EINFÜHRUNG IN DIE GRUPPENTHEORIE

BORIS BETZHOLZ UND TOBIAS SCHWARZ

Seminarvortrag im Rahmen des Seminars Gruppen und Codes bei Frau Dr. Baumeister

1. Einleitung

Definition 1.1. Gruppe
Eine Menge $\mathcal{M}$ mit einer Verknüpfung "$\circ$": $\mathcal{M} \times \mathcal{M} \to \mathcal{M}$ heisst Gruppe wenn gilt:

- $\exists e \in \mathcal{M}\ \forall g \in \mathcal{M} :\ eg = ge = g$
- $\forall g \in \mathcal{M}\ \exists h \in \mathcal{M} :\ gh = hg = e$
- $\forall g, h, k \in \mathcal{M} :\ (gh)k = g(hk)$

Satz und Definition 1.2. $\mathbf{S_n}$
Die Menge aller Bijektionen auf einer Menge mit n-Elementen bildet mit der Komposition eine Gruppe. Wir nennen diese Gruppe $\mathbf{S_n}$ oder auch Permutationen auf $\mathcal{M}$.

Definition 1.3. Untergruppe
Eine Untergruppe U einer Gruppe G muss die folgenden Eigenschaften erfüllen.

- U muss das eins Element beinhalten
- $\forall g, h \in U :\ gh \in U$

Um eine Permutation notieren zu können benutzt unter anderem man die Zyklen–Schreibweise:
Sei $\pi \in \mathbf{S_n}$ eine Permutation über der Menge $\{1, \ldots, n\}$. Man schreibt π nun in der Form $(1, \pi(1), \pi(\pi(1)), \ldots$ bis man wieder bei 1 angelangt und schliesst die Klammer. Nun nimmt man eine Zahl die noch nicht in der Klammer steht und fährt analog vorran bis alle Zahlen der Menge geschrieben wurden, wobei man Zyklen mit nur einem Eintrag nicht auf schreiben muss.

Beispiel 1.4. Sei $n = 5$ und $\pi(i) = i$ für $i > 3$ sowie $\pi(1) = 2, \pi(2) = 3, \pi(3) = 1$ so schreiben wir (1 2 3) als Zyklus für π.

Definition 1.5. Fixpunkt und Transposition
Sei $\pi \in \mathbf{S_n}$, ein Wert i heisst *Fixpunkt* falls gilt $\pi(i) = i$. Vertauscht π genau zwei Werte so nennt man π eine *Transposition*.

Definition 1.6. Signum
Sei $\pi \in \mathbf{S_n}$ und i, j zwei Werte, wir sagen π hat einen Fehlstand falls $i < j$ aber $\pi(i) > \pi(j)$ gilt. Sei nun $a(\pi)$ die Zahl der Fehlstände von π, so ist der Signum definiert durch

$$sign(\pi) = \begin{cases} +1, & \text{falls } a(\pi) \text{ gerade,} \\ -1, & \text{falls } a(\pi) \text{ ungerade.} \end{cases}$$

Satz und Definition 1.7. Alterniernde Gruppe A_n
Die Menge $A_n := \{\pi \in \mathbf{S_n} \mid sign(\pi) = 1\}$ bildet eine Untergruppe von $\mathbf{S_n}$ und man nennt sie die *Alterniernde Gruppe*.

Beispiel 1.8. Untergruppen von $\mathbf{S_n}$

(1) Die Diedergruppe D_n. Sie wird erzeugt durch die Permutationen:
$\sigma = (1, \ldots, n)$ und $\tau = \begin{pmatrix} 1\,2\,3\,\ldots\,n \\ 1\,n\,n-1\,\ldots\,2 \end{pmatrix}$
(2) Die Kleinsche Vierergruppe K_4:
$K_4 = \{id, (12)(34), (13)(24), (14)(23)\}$

Definition 1.9. Konjugation
Die Verknüpfung $G \times G \to G$, $h^g \mapsto ghg^{-1}$ nennen wir Konjugation. Man nennt zwei Elemente $g, h \in G$ konjungiert falls es ein $k \in G$ gibt mit $g = khk^{-1}$.

