# Endliche Permutationsgruppen

Stephan Klaus

Vorlesung Sommer Semester 2024

Skript: Wolfgang Schwarz

In der historischen Entwicklung der Gruppentheorie haben Permutationsgruppen eine große Rolle gespielt, da Gruppen immer zusammen mit ihrer Wirkung auf andere mathematische Objekte untersucht wurden (z.B. als Permutationen der Nullstellen eines Polynoms in der Galois-Theorie oder der geometrischen Symmetrien eines regulären Polyeders mit ihrer Wirkung auf Ecken, Kanten und Flächen).

## Inhaltsverzeichnis

# 1. Grundlagen der Gruppentheorie und Gruppenoperationen

## 1.1. Gruppenaxiome

**Definition 1.1.** Eine Menge $G$ zusammen mit einer Abbildung

$$\begin{aligned} \cdot : G \times G &\longrightarrow G \\ (a, b) &\longmapsto a \cdot b = ab \end{aligned}$$

ist eine Gruppe $(G, \cdot)$, wenn die Abbildung folgende Eigenschaften erfüllt:

- Assoziativität

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \text{für alle } a, b, c \in G \tag{G1}$$

- Neutrales Element

$$\text{Es gibt ein Element } e \in G \quad \text{mit} \quad a \cdot e = a \quad \text{für alle } a \in G \tag{G2}$$

- Inverses Element

$$\text{für alle } a \in G \text{ gibt es ein Element } a^{-1} \in G \quad \text{mit} \quad a \cdot a^{-1} = e \tag{G3}$$

Die Gruppe heißt abelsch oder kommutativ, wenn überdies gilt:

- Kommutativität

$$a \cdot b = b \cdot a \quad \text{für alle } a, b \in G \tag{G4}$$

Statt $\cdot$ wird die Verknüpfung in abelschen Gruppen häufig mit + bezeichnet.

Die Anzahl $|G|$ der Elemente in $G$ heißt Ordnung von $G$.

Die Gruppenaxiome G1, G2 und G3 sind Minimalanforderungen in dem Sinne, dass nur die Existenz eines rechts-neutralen und rechts-inversen Elementes gefordert wird. Tatsächlich ist ein rechts-neutrales Element gleichzeitig links-neutral und ein rechts-inverses Element gleichzeitig links-invers. Das wird in dem folgenden Satz zusammengefasst.

**Proposition 1.2.** *1) Rechts- und Links-Inverse stimmen überein.*

$$a^{-1} \cdot a = e \quad \textit{für alle } a \in G$$

*2) Rechts- und links-neutrale Elemente stimmen überein.*

$$e \cdot a = a \cdot e = a \quad \textit{für alle } a \in G$$

*3) Kürzungsregel*

$$\begin{aligned} a \cdot x = b &\iff x = a^{-1} \cdot b \\ x \cdot a = b &\iff x = b \cdot a^{-1} \end{aligned}$$

*4) Das inverse Element des neutralen Elements e ist wieder e.*

*5) Das neutrale Element e ist eindeutig.*

*6) Das inverse Element ist eindeutig.*

*Beweis.* ad 1)

$$\begin{aligned} a^{-1} \cdot a &= a^{-1} \cdot a \cdot e \\ &= a^{-1} \cdot a \cdot a^{-1} \cdot (a^{-1})^{-1} \\ &= a^{-1} \cdot e \cdot (a^{-1})^{-1} \\ &= a^{-1} \cdot (a^{-1})^{-1} \\ &= e \end{aligned}$$

ad 2)

$$\begin{aligned} e \cdot a &= a \cdot a^{-1} \cdot a \\ &= a \cdot e \\ &= a \end{aligned}$$

ad 3)

$$\begin{aligned} a \cdot x &= b \\ a^{-1} \cdot a \cdot x &= a^{-1} \cdot b \\ x &= a^{-1} \cdot b \end{aligned}$$

ad 4) Nach G3 gilt

$$\begin{aligned} e \cdot e^{-1} &= e \\ e^{-1} \cdot e \cdot e^{-1} &= e^{-1} \cdot e \\ e^{-1} &= e \quad \text{mit Aussage 2)} \end{aligned}$$

ad 5) Sei $e'$ ein zweites neutrales Element. Nach G2 gilt dann:

$$\begin{aligned} e \cdot e' &= e \\ e^{-1} \cdot e \cdot e' &= e^{-1} \cdot e \\ e' &= e \quad \text{mit Aussage 4)} \end{aligned}$$

ad 6) Folgt aus der Kürzungsregel 3).

□

### 1.1.1. Beispiele für Gruppen

**Beispiel 1.3.** 1. Die ganzen Zahlen bilden mit der Addition als Verknüpfung eine Gruppe $(\mathbb{Z}, +)$.

2. Sei $K$ ein Körper. Dann ist $(K, +)$ mit der Addition eine abelsche Gruppe. Mit $K^* = K \setminus \{0\}$ ist $(K^*, \cdot)$ mit der Multiplikation eine abelsche Gruppe.

3. Die Menge aller invertierbaren $2 \times 2$ Matrizen über einem Körper $K$ bildet mit der Matrix-Multiplikation eine Gruppe, die allgemeine lineare Gruppe:

$$GL(2, K) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in K,\ ad - bc \neq 0 \right\}$$

Das neutrale Element ist die Einheitsmatrix. Die Assoziativität ergibt sich automatisch, wenn man die Matrizen als lineare Abbildungen betrachtet. Wenn der Körper $K$ endlich ist ($|K| = q$), dann ergibt sich für die Ordnung von $GL(2, K)$

$$|GL(2, K)| = (q^2 - 1)(q^2 - q)$$

Denn für die erste Spalte gibt es $(q^2 - 1)$ Möglichkeiten (alle außer der Nullspalte). Für die zweite Spalte gibt es $(q^2 - q)$ Möglichkeiten (alle außer den Vielfachen der ersten Spalte).

4. Auch die Menge aller invertierbaren $n \times n$ Matrizen über einem Körper $K$ bilden eine Gruppe.

5. Sei $X$ eine Menge. Dann bilden alle bijektiven Abbildungen $f : X \to X$ mit der Verknüpfung von Abbildungen eine Gruppe.

$$S(X) = \{ f : X \to X \mid f \quad \text{bijektiv} \}$$

6. Wenn die Menge $X$ endlich und $n$ die Anzahl der Elemente in $X$ ist, dann heisst $S(X) = S_n$ die symmetrische Gruppe. Die bijektiven Abbildungen sind dann alle Permutationen der $n$ Elemente. Somit ergibt sich für die Ordnung der symetrischen Gruppe:

$$| S_n | = n!$$

7. Rubiks Cube: Die Drehungen der Seiten erzeugen eine Gruppe.

## 1.2. Untergruppen

**Definition 1.4.** Sei $G$ eine Gruppe. Dann heisst $H \subseteq G$ Untergruppe von $G$, wenn gilt

- $H$ ist nicht leer.

$$H \neq \varnothing \tag{UG1}$$

- $H$ enthält auch alle Inversen.

$$\text{für alle } a \in H \quad \text{gilt} \quad a^{-1} \in H \tag{UG2}$$

- $H$ enthält alle Verknüpfungen.

$$\text{für alle } a, b \in H \quad \text{gilt} \quad a \cdot b \in H \tag{UG3}$$

Notation: $H < G$

In jeder Untergruppe $H < G$ gelten auch die Gruppenaxiome. Daher ist jede Untergruppe auch selbst eine Gruppe.

### 1.2.1. Beispiele für Untergruppen

**Beispiel 1.5.** 1. In der allgemeinen linearen Gruppe $GL(2,\mathbb{R})$ bilden die orthogonalen Matrizen eine Untergruppe, die orthogonale Gruppe.

$$O(2) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid A^T \cdot A = Id \right\}$$

Die Determinante der orthogonalen Matrizen ist entweder 1 oder $-1$.

2. In der Gruppe der orthogonalen Matrizen bilden die Matrizen mit Determinante 1 ein Untergruppe: die spezielle, lineare Gruppe oder Drehgruppe.

$$SO(2) = \{ A \in O(2) \mid \det A = 1 \}$$

Orthogonale Matrizen $A \in SO(2)$ haben die Form

$$A = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

3. Analog bilden $O(n)$ und $SO(n)$ Untergruppen in der allgemeinen linearen Gruppe vom Grad $n$.

4. In der multiplikativen Gruppe der komplexen Zahlen $(\mathbb{C}^*, \cdot)$ bildet der Einheitskreis eine Untergruppe.

$$S^1 = \{ z \in \mathbb{C} \mid |z| = 1 \}$$

Diese ist isomorph zur Drehgruppe $SO(2)$.

5. Im Einheitskreis $S^1$ bilden regelmäßige $n$-Ecke ($n \in \mathbb{N}$) Untergruppen: die zyklischen Gruppen der Ordnung $n$. In komplexer Schreibweise erhält man mit $a = e^{\frac{2\pi i}{n}}, a^n = 1$

$$\begin{aligned} C_n &= \{ a^k \mid 0 \le k \le (n-1) \} \\ &= \{ 1, a, a^2, \cdots, a^{n-1} \} \end{aligned}$$

Die multiplikative, zyklische Gruppe $C_n$ ist isomorph zur additiven Restklassengruppe

$$C_n \cong \mathbb{Z}/n = \{ 0, 1, \cdots, n-1 \}$$

6. In der allgemeinen linearen Gruppe über beliebigen Körpern $K$ bilden Matrizen mit Determinante 1 die spezielle, lineare Gruppe.

$$SL(n,K) = \{\, A \in GL(n,K) \,|\, detA = 1 \,\}$$

7. Mit den folgenden Elementen aus $GL(2,\mathbb{C})$

$$\begin{aligned} e &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ i &= \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} \\ j &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ k &= \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix} \end{aligned}$$

wird die Untergruppe

$$Q_8 = \{\, e\,,\, -e\,,\, i\,,\, -i\,,\, j\,,\, -j\,,\, k\,,\, -k \,\}$$

gebildet, die Quaternionengruppe. Es gelten folgende Relationen:

$$\begin{aligned} -e &= i^2 = j^2 = k^2 \\ ij &= k \\ jk &= i \\ ki &= j \end{aligned}$$

Damit erhält man folgende Verknüpfungstabelle:

| | e | -e | i | -i | j | -j | k | -k |
|---|---|---|---|---|---|---|---|---|
| e | e | -e | i | -i | j | -j | k | -k |
| -e | -e | e | -i | i | -j | j | -k | k |
| i | i | -i | -1 | 1 | k | -k | -j | j |
| -i | -i | i | 1 | -1 | -k | k | j | -j |
| j | j | -j | -k | k | -1 | 1 | i | -i |
| -j | -j | j | k | -k | 1 | -1 | -i | i |
| k | k | -k | j | -j | -i | i | -1 | 1 |
| -k | -k | k | -j | j | i | -i | 1 | -1 |

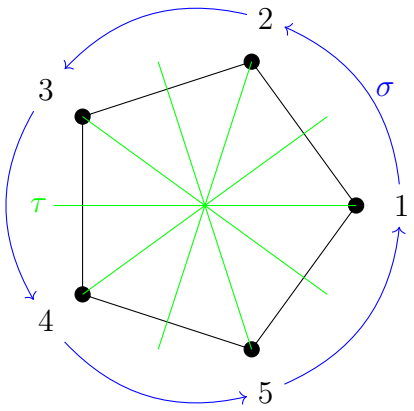
Die Quaternionengruppe $Q_8$ ist eine dizyklische Gruppe. Diese erhält man aus Erzeugern $i, j$ und Relationen.

$$Q_8 = \langle\, i, j \,|\, i^4 = 1, i^2 = j^2, j \cdot i \cdot j^{-1} = i^{-1} \,\rangle$$

8. Sei $X \subset \mathbb{R}^2$ eine Teilmenge. Dann bildet

$$H = \{\varphi \in O(2) \,|\, \varphi(X) = X\}$$

eine Untergruppe. Zur Veranschaulichung sei $X$ zum Beispiel ein regelmäßiges $n$-Eck im Einheitskreis um den Ursprung mit einer Ecke in $(1, 0)$.




In dem dargestellten 5-Eck ist $\sigma$ die Drehung um den Ursprung um 72° und $\tau$ die Spiegelung an der $x$-Achse. Als Isometriegruppe eines regelmäßigen $n$-Ecks erhält man die Diedergruppe

$$\begin{aligned} D_n &= \langle\, \sigma, \tau \,|\, \sigma^n = \tau^2 = e, \sigma \cdot \tau = \tau \cdot \sigma^{-1} \,\rangle \\ &= \{\, e\,,\, \sigma\,,\, \sigma^2\,,\, \cdots,\, \sigma^{n-1}\,,\, \tau \cdot \sigma\,,\, \tau \cdot \sigma^2\,,\, \cdots,\, \tau \cdot \sigma^{n-1} \,\} \end{aligned}$$

## 1.3. Verknüpfungen von Gruppen

Sei G eine Gruppe, $I$ eine Indexmenge und $H_i < G$ für alle $i \in I$ Untergruppen in $G$. Dann ist die Schnittmenge

$$H = \bigcap_{i \in I} H_i < G$$

wieder eine Untergruppe in $G$.
Für eine Teilmenge $A \subset G$ erhalten wir

$$\langle A \rangle = \bigcap_{A \subset H < G} H < G$$

die kleinste Untergruppe von $G$, die $A$ enthält: die von $A$ erzeugte Untergruppe. In Beispiel 8 gibt es folgende Untergruppen:

$$\begin{aligned} \langle \sigma \rangle &= C_n < D_n \\ \langle \tau \rangle &= C_2 < D_n \end{aligned}$$

Seien $G$ und $H$ Gruppen, dann ist auch das kartesische Produkt $G \times H$ mit der Verknüpfung

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot g_2, h_1 \cdot h_2) \quad \text{für alle } g_1, g_2 \in G \text{ und alle } h_1, h_2 \in H$$

eine Gruppe.

## 1.4. Abbildungen zwischen Gruppen

**Definition 1.6.** Seien $G$ und $H$ Gruppen.

1. Eine Abbildung
$$\phi : G \longrightarrow H$$
heisst Homomorphismus, wenn gilt:
$$\phi(a \cdot b) = \phi(a) \cdot \phi(b) \quad \text{für alle } a, b \in G$$

2. $\phi$ heisst Isomorphismus, wenn $\phi$ ein bijektiver Homomorphismus ist.

3. $G$ und $H$ heissen isomorph, wenn es einen Isomorphismus $\phi : G \longrightarrow H$ gibt.

4. Ein Isomorphismus $\phi : G \longrightarrow G$ einer Gruppe in sich selbst heisst Automorphismus.

Alle Automorphismen auf einer Gruppe $G$ werden mit $Aut(G)$ bezeichnet.

$$Aut(G) = \{ \phi : G \to G \,|\, \phi \text{ Automorphismus } \}$$

**Lemma 1.7.** *Wenn $\phi : G \longrightarrow H$ ein Isomorphismus ist, dann auch $\phi^{-1} : H \longrightarrow G$. Das heisst, Gruppen-Isomorphie ist eine Äquialenzrelation.*

*Beweis.* Dazu betrachten wir zwei Elemente $a \in H, b \in H$. Dazu gibt es Urbilder $a' = \phi^{-1}(a) \in G, b' = \phi^{-1}(b) \in G$. Wir erhalten:

$$\begin{aligned} \phi^{-1}(a \cdot b) &= \phi^{-1}(\phi(a') \cdot \phi(b')) \\ &= \phi^{-1}(\phi(a' \cdot b')) \quad \text{da } \phi \text{ Homomorphismus} \\ &= a' \cdot b' \\ &= \phi^{-1}(a) \cdot \phi^{-1}(b) \end{aligned}$$

□

**Korollar 1.8.** *Die Automorphismen $Aut(G)$ auf einer Gruppe $G$ bilden mit der Hintereinanderausführung als Verknüpfung wieder eine Gruppe.*

**Lemma 1.9.** *Die Abbildung*

$$\begin{aligned} \varphi_a : G &\longrightarrow G \\ g &\longmapsto a \cdot g \end{aligned}$$

*ist bijektiv und damit ein Isomorphismus.*

*Beweis.* Der Beweis folgt aus der Kürzungsregel Satz 1.2 3). □

**Definition 1.10.** Sei $\varphi : G \to H$ ein Homomorphismus von der Gruppe $G$ in die Gruppe $H$. Dann heisst

$$Ker(\varphi) = \{ a \in G \,|\, \varphi(a) = e \}$$

Kern von $\varphi$.

$$Im(\varphi) = \{ \varphi(a) \in H \,|\, a \in G \}$$

heisst Bild von $\varphi$.

**Lemma 1.11.** *Ein Homomorphismus $\varphi : G \to H$ ist genau dann injektiv, wenn $Ker(\varphi) = \{e\}$.*

*Beweis.* Wenn $\varphi$ injektiv ist, dann kann nur das neutrale Element $e \in G$ auf das neutrale Element $\varphi(e) = e \in H$ abgebildet werden.
Sei umgekehrt $\varphi(a) = \varphi(b)$. Dann gilt:

$$\begin{aligned} e &= \varphi(a) \cdot (\varphi(b))^{-1} \\ &= \varphi(a \cdot b^{-1}) \\ \Rightarrow \quad a \cdot b^{-1} &\in Ker(\varphi) \\ \Rightarrow \quad a \cdot b^{-1} &= e \\ \Rightarrow \quad a &= b \end{aligned}$$

□

**Proposition 1.12.** *Sei $G$ eine abelsche Gruppe und $N < G$ und $H < G$ Untergruppen mit den Eigenschaften*

1. $$N \cap H = \{e\}$$

2. $$|N| \cdot |H| = |G|$$

*Dann ist $G$ isomorph zum Produkt $N \times H$.*

*Beweis.* Wir betrachten die Abbildung

$$\begin{aligned} \varphi : N \times H &\longrightarrow G \\ (n, h) &\longmapsto n \cdot h \end{aligned}$$

$\varphi$ ist ein Homomorphismus, da $G$ abelsch ist.
$\varphi$ ist surjektiv, da $|N| \cdot |H| = |G|$ vorausgesetzt wurde.
$\varphi$ ist auch injektiv. Denn

$$\begin{aligned} n \cdot h = e \quad &\Rightarrow \quad n = h^{-1} \\ &\Rightarrow \quad n \in N \cap H \\ &\Rightarrow \quad n = e \end{aligned}$$

Analog folgt $h = e$. □

**Beispiel 1.13.** Für nicht-abelsche Gruppen ist die Aussage des Satzes im allgemeinen falsch. In der Diedergruppe $D_n = \langle a, b \rangle$ bilden die Drehungen

$$N = \{e, a, a_2, \cdots, a^{n-1}\}$$

eine Untergruppe sowie die Spiegelung an der $x$-Achse

$$H = \{e, b\}$$

Die Voraussetzungen des Satzes sind erfüllt. Aber das Produkt der abelschen Gruppen $N \times H$ ist wieder abelsch, während $D_n$ nicht abelsch ist.

## 1.5. Nebenklassen

**Definition 1.14.** Sei $G$ eine endliche Gruppe und $H < G$ eine Untergruppe. Für jedes $g \in G$ heissen

$$g \cdot H := \{\, g \cdot h \,|\, h \in H \,\}$$

Linksnebenklassen von $H$.

Die Anzahl der Linksnebenklassen heisst Index von $H$ in $G$.

$$|\, G : H \,|$$

Einige wichtige Eigenschaften von Linksnebenklassen fassen wir in folgendem Satz zusammen.

**Theorem 1.15.** *Sei $H < G$ eine Untergruppe in $G$.*

*a) Die Anzahl der Elemente in den Linksnebenklassen von $H$ ist gleich der Anzahl der Elemente von $H$.*

*b) Die Linksnebenklassen bilden eine Zerlegung von $G$ und es gilt:*

$$aH \cap bH = \begin{cases} \varnothing & oder \\ aH = bH \end{cases}$$

*c) $a \in aH$*

*Beweis.* ad a) Die Abbildung

$$\begin{aligned} H &\longrightarrow aH \\ h &\longmapsto a \cdot h \end{aligned}$$

ist nach Definition von Linksnebenklassen surjektiv und wegen der Kürzungsregel auch injektiv und damit bijektiv. Also haben alle Linksnebenklassen von $H$ genau so viele Elemente wie $H$ selbst.

ad b) Wir nehmen an $aH \cap bH \neq \varnothing$. Es genügt zu zeigen, das $aH \subseteq bH$. Durch Vertauschung von $a$ und $b$ erhalten wir analog die andere Inklusion.
Für $c \in aH \cap bH$ gibt es Elemente $h_1, h_2 \in H$ mit

$$c = a \cdot h_1 = b \cdot h_2$$

Daraus folgt

$$\begin{aligned} a &= b \cdot h_2 \cdot h_1^{-1} \\ aH \ni a \cdot h &= b \cdot h_2 \cdot h_1^{-1} \cdot h \in bH \end{aligned}$$

ad c) $a = a \cdot e \in aH$

□

Für eine Untergruppe $H < G$ kann man die Menge der Linksnebenklassen betrachten.

$$G/H = \{\, aH \,|\, a \in G \,\}$$

Nun stellt sich die Frage, ob $G/H$ auch eine Gruppenstruktur besitzt. Dies ist im allgemeinen nicht der Fall. Denn

$$aH \cdot bH = (a \cdot b)H$$

gilt in nicht-abelschen Gruppen nur für spezielle Untergruppen. Diese speziellen Untergruppen spielen eine besondere Rolle in der Gruppentheorie und erhalten einen eigenen Namen.

**Definition 1.16.** Eine Untergruppe $N < G$ heisst Normalteiler, wenn gilt

$$aNa^{-1} = \{\, aha^{-1} \,|\, h \in N \,\} \subseteq N \quad \text{für alle } a \in G$$

Notation: $N \triangleleft G$

Die Definition ist äquivalent mit der Eigenschaft

$$aN = Na \quad \text{für alle } a \in G$$

In diesem Fall bilden die Linksnebenklassen einer Gruppe $G/N$ wieder eine Gruppe, die Quotientengruppe, die zu einer Untergruppe in $G$ isomorph ist.

**Lemma 1.17.** *Der Durchschnitt von Normalteilern einer Gruppe ist wieder ein Normalteiler.*

*Beweis.* Gegeben seien Normalteiler $N_i \triangleleft G$. Dann gilt

$$\begin{aligned} g \cdot (\bigcap_{i \in I} N_i) \cdot g^{-1} &= \bigcap_{i \in I} (g \cdot N_i \cdot g^1) \\ &\subseteq \bigcap_{i \in I} N_i \quad \text{da} \quad N_i \triangleleft G \end{aligned}$$

□

**Theorem 1.18.** *1. Homomorphiesatz*
*Sei*

$$\varphi : G \longrightarrow H$$

*ein Homomorphismus. Dann ist der Kern $N = Ker(\varphi) \subseteq G$ ein Normalteiler in $G$ und die Quotientengruppe $Q = G/N$ ist isomorph zum Bild $Im(\varphi)$. Das heisst, die Abbildung*

$$\begin{aligned} \hat{\varphi} : G/N &\longrightarrow Im(\varphi) \\ g\,N &\longmapsto \varphi(g) \end{aligned}$$

*ist ein Isomorphismus.*

*Beweis.* Sei $h \in N = Ker(\varphi)$ und $a \in G$ beliebig. Dann ist zu zeigen, dass $a \cdot h \cdot a^{-1} \in N$.

$$\begin{aligned} \varphi(a \cdot h \cdot a^{-1}) &= \varphi(a) \cdot \varphi(h) \cdot \varphi(a^{-1}) \\ &= \varphi(a) \cdot \varphi(a^{-1}) \\ &= \varphi(a \cdot a^{-1}) \\ &= e \end{aligned}$$

Die Abbildung $\hat{\varphi}$ ist wohldefiniert. Denn

$$\begin{aligned} aN = bN &\Leftrightarrow b^{-1}a \in N \\ &\Leftrightarrow \varphi(b^{-1}a) = e \\ &\Leftrightarrow \hat{\varphi}(aN) = \varphi(a) = \varphi(b) = \hat{\varphi}(bN) \end{aligned}$$

Dies zeigt gleichzeitig die Injektivität. Die Surjektivität ergibt sich automatisch. □

**Definition 1.19.** Eine Gruppe $G$ heisst einfach, wenn sie keinen nicht-trivialen Normalteiler besitzt.

**Definition 1.20.** Sei $G$ eine Gruppe. Die Menge aller Elemente in G, die mit allen anderen Elemente kommutieren, heisst Zentrum von G.

$$Z(G) := \{\, g \in G \mid gh = hg \text{ für alle } h \in G \,\}$$

## 1.6. Der Satz von Lagrange

**Definition 1.21.** Sei $g \in G$ ein Element in einer endlichen Gruppe. Dann heisst

$$n := \min\{\, k \in \mathbb{N} \mid g^k = 1 \,\}$$

Ordnung von $g$.

**Theorem 1.22.** *Satz von Lagrange*
*Sei $G$ ein endliche Gruppe und $H < G$ eine Untergruppe. Dann gilt*

$$|G| = |G : H| \cdot |H|$$

*Das heisst, dass die Ordnung einer Untergruppe $H < G$ die Ordnung von $G$ teilt.*

*Beweis.* Nach Satz 1.15 a) besitzen alle Linksnebenklassen von $H$ dieselbe Anzahl von Elementen wie $H$. Nach Aussage b) des Satzes bilden die Nebenklassen von $H$ eine Partition von $G$. Daraus folgt

$$|H| \cdot |G : H| = |G|$$

□

**Korollar 1.23.** *Die Ordnung eines Gruppenelements teilt die Ordnung der Gruppe.*

## 1.7. Präsentation einer Gruppe

In diesem Abschnitt geht es darum, eine Gruppe möglichst effizient zu beschreiben. Die Verknüpfungstabelle ist sehr ausführlich und enthält meist viele Redundanzen. Andrerseits sind zyklische Gruppen durch die Angabe des erzeugenden Elements und seiner Ordnung bereits vollständig beschrieben.

**Beispiel 1.24.** 1. Zyklische Gruppen

$$C_n = \langle a | a^n = e \rangle$$

2. Diedergruppen

$$D_n = \langle a, b | a^n = b^2 = e, b \cdot a = a^{-1} \cdot b \rangle$$

Die Beschreibung einer Gruppe durch Erzeugende und Relationen wollen wir nun formalisieren.

### 1.7.1. Wort Gruppen

**Definition 1.25.** Sei $A$ eine endliche Menge von Symbolen und $A^{-1}$ die Menge der zugehörigen inversen Symbolen.

$$A^{-1} = \{ a^{-1} \mid a \in A \}$$

- Dann ist die Wortmenge, die aus den Symbolen gebildet werden kann, so definiert:

$$W(A) = \{ a_1 a_2 \cdots a_k \mid a_i \in A \cup A^{-1} \ k \in \mathbb{N} \cup \{0\} \}$$

- Ein Wort heisst reduziert, wenn keine Paare $aa^{-1}$ oder $a^{-1}a$ darin vorkommen.
- Die Menge aller reduzierten Wörter wird mit $F(A)$ bezeichnet.

**Lemma 1.26.** *Jedes Wort $w \in W(A)$ läßt sich in eindeutiger Weise zu einem reduzierten Wort $w' = red(w) \in F(A)$ reduzieren.*

*Beweis.* Durch Löschung aller Paare $aa^{-1}$ oder $a^{-1}a$ in $w$ ergibt sich das reduzierte Wort $w'$. Wenn ein solches Paar am Anfang des Wortes steht, bleibt für die Löschung keine Wahl. Wenn $aa^{-1}a$ in der Mitte auftritt, bleibt immer $a$ übrig, egal ob zuerst das linke oder das rechte Paar entfernt wird. Analog für $a^{-1}aa^{-1}$ □

**Satz 1.27.** *Die Menge der reduzierten Worte $F(A)$ bildet die Wort-Gruppe mit folgender Verknüpfung. Zwei (reduzierte) Worte werden hintereinander geschrieben und reduziert.*

$$w_1 \circ w_2 = red(w_1 w_2)$$

*Beweis.* Die Assoziativität ergibt sich aus

$$\begin{aligned} w_1 \circ (w_2 \circ w_3) &= red(w_1 red(w_2 w_3)) \\ &= red(w_1 w_2 w_3) \\ (w_1 \circ w_2) \circ w_3 &= red(red(w_1 w_2) w_3) \\ &= red(w_1 w_2 w_3) \end{aligned}$$

Das neutrale Element ist das leere Wort $\varnothing$.
Das inverse Element erhält man, wenn man die inversen Buchstaben in umgekehrter Reihenfolge aufschreibt.

$$\begin{aligned} w^{-1} &= (a_1 a_2 \cdots a_k)^{-1} \\ &= a_k^{-1} \cdots a_2^{-1} a_1^{-1} \\ \Rightarrow w \circ w^{-1} &= red(a_1 1 a_2 \cdots a_k a_k^{-1} \cdots a_2^{-1} a_1^{-1}) \\ &= \varnothing \end{aligned}$$

□

**Beispiel 1.28.** Sei $G$ eine Gruppe und $\{x_1, x_2, \cdots, x_s\} \subseteq G$ eine Auswahl von $s$ Elemente in $G$. Weiter sei mit $A = \{a_1, a_2, \cdots, a_s\}$ eine Menge mit $s$ Buchstaben gegeben. Dann existiert ein Homomorphismus

$$\begin{aligned} \varphi : F(A) &\longrightarrow G \\ a_i &\longmapsto x_i \\ a_i^{-1} &\longmapsto x_i^{-1} \end{aligned}$$

Die Gruppe $G$ wird genau dann von $x_1, x_2, \cdots, x_s$ erzeugt, wenn $\varphi$ surjektiv ist.

**Definition 1.29.** Sei $A$ eine Menge von Buchstaben, $F(A)$ die Wort-Gruppe und $R \subseteq F(A)$ eine Menge von Wörtern. Wir definieren den kleinsten Normalteiler in $F(A)$, der $R$ enthält durch

$$N_R = \bigcap_{R \subseteq N \trianglelefteq F(A)} N$$

Die Faktorgruppe wird bezeichnet durch

$$\langle A : R \rangle = F(A)/N_R$$

**Definition 1.30.** Sei $G$ eine Gruppe und $\{x_1, x_2, \cdots, x_s\} \subseteq G$ Erzeuger von $G$. Weiter sei mit $A = \{a_1, a_2, \cdots, a_s\}$ eine Menge mit $s$ Buchstaben gegeben sowie eine Menge $R \subseteq F(A)$. Dann existiert ein surjektiver Homomorphismus

$$\begin{aligned} \varphi : F(A) &\longrightarrow G \\ a_i &\longmapsto x_i \\ a_i^{-1} &\longmapsto x_i^{-1} \end{aligned}$$

Dieser induziert einen Isomorphismus

$$\varphi' : \langle A : R \rangle = F(A)/Ker(\varphi) \longrightarrow G$$

Das heisst

$$\varphi(w) = e \quad \text{für alle } w \in R$$

Der Isomorphismus $\varphi'$ heisst Präsentation von $G$.
Die Wörter in $R$ nennt man Relationen.

Wenn $\mid A \mid$ gross ist, wird die Gruppe schnell immens gross.

**Beispiel 1.31.** Beim Rubiks Cube erzeugen bereits die 6 Drehungen der Seitenflächen des Würfels eine beachtlich große Gruppe. Dabei ist die Relation, dass 4-malige Drehung auf die Ausgangposition zurückführt, bereits berücksichtigt.

$$|\langle A : R \rangle| = 43\ 252\ 003\ 274\ 489\ 856\ 000 \approx 43 \cdot 10^{18}$$

Zu endlichen Präsentationen von Gruppen hat Max Dehn zu Beginn des 20. Jahrhunderts drei Probleme formuliert.

1. Das Wortproblem
   Wann stellen zwei Worte $w_1, w_2 \in F(A)$ dasselbe Element in $G$ dar?

2. Das Konjugationsproblem
   Wann stellen zwei Worte $w_1, w_2 \in F(A)$ konjugierte Elemente in $G$ dar?

3. Das Isomorphieproblem
   Wann stellen zwei Präsentationen isomorphe Gruppen dar?

Burnside hat 1902 die Frage gestellt, ob jede endlich erzeugte Gruppe, in der jedes Element endliche Ordnung hat, notwendigerweise endlich ist. Erst im Jahr 1964 fanden Golod und Schafarewitsch eine unendliche Gruppe, die endlich erzeugt ist und deren Elemente alle eine endliche Ordnung haben.

Es sei noch erwähnt, dass es im allgemeinen keinen Algorithmus gibt, der die Ordnung $|\langle A : R\rangle|$ berechnet.

### 1.7.2. Zykeldarstellung von Permutationen

Bevor wir eine Präsentation der symmetrischen Gruppe $S_n$ beschreiben, führen wir noch einige Eigenschaften der Zykeldarstellung von Permutationen an.

**Definition 1.32.** Sei $\sigma \in S_n$ eine Permutation von $n$ Elementen $\{ 1, 2, \cdots, n \}$.

1. Ein Teil einer Permutation heisst $k$-Zykel, wenn für $k \leq n$ die Elemente $\{ a_1, a_2, \cdots, a_k \}$ nacheinander in sich abgebildet werden.

   $$a_1 \to a_2 \to \cdots \to a_k \to a_1$$

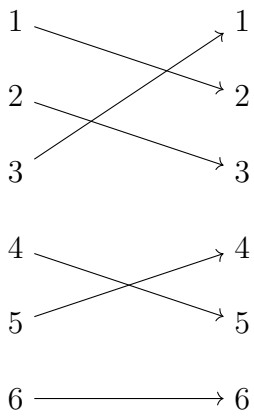
   Notation: $( a_1, a_2, \cdots, a_k )$
   Es ist egal, welches Element am Anfang steht.

2. Zwei Zykel $\sigma$ und $\tau$ heissen disjunkt, wenn keine Zahl $a$ in beiden Zykeln vorkommt.

3. 2-Zykel $( a_1, a_2 )$, bei denen 2 Elemente vertauscht werden, heissen Transpositionen.

4. Transposition benachbarter Elemente $( i, i{+}1 ) = \xi_i$ heissen Nachbar-Vertauschungen.

**Beispiel 1.33.** Wir veranschaulichen die Zykeldarstellung an folgender Permutation $g \in S_6$.



Die Zykeldarstellung für $g$ lautet:

$$g = (123)(45)(6) = (123)(45)$$

Denn Zykel, die nur ein Element enthalten, können weggelassen werden.

**Satz 1.34.** *a) Wenn zwei Zykel $\sigma$ und $\tau$ disjunkt sind, kommutieren sie.*

$$\sigma \cdot \tau = \tau \cdot \sigma$$

*b) Jede Permutation läßt sich als Produkt disjunkter Zykel schreiben und diese Darstellung ist bis auf die Reihenfolge eindeutig.*

*Beweis.* ad a) Seien $\sigma = (a_1, a_2, \cdots, a_r)$ und $\tau = (b_1, b_2, \cdots, b_s)$ disjunkte Zykel und $\omega = \sigma\cdot\tau$ und $\rho = \tau \cdot \sigma$. Dann ist

$$\omega(c) = \left\{ \begin{array}{llll} a_{k+1} & \text{für} & c = a_k & , \quad 1 \le k < r \\ a_1 & \text{für} & c = a_r & \\ b_{k+1} & \text{für} & c = b_k & , \quad 1 \le k < s \\ b_1 & \text{für} & c = b_s & \\ c & \text{sonst} & & \end{array} \right\} = \rho(c)$$

ad b) Sei $\sigma \in S_n$ eine beliebige Permutation. Wir wählen eine beliebige Zahl $i_1 \in I_1 = \{ 1, 2, \cdots, n \}$ und betrachten die Folge

$$i_1 \to \sigma(i_1) \to \sigma^2(i_1) \to \cdots$$

Da $I_1$ endlich und $\sigma$ bijektiv ist, existiert ein $1 \le k \le n$ mit $\sigma^k(i_1) = i_1$ und

$$(\ i_1, \sigma(i_1), \sigma^2(i_1), \cdots, \sigma^k(i_1)\ )$$

liefert einen ersten Zykel. Nun setzen wir

$$I_2 = I_1 \setminus \{\ i_1, \sigma(i_1), \sigma^2(i_1), \cdots, \sigma^k(i_1)\ \}$$

Falls $I_2 = \varnothing$ sind wir fertig. Andernfalls setzen wir den Prozess fort, bis $I_m = \varnothing$ ist. □

**Lemma 1.35.** *Die symmetrische Gruppe $S_n (n > 1)$ wird von $(n-1)$ Transpositionen*

*erzeugt.*

$$S_n = \langle\ \xi_1, \cdots, \xi_{n-1}\ \rangle$$

*Beweis.* Wir bemerken: Transpositionen sind zu sich selbst invers.
Der Beweis wird durch Induktion nach $n$ geführt.
Für $n = 2$ gibt es nur eine Transposition $(\ 1, 2\ )$.
Sei nun $\sigma \in S_n$. Nun führen wir eine Induktion nach $n - \sigma(n)$ durch.
Aus $n - \sigma(n) = 0$ folgt $\sigma(n) = n$ und $\sigma$ kann als Permutation in $S_{n-1}$ aufgefasst werden und wird nach Induktionsvorraussetzung durch Transpositionen erzeugt.
Sei nun $\sigma(n) = i \neq n$. Dann setzen wir $\tau = (\ i, i+1\ ) \cdot \sigma$. Dann folgt

$$\tau(n) = \sigma(n) + 1$$

Für $\tau$ gilt wegen $n - \tau(n) = n - \sigma(n) - 1$ die Induktionsvoraussetzung. Also ist

$$\sigma = (\ i, i+1\ ) \cdot \tau = (\ i, i+1\ ) \cdot \xi_1 \cdots \xi_{n-1}$$

□

**Bemerkung 1.36.** Für die Transpositionen gelten folgende Relationen.

$$\xi_i^2 = id \quad \text{für alle } 0 \leq i < n$$

$$(\xi_i \cdot \xi_j)^2 = id \quad \text{für } \ 0 \leq i, j < n\ ,\ j \geq i + 2$$

$$\begin{aligned} \xi_i \cdot \xi_{i+1} &= (\ i, i+1\ ) \cdot (\ i+1, i+2\ ) \\ &= (\ i, i+2, i+1\ ) \\ \Rightarrow\ (\xi_i \cdot \xi_{i+1})^3 &= id \end{aligned}$$

Dies sind auch alle Relationen, die für eine Präsentation der symmetrischen Gruppe benötigt werden.

### 1.7.3. Präsentationen symmetrischer Gruppen

**Theorem 1.37.** *Symmetrische Gruppen $S_n, n \geq 2$ haben die Präsentation*

$$S_n = \langle\, \xi_1, \cdots, \xi_{n-1} \,|\, \xi_i^2 = e\,,\ (\xi_i \cdot \xi_j)^2 = e\,,\ (\xi_i \cdot \xi_{i+1})^3 = e \text{ für alle } 1 \leq i, j < n\ ,\ j \geq i+2 \,\rangle$$

*Beweis.* Wir fassen die Transpositionen als Buchstaben in $A$ auf.

$$A = \{ \xi_1, \cdots, \xi_{n-1} \}$$

Die Relationen sind:

$$R = \{ \xi_i^2 = e \,,\, (\xi_i \cdot \xi_j)^2 = e \,,\, (\xi_i \cdot \xi_{i+1})^3 = e \text{ für alle } 1 \leq i, j < n \;,\; j \geq i+2 \}$$

Nun führen wir eine Induktion nach $n$ durch. Für $n = 2$ besteht $S_2$ aus allen Permutationen der Menge $\{ 1, 2 \}$. Das heisst $S_2$ wird von einer Transposition $\xi_1 = ( 1, 2 )$ erzeugt. Für $n$ betrachten wir die Untergruppe

$$H = \langle \xi_1, \cdots, \xi_{n-2} \rangle < S_n$$

Für $H \simeq S_{n-1}$ gilt die Induktionsvoraussetzung und $H$ hat $(n-1)!$ Elemente.
Behauptung: $S_n$ ist die disjunkte Vereinigung der $n$ Nebenklassen von $H$.

$$S_n = H \cup H\xi_{n-1} \cup H\xi_{n-1}\xi_{n-2} \cup \cdots \cup H\xi_{n-1}\xi_{n-2}\cdots\xi_1$$

Dann ist $| \langle A : R \rangle | = n!$ und

$$\varphi : \langle A : R \rangle \longrightarrow S_n$$

ein Isomorphismus.
Sei nun $w \in F(A)$ ein Wort. Wenn $\xi_{n-1}$ nicht in $w$ vorkommt, dann gilt $w \in H$. Andernfalls hat $w$ die Form

$$w = \underbrace{\star \;\; \star \;\; \star}_{\in H} \; \xi_{n-1} \; \underbrace{\star \;\; \star \;\; \star}_{=\beta}$$

Wobei $\xi_{n-1}$ so weit links wie möglich auftritt und $\beta$ die Länge $s \geq 0$ hat. Wir wollen nun zeigen, dass $w$ in einer der oben genannten Nebenklassen von $H$ liegt. Dazu verkürzen wir $\beta$ rechts von $\xi_{n-1}$ mithilfe der Relationen und bringen damit $w$ in die Form

$$w = \underbrace{\star \;\; \star \;\; \star}_{\in H} \; \xi_{n-1} \; \xi_{n-2} \cdots \xi_k$$

Für $s = 0$ ist

$$w = \underbrace{\star \;\; \star \;\; \star}_{\in H} \; \xi_{n-1} \in H\xi_{n-1}$$

Sei nun $s \geq 1$ und $\beta = \xi_j \gamma$.

$$w = \underbrace{\star \ \star \ \star}_{\in H} \ \xi_{n-1} \ \xi_j \gamma$$

Wir setzen $m = n-1$, da die Überlegungen damit übersichtlicher werden und sich leichter auf weitere Schritte übertragen lassen.

1. $\underline{j \leq m-2}$
   Dann kann $\xi_j$ mit $\xi_m$ vertauscht werden und wir erhalten

   $$w = \underbrace{\star \ \star \ \star}_{\in H} \ \xi_{n-1} \ \gamma$$

   Und $\gamma$ ist auf die Länge $s-1$ verkürzt worden.

2. $\underline{j = m-1}$
   Dann ist

   $$w = \underbrace{\star \ \star \ \star}_{\in H} \ \xi_{n-1} \ \xi_{n-2} \ \gamma$$

   Und $\gamma = \beta'$ ist auf die Länge $s-1$ verkürzt worden.

$j \geq m$ kann in diesem Schritt nicht vorkommen, da es nur $n-1$ Buchstaben gibt. Wir wiederholen diese Schritte nun für die Ausgangssituation

$$w = \underbrace{\star \ \star \ \star}_{\in H} \ \xi_{n-1} \ \xi_{n-2} \cdots \xi_{m+1} \ \xi_m \ \xi_j \ \gamma$$

Die Fälle $j \leq m-2$ und $j = m-1$ können wie oben behandelt werden. Wir müssen allerdings noch Fälle mit grösseren $j$ betrachten.

1. $\underline{j = m}$
   Dann ist

   $$w = \underbrace{\star \ \star \ \star}_{\in H} \ \xi_{n-1} \ \xi_{n-2} \cdots \xi_{m+1} \ \gamma$$

   Und $\gamma = \beta'$ ist auf die Länge $s-1$ verkürzt worden.

2. $\underline{j = m+1}$

Dann ist

$$\begin{aligned} w &= \underbrace{\star\ \star\ \star}_{\in H}\ \xi_{n-1} \cdots \xi_{m+2}\ \xi_{m+1}\ \xi_m\ \xi_{m+1}\ \gamma \\ &= \underbrace{\star\ \star\ \star}_{\in H}\ \xi_{n-1} \cdots \xi_{m+2}\ \xi_m\ \xi_{m+1}\ \xi_m\ \gamma \\ &= \underbrace{\star\ \star\ \star}_{\in H}\ \xi_{n-1} \cdots \xi_{m+2}\ \xi_{m+1}\ \xi_m\ \gamma \end{aligned}$$

Denn

$$(\ \xi_m\xi_{m+1}\ )^3 = id \quad \Rightarrow \quad \xi_{m+1}\xi_m\xi_{m+1} = \xi_m\xi_{m+1}\xi_m$$

und $\xi_m$ kann nach links in den $H$-Teil geschoben werden.

3. $\underline{j > m+1}$
   Dann kann $\xi_j$ mit allen $\xi_k, m \le k \le j-1$ vertauscht werden und wir erhalten.

$$\begin{aligned} w &= \underbrace{\star\ \star\ \star}_{\in H}\ \xi_{n-1} \cdots \xi_{j+1}\ \underline{\xi_j\ \xi_{j-1}\ \xi_j}\ \xi_{j-2} \cdots \xi_m\ \gamma \\ &= \underbrace{\star\ \star\ \star}_{\in H}\ \xi_{n-1} \cdots \xi_{j+1}\ \underline{\xi_{j-1}\ \xi_j\ \xi_{j-1}}\ \xi_{j-2} \cdots \xi_m\ \gamma \\ &= \underbrace{\star\ \star\ \star}_{\in H}\ \xi_{n-1} \cdots \xi_{j+1}\ \underline{\xi_j\ \xi_{j-1}}\ \xi_{j-2} \cdots \xi_m\ \gamma \end{aligned}$$

   Hierbei wurde wieder $\xi_j\xi_{j-1}\xi_j = \xi_{j-1}\xi_j\xi_{j-1}$ verwendet. Und das linke $\xi_{j-1}$ kann in den $H$-Teil geschoben werden.

In allen Fällen konnte der rechte Teil $\beta$ um einen Buchstaben zu $\gamma$ verkürzt werden. Nach endlich vielen Schritten erhält man $w$ in der gewünschten Form. □

### 1.7.4. Präsentationen alternierender Gruppen

**Definition 1.38.** Das Signum einer Permutation $\sigma \in S_n$ wird gegeben durch folgenden Homomorphismus aus $S_n$ in die multiplikative Zweier-Gruppe.

$$\begin{aligned} sign : S_n &\longrightarrow \{\ 1\ ,\ -1\ \} \\ id &\longmapsto 1 \\ \xi_i &\longmapsto -1 \quad \text{für alle } 0 \le i \le n-1 \end{aligned}$$

Eine Permutation $\sigma$ heisst gerade, wenn $sign(\sigma) = 1$, andernfalls ungerade.

Nach Lemma 1.35 genügt es, *sign* für die Erzeugenden $\xi_i$ anzugeben. $\sigma$ ist genau

dann gerade, wenn $\sigma$ ein Produkt einer geraden Anzahl von Transpositionen ist.

**Definition 1.39.** Der Kern des Homomorphismus *sign* bildet einen Normalteiler in $S_n$ und heisst alternierende Gruppe.

$$A_n = Ker(sign) = \{\ \sigma \in S_n \mid sign(\sigma) = 1\ \}$$

Für $n \geq 2$ besitzt die alternierende Gruppe $\frac{n!}{2}$ Elemente.

**Theorem 1.40.** *Die alternierende Gruppe $A_n, n \geq 3$ wird erzeugt von*

$$\begin{aligned} \xi_1 &= (\ 1\ ,\ 2\ ,\ 3\ ) \\ \xi_i &= (\ 1\ ,\ 2\ ) \cdot (\ i+1\ ,\ i+2\ ) \quad \textit{für alle } 2 \leq i \leq n-2 \end{aligned}$$

*mit den Relationen*

$$\begin{aligned} \xi_1^3 &= e \\ \xi_i^2 &= e \quad \textit{für alle } 2 \leq i \leq n-2 \\ (\ \xi_i \cdot \xi_{i+1}\ )^3 &= e \quad \textit{für alle } 1 \leq i \leq n-3 \\ (\ \xi_i \cdot \xi_j\ )^2 &= e \quad \textit{für alle } 1 \leq i \leq n-4\ ,\ i+1 < j \leq n-2 \end{aligned}$$

*Die alternierende Gruppe $A_n$ hat also die Präsentation*

$$A_n = \left\langle \xi_1, \cdots, \xi_{n-2} \middle| \left\{ \begin{aligned} \xi_1^3 &= e \\ \xi_i^2 &= e \textit{ für alle } 2 \leq i \leq n-2 \\ (\xi_i \cdot \xi_{i+1})^3 &= e \textit{ für alle } 1 \leq i \leq n-3 \\ (\xi_i \cdot \xi_j)^2 &= e \textit{ für alle } 1 \leq i \leq n-4\ ,\ i+1 < j \leq n-2 \end{aligned} \right\} \right\rangle$$

*Beweis.* Wir fassen die Erzeugenden als Buchstaben in $B$ auf.

$$B = \{\ \xi_1, \cdots, \xi_{n-2}\ \}$$

Die Relationen sind:

$$R = \left\{ \begin{aligned} \xi_1^3 &= e \\ \xi_i^2 &= e \text{ für alle } 2 \leq i \leq n-2 \\ (\xi_i \cdot \xi_{i+1})^3 &= e \text{ für alle } 1 \leq i \leq n-3 \\ (\xi_i \cdot \xi_j)^2 &= e \text{ für alle } 1 \leq i \leq n-4\ ,\ i+1 < j \leq n-2 \end{aligned} \right\}$$

Nun führen wir eine Induktion nach $n$ durch. Für $n = 3$ besteht $A_3$ aus allen geraden

Permutationen der Menge $\{\ 1,2,3\ \}$. Das heisst $A_3$ wird von der Erzeugenden $\xi_1 = (\ 1,2,3\ )$ erzeugt und hat die Ordnung $3 = \frac{3!}{2}$.

Sei nun $n \geq 4$. Wie im vorigen Satz 1.37 für die symmetrischen Gruppen betrachten wir

$$H = \langle\ \xi_1, \cdots, \xi_{n-3}\ \rangle < A_n$$

Für $H \simeq A_{n-1}$ gilt die Induktionsvoraussetzung und $H$ hat $\frac{(n-1)!}{2}$ Elemente.
Behauptung: $A_n$ ist die disjunkte Vereinigung der folgenden $n$ Nebenklassen von $H$.

$$A_n = H \cup H\xi_{n-2} \cup H\xi_{n-2}\xi_{n-3} \cup \cdots \cup H\xi_{n-2}\xi_{n-3}\cdots\xi_1 \cup H\xi_{n-2}\xi_{n-3}\cdots\xi_2\xi_1^2$$

Dann ist $|\ \langle B : R\rangle\ | = \frac{n!}{2}$ und

$$\varphi : \langle B : R\rangle \longrightarrow A_n$$

ein Isomorphismus.
Sei nun $w \in F(B)$ ein Wort. Wenn $\xi_{n-2}$ nicht in $w$ vorkommt, dann gilt $w \in H$. Andernfalls hat $w$ die Form

$$w = \underbrace{\star\ \star\ \star}_{\in H}\ \xi_{n-2}\ \beta$$

Wobei $\xi_{n-2}$ so weit links wie möglich auftreten soll und $\beta$ die Länge $s \geq 0$ hat. Wir wollen nun zeigen, dass $w$ in einer der oben genannten Nebenklassen von $H$ liegt. Dazu verkürzen wir $\beta$ rechts von $\xi_{n-2}$ schrittweise mithilfe der Relationen und bringen damit $w$ in eine der Formen

$$\begin{aligned} w &= \underbrace{\star\ \star\ \star}_{\in H}\ \xi_{n-2}\ \xi_{n-3} \cdots \xi_k \quad \text{für } 2 \leq k \leq n-2 \\ \text{oder}\quad w &= \underbrace{\star\ \star\ \star}_{\in H}\ \xi_{n-2}\ \xi_{n-3} \cdots \xi_1 \\ \text{oder}\quad w &= \underbrace{\star\ \star\ \star}_{\in H}\ \xi_{n-2}\ \xi_{n-3} \cdots \xi_1^2 \end{aligned}$$

Für $s = 0$ ist

$$w = \underbrace{\star\ \star\ \star}_{\in H}\ \xi_{n-2} \in H\xi_{n-2}$$

Sei nun $s \geq 1$ und $\beta = \xi_j\gamma$.

$$w = \underbrace{\star\ \star\ \star}_{\in H}\ \xi_{n-2}\ \xi_j\gamma$$

Wir setzen $m = n-2$, da die Überlegungen damit übersichtlicher werden und sich leichter auf die folgenden Schritte übertragen lassen.

1. $\underline{j = m-1}$
   Dann ist
   $$w = \underbrace{\star \ \star \ \star}_{\in H} \ \xi_m \ \xi_{m-1} \ \gamma$$
   Und $\gamma = \beta'$ ist auf die Länge $s-1$ verkürzt worden.

2. $\underline{2 \leq j \leq m-2}$
   Dieser Fall kann nur für $n \geq 6$ auftreten. Da $n \geq 4$ ist und damit $m \geq 2$, folgt aus der Relation $(\xi_j \cdot \xi_m)^2 = e$ auch die Gleichung $\xi_m \cdot \xi_j = \xi_j^2 \cdot \xi_m$. Das heisst $\xi_j$ kann in den linken Teil verschoben werden und $\gamma = \beta'$ ist auf die Länge $s-1$ verkürzt worden.

3. $\underline{j = 1}$
   Für $m = 2$ also $n = 4$ erhält $w$ die Form
   $$w = \underbrace{\star \ \star \ \star}_{\in H} \ \xi_2 \ \xi_1\gamma$$
   Und $\gamma = \beta'$ ist auf die Länge $s-1$ verkürzt worden.
   Für $m > 2$ folgt aus den Relationen $(\xi_1 \cdot \xi_m)^2 = e$ und $\xi_1^3 = e$ auch die Gleichung $\xi_m \cdot \xi_1 = \xi_1^2 \cdot \xi_m$. Das heisst $\xi_1$ kann in den linken Teil verschoben werden und $\gamma = \beta'$ ist auf die Länge $s-1$ verkürzt worden.

$j \geq m$ kann in diesem Schritt nicht vorkommen, da es nur $n-1$ Buchstaben gibt.

Nun führen wir einen weiteren Schritt für die folgende allgemeine Ausgangssituation durch:
$$w = \underbrace{\star \ \star \ \star}_{\in H} \ \xi_{n-1} \ \xi_{n-2} \cdots \xi_{m+1} \ \xi_m \ \beta$$
Wobei $\beta$ die Länge $s \geq 0$ haben soll. Für $s = 0$ ist
$$w = \underbrace{\star \ \star \ \star}_{\in H} \ \xi_{n-2} \cdots \xi_{m+1} \ \xi_m \in H\xi_{n-2}\cdots\xi_m$$
Sei nun $s \geq 1$ und $\beta = \xi_j\gamma$.
$$w = \underbrace{\star \ \star \ \star}_{\in H} \ \xi_{n-2}\cdots \ \xi_m \ \xi_j\gamma$$
Wir müssen nun die Fälle $m \geq 2$ und $m = 1$ gesondert betrachten.

1. $\underline{m \geq 2}$
   Die Fälle $j = m-1$ und $2 \leq j \leq m-2$ und $j = 1$ können wie oben behandelt werden. Wir müssen allerdings noch Fälle mit grösseren $j$ betrachten.

a) $\underline{j = m}$
Dieser Fall kann für $m \geq 2$ nach vorangegangenen Schritten vorkommen. Mit der Relation $\xi_m^2 = e$ erhalten wir

$$w = \star \ \star \ \star \ \xi_{n-1} \cdots \xi_{m-1} \ \gamma$$

und $\beta' = \gamma$ ist auf die Länge $s - 1$ verkürzt worden.

b) $\underline{j = m + 1}$
Dann ist

$$\begin{aligned} w &= \underbrace{\star \ \star \ \star}_{\in H} \ \xi_{n-1} \cdots \xi_{m+2} \ \xi_{m+1} \ \xi_m \ \xi_{m+1} \ \gamma \\ &= \underbrace{\star \ \star \ \star}_{\in H} \ \xi_{n-1} \cdots \xi_{m+2} \ \xi_m \ \xi_{m+1} \ \xi_m \ \gamma \\ &= \underbrace{\star \ \star \ \star}_{\in H} \ \xi_{n-1} \cdots \xi_{m+2} \ \xi_{m+1} \ \xi_m \ \gamma \end{aligned}$$

Da in diesem Fall $m \geq 2$ gilt, folgt aus der Relation $( \ \xi_m \xi_{m+1} \ )^3 = e$

$$\xi_{m+1} \xi_m \xi_{m+1} = \xi_m \xi_{m+1} \xi_m$$

und das links stehende $\xi_m$ kann mit der Relation $(\xi_k \xi_m)^2 = e$ für $k \geq m + 2$ nach links in den $H$-Teil geschoben werden.

c) $\underline{j > m + 1}$
Dann kann $\xi_j$ mit allen $\xi_k, m \leq k < j - 1$ vertauscht werden und wir erhalten:

$$\begin{aligned} w &= \underbrace{\star \ \star \ \star}_{\in H} \ \xi_{n-1} \cdots \xi_{j+1} \ \underline{\xi_j \ \xi_{j-1} \ \xi_j} \ \xi_{j-2} \cdots \xi_m \ \gamma \\ &= \underbrace{\star \ \star \ \star}_{\in H} \ \xi_{n-1} \cdots \xi_{j+1} \ \underline{\xi_{j-1} \ \xi_j \ \xi_{j-1}} \ \xi_{j-2} \cdots \xi_m \ \gamma \\ &= \underbrace{\star \ \star \ \star}_{\in H} \ \xi_{n-1} \cdots \xi_{j+1} \ \underline{\xi_j \ \xi_{j-1}} \ \xi_{j-2} \cdots \xi_m \ \gamma \end{aligned}$$

Hierbei wurde wieder $\xi_j \xi_{j-1} \xi_j = \xi_{j-1} \xi_j \xi_{j-1}$ verwendet. Und das linke $\xi_{j-1}$ kann in den $H$-Teil geschoben werden.

