1 Operationen auf Mengen

Symmetrien, d. h. strukturerhaltende Bijektionen eines Objekts Ω, spielen in vielen Naturwissenschaften eine Rolle. Beispielsweise interessiert man sich in der Chemie für die Isometrien des euklidischen Raums, die die Atomanordnung eines Moleküls nicht verändern. Im einfachsten Fall ist Ω eine Menge ohne weitere Struktur. Die Symmetrien bilden dann die symmetrische Gruppe auf Ω, deren wichtigsten Eigenschaften wir im ersten Abschnitt vorstellen. Mittels Gruppenoperationen realisieren wir anschließend jede abstrakte Gruppe als Permutationsgruppe, d. h. als Untergruppe einer symmetrischen Gruppe (Satz von Cayley). Dies ermöglicht in vielen Fällen effiziente Berechnungen zum Beispiel mit Computer. Als nützliches Hilfsmittel beweisen wir die Bahnengleichung. Nachdem wir eine Reihe prominenter Operationen wie Linksmultiplikation oder Konjugation kennen gelernt haben, geben wir im zweiten Abschnitt einige interessante Anwendungen. Von fundamentaler Bedeutung sind hierbei Burnsides Lemma und die Sätze von Cauchy und Sylow über die Existenz und Eindeutigkeit von p-Untergruppen, wobei p eine Primzahl ist. Wir überlegen uns außerdem wie man jede Operation bis auf Isomorphie durch eine Auswahl an gewissen Untergruppen charakterisieren kann. Im dritten Abschnitt zerlegen wir eine vorgegebene Permutationsgruppe in ihre primitiven Bestandteile. Diese primitiven Bestandteile stehen in Korrespondenz zu den maximalen Untergruppen.

Sofern nichts Gegenteiliges gesagt wird, sind unsere Gruppen immer endlich. Insbesondere sei G stets eine endliche Gruppe mit neutralem Element 1. Außerdem sei Ω stets eine nichtleere, endliche Menge. Die Menge der natürlichen Zahlen $\mathbb{N} = \{1, 2, \ldots\}$ enthalte nicht die 0.

1.1 Symmetrische Gruppen

Definition 1.1.

(i) Die Menge aller Bijektionen auf Ω bildet die *symmetrische Gruppe* $\mathrm{Sym}(\Omega)$ bzgl. Komposition von Abbildungen. Im Fall $\Omega = \{1, \ldots, n\}$ für $n \in \mathbb{N}$ setzt man $S_n := \mathrm{Sym}(\Omega)$. Im Allgemeinen ist offenbar $\mathrm{Sym}(\Omega) \cong S_{|\Omega|}$ und $|\mathrm{Sym}(\Omega)| = |\Omega|!$.

(ii) Die Elemente von $\mathrm{Sym}(\Omega)$ nennt man *Permutationen*. Eine Permutation $\sigma \in \mathrm{Sym}(\Omega)$ lässt sich als Matrix der Form

$$\begin{pmatrix} \cdots & \omega & \cdots \\ \cdots & \sigma(\omega) & \cdots \end{pmatrix} \qquad (\omega \in \Omega)$$

B. Sambale, *Endliche Permutationsgruppen*, DOI 10.1007/978-3-658-17597-9_2

angeben. Man nennt σ einen *k-Zyklus* (oder Zyklus der *Länge* k), falls paarweise verschiedene $\omega_1, \ldots, \omega_k \in \Omega$ existieren, sodass $\sigma(\omega_i) = \omega_{i+1}$ für $i = 1, \ldots, k-1$, $\sigma(\omega_k) = \omega_1$ und $\sigma(\alpha) = \alpha$ für alle $\alpha \in \Omega \setminus \{\omega_1, \ldots, \omega_k\}$ gilt. Man schreibt dann $\sigma = (\omega_1, \ldots, \omega_k)$. Diese Darstellung ist eindeutig bis auf „Rotation", d. h.

$$\sigma = (\omega_2, \ldots, \omega_k, \omega_1) = \ldots = (\omega_k, \omega_1, \ldots, \omega_{k-1}).$$

Zyklen der Länge 2 heißen *Transpositionen*. Jede Transposition ist eine *Involution*, d. h. ein Element der Ordnung 2.

(iii) Zyklen $\sigma = (\omega_1, \ldots, \omega_k)$ und $\tau = (\alpha_1, \ldots, \alpha_l)$ heißen *disjunkt*, falls

$$\{\omega_1, \ldots, \omega_k\} \cap \{\alpha_1, \ldots, \alpha_l\} = \varnothing.$$

Offenbar ist dann $\sigma\tau = \tau\sigma$. Im Allgemeinen lässt sich jede Permutation σ als Produkt paarweise disjunkter Zyklen $\sigma = \sigma_1 \ldots \sigma_s$ schreiben. Dabei sind die Zyklen σ_i bis auf Rotation und Reihenfolge eindeutig. Zyklen der Länge 1 (d. h. *Fixpunkte* von σ) lässt man in dieser Darstellung oft weg. Hat σ_i Länge l_i, so hat σ *Zyklentyp* $(l_1, \ldots, l_s)$, wobei wir $l_1 \geq \ldots \geq l_s$ annehmen. Gleiche Längen $l_1 = \ldots = l_t$ fassen wir gelegentlich in der Form l_1^t zusammen. Es gilt

$$\boxed{|\langle\sigma\rangle| = \mathrm{kgV}(l_1, \ldots, l_s).}$$

Satz 1.2. *Es existiert ein Homomorphismus* $\mathrm{sgn} : \mathrm{Sym}(\Omega) \to \{\pm 1\}$ *mit*

$$\boxed{\mathrm{sgn}(\sigma) = l_1 + \ldots + l_s - s}$$

für $\sigma \in \mathrm{Sym}(\Omega)$ *mit Zyklentyp* $(l_1, \ldots, l_s)$. *Man nennt* sgn Signum (*oder* Signatur).