Lemma 1.10.
Konjugiertheit ist eine Äquivalenzrelation.

Definition 1.11. Zentralisator
Sei G Gruppe und $g \in G$ der Zentralisator ist definiert durch:
$Z_G(g) := \{h \in G | hg = gh\}$.

2. Präsentation und Charakter

Sei $G_\pi \in Mat_n(\mathbb{C})$ mit $g_{ij} = \begin{cases} 1, & \text{falls } \pi(i) = j, \\ 0, & \text{sonst.} \end{cases}$.
So nennt man G_π Permutationsmatrix oder Präsentation/Darstellung von π.

Bemerkung 2.1. Eine Darstellung kann verschiedenste Dimensionen haben, es gibt zum Beispiel immer eine 1-dimensionale Darstellung, die 1.

Definition 2.2. Charakter
Sei $\pi \in \mathbf{S_n}$ und G_π die zugehörige Präsentation, so nennt man $\chi_\pi := spur(G_\pi)$ den Charakter von π.

Lemma 2.3.
Der Charakter ist konstant auf einer Konjugiertenklasse.

Deshalb lohnt es sich nur die Charaktere der Konjugiertenklassen anzusehen. Auerdem kann man zeigen, dieses Thema gehört der Darstellungstheorie endlicher Gruppen, dass sich Charakter auf irreduzible Charaktere zurück führen lässt.
Und so betrachtet man Charahtertafeln, die nur leider nicht immer einfach zu bestimmen sind.
Hier ein paar Hilfen ohne Beweis:

Definition 2.4.
Seien χ_1 und χ_2 zwei Charakere so definere: $\langle \chi_1, \chi_2 \rangle := \sum_{i=1}^{l} \frac{\chi_1(g_i)\chi_2(g_i)}{|Z_G(g_i)|}$, wobei l die Zahl der Konjugiertenklassen und g_i ein Repräsenteand ist.

Proposition 2.5.
Sind χ_i, χ_j zwei Charakere so gilt: $\langle \chi_i, \chi_j \rangle = \delta_{ij} \Leftrightarrow \chi_i, \chi_j$ irreduzibel.

Proposition 2.6.
$|G| = \sum_{i=1}^{l} \chi_i(id)^2$ mit wobei l die Zahl der Konjugiertenklassen.

Beispiel 2.7. Charaktertafel der $\mathbf{S_3}$

3. Fehlerkorrigierende Codes mit Hilfe von Gruppen

Definition 3.1. Code
Ein *Code* ist ein Menge $\mathcal{C}$von Ketten von Symbolen, genannt *Codewörter*, aus einem gegebenen Alphabet.
Falls alle Codewörter dieselbe Länge haben, so heisst ein Code *Blockcode*.

Definition 3.2.
Seien $\mathcal{C}$ein Blockcode und $x, y \in \mathcal{C}$, etwa $x = x_1x_2x_3\dots$, $y = y_1y_2y_3\dots$.
Dann ist der *Hammingabstand* von x zu y:
$d_H(x,y) := |\{i \in \{1,\dots;n\} | x_i \neq y_i\}|$
und der *Minimalabstand* von $\mathcal{C}$:
$d(\mathcal{C} := min_{x,y\in\,\mathcal{C},\,x\neq y} d_H(x,y)$.

Definition 3.3.
Ist $r \leq \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor$, so heisst $\mathcal{C}$*r-fehlerkorrigierend*.
Betrache nun als Code eine Untergruppe der $\mathbf{S_n}$und Codewörter Ketten der Länge n aus dem Alphabet $\{1,\dots,n\}$. Dann gilt für den Minimalabstand:
$d(\mathcal{C}) = n - max_{g\in\mathcal{C},\,g\neq 1}|Fix(g)|$.