2. $\underline{m = 1}$
Hier müssen wieder zwei Fälle unterschieden werden.

a) $\underline{w = \star \ \star \ \star \ \xi_{n-1} \cdots \xi_2 \ \xi_1 \ \xi_j \ \gamma}$
Wir sehen uns wieder die verschiedenen Werte für $j$ an.

i. $\underline{j = 1}$
Dann ist

$$w = \underbrace{\star \ \star \ \star \ \xi_{n-1} \cdots \xi_2 \ \xi_1^2}_{\in H \ \xi_{n-1} \cdots \xi_2 \ \xi_1^2} \ \gamma$$

Und $\beta' = \gamma$ ist auf die Länge $s - 1$ verkürzt worden.

ii. $\underline{j = 2}$
Aus den Relationen $(\xi_1 \ \xi_2)^3 = e$ und $\xi_1^3 = e$ folgt $\xi_2 \ \xi_1 \ \xi_2 = \xi_1^2 \ \xi_2 \ \xi_1^2$ und damit

$$\begin{aligned} & w = \star \ \star \ \star \ \xi_{n-1} \cdots \xi_3 \ \underline{\xi_2 \ \xi_1 \ \xi_2} \ \gamma \\ \Rightarrow \quad & w = \star \ \star \ \star \ \xi_{n-1} \cdots \xi_3 \ \underline{\xi_1^2 \ \xi_2 \ \xi_1^2} \ \gamma \\ \Rightarrow \quad & w = \star \ \star \ \star \ \xi_{n-1} \cdots \xi_3 \ \underline{\xi_2 \ \xi_1^2} \ \gamma \end{aligned}$$

Denn $\xi_1$ kann mit allen $\xi_k$ für $k \geq 3$ vertauscht werden. Damit ist $\beta' = \gamma$ auf die Länge $s - 1$ verkürzt worden.

iii. $\underline{j > 2}$
In diesem Fall kann $\xi_j$ mit allen $\xi_k$ , $1 \leq k < j - 1$ vertauscht werden und wir erhalten:

$$\begin{aligned} & w = \star \ \star \ \star \ \xi_{n-1} \cdots \xi_{j+1} \ \underline{\xi_j \ \xi_{j-1} \ \xi_j} \ \xi_{j-2} \cdots \xi_1 \ \gamma \\ \Rightarrow \quad & w = \star \ \star \ \star \ \xi_{n-1} \cdots \xi_{j+1} \ \underline{\xi_{j-1} \ \xi_j \ \xi_{j-1}} \ \xi_{j-2} \cdots \xi_1 \ \gamma \\ \Rightarrow \quad & w = \star \ \star \ \star \ \xi_{n-1} \cdots \xi_{j+1} \ \underline{\xi_j \ \xi_{j-1}} \ \xi_{j-2} \cdots \xi_1 \ \gamma \end{aligned}$$

Hierbei wurde wieder $\xi_j \xi_{j-1} \xi_j = \xi_{j-1} \xi_j \xi_{j-1}$ verwendet. Und das linke $\xi_{j-1}$ kann in den $H$-Teil geschoben werden.

b) $\underline{w = \star \ \star \ \star \ \xi_{n-1} \cdots \xi_2 \ \xi_1^2 \ \xi_j \ \gamma}$
Wir sehen uns wieder die verschiedenen Werte für $j$ an.

i. $\underline{j = 1}$
Dieser Fall kann nach den vorangegangenen Schritten vorkommen. Mit der Relation $\xi_1^3 = e$ erhalten wir

$$w = \star \ \star \ \star \ \xi_{n-1} \cdots \xi_2 \ \gamma$$

und $\beta' = \gamma$ ist auf die Länge $s - 1$ verkürzt worden.

ii. $\underline{j = 2}$
Aus den Relationen $(\xi_1 \ \xi_2)^3 = e$ und $\xi_1^3 = e$ folgt $\xi_2 \ \xi_1^2 \ \xi_2 = \xi_1 \ \xi_2 \ \xi_1$ und

damit

$$\begin{aligned} & w = \star\ \star\ \star\ \xi_{n-1} \cdots \xi_3\ \underline{\xi_2\ \xi_1^2\ \xi_2}\ \gamma \\ \Rightarrow\ & w = \star\ \star\ \star\ \xi_{n-1} \cdots \xi_3\ \underline{\xi_1\ \xi_2\ \xi_1}\ \gamma \\ \Rightarrow\ & w = \star\ \star\ \star\ \xi_{n-1} \cdots \xi_3\ \underline{\xi_2\ \xi_1}\ \gamma \end{aligned}$$

Denn $\xi_1$ kann mit allen $\xi_k$ für $k \geq 3$ vertauscht werden. Damit ist $\beta' = \gamma$ auf die Länge $s-1$ verkürzt worden.

iii. $\underline{j > 2}$
Dieser Fall wird analog behandelt wie oben.

In allen Fällen konnte der rechte Teil $\beta$ um einen Buchstaben zu $\gamma$ verkürzt werden. Nach endlich vielen Schritten erhält man $w$ in der gewünschten Form. □

## 1.8. Gruppenoperationen

Die Permutationen einer endlichen symmetrischen Gruppe $S_n$ bilden die Menge $X = [n]$ in sich ab und vertauschen damit die Elemente der Menge $X$. Man kann dies auch so formulieren, dass die symmetrische Gruppe auf die Menge $X$ wirkt. So eine Wirkung können auch andere Gruppen auf andere Mengen haben. Dies soll nun verallgemeinert und formalisiert werden.

**Definition 1.41.** Sei $G$ eine Gruppe und $X$ eine Menge. Die Gruppe $G$ wirkt auf die Menge $X$ oder $G$ operiert auf $X$, wenn es eine Abbildung

$$\rho : G \times X \longrightarrow X$$

gibt mit den Eigenschaften

(1)
$$\rho(1, x) = x \quad \text{für alle } x \in X$$

(2)
$$\rho(g', \rho(g, x)) = \rho(g'g, x) \quad \text{für alle } x \in X \text{und alle } g, g' \in G$$

Man nennt dies auch eine Permutationsdarstellung der Gruppe $G$ auf die Menge $X$.

Eine einfachere Schreibweise ist $\rho(g, x) = gx$. In dieser Schreibweise vereinfacht sich die Eigenschaft (2) zu $g'(gx) = (g'g)x$ und die Assoziativität wird deutlich.

**Lemma 1.42.** *Die Abbildung $\rho : G \times X \to X$ ist genau dann eine Permutationsdarstellung der Gruppe $G$ auf die Menge $X$, wenn es einen Homomorphismus $\bar{\rho}$ von $G$ in die symmetrische Gruppe $Sym(X)$ gibt.*

$$\bar{\rho} : G \longrightarrow Sym(X) := \{\ f : X \to X \ \textit{bijektiv}\ \}$$

*Beweis.* Sei $\rho : G \times X \to X$ eine Permutationsdarstellung der Gruppe $G$ auf die Menge $X$. Dann konstruieren wir folgende Abbildung:

$$\begin{aligned} \bar{\rho} : G &\longrightarrow S(X) \\ g &\longmapsto \bar{\rho}_g \\ \bar{\rho}_g : X &\longrightarrow X \\ x &\longmapsto \rho(g, x) = gx \end{aligned}$$

$\bar{\rho}_g$ ist surjektiv. Denn für jedes $y \in X$ gilt $\bar{\rho}_g(g^{-1}y) = y$ und damit ist $g^{-1}y$ das Urbild von $y$ unter der Abbildung $\bar{\rho}_g$.
$\bar{\rho}_g$ ist injektiv. Denn sei $\bar{\rho}_g(x) = \bar{\rho}_g(y)$. Dann betrachten wir

$$\begin{aligned} x &= (g^{-1}g)x \\ &= g^{-1}(\bar{\rho}_g(x)) \\ &= g^{-1}(\bar{\rho}_g(y)) \\ &= (g^{-1}g)y \\ &= y \end{aligned}$$

Also ist $\bar{\rho}_g$ bijektiv und damit $\bar{\rho}_g \in Sym(X)$.
Nun zeigen wir noch, dass $\bar{\rho}$ ein Homomorphismus ist. Für $g, h \in G$ und $x \in X$ gilt:

$$\begin{aligned} \bar{\rho}_{gh}(x) &= (gh)x \\ &= g(hx) \\ &= g(\bar{\rho}_h(x)) \\ &= \bar{\rho}_g(\bar{\rho}_h(x)) \\ &= (\bar{\rho}_g\bar{\rho}_h)(x) \end{aligned}$$

Sei umgekehrt ein Homomorphismus

$$\begin{aligned} \bar{\rho} : G &\longrightarrow Sym(X) \\ g &\longmapsto \bar{\rho}_g \end{aligned}$$

gegeben. Dann konstruieren wir die Permutationsdarstellung von $G$ auf $X$ wie folgt:

$$\begin{aligned} \rho : G \times X &\longrightarrow X \\ (g, x) &\longmapsto \bar{\rho}_g(x) = gx \end{aligned}$$

Da der Homomorphismus $\bar{\rho}$ das neutrale Element $1 \in G$ in die Identität in $Sym(X)$ abbildet, gilt $x = \bar{\rho}_1(x) = 1x$ und damit ist die Eigenschaft (1) erfüllt.
Da $\bar{\rho}$ ein Homomorphismus ist, gilt $\bar{\rho}_{gh} = \bar{\rho}_g \bar{\rho}_h$. Daraus folgt

$$\begin{aligned} (gh)x &= \bar{\rho}_{gh}(x) \\ &= (\bar{\rho}_g \bar{\rho}_h)(x) \\ &= \bar{\rho}_g(\bar{\rho}_h(x)) \\ &= g(hx) \end{aligned}$$

Und damit ist die Eigenschaft (2) erfüllt. □

Im folgenden betrachten wir die Permutationsdarstellung $\rho$ und den Homomorphismus $\bar{\rho} : G \to Sym(X)$ als gleichwertig und lassen den Querstrich wieder weg.

Ist die Gruppe $G \leq Sym(X)$ eine Untergruppe der symmetrischen Gruppe $Sym(X)$, dann nennt man $G$ Permutationsgruppe.

Der Kern von $\rho$ ist gegeben durch

$$Ker(\rho) = \{\ g \in G \mid \rho_g = id_X \text{ also } \ gx = x \text{ für alle } x \in X\ \}$$

Nach dem 1. Homomorphiesatz 1.18 gilt

$$G/Ker(\rho) \simeq Im(\rho) =: \bar{G} \leq Sym(X)$$

Das Bild $Im(\rho) = \bar{G}$ ist die assoziierte Permutationsgruppe zu $\rho$.

**Definition 1.43.** Die Permutationsdarstellung $\rho$ heisst effektiv oder treu, wenn der Kern von $\rho$ die triviale Gruppe ist. Das heisst, die Gruppe $G$ ist injektiv in die symmetrische Gruppe $Sym(X)$ eingebettet.

Alle Permutationsdarstellungen bilden die Kategorie PREP mit den Objekten

$$\rho : G \curvearrowright X$$

und den Morphismen

$$(\alpha, f) : (\rho : G \curvearrowright X) \to (\rho' : G' \curvearrowright X')$$

Dabei ist $\alpha : G \to G'$ ein Gruppen Homomorphismus und $f : X \to X'$ eine äquivariante Abbildung mit den Eigenschaften

$$\begin{aligned} f(\rho(g,x) &= \rho'(\alpha(g), f(x)) \quad \text{beziehungsweise} \\ f(gx) &= \alpha(g)f(x) \quad \text{für alle } x \in X \text{ und alle } g \in G \end{aligned}$$

Für eine feste Gruppe $G$ bilden alle Permutationsdarstellungen von $G$ eine Unterkategorie PREP(G).

In dieser Vorlesung werden nur endliche Permutationsdarstellungen $\rho$ behandelt. Die Ordnung von $\rho$ ist dann gegeben durch

$$\mid G \mid = m < \infty$$

Der Grad von $\rho$ ist gegeben durch

$$\mid X \mid = n < \infty$$

Die Menge $X$ ist dann isomorph zu $X \cong [n] = \{1, 2, \cdots, n\}$. Dabei gilt auch $[0] = \varnothing$. Wir haben nun verschiedene Beispiele für Permutationsdarstellungen auf der endlichen Menge $[n]$.

**Beispiel 1.44.** Die symmetrische Gruppe $S_n$ operiert auf der Menge $[n]$ durch Permutation.

**Beispiel 1.45.** Als Untergruppe der symmetrischen Gruppe operiert die alternierende Gruppe $A_n$ auf auf der Menge $[n]$ ebenfalls durch Permutation.

**Beispiel 1.46.** Die multiplikative, zyklische Gruppe $C_n$ wirkt auf $[n] \simeq \{1, e^{\frac{2\pi i}{n}}, e^{\frac{4\pi i}{n}}, \cdots, e^{\frac{2(n-1)\pi i}{n}}\}$ durch Multiplikation oder auf den Hochzahlen durch Addition.

Wir benötigen nun noch weitere Begriffe im Zusammenhang mit Gruppenoperationen.

### 1.8.1. Bahnen und Stabilisatoren von Gruppenoperationen

**Definition 1.47.** Die Gruppe $G$ operiere auf der Menge $X$. Dann wird für $x \in X$

$$Gx = \{ gx \mid g \in G \}$$

Orbit oder Bahn durch $x$ genannt.

Zwei Elemente $x, y \in X$ heissen äquivalent, wenn sie sich in derselben Bahn befinden. Das heisst, es gibt ein $g \in G$, so dass gilt:

$$gx = y$$

Die Äquivalenzklassen $[x]$ sind genau die Orbits $Gx$.

**Proposition 1.48.** *Die Orbits bilden eine disjunkte Zerlegung von $X$.*

$$X = \bigsqcup_{[x] \in X/G} Gx \quad \text{mit } X/G = X/\sim$$

**Definition 1.49.** Die Operation $G \curvearrowright X$ heisst transitiv, wenn es nur eine Bahn gibt. Das heisst, es gibt ein $x \in X$ mit

$$Gx = X$$

**Proposition 1.50.** *Folgende Eigenschaften einer Operation $G \curvearrowright X$ sind äquivalent:*

*(i) Die Operation $G \curvearrowright X$ ist transitiv.*

*(ii) Für alle $x \in X$ gilt*

$$Gx = X$$

*(iii) Für alle $x \in X$ gibt es ein $g \in G$ mit*

$$gx = x$$

*(iv) Es gibt nur eine Äquivalenzklasse*

$$|X/G| = 1$$

**Definition 1.51.** Für ein $x \in X$ heisst die Untergruppe

$$G_x = \{ g \in G \mid gx = x \} \leq G$$

Stabilisator von $x$.

**Proposition 1.52.** *Für jedes $x \in X$ ist die Abbildung aus den Linksnebenklassen des Stabilisators in den Orbit*

$$\begin{aligned} G/G_x &\longrightarrow Gx \subseteq X \\ gG_x &\longmapsto gx \end{aligned}$$

*eine Bijektion.*

**Korollar 1.53.** *Bahn-Standgruppen-Satz*
*Die Gruppe $G$ operiere auf der Menge $X$. Dann ist für jedes $x \in X$ das Produkt aus der Anzahl der Orbits von $x$ mit der Ordnung der Standgruppe gleich der Ordnung der Gruppe $G$.*

$$|G| = |Gx| \cdot |G_x|$$

**Definition 1.54.** Sei $U \leq G$ eine Untergruppe in $G$. Die Permutationsdarstellung

$$\begin{aligned} G &\curvearrowright G/U \\ (g, hU) &\mapsto ghU \end{aligned}$$

auf den Linksnebenklassen von $U$ heisst homogener Raum zur Untergruppe $U$.

Der Kern dieser Operation $\mathrm{Ker}(g \curvearrowright G/U)$ heisst Core von $U$ in $G$.

**Proposition 1.55.** *Die Operation $G \curvearrowright G/U$ ist transitiv.*

**Proposition 1.56.** *(i) Sei $G \curvearrowright X$ eine Permutationsdarstellung. Dann gilt für alle $g \in G$ und alle $x \in X$*

$$G_{gx} = gG_xg^{-1}$$

*(ii) Für $x \in X$ und $y = gx$ mit beliebigem $g \in G$ stimmt die Anzahl der $G_x$-Orbits mit der Anzahl der $G_y$-Orbits überein.*

*Beweis.* Die Aussage (i) ist durch Nachrechnen einfach zu verifizieren.

$$\begin{aligned} G_{gx} &= \{\, h \in G \,|\, hgx = gx \,\} \\ &= \{\, h \in G \,|\, g^{-1}hgx = x \,\} \\ &= \{\, h \in G \,|\, g^{-1}hg \in G_x \,\} \\ &= \{\, h \in gG_xg^{-1} \,\} \end{aligned}$$

Zum Beweis der Aussage (ii) betrachten wir die $G_x$-Orbits in $X$.

$$G_x z_i \quad \text{mit } 1 \leq i \leq k \text{ und } z_i \in X$$

Dabei ist $X$ die disjunkte Vereinigung dieser Orbits. Sei nun $w_i = gz_i \in X$. Nach Aussage (i) gilt für die $G_y$-Orbits

$$\begin{aligned} G_y w_i &= G_{gx} w_i \\ &= g G_x g^{-1} w_i \\ &= g G_x z_i \end{aligned}$$

Das heisst, die $G_y$-Orbits gehen durch die Permutation $g \in G$ aus den $G_x$-Orbits hervor. □

**Definition 1.57.** Die Permutationsdarstellung

$$\begin{aligned} c : G &\curvearrowright G \\ (g,h) &\mapsto g \circ h = ghg^{-1} \end{aligned}$$

heisst Konjugation.

Die Orbits der Konjugation sind die Konjugationsklassen

$$\mathcal{C}l(h) = \{\, ghg^{-1} \,|\, g \in G \,\} \subseteq G$$

Die Stabilisatoren von $h \in G$ unter der Konjugation heissen Zentralisator.

$$C_G(h) = G_h = \{\, g \in G \,|\, gh = hg \,\} \leq G$$

**Definition 1.58.** Die Gruppe $G$ operiert auch auf der Menge ihrer Untergruppen $\{\, H < G \,\}$ durch Konjugation:

$$\begin{aligned} G &\curvearrowright \{\, H < G \,\} \\ (g,H) &\mapsto gHg^{-1} \end{aligned}$$

Der Stabilisator von $H < G$ unter der Konjugation heisst Normalisator von $H$ in $G$.

$$N_G(H) = G_H = \{\, g \in G \,|\, gH = Hg \,\}$$

**Bemerkung 1.59.** Der Name Normalisator erklärt sich daraus, dass $H \lhd G_H$ Normal-

teiler im Stabilisator $G_H$ ist. Gleichzeitig ist $G_H$ die größte Untergruppe in $G$, in der $H$ Normalteiler ist.

**Proposition 1.60.** *Sei $G$ eine Gruppe und $P < G$ eine Untergruppe. Dann ist der Zentralisator von $P$ Normalteiler im Normalisator von $P$.*

$$\begin{array}{rcl} C_G(P) & \triangleleft & N_G(P) \\ \{\, g \in G \,|\, g \cdot x \cdot g^{-1} = x \text{ für alle } x \in P \,\} & \triangleleft & \{\, g \in G \,|\, g \cdot P \cdot g^{-1} = P \,\} \end{array}$$

*Und es gibt einen injektiven Homomorphismus*

$$N_G(P)/C_G(P) \longrightarrow Aut(P)$$

*Beweis.* Der Normalisator $N_G(P)$ wirkt auf $P$ durch Konjugation und es gibt einen Homomorphismus

$$\begin{array}{rcl} \varphi : N_G(P) & \longrightarrow & Aut(P) \\ g & \longmapsto & \left\{ \begin{array}{ccc} P & \longrightarrow & P \\ x & \longmapsto & g \cdot x \cdot g^{-1} \end{array} \right. \end{array}$$

Der Kern dieses Homomorphismus $Ker(\varphi)$ ist genau der Zentralisator $C_G(P)$. Als Kern eines Homomorphismus ist $C_G(P) = Ker(\varphi)$ Normalteiler in $N_G(P)$. □

**Theorem 1.61.** *Sei $p$ eine Primzahl und $G$ eine Gruppe der Ordnung $p^n$ , $n \geq 2$. Dann ist das Zentrum $Z(G)$ nicht trivial.*

*Beweis.* Die Gruppe $G$ operiert auf $G$ durch Konjugation.

$$g \circ g' = g \cdot g' \cdot g^{-1}$$

Die Orbits dieser Operation sind genau die Konjugiertenklassen. Und diese sind nach Proposition 1.52 isomorph zu den Linksnebenklassen des Stabilisators (hier: Zentralisator)

$$\begin{array}{rcl} \mathcal{C}l(g') & = & \{\, gg'g^{-1} \,|\, g \in G \,\} \\ & \cong & G/C_G(g') \end{array}$$

Die Zentralisatoren $C_G(g')$ sind Untergruppen in $G$. Somit ist die Ordnung nach dem Satz von Lagrange 1.22 eine Potenz von $p$, da die Ordnung einer Untergruppe stets die

Gruppenordnung teilt. Also gibt es ein $m \in \mathbb{N}$ mit

$$|C_G(g')| = p^m$$

Daraus folgt

$$|\mathcal{C}l(g')| = p^{n-m}$$

Das Zentrum enthält nun alle Elemente $g'$, deren Konjugiertenklasse $\mathcal{C}l(g')$ nur $g'$ enhält.

$$\begin{aligned} Z(G) &= \{ g' \in G \mid gg'g^{-1} = g' \text{ für alle } g \in G \} \\ &= \{ g' \in G \mid |C_G(g')| = 1 \} \end{aligned}$$

Für Elemente, die nicht im Zentrum liegen $g' \notin Z(G)$, ist die Ordnung der Konjugiertenklasse $C_G(g')$ somit ein Vielfaches von $p$ und die Ordnung der Gruppe ist die Summe der Anzahl der Elemente im Zentrum plus ein Vielfaches von $p$.

$$\begin{aligned} |G| &= |Z(G)| + pk \\ &= p^n \end{aligned}$$

Dies ist nur möglich, wenn das Zentrum nicht nur aus dem neutralen Element besteht, das heisst nicht trivial ist. □

Das Zentrum einer Gruppe ist stets ein Normalteiler. Somit ergibt sich als Folgerung:

**Korollar 1.62.** *Eine p-Gruppe der Ordnung $p^n$ , $n \geq 2$ ist nicht einfach.*

**Bemerkung 1.63.** Das Zentrum von $G$ ist der Durchschnitt aller Zentralisatoren.

$$Z(G) = \bigcap_{h \in G} C_G(h)$$

**Bemerkung 1.64.** Transitive Permutationsdarstellungen von $G$ entsprechen den Untergruppen von $G$ bis auf Konjugation.

**Proposition 1.65.** *Sei $U \leq G$ eine Untergruppe in $G$ und $s : G \curvearrowright G/U$ die in Definition 1.54 definierte Operation. Dann ist der Kern $Ker(s)$ der Durchschnitt aller Konjugationsbilder von $U$.*

$$Ker(G \curvearrowright G/U) = \bigcap_{h \in G} c_h(U)$$

*Beweis.* Für ein beliebiges Element $g \in Ker(G \curvearrowright G/U)$ gilt:

$$\begin{aligned} g \in Ker(G \curvearrowright G/U) &\Leftrightarrow ghU = hU \quad \text{für alle } h \in G \\ &\Leftrightarrow h^{-1}ghU = U \quad \text{für alle } h \in G \\ &\Leftrightarrow h^{-1}gh \in U \quad \text{für alle } h \in G \\ &\Leftrightarrow g \in hUh^{-1} \quad \text{für alle } h \in G \end{aligned}$$

□

Wir betrachten nun die Abschätzungen für die Anzahl der Elemente in $X$. Für eine Untergruppe $U \leq G$ gilt nach 1.14

$$|G/U| = |G : U| = \frac{|G|}{|U|}$$

Mit

$$X = \bigsqcup_{[x] \in X/G} Gx \simeq \bigsqcup_{[x] \in X/G} G/G_x$$

erhalten wir

$$\begin{aligned} |X| &= \sum_{[x] \in X/G} \frac{|G|}{|G_x|} \\ &= |G| \sum_{[x] \in X/G} |G_x|^{-1} \end{aligned}$$

Zusammen mit $0 \leq |G_x|^{-1} \leq 1$ folgt die Ungleichung

$$|X| \leq |G| \cdot |X/G|$$

**Definition 1.66.** Die Gruppe $G$ operiere auf der Menge $X$ und $g \in G$ sei ein Element in $G$. Dann ist die Fixpunktmenge von $g$ definiert durch

$$X^g := \{ x \in X \mid gx = x \}$$

Die Fixpunktmenge der ganzen Gruppe $G$ ist definiert durch

$$\begin{aligned} X^G &:= \{ x \in X \mid gx = x \text{ für alle } g \in G \} \\ &= \bigcap_{g \in G} X^g \end{aligned}$$

Die Gruppe $G$ operiert genau dann fixpunktfrei auf der Menge $X$, wenn $X^G = \varnothing$ gilt.

Die Operation $G \curvearrowright X$ heisst trivial, wenn jeder Punkt Fixpunkt ist. Das heisst

$$\begin{aligned} & gx = x \quad \text{für alle } x \in X \text{ und alle } g \in G \\ \Leftrightarrow \quad & G_x = G \quad \text{für alle } x \in X \\ \Leftrightarrow \quad & X^G = G \end{aligned}$$

Die Operation $G \curvearrowright X$ heisst frei oder semiregulär, wenn für alle $1 \neq g \in G$ die Fixpunktmenge $X^g = \varnothing$ leer ist. Das heisst

$$\begin{aligned} & G_x = 1 \quad \text{für alle } x \in X \\ \Leftrightarrow \quad & |X| = |G| \cdot |X/G| \end{aligned}$$

Die Operation $G \curvearrowright X$ heisst regulär, wenn sie frei und transitiv ist. Das heisst

$$X \simeq G$$

### 1.8.2. Lemma von Burnside

Bevor wir nun das Lemma von Burnside formulieren und beweisen, sind noch folgende Hinweise auf die Namensgebung und geschichtliche Entwicklung interessant. Burnside erwähnt und beweist das Lemma um 1900 in seinem Buch "Theory of groups of finite order" [Bur00] und schreibt es Frobenius zu. Man findet es auch im Artikel [Bur09] von Burnside. Tatsächlich war es jedoch Cauchy bereits im Jahre 1845 bekannt. Daher ist das Lemma auch als Cauchy-Frobenius-Lemma oder das Lemma, das nicht von Burnside ist, bekannt.

**Lemma 1.67.** *Lemma von Burnside*
*Sei $G$ eine endliche Gruppe und $G$ operiere auf der Menge $X$. Für ein Element $g \in G$ bezeichne*

$$X^g := \{ x \in X \mid gx = x \}$$

*die Menge der Fixpunkte in $X$ unter dem Element $g \in G$. Dann gilt für die Anzahl der Bahnen $|X/G|$*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

Das Lemma bringt die Anzahl der Bahnen in Zusammenhang mit der Anzahl der Fixpunkte. Die Anzahl der Bahnen ist der Mittelwert aller Fixpunkte der Gruppenelemente.

*Beweis.* Zum Beweis betrachten wir den zweigeteilten Graph, dessen Ecken aus den Elementen der Gruppe $G$ und der Menge $X$ bestehen. Eine Kante zwischen $g \in G$ und $x \in X$ liegt genau dann vor, wenn $gx = x$ gilt. Andere Kanten sind nicht zugelassen. Die Anzahl der Kanten ausgehend von den Gruppenelementen sind genau die Summe der Anzahlen in den Fixpunktmengen $X^g$.

$$\sum_{g \in G} |X^g|$$

Die Anzahl der Kanten ausgehend von den Elementen in $X$ erhalten wir aus der Summe der Anzahlen in den Stabilisatoren $G_x$.

$$\begin{aligned} \sum_{x \in X} |G_x| &= \sum_{x \in X} \frac{|G|}{|Gx|} \\ &= \sum_{[x] \in X/G} |Gx| \, \frac{|G|}{|Gx|} \\ &= |G| \cdot |X/G| \end{aligned}$$

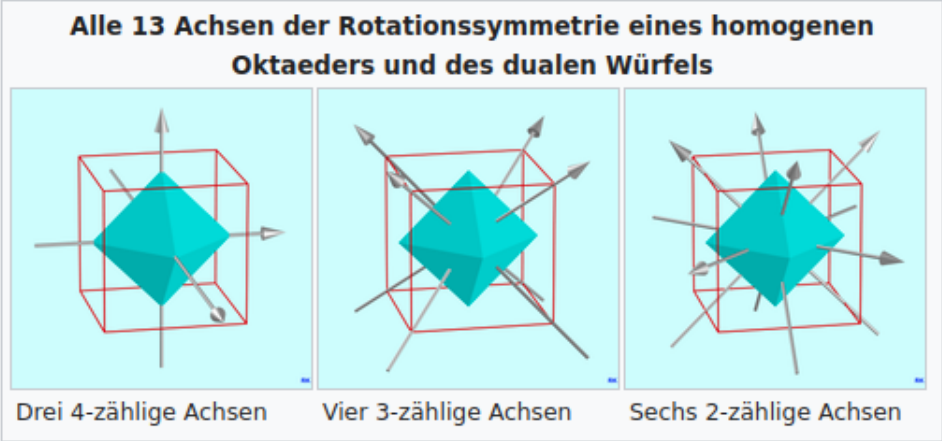
Durch Gleichsetzung folgt die Behauptung. □

Ergänzend zur Vorlesung betrachten wir in einem Beispiel die Anwendung des Lemmas von Burnside auf die Einfärbungen eines Würfels.

**Beispiel 1.68.** Die Seiten eines Würfels werden mit 3 verschiedenen Farben eingefärbt. Die Menge aller möglichen Seitenfärbungen bezeichnen wir mit $X$. Es gibt insgesamt $3^6 = 729$ Möglichkeiten, die 6 Seiten des Würfels mit 3 Farben einzufärben.

Die Drehgruppe des Würfels operiert auf $X$ und einige Einfärbungen gehen durch Drehungen des Würfels ineinander über. Das heisst, sie liegen in derselben Bahn. Alle Einfärbungen in derselben Bahn bilden ein Muster, das bei Drehungen erhalten bleibt. Mit Hilfe des Lemmas von Burnside kann nun die Anzahl der verschiedenen Muster bestimmt werden.

Wir betrachten zunächst die Drehgruppe des Würfels. Sie wird auch Oktaedergruppe genannt, da Oktaeder und Würfel als duale Körper dieselbe Drehgruppe besitzen. In diesem Zusammenhang betrachten wir nur Drehungen des Würfels und lassen keine Spiegelungen zu. In der erweiterten Oktaedergruppe sind auch Spiegelungen enthalten. Die Elemente der Oktaedergruppe können aus den Rotationsachsen bestimmt werden.




(Aus https://de.wikipedia.org/wiki/Oktaedergruppe)
Es gibt 3 Achsen durch gegenüberliegende Seiten des Würfels, die 3 Drehungen um jeweils 90° erlauben.
Es gibt 4 Achsen durch gegenüberliegende Ecken des Würfels, die 2 Drehungen um jeweils 120° erlauben.
Und es gibt 6 Achsen durch gegenüberliegende Kanten des Würfels, die eine Drehung um 180° erlauben.
Zusammen mit der Identität ergibt dies $3 \cdot 3 + 4 \cdot 2 + 6 + 1 = 24$ Drehungen. Die Oktaedergruppe ist isomorph zur symmetrischen Gruppe $S_4$ der Permutationen der 4 Drehachsen durch gegenüberliegende Ecken.

Nun untersuchen wir die Anzahl der Fixpunkte in den Einfärbungen $X$ bei den einzelnen Drehungen. Die Drehungen um die 3 Achsen durch gegenüberliegende Seiten um 90° und 270° lassen die Farben dieser Seiten fest. Die restlichen 4 Seiten werden gedreht und müssen somit die gleiche Farbe haben. Jede solche Drehung läßt also $3^3$ Einfärbungen fest. Und es gibt insgesamt $3 \cdot 2 = 6$ solche Drehungen.
Die Drehungen um die 3 Achsen durch gegenüberliegende Seiten um 180° lassen die Farben dieser Seiten fest und führen von den restlichen 4 Seiten gegenüberliegende Paare ineinander über. Diese 3 Drehungen lassen also $3^4$ Einfärbungen fest.
Bei Drehungen um Achsen durch gegenüberliegende Ecken des Würfels müssen die drei angrenzenden Seiten dieser Ecken jeweils gleich gefärbt sein. Jede solche Drehung läßt also $3^2$ Einfärbungen fest. Und es gibt insgesamt $4 \cdot 2 = 8$ solche Drehungen.
Bei Drehungen um Achsen durch gegenüberliegende Kanten des Würfels müssen die angrenzenden Seiten dieser Kanten jeweils gleich gefärbt sein sowie die restlichen beiden Seiten. Jede solche Drehung läßt also $3^3$ Einfärbungen fest. Und es gibt insgesamt 6 solche Drehungen.

Die Identität läßt natürlich alle $3^6$ Einfärbungen fest. Insgesamt erhalten wir

$$\frac{1}{24}(6 \cdot 3^3 + 3 \cdot 3^4 + 8 \cdot 3^2 + 6 \cdot 3^3 + 3^6) = 57$$

verschiedene Muster.

Allgemein erhält man für n Farben

$$\frac{1}{24}(n^6 + 3 \cdot n^4 + 12 \cdot n^3 + 8 \cdot n^2)$$

verschiedene Muster.

# 2. Automorphismen von Strukturen

Die Automorphismen einer unstrukturierten Menge $X$ sind als bijektive Abbildungen oder Permutationen in der symmetrischen Gruppe $Sym(X)$ zusammengefasst. Interessanter sind natürlich Automorphismen auf strukturierten Mengen, die die Struktur erhalten.

## 2.1. Automorphismen von Graphen

**Definition 2.1.** Ein ungerichteter Graph besteht aus einer Menge $V$ von Knoten (vertices) und einer Menge $E$ von Kanten (edges), wobei die Kanten jeweils 2 Knoten miteinander verknüpfen. Das heisst, eine Kante ist eine 2-elementige Teilmenge der Potenzmenge von $V$.

$$E \subseteq \mathcal{P}_2(V)$$

Ein Automorphismus eines Graphen ist eine bijektive Abbildung $f$ der Knoten in sich, die die Kanten erhält. Das heisst

$$\{v, w\} \in E \Rightarrow \{f(v), f(w)\} \in E$$

Alle Automorphismen eines Graphen bilden die Automorphismengruppe $Aut(V, E)$ des Graphen. Der Mathematiker Roberto Frucht hat 1938 die Frage geklärt, ob es zu jeder Gruppe einen Graphen gibt, der diese als Automorphismengruppe besitzt.

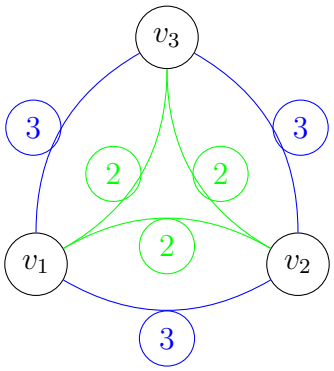
**Theorem 2.2.** *Satz von Frucht*
*Zu jeder Gruppe $G$ gibt es einen Graphen $\Gamma$, dessen Automorphismengruppe $Aut(\Gamma)$ isomorph zu dieser Gruppe ist.*

*Beweis.* Da der Artikel von Frucht [Fru39] allgemein im PDF Format unter
www.numdam.orgitemCM_1939__6__239_0.pdf
oder Suche “frucht herstellung” in scholar.google.de
zugänglich ist, skizzieren wir hier nur die Beweisidee.

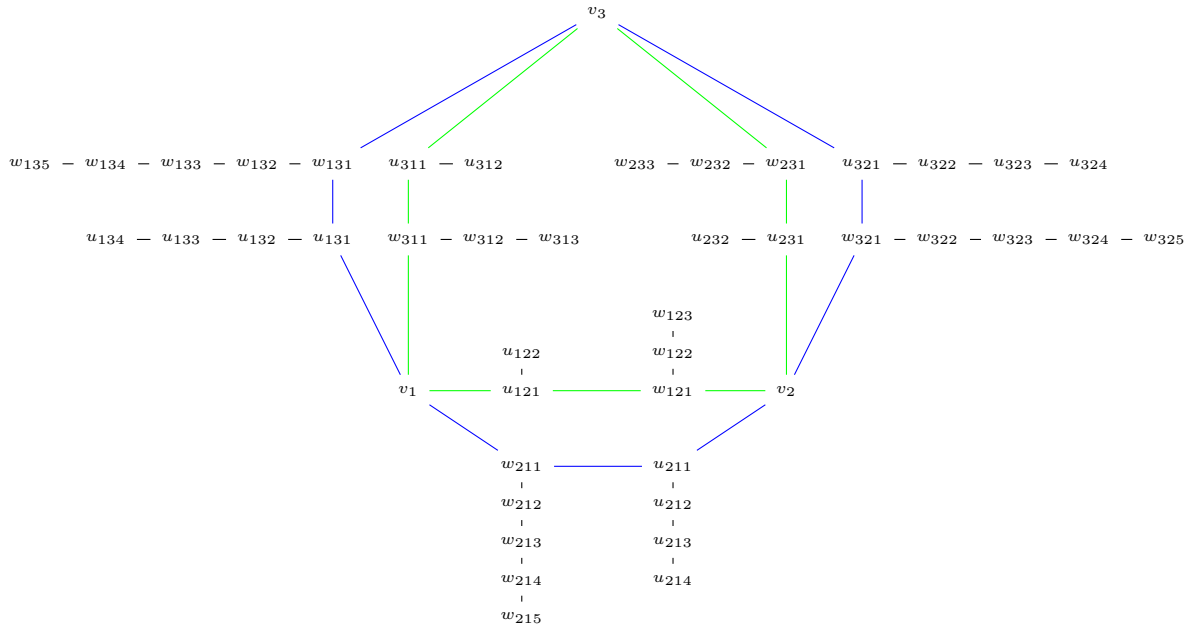
Der Beweis von Frucht ist konstruktiv. Das heisst, es wird ein Graph $\Gamma$ konstruiert, der die Gruppe $G$ als Automorphismengruppe besitzt. Zunächst werden die $n$ Gruppenelemente den Knoten eines Graphen folgendermaßen zugeordnet.

$$\begin{aligned} f : G &\longrightarrow V(\Gamma) = \{v_1, v_2, \cdots, v_n\} \\ g_i &\longmapsto v_i \\ 1 &\longmapsto v_1 \end{aligned}$$

Man konstruiert nun einen Cayleyschen Farbgraphen, indem je zwei Knoten $v_i, v_j$ durch gerichtete Kanten mit den Farben $f(g_i \cdot g_j^{-1})$ und $f(g_j \cdot g_i^{-1})$ verbunden werden. Dieser hat $n$ Knoten und $n(n-1)$ Kanten. Die Gruppenelemente beschreiben genau die Automorphismen des Cayleyschen Farbgraphen, bei denen Richtung und Farbe der Kanten erhalten bleiben.




Jede gerichtete Kante mit der Farbe $\nu$ wird nun ersetzt durch 3 ungerichtete Kanten, indem 2 neue Knoten eingefuegt werden. An den neuen Knoten werden nun neue, lineare Graphen der Länge $2\nu - 3$ beziehungsweise $2\nu - 2$ angefügt.




Nun muss noch gezeigt werden, dass der so entstehende Graph mit $n^2(2n-1)$ Knoten dieselbe Automorphismengruppe wie der Cayleysche Farbgraph also $G$ hat. Dies erfolgt in zwei Schritten. Eine Transformation des neuen Graphen, die einen Punkt $v_i$ des Cayleyschen Farbgraphen fest läßt, muss die Identität sein. Denn die Nachbarpunkte $u_{ij1}$ und $w_{ji1}$ können wegen der unterschiedlichen Längen der Fortsätze nicht vertauscht sondern müssen in sich abgebildet werden. Bei einer beliebigen Transformation kann ein Punkt $v_i$ nur in einen Punkt $v_j$ übergehen, da von diesem $2n-2$ Kanten ausgehen, von $u_{ijk}$ und $w_{ijk}$ jedoch jeweils höchstens 3. Frucht behandelt den Fall $n = 2$ dabei gesondert. Nun zeigt man, dass es nur eine Transformation gibt, die $v_i$ in $v_j$ überführt. □

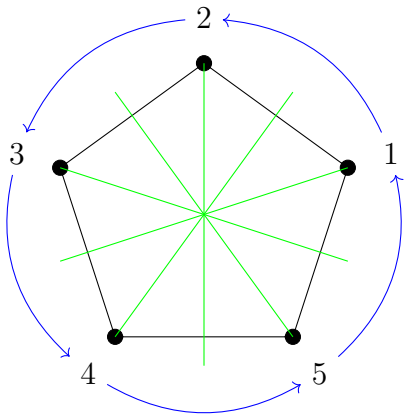
**Bemerkung 2.3.** Da sich die Automorphismengruppe eines Graphen nicht ändert, wenn man an alle Knoten des Graphen eine neue Kante zu einem neuen Knoten anfügt, gibt es sogar unendlich viele Graphen, die eine vorgegebene Gruppe als Automorphismengruppe besitzen.

**Beispiel 2.4.** Ein Fünfeck bildet einen zyklischen Graph $\Gamma_5$ mit den Ecken

$$V = \{1, 2, 3, 4, 5\}$$

und den Kanten

$$E = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 5\}, \{1, 5\}\}$$




Die Automorphismen des Graphen sind 5 Drehungen um jeweils $0°, 72°, 144°, 216°, 288°$ und 5 Spiegelungen an Achsen durch jeweils einen Knoten und den Mittelpunkt der gegenüberliegenden Kante. Die Automorphismengruppe des Graphen $\Gamma_5$ ist die Diedergruppe vom Grad 5.

Die Diedergruppen betrachten wir später für allgemeine $n \geq 3$.

## 2.2. Automorphismengruppe von algebraischen Strukturen

Eine Gruppe $G$ wirkt durch die Verknüpfung von links als natürlicher Operation auf sich selbst. Der Homomorphismus

$$\begin{aligned} \rho : G &\longrightarrow Sym(G) \\ g &\longmapsto \rho_g(h) = gh \end{aligned}$$

ist injektiv, denn

$$\begin{aligned} g \in Ker(\rho) &\Rightarrow \rho_g = id \\ &\Rightarrow \rho_g(h) = gh = h \quad \text{für alle } h \in G \\ &\Rightarrow g = 1 \end{aligned}$$

Damit erhalten wir als Folgerung den Satz von Cayley.

**Theorem 2.5.** *Satz von Cayley*
*Jede Gruppe ist isomorph zu einer Untergruppe einer symmetrischen Gruppe.*

**Bemerkung 2.6.** Wenn $G$ die Ordnung $n = |G|$ hat, dann ist eine Einbettung in die symmetrische Gruppe $S_n \simeq Sym(G)$ immer möglich. Die Ordnung $n!$ dieser symmetrischen Gruppe ist natürlich sehr viel größer als die Ordnung $n$ der Gruppe. Eine

interessante Frage ist, ob eine Einbettung auch in eine kleinere symmetrische Gruppe $S_m, m < n!$ möglich ist.

David Johnson hat in einem Artikel 1971 [Joh71] bewiesen, dass dies für folgende Gruppen nicht der Fall ist:

1. Kleinsche Vierergruppe $C_2 \times C_2$
   Denn $C_2 \times C_2$ läßt sich zwar in $S_4$ einbetten aber nicht in $S_3$. In $C_2 \times C_2$ haben alle Elemente die Ordnung 2, während in $S_3$ das Produkt von zwei Element der Ordnung 2 ein Element der Ordnung 3 ergibt.

2. Zyklische Gruppen mit einer Primzahlpotenz als Ordnung $C_{p^k}$
   Denn $C_p$ enthält nur Elemente der Ordnung $p$ und nach dem Satz von Lagrange 1.22 kann keine symmetrische Gruppe der Ordnung $k < p$ ein solches Element enthalten.

3. Verallgemeinerte Quaternionengruppen $Q_{2k}, k \geq 3$

Alle anderen Gruppen können in kleinere symmetrische Gruppen $S_m, m < n!$ eingebettet werden. Für den detaillierten Beweis sei auf den Artikel von David Johnson [Joh71] verwiesen.

### 2.2.1. Automorphismengruppen von Gruppen

Die Automorphismengruppe einer Gruppe $G$ besteht aus allen bijektiven Homomorphismen von der Gruppe auf sich selbst.

$$Aut(G) = \{\alpha : G \to G \text{ bijektiv und homomorph}\}$$

Wir betrachten nun folgenden Homomorphismus von der Gruppe $G$ in ihre Automorphismengruppe $Aut(G)$:

$$\begin{array}{rcl} c : G & \longrightarrow & Aut(G) \\ g & \longmapsto & \left\{ \begin{array}{rcl} c_g : G & \longrightarrow & G \\ h & \longmapsto & g \cdot h \cdot g^{-1} \end{array} \right. \end{array}$$

Der Kern von $c$ ist gegeben durch

$$Ker(c) = \{\, g \in G \,|\, c_g = id \,\}$$

Wegen

$$\begin{aligned} g \in Ker(c) &\iff c_g = id \\ &\iff c_g(h) = h \quad \text{für alle } h \in G \\ &\iff g \cdot h \cdot g^{-1} = h \quad \text{für alle } h \in G \\ &\iff g \cdot h = h \cdot g \quad \text{für alle } h \in G \end{aligned}$$

heisst das, dass $g$ im Zentrum $Z(G)$ liegt. Der Kern von $c$ stimmt also mit dem Zentrum überein.

$$Ker(c) = Z(G)$$

**Definition 2.7.** Das Bild $Im(c)$ der Abbildung $c$ enthält die inneren Automorphismen der Gruppe $G$.

$$Im(c) = Inn(g) \triangleleft Aut(G)$$

**Proposition 2.8.** *Die inneren Automorphismen sind ein Normalteiler in der Automorphismengruppe.*

**Definition 2.9.** Der Quotient

$$Out(G) = Aut(G)/Inn(G)$$

ist die Gruppe der äußeren Automorphismen.

**Bemerkung 2.10.** Die folgende Sequenz

$$1 \longrightarrow Z(G) \longrightarrow G \xrightarrow{c} Aut(G) \longrightarrow Out(G) \longrightarrow 1$$

ist exakt. Das heisst, das Bild einer Abbildung stimmt mit dem Kern der nachfolgenden Abbildung überein. Die Einbettung $Z(G) \longrightarrow G$ ist injektiv und die Projektion $Aut(G) \longrightarrow Out(G)$ ist natürlich surjektiv.

Wegen dieser Eigenschaften enthält die Automorphismengruppe viele Informationen über die Struktur der Gruppe. Die Automorphismengruppe ist aber auch wichtig für die Konstruktion neuer Gruppen mithilfe des semidirekten Produkts.

Wir betrachten nun die zyklische Gruppe $C_n$ der Ordnung $n$ und wollen ihre Automorphismengruppe bestimmen. Da $C_n$ kommutativ ist, stimmt die Gruppe mit ihrem Zentrum überein $Z(C_n) = C_n$.

**Theorem 2.11.** *Die Automorphismengruppe der zyklischen Gruppe $C_n$ ist isomorph zur Einheitengruppe von $\mathbb{Z}/n$.*

$$Aut(\mathbb{Z}/n) \cong (\mathbb{Z}/n)^* = \{\, 1 \le k \le n-1 \,|\, ggT(k,n) = 1 \,\}$$

*Die Anzahl der Automorphismen ist*

$$|\, Aut(\mathbb{Z}/n) \,| = \varphi(n)$$

*Wobei $\varphi(n)$ die Eulersche $\varphi$-Funktion ist.*

Die Eulersche $\varphi$-Funktion gibt an, wieviele zu $n$ teilerfremde positive natürliche Zahlen kleiner als $n$ es gibt.

$$\begin{aligned} \varphi : \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\longmapsto |\{\, a \in \mathbb{N} \,|\, 1 \le a \le n \ ,\ ggT(a,n) = 1 \,\}| \end{aligned}$$

Mit der Primzahlzerlegung der natürlichen Zahl $n$ erhalten wir:

$$\begin{aligned} n &= p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r} \\ \Rightarrow \quad \varphi(n) &= (p_1 - 1) \cdot p_1^{e_1 - 1} \cdot (p_2 - 1) \cdot p_2^{e_2 - 1} \cdots (p_r - 1) \cdot p_r^{e_r - 1} \\ \text{oder} \quad \varphi(n) &= n \cdot \prod_{p \mid n} \left(1 - \frac{1}{p}\right) \end{aligned}$$

*Beweis.* Wir betrachten einen beliebigen Automorphismus $\alpha$ und ein beliebiges Element $0 \neq a \in \mathbb{Z}/n$. Dann gilt

$$\begin{aligned} \alpha(a) &= \underbrace{\alpha(1 + 1 + \cdots + 1)}_{\text{a mal}} \\ &= \underbrace{\alpha(1) + \cdots + \alpha(1)}_{\text{a mal}} \\ &= a \cdot \alpha(1) \end{aligned}$$

Das heisst $\alpha$ ist durch den Wert $\alpha(1) = k$ vollständig bestimmt. $\alpha$ ist aber nicht für alle

$k$ injektiv.

$$\begin{aligned} \alpha \quad \text{ist injektiv} \quad &\Longleftrightarrow \quad Ker(\alpha) = \{0\} \\ &\Longleftrightarrow \quad \alpha(a) \neq 0 \quad \text{für alle } 0 \neq a \in \mathbb{Z}/n \\ &\Longleftrightarrow \quad a \cdot k \neq 0 \mod n \quad \text{für alle } 0 \neq a \in \mathbb{Z}/n\mathbb{Z} \\ &\Longleftrightarrow \quad ggT(k,n) = 1 \end{aligned}$$

□

**Korollar 2.12.** *Falls $n = p$ prim ist, dann gilt*

$$\begin{aligned} Aut(C_p) &= C_p^* \cong C_{p-1} \\ \mid Aut(C_p) \mid &= p-1 \end{aligned}$$

Die Automorphismengruppe der zyklischen Gruppe $C_n$ ist das Produkt der Automorphismengruppen der zyklischen Untergruppen $C_{p_i^{e_i}}$. Dabei ist $p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r} = n$ die Primfaktorzerlegung von $n$.

$$Aut(C_n) = Aut(C_{p_1^{e_1}}) \times \cdots \times Aut(C_{p_r^{e_r}})$$

**Theorem 2.13.** *Sei $n \in \mathbb{N}$ und $p \geq 3$ eine Primzahl. Dann hat die Automorphismengruppe der zyklischen Gruppe $C_{p^n}$ die Ordnung $p^n - p^{n-1}$ und ist zyklisch. Das heisst*

$$Aut(C_{p^n}) \cong (\mathbb{Z}/p^n)^*$$

*Beweis.* Nach Satz 2.11 folgt sofort

$$\mid Aut(C_p) \mid = \mid \{\, 1 \leq k \leq n-1 \mid ggT(k,n) = 1 \,\} \mid = \varphi(p^n)$$

Wobei die Eulersche $\varphi$-Funktion angibt, wieviele teilerfremde Zahlen es zu $p^n$ gibt, die kleiner sind als $p^n$. Da $p$ eine Primzahl ist, sind nur folgende Vielfache von $p$ kleiner $p^n$ nicht teilerfremd zu $p^n$:

$$1 \cdot p \ , \ 2 \cdot p \ , \ \cdots \ , \ p^{n-1} \cdot p = p^n$$

Das sind $p^{n-1}$ Zahlen. Also gilt

$$\mid Aut(C_p) \mid = p^n - p^{n-1}$$

Es bleibt nur zu zeigen, dass die Einheitengruppe $(\mathbb{Z}/p^n)^*$ zyklisch ist.

Die Beweisidee ist natürlich, ein Element der Ordnung $p^n - p^{n-1}$ in $(\mathbb{Z}/p^n)^*$ zu finden. Dies soll im einfachsten Fall $(p = 3, n = 2)$ veranschaulicht werden.

Wir betrachten also die Automorphismen der zyklischen Gruppe $C_9$. Die Einheitengruppe hat $6 = 3^2 - 3$ Elemente

$$(\mathbb{Z}/9)^* = \{1, 2, 4, 5, 7, 8\}$$

Nun betrachten wir den folgenden Homomorphismus der multiplikativen Gruppen

$$\begin{aligned} \beta : (\mathbb{Z}/9)^* &\longrightarrow (\mathbb{Z}/3)^* \\ a &\longmapsto a \mod 3 \end{aligned}$$

und erhalten als Kern

$$B = Ker(\beta) = \{1, 4, 7\}$$

Die Untergruppe $B$ ist Normalteiler in $(\mathbb{Z}/9)^*$, ist zyklisch und wird von 4 erzeugt.

$$B = \langle 4 \rangle$$

Denn

$$\begin{aligned} 4^2 = 16 &= 7 \mod 9 \\ 4^3 = 64 &= 1 \mod 9 \end{aligned}$$

Man hätte genausogut 7 nehmen können aber mit $4 = 1 + 3 = b$ klappt es immer. Aus diesem Erzeuger konstruieren wir einen Erzeuger $y$ für $(\mathbb{Z}/9)^*$ also ein Element der Ordnung 6. Dazu benötigen wir auch einen Erzeuger $a = 2$ von $(\mathbb{Z}/3)^* = \langle 2 \rangle$. Den gibt es, da $(\mathbb{Z}/3)^*$ zyklisch ist. Aus $2^2 = 4 = 1 \mod 3$ folgt $2^2 \in B$. Da $B$ zyklisch ist, ist folgende Abbildung ein Isomorphismus:

$$\begin{aligned} \varphi : B &\longrightarrow B \\ x &\longmapsto x^2 \end{aligned}$$

Denn $\varphi$ ist injektiv, da $x^2 = 1 \Rightarrow x = 1$. Und ein injektiver Homomorphismus endlicher Gruppen ist auch surjektiv. Daher gibt es ein $y \in B$ mit $y^2 = \frac{b}{a^2} = 4$.

Mit $z = y \cdot a$ haben wir einen Erzeuger von $(\mathbb{Z}/9)^*$ gefunden. Denn nach Konstruktion

gilt

$$\begin{aligned} z^{p-1} &= y^2 \cdot a^2 = b = 4 \mod 9 \\ (z^{p-1})^{p^{n-1}} &= b^3 = 4^3 = 64 = 1 \mod 9 \end{aligned}$$

Nun führen wir den Beweis für den allgemeinen Fall. Wir untersuchen also die Automorphismen der zyklischen Gruppe $C_{p^n}$. Nun betrachten wir den folgenden Homomorphismus der multiplikativen Gruppen

$$\begin{aligned} \beta : (\mathbb{Z}/p^n\mathbb{Z})^* &\longrightarrow (\mathbb{Z}/p\mathbb{Z})^* \\ a &\longmapsto a \mod p \end{aligned}$$

und erhalten als Kern

$$B = Ker(\beta) = \{1 + a_1 \cdot p + a_2 \cdot p^2 + \cdots + a_{n-1} \cdot p^{n-1} \mid 0 \leq a_i \leq p-1\}$$

$B$ hat $p^{n-1}$ Elemente. $B$ ist Normalteiler in $(\mathbb{Z}/p^n\mathbb{Z})^*$ und ist zyklisch mit Erzeuger $(1+p)$. Denn für $m \in \mathbb{N}$ gilt allgemein

$$\begin{aligned} (1+p)^{p^m} &= 1 + p^m \cdot p + \begin{pmatrix} p^m \\ 2 \end{pmatrix} \cdot p^2 \cdots \\ &= 1 \mod p^{m+1} \\ &\neq 1 \mod p^{m+2} \end{aligned}$$

Für $m = n-1$ ergibt sich, dass $(1+p)$ die Ordnung $p^{n-1}$ hat und somit ein Erzeuger von $B$ ist.

Aus diesem Erzeuger konstruieren wir einen Erzeuger $y$ für $(\mathbb{Z}/p^n\mathbb{Z})^*$ also ein Element der Ordnung $p^n - p^{n-1} = p^{n-1} \cdot (p-1)$. Dazu benötigen wir auch einen Erzeuger $a$ von $(\mathbb{Z}/p\mathbb{Z})^*$. Den gibt es, da $(\mathbb{Z}/p\mathbb{Z})^*$ zyklisch ist.

Da $a^{p-1} = 1 \mod p$, gilt $a^{p-1} \in B$. Da $B$ zyklisch ist, ist folgende Abbildung ein Isomorphismus:

$$\begin{aligned} \varphi : B &\longrightarrow B \\ x &\longmapsto x^{p-1} \end{aligned}$$

Denn $\varphi$ ist injektiv, da $x^{p-1} = 1 \Rightarrow x = 1$. Und ein injektiver Homomorphismus endlicher Gruppen ist auch surjektiv. Daher gibt es ein $y \in B$ mit $y^{p-1} = \frac{b}{a^{p-1}}$.

Mit $z = y \cdot a$ haben wir einen Erzeuger von $(\mathbb{Z}/p^n\mathbb{Z})^*$ gefunden. Denn nach Konstruktion gilt

$$\begin{aligned} z^{p-1} &= y^{p-1} \cdot a^{p-1} = b \\ (z^{p-1})^{p^{n-1}} &= b^{p^{n-1}} = 1 \mod p^n \end{aligned}$$

□

Der obige Satz gilt nicht für $p = 2$ wie folgendes Beispiel zeigt.

**Beispiel 2.14.** Wir betrachten $p = 2$ und $n = 3$ und untersuchen die Automorphismengruppe von $C_8$. Nach Satz 2.11 besteht diese aus allen Einheiten.

$$(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$$

Diese ist nicht zyklisch, da alle Elemente die Ordnung 2 haben.

$$\begin{aligned} 1^2 &= 1 \\ 3^2 &= 9 = 1 \mod 8 \\ 5^2 &= 25 = 1 \mod 8 \\ 7^2 &= 49 = 1 \mod 8 \end{aligned}$$

Daraus folgt, dass die Automorphismengruppe $Aut(C_8)$ isomorph zur Kleinschen Vierergruppe ist.

$$Aut(C_8) \simeq (\mathbb{Z}/8\mathbb{Z})^* \simeq C_2 \times C_2$$

**Theorem 2.15.** *1. Die Automorphismengruppe der zyklischen Gruppe $C_4$ ist*

$$Aut(C_4) \cong C_2$$

*2. Für $n \geq 3$ ist die Automorphismengruppe der zyklischen Gruppe $C_{2^n}$*

$$Aut(C_{2^n}) \cong C_2 \times C_{2^{(n-2)}}$$

*Beweis.* Wir können zwei Automorphismen direkt angeben:

$$\begin{aligned} \varphi_1 : C_{2^n} &\longrightarrow C_{2^n} \\ a &\longmapsto a^{-1} \\ \varphi_2 : C_{2^n} &\longrightarrow C_{2^n} \\ a &\longmapsto a^5 \quad \text{nur für } n \geq 3 \end{aligned}$$

$\varphi_1$ hat offensichtlich die Ordnung 2 und für $C_4$ ist die Aussage bewiesen. Für $C_{2^n}$ $n \geq 3$ erhalten wir den ersten Faktor $C_2 \simeq \langle \varphi_1 \rangle$. $\varphi_2$ hat die Ordnung $2^{(n-2)}$. Denn

$$\begin{aligned} \varphi_2^{(n-2)}(a) &= a^{5^{2^{(n-2)}}} \\ \Rightarrow \quad 5^{2^{(n-2)}} &= (1+4)^{2^{(n-2)}} \\ &= 1 + 4 \cdot 2^{(n-2)} + \cdots \\ &= 1 \mod 2^n \\ \Rightarrow \quad \varphi_2^{(n-2)}(a) &= a \\ \text{und} \quad \varphi_2^{(n-3)}(a) &= a^{5^{2^{(n-3)}}} \\ \Rightarrow \quad 5^{2^{(n-3)}} &= (1+4)^{2^{(n-3)}} \\ &= 1 + 4 \cdot 2^{(n-3)} + \cdots \\ &= 3 \mod 2^n \\ \Rightarrow \quad \varphi_2^{(n-3)}(a) &= a^3 \neq a \end{aligned}$$

Ausserdem kommutieren $\varphi_1$ und $\varphi_2$. Denn

$$(\varphi_1 \circ \varphi_2)(a) = \varphi_1(a^5) = a^{-5} = \varphi_1^5(a) = \varphi_2(\varphi_1(a))$$

Und für alle $b \in \mathbb{N}$ gilt

$$\varphi_2^b \neq \varphi_1$$

denn

$$\begin{aligned} 5^b &= -1 \mod 2^n \\ \Leftrightarrow \quad 1 &= -1 \mod 4 \; \lightning \end{aligned}$$

Somit erzeugen $\varphi_1$ und $\varphi_2$ insgesamt $2 \cdot 2^{(n-2)} = 2^{(n-1)}$ Automorphismen. Es kann aber

höchstens $2^{(n-1)}$ Automorphismen geben. Denn es gibt nur folgende Möglichkeiten:

$$\varphi_i : a \longmapsto a^i \quad 1 \leq i \leq 2^{(n-1)}$$

□

Im allgemeinen ist die Bestimmung der Automorphismengruppe einer Gruppe nicht so einfach. Für die symmetrischen Gruppen $S_n$ der Ordnung $n \geq 3$ ist die Gruppe der inneren Automorphismen wegen $Z(S_n) = 1$ isomorph zur Gruppe selbst.

$$Inn(S_n) \cong S_n$$

Für die äußeren Automorphismen der symmetrischen Gruppen $S_n$ mit $n \geq 3$ bewies Otto Hölder 1895 folgende Aussage.

