Skript zur Vorlesung „GAGA B“
Gruppen, Algorithmen, Geometrien & Anwendungen
Universität Stuttgart, Wintersemester 2020/21

Davide Cesare Veniani
(basierend auf einem Skript von Meinolf Geck)

29. November 2022

Inhaltsverzeichnis

1 Gruppen **5**
- 1.1 Untergruppen . . . 6
- 1.2 Gruppenoperationen . . . 9
- 1.3 Symmetrische Gruppen . . . 12
- 1.4 Aufgaben . . . 14

2 Schreier–Sims-Algorithmus **21**
- 2.1 Bahnenalgorithmen . . . 21
- 2.2 Schreiers Untergruppenlemma . . . 23
- 2.3 Schreier–Sims-Algorithmus . . . 25
- 2.4 Membership-Test . . . 26
- 2.5 Aufgaben . . . 26

3 Präsentationen **27**
- 3.1 Freie Gruppen . . . 27
- 3.2 Definition und Beispiele . . . 29
- 3.3 Symmetrische Gruppen . . . 32
- 3.4 Aufgaben . . . 34

4 BN-Paare **35**
- 4.1 Allgemeine lineare Gruppen . . . 36
- 4.2 Bruhat-Zerlegung . . . 40
- 4.3 Aufgaben . . . 43
- 4.4 Coxeter-Gruppen und Weyl-Gruppen . . . 47
- 4.5 Aufgaben . . . 51

Kapitel 1

Gruppen

Wir bezeichnen mit $|S|$ die Mächtigkeit einer Menge S, mit $A \dot\cup B$ die Vereinigung zweier disjunkten Teilmengen $A \subseteq S$ und $B \subseteq S$ und mit $\mathrm{Diag}(a_1, \dots, a_n)$ eine $n \times n$-Diagonalmatrix mit Einträgen $a_1, \dots, a_n$ auf der Diagonale.

Definition 1.1. Eine *Gruppe* ist eine nicht-leere Menge G zusammen mit einer Abbildung

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

genannt *Verknüpfung* oder *Multiplikation*, mit folgenden Eigenschaften:

- Die Verknüpfung $*$ ist *assoziativ*, d. h. $a * (b * c) = (a * b) * c$ für alle $a, b, c \in G$.
- Es gibt ein *neutrales Element* $1_G \in G$ mit $a * 1_G = 1_G * a = a$ für alle $a \in G$.
- Zu jedem $a \in G$ gibt es ein *inverses Element* $a^{-1} \in G$ mit $a * a^{-1} = a^{-1} * a = 1_G$.

Wir werden sowohl endliche als auch unendliche Gruppen betrachten. Falls klar, schreiben wir einfach 1 statt 1_G und ab statt $a * b$.

Definition 1.2. Eine Gruppe heißt *abelsch*, falls $ab = ba$ für alle $a, b \in G$.

Definition 1.3. Die Menge S der bijektiven Abbildungen $\pi : \{1, \dots, n\} \to \{1, \dots, n\}$ bildet zusammen mit der üblichen Verknüpfung $\circ$ eine Gruppe namens *symmetrische Gruppe (vom Grad n)*. Die Elemente von S_n heißen *Permutationen*. Die Gruppe S_n ist endlich, genauer gesagt

$$|\mathrm{S}_n| = n! = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1.$$

Falls $\pi(i) = j_i$ für $i = 1, \dots, n$, schreiben wir

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}.$$

Beispiel 1.4. Gegeben $\pi, \sigma \in \mathrm{S}_3$ definiert durch

$$\pi := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

dann gilt

$$\pi\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Insbesondere ist S_3 (so wie jede symmetrische Gruppe S_n mit $n > 2$) keine abelsche Gruppe.

Beispiel 1.5. Im Allgemeinen bildet die Menge $\mathrm{M}_n(K)$ der $n \times n$-Matrizen mit Koeffizienten aus einem Körper K, zusammen mit der üblichen Matrizenmultiplikation, keine Gruppe, denn nicht alle Matrizen sind invertierbar. Wir betrachten die Menge $\mathrm{GL}_n(K)$ der *regulären* Matrizen $A \in \mathrm{M}_n(K)$, also mit $\det(A) \neq 0$. Dies ist nämlich eine Gruppe, namens *allgemeine lineare Gruppe*, deren neutrales Element die $n \times n$-Einheitsmatrix $\mathbf{1}_n = \mathrm{Diag}(1, \dots, 1)$ ist. Der Körper K besitzt unendlich viele Elemente genau dann, wenn $\mathrm{GL}_n(K)$ eine unendliche Gruppe ist.

Definition 1.6. Eine Abbildung $\varphi\colon G \to G'$ zwischen Gruppen $(G, *)$, $(G', \bullet)$ heißt *Homomorphismus*, falls $\varphi(a * b) = \varphi(a) \bullet \varphi(b)$ für alle $a, b \in G$. Ein Homomorphismus, der bijektiv ist, heißt *Isomorphismus*. Die Gruppen heißen dann *isomorph*, in Zeichen $G \cong G'$.

1.1 Untergruppen

Definition 1.7. Für beliebige Teilmengen $S_1, S_2, \dots, S_r \subseteq G$ einer Gruppe G setzen wir

$$S_1 S_2 \cdots S_r := \{\, g_1 g_2 \cdots g_r \mid g_1 \in S_1, g_2 \in S_2, \dots, g_r \in S_r \,\} \subseteq G.$$

Enthält S_i nur ein Element g, so schreiben wir $S_1 \cdots S_{i-1} g S_{i+1} \cdots S_r$ statt $S_1 \cdots S_{i-1} \{g\} S_{i+1} \cdots S_r$. Außerdem definieren wir für $S \subseteq G$

$$S^{-1} := \{\, g^{-1} \mid g \in S \,\} \subseteq G.$$

Definition 1.8. Eine Teilmenge $H \subseteq G$ heißt *Untergruppe*, in Zeichen $H \leq G$, falls die folgenden Eigenschaften gelten: $1_G \in H$, $HH \subseteq H$ und $H^{-1} \subseteq H$. Die Untergruppe H bildet eine Gruppe zusammen mit der Einschränkung der Verknüpfung $*$ von G.

Definition 1.9. Es sei $H \leq G$ eine Untergruppe. Die Teilmengen der Form gH und Hg mit $g \in G$ heißen *linke* bzw. *rechte Nebenklassen* von H.

Bemerkung 1.10. Es seien $S \subseteq G$ eine Teilmenge und $H \leq G$ eine Untergruppe. Dann ist $SH = H$ genau dann, wenn $S \subseteq H$. Insbesondere ist $gH = H$ genau dann, wenn $g \in H$.

Beispiel 1.11. Eine Untergruppe von $\mathrm{GL}_n(K)$ heißt *Matrizengruppe*. Die Matrizengruppen

$$\mathrm{SL}_n(K) := \{ A \in \mathrm{GL}_n(K) \mid \det(A) = 1 \},$$
$$\mathrm{O}_n(K) := \{ A \in \mathrm{GL}_n(K) \mid A^{\mathrm{t}} A = 1 \},$$

wobei A^{t} die zu A transponierte Matrix bezeichnet, heißen *spezielle lineare Gruppe* bzw. *orthogonale Gruppe*.

Definition 1.12. Es sei G eine Gruppe und $S \subseteq G$ eine Teilmenge. Dann heißt

$$\langle S \rangle := \bigcap_{S \subseteq H \leq G} H$$

die *von S erzeugte Untergruppe* von G.

Die Teilmenge $\langle S \rangle$ is tatsächlich eine Untergruppe von G. Falls $S = \emptyset$, dann $\langle S \rangle = \{1_G\}$. Für $S \neq \emptyset$ gilt

$$\langle S \rangle = \{ x_1 * \ldots * x_r \mid r \geq 1, x_i \in S \text{ oder } x_i^{-1} \in S \}.$$

Insbesondere, falls $S = \{g\}$ nur ein Element enthält, dann gilt

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

wobei $g^m := g * \ldots * g$ (m-mal) für $m > 0$, $g^0 := 1_G$ und $g^m := (g^{-1})^{-m}$ für $m < 0$. Mit dieser Regel gilt $g^m * g^n = g^{m+n}$ für alle $m, n \in \mathbb{Z}$.

Definition 1.13. Für $g \in G$ heißt $\mathrm{Ord}(g) = |\langle g \rangle|$ die *Ordnung* von g. Ist $G = \langle g \rangle$ für ein $g \in G$, so heißt G *zyklisch*. Insbesondere ist dann G abelsch.

Satz 1.14 (Satz von Lagrange)**.** *Ist G eine endliche Gruppe und $H \leq G$ eine Untergruppe, so gilt $|H| \mid |G|$ (in Worten: $|H|$ teilt $|G|$). Insbesondere* $\mathrm{Ord}(g) \mid |G|$ *für alle $g \in G$.*

Beweis. Zwei Nebenklassen gH und $g'H$ sind entweder gleich oder disjunkt und jede Nebenklasse enthält genau $|H|$ Elemente. □

Definition 1.15. Eine Untergruppe $H \leq G$ heißt *Normalteiler*, falls $ghg^{-1} \in H$ für alle $g \in G$ und $h \in H$ (äquivalent: $gHg^{-1} = H$). In Zeichen: $H \trianglelefteq G$. Die Schreibweise $H \triangleleft G$ bedeutet $H \trianglelefteq G$ und $H \neq G$.

Definition 1.16. Der *Kernel* eines Homomorphismus $\varphi : G \to G'$ ist der Normalteiler

$$\mathrm{Ker}(\varphi) := \{ g \in G \mid \varphi(g) = 1_{G'} \}.$$

Wenn $H \trianglelefteq G$ gilt, ist jede linke Nebenklasse gH gleich der rechten Nebenklasse Hg. Folglich kann man die *Faktorgruppe* bilden, die aus den Nebenklassen besteht:

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

Die induzierte Verknüpfung $(g_1H)(g_2H) := g_1g_2H$ sowie der *kanonische Homomorphismus*

$$\varphi\colon G \to G/H, \quad g \mapsto gH$$

sind dann wohldefiniert. Bemerke: $\mathrm{Ker}(\varphi) = H$.

Satz 1.17 (Homomorphiesatz)**.** *Sind G_1, G_2 zwei Gruppen und $\varphi\colon G_1 \to G_2$ ein Homomorphismus, dann ist der Quotient $G_1/\mathrm{Ker}(\varphi)$ isomorph zum Bild $\varphi(G_1) \subseteq G_2$.* □

Definition 1.18. Es seien $H \leq G$ und $N \trianglelefteq G$ eine Untergruppe bzw. ein Normalteiler von G. Das *Komplexprodukt* (oder einfach *Produkt*) von H und N ist $HN = \{\, hn \mid h \in H, n \in N \,\} \subseteq G$.

Satz 1.19 (Erster Isomorphiesatz)**.** *Es seien $H \leq G$ und $N \trianglelefteq G$. Dann ist HN eine Untergruppe von G und es gilt $N \trianglelefteq HN$ und $H \cap N \trianglelefteq H$. Übrigens*

$$H/(H \cap N) \cong HN/N.$$ □

Definition 1.20. Eine nicht-triviale Gruppe G heißt *einfach*, wenn $\{1\}$ und G die einzigen Normalteiler von G sind.

Einfache Gruppen sind die elementaren Bausteine der Gruppentheorie. Endliche einfache Gruppen wurden im 20. Jahrhundert klassifiziert. Eine Liste davon kann man auf `en.wikipedia.org/wiki/List_of_finite_simple_groups` finden. Die Liste besteht aus 18 Familien und 26 sogenannten *sporadischen* Gruppen.

Beispiel 1.21. Zyklische Gruppen $G := \mathrm{Z}_p = \mathbb{Z}/p\mathbb{Z}$ der Primordnung p sind einfache Gruppen. Eine solche Gruppe besitzt nämlich keine anderen Untergruppen außer $\{1\}$ und G. Alle abelschen(!) einfachen Gruppen haben diese Gestalt (siehe Aufgabe 1.47).

Definition 1.22. Der *Kommutator* zweier Elemente g und h einer Gruppe G ist das Element $[g,h] := ghg^{-1}h^{-1}$. Die Untergruppe $\mathrm{K}(G)$, die von allen Kommutatoren erzeugt wird, heißt *Kommutatorgruppe* und wird oft auch mit $[G,G]$, G' oder $G^{(1)}$ bezeichnet:

$$\mathrm{K}(G) := \langle\, [g,h] \mid g,h \in G \,\rangle.$$

Bemerke: Das Produkt zweier Kommutatoren muss kein Kommutator sein. Die Kommutatorgruppe ist immer ein guter Kandidat, um zu sehen, ob eine Gruppe einfach ist oder nicht, denn es gilt immer $\mathrm{K}(G) \trianglelefteq G$ (siehe Aufgabe 1.48).

Beispiel 1.23. Die fünf Mathieu-Gruppen $\mathrm{M}_{11}, \mathrm{M}_{12}, \mathrm{M}_{22}, \mathrm{M}_{23}, \mathrm{M}_{24}$ sind sporadische Gruppen und wurden zwischen 1861 und 1873 vom französischen Mathematiker Émile Léonard Mathieu gefunden. Die *Mathieu-Gruppe* M_{11} ist die Untergruppe von S_{11} erzeugt von

$$\pi := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 1 \end{pmatrix},$$

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 1 & 2 & 7 & 10 & 6 & 4 & 11 & 3 & 9 & 5 & 8 \end{pmatrix}.$$

Es gilt $\mathrm{Ord}(\pi) = 11$ und $\mathrm{Ord}(\sigma) = 4$. Was ist $|\mathrm{M}_{11}|$?

Beispiel 1.24. Die vier Janko-Gruppen J_1, J_2, J_3, J_4 sind sporadische Gruppen und wurden zwischen 1965 und 1976 vom kroatischen Mathematiker Zvonimir Janko gefunden. Es sei $K = \mathbb{F}_{11}$ der Körper mit 11 Elementen. Die *Janko-Gruppe* J_1 ist die Untergruppe von $GL_7(K)$ erzeugt von

$$A := \begin{pmatrix} -2 & 1 & 1 & 3 & 1 & 3 & 3 \\ 1 & 1 & 3 & 1 & 3 & 3 & -2 \\ 1 & 3 & 1 & 3 & 3 & -2 & 1 \\ 3 & 1 & 3 & 3 & -2 & 1 & 1 \\ 1 & 3 & 3 & -2 & 1 & 1 & 3 \\ 3 & 3 & -2 & 1 & 1 & 3 & 1 \\ 3 & -2 & 1 & 1 & 3 & 1 & 3 \end{pmatrix}, \quad B := \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Es gilt $\mathrm{Ord}(A) = 2$ und $\mathrm{Ord}(B) = 7$. Was ist $|J_1|$?

1.2 Gruppenoperationen

Definition 1.25. Es seien G eine Gruppe und X eine nicht-leere Menge. Wir sagen, dass G *links auf X operiert* oder dass X eine *linke G-Menge* ist, wenn es eine Abbildung

$$\mu : G \times X \to X, \quad (g, x) \mapsto g \cdot x$$

gibt mit folgenden Eigenschaften:

- $1_G \cdot x = x$ für alle $x \in X$,
- $(g * h) \cdot x = g \cdot (h \cdot x)$ für alle $g, h \in G$ und $x \in X$.

Für eine *rechte G-Menge* schreibt man $x \cdot g$ statt $g \cdot x$ und es gilt $x \cdot (g * h) = (x \cdot g) \cdot h$.

Beispiel 1.26. Die Gruppe $G = S_n$ operiert auf der Menge $X = \{1, \dots, n\}$ durch

$$(\pi, i) \mapsto \pi(i), \quad \pi \in G, i \in X.$$

Definition 1.27. Der *Kern* der Operation μ ist die Untergruppe

$$\mathrm{Ker}(\mu) := \{\, g \in G \mid g \cdot x = x \text{ für alle } x \in X \,\}.$$

Dies ist immer ein Normalteiler von G. Die Operation μ heißt *treu*, falls $\mathrm{Ker}(\mu) = \{1\}$.

Beispiel 1.28. Es sei K ein Körper. Jede Matrizengruppe $G \leq GL_n(K)$ operiert auf der Menge $V = K^n$ der Spaltenvektoren durch Multiplikation:

$$(A, v) \mapsto Av.$$

Diese Operation ist treu: Falls $Av = v$ für alle $v \in V$, dann ist A gleich der Einheitsmatrix $\mathbf{1}_n$.

Es sei nun $\mathbb{P}(V)$ der *projektive Raum* von V, d. h. die Menge der 1-dimensionalen Teilräume von V. Für $v \in V \setminus \{0\}$ bezeichnen wir mit $[v]$ den von v erzeugten Teilraum. Ist $A \in G$ und

$v \in V \setminus \{0\}$, so ist auch $Av \neq 0$. Übrigens gilt $A(cv) = cAv$ für alle $c \in K$. Also operiert G auf $\mathbb{P}(V)$ durch

$$G \times \mathbb{P}(V) \to \mathbb{P}(V), \quad (A, [v]) \mapsto [Av].$$

Lemma 1.29. *Setze $K^\times = K \setminus \{0\}$. Der Kern der Operation einer Matrizengruppe $G \leq \mathrm{GL}_n(K)$ auf $\mathbb{P}(V)$ ist die Untergruppe*

$$\{\, A \in G \mid A = a\mathbf{1}_n,\ a \in K^\times \,\}.$$

Beweis. Falls $A = a\mathbf{1}_n$, dann $[Av] = [av] = [v]$, also operiert A trivial auf $\mathbb{P}(V)$. Umgekehrt sei $A \in G$, sodass A trivial auf $\mathbb{P}(V)$ operiert. Es sei $\{e_1, e_2, \dots, e_n\}$ die Standardbasis von V. Dann ist Ae_i gleich der i-te Spalte von A. Aus $[Ae_i] = [e_i]$ für $1 \leq i \leq n$ folgt es, dass es $a_1, \dots, a_n \in K$ gibt mit $Ae_i = a_i e_i$ für $1 \leq i \leq n$, d. h. $A = \mathrm{Diag}(a_1, \dots, a_n)$. Übrigens gilt Folgendes für alle $i \neq j$:

$$[e_i + e_j] = [A(e_i + e_j)] = [a_i e_i + a_j e_j],$$

sprich es gibt $a \in K$ mit $a(e_i + e_j) = a_i e_i + a_j e_j$. Da e_i und e_j linear unabhängig ist, muss $a = a_i = a_j$, d. h. $A = a\mathbf{1}_n$. Aus $\det(A) \neq 0$ folgt $a \neq 0$. □

Bezeichnung 1.30. Für festes $x \in X$ heißt $\mathcal{O}_x := \{\, g \cdot x \mid g \in G \,\}$ die *Bahn* von x unter der Operation von G. Dies ist eine Teilmenge von X.

Bezeichnung 1.31. Weiterhin heißt $\mathrm{Stab}_G(x) = G_x := \{\, g \in G \mid g \cdot x = x \,\}$ der *Stabilisator* von x. Dies ist eine Untergruppe von G.

Satz 1.32 (Bahnensatz)**.** *Die folgende Abbildung ist wohldefiniert und bijektiv:*

$$\mu_x : \mathcal{O}_x \to G/G_x, \quad g \cdot x \mapsto gG_x.$$

Insbesondere ist $|G| < \infty$, so folgt $|\mathcal{O}_x| < \infty$ und $|\mathcal{O}_x| = |G/G_x| = |G|/|G_x|$. □

Für $x, y \in X$ sind $\mathcal{O}_x, \mathcal{O}_y$ entweder gleich oder disjunkt. Also ist X disjunkte Vereinigung von Bahnen.

Definition 1.33. Eine Gruppenoperation von G auf X heißt *transitiv*, wenn es nur eine Bahn gibt, d. h., für alle x und $y \in X$ gibt es stets ein $g \in G$ mit $g \cdot x = y$.

Beispiel 1.34. Die Gruppe $G = \mathrm{S}_n$ operiert auf der Menge $X = \{1, \dots, n\}$. Diese Operation ist transitiv, denn zum Beispiel $X = \mathcal{O}_1$. Es gilt nämlich $(1\ i) \cdot 1 = i$ für jedes $i \in X, i > 1$.

Beispiel 1.35. Es sei K ein Körper. Die Gruppe $G = \mathrm{GL}_n(K)$ operiert auf der Menge $V = K^n$ der Spaltenvektoren mit Koeffizienten aus K. Der Nullvektor $0 \in V$ bildet eine Bahn $\mathcal{O}_0 = \{0\}$, denn $A0 = 0$ für alle $A \in G$. Dann betrachten wir den Spaltenvektor

$$e_1 = (1, 0, \dots, 0)^{\mathrm{t}}.$$

Der Vektor Ae_1 ist die erste Spalte von der Matrix A. Da jeder Spaltenvektor $v \neq 0$ zu einer Basis von V ergänzt werden kann, gibt es $A \in \mathrm{GL}_n(K)$ mit $Ae_1 = v$. Also ist V die disjunkte Vereinigung von zwei Bahnen

$$V = \mathcal{O}_0 \dot\cup \mathcal{O}_{e_1}$$

und die Operation ist nicht transitiv.

Beispiel 1.36. Falls G eine Gruppe ist, dann operiert G auf $X = G$ durch Linksmultiplikation:

$$G \times X \to X, \quad g \cdot x := g * x.$$

Diese Operation ist transitiv, denn $\mathcal{O}_1 = G$, und treu, denn falls $g * x = x$ für alle $x \in G$, dann insbesondere für $x = 1$, sprich $g = g * 1 = 1$. Also ist G isomorph zu einer Untergruppe von

$$\mathrm{S}_X = \{\, f : X \to X \mid f \text{ bijektiv} \,\}.$$

Dies ist die Idee vom Beweis des Satzes von Cayley (Satz 1.39): Ist $|G| = n < \infty$, so ist G isomorph zu einer Untergruppe von $\mathrm{S}_G \cong \mathrm{S}_n$.