Beweis. Da der Isomorphismus $\mathrm{Sym}(\Omega) \cong S_{|\Omega|}$ den Zyklentyp erhält, können wir $\Omega = \{1, \ldots, n\}$ annehmen. Wir definieren

$$\mathrm{sgn}(\sigma) := \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

für $\sigma \in S_n$. Für $\sigma, \tau \in S_n$ gilt dann

$$\begin{aligned}
\mathrm{sgn}(\sigma\tau) &= \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j - i} \\
&= \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \frac{\tau(j) - \tau(i)}{j - i} \\
&= \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \prod_{1 \leq i < j \leq n} \frac{\tau(j) - \tau(i)}{j - i} = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau).
\end{aligned}$$

Also ist sgn ein Homomorphismus. Für jede Transposition σ gilt offenbar $\mathrm{sgn}(\sigma) = -1$. Da sich jeder k-Zyklus $\sigma = (a_1, \ldots, a_k)$ als Produkt von Transpositionen $\sigma = (a_1, a_2)(a_2, a_3) \ldots (a_{k-1}, a_k)$ schreiben lässt, gilt $\mathrm{sgn}(\sigma) = (-1)^{k-1}$. Daraus folgt die Behauptung. $\square$

Bemerkung 1.3. Der Kern von sgn ist die *alternierende Gruppe* $\mathrm{Alt}(\Omega) \trianglelefteq \mathrm{Sym}(\Omega)$. Nach dem Homomorphiesatz gilt $|\mathrm{Sym}(\Omega) : \mathrm{Alt}(\Omega)| = 2$, falls $|\Omega| \ge 2$. Analog zu S_n definiert man A_n. Die Elemente in A_n (bzw. $S_n \setminus A_n$) heißen *gerade* (bzw. *ungerade*) Permutationen.

Definition 1.4. Eine *Operation* (seltener auch *Wirkung*, engl. action) von G auf Ω ist ein Homomorphismus $f : G \to \mathrm{Sym}(\Omega)$. Man sagt auch: G *operiert* auf Ω oder Ω ist eine *G-Menge*. Wir schreiben

$$\boxed{{}^g\omega := (f(g))(\omega) \in \Omega}$$

für $g \in G$ und $\omega \in \Omega$. Die Zahl $|\Omega|$ ist der *Grad* von f. Sofern die Operation im Kontext klar ist, werden wir im Folgenden Eigenschaften von Operationen auch den entsprechenden Gruppen zuordnen (z. B. der Grad von G).

Bemerkung 1.5.

(i) Für eine Operation $f : G \to \mathrm{Sym}(\Omega)$ gilt offenbar $\boxed{{}^1\omega = \omega}$ und $\boxed{{}^g({}^h\omega) = {}^{gh}\omega}$ für $g, h \in G$ und $\omega \in \Omega$.

Seien nun umgekehrt Elemente ${}^g\omega \in \Omega$ für $g \in G$ und $\omega \in \Omega$ gegeben, sodass ${}^1\omega = \omega$ und ${}^g({}^h\omega) = {}^{gh}\omega$ gilt. Aus ${}^g\alpha = {}^g\beta$ $(\alpha, \beta \in \Omega)$ folgt dann

$$\alpha = {}^1\alpha = {}^{g^{-1}g}\alpha = {}^{g^{-1}}({}^g\alpha) = {}^{g^{-1}}({}^g\beta) = \beta.$$

Also ist $f_g : \Omega \to \Omega$, $\omega \mapsto {}^g\omega$ eine Bijektion. Wegen $f_{gh}(\omega) = {}^{gh}\omega = {}^g({}^h\omega) = (f_g \circ f_h)(\omega)$ für $g, h \in G$ und $\omega \in \Omega$ ist $f : G \to \mathrm{Sym}(\Omega)$, $g \mapsto f_g$ ein Homomorphismus (also eine Operation).

(ii) In vielen Büchern werden Abbildungen von rechts angewendet. Man schreibt dann ω^g statt ${}^g\omega$.

Beispiel 1.6.

(i) Es existiert stets die *triviale* Operation $G \to \mathrm{Sym}(\Omega)$ mit $g \mapsto \mathrm{id}_\Omega$ für alle $g \in G$.

(ii) Für $G \le \mathrm{Sym}(\Omega)$ liefert die Inklusionsabbildung $G \hookrightarrow \mathrm{Sym}(\Omega)$ eine *natürliche* Operation.

Definition 1.7. Eine Operation $f : G \to \mathrm{Sym}(\Omega)$ heißt *treu*, falls f injektiv ist. In diesem Fall ist G also zu einer Untergruppe von $\mathrm{Sym}(\Omega)$ isomorph. Man sagt dann: G ist eine *Permutationsgruppe* auf Ω.

Satz 1.8 (Cayley). *Jede Gruppe G ist eine Permutationsgruppe auf sich selbst. Insbesondere ist G zu einer Untergruppe von $S_{|G|}$ isomorph.*

Beweis. Für $g, x \in G$ sei ${}^gx := gx$. Dann ist ${}^1x = x$ und ${}^{gh}x = (gh)x = g(hx) = {}^g({}^hx)$ für $g, h, x \in G$. Nach Bemerkung 1.5 operiert G also auf sich selbst durch Multiplikation von links. Operiert $g \in G$ trivial, so ist $g = {}^g1 = 1$. Daher ist die Operation treu. $\square$

Bemerkung 1.9.

(i) Im Allgemeinen kann man jede Operation $f : G \to \mathrm{Sym}(\Omega)$ in eine treue Operation $\overline{f} : G/\mathrm{Ker}(f) \to \mathrm{Sym}(\Omega)$, $g\mathrm{Ker}(f) \mapsto f(g)$ umwandeln. Wir werden uns daher oft auf Permutationsgruppen beschränken.

(ii) Aus historischer Sicht gab es zuerst Permutationsgruppen, bevor Cayley 1854 die abstrakten Gruppenaxiome einführte.

Definition 1.10. Für eine Operation $f : G \to \mathrm{Sym}(\Omega)$ ist

$$\alpha \sim \beta :\Longleftrightarrow \exists\, g \in G : {}^g\alpha = \beta \qquad\qquad (\alpha, \beta \in \Omega)$$

offenbar eine Äquivalenzrelation auf Ω.

(i) Die Äquivalenzklassen heißen *Bahnen* (engl. orbits) von f.

(ii) Mit ${}^G\omega := \{{}^g\omega : g \in G\}$ wird die Bahn bezeichnet, die $\omega \in \Omega$ enthält. Dabei ist $|{}^G\omega|$ die *Länge* der Bahn.

(iii) Gibt es nur eine Bahn, so ist f *transitiv*, d. h. für je zwei Elemente $\alpha, \beta \in \Omega$ existiert ein $g \in G$ mit ${}^g\alpha = \beta$. Anderenfalls ist f *intransitiv.*

(iv) Für $\omega \in \Omega$ ist $\boxed{G_\omega := \{g \in G : {}^g\omega = \omega\} \le G}$ der *Stabilisator* von ω.

Beispiel 1.11.

(i) Die Zyklen von $\sigma \in S_n$ entsprechen genau den Bahnen von $\langle\sigma\rangle$.