**Theorem 2.16.** *Satz von Hölder 1895*
*Die Gruppe der äußeren Automorphismen einer symmetrischen Gruppe $S_n$ mit $n \geq 3$ ist gegeben durch*

$$Out(S_n) \cong \begin{cases} C_2 & \text{für} \quad n = 6 \\ 1 & \text{sonst} \end{cases}$$

Der Beweis ist etwas versteckt im Artikel [Höl95].

### 2.2.2. Semidirektes Produkt von Gruppen

**Definition 2.17.** Seien $N$ und $Q$ Gruppen und

$$\begin{aligned} \alpha : Q &\longrightarrow Aut(N) \\ q &\longmapsto \alpha_q : N \to N \end{aligned}$$

ein Homomorphismus. Dann heisst

$$N \rtimes_\alpha Q = \{ (n, q) \,|\, n \in N \,,\, q \in Q \}$$

mit der Verknüpfung

$$(n_1, q_1) \cdot (n_2, q_2) = (n_1 \cdot \alpha_{q_1}(n_2), q_1 \cdot q_2)$$

semidirektes Produkt.

Die Definition ist äqivalent zu folgender Eigenschaft.

**Proposition 2.18.** *Sei $N \triangleleft G$ Normalteiler in einer Gruppe $G$ und $Q = G/N$ die Quotientengruppe. Dann ist die Gruppe $G$ genau dann das semidirekte Produkt von $N$ und $Q$, wenn es einen Spalt-Homomorphismus*

$$s : Q \longrightarrow G$$

*gibt, so dass*

$$G = \{ n \cdot s(q) \,|\, n \in N, q \in Q \}$$

*und mit der Projektion $\pi : G \to Q$ gilt $\pi \circ s = id_Q$. Der Spalt-Homomorphismus induziert einen Homomorphismus*

$$\begin{array}{rcl} \alpha : Q & \longrightarrow & Aut(N) \\ q & \longmapsto & \left\{ \begin{array}{rcl} \alpha_q : N & \longrightarrow & N \\ n & \longmapsto & s(q) \cdot n \cdot s(q)^{-1} \end{array} \right. \end{array}$$

### 2.2.3. Diedergruppen

Wir betrachten ein regelmäßiges n-Eck als Graph $\Gamma_n$. Wie im Beispiel für $n = 5$ besteht die Automorphismengruppe von $\Gamma_n$ aus $n$ Drehungen und $n$ Spiegelungen. Man beachte, dass für gerade $n = 2m$ die Hälfte der Spiegelachsen durch zwei gegenüberliegende Eckpunkte geht und die andere Hälfte durch die Mitten gegenüberliegender Seiten.

$$Aut(\Gamma_n) = D_n$$

Die $n$ Drehungen bilden eine zyklische Untergruppe $C_n \triangleleft D_n$, die sogar ein Normalteiler in $D_n$ ist. Der Quotient $D_n/C_n = C_2$ besteht aus der Identität und einer Spiegelung. Dies ist ein Beispiel für ein semidirektes Produkt

$$D_n = C_n \rtimes C_2$$

Damit sind Diedergruppen Automorphismengruppen von zyklischen Graphen oder regelmäßigen Vielecken und ein Spezialfall von semidirekten Produkten.

# 3. Anwendungen in Gruppentheorie, Algebra und Kombinatorik

## 3.1. Sylow-Sätze

Der norwegische Mathematiker Ludwig Sylow bewies 1872 weitreichende Aussagen über Untergruppen einer Gruppe.

Bevor wir die Sylow-Sätze beweisen, betrachten wir noch zwei Eigenschaften von Binomialkoeffizienten.

**Lemma 3.1.** *Im Polynomring über den ganzen Zahlen $\mathbb{Z}[X]$ gilt für jede Primzahl $p$*

$$(1+x)^p \equiv 1 + x^p \mod p$$

*Das heisst*

$$\binom{p}{k} \equiv 0 \mod p \quad \textit{für alle } 1 \leq k \leq p-1$$

*Allgemeiner gilt*

$$(1+x)^{p^n} \equiv 1 + x^{p^n} \mod p$$

*und*

$$(1+x)^{p^n k} \equiv 1 + k \cdot x^{p^n} \mod p$$

*Beweis.* Für $1 \leq k \leq p-1$ taucht $p$ genau einmal im Zähler des Binomialkoeffizienten auf.

$$\binom{p}{k} = \frac{p \cdot (p-1) \cdots (p-k+1)}{k \cdot (k-1) \cdots 1}$$

Denn alle anderen Faktoren im Zähler sind kleiner als $p$. Da $k \leq p-1$ vorausgesetzt ist, gibt es keinen Faktor $p$ im Nenner. Somit gibt es in der Primfaktorzerlegung von $\binom{p}{k}$ genau einen Faktor $p$.

Wiederholte Anwendung der Formel für $(1+x)^p$ ergibt:

$$\begin{aligned} (1+x)^p &\equiv 1 + x^p \mod p \\ (1+x)^{p^2} &\equiv 1 + x^{p^2} \mod p \\ \cdots &\quad \cdots \\ (1+x)^{p^n} &\equiv 1 + x^{p^n} \mod p \end{aligned}$$

Analog erhalten wir

$$\begin{aligned}(1+x)^{p^n k} &\equiv ((1+x)^{p^n})^k \mod p \\ &\equiv (1+x^{p^n})^k \mod p \\ &\equiv 1 + k \cdot x^{p^n} \mod p\end{aligned}$$

□

**Theorem 3.2.** *Lucas Theorem*
*Sei $p \in \mathbb{P}$ eine Primzahl und*

$$\begin{aligned}n &= \sum_{i=0}^{r} n_i \cdot p^i \\ k &= \sum_{i=0}^{r} k_i \cdot p^i\end{aligned}$$

*die p-adischen Entwicklungen von n und k. Dann gilt*

$$\binom{n}{k} \equiv \prod_{i=0}^{r} \binom{n_i}{k_i} \mod p$$

*Beweis.* Der Beweis folgt dem Artikel von 1947 von Fine [Fin47]. Nach dem Einsetzen der $p$-adischen Entwicklung von $n$ erhält man aus $(1+x)^n$ ein Produkt aus $(1+x)^{n_i \cdot p^i} \equiv (1+x^{p^i})^{n_i} \mod p$ nach Lemma 3.1. Die Faktoren sind für jedes $i$ Polynome in $x^{p^i}$ vom Grad kleiner als $p$. Nach dem Ausmultiplizieren sammelt man die Koeffizienten der Monome $x^k$ und erhält die Behauptung.

$$\begin{aligned}\sum_{k=0}^{n} \binom{n}{k} x^k &= (1+x)^n \\ &= \prod_{i=0}^{r} \left((1+x)^{p^i}\right)^{n_i} \\ &\equiv \prod_{i=0}^{r} \left(1+x^{p^i}\right)^{n_i} \mod p \\ &= \prod_{i=0}^{r} \left( \sum_{j_i=0}^{n_i} \binom{n_i}{j_i} x^{j_i \cdot p^i} \right) \\ &= \prod_{i=0}^{r} \left( \sum_{j_i=0}^{p-1} \binom{n_i}{j_i} x^{j_i \cdot p^i} \right)\end{aligned}$$

Ausmultiplizieren ergibt

$$\begin{aligned}
&= \sum \Big( \prod_{i=0}^{r} \binom{n_i}{j_i} \cdot \underbrace{\prod_{i=0}^{r} x^{j_i \cdot p^i}}_{!= x^k} \Big) \\
&= \sum_{k=0}^{n} \Big( \sum_{\sum_{i=0}^{r} j_i \cdot p^i = k} \prod_{i=0}^{r} \binom{n_i}{j_i} \Big) x^k \\
&= \sum_{k=0}^{n} \Big( \prod_{i=0}^{r} \binom{n_i}{k_i} \Big) x^k
\end{aligned}$$

Denn die innere Summe $\sum_{\sum_{i=0}^{r} j_i \cdot p^i = k}$ über alle $\{j_0, \cdots, j_r\}$ mit $\sum_{i=0}^{r} j_i \cdot p^i = k$ mit $0 \leq j_i \leq n_i < p$ besteht aus einem Summanden, da die $p$-adische Entwicklung eindeutig ist. Somit gilt $j_i = k_i$. □

**Beispiel 3.3.** Mit Hilfe des Lucas Theorems kann leicht festgestellt werden, ob ein Binomialkoeffizient durch eine Primzahl $p$ teilbar ist. Insbesondere kann durch die binäre Darstellung ermittelt werden, ob ein Binomialkoeffizient gerade oder ungerade ist. Der Binomialkoeffizient $\binom{1023}{31}$ ist ungerade. Denn es gilt:

$$\begin{aligned}
\binom{1023_{(10)}}{31_{(10)}} &= \binom{1\,1\,1\,1\,1\,1\,1\,1\,1\,1_{(2)}}{0\,0\,0\,0\,1\,1\,1\,1\,1_{(2)}} \quad \text{in binärer Darstellung} \\
&\equiv \binom{1}{0}^4 \cdot \binom{1}{1}^5 \mod 2 \\
&= 1 \mod 2
\end{aligned}$$

Modulo 2 hat das Pascalsche Dreieck folgende Struktur:

$$\begin{array}{ccccccccccccccc}
 & & & & & & & 1 & & & & & & & \\
 & & & & & & 1 & & 1 & & & & & & \\
 & & & & & 1 & & 0 & & 1 & & & & & \\
 & & & & 1 & & 1 & & 1 & & 1 & & & & \\
 & & & 1 & & 0 & & 0 & & 0 & & 1 & & & \\
 & & 1 & & 1 & & 0 & & 0 & & 1 & & 1 & & \\
 & 1 & & 0 & & 1 & & 0 & & 1 & & 0 & & 1 &
\end{array}$$

**Definition 3.4.** Sei $G$ eine Gruppe mit der Ordnung $|G| = p^a \cdot m$ mit $p, a, m \in \mathbb{N}$, $p$ eine

Primzahl und $p$ kein Teiler von $m$. Dann heisst eine Untergruppe $U$ der Ordnung $p^a$ $p$-Sylow-Untergruppe. Alle $p$-Sylow-Untergruppen werden unter

$$Syl_p(G) = \{\ U < G \mid |U| = p^a\ \}$$

zusammengefaßt. Ihre Anzahl wird mit

$$n_p = |\,Syl_p(G)\,|$$

bezeichnet.

**Theorem 3.5.** *Satz von Sylow*
*Sei $G$ eine Gruppe mit der Ordnung $|G| = p^a \cdot m$ mit $p, a, m \in \mathbb{N}$, $p$ eine Primzahl und $p$ kein Teiler von $m$. Dann gilt:*

*a) Es gibt $p$-Sylow-Untergruppen.*

*b) Sei $U$ eine $p$-Sylow-Untergruppe und $V \leq G$ eine Untergruppe der Ordnung $p^b$. Dann ist $V$ eine Untergruppe in einer zu $U$ konjugierten Gruppe. Das heisst, es existiert ein $g \in G$ mit $V \leq gUg^{-1}$.*
*Für $b = a$ folgt hieraus insbesondere, dass zwei $p$-Sylow-Untergruppen konjugiert und damit isomorph zueinander sind.*

*c) Für die Anzahl $n_p$ der $p$-Sylow-Untergruppen gilt:*

$$n_p = 1 \mod p$$

*d) Die Anzahl $n_p$ der $p$-Sylow-Untergruppen teilt $m$.*

$$n_p \mid m$$

*Beweis.* ad a) Wir betrachten die Menge $\Omega$ aller $p^a$-elementigen Teilmengen von $G$.

$$\Omega = \{\ S \subset G \mid |S| = p^a\ \}$$

Nach dem Lucas Theorem 3.2 gilt für die Größe von $\Omega$

$$|\,\Omega\,| = \binom{p^a m}{p^a} \equiv m \mod p$$

Nach Voraussetzung ist also $p$ kein Teiler der Größe von $\Omega$. Die Gruppe $G$ wirkt auf $\Omega$ durch Links-Multiplikation

$$g \circ S = \{\ g \cdot s \mid s \in S\ \}$$

Mit der Kürzungsregel folgt, dass alle Mengen $g \circ S$ dieselbe Anzahl von Elementen haben.

$$|\, g \circ S \,| = p^a \quad \text{für alle } g \in G$$

Die Orbits bilden eine Zerlegung von $\Omega$ mit den Repräsentanten $S_i$.

$$\Omega = \bigsqcup_i G \circ S_i$$

Für ein gegebenes $i$ überdecken die Mengen $g \circ S_i$ die Gruppe $G$:

$$G = \bigcup_{g \in G} g \circ S_i$$

Denn sei $x \in G$. Dann wählen wir ein $y \in S_i$ und $g = xy^{-1} \in G$. Wegen $gy = x$ gilt $x \in g \circ S_i$.

Nun gibt es ein $S_0 \in \Omega$, dessen Bahngröße nicht durch $p$ teilbar ist. Da alle Bahnen disjunkt oder gleich sind und $\Omega$ überdecken, würde sonst für alle $S \in \Omega$ gelten:

$$\begin{aligned} & p \mid |G \circ S| \\ \Rightarrow\ & p \mid |\Omega| \\ \Rightarrow\ & p \mid \binom{p^a m}{p^a} \equiv m \mod p \end{aligned}$$

im Widerspruch zur Voraussetzung.

Der Stabilisator von diesem $S_0$

$$G_{S_0} = \{\ g \in G \mid g \circ S_0 = S_0\ \}$$

ist eine $p$-Sylow-Untergruppe. Denn es gilt:

$$\left.\begin{aligned} p \nmid |G \circ S_0| \\ |G \circ S_0| \mid |G| = p^a m \end{aligned}\right\} \Rightarrow |G \circ S_0| = m$$

Daraus folgt:

$$\begin{aligned} |\, G_{S_0} \,| &= \frac{|\, G \,|}{|\, G \circ S_0 \,|} \\ &= \frac{p^a m}{m} \\ &= p^a \end{aligned}$$

ad b) Sei $U \leq G$ eine $p$-Sylow-Untergruppe, also $|\, U \,| = p^a$. Die Untergruppe $V \leq G$ wirkt auf die Menge der Nebenklassen $\{\, G/U \,\}$ per Linksmultiplikation $v \circ (xU) = (v \cdot x)U$. Die Anzahl der Nebenklassen ist nach Voraussetzung $|\, G/U \,| = m$. Für die Größen der Bahnen und Standgruppen gilt

$$p^b = |\, V \,| = |\, \text{Bahn} \,| \cdot |\, \text{Standgruppe} \,|$$

Alle Standgruppen sind aber Untergruppen in $V$ und haben daher die Ordnung $p^c$ und damit haben die Bahnen $p^{b-c}$ Elemente.
Da die Bahnen eine Zerlegung von $\{\, G/U \,\}$ bilden und $p$ kein Teiler von $m$ ist, muss es mindestens eine Bahn der Länge 1 geben. Also gibt es ein $g \in G$ mit

$$\begin{aligned} v \circ gU &= gU \quad \text{für alle } v \in V \\ \Rightarrow \quad Vg &\subseteq gU \\ \Rightarrow \quad V &\leq gUg^{-1} \end{aligned}$$

ad c) Nach Aussage b) wissen wir, dass alle $p$-Sylow-Untergruppen konjugiert sind. Wir wählen eine $p$-Sylow-Untergruppe $U$ aus. Dann gilt:

$$\begin{aligned} Syl_p(G) &= \{\, V < G \mid |\, V \,| = p^a \,\} \\ &= \{\, gUg^{-1} \mid g \in G \,\} \end{aligned}$$

Die ausgezeichnete $p$-Sylow-Untergruppe $U$ operiert auf $Syl_p(G)$ durch Konjugation. Die Bahn durch $gUg^{-1}$ bezeichnen wir kürzer mit

$$Ug = \{\, ugUg^{-1}u^{-1} \mid u \in U \,\}$$

Der Stabilisator ist

$$U_g = \{\, u \in U \mid ugUg^{-1}u^{-1} = gUg^{-1} \,\}$$

Und es gilt

$$\begin{aligned} |Ug| &= \frac{|U|}{|U_g|} \\ &= \begin{cases} 1 & \text{falls} \quad gUg^{-1} = U \\ c \cdot p & \text{falls} \quad gUg^{-1} \neq U \end{cases} \end{aligned}$$

Da zwei Bahnen entweder disjunkt oder gleich sind, kann es nur eine einelementige Bahn durch $U$ geben. Die Anzahl der Elemente in den anderen Bahnen sind durch $p$ teilbar. Somit erhalten wir

$$\begin{aligned} n_p &= |Syl_p(G)| \\ &\equiv 1 \mod p \end{aligned}$$

ad d) Nun betrachten wir die Wirkung von $G$ auf $Syl_p(G)$ durch Konjugation. Wegen Aussage b) ist diese transitiv, es gibt also nur eine Bahn. Und diese stimmt mit $Syl_p(G)$ überein. Der Stabilisator sei $G_U$. Dann gilt

$$\begin{aligned} |G| &= |Syl_p(G)| \cdot |G_U| \\ p^a \cdot m &= n_p \cdot |G_U| \\ \Rightarrow \quad n_p &\mid m \end{aligned}$$

Denn nach Aussage c) kann $n_p$ kein Vielfaches von $p$ sein.

□

**Lemma 3.6.** *Sei $P \leq G$ eine Sylowuntergruppe in $G$. Dann ist der Normalisator von $P$ in $G$ der Stabilisator von $P$ unter der Konjugation auf $Syl_p(G)$*

$$N_G(P) = \{ g \in G \mid gP = Pg \} = G_P$$

*und es gilt*

$$n_p(G) = \frac{|G|}{|N_G(P)|}$$

*Beweis.* Die erste Aussage folgt direkt aus der Definition des Normalisators 1.58. Die Formel für die Anzahl der $p$-Sylowuntergruppen folgt aus dem Bahn-Standgruppen-Satz 1.53. □

**Beispiel 3.7.** In diesem Beispiel werden mit Hilfe des Satzes von Sylow Gruppen der

Ordnung 15 untersucht. 15 hat 2 Primteiler.

$$|\,G\,| = 15 = 3 \cdot 5$$

Nach dem Satz von Sylow 3.5 gibt es eine 3-Sylow-Untergruppe. Diese ist eindeutig. Denn es gilt:

$$n_3 \,|5 \text{ und } n_3 = 1 \mod 3 \quad \Rightarrow n_3 = 1$$

Die 3-Sylow-Untergruppe ist ein Normalteiler und hat 2 Elemente der Ordnung 3 und ist isomorph zur zyklischen Gruppe $C_3$.

Es gibt auch genau eine 5-Sylow-Untergruppe. Denn nach dem Satz von Sylow 3.5 gilt:

$$n_5 | 3 \text{ und } n_5 = 1 \mod 5 \quad \Rightarrow n_5 = 1$$

Diese ist ein Normalteiler und hat 4 Elemente der Ordnung 5 und ist isomorph zur zyklischen Gruppe $C_5$.

Also ist jede Gruppe $G$ der Ordnung 15 abelsch und hat 8 Elemente der Ordnung 15. $G$ hat die Darstellung

$$G \simeq C_3 \times C_5 = C_{15}$$

## 3.2. Verlagerungssatz von Burnside

**Definition 3.8.** Sei $G$ eine Gruppe und $H < G$ eine Untergruppe. Der Kommutator von $H$ ist definiert durch

$$[H,H] = \langle\, [a,b] = aba^{-1}b^{-1} \,|\, a,b \in H \,\rangle$$

Die Abelisierung von $H$ ist die Faktorgruppe von $H$ mit der aus dem Kommutator $[H,H]$ erzeugten Untergruppe.

$$H^{ab} = H/\langle [H,H] \rangle$$

**Definition 3.9.** Burnside-Verlagerungsabbildung
Sei $G$ eine Gruppe und $H < G$ eine Untergruppe und $x_1, \cdots, x_n$ Vertreter der Linksnebenklassen $G/H$ mit

$$G = \bigcup_{i=1}^{n} x_i \cdot H$$

Für jedes $y \in G$ und jedes $i \in \{1, \cdots, n\}$ ist $y \cdot x_i \in x_j \cdot H$. Daher gibt es $h_i = h_i(y) \in H$, so

dass folgendes gilt:

$$y \cdot x_i = x_{\sigma(i)} \cdot h_i(y) \quad \text{mit } \sigma(i) = j$$

Dann heisst ist eine Abbildung

$$\begin{aligned} T_{G,H} : G &\longrightarrow H^{ab} \\ y &\longmapsto \prod_{i=1}^{n} h_i \end{aligned}$$

Burnside-Verlagerungsabbildung.

**Satz 3.10.** *Die Burnside-Verlagerungsabbildung ist wohl definiert.*

*Beweis.* Wir müssen zeigen, dass $h_1(y) \cdot \cdots \cdot h_n(y) \in H^{ab}$ unabhängig von der Wahl der Vertreter $x_1, \cdots, x_n$ ist.
Zunächst zeigen wir, dass $\sigma$ eine Permutation ist. Für $\sigma(i) = \sigma(j)$ gilt mit $h_i = h_i(y)$

$$\begin{aligned} x_i^{-1} \cdot x_j &= x_i^{-1} \cdot y^{-1} \cdot y \cdot x_j \\ &= (y \cdot x_i)^{-1} \cdot (y \cdot x_j) \\ &= (x_{\sigma_i} \cdot h_i)^{-1} \cdot x_{\sigma_j} \cdot h_j \\ &= h_i^{-1} \cdot \underbrace{x_{\sigma_i}^{-1} \cdot x_{\sigma_j}}_{=e} \cdot h_j \quad \text{da } \sigma(i) = \sigma(j) \\ &= h_i^{-1} \cdot h_j \\ &\in H \\ \Rightarrow \quad x_i \cdot H &= x_j \cdot H \\ \Rightarrow \quad i &= j \end{aligned}$$

Seien nun $z_1, \cdots, z_n$ andere Vertreter von $G/H$ und

$$y \cdot z_i = z_{\pi(i)} \cdot g_i \quad \text{mit } g_i = g_i(y) \tag{*}$$

Da $G = \bigcup_{i=1}^{n} x_i \cdot H$ gilt, folgt

$$z_i = x_{\tau(i)} \cdot \tilde{h}_i$$

und $\sigma$, $\pi$ und $\tau$ sind Permutationen. Mit $(\tau^{-1} \cdot \sigma \cdot \tau)(i)$ anstelle von $i$ folgt:

$$\begin{aligned} z_{(\tau^{-1}\cdot\sigma\cdot\tau)(i)} &= x_{(\sigma\cdot\tau)(i)} \cdot \tilde{h}_{(\tau^{-1}\cdot\sigma\cdot\tau)(i)} \\ y \cdot z_i &= y \cdot x_{\tau(i)} \cdot \tilde{h}_i \\ &= x_{(\sigma\cdot\tau)(i)} \cdot h_{\tau(i)} \cdot \tilde{h}_i \\ &= z_{(\tau^{-1}\cdot\sigma\cdot\tau)(i)} \cdot \tilde{h}^{-1}_{(\tau^{-1}\cdot\sigma\cdot\tau)(i)} \cdot h_{\tau(i)} \cdot \tilde{h}_i \end{aligned}$$

Ein Vergleich mit Gleichung (*) liefert:

$$\begin{aligned} \pi &= \tau^{-1} \cdot \sigma \cdot \tau \\ g_i &= \tilde{h}^{-1}_{(\tau^{-1}\cdot\sigma\cdot\tau)(i)} \cdot h_{\tau(i)} \cdot \tilde{h}_i \end{aligned}$$

Daraus folgt

$$\begin{aligned} \prod_{i=1}^{n} g_i &= \prod_{i=1}^{n} \tilde{h}^{-1}_{(\tau^{-1}\cdot\sigma\cdot\tau)(i)} \cdot \prod_{i=1}^{n} h_{\tau(i)} \cdot \prod_{i=1}^{n} \tilde{h}_i \\ &= \prod_{i=1}^{n} h_{\tau(i)} \end{aligned}$$

□

**Satz 3.11.** *Sei $G$ eine Gruppe und $H < G$ eine Untergruppe. Die Verlagerungsabbildung*

$$\begin{aligned} T_{G,H} : G &\longrightarrow H^{ab} \\ y &\longmapsto \prod_{i=1}^{n} h_i \end{aligned}$$

*ist ein Homomorphismus.*

*Beweis.* Seien $y, z \in G$ und

$$\begin{aligned} y \cdot x_i &= x_{\sigma(i)} \cdot h_i \\ z \cdot x_i &= x_{\tau(i)} \cdot g_i \end{aligned}$$

mit Permutationen $\sigma$ und $\tau$. Dann gilt

$$\begin{aligned} y \cdot z \cdot x_i &= y \cdot x_{\tau(i)} \cdot g_i \\ &= x_{(\sigma\cdot\tau)(i)} \cdot h_{\tau(i)} \cdot g_i \end{aligned}$$

Daraus folgt

$$\begin{aligned} \prod_{i=1}^{n} h_{\tau(i)} \cdot g_i &= \prod_{i=1}^{n} h_i \cdot \prod_{i=1}^{n} g_i \\ \Rightarrow \quad T(y \cdot z) &= T(y) \cdot T(z) \end{aligned}$$

□

**Lemma 3.12.** *Sei $G$ eine Gruppe und $H < G$ eine Untergruppe, $x_1, \cdots, x_n$ Vertreter der Linksnebenklassen $G/H$ mit*

$$G = \bigcup_{i=1}^{n} x_i \cdot H$$

*$\sigma \in S_n$ sei eine zyklische Permutation der Ordnung $k$ und es gelte*

$$y \cdot x_i = x_{\sigma(i)} \cdot h_i$$

*Dann gilt*

$$\begin{aligned} x_1^{-1} \cdot y^k \cdot x_1 &\in H \\ x_1^{-1} \cdot y^m \cdot x_1 &\notin H \quad \textit{für alle } m < k \end{aligned}$$

*Beweis.* Nach einer Umnummerierung ist $\sigma = (1, 2, \cdots, k)$ und wir erhalten

$$\begin{aligned} y \cdot x_1 &= x_2 \cdot h_1 \\ y \cdot x_2 &= x_3 \cdot h_2 \\ &\cdots \\ y \cdot x_{k-1} &= x_k \cdot h_{k-1} \\ y \cdot x_k &= x_1 \cdot h_k \\ \Rightarrow \quad h_k \cdot h_{k-1} \cdots h_1 &= x_1^{-1} \cdot y \cdot \underbrace{x_k \cdot h_{k-1}}_{=y \cdot x_{k-1}} \cdot h_{k-2} \cdots h_1 \\ &= x_1^{-1} \cdot y^2 \cdot \underbrace{x_{k-1} \cdot h_{k-2}}_{=y \cdot x_{k-2}} \cdot h_{k-3} \cdots h_1 \\ &\cdots \\ &= x_1^{-1} \cdot y^k \cdot x_1 \\ &\in H \end{aligned}$$

Für $m < k$ erhalten wir

$$\begin{aligned} x_1^{-1} \cdot y^m \cdot x_1 &= x_1^{-1} \cdot x_{m+1} \cdot x_{m+1}^{-1} \cdot y^m \cdot x_1 \\ &= x_1^{-1} \cdot x_{m+1} \cdot \underbrace{h_m \cdots h_1}_{\in H} \\ &\notin H \quad \text{da } x_1^{-1} \cdot x_{m+1} \notin H \end{aligned}$$

□

Als Folgerung erhalten wir folgende Beschreibung der Verlagerungsabbildung.

**Korollar 3.13.** *Sei $G$ eine Gruppe und $H < G$ eine Untergruppe, $x_1, \cdots, x_n$ Vertreter der Linksnebenklassen $G/H$ mit*

$$G = \bigcup_{i=1}^{n} x_i \cdot H$$

*Dann gibt es eine Teilmenge $\{z_1, \cdots, z_r\} \subseteq \{x_1, \cdots, x_n\}$ und $n_1, \cdots, n_r$, so dass die Verlagerungsabbildung folgende Darstellung hat:*

$$\begin{aligned} T : G &\longrightarrow H^{ab} \\ y &\longmapsto T(y) = \prod_{i=1}^{r} z_i^{-1} \cdot y^{n_i} \cdot z_i \end{aligned}$$

*wobei $n_i$ minimal sind mit*

$$z_i^{-1} \cdot y^{n_i} \cdot z_i \in H$$

**Lemma 3.14.** *Sei $G$ eine Gruppe und $P \in Syl_p(G)$ eine $p$-Sylowuntergruppe, die Elemente $x, y \in C_G(P)$ im Zentralisator von $P$ seien konjugiert in $G$. Dann sind $x, y$ auch konjugiert im Normalisator $N_G(P)$.*

*Beweis.* Sei $x \in C_G(P)$. Dann gibt es für das konjugierte $y$ ein $h \in G$ mit

$$y = h \cdot x \cdot h^{-1}$$

Für alle $b \in P$ gilt

$$\begin{aligned} y \cdot (h \cdot b \cdot h^{-1}) \cdot y^{-1} &= h \cdot x \cdot h^{-1} \cdot h \cdot b \cdot h^{-1} \cdot h \cdot x^{-1} \cdot h^{-1} \\ &= h \cdot \underbrace{x \cdot b \cdot x^{-1}}_{= b} \cdot h^{-1} \quad \text{da } x \in C_G(P) \\ &= h \cdot b \cdot h^{-1} \end{aligned}$$

Das heisst $y$ kommutiert mit allen Elementen aus $h \cdot P \cdot h^{-1}$. Also sind $P$ und $h \cdot P \cdot h^{-1}$ $p$-Sylowuntergruppen von

$$C_G(y) = \{ a \in G \mid a \cdot y = y \cdot a \} = C_G(\langle y \rangle)$$

Wir wenden den Satz von Sylow 3.5 auf $C_G(\langle y \rangle)$ an. Danach gibt es ein $g \in C_G(\langle y \rangle)$, so dass gilt:

$$\begin{aligned} g \cdot (h \cdot P \cdot h^{-1}) \cdot g^{-1} &= P \\ (g \cdot h) \cdot P \cdot (g \cdot h)^{-1} &= P \\ \Rightarrow \quad g \cdot h &\in N_G(P) \end{aligned}$$

Also gibt es für $x \in G$ ein Element $g \cdot h \in N_G(P)$, so dass gilt:

$$\begin{aligned} (g \cdot h) \cdot x \cdot (g \cdot h)^{-1} &= g \cdot (\underbrace{h \cdot x \cdot h^{-1}}_{= y}) \cdot g^{-1} \\ &= y \quad \text{da } g \in C_G(y) \end{aligned}$$

Somit sind $x$ und $y$ auch konjugiert in $N_G(P)$. □

**Theorem 3.15.** *Burnside-Verlagerungssatz*
*Sei $G$ eine endliche Gruppe und $P \in Syl_p(G)$ eine $p$-Sylowuntergruppe, deren Zentralisator mit dem Normalisator übereinstimmt.*

$$C_G(P) = N_G(P)$$

*Dann gibt es einen Normalteiler $N \lhd G$, so dass $G$ ein semidirektes Produkt aus $N$ und $P$ ist.*

$$G = N \rtimes P$$

*Beweis.* $P$ ist Normalteiler in $N_G(P) = C_G(P)$. Also ist $P$ abelsch und es gilt

$$P = C_G(P) = N_G(P)$$

Sei $e \neq y \in P$. Dann existieren $z_1, \cdots, z_r \in G$, so dass die Verlagerungsabbildung folgende Form hat:

$$T(y) = \prod_{i=1}^{r} z_i^{-1} \cdot y^{n_i} \cdot z_i$$

mit $n_i$ minimal, so dass $z_i^{-1} \cdot y^{n_i} \cdot z_i \in P$.
Daraus folgt, dass $z_i^{-1} \cdot y^{n_i} \cdot z_i$ und $y^{n_i}$ konjugiert in $G$ sind. Nach Lemma 3.14 sind sie

auch konjugiert in $P = N_G(P)$. Also existieren $x_1, \cdots, x_r \in P$, so dass gilt

$$x_i^{-1} \cdot y^{n_i} \cdot x_i = z_i^{-1} \cdot y^{n_i} \cdot z_i$$

Damit erhält man

$$\begin{aligned} T(y) &= \prod_{i=1}^{r} z_i^{-1} \cdot y^{n_i} \cdot z_i \\ &= \prod_{i=1}^{r} \underbrace{x_i^{-1} \cdot y^{n_i} \cdot x_i}_{\in P} \\ &= \prod_{i=1}^{r} y^{n_i} \quad \text{da } P \text{ abelsch} \\ &= y^n \quad \text{mit } n = \sum_{i=1}^{r} n_i \\ &\neq e \quad \text{denn } n \nmid p^k \end{aligned}$$

Daraus folgt, dass $T : P \longrightarrow P$ injektiv ist und $Ker(T) = N \lhd G$ ist der gesuchte Normalteiler mit $N \cap P = \{e\}$. Somit ist

$$G = N \rtimes P$$

□

## 3.3. Kranzprodukt

Für die Konstruktion von Gruppen aus kleineren Gruppen gibt es verschiedene Möglichkeiten. In Abschnitt 2.2.2 haben wir das semidirekte Produkt definiert, bei dem die Verknüpfung auf der ersten Komponente über einen Automorphismus auf der ersten Komponente definiert ist.

Bei dem Kranzprodukt, das wir nun einführen wollen, wird dieser Automorphismus von einer Permutationsdarstellung der zweiten Komponente induziert. Wir betrachten die Gruppen $H$ und $Q$ und eine Permutationsdarstellung $\rho : Q \curvearrowright X$ vom Grad $n = |X| \neq 0$. Alle Abbildungen von $X$ nach $H$ bilden eine Gruppe, die isomorph zum $n$-fachen Produkt von $H$ ist.

$$\begin{aligned} H^X &= \{ h : X \to H \} \\ &\cong \underbrace{H \times H \times \cdots \times H}_{n \ mal} \end{aligned}$$

Die Wirkung $\rho$ von $G$ auf $X$ kann auf $H^X$ fortgesetzt werden.

$$\begin{array}{rcl} Q \times H^X & \longrightarrow & H^X \\ (q,h) & \longmapsto & \left\{ \begin{array}{rcl} q \circ h : X & \to & H \\ x & \mapsto & h(q^{-1}x) \end{array} \right. \end{array}$$

Somit ist jedem $q \in Q$ ein Automorphismus auf $H^X$ zugeordnet und wir erhalten einen Homomorphismus von $Q$ in die Automorphismengruppe $Aut(H^X)$ von $H^X$.

$$\begin{array}{rcl} \rho^* : G & \longrightarrow & Aut(H^X) \\ q & \longmapsto & \left\{ \begin{array}{rcl} H^X & \longrightarrow & H^X \\ h & \longmapsto & hq^{-1} \end{array} \right. \end{array}$$

Nach diesen Vorbemerkungen kann nun das Kranzprodukt definiert werden.

**Definition 3.16.** Seien Gruppen $H$ und $Q$ und eine Permutationsdarstellung $\rho : Q \curvearrowright X$ vom Grad $n = |X| \neq 0$ gegeben. Dann wird durch $\rho$ auch ein Homomorphismus $\rho^*$ von $Q$ in die Automorphismengruppe $Aut(H^X)$ induziert. Das Kranzprodukt ist definiert durch

$$H \wr_\rho Q := H^X \rtimes_{\rho^*} Q$$

**Bemerkung 3.17.** Die Gruppe $H^X$ ist Normalteiler im Kranzprodukt $H \wr_\rho Q$ und wird Basis des Kranzproduktes genannt. Die Gruppe $Q$ ist die Quotientengruppe.

**Bemerkung 3.18.** Die Ordnung des Kranzproduktes $H \wr_\rho Q$ ist

$$|H \wr_\rho Q| = |H|^n \cdot |Q|$$

**Bemerkung 3.19.** Man spricht von einem Standard Kranzprodukt, wenn die Menge $X$ mit der Gruppe $Q$ übereinstimmt und die Operation $Q \curvearrowright Q$ die Linksmultiplikation ist.

**Bemerkung 3.20.** Wenn im Kranzprodukt $H \wr Q$ zusätzlich die Gruppe $H$ auf einer Menge $Y$ operiert, dann können diese beiden Operationen zu einer Operation des Kranzproduktes auf $Y \times X$ erweitert werden.

Die $Q$-Komponente von $H \wr Q$ operiert auf $Y \times X$ wie auf $X$, wobei $Y$ fest gelassen wird.

$$\begin{array}{rcl} H \wr Q & \curvearrowright & Y \times X \\ (q,y,x) & \longmapsto & q^*(y,x) = (y, qx) \end{array}$$

Die so definierten Elemente $q^*$ bilden eine Untergruppe

$$Q^* = \{ q^* \mid q \in Q \} < S_{Y \times X}$$

in der symmetrischen Gruppe $S_{Y \times X}$. Die Abbildung

$$\begin{array}{ccc} Q & \longrightarrow & Q^* \\ q & \longmapsto & q^* \end{array}$$

ist ein Isomorphismus.

Die Operation der $H^X$-Komponente von $H \wr Q$ auf $Y \times X$ muss für jedes $x \in X$ definiert werden.

$$\begin{array}{rcl} H \wr Q & \curvearrowright & Y \times X \\ (h, x, y, x') & \longmapsto & h_x^*(y, x') = \begin{cases} (hy, x') & \text{falls} \quad x = x' \\ (y, x') & \text{falls} \quad x \neq x' \end{cases} \end{array}$$

Die so definierten Elemente $h_x^*$ bilden für jedes $x \in X$ eine Untergruppe

$$H_x^* = \{ h_x^* \mid h \in H \} < S_{Y \times X}$$

in der symmetrischen Gruppe $S_{Y \times X}$. Die Abbildung

$$\begin{array}{ccc} H & \longrightarrow & H_x^* \\ h & \longmapsto & h_x^* \end{array}$$

ist für jedes $x \in X$ ein Isomorphismus.

**Theorem 3.21.** *Die Gruppe $H$ operiere auf der Menge $Y$ und die Gruppe $Q$ operiere auf der Menge $X$. Dann operiert das Kranzprodukt $H \wr Q$ auf der Menge $Y \times X$ und das Kranzprodukt ist isomorph zu der von den oben definierten Gruppen $H_x^*$ und $Q^*$ erzeugten Untergruppe $W \subseteq S_{Y \times X}$ in der symmetrischen Gruppe $S_{Y \times X}$.*

$$H \wr Q \cong W = \langle Q^*, H_x^* \mid x \in X \rangle < S_{Y \times X}$$

*Beweis.* Für den Beweis verweise ich auf das Buch von Rotman [Rot12]. □

Eine wichtige Eigenschaft des Kranzproduktes ist, dass sich jede Erweiterung einer Gruppe $N$ durch $Q$ als Kranzprodukt darstellen lässt. Denn jede endliche Gruppe ist

als Erweiterung von einfachen endlichen Gruppen darstellbar.

**Proposition 3.22.** *Ist $H$ eine Erweiterung von $N$ durch $Q$, so lässt sich $H$ als eine Untergruppe eines Kranzprodukts aus $N$ und $Q$ darstellen.*

## 3.4. Die Struktur von $p$-Sylowuntergruppen der symmetrischen Gruppe $S_{p^n}$

Eine weitere Anwendung findet das Kranzprodukt in der Darstellung von $p$-Sylowuntergruppen. Wir erläutern die Vorgehensweise an Beispielen.

**Beispiel 3.23.** Im ersten Beispiel betrachten wir $p$-Sylowuntergruppen der symmetrischen Gruppe $S_p$ für eine Primzahl $p$. Die Ordnung von $S_p$ ist

$$\begin{aligned} |S_p| &= p! \\ &= p \cdot (p-1) \cdot (p-2) \cdots 2 \cdot 1 \\ &= p^1 \cdot m \\ \text{und } p &\nmid m \end{aligned}$$

Da es für Primzahlen $p$ bis auf Isomorphie nur die zyklische Gruppe $C_p$ mit der Ordnung $p$ gibt, sind alle $p$-Sylowuntergruppen von $S_p$ isomorph zu $C_p$. Die Anzahl der verschiedenen $p$-Sylowuntergruppen kann hier genau bestimmt werden.

Wir erläutern dies für $p = 5$. Die 5-Sylowuntergruppen werden von Elementen der Ordnung 5 erzeugt. Diese sind als 5-Zykel $(1\,\sigma(2)\,\sigma(3)\,\sigma(4)\,\sigma(5))$ darstellbar. Dabei ist $(\sigma(2)\,\sigma(3)\,\sigma(4)\,\sigma(5))$ eine Permutation von $(2\,3\,4\,5)$. Es gibt somit $4! = 24$ Elemente der Ordnung 5. Jeweils 4 dieser Elemente bilden mit der Identität eine zyklische Gruppe $C_5$. Also gibt es $\frac{4!}{4} = 3! = 6$ verschiedene 5-Sylowuntergruppen in $S_5$.

Dieselbe Überlegung führt für beliebige Primzahlen $p$ auf eine Anzahl von $(p-2)!$ $p$-Sylowuntergruppen $C_p$ in der symmetrischen Gruppe $S_p$.

**Beispiel 3.24.** In diesem Beispiel untersuchen wir die $p$-Sylowuntergruppen der sym-

metrischen Gruppe $S_{p^2}$. Die Ordnung von $S_{p^2}$ ist

$$\begin{aligned} |S_{p^2}| &= (p^2)! \\ &= p^2 \cdot (p^2-1) \cdots \underbrace{(p^2-p) \cdots (p^2-2p) \cdots (p^2-3p) \cdots p}_{(p-1)\ mal} \cdot (p-1) \cdots 1 \\ &= p^{2+(p-1)} \cdot m \\ &= p^{(p+1)} \cdot m \\ \text{und } p &\nmid m \end{aligned}$$

Nach Beispiel 3.23 ist $C_p$ eine $p$-Sylowuntergruppe der symmetrischen Gruppe $S_p$, die ebenfalls auf $[p]$ operiert. Wir bilden das Kranzprodukt mit einer weiteren zyklischen Gruppe $C_p$, die natürlicherweise auch auf $[p]$ operiert. Nach Theorem 3.21 operiert das Kranzprodukt $C_p \wr C_p$ auf der Produktmenge $[p] \times [p] = [p^2]$. Zudem ist das Kranzprodukt $C_p \wr C_p \cong W \leq S_{p^2}$ isomorph zu einer Untergruppe in $S_{p^2}$. Nach Bemerkung 3.18 ist die Ordnung des Kranzproduktes

$$|C_p \wr C_p| = p^p \cdot p = p^{(p+1)}$$

Dies stimmt mit der erwarteten Ordnung einer $p$-Sylowuntergruppe in $S_{p^2}$ überein.

Bevor wir allgemein die $p$-Sylowuntergruppen der symmetrischen Gruppe $S_{p^n}$ untersuchen, müssen wir die Ordnung der $p$-Sylowuntergruppen in $S_{p^n}$ kennen.

**Bemerkung 3.25.** Für zwei natürliche Zahlen $k \leq n$ sei $t = \lfloor \frac{m}{k} \rfloor$ die kleinste natürliche Zahl kleiner als $\frac{m}{k}$. Dann gilt

$$k \leq 2k \leq \cdots \leq tk \leq m \quad \text{aber } (t+1)k > m$$

Somit ist $t$ die Anzahl der Vielfachen von $k$, die kleiner sind als $m$. In $m! = 1 \cdot 2 \cdots m$ tauchen genau $t$ Faktoren auf, die durch $k$ teilbar sind. Die Ordnung der $p$-Sylowuntergruppen in $S_m$ ist gegeben durch $p^\mu$ mit $m = p^\mu \cdot r$ und $p \nmid r$. Für den Exponent $\mu$ gilt aber

$$\mu = \lfloor \frac{m}{p} \rfloor + \lfloor \frac{m}{p^2} \rfloor + \cdots$$

Wenn $m = p^n$ selbst eine Potenz der Primzahl $p$ ist, erhalten wir

$$\mu = \mu(n) = p^{n-1} + p^{n-2} + \cdots + 1$$

**Proposition 3.26.** *Die Ordnung einer $p$-Sylowuntergruppe der symmetrischen Gruppe*

*$S_{p^n}$ ist gegeben durch*

$$p^{\mu(n)} = p^{(p^{n-1}+p^{n-2}+\cdots+1)}$$

**Theorem 3.27.** *Kaloujnine, 1948*
*Sei $p$ eine Primzahl und $S_{p^n}$ die symmetrische Gruppe der Ordnung $p^n$ für $n \in \mathbb{N}$. Dann sind die $p$-Sylowuntergruppen $n$-fach iterierte Kranzprodukte der zyklischen Gruppen $C_p$.*

*Beweis.* Der Beweis erfolgt durch Induktion nach $n$. Für $n = 1$ haben wir bereits in Beispiel 3.23 gezeigt, dass die $p$-Sylowuntergruppen der symmetrischen Gruppe $S_p$ isomorph zur zyklischen Gruppe $C_p \cong \mathbb{Z}/p$ sind. Für den Induktionschritt betrachten wir eine Menge $X$ mit $p^n$ Elementen. Die symmetrische Gruppe $S_{p^n}$ operiert auf $X$. Die $p$-Sylowuntergruppe $H < S_{p^n}$ operiert ebenfalls auf $X$. Nach Induktionsvoraussetzung ist die $p$-Sylowuntergruppe $H$ von $S_{p^n}$ ein $n$-fach iteriertes Kranzprodukt der zyklischen Gruppen $C_p$.

$$H \cong \underbrace{C_p \wr C_p \wr \cdots \wr C_p}_{n \text{ mal}}$$

Eine zusätzliche zyklische Gruppe $Q = \mathbb{Z}/p \cong C_p$ operiere auf sich ($Y \simeq \mathbb{Z}/p = \{0, 1, \cdots, p-1\}$) durch Linksmultiplikation.

$$\begin{array}{rcl} Q & \curvearrowright & Y \\ (1, i) & \mapsto & 1 \circ i = 1 + i \mod p \end{array}$$

Nach Theorem 3.21 operiert das Kranzprodukt $H \wr Q$ auf $Y \times X$ und ist isomorph zu einer Untergruppe $W$ in der symmetrischen Gruppe $S_{Y \times X}$. Nach Induktionsvoraussetzung hat $H$ als $p$-Sylowuntergruppe in $S_{p^n}$ die Ordnung $|H| = p^{\mu(n)}$. Somit hat das Kranzprodukt $H \wr Q$ die Ordnung $|H \wr Q| = p^{\mu(n)} \cdot p = p^{\mu(n+1)}$. Dies stimmt mit der Ordnung einer $p$-Sylowuntergruppe in $S_{p^{n+1}} \cong S_{Y \times X}$ überein. □

Das obige Ergebnis für $p$-Sylowuntergruppen der symmetrische Gruppe $S_{p^n}$ kann auf beliebige symmetrische Gruppen $S_m$ erweitert werden.

**Korollar 3.28.** *Die $p$-Sylowuntergruppen einer symmetrischen Gruppe $S_m$ sind das direkte Produkt*

$$\underbrace{C_p \times \cdots \times C_p}_{a_1 \text{ mal}} \times \underbrace{C_p \wr C_p \times \cdots \times C_p \wr C_p}_{a_2 \text{ mal}} \times \cdots \times \underbrace{\overbrace{C_p \wr \cdots \wr C_p}^{t \text{ mal}} \times \cdots \times \overbrace{C_p \wr \cdots \wr C_p}^{t \text{ mal}}}_{a_t \text{ mal}}$$

*Dabei ist*

$$m = a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots + a_t \cdot p^t \quad 0 \le a_j \le p - 1$$

*die p-adische Darstellung von m.*

*Beweis.* Wir betrachten die $p$-adische Darstellung von $m$:

$$m = a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots + a_t \cdot p^t \quad 0 \leq a_j \leq p-1$$

Die Menge $X = [m]$, auf der $S_m$ operiert, zerfällt in

$$\begin{array}{ll} a_0 & 1-\text{elementige Mengen} \quad (Y_0)_{i_0} \\ a_1 & p-\text{elementige Mengen} \quad (Y_1)_{i_1} \\ a_2 & p^2-\text{elementige Mengen} \quad (Y_2)_{i_2} \\ \vdots & \vdots \\ a_t & p^t-\text{elementige Mengen} \quad (Y_t)_{i_t} \end{array}$$

Auf jeder dieser Mengen $(Y_j)_{i_j}$ operiert eine symmetrische Gruppe $S_{(Y_j)_{i_j}} \cong S_{p^j}$. Theorem 3.27 liefert die Struktur der $p$-Sylowuntergruppen in jeder dieser symmetrischen Gruppen. Da die Permutationen auf den Mengen $(Y_j)_{i_j}$ disjunkt sind und daher kommutieren, ist das direkte Produkt aller $p$-Sylowuntergruppen eine Untergruppe in $S_X$ der Ordnung $p^N$ mit

$$N = a_1 + a_2 \cdot \mu(2) + \cdots + a_t \cdot \mu(t)$$

Wegen

$$\begin{aligned} m &= a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots + a_t \cdot p^t \\ \Rightarrow \quad \lfloor \frac{m}{p} \rfloor + \lfloor \frac{m}{p^2} \rfloor + \cdots &= (a_1 + a_2 \cdot p + a_3 \cdot p^2 + \cdots + a_t \cdot p^{t-1}) \\ &\quad + (a_2 + a_3 \cdot p + a_4 \cdot p^2 + \cdots + a_t \cdot p^{t-2}) \\ &\quad + (a_3 + a_4 \cdot p + a_5 \cdot p^2 + \cdots + a_t \cdot p^{t-3}) + \cdots \\ &= a_1 + a_2 \cdot (p+1) + a_3 \cdot (p^2 + p + 1) + \cdots \\ &= a_1 + a_2 \cdot \mu(2) + a_3 \cdot \mu(3) + \cdots + a_t \cdot \mu(t) \\ &= N \end{aligned}$$

stimmt $p^N$ mit der Ordnung der $p$-Sylowuntergruppen in $S_m$ überein. □

**Bemerkung 3.29.** Wie Wolfram Jehne in [JW13] erwähnt, enthält die Sudoku-Gruppe zwei Kranzprodukte von $S_3$ als Untergruppen. Die Ordnung der Sudoku-Gruppe ist $2 \cdot 6^6 \cdot 6^2 = 3\,359\,232$.

## 3.5. Satz von Wedderburn

Zur Formulierung des Satzes von Wedderburn benötigen wir den Begriff des Schiefkörpers.

**Definition 3.30.** Eine abelsche, additive Gruppe $K$ ist ein Schiefkörper, wenn $K^* = K \setminus \{0\}$ eine multiplikative Gruppe ist und folgende Distributivgesetze gelten

$$\begin{aligned}(a+b)\cdot c &= a\cdot c + b\cdot c\\ a\cdot(c+b) &= a\cdot c + a\cdot b\end{aligned}$$

Wenn die multiplikative Gruppe $K^*$ ebenfalls kommutativ ist, ist der Schiefkörper ein Körper.

**Beispiel 3.31.** Ein bekanntes Beispiel für einen Schiefkörper bilden die Hamiltonschen Quaternionen.

$$\mathbb{H} = 1\cdot\mathbb{R} \oplus i\cdot\mathbb{R} \oplus j\cdot\mathbb{R} \oplus k\cdot\mathbb{R}$$

mit den Verknüpfungen

$$\begin{aligned} i^2 &= j^2 = k^2 = -1\\ ij &= -ij = k\\ jk &= -kj = i\\ ki &= -ik = j\end{aligned}$$

Wie bei den komplexen Zahlen kann man auch zu einer Quaternion $q = t + ix + jy + kz$ die konjugierte Quaternion $\bar{q} = t - ix - jy - kz$ bilden und erhält die Norm

$$|q|^2 = q\cdot\bar{q} = \bar{q}\cdot q = t^2 + x^2 + y^2 + z^2$$

Die inverse Quaternion ergibt sich dann zu $q^{-1} = \frac{\bar{q}}{|q|^2}$.

Die Quaternionen $1, -1, i, -i, j, -j, k, -k$ bilden mit den obigen Verknüpfungen die Quaternionengruppe $Q_8$ mit der Verknüpfungstabelle:

| | 1 | -1 | i | -i | j | -j | k | -k |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | -1 | i | -i | j | -j | k | -k |
| -1 | -1 | 1 | -i | i | -j | j | -k | k |
| i | i | -i | -1 | 1 | k | -k | -j | j |
| -i | -i | i | 1 | -1 | -k | k | j | -j |
| j | j | -j | -k | k | -1 | 1 | i | -i |
| -j | -j | j | k | -k | 1 | -1 | -i | i |
| k | k | -k | j | -j | -i | i | -1 | 1 |
| -k | -k | k | -j | j | i | -i | 1 | -1 |

Die Quaternionengruppe $Q_8$ ist eine dizyklische Gruppe. Diese erhält man aus Erzeugern $i, j$ und Relationen.

$$Q_8 = \langle i, j \,|\, i^4 = 1, i^2 = j^2, j \cdot i \cdot j^{-1} = i^{-1} \rangle$$

Zum Beweis des Satzes von Wedderburn sind zwei Lemmata hilfreich.

**Lemma 3.32.** *Sind $q, n, m \in \mathbb{N}$ natürliche Zahlen mit $q \geq 2$ und $n, m \geq 1$, Dann gilt $q^m - 1 \,|\, q^n - 1$ genau dann, wenn $m \,|\, n$.*

*Beweis.* Wir betrachten die Polynome $x^m - 1$ und $x^n - 1$. Das Polynom $x^m - 1$ teilt $x^n - 1$ genau dann, wenn es ein Polynom $f(x)$ gibt mit

$$x^n - 1 = f(x) \cdot (x^m - 1)$$

Das Polynom $f(x)$ kann bestimmt werden:

$$(x^n - 1) : (x^m - 1) = \underbrace{x^{n-m} + x^{n-2m} + \cdots + x^{n-rm} + 1}_{=f(x)}$$

$$\begin{array}{rcl}
x^n & - & x^{n-m} \\
\hline
 & & x^{n-m} \\
 & & x^{n-m} - x^{n-2m} \\
 & & \hline
 & & x^{n-2m} \\
 & & \ddots \\
 & & x^{n-rm} - 1 \\
 & & x^{n-rm} - 1 \\
 & & \hline
 & & 0
\end{array}$$

Bei der Division bleibt genau dann kein Rest, wenn gilt:

$$\begin{array}{rcl}
m & = & n - rm \\
\Leftrightarrow \quad n & = & (r+1)m \\
\Leftrightarrow \quad n & \mid & m
\end{array}$$

□

**Lemma 3.33.** *Sind $q, n \in \mathbb{N}$ natürliche Zahlen mit $q \geq 2$ und $n \geq 1$ und sind $n_1, \cdots, n_r \in \mathbb{N}$ Teiler von $n$ und es gelte*

$$q^n - 1 = q - 1 + \sum_{i=1}^{r} \frac{q^n - 1}{q^{n_i} - 1}$$

*Dann ist $n = 1$ und $r = 0$.*

*Beweis.* Für jeden Teiler $d|n$ ist das Kreisteilungspolynom $\Phi_n$ Teiler von $\frac{x^n-1}{x^d-1}$. Da $\Phi_n(q)$ die linke Seite und alle Summanden der Summe auf der rechten Seite teilt, teilt $\Phi_n(q)$ auch $q-1$. Das Kreisteilungspolynom $\Phi_n(q)$ hat jedoch alle primitiven $n$-ten Einheitswurzeln $\zeta$ als Nullstellen. Insbesondere gilt

$$\Phi_n(q) = \prod_{\zeta} (q - \zeta)$$

Nun ist $q \geq 2$ eine reelle Zahl. Wie man leicht in der komplexen Ebene am Einheitskreis einsieht, gilt für alle primitiven $n$-ten Einheitswurzeln $\zeta \neq 1$

$$|q - \zeta| > |q - 1|$$

Gäbe es eine primitive $n$-te Einheitswurzel $\zeta \neq 1$, so folgte

$$\begin{aligned} |\Phi_n(q)| &= \prod_{\zeta} |q - \zeta| \\ &> \prod_{\zeta} |q - 1| \\ &\geq |q - 1| \end{aligned}$$

im Widerspruch zu $\Phi_n(q) \,|\, q - 1$. □

**Theorem 3.34.** *Kleiner Satz von Wedderburn*
*Jeder endliche Schiefkörper ist ein kommutativer Körper.*

*Beweis.* Der Beweis geht von einem endlichen Schiefkörper $K$ aus. Die multiplikative Gruppe wird mit $G = K \setminus \{0\}$ bezeichnet. Ihr Zentrum sei

$$Z(G) = \{ g \in G \,|\, gh = hg \text{ für alle } h \in G \}$$

Zusammen mit $\{0\}$ bildet dies einen endlichen, kommutativen Körper $L = Z(G) \cup \{0\}$ mit $q = |L|$ Elementen. Als Körpererweiterung von $L$ ist $K$ ein Vektorraum über $L$ mit der Dimension $\dim_L K = n$. Somit hat $K$ $q^n$ Elemente.

Die multiplikative Gruppe $G$ operiert auf sich selbst durch Konjugation. Die Bahnen durch ein Element $g \in Z(G)$ aus dem Zentrum bestehen genau aus diesem einen Element.

Denn für eine Bahn durch $g \in Z(G)$ gilt:

$$\begin{aligned} Gg &= \{ h \circ g = hgh^{-1} \mid h \in G \} \\ &= \{ hgh^{-1} = ghh^{-1} \mid h \in G \} \\ &\quad \text{denn } g \text{ liegt im Zentrum} \\ &= \{ g \} \end{aligned}$$

Da alle Bahnen eine disjunkte Zerlegung von $G$ bilden, summieren sich die Bahngrößen zur Ordnung von $G$. Dabei unterscheiden wir die einelementigen Bahnen durch Elemente des Zentrums und $r$ Bahnen $Gg_i$ mit zwei oder mehr Elementen. Die Stabilisatoren der größeren Bahnen sind Untergruppen in $G$.

$$G_{g_i} = \{ g \in G \mid gg_ig^{-1} = g_i \}$$

Zusammen mit der $0 \in K$ sind diese auch Vektorräume der Dimension $n_i = \dim_L(G_{g_i} \cup \{0\})$ mit $q^{n_i}$ Elementen. Damit erhalten wir:

$$|G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|G_{g_i}|}$$

Mit $q = |L|$ folgt daraus:

$$q^n - 1 = q - 1 + \sum_{i=1}^{r} \frac{q^n - 1}{q^{n_i} - 1}$$

Da Brüche unter der Summe von den Bahnen mit zwei oder mehr Elementen herrühren, muß $n_i < n$ für alle $i$ gelten. Darüberhinaus sind nach Lemma 3.32 alle $n_i$ Teiler von $n$. Wir können also Lemma 3.33 anwenden und erhalten $n = 1$ und $r = 0$. Die Körper $L = K$ stimmen also überein und $K$ ist kommutativ. □

Ein etwas anderer Beweis, der Körpererweiterungen verwendet, wird von van der Waerden in [DW67] gegeben.