Beispiel 1.37. Jede Gruppe G operiert auf $X = G$ auch durch *Konjugation*:

$$G \times X \to X, \quad g \cdot x := gxg^{-1}.$$

Es gilt $\mathcal{O}_1 = \{1\}$, also ist diese Operation niemals transitiv sobald $G \neq \{1\}$. Der Kern von dieser Operation heißt *Zentrum* von G und wird mit $\mathrm{Z}(G)$ bezeichnet. Es gilt

$$\mathrm{Z}(G) = \{\, g \in G \mid gx = xg \text{ für alle } x \in G \,\}.$$

Die Bahnen von dieser Operation heißen *Konjugationsklassen* und zwei Elemente $g, h \in G$ heißen *konjugiert*, falls g, h zur selben Konjugationsklasse gehören. Der Stabilisator G_x von $x \in G$ heißt *Zentralisator* und ist gegeben durch

$$\{\, g \in G \mid gxg^{-1} = x \,\} = \{\, g \in G \mid gx = xg \,\}.$$

Beispiel 1.38. Es seien G eine Gruppe, H und K Untergruppen von G. Eine Teilmenge der Form

$$HgK = \{\, hgk \mid h \in H,\, k \in K \,\}$$

mit $g \in G$ heißt *Doppelnebenklasse*. Die Gruppe $H \times K$ operiert auf der Menge $X = G$ durch

$$(H \times K) \times X, \quad (h, k) \cdot g := hgk^{-1}.$$

Die Bahn von G ist genau die Doppelnebenklasse HgK. Aus dem Bahnensatz folgt: Die Gruppe G ist Vereinigung disjunkter Doppelnebenklassen.

1.3 Symmetrische Gruppen

Die symmetrische Gruppe S_n spielt eine sehr wichtige Rolle in der Gruppentheorie. Grund dafür ist wohl der nächste Satz.

Satz 1.39 (Satz von Cayley)**.** *Es sei G eine endliche Gruppe. Dann gibt es ein $n \in \mathbb{N}$, sodass G isomorph zu einer Untergruppe von S_n ist.* □

Wir führen eine vereinfachte Schreibweise für Elemente von S_n ein. Es sei $\sigma \in S_n$ und nehmen wir an, dass es $i_1, \dots, i_d \in \{1, \dots, n\}$ gibt, mit

$$\sigma(i_1) = i_2,\ \sigma(i_2) = i_3,\ \dots,\ \sigma(i_{d-1}) = i_d,\ \sigma(i_d) = i_1,$$

und dass $\sigma(j) = j$ für jedes $j \in \{1, \dots, n\} \setminus \{i_1, \dots, i_d\}$. Dann heißt σ *d-Zyklus* (oder *zyklische Permutation* oder einfach *Zyklus*) und wir schreiben

$$\sigma = (i_1\ i_2\ \dots\ i_d).$$

Ein d-Zyklus hat Ordnung d. Jeder 1-Zyklus ist gleich der Identität $\mathrm{id} \in S_n$. Ein 2-Zyklus $\sigma = (i\ j)$ heißt *Transposition*: σ vertauscht genau zwei Ziffern i, j und lässt alle anderen fest.

Beispiel 1.40. Gegeben $\sigma = (3\ 4\ 5) \in S_5$ können wir äquivalent schreiben

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

Es gilt übrigens $\sigma^2 = (3\ 5\ 4)$ und $\sigma^3 = \mathrm{id}$.

Beispiel 1.41. Jedes $\pi \in S_n$ lässt sich als Produkt von *disjunkten* Zyklen schreiben. Zum Beispiel,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 1 & 2 & 7 & 10 & 6 & 4 & 11 & 3 & 9 & 5 & 8 \end{pmatrix} = (1)(2)(3\ 7\ 11\ 8)(4\ 10\ 5\ 6)(9).$$

Die 1-Zyklen (1), (2) und (9) können wir weglassen: $\sigma = (3\ 7\ 11\ 8)(4\ 10\ 5\ 6)$.

Sind σ und σ' disjunkte(!) Zyklen, so gilt $\sigma\sigma' = \sigma'\sigma$. (Aber im Allgemeinen ist S_n keine abelsche Gruppe, siehe Beispiel 1.4.)

Lemma 1.42. *Die Gruppe S_n wird von Transpositionen erzeugt.*

Beweis. Jede Permutation lässt sich als Produkt von (disjunkten) Zyklen schreiben und jeder d-Zyklus lässt sich als Produkt von $d - 1$ Transpositionen schreiben, denn es gilt

$$(i_1\ i_2\ \dots\ i_d) = (i_1\ i_2)(i_2\ i_3) \dots (i_{d-1}\ i_d). \tag{1.1}$$

Daher ist jede Permutation gleich einem Produkt von Transpositionen. □

Definition 1.43. Es sei $\pi \in \mathrm{S}_n$. Ein *Fehlstand* in π ist ein Paar (i, j) mit $i, j \in \{1, \dots, n\}$, $i < j$ und $\pi(i) > \pi(j)$. Die Permutation π ist *gerade* falls es eine gerade Anzahl von Fehlständen in π gibt, sonst ist π *ungerade*. Das *Signum* (oder *Vorzeichen*)

$$\operatorname{sgn} : \mathrm{S}_n \to \{1, -1\}$$

ist die Funktion, der gerade Permutationen auf 1 und ungerade auf -1 abbildet.

Das Signum ist nach Aufgabe 1.52 ein Gruppenhomomorphismus. Jede Transposition ist ungerade. Aus (1.1) folgt dann: Für ein d-Zyklus σ gilt $\operatorname{sgn}(\sigma) = (-1)^{d-1}$.

Definition 1.44. Die Untergruppe der geraden Permutationen von S_n heißt *alternierende Gruppe (vom Grad n)* und wird mit A_n bezeichnet. Dies ist genau der Kern vom Signum.

Die Gruppe A_2 ist trivial. Die Gruppe $\mathrm{A}_3 \cong \mathrm{Z}_3$ hat Ordnung 3 und ist also zyklisch. Für $n \geq 4$ ist A_n nicht abelsch, denn zum Beispiel

$$(1\ 2\ 3)(2\ 3\ 4) \neq (2\ 3\ 4)(1\ 2\ 3).$$

Die Gruppe A_4 ist aber nicht einfach, weil

$$\mathrm{K}(\mathrm{A}_4) = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \lhd \mathrm{A}_4.$$

Satz 1.45. *Für $n \geq 5$ ist A_n eine einfache Gruppe.*

Beweis. Es sei $N \trianglelefteq \mathrm{A}_n$ ein Normalteiler mit $N \neq \{\mathrm{id}\}$. Wir wollen zeigen, dass $N = \mathrm{A}_n$ und wegen Aufgabe 1.53 (wo die Hypothese $n \geq 5$ notwendig ist!) genügt es zu zeigen, dass alle Elemente der Form $(i\ j)(k\ l)$ mit i, j, k, l paarweise verschieden zu N gehören.

Da $N \neq \{\mathrm{id}\}$, gibt es $\pi \in N$ mit $\pi \neq \mathrm{id}$. Wir schreiben π als Produkt von disjunkten Zyklen $\pi = \sigma_1 \cdots \sigma_m$. Falls alle Zyklen σ_i Transpositionen sind, dann muss $m \geq 2$ (und gerade) sein, denn $\pi \in \mathrm{A}_n$ ist eine gerade Permutation. Es können also vier Fälle vorkommen:

(I) π ist das Produkt von mindestens zwei Transpositionen: $\pi = (a\ b)(c\ d) \cdot \dots$
(II) π ist ein 3-Zyklus: $\pi = (a\ b\ c)$.
(III) π ist das Produkt von mindestens zwei 3-Zyklen: $\pi = (a\ b\ c)(d\ e\ f) \cdot \dots$
(IV) mindestens ein σ_i hat Länge ≥ 4: $\pi = (a\ b\ c\ d\ \dots) \cdot \dots$

Da $N \trianglelefteq \mathrm{A}_n$, gilt $\sigma\pi^{-1}\sigma^{-1} \in N$, also auch $\pi\sigma\pi^{-1}\sigma^{-1} \in N$.

Im Fall (I) nehmen wir $\sigma = (a\ b\ c)$. Dann ist $\pi\sigma\pi^{-1} = (b\ a\ d)$ wegen Aufgabe 1.51, also

$$\pi\sigma\pi^{-1}\sigma^{-1} = (b\ a\ d)(a\ c\ b) = (a\ c)(b\ d) \in N.$$

Im Fall (II) nehmen wir $\sigma = (a\ b\ d)$. Ähnlich gilt

$$\pi\sigma\pi^{-1}\sigma^{-1} = (b\ c\ d)(a\ d\ b) = (a\ b)(c\ d) \in N.$$

Im Fall (III) nehmen wir $\sigma = (a\ b\ d)$. Ähnlich gilt

$$\pi\sigma\pi^{-1}\sigma^{-1} = (b\ c\ e)(a\ d\ b) = (a\ d\ c\ e\ b) \in N,$$

d. h., wir sind im Fall (IV).

Im Fall (IV) nehmen wir $\sigma = (a\ b\ c)$. Ähnlich gilt

$$\pi\sigma\pi^{-1}\sigma^{-1} = (b\ c\ d)(a\ c\ b) = (a\ d\ b) \in N,$$

d. h., wir sind im Fall (II).

Also haben wir gezeigt, dass es in jedem Fall paarweise verschiedene $i, j, k, l \in \{1, \dots, n\}$ gibt, sodass $(i\ j)(k\ l) \in N$.

Sind nun $i', j', k', l' \in \{1, \dots, n\}$ beliebig paarweise verschieden, wollen wir ebenso zeigen, dass $(i'\ j')(k'\ l') \in N$. Der Klarheit halber nehmen wir an, dass $i' = 1, j' = 2, k' = 3, l' = 4$, obwohl ein analoges Argument für beliebige i', j', k', l' gilt. Betrachte

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ i & j & k & l & 5 & \cdots & n \end{pmatrix}, \quad \sigma' = (i\ j)\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ j & i & k & l & 5 & \cdots & n \end{pmatrix}.$$

Dann ist entweder $\sigma \in \mathrm{A}_n$ oder $\sigma' \in \mathrm{A}_n$. Es gilt aber wegen Aufgabe 1.51

$$\sigma(1\ 2)(3\ 4)\sigma^{-1} = \sigma'(1\ 2)(3\ 4)\sigma'^{-1} = (i\ j)(k\ l).$$

In beiden Fällen gilt also $(1\ 2)(3\ 4) \in N$, was wir zeigen wollten. □

1.4 Aufgaben

Aufgabe 1.46. Bestimme alle Untergruppen von S_3.

Lösung. Die Gruppe S_3 enthält 6 Elemente, nämlich $\mathrm{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)$, der Ordnung $1, 2, 2, 2, 3$ bzw. 3.

Es sei $H \leq \mathrm{S}_3$ eine Untergruppe. Dann gilt $|H| \mid |\mathrm{S}_3| = 6$ nach dem Satz von Lagrange, also $|H| = 1, 2, 3$ oder 6.

Ist $|H| = 1$ oder $|H| = 6$, dann $H = \{\mathrm{id}\}$ oder $H = \mathrm{S}_3$. Ist $|H| = 2$, dann $H = \{1, g\}$, wobei g ein Element der Ordnung 2 ist. Es gibt drei Möglichkeiten: $H = \{\mathrm{id}, (1\ 2)\}, \{\mathrm{id}, (1\ 3)\}$ oder $H = \{\mathrm{id}, (2\ 3)\}$.

Schließlich sei $|H| = 3$. Dann ist $H = \{1, g, g^2\}$ eine zyklische Gruppe, wobei g ein Element der Ordnung 3 ist. Es git nur eine Möglichkeit, nämlich $H = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$. □

Aufgabe 1.47. Es sei G eine abelsche Gruppe. Zeige:

(a) Für jedes $d \in \mathbb{Z}$ sind $\{\ g^d \mid g \in G\ \}$ und $\{\ g \in G \mid g^d = 1\ \}$ Untergruppen von G.

(b) Jede Untergruppe $H \leq G$ ist ein Normalteiler.

(c) Falls G einfach ist, dann ist G eine zyklische Gruppe der Primordnung.

Lösung. (a) Es gilt immer $(g^d)^{-1} = (g^{-1})^d$ für jedes $g \in G$. Da G abelsch ist, gilt auch $(g_1 g_2)^d = g_1^d g_2^d$. Aus diesen zwei Bemerkungen folgt die Aussage über die zwei Untergruppen.

(b) Da G abelsch ist, gilt $ghg^{-1} = hgg^{-1} = h \in H$ für jedes $h \in H$ und $g \in G$.

(c) Es sei $g \in G$ mit $g \neq 1$. Nach (b) ist die Untergruppe $\langle g \rangle \leq G$ ein Normalteiler, also muss $\langle g \rangle = G$ gelten, weil G einfach ist. Also ist G zyklisch. Es sei $n = \mathrm{Ord}(g)$ und nehmen wir an, dass n nicht prim ist, also $n = dm$ mit $1 < d, m < n$. Die Untergruppe $H = \{ h \in G \mid h^d = 1 \}$ ist nach (a) und (b) ein Normalteiler mit $H \neq \{1\}$, weil $g^m \in H$ (und $g^m \neq 1$ wegen $m < n = \mathrm{Ord}(g)$). Da G einfach ist, muss $H = G$ gelten, d. h. $g^d = 1$, aber das widerspricht $d < n = \mathrm{Ord}(g)$. □

Aufgabe 1.48. Es sei G eine Gruppe und $H \trianglelefteq G$ ein Normalteiler. Zeige:
(a) Es gilt $\mathrm{K}(G) \trianglelefteq G$, wobei $\mathrm{K}(G)$ die Kommutatorgruppe von G ist.
(b) Genau dann ist G/H abelsch, wenn $\mathrm{K}(G) \subseteq H$.

Lösung. (a) Für alle $a, b, g \in G$ gilt

$$\begin{aligned} g[a,b]g^{-1} &= gaba^{-1}b^{-1}g^{-1} = (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) \\ &= (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} = [gag^{-1}, gbg^{-1}] \in \mathrm{K}(G) \end{aligned}$$

Es sei nun $h \in \mathrm{K}(G)$ (Erinnerung: h muss selbst kein Kommutator sein). Da $[a,b]^{-1} = [b,a]$ können wir annehmen, dass es $a_1, b_1, a_2, b_2, \ldots, a_r, b_r \in G$ gibt mit $h = [a_1, b_1][a_2, b_2] \cdots [a_r, b_r]$. Dann

$$ghg^{-1} = (g[a_1,b_1]g^{-1})(g[a_2,b_2]g^{-1}) \cdots (g[a_r,b_r]g^{-1}) \in \mathrm{K}(G).$$

(b) Es sei $G \to G/H, g \mapsto \bar{g}$ der kanonische Isomorphismus. Nehmen wir an, dass G/H abelsch ist. Es seien $a, b \in G$. Dann $\bar{a}\bar{b} = \bar{b}\bar{a}$, d. h. $\overline{[a,b]} = \bar{a}\bar{b}\bar{a}^{-1}\bar{b}^{-1} = \bar{1}$, also $[a,b] \in H$ und damit $\mathrm{K}(G) \subseteq H$, da $\mathrm{K}(G)$ von allen Elementen der Form $[a,b]$ erzeugt wird.

Umgekehrt nehmen wir an, dass $\mathrm{K}(G) \subseteq H$ und seien $\bar{a}, \bar{b} \in G/H$. Aus $[a,b] = aba^{-1}b^{-1} \in \mathrm{K}(G) \subseteq H$ folgt $\overline{aba^{-1}b^{-1}} = \bar{1}$ und damit $\bar{a}\bar{b} = \bar{b}\bar{a}$. □

Aufgabe 1.49. Es seien $d, n \in \mathbb{N}$, G eine zyklische Gruppe der Ordnung n, $H = \{ g^d \mid g \in G \}$ und $K = \{ g \in G \mid g^d = 1 \}$. Zeige: $|H| = n/\,\mathrm{ggT}(n,d)$ und $|K| = \mathrm{ggT}(n,d)$.

Lösung. Es seien a ein Erzeuger von G und $m = \mathrm{ggT}(n,d)$. Dann gibt es n', d' teilerfremd mit $n = mn'$ und $d = md'$. Bemerke: $dn' = md'n' = d'n$. Wir definieren $H' = \{1, a^d, a^{2d}, \ldots, a^{(n'-1)d}\}$ und $K' = \{1, a^{n'}, a^{2n'}, \ldots, a^{(m-1)n'}\}$. Offensichtlich gilt $|H'| = n' = n/m$ und $|K'| = m$. Wir behaupten, dass $H = H'$ und $K = K'$.

Die Inklusion $H \supseteq H'$ ist klar. Nun sei $h \in H$. Dann ist $h = g^d = a^{id}$ für ein $i \in \mathbb{Z}$. Durch Division mit Rest finden wir j, s mit $0 \leq j < n'$ und $i = j + n's$. Wir erhalten

$$h = a^{id} = a^{(j+n's)d} = a^{jd}a^{dn's} = a^{jd}a^{d'ns} = a^{jd}(a^n)^{d's} = a^{jd} \in H',$$

also auch $H \subseteq H'$ und damit $H = H'$.

Es sei $k \in K'$. Dann gilt $k = a^{in'}$ mit $0 \leq i < m$, also $k^d = a^{in'd} = (a^n)^{id'} = 1$ und damit $k \in K$. Dies zeigt $K \supseteq K'$. Umgekehrt sei $k \in K$. Schreibe $k = a^i$ mit $i \in \mathbb{Z}$. Per Definition von K gilt $k^d = a^{id} = 1$, also $\mathrm{Ord}(a) = n \mid id$. Es gibt dann $s \in \mathbb{Z}$ mit $imd' = id = sn = smn'$, d. h. $id' = sn'$.

Das bedeutet, dass $d'|sn'$, aber d' und n' sind teilerfremd, also $d'|s$. Schreibe $s = jd'$ mit $j \in \mathbb{Z}$. Dann gilt $i = jn'$. Durch Division mit Rest finden wir l, t mit $0 \leq l < m$ und $j = l + mt$. Wir erhalten

$$k = a^i = a^{jn'} = a^{ln'} a^{mn't} = a^{ln'} (a^n)^t = a^{ln'} \in K'.$$

Dies zeigt $K \subseteq K'$ und damit $K = K'$. □

Aufgabe 1.50. Es seien $H, K, N \leq G$ Untergruppen einer Gruppe G mit $H \trianglelefteq K$ und $N \trianglelefteq G$. Zeige: $HN \trianglelefteq KN$.

Lösung. Wähle $h \in H, k \in K, m, n \in N$. Zu zeigen ist $(km)hn(km)^{-1} \in HN$.

Wir definieren $h' = khk^{-1}$ und $n' = h^{-1}mh$. Es gilt $h' \in H$, weil $H \trianglelefteq K$, und $n' \in N$, weil $N \trianglelefteq G$). Übrigens

$$(km)hn(km)^{-1} = (khk^{-1})(k(h^{-1}mh)nm^{-1}k^{-1}) = h'(kn'nm^{-1}k^{-1})$$

Da $n'' = n'nm^{-1} \in N$ ist auch $kn''k^{-1} \in N$ (immer wegen $N \trianglelefteq G$). □

Aufgabe 1.51. Zeige: Falls $\sigma = (i_1\ i_2\ \dots\ i_d) \in \mathrm{S}_n$ ein d-Zyklus ist und $\pi \in \mathrm{S}_n$, dann

$$\pi\sigma\pi^{-1} = (\pi(i_1)\ \pi(i_2)\ \dots\ \pi(i_d)).$$

Bestimme damit die Anzahl der Konjugationsklassen in S_n.

Lösung. Es sei $\sigma' = (\pi(i_1)\ \pi(i_2)\ \dots\ \pi(i_d))$. Zu zeigen ist $\pi\sigma\pi(i) = \sigma'(i)$ für alle $i \in \{1, \dots, n\}$. Es sei also $i \in \{1, \dots, n\}$ fest. Da $\pi\colon \{1, \dots, n\} \to \{1, \dots, n\}$ bijektiv ist, gibt es $j \in \{1, \dots, n\}$ mit $\pi(j) = i$. Wir unterscheiden nun zwei Fälle: $j \in \{i_1, \dots, i_d\}$ oder $j \notin \{i_1, \dots, i_d\}$. Im ersten Fall ist $j = i_m$, $1 \leq m \leq d$, also gilt $\sigma(j) = i_{m+1}$ (wobei $i_{d+1} = i_1$) und $\sigma'(\pi(j)) = \pi(i_{m+1})$. Dementsprechend gilt

$$\pi\sigma\pi^{-1}(i) = \pi\sigma\pi^{-1}(\pi(j)) = \pi\sigma(j) = \pi(i_{m+1}) = \sigma'(\pi(j)) = \sigma'(i)$$

wie gewünscht. Im zweiten Fall ist $\pi(j) \notin \{\pi(i_1), \dots, \pi(i_d)\}$, also $\sigma(j) = j$ und $\sigma'(\pi(j)) = \pi(j)$. Damit gilt auch in diesem Fall wie gewünscht

$$\pi\sigma\pi^{-1}(i) = \pi\sigma\pi^{-1}(\pi(j)) = \pi\sigma(j) = \pi(j) = \sigma'(\pi(j)) = \sigma'(i).$$

Nun behaupten wir, dass die Anzahl der Konjugationsklassen in S_n gleich der Anzahl der Partitionen von n, d. h. der Anzahl der Möglichkeiten die Zahl n als Summe $n = \sum_{i=1}^{r} d_i$ darzustellen mit $d_i \in \mathbb{N}$ (ohne Berücksichtigung der Reihenfolge). Es sei $\tau \in \mathrm{S}_n$ beliebig. Dann lässt sich τ als Produkt von disjunkten Zyklen $\tau = \sigma_1\sigma_2 \cdots \sigma_r$ schreiben, wobei $\sigma_l = (i_{l,1}\ i_{l,2}\ \dots\ i_{l,d_l})$ für $1 \leq l \leq r$. Zu diesem Produkt können wir gegebenenfalls 1-Zyklen hinzufügen, damit

$$\{i_{1,1}, i_{1,2}, \dots, i_{1,d_1}\} \cup \{i_{2,1}, \dots, i_{2,d_2}\} \cup \dots \cup \{i_{r,1}, \dots, i_{r,d_r}\} = \{1, \dots, n\}$$

gilt. Dann definieren wir die Permutation π, sodass

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & n \\ i_{1,1} & i_{1,2} & \dots & i_{1,d_1} & i_{2,1} & \dots & i_{2,d_2} & \dots & i_{r,1} & \dots & i_{r,d_r}. \end{pmatrix}$$

Damit gilt

$$\pi\tau\pi^{-1} = (1\ 2\ \dots\ d_1)(d_1+1\ \dots\ d_1+d_2)\cdots(\sum_{i=1}^{r-1} d_i + 1\ \dots\ \sum_{i=1}^{r} d_r).$$

Offensichtlich hängt die Permutation auf der rechten Seite nur von der Partition $n = \sum_{i=1}^{r} d_i$ ab. Also ist die Behauptung bewiesen. □

Aufgabe 1.52. Zeige, dass die folgende Formel für alle $\pi \in \mathrm{S}_n$ gilt:

$$\operatorname{sgn}(\pi) = \prod_{1 \le i < j \le n} \frac{\pi(j) - \pi(i)}{j - i}.$$

Folgere daraus, dass $\operatorname{sgn} : \mathrm{S}_n \to \{1, -1\}$ ein Gruppenhomomorphismus ist.