(ii) Sei $H \le G$. Dann operiert H auf G durch Multiplikation von rechts, d. h. ${}^hx := xh^{-1}$ für $h \in H$ und $x \in G$. Die Bahnen sind dabei die Linksnebenklassen $xH \in G/H$. Außerdem operiert G transitiv auf G/H durch ${}^g(xH) := gxH$ für $g, x \in G$ (im Fall $H = 1$ ist dies die Operation aus Satz 1.8).

(iii) Jede Gruppe G operiert auf sich selbst durch *Konjugation*, d. h. ${}^gx := gxg^{-1}$ für $g, x \in G$. Die Bahnen sind dabei die *Konjugationsklassen* von G und der Stabilisator von $x \in G$ ist der *Zentralisator*

$$\mathrm{C}_G(x) := \{g \in G : gx = xg\}.$$

Die Anzahl aller Konjugationsklassen ist die *Klassenzahl* $k(G)$ von G. Zwei Elemente in der gleichen Konjugationsklasse heißen *konjugiert.* Der Kern der Operation ist das *Zentrum*

$$\mathrm{Z}(G) := \bigcap_{x \in G} \mathrm{C}_G(x) = \{g \in G : gx = xg \ \forall x \in G\}$$

von G und das Bild ist die *innere Automorphismengruppe* $\mathrm{Inn}(G)$ von G. Insbesondere ist

$$G/\mathrm{Z}(G) \cong \mathrm{Inn}(G) \le \mathrm{Aut}(G) \le \mathrm{Sym}(G).$$

Für $\alpha \in \mathrm{Aut}(G)$ und $g, x \in G$ gilt $\alpha({}^g x) = {}^{\alpha(g)}\alpha(x)$. Dies zeigt $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. Die Faktorgruppe $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$ heißt *äußere Automorphismengruppe* von G.

Ist konkret $G = S_n$ und $x = (\alpha, \beta, \ldots) \in G$ ein Zyklus, so ist ${}^g x = gxg^{-1} = ({}^g\alpha, {}^g\beta, \ldots)$ für $g \in G$. Die Konjugationsklassen von S_n sind also genau die Mengen von Permutationen mit gleichem Zyklentyp. Somit ist $k(S_n)$ die Anzahl der Partitionen von n.

(iv) Jede Gruppe G operiert auf der Menge ihrer Untergruppen durch Konjugation, d. h. ${}^g X := gXg^{-1} = \{gxg^{-1} : x \in X\}$ für $g \in G$ und $X \le G$. Die Bahnen heißen dabei wieder Konjugationsklassen und der Stabilisator von $X \le G$ ist der *Normalisator*

$$\mathrm{N}_G(X) := \{g \in G : gX = Xg\}.$$

Die Bahnen der Länge 1 entsprechen den Normalteilern von G. Sicher operiert $\mathrm{N}_G(X)$ durch Konjugation auf X mit Kern $\mathrm{C}_G(X) := \bigcap_{x \in X} \mathrm{C}_G(x)$. Insbesondere ist $\mathrm{N}_G(X)/\mathrm{C}_G(X)$ zu einer Untergruppe von $\mathrm{Aut}(X)$ isomorph. Für $H \le G$ schreiben wir $\mathrm{N}_H(X) := \mathrm{N}_G(X) \cap H$ und $\mathrm{C}_H(X) := \mathrm{C}_G(X) \cap H$, selbst wenn X nicht in H liegt.

(v) Seien $H, K \le G$. Dann operiert $H \times K$ auf G via ${}^{(h,k)}x := hxk^{-1}$ für $(h, k) \in H \times K$ und $x \in G$. Die Bahnen haben die Form HxK und heißen *Doppelnebenklassen*. Wir setzen $H\backslash G/K := \{HxK : x \in G\}$. Für $x \in G$ gilt

$$|HxK| = |HxKx^{-1}| = |H : H \cap xKx^{-1}||xKx^{-1}| = |H : H \cap xKx^{-1}||K|.$$

Bemerkung 1.12.

(i) Für $g \in G$ und $\omega \in \Omega$ ist $\boxed{G_{{}^g\omega} = gG_\omega g^{-1},}$ denn

$$G_{{}^g\omega} = \{x \in G : {}^{xg}\omega = {}^g\omega\} = \{x \in G : g^{-1}xg \in G_\omega\} = gG_\omega g^{-1}.$$

Insbesondere gilt $\mathrm{C}_G(gxg^{-1}) = g\mathrm{C}_G(x)g^{-1}$, $\mathrm{C}_G(gXg^{-1}) = g\mathrm{C}_G(X)g^{-1}$ und $\mathrm{N}_G(gXg^{-1}) = g\mathrm{N}_G(X)g^{-1}$ für $g, x \in G$ und $X \le G$.

(ii) Ist Δ eine Bahn der Operation $G \to \mathrm{Sym}(\Omega)$, so erhält man durch Einschränken eine transitive Operation $G \to \mathrm{Sym}(\Delta)$ mit Kern

$$\boxed{G_\Delta := \bigcap_{\delta \in \Delta} G_\delta \trianglelefteq G.}$$

Insbesondere ist G/G_Δ eine transitive Permutationsgruppe. Wir schreiben auch $G_{\delta_1 \ldots \delta_k}$ anstelle von $G_{\{\delta_1, \ldots, \delta_k\}}$. Ist Δ keine Bahn von G, so kann man die Überlegungen auf $\boxed{G_{(\Delta)} := \{g \in G : {}^g\Delta = \Delta\} \le G}$ anwenden.

(iii) Sei G eine Permutationsgruppe auf Ω mit Bahnen $\Delta_1, \ldots, \Delta_s$. Dann ist die Abbildung

$$G \to \bigtimes_{i=1}^{s} G/G_{\Delta_i},$$
$$g \mapsto (gG_{\Delta_1}, \ldots, gG_{\Delta_s})$$

ein Monomorphismus, denn $\bigcap_{i=1}^s G_{\Delta_i} = G_\Omega = 1$. Insbesondere ist G zu einer Untergruppe von $\bigtimes_{i=1}^s G/G_{\Delta_i}$ isomorph. Die transitiven Permutationsgruppen verdienen daher besondere Beachtung.

