Skript zur Vorlesung „GAGA B“
Gruppen, Algorithmen, Geometrien & Anwendungen
Universität Stuttgart, Wintersemester 2022/23

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

17. Januar 2023

Inhaltsverzeichnis

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

[4] 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

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

[6] Serre J.P., *Linear representations of finite groups*, Graduate Texts in Mathematics, vol. 42, Springer-Verlag, 1977.

[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

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 $\mathbf{1}_n = \mathrm{Diag}(1, \ldots, 1)$ 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 $S_1, S_2, \ldots, S_r \subseteq G$ einer Gruppe G setzen wir

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

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 $\mathrm{K}(G) \trianglelefteq G$.

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 $\pi \in S_n$. 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*)

$$\operatorname{sgn} : S_n \to \{1, -1\}$$

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

Das Signum ist 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 $A_3 \cong Z_3$ 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

$$K(A_4) = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \lhd A_4.$$

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

Beweis. Es sei $N \trianglelefteq A_n$ ein Normalteiler mit $N \neq \{\mathrm{id}\}$. Wir wollen zeigen, dass $N = A_n$ und wegen Aufgabe 1.50 (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 $\pi \in A_n$ 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 $N \trianglelefteq A_n$, 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 1.49, 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 1.49

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

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 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 $d' \mid sn'$, aber d' und n' sind teilerfremd, also $d' \mid s$. 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 1.49. Zeige: Falls $\sigma = (i_1\ i_2\ \ldots\ i_d) \in \mathrm{S}_n$ ein d-Zyklus ist und $\pi \in \mathrm{S}_n$, dann

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

Aufgabe 1.50. Zeige:

(a) Für $n \geq 3$ 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 $n \geq 5$ gilt

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

Lösung. (a) Es sei $H \leq \mathrm{S}_n$ 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 $1 = \mathrm{sgn}(\tau) = \prod_{i=1}^{r} \mathrm{sgn}(\sigma_i) = (-1)^r$. Angenommen, $r \geq 2$ (sonst $\tau = \mathrm{id}$), seien $\sigma_1 = (i\ j)$ und $\sigma_2 = (k\ l)$. Setze $I = \{i, j, k, l\}$. Da $i \neq j$, gilt $2 \leq |I| \leq 4$.

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 $n \geq 5$ und $K = \langle\, (i\ j)(k\ l) \mid i, j, k, l \text{ paarweise verschieden} \,\rangle \leq \mathrm{S}_n$. Klar gilt $K \subseteq \mathrm{A}_n$. Ist $\sigma = (i\ j\ k)$ ein 3-Zyklus, so gibt es $l, m \in \{1, \ldots, n\}$, 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 $\mathrm{A}_n = K$. □

Bis hier Woche 1-2

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 [3, §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 [3, §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]).

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]).

Bis hier Woche 3-4

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 3.30.

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 [5]).

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 3.30 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

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

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

3.4 Endliche Coxeter-Gruppen

Wir betrachten in diesem Abschnitt eine spezielle Klasse von Präsentationen, die die Präsentation für die symmetrische Gruppe S_n verallgemeinert.

Definition 3.18. Eine *Coxeter-Matrix* ist eine Matrix $M = (m_{ij}) \in \mathrm{M}_d(\mathbb{Z})$ mit $d \in \mathbb{N}$, $m_{ii} = 1$ für jedes i und $m_{ij} = m_{ji} \geq 2$ für alle $i \neq j$. Es sei F die freie Gruppe auf $S = \{s_1, \dots, s_n\}$ und $R = \{ (s_i s_j)^{m_{ij}} \mid 1 \leq i, j \leq n \}$. Dann heißt $W(M) := \langle S \mid R \rangle$ die *Coxeter-Gruppe* zur Matrix M.

Bezeichnen wir die Bilder der $s_i \in S$ in $W(M)$ mit $\bar{s}_i$, so gilt also $\bar{s}_i^2 = 1$ und $(\bar{s}_i \bar{s}_j)^{m_{ij}} = 1$ für alle i, j. Insbesondere $\bar{s}_i \bar{s}_j = \bar{s}_j \bar{s}_i$ wenn $m_{ij} = 2$.

Beispiel 3.19. Für $n \geq 2$ sei $M \in \mathrm{M}_{n-1}(\mathbb{Z})$ die Coxeter–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.

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

Bezeichnung 3.20. Eine Coxeter-Matrix $M = (m_{ij}) \in \mathrm{M}_d(\mathbb{Z})$ kann in einem indizierten Graphen $\Gamma = \Gamma(M)$ mit d Knoten $\{1, \dots, d\}$ kodiert werden. Zwei Knoten i und j, $i \neq j$, sind genau dann mit einer Kante verbunden, falls $m_{ij} \geq 3$. Ist $m_{ij} \geq 4$, so wird diese Kante mit m_{ij} indiziert.

Die indizierten Graphen in Abbildung 3.1 und Abbildung 3.2 auf Seite 33 heißen *Coxeter–Diagramme* bzw. *erweiterte Coxeter–Diagramme*.

