H$$

ist eine Untergruppe von H.

Beispiele.

1. $\{\text{Drehungen des regulären Dreiecks}\} = S(\Delta) \cap \mathrm{SO}(2) \cong \mathbb{Z}/3$.
2. Für $g \in G$ eine Element einer Gruppe ist

$$\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$$

eine Untergruppe von G, die **von g erzeugte Untergruppe**. Die **Ordnung** eines Gruppenelements ist

$$\mathrm{ord}(g) := |\langle g \rangle| \in \mathbb{N} \cup \{\infty\}.$$

Mit dieser Notation gilt:

$$\langle g \rangle \cong \begin{cases} \mathbb{Z}/n, & \text{falls } n = \mathrm{ord}(g) < \infty, \\ \mathbb{Z}\,, & \text{falls } \mathrm{ord}(g) = \infty. \end{cases}$$

Die Permutationsgruppen S_n

Sei M eine Menge. Dann ist die Menge der bijektiven Abbildungen

$$\mathrm{Bij}(M) := \{\sigma : M \to M \mid \sigma \text{ ist bijektiv}\}$$

zusammen mit der Komposition von Abbildungen

$$\circ\colon \mathrm{Bij}(M) \times \mathrm{Bij}(M) \to \mathrm{Bij}(M),\ (\sigma, \tau) \mapsto \sigma \circ \tau$$

eine Gruppe. Neutrales Element ist die identische Abbildung

$$\mathrm{id}_M\colon M \to M, \quad x \mapsto x.$$

Das Inverse zu σ ist die Umkehrabbildung σ^{-1}.

Inbesondere haben wir die folgenden Gruppen:
Definition. Für $M = \{1, \ldots, n\}$ heißt

$$S_n = \mathrm{Bij}(\{1, \ldots, n\})$$

die **Gruppe der Permutationen** von $\{1, \ldots, n\}$. Ein Element $\sigma \in S_n$ nennt man eine **Permutation**.

Häufig werden Permutationen $\sigma \in S_n$ in Tabellenform angegeben:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Beispiel. Wir betrachten zwei Permutationen für den Fall $n = 3$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3.$$

Für diese gilt:

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \neq \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Satz. $|S_n| = n!$

Beweis. Für $\sigma(1)$ haben wir n Wahlmöglichkeiten. Danach für $\sigma(2)$ nur noch $n-1$ Wahlmöglichkeiten, da $\sigma(2) \neq \sigma(1)$ wegen der Bijektivität gelten muss . Im k-ten Schritt haben wir nur noch $n-k+1$ Wahlen für $\sigma(k)$, da $\sigma(k) \notin \{\sigma(1), \dots, \sigma(k-1)\}$ gelten muss. Also insgesamt gibt es $n(n-1)\cdots 1 = n!$ Möglichkeiten. □

Ende Teil 2

Zyklische Permutationen

Definition. Für $k \geq 2$ seien $i_1, \ldots, i_k \in \{1, \ldots, n\}$ paarweise verschiedene Elemente. Dann bezeichnet

$$(i_1 \ i_2 \ \ldots \ i_k) \in S_n$$

die zyklische Vertauschung, die

$$i_1 \mapsto i_2, i_2 \mapsto i_3, \ldots \quad \text{und schließlich} \quad i_k \mapsto i_1$$

abbildet und alle anderen Elemente von $\{1, \ldots, n\}$ festlässt. Eine solche Permutation heißt **Zykel**.

Beispiel. Eine Permutation in Zykelschreibweise:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix} = (1\ 2\ 3\ 4) = (2\ 3\ 4\ 1) \in S_5.$$

Zykelschreibweise von Permutationen

Bemerkung. Jede Permutation $\sigma \in S_n$ ist die Komposition von **disjunkten Zykeln** (auch **elementfremden Zykeln**)

$$\sigma = (i_{11}\ i_{12}\ \ldots\ i_{1k_1}) \cdot (i_{21}\ \ldots\ i_{2k_2}) \cdots (i_{r1}\ \ldots i_{rk_r}),$$

wobei die $i_{j\ell}$ paarweise verschieden sind.

Beispiel. Einige Permutationen als Komposition elementfremder Zykeln geschrieben:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\ 2)(3\ 4) = (3\ 4)(1\ 2) \in S_4,$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 5 & 7 & 1 & 3 & 6 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 1 & 2 & 7 \end{pmatrix} =$$

Komposition von nicht disjunkten Zyklen

Es ist klar, dass Produkte disjunkter Zykeln kommutativ sind. Für nicht disjunkte ist dies nicht unbedingt der Fall.
Beispiel. Es gilt:

$$(1\ 2\ 3)(3\ 4\ 5) = (1\ 2\ 3\ 4\ 5) \text{ und } (3\ 4\ 5)(1\ 2\ 3) = (1\ 2\ 4\ 5\ 3).$$

Wie bei Abbildungen werden Kompositionen von Permutationen von rechts nach links berechnet: $(f \circ g)(x) = f(g(x))$.

$$(1\ 2)(3\ 4)(1\ 2\ 3\ 4) =$$

Transpositionen

Definition. Eine **Transposition** in S_n ist eine Permutation τ der Gestalt $\tau = (kl)$.