Satz 1.13. *Für eine Operation von G auf Ω und $\omega \in \Omega$ ist* $\boxed{|{}^G\omega| = |G : G_\omega|.}$ *Ist $\omega_1, \ldots, \omega_s \in \Omega$ ein Repräsentantensystem für die Bahnen von G, so gilt*

$$\boxed{|\Omega| = \sum_{i=1}^s |G : G_{\omega_i}|.} \qquad \text{(Bahnengleichung)}$$

Beweis. Für die erste Aussage genügt es zu zeigen, dass die Abbildung $f : G/G_\omega \to {}^G\omega$, $gG_\omega \mapsto {}^g\omega$ wohldefiniert und bijektiv ist. Für $g, h \in G$ gilt

$$gG_\omega = hG_\omega \iff h^{-1}g \in G_\omega \iff {}^{h^{-1}g}\omega = \omega \iff {}^h\omega = {}^g\omega.$$

Dies zeigt, dass f wohldefiniert und injektiv ist. Die Surjektivität ist trivial. Die letzte Aussage folgt, da Ω die disjunkte Vereinigung der Bahnen ist. □

Beispiel 1.14.

(i) Sind $x_1, \ldots, x_s \in G$ Repräsentanten für die Konjugationsklassen von G mit $x_1, \ldots, x_r \in \mathrm{Z}(G)$ und $x_{r+1}, \ldots, x_s \notin \mathrm{Z}(G)$, so erhält man

$$\boxed{|G| = \sum_{i=1}^s |G : \mathrm{C}_G(x_i)| = |\mathrm{Z}(G)| + \sum_{i=r+1}^s |G : \mathrm{C}_G(x_i)|} \qquad \text{(Klassengleichung)}$$

aus Beispiel 1.11. Dies zeigt zum Beispiel, dass jede nicht-triviale p-Gruppe ein nicht-triviales Zentrum besitzt (betrachte die Klassengleichung modulo p).

(ii) Für eine transitive Operation gilt $|\Omega| = |G : G_\omega|$ für alle $\omega \in \Omega$. Nach Lagrange ist insbesondere $\boxed{|\Omega| \mid |G|.}$

1.2 Anwendungen

Satz 1.15 („Burnsides Lemma“). *Sei s die Anzahl der Bahnen einer Operation $G \to \mathrm{Sym}(\Omega)$. Sei $f(g)$ die Anzahl der Fixpunkte von $g \in G$. Seien $x_1, \ldots, x_r \in G$ Repräsentanten für die Konjugationsklassen von G. Dann gilt*

$$\boxed{s = \frac{1}{|G|} \sum_{g \in G} f(g) = \sum_{i=1}^r \frac{f(x_i)}{|\mathrm{C}_G(x_i)|}.}$$

Beweis. Sei $\omega_1, \ldots, \omega_s \in \Omega$ ein Repräsentantensystem für die Bahnen von G. Nach Bemerkung 1.12 und Satz 1.13 ist

$$\begin{aligned} \sum_{g \in G} f(g) &= \bigl|\{(g, \omega) \in G \times \Omega : {}^g\omega = \omega\}\bigr| = \sum_{\omega \in \Omega} |G_\omega| \\ &= \sum_{i=1}^s |{}^G\omega_i||G_{\omega_i}| = \sum_{i=1}^s |G : G_{\omega_i}||G_{\omega_i}| = |G|s. \end{aligned}$$

Ist $\Delta \subseteq \Omega$ die Menge der Fixpunkte von $g \in G$, so ist ${}^h\Delta := \{{}^h\delta : \delta \in \Delta\}$ die Menge der Fixpunkte von hgh^{-1} für $h \in G$. Insbesondere gilt $f(g) = f(hgh^{-1})$. Die zweite Gleichheit folgt nun aus der Klassengleichung. $\square$

Bemerkung 1.16.

(i) Satz 1.15 wurde vor Burnside bereits von Frobenius bewiesen. Da viele Sätze in der Gruppentheorie nach Burnside benannt sind, wird die Aussage in Satz 1.15 auch scherzhaft als „Not Burnside's Lemma" bezeichnet (siehe [281]).

(ii) Satz 1.15 ist besonders dann nützlich, wenn Ω zu groß ist, um die Bahnen direkt zu zählen. In den Aufgaben und späteren Kapiteln werden wir zahlreiche Anwendungen besprechen.

(iii) Die Funktion f in Satz 1.15 ist der *Permutationscharakter* der Operation.

Satz 1.17 (Cauchy)**.** *Für jeden Primteiler p von $|G|$ besitzt G ein Element der Ordnung p.*

Beweis (McKay)*.* Sei

$$\Omega := \bigl\{(x_1, \ldots, x_p) \in G^p : x_1 \ldots x_p = 1\bigr\}.$$

Für jedes Tupel $(x_1, \ldots, x_{p-1}) \in G^{p-1}$ existiert genau ein $x_p \in G$ mit $x_1 \ldots x_p = 1$. Also ist $|\Omega| = |G|^{p-1} \equiv 0 \pmod p$. Aus $x_1 \ldots x_p = 1$ folgt $x_2 \ldots x_p = x_1^{-1}$ und $x_2 \ldots x_p x_1 = 1$. Dies zeigt, dass $\mathbb{Z}/p\mathbb{Z}$ durch

$$^{(k+p\mathbb{Z})}(x_1, \ldots, x_p) := (x_{1+k}, \ldots, x_{p+k})$$

auf Ω operiert, wobei die Indizes modulo p zu lesen sind. Sicher ist $(1, \ldots, 1) \in \Omega$ ein Fixpunkt von $\mathbb{Z}/p\mathbb{Z}$. Nach der Bahnengleichung (modulo p) muss $\mathbb{Z}/p\mathbb{Z}$ mindestens einen weiteren Fixpunkt $(x_1, \ldots, x_p) \in \Omega$ haben. Dann ist $1 \neq x_1 = \ldots = x_p$ und $x_1^p = 1$. $\square$

Satz 1.18 (Sylow)**.** *Sei $|G| = p^a m$ für eine Primzahl $p \nmid m$. Dann existiert eine p-*Sylowgruppe *P von G, d. h. $|P| = p^a$. Wir schreiben $P \in \mathrm{Syl}_p(G)$. Jede p-Untergruppe von G ist zu einer Untergruppe von P konjugiert. Außerdem gilt*

$$\boxed{|\mathrm{Syl}_p(G)| = |G : \mathrm{N}_G(P)| \equiv 1 \pmod p.}$$

Beweis (Frobenius)*.* Wir zeigen die Existenz von P durch Induktion nach $|G|$. Im Fall $m = 1$ können wir $P = G$ setzen. Sei also $m > 1$. Nehmen wir zunächst an, dass $|\mathrm{Z}(G)|$ durch p teilbar ist. Nach Cauchy existiert dann ein $z \in \mathrm{Z}(G)$ der Ordnung p. Nach Induktion besitzt $G/\langle z\rangle$ eine p-Sylowgruppe $P/\langle z\rangle$. Wegen $|G : P| = |G/\langle z\rangle : P/\langle z\rangle|$ ist dann $P \in \mathrm{Syl}_p(G)$.