Der Satz von Wedderburn hat Auswirkungen in der synthetischen, ebenen, projektven Geometrie. Diese Ergänzung zur Vorlesung wird im Anhang A beschrieben.

## 3.6. Eigenschaften endlicher Körper

Wir stellen hier noch einige Eigenschaften endlicher Körper zusammen.

**Proposition 3.35.** *Die multiplikative Gruppe eines endlichen Körpers ist zyklisch.*

*Beweis.* Sei $K$ ein endlicher Körper. Dann ist die multiplikative Gruppe $K^*$ abelsch und isomorph zum Produkt zyklischer Gruppen.

$$K^* \cong C_{n_1} \times \cdots \times C_{n_s} \quad \text{wobei jedes } n_i \text{ das nachfolgende } n_{i+1} \text{ teilt}$$

Die Gleichung $x^{n_1} = 1$ hat $n_1^s$ Lösungen. Da aber jedes Polynom $0 \neq f \in K[x]$ höchstens $deg(f) = n_1$ Lösungen hat, folgt $s = 1$ und

$$K^* \cong C_{n_1}$$

□

**Definition 3.36.** Die Charakteristik eines Körpers $\mathbb{F}$ ist die kleinste natürliche Zahl $\chi(\mathbb{F}) = n$ für die gilt:

$$\underbrace{1 + \cdots + 1}_{n \text{ mal}} = 0$$

Falls die Summe stets ungleich 0 ist, wird $\chi(\mathbb{F}) = 0$ definiert.

**Lemma 3.37.** *Die Charakteristik eines Körpers ist entweder* 0 *oder eine Primzahl.*

*Beweis.* Wir nehmen an, die Charakteristik eines Körpers $\mathbb{F}$ wäre $\chi(\mathbb{F}) = n = p \cdot q$ mit $p < n$ und $q < n$. Dann gilt:

$$\underbrace{1 + \cdots + 1}_{p \cdot q \text{ mal}} = (p \cdot q) \cdot 1 = 0$$

$$\Rightarrow \quad (p \cdot 1) \cdot (q \cdot 1) = 0 \quad \Rightarrow \quad \begin{cases} (p \cdot 1) = 0 & \text{oder} \\ (q \cdot 1) = 0 \end{cases}$$

Dies steht ein Widerspruch zur Minimalität von $n$. □

**Beispiel 3.38.** Für eine Primzahl $p$ bilden die Restklassen $\mathbb{Z}/p$ einen Körper der Charakteristik $p$. Da diese auch $p$ Elemente haben, werden sie Primkörper genannt. Es sind auch bis auf Isomorphie die einzigen Körper mit $p$ Elementen.

**Bemerkung 3.39.** Endliche Körper haben immer eine endliche Charakteristik. Es gibt jedoch auch unendliche Körper mit endlicher Charakteristik, zum Beispiel den Quotientenkörper des Polynomrings $(\mathbb{Z}/p)[X]$.

**Lemma 3.40.** *Jeder endliche Körper hat $p^r$ Elemente, wobei $p$ eine Primzahl und $r \in \mathbb{N}$ ist.*

*Beweis.* Jeder endliche Körper $\mathbb{F}$ hat eine endliche Charakteristik $p \in \mathbb{P}$. Er ist somit eine Erweiterung des Primkörpers $\mathbb{Z}/p$. Der Körper $\mathbb{F}$ kann als $r$-dimensionaler Vektorraum über $\mathbb{Z}/p$ aufgefaßt werden mit der Basis $(e_1, \cdots, e_r)$. Die Elemente $a \in \mathbb{F}$ lassen sich als Linearkombinationen darstellen:

$$a = \sum_{i=1}^{r} \lambda_i \cdot e_i \quad \text{mit } \lambda_i \in \mathbb{Z}/p$$

Dafür gibt es genau $p^r$ Möglichkeiten. □

### 3.6.1. Frobenius Automorphismus

**Definition 3.41.** Sei $\mathbb{F}$ ein endlicher Körper der Charakteristik $p$. Dann heisst die Abbildung

$$\begin{aligned} \varphi_p : \mathbb{F} &\longrightarrow \mathbb{F} \\ a &\longmapsto a^p \end{aligned}$$

Frobenius Automorphismus.

Die Homomorphie bezüglich der multiplikativen Gruppe ergibt sich direkt aus der Definition. Die Homomorphie bezüglich der additiven Gruppe folgt aus

$$(a+b)^p = a^p + b^p$$

Denn für $1 \leq k \leq p-1$ sind alle Binomialkoeffizienten $\begin{pmatrix} p \\ k \end{pmatrix} = 0$ gleich Mull. Da ein Körper keine Nullteiler enthält, ist $\varphi_p$ injektiv, und in endlichen Körpern auch bijektiv.

## 3.7. Reelle Polynome mit ganzzahligen Werten

**Definition 3.42.** Reelle Polynome mit ganzzahligen Werten auf den ganzen Zahlen werden bezeichnet mit:

$$P_{\mathbb{Z}} = \{\, p \in \mathbb{R}[X] \,|\, p(\mathbb{Z}) \subset \mathbb{Z} \,\}$$

Es ist klar, dass alle Polynome mit ganzahligen Koeffizienten in $P_{\mathbb{Z}}$ enthalten sind.

$$\mathbb{Z}[X] \subseteq P_{\mathbb{Z}}$$

Zusätzlich sind für $x \in \mathbb{R}$ und $n \in \mathbb{N}$ die Binomialpolynome

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}$$

ebenfalls in $P_{\mathbb{Z}}$ enthalten. Für $x \in \mathbb{N}$ folgt das direkt aus der Definition der Binomialkoeffizienten. Und für $-x \in \mathbb{N}$ gilt

$$\binom{-x}{n} = \binom{x+n-1}{n}$$

Tatsächlich sind alle reellen Polynome mit ganzzahligen Werten auf den ganzen Zahlen Linearkombinationen von Binomialpolynomen mit ganzzahligen Koeffizienten.

**Theorem 3.43.** *Alle reellen Polynome mit ganzahligen Werten für ganze Zahlen lassen sich als Linearkombination aus Binomialpolynomen mit ganzzahligen Koeffizienten schreiben.*

$$P_{\mathbb{Z}} = \bigoplus_{n=0}^{\infty} \binom{x}{n} \cdot \mathbb{Z}$$

*Das heisst*

$$p \in P_{\mathbb{Z}} \quad \Leftrightarrow \quad p(x) = \sum_{k=0}^{deg(p)} a_k \cdot \binom{x}{k} \quad mit\ a_k \in \mathbb{Z} \tag{PZ}$$

*Für die Koeffizienten $a_k$ gilt:*

$$\begin{aligned} a_k &= p(k) - \binom{k}{1} p(k-1) + \binom{k}{2} p(k-2) \mp \cdots \\ &= \sum_{j=0}^{k} (-1)^j \binom{k}{j} p(k-j) \end{aligned}$$

*Beweis.* Es ist klar, dass alle Polynome mit der Darstellung (PZ) für ganzzahlige Argumente ganzzahlige Werte annehmen.

Sei nun $p \in P_{\mathbb{Z}}$ mit Grad $\deg p = n$. Dann müssen wir zeigen, dass $p$ sich wie in Gleichung (PZ) darstellen läßt. Hierzu verwenden wir die Eigenschaft, dass zwei Polynome vom Grad $n$ übereinstimmen, wenn sie bereits in $n+1$ Werten übereinstimmen. Wir betrachten nun ein Polynom $f$ mit der Darstellung

$$f(x) = \sum_{j=0}^{n} a_j \cdot \binom{x}{j}$$

Nun müssen wir zeigen, dass die beiden Polynome übereinstimmen und die Koeffizienten $a_k$ ganzzahlig sind. Die beiden Polynome stimmen überein, wenn sie in $n+1$ Werten übereinstimmen.

$$f(k) = \sum_{j=0}^{n} a_j \cdot \begin{pmatrix} k \\ j \end{pmatrix} = p(k) \quad \text{für } 0 \le k \le n$$

Die Koeffizienten $a_j$ erfüllen also bei gegebenen Werten $p(k)$ ein lineares Gleichungssystem mit dem Pascalschen Dreieck als Matrix.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 1 & 2 & 1 & 0 & 0 & \cdots & 0 \\ 1 & 3 & 3 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \binom{n}{1} & \binom{n}{2} & \binom{n}{3} & \binom{n}{4} & \cdots & 1 \end{pmatrix} = \begin{pmatrix} p(0) \\ p(1) \\ p(2) \\ p(3) \\ \vdots \\ p(n) \end{pmatrix}$$

Das Pascalsche Dreieck ist als Matrix invertierbar und es gilt:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 1 & 2 & 1 & 0 & 0 & \cdots & 0 \\ 1 & 3 & 3 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \binom{n}{1} & \binom{n}{2} & \binom{n}{3} & \binom{n}{4} & \cdots & 1 \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \cdots & 0 \\ -1 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 1 & -2 & 1 & 0 & 0 & \cdots & 0 \\ -1 & 3 & -3 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ (-1)^n & (-1)^{n-1}\binom{n}{1} & (-1)^{n-2}\binom{n}{2} & (-1)^{n-3}\binom{n}{3} & (-1)^{n-4}\binom{n}{4} & \cdots & 1 \end{pmatrix}$$

Somit ist das Gleichungssystem eindeutig und ganzzahlig lösbar mit

$$\begin{aligned} a_k &= \sum_{j=0}^{k} (-1)^{k-j} \left( \begin{array}{c} k \\ j \end{array} \right) p(j) \\ &= \sum_{j=0}^{k} (-1)^{j} \left( \begin{array}{c} k \\ j \end{array} \right) p(k-j) \end{aligned}$$

□

**Bemerkung 3.44.** Für die Monome $p(x) = x^n$ erhalten wir folgende Koeffizienten

$$a_k^{(n)} = \sum_{j=0}^{k} (-1)^{k-j} \left( \begin{array}{c} k \\ j \end{array} \right) j^n$$

Mit den Stirling-Zahlen 2. Art

$$S_k^n = \frac{1}{k!}\, a_k^{(n)} = \frac{1}{k!} \sum_{j=0}^{k} (-1)^{k-j} \left( \begin{array}{c} k \\ j \end{array} \right) j^n$$

erhalten wir

$$x^{(n)} = \sum_{k=0}^{n} k!\, S_k^n \left( \begin{array}{c} x \\ k \end{array} \right)$$

Das heisst, dass die Binomialpolynome $\left( \begin{array}{c} x \\ k \end{array} \right)$ ebensowie die Monome $x^n$ eine Basis im Polynomraum $\mathbb{R}[X]$ bilden und der Basiswechsel durch die Matrix $\left(k!\, S_k^n\right)$ vermittelt wird.

Der schottische Mathematiker James Stirling untersuchte die Stirlingzahlen bereits 1730. Die Bezeichnung Stirlingzahlen erhielten sie allerdings erst 1906 von Niels Nielsen.

Ebenso wie die Binomialkoeffizienten gibt es auch für Stirlingzahlen eine Rekursionsformel.

$$S_k^n = S_{k-1}^{n-1} + k \cdot S_k^{n-1}$$

Der Nachweis benutzt natürlich die Rekursionsformel der Binomialkoeffizienten in der Form

$$\left( \begin{array}{c} k-1 \\ j \end{array} \right) - \left( \begin{array}{c} k \\ j \end{array} \right) = - \left( \begin{array}{c} k-1 \\ j-1 \end{array} \right)$$

$$\begin{aligned}
S_{k-1}^{n-1} + k \cdot S_k^{n-1} &= \frac{1}{(k-1)!} \sum_{j=0}^{k-1} (-1)^{k-j-1} \left( \left( \begin{array}{c} k-1 \\ j \end{array} \right) - \left( \begin{array}{c} k \\ j \end{array} \right) \right) j^{n-1} + \frac{k}{k!} (-1)^{k-k} \left( \begin{array}{c} k \\ k \end{array} \right) k^{n-1} \\
&= \frac{1}{(k-1)!} \sum_{j=0}^{k-1} (-1)^{k-j} \left( \begin{array}{c} k-1 \\ j-1 \end{array} \right) j^{n-1} + \frac{k^n}{k!} \\
&= \frac{1}{k!} \sum_{j=0}^{k-1} (-1)^{k-j} \left( \begin{array}{c} k \\ j \end{array} \right) j^n + \frac{k^n}{k!} \\
&= \frac{1}{k!} \sum_{j=0}^{k} (-1)^{k-j} \left( \begin{array}{c} k \\ j \end{array} \right) j^n \\
&= S_k^n
\end{aligned}$$

In der Kombinatorik bezeichnen die Stirlingzahlen 2. Art die Anzahl der Einteilungen einer $n$-elementigen Menge in $k$ Blöcke.

## 3.8. Doppelte Binomialpolynome

Wenn anstelle der Variablen $y$ ein Binomialpolynom $\left( \begin{array}{c} x \\ n \end{array} \right)$ in das Binomialpolynom $\left( \begin{array}{c} y \\ m \end{array} \right)$ eingesetzt wird, erhält man wieder ein Polynom, das auf den ganzen Zahlen ganzzahlige Werte annimmt. Nach Theorem 3.43 läßt es sich als Linearkombination aus Binomialpolynomen darstellen.

$$\left( \begin{array}{c} \left( \begin{array}{c} x \\ n \end{array} \right) \\ m \end{array} \right) = \sum_{k=0}^{nm} a_k^{(n,m)} \cdot \left( \begin{array}{c} x \\ k \end{array} \right) \quad \text{mit } n, m \in \mathbb{N} \text{ und } x \in \mathbb{R}$$

In den zwei folgenden Beispielen berechnen wir doppelte Binomialpolynome. Dabei verwenden wir die Division von Polynomen mit Rest.

**Beispiel 3.45.**

$$\begin{aligned}
\left(\left(\begin{array}{c} x \\ 2 \\ 2 \end{array}\right)\right) &= \frac{1}{2}\left(\begin{array}{c} x \\ 2 \end{array}\right)\left(\left(\begin{array}{c} x \\ 2 \end{array}\right)-1\right) \\
&= \frac{1}{8}\,x\cdot(x-1)\cdot\big(x\cdot(x-1)-2\big) \\
&= \frac{1}{8}\,x\cdot(x-1)\cdot(x-2)\cdot(x+1) \\
&= \frac{1}{8}\,x\cdot(x-1)\cdot(x-2)\cdot(x-3+4) \\
&= \frac{1}{8}\big(4\,x\cdot(x-1)\cdot(x-2)+x\cdot(x-1)\cdot(x-2)\cdot(x-3)\big) \\
&= 3\left(\begin{array}{c} x \\ 3 \end{array}\right)+3\left(\begin{array}{c} x \\ 4 \end{array}\right)
\end{aligned}$$

**Beispiel 3.46.**

$$\begin{aligned}
\left(\left(\begin{array}{c} x \\ 2 \\ 3 \end{array}\right)\right) &= \frac{1}{6}\left(\begin{array}{c} x \\ 2 \end{array}\right)\left(\left(\begin{array}{c} x \\ 2 \end{array}\right)-1\right)\left(\left(\begin{array}{c} x \\ 2 \end{array}\right)-2\right) \\
&= \frac{1}{48}\,x\cdot(x-1)\cdot\big(x\cdot(x-1)-2\big)\cdot\big(x\cdot(x-1)-4\big) \\
&= \frac{1}{48}\,x\cdot(x-1)\cdot\big(x^2-x-2\big)\cdot\big(x^2-x-4\big) \\
&= \frac{1}{48}\,x\cdot(x-1)\cdot(x-2)\cdot(x+1)\cdot\big(x^2-x-4\big) \\
&= \frac{1}{48}\,x\cdot(x-1)\cdot(x-2)\cdot\big(x^3-5x-4\big) \\
&= \frac{1}{48}\,x\cdot(x-1)\cdot(x-2)\cdot\big((x-3)\cdot(x^2+3x+4)+8\big) \\
&= \frac{1}{6}\,x\cdot(x-1)\cdot(x-2)+\frac{1}{48}\,x\cdot(x-1)\cdot(x-2)\cdot(x-3)\cdot\big((x-4)\cdot(x+7)+32\big) \\
&= \left(\begin{array}{c} x \\ 3 \end{array}\right)+16\left(\begin{array}{c} x \\ 4 \end{array}\right)+30\left(\begin{array}{c} x \\ 5 \end{array}\right)+15\left(\begin{array}{c} x \\ 6 \end{array}\right)
\end{aligned}$$

**Proposition 3.47.** *Für $x \in \mathbb{N}$ bezeichnet der Binomialkoeffizient $\left(\begin{array}{c} x \\ n \end{array}\right)$ die Anzahl der*

*n-elementigen Teilmengen von* $[x]$.

$$\left( \begin{array}{c} x \\ n \end{array} \right) = |\,\mathcal{P}_n([x])\,|$$

*Der doppelte Binomialkoeffizient bezeichnet also die Anzahl der m-elementigen Teilmengen in der Menge der n-elementigen Teilmengen von* $[x]$.

$$\left( \begin{array}{c} \left( \begin{array}{c} x \\ n \end{array} \right) \\ m \end{array} \right) = |\,\mathcal{P}_m(\mathcal{P}_n([x]))\,|$$

*Die symmetrische Gruppe* $S_x$ *operiert sowohl auf* $[x]$ *wie auch auf den n-elementigen Teilmengen.*

$$\begin{aligned} S_x &\curvearrowright [x] \\ S_x &\curvearrowright \mathcal{P}_n([x]) \\ S_x &\curvearrowright \mathcal{P}_m(\mathcal{P}_n([x])) \end{aligned}$$

### 3.8.1. Graphentheoretische Betrachtung der Beispiele

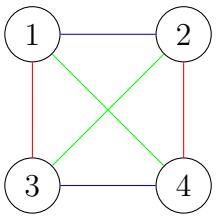
Nun betrachten wir die Zahlen $1, 2, \cdots, x$ als Ecken eines Graphen. Die Kanten des Graphen sind 2-elementige Teilmengen in $[x]$, also Elemente in $\mathcal{P}_2([x])$. Alle Graphen mit $m$ Kanten bilden die Menge $\mathcal{P}_m(\mathcal{P}_2([x]))$. Mit dieser Überlegung können wir die Koeffizienten aus den Beispielen anschaulicher herleiten.

Wir betrachten zunächst die Anzahl der Graphen mit zwei Kanten aus Beispiel 3.45 und nehmen an, dass die Menge $[x]$ mindestens 4 Elemente besitzt ($x \geq 4$). Es gilt

$$\left( \begin{array}{c} \left( \begin{array}{c} x \\ 2 \end{array} \right) \\ 2 \end{array} \right) = |\,\mathcal{P}_2(\mathcal{P}_2([x]))\,|$$

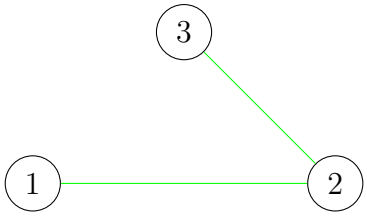
Es gibt zwei unterschiedliche Typen von Graphen mit zwei Kanten:

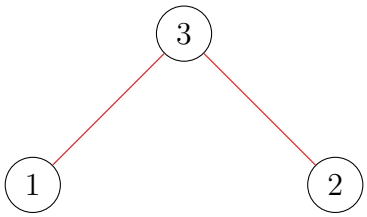
a) Die Kanten haben keine Ecke gemeinsam. Die vier Ecken können auf 3 verschiedene Arten durch die zwei Kanten verbunden werden.

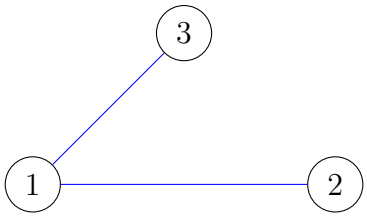



Mit der Auswahl der vier Ecken des Graphen aus den $x$ Ecken erhalten wir also $\begin{pmatrix} x \\ 4 \end{pmatrix} \cdot 3$ verschiedene Graphen dieser Art mit zwei Kanten.

b) Die Kanten haben eine Ecke gemeinsam. Die drei Ecken können auf 3 verschiedene Arten durch die zwei Kanten verbunden werden.




Mit der Auswahl der drei Ecken des Graphen aus den $x$ Ecken erhalten wir also $\begin{pmatrix} x \\ 3 \end{pmatrix} \cdot 3$ verschiedene Graphen dieser Art mit zwei Kanten.

Somit erhalten wir insgesamt für die Anzahl der Graphen mit zwei Kanten und $x$ Ecken:

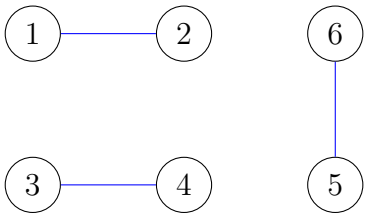
$$\left( \left( \begin{array}{c} x \\ 2 \end{array} \right) \right) = 3 \left( \begin{array}{c} x \\ 3 \end{array} \right) + 3 \left( \begin{array}{c} x \\ 4 \end{array} \right)$$

Wir betrachten nun Beispiel 3.46 als Graphen mit drei Kanten und nehmen an, dass die Menge $[x]$ mindestens 6 Elemente besitzt ($x \geq 6$). Es gilt

$$\left( \left( \begin{array}{c} x \\ 2 \end{array} \right) \right) = |\mathcal{P}_3(\mathcal{P}_2([x]))|$$

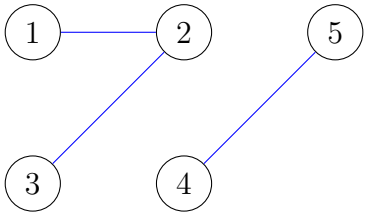
Es gibt folgende 5 unterschiedliche Typen von Graphen mit drei Kanten, die einzeln betrachtet werden.

a) Keine Kante hat eine gemeinsame Ecke mit einer anderen Kante.



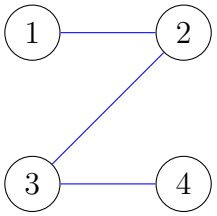

Wenn die 6 Ecken mit Kanten aus der Menge $[x]$ ausgewählt sind, gibt es noch $\left( \begin{array}{c} 6 \\ 2 \end{array} \right) = 15$ Möglichkeiten, die Kanten als 2-elementige Teilmengen in $[x]$ auszuwählen.

b) Genau zwei Kanten haben eine Ecke gemeinsam.



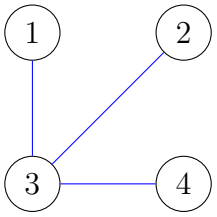

Wenn die 5 Ecken mit Kanten aus der Menge $[x]$ ausgewählt sind, gibt es noch $\left( \begin{array}{c} 5 \\ 3 \end{array} \right) = 10$ Möglichkeiten, die 3 Ecken mit 2 Kanten auszuwählen. Für jede dieser Möglichkeiten haben wir wie in Beispiel 3.45 noch 3 weitere Möglichkeiten, die zwei Kanten zu verteilen. Das ergibt zusammen 30 Möglichkeiten.

c) Die drei Kanten verbinden 4 Ecken linear.



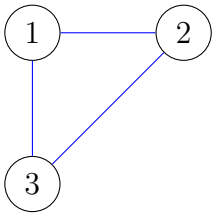

Wenn die 4 Ecken mit Kanten aus der Menge $[x]$ ausgewählt sind, gibt es noch $\binom{4}{2} = 6$ Möglichkeiten, die 2 Endpunkte der drei Kanten auszuwählen. Die 2 übrigen Punkte können noch auf 2 verschiedene Arten mit Kanten verbunden werden. Das ergibt zusammen 12 Möglichkeiten.

d) Die drei Kanten gehen von einer Ecke aus.




Wenn die 4 Ecken mit Kanten aus der Menge $[x]$ ausgewählt sind, gibt es noch 4 Möglichkeiten, die gemeinsame Ecke der drei Kanten auszuwählen.

e) Die drei Kanten bilden ein Dreieck.




Nach Auswahl der 3 Ecken liegt der Graph fest.

Somit erhalten wir insgesamt für die Anzahl der Graphen mit drei Kanten und $x$ Ecken:

$$\left(\binom{x}{2}\right) = \binom{x}{3} + 16\binom{x}{4} + 30\binom{x}{5} + 15\binom{x}{6}$$

# 4. Klassifikation von Permutationsdarstellungen und Burnside-Ring

## 4.1. Arithmetik von Permutationsdarstellungen

Nun soll für eine feste, endliche Gruppe $G$ die Struktur aller endlichen Permutationsdarstellungen untersucht werden.

**Definition 4.1.** Seien

$$\begin{aligned} \rho : G &\curvearrowright X \\ \rho' : G &\curvearrowright X' \end{aligned}$$

zwei endliche Permutationsdarstellungen einer vorgegebenen, endlichen Gruppe $G$. Dann ist durch

$$\rho + \rho' : G \curvearrowright (X \sqcup X')$$

die Summe von $\rho$ und $\rho'$ definiert. Dabei ist $X \sqcup X'$ die disjunkte Vereinigung von $X$ und $X'$. Das Produkt von $\rho$ und $\rho'$ wird durch

$$\begin{aligned} \rho \times \rho' : G &\curvearrowright X \times X' \\ (g; x, x') &\mapsto (gx, gx') \end{aligned}$$

definiert.

Die folgenden Eigenschaften dieser Verknüpfungen sind unmittelbar klar.

**Proposition 4.2.**

- *Die Summe $\rho + \rho'$ ist assoziativ.*
- *Die Summe $\rho + \rho'$ ist kommutativ.*
- *Die Summe $\rho + \rho'$ hat $G \curvearrowright \varnothing$ als 0-Element.*
- *Das Podukt $\rho \times \rho'$ ist assoziativ.*
- *Das Podukt $\rho \times \rho'$ ist kommutativ.*
- *Das Podukt $\rho \times \rho'$ hat $G \curvearrowright [1]$ als 1-Element.*
- *Es gilt das Distributivgesetz*

$$(\rho + \rho') \times \rho'' = \rho \times \rho'' + \rho' \times \rho''$$

Damit bilden die Permutationsdarstellungen einer vorgegebenen Gruppe $G$ einen kommutativen Halbring $(PREP(G), +, \times)$.

**Beispiel 4.3.** Die natürlichen Zahlen bilden mit Addition und Multiplikation einen kommutativen Halbring $(\mathbb{N}, +, \cdot)$ mit 0- und 1-Element.

Wie die natürlichen Zahlen zum Ring der ganzen Zahlen erweitert werden können, kann auch jeder andere kommutative Halbring zu einem Ring erweitert werden. Das Verfahren dieser Vervollständigung wird nach Grothendieck benannt.

**Lemma 4.4.** *Sei $(H, +, \cdot)$ ein kommutativer Halbring. Dann wird durch*

$$(h_1, h_2) \sim (h_1', h_2') \quad \Leftrightarrow \quad \text{es gibt ein } h \in H \text{ mit } h_1 + h_2' + h = h_1' + h_2 + h$$

*eine Äquivalenzrelation auf $H \times H$ definiert.*

*Beweis.* Die Reflexivität ist klar.

Die Symmetrie folgt aus der Kommutativität der Addition.

Sei nun $(h_1, h_2) \sim (h_1', h_2')$ und $(h_1', h_2') \sim (h_1'', h_2'')$ dann gibt es $h, \bar{h} \in H$, so dass gilt:

$$\begin{array}{rcl} h_1 + h_2' + h & = & h_1' + h_2 + h \\ h_1' + h_2'' + \bar{h} & = & h_1'' + h_2' + \bar{h} \\ \hline h_1 + h_2'' + \underbrace{h + h_1' + h_2' + \bar{h}}_{=\tilde{h}} & = & h_1'' + h_2 + \underbrace{h + h_1' + h_2' + \bar{h}}_{=\tilde{h}} \end{array}$$

Somit gibt es ein $\tilde{h} \in H$ mit $h_1 + h_2'' + \tilde{h} = h_1'' + h_2 + \tilde{h}$ und $(h_1, h_2)$ und $(h_1', h_2')$ sind äquivalent. Damit ist die Transitivität bewiesen. □

**Bemerkung 4.5.** Die Äquivalenzklassen $[(h_1, h_2)]$ kann man sich als Differenz $h_1 - h_2$ vorstellen.

**Proposition 4.6.** *Die Äquivalenzklassen $[(h_1, h_2)] \in H \times H$ bilden mit der Addition*

$$[(h_1, h_2)] + [(h_1', h_2')] := [(h_1 + h_1', h_2 + h_2')]$$

*und der Multiplikation*

$$[(h_1, h_2)] \cdot [(h_1', h_2')] := [(h_1 \cdot h_1' + h_2 \cdot h_2', h_1 \cdot h_2' + h_1' \cdot h_2)]$$

*einen kommutativen Ring*

$$\hat{H} = H \times H / \sim$$

*Der Halbring $H$ ist in $\hat{H}$ eingebettet:*

$$\begin{aligned} H &\longrightarrow \hat{H} \\ h &\longmapsto [(h,0)] \end{aligned}$$

**Definition 4.7.** Die Grothendieck Vervollständigung der Permutationsdarstellungen einer Gruppe $G$ wird Burnside Ring genannt.

$$B(G) \coloneqq (\widehat{PREP(G)}, +, \times)$$

**Proposition 4.8.** *Die endlichen Permutationsdarstellungen einer Gruppe $G$ sind isomorph zur freien abelschen Halbgruppe, die von den Konjugationsklassen der Untergruppen von $G$ erzeugt wird.*

$$PREP(G) \simeq \mathbb{N} \cdot \mathcal{U}(G)/c$$

*Beweis.* Eine endliche Permutationsdarstellung der Gruppe $G$ ist bis auf Isomorphie gegeben durch:

$$\rho : G \curvearrowright X \simeq [n]$$

Für jedes $i \in [n]$ bilden die Bahnen $Gi$ nach Proposition 1.48 eine disjunkte Zerlegung von $[n]$. Zu jeder Bahn gibt es nach Proposition 1.52 eine Bijektion zur Linksnebenklasse des entsprechenden Stabilisators:

$$Gi \simeq G/G_i$$

Dabei sind die Stabilisatoren $G_i$ nach Proposition 1.56 bis auf Konjugation Untergruppen von $G$. □

**Beispiel 4.9.** Wir betrachten endliche Permutationsdarstellungen der zyklischen Gruppe.

$$G = \underbrace{C_n}_{\simeq \mathbb{Z}/n} = \langle e^{\frac{2\pi i}{n}} \rangle \subset U_1 \subset \mathbb{C}$$

Da $C_n$ abelsch ist, ist die Konjugation trivial und es gilt:

$$\mathcal{U}(C_n)/c = \mathcal{U}(C_n)$$

Für jeden Teiler $d \mid n$ gibt es eine Untergruppe $U \leq C_n$ und umgekehrt. Es gilt also

$$PREP(G) \simeq \bigoplus_{d \mid n} \mathbb{N} \cdot \rho_d$$

Dabei ist die Permutationsdarstellung $\rho_d$ gegeben durch:

$$\begin{aligned} \rho_d : C_n &\curvearrowright [d] \simeq \mathbb{Z}/d \\ (e^{\frac{2\pi i}{n}}, j) &\mapsto 1 + j \end{aligned}$$

## 4.2. Erzeugende Funktion von Permutationsdarstellungen

**Bemerkung 4.10.** Mit dem Grad einer Permutationsdarstellung ist ein Halbring-Homomorphismus in die natürlichen Zahlen gegeben.

$$\begin{aligned} deg : PREP(G) &\longrightarrow \mathbb{N} \\ \rho : G \curvearrowright X &\longmapsto |X| \end{aligned}$$

Denn für $\rho : G \curvearrowright X$ und $\rho' : G \curvearrowright X'$ gilt

$$\begin{aligned} deg(\rho + \rho') &= deg(\rho) + deg(\rho') \\ deg(\rho \times \rho') &= deg(\rho) \cdot deg(\rho') \end{aligned}$$

Damit kann eine erzeugende Funktion mit den Anzahlen der Permutationsdarstellungen einer gegebenen Gruppe $G$ in Form einer formalen Potenzreihe aufgestellt werden.

$$\begin{aligned} p_t(G) &= \sum_{n=0}^{\infty} a_n t^n \\ \text{mit } a_n &= |\{ \rho : G \curvearrowright X \mid |X| = n \}| \\ &= |deg^{-1}(n)| \end{aligned}$$

**Proposition 4.11.** *Die erzeugende Funktion von Permutationsdarstellungen einer Gruppe $G$ läßt sich als Produkt schreiben.*

$$p_t(G) = \prod_{[U] \in \mathcal{U}(G)/c} (1 - t^{|G:U|})^{-1} \qquad (p_t)$$

*Beweis.* □

**Beispiel 4.12.** In diesem Beispiel wird die erzeugende Funktion der Permutationsdarstellungen der Kleinschen Vierergruppe $G = C_2 \times C_2$ untersucht. Mit $C_2 = \{ 1, \alpha \}$

enthält $G$ die Elemente

$$\begin{aligned} e &= (1,1) \\ a &= (\alpha,1) \\ b &= (1,\alpha) \\ c &= (\alpha,\alpha) = ab \end{aligned}$$

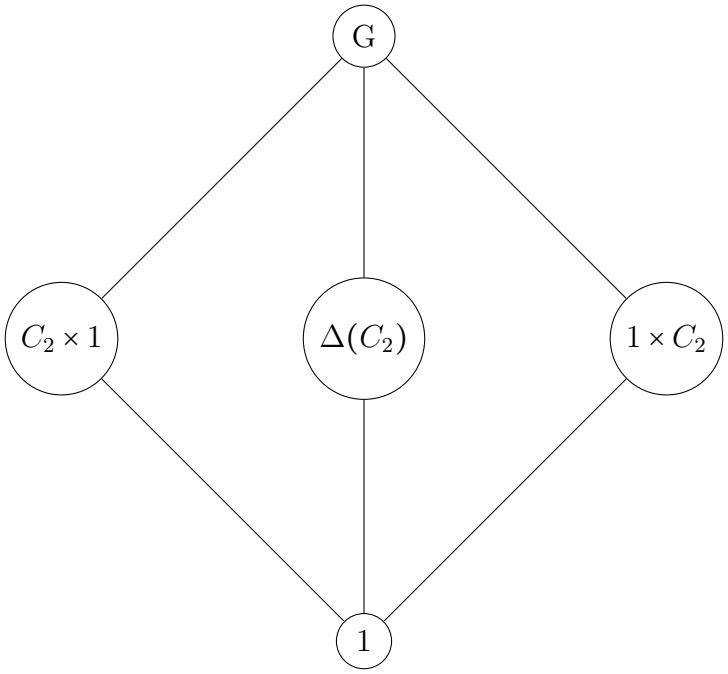
mit der Verknüpfungstabelle

| $\circ$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ |

Dabei sind die Untergruppen

$$\begin{aligned} C_2 \times 1 &= \{(1,1),(1,\alpha)\} = \{1, a\} \\ 1 \times C_2 &= \{(1,1),(\alpha,1)\} = \{1, b\} \\ \Delta(C_2) &= \{(1,1),(\alpha,\alpha)\} = \{1, c\} \end{aligned}$$

farbig hinterlegt. Da die Kleinsche Vierergruppe kommutativ und somit die Konjugation trivial ist, sind diese drei Untergruppen nicht konjugiert.



Nach der Formel $(p_t)$ erhalten wir für die erzeugende Funktion der Permutationsdarstellungen der Kleinschen Vierergruppe also

$$\begin{aligned} p_t(C_2 \times C_2) &= (1-t)^{-1} \cdot (1-t^2)^{-3} \cdot (1-t^4)^{-1} \\ &= 1 + t + 4t^2 + 4t^3 + 11t^4 + 11t^5 + 24t^6 + \cdots \end{aligned}$$

Aus den Koeffizienten kann man ablesen, dass es eine Permutationsdarstellung zur leeren Menge und eine zu einelementigen Mengen, die wir als isomorph betrachten, gibt. Wir geben nun die vier Permutationsdarstellungen der Kleinschen Gruppe auf eine 2-elementige Menge $X = \{\triangle, \diamond\}$ an. Wegen $c = ab$ kann $ax = bx = cx = abx = aax = ex$ nur für $ax = bx = cx = ex = x$ gelten. Aus $ax = y \neq x$ folgt aber $ay = x$ sowie $cx = by$ und $bx = cy$, so dass mit der Wahl von $bx$ die Permutationsdarstellung fest liegt. Dies führt auf folgende 4 Permutationsdarstellungen:

| | $\triangle$ | $\diamond$ | $\triangle$ | $\diamond$ | $\triangle$ | $\diamond$ | $\triangle$ | $\diamond$ |
|---|---|---|---|---|---|---|---|---|
| $e$ | $\triangle$ | $\diamond$ | $\triangle$ | $\diamond$ | $\triangle$ | $\diamond$ | $\triangle$ | $\diamond$ |
| $a$ | $\triangle$ | $\diamond$ | $\triangle$ | $\diamond$ | $\diamond$ | $\triangle$ | $\diamond$ | $\triangle$ |
| $b$ | $\triangle$ | $\diamond$ | $\diamond$ | $\triangle$ | $\triangle$ | $\diamond$ | $\diamond$ | $\triangle$ |
| $c$ | $\triangle$ | $\diamond$ | $\diamond$ | $\triangle$ | $\diamond$ | $\triangle$ | $\triangle$ | $\diamond$ |
| *Orbits* | $G\triangle = \{\triangle\}$ | $G\diamond = \{\diamond\}$ | $G\triangle = G\diamond = \{\triangle, \diamond\}$ | | $G\triangle = G\diamond = \{\triangle, \diamond\}$ | | $G\triangle = G\diamond = \{\triangle, \diamond\}$ | |
| *Stab* | $G_\triangle = G$ | $G_\diamond = G$ | $G_\triangle = G_\diamond = C_2 \times 1$ | | $G_\triangle = G_\diamond = 1 \times C_2$ | | $G_\triangle = G_\diamond = \Delta(C_2)$ | |

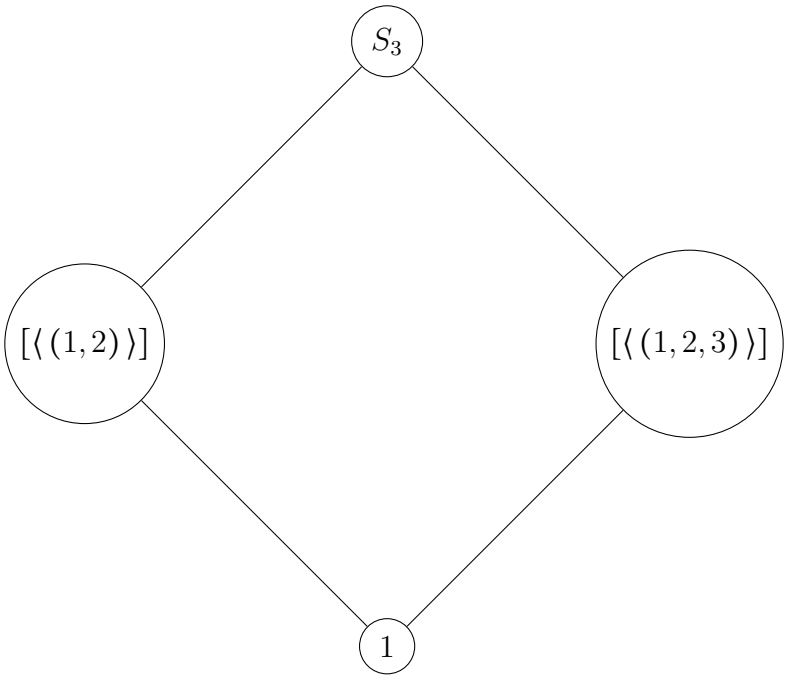
Die gleichen Permutationsdarstellungen erhalten wir auch für eine 3-elementige Menge $X = \{\triangle, \diamond, \star\}$. Denn alle vier angegebenen Permutationdarstellungen für zweielementige Mengen müssen das dritte Element in sich überführen. Für $x \neq y \neq z \in X$ gilt nämlich

$$\begin{aligned} & ax = y \quad | \cdot a \\ \Rightarrow \quad & ay = x \\ \text{wäre} \quad & az = x \quad | \cdot a \\ \Rightarrow \quad & z = ax = y \ \lightning \\ \text{somit} \quad & az = z \quad | \cdot c \\ \Rightarrow \quad & bz = cz \\ \text{wäre} \quad & bz = cz = x \quad | \cdot a \\ \Rightarrow \quad & cz = bz = ax = y \ \lightning \\ \text{somit} \quad & bz = cz = z \end{aligned}$$

**Beispiel 4.13.** In diesem Beispiel leiten wir die erzeugende Funktion der Permutationsdarstellungen der symmetrischen Gruppe $G = S_3$ her. In Zykeldarstellung sind die Elemente folgende Permutationen

$$S_3 = \{1\,,\,(1,2)\,,\,(2,3)\,,\,(1,3)\,,\,(1,2,3)\,,\,(1,3,2)\,\}$$

Die symmetrische Gruppe hat drei zueinander konjugierte Untergruppen der Ordnung 2 und eine Untergruppe der Ordnung 3.




Nach der Formel $(p_t)$ erhalten wir für die erzeugende Funktion der Permutationsdarstellungen der Kleinschen Vierergruppe also

$$\begin{aligned} p_t(S_3) &= (1-t)^{-1}\cdot(1-t^2)^{-1}\cdot(1-t^3)^{-1}\cdot(1-t^6)^{-1} \\ &= 1+t+2t^2+3t^3+4t^4+5t^5+8t^6+9t^7+\cdots \end{aligned}$$

Aus den Koeffizienten kann man ablesen, wieviele Permutationsdarstellungen es zu isomorphen $n$-elementigen Mengen gibt.

# 5. Primitive Permutationsdarstellungen

## 5.1. Rang einer transitiven Permutationsdarstellung

Wie wir in Definition 1.49 und Proposition 1.50 gesehen haben, ist eine Permutationsdarstellung $\rho : G \curvearrowright X$ transitiv, wenn es nur einen Orbit $X = Gx$ gibt.

Die Operation $\rho_x : G_x \curvearrowright X$ eines Stabilisators von $\rho$ ist jedoch im allgemeinen nicht mehr transitiv. Nach Proposition 1.56 sind alle Stabilisatoren $G_{gx} = g\,G_x\,g^{-1}$ konjugiert und die Anzahl der $G_x$-Orbits in $X$ ist unabhängig von $x \in X$.

**Definition 5.1.** Die Gruppe $G$ operiere transitiv auf der Menge $X$ ($\rho : G \curvearrowright X$). Die Anzahl der Orbits der Operation $\rho_x : G_x \curvearrowright X$ von einem Stabilisator $G_x$ von $\rho$ auf die Menge $X$ heisst Rang $rk(\rho)$.

**Lemma 5.2.** *Der Rang einer transitiven Operation $\rho : G \curvearrowright X$ ist die Anzahl der $G$-Orbits auf $X \times X$.*

*Beweis.* Die Operation $\rho_\times : G \curvearrowright X \times X$ ist definiert durch

$$\begin{array}{rcl} G \times (X \times X) & \longrightarrow & X \times X \\ (g, x, y) & \longmapsto & (gx, gy) \end{array}$$

Ein typischer Orbit der Operation $G \curvearrowright X \times X$ ist gegeben durch:

$$\begin{aligned} G(x,y) &= \{\,(gx, gy) \mid g \in G\} \\ &= \{\,(x, gy) \mid g \in G\} \quad \text{da } \rho \text{ transitiv ist} \\ &= \{\,gy \mid g \in G \text{ und } gx = x\,\} \\ &= \{\,gy \mid g \in G_x\,\} \\ &= G_x y \end{aligned}$$

Das heisst, die Orbits $G(x, y)$ der Operation $\rho_\times$ stimmen mit den Orbits der Operation $\rho_x : G_x \curvearrowright X$ überein und daher auch ihre Anzahl. □

**Theorem 5.3.** *Der Rang einer transitiven Operation $\rho : G \curvearrowright X$ steht in Zusammenhang mit der Mächtigkeit der Fixpunktmengen. Es gilt die Formel:*

$$rk(\rho) = \frac{1}{|G|} \cdot \sum_{g \in G} |X^g|^2$$

*Beweis.* Wie beim Beweis des Lemmas von Burnside 1.67 betrachten wir den zweigeteilten Graph, dessen Ecken aus den Elementen der Gruppe $G$ und der Menge $X \times X$

bestehen. Eine Kante zwischen $g \in G$ und $(x, y) \in X \times X$ liegt genau dann vor, wenn $(gx, gy) = (x, y)$ gilt. Andere Kanten sind nicht zugelassen. Die Anzahl der Kanten ausgehend von den Gruppenelementen sind genau die Summe der Anzahlen in den Fixpunktmengen $(X \times X)^g = X^g \times X^g$ für alle $g \in G$.

$$\sum_{g \in G} |(X \times X)^g| = \sum_{g \in G} |X^g|^2$$

Die Anzahl der Kanten ausgehend von den Elementen in $X$ erhalten wir aus der Summe der Anzahlen in den Stabilisatoren $G_{(x,y)}$.

$$\begin{aligned}
\sum_{(x,y) \in X \times X} |G_{(x,y)}| &= \sum_{(x,y) \in X \times X} \frac{|G|}{|G(x,y)|} \\
&= \sum_{[(x,y)] \in (X \times X)/G} |G(x,y)| \, \frac{|G|}{|G(x,y)|} \\
&= |G| \cdot |(X \times X)/G| \\
&= |G| \cdot rk(\rho) \quad \text{nach Lemma 5.2}
\end{aligned}$$

Durch Gleichsetzung folgt die Behauptung. □

## 5.2. Blockzerlegung von Permutationsdarstellungen

Bei der Klassifizierung einfacher Gruppen (siehe Definition 1.19) sind die Eigenschaften von Wirkungen der Gruppe von großer Bedeutung. Eine stärkere Eigenschaft als die Transitivität ist die Primitivität, die wir nun erläutern.

**Definition 5.4.** Die Gruppe $G$ wirke auf die Menge $X$. Eine nichtleere Teilmenge $\varnothing \neq B \subseteq X$ heisst Block, wenn für alle $g \in G$ gilt:

$$g \circ B = B \quad \text{oder} \quad (g \circ B) \cap B = \varnothing$$

Ein Block heisst trivial, wenn er entweder nur aus einem Element besteht ($B = \{ x \}$) oder ganz $X$ umfasst ($B = X$).

**Proposition 5.5.** *Wenn $B \subseteq X$ ein Block ist, dann ist auch $gB$ für alle $g \in G$ ein Block.*

*Beweis.* Wir nehmen an, für ein $h \in G$ ist $gB \cap hgB \neq \varnothing$. Dann ist $gB$ ein Block, wenn $gB = hgB$ gilt. Aus $gB \cap hgB \neq \varnothing$ folgt $B \cap g^{-1}hgB \neq \varnothing$. Da $B$ ein Block ist, muss also $B = g^{-1}hgB$ gelten. Und daraus folgt $gB = hgB$. □

Für transitive Permutationsdarstellungen $\rho : G \curvearrowright X$ gibt es interessante Eigenschaften von Blöcken.

**Theorem 5.6.** *Sei $\rho : G \curvearrowright X$ eine transitive Permutationsdarstellung mit $|X| = n$ und $B \subseteq X$ ein nichttrivialer Block. Dann gibt es Elemente $g_1, \cdots, g_m \in G$, so dass*

$$Y = \{ g_1 B, \cdots, g_m B \}$$

*eine Partition von $X$ ist. Das heisst*

$$X = \bigsqcup_{i=1}^{m} g_i B$$

*Die Blockgröße $|B|$ teilt $n$.*
*Auf $Y$ wird eine transitive Operation von $G$ induziert.*

*Beweis.* Da der Block $B$ nichttrivial ist, gibt es Elemente

$$\begin{aligned} b &\in B \\ \text{und} \quad x_1 &\in X \setminus B \end{aligned}$$

Da $G$ auf $X$ transitiv operiert, gibt es ein $g_1 \in G$ mit $g_1 b = x_1$. Nun ist $x_1 \in g_1 B \setminus B$. Somit ist $g_1 B \neq B$. Da $B$ ein Block ist, muss also $g_1 B \cap B = \varnothing$ gelten. Falls $X = B \cup g_1 B$ ist, ist $Y = \{ B, g_1 B \}$ die behauptete Partition von $X$. Andernfalls wählen wir $x_2 \in X \setminus (B \cup g_1 B)$ und $g_2 \in G$ mit $g_2 b = x_2$. Da $B$ ein Block ist, muss $g_2 B \cap B = \varnothing$ gelten. Da $g_1 B$ ebenfalls ein Block und $x_1 \neq x_2$ ist, muss $g_2 B \cap g_1 B = \varnothing$ gelten. Daraus folgt $g_2 B \cap (B \cup g_1 B) = \varnothing$. Da $X$ endlich ist, erhält man nach endlich vielen Schritten die behauptete Partition von $X$.

Alle Blöcke $g_i B$ haben wegen $g_i B = B$ dieselbe Anzahl von Elementen. Somit gilt

$$|X| = m \cdot |B|$$

Zum Nachweis der Transitivität der Permutationsdarstellung $G \curvearrowright Y$ betrachten wir zwei Blöcke $g_i B, g_j B \in Y$ und ein $x \in B$. Da $G$ auf $X$ transitiv operiert, gibt es ein $g \in G$ mit $g(g_i x) = (g_j x)$. Daraus folgt

$$\begin{aligned} \varnothing &\neq g\, g_i\, B \cap g_j\, B \\ &= (g\, g_i\, g_j^{-1})\, g_j\, B \cap g_j\, B \end{aligned}$$

Da $g_j\, B$ ein Block ist, muss also $(g\, g_i\, g_j^{-1})\, g_j\, B = g\, g_i\, B = g_j\, B$ gelten. Damit ist die

Transitivität von $G \curvearrowright Y$ bewiesen. □

**Definition 5.7.** Sei $\rho : G \curvearrowright X$ eine Permutationsdarstellung. Eine Äquivalenzrelation $\sim$ auf $X$ heisst $\rho$-äquivariant oder $G$-invariant, wenn mit $x \sim y$ auch $g \circ x \sim g \circ y$ für alle $g \in G$ gilt.

**Bemerkung 5.8.** Es gibt zwei triviale $\rho$-äquivariante Äquivalenzrelationen auf $X$.

(i) $x \sim y \quad \Leftrightarrow \quad x = y$

(iI) $x \sim y \quad$ für alle $\quad x, y \in X$

**Bemerkung 5.9.** Die Äquivalenzklassen einer $\rho$-äquivarianten Äquivalenzrelationen auf $X$ sind Blöcke.

**Theorem 5.10.** *Sei $\rho : G \curvearrowright X$ eine transitive Permutationsdarstellung und $G_x$ für ein $x \in X$ der Stabilisator. Eine Teilmenge $G_x \subseteq K \subseteq G$ ist genau dann eine Untergruppe in $G$, wenn $K \circ x$ ein Block ist.*

*Anders formuliert: Für alle Blöcke $B$ mit $x \in B$ gibt es eine Untergruppe $K \leq G$ mit $G_x \leq K$ und $B = K \circ x$.*

*Beweis.* Sei $K$ eine Untergruppe in $G$ mit $G_x \leq K$. Dann ist zu zeigen, dass $K \circ x$ ein Block ist.
Für $g \in G$ mit $g \circ (K \circ x) \cap K \circ x = \varnothing$ ist die zweite Blockeigenschaft erfüllt. Annahme: Für ein $g \in G$ sei $g \circ (K \circ x) \cap K \circ x \neq \varnothing$. Dann gibt es $\alpha, \beta \in K$ mit $g \cdot \alpha \circ x = \beta \circ x$. Dann folgt:

$$\begin{array}{lrcll} & \beta^{-1} \cdot g \cdot \alpha \circ x & = & x & \\ \Rightarrow & \beta^{-1} \cdot g \cdot \alpha & \in & G_x & \leq K \\ \Rightarrow & \beta \cdot \beta^{-1} \cdot g \cdot \alpha \cdot \alpha^{-1} & = & g & \in K \\ \Rightarrow & K \circ x & = & g \circ K \circ x & \end{array}$$

Somit erfüllt $K \circ x$ die erste Blockeigenschaft.

Sei umgekehrt $B$ ein Block mit $x \in B$. Dann definieren wir die Menge $K$ durch:

$$K = \{\, g \in G \,|\, g \circ B = B \,\}$$

Die Standgruppe $G_x$ ist Teilmenge in $K$. Denn für alle $g \in G_x$ gilt

$$\begin{array}{lrcll} & g \circ x & = & x & \\ \Rightarrow & g \circ B \cap B & \neq & \varnothing & \\ \Rightarrow & g \circ B & = & B & \text{da } B \text{ ein Block ist} \end{array}$$

Wir zeigen nun, dass $K$ eine Gruppe ist. Seien dazu $g, h \in K$.

$$\begin{array}{rrcl} & g \circ B & = & B \quad \text{und} \quad h \circ B = B \\ \Rightarrow & (g \cdot h) \circ B & = & g \circ B = B \\ \Rightarrow & g \cdot h & \in & K \end{array}$$

Somit liegt das Produkt von zwei Elementen in $K$ wieder in $K$. Für $g \in K$ berechnen wir das inverse Element wie folgt:

$$\begin{array}{rrcl} & g \circ B & = & B \quad \text{und} \quad y \in B \\ \Rightarrow \text{ es gibt ein } & w & \in & B \quad \text{mit} \quad g \circ w = y \\ \Rightarrow & g^{-1} \circ y & = & w \\ \Rightarrow & g^{-1} & \in & K \end{array}$$

Somit ist $K$ eine Untergruppe in $G$ und es gilt

$$G_x \leq K \leq G$$

Nach Definition von $K$ gilt $g \circ B = B$ für alle $g \in K$ also insbesondere $g \circ x \in B$. Daraus folgt $K \circ x \subseteq B$.

Der Beweis der anderen Inklusion benutzt die Voraussetzung, dass $G$ transitiv auf $X$ wirkt. Sei also $\delta \in B$ beliebig. Wir müssen zeigen, dass $\delta$ auch in $K \circ x$ liegt. Da $G$ transitiv auf $X$ wirkt, existiert ein $g \in G$, so dass $g \circ x = \delta$ ist. Daraus folgt

$$\begin{array}{rrcl} & \delta & \in & B \cap g \circ B \\ \Rightarrow & g \circ B & = & B \\ \Rightarrow & g & \in & K \\ \Rightarrow & B & \subseteq & K \circ x \end{array}$$

□

**Bemerkung 5.11.** Ein Block $B$ mit $x \in B$ korrespondiert also mit einer Untergruppe $K$ in $G$, die wiederum die Standgruppe $G_x$ enthält.

$$G_x \leq K \leq G$$

Die Standgruppe $G_x$ ist also genau dann maximal, wenn es keine Blöcke $B$ mit $x \in B$ gibt ausser

$$\begin{array}{rcl} B = X & \longleftrightarrow & K = G \quad \text{oder} \\ B = \{x\} & \longleftrightarrow & K = G_x \end{array}$$

**Definition 5.12.** Eine transitive Permutationsdarstellung $\rho : G \curvearrowright X$ heisst primitiv, wenn sie nur triviale Blockzerlegungen zuläßt.

Aus Theorem 5.10 erhalten wir als Folgerung eine andere Kennzeichnung der Primitivität.

**Korollar 5.13.** *Eine transitive Permutationsdarstellung $\rho : G \curvearrowright X$ ist genau dann primitiv, wenn für alle $x \in X$ der Stabilisator $G_x$ eine maximale Untergruppe in $G$ ist. Das heisst, für alle $x \in X$ gilt:*

$$G_x = \begin{cases} G_x & \textit{oder} \\ G \end{cases}$$

Nach Theorem 5.6 teilt bei transitiven Permutationsdarstellung $\rho : G \curvearrowright X$ die Blockgröße die Größe von $X$. Daraus folgt:

**Lemma 5.14.** *Transitive Permutationsdarstellungen $\rho : G \curvearrowright X$ vom Grad $p \in \mathbb{P}$ sind stets primitiv.*

# 6. Mehrfach transitive Operationen

**Definition 6.1.** Sei $G \curvearrowright X$ eine Permutationsdarstellung. Die Menge disjunkter $k$-Tupel in $X$ sei

$$X^{[k]} = \{ (x_1, x_2, \cdots, x_k) \,|\, x_i \neq x_j \text{ für alle } i \neq j \}$$

Die Operation $G \curvearrowright X$ ist genau dann $k$-fach transitiv, wenn die Operation $G \curvearrowright X^{[k]}$ transitiv ist.

**Bemerkung 6.2.** Die 1-Transitivität stimmt mit der bereits in 1.49 definierten Transitivität überein.

**Bemerkung 6.3.** Die Operation $G \curvearrowright X$ ist genau dann $k$-fach transitiv, wenn es für alle disjunkten $k$-Tupel $(x_1, x_2, \cdots, x_k)$, $(y_1, y_2, \cdots, y_k) \in X^{[k]}$ ein Element $g \in G$ gibt, so dass für alle $1 \leq i \leq k$ $gx_i = y_i$ gilt.

**Definition 6.4.** Für ein $(x_1, x_2, \cdots, x_k) \in X^{[k]}$ heisst die Untergruppe

$$\begin{aligned} G_{x_1, x_2, \cdots, x_k} &= \{ g \in G \,|\, gx_i = x_i \text{ für } 1 \leq i \leq k \} \\ &= \bigcap_{i=1}^{k} G_{x_i} \end{aligned}$$

$k$-facher Stabilisator.

**Bemerkung 6.5.** Für ein disjunktes $k$-Tupel $(x_1, x_2, \cdots, x_k) \in X^{[k]}$ bilden die $j$-fachen Stabilisatoren $(1 \leq j \leq k)$ eine Kette von Untergruppen:

$$G \geq G_{x_1} \geq G_{x_1 x_2} \geq \cdots \geq G_{x_1 x_2 \cdots x_k}$$

Wenn die Permutationsdarstellung $G \curvearrowright X$ $k$-transitiv ist, dann ist sie auch $(k-1)$-transitiv.

**Bemerkung 6.6.** Wenn $n = |X|$ die Anzahl der Elemente in $X$ ist, dann hat die Menge der disjunkten $k$-Tupel folgende Mächtigkeit:

$$|X^{[k]}| = n \cdot (n-1) \cdots (n-k+1)$$

Für eine $k$-transitive Permutationsdarstellung $G \curvearrowright X$ gilt somit:

$$|G| = n \cdot (n-1) \cdots (n-k+1) \cdot |G_{x_1 x_2 \cdots x_k}|$$

Ist eine $k$-transitive Permutationsdarstellung $G \curvearrowright X$ überdies effektiv oder treu, dann ist die Gruppe $G \hookrightarrow S_n$ in der symmetrischen Gruppe $S_n$ eingebettet. Die Ordnung von $G$ ist dann Teiler von $n!$ und die Ordnung der $k$-fachen Stabilisatoren $G_{x_1 x_2 \cdots x_k}$ teilt $(n-k)!$.

**Definition 6.7.** Die Operation $G \curvearrowright X$ ist scharf $k$-fach transitiv, wenn die Operation $G \curvearrowright X^{[k]}$ regulär, das heisst transitiv und frei, ist.