Satz. *Jede Permutation ist ein Produkt von Transpositionen.*

Beweis. Es reicht, dies für einen Zykel $(i_1 \dots i_k) \in S_n$ zu zeigen. Es gilt:

$$(i_1\ i_2\ \dots\ i_k) = (i_1\ i_2)(i_2\ i_3)\dots(i_{k-1}\ i_k).$$

Für das rechte Produkt gilt:

$$i_1 \mapsto i_2,$$

da außer (i_1, i_2) alle anderen Transpositionen i_1 fest lassen. Allgemeiner ergibt sich $i_l \mapsto i_{l+1}\ \forall l < k$. Schließlich

$$i_k \overset{(i_{k-1}\ i_k)}{\longmapsto} i_{k-1} \mapsto i_{k-2} \mapsto \dots \mapsto i_2 \overset{(i_1\ i_2)}{\longmapsto} i_1.$$

□

Beispiel. Ein Dreierzykel ist Produkt von zwei Transpositionen:

$$(3\ 1\ 2) = (1\ 2\ 3) = (1\ 2)(2\ 3).$$

Das Signum einer Permutation

Definition. Sei $\sigma \in S_n$ eine Permutation. Dann heißt

$$\operatorname{sign}(\sigma) := \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i}$$

das **Signum** von σ. Es gilt $\operatorname{sign}(\sigma) \in \{\pm 1\}$.

Beweis. Es gilt tatsächlich $\operatorname{sign}(\sigma) \in \{\pm 1\}$, da jeder Faktor $j - i$ des Nenners bis auf Vorzeichen auch genau einmal im Zähler vorkommt: Schreiben wir nämlich

$$j' = \sigma^{-1}(j), \quad i' = \sigma^{-1}(i),$$

dann ist

$$\sigma(j') - \sigma(i') = j - i.$$

Ist $i' < j'$, so ist das Vorzeichen $+$; gilt $i' > j'$, dann haben wir einen Faktor -1. □

Satz. *Seien $\sigma, \tau \in S_n$. Dann gilt:*

1. $\operatorname{sign}(\sigma \circ \tau) = \operatorname{sign}\sigma \cdot \operatorname{sign}\tau$.
2. $\operatorname{sign}(\sigma) = (-1)^a$,

wobei a die Anzahl der Transpositionen in irgendeiner Zerlegung von σ in ein Produkt von Transpositionen ist.

Beweis. Zu 1.:

$$\begin{aligned}
\operatorname{sign}(\sigma \circ \tau) &= \prod_{i<j} \frac{(\sigma \circ \tau)(j) - (\sigma \circ \tau)(i)}{j - i} \\
&= \left[\prod_{i<j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)}\right] \left[\prod_{i<j} \frac{\tau(j) - \tau(i)}{j - i}\right] \\
&= \operatorname{sign}(\sigma) \cdot \operatorname{sign}(\tau),
\end{aligned}$$

da mit $\{i, j\}$ auch $\{\tau(i), \tau(j)\}$ alle 2-elementigen Teilmengen von $\{1, \ldots, n\}$ durchläuft und

$$\frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} = \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)}$$

gilt.

Zu 2.: Wegen 1. reicht es, $\operatorname{sign}(\tau) = -1$ für Transpositionen $\tau = (kl)$ zu zeigen. Es gilt

$$\begin{aligned}\operatorname{sign}(12) &= \prod_{\substack{i<j,\\ i=1,j=2}} \frac{1-2}{2-1} \prod_{\substack{i<j\\ i=1,j\neq 2}} \frac{j-2}{j-1} \prod_{\substack{i<j,\\ i=2}} \frac{j-1}{j-2} \prod_{\substack{i<j\\ 2<i}} \frac{j-i}{j-i} \\ &= \frac{1-2}{2-1} \prod_{2<j} \frac{j-2}{j-1} \prod_{2<j} \frac{j-1}{j-2} = -1.\end{aligned}$$

Für eine beliebige Transposition $\tau = (kl)$ betrachten wir eine Permutation σ mit $\sigma(1) = k$ und $\sigma(2) = l$. Dann gilt

$$(kl) = \sigma(12)\sigma^{-1}.$$

Also für $\tau = (kl) = \sigma(12)\sigma^{-1}$ folgt

$$\begin{aligned} \operatorname{sign}(\tau) &\overset{1.}{=} \operatorname{sign}(\sigma)\operatorname{sign}(12)\operatorname{sign}(\sigma^{-1}) \\ &= \operatorname{sign}(\sigma)(-1)\operatorname{sign}(\sigma^{-1}) = -\operatorname{sign}(\sigma)\operatorname{sign}(\sigma^{-1}) \\ &\overset{1.}{=} -\operatorname{sign}(\mathrm{id}) = -1. \end{aligned}$$

□

Korollar. $\operatorname{sign}\colon S_n \to \{\pm 1\}$ *ist ein Gruppenhomomorphismus.*

Definition. $A_n := \ker(\operatorname{sign}\colon S_n \to \{\pm 1\})$ heißt die **alternierende (Unter-)Gruppe** von S_n.

Für $n = 3$ ist S_3 isomorph zur Symmetriegruppe eines gleichseitigen Dreiecks

S_4 ist isomorph zur Symmetriegruppe des Tetraeders

Drehungen (123)

(12)(34)

Spiegelung (12)

Drehspiegelungen (1234)

Ende Teil 4