Sei nun $|\mathrm{Z}(G)| \not\equiv 0 \pmod p$. Die Klassengleichung liefert ein $x \in G \setminus \mathrm{Z}(G)$ mit $p \nmid |G : \mathrm{C}_G(x)|$. Wegen $x \notin \mathrm{Z}(G)$ ist $\mathrm{C}_G(x) < G$ und nach Induktion existiert $P \in \mathrm{Syl}_p(\mathrm{C}_G(x))$. Offenbar ist dann auch $P \in \mathrm{Syl}_p(G)$.

Sei nun $U \leq G$ eine p-Untergruppe. Die Bahnenlängen der Operation von U auf G/P durch Linksmultiplikation sind dann Teiler von $|U|$, also p-Potenzen. Wegen

$p \nmid m = |G : P|$ existiert ein Fixpunkt $xP \in G/P$ von U, d. h. $Ux \subseteq UxP = xP$ und $x^{-1}Ux \leq P$. Dies zeigt die zweite Behauptung. Insbesondere ist jede p-Sylowgruppe von G zu P konjugiert und $|\mathrm{Syl}_p(G)| = |G : \mathrm{N}_G(P)|$.

Für die letzte Behauptung zählen wir die Fixpunkte von P auf G/P. Es gilt $Px \subseteq PxP = xP$ genau dann, wenn $x \in \mathrm{N}_G(P)$. Die Bahnengleichung liefert

$$|G : \mathrm{N}_G(P)||\mathrm{N}_G(P) : P| = |G : P| \equiv |\mathrm{N}_G(P) : P| \not\equiv 0 \pmod p$$

und $|G : \mathrm{N}_G(P)| \equiv 1 \pmod p$. □

Satz 1.19 („Frattini-Argument“). *Sei $G \to \mathrm{Sym}(\Omega)$ eine Operation und $H \leq G$ eine transitive Untergruppe. Dann ist $G = HG_\omega$ für alle $\omega \in \Omega$.*

Beweis. Sei $g \in G$ beliebig. Dann existiert ein $h \in H$ mit ${}^g\omega = {}^h\omega$. Also ist $g = h(h^{-1}g) \in HG_\omega$. □

Beispiel 1.20. Sei $N \trianglelefteq G$ und $P \in \mathrm{Syl}_p(N)$. Dann operiert G auf $\mathrm{Syl}_p(N)$ durch Konjugation und Satz 1.19 liefert $G = N\mathrm{N}_G(P)$.

Definition 1.21. Zwei Operationen $G \to \mathrm{Sym}(\Omega)$ und $G \to \mathrm{Sym}(\Omega')$ sind *isomorph* (oder *ähnlich*), falls es eine Bijektion $\varphi : \Omega \to \Omega'$ und ein $\alpha \in \mathrm{Aut}(G)$ mit

$$\boxed{{}^{\alpha(g)}\varphi(\omega) = \varphi({}^g\omega)}$$

für $g \in G$ und $\omega \in \Omega$ gibt. Gegebenenfalls sind Ω und Ω' *isomorphe G-Mengen* und wir schreiben $\Omega \cong \Omega'$. In den Anwendungen ist oft $\alpha = \mathrm{id}_G$.

Bemerkung 1.22. Wie üblich haben zwei isomorphe Operationen die gleichen Eigenschaften (trivial, treu, transitiv, ...). Man interessiert sich daher in der Regel nur für Operationen bis auf Isomorphie.

Beispiel 1.23. Für G-Mengen Ω, Δ und Γ ist offenbar auch die disjunkte Vereinigung $\Omega \sqcup \Delta$ eine G-Menge. Via ${}^g(\omega, \delta) := ({}^g\omega, {}^g\delta)$ wird auch $\Omega \times \Delta$ zu einer G-Menge. Dabei gilt offenbar

$$\Omega \times \Delta \cong \Delta \times \Omega,$$
$$\Omega \times (\Delta \sqcup \Gamma) \cong (\Omega \times \Delta) \sqcup (\Omega \times \Gamma).$$

Satz 1.24. *Sei $\omega_1, \ldots, \omega_s$ ein Repräsentantensystem für die Bahnen einer Operation $f : G \to \mathrm{Sym}(\Omega)$. Dann ist f isomorph zu der Operation von G auf $\Delta := \bigsqcup_{i=1}^s G/G_{\omega_i}$ durch Linksmultiplikation.*

Beweis. Nach Satz 1.13 ist die Abbildung $\varphi : \Delta \to \Omega$, $gG_{\omega_i} \mapsto {}^g\omega_i$ eine wohldefinierte Bijektion. Für $g \in G$ und $xG_{\omega_i} \in \Delta$ gilt außerdem ${}^g\varphi(xG_{\omega_i}) = {}^g({}^x\omega_i) = {}^{gx}\omega_i = \varphi(gxG_{\omega_i}) = \varphi({}^g(xG_{\omega_i}))$. □

Bemerkung 1.25.

(i) Man kann jede Operation von G also auch durch Angabe von Untergruppen beschreiben (je eine Untergruppe pro Bahn). Aufgabe 1.5 beschäftigt sich dabei mit der Eindeutigkeit.

(ii) Sei Ω eine G-Menge und $H \leq G$. Durch Einschränkung ist Ω auch eine H-Menge, die wir mit Ω_H bezeichnen. Wir konstruieren nun umgekehrt eine G-Menge aus einer H-Menge (siehe auch Aufgabe 1.7).

Satz 1.26. *Sei $H \leq G$ und Δ eine H-Menge. Dann existiert eine G-Menge Δ^G mit folgenden Eigenschaften:*

(i) $|\Delta^G| = |G : H||\Delta|$.

(ii) $\Delta^H \cong \Delta$.

(iii) $(\Delta \sqcup \Gamma)^G \cong \Delta^G \sqcup \Gamma^G$ *für jede H-Menge Γ.*

(iv) (Frobenius-Reziprozität) $(\Delta \times \Omega_H)^G \cong \Delta^G \times \Omega$ *für jede G-Menge Ω.*

(v) $(\Delta^K)^G \cong \Delta^G$ *für $H \leq K \leq G$.*

Man nennt Δ^G die von Δ induzierte *G-Menge.*

Beweis. Offenbar operiert H auf $G \times \Delta$ via ${}^h(g, \delta) := (gh^{-1}, {}^h\delta)$ für $h \in H$ und $(g, \delta) \in G \times \Delta$. Sei Δ^G die Menge der Bahnen von H auf $G \times \Delta$. Ist $[g, \delta] \in \Delta^G$ die Bahn von $(g, \delta) \in G \times \Delta$, so definieren wir

$$ {}^x[g, \delta] := [xg, \delta] \qquad\qquad (x \in G). $$

Dies ist offensichtlich eine wohldefinierte Operation, d. h. Δ^G ist eine G-Menge.