Lösung. Siehe de.wikipedia.org/wiki/Vorzeichen_(Permutation). □

Aufgabe 1.53. Zeige:

(a) Für $n \ge 3$ wird die Gruppe A_n von 3-Zyklen erzeugt. (Hinweis: Schreibe die Permutation (1 2)(3 4) als Produkt von 3-Zyklen in A_4, und finde dann eine allgemeine Regel für A_n.)

(b) Für $n \ge 5$ gilt

$$\mathrm{A}_n = \langle\, (i\ j)(k\ l) \mid i, j, k, l \text{ paarweise verschieden} \,\rangle.$$

Lösung. (a) Es sei $H \le \mathrm{S}_n$ die von allen 3-Zyklen erzeugte Untergruppe. Zu zeigen ist $H = \mathrm{A}_n$.

Das Signum von einem d-Zyklus ist $(-1)^{d+1}$, also gilt $H \subseteq \mathrm{A}_n$.

Nun sei $\tau \in \mathrm{A}_n$ beliebig. Dann ist τ das Produkt von r (nicht notwendig disjunkten) Transpositionen $\tau = \sigma_1 \cdots \sigma_r$ mit r gerade, denn es gilt $1 = \operatorname{sgn}(\tau) = \prod_{i=1}^{r} \operatorname{sgn}(\sigma_i) = (-1)^r$. Angenommen, $r \ge 2$ (sonst $\tau = \mathrm{id}$), seien $\sigma_1 = (i\ j)$ und $\sigma_2 = (k\ l)$. Setze $I = \{i, j, k, l\}$. Da $i \ne j$, gilt $2 \le |I| \le 4$.

Ist $|I| = 2$, d. .h. $\{i, j\} = \{k, l\}$, so gilt $\sigma_1 = \sigma_2$ und damit $\tau = \sigma_3 \cdots \sigma_r$. Ist $|I| = 3$, so können wir ohne Einschränkung der Allgemeinheit annehmen, dass $j = l$. Dann gilt $\tau = (i\ j)(k\ j)\sigma_3 \cdots \sigma_r = (i\ j\ k)\sigma_3 \cdots \sigma_r$. Ist schließlich $|I| = 4$, so gilt $\tau = (i\ j)(k\ j)\sigma_3 \cdots \sigma_r = (k\ j\ l)(i\ k\ j)\sigma_3 \cdots \sigma_r$. Nun können wir mit $\tau' = \sigma_3 \cdots \sigma_r$ per Induktion auf r argumentieren und damit zeigen, dass τ ein Produkt von 3-Zyklen ist. Damit gilt $H \supseteq \mathrm{A}_n$, also $H = \mathrm{A}_n$ wie gewünscht.

(b) Es sei $n \ge 5$ und $K = \langle\, (i\ j)(k\ l) \mid i, j, k, l \text{ paarweise verschieden} \,\rangle \le \mathrm{S}_n$. Klar gilt $K \subseteq \mathrm{A}_n$. Ist $\sigma = (i\ j\ k)$ ein 3-Zyklus, so gibt es $l, m \in \{1, \dots, n\}$, sodass i, j, k, l, m paarweise verschieden sind. Es gilt $(i\ j\ k) = (i\ l)(j\ m)(j\ l)(i\ m)(l\ m)(j\ k)$, also ist jeder 3-Zyklus in K. Nach (a) wird A_n von 3-Zyklen erzeugt. Dementsprechend gilt $\mathrm{A}_n \subseteq K$ und damit $\mathrm{A}_n = K$. □

Aufgabe 1.54. Zeige: Für alle $n \ge 1$ gilt $\mathrm{K}(\mathrm{S}_n) = \mathrm{A}_n$.

Lösung. Für $n = 1, 2$ können wir das einfach ausrechnen. Es sei nun $n \geq 3$. Für alle $\sigma, \tau \in \mathrm{S}_n$ gilt

$$\operatorname{sgn}([\sigma, \tau]) = \operatorname{sgn}(\sigma\tau\sigma^{-1}\tau^{-1}) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)\operatorname{sgn}(\sigma^{-1})\operatorname{sgn}(\tau^{-1}) = \operatorname{sgn}(\sigma)^2\operatorname{sgn}(\tau)^2 = 1 \cdot 1 = 1,$$

also $[\sigma, \tau] \in \mathrm{A}_n$ und damit $\mathrm{K}(\mathrm{S}_n) \subseteq \mathrm{A}_n$. Nach Aufgabe 1.53 wird A_n aus 3-Zyklen erzeugt. Aber jeder 3-Zyklus ist ein Kommutator, denn es gilt

$$(i\ j\ k) = (j\ k)(i\ j)(j\ k)(i\ j) = (i\ j\ k) = [(j\ k), (i\ j)].$$

Daher ist auch $\mathrm{K}(\mathrm{S}_n) \supseteq \mathrm{A}_n$, also $\mathrm{K}(\mathrm{S}_n) = \mathrm{A}_n$. □

Aufgabe 1.55. Es sei G eine Gruppe und $\mathrm{Z}(G)$ ihr Zentrum. Zeige:

(a) Es gilt $\mathrm{Z}(G) \trianglelefteq G$.
(b) Genau dann ist G abelsch, wenn $G = \mathrm{Z}(G)$.
(c) Falls $G/\mathrm{Z}(G)$ zyklisch ist, dann ist G abelsch.

Lösung. Aussage (a) folgt von der Tatsache, dass $\mathrm{Z}(G)$ der Kern von einer Gruppenoperation ist. Aussage (b) ist trivial.

(c) Nehmen wir an, dass $G \neq \mathrm{Z}(G)$. Es sei $g \in G$, sodass $\bar{g} = g\,\mathrm{Z}(G)$ ein Erzeuger von $G/\mathrm{Z}(G)$ ist. Insbesondere $g \notin \mathrm{Z}(G)$, also gibt es $h \in G$ mit $gh \neq hg$. Da $G/\mathrm{Z}(G)$ von $\bar{g}$ erzeugt wird, muss $\bar{h} = \bar{g}^n$ für ein gewisses $n \in \mathbb{Z}$ sein, also $h = g^n a$ für ein $a \in \mathrm{Z}(G)$. Aber dann ist

$$gh = gg^n a = g^{n+1}a = g^n ga = g^n ag = hg,$$

was ein Widerspruch zu $gh \neq hg$ ist. Wir schließen, dass $G = \mathrm{Z}(G)$, d. h., G ist abelsch. □

Aufgabe 1.56. Die Gruppe G operiere auf der Menge $X \neq \emptyset$. Für $1 \leq k \leq |X|$ heißt die Operation *k-fach transitiv*, wenn es zu beliebigen, paarweise verschiedenen Elementen $x_1, \ldots, x_k \in X$ und beliebigen, paarweise verschiedenen Elementen $y_1, \ldots, y_k \in X$ stets ein $g \in G$ gibt mit $g \cdot x_i = y_i$ für $1 \leq i \leq k$. Zeige:

(a) Der Stabilisator G_x von $x \in X$ operiert auf $X \setminus \{x\}$.
(b) Angenommen, die Operation von G auf X ist transitiv, ist sie k-fach transitiv für $k \geq 2$ genau dann, wenn für ein $x \in X$ der Stabilisator G_x noch $(k-1)$-transitiv auf $X \setminus \{x\}$ operiert.
(c) Die Gruppe S_n operiert n-fach transitiv auf $\{1, \ldots, n\}$.
(d) Für $n \geq 3$ operiert A_n auf $\{1, \ldots, n\}$ noch $(n-2)$-fach transitiv.

Lösung. (a) Es sei $g \in G_x$ und $y \in X \setminus x$. Da G_x eine Untergruppe ist, gilt auch $g^{-1} \in G_x$. Es kann nicht sein, dass $g \cdot y = x$, sonst wäre $y = (g^{-1}g) \cdot y = g^{-1} \cdot (g \cdot y) = g^{-1} \cdot x = x$. Also $g \cdot y \in X \setminus \{x\}$, d. h., G_x operiert auf $X \setminus \{x\}$.

(b) Nehmen wir zunächst an, dass G k-fach transitiv auf X operiert mit $k \geq 2$. Es sei $x \in X$ beliebig. Es seien $x_1, \ldots, x_{k-1} \in X \setminus \{x\}$ paarweise verschieden und $y_1, \ldots, y_{k-1} \in X \setminus \{x\}$ auch paarweise verschieden. Dann sind $x_1, \ldots, x_{k-1}, x$ paarweise verschieden, genauso wie $y_1, \ldots, y_{k-1}, x$. Da die Operation k-fach transitiv ist, gibt es $g \in G$ mit $g \cdot x_i = y_i$ für $1 \leq i \leq k-1$ und $g \cdot x = x$, sprich $g \in G_x$. Das bedeutet: G_x operiert $(k-1)$-fach transitiv auf $X \setminus \{x\}$.

Umgekehrt nehmen wir an, dass G_x noch $(k-1)$-fach transitiv auf $X \setminus \{x\}$. Es seien $x_1, \dots, x_k \in X$ paarweise verschieden und $y_1, \dots, y_k \in X$ paarweise verschieden. Wir wollen $g \in G$ finden mit $g \cdot x_i = y_i$. Nach Voraussetzung ist die Operation von G transitiv auf X, also gibt es $g_1, g_2 \in G$ mit $g_1 \cdot x_k = x$ und $g_2 \cdot y_k = x$. Definiere $x_i' = g_1 \cdot x_i$ und $y_i' = g_2 \cdot y_i$ für $1 \leq i \leq k-1$. Wie oben können wir argumentieren, dass $x_1', \dots, x_{k-1}' \in X \setminus x$ paarweise verschieden sind, genauso wie $y_1', \dots, y_{k-1}' \in X \setminus x$. Dann finden wir $h \in G_x$ mit $h \cdot x_i' = y_i'$ für $1 \leq i \leq k-1$. Setze $g = g_2^{-1} h g_1$. Dann gilt wie gewünscht $g \cdot x_i = g_2^{-1} \cdot (h \cdot (g_1 \cdot x_i)) = g_2^{-1} \cdot (h \cdot x_i') = g_2^{-1} \cdot y_i' = y_i$ für $1 \leq i \leq k-1$ und $g \cdot x_k = g_2^{-1} \cdot (h \cdot (g_1 \cdot x_k)) = g_2^{-1} \cdot (h \cdot x) = g_2^{-1} \cdot x = y_k$.

(c) Wir wissen, dass für jedes $n \geq 1$ die Gruppe S_n transitiv auf $X = \{1, \dots, n\}$ operiert. Klar operiert S_2 2-fach transitiv auf $\{1, 2\}$. Nun sei $x = n \geq 3$ und $G = \mathrm{S}_n$. Per Induktion auf n operiert $G_x \cong \mathrm{S}_{n-1}$ noch $(n-1)$-fach transitiv auf $X \setminus \{x\} = \{1, \dots, n-1\}$. Nach (b) operiert dann $G = \mathrm{S}_n$ n-fach transitiv auf $X = \{1, \dots, n\}$.

(d) Es seien $x_1, \dots, x_{n-2} \in \{1, \dots, n\}$ paarweise verschieden und $y_1, \dots, y_{n-2} \in \{1, \dots, n\}$ auch. Dann gibt es noch $x_{n-1}, x_n, y_{n-1}, y_n \in \{1, \dots, n\}$, sodass $x_1, \dots, x_n$ und $y_1, \dots, y_n$ jeweils paarweise verschieden sind. Nach (b) gibt es $\pi \in \mathrm{S}_n$ mit $\pi \cdot x_i = y_i$ für $1 \leq i \leq n$. Dann ist entweder $\pi \in \mathrm{A}_n$ oder $\pi' = (y_{n-1}\ y_n)\pi \in \mathrm{A}_n$. Da auch $\pi' \cdot x_i = y_i$ für $1 \leq i \leq n-2$, ist die Operation von A_n auf $\{1, \dots, n\}$ noch $(n-2)$-transitiv. □

Bemerkung 1.57. Mehrfache Transitivität ist eine sehr starke Bedingung. Es gilt der Satz: Die einzigen 4-fach transitiven Gruppen sind S_n $(n \geq 4)$, A_n $(n \geq 6)$ und vier weitere Gruppen, von denen die kleinste die in Beispiel 1.23 erwähnte Mathieu-Gruppe M_{11} ist (siehe `en.wikipedia.org/wiki/Mathieu_group`).

Aufgabe 1.58. Bestimme das Zentrum von S_n und das Zentrum von A_n.

Lösung. Man kann einfach ausrechnen (zum Beispiel mit `SymmetricGroup`, `AlternatingGroup` und `Centre` in GAP), dass $\mathrm{Z}(\mathrm{S}_2) = \mathrm{S}_2$, $\mathrm{Z}(\mathrm{A}_2) = \mathrm{A}_2 = \{\mathrm{id}\}$, $\mathrm{Z}(\mathrm{S}_3) = \{\mathrm{id}\}$, $\mathrm{Z}(\mathrm{A}_3) = \mathrm{A}_3$, $\mathrm{Z}(\mathrm{S}_4) = \{\mathrm{id}\}$, $\mathrm{Z}(\mathrm{A}_4) = \{\mathrm{id}\}$. Wir behaupten, dass $\mathrm{Z}(\mathrm{S}_n) = \mathrm{Z}(\mathrm{A}_n) = \{\mathrm{id}\}$ für alle $n \geq 5$.

Es sei also $n \geq 5$ fest. Es gilt $\mathrm{Z}(\mathrm{A}_n) \trianglelefteq \mathrm{A}_n$ und wir wissen, dass A_n einfach und nicht abelsch ist. Daher gilt $\mathrm{Z}(\mathrm{A}_n) = \{\mathrm{id}\}$.

Es sei nun $\tau \in \mathrm{Z}(\mathrm{S}_n)$ beliebig. Dann $\tau^2 \in \mathrm{Z}(\mathrm{S}_n) \cap \mathrm{A}_n \subseteq \mathrm{Z}(\mathrm{A}_n) = \{\mathrm{id}\}$, d. h. $\tau^2 = \mathrm{id}$. Dementsprechend ist τ das Produkt von r disjunkten Transpositionen. (Es gilt nämlich: Ist $\tau = \sigma_1 \cdots \sigma_r$ das Produkt von disjunkten Zyklen der Länge $d_1, \dots, d_r$, so gilt $\mathrm{Ord}(\tau) = \mathrm{kgV}(d_1, \dots, d_r)$.)

Ist $r = 1$, so gilt $\tau = (i\ j)$. Wähle $k \in \{1, \dots, n\} \setminus \{i, j\}$ und setze $\sigma = (j\ k)$. Dann gilt $\sigma\tau = (i\ k\ j) \neq (i\ j\ k) = \tau\sigma$, also $\tau \notin \mathrm{Z}(\mathrm{S}_n)$, Widerspruch. Ist $r \geq 1$, so gilt $\tau = (i\ j)(k\ l)\sigma_3 \cdots \sigma_r$. Setze $\sigma = (j\ k)$. Dann gilt $\sigma\tau = (i\ k\ l\ j)\sigma_3 \cdots \sigma_r \neq (i\ j\ l\ k)\sigma_3 \cdots \sigma_r = \tau\sigma$, also wieder $\tau \notin \mathrm{Z}(\mathrm{S}_n)$, Widerspruch. Dementsprechend ist $r = 0$, d. h. $\tau = \mathrm{id}$, und damit $\mathrm{Z}(\mathrm{S}_n) = \{\mathrm{id}\}$. □

Kapitel 2

Schreier–Sims-Algorithmus

Der Schreier–Sims-Algorithmus ist ein nach dem österreichischen Mathematiker Otto Schreier und dem amerikanischen Mathematiker Charles Sims genannter Algorithmus zur Bestimmung der Ordnung einer endlichen *Permutationsgruppe*, sprich einer Untergruppe $G \leq \mathrm{S}_n$.

2.1 Bahnenalgorithmen

Es seien G eine Gruppe und X eine nicht-leere Menge, auf der G operiert. Zuerst beschreiben wir einen Algorithmus, der die Bahn $\mathcal{O}_x$ von einem vorgegebenem Element $x \in X$ bestimmt.

Bemerkung 2.1. In GAP kann man eine Gruppenoperation durch eine GAP-Funktion `acts` beschreiben, die ein Element `x` von X und ein Element `g` von G annimmt und ein Element `acts(x,g)` von X rausgibt. Als in anderen Computeralgebrasystemen wie SAGE werden *rechte* statt linke Gruppenoperationen bevorzugt. Die Standardoperation von S_n auf $\{1, \dots, n\}$ heißt `OnPoints`. Alternativ kann man `OnPoints(x,g)` mit `x^g` abkürzen.

```
1 gap> g:= (2,4,5)(3,6);;
2 gap> x:= 4;;
3 gap> x^g;
4 5
5 gap> OnPoints(1,g);
6 1
```

Algorithmus 2.2 (Allgemeiner Bahnenalgorithmus)**.** Input: ein endliches Erzeugendensystem S einer Gruppe G, ein Element x einer G-Menge X. Output: die Bahn $O = \mathcal{O}_x$ von x unter G.

Es ist keine gute Idee, zu versuchen, zuerst die komplette Menge G zu bestimmen. Die Gruppe G kann nämlich riesig im Vergleich zur Bahn $\mathcal{O}_x$ sein. Zum Beispiel: $G = \mathrm{S}_n$ und $\mathcal{O}_x = \{1, \dots, n\}$.

Beschreibung. Wir beschreiben den Algorithmus als GAP-Funktion:

```
1  bahn:= function(S,x,acts)
2      O:= [x];                          # Initialisierung
3      i:= 1;
4      while i <= Length(O) do           # Schleife
5          y:= O[i];
6          for g in S do
7              y1:= acts(y,g);
8              if not y1 in O then
9                  Add(O,y1);
10             fi;
11         od;
12         i:= i+1;
13     od;
14     return O;
15 end
```

Nach Konstruktion gehören nämlich alle Elemente in O zur Bahn $\mathcal{O}_x$. Umgekehrt gilt nach Konstruktion $g \cdot y \in O$ für jedes $y \in O$ und $g \in S$. Wegen $G = \langle S \rangle$ folgt $g \cdot O \subseteq O$ für alle $g \in G$, also ist O Vereinigung von Bahnen. Die Schleife bricht ab, weil nach jeder Runde i erhöht wird und irgendwann größer als $|O|$ wird. □

Bemerkung 2.3. In modernen Programmiersprachen wie GAP kann man den Code ein bisschen besser organisieren:

```
1  bahn:= function(S,x,acts)
2      O:= [x];                          # Initialisierung
3      for y in O do                     # Schleife
4          for g in S do
5              y1:= acts(y,g);
6              if not y1 in O then
7                  Add(O,y1);
8              fi;
9          od;
10     od;
11     return O;
12 end;
```

Man braucht nämlich nicht den extra Index i und die Abfrage $i \leq |O|$, sondern die Schleife läuft durch über O, welches im Verlauf der Rechnung größer wird. Man stelle sich O als Liste vor, die rechts weiter aufgefüllt wird, und y ist ein Index, der ganz links in der List anfängt und dann Schritt für Schritt nach rechts geht.

Wir benötigen noch eine Ergänzung zum allgemeinen Bahnenalgorithmus (Algorithmus 2.2).

Es sei $\mathcal{O}_x = \{x_1, \dots, x_m\}$ mit $x_1 = x$. Dann möchten wir auch noch Elemente $t_1, \dots, t_m \in G$ mit $t_i \cdot x = x_i$ für $1 \leq i \leq m$ (mit $t_1 = 1$).

Algorithmus 2.4 (Ergänzter Bahnenalgorithmus)**.** Input: ein endliches Erzeugendensystem S einer Gruppe G, ein Element x einer G-Menge X. Output: das Paar (O, T), wobei O die Bahn $\mathcal{O}_x = \{x_1, \dots, x_m\}$ von x unter G ist und T eine Liste von Elementen $T = [t_1, \dots, t_m]$ mit $x_i = t_i \cdot x$.

Beschreibung. Der GAP-Befehl für das neutrale Element einer Gruppe G heißt `One(G)` (siehe [4, §31.10-2]).

```
1  bahn2:= function(S,x,acts)
2      O:= [x];                          # Initialisierung
3      T:= [One(Group(S))];
4      i:= 1;
5      while i <= Length(O) do           # Schleife
6          y:= O[i];
7          for g in S do
8              y1:= acts(y,g);
9              if not y1 in O then
10                 Add(O,y1);
11                 Add(T,T[i]*g);        # einziger Unterschied
12             fi;
13         od;
14         i:= i+1;
15     od;
16     return [O,T];
17 end;
```

Wir müssen `T[i]*g` statt `g*T[i]` schreiben, denn GAP-Gruppen operieren rechts. □

Bemerkung 2.5. Es sei $\mathcal{O}_x = \{x_1, \dots, x_m\}$ die Bahn (mit $x_1 = x$) und G_x der Stabilisator von x (Bezeichnung 1.31). Es seien wie oben $t_1, \dots, t_m \in G$ mit $t_1 = 1$ und $x_i = t_i \cdot x$. Aus dem Bahnensatz (Satz 1.32) folgt

$$G/G_x = \dot{\bigcup}_{i=1,\dots,m} t_i G_x.$$

Die Teilmenge $T = \{t_1, \dots, t_m\}$ ist also ein Vertretersystem der Nebenklassen von G nach G_x.