Betrachte z.B. die oben definierte Coxeter-Matrix $M \in \mathrm{M}_{n-1}(\mathbb{Z})$ für S_n. Der entsprechende Graph $\Gamma(M)$ ist gleich dem Coxeter–Diagramm $\mathbf{A}_{n-1}$. Die zu dem Graphen $I_2(m)$ (für $m \geq 3$) gehörige Coxeter-Gruppe ist die Diedergruppen der Ordnung $2m$.

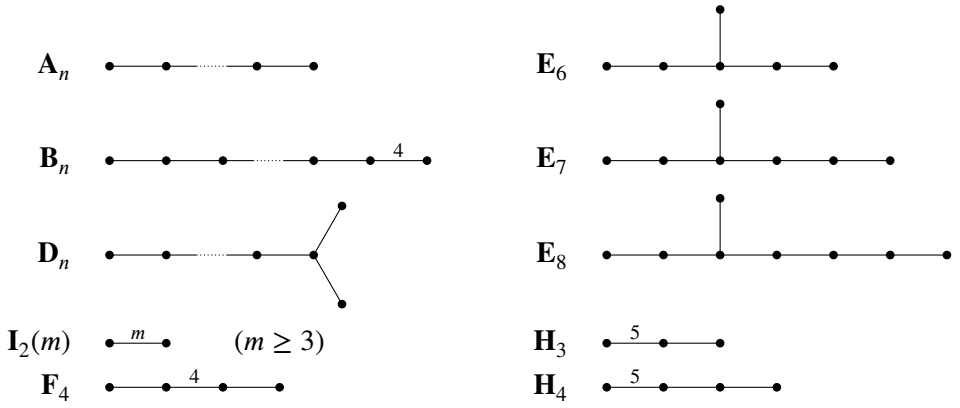


Abbildung 3.1: Coxeter–Diagramme. (Die Anzahl der Knoten von $\mathbf{A}_n, \mathbf{B}_n, \mathbf{D}_n$ ist gleich n.)

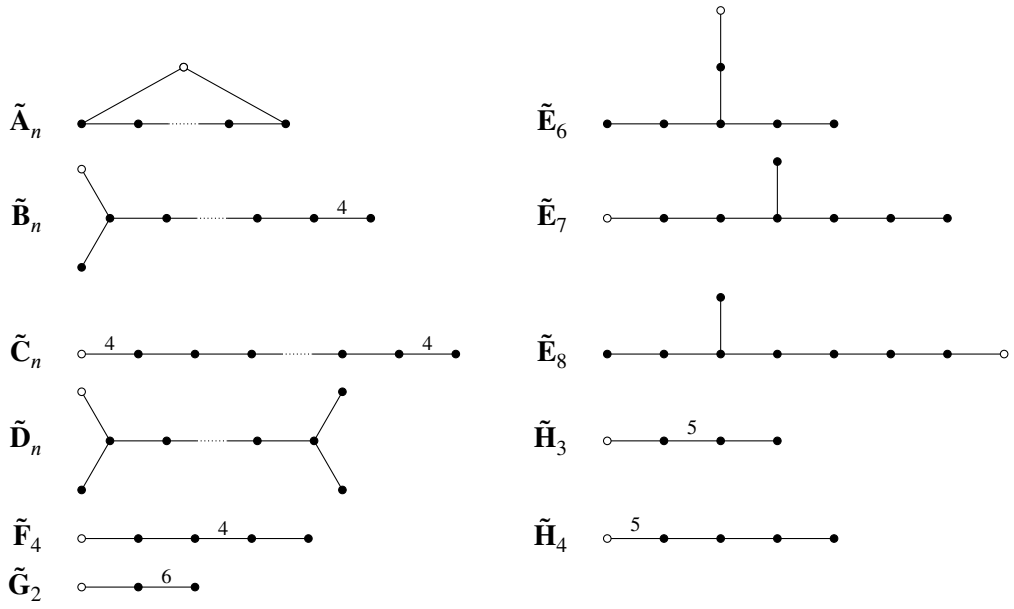


Abbildung 3.2: Erweiterte Coxeter–Diagramme. (Die Anzahl der Knoten von $\tilde{\mathbf{A}}_n, \tilde{\mathbf{B}}_n, \tilde{\mathbf{C}}_n, \tilde{\mathbf{D}}_n$ ist gleich $n + 1$.)

Wir fixieren nun eine Coxeter-Matrix $M = (m_{ij})_{1\le i,j\le d}$ mit Coxeter-Gruppe $W = W(M)$.

Bezeichnung 3.21. Es sei V ein $\mathbb{R}$-Vektorraum mit Basis $\{e_1, \dots, e_d\}$. Für $1 \le i \le d$ definieren wir die linearen Abbildungen $\rho_i : V \to V$ durch

$$\rho_i(e_j) = e_j + 2\cos(\pi/m_{ij})e_i.$$

Man rechnet leicht nach: $\rho_i(e_i) = -e_i$ und $\rho_i^2 = \mathrm{id}_V$ für alle i.