4. Scharf k-transitive Gruppen

Definition 4.1.
Sei $G \leq \mathbf{S_n}$. Dann heisst G *(scharf) k-transitiv*, falls es für je zwei k-Tupel $(x_1,\dots,x_k)$, $(y_1,\dots,y_k) \in \{1,\dots,n\}^k$ mit $x_i = x_j \leftrightarrow i = j$ beziehungsweise $y_i = y_j \leftrightarrow i = j$ genau ein $g \in G$ gibt $((x-1,\dots,x_k))g = (y_1,\dots,y_k)$.

Satz 4.2.
Sei G eine scharf k-transitive Permutationsgruppe vom Grad n. Dann gilt:
$d(G) = n - k + 1$.

Beispiel 4.3.

- $\mathbf{S_n}$ ist scharf n-transitiv und auch scharf $(n-1)$-transitiv
- A_n ist scharf $(n-2)$-transitiv

Klassifikation:

- $k \geq 6$ lediglich $\mathbf{S_k}$, $\mathbf{S_{k+1}}$ und A_{k+2}
- $k = 5$ $\mathbf{S_5}$, $\mathbf{S_6}$, A_7 und die Matheu-Gruppe
  $M_{12} := \langle (12)(34)(56)(78)(910)(1112), (132)(475)(8911) \rangle$
- $k = 4$ $\mathbf{S_4}$, $\mathbf{S_5}$, A_6 und $M_{11} := \{g \in M_{12} | (1)g = 1\} =: (M_{12})_1$
- $k = 3$ Die Gruppe

$$PGL(2,q) := \{\tau : x \mapsto \frac{ax+b}{cx+d} | a,b,c,d \in GF(q),\ ad - bc \neq 0\}$$

  operiert auf der 'projektiven Gerade' $GF(q) \cup \{\infty\}$ (dabei ist $\mathbf{S_3} \cong PGL(2,3)$, $A_5 \cong PGL(2,4)$)
- $k = 2$Die Gruppe:

$$AGL(1,F) := \{\tau : x \mapsto ax + b | a,b \in F\},$$

  wobei F ein endlicher Fastkörper
  operiert auf F (dabei ist $AGL(1,GF(2)) \cong \mathbf{S_2}$, $AGL(1,GF(3)) \cong \mathbf{S_3}$ und $AGL(1,GF(4)) \cong A_5$)
  Fastkrpererfüllt alle Axiome eines Körpers bis auf die Kommutativität der Multipliktation udn das Links–Distributivgesetz.

5. Uncoverings

Definition 5.1.
Eine Menge U von k-Teilmengen von $\Omega = \{1, \ldots, n\}$ heisst (n,k,r)–Uncovering, falls für jede r-Teilmenge R ein $K \subset U$ existiert mit $K \cap R = \emptyset$.

Beispiel 5.2.
$k \leq n - r \Rightarrow U = \begin{pmatrix} \Omega \\ k \end{pmatrix}$ ist ein Uncovering

Beispiel 5.3.
$G = PGL(2,7) \rightarrow n = 8, k = 3, r = \left\lfloor \frac{5}{2} \right\rfloor = 2$. Finde also ein minimales $(8,3,2)$–Uncovering.

$$\begin{array}{ccc} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 2 & 3 & 7 \\ 1 & 7 & 8 \end{array}$$

6. Basis–Transivtive Gruppen

Definition 6.1. Basis
Sei $G \leq \mathbf{S_n}$. Dann ist eine *Basis* von G ein Tupel $(x_1, \ldots, x_b) \in \{1, \ldots, n)^b$, so dass $G_{(x_1,\ldots,x_b)} = \{id\}$; das heisst wenn ein Element $g \in G$ die Elemente $x_1, \ldots, x_b$ fest lässt ist g bereits die Identität. Eine *irredundante* Basis ist eine Basis mit

$$G_{(x_1,\ldots,x_b)} \lneqq G_{(x_1,\ldots,x_i)} \text{für} i = 1 \ldots, b-1$$

Beispiel 6.2.
Sei G eien scharf k-transitive Gruppe. Dann bildet jede Folge von k unterschiedlichen Punkten eine irredundante Basis.