2.2 Schreiers Untergruppenlemma

Es sei G eine beliebige Gruppe, $S \subseteq G$ eine Teilmenge mit $G = \langle S \rangle$, $H \leq G$ eine beliebige Untergruppe und $T \subseteq G$ ein Nebenklassenvertretersystem von H in G, d. h.

$$G = \dot{\bigcup}_{t \in T} tH.$$

Ohne Einschränkung der Allgemeinheit können wir annehmen dass $1 \in T$. Wir definieren die Abbildung $\tau : G \to T$ (genannt *Schnitt*), indem wir $\tau(g)$ gleich demjenigen eindeutigen Element $t \in T$ mit $gH = tH$ setzen. Also gilt

$$\tau(g)H = gH$$

für alle $g \in G$. Da $1 \in T$, gilt $\tau(h) = 1$ für jedes $h \in H$.

Lemma 2.6. *Jedes Element der Form $\tau(g)^{-1}g$ mit $g \in G$ liegt in H.*

Beweis. Es gilt nämlich

$$\tau(g)^{-1}gH = \tau(g)^{-1}(gH) = \tau(g)^{-1}(\tau(g)H) = (\tau(g)^{-1}\tau(g))H = H. \qquad \square$$

Satz 2.7 (Schreiers Untergruppenlemma)**.** *Mit obigen Bezeichungen und angenommen, dass $s^{-1} \in S$ für jedes $s \in S$, gilt*

$$H = \langle\, \tau(st)^{-1}st \mid s \in S,\, t \in T \,\rangle.$$

Beweis. Die Inklusion $H \supseteq \langle\, \tau(st)^{-1}st \mid s \in S,\, t \in T \,\rangle$ folgt unmittelbar von Lemma 2.6.

Es sei nun $h \in H$ ein beliebiges Element. Wegen der Annahme können wir $s_1, \dots, s_k \in S$ finden mit $h = s_1 s_2 \cdots s_k$. Für $0 \le i \le k$ setze

$$t_i := \tau(s_{i+1} \cdots s_k).$$

Insbesondere $t_0 = \tau(s_1 \cdots s_k) = \tau(h) = 1$ und $t_k = \tau(1) = 1$. Damit erhalten wir

$$h = (t_0^{-1}s_1t_1)(t_1^{-1}s_2t_2) \cdots (t_{k-1}^{-1}s_kt_k). \tag{2.1}$$

Nun bemerken wir, dass

$$\begin{aligned}(s_it_i)H &= s_i(t_iH) = s_i(\tau(s_{i+1} \cdots s_k)H) = s_i(s_{i+1} \cdots s_kH)\\ &= s_is_{i+1} \cdots s_kH = \tau(s_is_{i+1} \cdots s_k)H = t_{i-1}H.\end{aligned}$$

Per Definition von τ gilt also $\tau(s_it_i) = t_{i-1}$ für $1 \le i \le k$. Damit können wir (2.1) umschreiben:

$$h = (\tau(s_1t_1)^{-1}s_1t_1)(\tau(s_2t_2)^{-1}s_2t_2) \cdots (\tau(s_kt_k)^{-1}s_kt_k).$$

Wir sehen also, dass h das Produkt von Elementen der Form $\tau(st)^{-1}st$ mit $s \in S$ und $t \in T$ ist. $\square$

Folgerung 2.8. *Ist G endlich erzeugt und $H \le G$ eine Untergruppe des endlichen Index, so ist auch H endlich erzeugt.*

Beweis. Falls T ein Nebenklassenvertreter von H ist, ist $|T|$ gleich dem Index von H in G, also endlich. Falls $G = \langle S \rangle$ mit S einer endlichen Teilmenge, können wir ohne Einschränkung annehmen, dass $s^{-1} \in S$ für jedes $s \in S$: Falls nicht, dann fügen wir s^{-1} in S hinzu (die Mächtigkeit von S bleibt endlich). Bei Schreiers Untergruppenlemma (Satz 2.7) wird H von der endlichen Teilmenge $\{\, \tau(st)^{-1}st \mid s \in S,\, t \in T \,\}$ erzeugt. $\square$

Bemerkung 2.9. Folgerung 2.8 ist nicht trivial, denn es gibt endliche erzeugte Gruppen G mit einer Untergruppen H, die nicht endlich erzeugt ist. Zum Beispiel kann man Folgendes zeigen: Die Kommutatorgruppe $H = \mathrm{K}(G)$ der freien Gruppe G über zwei Elemente (siehe Definition 3.1) ist nicht endlich erzeugt.

2.3 Schreier–Sims-Algorithmus

Algorithmus 2.10 (Schreier–Sims)**.** Input: ein endliches Erzeugendensystem S einer Permutationsgruppe $G = \langle S \rangle \subseteq \mathrm{S}_n$. Output: die Ordnung von G.

Beschreibung. 1. Schritt: Finde $x \in \{1, \dots, n\}$ mit $g \cdot x \neq x$ für ein $g \in S$. (Ist $g \cdot x = x$ für alle $g \in S$ und alle $x \in \{1, \dots, n\}$, so $g = \mathrm{id}$ für alle $g \in S$ und damit $G = \{\mathrm{id}\}$.)

2. Schritt: Benutze Algorithmus 2.4, um die Bahn $\mathcal{O}_x \subseteq \{1, \dots, n\}$ zu bestimmen sowie Elemente $t_1, \dots, t_m \in G$ mit $m = |\mathcal{O}_x|$, $\mathcal{O}_x = \{\, t_i \cdot x \mid 1 \leq i \leq m \,\}$ und $t_1 = \mathrm{id}$. Setze $T := \{t_1, \dots, t_m\}$. Dann ist es leicht zu sehen, dass T ein Nebenklassenvertretersystem des Stabilisators $H = G_x$ in G ist.

3. Schritt: In diesem Schritt werden durch Schreiers Untergruppenlemma (Satz 2.7) Erzeuger des Stabilisators $H = G_x$ gefunden. Wir benutzen die GAP-Funktion `First` (siehe [4, §21.20-22]).

```
1 R = [];
2 for s in S do
3     for t in T do
4         y:= x^(t*s);
5         r:= First(T, t -> x^t = y);
6         Add(R, t*s*r^-1);
7     od;
8 od;
```

Es gilt nämlich $\tau(st) = r$, denn per Konstruktion $r \in T$ und $st \cdot x = r \cdot x$, also $r^{-1}st \in G_x$, d. h. $rG_x = stG_x$. (Immer wegen Rechts-/Linksoperationen schreiben wir `t*s*r^-1` statt `r^-1*s*t`).

4. Schritt: Fahre fort mit Rekursion, wende analoges Verfahren auf die Untergruppe $H = G_x$ an. Wegen $|G| = |\mathcal{O}_x| \cdot |G_x|$ und $|\mathcal{O}_x| > 1$, da $g \cdot x \neq x$, muss $|G_x| < |G|$ sein. Die Schleife bricht also ab. □

Beispiel 2.11. Wir können nun die Mächtigkeit der in Beispiel 1.23 definierten Mathieu-Gruppe $\mathrm{M}_{11} \leq \mathrm{S}_{11}$ berechnen: $|\mathrm{M}_{11}| = 7920$.

Beispiel 2.12. Um die Mächtigkeit der in Beispiel 1.24 definierten Janko-Gruppe $\mathrm{J}_1 = \langle A, B \rangle \leq \mathrm{GL}_7(\mathbb{F}_{11})$ zu bestimmen, müssen wir sie zuerst in eine geschickte Permutationsgruppe umwandeln. Klar operiert J_1 auf dem Vektorraum $V = \mathbb{F}_{11}^7$ und auf dem projektiven Raum $\mathbb{P}(V)$, aber diese Mengen sind viel zu groß, denn sie haben $11^7 \approx 20\,000\,000$ bzw. $(11^7 - 1)/10 \approx 2\,000\,000$ Elemente.

Die Gruppe J_1 operiert aber auch auf jede Bahn $\mathcal{O}_p \subseteq \mathbb{P}(V)$ von $p \in \mathbb{P}(V)$ unter J_1. Die Idee ist also ein p zu suchen, damit die Bahn $\mathcal{O}_p$ möglichst klein ist. Falls $p = [v]$ mit $v \in V$ ein Eigenvektor

von $C \in \mathrm{J}_1$, dann $\langle C \rangle \subseteq \mathrm{Stab}_{\mathrm{J}_1}(p)$, also $\mathrm{Ord}(C) \mid |\mathrm{Stab}_{\mathrm{J}_1}(p)|$. Je größer $\mathrm{Ord}(C)$ ist, desto größer ist $|\mathrm{Stab}_{\mathrm{J}_1}(p)|$, also desto kleiner ist $|\mathcal{O}_p|$ wegen des Bahnensatzes (Satz 1.32).

Zum Beispiel, das Produkt $C = BABAB$ hat Ordnung 11 und einen 1-dimensionalen Eigenraum $p = [v]$ zum Eigenwert 1. Übrigens $|\mathcal{O}_p| = 1540$. Da $\mathcal{O}_p$ eine Basis von $V = \mathbb{F}_{11}^7$ enthält, gibt es einen injektiven Homomorphismus $\varphi : \mathrm{J}_1 \to \mathrm{S}_{1540}$. Nachdem wir die Bilder $\varphi(A)$ und $\varphi(B)$ bestimmt haben, können wir den Schreier–Sims-Algorithmus anwenden: Wir finden $|\mathrm{J}_1| = 175560$.

2.4 Membership-Test

Algorithmus 2.13 (Membership-Test)**.** Input: S ein endliches Erzeugendensystem einer Permutationsgruppe $G = \langle S \rangle \subseteq \mathrm{S}_n$, ein Element $g \in \mathrm{S}_n$. Output: `True` falls $g \in G$, sonst `False`.

Beschreibung. 1. Schritt. Es sei $x \in \{1, \dots, n\}$ wie im 1. Schritt von Algorithmus 2.10. Berechne das Paar $(\mathcal{O}_x, T)$ mit Algorithmus 2.4. Falls $g \cdot x \notin \mathcal{O}_x$, so ist $g \notin G$, also ist die Antwort `False`. Es sei nun $g \cdot x \in \mathcal{O}_x$ und $t \in T$ mit $g \cdot x = t \cdot x$. Dann $t^{-1}g \cdot x = x$. Das bedeutet, dass $g \in G$ genau dann, wenn $t^{-1}g \in G_x$.

2. Schritt. Wende Rekursion auf G_x an, um $t^{-1}g \in G_x$ zu testen. (Mit dem Schritt 3. aus Algorithmus 2.10 erhalten wir ein endliches Erzeugendensystem von G_x. □

Bemerkung 2.14. Das vom Schreier–Sims-Algorithmus produzierte Erzeugendensystem von G_x enthält viele überflüssige Elemente. Um einen optimalen Algorithmus zu erhalten, sollte man dieses Problem näher studieren (siehe dazu [1, §1.14]).

2.5 Aufgaben

Aufgabe 2.15. Mache dich mit dem Computeralgebrasystem GAP vertraut (dies ist frei verfügbar unter `www.gap-system.org`). Einen guten Einstieg liefert das Tutorial unter `www.gap-system.org/Manuals/doc/tut/chap0.html`. Dort wird insbesondere Kapitel 5 zu Gruppen für uns interessant sein.

(a) Lese in `www.gap-system.org/Doc/Examples/rubik.html` wie man Rubiks Zauberwurfel mit GAP untersuchen kann.

(b) Es sei $G \leq \mathrm{S}_n$, gegeben durch endlich viele erzeugende Elemente. Schreibe ein Programm, welches testet, ob die Operation von G auf $\{1, \dots, n\}$ transitiv bzw. k-fach transitiv für $k \geq 1$ ist (siehe Aufgabe 1.56). Teste mit deinem Programm die Mathieu-Gruppe M_{11}.

Kapitel 3

Präsentationen

Außer Permutationen und Matrizen gibt es noch mindestens eine weitere allgemeine Methode, um Gruppen zu konstruieren.

3.1 Freie Gruppen

Definition 3.1. Es sei F eine Gruppe und $S \subseteq F$ ein Erzeugendensystem für F. Dann heißt F *freie Gruppe auf* S, wenn es zu jeder Gruppe G und jeder Abbildung $f : S \to G$ stets einen Gruppenhomomorphismus $\varphi : F \to G$ gibt mit $\varphi|_S = f$.

Da $F = \langle S \rangle$ ist dann φ eindeutig bestimmt.

Beispiel 3.2. Die triviale Gruppe $F = \{1\}$ ist eine freie Gruppe auf $S = \emptyset$.

Beispiel 3.3. Die Gruppe $F = (\mathbb{Z}, +)$ ist eine freie Gruppe auf $S = \{1\}$. Es gilt nämlich $\mathbb{Z} = \langle 1 \rangle$ und für jede beliebige Gruppe G und Abbildung $f : S \to G$ mit $f(1) = g \in G$ können wir den Homomorphismus $\varphi : F \to G$, $m \mapsto g^m$ definieren, der die Bedingung $\varphi|_S = f$ erfüllt.

Satz 3.4 (Hauptsatz)**.** *Für jede beliebige Menge S gibt es eine Gruppe F mit $S \subseteq F$, sodass F frei auf S ist. Die Gruppe F ist bis auf Isomorphie eindeutig bestimmt.*

Beweis. Zuerst beweisen wir die Eindeutigkeit. Es sei auch $F' \supseteq S$ eine freie Gruppe auf S. Ist $f : S \to F'$ die Inklusion, dann gibt es einen Homomorphismus $\varphi : F \to F'$ mit $\varphi|_S = f$, weil F frei ist. Analog: Ist $g : S \to F$ die Inklusion, dann gibt es einen Homomorphismus $\psi : F' \to F$ mit $\psi|_S = g$, weil F' frei ist. Für alle $s \in S$ gilt

$$\psi \circ \varphi(s) = \psi \circ f(s) = \psi(s) = s.$$

Dann ist $\psi \circ \varphi = \mathrm{id}_F$, denn F wird von S erzeugt. Analog ist $\varphi \circ \psi = \mathrm{id}_{F'}$, also $F \cong F'$.

Jetzt wollen wir die Existenz beweisen. Ist $S = \emptyset$, so können wir die triviale Gruppe $F = \{1\}$ nehmen (siehe Beispiel 3.2). Nehmen wir nun $S \neq \emptyset$ an. Es seien $\bar{S}$ eine Menge, die gleichmächtig zu S ist und

$$S \to \bar{S}, \quad s \mapsto \bar{s}$$

eine Bijektion. Wir definieren auch $\bar{\bar{s}} = s$. Es seien $A = S \cup \bar{S}$, $X_0 = \{()\}$ und

$$X_n = \{ (x_1, \dots, x_n) \mid x_i \in A \}.$$

für $n \geq 1$. Wir setzen $W = \bigcup_{n \geq 0} X_n$, die Menge aller *Wörter* endlicher Länge in $A = S \cup \bar{S}$.

Wir sagen, dass ein Wort $w = (w_1, \dots, w_n) \in W$ *reduziert* ist, wenn $w_{i+1} \neq \bar{w}_i$ für alle i gilt. (Das leere Wort ( ) wird auch als reduziert bezeichnet.) Es sei $W_{\text{red}} = \{ w \in W \mid w \text{ ist reduziert} \}$ die Teilmenge aller reduzierten Wörter. Wir identifizieren A mit den Wörtern (x) mit einer Buchstabe $x \in A$. Dann $S \subset A \subset W_{\text{red}}$.

Wir definieren folgende Multiplikation auf W_{red}. Es seien $u = (u_1, \dots, u_n)$ und $v = (v_1, \dots, v_m) \in W_{\text{red}}$. Dann setzen wir

$$u \bullet v = (u_1, \dots, u_{n-r}, v_{r+1}, \dots, v_m) \in W_{\text{red}},$$

wobei $r \geq 0$ dadurch bestimmt ist, dass $u_n = \bar{v}_1, u_{n-1} = \bar{v}_2, \dots, u_{n-r+1} = \bar{v}_r$ und $u_{n-r} \neq \bar{v}_{r+1}$. Wir haben dann folgende Regel:

$$(u_1, \dots, u_n) \bullet (v_1, \dots, v_m) = (u_1, \dots, u_{n-1}) \bullet (v_2, \dots, v_m), \text{ falls } u_n = \bar{v}_1. \tag{3.1}$$

Wir behaupten: Damit wird $(W_{\text{red}}, \bullet)$ eine Gruppe. Offenbar ist ( ) das neutrale Element. Ist $w = (w_1, \dots, w_n) \in W_{\text{red}}$, so setze $\bar{w} = (\bar{w}_n, \dots, \bar{w}_1) \in W_{\text{red}}$. Dann $w \bullet \bar{w} = \bar{w} \bullet w = ()$, also ist $\bar{w}$ das inverse Element zu w. Es bleibt noch zu zeigen, dass $\bullet$ assoziativ ist. Es seien also $u = (u_1, \dots, u_l), v = (v_1, \dots, v_m), w = (w_1, \dots, w_n) \in W_{\text{red}}$.

Behauptung 3.5. $(u \bullet v) \bullet w = u \bullet (v \bullet w)$.

Beweis der Behauptung per Induktion auf m. Ist $m = 0$, so $v = ()$ und die Aussage gilt. Es sei nun $m = 1$, also $v = (x)$ mit $x \in A$. Wir unterscheiden vier Fälle, je nachdem ob $u_l = \bar{x}$ oder $u_l \neq \bar{x}$ und $w_1 = \bar{x}$ oder $w_1 \neq \bar{x}$. Zum Beispiel (die anderen drei Fälle können analog bewiesen werden), ist $u_l \neq \bar{x}$ und $w_1 = \bar{x}$, dann ist $u \bullet v = (u_1, \dots, u_l, x)$ und $v \bullet w = (w_2, \dots, w_n)$. Mit (3.1) folgt

$$(u \bullet v) \bullet w = (u_1, \dots, u_l, x) \bullet (w_1, \dots, w_n) = (u_1, \dots, u_l) \bullet (w_2, \dots, w_n) = u \bullet (v \bullet w).$$

Es sei schließlich $m > 1$. Definiere $v' = (v_1, \dots, v_{m-1})$ und $v'' = (v_m)$, damit $v = v' \bullet v''$. Wir wenden dann Induktion auf v' und den Fall $m = 1$ auf v'' an und erhalten

$$\begin{aligned}(u \bullet v) \bullet w = (u \bullet (v' \bullet v'')) \bullet w = ((u \bullet v') \bullet v'') \bullet w = (u \bullet v') \bullet (v'' \bullet w) \\ = u \bullet (v' \bullet (v'' \bullet w)) = u \bullet ((v' \bullet v'') \bullet w) = u \bullet (v \bullet w),\end{aligned}$$

was zu zeigen war. □

Zum Schluss beweisen wir, dass W_{red} frei auf S ist. Es sei $(G, \cdot)$ eine beliebige Gruppe und $f : S \to G$ eine Abbildung. Wir können f auf A fortsetzen durch $f(\bar{s}) = f(s)^{-1}$ für alle $s \in S$. Wir definieren dann $\varphi : W_{\text{red}} \to G$ durch $\varphi(( )) = 1_G$ und

$$w = (w_1, \dots, w_n) \in W_{\text{red}} \mapsto \varphi(w) = f(w_1) \cdot \dots \cdot f(w_n) \in G.$$

Wir behaupten, dass φ ein Homomorphismus ist. Es seien $u = (u_1, \dots, u_n)$ und $v = (v_1, \dots, v_m) \in W_{\text{red}}$ mit $u_n = \bar{v}_1, u_{n-1} = \bar{v}_2, \dots, u_{n-r+1} = \bar{v}_r$ und $u_{n-r} \neq \bar{v}_{r+1}$. Dann $f(u_n) = f(\bar{v}_1) = f(v_1)^{-1}$, $f(u_{n-1}) = f(v_2)^{-1}, \dots, f(u_{n-r+1}) = f(v_r)^{-1}$, also

$$\begin{aligned}\varphi(u) \cdot \varphi(v) &= f(u_1) \cdot \dots \cdot f(u_{n-r}) \cdot f(u_{n-r+1}) \cdot \dots \cdot f(u_n) \cdot f(v_1) \cdot \dots \cdot f(v_r) \cdot f(v_{r+1}) \cdot \dots \cdot f(v_m) \\ &= f(u_1) \cdot \dots \cdot f(u_{n-r}) \cdot f(v_{r+1}) \cdot \dots \cdot f(v_m) = \varphi(u_1, \dots, u_{n-r}, v_{r+1}, \dots, v_m) = \varphi(u \bullet v),\end{aligned}$$

was wir zeigen wollten. □

Folgerung 3.6. *Jede Gruppe ist isomorph zu einer Faktorgruppe einer freien Gruppe nach einem Normalteiler.*

Beweis. Gegeben eine beliebige Gruppe G, sei $S \subseteq G$ ein Erzeugendensystem und $f : S \to G$ die Inklusion. Beim Satz 3.4 existiert eine freie Gruppe F auf S, also gibt es einen Homomorphismus $\varphi : F \to G$ mit $\varphi|_S = f$. Insbesondere ist $s = f(s) = \varphi(s)$ für jedes $s \in S$. Das impliziert, dass φ surjektiv ist. Es folgt also vom Homomorphiesatz (Satz 1.17), dass $G \cong F / \operatorname{Ker}(\varphi)$. □

3.2 Definition und Beispiele

Definition 3.7. Es sei G eine Gruppe und $R \subseteq G$ eine Teilmenge. Dann heißt

$$\langle\langle R \rangle\rangle = \bigcap_{R \subseteq H \trianglelefteq G} H$$

das *Normalteilerzeugnis von* R oder der *von* R *erzeugte Normalteiler* von G. Dies ist der kleinste Normalteiler von G, der R enthält.

Definition 3.8. Es seien S ein Erzeugendensystem einer Gruppe G, F die freie Gruppe auf S, $\varphi : F \to G$ der surjektive Homomorphismus wie oben und $N = \operatorname{Ker}(\varphi)$ (also $G \cong F/N$). Falls $R \subseteq F$ eine Teilmenge ist mit $N = \langle\langle R \rangle\rangle$, so schreibt man

$$G = \langle\, S \mid R \,\rangle$$

und man nennt diese eine *Präsentation* für G. Die Elemente von S heißen *Erzeuger* und die Elemente von R heißen *(definierende) Relationen*.

Für $r \in R$ ist $r \in N$, also $\varphi(r) = 1$ in G. Man sagt: „Wörter in R werden gleich 1 in G."