Lemma 3.22. *Es seien $i \neq j$ und $U \subseteq V$ der von e_i und e_j erzeugte Teilraum. Dann gilt $\rho_i(U) \subseteq U$ und $\rho_j(U) \subseteq U$ und es gibt einen Teilraum $U' \subseteq V$ mit $V = U \oplus U'$ und $\rho_i|_{U'} = \rho_j|_{U'} = \mathrm{id}_{U'}$.*

Beweis. Es gilt $\rho_i(e_i) = -e_i \in U$ und $\rho_i(e_j) = e_j + 2\cos(\pi/mij)e_i \in U$, also $\rho_i(U) \subseteq U$. Genauso gilt $\rho_j(e_i), \rho_j(e_j) \in U$. Nun wollen wir U' konstruieren. Für $l \neq i, j$ betrachte folgendes Gleichungssystem mit unbekannten x_l, y_l:

$$\begin{aligned} x_l - \cos(\pi/m_{ij})y_l &= \cos(\pi/m_{il}),\\ -\cos(\pi/m_{ij})x_l + y_l &= \cos(\pi/m_{jl}). \end{aligned}$$

Das Gleichungssystem hat genau eine Lösung x_l, y_l, denn es gilt

$$\det\begin{pmatrix} 1 & -\cos(\pi/m_{ij}) \\ -\cos(\pi/m_{ij}) & 1 \end{pmatrix} = 1 - \cos^2(\pi/m_{ij}) > 0,$$

weil $i \neq j$, also $m_{ij} \ge 2$ und $\cos^2(\pi/m_{ij}) < 1$. Es seien $e_l' = e_l + x_l e_i + y_l e_j$ und U' der von $\{\, e_l' \mid l \neq i, j \,\}$ erzeugte Teilraum. Bemerke: $\dim(U') = d - 2$ und $U \cap U' = \{0\}$. Außerdem gilt

$$\begin{aligned} \rho_i(e_l') &= \rho_i(e_l) + x_l\rho_i(e_i) + y_l\rho_i(e_j) = e_l + 2\cos(\pi/m_{il})e_i - x_l e_i + y_l\big(e_j + 2\cos(\pi/m_{ij})e_i\big)\\ &= e_l + \big(2\cos(\pi/m_{il}) + 2\cos(\pi/m_{ij})y_l - x_l\big)e_i + y_l e_j = e_l + x_l e_i + y_l e_j = e_l', \end{aligned}$$

also $\rho_i|_{U'} = \mathrm{id}_{U'}$. Genauso gilt $\rho_j(e_l') = e_l'$. □

Bis hier Woche 5

Folgerung 3.23. *Es gibt einen Homomorphismus $\rho : W \to \mathrm{GL}(V)$ mit $\rho(s_i) = \rho_i$ für $1 \le i \le d$.*

Beweis. Es gilt $\rho_i^2 = \mathrm{id}_V$ für alle i. Wegen $W = \langle\, S \mid R \,\rangle$ müssen wir dann noch zeigen, dass $(\rho_i\rho_j)^{m_{ij}} = \mathrm{id}_V$ für alle $i \neq j$ gilt. Es seien also $i \neq j$ fest und betrachte die Zerlegung $V = U \oplus U'$ und die Basis $B = \{\, e_i, e_j, e_l' \mid l \neq i, j \,\}$ wie in Lemma 3.22. Die Matrizen von ρ_i und ρ_j bezüglich B sind also

$$\left(\begin{array}{cc|c} -1 & 2\cos(\pi/m_{ij}) & 0 \\ 0 & 1 & \\ \hline & 0 & \mathbf{1}_{n-2} \end{array}\right) \quad \text{bzw.} \quad \left(\begin{array}{cc|c} 1 & 0 & 0 \\ 2\cos(\pi/m_{ij}) & -1 & \\ \hline & 0 & \mathbf{1}_{n-2} \end{array}\right),$$

also ist die Matrix von $\rho_i\rho_j$ bezüglich B gleich

$$\left(\begin{array}{c|c} A & 0 \\ \hline 0 & \mathbf{1}_{n-2} \end{array}\right), \quad \text{mit} \quad A := \begin{pmatrix} -1 & 2\cos(\pi/m_{ij}) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2\cos(\pi/m_{ij}) & -1 \end{pmatrix}.$$

Man rechnet nach dass $\det(A) = 1$ und $\mathrm{Spur}(A) = -2 + 4\cos^2(\pi/m_{ij}) = 2\cos(2\pi/m_{ij})$ gilt. Also ist das charakteristische Polynom von A gegeben durch $\chi_A = X^2 - 2\cos(2\pi/m_{ij})X + 1 = (X - \zeta_m)(X - \zeta_m^{-1})$, wobei $\zeta_m = \exp(2\pi/m_{ij}) \in \mathbb{C}$ eine Einheitswurzel der Ordnung m_{ij} ist. Folglich ist A diagonalisierbar mit Eigenwerten $\zeta_m^{\pm 1}$. Also hat A Ordnung m_{ij}. □