(i) Da die Bahnen von H auf $G \times \Delta$ alle Länge $|H|$ haben, gilt $|\Delta^G| = |G : H||\Delta|$.

(ii) Wir betrachten die Abbildung $\varphi : \Delta \to \Delta^H$, $\delta \mapsto [1, \delta]$. Für $\delta \neq \delta'$ sind $(1, \delta)$ und $(1, \delta')$ sicher nicht in der gleichen Bahn unter H. Also ist φ injektiv und wegen $|\Delta^H| = |\Delta|$ auch surjektiv. Für $h \in H$ und $\delta \in \Delta$ gilt schließlich

$$ {}^h\varphi(\delta) = {}^h[1, \delta] = [h, \delta] = [hh^{-1}, {}^h\delta] = [1, {}^h\delta] = \varphi({}^h\delta). $$

(iii) Da jede Bahn von H auf $\Delta \sqcup \Gamma$ entweder in Δ oder in Γ liegt, sind die Mengen $(\Delta \sqcup \Gamma)^G$ und $\Delta^G \sqcup \Gamma^G$ gleich und die Identität liefert einen Isomorphismus.

(iv) Wir betrachten die Abbildung

$$ \begin{aligned} \varphi : (\Delta \times \Omega_H)^G &\to \Delta^G \times \Omega, \\ [g, (\delta, \omega)] &\mapsto \big([g, \delta], {}^g\omega\big). \end{aligned} $$

Für $h \in H$ gilt

$$ \varphi\big([gh^{-1}, {}^h(\delta, \omega)]\big) = \big([gh^{-1}, {}^h\delta], {}^{gh^{-1}h}\omega\big) = \big([g, \delta], {}^g\omega\big) = \varphi\big([g, (\delta, \omega)]\big). $$

Also ist φ wohldefiniert und offenbar auch surjektiv. Wegen $|(\Delta \times \Omega_H)^G| = |G : H||\Delta||\Omega| = |\Delta^G \times \Omega|$ ist φ auch injektiv. Für $x \in G$ gilt schließlich

$$\begin{aligned} {}^x\varphi\big([g,(\delta,\omega)]\big) &= {}^x\big([g,\delta],{}^g\omega\big) = \big([xg,\delta],{}^{xg}\omega\big) \\ &= \varphi\big([xg,(\delta,\omega)]\big) = \varphi\big({}^x[g,(\delta,\omega)]\big). \end{aligned}$$

(v) Wie zuvor zeigt man leicht, dass die Abbildung

$$\begin{aligned} \varphi : (\Delta^K)^G &\to \Delta^G, \\ [g,[k,\delta]] &\mapsto [gk,\delta] \end{aligned}$$

die gewünschten Eigenschaften hat. □

1.3 Reguläre und primitive Operationen

Definition 1.27. Eine transitive Operation $G \to \mathrm{Sym}(\Omega)$ heißt *regulär*, falls $|G| = |\Omega|$ gilt.

Bemerkung 1.28. Sei $f : G \to \mathrm{Sym}(\Omega)$ regulär und sei $\omega \in \Omega$. Da f transitiv ist, gilt $|G| = |\Omega| = |G : G_\omega|$, d. h. $G_\omega = 1$. Insbesondere ist f treu. Nach Satz 1.24 ist f isomorph zu der Operation aus Satz 1.8. Man kann also von „der" regulären Operation von G sprechen.

Definition 1.29. Sei $f : G \to \mathrm{Sym}(\Omega)$ eine transitive, nicht-triviale Operation. Eine Teilmenge $\Delta \subseteq \Omega$ mit $1 < |\Delta| < |\Omega|$ heißt *Block* von f, falls für jedes $g \in G$ die Mengen ${}^g\Delta$ und Δ entweder gleich oder disjunkt sind. Existieren Blöcke, so heißt f *imprimitiv* und anderenfalls *primitiv*.

Bemerkung 1.30.

(i) Sei Δ ein Block einer Operation $G \to \mathrm{Sym}(\Omega)$ und sei $x \in G$. Dann ist sicher $|{}^x\Delta| = |\Delta|$. Für $g \in G$ gilt

$$^g({}^x\Delta) \cap {}^x\Delta = {}^{gx}\Delta \cap {}^x\Delta = {}^x({}^{x^{-1}gx}\Delta \cap \Delta) \in \{{}^x\Delta, \varnothing\}.$$

Daher ist auch ${}^x\Delta$ ein Block. Da G transitiv auf Ω operiert, ist $\mathcal{B} := \{{}^g\Delta : g \in G\}$ ein Partition von Ω. Insbesondere ist $|\Omega| = |\Delta||\mathcal{B}|$ und $\boxed{|\Delta| \mid |\Omega| \mid |G|.}$ Außerdem operiert G sicher transitiv auf $\mathcal{B}$.

(ii) Um Verwechselungen mit dem Bahnenbegriff zu vermeiden, sind Blöcke für intransitive Operationen nicht definiert.

Beispiel 1.31.

(i) Nach Bemerkung 1.30 ist jede transitive Operation mit Primzahlgrad primitiv.

(ii) Nach (i) sind die natürlichen Operationen von S_2, S_3 und A_3 primitiv. Sei nun $n \geq 4$ und $\Delta \subseteq \{1, \ldots, n\}$ mit $1 < |\Delta| < n$. Für verschiedene Elemente $\alpha, \beta \in \Delta$ existiert dann ein 3-Zyklus $g \in A_n$ mit ${}^g\alpha = \alpha$ und ${}^g\beta \in \Omega \setminus \Delta$. Also ist Δ kein Block und S_n und A_n sind primitiv.

(iii) Die *Kleinsche Vierergruppe* $V_4 := \langle (1,2)(3,4), (1,3)(2,4) \rangle$ operiert regulär und imprimitiv auf $\{1, 2, 3, 4\}$ (jede 2-elementige Teilmenge ist ein Block).

Definition 1.32. Eine echte Untergruppe $M < G$ heißt *maximal*, falls keine Untergruppe $H \leq G$ mit $M < H < G$ existiert.