Umgekehrt kann man diese Idee auch dazu benutzen, um Gruppen zu konstruieren. Es seien S eine Menge ist, F die freie Gruppe auf S und $R \subseteq F$ eine Teilmenge. Dann definieren wir die Gruppe

$$\langle S \mid R \rangle = F/N,$$

wobei $N = \langle\langle R \rangle\rangle$ der von R erzeugte Normalteiler ist.

Damit bekommt man zwei grundlegende Aufgabenstellungen.

(1) Gegeben eine Gruppe G mit Erzeugendensystem S, sei F die freie Gruppe auf S. Finde möglichst geschickte Teilmenge $R \subseteq F$, sodass $G = \langle S \mid R \rangle$.
(2) Gegeben eine Menge S und eine Teilmenge $R \subseteq F$ der freien Gruppe F auf S, sei $N = \langle\langle R \rangle\rangle$. Konstruiere $G = F/N$. (Zum Beispiel, entscheide ob $|G| = \infty$ oder $|G| < \infty$.)

Zur zweiten Aufgabenstellung gibt es einen wichtigen Satz von Novikov (1955), Booke (1958) und Britton (1963): Es existiert eine endliche Menge S und eine endliche Teilmenge $R \subseteq F$ der freien Gruppe F auf S, sodass das *Wortproblem* in $\langle S \mid R \rangle$ unentscheidbar ist, d. h., es gibt keinen Algorithmus, der in endlich vielen Schritten entscheidet, ob ein gegebenes Wort in F gleich 1 in $\langle S \mid R \rangle$ wird oder nicht (siehe [7, Chapter 12]).

Lemma 3.9 (Relationenlemma)**.** *Es seien F die freie Gruppe auf dem Erzeugendensystem S einer Gruppe G, $\varphi\colon F \to G$ ein surjektiver Homomorphismus wie oben (mit $\varphi|_S = \mathrm{id}$) und $R \subseteq F$ eine Teilmenge mit $\varphi(r) = 1_G$ für alle $r \in R$. Dann ist G isomorph zu einer Faktorgruppe von $\langle S \mid R \rangle$. Insbesondere*

$$|G| \leq |\langle S \mid R \rangle|.$$

Beweis. Es seien $M = \mathrm{Ker}(\varphi)$ und $N = \langle\langle R \rangle\rangle$ (also $\langle S \mid R \rangle = F/N$). Nach Voraussetzung ist $R \subseteq M$, also auch $N \subseteq M$. Definiere $\psi\colon F/N \to F/M$ durch $fN \mapsto fM$. Dies ist wohldefiniert, denn $N \subseteq M$. Klar ist ψ ein surjektiver Homomorphismus. Aus dem Homomorphiesatz (Satz 1.17) folgt dann

$$G \cong F/M \cong (F/N)/\mathrm{Ker}(\psi) = \langle S \mid R \rangle/\mathrm{Ker}(\psi). \qquad \square$$

Beispiel 3.10 (Zyklische Gruppen)**.** Betrachte die zyklische Gruppe $G = \langle g \rangle$ der Ordnung $n \geq 1$. Es sei F die freie Gruppe auf $S = \{x\}$, mit $x = g$ (wir verwenden zwei verschiedene Symbole, um nicht durcheinander zu kommen), und $\varphi\colon F \to G$ der Homomorphismus wie oben mit $\varphi(x) = g$. Es sei $R = \{x^n\} \subset F$. Da $\varphi(x^n) = \varphi(x)^n = g^n = 1_G$, sind die Voraussetzungen des Relationenlemmas (Lemma 3.9) erfüllt. Damit ist G isomorph zu einer Faktorgruppe von $H = \langle x \mid x^n \rangle = F/\langle\langle R \rangle\rangle$. Um zu zeigen, dass eigentlich $G \cong H$ gilt, müssen wir noch zeigen, dass $|H| \leq n$. Dazu bemerken wir, dass $F = \langle x \rangle$ per Definition, also muss $H = \langle \bar{x} \rangle$ sein, wobei $\bar{x}$ die Nebenklasse $x\langle\langle R \rangle\rangle$ ist. Wegen $x^n \in R$ ist $\bar{x}^n = 1_H$, also $\mathrm{Ord}(\bar{x}) \leq n$ und $|H| \leq n$.

Damit haben wir gezeigt, dass für jedes $n \geq 1$ die Gruppe

$$\langle x \mid x^n \rangle$$

die zyklische Gruppe der Ordnung n ist.

Beispiel 3.11 (Diedergruppen)**.** Es sei $m \geq 3$ und $\zeta_m = \exp(2\pi i/m) = \cos(2\pi/m) + i\sin(2\pi/m) \in \mathbb{C}$. Dann ist $E_m = \{1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{m-1}\}$ die Menge der m-ten Einheitswurzeln. Es seien

$$\alpha : \mathbb{C} \to \mathbb{C}, \quad z \mapsto \bar{z},$$
$$\beta : \mathbb{C} \to \mathbb{C}, \quad z \mapsto \zeta_m z$$

die komplexe Konjugation (sprich die Spiegelung an der reellen Achse) bzw. die Drehung gegen den Uhrzeigersinn um $2\pi/m$. Beide α und β sind bijektiv. Bemerke, dass $\zeta_m\bar{\zeta}_m = |\zeta_m|^2 = 1$, also $\zeta_m^{-1} = \bar{\zeta}_m$. Übrigens gilt $\alpha(E_m) \subseteq E_m$ und $\beta(E_m) \subseteq E_m$, also können wir die Einschränkungen $\rho = \beta|_{E_m}$ (*Rotation*) und $\sigma = \alpha|_{E_m}$ (*Spiegelung*) betrachten.

Die Gruppe D_m, die von ρ und σ erzeugt wird, heißt *Diedergruppe*. Offensichtlich haben ρ und σ Ordnung m bzw. 2. Außerdem gilt

$$\beta\circ\alpha\circ\beta\circ\alpha(z) = \zeta_m\overline{\zeta_m\bar{z}} = \zeta_m\bar{\zeta}_m\bar{\bar{z}} = z,$$

d. h. $\beta\circ\alpha\circ\beta\circ\alpha = \mathrm{id}$, also $\sigma\rho\sigma\rho = 1$. Mit $\sigma^2 = 1$ folgt $\rho\sigma = \sigma\rho^{-1}$. Es sei nun ein (reduziertes, endliches) Wort in den Buchstaben $\{\rho, \sigma\}$. Jedes Mal, dass $\rho\sigma$ vorkommt, können wir $\rho\sigma$ mit $\sigma\rho^{-1}$ tauschen. Das bedeutet, dass jedes $g \in \mathrm{D}_m$ lässt sich als $g = \rho^n$ oder $g = \sigma\rho^n$ mit $n \in \mathbb{Z}$ schreiben. Also besitzt D_m genau $2m$ Elemente, nämlich die m Rotationen $1, \rho, \rho^2 \ldots, \rho^{m-1}$ und die m Spiegelungen $\sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{m-1}$. Damit haben wir sogar gezeigt, dass

$$\mathrm{D}_m \cong \langle\, \rho, \sigma \mid \rho^m,\ \sigma^2,\ \sigma\rho\sigma\rho \,\rangle.$$

Es gibt auch eine andere gebräuchliche Präsentation der Diedergruppe, siehe Aufgabe 3.19.

Beispiel 3.12 (Dreiecksgruppen)**.** Für $l, m, n \in \mathbb{N}$ definiert man die *Dreiecksgruppe*

$$\Delta(l, m, n) = \langle\, a, b, c \mid a^2, b^2, c^2, (ab)^l, (bc)^m, (ca)^n \,\rangle$$

Man kann zeigen, dass $|\Delta(l, m, n)| < \infty$ genau dann, wenn

$$\frac{1}{l} + \frac{1}{m} + \frac{1}{n} > 1.$$

Beispiel 3.13 (Rationale Zahlen)**.** Es sei $G = (\mathbb{Q}, +)$ die abelsche Gruppe der rationalen Zahlen. (Wir benutzen die additive Schreibweise: $g + h$ statt gh, $-g$ statt g^{-1} und ng statt g^n für $g, h \in G$, $n \in \mathbb{Z}$.) Für $n \in \mathbb{N}$ setze $s_n = 1/n! \in \mathbb{Q}$. Dann wird G von $S = \{\, s_n \mid n \in \mathbb{N} \,\}$ erzeugt, denn jedes $g \in \mathbb{Q}$ lässt sich als $g = a/b$ mit $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ schreiben und es gilt

$$g = a/b = a(b-1)!s_b.$$

Es gilt die Relation $ns_n = s_{n-1}$ (oder $s_n^n = s_{n-1}$ in multiplikativer Schreibweise) für alle $n > 1$. Aus Lemma 3.9 folgt, dass $(\mathbb{Q}, +)$ zu einer Faktorgruppe von

$$\langle\, \{\, x_n \mid n \in \mathbb{N} \,\} \mid x_n^n = x_{n-1} \text{ für alle } n > 1 \,\rangle$$

isomorph ist. Man kann zeigen, dass $(\mathbb{Q}, +)$ sogar isomorph zu dieser Gruppe ist (siehe [6]).

Beispiel 3.14 (Unlösbares Wortproblem)**.** Definiere

$$G = \langle\, a, b, c, d, e \mid ac = ca,\ ad = da,\ bc = cb,\ bd = db,\ ce = eca,\ de = edb,\ cca = ccae \,\rangle.$$

Dann ist das Wortproblem in G unlösbar, d. h., es gibt keinen Algorithmus, der in endlich vielen Schritten entscheidet, ob ein gegebenes Wort in a, b, c, d, e in G gleich 1 wird oder nicht. Dies is vermutlich das einfachste denkbare Beispiel (siehe [2]).

3.3 Symmetrische Gruppen

Lemma 3.15. *Für $i = 1, \dots, n-1$ setze $s_i = (i\ i+1) \in \mathrm{S}_n$. Dann wird die symmetrische Gruppe S_n von den $n-1$ Transpositionen $s_1, \dots, s_{n-1}$ erzeugt.*

Beweis. Für $n = 2$ ist $\mathrm{S}_2 = \{\mathrm{id}, s_1\} = \langle s_1 \rangle$ wie gewünscht. Es seien nun $n > 2$, $G = \langle s_1, \dots, s_{n-1} \rangle \leq \mathrm{S}_n$ und $H = \langle s_1, \dots, s_{n-2} \rangle \leq \mathrm{S}_n$. Nach Induktion ist $H \cong \mathrm{S}_{n-1}$, also $|H| = (n-1)!$. Die Gruppe G operiert transitiv auf $\{1, \dots, n\}$, denn $s_1 \cdot 1 = (1\ 2) \cdot 1 = 2$, $s_2 \cdot 2 = 3$, …, $s_{n-1} \cdot (n-1) = n$. Nach dem Bahnensatz (Satz 1.32) gilt $|G| = n|\mathrm{Stab}_G(n)|$, wobei $\mathrm{Stab}_G(n)$ der Stabilisator von n ist. Aber $H \subseteq \mathrm{Stab}_G(n)$, also $(n-1)! = |H| \leq |\mathrm{Stab}_G(n)|$. Damit folgt $|G| \geq n(n-1)! = n!$, also $G = \mathrm{S}_n$. □

Satz 3.16 (Präsentation für die symmetrische Gruppe S_n)**.** *Für alle $n \geq 2$ gilt*

$$\mathrm{S}_n \cong \langle\, x_1, \dots, x_{n-1} \mid x_i^2,\ (x_i x_{i+1})^3,\ (x_i x_j)^2 \text{ falls } |i-j| > 1 \,\rangle.$$

Zum Beispiel, $\mathrm{S}_3 \cong \langle\, x_1, x_2 \mid x_1^2,\ x_2^2,\ (x_1 x_2)^3 \,\rangle$ (mit Aufgabe 3.19 ist es dann offensichtlich, dass S_3 isomorph zur Diedergruppe D_3 ist) und $\mathrm{S}_4 \cong \langle\, x_1, x_2, x_3 \mid x_1^2,\ x_2^2,\ x_3^2,\ (x_1 x_2)^3,\ (x_2 x_3)^3,\ (x_1 x_3)^2 \,\rangle$.

Beweis. 1. Schritt: Nach Lemma 3.15 ist $\mathrm{S}_n = \langle \tau_1, \dots, \tau_{n-1} \rangle$, wobei $\tau_i = (i\ i+1)$. Klar gelten $\tau_i^2 = \mathrm{id}$ und $(\tau_i \tau_{i+1})^3 = \mathrm{id}$, denn $\tau_i \tau_{i+1} = (i\ i+1\ i+2)$ ist ein 3-Zyklus. Für $|i-j| > 1$ sind s_i und s_j disjunkt, also $\tau_i \tau_j = \tau_j \tau_i$ und damit $(\tau_i \tau_j)^2 = \mathrm{id}$. Also sind alle Relationen erfüllt.

2. Schritt: Es seien F die freie Gruppe auf $S = \{x_1, \dots, x_{n-1}\}$ und

$$R = \{x_i^2,\ (x_i x_{i+1})^3,\ (x_i x_j)^2 \text{ falls } |i-j| > 1\} \subset F.$$

Definiere $\varphi : F \to \mathrm{S}_n$ mit $\varphi(x_i) = s_i$ für $1 \leq i \leq n-1$. Nach dem ersten Schritt ist $\varphi(r) = 1$ für jedes $r \in R$. Nach dem Relationenlemma (Lemma 3.9) ist S_n isomorph zu einer Untergruppe von $G_n = \langle\, S \mid R \,\rangle$. Es gelten folgende Relationen, wobei $\bar{x}_i \in G_n = F/\langle\langle R \rangle\rangle$ die Klasse von $x_i \in F$ ist:

$$\bar{x}_i^2, \quad \bar{x}_i \bar{x}_{i+1} \bar{x}_i = \bar{x}_{i+1} \bar{x}_i \bar{x}_{i+1}, \quad \bar{x}_i \bar{x}_j = \bar{x}_j \bar{x}_i \text{ falls } |i-j| > 1.$$

Aus $x_i^2 \in R$ folgt nämlich $\bar{x}_i^{-1} = \bar{x}_i$. Aus $(x_i x_{i+1})^3 \in R$ folgt $\bar{x}_i \bar{x}_{i+1} \bar{x}_i \bar{x}_{i+1} \bar{x}_i \bar{x}_{i+1} = 1$, also $\bar{x}_i \bar{x}_{i+1} \bar{x}_i = \bar{x}_{i+1}^{-1} \bar{x}_i^{-1} \bar{x}_{i+1}^{-1} = \bar{x}_{i+1} \bar{x}_i \bar{x}_{i+1}$. Falls $|i-j| > 1$ folgt schließlich aus $(x_i x_j)^2 \in R$, dass $\bar{x}_i \bar{x}_j \bar{x}_i \bar{x}_j = 1$, also $\bar{x}_i \bar{x}_j = \bar{x}_j^{-1} \bar{x}_i^{-1} = \bar{x}_j \bar{x}_i$.

3. Schritt. Es seien nun $\tilde{F}$ die freie Gruppe auf $\tilde{S} = \{y_1, \dots, y_{n-1}\}$ und

$$\tilde{R} = \{y_i^2,\ y_i y_{i+1} y_i y_{i+1}^{-1} y_i^{-1} y_{i+1}^{-1},\ y_i y_j y_i^{-1} y_j{}^{-1} \text{ falls } |i-j| > 1\} \subset \tilde{F}.$$

Definiere $\psi : F \to G_n$ mit $\varphi(y_i) = \bar{x}_i$ für $1 \le i \le n-1$. Nach dem zweiten Scrhitt ist $\psi(r) = 1$ für jedes $r \in \tilde{R}$. Nach dem Relationenlemma ist G_n isomorph zu einer Untergruppe von $\tilde{G}_n = \langle\, \tilde{S} \mid \tilde{R} \,\rangle$. Es gilt also

$$n! = |\mathrm{S}_n| \le |G_n| \le |\tilde{G}_n|.$$

Dementsprechend reicht es zu zeigen, dass

$$|\tilde{G}_n| \le n! \tag{3.2}$$

Falls $n = 2$ ist $\tilde{G}_2 = \langle\, y_1 \mid y_1^2 \,\rangle$ zyklisch der Ordnung 2 (siehe Beispiel 3.10), also gilt (3.2).

Wir schreiben $G = \tilde{G}_n$, $g_i = \bar{y}_i$ für die Klasse von $y_i \in \tilde{F}$ in $G = \tilde{F}/\langle\langle \tilde{R} \rangle\rangle$ und $H = \langle g_2, \dots, g_{n-1} \rangle \le G$. Offensichtlich ist $H \cong \tilde{G}_{n-1}$, also $|H| \le (n-1)!$ per Induktion. Wir müssen also noch zeigen: $|G/H| \le n$, d. h., es gibt höchstens n Nebenklassen von H. Dazu definieren wir

$$t_0 = 1,\ t_1 = g_1,\ t_2 = g_2 g_1,\ \dots,\ t_{n-1} = g_{n-1} g_{n-2} \cdots g_1.$$

Es sei $X = \bigcup_{i=0}^{n-1} t_i H$ die Vereinigung der zu t_i zugehörige Nebenklassen. Zu zeigen ist: $G = X$.

Behauptung 3.17. *Für alle $i \in \{0, \dots, n-1\}$ und $j \in \{1, \dots, n-1\}$ ist $g_j t_i \in X$.*

Beweis der Behauptung. Wir unterscheiden mehrere Fälle:

(I) Falls $i = 0, j > 1$: $g_j t_0 = g_j \in H = t_0 H \subseteq X$, denn $j > 1$.

(II) Falls $i = 0, j = 1$: $g_1 t_0 = g_1 = t_1 \in t_1 H \subseteq X$.

(III) Falls $i > 0, j > i+1$: $g_j t_i = g_j g_i g_{i-1} \cdots g_1$; wegen $j > i+1$ vertauscht g_j mit allen Faktoren, also $g_j t_i = t_i g_j \in t_i H \subseteq X$.

(IV) Falls $i > 0, j = i+1$: $g_j t_i = g_{i+1} g_i \cdots g_1 = t_{i+1} \in t_{i+1} H \subseteq X$.

(V) Falls $i > 0, j = i$: $g_j t_i = g_i g_i g_{i-1} \cdots g_1 = g_{i-1} \cdots g_i = t_{i-1} \in t_{i-1} H \subseteq X$ wegen $g_i^2 = 1$.

(VI) Falls $i > 0, j = i-1$: $g_j t_i = g_{i-1} g_i g_{i-1} g_{i-2} \cdots g_1 = g_i g_{i-1} g_i g_{i-2} \cdots g_1 = g_i g_{i-1} g_{i-2} \cdots g_1 g_i = t_i g_i \in t_i H \subseteq X$ wegen $j \ge 1$, also $i \ge 2$.

(VII) Falls $i > 0, j < i-1$: $g_j t_i = g_j g_i \cdots g_{j+1} g_j g_{j-1} \cdots g_1 = g_i g_{i-1} \cdots g_j g_{j+1} g_j g_{j-1} \cdots g_1 = g_i g_{i-1} \cdots g_{j+1} g_j g_{j+1} g_{j-1} \cdots g_1 = g_i g_{i-1} \cdots g_{j+1} g_j g_{j-1} \cdots g_1 g_{j+1} = t_i g_{j+1} \in t_i H \subseteq X$.

Damit sind alle Fälle abgehandelt. □

Es sei nun $g \in G$ ein beliebiges Element. Aus $G = \langle g_1, \dots, g_{n-1} \rangle$ und $g_i = g_i^{-1}$ folgt $g = g_{j_1} \cdots g_{j_k}$ für gewisse $j_1, \dots, j_k \in \{1, \dots, n-1\}$. Setze $i_0 = 0$. Nach Behauptung 3.17 wissen wir, dass $g_{j_k} t_0 \in X$, also dass es $i_1 \in \{0, \dots, n-1\}$ und $h_1 \in H$ existieren mit $g_{j_k} t_{i_0} = t_{i_1} h_1$. Analog gibt es $i_2, \dots, i_k \in \{0, \dots, n-1\}$ und $h_2, \dots, h_k \in H$ mit

$$g_{j_k} t_{i_0} = t_{i_1} h_1,\ g_{j_{k-1}} t_{i_1} = t_{i_2} h_2,\ \dots,\ g_{j_1} t_{i_{k-1}} = t_{i_k} h_k.$$

Damit gilt

$$\begin{aligned} g = g_{j_1} \cdots g_{j_{k-2}} g_{j_{k-1}} g_{j_k} \cdot 1 &= g_{j_1} \cdots g_{j_{k-2}} g_{j_{k-1}} (g_{j_k} \cdot t_{i_0}) \\ &= g_{j_1} \cdots g_{j_{k-2}} g_{j_{k-1}} (t_{i_1} h_1) = g_{j_1} \cdots g_{j_{k-2}} (g_{j_{k-1}} t_{i_1}) h_1 \\ &= g_{j_1} \cdots g_{j_{k-2}} (t_{i_2} h_2) h_1 = g_{j_1} \cdots (g_{j_{k-2}} t_{i_2}) h_2 h_1 \\ &= g_{j_1} \cdots (t_{i_3} h_3) h_2 h_1 = \ldots \\ &= t_{i_k} h_k h_{k-1} \cdots h_2 h_1 \in t_{i_k} H \subseteq X. \end{aligned}$$

Das zeigt $G \subseteq X$, also $G = X$. □

3.4 Aufgaben

Aufgabe 3.18. Es sei G eine Gruppe und $R \subseteq G$.
(i) Zeige: $\langle\langle R \rangle\rangle = \langle \{ grg^{-1} \mid g \in G, r \in R \} \rangle$.
(ii) Es sei nun G frei auf $\{x, y\}$ $(x \neq y)$. Zeige: $\mathrm{K}(G) = \langle\langle [x, y] \rangle\rangle$. Gilt $y^2 x^2 \in \langle\langle R \rangle\rangle$?

Aufgabe 3.19. Zeige: Die in Beispiel 3.11 definierte Diedergruppe D_m ist isomorph zu

$$\langle\, s, t \mid s^2,\ t^2,\ (st)^m \,\rangle.$$

Aufgabe 3.20. Zeige: $\mathrm{A}_4 \cong \langle\, x, y \mid x^3,\ y^3,\ (xy)^2 \,\rangle$.