Bezeichnung 3.24. Es sei V ein $\mathbb{R}$-Vektorraum mit Basis $\{e_1, \dots, e_d\}$. Zur Coxeter-Matrix $M = (m_{ij}) \in \mathrm{M}_d(\mathbb{Z})$ definieren wir eine symmetrische Bilinearform $\beta : V \times V \to \mathbb{R}$ durch

$$\beta(e_i, e_j) := -\cos(\pi/m_{ij}) \quad \text{für } 1 \le i, j \le d.$$

Lemma 3.25. *Ist $|W| < \infty$, so ist β positiv definit.*

Beweis. Betrachte den Homomorphismus $\rho : W \to \mathrm{GL}(V)$ aus Folgerung 3.23 und es sei G das Bild von ρ. Nach Voraussetzung ist $|W| < \infty$, also auch $|G| < \infty$. Es sei $\langle\ ,\ \rangle : V \times V \to \mathbb{R}$ das (symmetrische, positiv definite) Standardskalarprodukt, sprich

$$\langle e_i, e_j \rangle = \begin{cases} 1 & \text{falls } i = j, \\ 0 & \text{falls } i \neq j. \end{cases}$$

Dann definieren wir $\Phi : V \times V \to \mathbb{R}$ durch

$$\Phi(v, w) = \sum_{g \in G} \langle g(v), g(w) \rangle.$$

Offensichtlich ist Φ eine symmetrische Bilinearform. Für jedes $v \in V$ ist $\langle g(v), g(v) \rangle \ge 0$, also $\Phi(v, v) \ge 0$. Ist $\Phi(v, v) = 0$, so ist $\langle g(v), g(v) \rangle = 0$ für alle $g \in G$, insbesondere für $g = \mathrm{id}$, also $\langle v, v \rangle = 0$, d. h. $v = 0$. Deshalb ist auch Φ positiv definit. Außerdem ist Φ G-invariant, sprich

$$\Phi(g(v), g(w)) = \Phi(v, w)$$

für alle $v, w \in V$ und $g \in G$. Es gilt nämlich

$$\Phi(g(v), g(w)) = \sum_{h \in G} \langle h(g(v)), h(g(w)) \rangle = \sum_{h \in G} \langle hg(v), hg(w) \rangle = \sum_{h \in G} \langle h(v), h(w) \rangle = \Phi(v, w),$$

denn mit h durchläuft auch gh alle Elemente von G. Damit folgt jetzt

$$\Phi(e_i, e_j) = \Phi(\rho_i(e_i), \rho_i(e_j)) = \Phi\big(-e_i, e_j + 2\cos(\pi/m_{ij})e_i\big) = -\Phi(e_i, e_j) - 2\cos(\pi/m_{ij})\Phi(e_i, e_i),$$

also

$$\Phi(e_i, e_j) = -\cos(\pi/m_{ij})/\delta_i,$$

wobei $\delta_i = \Phi(e_i, e_i)^{-1} > 0$. Eine analoge Rechnung mit ρ_j anstelle von ρ_i zeigt, dass $\Phi(e_i, e_j) = -\cos(\pi/m_{ij})/\delta_j$. Also: Ist $\Phi(e_i, e_j) \neq 0$, so folgt $\delta_i = \delta_j$.

Es sei nun $v = \sum_{i=1}^d x_i e_i \in V$ beliebig mit $x_i \in \mathbb{R}$. Setze $v' = \sum_{i=1}^d \sqrt{\delta_i} x_i e_i \in V$. Dann gilt

$$\beta(v, v) = \beta\Big(\sum_{i=1}^d x_i e_i, \sum_{i=1}^d x_i e_i\Big) = \sum_{i,j=1}^d x_i x_j \beta(e_i, e_j) = -\sum_{i,j=1}^d x_i x_j \cos(\pi/m_{ij}) = \sum_{i,j=1}^d x_i x_j \delta_i \Phi(e_i, e_j).$$

Nun ist es $\Phi(e_i, e_j) = 0$ oder $\delta_i = \delta_j$, also $\delta_i = \sqrt{\delta_i}\sqrt{\delta_j}$. Deshalb können wir so fortsetzen:

$$\beta(v, v) = \sum_{i,j=1}^d (\sqrt{\delta_i} x_i)(\sqrt{\delta_j} x_j)\Phi(e_i, e_j) = \Phi\Big(\sum_{i=1}^d \sqrt{\delta_i} x_i e_i, \sum_{j=1}^d \sqrt{\delta_j} x_j e_j\Big) = \Phi(v', v') \geq 0.$$

Ist $\beta(v, v) = 0$, so $\Phi(v', v') = 0$, d. h. $v' = 0$ und damit auch $v = 0$. Also ist β auch definit positiv. □