**Proposition 6.8.** *Die Permutationsdarstellung $G \curvearrowright X^{[k]}$ ist frei, wenn eine der folgenden Bedingungen erfüllt ist.*

*(i) Aus $gx_i = x_i$ für alle $1 \leq i \leq k$ folgt $g = 1$.*

*(ii) Wenn $gx_i = y_i$ für alle $1 \leq i \leq k$ gilt, ist $g$ eindeutig bestimmt.*

*(iii) Für ein $k$-Tupel $(x_1 \cdots x_k) \in X^{[k]}$ ist der $k$-fache Stabilisator $G_{x_1 \cdots x_k}$ trivial. Dies gilt dann auch für alle $k$-Tupel.*

Als Folgerung erhalten wir:

**Korollar 6.9.** *Die Ordnung einer scharf $k$-fach transitiven Permutationsdarstellung $G \curvearrowright X$ ist:*

$$|G| = n \cdot (n-1) \cdots (n-k+1)$$

*Die Permutationsdarstellung ist dann auch effektiv oder treu.*

## 6.1. Triviale Beispiele für k-fache Transitivität

**Beispiel 6.10.** Die symmetrische Gruppe $S_n$ wirkt auf die Menge $[n]$ $n$-transitiv und damit auch $k$-transitiv für $1 \leq k \leq n$. Denn für jedes $n$-Tupel $(x_1 \cdots x_n) \in [n]^{[n]}$ gibt es eine Permutation $\sigma \in S_n$ mit $(x_1 \cdots x_n) = \sigma(1 \cdots n)$.

Die Wirkung ist auch scharf $n$-transitiv. Denn wenn für ein $n$-Tupel $gx_i = x_i$ für alle $1 \leq i \leq n$ gilt, dann muss $g$ die Identität sein.

**Beispiel 6.11.** Die alternierende Gruppe $A_n$ wirkt auf die Menge $[n]$ $(n-2)$-transitiv für$n \geq 3$ und damit auch $k$-transitiv für $1 \leq k \leq n-2$. Denn zu jedem $(n-2)$-Tupel $(x_1 \cdots x_{n-2})$ gibt es genau ein Paar $(x_{n-1}, x_n)$, so dass $(x_1 \cdots x_n)$ ein $n$-Tupel mit Signum $+1$ ist.

Die Wirkung ist auch scharf $(n-2)$-transitiv. Denn wenn für ein $(n-2)$-Tupel $gx_i = x_i$ für alle $1 \leq i \leq n-2$ gilt, dann kann diese nur auf eine Weise zu einem $n$-Tupel mit Signum $+1$ ergänzt werden und $g$ muss dann die Identität sein.

Diese beiden naheliegenden Beispiele heissen auch trivial.

Die $k$-Transitivität stellt eine starke Bedingung an die Gruppe dar wie das folgende Theorem zeigt.

**Theorem 6.12.** *Sei $G \curvearrowright X$ eine endliche, effektive (treue) und $k$-transitive Permutationsdarstellung mit $k \geq 4$. Dann gilt:*

$k = 4$ *Die Operation $G \curvearrowright X$ ist trivial oder die Gruppe $G$ ist isomorph zu einer der Mathieu Gruppen $M_{11}$, $M_{12}$, $M_{23}$ oder $M_{24}$.*

$k = 5$ *Die Operation $G \curvearrowright X$ ist trivial oder die Gruppe $G$ ist isomorph zu einer der Mathieu Gruppen $M_{12}$ oder $M_{24}$.*

$k \geq 6$ *Hier gibt es nur noch die triviale Operation $G \curvearrowright X$ mit den Gruppen $S_n$ oder $A_n$.*

*Beweis.* Der Beweis wurde erst 1999 von Peter Cameron in [Cam99] gegeben und benötigt einige Ergebnisse aus der Klassifizierung einfacher Gruppen. □

**Bemerkung 6.13.** Die Mathieu Gruppe $M_{22}$ ist 3-transitiv.

Die mehrfache Transitivität ist also wichtig beim Nachweis der Einfachheit einer Gruppe. Einige einfache Gruppen sind jedoch nicht 2-transitiv. Bei diesen genügt die Transitivität und Primitivität.

**Lemma 6.14.** *Jede 2-transitive Operation $G \curvearrowright X$ ist primitiv.*

*Beweis.* Wir nehmen an, die Operation wäre nicht primitiv. Dann gibt es einen nichttrivialen Block $B$ und Elemente $x \neq y \in B$ und $z \notin B$. Da die Operation als 2-transitiv vorausgesetzt ist, gibt es ein Element $g \in G$ in der Gruppe mit

$$\left.\begin{array}{rcl} gx & = & x \\ gy & = & z \end{array}\right\} \Rightarrow \left\{\begin{array}{rcl} gB & \neq & B \\ gB \cap B & \neq & \varnothing \end{array}\right.$$

Dies widerspricht der Blockeigenschaft von $B$. □

Eine weitere Kennzeichnung der $k$-Transitivität wird im folgenden Reduktionslemma beschrieben.

**Lemma 6.15.** *Reduktionslemma*

*a) Eine Permutationsdarstellung $G \curvearrowright X$ ist genau dann $k$-transitiv, wenn für alle $x \in X$ die Stabilisatoren $G_x$ auf $X \setminus \{x\}$ $(k-1)$-transitiv operieren. Dabei ist $k \geq 2$ vorausgesetzt.*

*Dieselbe Aussage gilt für scharfe $k$-Transitivität.*

*b) Wenn in einer transitiven Permutationsdarstellung $G \curvearrowright X$ ein $x \in X$ existiert, so dass der Stabilisator $G_x$ $(k-1)$-transitiv auf $X$ operiert, dann ist $G \curvearrowright X$ $k$-transitiv.*

*Beweis.* ad a) Sei $G \curvearrowright X$ $k$-transitiv und $x \in X$ beliebig. Wir wählen zwei $(k-1)$-Tupel:

$$\begin{array}{rcl} (x_1, \cdots, x_{k-1}) & \in & (X \setminus \{x\})^{[k-1]} \\ (y_1, \cdots, y_{k-1}) & \in & (X \setminus \{x\})^{[k-1]} \end{array}$$

Diese können mit $x$ zu $k$-Tupeln ergänzt werden.

$$\begin{array}{rcl} (x_1, \cdots, x_{k-1}, x) & \in & X^{[k]} \\ (y_1, \cdots, y_{k-1}, x) & \in & X^{[k]} \end{array}$$

Da $G$ auf $X$ $k$-transitiv operiert, gibt es ein $g \in G$ mit

$$\begin{array}{rcll} y_i & = & gx_i & \text{für } 1 \leq i \leq k-1 \\ \text{und} \quad x & = & gx & \\ \text{also} \quad x & \in & G_x & \end{array}$$

Daraus folgt, dass $G_x$ auf $X \setminus \{x\}$ $(k-1)$-transitiv operiert.

Umgekehrt operiere $G_x$ für jedes $x \in X$ auf $X \setminus \{x\}$ $(k-1)$-transitiv. Für zwei $k$-Tupel

$$\begin{aligned}(x_1, \cdots, x_{k-1}, x_k) &\in X^{[k]} \\ (y_1, \cdots, y_{k-1}, y_k) &\in X^{[k]}\end{aligned}$$

gibt es ein $g \in G_{x_k}$ mit $y_i = gx_i$ für $1 \leq i \leq k-1$ sowie $g' \in G_{y_1}$ mit $y_i = g'y_i$ für $2 \leq i \leq k-1$ und $y_k = g'x_k$. Somit existiert $g'g \in G$ mit $y_i = g'gx_i$ für $1 \leq i \leq k$. Dies zeigt die $k$-Transitivität.

ad b) Hier ist zusätzlich die Transitivität von $G \curvearrowright X$ vorausgesetzt. Es genügt zu zeigen, dass ein vorgegebenes $k$-Tupel $(x_1, x_2, \cdots, x_{k-1}, x)$ mit einem Element $\tilde{g} \in G$ auf ein beliebiges $k$-Tupel $(y_1, y_2, \cdots, y_{k-1}, y_k)$ abgebildet werden kann. Da $G$ auf $X$ transitiv operiert, gibt es ein $g \in G$ mit $g \circ x = y_k$. Im Stabilisator $G_x$ gibt es wegen der $(k-1)$-Transitivität ein $h \in G_x$ mit

$$h \circ x_i = g^{-1} \circ y_i \quad \text{für alle } 1 \leq i \leq k-1$$

Aus $h \in G_x$ folgt $h \circ x = x$. Für $\tilde{g} = g \cdot h$ gilt also

$$\begin{aligned}\tilde{g} \circ x_i = (g \cdot h) \circ x_i &= y_i \quad \text{für alle } 1 \leq i \leq k-1 \\ \text{und} \quad \tilde{g} \circ x = g \circ x &= y_k\end{aligned}$$

□

## 6.2. Doppelnebenklassen

Für weitere Eigenschaften der Transitivität benötigen wir den Begriff der Doppelnebenklasse.

**Definition 6.16.** Seien $H$ und $H'$ Untergruppen in $G$. Dann operiert $H' \times H$ auf $G$ durch

$$\begin{aligned}(H' \times H) \times G &\longrightarrow G \\ (h', h, g) &\longmapsto h'gh^{-1}\end{aligned}$$

Der Orbit eines Elementes $g \in G$ heisst Doppelnebenklasse und wird mit $H'gH$ bezeichnet.

Der Orbitraum wird mit $H' \backslash G / H$ bezeichnet.

**Proposition 6.17.** *Die Permutationsdarstellung $\rho : G \curvearrowright X$ sei 2-transitiv und $x \in X$ sowie $g \notin G_x$. Dann hat $\rho$ den Rang $rk(\rho) = 2$ und die Gruppe $G$ ist die disjunkte Vereinigung des Stabilisators $G_x$ mit der Doppelnebenklasse $G_x g G_x$.*

$$G = G_x \sqcup G_x g G_x$$

*Beweis.* Aus dem Reduktionslemma 6.15 folgt, dass $G_x$ auf $X \setminus \{ x \}$ transitiv operiert. Also hat $G_x$ zwei Orbits in $X$. Diese sind

$$\{ x \}$$
$$X \setminus \{ x \}$$

Somit ist der Rang $rk(\rho) = 2$.

Sei nun $h \notin G_x$. Dann sind

$$(hx, x) \in X^{[2]}$$
$$(gx, x) \in X^{[2]}$$

zwei disjunkte Paare in $X$. Da $\rho$ 2-transitiv ist, gibt es ein $k \in G$ mit

$$\begin{aligned} gx &= khx \\ x &= kx \end{aligned}$$

Somit ist $k \in G_x$ und es gilt:

$$\begin{aligned} & gkx = khx \\ \Rightarrow \quad & k^{-1}gkx = hx \\ \Rightarrow \quad & h \in G_x g G_x \end{aligned}$$

Daraus folgt:

$$G = G_x \sqcup G_x g G_x$$

□

**Lemma 6.18.** *Sei $\rho : G \curvearrowright X$ eine transitive Permutationsdarstellung und $x \in X$. Dann ist der Rang gleich der Anzahl der Doppelnebenklassen.*

$$rk(\rho) = |\, G_x g G_x \,|$$

*Beweis.* Sei $x \in X$ und $G_x$ der Stabilisator von $x$. Nach Definition 5.1 ist der Rang einer transitiven Permutationsdarstellung gleich der Anzahl der $G_x$ Orbits in $X$. Nun betrachten wir die Abbildung

$$\begin{aligned} \{\, G_x y \subseteq X \text{ Bahn } \} &\longrightarrow G_x \backslash G / G_x \\ G_x y &\longmapsto G_x g G_x \quad \text{wobei } y = gx \end{aligned}$$

aus dem Orbitraum von $G_x$ in die Doppelnebenklassen. Da $\rho$ transitiv ist, existiert zu jedem $y \in X$ ein $g \in G$ mit $y = gx$. Die Abbildung ist wohldefiniert. Denn für einen anderen Representanten $y'$ der Bahn $G_x y$ gilt:

$$\begin{aligned} & & G_x y' &= G_x y \\ \Rightarrow & & y' &= \bar{g} y \quad \text{mit } \bar{g} \in G_x \\ & \text{und} & y' &= g' x \quad \text{mit } g' \in G \\ \Rightarrow & & y' &= g' g^{-1} y \\ \Rightarrow & & \bar{g} &= g' g^{-1} \\ & & g' &= \bar{g} g \\ \Rightarrow & & G_x g' G_x &= G_x g G_x \end{aligned}$$

Die Abbildung ist surjektiv. Denn für jede Doppelnebenklasse $G_x g G_x$ existiert ein Orbit $G_x y$ mit $y = gx$.

Die Abbildung ist auch injektiv. Denn sei $G_x g G_x = G_x g' G_x$. Dann gibt es $h, h' \in G_x$ mit $g' = hgh'$ und aus $y = gx$ und $y' = g'x$ folgt $y' = hgh'x = hgx$. Somit stimmen die Bahnen $G_x y$ und $G_x y'$ überein. Aus der Bijektivität folgt nun die Behauptung. □

# 7. Projektive, lineare Gruppen

**Definition 7.1.** Sei $\mathbb{F}$ ein Körper und $n \in \mathbb{N}$ eine natürliche Zahl. Dann heisst die Menge aller Geraden in $\mathbb{F}^{n+1}$

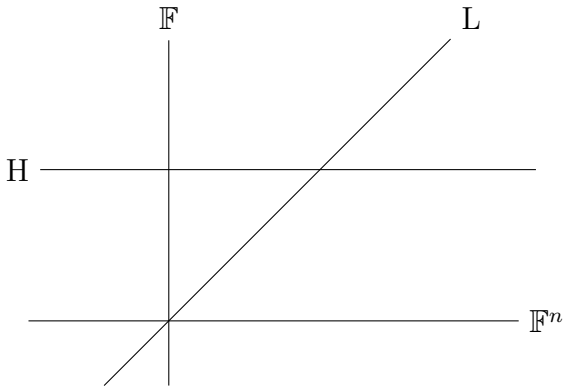
$$\mathbb{F}P^n = \{\, L \subseteq \mathbb{F}^{n+1} \mid \dim_{\mathbb{F}} L = 1 \,\}$$

projektiver Raum über $\mathbb{F}$ der Dimension $n$.

**Bemerkung 7.2.** Da Geraden im $(n+1)$-dimensionalen Vektorraum über dem Körper $\mathbb{F}$ von einem Vektor $\mathfrak{v}$ und seinen Vielfachen $\lambda\mathfrak{v}$ mit $0 \neq \lambda \in \mathbb{F}$ erzeugt werden, bildet jede Gerade eine Äquivalenzklasse folgender Äquivalenzrelation:

$$\mathfrak{v} \sim \mathfrak{w} \quad \Leftrightarrow \quad \text{es gibt ein } 0 \neq \lambda \in \mathbb{F} \quad \text{mit } \mathfrak{w} = \lambda\mathfrak{v}$$

**Bemerkung 7.3.** Zur Veranschaulichung wählen wir eine Basis $(\mathfrak{e}_1, \cdots, \mathfrak{e}_n, \mathfrak{e}_{n+1})$ in $\mathbb{F}^{n+1}$ und definieren eine Hyperebene $H = \mathbb{F}^n \times \mathfrak{o} + \mathfrak{e}_{n+1}$. Eine beliebige Gerade $L$ liegt entweder komplett in $\mathbb{F}^n$ oder sie schneidet die Hyperebene $H$ in einem Punkt.




Somit ist ein $n$-dimensionaler projektiver Raum die disjunkte Vereinigung von $\mathbb{F}^n$ mit einem $n-1$-dimensionalen projektiven Raum $\mathbb{F}P^{n-1}$:

$$\mathbb{F}P^n = \mathbb{F}^n \sqcup \mathbb{F}P^{n-1}$$

Durch weitere Aufspaltungen erhält man schliesslich:

$$\mathbb{F}P^n = \mathbb{F}^n \sqcup \mathbb{F}^{n-1} \sqcup \cdots \sqcup \underbrace{\mathbb{F}^0}_{=\{\infty\}}$$

Die projektive Gerade ist ein eindimensionaler projektiver Raum. Dieser ergibt sich aus dem lineare Vektorraum $\mathbb{F}^1$ durch die projektive Erweiterung mit dem unendlich fernen Punkt.

$$\begin{aligned} \mathbb{F}P^1 &= \mathbb{F} \sqcup \{\infty\} \\ &= \hat{\mathbb{F}} \end{aligned}$$

Eine projektive Ebene als zweidimensionaler projektiver Raum ergibt sich aus einem zweidimensionalen Vektorraum $\mathbb{F}^2$ durch Hinzunahme einer unendlich fernen, projektiven Geraden.

$$\begin{aligned} \mathbb{F}P^2 &= \mathbb{F}^2 \sqcup \mathbb{F} \sqcup \{\infty\} \\ &= \mathbb{F}^2 \sqcup \mathbb{F}P^1 \end{aligned}$$

Die Definition von projektiven Räumen und die oben genannten Eigenschaften sind

unabhängig von der Größe des Körpers. Im folgenden betrachten wir endliche projektive Räume über endlichen Körpern. Die grundlegenden Eigenschaften endlicher Körper wurden in Abschnitt 3.6 zusammengestellt.

**Proposition 7.4.** *Die Anzahl der Elemente in einem n-dimensionalen projektiven Raum über einem endlichen Körper $\mathbb{F}_q$ mit $q = p^r$ Elementen ist*

$$|\,\mathbb{F}_q P^n\,| = \frac{q^{n+1}-1}{q-1} = 1 + q + \cdots + q^n$$

*Beweis.* Mit der multiplikativen Gruppe $\mathbb{F}^* \subset \mathbb{F}$ läßt sich die Menge der Geraden in $\mathbb{F}^{n+1}$ schreiben als

$$\{\, L \subseteq \mathbb{F}^{n+1} \mid \dim_{\mathbb{F}} L = 1 \,\} = \mathbb{F}^{n+1} \setminus \{\, 0 \,\}/\mathbb{F}^*$$

□

## 7.1. Lineare Gruppen

**Definition 7.5.** Die allgemeine lineare Gruppe vom Grad $n$ über einem Körper $\mathbb{F}$ ist gegeben durch alle regulären $n \times n$ Matrizen mit Einträgen aus $\mathbb{F}$.

$$Gl_n(\mathbb{F}) = \{\, A \in \mathbb{F}^{n\times n} \mid \det A \in \mathbb{F}^* \,\}$$

Die spezielle lineare Gruppe vom Grad $n$ über einem Körper $\mathbb{F}$ ist gegeben durch alle $n \times n$ Matrizen mit Einträgen aus $\mathbb{F}$ und Determinante 1.

$$Sl_n(\mathbb{F}) = \{\, A \in \mathbb{F}^{n\times n} \mid \det A = 1 \,\}$$

**Proposition 7.6.** *Die allgemeine lineare Gruppe operiert effektiv oder treu auf $\mathbb{F}^n$.*

$$\rho : Gl_n(\mathbb{F}) \curvearrowright \mathbb{F}^n \quad \textit{ist treu}$$

*Beweis.* Nach Lemma 1.42 und Definition 1.43 müssen wir zeigen, dass der Kern von $\rho : Gl_n(\mathbb{F}) \to Sym(\mathbb{F}^n)$ trivial ist. Dies ist gleichbedeutend damit, dass das Urbild der Identität in $Sym(\mathbb{F}^n)$ die Einheitsmatrix in $Gl_n(\mathbb{F})$ ist. Das heisst insbesondere für Basisvektoren $\mathfrak{e}_i \in \mathbb{F}^n$:

$$\begin{aligned} A \in Ker(\rho) &\Leftrightarrow A \cdot \mathfrak{e}_i = \mathfrak{e}_i \quad \text{für alle } 1 \le i \le n \\ &\Leftrightarrow A \cdot \mathbb{1} = \mathbb{1} \\ &\Leftrightarrow A = \mathbb{1} \end{aligned}$$

□

Die allgemeine lineare Gruppe $Gl_n(\mathbb{F})$ operiert auch auf dem projektiven Raum $\mathbb{F}P^{n-1}$, allerdings ist diese Operation nicht mehr effektiv oder treu.

**Proposition 7.7.** *Die Operation der allgemeinen linearen Gruppe $Gl_n(\mathbb{F})$ auf dem projektiven Raum $\mathbb{F}P^{n-1}$ hat das Zentrum der allgemeinen linearen Gruppe $Gl_n(\mathbb{F})$ als Kern.*

$$\begin{aligned} \rho : Gl_n(\mathbb{F}) &\curvearrowright \mathbb{F}P^{n-1} \\ \Rightarrow \quad Ker(\rho) &= Z(Gl_n(\mathbb{F})) = \{ \lambda \cdot \mathbb{1} \mid \lambda \in \mathbb{F}^* \} \end{aligned}$$

*Beweis.* Ein Element im projektiven Raum $\mathbb{F}P^{n-1}$ ist eine Gerade $L \in \mathbb{F}^n$ repräsentiert durch einen Vektor $\mathfrak{o} \neq \mathfrak{v}$ und seinen Vielfachen $\lambda \cdot \mathfrak{v}$ mit $\lambda \in \mathbb{F}^*$. Somit liegen alle Diagonalmatrizen $\lambda \cdot \mathbb{1} \in Ker(\rho)$ im Kern von $\rho$. Da alle Diagonalmatrizen mit allen anderen Matrizen kommutieren, liegen diese auch im Zentrum. Das Zentrum enthält aber auch keine anderen Matrizen. Denn sei $A \neq \lambda \cdot \mathbb{1}$. Dann gibt es einen Vektor $\mathfrak{v}$, für den $\mathfrak{v}$ und $A \cdot \mathfrak{v}$ linear unabhängig sind. Daraus folgt, dass $A$ nicht im Kern von $\rho$ liegt. Nun ergänzen wir $\mathfrak{v}$ und $A \cdot \mathfrak{v}$ zu einer Basis

$$(\mathfrak{v}, \mathfrak{v} + A \cdot \mathfrak{v}, \mathfrak{v}_3, \cdots \mathfrak{v}_n)$$

Wir konstruieren eine lineare Abbildung $B$ durch

$$\begin{aligned} B \cdot \mathfrak{v} &= \mathfrak{v} \\ B \cdot (A \cdot \mathfrak{v}) &= \mathfrak{v} + A \cdot \mathfrak{v} \\ B \cdot \mathfrak{v}_i &= \mathfrak{v}_i \quad \text{für } 3 \leq i \leq n \end{aligned}$$

Dann gilt

$$\begin{aligned} B \cdot (A \cdot \mathfrak{v}) &= \mathfrak{v} + A \cdot \mathfrak{v} \\ A \cdot (B \cdot \mathfrak{v}) &= A \cdot \mathfrak{v} \\ &\neq B \cdot (A \cdot \mathfrak{v}) \end{aligned}$$

Somit liegt $A$ nicht im Zentrum. □

**Proposition 7.8.** *Das Zentrum der speziellen, linearen Gruppe $Sl_n(\mathbb{F})$ ist gegeben durch*

$$SZ_n = Sl_n(\mathbb{F}) \cap Z(Gl_n(\mathbb{F}))$$

**Definition 7.9.** Die projektive, lineare Gruppe ist definiert durch

$$PGl_n(\mathbb{F}) \coloneqq Gl_n(\mathbb{F})/Z(Gl_n(\mathbb{F}))$$

Die projektive, spezielle, lineare Gruppe ist definiert durch

$$PSl_n(\mathbb{F}) \coloneqq Sl_n(\mathbb{F})/SZ_n$$

**Bemerkung 7.10.** Lineare Gruppen über endlichen Körpern $\mathbb{F}_q$ werden häufig auch in der folgenden, abgekürzten Schreibweise bezeichnet.

$$\begin{aligned} Gl_n(\mathbb{F}_q) &= Gl_n(q) \\ Sl_n(\mathbb{F}_q) &= Sl_n(q) \\ PGl_n(\mathbb{F}_q) &= PGl_n(q) \\ PSl_n(\mathbb{F}_q) &= PSl_n(q) \end{aligned}$$

**Bemerkung 7.11.** Das folgende, kommutative Diagramm veranschaulicht den Zusammenhang der genannten linearen Gruppen.

$$\begin{array}{ccccc} SZ_n & \longrightarrow & Z(Gl_n(\mathbb{F})) & \xrightarrow{(\cdot)^n} & (\mathbb{F}^*)^n \\ \downarrow & & \downarrow & & \downarrow \\ Sl_n(\mathbb{F}) & \longrightarrow & Gl_n(\mathbb{F}) & \xrightarrow{det} & \mathbb{F}^* \\ \downarrow & & \downarrow & & \downarrow \\ PSl_n(\mathbb{F}) & \longrightarrow & PGl_n(\mathbb{F}) & \longrightarrow & (\mathbb{F}^*)^n/\mathbb{F}^* \end{array}$$

## 7.2. Wirkung der projektiven, speziellen, linearen Gruppe auf projektive Räume

**Theorem 7.12.** *Die projektiven, speziellen, linearen Gruppen $PSl_n(\mathbb{F})$ wirken effektiv (treu) und für $n \geq 2$ 2-transitiv auf die projektiven Räume $\mathbb{F}P^{n-1}$.*

*Beweis.* Wir müssen zeigen, dass der Homomorphismus

$$\rho : PSl_n(\mathbb{F}) \longrightarrow Sym(\mathbb{F}P^{n-1})$$

injektiv ist, das heisst, der Kern $Ker(\rho)$ trivial ist. Wir betrachten also die identische Abbildung, die alle eindimensionalen Unteräume von $\mathbb{F}^n$ in sich selbst abbildet. Diese

wird bezüglich einer Basis $(\mathfrak{e}_1, \cdots, \mathfrak{e}_n)$ vermittelt durch eine Matrix $A \in Gl_n(\mathbb{F})$ mit der Eigenschaft

$$\begin{aligned} A(\mathbb{F} \cdot \mathfrak{e}_i) &= \mathbb{F} \cdot \mathfrak{e}_i \\ \Rightarrow \quad A(\mathfrak{e}_i) &= \lambda_i \cdot \mathfrak{e}_i \end{aligned}$$

Für den eindimensionalen Unterraum $\mathbb{F} \cdot (\mathfrak{e}_1 + \mathfrak{e}_i)$ erhalten wir

$$\begin{aligned} A(\mathbb{F} \cdot (\mathfrak{e}_1 + \mathfrak{e}_i)) &= \mathbb{F} \cdot (\mathfrak{e}_1 + \mathfrak{e}_i) \\ \Rightarrow \quad A(\mathfrak{e}_1 + \mathfrak{e}_i) &= \lambda \cdot (\mathfrak{e}_1 + \mathfrak{e}_i) \\ \Leftrightarrow \quad A(\mathfrak{e}_1) + A(\mathfrak{e}_i) &= \lambda_1 \cdot \mathfrak{e}_1 + \lambda_i \cdot \mathfrak{e}_i \\ \Leftrightarrow \quad \lambda &= \lambda_1 = \lambda_i \end{aligned}$$

Da dies für alle $i = 2, \cdots, n$ gilt, ist $A$ eine Diagonalmatrix $\lambda \cdot \mathbb{1}$ und somit das neutrale Element in $PSl_n(\mathbb{F})$.

Zum Nachweis der 2-Transitivität betrachten wir zwei Geradenpaare durch den Ursprung in $\mathbb{F}^n$. Diese seien durch die Vektoren $\mathfrak{v}_i$ und $\mathfrak{w}_i$ für $i = 1, 2$ gegeben. Die Vektoren $\mathfrak{v}_i$ und $\mathfrak{w}_i$ können jeweils zu einer Basis $(\mathfrak{v}_1, \mathfrak{v}_2, \cdots, \mathfrak{v}_n)$ und $(\mathfrak{w}_1, \mathfrak{w}_2, \cdots, \mathfrak{w}_n)$ in $\mathbb{F}^n$ ergänzt werden. Damit ist eine lineare Abbildung

$$\begin{aligned} A : \mathbb{F}^n &\longrightarrow \mathbb{F}^n \\ \mathfrak{v}_j &\longmapsto \mathfrak{w}_j \end{aligned}$$

definiert, für die nach Skalierung $det(A) = 1$ gilt. Somit vermittelt $A \in PSl_n(\mathbb{F})$ die gesuchte 2-transitive Wirkung auf $X$. □

## 7.3. Ordnungen der linearen Gruppen

**Proposition 7.13.** *Sei $\mathbb{F}_q$ ein Körper mit $q$ Elementen und $n \in \mathbb{N}$. Dann gelten für die Ordnungen der linearen Gruppen folgende Formeln:*

*(i)* *Ordnung der allgemeinen linearen Gruppe*

$$|\, Gl_n(\mathbb{F}_q)\,| = q^{\binom{n}{2}} \cdot \prod_{k=1}^{n} (q^k - 1)$$

*Dies ist gleichzeitig die Anzahl der Basen in $\mathbb{F}_q^n$.*

*(ii)* *Ordnung des Zentrums der allgemeinen linearen Gruppe*

$$|\,Z(Gl_n(\mathbb{F}_q))\,| = q-1$$

*(iii)* *Ordnung der projektiven linearen und speziellen linearen Gruppe*

$$|\,PGl_n(\mathbb{F}_q)\,| = |\,Sl_n(\mathbb{F}_q)\,| = q^{\binom{n}{2}} \cdot \prod_{k=2}^{n} (q^k - 1)$$

*(iv)* *Ordnung des Zentrums der speziellen linearen Gruppe*

$$|\,SZ_n(\mathbb{F}_q)\,| = \mathrm{ggT}(n, q-1)$$

*(v)* *Ordnung der projektiven speziellen linearen Gruppe*

$$|\,PSl_n(\mathbb{F}_q)\,| = \frac{1}{\mathrm{ggT}(n,q-1)} \cdot q^{\binom{n}{2}} \cdot \prod_{k=2}^{n} (q^k - 1)$$

*Beweis.* (i) Die Ordnung der allgemeinen linearen Gruppe $Gl_n(\mathbb{F}_q)$ kann durch folgende Überlegungen leicht bestimmt werden. Eine beliebige Matrix $A \in Gl_n(\mathbb{F}_q)$ wird durch Spaltenvektoren dargestellt.

$$A = \begin{pmatrix} | & | & \cdots & | \\ b_1 & b_2 & \cdots & b_n \\ | & | & \cdots & | \end{pmatrix}$$

Für den Vektor $b_1 \neq 0$ gibt es $q^n - 1$ Möglichkeiten in $\mathbb{F}_q^n$.
Für den Vektor $b_2 \in \mathbb{F}_q^n \setminus \mathbb{F}_q \cdot b_1$ gibt es $q^n - q$ Möglichkeiten.
Für den Vektor $b_n \in \mathbb{F}_q^n \setminus (\mathbb{F}_q \cdot b_1 + \cdots + \mathbb{F}_q \cdot b_{n-1})$ erhält man schliesslich $q^n - q^{n-1}$ Möglichkeiten. Daraus folgt

$$\begin{aligned} |\,Gl_n(\mathbb{F}_q)\,| &= (q^n-1)\cdot(q^n-q)\cdots(q^n-q^{n-1}) \\ &= q^{\binom{n}{2}} \cdot \prod_{k=1}^{n} (q^k - 1) \end{aligned}$$

Die Spaltenvektoren $b_i$ bilden auch eine Basis in $\mathbb{F}_q^n$.

(ii) Nach Proposition 7.7 besteht das Zentrum der allgemeinen, linearen Gruppe $Gl_n(\mathbb{F}_q)$

aus allen Vielfachen ungleich Null der Einheitsmatrix. Somit ist

$$\begin{aligned} |\,Z(Gl_n(\mathbb{F}_q))\,| &= |\,\mathbb{F}_q^*\,| \\ &= q-1 \end{aligned}$$

(iii) Als Kern der Determinantenabbildung

$$\det : Gl_n(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^*$$

hat die spezielle, lineare Gruppe $Sl_n(\mathbb{F}_q)$ die Ordnung

$$\begin{aligned} |\,Sl_n(\mathbb{F}_q)\,| &= \frac{|\,Gl_n(\mathbb{F}_q)\,|}{|\,\mathbb{F}_q^*\,|} \\ &= \frac{q^{\binom{n}{2}} \cdot \prod_{k=1}^{n}(q^k-1)}{q-1} \\ &= q^{\binom{n}{2}} \cdot \prod_{k=2}^{n}(q^k-1) \end{aligned}$$

Da $Z(Gl_n(\mathbb{F}_q))$ isomorph zu $\mathbb{F}_q^*$ ist, gilt dieselbe Überlegung auch für die projektive, lineare Gruppe $PGl_n(\mathbb{F}_q)$.

(iv) Die Gruppe $SZ_n$ ist der Kern der Abbildung

$$\begin{aligned} (\cdot)^n : \mathbb{F}_q^* &\longrightarrow \mathbb{F}_q^* \\ b &\longmapsto b^n \end{aligned}$$

Sei nun $d = \mathrm{ggT}(n, q-1)$ und $x = \frac{q-1}{d}$. Dann ist der Kern gegeben durch

$$SZ_n = \{\, b^{i\cdot x} \,|\, 1 \le i \le d \,\}$$

Denn alle diese Elemente werden auf 1 abgebildet.

$$b^{i\cdot x\cdot n} = b^{i\cdot\frac{q-1}{d}\cdot n} = b^{(q-1)\cdot i\cdot\frac{n}{d}} \quad \text{da } \frac{n}{d} \in \mathbb{N}$$

(v) Die Ordnung der projektiven, speziellen, linearen Gruppe $PSl_n(\mathbb{F}_q)$ ergibt sich nun durch Quotientenbildung aus $Sl_n(\mathbb{F}_q)$ und $SZ_n$.

□

**Beispiel 7.14.** Für $n = 2$ und $\mathbb{F}_2$ erhalten wir

$$PSl_2(\mathbb{F}_2) = Sl_2(\mathbb{F}_2)/D = Sl_2(\mathbb{F}_2) = Gl_2(\mathbb{F}_2) \simeq S_3$$

Denn die Diagonalmatrizen $D = \{Id\}$ bestehen nur aus der Einheitsmatrix. Und $Gl_2(\mathbb{F}_2)$ hat die Ordnung 6 und ist nicht abelsch.
$PSl_2(\mathbb{F}_2)$ ist also nicht einfach.

**Beispiel 7.15.** Für $n = 2$ und $\mathbb{F}_3$ gilt

$$D = \left\{ Id \, , \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

Die allgemeine, lineare Gruppe $Gl_2(\mathbb{F}_3)$ hat die Ordnung $(3^2 - 1) \cdot (3^2 - 3) = 48$. Da die Determinante einer Matrix in $\mathbb{F}_3$ nur die Werte +1 oder −1 annehmen kann, hat $Sl_2(\mathbb{F}_3)$ die Ordnung 24 und $PSl_2(\mathbb{F}_3)$ die Ordnung 12.
$PSl_2(\mathbb{F}_3)$ ist isomorph zur alternierenden Gruppe $A_4$ und damit nicht einfach.

**Beispiel 7.16.** Für $n = 2$ und $\mathbb{F}_4$ gilt

$$|\, Gl_2(\mathbb{F}_4) \,| = (4^2 - 1) \cdot (4^2 - 4) = 180$$

Daraus ergibt sich

$$|\, Sl_2(\mathbb{F}_4) \,| = |\, Ker(\det) \,| = \frac{180}{3} = 60$$

Für die Diagonalmatrizen darin ergibt sich

$$D = \{ \; Id \; \}$$

da $\mathbb{F}_4$ die Charakteristik 2 hat. Somit hat $PSl_2(\mathbb{F}_4)$ die Ordnung 60. Da $PSl_2(\mathbb{F}_4)$ einfach ist, wie wir später zeigen werden, und es nach Theorem 9.3 nur eine einfache Gruppe der Ordnung 60 gibt, ist $PSl_2(\mathbb{F}_4)$ isomorph zur alternierenden Gruppe $A_5$.

**Beispiel 7.17.** Für $n = 2$ und $\mathbb{F}_5$ gilt

$$|\, Gl_2(\mathbb{F}_5) \,| = (5^2 - 1) \cdot (5^2 - 5) = 480$$

Daraus ergibt sich

$$|\, Sl_2(\mathbb{F}_5) \,| = |\, Ker(\det) \,| = \frac{480}{4} = 120$$

Für die Diagonalmatrizen darin ergibt sich

$$D = \left\{ Id\ ,\ \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} \right\}$$

Somit hat $PSl_2(\mathbb{F}_5)$ die Ordnung 60. Da $PSl_2(\mathbb{F}_5)$ einfach ist, wie wir später zeigen werden, und es nach Theorem 9.3 nur eine einfache Gruppe der Ordnung 60 gibt, ist $PSl_2(\mathbb{F}_5)$ isomorph zur alternierenden Gruppe $A_5$.

**Beispiel 7.18.** Für $n = 2$ und $\mathbb{F}_7$ gilt

$$|\,Gl_2(\mathbb{F}_7)\,| = (7^2 - 1) \cdot (7^2 - 7) = 2016$$

Daraus ergibt sich

$$|\,Sl_2(\mathbb{F}_7)\,| = |\,Ker(\det)\,| = \frac{2016}{6} = 336$$

Für die Diagonalmatrizen darin ergibt sich

$$D = \left\{ Id\ ,\ \begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix} \right\}$$

Somit hat $PSl_2(\mathbb{F}_7)$ die Ordnung 168. Da $PSl_2(\mathbb{F}_7)$ einfach ist, wie wir später zeigen werden, und es nur eine einfache Gruppe mit der Ordnung 168 gibt, ist $PSl_2(\mathbb{F}_7)$ isomorph zur allgemeinen, linearen Gruppe $Gl_3(\mathbb{F}_2)$. Die Eindeutigkeit der einfachen Gruppe der Ordnung 168 ist allerdings nicht einfach zu beweisen.

**Beispiel 7.19.** Für $n = 2$ und $\mathbb{F}_9$ ergibt sich die Ordnung der projektiven, speziellen, linearen Gruppe $PSl_2(\mathbb{F}_9)$ nach Proposition 7.13 zu

$$\begin{aligned} |\,PSl_2(\mathbb{F}_9)\,| &= \frac{1}{2} \cdot 9 \cdot (9^2 - 1) \\ &= 3 \cdot \underbrace{3 \cdot 2}_{=6} \cdot 4 \cdot 5 \\ &= 3 \cdot 4 \cdot 5 \cdot 6 \\ &= \frac{1}{2} \cdot 6! \\ &= 360 \end{aligned}$$

Sie hat also dieselbe Ordnung wie die alternierende Gruppe $A_6$. Da $PSl_2(\mathbb{F}_9)$ einfach ist, wie wir später zeigen werden, und es nur eine einfache Gruppe mit der Ordnung 360 gibt, ist $PSl_2(\mathbb{F}_9)$ isomorph zur alternierenden Gruppe $A_6$.

Es könnte nun der Eindruck entstehen, dass es zu einer gegebenen Gruppenordnung nur eine einfache Gruppe geben kann. Dass dem nicht so ist, zeigt folgendes Beispiel. Zu der Gruppenordnung 20 160 gibt es zwei nicht-isomorphe, einfache Gruppen.

**Beispiel 7.20.** Für $n = 3$ und $q = 4$ ist

$$\mathrm{ggT}(n, q-1) = \mathrm{ggT}(3,3) = 3$$

Damit ergibt sich die Ordnung der projektiven, speziellen, linearen Gruppe $PSl_3(\mathbb{F}_4)$ zu

$$\begin{aligned} |\,PSl_3(\mathbb{F}_4)\,| &= \frac{1}{3}\cdot 4^3\cdot(4^2-1)\cdot(4^3-1) \\ &= 4\cdot 4\cdot 4\cdot 5\cdot 3\cdot 3\cdot 7 \\ &= 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8 \\ &= \frac{1}{2}\cdot 8! \\ &= 20\,160 \end{aligned}$$

Sie hat also dieselbe Ordnung wie die alternierende Gruppe $A_8$. Obwohl beide Gruppen die gleiche Ordnung haben, sind sie nicht isomorph.

Denn in $A_8$ haben die Elemente

$$\begin{aligned} \sigma_1 &= (1\ 2)\,(3\ 4) \\ \sigma_2 &= (1\ 2)\,(3\ 4)\,(5\ 6)\,(7\ 8) \end{aligned}$$

die Ordnung 2 und sind nicht konjugiert.

In $PSl_3(\mathbb{F}_4)$ hingegen sind alle Elemente $A$ der Ordnung 2 konjugiert. Da für die Charakteristik $\chi(\mathbb{F}_4) = 2$ gilt, ist das Minimalpolynom von $A$

$$x^2 - 1 = (x-1)^2$$

Die Jordansche Normalform von $A$ ist

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Das heisst, für jede Matrix $A$ mit $A^2 = \mathbb{1}$ existiert eine Matrix $B \in PSl_3(\mathbb{F}_4)$ mit

$$B \cdot A \cdot B^{-1} = J$$

Also sind alle Elemente $A$ der Ordnung 2 in $PSl_3(\mathbb{F}_4)$ konjugiert.

Die projektive, spezielle, lineare Gruppe $PSl_4(\mathbb{F}_2)$ hat ebenfalls 20 160 Elemente. Diese ist isomorph zur alternierenden Gruppe $A_8$.

Außer den genannten Beispielen gibt es keine weiteren Isomorphien zwischen projektiven, speziellen, linearen Gruppen und alternierenden Gruppen.

## 7.4. Projektive Geraden und gebrochen lineare Transformationen

Die projektiven, linearen Gruppen operieren nach Theorem 7.12 effektiv und 2-transitiv auf projektiven Räumen. In projektiven Geraden (eindimensionalen, projektiven Räumen) kann die Operation als gebrochen lineare Transformation aufgefaßt werden.

$$\begin{array}{rcl} \hat{\mathbb{F}} & \longrightarrow & \hat{\mathbb{F}} \\ x & \longmapsto & f(x) = \dfrac{ax+b}{cx+d} \quad \text{mit } ad-bc \neq 0 \\ x & \longmapsto & f(x) = \infty \quad \text{falls } cx+d = 0 \\ \infty & \longmapsto & \begin{cases} \frac{a}{c} & \text{für } c \neq 0 \\ \infty & \text{für } c = 0 \end{cases} \end{array}$$

Alle gebrochen linearen Transformationen bilden eine Gruppe. Diese wird mit

$$LF(\mathbb{F})$$

bezeichnet. Sie wirkt auf die projektive Gerade.

$$LF(\mathbb{F}) \curvearrowright \mathbb{F}P^1 = \mathbb{F} \cup \{ \infty \} = \hat{\mathbb{F}}$$

**Lemma 7.21.** *Die gebrochen linearen Transformationen $LF(\mathbb{F})$ sind isomorph zur projektiven, linearen Gruppe $PGl_2(\mathbb{F})$.*

*Beweis.* Wir betrachten die Abbildung

$$\begin{array}{rcl} \varphi : Gl_2(\mathbb{F}) & \longrightarrow & LF(\mathbb{F}) \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & f(x) = \dfrac{ax+b}{cx+d} \end{array}$$

Dies ist ein Gruppenhomomorphismus. Denn

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}$$

$$\begin{aligned} x &\longmapsto \frac{a_1\frac{a_2x+b_2}{c_2x+d_2} + b_1}{c_1\frac{a_2x+b_2}{c_2x+d_2} + d_2} \\ &= \frac{a_1 \cdot (a_2x + b_2) + b_1 \cdot (c_2x + d_2)}{c_1 \cdot (a_2x + b_2) + d_2 \cdot (c_2x + d_2)} \\ &= \frac{(a_1a_2 + b_1c_2) \cdot x + (a_1b_2 + b_1d_2)}{(c_1a_2 + d_1c_2) \cdot x + (c_1d_2 + d_1d_2)} \end{aligned}$$

Der Kern dieser Abbildung ist genau das Zentrum von $Gl_2(\mathbb{F})$. Denn

$$\begin{aligned} f = Id &\Leftrightarrow x = \frac{ax+b}{cx+d} \quad \text{für alle } x \in \hat{\mathbb{F}} \\ &\Leftrightarrow c \cdot x^2 + (d-a) \cdot x - b = 0 \\ &\Leftrightarrow \begin{cases} c = 0 \\ a = d \\ b = 0 \end{cases} \\ &\Leftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in Z(Gl_2(\mathbb{F})) \end{aligned}$$

Somit ist die Abbildung

$$\varphi : PGl_2(\mathbb{F}) = Gl_2(\mathbb{F})/Z(Gl_2(\mathbb{F})) \longrightarrow LF(\mathbb{F})$$

ein injektiver Homomorphismus. Zum Nachweis der Surjektivität zählen wir die Elemente in $LF(\mathbb{F})$. Für $a = 0$ kann $d$ alle $q$ Elemente annehmen. Aus der Bedingung $ad - bc \neq 0$ folgt $c \neq 0$. Durch geeignete Erweiterung des Bruches kann also $c = 1$ erreicht werden, so dass $b$ alle $q-1$ Elemente ungleich Null sein kann.
Für $a \neq 0$ kann durch geeignete Erweiterung des Bruches $a = 1$ erreicht werden. Für $b$ und $c$ können alle $q$ Elemente gewählt werden. Da $d \neq bc$ gelten muss, können dafür $q-1$ Elemente gewählt werden. Somit erhalten wir

$$|LF(\mathbb{F})| = (q-1) \cdot (q+q^2) = (q-1) \cdot q \cdot (q+1) = q \cdot (q^2-1)$$

Dies ist dieselbe Mächtigkeit, die wir in Proposition 7.13 für $PGl_2(\mathbb{F})$ ermittelt haben. Daher ist die Abbildung $\varphi$ auch surjektiv und die Gruppen $PGl_2(\mathbb{F})$ und $LF(\mathbb{F})$ sind

isomorph. □

**Bemerkung 7.22.** Die Untergruppe $PLF(\mathbb{F}_q)$ der gebrochen linearen Transformationen mit Determinante 1

$$f(\xi) = \frac{a\xi + b}{c\xi + d} \quad \text{mit } ad - bc = 1$$

sind isomorph zur projektiven speziellen linearen Gruppe $PSl_2(\mathbb{F}_q)$. Denn der Quotient kann mit dem Kehrwert der Wurzel der Determinante $ad - bc$ erweitert werden, falls diese existiert, um für die Determinante den Wert 1 zu erreichen. Wie im Beweis zu Proposition 7.13 gezeigt, bilden die Einheitswurzeln genau das Zentrum $Sl_2(\mathbb{F}_q)$ von $PGl_2(\mathbb{F}_q)$ und es gilt $|Sl_2(\mathbb{F}_q)| = \text{ggT}(2, q-1)$. Das heisst, dass für gerade $q = 2^r$ das Zentrum $Sl_2(\mathbb{F}_{2^r})$ trivial ist und die projektive spezielle lineare Gruppe isomorph ist zur projektiven linearen Gruppe: $PSl_2(\mathbb{F}_{2^r}) \simeq PGl_2(\mathbb{F}_{2^r})$.

**Theorem 7.23.** *Die Gruppe der gebrochen linearen Transformationen $LF(\mathbb{F}_q)$ operiert scharf-3-transitiv auf der projektiven Geraden.*

*Beweis.* Wir zeigen, dass es zu 3 paarweise verschiedenen Punkte $x, y, z \in \hat{\mathbb{F}}$ eine eindeutige gebrochen lineare Transformation

$$f(\xi) = \frac{a\xi + b}{c\xi + d} \quad \text{mit } ad - bc \neq 0$$

gibt, die $x, y, z$ in $0, 1, \infty \in \hat{\mathbb{F}}$ abbildet. Aus den Bedingungen folgt:

$$\begin{aligned}
f(x) = \frac{ax+b}{cx+d} &= 0 \\
f(y) = \frac{ay+b}{cy+d} &= 1 \\
f(z) = \frac{az+b}{cz+d} &= \infty \\
\Rightarrow \quad a &= -\frac{b}{x} \\
\text{und} \quad c &= -\frac{d}{z} \\
\text{und damit} \quad 1 &= \frac{-\frac{b}{x}y + b}{-\frac{d}{z}y + d} \\
&= \frac{b(x-y)z}{d(z-y)x} \\
\Rightarrow \quad \frac{b}{d} &= \frac{x(z-y)}{z(x-y)}
\end{aligned}$$

Da der Bruch durch einen beliebigen Faktor ungleich Null erweitert werden kann, können wir

$$\begin{aligned} b &= x(z-y) \\ d &= z(x-y) \end{aligned}$$

wählen. Damit ergibt sich

$$\begin{aligned} a &= y-z \\ c &= y-x \end{aligned}$$

Die Determinante

$$\delta = ad - bc = z(x-y)(y-z) - x(z-y)(y-x) = (x-y)(y-z)(z-x) \neq 0$$

ist ungleich Null, da die Punkte $x, y, z$ als paarweise verschieden vorausgesetzt wurden. □

**Bemerkung 7.24.** Wenn anstelle eines endlichen Körpers der Körper $\mathbb{C}$ der komplexen Zahlen zugrunde gelegt wird, dann entsprechen den gebrochen linearen Transformationen genau die Möbius Transformationen auf der Riemannschen Zahlenkugel.

## 7.5. Gebrochen semilineare Transformationen

Der Begriff der allgemeinen, linearen Abbildungen kann erweitert werden, indem zusätzlich ein Körperautomorphismus angewendet wird.

**Definition 7.25.** Sei $A \in Gl_n(\mathbb{F})$ eine lineare Abbildung und $\alpha \in Aut(\mathbb{F})$ ein Körperautomorphismus. Dann ist eine semilineare Abbildung gegeben durch

$$\begin{aligned} (A,\alpha) : \mathbb{F}^n &\longrightarrow \mathbb{F}^n \\ \mathfrak{v} &\longmapsto A \cdot \alpha(\mathfrak{v}) \end{aligned}$$

Dabei wird der Körperautomorphismus $\alpha$ auf jede Komponente des Vektors $\mathfrak{v}$ angewendet.
Alle semilinearen Abbildungen bilden die allgemeine, semilineare Gruppe

$$\Gamma L_n(\mathbb{F})$$

**Proposition 7.26.** *Die allgemeine, semilineare Gruppe ist das semidirekte Produkt der allgemeinen, linearen Gruppe mit der Automorphismengruppe des Körpers.*

$$\Gamma L_n(\mathbb{F}) = Gl_n(\mathbb{F}) \rtimes Aut(\mathbb{F})$$

**Bemerkung 7.27.** Körperautomorphismen sind Gruppenautomorphismen sowohl der additiven wie auch der multiplikativen Gruppe des Körpers. Es gibt daher Körper, die ausser der Identität keine weiteren Automorphismen zulassen. Dazu gehören Primkörper $\mathbb{F}_p$, die rationalen Zahlen $\mathbb{Q}$ und die reellen Zahlen $\mathbb{R}$. In diesen Körpern stimmen semilineare Abbildungen mit linearen Abbildungen überein. Beispiele für Körper mit nichttrivialen Automorphismen sind $\mathbb{F}_q$ mit $q = p^r, r > 1$, die Erweiterungen der rationalen Zahlen wie $\mathbb{Q}(\sqrt{2})$ und die komplexen Zahlen $\mathbb{C}$.

**Bemerkung 7.28.** Da Primkörper $\mathbb{F}_p$ nur die Identität als Automorphismus zulassen, ist die Automorphismengruppe eines endlichen Körpers $\mathbb{F}_q$ mit $q = p^r$ identisch mit der Galois-Gruppe der Erweiterung $\mathbb{F}_q$ über $\mathbb{F}_p$:

$$Aut(\mathbb{F}_q) = Gal(\mathbb{F}_q/\mathbb{F}_p) \cong C_r$$

**Bemerkung 7.29.** Analog ergibt sich die projektive, semilineare Gruppe als semidirektes Produkt der projektiven, linearen Gruppe mit der Automorphismengruppe des Körpers.

$$P\Gamma L_n(\mathbb{F}) = PGl_n(\mathbb{F}) \rtimes Aut(\mathbb{F})$$

**Bemerkung 7.30.** Im eindimensionalen Fall einer projektiven Geraden erhält man aus der Gruppe der gebrochen linearen Transformationen die Gruppe der gebrochen semilinearen Transformationen.

$$\begin{aligned} \Gamma F(\mathbb{F}) &= LF(\mathbb{F}) \rtimes Aut(\mathbb{F}) \\ &= \{\, f(x) = \frac{a\alpha(x) + b}{c\alpha(x) + d} \,|\, \alpha \in Aut(\mathbb{F}) \,\} \end{aligned}$$

## 7.6. Kollineationen und Hauptsatz der projektiven Geometrie

**Definition 7.31.** In einem projektiven Raum $\mathbb{F}P^n$ heissen projektive Unterräume der Dimension 1 Geraden.

Analytisch können Geraden durch die Linearkombination von zwei Punkten beschrieben werden.

$$g(Q, R) = \{\, \lambda Q + \mu R \,|\, \lambda, \mu \in \mathbb{F} \,\}$$

**Definition 7.32.** Eine bijektive Abbildung eines projektiven Raumes $\mathbb{F}P^n$ auf sich

$$\kappa : \mathbb{F}P^n \longrightarrow \mathbb{F}P^n$$

heisst Kollineation, wenn sie Geraden wieder in Geraden abbildet.
Die Menge aller Kollineationen bezeichnen wir mit

$$Coll(\mathbb{F}P^n)$$

**Bemerkung 7.33.** Kollineationen bilden auch projektive Unterräume der Dimension $1 < k < n$ in projektive Unterräume derselben Dimension ab. Denn alle Geraden werden per Definition in Geraden abgebildet. Wenn ein Punkt $Q$ nicht auf der Geraden $g$ liegt, dann bilden alle Geraden $h(Q, R)$ durch $Q$ und Punkten $R \in g$ auf der Geraden $g$ eine Ebene $\epsilon$. Jede Kollineation $\kappa$ bildet den Punkt $Q$ in einen Punkt $\kappa(Q) = Q' \notin \kappa(g)$ ab, der nicht auf der Bildgeraden von $\kappa(g) = g'$ liegt. Ebenso werden alle Geraden durch $Q'$ und die Bildpunkte $R' = \kappa(R) \in g'$ in Geraden $h'$ abgebildet, die wiederum eine Ebene durch $Q'$ und $g'$ bilden und damit die Bildebene $\kappa(\epsilon)$ aufspannen. Diese Argumentation gilt auch für höhere Dimensionen.

Kollineationen sind also natürliche Abbildungen eines projektiven Raumes in sich, die die projektive Struktur erhalten. Und die Kollineationen bilden eine Gruppe. Es ist klar, dass alle projektiven, semilinearen Abbildungen Kollineationen sind. Denn jede lineare Abbildung bildet Geraden wieder in Geraden ab und jeder Körperautomorphismus verschiebt nur die Punkte auf der Geraden. Umgekehrt gibt es aber auch keine weiteren Kollineationen. Dies ist die Aussage des Hauptsatzes der projektiven Geometrie.

**Theorem 7.34.** *Hauptsatz der projektiven Geometrie*
*Die Gruppe der Kollineationen $Coll(\mathbb{F}P^n)$ ist isomorph zur projektiven, semilinearen Gruppe $P\Gamma L_n(\mathbb{F})$.*

*Beweis.* Der Beweis erfolgt in Anlehnung an den Beweis im Buch "Lineare Algebra und analytische Geometrie" von Hermann Schaal [Sch80], das leider vergriffen ist.

Es muss nur noch gezeigt werden, dass eine Kollineation $\kappa \in Coll(\mathbb{F}P^n)$ durch eine Gleichung

$$\mathfrak{y} = A \cdot \alpha(\mathfrak{x})$$

mit $A \in P\Gamma L_n(\mathbb{F})$ und $\alpha \in Aut(\mathbb{F})$ dargestellt werden kann. Aus der Geradentreue folgt mit Bemerkung 7.33, dass auch projektive Koordinatensysteme in solche abgebildet

werden. Zu einem projektiven Koordinatensystem

$$\mathfrak{a}_0, \mathfrak{a}_1, \cdots, \mathfrak{a}_n, \mathfrak{e} = \mathfrak{a}_0 + \mathfrak{a}_1 + \cdots + \mathfrak{a}_n$$

erhält man durch $\kappa$ also ein Bildkoordinatensystem, das mit einer projektiven, linearen Abbildung $\varphi \in PGl_n(\mathbb{F})$ auf das ursprüngliche Koordinatensystem zurück abgebildet werden kann. Nun muss nur noch gezeigt werden, dass $\psi = \kappa \circ \varphi \in Aut(\mathbb{F})$ durch einen Körperautomorphismus dargestellt werden kann. Es ist klar, dass $\psi$ geradentreu ist.

$$\begin{aligned}
\psi : \mathbb{F}P^n &\longrightarrow \mathbb{F}P^n \\
\mathfrak{x} &\longmapsto \mathfrak{y} = \psi(\mathfrak{x}) \\
\text{in projektiven Koordinaten } [x_0, \cdots, x_n] &\longmapsto [y_0, \cdots, y_n] \\
\text{insbesondere } \mathfrak{a}_0 = [1, 0, \cdots, 0] &\longmapsto \mathfrak{a}_0 = [1, 0, \cdots, 0] \\
&\cdots \\
\mathfrak{a}_n = [0, \cdots, 0, 1] &\longmapsto \mathfrak{a}_n = [0, \cdots, 0, 1] \\
\mathfrak{e} = [1, \cdots, 1, 1] &\longmapsto \mathfrak{e} = [1, \cdots, 1, 1]
\end{aligned}$$

Wir konstruieren nun den Bildpunkt $\mathfrak{y}$ eines beliebigen Punktes $\mathfrak{x}$ mit hilfe der Geradentreue. Die Hyperebene durch $\mathfrak{x}$ und den Punkten $\mathfrak{a}_k$ ohne $\mathfrak{a}_0$ und $\mathfrak{a}_j$ schneidet die Gerade durch $\mathfrak{a}_0$ und $\mathfrak{a}_j$ in einem Punkt $\mathfrak{x}_j = [1, 0, \cdots, x'_j, 0, \cdots, 0]$. Dabei ist $x'_j = \frac{x_j}{x_0}$ die inhomogene Koordinate. Aus der Geradentreue folgt nun dasselbe für den Bildpunkt $\mathfrak{y}$, so dass $\psi$ durch skalare Funktionen $y'_j = f_j(x'_j)$ dargestellt werden kann. Da der Einheitspunkt $\mathfrak{e}$ in sich abgebildet wird, gilt

$$x'_1 = x'_2 = \cdots = x'_n = \lambda \quad \Rightarrow \quad f_1(\lambda) = f_2(\lambda) = \cdots = f_n(\lambda)$$

Das heisst, die skalaren Funktion $f_j$ stimmen alle überein und es gilt

$$\begin{aligned}
f(0) &= 0 \quad \text{wegen } \psi(\mathfrak{a}_0) = \mathfrak{a}_0 \\
f(1) &= 1 \quad \text{wegen } \psi(\mathfrak{e}) = \mathfrak{e}
\end{aligned}$$

Wir betrachten nun Geraden in der Ebene $A_0, A_1, A_2$. Diese haben in inhomogenen Koordinaten die Gleichung

$$x'_2 = c_1 x'_1 + c_0$$

Die Abbildung $\psi$ bildet diese Geraden wieder in Geraden ab mit der Gleichung

$$y_2' = d_1 y_1' + d_0$$

Dabei gilt für alle $x_1 \in \mathbb{F}$

$$\begin{aligned} f(c_1 x_1' + c_0) &= d_1 f(x_1') + d_0 \\ \Rightarrow \quad f(c_0) &= d_0 \quad \text{für } x_1' = 0 \\ \Rightarrow \quad f(c_1) &= d_1 \quad \text{für } x_1' = 1 \\ \Rightarrow \quad f(c_1 x_1' + c_0) &= f(c_1) f(x_1') + f(c_0) \end{aligned}$$

Setzt man in der letzten Gleichung $x_1' = 1$, $c_1 = a$ und $c_0 = b$, folgt

$$f(a + b) = f(a) + f(b)$$

Setzt man $x_1' = b$, $c_1 = a$ und $c_0 = 0$, folgt

$$f(a \cdot b) = f(a) \cdot f(b)$$

Dies kennzeichnet einen Körperautomorphismus. □

## 7.7. Der Satz von Zassenhaus

In Abschnitt 6 wurde bereits ausgeführt, dass die Transitivität und insbesondere eine mehrfache Transitivität eine starke Bedingung an eine Permutationsgruppe darstellt. Zassenhaus hat 1936 ein Ergebnis für scharf-3-transitive Permutationsgruppen bewiesen. Dazu betrachten wir zunächst eine Untergruppe $M(q) < \Gamma F(q)$ der Gruppe der gebrochen semilinearen Transformationen für $q = p^{2r} (p \neq 2)$.