Aufgabe 3.21. Für $l, m, n \in \mathbb{N}$ heißt $\mathrm{D}(l, m, n) = \langle\, x, y \mid x^l,\ y^m,\ (xy)^n \,\rangle$ *von-Dyck-Gruppe* (oder *gewöhnliche Dreiecksgruppe*). Zeige:
(a) $\mathrm{D}(l, m, n) \cong \mathrm{D}(m, l, n) \cong \mathrm{D}(n, m, l)$.
(b) $\mathrm{D}(l, m, n)$ ist isomorph zu einer Untergruppe einer Dreiecksgruppe.

Bemerkung 3.22. Eine Gruppe heißt *Hurwitz-Gruppe*, falls sie isomorph zu einer Faktorgruppe der von-Dyck-Gruppe $\mathrm{D}(2, 3, 7)$ ist. Hurwitz-Gruppen spielen eine wichtige Rolle in der Geometrie, besonders in der Theorie der Riemannschen Flächen (siehe [3]).

Kapitel 4

BN-Paare

Definition 4.1. Es seien G eine Gruppe und B, N zwei Untergruppen von G. Wir sagen, dass B und N ein *BN-Paar* (oder *Tits-System*) bilden, falls folgende Axiome gelten:

(BN1) Die Gruppe G wird von B und N erzeugt: $G = \langle B, N \rangle$.

(BN2) Es gilt $H := B \cap N \trianglelefteq N$ und es gibt $S \subseteq N$ mit $s^2 \in H$ für alle $s \in S$, sodass

$$W := N/H = \langle\, sH \mid s \in S \,\rangle. \tag{4.1}$$

(BN3) Es gilt $sBs \nsubseteq B$ für alle $s \in S$.

(BN4) Es gilt $sBn \subseteq BsnB \cup BnB$ für alle $s \in S$ und $n \in N$.

Die Untergruppe B heißt *Borel-Untergruppe*, H heißt *Cartan-Untergruppe* und W heißt *Weyl-Gruppe*. Außerdem sagen wir, dass das BN-Paar *gesättigt* ist, falls gilt

(BN5) $H = \bigcap_{n \in N} nBn^{-1}$.

Bemerkung 4.2. Aus $H \trianglelefteq N$ folgt $H = nHn^{-1} \subseteq nBn^{-1}$ für jedes $n \in N$, also ist die Inklusion $H \subseteq \bigcap_{n \in N} nBn^{-1}$ immer wahr.

Bemerkung 4.3. Es bezeichne $A^{-1} = \{\, a^{-1} \mid a \in A \,\}$ für eine Teilmenge $A \subseteq G$. Aus (BN4) folgt $(sBn)^{-1} \subseteq (BsnB)^{-1} \cup (BnB)^{-1}$ für jedes $s \in S$ und $n \in N$, d. h.

(BN4′) Es gilt $nBt \subseteq BntB \cup BnB$ für alle $t \in S$ und $n \in N$.

Beispiel 4.4. Es seien G eine Gruppe und X eine Menge mit $|X| \geq 3$, sodass G 2-fach transitiv auf X operiert. Wähle $x \in X$ und setze $B = \mathrm{Stab}_G(x)$. Es sei auch $x' \in X$ mit $x' \neq x$. Da G 2-fach transitiv operiert gibt es $s \in G$ mit $s \cdot x = x'$ und $s \cdot x' = x$. Es sei $N = \langle s \rangle$. Wir behaupten, dass B und N ein BN-Paar mit $|W| = 2$ bilden.

Um das zu zeigen, seien $g \in G$ beliebig und $x'' = g \cdot x$. Ist $x'' = x$, so ist $g \in \mathrm{Stab}_G(x) = B$. Ist $x'' \neq x$, dann gibt es $h \in G$ mit $h \cdot x = x$ und $h \cdot x' = x''$, denn G operiert 2-fach transitiv. Insbesondere $h \in B$ und $g \cdot x = x'' = h \cdot x' = h \cdot (s \cdot x) = (hs) \cdot x$, also $(hs)^{-1} g \in B$, d. h. $g \in hsB \subseteq BsB$. Dies zeigt:

$$G = B \dot{\cup} BsB, \tag{4.2}$$

denn B und BsB zwei Doppelnebenklassen sind, also notwendig disjunkt (siehe Beispiel 1.38).

Beide B und BsB sind Teilmengen von $\langle B, N\rangle$. Voraussetzung (BN1) ist dementsprechend erfüllt.

Übrigens ist N eine zyklische und damit abelsche Gruppe, also ist jede Untergruppe von N ein Normalteiler, insbesondere $H = B \cap N \trianglelefteq N$. Wir setzen $S = \{s\} \subseteq N$. Aus $s^2 \cdot x = s \cdot (s \cdot x) = s \cdot x' = x$ folgt $s^2 \in B \cap N \subseteq H$. Die Gruppe $W = N/H$ wird offensichtlich von sH erzeugt, also ist Voraussetzung (BN2) ebenso erfüllt. Es gilt $|W| = 2$, weil $s \notin B$.

Wäre $sBs \subseteq B$, dann $Bs \subseteq s^{-1}B$, also $BsB \subseteq s^{-1}B$. Wegen (4.2) wäre also $G = B \dot\cup s^{-1}B$, d. h. $|G/B| = 2$. Da G transitiv auf X operiert, ist aber nach dem Bahnensatz (Satz 1.32) $|X| = |G/\operatorname{Stab}_G(x)| = |G/B|$. Das widerspricht $|X| \geq 3$, also muss auch Voraussetzung (BN3) gelten.

Schließlich müssen wir Voraussetzung (BN4) nachweisen. Es sei $n \in N$, also $n = s^i$ für ein $i \in \mathbb{Z}$. Ist i gerade, so $n \in \langle s^2\rangle \subseteq H \subseteq B$ und damit $sBn = sB = snB \subseteq BsnB$. Ist i ungerade, so $sn = s^{i+1} \in \langle s^2\rangle \subseteq H \subseteq B$ und damit $BsnB = B$ und $BnB = BsB$. Wegen (4.2) gilt also $sBn \subseteq G = B \cup BsB = BsnB \cup BnB$, was zu zeigen war.

4.1 Allgemeine lineare Gruppen

Es sei K ein beliebiger Körper. Wir wollen hier ein BN-Paar für $G = \mathrm{GL}_n(K)$ konstruieren.

Definition 4.5. Eine Matrix $A = (a_{ij}) \in \mathrm{M}_n(K)$ heißt *obere Dreiecksmatrix* falls $a_{ij} = 0$ für alle $1 \leq i < j \leq n$, d. h. A hat folgende Gestalt:

$$A = \begin{pmatrix} * & * & \cdots & * \\ & * & \ddots & \vdots \\ & & \ddots & * \\ 0 & & & * \end{pmatrix}.$$

Eine Matrix $A \in \mathrm{M}_n(K)$ heißt *untere Dreiecksmatrix* falls A^{t} eine obere Dreiecksmatrix ist.

Definition 4.6. Eine Matrix $A \in \mathrm{M}_n(K)$ heißt *Monomialmatrix*, wenn es in jeder Zeile und Spalte von A genau einen Eintrag ungleich 0 gibt. Eine Matrix $A \in \mathrm{M}_n(K)$ heißt *Permutations-* oder *Vertauschungsmatrix*, wenn in jeder Zeile und Spalte von A genau ein Eintrag gleich 1 gibt und alle andere gleich 0 sind. Jede Permutationsmatrix $P_\sigma = (p_{ij})$ entspricht einer Permutation $\sigma \in \mathrm{S}_n$ durch folgende Regel: Genau dann ist $p_{ij} = 1$, wenn $i = \sigma(j)$ ist, sonst ist $p_{ij} = 0$.

Bezeichnung 4.7. Wir führen folgende Bezeichnung ein:

$$\begin{aligned} B &:= \{\text{obere Dreiecksmatrizen in } G\}, \\ B' &:= \{\text{untere Dreiecksmatrizen in } G\}, \\ N &:= \{\text{Monomialmatrizen in } G\}, \\ V &:= \{\text{Permutationsmatrizen in } G\}, \\ H &:= \{\text{Diagonalmatrizen in } G\}. \end{aligned}$$

Weiterhin setzen wir $U := \{ A = (a_{ij}) \in B \mid a_{ii} = 1 \text{ für alle } 1 \leq i \leq n \}$. Also ist jede Matrix $A \in U$ der Form

$$A = \begin{pmatrix} 1 & * & \cdots & * \\ & 1 & \ddots & \vdots \\ & & \ddots & * \\ 0 & & & 1 \end{pmatrix}.$$

Offensichtlich gilt $H = B \cap N = B \cap B'$. Übrigens sind all diese Teilmengen Untergruppen (Aufgabe 4.22).

Bezeichnung 4.8. Darüber hinaus führen wir folgende Teilmengen ein, die ebenfalls Untergruppen sind, wobei $E_{ij} = (e_{kl})$ die Matrix ist mit $e_{kl} = 1$ für $k = i$ und $l = j$, sonst $e_{kl} = 0$.

$$\begin{aligned} X_{ij} &:= \{ \mathbf{1}_n + tE_{ij} \mid t \in K \}, \\ X_i &:= X_{i,i+1}, \\ X_i' &:= X_{i+1,i}, \\ Y_i &:= \{ A = (a_{ij}) \in U \mid a_{i,i+1} = 0 \}. \end{aligned}$$

Lemma 4.9. *Die Untergruppe H ist ein Normalteiler von N und es gilt $N/H \cong \mathrm{S}_n$.*

Beweis. Nach Aufgabe 4.22 lässt sich jedes Element in N als DP_σ schreiben, mit $D \in H$ und $P_\sigma \in V$. Es gilt

$$P_\sigma \operatorname{Diag}(a_1, \ldots, a_n) P_\sigma^{-1} = \operatorname{Diag}(a_{\sigma(1)}, \ldots, a_{\sigma(n)}) \tag{4.3}$$

und das Produkt von Diagonalmatrizen ist eine Diagonalmatrix, also $H \trianglelefteq N$. Aus dem gleichen Grund ist der folgende Homomorphismus surjektiv:

$$\psi : V \hookrightarrow N \to N/H,$$

wobei $V \hookrightarrow N$ die Inklusion ist. Aus $\operatorname{Ker}(\psi) = V \cap H = \{\mathbf{1}_n\}$ folgt, dass ψ sogar ein Isomorphismus ist. Wir schließen mit Aufgabe 4.22, dass $N/H \cong V \cong \mathrm{S}_n$. □

Satz 4.10. *Es sei K ein beliebiger Körper. Dann bilden die Untergruppe B der oberen Dreiecksmatrizen und die Untergruppe N der Monomialmatrizen in $\mathrm{GL}_n(K)$ ein gesättigtes BN-Paar, sodass die zugehörige Weyl-Gruppe isomorph zu S_n ist.*

Beweis. Nach dem Gauß-Verfahren lässt sich jede invertierbare Matrix durch elementare Zeilen- und Spaltenumformungen auf die Einheitsmatrix bringen. Elementare Umformungen entsprechen Multiplikation von links oder rechts mit Elementarmatrizen der folgenden Gestalten:

- Diagonalmatrizen $\operatorname{Diag}(1, \ldots, 1, t, 1, \ldots, 1) \in H \subseteq B$.
- Permutationsmatrizen $P_{(i\ j)} \in V \subseteq N$.
- Elementarmatrizen $R_{ij}(c) \in B$ mit $i < j$.
- Elementarmatrizen $R_{ij}(c) \in B'$ mit $j < i$, wobei B' die Untergruppe der unteren Dreiecksmatrizen ist.

(Die Elementarmatrizen $R_{ij}(c)$ sind wie folgt definiert: Für $i \neq j$ ist $R_{ij}(c) = (a_{ij}) \in \mathrm{M}_n(K)$ definiert durch $a_{i'i'} = 1$ für $1 \leq i' \leq n$, $a_{ij} = c$ und $a_{i'j'} = 0$ für alle andere i', j'. Bemerke: $R_{ij}(c) \in \mathrm{SL}_n(K)$.)

Damit ist $G = \langle B, N, B' \rangle$. Dazu sei

$$n_0 = \begin{pmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{pmatrix} = P_\sigma \in V, \text{ wobei } \sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ n & n-1 & \dots & 1 \end{pmatrix}.$$

Dann gilt $n_0^{-1} = n_0$ und

$$n_0 \begin{pmatrix} * & * & \cdots & * \\ & * & \ddots & \vdots \\ & & \ddots & * \\ 0 & & & * \end{pmatrix} n_0 = n_0 \begin{pmatrix} * & \cdots & * & * \\ \vdots & \iddots & * & \\ * & \iddots & & \\ * & & & 0 \end{pmatrix} = \begin{pmatrix} * & & & 0 \\ * & \ddots & & \\ \vdots & \ddots & * & \\ * & \cdots & * & * \end{pmatrix},$$

also ist $B' = n_0 B n_0 \subseteq \langle B, N \rangle$ und damit ist Voraussetzung (BN1) erfüllt.

Wir haben schon in Lemma 4.9 gezeigt, dass $H \trianglelefteq N$ und $W = N/H \cong \mathrm{S}_n$. Für $i = 1, \dots, n-1$ seien $\tau_i = (i \ i+1)$ und $s_i = P_{\tau_i}$. Bemerke: $s_i^2 = \mathbf{1}_n$. Setze $S = \{s_1, \dots, s_{n-1}\}$. Aus Lemma 3.15 folgt dann Voraussetzung (BN2).

Aus Aufgabe 4.23 folgt $B = HU = HX_iY_i$ und

$$s_i B s_i = (s_i H s_i)(s_i X_i s_i)(s_i Y_i s_i) = H X_i' Y_i.$$

Wäre $s_i B s_i \subseteq B$, dann wäre auch $X_i' \subseteq B$, was aber nicht wahr ist. Also ist Voraussetzung (BN3) ebenso erfüllt.

Jedes $n \in N$ lässt sich als $n = dp$ darstellen mit $d \in H$ und $p \in V$, also ist $Bn = Bdp = Bp$. Wegen (4.3) ist $s_i d = d' s_i$ für ein $d' \in H$. Damit

$$\begin{aligned} s_i Bn &= s_i Bp, \\ Bs_i nB &= Bs_i dpB = Bd' s_i pB = Bs_i pB, \\ BnB &= BpB. \end{aligned}$$

D. h.: Um Voraussetzung (BN4) nachzuweisen, können wir annehmen, dass $n = p = P_\sigma \in V$. Es gilt

$$s_i Bn = (s_i H s_i)(s_i Y_i s_i)(s_i X_i n) = H Y_i s_i X_i n \subseteq B s_i X_i n. \tag{4.4}$$

Wir müssen zwei Fälle unterscheiden:

(I) $\sigma^{-1}(i) < \sigma^{-1}(i+1)$,

(II) $\sigma^{-1}(i) > \sigma^{-1}(i+1)$.

Im Fall (I) ist $X_{\sigma^{-1}(i),\sigma^{-1}(i+1)} \subseteq B$, also

$$s_i Bn \subseteq Bs_i X_i n = Bs_i n(n^{-1} X n) = Bs_i n X_{\sigma^{-1}(i),\sigma^{-1}(i+1)} \subseteq Bs_i nB.$$

Im Fall (II) setze $n' = s_i n$. Dann $n' = P_{\sigma'} \in V$ mit $\sigma' = \tau_i \sigma$. Dann $\sigma'^{-1}(i) = \sigma^{-1}\tau_i(i) = \sigma^{-1}(i+1) < \sigma^{-1}(i) = \sigma^{-1}\tau_i(i+1) = \sigma'^{-1}(i+1)$. Aus Fall (I) folgt

$$s_i B n' \subseteq B s_i n' B = BnB. \tag{4.5}$$

Jede Matrix in X_i' ist von der Form

$$\begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & 1 & 0 & & & \\ & & & t & 1 & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix}$$

mit $t \in K$. Für $t \neq 0$ gilt

$$\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} = \begin{pmatrix} 1 & t^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t & 0 \\ 0 & -t^{-1} \end{pmatrix}.$$

Also ist

$$X_i' \subseteq \{\mathbf{1}_n\} \cup X_i s_i X_i H \subseteq B \cup B s_i B.$$

Offensichtlich ist $Bn' = Bs_i n \subseteq Bs_i nB$. Aus (4.4) und (4.5) folgt nun

$$\begin{aligned} s_i Bn &\subseteq Bs_i X_i n = B(s_i X_i s_i) s_i n = B X_i' n' \\ &\subseteq B(B \cup Bs_i B)n' = Bn' \cup Bs_i Bn' \subseteq Bs_i n \cup Bs_i n' B = Bs_i nB \cup BnB. \end{aligned}$$

Damit haben wir gezeigt, dass Voraussetzung (BN4) in beiden Fällen erfüllt ist.

Schließlich folgt aus Bemerkung 4.2 mit $n = n_0$ wie oben

$$H \subseteq \bigcap_{n \in N} nBn^{-1} \subseteq B \cap n_0 B n_0^{-1} = B \cap B' = H,$$

d. h., das BN-Paar ist gesättigt. □

Bemerkung 4.11. Betrachte $\mathrm{SL}_n(K)$. Es seien $B' = B \cap \mathrm{SL}_n(K)$ und $N' = N \cap \mathrm{SL}_n(K)$. Dann bilden B', N' ein BN-Paar in $\mathrm{SL}_n(K)$ und die zugehörige Weyl-Gruppe ist wieder isomorph zu S_n (siehe Aufgabe 4.25).

4.2 Bruhat-Zerlegung

Es sei nun G eine Gruppe mit einem BN-Paar $B, N \leq G$ und Weyl-Gruppe $W = N/H$, wobei $H = B \cap N$. Es sei

$$N \to N/H, \quad n \mapsto \bar{n}$$

der kanonische Isomorphismus. Bemerke: Sind $n_1, n_2 \in N$ mit $\bar{n}_1 = \bar{n}_2$, so gelten $n_1 B = n_2 B$ und $Bn_1 = Bn_2$, denn $n_1 n_2^{-1} \in H \subseteq B$. Aus diesem Grund werden wir oft n mit $\bar{n}$ identifizieren. Insbesondere werden wir ein $s \in S$ als Element von W betrachten mit $s^2 = 1$. Unter dieser Identifizierung ist (4.1) äquivalent zu $W = \langle S \rangle$. Wegen (BN3) ist $s \neq 1$ für alle $s \in S$, also $\mathrm{Ord}(s) = 2$.

Definition 4.12. Jedes $w \in W$ lässt sich als $w = s_1 \cdots s_m$ mit $s_i \in S$ darstellen. Ein solcher Ausdruck heißt *reduziert*, wenn m minimal ist. In diesem Fall heißt $\ell(w) := m$ die *Länge* von w.

Bemerkung 4.13. Es gilt $\ell(1) = 0$ und $\ell(s) = 1$ für jedes $s \in S$. Ist $w \in W$, $w \neq 1$, so gibt es stets ein $s \in S$ mit $\ell(sw) = \ell(w) - 1$, denn sei $w = s_1 \cdots s_m$ mit $s_i \in S$ und $\ell(w) = m$, dann

$$s_1 w = s_1 s_1 s_2 \cdots s_m = s_2 \cdots s_m,$$

und die rechte Seite ist notwendig reduziert (sonst wäre der Ausdruck für w auch nicht reduziert). Analog: Ist $w \in W$, $w \neq 1$, so gibt es stets ein $t \in S$ mit $\ell(wt) = \ell(wt) - 1$. Diese Eigenschaften werden oft bei Induktionsargumenten verwendet. Mit ähnlichen Argumenten erhält man folgende Formel für beliebige $s \in S$ und $w \in W$:

$$\ell(w) - 1 \leq \ell(sw) \leq \ell(w) + 1. \tag{4.6}$$

Lemma 4.14. *Gegeben $J \subseteq S$, setze $W_J := \langle J \rangle \leq W$, $N_J := \pi^{-1}(W_J) \leq N$. Dann ist $P_J := BN_JB$ eine Untergruppe von G. Insbesondere gilt*

$$G = BNB = \bigcup_{n \in N} BnB.$$

Beweis. Ist $p \in P_J$, so $p = bnb'$ mit $b, b' \in B$ und $n \in N_J$. Dann $p^{-1} = b'^{-1} n^{-1} b^{-1} \in BN_JB = P_J$, also ist P_J abgeschlossen unter Inversen.

Für jedes $s_i \in J$ gilt wegen (BN4)

$$s_i P_J = s_i BN_JB \subseteq Bs_i N_JB \cup BN_JB \subseteq BN_JB \cup BN_JB = P_J,$$

also ist $N_J P_J \subseteq P_J$. Aus $BP_J = P_J$ folgt dann

$$P_J P_J = BN_JBP_J = BN_JP_J \subseteq BP_J = P_J.$$

Damit ist P_J abgeschlossen auch unter Multiplikation, d. h. $P_J \leq G$.

Die letzte Aussage folgt unmittelbar aus dem Fall $J = S$. □

Bezeichnung 4.15. Für $w \in W$ setzen wir $C(w) := BwB \subseteq G$. Dies bedeutet, dass wir $n \in N$ finden mit $\bar{n} = w$ und dass $C(w) = BnB$, wobei n mit $\bar{n} = w$ identifiziert wird.

Satz 4.16 (Bruhat-Zerlegung)**.** *Es sei G eine Gruppe mit BN-Paar und Weyl-Gruppe W. Dann ist $C(w) \neq C(w')$ für alle $w, w' \in W$ mit $w \neq w'$ und es gilt*

$$G = \dot{\bigcup}_{w \in W} C(w).$$

Für $s \in S$ und $w \in W$ gilt $\ell(sw) = \ell(w) \pm 1$. Außerdem gelten folgende Multiplikationsregeln

$$C(s)C(w) = \begin{cases} C(sw) & \text{falls } \ell(sw) = \ell(w) + 1, \\ C(sw) \cup C(w) & \text{falls } \ell(sw) = \ell(w) - 1. \end{cases}$$

Beweis. Aus Lemma 4.14 wissen wir bereits, dass $G = \bigcup_{n \in N} BnB$. Wir müssen also noch zeigen, dass die Vereinigung disjunkt ist, wenn $n \in N$ nur über Repräsentanten von $w \in W$ läuft. Dazu reicht folgende Behauptung.

Behauptung 4.17. *Sind $y, w \in W$ mit $C(y) = C(w)$, so $y = w$.*

Beweis der Behauptung. Ohne Einschränkung der Allgemeinheit nehmen wir an, dass $\ell(y) \leq \ell(w)$. Wir fahren nach Induktion über $\ell(y)$ fort. Ist $\ell(y) = 0$, so $y = 1$ und $C(y) = B = BnB$ mit $\bar{n} = w$. Aber dann $n \in B \cap N = H$, also $w = \bar{n} = 1$.