Bemerkung 3.26. Es seien V ein $\mathbb{R}$-Vektorraum der Dimension $d < \infty$ mit Basis $\{e_1, \dots, e_d\}$ und $\alpha : V \times V \to \mathbb{R}$ eine positiv definite symmetrische Bilinearform. Nach dem Gram-Schmidtschen Orthogonalisierungsverfahren können wir ein Orthonormalsystem $\{b_1, \dots, b_d\}$ finden, sprich eine Basis von V, sodass $\alpha(b_i, b_i) = 1$ und $\alpha(b_i, b_j) = 0$ falls $i \neq j$. Es seien T die Basiswechselmatrix, $A = (\alpha(e_i, e_j))$ die Gram-Matrix von α bezüglich $\{e_1, \dots, e_d\}$ und $B = (\alpha(b_i, b_j))$ die Gram-Matrix von α bezüglich $\{b_1, \dots, b_d\}$. Dann ist $B = \mathbf{1}_d$ und $A = T^{\mathrm{t}} B T = T^{\mathrm{t}} T$. Damit ist $\det(A) = \det(T^{\mathrm{t}} T) = \det(T^{\mathrm{t}}) \det(T) = \det(T)^2 > 0$.

Es sei nun $I \subseteq \{1, \dots, d\}$ eine Teilmenge und $U \subseteq V$ der von $\{ e_i \mid i \in I \}$ erzeugte Teilraum. Dann ist $A_I = (\alpha(e_i, e_j))_{i,j \in I}$ die Gram-Matrix der Einschränkung $\gamma = \alpha|_{U \times U}$ von α auf U. Offensichtlich ist γ immer noch positiv definit, also mit vorherigem Argument gilt $\det(A_I) > 0$.

Mit den Bezeichnungen aus Lemma 3.25 gilt also

$$\det(-\cos(\pi/m_{ij}))_{i,j \in I} > 0,$$

für alle Teilmengen $I \subseteq \{1, \dots, d\}$.

Satz 3.27 (Klassifikation der endlichen Coxeter-Gruppen)**.** *Es seien $M = (m_{ij}) \in \mathrm{M}_d(\mathbb{Z})$ eine Matrix mit $m_{ii} = 1$ für alle i und $m_{ij} = m_{ji} \geq 2$ für alle $i \neq j$, $W := W(M)$ die zugehörige Coxeter-Gruppe und $\Gamma := \Gamma(M)$ der zugehörige Graph. Ist W endlich, so ist Γ eine Vereinigung von Coxeter–Dynkin-Diagrammen.*

Beweis. 1. Schritt. Es sei V der $\mathbb{R}$-Vektorraum mit Basis $\{e_1, \dots, e_d\}$. Die in Lemma 3.25 definierte Bilinearform $\beta : V \times V \to \mathbb{R}$ ist positiv definit. Es sei $I \subseteq \{1, \dots, d\}$ und $M' = (m'_{ij})_{i,j \in I} \in \mathrm{M}_{|I|}(\mathbb{Z})$ eine Matrix mit $m_{ii} = 1$ für jedes $i \in I$ und

$$2 \leq m'_{ij} \leq m_{ij} \tag{3.3}$$

für alle $i, j \in I$ mit $i \neq j$. Betrachte den von $\{ e_i \mid i \in I \}$ erzeugten Teilraum V' und definiere $\beta' : V' \times V' \to \mathbb{R}$ durch

$$\beta'(e_i, e_j) = -\cos(\pi/m'_{ij})$$

für $i, j \in I$. Bemerke: Der Graph $\Gamma' = \Gamma(M')$ entsteht aus Γ durch Weglassen von einigen Knoten und Verringerung der Indizes an den Kanten (eventuell inklusiv Weglassen einer Kante). Einen solchen Graphen nennen wir *Teilgraph* von Γ.

Behauptung 3.28. *Die Bilinearform β' ist auch positiv definit.*

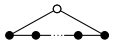
Beweis der Behauptung. Jedes $v' \in V'$ lässt sich als $v' = \sum_{i \in I} x_i e_i$ mit $x_i \in \mathbb{R}$ schreiben. Wir setzen $y_i = |x_i|$ falls $i \in I$ und $y_i = 0$ sonst. Der Vektor $v = \sum_{i=1}^{d} y_i e_i \in V$ erfüllt

$$\beta(v, v) = \sum_{i,j=1}^{d} y_i y_j \beta(e_i, e_j) = \sum_{i,j=1}^{d} |x_i||x_j|\beta(e_i, e_j) = \sum_{i \in I} |x_i|^2 - \sum_{i,j \in I,\, i \neq j} |x_i||x_j| \cos(\pi/m_{ij}),$$

denn $\beta(e_i, e_i) = -\cos(\pi/m_{ii}) = -\cos(\pi) = 0$ nach Definition. Aus (3.3) folgt $0 \leq \cos(\pi/m'_{ij}) \leq \cos(\pi/m_{ij})$ für alle $i, j \in I$ mit $i \neq j$. Damit

$$\beta(v, v) \leq \sum_{i \in I} x_i^2 - \sum_{i,j \in I,\, i \neq j} x_i x_j \cos(\pi/m'_{ij}) = \sum_{i,j \in I} \beta'(e_i, e_j) = \beta'(v', v').$$