**Proposition 7.35.** *Sei $q = p^{2r} (p \neq 2)$. Dann ist der folgende Automorphismus $\sigma$ idempotent.*

$$\begin{aligned} \sigma : \mathbb{F}_q &\longrightarrow \mathbb{F}_q \\ x &\longmapsto x^{p^r} \end{aligned}$$

*Beweis.* Wir müssen zeigen, dass

$$\sigma^2 = \mathbb{1}$$

gilt. Für beliebige $x \in \mathbb{F}_q$ rechnet man:

$$\begin{aligned}\sigma(\sigma(x)) &= \sigma(x^{p^r}) \\ &= (x^{p^r})^{p^r} \\ &= x^{p^r \cdot p^r} \\ &= x^{p^{2r}} \\ &= x^q \\ &= x\end{aligned}$$

Denn die multiplikative Gruppe von $\mathbb{F}_q$ hat nur $q-1$ Elemente und ist zyklisch nach Korollar **??**. □

**Bemerkung 7.36.** Tatsächlich ist in diesem Fall der Automorphismus $\sigma$ durch $\sigma^2 = \mathbb{1}$ eindeutig bestimmt.

Eine gebrochen lineare Funktion $f(x) = \frac{ax+b}{cx+d}$ ändert sich nicht, wenn Zähler und Nenner mit einer Zahl $\mu \in \mathbb{F}_q^*$ multipliziert werden. Die Determinante lautet dann aber $\mu^2(ad-bc)$. Das heisst, in Körpern $\mathbb{F}_q$ mit $q = p^r (p \neq 2)$ können wir gebrochen lineare Transformationen mit einer Quadratzahl als Determinante von solchen unterscheiden, deren Determinante keine Quadratzahl ist. Wir können also folgende Teilmengen in der Gruppe der gebrochen linearen Transformationen $\Gamma F(q)$ definieren.

**Definition 7.37.** Sei $q = p^{2r} (p \neq 2)$ und $\sigma \in Aut(\mathbb{F}_q)$ wie in Proposition 7.35. Dann sind in $\Gamma F(q)$ folgende Teilmengen definiert:

$\underline{S}$

$$S = \{\, x \mapsto \frac{ax+b}{cx+d} \mid (ad-bc) \in (\mathbb{F}_q^*)^2 \,\}$$

$\underline{T}$

$$T = \{\, x \mapsto \frac{a\sigma(x)+b}{c\sigma(x)+d} \mid (ad-bc) \notin (\mathbb{F}_q^*)^2 \,\}$$

$\underline{M(q)}$

$$M(q) = S \cup T$$

**Proposition 7.38.** *(i) $S$ ist eine Untergruppe in $\Gamma F(q)$.*

*(ii) $M(q)$ ist eine Untergruppe in $\Gamma F(q)$.*

*(iii) $M(q)$ operiert scharf-3-transitiv auf $\hat{\mathbb{F}}_q$.*

*(iv) Die Ordnung von $M(q)$ ist*

$$|M(q)| = (q+1) \cdot q \cdot (q-1) = q \cdot (q^2-1)$$

*Beweis.* ad (i) Die Identität $\mathbb{1} : x \mapsto x$ ist wegen $\det(\mathbb{1}) = 1 = 1^2$ in $S$ enthalten. Die Verknüpfung von zwei Elementen $s_1, s_2$ in $S$ ist wieder in $S$. Denn die Determinanten der entsprechenden Matrizen $\begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}$ multiplizieren sich bei der Verknüpfung und das Produkt von Quadratzahlen ist wieder eine Quadratzahl. Zu jedem Element $s \in S$ ist die inverse Transformation $s^{-1}$ wieder in $S$. Denn Matrix von $s$ ist invertierbar, da die Determinante ungleich Null ist. Und der Kehrwert der Determinante ist wieder eine Quadratzahl.

ad (ii) Wegen Item (i) ist nur noch zu zeigen, dass Verknüpfungen mit und Inverse von $t \in T$ wieder in $M(q)$ liegen. Da $\sigma$ idempotent ist, lautet die Inverse zu

$$t : x \longmapsto \frac{a\sigma(x) + b}{c\sigma(x) + d}$$

$$t^{-1} : x \longmapsto \frac{d\sigma(x) - b}{-c\sigma(x) + a}$$

mit derselben Determinante. Da das Produkt einer Quadratzahl mit einer Nicht-Quadratzahl keine Quadratzahl sein kann, liegt die Verknüpfung einer Transformation $s \in S$ mit $t \in T$ stets wieder in $T$. Dagegen liegt die Verknüpfung von zwei Transformationen aus $T$ in $S$. Denn in endlichen Körpern ist das Produkt von zwei Nicht-Quadratzahlen eine Quadratzahl. In endlichen Körpern ist die multiplikative Gruppe die zyklische Gruppe $C_{q-1} \cong \mathbb{Z}/(q-1)$, die isomorph zum additiven Restklassenring ist. Hier entsprechen die geraden Zahlen den Quadratzahlen in $C_{q-1}$ und die Addition zweier ungeraden Zahlen ist gerade.

ad (iii) Wie im Beweis der 3-Transitivität von $LF(\mathbb{F})$ in Theorem 7.23 kann eine eindeutige, gebrochen semilineare Transformation in $M(q)$ konstruiert werden, die das Tripel $0, 1, \infty$ in ein beliebiges Tripel $x, y, z$ abbildet. Falls die Determinante dieser Abbildung keine Quadratzahl ist, wird der Automorphismus $\sigma$ angewendet. Man beachte, dass $\sigma(0) = 0, \sigma(1) = 1$ und $\sigma(\infty) = \infty$ gilt.

ad (iv) Dies folgt direkt aus Item (iii) und Korollar 6.9.

□

**Bemerkung 7.39.** Die Untergruppe $S < M(q)$ hat den Index 2 und ist damit Normalteiler in $M(q)$. Daher ist $M(q)$ nicht einfach.

Wir haben nun zwei verschiedene Permutationsgruppen $LF(\mathbb{F}_q) = PGL_2(q) \neq M(q)$ gefunden, die beide scharf-3-transitiv auf der projektiven Geraden $\hat{\mathbb{F}}_q$ operieren. Der Satz von Zassenhaus sagt nun aus, dass es auch keine weiteren scharf-3-transitiven Permutationsgruppen gibt.

**Theorem 7.40.** *Satz von Zassenhaus, 1936*
*Eine scharf-3-transitive Permutationsgruppe $G \curvearrowright X$ ist entweder isomorph zu*

$$PGL_2(q) \curvearrowright \hat{\mathbb{F}}_q$$

*oder*

$$M(q) \curvearrowright \hat{\mathbb{F}}_q \quad \text{für } q = p^{2r}, p \neq 2$$

*Insbesondere haben die Operationen den Grad $q+1$ und die Gruppenordnung ist $q \cdot (q^2-1)$.*

**Beispiel 7.41.** Die kleinste mögliche Gruppe $M(q)$ erhalten wir für $p = 3$ und $r = 1$. Damit ist $q = p^{2r} = 3^2 = 9$. Die Ordnung von $M(9)$ ist dann

$$|M(9)| = 8 \cdot 9 \cdot 10 = 720$$

Diese stimmt mit der Ordnung der projektiven, linearen Gruppe $PGl_2(9)$ überein. Beide operieren auf der projektiven Geraden $\hat{\mathbb{F}}_9$ und sind nicht isomorph.

# 8. Mathieu-Gruppen

Der französische Mathematiker Emile Leonard Mathieu (15. Mai 1835 bis 19. Oktober 1890) studierte Gruppen mit mehrfach transitiver Wirkung. Die Gruppen $M_{10}$, $M_{11}$ und $M_{12}$ hat er 1861 gefunden. 1873 kamen die Gruppen $M_{21}$, $M_{22}$, $M_{23}$ und $M_{24}$ dazu. Der Index gibt die Mächtigkeit der Menge an, auf die die Mathieu-Gruppe wirkt. Bis auf die Gruppe $M_{10}$ mit der Ordnung 720 sind alle genannten Gruppen einfach. Das wurde allerdings erst 1890 nach einigen Fehlversuchen bewiesen. Sie gehören zu den sporadischen, einfachen Gruppen, die keiner Klasse wie die alternierenden oder projektiven, speziellen, linearen Gruppen angehören. Erst 1965 wurde von Zvonimir Janko eine weitere sporadische, einfache Gruppen gefunden - die Gruppe $J_1$ mit der Ordnung $2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 = 175\,560$.

Zu Ehren von Emile Mathieu wurde der Asteroid 27947 Emilemathieu genannt.

Die Konstruktion der Mathieu-Gruppen folgt einem einheitlichen Konzept, das zunächst erläutert wird. Eine k-transitive Permutationsgruppe $G \curvearrowright X$ wird durch Hinzunahme eines weiteren Elementes zur Menge $X$ zu einer $(k+1)$-transitiven Permutationsgruppe $\hat{G} \curvearrowright \hat{X}$ erweitert. Die Bedingungen, unter denen diese Erweiterung funktioniert, sind allerdings nur für die 7 Mathieu-Gruppen erfüllt.

## 8.1. Erweiterungssatz von Witt

**Theorem 8.1.** *Erweiterungssatz von Witt*
*Die Gruppe $G$ operiere auf einer $n$-elementigen Menge $X = [n]$ $k$-transitiv mit $k \geq 2$. Die Menge $X$ wird durch ein Element $\infty$ zur Menge $\hat{X} = X \cup \{\infty\} \cong [n+1]$ erweitert. Für die Elemente $x \in X$, $g \in G \setminus G_x$ und $h \in S_{\hat{X}} \setminus S_X$ werden folgende Eigenschaften vorausgesetzt:*

*(i)* $h^2 \in G$, *insbesondere* $h^2(\infty) = \infty$

*(ii)* $(gh)^3 \in G$, *insbesondere* $(gh)^3(\infty) = \infty$

*(iii)* $hG_xh = G_x$

*Dann erzeugt $G$ und $h$ eine Untergruppe $G < \hat{G} = \langle G, h \rangle = G \cup GhG \leq S_{\hat{X}}$ in der erweiterten symmetrischen Gruppe $S_{\hat{X}}$. Die Permutationsgruppe $\hat{G} \curvearrowright \hat{X}$ ist $(k+1)$-transitiv und hat die Ordnung*

$$|\hat{G}| = (n+1) \cdot |G|$$

*Beweis.* Zunächst bemerken wir einige Folgerungen aus den Eigenschaften.

(i) Da $g \notin G_x$ vorausgesetzt ist, ist $x$ kein Fixpunkt von $g$.

$$g \circ x \neq x$$

(ii) Da $h \notin S_X$ vorausgesetzt ist, ist $\infty$ kein Fixpunkt von $h$.

$$h \circ \infty \neq \infty$$

(iii) Aus der Voraussetzung $(gh)^3 \in G$ folgt

$$\underbrace{g^{-1} \cdot h^{-1} \cdot \underbrace{g^{-1} \cdot (gh)}_{} \cdot (gh) \cdot (gh)}_{= 1} = h \cdot g \cdot h \in G$$

(iv) Nach Proposition 6.17 ist $G$ die disjunkte Vereinigung des Stabilisators $G_x$ mit der Doppelnebenklasse $G_x\,h\,G_x$.

$$G = G_x \sqcup G_x g G_x$$

Wir zeigen nun, dass $G \cup G\cdot h\cdot G$ abgeschlossen ist gegenüber Produkt und Inversenbildung und daher eine Gruppe ist.

$$a \in G \quad \Rightarrow \quad a^{-1} \in G$$

Sei $a' = g_1 \cdot h \cdot g_2 \in G\cdot h\cdot G$. Dann ergibt sich für die Inverse

$$\begin{aligned} a'^{-1} &= (g_1 \cdot h \cdot g_2)^{-1} \\ &= g_2^{-1} \cdot h^{-1} \cdot g_1^{-1} \\ &= g_2^{-1} \cdot \underbrace{(h^2)^{-1}}_{\in G} \cdot h \cdot g_1^{-1} \\ &\in G\cdot h\cdot G \end{aligned}$$

Damit liegt für alle Elemente $a \in G \cup G\cdot h\cdot G$ die Inverse $a^{-1}$ wieder in $G \cup G\cdot h\cdot G$. Bevor wir zeigen, dass $G \cup G\cdot h\cdot G$ auch bezüglich Produktbildung abgeschlossen ist, beweisen wir eine nützliche Formel für $h\cdot G\cdot h$.

$$\begin{aligned} h\cdot G\cdot h &= h\cdot (G_x \cup G_x\cdot g\cdot G_x)\cdot h \\ &= (h\cdot G_x\cdot h) \cup (h\cdot G_x\cdot \underbrace{hh^{-1}}_{\text{eingefügt}} \cdot g \cdot \underbrace{h^{-1}h}_{\text{eingefügt}} \cdot G_x\cdot h) \\ &= G_x \cup \underbrace{h\cdot G_x\cdot h}_{=G_x}\cdot h^{-1}\cdot g\cdot h^{-1}\cdot \underbrace{h\cdot G_x\cdot h}_{=G_x} \\ &= G_x \cup \underbrace{G_x\cdot (h^2)^{-1}}_{\subseteq G}\cdot h\cdot g\cdot h\cdot \underbrace{(h^2)^{-1}\cdot G_x}_{\subseteq G} \\ &\subseteq G \cup G\cdot g^{-1}\cdot h^{-1}\cdot g^{-1}\cdot \underbrace{(gh)^3}_{\in G}\cdot G \\ &= G \cup G\cdot h\cdot G \end{aligned}$$

Seien nun

$$\begin{aligned} a_1\cdot h\cdot a_2 &\in G\cdot h\cdot G \\ b_1\cdot h\cdot b_2 &\in G\cdot h\cdot G \end{aligned}$$

zwei Elemente in $G \cdot h \cdot G$. Dann gilt für das Produkt

$$a_1 \cdot \underbrace{h \cdot a_2 \cdot b_1 \cdot h}_{\in h \cdot G \cdot h \subseteq G \cup G \cdot h \cdot G} \cdot b_2 \in G \cup G \cdot h \cdot G$$

Da $G \cup G \cdot h \cdot G$ eine Gruppe ist und $G$ und $h$ enthält, stimmt sie mit $\hat{G}$ überein.

Die Gruppe $\hat{G}$ operiert transitiv auf $\hat{X}$. Die Standgruppe von $\infty$ ist $\hat{G}_\infty = G$. Da $G \curvearrowright X$ $n$-transitiv ist, operiert nach dem Reduktionslemma 6.15 Teil b) die Gruppe $\hat{G}$ $(k+1)$-transitiv auf $\hat{X}$. Die Bahn von $\infty$ ist $\hat{G}\infty = G\infty \cup GhG\infty = \{\infty\} \cup X$. Denn nach Voraussetzung ist $h \circ \infty \in X$. Nach dem Bahn-Standgruppen-Satz 1.53 gilt also

$$|\hat{G}| = |G| \cdot (n+1)$$

□

## 8.2. Konstruktion der Mathieu-Gruppe $M_{11}$

Als Ausgangspunkt für die Konstruktion der Mathieu-Gruppe $M_{11}$ wählen wir die Mathieu-Gruppe $M_{10}$. Diese haben wir bereits in Definition 7.37 und Proposition 7.38 kennengelernt. Diese wirkt 3-transitiv auf die 10-elementige Menge $\hat{\mathbb{F}}_9$.

**Definition 8.2.** Die Mathieu-Gruppe $M_{10}$ ist identisch mit der Gruppe $M(9)$ aus Definition 7.37.

**Theorem 8.3.** *Es gibt eine transitive Erweiterung von $M_{10} \curvearrowright \hat{\mathbb{F}}_9$: Die Mathieu-Gruppe $M_{11}$. Diese hat die Ordnung*

$$|M_{11}| = |M_{10}| \cdot 11 = 7\,920$$

*Sie operiert 4-transitiv auf* $[11]$.

*Beweis.* In Proposition 7.38 haben wir gesehen, dass $M_{10} \curvearrowright X$ 3-transitiv operiert auf

$$X = \hat{\mathbb{F}}_9 = \mathbb{F}_9 \cup \{\infty\} \cong [10]$$

Und die Ordnung ist $|M_{10}| = 720$. Wir wenden den Erweiterungssatz von Witt 8.1 auf die Gruppe $G = M_{10}$ und die Menge $X = \hat{\mathbb{F}}_9$ an. Da $\infty \in \hat{\mathbb{F}}_9$ bereits in $X$ enthalten ist, erweitern wir die Menge $X$ durch das Symbol $\omega$. Nun müssen Elemente $x \in X$, $g \in G \setminus G_x$ und $h \in S_{\hat{X}} \setminus S_X$ so gewählt werden, dass die Bedingung im Erweiterungssatz von Witt erfüllt sind.

$\underline{x}$ Für $x \in X$ wird $x = \infty \in \hat{\mathbb{F}}_9$ gewählt.

$\underline{g}$ Zur Auswahl von $g \in G \setminus G_\infty$ nutzen wir die Struktur der Menge $X$ als projektiver Gerade aus. Somit kann die Gruppe $G = M_{10} = M(9) = S \cup T$ als Gruppe von semilinearen Transformationen auf $\hat{\mathbb{F}}_9$ aufgefasst werden. Wir wählen

$$\begin{aligned} g : \hat{\mathbb{F}}_9 &\longrightarrow \hat{\mathbb{F}}_9 \\ \lambda &\longmapsto g(\lambda) = \frac{1}{\lambda} \end{aligned}$$

Als semilineare Transformation ist $g$ idempotent. Das heisst, $g$ hat als Gruppenelement die Ordnung 2. Andrerseits wirkt $g$ als Permutation auf $\hat{\mathbb{F}}_9$ als 10-elementige Menge. Da die multiplikative Gruppe im Körper $\mathbb{F}_9 \cong C_8$ isomorph zur zyklischen Gruppe $C_8$ ist, können mit dem erzeugenden Element $\pi \in C_8$ die Elemente der projektiven Geraden $\hat{\mathbb{F}}_9$ wie folgt angegeben werden:

$$\hat{\mathbb{F}}_9 = \{\, 0\,,\ \infty\,,\ 1\,,\ \pi\,,\ \pi^2\,,\ \pi^3\,,\ \pi^4\,,\ \pi^5\,,\ \pi^6\,,\ \pi^7 \,\}$$

Als Permutation auf diesen Elementen kann $g$ wie folgt dargestellt werden:

$$g = (0\ \infty) \cdot (\pi\ \pi^7) \cdot (\pi^2\ \pi^6) \cdot (\pi^3\ \pi^5)$$

Wegen $g(0) = \infty$ gilt $g \notin G_\infty$.

$\underline{h}$ Das Element $h \in S_{\hat{X}} \setminus S_X$ wird wie folgt gewählt:

$$h = (\infty\ \omega) \cdot (\pi\ \pi^2) \cdot (\pi^3\ \pi^7) \cdot (\pi^5\ \pi^6)$$

Die Gültigkeit der Bedingungen im Erweiterungssatz von Witt 8.1 können nun leicht nachgeprüft werden. Da $h$ die Ordnung 2 hat, gilt:

$$h^2 = \mathbb{1}$$

Und

$$g\,h = (0\ \omega\ \infty) \cdot (\pi\ \pi^3\ \pi^6) \cdot (\pi^2\ \pi^5\ \pi^7)$$

Damit hat $g\,h$ die Ordnung 3 und es gilt $(g\,h)^3 = \mathbb{1}$. Für ein beliebiges Element $k \in G_\infty$

gilt

$$\begin{aligned} k(\infty) &= \infty \\ \text{sowie} \quad k(\omega) &= \omega \end{aligned}$$

Somit ist

$$\begin{aligned} (h\,k\,h)(\infty) &= (h\,k)(\omega) \\ &= h(\omega) \\ &= \infty \\ \Rightarrow \quad G_\infty &\subseteq hG_\infty h \\ \Rightarrow \quad hG_\infty h &\subseteq h^2 G_\infty h^2 = G_\infty \text{wegen } h^2 = \mathbb{1} \end{aligned}$$

□

## 8.3. Konstruktion der Mathieu-Gruppe $M_{12}$

Dieselbe Vorgehensweise wie in Theorem 8.3 bei der Konstruktion der Mathieu-Gruppe $M_{11}$ kann nochmals angewendet werden. Als Ausgangspunkt für die Konstruktion der Mathieu-Gruppe $M_{12}$ wählen wir die Mathieu-Gruppe $M_{11}$ aus Theorem 8.3. Diese wirkt 4-transitiv auf die 11-elementige Menge $\hat{\mathbb{F}}_9 \cup \{\,\omega\,\}$.

**Theorem 8.4.** *Es gibt eine transitive Erweiterung von $M_{11} \curvearrowright \hat{\mathbb{F}}_9 \cup \{\,\omega\,\}$: Die Mathieu-Gruppe $M_{12}$. Diese hat die Ordnung*

$$|\,M_{12}\,| = |\,M_{11}\,| \cdot 12 = 95\,040$$

*Sie operiert 5-transitiv auf* $[12]$.

*Beweis.* In Theorem 8.3 haben wir gesehen, dass $M_{11} \curvearrowright X$ 4-transitiv operiert auf

$$X = \mathbb{F}_9 \cup \{\,\infty\,\omega\,\} \cong [11]$$

Und die Ordnung ist $|\,M_{10}\,| = 7\,920$. Wir wenden den Erweiterungssatz von Witt 8.1 auf die Gruppe $G = M_{11}$ und die Menge $X = \mathbb{F}_9 \cup \{\,\infty\,\omega\,\}$ an. Die Menge $X$ wird durch ein neues Element $\tau$ zu $\hat{X} = X \cup \{\,\tau\,\}$ erweitert. Nun müssen Elemente $x \in X$, $g \in G \setminus G_x$ und $h \in S_{\hat{X}} \setminus S_X$ so gewählt werden, dass die Bedingung im Erweiterungssatz von Witt erfüllt sind.

$\underline{x}$ Für $x \in X$ wird $x = \omega$ gewählt.

$\underline{g}$ Für $g \in G \setminus G_\omega$ kann das Element $h$ aus der Konstruktion der Mathieu-Gruppe $M_{11}$ gewählt werden.

$$g = (\infty\ \omega) \cdot (\pi\ \pi^2) \cdot (\pi^3\ \pi^7) \cdot (\pi^5\ \pi^6)$$

Wie bei der Konstruktion von $M_{11}$ in Theorem 8.3 ist $\pi$ wieder ein erzeugendes Element der zyklischen Gruppe $C_8$. Wegen $g(\omega) = \infty$ gilt $g \notin G_\omega$.

$\underline{h}$ Das Element $h \in S_{\hat{X}} \setminus S_X$ wird wie folgt gewählt:

$$h = (\omega\ \tau) \cdot (\pi\ \pi^3) \cdot (\pi^2\ \pi^6) \cdot (\pi^5\ \pi^7)$$

Die Gültigkeit der Bedingungen im Erweiterungssatz von Witt 8.1 können nun leicht nachgeprüft werden. Da $h$ die Ordnung 2 hat, gilt:

$$h^2 = \mathbb{1}$$

Weiter gilt:

$$g\,h = (\infty\ \tau\ \omega) \cdot (\pi\ \pi^7\ \pi^7) \cdot (\pi^2\ \pi^3\ \pi^5)$$

Damit hat $g\,h$ die Ordnung 3 und es gilt $(g\,h)^3 = \mathbb{1}$. Für ein beliebiges Element $k \in G_\omega$ gilt

$$\begin{aligned} k(\omega) &= \omega \\ \text{sowie} \quad k(\tau) &= \tau \end{aligned}$$

Somit ist

$$\begin{aligned} (h\,k\,h)(\omega) &= (h\,k)(\tau) \\ &= h(\tau) \\ &= \omega \\ \Rightarrow \quad G_\omega &\subseteq hG_\omega h \\ \Rightarrow \quad hG_\omega h &\subseteq h^2 G_\omega h^2 = G_\omega \text{wegen } h^2 = \mathbb{1} \end{aligned}$$

□

Eine nochmalige Anwendung des Verfahrens auf die Mathieu-Gruppe $M_{12}$ ist leider

nicht mehr möglich. Jedoch ist die Konstruktion mit der projektiven, speziellen, linearen Gruppe $PSl_3(\mathbb{F}_4)$ als Ausgangspunkt erfolgreich und führt auf die weiteren Mathieu-Gruppen $M_{22}, M_{23}$ und $M_{24}$.

## 8.4. Konstruktion der Mathieu-Gruppe $M_{22}$

**Theorem 8.5.** *Es gibt eine transitive Erweiterung von $PSl_3(\mathbb{F}_4) \curvearrowright \mathbb{F}_4P^2$: Die Mathieu-Gruppe $M_{22}$. Diese hat die Ordnung*

$$|M_{22}| = |PSl_3(\mathbb{F}_4)| \cdot 22 = 443\,520$$

*Sie operiert 3-transitiv auf* $[22]$.

*Beweis.* Nach Proposition 7.4 beträgt die Anzahl der Elemente in der projektiven Ebene $\mathbb{F}_4P^2$

$$|\mathbb{F}_4P^2| = 4^2 + 4 + 1 = 21$$

Mit den Bezeichnungen des Erweiterungssatzes von Witt 8.1 wird zur projektiven Ebene $X = \mathbb{F}_4P^2$ ein neues Symbol $\infty$ hinzugenommen und man erhält

$$\hat{X} = X \cup \{\infty\}$$

mit 22 Elementen. Die Ausgangsgruppe wird wieder mit $G = PSl_3(\mathbb{F}_4)$ bezeichnet. Nun müssen Elemente $x \in X$, $g \in G \setminus G_x$ und $h \in S_{\hat{X}} \setminus S_X$ so gewählt werden, dass die Bedingung im Erweiterungssatz von Witt erfüllt sind.

$\underline{x}$ Für $x \in X$ wird ein Punkt in der projektiven Ebene gewählt. Dieser habe die projektiven Koordinaten

$$x = [1, 0, 0]$$

$\underline{g}$ Für $g \in G \setminus G_x$ wählen wir eine projektive Abbildung, die die ersten beiden Koordinaten vertauscht. Diese wird durch folgende Matrix dargestellt:

$$g = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Es ist klar, dass $g$ die Ordnung 2 hat und $x$ kein Fixpunkt von $g$ ist. Da $\det(g) = 1$ in $\mathbb{F}_4$ gilt, ist $g \in PSl_3(\mathbb{F}_4)$.

$\underline{h}$ Zur Auswahl von $h$ betrachten wir die Abbildung

$$\begin{aligned} f_1 : \mathbb{F}_4P^2 &\longrightarrow \mathbb{F}_4P^2 \\ [\lambda,\mu,\nu] &\longmapsto [\lambda^2+\mu\nu, \mu^2, \nu^2] \end{aligned}$$

Dies ist eine Involution. Da $\mathbb{F}_4$ die Charakteristik 2 hat und die multiplikative Gruppe $\mathbb{F}_4^* \cong C_3$ die zyklische Gruppe der Ordnung 3 ist, gilt nämlich:

$$\begin{aligned} f_1(f_1([\lambda,\mu,\nu])) &= f_1([\lambda^2+\mu\nu, \mu^2, \nu^2]) \\ &= [(\lambda^2+\mu\nu)^2+\mu^2\nu^2, \mu^4, \nu^4] \\ &= [\lambda^4+2\lambda^2\mu\nu+2\mu^2\nu^2, \mu, \nu] \\ &= [\lambda,\mu,\nu] \end{aligned}$$

Damit wählen wir $h \in S_{\hat{X}} \setminus S_X$ wie folgt:

$$h = (\infty\ x) \cdot f_1$$

Die Gültigkeit der Bedingungen im Erweiterungssatz von Witt 8.1 können nun leicht nachgeprüft werden. Da $f_1$ eine Involution ist, hat $h$ die Ordnung 2 und es gilt insbesondere

$$h^2 = \mathbb{1} \in G$$

Zum Nachweis, dass $(gh)^3 \in G_x$ gilt, unterscheiden wir verschiedene Fälle $[\lambda,\mu,\nu] =$

$\underline{\infty}$

$$\begin{aligned} (ghghgh)(\infty) &= (ghghg)([1,0,0]) \\ &= (ghgh)([0,1,0]) \\ &= (ghg)([0,1,0]) \\ &= (gh)([1,0,0]) \\ &= g(\infty) \\ &= \infty \end{aligned}$$

$\underline{[1,0,0]}$

$$\begin{aligned}(ghghgh)([1,0,0]) &= (ghghg)(\infty)\\ &= (ghgh)(\infty)\\ &= (ghg)([1,0,0])\\ &= (gh)([0,1,0])\\ &= g([0,1,0])\\ &= [1,0,0]\end{aligned}$$

$\underline{[0,1,0]}$

$$\begin{aligned}(ghghgh)([0,1,0]) &= (ghghg)([0,1,0])\\ &= (ghgh)([1,0,0])\\ &= (ghg)(\infty)\\ &= (gh)(\infty)\\ &= g([1,0,0])\\ &= [0,1,0]\end{aligned}$$

$\underline{[\lambda,\mu,\nu]}$

$$\begin{aligned}(ghghgh)([\lambda,\mu,\nu]) &= (ghghg)([\lambda^2+\mu\nu,\mu^2,\nu^2])\\ &= (ghgh)([\mu^2,\lambda^2+\mu\nu,\nu^2])\\ &= (ghg)([\mu(1+\nu^3)+\lambda^2\nu^2,\lambda+\mu^2\nu^2,\nu])\\ &= (gh)([\lambda+\mu^2\nu^2,\mu(1+\nu^3)+\lambda^2\nu^2,\nu])\\ &= g([\lambda^2+\underbrace{\mu\nu+\mu\nu}_{=0}+\mu\nu+\lambda\nu^3,\mu^2(1+\nu^3)+\lambda\nu,\nu^2])\\ &= [\lambda\nu+\mu^2(1+\nu^3),\lambda^2(1+\nu^3)+\mu\nu,\nu^2]\\ &= \begin{cases}[\lambda\nu,\mu\nu,\nu^2] & \text{für} \quad \nu\neq 0 \Rightarrow (1+\nu^3)=0\\ \quad =[\lambda,\mu,\nu] & \\ \hline [\mu^2,\lambda^2,0] & \text{für} \quad \nu=0\\ \quad =[(\lambda\mu)\mu^2,(\lambda\mu)\lambda,0] & \text{denn} \quad (\lambda\mu)\neq 0\\ \quad =[\lambda,\mu,0] & \end{cases}\end{aligned}$$

Daraus folgt $(gh)^3 = \mathbb{1} \in G$. Zum Nachweis der dritten Bedingung ($hG_xh = G_x$) beachten

wir, dass eine allgemeine Matrix $k \in G_x \leq PSl_3(\mathbb{F}_4)$ modulo einer skalaren Matrix folgende Form hat:

$$k = \begin{pmatrix} 1 & * & * \\ 0 & a & b \\ 0 & c & d \end{pmatrix}$$

mit der Determinante

$$\det(k) = ad - bc = 1$$

Nun wenden wir $hkh$ auf ein beliebiges Element in $\mathbb{F}_4P^2 \setminus \{[1,0,0]\}$ an und erhalten

$$\begin{aligned}
(hkh)([\lambda,\mu,\nu]) &= h \begin{pmatrix} 1 & * & * \\ 0 & a & b \\ 0 & c & d \end{pmatrix} \begin{pmatrix} \lambda^2 + \mu\nu + *\mu^2 + *\nu^2 \\ a\mu^2 + b\nu^2 \\ c\mu^2 + d\nu^2 \end{pmatrix} \\
&= \begin{pmatrix} \lambda^2 + \overbrace{\mu^2\nu^2 + ad\mu^2 + bc\nu^2}^{=\,0} + (* + ac)\mu + (* + bd)\nu \\ a^2\mu + b^2\nu \\ c^2\mu + d^2\nu \end{pmatrix} \\
&= \underbrace{\begin{pmatrix} 1 & * & * \\ 0 & a^2 & b^2 \\ 0 & c^2 & d^2 \end{pmatrix}}_{=\,k' \in G_x} \begin{pmatrix} \lambda \\ \mu \\ \nu \end{pmatrix}
\end{aligned}$$

Also ist $hkh \in G_x$ und wegen $h^2 = \mathbb{1}$ folgt auch

$$hG_xh = G_x$$

Nach Theorem 7.12 operiert die projektive, spezielle, lineare Gruppe $PSl_3(\mathbb{F}_4)$ 2-transitiv auf der projektiven Ebene $\mathbb{F}_4P^2$. Die gefundene Erweiterung

$$M_{22} = \langle\, PSl_3(\mathbb{F}_4)\,,\, h \,\rangle = PSl_3(\mathbb{F}_4) \cup PSl_3(\mathbb{F}_4)\, h\, PSl_3(\mathbb{F}_4)$$

hat nach dem Erweiterungssatz von Witt 8.1 die Ordnung

$$|\, PSl_3(\mathbb{F}_4)\,| \cdot 22 = 443\,520$$

und operiert 3-transitiv auf [22]. □

## 8.5. Konstruktion der Mathieu-Gruppe $M_{23}$

Ausgehend von der Mathieu-Gruppe $M_{22}$ führt dieselbe Vorgehensweise wie bei der Konstruktion der Mathieu-Gruppe $M_{22}$ auf eine neue Mathieu-Gruppe.

**Theorem 8.6.** *Es gibt eine transitive Erweiterung von $M_{22} \curvearrowright \mathbb{F}_4P^2 \cup \{\infty\}$: Die Mathieu-Gruppe $M_{23}$. Diese hat die Ordnung*

$$|M_{23}| = |M_{22}| \cdot 23 = 10\ 200\ 960$$

*Sie operiert 4-transitiv auf* $[23]$.

*Beweis.* Nach Theorem 8.5 beträgt die Anzahl der Elemente in der Menge

$$X = \mathbb{F}_4P^2 \cup \{\infty\}$$

$$|\mathbb{F}_4P^2 \cup \{\infty\}| = 22$$

Mit den Bezeichnungen des Erweiterungssatzes von Witt 8.1 wird zur Menge $X$ ein neues Symbol $\omega$ hinzugenommen und man erhält

$$\hat{X} = X \cup \{\omega\}$$

mit 23 Elementen. Die Ausgangsgruppe wird wieder mit $G = M_{22}$ bezeichnet. Nun müssen Elemente $x \in X$, $g \in G \setminus G_x$ und $h \in S_{\hat{X}} \setminus S_X$ so gewählt werden, dass die Bedingung im Erweiterungssatz von Witt erfüllt sind.

$\underline{x}$ Für $x \in X$ wird

$$x = \infty$$

gewählt.

$\underline{g}$ Für $g \in G \setminus G_x$ wählen wir $h$ aus der Konstruktion von $M_{22}$ (8.5).

$$g = (\infty\ x) \cdot f_1$$

Das Element $g$ hat die Ordnung 2 und $x$ ist kein Fixpunkt von $g$.

$\underline{h}$ Zur Auswahl von $h$ benötigen wir die Struktur des Körpers $\mathbb{F}_4$. Dieser entsteht aus dem Primkörper $\mathbb{F}_2$ mit dem irreduziblen Polynom $1 + t + t^2$ und es gilt

$$\mathbb{F}_4 \cong \mathbb{F}_2[t]/(1 + t + t^2)$$

Es gilt also

$$\begin{aligned} \mathbb{F}_4 &\cong \{0\,,\,1\,,\,t\,,\,1+t\,\} \\ \text{mit} \quad t^2 &= 1+t \end{aligned}$$

Damit konstruieren wir die Abbildung

$$\begin{aligned} f_2 : \mathbb{F}_4 P^2 &\longrightarrow \mathbb{F}_4 P^2 \\ [\lambda,\mu,\nu] &\longmapsto [\lambda^2, \mu^2, t\cdot\nu^2] \end{aligned}$$

Dies ist eine Involution. Denn es gilt:

$$\begin{aligned} f_2(f_2([\lambda,\mu,\nu])) &= f_2([\lambda^2,\mu^2,t\cdot\nu^2]) \\ &= [\lambda^4,\mu^4,t\cdot t^2\cdot\nu^4] \\ &= [\lambda,\mu,t\cdot(t+1)\cdot\nu] \\ &= [\lambda,\mu,\nu] \end{aligned}$$

Damit wählen wir $h \in S_{\hat{X}} \setminus S_X$ wie folgt:

$$h = (\infty\ \omega)\cdot f_2$$

Wir prüfen nun die Gültigkeit der Bedingungen im Erweiterungssatz von Witt 8.1. Da $f_2$ eine Involution ist, hat $h$ die Ordnung 2 und es gilt insbesondere

$$h^2 = \mathbb{1} \in G$$

Zum Nachweis, dass $(gh)^3 \in G$ gilt, unterscheiden wir verschiedene Fälle $[\lambda,\mu,\nu] =$

$\underline{\omega}$

$$\begin{aligned} (ghghgh)(\omega) &= (ghghg)(\infty) \\ &= (ghgh)([1,0,0]) \\ &= (ghg)([1,0,0]) \\ &= (gh)(\infty) \\ &= g(\omega) \\ &= \omega \end{aligned}$$

$\underline{\infty}$

$$\begin{aligned}(ghghgh)(\infty) &= (ghghg)(\omega)\\ &= (ghgh)(\omega)\\ &= (ghg)(\infty)\\ &= (gh)(\omega)\\ &= g(\infty)\\ &= \infty\end{aligned}$$

$\underline{[1,0,0]}$

$$\begin{aligned}(ghghgh)([1,0,0]) &= (ghghg)([1,0,0])\\ &= (ghgh)(\infty)\\ &= (ghg)(\omega)\\ &= (gh)(\omega)\\ &= g(\infty)\\ &= [1,0,0]\end{aligned}$$

$\underline{[\lambda,\mu,\nu]}$

$$\begin{aligned}(ghghgh)([\lambda,\mu,\nu]) &= (ghghg)([\lambda^2,\mu^2,t\cdot\nu^2])\\ &= (ghgh)(\lambda^4+t\mu^2\nu^2,\mu^4,t^2\cdot\nu^4])\\ &= (ghg)([\lambda^2+t^2\mu\nu,\mu^2,t^2\cdot\nu^2])\\ &= (gh)([\lambda+(t+t^2)\cdot\mu^2\nu^2,\mu,t\cdot\nu])\\ &= g([\lambda^2+\mu\nu,\mu^2,\nu^2])\\ &= [\lambda,\mu,\nu]\end{aligned}$$

Daraus folgt $(gh)^3 = \mathbb{1} \in G$.

Zum Nachweis der dritten Bedingung ($hG_xh = G_x$) beachten wir, dass in diesem Fall $x = \infty$ gewählt wurde und daher der Stabilisator $G_x$ identisch ist mit der speziellen, projektiven, linearen Gruppe $PSl_3(\mathbb{F}_4)$. Diese operiert 2-transitiv auf der projektiven Ebene $\mathbb{F}_4P^2$ und wir können nach Proposition 6.17 $PSl_3(\mathbb{F}_4)$ als disjunkte Vereinigung

des Stabilisators $(PSl_3(\mathbb{F}_4))_{[1,0,0]}$ mit der Doppelnebenklasse zu

$$v = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

schreiben:

$$G_x = PSl_3(\mathbb{F}_4) = (PSl_3(\mathbb{F}_4))_{[1,0,0]} \sqcup (PSl_3(\mathbb{F}_4))_{[1,0,0]}\, v\, (PSl_3(\mathbb{F}_4))_{[1,0,0]}$$

Nun gilt

$$\begin{aligned} (h \cdot v \cdot h)([\lambda, \mu, \nu]) &= (h \cdot v)([\lambda^2, \mu^2, t \cdot \nu^2]) \\ &= h([\mu^2, \lambda^2, t \cdot \nu^2]) \\ &= [\mu, \lambda, \nu] \quad \text{wegen } t^3 = 1 \\ &= v([\lambda, \mu, \nu]) \end{aligned}$$

Es genügt also zu zeigen, dass gilt

$$h\ (PSl_3(\mathbb{F}_4))_{[1,0,0]}\ h \subseteq (PSl_3(\mathbb{F}_4))_{[1,0,0]}$$

Denn dann folgt auch

$$\begin{aligned} h\ PSl_3(\mathbb{F}_4)\ h &= h\ (PSl_3(\mathbb{F}_4))_{[1,0,0]}\ h \sqcup h\ (PSl_3(\mathbb{F}_4))_{[1,0,0]}\ v\ (PSl_3(\mathbb{F}_4))_{[1,0,0]}\ h \\ &\subseteq (PSl_3(\mathbb{F}_4))_{[1,0,0]} \sqcup h\ (PSl_3(\mathbb{F}_4))_{[1,0,0]}\ h\ \underbrace{h\ v\ h}_{=\ v}\ h\ (PSl_3(\mathbb{F}_4))_{[1,0,0]}\ h \\ &\subseteq (PSl_3(\mathbb{F}_4))_{[1,0,0]} \sqcup (PSl_3(\mathbb{F}_4))_{[1,0,0]}\, v\, (PSl_3(\mathbb{F}_4))_{[1,0,0]} \\ &= PSl_3(\mathbb{F}_4) \end{aligned}$$

Eine allgemeine Matrix $k \in (PSl_3(\mathbb{F}_4))_{[1,0,0]}$ hat modulo einer skalaren Matrix folgende Form:

$$k = \begin{pmatrix} 1 & * & * \\ 0 & a & b \\ 0 & c & d \end{pmatrix}$$

mit der Determinante

$$\det(k) = ad - bc = 1$$

Nun wenden wir $hkh$ auf ein beliebiges Element in $\mathbb{F}_4P^2$ an und erhalten

$$\begin{aligned}(hkh)([\lambda,\mu,\nu]) &= h\begin{pmatrix}1 & * & *\\ 0 & a & b\\ 0 & c & d\end{pmatrix}\begin{pmatrix}\lambda^2+*\mu^2+*t\cdot\nu^2\\ a\mu^2+bt\cdot\nu^2\\ c\mu^2+dt\cdot\nu^2\end{pmatrix}\\ &= \begin{pmatrix}\lambda+*\mu+*\nu\\ a^2\mu+b^2t^2\cdot\nu\\ c^2\mu+d^2t^2\cdot\nu\end{pmatrix}\\ &= \underbrace{\begin{pmatrix}1 & * & *\\ 0 & a^2 & b^2\\ 0 & c^2 & d^2\end{pmatrix}}_{=\,k'\in(PSl_3(\mathbb{F}_4))_{[1,0,0]}}\begin{pmatrix}\lambda\\ \mu\\ \nu\end{pmatrix}\end{aligned}$$

Also ist $hkh \in (PSl_3(\mathbb{F}_4))_{[1,0,0]}$ und wegen $h^2 = \mathbb{1}$ folgt auch

$$h(PSl_3(\mathbb{F}_4))_{[1,0,0]}h = (PSl_3(\mathbb{F}_4))_{[1,0,0]}$$

Nach Theorem 8.5 operiert die Mathieu-Gruppe $M_{22}$ 3-transitiv auf der Menge

$$\mathbb{F}_4P^2 \cup \{\infty\} \simeq [22]$$

Die gefundene Erweiterung

$$M_{23} = \langle M_{22}, h\rangle = M_{22} \cup M_{22}\cdot h\cdot M_{22}$$

hat nach dem Erweiterungssatz von Witt 8.1 die Ordnung

$$|M_{22}|\cdot 23 = 10\ 200\ 960$$

und operiert 4-transitiv auf [23]. □

## 8.6. Konstruktion der Mathieu-Gruppe $M_{24}$

Obige Vorgehensweise kann nochmals auf die Mathieu-Gruppe $M_{23}$ angewendet werden und man erhält eine neue Mathieu-Gruppe.

**Theorem 8.7.** *Es gibt eine transitive Erweiterung von* $M_{23} \curvearrowright \mathbb{F}_4P^2 \cup \{\infty, \omega\}$*: Die*

*Mathieu-Gruppe $M_{24}$. Diese hat die Ordnung*

$$|M_{24}| = |M_{23}| \cdot 24 = 244\ 823\ 040$$

*Sie operiert 5-transitiv auf* $[24]$.

*Beweis.* Die Beweisführung geht ähnlich wie bei der Konstruktion der Mathieu-Gruppe $M_{23}$. Nach Theorem 8.6 beträgt die Anzahl der Elemente in der Menge

$$X = \mathbb{F}_4 P^2 \cup \{ \infty\, \omega \}$$

$$|\mathbb{F}_4 P^2 \cup \{ \infty\, \omega \}| = 23$$

Mit den Bezeichnungen des Erweiterungssatzes von Witt 8.1 wird zur Menge $X$ ein neues Symbol $\tau$ hinzugenommen und man erhält

$$\hat{X} = X \cup \{ \tau \}$$

mit 24 Elementen. Die Ausgangsgruppe wird wieder mit $G = M_{23}$ bezeichnet. Nun müssen Elemente $x \in X$, $g \in G \setminus G_x$ und $h \in S_{\hat{X}} \setminus S_X$ so gewählt werden, dass die Bedingung im Erweiterungssatz von Witt erfüllt sind.

$\underline{x}$ Für $x \in X$ wird

$$x = \omega$$

gewählt.

$\underline{g}$ Für $g \in G \setminus G_x$ wählen wir $h$ aus der Konstruktion von $M_{23}$ (8.6).

$$g = (\infty\ \omega) \cdot f_2$$

Das Element $g$ hat die Ordnung 2 und $x$ ist kein Fixpunkt von $g$.

$\underline{h}$ Zur Auswahl von $h$ konstruieren wir die Abbildung

$$\begin{aligned} f_3 : \mathbb{F}_4 P^2 &\longrightarrow \mathbb{F}_4 P^2 \\ [\lambda, \mu, \nu] &\longmapsto [\lambda^2, \mu^2, \nu^2] \end{aligned}$$

Dies ist eine Involution. Denn es gilt:

$$\begin{aligned} f_3(f_3([\lambda, \mu, \nu])) &= f_3([\lambda^2, \mu^2, \nu^2]) \\ &= [\lambda, \mu, \nu] \end{aligned}$$

Damit wählen wir $h \in S_{\hat{X}} \setminus S_X$ wie folgt:

$$h = (\tau\ \omega) \cdot f_3$$

Wir prüfen nun die Gültigkeit der Bedingungen im Erweiterungssatz von Witt 8.1. Da $f_3$ eine Involution ist, hat $h$ die Ordnung 2 und es gilt insbesondere

$$h^2 = \mathbb{1} \in G$$

Zum Nachweis, dass $(gh)^3 \in G$ gilt, unterscheiden wir verschiedene Fälle $[\lambda, \mu, \nu] =$

$\underline{\tau}$

$$\begin{aligned}(ghghgh)(\tau) &= (ghghg)(\omega)\\ &= (ghgh)(\infty)\\ &= (ghg)(\infty)\\ &= (gh)(\omega)\\ &= g(\tau)\\ &= \tau\end{aligned}$$

$\underline{\omega}$

$$\begin{aligned}(ghghgh)(\omega) &= (ghghg)(\tau)\\ &= (ghgh)(\tau)\\ &= (ghg)(\omega)\\ &= (gh)(\infty)\\ &= g(\infty)\\ &= \omega\end{aligned}$$

$\underline{\infty}$

$$\begin{aligned}(ghghgh)(\infty) &= (ghghg)(\infty)\\ &= (ghgh)(\omega)\\ &= (ghg)(\tau)\\ &= (gh)(\tau)\\ &= g(\omega)\\ &= \infty\end{aligned}$$

$\underline{[\lambda,\mu,\nu]}$

$$\begin{aligned}(ghghgh)([\lambda,\mu,\nu]) &= (ghghg)([\lambda^2,\mu^2,\nu^2])\\ &= (ghgh)(\lambda,\mu,t\cdot\nu])\\ &= (ghg)([\lambda^2,\mu^2,t^2\cdot\nu^2])\\ &= (gh)([\lambda,\mu,t^2\cdot\nu])\\ &= g([\lambda^2,\mu^2,t\cdot\nu^2])\\ &= [\lambda,\mu,\nu]\end{aligned}$$

Daraus folgt $(gh)^3 = \mathbb{1} \in G$.

Zum Nachweis der dritten Bedingung ($hG_xh = G_x$) beachten wir, dass in diesem Fall $x = \omega$ gewählt wurde und daher der Stabilisator $G_x$ identisch ist mit der Mathieu-Gruppe $M_{22}$. Diese operiert 4-transitiv auf der Menge $\mathbb{F}_4P^2 \cup \{\infty\}$ und wir können diese nach Proposition 6.17 als disjunkte Vereinigung des Stabilisators $(M_{22})_\infty$ mit der Doppelnebenklasse zu

$$v = \begin{pmatrix} 0 & 1 & 0\\ 1 & 0 & 0\\ 0 & 0 & 1\end{pmatrix}$$

schreiben:

$$\begin{aligned}G_x &= M_{22}\\ &= (M_{22})_\infty \sqcup (M_{22})_\infty\, v\, (M_{22})_\infty\\ &= PSl_3(\mathbb{F}_4) \sqcup PSl_3(\mathbb{F}_4)\, v\, PSl_3(\mathbb{F}_4)\end{aligned}$$

Nun gilt

$$\begin{aligned}(h \cdot v \cdot h)([\lambda,\mu,\nu]) &= (h \cdot v)([\lambda^2,\mu^2,\nu^2]) \\ &= h([\mu^2,\lambda^2,\nu^2]) \\ &= [\mu,\lambda,\nu] \\ &= v([\lambda,\mu,\nu])\end{aligned}$$

Mit $h_1 = ([1,0,0]\,,\,\infty) f_1$ aus der Konstruktion von $M_{22}$ 8.5 gilt ausserdem

$$\begin{aligned}(h \cdot h_1 \cdot h)([1,0,0]) &= (h \cdot h_1)([1,0,0]) \\ &= h(\infty) \\ &= \infty \\ &= h_1([1,0,0]) \\ (h \cdot h_1 \cdot h)(\infty) &= (h \cdot h_1)(\infty) \\ &= h([1,0,0]) \\ &= [1,0,0] \\ &= h_1(\infty) \\ (h \cdot h_1 \cdot h)([\lambda,\mu,\nu]) &= (h \cdot h_1)([\lambda^2,\mu^2,\nu^2]) \\ &= h([\lambda+\mu^2\nu^2,\mu^2,\nu^2]) \\ &= [\lambda^2+\mu\nu,\mu,\nu] \\ &= h_1([\lambda,\mu,\nu])\end{aligned}$$

Es genügt also zu zeigen, dass gilt

$$h\ (PSl_3(\mathbb{F}_4))_{[1,0,0]}\ h \subseteq (PSl_3(\mathbb{F}_4))_{[1,0,0]}$$

Denn dann folgt auch

$$\begin{aligned}h\ PSl_3(\mathbb{F}_4)\ h &= h\ (PSl_3(\mathbb{F}_4))_{[1,0,0]}\ h \sqcup h\ (PSl_3(\mathbb{F}_4))_{[1,0,0]}\, h_1\, (PSl_3(\mathbb{F}_4))_{[1,0,0]}\ h \\ &\subseteq (PSl_3(\mathbb{F}_4))_{[1,0,0]} \sqcup (PSl_3(\mathbb{F}_4))_{[1,0,0]}\, h_1\, (PSl_3(\mathbb{F}_4))_{[1,0,0]} \\ &= PSl_3(\mathbb{F}_4)\end{aligned}$$

sowie

$$\begin{aligned}h\ M_{22}\ h &= h\ PSl_3(\mathbb{F}_4)\ h \sqcup h\ PSl_3(\mathbb{F}_4)\ v\ PSl_3(\mathbb{F}_4)\ h \\ &\subseteq PSl_3(\mathbb{F}_4) \sqcup PSl_3(\mathbb{F}_4)\, v\, PSl_3(\mathbb{F}_4) \\ &= M_{22}\end{aligned}$$

Eine allgemeine Matrix $k \in (PSl_3(\mathbb{F}_4))_{[1,0,0]}$ hat modulo einer skalaren Matrix folgende Form:

$$k = \begin{pmatrix} 1 & * & * \\ 0 & a & b \\ 0 & c & d \end{pmatrix}$$

mit der Determinante

$$\det(k) = ad - bc = 1$$

Nun wenden wir $hkh$ auf ein beliebiges Element in $\mathbb{F}_4P^2 \cup \{ \infty , \omega \}$ an und erhalten

$$\begin{aligned} (hkh)([\lambda,\mu,\nu]) &= h \begin{pmatrix} 1 & * & * \\ 0 & a & b \\ 0 & c & d \end{pmatrix} \begin{pmatrix} \lambda^2 + *\mu^2 + *\nu^2 \\ a\mu^2 + b\nu^2 \\ c\mu^2 + d\nu^2 \end{pmatrix} \\ &= \begin{pmatrix} \lambda + *\mu + *\nu \\ a^2\mu + b^2\nu \\ c^2\mu + d^2\nu \end{pmatrix} \\ &= \underbrace{\begin{pmatrix} 1 & * & * \\ 0 & a^2 & b^2 \\ 0 & c^2 & d^2 \end{pmatrix}}_{= k' \in PSl_3(\mathbb{F}_4)} \begin{pmatrix} \lambda \\ \mu \\ \nu \end{pmatrix} \end{aligned}$$

Also ist $hkh \in M_{22}$ und wegen $h^2 = \mathbb{1}$ folgt auch

$$hM_{22}h = M_{22}$$

Nach Theorem 8.6 operiert die Mathieu-Gruppe $M_{23}$ 4-transitiv auf der Menge

$$\mathbb{F}_4P^2 \cup \{ \infty , \omega \} \simeq [23]$$

Die gefundene Erweiterung

$$M_{24} = \langle M_{23} , h \rangle = M_{23} \cup M_{23} \cdot h \cdot M_{23}$$

hat nach dem Erweiterungssatz von Witt 8.1 die Ordnung

$$|M_{23}| \cdot 24 = 244\ 823\ 040$$

und operiert 5-transitiv auf [24]. □

# 9. Einfache Gruppen

Nach Definition 1.19 ist eine Gruppe einfach, wenn sie nur triviale Normalteiler hat. Ähnlich wie die natürlichen Zahlen aus Primzahlen zusammengesetzt sind, können einfache Gruppen als Grundbausteine der endlichen Gruppen aufgefaßt werden.

**Beispiel 9.1.** Für alle Primzahlen $p$ sind die zyklischen Gruppen $C_p$ einfach. Dies sind auch die einzigen abelschen, einfachen Gruppen.

## 9.1. Einfachheit der alternierenden Gruppen

Nach Definition 1.39 bilden die Permutationen mit geradem Signum die alternierenden Gruppen als Untergruppen der symmetrischen Gruppen. Die alternierende Gruppe $A_2 \simeq \{e\}$ ist die triviale Gruppe und $A_3 \simeq C_3$ ist als zyklische Gruppen mit Primzahlordnung einfach.