Satz 1.33. *Sei $G \to \mathrm{Sym}(\Omega)$ eine transitive Operation und $\omega \in \Omega$. Dann existiert eine Bijektion zwischen der Menge der Blöcke, die ω enthalten und der Menge der Untergruppen $H \leq G$ mit $G_\omega < H < G$. Insbesondere ist G genau dann primitiv, wenn G_ω eine maximale Untergruppe ist.*

Beweis. Nach Satz 1.24 können wir $\Omega = G/G_\omega$ annehmen. Der Punkt ω entspricht dabei der trivialen Nebenklasse $1G_\omega$. Für $G_\omega < H < G$ ist H/G_ω ein Block, der $1G_\omega$ enthält, denn $1 < |H : G_\omega| < |\Omega|$ und $gH \cap H \in \{H, \varnothing\}$ für $g \in G$. Sei umgekehrt $\Delta \subseteq \Omega$ ein Block, der $1G_\omega$ enthält. Sei

$$H := \{g \in G : gG_\omega \in \Delta\} \supseteq G_\omega.$$

Für $x, y \in H$ gilt $xG_\omega = x(1G_\omega) \in \Delta \cap x\Delta$. Da Δ ein Block ist, folgt $xyG_\omega \in x\Delta = \Delta$ und $xy \in H$. Dies zeigt $H \leq G$. Offenbar ist auch $|G_\omega| < |\Delta||G_\omega| = |H| < |G|$. □

Satz 1.34. *Sei $G \to \mathrm{Sym}(\Omega)$ eine imprimitive Operation mit Block Δ, der maximal bzgl. Inklusion gewählt ist. Dann ist die Operation von G auf $\mathcal{B} := \{{}^g\Delta : g \in G\}$ primitiv.*

Beweis. Wieder dürfen wir $\Omega = G/G_\omega$ mit $\omega \in \Omega$ nach Satz 1.24 annehmen. Nach Satz 1.33 ist $\Delta = H/G_\omega$ für eine maximale Untergruppe $H < G$. Dabei ist H gerade der Stabilisator von $\Delta \in \mathcal{B}$. Die Operation von G auf $\mathcal{B}$ ist also zur Operation auf G/H isomorph. Die Behauptung folgt nun aus Satz 1.33. □

Bemerkung 1.35. Sei $G \neq 1$ eine Permutationsgruppe auf Ω. Nach Bemerkung 1.12 existiert ein Normalteiler $N \trianglelefteq G$, sodass $G/N \neq 1$ eine transitive Permutationsgruppe ist. Weiter existiert nach Satz 1.34 ein Normalteiler $M/N \trianglelefteq G/N$, sodass $(G/N)/(M/N) \cong G/M$ eine primitive Permutationsgruppe ist. Da auch M treu auf Ω operiert, kann man diesen Prozess mit M statt G wiederholen. Dies liefert eine Folge von Untergruppen

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_k = G,$$

sodass die Faktoren G_i/G_{i-1} primitive Permutationsgruppen sind. Im Gegensatz zu Kompositionsfaktoren oder Hauptfaktoren sind die Faktoren G_i/G_{i-1} aber in keiner Weise eindeutig. Wir werden später alle primitiven Permutationsgruppen klassifizieren (Satz 5.6). Zum Beispiel ist jede primitive Permutationsgruppe vom Grad 34 zu A_{34} oder S_{34} isomorph.

1.4 Aufgaben

Aufgabe 1.1. Bestimmen Sie alle transitiven Permutationsgruppen vom Grad ≤ 4 bis auf Isomorphie. Welche davon sind regulär oder primitiv?

Aufgabe 1.2. Zeigen Sie, dass jede endliche Gruppe in einer alternierenden Gruppe enthalten ist.

Aufgabe 1.3. Sei G eine abelsche, transitive Permutationsgruppe. Zeigen Sie, dass G regulär ist.

Aufgabe 1.4. Zeigen Sie, dass eine transitive Operation $G \to \mathrm{Sym}(\Omega)$ genau dann treu ist, wenn G_ω für $\omega \in \Omega$ keinen nicht-trivialen Normalteiler von G enthält.

Aufgabe 1.5. Seien $\varphi : G \to S_n$ und $\psi : G \to S_n$ zwei treue Operationen. Zeigen Sie:

(a) φ und ψ sind genau dann isomorph, falls $\varphi(G)$ und $\psi(G)$ in S_n konjugiert sind.

(b) Seien S_φ und S_ψ die Stabilisatoren von 1 bzgl. φ und ψ. Sind φ und ψ transitiv, so sind φ und ψ genau dann isomorph, wenn ein $f \in \mathrm{Aut}(G)$ mit $f(S_\varphi) = S_\psi$ existiert.

Aufgabe 1.6 (Burnside)**.** Seien Ω und Δ G-Mengen, sodass für jede Untergruppe $H \le G$ die Anzahl der Fixpunkte von H auf Ω gleich der Anzahl der Fixpunkte von H auf Δ ist. Zeigen Sie $\Omega \cong \Delta$. Gilt auch die Umkehrung?

Aufgabe 1.7. Sei $H \le G$ und Δ eine H-Menge. Zeigen Sie:

(a) Operiert H treu auf Δ, so operiert G treu auf Δ^G.

(b) Es gibt eine Bijektion F zwischen der Menge der Bahnen von H auf Δ und der Menge der Bahnen von G auf Δ^G. Dabei gilt $|F(\Gamma)| = |G : H||\Gamma|$ für jede Bahn $\Gamma \subseteq \Delta$ von H. Insbesondere ist H genau dann transitiv, wenn G transitiv ist.

(c) Operiert G primitiv auf Δ^G, so ist $H = G$ oder $|\Delta| = 1$.

(d) Für $g \in G$ operiert ${}^gH = gHg^{-1}$ auf Δ mit ${}^x\delta := {}^{g^{-1}xg}\delta$ für $x \in {}^gH$ und $\delta \in \Delta$. Wir bezeichnen die entsprechende ${}^gH$-Menge mit Δ^g.

(e) (Clifford) Sei Ω eine transitive G-Menge und $\Delta \subseteq \Omega$ eine Bahn von $N \trianglelefteq G$. Dann gilt

$$\Omega_N \cong \bigsqcup_{gG_{(\Delta)} \in G/G_{(\Delta)}} \Delta^g.$$

(f) (Mackey-Formel) Für $K \le G$ gilt

$$(\Delta^G)_K \cong \bigsqcup_{KgH \in K\backslash G/H} \big((\Delta^g)_{K\cap {}^gH}\big)^K.$$

Aufgabe 1.8. Sei $G \to \mathrm{Sym}(\Omega)$ eine imprimitive Operation und $\Delta \subseteq \Omega$ ein Block, der bzgl. Inklusion minimal ist. Zeigen Sie, dass $G_{(\Delta)}$ primitiv auf Δ operiert.