Da β positiv definit ist, muss $\beta'(v', v') \geq 0$ sein. Ist $\beta'(v', v') = 0$, so $\beta(v, v) = 0$, also $v = 0$ und damit $v' = 0$. □

2. Schritt. Zusammen mit Aufgabe 3.32 und Bemerkung 3.26 zeigt dies: Jeder Teilgraph von Γ darf kein erweitertes Coxeter–Dynkin-Diagramm sein. Aus dieser Eigenschaft werden wir nun folgern, dass Γ eine Vereinigung von Coxeter–Dynkin-Diagrammen sein muss. Ohne Einschränkung der Allgemeinheit können wir annehmen, dass Γ zusammenhängend ist. Insbesondere ist Γ ein *Baum*, d. h. Γ enthält keine geschlossenen Pfade, sonst wäre $\tilde{\mathbf{A}}_n$  ein Teilgraph von Γ.

Alle Graphen mit 2 Knoten sind Coxeter–Dynkin-Diagramme vom Typ $\mathbf{I}_2(m)$  .

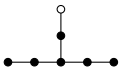
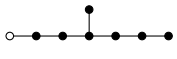
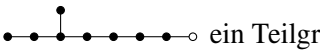
Angenommen, Γ ist ein Baum mit 3 Knoten, dann gilt bis auf Umsortieren der Indizes $m_{13} = 2$ und $m_{12}, m_{23} \geq 3$. Es können nicht beide $m_{12}, m_{23} \geq 4$, sonst wäre $\tilde{\mathbf{C}}_4$  ein Teilgraph. Wäre m_{12} oder $m_{23} \geq 6$, so wäre $\tilde{\mathbf{G}}_2$ ein Teilgraph. Also sind die einzigen Möglichkeiten:

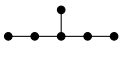
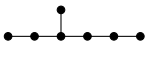
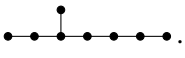
$$\Gamma = \mathbf{A}_3 \text{ } \bullet\!\!-\!\!\bullet\!\!-\!\!\bullet, \quad \Gamma = \mathbf{B}_3 \text{ } \bullet\!\!-\!\!\overset{4}{\bullet}\!\!\bullet \quad \text{oder} \quad \Gamma = \mathbf{H}_3 \text{ } \bullet\!\!\overset{5}{-}\!\!\bullet\!\!-\!\!\bullet.$$

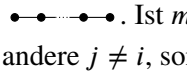
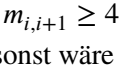
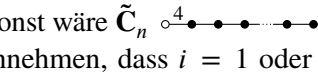
Schließlich nehmen wir an, Γ hat $d \geq 4$ Knoten. Ein *Verzweigungspunkt* ist ein Knoten, von dem mindestens 3 Kanten abgehen. Wir unterscheiden zwei Fälle, je nachdem ob Γ einen Verzweigungspunt hat oder nicht.

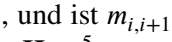
Hat Γ einen Verzweigungspunkt $i \in \{1, \ldots, d\}$, dann gibt es genau 3 Kanten, die von i abgehen, sonst wäre $\tilde{\mathbf{D}}_3$  ein Teilgraph. Übrigens darf keine Kante mit $m \geq 4$ indiziert sein, sonst wäre

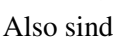
$\tilde{\mathbf{B}}_n$  ein Teilgraph, und es darf keine anderen Verzweigungspunkte außer i geben, sonst wäre $\tilde{\mathbf{D}}_n$  (mit $n \geq 4$) ein Teilgraph. Also gehen von i genau 3 Äste ab mit jeweils p, q, r Kanten.

Wären alle $p, q, r \geq 2$, so wäre $\tilde{\mathbf{E}}_6$  ein Teilgraph. Also können wir annehmen, dass $p = 1$. Wären dann beide $q, r \geq 3$, so wäre $\tilde{\mathbf{E}}_7$  ein Teilgraph. Also können wir annehmen, dass $q = 1$, in welchem Fall wir einen Graphen vom Typ $\mathbf{D}_n$  erhalten, oder $q = 2$. Dann muss $r \leq 4$ sein, sonst wäre $\tilde{\mathbf{E}}_8$  ein Teilgraph. Also sind die einzigen Möglichkeiten:

$\Gamma = \mathbf{E}_6$  , $\Gamma = \mathbf{E}_7$  oder $\Gamma = \mathbf{E}_8$  .