**Proposition 9.2.** *Die alternierende Gruppe $A_4$ ist nicht einfach.*

*Beweis.* Wir nehmen an, $A_4$ wäre einfach, und führen dies zu einem Widerspruch. Nach dem Satz von Sylow 3.5 gibt es 4 3-Sylow-Untergruppen. Denn eine $p$-Sylow-Untergruppe ist stets ein Normalteiler. In diesen 4 3-Sylow-Untergruppen gibt es jeweils 2 Elemente der Ordnung 3, also insgesamt $8 = 2 \cdot 4$. Da $A_4$ die Ordnung $12 = \frac{24}{2} = \frac{6!}{2}$ hat, bleiben für 2-Sylow-Untergruppen nur noch 4 Elemente übrig. Das heisst, es kann nur eine 2-Sylow-Untergruppe geben und diese ist ein nicht-trivialer Normalteiler in $A_4$ im Widerspruch zur Annahme. □

**Theorem 9.3.** *Die alternierende Gruppe $A_5$ ist einfach.*

*Beweis.* Eine Gruppe $G$ wirkt auf sich durch Konjugation $g \circ x = g \cdot x \cdot g^{-1}$. Die Bahnen $G \circ x$ dieser Wirkung heissen Konjugationsklassen. Für einen Normalteiler $N \lhd G$ gilt

$$g \cdot N \cdot g^{-1} = N \quad \text{für alle } g \in G$$

Daraus folgt, dass $N$ die Vereinigung von Konjugationsklassen ist.

$$G \circ x = \{\, g \cdot x \cdot g^{-1} \mid g \in G \,\}$$

Wir bestimmen nun die Konjugationsklassen in $S_5$. Für einen beliebigen Zykel gilt

$$g \circ (1, 2, \cdots, k) \circ g^{-1} = (g(1), g(2), \cdots, g(k)) \quad \text{für alle } g \in S_5$$

Die Zykeltypen entsprechen den Konjugationsklassen. Die folgende Liste enthält die Konjugationsklassen für die unterschiedlichen Zykeltypen. In $A_5$ kommen nur die Konjugationsklassen mit geraden Elemente vor.

| Relevant in | Zykeltyp $\sigma$ | Mächtigkeit der Konjugationsklasse $(S_5 \circ \sigma)$ | Mächtigkeit der Standgruppe in $S_5$ $S_{5_\sigma}$ |
|---|---|---|---|
| $A_5$ und $S_5$ | e | 1 | 120 |
| $S_5$ | (1,2) | $\binom{5}{2} = 10$ | 12 |
| $A_5$ und $S_5$ | (1,2,3) | $2 \cdot \binom{5}{2} = 20$ | 6 |
| $S_5$ | (1,2,3,4) | $5 \cdot 3! = 30$ | 4 |
| $A_5$ und $S_5$ | (1,2,3,4,5) | $4! = 24$ | 5 |
| $A_5$ und $S_5$ | $(1,2) \circ (3,4)$ | $5 \cdot 3 = 15$ | 8 |
| $S_5$ | $(1,2,3) \circ (4,5)$ | $10 \cdot 2 = 20$ | 6 |
| Summe $S_5$ | | 120 | |
| Summe $A_5$ | | 60 | |

Allerdings müssen die gelisteten Konjugationsklassen nicht zwingend in $A_5$ wieder eine Konjugationsklasse sein, da sie dort nicht mehr mit allen Elementen in $S_5$ konjugiert werden. Für eine gerade Permutation $\sigma$ gilt nach dem Bahn-Standgruppen-Satz 1.53

$$\begin{aligned} |S_n| &= |(S_n \circ \sigma)| \cdot |S_{n_\sigma}| \\ |A_n| &= |(A_n \circ \sigma)| \cdot |A_{n_\sigma}| \end{aligned}$$

Sei $g \in S_{n_\sigma}$ eine ungerade Permutation. Dann ist $g \notin A_{n_\sigma}$ aber $g^2 \in A_{n_\sigma}$. Das heisst

$$\begin{aligned} & & S_{n_\sigma} &\neq A_{n_\sigma} \\ \Leftrightarrow & \text{ es gibt eine ungerade Permutation } g & &\in S_{n_\sigma} \\ & \Leftrightarrow & |S_{n_\sigma}| &= 2 \cdot |A_{n_\sigma}| \\ & \Leftrightarrow & |(S_n \circ \sigma)| &= |(A_n \circ \sigma)| \end{aligned}$$

In diesem Fall spaltet sich die Konjugationsklasse aus $S_5$ in $A_5$ in zwei Teile. In $A_5$ sind folgende Permutationen nicht konjugiert:

$$\begin{aligned} \sigma_1 &= (1,2,3,4,5) \\ \sigma_2 &= (1,2,3,5,4) \end{aligned}$$

Für alle $g$ mit $g \circ (1,2,3,4,5) \circ g^{-1} = (1,2,3,5,4)$ ist $g$ nämlich ungerade.

$$\begin{array}{lllll}
g(1)=1 & \Rightarrow & g(2)=2\ ,\ g(3)=3\ ,\ g(4)=5\ ,\ g(5)=4 & \Rightarrow & g=(4,5) \quad \text{ungerade} \\
g(1)=2 & \Rightarrow & g(2)=3\ ,\ g(3)=5\ ,\ g(4)=4\ ,\ g(5)=1 & \Rightarrow & g=(1,2,3,5) \quad \text{ungerade} \\
g(1)=3 & \Rightarrow & g(2)=5\ ,\ g(3)=4\ ,\ g(4)=1\ ,\ g(5)=2 & \Rightarrow & g=(1,3,4)\circ(2,5) \quad \text{ungerade} \\
g(1)=4 & \Rightarrow & g(2)=1\ ,\ g(3)=2\ ,\ g(4)=3\ ,\ g(5)=5 & \Rightarrow & g=(1,4,3,2) \quad \text{ungerade} \\
g(1)=5 & \Rightarrow & g(2)=4\ ,\ g(3)=1\ ,\ g(4)=2\ ,\ g(5)=3 & \Rightarrow & g=(1,5,3)\circ(2,4) \quad \text{ungerade}
\end{array}$$

Damit erhalten wir folgende Konjugationsklassen in $A_5$:

| Zykeltyp | Mächtigkeit der Konjugationsklasse |
|---|---|
| e | 1 |
| (1,2,3) | 20 |
| (1,2) ∘ (3,4) | 15 |
| (1,2,3,4,5) | 12 |
| (1,2,3,5,4) | 12 |

Mit der obigen Feststellung, dass ein Normalteiler $N \triangleleft A_n$ die Vereinigung von Konjugationsklassen ist, kann folgende Liste der Mächtigkeiten von Normalteilern aufgestellt werden:

$$\begin{aligned}
1 &\mid 60 \\
1+20=21 &\nmid 60 \\
1+15=16 &\nmid 60 \\
1+12=12 &\nmid 60 \\
1+20+15=36 &\nmid 60 \\
1+20+12=33 &\nmid 60 \\
1+15+12=28 &\nmid 60 \\
1+12+12=25 &\nmid 60 \\
1+20+15+12=48 &\nmid 60 \\
1+15+12+12=40 &\nmid 60 \\
1+20+15+12+12=60 &\mid 60
\end{aligned}$$

Wir finden darin nur die zwei trivialen Kombinationen $N = \{e\}$ oder $N = A_5$, in denen das neutrale Element enthalten ist und deren Mächtigkeit $|A_5| = 60$ teilt. Damit ist $A_5$ einfach. □

Es erhebt sich die Frage, ob es weitere einfache Gruppen in der Klasse der alternierenden Gruppen gibt. In der Tat sind alle alternierenden Gruppen $A_n$ für $n \geq 5$ einfach. Zunächst beweisen wir dazu das folgende Lemma:

**Lemma 9.4.** *Sei $H \triangleleft A_n$ ein Normalteiler in der alternierenden Gruppe $A_n$ mit $n \geq 5$. Wenn $H$ einen 3-Zykel enthält, dann gilt bereits $H = A_n$.*

*Beweis.* Nach Theorem 1.40 werden alternierende Gruppen $A_n$ von 3-Zykeln erzeugt. Denn

$$A_n = \{\sigma_1, \cdots, \sigma_{2n} \mid \sigma_i \; Paarvertauschung\}$$

Die Paarvertauschungen können als 3-Zykel geschrieben werden.

$$\begin{aligned} (1,2) \circ (2,3) &= (1,2,3) \\ (1,2) \circ (3,4) &= (1,2,3) \circ (2,3,4) \end{aligned}$$

Nach einer eventuellen Umnummerierung kann man annehmen, der Zykel $(1,2,3)$ sei in $H$. Wir müssen zeigen, dass ein beliebiger Zykel $(a,b,c)$ ebenfalls in $H$ ist. Dazu betrachten wir eine Permutation $\sigma \in S_n$ mit der Eigenschaft

$$\begin{aligned} \sigma(1) &= a \\ \sigma(2) &= b \\ \sigma(3) &= c \end{aligned}$$

Falls $\sigma$ ungerade ist, erhalten wir mit $d \neq f \notin \{a,b,c\}$ die gerade Permutation

$$\tilde{\sigma} = \sigma \circ (d,f)$$

Da $H$ Normalteiler in $A_n$ ist, liegt der mit $\sigma$ bzw $\tilde{\sigma}$ konjugierte, ursprüngliche Zykel auch in $H$.

$$\sigma \circ (1,2,3) \circ \sigma^{-1} = (a,b,c) \in H$$

□

**Theorem 9.5.** *Die alternierenden Gruppen $A_n$ sind für $n \geq 5$ einfach.*

*Beweis.* Der Beweis erfolgt durch Induktion.

Für $n = 5$ wurde die Einfachheit von $A_5$ in Satz 9.3 bereits bewiesen.

Wir nehmen an, $H$ sei Normalteiler in $A_n$ und $e \neq g \in H$ ein Element in $H$. Die Permutation $g$ kann einen Fixpunkt haben oder fixpunktfrei sein.

1. $g$ hat einen Fixpunkt
   Nach einer eventuellen Umnummerierung können wir $g(n) = n$ annehmen. Dann ist
   $$g \in H \cap A_{n-1} \lhd A_{n-1}$$
   $H \neq \{e\}$ und nach Induktionsvoraussetzung ist $A_{n-1}$ einfach. Also ist $H = A_{n-1}$ und enthält einen 3-Zykel. Somit gilt nach Lemma 9.4 $H = A_n$.

2. $g$ ist fixpunktfrei
   Wir betrachten die Menge $X = \{1, g(1), g^2(1), g^{-1}(1)\}$ und wählen $a \notin X$. Wir setzen
   $$h = (1, g(1), a) \in A_n$$
   Da $g$ keinen Fixpunkt hat, ist dies ein 3-Zykel und es gilt.
   $$g \circ h \circ g^{-1} = (g(1), g^2(1), g(a))$$
   Wir setzen $\sigma = g \circ h \circ g^{-1} \circ h^{-1}$. $\sigma$ liegt in $H$, da $H$ Normalteiler ist.
   $$\sigma = \begin{cases} (1, a, g^2(1), g(a), g(1)) & \text{wenn} \quad g^2(1) \neq 1 \\ (1, a) \circ (g(a), g(1)) & \text{wenn} \quad g^2(1) = 1 \end{cases}$$
   $\sigma$ ist also entweder ein 5-Zykel oder das Produkt von zwei 2-Zykeln und läßt die übrigen Elemente fest. Da $n > 5$, hat $\sigma$ also mindestens einen Fixpunkt und wir können Fall 1 anwenden.

□

Die alternierende Gruppe $A_5$ mit der Ordnung 60 ist die erste einfache Gruppe in dieser Klasse. Wir untersuchen nun die Frage, ob diese auch die einzige einfache Gruppe mit Ordnung 60 ist. Zur Vorbereitung benötigen wir folgendes Lemma.

**Lemma 9.6.** *Wenn die Operation einer einfachen Gruppe $G$ mit mehr als 3 Elementen auf eine Menge mit $m$ Elementen nicht trivial ist, dann gibt es einen injektiven Homomorphismus in die alternierende Gruppe $A_m$ und die Ordnung der Gruppe teilt $\frac{m!}{2}$.*

**Theorem 9.7.** *Die alternierende Gruppe $A_5$ ist mit 60 Elementen die kleinste, nichtabelsche, einfache Gruppe und bis auf Isomorphie die einzige einfache Gruppe der Ordnung 60.*

*Beweis.* Eine einfache Gruppe $G$ der Ordnung 60 wirkt nach dem Satz von Sylow 3.5 durch Konjugation auf die Menge der 2-Sylowuntergruppen $Syl_(G)$. Nach dem Satz von Sylow ist die Anzahl $n_2$ der 2-Sylowuntergruppen entweder 1 , 3 , 5 oder 15.

$n_2 = 1$ Dieser Fall kann ausgeschlossen werden, da $G$ als einfach vorausgesetzt ist.

$n_2 = 3$ In diesem Fall erhalten wir nach Lemma 9.6 eine Einbettung von $G \hookrightarrow A_3$. Dies ist jedoch nicht möglich, da $G$ 60 Elemente hat und $A_3$ nur 3.

$n_2 = 5$ In diesem Fall erhalten wir nach Lemma 9.6 eine Einbettung von $G \hookrightarrow A_5$. Da $G$ und $A_5$ dieselbe Ordnung haben, sind sie isomorph.

$n_2 = 15$ In diesem Fall beweist man zunächst die Behauptung, dass es zwei 2-Sylowuntergruppen $P \neq Q$ gibt, deren Schnitt nicht trivial ist: $D = P \cap Q \neq \{1\}$. Nun betrachtet man den Normalisator $N_G(D)$, zeigt, dass dieser nur die Ordnung 12 haben kann, und wendet Lemma 9.6 auf die Gruppe $G$ und die Menge $X = G/N_G(D)$ an. Da $X$ 5 Elemente besitzt, erhält man wie oben die Isomorphie $G \cong A_5$.

□

## 9.2. Die Einfachheit der projektiven, speziellen, linearen Gruppen

Die Beweisführung folgt der Vorlesung [dJ21] über Gruppentheorie von Theodorus de Jong an der JGU Mainz im Wintersemester 2021/22. Dazu sind zunächst einige Vorbereitungen notwendig.

### 9.2.1. Das Lemma von Iwasawa

**Definition 9.8.** Sei $G$ eine Gruppe und $a, b \in G$. Dann heisst

$$[a,b] = a \cdot b \cdot a^{-1} \cdot b^{-1}$$

Kommutator von $a, b$.
Alle Kommutatoren erzeugen die Kommutatorgruppe $G' < G$.

$$G' = [G,G] = \langle [a,b] \mid a, b \in G \rangle$$

**Lemma 9.9.** *Die Kommutatorgruppe $G'$ von $G$ ist Normalteiler in $G$.*

*Beweis.* Für $a, b, g \in G$ gilt

$$\begin{aligned} g \cdot [a,b] \cdot g^{-1} &= g \cdot a \cdot b \cdot a^{-1} \cdot b^{-1} \cdot g^{-1} \\ &= g \cdot a \cdot g^{-1} \cdot g \cdot b \cdot g^{-1} \cdot g \cdot a^{-1} \cdot g^{-1} \cdot g \cdot b^{-1} \cdot g^{-1} \\ &= [g \cdot a \cdot g^{-1}, g \cdot b \cdot g^{-1}] \\ &\in G' \end{aligned}$$

□

**Lemma 9.10.** *$G/G'$ ist abelsch.*

*Beweis.* Für $a, b \in G$ gilt

$$\begin{aligned} a \cdot b &= a \cdot b \cdot a^{-1} \cdot b^{-1} \cdot b \cdot a \\ &= [a, b] \cdot b \cdot a \end{aligned}$$

Daraus folgt

$$\begin{aligned} aG' \cdot bG' &= a \cdot bG' \\ &= [a, b] \cdot b \cdot aG' \\ &= b \cdot aG' \\ &= bG' \cdot aG' \end{aligned}$$

□

**Lemma 9.11.** *Lemma von Iwasawa*
*Sei $X$ eine Menge und $G$ eine Gruppe mit folgenden Eigenschaften:*

*I1 Die Kommutatorgruppe $G'$ von $G$ stimmt mit $G$ überein.*

$$G' = G$$

*I2 $G$ wirkt auf $X$ primitiv und treu.*

*I3 In jeder Standgruppe existiert ein abelscher Normalteiler.*

$$\text{für alle } x \in X \quad \text{existiert } A \triangleleft G_x \text{ abelsch}$$

*I4 $G$ wird von den Konjugierten von $A$ erzeugt.*

*Dann ist $G$ einfach.*

*Beweis.* Sei $N$ ein Normalteiler in $G$ und $x \in X$. Die Standgruppe von $x$ sei $H$.

$$H = \{ g \in G \mid g \circ x = x \}$$

Wir unterscheiden nun 2 Fälle:

$\underline{N < H}$ Da $G$ primitiv also insbesondere transitiv auf $X$ wirkt, gibt es für alle $y \in X$ ein $g \in G$ mit $g \circ x = y$. Weiter gilt

$$\begin{aligned} N < H &\Rightarrow g \cdot N \cdot g^{-1} < g \cdot H \cdot g^{-1} \\ &\Rightarrow N < g \cdot H \cdot g^{-1} \quad \text{da } N \lhd G \end{aligned}$$

Daraus folgt: für alle $h \in N$ existiert ein $\tilde{h} \in H$, so dass $h = g \cdot \tilde{h} \cdot g^{-1}$. Für alle $y \in X$ gilt dann

$$\begin{aligned} h \circ y &= (g \cdot \tilde{h} \cdot g^{-1}) \circ y \\ &= (g \cdot \tilde{h}) \circ x \\ &= g \circ x \quad \text{da } \tilde{h} \in H = G_x \\ &= y \end{aligned}$$

Das heisst $N$ wirkt trivial auf $X$. Da $G$ treu auf $X$ wirkt, muss $N = \{e\}$ gelten.

$\underline{N \not< H}$ Da $N$ Normalteiler in $G$ ist, folgt

$$G_x = H \subsetneqq H \cdot N < G$$

Da $G$ primitiv auf $X$ wirkt und $G_x \neq H \cdot N$ ist, muss $G$ mit $H \cdot N$ übereinstimmen. Jedes Element $k \in G$ kann also als Produkt geschrieben werden.

$$k = h \cdot n \quad \text{mit } h \in H \text{ und } n \in N$$

Nach Voraussetzung I3 existiert ein abelscher Normalteiler $A \lhd G_x$ und nach Voraussetzung I4 wird $G$ von den Konjugierten $g \cdot A \cdot g^{-1}$ erzeugt. Also hat jedes Element $g \in G$ eine Darstellung als Produkt von $k^{-1} \cdot a \cdot k$ mit $a \in A$ und $k \in G$. Es gilt somit

$$\begin{aligned} g &= k^{-1} \cdot a \cdot k \\ &= n^{-1} \cdot h^{-1} \cdot a \cdot h \cdot n \\ &= n^{-1} \cdot b \cdot n \quad \text{da } A \lhd G_x = H \Rightarrow h^{-1} \cdot a \cdot h = b \in A \\ &= b \cdot \underbrace{(b^{-1} \cdot n^{-1} \cdot b \cdot n)}_{\in N} \\ &\in A \cdot N \\ \Rightarrow \quad G &= A \cdot N \end{aligned}$$

Mit dem Homomorphiesatz erhalten wir

$$G/N = A \cdot N/N \simeq A/A \cap N \quad \text{abelsch}$$

Nach Voraussetzung I1 ($G = G' = [G, G]$) hat $G$ keine nicht-trivialen, abelschen Quotienten. Daher ist $N = G' = G$.

In beiden Fällen ist $N$ kein echter Normalteiler in $G$. Also ist $G$ einfach. □

Wir zeigen jetzt, dass die Voraussetzungen im Lemma von Iwasawa für die projektiven speziellen linearen Gruppen $PSL(n, \mathbb{F})$ mit Ausnahme von $PSL(2, \mathbb{F}_2)$ und $PSL(2, \mathbb{F}_3)$ erfüllt sind. Dazu betrachten wir zunächst die Erzeugenden der speziellen, linearen Gruppe.

### 9.2.2. Erzeugende der speziellen, linearen Gruppe

**Definition 9.12.** Sei $\mathbb{F}$ ein Körper, $\lambda \in \mathbb{F}$, $n \in \mathbb{N}$. Dann heisst folgende Matrix

$$Q_{ij}(\lambda) = \mathbb{1} + \lambda \cdot E_{ij} \quad i \neq j \in \{1, \cdots, n\}$$

Elementarmatrix. Dabei ist $\mathbb{1}$ die Einheitsmatrix und $E_{ij}$ ist eine Matrix, die nur in der $i$-ten Zeile und $j$-ten Spalte eine 1 und sonst nur 0 Einträge hat.

**Lemma 9.13.** *Die Elementarmatrizen haben folgende Eigenschaften:*

*(i)*
$$det(Q_{ij}(\lambda)) = 1$$

*(ii)*
$$Q_{ij}(\lambda)^{-1} = Q_{ij}(-\lambda)$$

**Bemerkung 9.14.** Seien $Q_{ij}(\lambda) \in \mathbb{F}^{n \times n}$ und $A \in \mathbb{F}^{n \times n}$. Dann entspricht dem Produkt $Q_{ij}(\lambda) \cdot A$ eine Zeilenoperation auf $A$. Das $\lambda$-fache der $j$-ten Zeile wird zur $i$-ten Zeile addiert.

**Lemma 9.15.** *Die Elementarmatrizen $Q_{ij}(\lambda)$ erzeugen die spezielle lineare Gruppe $SL(n, \mathbb{F})$.*

*Beweis.* Durch Zeilenoperationen kann jede Matrix $A \in SL(n, \mathbb{F})$ in Diagonalgestalt gebracht werden. Es gibt also eine endliche Folge $\{Q_1, \cdots, Q_k\}$ von Matrizen $Q_{ij}(\lambda)$, so

dass gilt

$$Q_1 \cdot \dots \cdot Q_k \cdot A = \begin{pmatrix} a_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n \end{pmatrix} \in \mathbb{F}^{3\times 3}$$

Da bei diesen Zeilenoperationen die Determinante erhalten bleibt, gilt

$$1 = det(A) = det(Q_1 \cdot \dots \cdot Q_k \cdot A) = \prod_{i=1}^{n} a_i$$

Durch weitere Zeilenoperationen kann erreicht werden, dass alle $a_i = 1$ sind. Dann ist $A$ das Produkt von Matrizen der Gestalt $Q_{ij}(\lambda)$. Wir zeigen dies für $n = 2$ und der Matrix

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

Wir berechnen

$$\begin{aligned}
& Q_{12}(-\frac{1}{a}) \cdot Q_{21}(a-1) \cdot Q_{12}(1) \cdot Q_{21}(\frac{1-a}{a}) \cdot \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \\
= & \begin{pmatrix} 1 & -\frac{1}{a} \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ a-1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ \frac{1-a}{a} & 1 \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \\
= & \begin{pmatrix} 1 & -\frac{1}{a} \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ a-1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ 1-a & b \end{pmatrix} \\
= & \begin{pmatrix} 1 & -\frac{1}{a} \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ a-1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1-a \\ b & b \end{pmatrix} \\
= & \begin{pmatrix} 1 & -\frac{1}{a} \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ b & ab \end{pmatrix} \\
= & \begin{pmatrix} 1 & 0 \\ 0 & ab \end{pmatrix}
\end{aligned}$$

Analog kann eine Diagonalmatrix

$$\begin{pmatrix} a_1 & 0 & 0 & \cdots & 0 \\ 0 & a_2 & 0 & \cdots & 0 \\ 0 & 0 & a_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_n \end{pmatrix}$$

überführt werden in

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & a_1 \cdot a_2 & 0 & \cdots & 0 \\ 0 & 0 & a_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_n \end{pmatrix}$$

Schliesslich erhält man

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_1 \cdot \cdots \cdot a_n \end{pmatrix}$$

mit $a_1 \cdot \cdots \cdot a_n = 1$. □

**Proposition 9.16.** *Die speziellen, linearen Gruppen $G = SL(n, \mathbb{F})$ stimmen mit Ausnahme von $SL(2, \mathbb{F}_2)$ und $SL(2, \mathbb{F}_3)$ mit ihrer Kommutatorgruppe überein.*

$$G = G' = [G, G]$$

*Beweis.* Nach Lemma 9.15 wird $G$ von Elementarmatrizen $Q_{ij}(\lambda)$ erzeugt. Daher genügt es zu zeigen, dass jede Elementarmatrix als Kommutator dargestellt werden kann. Dabei müssen die Fälle $n = 2$ und $n \geq 3$ unterschieden werden.

$\underline{n = 2}$ Wir berechnen den Kommutator der Matrizen

$$A = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$$
$$B = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

und erhalten

$$\begin{aligned} A \cdot B \cdot A^{-1} \cdot B^{-1} &= \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} a & a \cdot b \\ 0 & a^{-1} \end{pmatrix} \cdot \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a^2 \cdot b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & b \cdot (a^2 - 1) \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Eine allgemeine Elementarmatrix $Q_{12}(\lambda)$ ist also genau dann ein Kommutator, wenn es Elemente $a, b \in \mathbb{F}$ gibt, so dass gilt:

$$\lambda = b \cdot (a^2 - 1)$$

Das muss auch für $\lambda \neq 0$ gelten. Das heisst, $a$ darf keinen der Werte $0, +1, -1$ annehmen. Daraus folgt wiederum, $\mathbb{F}$ muss mindestens 4 Elemente haben.
Analog findet man für $Q_{21}(\lambda)$ zwei Matrizen, deren Kommutator $Q_{21}(\lambda)$ ergibt.

$\underline{n \geq 3}$ Wir zeigen exemplarisch, dass die Elementarmatrix

$$Q_{13}(\lambda) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \lambda & 0 & 1 \end{pmatrix}$$

Kommutator von zwei Matrizen ist. Diese sind

$$\begin{aligned} A &= \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ B &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -\lambda & 1 \end{pmatrix} \end{aligned}$$

Damit berechnet man

$$\begin{aligned}
A \cdot B \cdot A^{-1} \cdot B^{-1} &= \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -\lambda & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \lambda & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & -\lambda & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \lambda & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \lambda & -\lambda & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \lambda & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \lambda & 0 & 1 \end{pmatrix} \\
&= Q_{13}(\lambda)
\end{aligned}$$

□

**Proposition 9.17.** *Sei $G = PSl_n(\mathbb{F}_q)$ eine projektive, spezielle, lineare Gruppe und $\mathbb{F}_q P^{n-1}$ der $(n-1)$-dimensionale, projektive Raum über $\mathbb{F}_q$. Sei $p \in \mathbb{F}_q P^{n-1}$ ein projektiver Punkt in $\mathbb{F}_q P^{n-1}$ und $G_p$ die Standgruppe. Für $w \in \mathbb{F}_q^{n-1}$ seien Matrizen $M_w$ definiert durch*

$$M_w = \left(\begin{array}{c|ccc} 1 & - & w & - \\ \hline 0 & & & \\ \vdots & & \mathbb{1} & \\ 0 & & & \end{array}\right)$$

*Dann ist*

$$A = \{\, M_w \,|\, w \in \mathbb{F}_q^{n-1} \,\} \lhd G_p$$

*ein abelscher Normalerteiler in $G_p$.*

*Beweis.* Ohne Einschränkung der Allgemeinheit können wir eine Basis $(e_1, \cdots, e_n)$ in $\mathbb{F}_q^n$

so wählen, dass $p = \mathbb{F}_q \cdot e_1$ ist. Mit $y \in \mathbb{F}_q^n$ gilt

$$\begin{aligned} M_w(e_1) &= e_1 \\ M_w(y) &= \begin{pmatrix} 1 & w_2 & \cdots & w_n \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \\ &= \begin{pmatrix} y_1 + w_2 \cdot y_2 + \cdots + w_n \cdot y_n \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \\ &= w \cdot y \cdot e_1 + y \end{aligned}$$

Für $M_v$ und $M_w$ in $A$ gilt

$$\begin{aligned} (M_w \cdot M_v)(y) &= M_w((v \cdot y) \cdot e_1 + y) \\ &= (v \cdot y) \cdot e_1 + (w \cdot y) \cdot e_1 + y \\ &= ((v + w) \cdot y) \cdot e_1 + y \\ &= M_{v+w}(y) \end{aligned}$$

Daraus folgt, dass $A \simeq \mathbb{F}^{n-1}$ abelsch ist.

Wir zeigen nun, dass $A$ Normalteiler in $G_p$ ist. Sei $g \in G_p$ beliebig. Dann gilt $gp = p = \mathbb{F} \cdot e_1$ und $g$ kann durch eine Matrix der Gestalt

$$\tilde{M}_g = \left(\begin{array}{c|ccc} c & - & v & - \\ \hline 0 & & & \\ \vdots & & B & \\ 0 & & & \end{array}\right)$$

beschrieben werden, wobei $c \neq 0$, $det(B) = \frac{1}{c}$ und $v \in \mathbb{F}^{n-1}$ ist. Das Inverse von $g$ ist dann gegeben durch die Matrix:

$$\tilde{M}_g^{-1} = \left(\begin{array}{c|ccc} c^{-1} & - & -c^{-1} \cdot v \cdot B^{-1} & - \\ \hline 0 & & & \\ \vdots & & B^{-1} & \\ 0 & & & \end{array}\right)$$

Wir berechnen zunächst exemplarisch die Wirkung des Konjugiums $g \cdot M_w \cdot g^{-1}$ von $M_w \in A$ auf $e_1$:

$$\begin{aligned} g(e_1) &= c \cdot e_1 \quad \text{für ein } c \in \mathbb{F}^* \\ g^{-1}(e_1) &= \frac{1}{c} \cdot e_1 \\ g \cdot M_w \cdot g^{-1}(e_1) &= g \cdot M_w(\frac{1}{c} \cdot e_1) \\ &= g(\frac{1}{c} \cdot e_1) \\ &= e_1 \end{aligned}$$

Allgemeiner berechnen wir

$$\begin{aligned} \tilde{M}_g \cdot M_w \cdot \tilde{M}_g^{-1} &= \begin{pmatrix} c & v \\ 0 & B \end{pmatrix} \cdot \begin{pmatrix} 1 & w \\ 0 & \mathbb{1} \end{pmatrix} \cdot \begin{pmatrix} c^{-1} & -c^{-1} \cdot v \cdot B^{-1} \\ 0 & B^{-1} \end{pmatrix} \\ &= \begin{pmatrix} c & c \cdot w + v \\ 0 & B \end{pmatrix} \cdot \begin{pmatrix} c^{-1} & -c^{-1} \cdot v \cdot B^{-1} \\ 0 & B^{-1} \end{pmatrix} \\ &= \begin{pmatrix} 1 & c \cdot w \cdot B^{-1} \\ 0 & \mathbb{1} \end{pmatrix} \\ &= M_{c \cdot w \cdot B^{-1}} \\ &\in A \end{aligned}$$

Damit ist gezeigt, dass $A$ Normalteiler in $G_x$ ist. □

**Proposition 9.18.** *Sei $G = PSl_n(\mathbb{F})$ eine projektive, spezielle, lineare Gruppe und*

$$A = \{ M_w \mid w \in \mathbb{F}^{n-1} \}$$

*mit*

$$M_w = \left(\begin{array}{c|ccc} 1 & - & w & - \\ \hline 0 & & & \\ \vdots & & Id & \\ 0 & & & \end{array}\right)$$

*wie in Proposition 9.17. Dann wird $G$ von Konjugierten aus $A$ erzeugt.*

*Beweis.* Da $G$ von Elementarmatrizen $Q_{ij}(\lambda)$ erzeugt wird, genügt es zu zeigen, dass $Q_{ij}(\lambda)$ zu einer Matrix $M_w \in A$ konjugiert ist. Durch eine einfache Vertauschung der

Basisvektoren $e_k \in \mathbb{F}^n$

$$(e_j, e_2, \cdots, e_{j-1}, e_1, e_{j+1}, \cdots, e_n)$$

erhält $Q_{ij}(\lambda)$ die Form

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & \lambda & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

Somit ist $Q_{ij}(\lambda)$ zu einer Matrix $M_w \in A$ konjugiert. □

Damit sind alle Voraussetzungen im Lemma von Iwasawa 9.11 erfüllt und wir erhalten die Einfachheit der projektiven, speziellen, linearen Gruppen als Folgerung.

**Korollar 9.19.** *Mit Ausnahme der in den Beispielen 7.14 und 7.15 genannten Gruppen $PSl_2(2)$ und $PSl_2(3)$ sind alle projektiven, speziellen, linearen Gruppen $PSl_n(q)$ über endlichen Körpern einfach.*

Die obigen 3 Beispiele bilden 3 von 18 unendlichen Familien einfacher Gruppen. Daneben gibt es 26 sogenannte sporadische, einfache Gruppen, die einzeln auftreten. Die Mathieu-Gruppen $M_{11}, M_{12}, M_{22}, M_{23}$ und $M_{24}$ sind die ersten sporadischen, einfachen Gruppen. Diese wurden bereits 1861 und 1873 von Mathieu entdeckt. Die Konstruktion haben wir in Abschnitt 8 behandelt.

## 9.3. Die Einfachheit der Mathieu-Gruppen

Nach Bemerkung 7.39 ist die Mathieu-Gruppe $M_{10} \cong M(9)$ nicht einfach, da sie die Gruppe $S$ der gebrochen linearen Funktionen als Normalteiler enthält. Die daraus konstruierte Mathieu-Gruppe $M_{11}$ ist hingegen einfach. Zum Beweis wird nur die 2-Transitivität benutzt und, dass $M_{11} < S_{11}$ eine Untergruppe der symmetrischen Gruppe $S_{11}$ ist. Zur Vorbereitung sind folgende drei Lemmata nützlich.

**Lemma 9.20.** *Frattini Argument*
*Sei $H \triangleleft G$ Normalteiler in $G$ und $H \neq G$ und $P \in Syl_p(H)$. Dann ist die Gruppe $G$ das Produkt aus $H$ und dem Normalisator von $P$ in $G$:*

$$G = H \cdot N_G(P)$$

*Beweis.* Sei $g \in G$ beliebig und $P < H$. Dann gilt

$$g \cdot P \cdot g^{-1} < g \cdot H \cdot g^{-1} = H \quad \text{da } H \triangleleft G$$

Nach dem Satz von Sylow 3.5 sind je zwei Sylowuntergruppen von $H$ konjugiert. Also gibt es $h \in H$, so dass gilt

$$h \cdot (g \cdot P \cdot g^{-1}) \cdot h^{-1} = P$$

Daraus folgt $h \cdot g \in N_G(P)$ und

$$g \in h^{-1} \cdot N_G(P) \subseteq H \cdot N_G(P)$$

□

**Lemma 9.21.** *Sei $G$ eine Gruppe und $p \in \mathbb{N}$ eine Primzahl, die die Gruppenordnung teilt: $p$ teilt $|G|$, $H$ ein Normalteiler in $G$: $H \lhd G$ und $P$ eine $p$-Sylowuntergruppe in $G$: $P \in Syl_p(G)$, so dass $G$ das semidirekte Produkt aus $H$ und $P$ ist.*

$$G = H \rtimes P$$

*Sei weiter $\varphi : G \longrightarrow G$ ein Automorphismus. Dann gilt $\varphi(H) = H$.*

*Beweis.* Sei $|P| = p^n$, $h \in H$ und $a \in P$. Dann berechnen wir

$$\begin{aligned}
(h \cdot a)^2 &= h \cdot a \cdot h \cdot a \\
&= h(\underbrace{\cdot a \cdot h \cdot a^{-1}}_{\in H}) \cdot a^2 \\
&= \tilde{h} \cdot a^2 \quad \text{mit } \tilde{h} \in H \\
&\quad \text{und weiter mit Induktion} \\
(h \cdot a)^k &= \tilde{h} \cdot a^k \quad \text{mit } \tilde{h} \in H
\end{aligned}$$

Sei $g \in H$ beliebig. Dann gibt es $h \in H$ und $a \in P$, so dass gilt:

$$\begin{aligned}
\varphi(g) &= h \cdot a \\
\varphi(g^{p^n}) &= \tilde{h} \cdot a^{p^n} \\
&= \tilde{h} \in H \quad \text{da } a^{p^n} = e \in P
\end{aligned}$$

Die Ordnung $k = o(g)$ ist teilerfremd zu $p^n$. Also gibt es nach dem erweiterten Euklidischen Algorithmus Bezout-Koeffizienten $x, y \in \mathbb{Z}$, so dass

$$x \cdot k + y \cdot p^n = 1$$

Damit errechnet man

$$\begin{aligned}\varphi(g) &= \varphi(g^{x\cdot k+y\cdot p^n}) \\ &= \varphi(\underbrace{g^{x\cdot k}}_{=e}) \cdot \varphi(g^{y\cdot p^n}) \\ &= (\varphi(g^{p^n}))^y \\ &= \tilde{h}^y \in H\end{aligned}$$

□

**Lemma 9.22.** *Die Gruppe $G$ wirke 2-transitiv und treu auf $X$. Sei $\{e\} \neq H \lhd G$ Normalteiler in $G$. Dann wirkt $H$ transitiv auf $X$.*

*Beweis.* Da $G$ treu auf $X$ wirkt, gibt es zu jedem $h \in H$ ein $x \in X$ mit $h \circ x = a \neq x$. Da $G$ 2-transitiv auf $X$ wirkt, gibt es zu jedem $b \in X$ ein $g \in G$, so dass

$$\begin{aligned}g \circ x &= x \\ g \circ a &= b\end{aligned}$$

Das heisst, es gilt sogar $g \in G_x$. Da $H \lhd G$ Normalteiler in $G$ ist, gilt $g \cdot h \cdot g^{-1} \in H$. Damit rechnet man:

$$\begin{aligned}(g \cdot h \cdot g^{-1}) \circ x &= (g \cdot h) \circ (g^{-1} \circ x) \\ &= (g \cdot h) \circ x \\ &= g \circ a \\ &= b\end{aligned}$$

Somit ist $H \circ x = X$. Also gibt es nur eine Bahn. Daraus folgt die Transitivität von $H$. □

**Satz 9.23.** *Die Mathieu Gruppe $M_{11}$ ist einfach.*

*Beweis.* Annahme: $M_{11}$ sei nicht einfach. Dann existiert ein nicht trivialer Normalteiler $H \lhd M_{11}$. Die Gruppe $M_{11}$ wirkt auf $\{1, \cdots, 11\}$ 2-transitiv und treu. Nach obigem Lemma 9.22 wirkt $H$ auf $\{1, \cdots, 11\}$ transitiv. Nach dem Bahn-Standgruppen-Satz 1.53 gilt

$$|H| = |Standgruppe| \cdot 11$$

Denn die Bahn umfasst wegen der Transitivität alle 11 Elemente. Es existiert also eine 11-Sylowuntergruppe $P \in Syl_{11}(H)$. Diese ist gleichzeitig eine 11-Sylowuntergruppe in

$M_{11}$. Diese ist zyklisch, da $11^2$ kein Teiler der Gruppenordnung $|M_{11}|$ und damit auch nicht von $|H|$ ist.

$$P \simeq C_{11}$$

Nach dem Satz von Sylow 3.5 gehen alle anderen 11-Sylowuntergruppen von $M_{11}$ durch Konjugation aus $P$ hervor. Da $H$ Normalteiler ist, gilt für alle $g \in M_{11}$:

$$g \cdot P \cdot g^{-1} < g \cdot H \cdot g^{-1} = H$$

Das heisst, dass alle 11-Sylowuntergruppen von $M_{11}$ sogar in $H$ liegen, und es folgt:

$$n_{11}(H) = n_{11}(M_{11})$$

Da $P$ als zyklische Gruppe abelsch ist, liegt $P$ im Zentralisator von $P$ in $M_{11}$.

$$P < C_{M_{11}}(P)$$

Tatsächlich gilt sogar Gleichheit. Denn sei ohne Beschränkung der Allgemeinheit $P$ erzeugt von $\sigma = (1, 2, \cdots, 11)$. Dann gilt für $g \in S_{11}$:

$$\begin{aligned} & g \cdot \sigma \cdot g^{-1} && \stackrel{!}{=} && \sigma \\ \Leftrightarrow \quad & (g(1), \cdots, g(11)) && \stackrel{!}{=} && (1, 2, \cdots, 11) \\ \Leftrightarrow \quad & g(1) = k && \stackrel{!}{\in} && \{1, 2, \cdots, 11\} \\ \Leftrightarrow \quad & g && = && \sigma^k \in P \end{aligned}$$

Nach Satz 1.60 gibt es einen injektiven Homomorphismus

$$N_{M_{11}}(P)/C_{M_{11}}(P) \longrightarrow Aut(P) = C_{10}$$

Daraus folgt für die Ordnung des Normalisators $N_{M_{11}}(P)$:

$$\begin{aligned} & |N_{M_{11}}(P)| && \text{teilt} && |P| \cdot |C_{10}| = 11 \cdot 10 = 110 \\ \Rightarrow \quad & |N_{M_{11}}(P)| && \in && \{11, 22, 55, 110\} \end{aligned}$$

Daraus ergibt sich nach Lemma 3.6 nun für die Anzahl der 11-Sylowuntergruppen in $M_{11}$:

$$n_{11}(M_{11}) = \frac{|M_{11}|}{|N_{M_{11}}(P)|} = \frac{8 \cdot 9 \cdot 10 \cdot 11}{|N_{M_{11}}(P)|} \in \{720, 360, 144, 72\}$$

Nach dem Satz von Sylow 3.5 gilt ausserdem $n_{11}(M_{11}) = 1 \mod 11$. Somit erhalten wir

$$\begin{aligned} n_{11}(M_{11}) &= 144 \\ |N_{M_{11}}(P)| &= 55 \end{aligned}$$

Wir betrachten nun Zentralisator und Normalisator von $P$ in $H$ und erhalten:

$$P < C_H(P) < N_H(P) < N_{M_{11}}(P)$$

Für die Ordnungen ergibt sich:

$$11 = |P| \leq |C_H(P)| \leq |N_H(P)| = \frac{|H|}{n_{11}(H)} < \frac{|M_{11}|}{n_{11}(M_{11})} = |N_{M_{11}}(P)| = 55$$

Denn $n_{11}(H) = n_{11}(M_{11})$. Daraus folgt $P = C_H(P) = N_H(P)$ und wir können den Verlagerungssatz von Burnside 3.15 auf $H$ anwenden. Es gibt also einen Normalteiler $K \lhd H$ mit $H \simeq K \rtimes P$. Der Normalteiler $K$ ist nicht trivial $K \neq \{e\}$. Sonst wäre $H = P \lhd M_{11}$ Normalteiler in $M_{11}$ und $P$ die einzige 11-Sylowuntergruppe in $G$. Wir folgern nun, dass auch $K$ ein Normalteiler in $M_{11}$ sein muss. Dazu betrachten wir für ein beliebiges $g \in M_{11}$ den Automorphismus

$$\begin{aligned} \varphi : H &\longrightarrow H \\ a &\longmapsto g \cdot a \cdot g^{-1} \end{aligned}$$

Dieser existiert, da $H$ Normalteiler in $M_{11}$ ist. Nach Lemma 9.21 angewendet auf $H = K \rtimes P$ gilt dann $\varphi(K) = K$. Ausgeschrieben heisst das:

$$g \cdot a \cdot g^{-1} \in K \quad \text{für alle } g \in M_{11} \quad \text{für alle } a \in K$$

Also ist $K$ ein Normalteiler in $M_{11}$. Wie am Anfang des Beweises gilt nun auch für $K$ $11 \mid |K|$. Da $H$ das semi-direkte Produkt aus $K$ und $P$ ist, muss $11^2$ die Ordnung von $H$ teilen. Die Ordnung von $M_{11}$ besitzt aber nur einen Primfaktor 11. Damit führt die Annahme, dass $H$ ein nicht-trivialer Normalteiler von $G$ ist, zu einem Widerspruch. □

Zum Nachweis der Einfachheit der anderen Mathieu-Gruppen beweisen wir einen allgemeineren Satz.

**Lemma 9.24.** *Sei $\{e\} \neq H \lhd G$ ein Normalteiler in $G$, so dass alle Elemente von $H \setminus \{e\}$ in $G$ konjugiert zueinander sind. Dann ist $H$ isomorph zu einem Produkt zyklischer*

*Gruppen der Ordnung p.*

$$H \simeq C_p^n \quad p \in \mathbb{N} \text{ Primzahl }, n \in \mathbb{N}$$

*Beweis.* Seien $h, \tilde{h} \in H$ und nicht das neutrale Element. Da nach Voraussetzung alle Elemente in $H$ konjugiert sind, gibt es ein $g \in G$, so dass

$$g \cdot h \cdot g^{-1} = \tilde{h}$$

Daraus folgt, dass alle Elemente in $H$ dieselbe Ordnung haben. Sei $k = |H|$ die Ordnung von $H$ und $p$ ein Primteiler in $k$. Für ein beliebiges $e \neq h \in H$ gilt:

$$o(h^{\frac{k}{p}}) = p$$

Also haben alle Elemente in $H$ die Ordnung $p$ und $H$ hat die Ordnung $|H| = p^n$. Nach Satz 1.61 ist das Zentrum von $H$ nicht trivial. Sei $e \neq a \in Z(H)$. Dann gilt

$$g \cdot a = a \cdot g \quad \text{für alle } g \in H$$

Wir zeigen nun, dass $g$ mit jedem weiteren Element $h \in H$ kommutiert. Nach Voraussetzung sind $a$ und $h$ in $G$ konjugiert. Es gibt also ein Element $x \in G$, so dass gilt:

$$\begin{aligned}
h &= x \cdot a \cdot x^{-1} \\
g \cdot h &= g \cdot x \cdot a \cdot x^{-1} \\
&= x \cdot (\underbrace{x^{-1} \cdot g \cdot x}_{\in H \text{ da } H \triangleleft G}) \cdot a \cdot x^{-1} \\
&= \underbrace{x \cdot a \cdot x^{-1}}_{=h} \cdot g \cdot x \cdot x^{-1} \quad \text{da } a \in Z(H) \\
&= h \cdot g
\end{aligned}$$

Also ist $H$ abelsch. Aus dem Satz über die Klassifizierung abelscher Gruppen folgt nun die Behauptung. □

**Satz 9.25.** *Die Gruppe $G$ wirke 2-transitiv und treu auf $X$ und die Anzahl der Elemente in $X$ sei keine Primzahlpotenz. Wenn für ein $a \in X$ die Standgruppe $G_a$ einfach ist, dann ist auch $G$ einfach.*

*Beweis.* Sei $H \triangleleft G$ ein Normalteiler in $G$.
Behauptung: Es gibt ein $b \in X$ , mit $H_b \neq \{e\}$.

Annahme: Für alle $b \in X$ gilt $H_b = \{e\}$. Dann betrachten wir folgende Abbildung:

$$\begin{aligned} \varphi : H \setminus \{e\} &\longrightarrow X \setminus \{b\} \\ h &\longmapsto h \circ b \end{aligned}$$

Die Abbildung $\varphi$ ist injektiv. Denn für $h_1, h_2 \in H$ rechnen wir

$$\begin{aligned} & \varphi(h_1) = \varphi(h_2) \\ \Leftrightarrow \quad & h_1 \circ b = h_2 \circ b \\ \Leftrightarrow \quad & h_2^{-1} \cdot h_1 \circ b = b \\ \Leftrightarrow \quad & h_2^{-1} \cdot h_1 \in H_b = \{e\} \\ \Leftrightarrow \quad & h_1 = h_2 \end{aligned}$$

Nach Lemma 9.22 ist $\varphi$ surjektiv. Also ist $\varphi$ bijektiv.
Die Standgruppe $G_b$ wirkt transitiv auf $X \setminus \{b\}$, da $G$ 2-transitiv auf $X$ wirkt. Für $h_1, h_2 \in H$ existiert also ein $\alpha \in G_b$, so dass gilt:

$$\begin{aligned} & \alpha \cdot h_1 \circ b = h_2 \circ b \\ \Rightarrow \quad & \underbrace{\alpha \cdot h_1 \cdot \alpha^{-1}}_{\in H} \circ b = h_2 \circ b \quad \text{denn } \alpha \in G_b \Rightarrow b = \alpha^{-1} \circ b \\ \varphi \text{ injektiv} \Rightarrow \quad & \alpha \cdot h_1 \cdot \alpha^{-1} = h_2 \end{aligned}$$

Somit sind je zwei Elemente in $H \setminus \{e\}$ konjugiert in $G$. Nach dem obigen Lemma 9.24 ist die Ordnung von $H$ dann $p^n$. Da $\varphi$ bijektiv ist, gilt dann auch $|X| = p^n$ im Widerspruch zur Voraussetzung.

$G_a$ und $G_b$ sind konjugiert, denn es existiert ein $g \in G$ mit

$$\begin{aligned} g \circ a &= b \quad \text{wegen der Transitivität von } G \\ \Rightarrow \quad (g \cdot \alpha \cdot g^{-1}) \circ b &= (g \cdot \alpha) \circ a \quad \text{für alle } \alpha \in G_a \\ &= g \circ a \quad \text{denn } \alpha \circ a = a \\ &= b \\ \Rightarrow \quad g \cdot \alpha \cdot g^{-1} &\in G_b \quad \text{für alle } \alpha \in G_a \\ \Rightarrow \quad g \cdot G_a \cdot g^{-1} &\subseteq G_b \end{aligned}$$

Analog zeigt man die umgekehrte Inklusion. Somit gilt $g \cdot G_a \cdot g^{-1} = G_b$. Daraus folgt, dass auch $G_b$ einfach ist. Die Standgruppe $H_b = H \cap G_b$ ist Normalteiler in $G_b$. Da

$H_b \neq \{e\}$ und $G_b$ einfach ist, gilt also $H_b = G_b$ und $G_b < H$ ist Untergruppe in $H$. Nach Lemma 9.22 wirkt $H$ transitiv auf $X$. Die Standgruppe $G_b$ ist aber nicht transitiv auf $X$, denn $b$ ist ein Fixpunkt. Da $G$ 2-transitiv auf $X$ wirkt, ist die Wirkung nach Lemma 6.14 auch primitiv. Das heisst, dass $G_b$ eine maximale Standgruppe in $G$ ist.

$$G_b \lneqq H \lhd G \quad \Rightarrow \quad H = G$$

Somit ist $G$ einfach. □

Als Folgerung erhalten wir die Einfachheit der restlichen Mathieu Gruppen.

**Korollar 9.26.** *Die Mathieu-Gruppen $M_{12}, M_{22}, M_{23}$ und $M_{24}$ sind einfach.*

*Beweis.* Die genannten Mathieu-Gruppen $G$ wirken treu und (mindestens) 2-transitiv auf eine Menge $X$ und nach Konstruktion gibt es jeweils ein Element in $X$ mit einer einfachen Standgruppe. Also sind sie nach obigem Satz 9.25 einfach. □

## 9.4. Ausblick auf die Klassifikation der endlichen, einfachen Gruppen

Die Klassifikation der endlichen, einfachen Gruppen wurde erst 1982 abgeschlossen. Es gibt 18 unendliche Familien einfacher Gruppen und zusätzlich 26 sporadische einfache Gruppen, die keiner Familie zugeordnet werden können. Wir haben hier mit den zyklischen Gruppen mit Primzahlordnung, den alternierenden Gruppen und den speziellen, projektiven, linearen Gruppen 3 unendliche Familien einfacher Gruppen kennengelernt.

Die 5 Mathieu-Gruppen $M_{11}, M_{12}, M_{22}$, $M_{23}$ und $M_{24}$ gehören zu den 26 sporadischen einfachen Gruppen.

## 9.5. Monstergruppe

Die größte sporadische, einfache Gruppe ist die Monstergruppe $F_1$ mit der Ordnung

$$|F_1| = 808.017.424.794.512.875.886.459.904.961.710.757.005.754.368.000.000.000 \approx 8{\cdot}10^{53}$$

Ihre Existenz wurde 1973 von B. Fischer und R. Griess vorhergesagt, aber erst 1980 endgültig von R. Griess konstruktiv bewiesen.

# 10. Kombinatorische Designs und Steiner-Systeme

**Definition 10.1.** Sei $X$ eine Menge mit $\nu$ Elementen. Eine Menge $\mathcal{B} \subseteq \mathcal{P}_k(X)$ von $k$-elementigen Teilmengen in $X$ heisst Blocksystem $(X, \mathcal{B})$ mit den Parametern $(\nu, k)$ , $1 \leq k \leq \nu$.

Die Elemente $B \in \mathcal{B}$ heissen Blöcke und die Anzahl $k$ ihrer Elemente Blockgröße.

Die Anzahl der Blöcke wird mit $b := |\mathcal{B}| =: \lambda_0$ bezeichnet.

Blocksysteme mit $k = 1$ oder $k = \nu$ heissen trivial.

Blocksysteme $\mathcal{B} = \mathcal{P}_k(X)$ heissen vollständig. Die Anzahl der Blöcke ist dann $b = \left( \begin{smallmatrix} \nu \\ k \end{smallmatrix} \right)$.

**Definition 10.2.** In einem Blocksystem $(X, \mathcal{B})$ heissen die Funktionen

$$\begin{aligned} \lambda_t : \mathcal{P}_t(X) &\longrightarrow \mathbb{N} \\ A &\longmapsto |\{ B \in \mathcal{B} \,|\, A \subseteq B \}| \end{aligned}$$

für $t = 1$ Grad-Funktion und für $2 \leq t \leq k$ höhere Grad-Funktion.

Ein Blocksystem $(X, \mathcal{B})$ heisst $t$-regulär oder Block-Design, wenn die Grad-Funktion für alle $t$-elementigen Teilmengen $A \in \mathcal{P}_t(X)$ konstant ist.

**Bemerkung 10.3.** Da die 1-elementigen Teilmengen $\mathcal{P}_1(X) \simeq X$ den Elementen von $X$ entsprechen, kann $\lambda_1(x) = |\{ B \in \mathcal{B} \,|\, x \in B \}|$ als Grad-Funktion der Punkte aufgefaßt werden.

**Proposition 10.4.** *In einem Blocksystem $(X, \mathcal{B})$ ist das Produkt aus der Anzahl der Blöcke mit der Blockgröße gleich der Summe der Grade der Punkte.*

$$\lambda_0 \cdot k = \sum_{x \in X} \lambda_1(x)$$

*Insbesondere gilt für 1-reguläre Blocksysteme mit $\lambda_1(x) = \lambda_1$ für alle $x \in X$*

$$\lambda_0 \cdot k = \lambda_1 \cdot \nu$$

*Beweis.* Zum Beweis werden die Elemente der Menge

$$S = \{ (x, B) \,|\, x \in B \text{ und } B \in \mathcal{B} \}$$

auf zwei Arten gezählt. Alle Blöcken $B$ haben $k$ Elemente und es gibt $\lambda_0$ Blöcke. Das

ergibt zusammen $|S| = \lambda_0 \cdot k$. Andrerseits gilt

$$\begin{aligned} \lambda_1(x) &= |\{ B \in \mathcal{B} \,|\, x \in B \}| \\ &= |\{ (x, B) \,|\, B \in \mathcal{B} \}| \end{aligned}$$

Da für $x_1 \neq x_2$ die Mengen $\{ (x_1, B) \,|\, B \in \mathcal{B} \}$ und $\{ (x_2, B) \,|\, B \in \mathcal{B} \}$ disjunkt sind und die Vereinigung aller dieser Mengen $S$ ergibt, ist die Summe über alle $x \in X$

$$|S| = \sum_{x \in X} \lambda_1(x)$$

□

**Definition 10.5.** Zwei Blocksysteme $(X, \mathcal{B})$ und $(X', \mathcal{B}')$ heissen isomorph, wenn es eine bijektive Abbildung $f : X \to X'$ gibt, die die Blöcke in sich abbildet. Das heisst:

$$\mathcal{B}' = \{ f(B) \,|\, B \in \mathcal{B} \}$$

Isomorphismen $f : X \to X$ eines Blocksystems in sich heissen Automorphismen. Die Menge der Automorphismen wird mit $\mathrm{Aut}(X, \mathcal{B})$ bezeichnet.

Die Menge aller Isotypen von $t$-regulären Blocksystemen wird mit

$$S_\lambda(t, k, \nu)$$

bezeichnet.

Für $t = 1$ heissen die Isotypen $S_\lambda(1, k, \nu)$ kurz reguläre Blocksysteme.

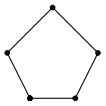
**Proposition 10.6.** *Die Automorphismen Aut$(X, \mathcal{B})$ eines Blocksystems $(X, \mathcal{B})$ bilden eine Untergruppe der symmetrischen Gruppe $S_X$.*

*Beweis.* Die Hintereinanderausführung eines Block-Automorphismus ist natürlich wieder ein Block-Automorphismus. Da $X$ und damit auch $S_X$ endlich ist, ist die Inverse eines Automorphismus $h$ gegeben durch $h^{-1} = h^m$ für ein $m \in \mathbb{N}$. □

**Bemerkung 10.7.** Für $t = k$ liegt ein vollständiges Blocksystem $\mathcal{B} = \mathcal{P}_k(X)$ vor. Da alle $A \in \mathcal{P}_k(X)$ auch in $\mathcal{B}$ liegen und mit genau einem Block, nämlich $B = A$, übereinstimmen, gilt $\lambda = 1$ und das Blocksystem ist $k$-regulär.

**Beispiel 10.8.** Reguläre Graphen
Für $t = 1$ und $k = 2$ kann der Isotyp $S_\lambda(1, 2, \nu)$ als $\lambda$-regulärer Graph mit $\nu$ Ecken

aufgefaßt werden. Die 2-elementigen Blöcke bilden die Kanten des Graphen und von jeder Ecke gehen $\lambda$ Kanten aus.

| $\lambda = 2, \nu = 5$ | $\lambda = 3, \nu = 4$ |
|---|---|
|  |  |

Es gibt allerdings nicht zu jeder Kombination von $\lambda$ und $\nu$ einen $\lambda$-regulären Graphen.

**Beispiel 10.9.** Vollständige Blocksysteme
Für die Isotypen $S_\lambda(t,k,\nu)$ vollständiger Blocksysteme $(X, \mathcal{P}_k(X))$ ist $\lambda$ festgelegt durch:

$$\lambda = \begin{pmatrix} \nu - t \\ k - t \end{pmatrix}$$

Denn $\lambda_t(A) = \lambda$ ist für alle $t$-elementigen Teilmengen $A$ konstant. Und die Anzahl der $k$-Blöcke, die eine Menge $A$ enthalten, entspricht der Anzahl $k-t$-elementiger Teilmengen in einer $\nu - t$-elementigen Menge $X'$.

**Definition 10.10.** Sei $(X, \mathcal{B}) \in S_\lambda(t,k,\nu)$ ein $t$-reguläres Block-Design mit $t \geq 2$ und $x \in X$. Alle Blöcke, die $x$ enthalten werden mit

$$star(x) := \{ B \in \mathcal{B} \mid x \in B \}$$

bezeichnet. Dann heisst

$$(X', \mathcal{B}')$$

mit $X' = X \setminus \{x\}$ und $\mathcal{B}' = \{ B \setminus \{x\} \mid B \in star(x) \}$ Kontraktion von $(X, \mathcal{B})$ bei $x$.

**Bemerkung 10.11.** Die Kontraktion eines Block-Designs hängt im allgemeinen von dem gewählten Element $x \in X$ ab. Wie das folgende Theorem zeigt, sind aber alle Kontraktionen isomorph.

**Theorem 10.12.** *Die Kontraktion $(X', \mathcal{B}')$ eines $t$-regulären Block-Designs $(X, \mathcal{B})$ ist ein $(t-1)$-reguläres Block-Design.*

$$(X', \mathcal{B}') \in S_\lambda(t-1, k-1, \nu-1)$$

*Beweis.* Wir betrachten eine $(t-1)$-elementige Menge $A' \subseteq X \setminus \{x\}$ und müssen zeigen, dass es $\lambda$ Blöcke $B' \in \mathcal{B}'$ gibt, die $A'$ enthalten. Nun fügen wir $x$ zu $A'$ hinzu und

erhalten $A = A' \cup \{x\}$. Die $t$-elementige Menge $A$ ist nach Definition in $\lambda$ Blöcken $B \in \mathcal{B}$ enthalten. Wenn nun $x$ aus diesen Blöcken $B$ wieder entfernt wird, erhalten wir genau so viele Blöcke $B' = B \setminus \{x\}$, in denen $A'$ enthalten ist. □

**Lemma 10.13.** *Seien $Y$ und $Z$ endliche Mengen und $W \subseteq Y \times Z$ eine Teilmenge des Kreuzproduktes. Für jedes $y \in Y$ sei*

$$\sharp(y, \cdot) := |\{ z \in Z \,|\, (y, z) \in W \}|$$

*und für jedes $z \in Z$ sei*

$$\sharp(\cdot, z) := |\{ y \in Y \,|\, (y, z) \in W \}|$$

*Wenn $\sharp(y, \cdot) = m$ für alle $y \in Y$ und $\sharp(\cdot, z) = n$ für alle $z \in Z$ konstant ist, dann gilt*

$$m \cdot |Y| = n \cdot |Z|$$

*Beweis.* Aus den Voraussetzungen folgt

$$\sum_{y \in Y} \sharp(y, \cdot) = |W| = \sum_{z \in Z} \sharp(\cdot, z)$$

Nach Aufsummierung ergibt sich daraus die Behauptung. □

**Theorem 10.14.** *Ein $t$-reguläres Blocksystem*

$$(X, \mathcal{B}) \in S_\lambda(t, k, \nu)$$

*mit $1 \leq t < k < \nu$. Dann ist die Anzahl der Blöcke*

$$b = \lambda_0 = \lambda \cdot \frac{\nu \cdot (\nu - 1) \cdots (\nu - t + 1)}{k \cdot (k - 1) \cdots (k - t + 1)}$$

*Die Anzahl der Blöcke, die $x \in X$ enthalten, ist unabhängig von $x$ und es gilt*

$$r = \lambda \cdot \frac{(\nu - 1) \cdots (\nu - t + 1)}{(k - 1) \cdots (k - t + 1)}$$

*Beweis.* Wir betrachten die Menge aller $t$-elementigen Teilmengen von $X$

$$Y = \{ A \subseteq X \,|\, |A| = t \}$$

Es gibt insgesamt

$$|Y| = \frac{1}{t!} \cdot \nu \cdot (\nu - 1) \cdots (\nu - t + 1)$$

$t$-elementige Teilmengen von $X$. Nun definieren wir

$$W = \{ (\{x_1, x_2, \cdots, x_t\}, B) \mid \{x_1, x_2, \cdots, x_t\} \subseteq B \} \subseteq Y \times \mathcal{B}$$

Da $(X, \mathcal{B})$ $t$-regulär ist, liegt jede $t$-elementige Teilmenge in genau $\lambda$ Blöcken und es gilt:

$$\sharp(\{x_1, x_2, \cdots, x_t\}, \cdot) = \lambda =: m$$

Da jeder Block $k$ Elemente enthält, gibt es

$$\frac{1}{t!} \cdot k \cdot (k-1) \cdots (k-t+1)$$

$t$-elementige Teilmengen in jedem Block und es gilt

$$\sharp(\cdot, B) = \frac{1}{t!} \cdot k \cdot (k-1) \cdots (k-t+1) =: n$$

Mit dem Abzählprinzip aus Lemma 10.13 ergibt sich die Anzahl der Blöcke zu

$$\begin{aligned} b = \lambda_0 &= |\mathcal{B}| \\ &= \frac{m}{n} |Y| \\ &= \frac{\lambda}{\frac{1}{t!} \cdot k \cdot (k-1) \cdots (k-t+1)} \cdot \frac{1}{t!} \cdot \nu \cdot (\nu-1) \cdots (\nu-t+1) \\ &= \lambda \cdot \frac{\nu \cdot (\nu-1) \cdots (\nu-t+1)}{k \cdot (k-1) \cdots (k-t+1)} \end{aligned}$$

Da $X' = X \setminus \{x\}$ nach Theorem 10.12 als Kontraktion $(X', \mathcal{B}')$ ein $(t-1)$-reguläres Blocksystem in $S_\lambda(t-1, k-1, \nu-1)$ ist, folgt die Formel für $r$ aus obiger Formel. □

Die Argumentation für die Anzahl der Blöcke, die ein Element $x \in X$ enthalten, kann fortgesetzt werden und wir erhalten als Folgerung.