Aufgabe 1.9. Sei $G \leq S_n$ regulär. Zeigen Sie $\mathrm{C}_{S_n}(G) \cong G$.

Aufgabe 1.10.

(a) Sei $G \to \mathrm{Sym}(\Omega)$ eine transitive Operation mit $|\Omega| > 1$. Zeigen Sie, dass mindestens ein Element aus G keine Fixpunkte auf Ω hat. Zeigen Sie außerdem, dass die fixpunktfreien Permutationen von G einen transitiven Normalteiler erzeugen.

(b) Wählt man $\sigma \in S_n$ zufällig und gleichverteilt, wie hoch ist die Wahrscheinlichkeit, dass σ keine Fixpunkte hat?

Aufgabe 1.11. Beweisen Sie den Satz von Wilson $(p-1)! \equiv -1 \pmod{p}$, indem Sie Sylow auf S_p anwenden (dabei ist p eine Primzahl).

Aufgabe 1.12. Sei $P \in \mathrm{Syl}_2(G)$ zyklisch. Zeigen Sie, dass ein Normalteiler $N \trianglelefteq G$ mit $G = NP$ und $N \cap P = 1$ existiert.

Aufgabe 1.13. Zeigen Sie, dass jede Gruppe der Ordnung 264 auflösbar ist.
Hinweis: Realisieren Sie ein Gegenbeispiel als Permutationsgruppe vom Grad 12.

Aufgabe 1.14 (Frobenius)**.** Sei $p^a \mid |G|$. Zeigen Sie, dass die Anzahl der Untergruppen der Ordnung p^a von G kongruent zu 1 modulo p ist.
Hinweis: Betrachten Sie die Operation von G auf den p^a-elementigen Teilmengen von G durch Linksmultiplikation.

Aufgabe 1.15. Seien P und Q verschiedene p-Sylowgruppen von G, sodass $|P \cap Q|$ möglichst groß ist. Dann ist $|\mathrm{Syl}_p(G)| \equiv 1 \pmod{|P : P \cap Q|}$.

Aufgabe 1.16. Sei G eine Permutationsgruppe vom Grad n mit r Bahnen. Zeigen Sie, dass man G mit $n - r$ Elementen erzeugen kann. Insbesondere lässt sich G immer mit $n - 1$ Elementen erzeugen.

Aufgabe 1.17.

(a) Sei $\sigma \in S_n$ ein Produkt von r disjunkten Zyklen (inklusive Einerzyklen). Zeigen Sie, dass σ ein Produkt von $n - r$ Transpositionen ist. Zeigen Sie auch, dass σ kein Produkt von weniger als $n - r$ Transpositionen ist.

(b) Zeigen Sie, dass jede Permutation $\sigma \in S_n$ ein Produkt von höchstens $\frac{3}{2}(n-1)$ Transpositionen der Form $(1, i)$ ist.

(c) Für $2 \leq i \leq n$ sei $T_i := \{1, (1, i), (2, i), \ldots, (i-1, i)\} \subseteq S_n$. Zeigen Sie, dass sich jede Permutation $\sigma \in S_n$ eindeutig in der Form $\sigma = t_2 \ldots t_n$ mit $t_i \in T_i$ für $i = 2, \ldots, n$ schreiben lässt.

(d) Zeigen Sie, dass jede Permutation $\sigma \in S_n$ ein Produkt von Transpositionen der Form $(i, i+1)$ ist. Sei $\sigma = t_1 \ldots t_m$ eine solche Darstellung, wobei m nicht minimal ist. Zeigen Sie, dass $1 \leq i < j \leq m$ mit $\sigma = t_1 \ldots t_{i-1} t_{i+1} \ldots t_{j-1} t_{j+1} \ldots t_m$ existieren.

(e) Bestimmen Sie die verschiedenen Zerlegungen aus (a)–(d) für $\sigma = (1, 5, 4, 2, 3) \in S_5$. Reduzieren Sie auch die Länge der vierten Zerlegung.

(f) Zeigen Sie $S_n = \langle (1, 2), (1, \ldots, n)\rangle$ für $n \geq 2$. Welcher Sortieralgorithmus verbirgt sich dahinter?

(g) (Keeler) Zeigen Sie, dass sich jede Permutation $\sigma \in S_n$ als Produkt von paarweise verschiedenen Transpositionen in $S_{n+2} \setminus S_n$ schreiben lässt.

Aufgabe 1.18.

(a) (Landau) Zeigen Sie, dass es bis auf Isomorphie nur endlich viele Gruppen mit einer vorgegebenen Klassenzahl gibt.
Hinweis: Beweisen Sie, dass die Klassengleichung nur endlich viele Lösungen hat.

(b) Bestimmen Sie alle Gruppen mit höchstens drei Konjugationsklassen.

(c) Zeigen Sie
$$\frac{k(H)}{|G : H|} \leq k(G) \leq k(H)|G : H|$$
für $H \leq G$.

(d) (Nagao) Zeigen Sie $k(G) \leq k(N)k(G/N)$ für $N \trianglelefteq G$.
Hinweis: Betrachten Sie für ein festes $g \in G$ die Operation $N \to \mathrm{Sym}(N)$ durch ${}^{x}y := gxg^{-1}yx^{-1}$ für $x, y \in N$.

Aufgabe 1.19. Der Organisator der diesjährigen Konferenz über Permutationsgruppen beschließt folgendes Experiment durchzuführen: Die 80 Teilnehmer der Konferenz sollen in den ersten 80 Zimmern des Hotels „Harmonie“ untergebracht werden, aber bislang kennt keiner der Teilnehmer seine Zimmernummer. Die Teilnehmer werden nun nacheinander gebeten ihr Zimmer zu suchen, indem sie in maximal 40 der 80 Zimmer einen Blick werfen dürfen. In jedem Zimmer liegt eine personalisierte Konferenzmappe, sodass ersichtlich ist, wem das Zimmer zugeordnet wurde. Die Teilnehmer dürfen sich vor dem Experiment eine Strategie überlegen, aber während des Experiments in keiner Weise kommunizieren. Das Experiment gilt als erfolgreich, wenn jeder Teilnehmer sein eigenes Zimmer findet. Man überlege sich eine Strategie, bei der die Erfolgswahrscheinlichkeit mehr als 30% beträgt. Zum Vergleich: Öffnet jeder Teilnehmer 40 zufällige Türen, so ist die Wahrscheinlichkeit nur $2^{-80} < 10^{-24}$.

http://www.springer.com/978-3-658-17596-2

Endliche Permutationsgruppen
Sambale, B.
2017, XI, 260 S. 9 Abb., Softcover
ISBN: 978-3-658-17596-2