Hat Γ keinen Verzweigungspunkt, dann gilt bis auf Umsortieren der Indizes $m_{ij} = 2$ für alle i, j mit $|i - j| \geq 2$ und $m_{i,i+1} \geq 3$ für alle $1 \leq i \leq d - 1$. Sind alle $m_{i,i+1} = 3$, dann erhalten wir $\Gamma = \mathbf{A}_n$  . Ist $m_{i,i+1} \geq 4$ für ein i, so ist $m_{i,i+1} \leq 5$ wegen $\tilde{\mathbf{G}}_2$  und es gilt $m_{j,j+1} = 3$ für alle andere $j \neq i$, sonst wäre $\tilde{\mathbf{C}}_n$  ein Teilgraph.

Lass uns zuerst annehmen, dass $i = 1$ oder $i = d - 1$. Ist $m_{i,i+1} = 4$, so sind wir im Fall $\Gamma = \mathbf{B}_n$  , und ist $m_{i,i+1} = 5$, so $d \leq 4$ wegen $\tilde{\mathbf{H}}_4$  , also sind wir im Fall $\Gamma = \mathbf{H}_3$  oder $\Gamma = \mathbf{H}_4$.

Schließlich nehmen wir an, dass $1 < i < d - 1$. Dann $m_{i,i+1} = 4$ wegen $\tilde{\mathbf{H}}_3$  und $d = 4$ wegen $\tilde{\mathbf{F}}_4$. Also sind wir im Fall $\Gamma = \mathbf{F}_4$. □

Bemerkung 3.29. Es sei Γ ein Coxeter–Diagramm. Bilde die zugehörige Coxeter-Matrix M, die Abbildungen ρ_i (Bezeichnung 3.21), und die Gruppe

$$G = \langle \rho_i \mid 1 \leq i \leq d \rangle \leq \mathrm{GL}(V).$$

Man kann zeigen, dass G stets eine endliche Gruppe. Daraufhin kann man sich fragen, was genau die Ordnungen $|G|$ sind und welche Gruppen man auf diese Weise erhält. Dazu siehe das Buch von Benson und Grove [4]. Die Antwort ist in folgender Tabelle zusammengefasst.

Γ	$\lvert G\rvert$
$\mathbf{A}_n$	$(n+1)!$
$\mathbf{B}_n$	$2^n n!$
$\mathbf{D}_n$	$2^{n-1} n!$
$\mathbf{I}_2(m)$	$2m$

Γ	$\lvert G\rvert$
$\mathbf{E}_6$	51840
$\mathbf{E}_7$	2903040
$\mathbf{E}_8$	696729600

Γ	$\lvert G\rvert$
$\mathbf{F}_4$	1152
$\mathbf{H}_3$	120
$\mathbf{H}_4$	14400

Um die exzeptionellen Fälle $\mathbf{E}_6, \mathbf{E}_7, \mathbf{E}_8, \mathbf{F}_4, \mathbf{H}_3, \mathbf{H}_4$ zu behandeln, benutzt man sinnvollerweise ein Computeralgebrasystem. Man kann folgendermaßen vorgehen:

(i) Gegeben der Graph Γ, bilde die Matrix $M = (m_{ij}) \in \mathrm{M}_d(\mathbb{Z})$.
(ii) Betrachte $V = \mathbb{R}^d$ und stelle die Matrizen A_i von ρ_i bezüglich der Standardbasis von $\mathbb{R}^d$ auf.
(iii) Erhalte damit eine explizite Matrizengruppe $G = \langle A_i \mid 1 \le i \le d \rangle \subseteq \mathrm{GL}(V)$.
(iv) Wandle G in eine Permutationsgruppe um. Dazu sei

$$X = \{ g(e_i) \mid g \in G,\ 1 \le i \le d \} \subseteq V$$

die Vereinigung der Bahnen der Standardbasisvektoren unter G. Dann operiert G auf X und da X eine Basis von V enthält, ist diese Operation treu. Wir erhalten damit $G \hookrightarrow \mathrm{S}_X$.
(v) Bestimme dann explizit die durch jede Matrix A_i induzierte Permutation σ_i von X.
(vi) Bestimme die Ordnung $|G| = |\langle \sigma_1, \dots, \sigma_d \rangle|$ mit dem Schreier–Sims-Algorithms (Kapitel 2).

Führt man die Rechnung explizit aus, so findet man $|X| = 72, 126, 240, 48, 30$ oder 120, falls $G = \mathbf{E}_6, \mathbf{E}_7, \mathbf{E}_8, \mathbf{F}_4, \mathbf{H}_3$ bzw. $\mathbf{H}_4$. Insbesondere $|X| < \infty$, was a priori nicht klar war, und damit $|G| < \infty$.

Diese Rechnungen wurden im Rahmen vom CHEVIE-Projekt („Chevalley+Lie“, siehe http://www.math.rwth-aachen.de/homes/CHEVIE/) durchgeführt.

3.5 Aufgaben

Aufgabe 3.30. 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 3.31. 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.

Aufgabe 3.32. Es seien $M \in \mathrm{M}_d(\mathbb{Z})$ ein Coxeter-Matrix, $\Gamma = \Gamma(M)$ der zugehörige Graph und $\beta = \beta(M)$ die zugehörige Bilinearform mit Gram-Matrix $B = B(M) = (-\cos(\pi/m_{ij}))$.