Es sei nun $y \in W$ mit $\ell(y) > 0$. Nach Bemerkung 4.13 gibt es $s \in S$ und $x \in W$ mit $y = sx$ und $\ell(y) = \ell(x) + 1$. Nach Voraussetzung gilt

$$sxB \subseteq BsxB = ByB = C(y) = C(w) = BwB.$$

Wegen (BN4) ist $xB \subseteq s^{-1}BwB = sBwB \subseteq BswB \cup BwB$, also

$$BxB \subseteq BswB \cup BwB.$$

Doppelnebenklassen sind aber gleich oder disjunkt. Deshalb ist $BxB = BswB$ oder $BxB = BwB$. Nach Induktion muss $x = sw$ oder $x = w$ sein. Der zweite Fall ist jedoch nicht möglich, denn $\ell(x) = \ell(y) - 1 < \ell(w)$. Also ist $x = sw$, d. h. $y = sx = ssw = w$. □

Nun wollen wir die Multiplikationsregel beweisen. Bemerke: $C(sw) = BswB \subseteq Bs\{1\}wB \subseteq BsBwB = C(s)C(w)$. Übrigens folgt aus (BN4), dass $C(s)C(w) = B(sBw)B \subseteq B(BswB \cup BwB)B = C(sw) \cup C(w)$. Deshalb gilt immer

$$C(sw) \subseteq C(s)C(w) \subseteq C(sw) \cup C(w). \tag{4.7}$$

Behauptung 4.18. *Ist $\ell(sw) \geq \ell(w)$, so $C(s)C(w) = C(sw)$.*

Beweis der Behauptung. Wegen (4.7) reicht es zu zeigen, dass $C(s)C(w) \cap C(w) = \emptyset$, was äquivalent zu $sBw \cap BwB = \emptyset$ ist. Ist $\ell(w) = 0$, dann $w = 1$ und $sBw \cap BwB = sB \cap B = \emptyset$, denn $s \notin B$.

Es sei nun $w \in W$ mit $\ell(w) > 0$. Nach Bemerkung 4.13 gibt es $t \in S$ und $y \in W$ mit $w = yt$ und $\ell(w) = \ell(y) + 1$. Dann ist $\ell(syt) = \ell(sw) \geq \ell(w) = \ell(y) + 1$, also $\ell(sy) \geq \ell(y)$ wegen (4.6). Per Induktion ist dann $sBy \cap ByB = \emptyset$. Deshalb gilt mit (BN4), (BN4′) und $wt = ytt = y$

$$\begin{aligned} sBy \cap BwBt \subseteq sBy \cap (ByB \cup BwB) = sBy \cap BwB \subseteq (BsyB \cup ByB) \cap BwB \\ = (C(sy) \cap C(w)) \cup (C(y) \cap C(w)) \end{aligned}$$

Ist $C(sy) \cap C(w) \neq \emptyset$, so $sy = w$ nach Behauptung 4.17. Aber dann $\ell(w) \leq \ell(sw) = \ell(ssy) = \ell(y)$. Ist $C(y) \cap C(w) \neq \emptyset$, so $y = w$ nach Behauptung 4.17. Aber dann $\ell(y) = \ell(w)$. Dies wiederspricht $\ell(w) = \ell(y) + 1$ in beiden Fällen. Dementsprechend ist $sBy \cap BwBt = \emptyset$, also

$$\emptyset = (sBy \cap BwBt)t = sBw \cap BwBt^2 = sBw \cap BwB,$$

was zu zeigen war. □

Behauptung 4.19. *Ist $\ell(sw) \leq \ell(w)$, so $C(s)C(w) = C(sw) \cup C(w)$.*

Beweis der Behauptung. Wegen (4.7) reicht es zu zeigen, dass $C(w) \subseteq C(s)C(w)$. Wegen (BN4) ist $sBs \subseteq Bs^2B \cup BsB = B \cup BsB$. Mit (BN3) folgt $sBs \cap BsB \neq \emptyset$, d. h. $sBw \cap BsBsw \neq \emptyset$, also

$$C(s)C(w) \cap C(s)C(sw) \neq \emptyset.$$

Setze $w' = sw$. Aus $\ell(sw') \geq \ell(w')$ folgt nach Behauptung 4.18

$$C(w) = C(sw') = C(s)C(w') = C(s)C(sw).$$

Schließlich ist $C(s)C(w) \cap C(w) \neq \emptyset$. Aber $C(w)$ ist eine Doppelnebenklasse und $C(s)C(w) = \bigcup_{b \in B} BsbwB$ ist eine Vereinigung von Doppelnebenklassen, also $C(w) \subseteq C(s)C(w)$. □

Wäre $\ell(sw) = \ell(w)$, dann hätten wir $C(sw) = C(s)C(w) = C(sw) \cup C(w)$, d. h. entweder $C(sw) = C(w)$ (sprich $sw = w$ nach Behauptung 4.17) oder $C(w) = \emptyset$. Beide Fälle sind nicht möglich, also $\ell(sw) \neq \ell(w)$. Damit schließen wir den Beweis. □

Folgerung 4.20 (Austauschlemma)**.** *Es seien $w \in W$ mit $\ell(w) = m$, $w = s_1 \cdots s_m$ ein reduzierter Ausdruck mit $s_i \in S$ und $s \in S$ beliebig mit $\ell(sw) < \ell(w)$. Dann gibt es $i \in \{1, \ldots, m\}$, sodass*

$$sw = s_1 \cdots s_{i-1} s_{i+1} \cdots s_m.$$

Beweis. Wegen $\ell(sw) < \ell(w)$ gilt $C(s)C(w) = C(sw) \cup C(w)$ nach Bruhat-Zerlegung (Satz 4.16), d. h. $BsBwB = BswB \cup BwB$ und insbesondere $sBw \cap BwB \neq \emptyset$. Folglich gibt es $b_1, b_2, b_3 \in B$ und $n \in N$ mit $\bar{n} = w$, sodass $sb_1n = b_2nb_3$, also

$$s = b_2nb_3n^{-1}b_1^{-1} \in BwBw^{-1}B = C(w)C(w^{-1}). \tag{4.8}$$

Behauptung 4.21. *Für alle $y \in W$ gilt*

$$C(w)C(y) \subseteq \bigcup_{0\le l\le m}\left(\bigcup_{1\le i_1<\ldots<i_l\le m} C(s_{i_1}\cdots s_{i_l}y)\right).$$

Beweis der Behauptung. Ist $m = 0$, d. h. $w = 1$, so $C(w)C(y) = C(y)$. Es sei nun $m > 0$. Nach Bruhat-Zerlegung und Induktion gilt

$$C(w)C(y) = C(s_1)C(s_2\cdots s_m)C(y) \subseteq \bigcup_{0\le l\le m}\left(\bigcup_{1\le i_2<\ldots<i_l\le m} C(s_1)C(s_{i_2}\cdots s_{i_l}y)\right).$$

Aus (BN4) folgt $C(s_1)C(s_{i_2}\cdots s_{i_l}y) \subseteq C(s_1s_{i_2}\cdots s_{i_l}y) \cup C(s_{i_2}\cdots s_{i_l}y)$. Damit erhalten wir die gewünschte Formel. □

Aus (4.8) folgt nach der Behauptung (mit $y = w^{-1}$), dass $s = xw^{-1}$, wobei $x = s_{i_1}\cdots s_{i_l}$, $1 \le i_1 < \ldots < i_l \le m$ und $l \le m$. Per Definition ist $\ell(x) \le l$. Dann $1 = \ell(s) = \ell(xw^{-1}) \ge \ell(w) - \ell(x) = m - \ell(x) \ge m - l$, d. h.

$$m - 1 \le l \le m.$$

Es gibt also zwei Möglichkeiten: entweder $l = m - 1$ oder $l = m$. Ist $l = m$, so $x = s_1\cdots s_m = w$, aber dann $s = 1$, was nicht möglich ist. Dementsprechend muss $l = m - 1$ sein, d. h. $sw = x = s_1\cdots s_{i-1}s_{i+1}\cdots s_m$ für ein $i \in \{1, \ldots, m\}$. □

4.3 Aufgaben

Aufgabe 4.22. In Bezug auf Bezeichnung 4.7 zeige:

(a) Die Menge U ist eine Untergruppe von B.
(b) Die Menge V der Permutationsmatrizen ist eine Untergruppe von N und es gilt $V \cong \mathrm{S}_n$.
(c) Es gelten $B = HU = UH$ und $N = HV = VH$.

Lösung. (a) Per Definition ist $U \subseteq B$, also müssen wir nur zeigen, dass U eine Gruppe ist. Es seien $A = (a_{ij})$ und $A' = (a'_{ij})$ zwei Matrizen in U. Dann gilt $a_{ij} = a'_{ij} = 0$ für $j < i$ und $a_{ii} = a'_{ii} = 1$. Für $j < i$ erhalten wir

$$\sum_{k=1}^{n} a_{ik}a'_{kj} = \sum_{k=1}^{i-1} a_{ik}a'_{kj} + \sum_{k=i}^{n} a_{ik}a'_{kj} = 0,$$

denn $a_{ik} = 0$ für $k < i$ und $a'_{kj} = 0$ für $k \ge i > j$. Analog gilt

$$\sum_{k=1}^{n} a_{ik}a'_{ki} = \sum_{k=1}^{i-1} a_{ik}a'_{ki} + a_{ii}a'_{ii} + \sum_{k=i+1}^{n} a_{ik}a'_{ki} = 1,$$

also $AA' \in U$. Es bleibt zu zeigen, dass $A^{-1} \in U$. Wir definieren die Matrix $A'' = (a''_{ij})$ mit

$$a''_{ij} = \begin{cases} 0 & j < i, \\ 1 & j = i, \\ \sum_{r=1}^{j-i} \sum_{i=l_0<\ldots<l_r=j} (-1)^r a_{l_0 l_1} a_{l_1 l_2} \cdots a_{l_{r-1} l_r} & j > i. \end{cases}$$

Offensichtlich gilt $A'' \in U$ und wir behaupten, dass $A'' = A^{-1}$. Wir müssen also nur zeigen dass $\sum_{k=1}^{n} a_{ik} a''_{ki} = 0$ für $j > i$. Tatsächlich gilt (mit $r = s + 1$ und $l_1 = m_0, \ldots, l_{s+1} = m_s$)

$$\begin{aligned} \sum_{k=1}^{n} a_{ik} a''_{ki} &= a_{ii} a''_{ij} + \sum_{k=i+1}^{j-1} a_{ik} a''_{kj} + a_{ij} a''_{jj} \\ &= a''_{ij} + a_{ij} + \sum_{k=i+1}^{j-1} a_{ik} \sum_{s=1}^{j-k} \sum_{k=m_0<\ldots<m_s=j} (-1)^s a_{m_0 m_1} \cdots a_{m_{s-1} m_s} \\ &= a''_{ij} + a_{ij} + \sum_{k=i+1}^{j-1} \sum_{s=1}^{j-k} \sum_{k=m_0<\ldots<m_s=j} (-1)^s a_{i m_0} a_{m_0 m_1} \cdots a_{m_{s-1} m_s} \\ &= a''_{ij} + a_{ij} - \sum_{r=2}^{j-i} \sum_{i=l_0<\ldots<l_r=j} (-1)^r a_{l_0 l_1} a_{l_1 l_2} \cdots a_{l_{r-1} l_r} \\ &= a''_{ij} - \sum_{r=1}^{j-i} \sum_{i=l_0<\ldots<l_r=j} (-1)^r a_{l_0 l_1} a_{l_1 l_2} \cdots a_{l_{r-1} l_r} = 0. \end{aligned}$$

(b) Offensichtlich ist jede Permutationsmatrix eine Monomialmatrix, also $V \subseteq N$. Die Menge V ist das Bild der (injektiven) Permutationsdarstellung $\mathrm{S}_n \to \mathrm{GL}_n(K)$, $\sigma \mapsto P_\sigma$, also ist V eine Gruppe mit $V \cong \mathrm{S}_n$.

(c) Es ist leicht zu sehen, dass $HU \subseteq B$ und $UH \subseteq B$. Es sei $A \in (a_{ij}) \in B$, also mit $a_{ij} = 0, i > j$. Bemerke: $\det(A) = \prod a_{ii} \neq 0$, also ist jedes $a_{ii} \neq 0$. Setze $D = \mathrm{Diag}(a_{11}, \ldots, a_{nn}$. Dann gilt $D \in H$, $C = AD^{-1} \in U$ und $C' = D^{-1}A \in U$, also $A = CD \in UH$ und $A = DC' \in HU$. Dies zeigt $B \subseteq UH$ und $B \subseteq HU$ und damit $B = UH$ und $B = HU$.

Ein analoges Argument gilt für $N = HV = VH$. □

Aufgabe 4.23. In Bezug auf Bezeichnung 4.8 zeige:

(a) Es gelten $U = X_i Y_i = Y_i X_i$ und $X_i \cap Y_i = \{\mathbf{1}_n\}$.
(b) Es gelten $s_i X_i s_i^{-1} = X'_i$ und $s_i Y_i s_i^{-1} = Y_i$.
(c) Es gilt $P_\sigma X_{ij} P_\sigma^{-1} = X_{\sigma(i),\sigma(j)}$.

Lösung. (a) Klar gilt $X_i \subset U$ und $Y_i \subset U$, also auch $X_i Y_i \subseteq U$. Umgekehrt sei $A = (a_{ij}) \in U$. Definiere die Matrix $A' = \mathbf{1}_n + a_{i,i+1} E_{i,i+1} \in X_i$. Dann gilt $(A')^{-1} = \mathbf{1}_n - a_{i,i+1} E_{i,i+1}$ und es ist leicht zu sehen, dass $A'' = (A')^{-1} A \in Y_i$. Damit $A = A' A'' \in X_i Y_i$, also $U = X_i Y_i$.

Ein analoges Argument zeigt $U = Y_i X_i$. Schließlich ist die Gleichung $X_i \cap Y_i = \{\mathbf{1}_n\}$ trivial.

(b) Sind $z_1, \dots, z_n$ die Zeilen der Matrix A, so sind $z_{\sigma(1)}, \dots, z_{\sigma(n)}$ die Zeilen der Matrix $P_\sigma A$. Sind $s_1, \dots, s_n$ die Spalten der Matrix A, so sind $s_{\sigma^{-1}(1)}, \dots, s_{\sigma^{-1}(n)}$ die Spalten der Matrix AP_σ. Deshalb gilt $P_\sigma A = (a_{\sigma(i)j}) = (a_{\sigma(i)\sigma^{-1}(\sigma(j))}) = A' P_\sigma$, wobei $A' = (a_{\sigma(i)\sigma(j)})$.

Die Aussagen (c) und (d) folgen unmittelbar aus (b), denn $s_i = s_i^{-1}$. □

Aufgabe 4.24. Zeige, dass B und V auch ein BN-Paar für $\mathrm{GL}_n(K)$ bilden, aber nicht gesättigt.

Aufgabe 4.25. Es sei G eine Gruppe und gegeben seien Untergruppen $B, N \subseteq G$, die ein BN-Paar bilden. Es sei $Z \subseteq G$ ein Normalteiler mit $Z \subseteq B$. (Zum Beispiel ist $Z = \bigcap_{g \in G} gBg^{-1}$ stets ein solcher Normalteiler – warum?). Es sei $\bar{G} = G/Z$. Zeige: Die Untergruppen $\bar{B} = B/Z$ und $\bar{N} = N/Z$ bilden ein BN-Paar in $\bar{G}$ und die kanonische Abbildung $N \to \bar{N}$ induziert einen Isomorphismus von $W = N/H$ auf die Weyl-Gruppe von $\bar{G}$. Damit folgt, dass auch

$$\mathrm{PGL}_n(K) = \mathrm{GL}_{n+1}(K)/\,\mathrm{Z}(\mathrm{GL}_{n+1}(K))$$

eine Gruppe mit einem BN-Paar ist.

Aufgabe 4.26. Es sei G eine Gruppe und gegeben seien Untergruppen $B, N \subseteq G$, die ein BN-Paar bilden. Es sei W die Weyl-Gruppe von G, mit Erzeugendensystem $S \subseteq W$.

(a) Es seien $w \in W$ und $s \in S$ mit $\ell(sw) < \ell(w)$. Zeige: $s \in BwBw^{-1}B$.

(b) Für eine beliebige Untergruppe $U \leq G$ definieren wir den *Normalisator* von U in G

$$\mathrm{N}_G(U) = \{\, g \in G \mid gUg^{-1} = U \,\}.$$

Zeige: $\mathrm{N}_G(B) = B$. (Hinweis: Es sei $g \in \mathrm{N}_G(B)$ und schreibe $g = bwb'$ mit $b, b' \in B$ und $w \in W$. Wäre $w \neq 1 \in W$, so wähle $s \in S$ mit $\ell(sw) < \ell(w)$ und wende dann (a) an.)

(c) Es sei $\mathrm{Z}(G)$ das Zentrum von G. Zeige: $\mathrm{Z}(G) \subseteq B$ und damit dann auch $\mathrm{Z}(G) \subseteq \bigcap_{g \in G} gBg^{-1}$.

Lösung. (a) Setze $p = \ell(w)$. Dann ist $\ell(sw) = p - 1$, also gibt es $s_2, \dots, s_p \in S$ mit $sw = s_2 \cdots s_p$. Wir setzen $s_1 = s$ und schreiben $w = s_1 s_2 \cdots s_p$. Dann gilt $w^{-1} = s_p \cdots s_2 s_1$. Wegen der Multiplikationsregeln der Bruhat-Zerlegung gilt

$$\begin{aligned}
C(w)C(w^{-1}) &= C(s_1 \cdots s_{p-1}s_p)C(s_p s_{p-1} \cdots s_1) \\
&= C(s_1) \cdots C(s_{p-1})C(s_p)C(s_p)C(s_{p-1}) \cdots C(s_1) \\
&= C(s_1) \cdots C(s_{p-1})\big(C(1) \cup C(s_p)\big)C(s_{p-1}) \cdots C(s_1) \\
&= C(s_1) \cdots C(s_{p-2})\big(C(s_{p-1})C(s_{p-1}) \cup C(s_{p-1})C(s_p)C(s_{p-1})\big)C(s_{p-2}) \cdots C(s_1) \\
&= C(s_1) \cdots C(s_{p-2})\big(C(1) \cup C(s_{p-1}) \cup C(s_{p-1})C(s_p)C(s_{p-1})\big)C(s_{p-2}) \cdots C(s_1) \\
&= C(1) \cup C(s_1) \cup C(s_1)C(s_2)C(s_1) \cup \ldots \cup C(s_1) \cdots C(s_{p-1})C(s_p)C(s_{p-1}) \cdots C(s_1).
\end{aligned}$$

Insbesondere gilt $s \in C(s) = C(s_1) \subseteq C(w)C(w^{-1}) = BwBw^{-1}B$.

(b) Es gilt $U \subseteq \mathrm{N}_G(U)$ für jede Untergruppe U, also bleibt es zu zeigen, dass $B \supseteq \mathrm{N}_G(B)$. Wegen (BN4) lässt sich jedes Element $g = bwb'$ mit $b, b' \in B$ und $w \in W$ schreiben (d. h. $g = bnb'$

mit $n \in N$ und $\bar{n} = w \in W$). Ist $g \in \mathrm{N}_G(B)$ so gilt $gBg^{-1} = B$, sprich $BwBw^{-1}B = B$. Wäre $w \neq 1$, dann finden wir $s \in S$ mit $\ell(sw) < \ell(w)$. Wegen (a) gilt $s \in B = C(1)$, aber das ist ein Widerspruch zur Bruhat-Zerlegung, denn $s \in C(s)$ und $C(1)$ und $C(s)$ sind disjunkte Teilmengen.

(c) Es gilt $\mathrm{Z}(G) \supseteq \mathrm{N}_G(U)$ für jede Untergruppe U, also $\mathrm{Z}(G) \subseteq \mathrm{N}_G(B) = B$. Aus $\mathrm{Z}(G) \trianglelefteq G$ folgt $\mathrm{Z}(G) = g\,\mathrm{Z}(G)g^{-1} \subseteq gBg^{-1}$ für jedes $g \in G$. □

Aufgabe 4.27. Es sei G eine Gruppe und gegeben seien Untergruppen $B, N \subseteq G$, die ein BN-Paar bilden. Es sei W die Weyl-Gruppe von G, mit Erzeugendensystem $S \subseteq W$. Zeige:

(a) Für $s \in S$ ist $B \cup BsB$ eine Untergruppe von G.

(b) Es sei $w \in W$, $w \neq 1$, sodass $B \cup BwB$ eine Untergruppe ist. Dann muss $w \in S$ gelten.

Es folgt also, dass das Erzeugendensystem S für W eindeutig bestimmt ist: Es ist genau die Menge aller $w \in W$, $w \neq 1$, sodass $B \cup BwB$ eine Untergruppe von G ist.

Lösung. (a) Ist $g \in B$, so ist selbstverständlich $g^{-1} \in B$, denn B eine Untergruppe ist. Aus $s^2 \in H$ folgt $s^{-1} = sh$ mit $h \in H \subseteq B$. Ist $g \in C(s)$, so gibt es $b_1, b_2 \in B$ mit $g = b_1 s b_2$, also $g^{-1} = b_2^{-1}s^{-1}b_1^{-1} = b_2^{-1}s(hb_1^{-1}) \in C(s)$.

Es fehlt also zu zeigen, dass $gg' \in B \cup C(s)$ für alle $g, g' \in B \cup C(s)$. Wegen der Multiplikationsregeln der Bruhat-Zerlegung gilt

$$C(s)C(s) = C(1) \cup C(s) = B \cup C(s).$$

Nun unterscheiden wir vier Fälle, je nachdem g und g' in B oder $C(s)$ liegen. Wir erhalten

$$gg' \in \begin{cases} B, & \text{falls } g \in B \text{ und } g' \in B, \\ C(s), & \text{falls } g \in B \text{ und } g' \in C(s), \\ C(s), & \text{falls } g \in C(s) \text{ und } g' \in B, \\ C(s)C(s) = B \cup C(s), & \text{falls } g \in C(s) \text{ und } g' \in C(s), \end{cases}$$

also $gg' \in B \cup C(s)$ in allen vier Fällen.