Beispiel 6.3.
$G = GL_n(q)$ operiert auf den Vektoren in $GF(q)^n$ ungleich 0. Dann bildet eine Basis des Vektorraumes $GF(q)^n$ eine irredundante Basis von G.

Satz 6.4.
Sei G gruppe, $g, h \in G$ und $(x_1, \ldots, x_b)$ eine Basis von G. Dann gilt:

$$(x_1, \ldots, x_b)^g = (x_1, \ldots, x_b)^h \Rightarrow g = h.$$

Definition 6.5.
Sei $G \leq \mathbf{S_n}$ r–fehlerkorrigierend. Dann ist ein *Uncovering durch Bases* von G eine Menge von Basen von G, so dass jede r–Teilmenge von $\{1, \ldots, n\}$ disjunkt ist von mindestens einer Basis.

Bemerkung 6.6. Falls G scharf k–transitiv, dann ist jedes (n, k, r)–Uncoverring ein Uncovering durch Basen.

Satz 6.7.
Sei $G \leq \mathbf{S_n}$. Dann existiert stets ein Uncovering durch Basen.

Definition 6.8.

- Eine Permutationsgruppe heisst *IBIS-Gruppe*, falls alle irredundanten Basen die gleiche Gröe besitzen.
- Sei G eine IBIS–Gruppe. Dann heisst die Gröe einer irredundanten Basis der *Rang von G*.

Definition 6.9.
Operiert eien Gruppe G transitiv auf ihren irredundanten Basen, so heisst G *basis–transitiv*.

Bemerkung 6.10. Scharf k-transitiv $\Rightarrow$ basis–transitiv $\Rightarrow$ IBIS–Gruppe.

Definition 6.11.
Sei G eine basis-transitive Gruppe von Grand n und Rang k und sei $(x_1, \ldots, x_k)$ eine irredundante Basis von G. Dann ist der *Typ von G* das Paar $(\{l_0, \ldots, l_{k-1}\}, n)$, wobei l_0 die Anzahl der Punkte ist, die von G festgelassen werden und l_i die Anzahl der Punkte, die von $G_{(x_1,\ldots,x_i)}$ festgelassen werden.

Bemerkung 6.12. $d(G) = n - l_{k-1}$

Klassifikation:

- $\mathbf{S_n}$: Rang $n-1$, Typ $(\{0, 1, \ldots, n-2\}, n)$
- A_n: Rang $n-2$, Typ $(\{0, 1, \ldots, n-3\}, n)$
- $GL_n(q)$: Rang n, Typ $(\{0, q-1, q^2-1, \ldots, q^{n-1}-1\}, q^{n-1}-1)$
- $AGL(n, q)$: Rang $n+1$, Typ $(\{0, q, q^2, \ldots, q^{n-1}\}, q^{n-1})$

–Rang 2

- die scharf 2-transitiven Gruppen mit Typ $(\{0, 1\}, n)$
- $C_{\frac{q-1}{2}} \times PSL(2, q)$ für $q \equiv 3 mod 4$, Typ $(\{0, \frac{q-1}{2}\}, \frac{q-1}{2})$
- $PSL(3, 2)$, Typ $(\{0, 2\}, 14)$
- $PSL(3, 3)$, Typ $(\{0, 6\}, 78)$

–Rang 3

- $PGL(2, q)$ und andere scharf 3-transitive Gruppen, Typ $(\{0, 1, 2\}, q-1)$
- 'Blow-ups' von $PGL(2, q)$, Typ $(\{0, q^d, 2q^d\}, q^d(q-1))$
- $A_j$operiert auf $GF(2)\backslash\{0\}$, $(\{0, 1, 3\}, 15)$
- $V \rtimes H$,wobei V die additive Gruppe von $GF(2)^4$ und H der Punkt-Stabilisator von A_7 ist. Operiert wie oben, Typ $(\{0, 2, 3\}, 16)$.