**Korollar 10.15.** *Sei $(X, \mathcal{B}) \in S_\lambda(t, k, \nu)$ mit $1 < t < k < \nu$ ein $t$-reguläres Blocksystem und $t' < t$. Dann ist die Anzahl der Blöcke, die eine $t'$-elementige Teilmenge enthalten*

$$\lambda' = \lambda_{t'} = \lambda \cdot \frac{(\nu-t') \cdots (\nu-t+1)}{(k-t') \cdots (k-t+1)}$$

Manchmal ist es zweckmäßiger, von der gesamten Anzahl der Blöcke ausgehend, die Anzahl der Blöcke zu berechnen, die $t'$ Elemente enthalten.

**Korollar 10.16.** *Sei $(X, \mathcal{B}) \in S_\lambda(t, k, \nu)$ mit $1 < t < k < \nu$ ein $t$-reguläres Blocksystem mit $b$ Blöcken und $t' < t$. Dann ist die Anzahl $\lambda'$ der Blöcke, die eine $t'$-elementige Teilmenge enthalten*

$$\lambda' = b \cdot \frac{k(k-1)\cdots(k-t'+1)}{\nu(\nu-1)\cdots(\nu-t'+1)}$$

*Beweis.* Zum Beweis lösen wir die Formel

$$b = \lambda \cdot \frac{\nu \cdot (\nu-1)\cdots(\nu-t+1)}{k \cdot (k-1)\cdots(k-t+1)}$$

aus Theorem 10.14 nach $\lambda$ auf und setzen dies in die Formel aus Korollar 10.15 ein.

$$\begin{aligned}
\lambda' &= \lambda \cdot \frac{(\nu-t')\cdots(\nu-t+1)}{(k-t')\cdots(k-t+1)} \\
&= b \cdot \frac{k \cdot (k-1)\cdots(k-t+1)}{\nu \cdot (\nu-1)\cdots(\nu-t+1)} \cdot \frac{(\nu-t')\cdots(\nu-t+1)}{(k-t')\cdots(k-t+1)} \\
&= b \cdot \frac{k(k-1)\cdots(k-t'+1)}{\nu(\nu-1)\cdots(\nu-t'+1)}
\end{aligned}$$

□

Die Regularität von Blocksystemen vererbt sich von $t$ auf alle kleineren $t' < t$.

**Theorem 10.17.** *Ein $t$-reguläres Blocksystem*

$$(X, \mathcal{B}) \in S_\lambda(t, k, \nu)$$

*mit $1 \le t < k < \nu$ ist für alle kleineren $t'$ $(1 \le t' < t)$ $t'$-regulär. Mit $\lambda' = \lambda_{t'}$ gilt*

$$(X, \mathcal{B}) \in S_{\lambda'}(t', k, \nu)$$

*und*

$$\lambda' \cdot \begin{pmatrix} k-t' \\ t-t' \end{pmatrix} = \lambda \cdot \begin{pmatrix} \nu-t' \\ t-t' \end{pmatrix}$$

*Beweis.* Nach Korollar 10.15 ist jedes $t$-reguläre Blocksystem auch $t'$-regulär und für die Anzahl $\lambda'$ der Blöcke, die eine $t'$-elementige Teilmenge enthalten, gilt:

$$\lambda' = \lambda \cdot \frac{(\nu-t')\cdots(\nu-t+1)}{(k-t')\cdots(k-t+1)}$$

Wir erweitern beide Seiten mit $\frac{(\nu-t)!}{(k-t)!}$ und rechnen

$$\begin{aligned} \lambda' \cdot \frac{(\nu-t)!}{(k-t)!} &= \lambda \cdot \frac{(\nu-t')!}{(k-t')!} \\ \Rightarrow \quad \lambda' \cdot \frac{(k-t')!}{(k-t)!} &= \lambda \cdot \frac{(\nu-t')!}{(\nu-t)!} \quad \mid \cdot \frac{1}{(t-t')!} \\ \Rightarrow \quad \lambda' \cdot \begin{pmatrix} k-t' \\ t-t' \end{pmatrix} &= \lambda \cdot \begin{pmatrix} \nu-t' \\ t-t' \end{pmatrix} \end{aligned}$$

□

**Bemerkung 10.18.** Die Erweiterung eines Block-Designs $(X, \mathcal{B})$ zu $(\tilde{X}, \tilde{\mathcal{B}})$, so dass die Kontraktion

$$(\tilde{X}', \tilde{\mathcal{B}}') = (X, \mathcal{B})$$

wieder das ursprüngliche Block-Design ist, existiert im allgemeinen nicht. Die notwendige Bedingung für die Existenz ist

$$b \cdot (\nu+1) \equiv 0 \mod (k+1)$$

Denn die Anzahl $b$ der Blöcke in $(\tilde{X}, \tilde{\mathcal{B}})$ muss ganzzahlig sein. Nach Theorem 10.14 gilt

$$\begin{aligned} \mathbb{Z} \quad \ni \quad & \frac{(\nu+1)}{(k+1)} \cdot \underbrace{\lambda \cdot \frac{\nu \cdot (\nu-1) \cdots (\nu-t+1)}{k \cdot (k-1) \cdots (k-t+1)}}_{= b \in \mathbb{Z}} \\ \Rightarrow \quad (k+1) \quad & \text{teilt} \quad b \cdot (\nu+1) \\ \Rightarrow \quad b \cdot (\nu+1) \quad & \equiv \quad 0 \mod (k+1) \end{aligned}$$

### 10.0.1. Steiner Systeme

Der Schweizer Mathematiker Jakob Steiner (1796 bis 1863) fand 1853 die besondere Bedeutung von Isotypen mit $\lambda = 1$. Das heisst: jede $t$-elementige Teilmenge ist genau in einem Block enthalten.

**Definition 10.19.** Isotypen mit $1 < t < k < \nu$ und dem Parameter $\lambda = 1$ heissen Steiner-Systeme. Bezeichnung:

$$S(t, k, \nu) := S_1(t, k, \nu)$$

Für $\nu \geq 3$ sind Steiner-Tripel-Systeme definiert durch

$$STS(\nu) := S(2, 3, \nu)$$

Die Blöcke bestehen aus 3 Elementen und heissen Tripel.

Für $\nu \geq 4$ sind Steiner-Quadrupel-Systeme definiert durch

$$SQS(\nu) := S(3,4,\nu)$$

Die Blöcke bestehen aus 4 Elementen und heissen Quadrupel.

**Bemerkung 10.20.** Kirkman fand 1847, dass Steiner-Tripel-Systeme $STS(\nu)$ dann und nur dann existieren, wenn gilt:

$$\nu \equiv \begin{cases} 1 & \mod 6 \\ 3 & \mod 6 \end{cases}$$

Denn es gibt insgesamt $\frac{\nu(\nu-1)}{2}$ Paare in $X = [\nu]$, von denen je drei ein Tripel bilden. Es gibt also $\frac{\nu(\nu-1)}{6}$ Tripel. Und daraus ergibt sich die Bedingung.

**Bemerkung 10.21.** Steiner-Quadrupel-Systeme $STS(\nu)$ existieren genau für

$$\nu \equiv \begin{cases} 2 & \mod 6 \\ 4 & \mod 6 \end{cases}$$

**Korollar 10.22.** *Aus Theorem 10.17 und Korollar 10.15 ergeben sich notwendige Bedingungen an die Existenz eines Steiner-Systems.*

$$\begin{pmatrix} \nu - t' \\ t - t' \end{pmatrix} \equiv 0 \mod \begin{pmatrix} k - t' \\ t - t' \end{pmatrix} \quad \textit{für alle } 1 \leq t' \leq t$$

**Bemerkung 10.23.** Diese Bedingungen sind nicht hinreichend, denn $t = 2, k = 6, \nu = 36$ erfüllen die Bedingungen aber ein Steiner-System $S(2,6,36)$ existiert nicht. Dies ist äquivalent zu Eulers Problem der 36 Offiziere aus dem Jahr 1779. In 6 Regimentern befinden sich 6 Offiziere mit 6 verschiedenen Dienstgraden. Diese sollen so in einem Quadrat angeordnet werden, dass ein Regiment und ein Dienstgrad nur einmal in jeder Zeile oder Spalte vorkommt. Erst im Jahr 1900 konnte G. Tarry beweisen, dass dies nicht möglich ist.

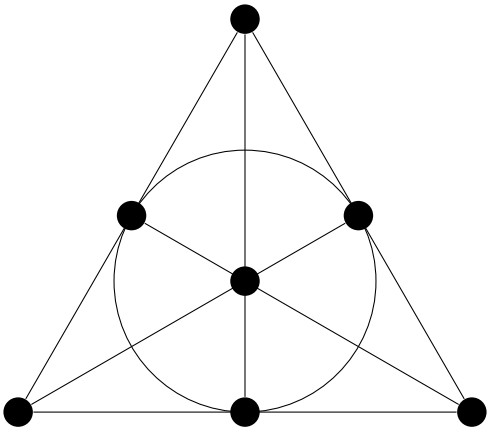
Die Existenz von Steiner-Systemen ist bis heute nur für wenige Kombinationen $(t,k,\nu)$ gelöst.

Für $t = 2$ können die Elemente von $X$ als Punkte aufgefaßt werden. Die Blöcke mit je zwei Punkten können dann als Geraden aufgefaßt werden. Jede Gerade enthält dann $k$ Punkte.

**Definition 10.24.** Steiner-Systeme $S(2,k,\nu)$ heissen endliche Geometrien.

**Beispiel 10.25.** Projektiven Ebenen $X = \mathbb{F}_q P^2$ über einem endlichen Körper $\mathbb{F}_q$ können als Steiner-Systeme $S(2,q+1,q^2+q+1)$ aufgefaßt werden. Nach Proposition 7.4 beträgt die Anzahl der Punkte $q^2+q+1$. Je zwei Punkte definieren eine Gerade (Blöcke). Auf jeder Geraden liegen $q+1$ Punkte.

Der erste Repräsentant ist die projektive Ebene über dem Körper $\mathbb{F}_2$. Diese wird nach ihrem Entdecker Gino Fano (1871 bis 1952), einem italienischen Mathematiker, Fano Ebene genannt.



Dies ist gleichzeitig das kleinstmögliche Steiner-Tripel-System $STS(7) = S(2,3,7)$

**Beispiel 10.26.** Affine Ebenen über einem endlichen Körper $\mathbb{F}_q$ können als Steiner-Systeme $S(2,q,q^2)$ aufgefaßt werden. Die Anzahl der Punkte in einer affinen Ebenen beträgt $q^2$. Je zwei Punkte definieren eine Gerade (Blöcke). Auf jeder Geraden liegen $q$ Punkte.

**Beispiel 10.27.** In einem $n$-dimensionalen affinen Raum ($n \geq 2$) über einem endlichen Körper $\mathbb{F}_q$ bilden die $m$-dimensionalen affinen Unterräume ($1 \leq m < n$) ein 2-reguläres Block-Design

$$AG_q^{n,m} = S_\lambda(2, q^m, q^n)$$

Dabei ist $q^n$ die Anzahl der Punkte im affinen Raum, die $m$-dimensionalen Unterräume bilden die Blöcke mit jeweils $q^m$ Punkten und je zwei Punkte liegen in $\lambda$ Blöcken. Es gilt:

$$\lambda = \frac{(q^{n-1}-1)(q^{n-2}-1)\cdots(q^{n-m+1}-1)}{(q^{m-1}-1)(q^{m-2}-1)\cdots(q-1)}$$

Es handelt sich also im allgemeinen um kein Steiner-System.

In affinen Räumen der Dimension $n \geq 3$ über dem Körper $\mathbb{F}_2$ liegen je drei Punkte in einer Ebene und es gilt $\lambda = 1$. Die affinen Ebenen des affinen Raumes $AG_2^n$ bilden also

ein Steiner-System:

$$AG_2^{n,2} = S(3,4,2^n)$$

**Beispiel 10.28.** In einem $n$-dimensionalen projektiven Raum ($n \geq 2$) über einem endlichen Körper $\mathbb{F}_q$ bilden die $m$-dimensionalen projektiven Unterräume ($1 \leq m < n$) ein 2-reguläres Block-Design

$$PG_q^{n,m} = S_\lambda(2, \frac{q^{m+1}-1}{q-1}, \frac{q^{n+1}-1}{q-1})$$

Dabei ist $\frac{q^{n+1}-1}{q-1}$ die Anzahl der Punkte im projektiven Raum, die $m$-dimensionalen Unterräume bilden die Blöcke mit jeweils $\frac{q^{m+1}-1}{q-1}$ Punkten und je zwei Punkte liegen in $\lambda$ Blöcken. Es gilt:

$$\lambda = \frac{(q^{n-1}-1)(q^{n-2}-1)\cdots(q^{n-m+1}-1)}{(q^{m-1}-1)(q^{m-2}-1)\cdots(q-1)}$$

Es handelt sich also im allgemeinen nicht um Steiner-System.

**Theorem 10.29.** *Die Automorphismengruppe $Aut(X,\mathcal{B})$ eines Steiner-Systems $(X,\mathcal{B}) \in S(t,k,\nu)$ operiert treu (effektiv) auf $\mathcal{B}$.*

*Beweis.* Nach Definition 1.43 müssen wir zeigen, dass ein Automorphismus $\varphi : X \to X$, der alle Böcke fest läßt, die Identität sein muss. Sei $\varphi(B) = B$ für alle $B \in \mathcal{B}$. Für ein beliebiges $x \in X$ betrachten wir alle Blöcke $star(x)$ die $x$ enthalten. Da $\varphi$ ein Automorphismus ist, gilt

$$\varphi(star(x)) = star(\varphi(x))$$

Da $\varphi$ die Blöcke fest läßt, gilt

$$\varphi(star(x)) = star(x)$$

Daraus folgt $star(x) = star(\varphi(x))$. Somit liegen $x$ und $\varphi(x)$ im selben Block und alle Blöcke, die $x$ enthalten, enthalten auch $\varphi(x)$. Das heisst, die Anzahl $r$ der Blöcke, die $x$ enthalten, stimmt mit der Anzahl $r'$ der Blöcke überein, die $\{x, \varphi(x)\}$ enthalten. Wäre $x \neq \varphi(x)$ dann folgt aus der Formel in Korollar 10.15

$$\begin{aligned} & & r &= r' \\ \Rightarrow \quad & \frac{(\nu-1)\cdot(\nu-2)\cdots(\nu-t+1)}{(k-1)\cdot(k-2)\cdots(k-t+1)} &= & \frac{(\nu-2)\cdots(\nu-t+1)}{(k-2)\cdots(k-t+1)} \\ & \Rightarrow \quad \nu-1 &= & k-1 \end{aligned}$$

Dies ist ein Widerspruch zur Voraussetzung $k < \nu$. Somit muss $\varphi(x) = x$ gelten und $\varphi$ ist die Identität. □

### 10.0.2. Konstruktion des kleinen Witt-Designs

Die Existenz der Steiner-Systeme $S(5,6,12)$ und $S(5,8,24)$ wurde 1931 von Carmichael [Car31] und 1938 von Witt [Wit38] bewiesen.

**Theorem 10.30.** *Das Steiner-System $W_{12} := S(5,6,12)$ existiert und wird kleines Witt-Design genannt.*

*Beweis.* Der Beweis folgt der Argumentation von Carmichael [Car31] aus dem Jahr 1931. Dies wird auch im Buch "Design Theory" von Beth, Jungnickel und Lenz [BJL99] beschrieben.

In der projektiven Geraden $\mathbb{F}_{11}P$ über dem Körper $\mathbb{F}_{11}$ gibt es 12 Elemente

$$\mathbb{F}_{11}P = \{\infty, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

Die projektive spezielle lineare Gruppe $PSl_2(\mathbb{F}_{11})$ ist nach Bemerkung 7.22 isomorph zur Gruppe der linear gebrochenen Transformationen mit Determinante 1. In der projektiven Geraden $\mathbb{F}_{11}P$ betrachten wir folgenden initialen Block mit 6 Elementen

$$B_0 = \{\infty, 1, 3, 4, 5, 9\}$$

Dieser wird von den 5 projektiven Abbildungen

$$\begin{array}{rcl} \mathbb{F}_{11}P & \longrightarrow & \mathbb{F}_{11}P \\ x & \longmapsto & 3^n \cdot x \quad \text{für } n \in \{0,1,2,3,4\} \end{array}$$

in sich abgebildet. Man beachte, dass $B_0$ neben $\infty$ genau die 5 Elemente ungleich 0 enthält, deren Wurzeln in $\mathbb{F}_{11}$ existieren. Diese Abbildungen bilden eine zyklische Untergruppe $C_5 < PSl_2(\mathbb{F}_{11})$ in der projektiven speziellen linearen Gruppe. Das heisst, die zyklische Untergruppe $C_5$ ist als Untergruppe enthalten im Stabilisator

$$PSl_2(\mathbb{F}_{11})_{B_0} = \{g \in PSl_2(\mathbb{F}_{11}) \mid gB_0 = B_0\}$$

Somit ist die Ordnung des Stabilisator ein Vielfaches von 5. Nach dem Bahn-Standgruppen-Satz 1.53 ist das Produkt aus der Ordnung des Stabilisators $5m$ mit der Anzahl der Bahnen, also der Anzahl verschiedener Bilder des initialen Blocks $b$, gleich der Gruppen-

ordnung.

$$\begin{aligned} |\, PSl_2(\mathbb{F}_{11}) &= 5m \cdot b \\ \Rightarrow \quad b &= \frac{660}{5m} = \frac{132}{m} \end{aligned}$$

Denn nach Proposition 7.13 hat $PSl_2(\mathbb{F}_{11})$ die Ordnung $\frac{1}{2} \cdot 10 \cdot 11 \cdot 12 = 660$. Für den Nachweis, dass die Bilder des initialen Blockes $B_0$ unter den Abbildungen $PSl_2(\mathbb{F}_{11})$ ein 5-reguläres Steiner-System bilden, muss nun gezeigt werden, dass $m = 1$ ist. Denn nach Korollar 10.16 berechnet sich dann die Anzahl der Blöcke, die eine 5-elementige Teilmenge enthält, zu

$$\begin{aligned} \lambda_5 &= b \cdot \frac{6(6-1)\cdots(6-5+1)}{12(12-1)\cdots(12-5+1)} \\ &= \frac{132}{1} \cdot \frac{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2}{12 \cdot 11 \cdot 10 \cdot 9 \cdot 8} \\ &= 1 \end{aligned}$$

Das heisst, es gibt nur einen Block der 5 vorgegebene Elemente enthält.

Es ist nun übersichtlicher, wenn wir die Blöcke zählen, die drei vorgegebene Elemente enthalten. Die Anzahl $\lambda_3$ dieser Blöcke ist nach Korollar 10.16

$$\lambda_3 = \frac{132}{m} \cdot \frac{6 \cdot 5 \cdot 4}{12 \cdot 11 \cdot 10} = \frac{12}{m}$$

Als die drei vorgegebenen Elemente werden $\{\infty, 0, 1\}$ gewählt, weil diese bei den gebrochen linearen Abbildungen eine Sonderrolle spielen. Insbesondere werden diese Elemente von der folgenden Abbildung in sich abgebildet.

$$\begin{aligned} \sigma : \mathbb{F}_{11}P &\longrightarrow \mathbb{F}_{11}P \\ x &\longmapsto 1 - \frac{1}{x} = \frac{x-1}{x} \end{aligned}$$

$$\begin{aligned} \sigma(\infty) &= 1 \\ \sigma(0) &= \infty \\ \sigma(1) &= 0 \end{aligned}$$

Die anderen Elemente werden wie folgt abgebildet.

| $x$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| $\sigma(x)$ | 6 | 8 | 9 | 3 | 10 | 4 | 5 | 7 | 2 |

Man rechnet leicht nach, dass $\sigma$ die Ordnung 3 hat. Aus dem initialen Block $B_0$ erhalten wir durch einfache gebrochen lineare Transformationen folgende Blöcke, die $\infty, 0, 1$ enthalten.

$$\begin{aligned} B_1 &= B_0 - 3 = \{\infty, 0, 1, 2, 6, 9\} \\ B_2 &= B_0 - 4 = \{\infty, 0, 1, 5, 8, 10\} \\ B_3 &= \frac{1}{1 - B_0} + 4 = \{\infty, 0, 1, 4, 8, 9\} \\ B_4 &= \frac{1}{3 - B_0} + 2 = \{\infty, 0, 1, 2, 7, 8\} \end{aligned}$$

Mit der Abbildung $\sigma$ ergeben sich 12 Blöcke mit den 3 Elementen $\infty, 0, 1$.

$$\begin{aligned} B_1 &= \{\infty, 0, 1, 2, 6, 9\} \\ \sigma(B_1) &= \{\infty, 0, 1, 6, 7, 10\} \\ \sigma^2(B_1) &= \{\infty, 0, 1, 2, 4, 10\} \\ B_2 &= \{\infty, 0, 1, 5, 8, 10\} \\ \sigma(B_2) &= \{\infty, 0, 1, 2, 3, 5\} \\ \sigma^2(B_2) &= \{\infty, 0, 1, 3, 6, 8\} \\ B_3 &= \{\infty, 0, 1, 4, 8, 9\} \\ \sigma(B_3) &= \{\infty, 0, 1, 5, 7, 9\} \\ \sigma^2(B_3) &= \{\infty, 0, 1, 3, 4, 7\} \\ B_4 &= \{\infty, 0, 1, 2, 7, 8\} \\ \sigma(B_4) &= \{\infty, 0, 1, 4, 5, 6\} \\ \sigma^2(B_4) &= \{\infty, 0, 1, 3, 9, 10\} \end{aligned}$$

Daraus folgt, dass $m = 1$ gelten muss. □

Man kann sogar zeigen, dass es bis auf Isomorphie nur ein Steiner-System $S(5, 5, 12)$ gibt

**Proposition 10.31.** *Das kleine Witt-Design $W_{12} = S(5, 6, 12)$ ist eindeutig.*

**Theorem 10.32.** *Die Automorphismengruppe von $W_{12}$ ist die Mathieu-Gruppe $M_{12} = Aut(W_{12})$.*

*Beweis.* Nach Theorem 8.4 wirkt die Mathieu-Gruppe $M_{12}$ 5-transitiv auf $\mathbb{F}_{11}P \simeq [12]$. Das heisst, wenn 5 Elemente $\{a,b,c,d,e\}$ in einem Block $\{a,b,c,d,e\} \cup \{r\}$ sind, dann liegen deren Bilder $\{\mu(a),\mu(b),\mu(c),\mu(d),\mu(e)\}$ unter der Wirkung eines Elementes $\mu \in M_{12}$ in der eindeutig bestimmten Menge $\{\mu(a),\mu(b),\mu(c),\mu(d),\mu(e)\} \cup \{\mu(r)\}$. Wegen der 5-Regularität von $W_{12}$ ist dies ebenfalls ein Block. □

Als Kontraktion ergibt sich:

**Korollar 10.33.** *Das Steiner-System $W_{11} := S(4,5,11)$ existiert.*

**Theorem 10.34.** *Die Automorphismengruppe von $W_{11}$ ist die Mathieu-Gruppe $M_{11} = Aut(W_{11})$.*

*Beweis.* Man erhält die Automorphismengruppe von $W_{11}$ aus der Automorphismengruppe von $W_{12}$, wenn nur die Automorphismen betrachtet werden, die das bei der Kontraktion weggelassene Element fest lassen. □

Eine Erweiterung des kleinen Witt-Designs $W_{12}$ ist dagegen nicht möglich.

**Theorem 10.35.** *Das kleine Witt-Design $W_{12} = S(5,6,12)$ kann nicht erweitert werden.*

*Beweis.* Zum Beweis rechnen wir die Bedingung aus Korollar 10.22 für das kleine Witt-Design $W_{12}$ nach. Aus $\nu = 12, k = 6$ und $t = 5$ erhalten wir für die Anzahl der Blöcke

$$\begin{aligned} b &= 1 \cdot \frac{\nu(\nu-1)\cdots(\nu-t+1)}{k(k-1)\cdots(k-t+1)} \\ &= \frac{12 \cdot 11 \cdot 10 \cdot 9 \cdot 8}{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2} \\ &= 11 \cdot 12 = 132 \end{aligned}$$

$k+1 = 7$ ist jedoch kein Teiler von $b \cdot (\nu+1) = 11 \cdot 12 \cdot 13$. □

### 10.0.3. Konstruktion des großen Witt-Designs

**Theorem 10.36.** *Das Steiner-System $W_{24} := S(5,8,24)$ existiert und wird großes Witt-Design genannt.*

*Beweis.* Es gibt verschiedene konstruktive Beweise für die Existenz des großen Witt-Designs $W_{24}$.

Eine Möglichkeit besteht darin, alle Blöcke mit 8 Elementen in lexigraphischer Reihenfolge aufzulisten. Dabei ist die Bedingung zu beachten, dass jeweils 5 Elemente nur in einem Block auftreten dürfen. Davon gibt es nach Theorem 10.14:

$$\frac{24 \cdot 23 \cdot 21 \cdot 20}{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4} = 759$$

In der Menge $X = [24]$ erhält man folgende Liste der Blöcke:

$$\begin{array}{cccccccc}
01 & 02 & 03 & 04 & 05 & 06 & 07 & 08 \\
01 & 02 & 03 & 04 & 09 & 10 & 11 & 12 \\
01 & 02 & 03 & 04 & 13 & 14 & 15 & 16 \\
\multicolumn{8}{c}{\ldots} \\
\multicolumn{8}{c}{753 \text{ weitere}} \\
\multicolumn{8}{c}{\ldots} \\
13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\
13 & 14 & 15 & 16 & 21 & 22 & 23 & 24 \\
17 & 18 & 19 & 20 & 21 & 22 & 23 & 24
\end{array}$$

Nach Korollar 10.15 kann die Anzahl der Blöcke mit vorgegebenen $1, 2, 3, 4$ oder 5 Elementen wie folgt angegeben werden:

$$\begin{array}{lcc}
\text{mit einem Element} & \frac{23 \cdot 22 \cdot 21 \cdot 20}{7 \cdot 6 \cdot 5 \cdot 4} & = 253 \\
\text{mit zwei Elementen} & \frac{22 \cdot 21 \cdot 20}{6 \cdot 5 \cdot 4} & = 77 \\
\text{mit drei Elementen} & \frac{21 \cdot 20}{5 \cdot 4} & = 21 \\
\text{mit vier Elementen} & \frac{20}{4} & = 5 \\
\text{mit fünf Elementen} & & 1
\end{array}$$

Alternativ führt eine ähnliche Konstruktionsmethode wie beim kleinen Witt-Design $W_{12}$ in Theorem 10.30 zum Erfolg. Dies wird ebenfalls in Carmichaels Artikel von 1931 [Car31] und im Buch "Design Theory" von Beth, Jungnickel und Lenz [BJL99] beschrieben.

Die Konstruktion geht von der projektiven Geraden $\mathbb{F}_{23}P$ über dem endlichen Körper $\mathbb{F}_{23}$ aus. Diese hat 24 Elemente.

$$\mathbb{F}_{23}P = \{\infty, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22\}$$

Die projektive spezielle lineare Gruppe $PSl_2(\mathbb{F}_{23})$ ist nach Bemerkung 7.22 isomorph zur Gruppe der gebrochenen linearen Transformationen mit Determinante 1. Nach Propo-

sition 7.13 hat diese Gruppe die Ordnung:

$$|\,PSl_2(\mathbb{F}_{23})\,| = \frac{1}{2}\cdot 23^{\binom{2}{2}}\cdot(23^2-1) = \frac{1}{2}\cdot 23\cdot 528 = 6\,072$$

Nun muss nur noch gezeigt werden, dass 8 dieser gebrochen linearen Transformationen einen initialen Block $B_0$ in sich abbilden. Dann ergeben sich insgesamt $6\,072/8 = 759$ unterschiedliche Blöcke mit jeweils 8 Elementen. Diese bilden dann die Blockstruktur in $S(5,8,23)$.

Die gebrochen linearen Transformationen

$$\alpha(x) = \frac{x+1}{-x+1}$$

und

$$\beta(x) = \frac{3x+1}{x-3}$$

erzeugen eine Untergruppe $U \in PSl_2(\mathbb{F}_{23})$ von gebrochen linearen Transformationen der Ordnung 8.

Die Determinante von $\alpha$ ist zwar 2, aber da $2 = 5^2 \mod 23$ ist, kann der Quotient von $\alpha$ mit $\frac{1}{5} = 14 \mod 23$ erweitert werden und hat dann die Determinante 1.

Die Determinante von $\beta$ ist $-10 = 13 \mod 23$ und $13 = 6^2 \mod 23$, so dass nach Erweiterung des Quotienten von $\beta$ mit $\frac{1}{6} = 4 \mod 23$ die Determinante 1 erreicht werden kann.

Somit gehören $\alpha$ und $\beta$ zur projektiven speziellen linearen Gruppe $PSl_2(\mathbb{F}_{23})$.

Man rechnet leicht nach, dass $\alpha$ die Ordnung 4 hat.

$$\begin{aligned}
\alpha^2(x) &= \frac{x+1-x+1}{-x-1-x+1} \\
&= \frac{2}{-2x} \\
&= -\frac{1}{x} \\
\alpha^4(x) &= -\frac{1}{-\frac{1}{x}} \\
&= x
\end{aligned}$$

Und $\beta$ hat die Ordnung 2.

$$\begin{aligned}\beta^2(x) &= \frac{3\cdot(3x+1)+x-3}{3x+1-3\cdot(x-3)}\\ &= \frac{9x+3+x-3}{3x+1-3x+9}\\ &= \frac{10x}{10}\\ &= x\end{aligned}$$

Überdies gilt die Relation $(\beta\alpha)^2 = id$.

$$\begin{aligned}(\beta\alpha)(x) &= \frac{3\cdot(x+1)-x+1}{x+1-3\cdot(-x+1)}\\ &= \frac{3x+3-x-1}{x+1+3x-3}\\ &= \frac{2x+4}{4x-2}\\ \Rightarrow\quad (\beta\alpha)^2(x) &= \frac{2\cdot(2x+4)+4\cdot(4x-2}{4\cdot(2x+4)-2\cdot(4x-2)}\\ &= \frac{4x+8+16x-8}{8x+16-8x+4}\\ &= \frac{20x}{20}\\ &= x\end{aligned}$$

Somit ist die von $\alpha$ und $\beta$ erzeugte Gruppe $U$ isomorph zum Kreuzprodukt der zyklischen Gruppen der Ordnung 4 und 2

$$U = C_4 \times C_2$$

und hat die Ordnung 8. In der folgenden Tabelle sind die Bilder unter den gebrochen linearen Transformationen zusammengestellt.

| $x$ | $\infty$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\alpha$ | 22 | 1 | $\infty$ | 20 | 21 | 6 | 10 | 7 | 14 | 2 | 16 | 9 | 8 | 3 | 18 | 13 | 12 | 5 | 19 | 7 | 4 | 11 | 15 | 0 |
| $\beta$ | 3 | 15 | 21 | 16 | $\infty$ | 13 | 8 | 14 | 17 | 5 | 20 | 11 | 10 | 22 | 4 | 6 | 0 | 2 | 7 | 19 | 18 | 9 | 1 | 12 |

Da $\alpha$ die Ordnung 4 hat, bildet $\alpha$ 6 Blöcke von jeweils 4 Elementen in sich ab. Analog bildet $\beta$ 12 Blöcke mit jeweils 2 Elemente in sich ab. Die von $\alpha$ und $\beta$ erzeugte Gruppe $U$ bildet 3 Blöcke mit jeweils 8 Elementen in sich ab. In der Tabelle ist einer dieser Blöcke grün hinterlegt, der die Elemente $\infty, 0, 1$ enthält. Dieser wird als initialer Block

gewählt.

$$B_0 = \{ \infty , 0 , 1 , 3 , 12 , 15 , 21 , 22 \}$$

Das heisst, die Gruppe $U$ ist als Untergruppe enthalten im Stabilisator

$$PSl_2(\mathbb{F}_{23})_{B_0} = \{g \in PSl_2(\mathbb{F}_{23}) \mid gB_0 = B_0 \}$$

Somit ist die Ordnung des Stabilisator ein Vielfaches von 8. Nach dem Bahn-Standgruppen-Satz 1.53 ist das Produkt aus der Ordnung des Stabilisators $8m$ mit der Anzahl der Bahnen, also der Anzahl verschiedener Bilder des initialen Blocks $b$, gleich der Gruppenordnung.

$$\begin{aligned} |PSl_2(\mathbb{F}_{23})| &= 8m \cdot b \\ \Rightarrow \quad b &= \frac{6072}{8m} = \frac{759}{m} \end{aligned}$$

Denn nach Proposition 7.13 hat $PSl_2(\mathbb{F}_{23})$ die Ordnung $\frac{1}{2} \cdot 24 \cdot 23 \cdot 22 = 6072$. Für den Nachweis, dass die Bilder des initialen Blockes $B_0$ unter den Abbildungen $PSl_2(\mathbb{F}_{23})$ ein 5-reguläres Steiner-System bilden, muss nun gezeigt werden, dass $m = 1$ ist. Denn nach Korollar 10.16 berechnet sich dann die Anzahl der Blöcke, die eine 5-elementige Teilmenge enthält, zu

$$\begin{aligned} \lambda_5 &= b \cdot \frac{8(8-1)\cdots(8-5+1)}{24(24-1)\cdots(24-5+1)} \\ &= \frac{759}{1} \cdot \frac{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4}{24 \cdot 23 \cdot 22 \cdot 21 \cdot 20} \\ &= 1 \end{aligned}$$

Das heisst, es gibt nur einen Block, der 5 vorgegebene Elemente enthält.

Wie bei der Konstruktion des kleinen Witt-Designs in Theorem 10.30 ist es nun übersichtlicher, wenn wir die Blöcke zählen, die drei vorgegebene Elemente enthalten. Die Anzahl $\lambda_3$ dieser Blöcke ist nach Korollar 10.16

$$\lambda_3 = \frac{759}{m} \cdot \frac{8 \cdot 7 \cdot 6}{24 \cdot 23 \cdot 22} = \frac{21}{m}$$

Als die drei vorgegebenen Elemente werden $\{ \infty , 0 , 1 \}$ gewählt, weil diese bei den gebrochen linearen Abbildungen eine Sonderrolle spielen. Insbesondere werden diese Ele-

mente von der Abbildung $\sigma$ aus dem Beweis zu Theorem 10.30 in sich abgebildet.

$$\begin{aligned} \sigma : \mathbb{F}_{23}P &\longrightarrow \mathbb{F}_{23}P \\ x &\longmapsto 1 - \frac{1}{x} = \frac{x-1}{x} \end{aligned}$$

Die Abbidlung $\sigma$ hat die Ordnung 3. Wenn wir also 7 Abbildungen in $PSl_2(\mathbb{F}_{23})$ finden, die den initialen Block in 7 verschiedene Blöcke, jedoch stets mit $\{\infty, 0, 1\}$, abbilden, liefert die Anwendung von $\sigma$ und $\sigma^2$ die restlichen 14 Blöcke und es muss $m = 1$ gelten. Die gesuchten 7 Abbildungen und ihre Blöcke sind:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $B_0$ | $\infty$ | 0 | 1 | 3 | 12 | 15 | 21 | 22 |
| $2B_0$ | $\infty$ | 0 | 2 | 6 | 1 | 7 | 19 | 21 |
| $2B_0 - 6$ | $\infty$ | 17 | 19 | 0 | 18 | 1 | 13 | 15 |
| $8B_0 - 7$ | $\infty$ | 16 | 1 | 17 | 20 | 21 | 0 | 8 |
| $B_0 + 2$ | $\infty$ | 2 | 3 | 5 | 14 | 17 | 0 | 1 |
| $2B_0 - 1$ | $\infty$ | 22 | 1 | 5 | 0 | 6 | 18 | 20 |
| $8B_0 - 4$ | $\infty$ | 19 | 4 | 20 | 0 | 1 | 3 | 11 |

Anmerkung: Da $2 = 5^2 \mod 23$ und $8 = 10^2 \mod 23$ Wurzeln in $mathbbF_{23}$ besitzen, gehören alle obigen Abbildung zur speziellen projektiven linearen Gruppe $PSl_2(\mathbb{F}_{23})$. □

Man kann sogar zeigen, dass es bis auf Isomorphie nur ein Steiner-System $S(5, 8, 24)$ gibt

**Proposition 10.37.** *Das große Witt-Design $W_{24} = S(5, 8, 24)$ ist eindeutig.*

**Korollar 10.38.** *Die Steiner-Systeme*

$$\begin{aligned} W_{23} &:= S(4, 7, 23) \\ W_{22} &:= S(3, 6, 22) \end{aligned}$$

*existieren.*

Die Existenz ergibt sich als Kontraktion von $W_{24}$ beziehungsweise $W_{23}$.

**Theorem 10.39.** *Die Automorphismengruppen von $W_{24}, W23$ und $W_{22}$ sind die Mathieu-*

*Gruppen*

$$\begin{aligned} M_{24} &= Aut(W_{24}) \\ M_{23} &= Aut(W_{23}) \\ M_{22} &= Aut(W_{22}) \end{aligned}$$

Eine Erweiterung des großen Witt-Designs $W_{24}$ ist nicht möglich.

**Theorem 10.40.** *Das große Witt-Design $W_{24} := S(5,8,24)$ kann nicht erweitert werden.*

*Beweis.* Zum Beweis rechnen wir die Bedingung aus Korollar 10.22 für das große Witt-Design $W_{24}$ nach. Aus $\nu = 24, k = 8$ und $t = 5$ erhalten wir für die Anzahl der Blöcke

$$\begin{aligned} b &= 1 \cdot \frac{\nu(\nu-1)\cdots(\nu-t+1)}{k(k-1)\cdots(k-t+1)} \\ &= \frac{24 \cdot 23 \cdot 22 \cdot 21 \cdot 20}{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4} \\ &= 3 \cdot 11 \cdot 23 = 132 \end{aligned}$$

$k + 1 = 9$ ist jedoch kein Teiler von $b \cdot (\nu + 1) = 3 \cdot 11 \cdot 23 \cdot 25$. □

# 11. Verbindungen zur Codierungstheorie

Im vorigen Abschnitt wurde die Verbindung der Gruppentheorie zu kombinatorischen Designs beschrieben. Eine weitere, interessante Verbindung besteht zur Codierungstheorie und zeigt, dass in der Mathematik alles mit allem zusammenhängt. Hier können allerdings nur die wesentlichen Begriffe und Zusammenhänge erläutert werden.

Die Motivation für die Codierungstheorie kommt aus der Nachrichtenübermittlung. Bei der Übertragung können Fehler auftreten. Passiert dies, ist die empfangene Nachricht nicht die gleiche wie die verschickte. Um dennoch die ursprüngliche, verschickte Nachricht wieder herzustellen, können zusätzliche Informationen mitgeschickt werden, die es erlauben festzustellen, ob bei der Übermittlung Fehler aufgetreten sind und diese möglicherweise zu beheben. Der Codierungstheorie beschäftigt sich mit dem Problem Codes zu finden, die möglichst viele Fehler korrigieren können. Die Codierungstheorie ist ein relativ junger Teil der Mathematik: Sie entstand erst in den 1940er Jahren. Der erste fehlerkorrigierende Code wurde 1947 von Hamming gefunden. Fehlerkorrigierende Codes werden beispielsweise seit 1970 von der NASA erfolgreich bei der Übertragung von Bildern aus dem Weltall benutzt.

**Definition 11.1.** Sei $Q$ eine endliche Menge von $q$ Symbolen oder Buchstaben. Diese heisst in der Codierungstheorie Alphabeth.

Ein Code-Wort $C$ der Länge $n$ ist ein Element aus dem $n$-fachen Produkt von $Q$.

Die Menge aller Code-Wörter bildet eine Teilmenge $\mathcal{C} \subseteq Q^n$ im $n$-fachen Produkt von $Q$ und wird Code genannt. Die Anzahl der Code-Wörter wird mit $c := |\mathcal{C}|$ bezeichnet.

Die Informationsrate eines Code-Wortes $C \in \mathcal{C}$ der Länge $n$ über einem Alphabeth $Q$ mit $q$ Symbolen ist definiert durch

$$R := \frac{\log_q c}{n}$$

**Bemerkung 11.2.** Für die Anzahl der Code-Wörter gilt $c \leq q^n$. Daraus folgt, dass die Informationsrate $R < 1$ stets kleiner 1 ist. Der Wert $1 - R$ wird auch Redundanz genannt.

Einige spezielle Codes haben besondere Bedeutung.

**Definition 11.3.** Ein Code mit dem Alphabeth $Q = \mathbb{F}_2 = \{0, 1\}$ heisst binärer Code.

Ein linearer Code liegt vor, wenn die Code-Wörter $\mathcal{C}$ einen linearen Unterraum von $Q^n$ bilden.

Zwei Codes der Länge $n$ heissen äquivalent, wenn alle Code-Wörter des einen Codes durch eine feste Permutation in die Code-Wörter des anderen Codes überführt werden können.

**Bemerkung 11.4.** Ein linearer Code $\mathcal{C}$ der Dimension $k$ hat die Informationsrate

$$R := \frac{\log_q q^k}{n} = \frac{k}{n}$$

Der amerikanische Mathematiker Richard Wesley Hamming (1915–1998) hat ein Maß für den Unterschied zwischen zwei Code-Wörtern definiert.

**Definition 11.5.** Seien $x, y \in \mathcal{C}$ zwei Code-Wörter der Länge $n$. Dann ist deren Hamming-Abstand definiert durch

$$d(x,y) := |\{\, i \in [n] \,|\, x_i \neq y_i \,\}|$$

Alle Code-Wörter $y$, die von $x$ einen Hamming-Abstand kleiner oder gleich einem vorgegebenen $r$ haben, liegen im Hamming-Ball.

$$B_r(x) := \{\, y \in \mathcal{C} \,|\, d(x,y) \leq r \,\}$$

Der Hamming-Abstand eines Codes $\mathcal{C}$ ist das Minimum aller Hamming-Abstände zweier Code-Wörter.

$$d(\mathcal{C}) := \min\{\, d(x,y) \,|\, x \neq y \in \mathcal{C} \,\}$$

Falls das Null-Wort $0^n \in \mathcal{C}$ im Code enthalten ist, ist das Hamming-Gewicht eines Code-Wortes $x \in \mathcal{C}$ definiert als

$$w(x) := d(x, 0^n)$$

Das Gewichtspolynom des Codes $\mathcal{C}$ ist definiert als

$$w_t(\mathcal{C}) := \sum_{i=0}^{n} a_i \cdot t^i \quad \text{mit } a_i := |\{\, x \in \mathcal{C} \,|\, w(x) = i \,\}|$$

**Bemerkung 11.6.** Der Hamming-Abstand definiert eine Metrik auf $Q^n$ und $\mathcal{C}$.

**Bemerkung 11.7.** Lineare Codes enthalten stets das Code-Wort 0. Somit ist für jedes Code-Wort $x \in \mathcal{C}$ das Gewicht $w(x)$ definiert.

**Proposition 11.8.** *Die Anzahl der Code-Wörter im Hamming-Ball $B_r(x)$ ist*

$$|\, B_r(x) \,| = \sum_{i=0}^{r} \binom{n}{i} \cdot (q-1)^i$$

**Definition 11.9.** Der Grad der Fehlerkorrektur eines Codes $\mathcal{C}$ mit dem Hamming-

Abstand $d(\mathcal{C})$ ist definiert als

$$e(\mathcal{C}) := \lfloor \frac{d(\mathcal{C}) - 1}{2} \rfloor$$

Der Code $\mathcal{C}$ heisst dann auch $e$-fehlerkorrigierend.

**Proposition 11.10.** *Bei einem e-fehlerkorrigierenden Code $\mathcal{C}$ sind die Hamming-Balls von zwei verschiedenen Code-Wörtern $x \neq y$ disjunkt.*

$$x \neq y \quad \Rightarrow \quad B_e(x) \cap B_e(y) = \varnothing$$

*Beweis.* Aus $e(\mathcal{C}) = \lfloor \frac{d(\mathcal{C})-1}{2} \rfloor$ folgt $2e(\mathcal{C}) < d(\mathcal{C})$. Aus der Annahme, es gäbe ein Code-Wort $z \in B_e(x) \cap B_e(y)$, folgt dann:

$$\begin{aligned} d(x,y) &\leq d(x,z) + d(y,z) \\ &\leq 2e \\ &< d(\mathcal{C}) \\ \Rightarrow \quad x &= y \end{aligned}$$

Denn $d(\mathcal{C})$ ist der minimale Abstand zweier verschiedener Code-Wörter. □

**Definition 11.11.** Ein Code $\mathcal{C}$ heisst perfekt mit dem Grad der Fehlerkorrektur $e(\mathcal{C})$, wenn die Vereinigung aller Hamming-Bälle $Q^n$ überdecken. Das heisst

$$\bigcup_{x \in \mathcal{C}} B_e(x) = Q^n$$

Ein Code $\mathcal{C}$ heisst fast perfekt, wenn die um einen Buchstaben verkürzten Code-Wörter aus $\mathcal{C}$ einen perfekten Code $\mathcal{C}'$ mit Hamming-Abstand $d(\mathcal{C}') = d(\mathcal{C}) - 1$ bilden.

**Bemerkung 11.12.** Nach Proposition 11.10 ist die Vereinigung der Hamming-Balls eines perfekten Codes in der obigen Definition sogar disjunkt.

**Proposition 11.13.** *Für einen perfekten Code $\mathcal{C}$ mit dem Grad der Fehlerkorrektur $e(\mathcal{C})$ gilt mit $c = |\mathcal{C}|$*

$$q^n = c \cdot \sum_{i=0}^{e} \left( \begin{array}{c} n \\ i \end{array} \right) \cdot (q-1)^i$$

**Korollar 11.14.** *In einem perfekten Code $\mathcal{C}$ mit dem Grad der Fehlerkorrektur $e(\mathcal{C})$ gibt es zu jedem $x \in Q^n$ ein Code-Wort $y \in \mathcal{C}$ mit dem Hamming-Abstand $d(x,y) \leq e$.*

Nach diesen Vorbereitungen kann nun gezeigt werden, dass das Witt-Design $W_{24}$ als Code interpretiert werden kann. Der Schweizer Elektroingenieur Marcel Jules Edouard

Golay fand diesen nach ihm benannten Code im Jahr 1949 ([Gol49]). Dieser Code wurde von der NASA bei den Voyager-Missionen benutzt, um Bilder von Jupiter und Saturn zur Erde zu schicken.

**Theorem 11.15.** *Auf dem Alphabeth $Q = \mathbb{F}_2$ gibt es bis auf Äquivalenz genau einen binären, linearen, fast perfekten Code $\mathcal{G}_{24}$ mit $2^{12} = 4\,096$ Code-Wörtern der Länge 24 und dem Hamming-Abstand $d(\mathcal{G}_{28}) = 8$.*

*Dieser Code heisst erweiterter binärer Golay-Code.*

**Bemerkung 11.16.** Der um ein Bit verkürzte erweiterte binäre Golay-Code ist perfekt und wird einfach binärer Golay-Code $\mathcal{G}_{23}$ genannt.

**Proposition 11.17.** *Der Grad der Fehlerkorrektur des erweiterten binären Golay-Codes $\mathcal{G}_{24}$ ist*

$$e(\mathcal{G}_{24}) = 3$$

**Proposition 11.18.** *Das Gewicht eines Code-Wortes $x \in \mathcal{G}_{24}$ ist durch 4 teilbar.*

*Das Gewichtspolynom des erweiterten binären Golay-Codes ist*

$$w_t(\mathcal{G}_{24}) = 1 + 759 \cdot t^8 + 2\,576 \cdot t^{12} + 759 \cdot t^{16} + t^{24}$$

**Proposition 11.19.** *Die 759 Code-Wörter mit Gewicht 8 im erweiterten binären Golay-Codes $\mathcal{G}_{24}$ sind isomorph zum Witt-Design $W_{24}$.*

$$\{\, x \in \mathcal{G}_{24} \,|\, w(x) = 8 \,\} \cong W_{24}$$

**Proposition 11.20.** *Die Automorphismengruppe des erweiterten binären Golay-Codes $\mathcal{G}_{24}$ ist die Mathieu-Gruppe $M_{24}$.*

# A. Folgerung des Satzes von Wedderburn in der Projektiven Geometrie

Der Satz von Wedderburn besagt, dass es keine echten, endlichen Schiefkörper gibt. Dies hat eine interessante Folgerung auf endliche projektive Ebenen. Wir geben hier zwei unterschiedliche Definitionen für projektive Ebenen. Die erste geht von einem Körper oder Schiefkörper aus.

**Definition A.1.** Sei $K$ ein Schiefkörper, $K^3$ ein Vektorraum der Dimension 3 über $K$ und $\sim$ die Äquivalenzrelation auf $K^3$, bei der zwei Vektoren $x, y \in K^3$ äquivalent sind, wenn sie sich nur um einen Faktor $0 \neq \lambda \in K$ unterscheiden.

$$x \sim y \;\Leftrightarrow\; y = \lambda \cdot x$$

Dann bilden die Äquivalenklassen die projektive Ebene $KP^2$ über dem Schiefkörper $K$.

$$KP^2 = K^3 / \sim$$

Die zweite, synthetische Definition stellt Bedingungen für die Punkte und Geraden einer projektiven Ebene auf.

**Definition A.2.** Sei $P$ eine Menge von Punkten und $L$ eine Menge von Geraden mit einer Inzidenz-Relation $I \subseteq P \times L$ so gegeben, dass

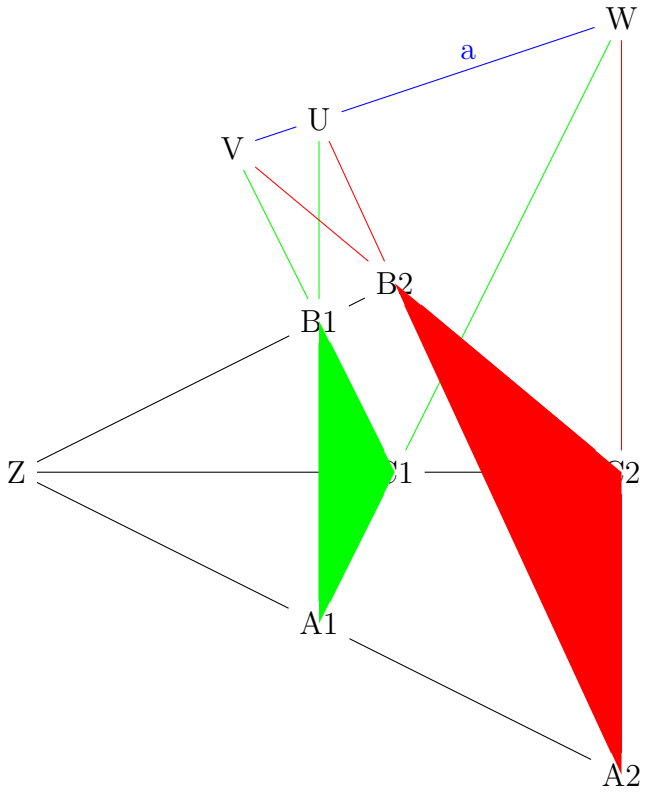
(i) Zu je zwei verschiedenen Punkten gibt es genau eine Gerade, die mit beiden inzidiert.

(ii) Zu je zwei verschiedenen Geraden gibt es genau einen Punkt, der mit beiden inzidiert.

(iii) Es gibt vier Punkte, von denen keine drei mit derselben Geraden inzidieren.

Dann heißt $(P, L, I)$ projektive Ebene.

**Definition A.3.** Eine projektive Ebene erfüllt die Schließungsfigur von Desargues oder ist desarguessch, wenn sich die Geraden durch zwei sich entsprechende Eckpunkte zweier Dreiecke $A_1B_1C_1$ und $A_2B_2C_2$ in einem Zentrum $Z$ schneiden und die sich entsprechenden verlängerten Seiten sich jeweils in Punkten $U, V, W$ schneiden und diese drei Punkte auf einer Geraden $a$ liegen.

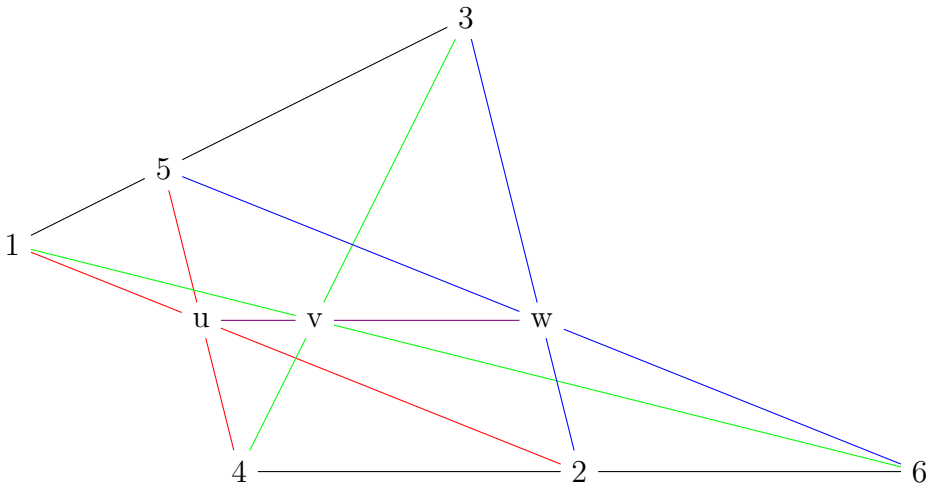



**Theorem A.4.** *Zu jeder projektiven, desarguesschen Ebene* $(P, L, I)$ *gibt es einen Schiefkörper* $K$*, dessen projektive Ebene* $KP^2$ *mit* $(P, L, I)$ *übereinstimmt.*

*Umgekehrt ist jede projektive Ebene über einem Schiefkörper desarguessch.*

Nun gibt es noch eine zweite, wichtige Schließungsfigur in projektiven Ebenen. Diese geht auf den griechischen Mathematiker Pappos von Alexandria zurück.

**Definition A.5.** Wenn bei einem Sechseck, dessen Ecken abwechselnd auf zwei verschiedenen Geraden liegen, die Schnittpunkte der Gegenseiten kollinear sind, dann erfüllt die projektive Ebene die Schließungsfigur von Pappos. Die projektive Ebene ist dann pappossch.




**Theorem A.6.** *Zu jeder projektiven, papposschen Ebene* $(P, L, I)$ *gibt es einen Körper* $K$*, dessen projektive Ebene* $KP^2$ *mit* $(P, L, I)$ *übereinstimmt.*

*Umgekehrt ist jede projektive Ebene über einem Körper pappossch.*

**Theorem A.7.** *Jede projektive, pappossche Ebene ist desarguessch.*

Mit dem Satz vonWedderburn 3.34 erhalten wir für endliche, projektive Ebenen folgende interessante Umkehrung.

**Korollar A.8.** *Jede endliche, projektive, desarguessche Ebene ist pappossch.*

Ein geometrischer Beweis für diese Aussage ist bis jetzt nicht gefunden worden.

# Literaturverzeichnis

[BJL99] Thomas Beth, Deiter Jungnickel, and Hanfried Lenz. *Design Theory: Volume 1.* Cambridge University Press, 1999.

[Bur00] W Burnside. On some properties of groups of odd order. *Proceedings of the London Mathematical Society*, 1(1):162–184, 1900.

[Bur09] William Burnside. Theory of groups of finite order. *Messenger of Mathematics*, 23:112, 1909.

[Cam99] Peter J Cameron. *Permutation groups*. Cambridge University Press, 1999.

[Car31] Robert Daniel Carmichael. Tactical configurations of rank two. *American Journal of Mathematics*, 53(1):217–240, 1931.

[CVLC91] Peter Jephson Cameron, Jacobus Hendricus Van Lint, and Peter J Cameron. *Designs, graphs, codes and their links*, volume 3. Cambridge University Press Cambridge, 1991.

[dJ21] Theodorus de Jong. *Gruppentheorie*. Vorlesung JGU Mainz, 2021.

[DM96] John D Dixon and Brian Mortimer. *Permutation groups*, volume 163. Springer Science & Business Media, 1996.

[DW67] Van Der Waerden. *Algebra II*. Springer-Verlag Berlin/Heidelberg/New York, 1967.

[Fin47] Nathan J Fine. Binomial coefficients modulo a prime. *The American Mathematical Monthly*, 54(10):589–592, 1947.

[Fru39] Robert Frucht. Herstellung von graphen mit vorgegebener abstrakter gruppe. *Compositio Mathematica*, 6:239–250, 1939.

[Gol49] Marcel JE Golay. Notes on digital coding. *Proc. IEEE*, 37:657, 1949.

[Höl95] Otto Hölder. Bildung zusammengesetzter gruppen. *Mathematische Annalen*, 46(3):321–422, 1895.

[Joh71] David Lawrence Johnson. Minimal permutation representations of finite groups. *American Journal of Mathematics*, 93(4):857–866, 1971.

[JW13] Wolfram Jehne and Herbert Wingen. *Eine mathematische Theorie der Sudokus*. Walter de Gruyter, 2013.

[Rot12] Joseph J Rotman. *An introduction to the theory of groups*, volume 148. Springer Science & Business Media, 2012.

[Sch80] Hermann Schaal. *Lineare Algebra und Analytische Geometrie I und II*. Vieweg, Braunschweig, 1980.

[VL98] Jacobus Hendricus Van Lint. *Introduction to coding theory*, volume 86. Springer Science & Business Media, 1998.

[Wit38] Ernst Witt. Über steinersche systeme. *Abh. Math. Sem. Univ. Hamburg*, 12(1938):265–275, 1938.