(b) Da $w \in C(w)$ und $B \cup C(w)$ eine Untergruppe ist, gilt $w^{-1} \in B \cup C(w)$. Es kann aber nicht $w^{-1} \in B$ sein, sonst $C(w^{-1}) = C(1)$, also $w^{-1} = 1$, was $w \neq 1$ widerspricht. Dementsprechend gilt $w^{-1} \in C(w)$, d. h. $C(w^{-1}) = C(w)$ und damit $w = w^{-1}$.

Damit $B \cup C(w)$ eine Untergruppe ist, muss gelten

$$C(w)C(w) \subseteq B \cup C(w). \tag{4.9}$$

Es sei $w = s_1 \cdots s_m$ ein minimaler Ausdruck für w. Wir nehmen mit $m \geq 2$. Setze $w_p = s_1 \cdots s_p$ und $t_p = w_p^{-1} = s_p \cdots s_1$. Bemerke: $w_m = w = w^{-1} = t_m$.

Für alle $0 \leq i \leq p-1$ gilt $C(s_i s_{i+1} \cdots s_p) = C(s_i)C(s_{i+1} \cdots s_p)$, also

$$C(w_p) = C(s_1 \cdots s_p) = C(s_1)C(s_2 \cdots s_p) = \ldots = C(s_1)C(s_2) \cdots C(s_p).$$

Damit erhalten wir

$$\begin{aligned} C(w_p)C(t_p) &= C(s_1)\cdots C(s_{p-1})C(s_p)C(s_p \dots s_1) \\ &= C(s_1)\cdots C(s_{p-1})\big(C(s_{p-1}\dots s_1) \cup C(s_p \cdots s_1)\big) \\ &= C(w_{p-1})\big(C(t_{p-1}) \cup C(t_p)\big) \\ &= C(w_{p-1})C(t_{p-1}) \cup C(w_{p-1})C(t_p). \end{aligned}$$

Per Induktion gilt also

$$\begin{aligned} C(w)C(w) &= C(w_m)C(t_m) \\ &= C(w_{m-1})C(t_{m-1}) \cup C(w_{m-1})C(t_m) \\ &= C(w_{m-2})C(t_{m-2}) \cup C(w_{m-2})C(t_{m-1}) \cup C(w_{m-1})C(t_m) \\ &= \dots = C(w_0)C(t_0) \cup \bigcup_{p=1}^{m} C(w_{p-1})C(t_p). \end{aligned}$$

Insbesondere gilt $C(s_1) = C(1)C(s_1) = C(w_0)C(t_1) \subseteq C(w)C(w)$. Wegen (4.9) gilt also $C(s_1) \subseteq B \cup C(w) = C(1) \cup C(w)$, aber das widerspricht die Bruhat-Zerlegung, denn $C(s_1)$, $C(1)$ und $C(w)$ sind disjunkt. □

4.4 Coxeter-Gruppen und Weyl-Gruppen

Definition 4.28. Es sei S eine Menge und $M = (m_{st})_{s,t\in S}$ eine (womöglich unendliche) quadratische Matrix mit Einträgen in $\mathbb{Z} \cup \{\infty\}$, sodass $m_{ss} = 1$ und $m_{st} = m_{ts} \geq 2$ für alle $s, t \in S$, $s \neq t$. Es sei F die freie Gruppe auf S und $R = \{\, (st)^{m_{st}} \mid s, t \in S, m_{st} < \infty \,\}$. Dann heißt

$$W(M) := \langle\, S \mid R \,\rangle$$

die *Coxeter-Gruppe* zur Matrix M.

Bezeichnen wir die Bilder der $s \in S$ in $W(M)$ mit $\bar{s}$, so gilt also $\bar{s}^2 = 1$ und $(\bar{s}\bar{t})^{m_{st}} = 1$ für alle $s, t \in S$ mit $m_{st} < \infty$. Insbesondere $\bar{s}\bar{t} = \bar{t}\bar{s}$ wenn $m_{st} = 2$.

Beispiel 4.29. Es sei $M \in \mathrm{M}_{n-1}(\mathbb{Z})$ die Matrix

$$M := \begin{pmatrix} 1 & 3 & & & 2 \\ 3 & 1 & 3 & & \\ & 3 & 1 & \ddots & \\ & & \ddots & \ddots & 3 \\ 2 & & & 3 & 1 \end{pmatrix}.$$

Wegen Satz 3.16 ist die zu M zugehörige Coxeter-Gruppe isomorph zu S_n. Dieses Ergebnis ist auch ein Spezialfall von Satz 4.38 angewandt auf $G = \mathrm{GL}_n(K)$.

Diedergruppen (Beispiel 3.11) und Dreiecksgruppen (Beispiel 3.12) sind auch Coxeter-Gruppen, denen wir schon begegnet sind.

Wir wollen nun den Zusammenhang zwischen BN-Paaren und Coxeter-Gruppen untersuchen. Nach dem Hauptsatz (Satz 4.38) ist die Weyl-Gruppe W einer Gruppe mit BN-Paar stets eine Coxeter-Gruppe. Was wir aber eigentlich brauchen ist nicht das BN-Paar, sondern nur, dass das Austauschlemma (Folgerung 4.20) gilt.

Zunächst seien W eine beliebige Gruppe und S ein Erzeugendensystem für W mit $\mathrm{Ord}(s) = 2$ für alle $s \in S$. Wegen $s = s^{-1}$ ist dann wieder jedes $w \in W$ darstellbar als $w = s_1 \cdots s_m$ mit $s_i \in S$. Ist m minimal, so heißt der Ausdruck wieder reduziert und $\ell(w) = m$ Länge von w. Wir nehmen jetzt an, dass die Aussage des Austauschlemmas gilt.

Annahme 4.30. *Es seien $w \in W$, $w = s_1 \cdots s_p$ ein reduzierter Ausdruck mit $s_i \in S$ und $s \in S$ ein beliebiges Element mit $\ell(sw) \leq \ell(w)$. Dann gibt es $i \in \{1, \ldots, p\}$ mit $sw = s_1 \cdots s_{i-1} s_{i+1} \cdots s_p$.*

Lemma 4.31. *Unter Annahme 4.30 seien $w \in W$ und $w = s_1 \cdots s_m$ ein beliebiger Ausdruck mit $s_i \in S$, nicht notwendig reduziert. Dann gibt es $1 \leq i_1 < \ldots < i_p \leq m$, sodass $w = s_{i_1} \cdots s_{i_p}$ ein reduzierter Ausdruck ist, d. h. $p = \ell(w)$.*

Beweis per Induktion auf m. Es sei $p = \ell(w)$. Ist $m = 0$ oder $m = 1$, so ist der Ausdruck $w = 0$ bzw. $w = s_1$ schon reduziert und die Aussage gilt. Es sei nun $m > 1$. Ist $w = s_1 \cdots s_m$ bereits reduziert, so ist nichts zu zeigen, denn $p = m$. Es sei also $p < m$. Dann gibt es ein $i \in \{1, \ldots, m-1\}$, sodass $s_{i+1} \cdots s_m$ reduziert, aber $s_i s_{i+1} \cdots s_m$ nicht reduziert ist. Nach Annahme 4.30 gibt es $j \in \{i+1, \ldots, m\}$ mit $s_i s_{i+1} \cdots s_m = s_{i+1} \cdots s_{j-1} s_{j+1} \cdots s_m$. Also ist

$$w = s_1 \cdots s_m = s_1 \cdots s_{i-1} s_{i+1} \cdots s_{j-1} s_{j+1} \cdots s_m.$$

Der Ausdruck auf der rechten Seite hat $m-2$ Faktoren. Die Behauptung folgt dann per Induktion. □

Bemerkung 4.32. Es seien $s, t \in S$ mit $s \neq t$ und $m = \mathrm{Ord}(st) < \infty$. Angenommen, $m_{st} = m$, dann ist die Untergruppe $W_{st} = \langle s, t \rangle \leq W$ isomorph zur Diedergruppe D_m der Ordnung $2m$ nach Aufgabe 3.19. Die $2m$ Elemente von W_{st} sind wie folgt gegeben:

$$1,\ s,\ st,\ sts,\ \ldots,\ sts\cdots\ (m-1 \text{ Faktoren}),$$
$$t,\ ts,\ tst,\ \ldots,\ tst\cdots\ (m-1 \text{ Faktoren}),\ \Delta_{st},$$

wobei

$$\Delta_{st} = ststs\cdots = tstst\cdots \quad \text{(jeweils } m \text{ Faktoren)}.$$

Die Gleichheit zwischen den zwei Ausdrücken für Δ_{st} folgt aus $1 = (st)^m$. Alle obigen Ausdrücke sind reduziert.

Definition 4.33. Ein *Monoid* ist eine Menge $\mathcal{M}$ zusammen mit einer assoziativen Verknüpfung $*$, sodass ein neutrales Element $e \in \mathcal{M}$ exisitiert.

Satz 4.34 (Matsumoto, Tits)**.** *Unter Annahme 4.30 seien $\mathcal{M}$ ein Monoid und $f : S \to \mathcal{M}$ eine Abbildung, sodass für alle $s, t \in S$ mit $s \neq t$ und $m_{st} = \mathrm{Ord}(st) < \infty$ gilt*

$$f(s) * f(t) * f(s) * \ldots = f(t) * f(s) * f(t) * \ldots \quad \textit{(jeweils } m_{st} \textit{ Faktoren)}. \tag{4.10}$$

Dann lässt sich f zu einer Abbildung $\hat{f} : W \to \mathcal{M}$ fortsetzen, sodass

$$\hat{f}(w) = f(s_1) * \ldots * f(s_p), \tag{4.11}$$

falls $w = s_1 \cdots s_p$ ein reduzierter Ausdruck mit $s_i \in S$ ist.

Beweis. Gegeben $w \in W$ und ein reduzierter Ausdruck $w = s_1 \cdots s_p$ mit $s_i \in S$, definieren wir $\hat{f}(w)$ genau wie in (4.11). Das Ziel ist es nun zu zeigen, dass $\hat{f}$ wohledefiniert ist, d. h., falls $w = t_1 \cdots t_p$ ein anderer reduzierter Ausdruck mit $t_i \in S$ ist, dann gilt in $\mathcal{M}$

$$f(s_1) * \ldots * f(s_p) = f(t_1) * \ldots * f(t_p). \tag{4.12}$$

Das zeigen wir per Induktion auf $p = \ell(w)$. Offensichtlich gibt es keine Ambiguität, wenn $p = 0$ oder $p = 1$, denn es muss $\hat{f}(1) = e$ und $\hat{f}(s) = f(s)$ für $s \in S$ sein. Es sei nun $p > 1$.

Es gilt $\ell(t_1 w) = \ell(t_2 \cdots t_p) = p - 1 < p$. Nach Annahme 4.30 angewandt auf w gibt es $i \in \{1, \ldots, p\}$ mit $t_1 w = s_1 \cdots s_{i-1} s_{i+1} \cdots s_p$, d. h.

$$w = t_1^{-1} s_1 \cdots s_{i-1} s_{i+1} \cdots s_p = t_1 s_1 \cdots s_{i-1} s_{i+1} \cdots s_p.$$

Behauptung 4.35. *Ist $i \neq p$, so gilt* (4.12).

Beweis der Behauptung. Falls $i \neq p$, dann sind $w s_p = t_1 s_1 \cdots s_{i-1} s_{i+1} \cdots s_{p-1} = s_1 \cdots s_{p-1}$ zwei reduzierte Ausdrücke für $w s_p$ (mit $p - 1$ Faktoren). Nach Induktion gilt

$$f(t_1) * f(s_1) * \ldots * f(s_{i-1}) * \ldots * f(s_{i+1}) * \ldots * f(s_{p-1}) = f(s_1) * \ldots * f(s_{p-1}).$$

Andererseits sind $t_1 w = s_1 \cdots s_{i-1} s_{i+1} \cdots s_p = t_2 \cdots t_p$ zwei reduzierte Ausdrücke für $t_1 w$ (mit $p - 1$ Faktoren). Nach Induktion gilt

$$f(s_1) * \ldots * f(s_{i-1}) * f(s_{i+1}) * \ldots * f(s_p) = f(t_2) * \ldots * f(t_p).$$

Damit erhalten wir

$$\begin{aligned} f(s_1) * \ldots * f(s_p) &= (f(s_1) * \ldots * f(s_{p-1})) * f(s_p) \\ &= (f(t_1) * f(s_1) * \ldots * f(s_{i-1}) * \ldots * f(s_{i+1}) * \ldots * f(s_{p-1})) * f(s_p) \\ &= f(t_1) * (f(s_1) * \ldots * f(s_{i-1}) * \ldots * f(s_{i+1}) * \ldots * f(s_{p-1}) * f(s_p)) \\ &= f(t_1) * f(t_2) * \ldots * f(t_p). \end{aligned}$$

□

Wir können also annehmen, dass $i = p$. Also $t_1 w = t_2 \cdots t_p = s_1 \cdots s_{p-1}$. Damit $w = t_1 s_1 \cdots s_{p-1}$ und nach Induktion

$$f(t_2) * \ldots * f(t_p) = f(s_1) * \ldots * f(s_{p-1}).$$

Es gilt $\ell(s_1 w) = \ell(s_2 \cdots s_{p-1}) = p - 1 < p$. Nach Annahme 4.30 ist $s_1 w$ gleich dem Produkt $t_1 s_1 \cdots s_{p-1}$ mit einem Faktor weniger. Nach den gleichen Argumenten wie in Behauptung 4.35 muss

dies wieder der letzte Faktor sein. Also $s_1 w = s_2 \cdots s_p = t_1 s_1 \cdots s_{p-2}$. Damit $w = s_1 t_1 s_1 \cdots s_{p-2}$ und nach Induktion

$$f(s_2) * \ldots * f(s_p) = f(t_1) * f(s_1) * \ldots * f(s_{p-2}).$$

Es gilt $\ell(t_1 w) = \ell(t_2 \cdots t_p) = p - 1 < p$. Nach Annahme 4.30 ist $t_1 w$ gleich dem Produkt $s_1 t_1 s_1 \cdots s_{p-2}$ mit einem Faktor weniger. Nach den gleichen Argumenten wie in Behauptung 4.35 muss dies wieder der letzte Faktor sein. Also $t_1 w = t_2 \cdots t_p = s_1 t_1 s_1 \cdots s_{p-3}$. Damit $w = t_1 s_1 t_1 s_1 \cdots s_{p-3}$ und nach Induktion

$$f(t_2) * \ldots * f(t_p) = f(s_1) * f(t_1) * f(s_1) * \ldots * f(s_{p-3}).$$

Nach $p-1$ Schritten werden alle Faktoren $s_2, \ldots, s_p$ verschwinden. Tauschen wir nun die Rollen von s und t und wenden genau die gleichen Argumente wieder an, so erhalten wir

$$w = t_1 s_1 t_1 s_1 t_1 \cdots = s_1 t_1 s_1 t_1 s_1 \cdots \tag{4.13}$$

und

$$f(s_1) * \ldots * f(s_p) = f(s_1) * f(t_1) * f(s_1) \cdot \ldots,$$
$$f(t_1) * \ldots * f(t_p) = f(t_1) * f(s_1) * f(t_1) \cdot \ldots,$$

jeweils mit p Faktoren. Aus (4.13) folgt $(s_1 t_1)^p = 1$, also $p \geq m_{s_1 t_1} = \mathrm{Ord}(s_1 t_1)$. Andererseits sind die Ausdrücke in (4.13) reduziert, also $p \leq m_{s_1 t_1}$ wegen Bemerkung 4.32. Schließlich muss $p = m_{s_1 t_1}$ sein, also folgt (4.12) aus Voraussetzung (4.10). □

Folgerung 4.36. *Unter Annahme 4.30 seien F die freie Gruppe auf S und*

$$R := \{ s^2 \mid s \in S \} \cup \{ (st)^{m_{st}} \mid s,t \in S, s \neq t, m_{st} = \mathrm{Ord}(st) < \infty \} \subseteq F.$$

Dann ist $W \cong \langle S \mid R \rangle$.

Beweis. Es sei $\bar{F} := \langle S \mid R \rangle = F / \langle\langle R \rangle\rangle$. Nach dem Relationenlemma (Lemma 3.9) gibt es einen surjektiven Homomorphismus $\varphi : \bar{F} \to W$ mit $\varphi(\bar{s}) = s$ für alle $s \in S$.

Die Gruppe $\bar{F}$ ist insbesondere ein Monoid. Wegen $(st)^{m_{st}} \in R$ gilt $(\bar{s}\bar{t})^{m_{st}} = 1$ und damit

$$\bar{s}\bar{t}\bar{s} \cdots = \bar{t}\bar{s}\bar{t} \cdots \quad \text{(jeweils } m_{st} \text{ Faktoren)}.$$

D. h., die Abbildung $f : S \to \bar{F}$ definiert durch $s \mapsto \bar{s}$ erfüllt die Voraussetzungen von Satz 4.34. Also gibt es eine Fortsetzung $\hat{f} : W \to \bar{F}$ mit $\hat{f}(w) = \bar{s}_1 \cdots \bar{s}_m$, wenn $w = s_1 \cdots s_m$ ein reduzierter Ausdruck mit $s_i \in S$ ist.

Behauptung 4.37. *Die Abbildung $\hat{f}$ ist ein Homomorphismus.*

Beweis der Behauptung. Wir müssen zeigen, dass $\hat{f}(yw) = \hat{f}(y)\hat{f}(w)$ für alle $y, w \in W$. Per Induktion nach $\ell(y)$ genügt es eigentlich zu zeigen, dass $\hat{f}(sw) = \bar{s}\hat{f}(w)$ für alle $s \in S$ und $w \in W$.

Angenommen $\ell(sw) > \ell(w)$, sei $w = s_1 \cdots s_m$ ein reduzierter Ausdruck mit $s_i \in S$. Dann ist $ss_1 \cdots s_m$ ebenfalls reduziert, also

$$\hat{f}(sw) = \hat{f}(ss_1 \cdots s_m) = \bar{s}\bar{s}_1 \cdots \bar{s}_m = \bar{s}\hat{f}(s_1 \cdots s_m) = \bar{s}\hat{f}(w).$$

Angenommen $\ell(sw) \leq \ell(w)$, setze $w' = sw$, sodass $w = sw'$. Dann ist $\ell(sw') > \ell(w')$, also $\hat{f}(sw') = \bar{s}\hat{f}(w')$ nach obiger Rechnung. Aus $s^2 \in R$ folgt $\bar{s}^2 = 1$, also $\hat{f}(sw) = \bar{s}\hat{f}(w)$. □

Damit sind φ und $\hat{f}$ jeweils Homomorphismen mit $\varphi \circ \hat{f} = \mathrm{id}_W$ und $\hat{f} \circ \varphi = \mathrm{id}_{\bar{F}}$. Das bedeutet, dass $W \cong \bar{F}$. □

Satz 4.38 (Hauptsatz)**.** *Es seien G eine Gruppe mit BN-Paar und W die zugehörige Weyl-Gruppe mit Erzeugendensystem S. Es sei $m_{st} \in \mathbb{Z} \cup \{\infty\}$ die Ordnung von $st \in W$ für $s, t \in S$. Dann ist W isomorph zur Coxeter-Gruppe $W(M)$, wobei $M = (m_{st})_{s,t \in S}$.*

Beweis. Die Weyl-Gruppe einer Gruppe mit BN-Paar erfüllt Annahme 4.30 wegen des Austauschlemmas (Folgerung 4.20). Die Behauptung des Satzes ist also eine Konsequenz von Folgerung 4.36. □

4.5 Aufgaben

Aufgabe 4.39. (Diese Aufgabe enthält eine weitere Anwendung des Lemmas von Matsumoto–Tits.)

Es sei W eine Gruppe, $S \subseteq W$ eine Teilmenge mit $W = \langle S \rangle$ und $\mathrm{Ord}(s) = 2$ für alle $s \in S$. Es gelte die Austauschbedingung fur (W, S). Es sei $\mathcal{M}$ die Potenzmenge von W. Wir definieren eine Verknüpfung $* \colon \mathcal{M} \times \mathcal{M} \to \mathcal{M}$ durch $A * B = \{\, ab \mid a \in A, b \in B \,\}$ für $A, B \in M$. Diese ist offenbar assoziativ, und die Menge $\{1\}$ ist neutrales Element bezüglich $*$. Betrachte nun die Abbildung

$$f \colon S \to \mathcal{M}, \quad s \mapsto \{1, s\}.$$

(a) Zeige: Die Voraussetzungen des Satzes von Matsumoto–Tits sind erfüllt. Also lässt sich f zu einer Abbildung $\hat{f} \colon W \to \mathcal{M}$ fortsetzen.
(b) Für $y, w \in W$ schreiben wir $y \preceq w$, wenn $y \in \hat{f}(w)$ gilt. Zeige: $y \preceq w$ impliziert $\ell(y) \leq \ell(w)$.
(c) Zeige, dass $\preceq$ eine partielle Ordnung auf W ist, die sogenannte *Bruhat–Chevalley-Ordnung*.
(d) Bestimme alle $y, w \in W = \mathrm{S}_3$ mit $y \preceq w$.
(e) Finde Elemente $y, w \in W = \mathrm{S}_4$ mit $\ell(y) < \ell(w)$ und $y \not\preceq w$.

Literaturverzeichnis

[1] Peter J. Cameron, *Permutation groups*, London Mathematical Society Student Texts, vol. 45, Cambridge University Press, Cambridge, 1999. MR 1721031

[2] Donald J. Collins, *A simple presentation of a group with unsolvable word problem*, Illinois J. Math. **30** (1986), no. 2, 230–234. MR 840121

[3] Marston Conder, *Hurwitz groups: a brief survey*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 2, 359–370. MR 1041434

[4] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.11.0*, 2020.

[5] L. C. Grove and C. T. Benson, *Finite reflection groups*, second ed., Graduate Texts in Mathematics, vol. 99, Springer-Verlag, New York, 1985. MR 777684

[6] David L. Johnson, *Presentations of groups*, second ed., London Mathematical Society Student Texts, vol. 15, Cambridge University Press, Cambridge, 1997. MR 1472735

[7] Joseph J. Rotman, *An introduction to the theory of groups*, fourth ed., Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1995. MR 1307623