(a) Es sei nun $d \ge 3$. Es gelte $m_{12} \ge 3$ und $m_{13} = m_{14} = \dots = m_{1d} = 2$. Es seien $M_1 = (m_{ij})_{2 \le i,j \le d}$ und $M_2 = (m_{ij})_{3 \le i,j \le d}$. Zeige:

$$\det(B(M)) = \det(B(M_1)) - \cos^2(\pi/m_{12}) \det(B(M_2)).$$

(b) Zeige: Ist Γ ein Coxeter–Dynkin-Diagramm, so ist $\det(B) > 0$. (Benutze die obige Gleichung, um Rekursionsformeln fur $\det(B(M))$ aufzustellen.) Verifiziere folgende Tabelle:

$\Gamma(M)$	$\mathbf{A}_n$	$\mathbf{B}_n$	$\mathbf{D}_n$	$\mathbf{I}_2(m)$	$\mathbf{E}_6$	$\mathbf{E}_7$	$\mathbf{E}_8$	$\mathbf{H}_3$	$\mathbf{H}_4$	$\mathbf{F}_4$
$\det(2B(M))$	$n+1$	2	4	$4\sin^2(\pi/m)$	3	2	1	$3-\sqrt{5}$	$(7-3\sqrt{5})/2$	1

(c) Zeige: Ist Γ ein erweitertes Coxeter–Dynkin-Diagramm, so ist $\det(B) \le 0$. (Verfahre analog.)

Bis hier Woche 6/7

Kapitel 4

Darstellungstheorie endlicher Gruppen

4.1 Definitionen und Beispiele

Definition 4.1. Es seien G eine Gruppe, K ein Körper, $n \in \mathbb{N}$. Eine *Matrixdarstellung* (oder einfach *Darstellung*) von G über K ist ein Gruppenhomomorphismus $\rho : G \to \mathrm{GL}_n(K)$. Wir nennen n den *Grad* von ρ. Der *Charakter* einer Darstellung $\rho : G \to \mathrm{GL}_n(K)$ ist die Funktion

$$\chi_\rho : G \to K, \quad g \mapsto \mathrm{Spur}(\rho(g)).$$

Eine Funktion $\chi : G \to K$ heißt *Charakter*, falls es eine Darstellung $\rho : G \to \mathrm{GL}_n(K)$ gibt mit $\chi = \chi_\rho$.

Beispiel 4.2. Wir bezeichnen $K \setminus \{0\}$ mit $K^\times$. Jeder Homomorphismus $\lambda : G \to K^\times$ ist der Charakter der Darstellung $\rho_\lambda : G \to \mathrm{GL}_1(K)$ vom Grad 1 gegeben durch $g \mapsto (\lambda(g))$. Ist λ der triviale Homomorphismus $g \mapsto 1$, so heißen ρ_λ und λ *triviale Darstellung* bzw. *trivialer Charakter*.

Bemerkung 4.3. Für jeden Charakter $\chi : G \to K$ gilt $\chi(1) = n \in \mathbb{N}$, wobei $\rho : G \to \mathrm{GL}_n(K)$ eine Darstellung mit $\chi = \chi_\rho$ ist.

Definition 4.4. 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 $p_{ij} = 0$. Damit erhalten wir folgende Darstellung:

$$\pi_n : \mathrm{S}_n \to \mathrm{GL}_n(K), \quad \sigma \mapsto P_\sigma. \tag{4.1}$$

Beispiel 4.5. Es sei X eine endliche G-Menge mit n Elementen. Der Einfachheit halber können wir annehmen, dass $X = \{1, \dots, n\}$. Betrachte $V = K^n$ mit Standardbasis $\{e_1, \dots, e_n\}$. Die *zu X assoziierte Permutationsdarstellung* ist folgendermaßen definiert:

$$\pi_X^G : G \to \mathrm{GL}_n(K), \quad g \mapsto (e_i \mapsto e_{g \cdot i}).$$

Bemerke, dass $\pi_X^G(g)$ eine Permutationsmatrix für jede $g \in G$ ist. Der Charakter von π_X^G ist

$$\chi_X^G : G \to K, \quad g \mapsto |\{ x \in X \mid g \cdot x = x \}|.$$

Beispiel 4.6. Betrachte $X = G$ als G-Menge durch Linksmultiplikation (Beispiel 1.36). Dann ist die assoziierte Permutationsdarstellung injektiv und gleich die Hintereinanderausführung

$$G \hookrightarrow \mathrm{S}_G = \mathrm{S}_n \to \mathrm{GL}_n(K),$$

wobei $G \hookrightarrow \mathrm{S}_n$ und $\mathrm{S}_n \to \mathrm{GL}_n(K)$ die Inklusion als Untergruppe gegeben vom Satz von Cayley bzw. die Abbildung in (4.1) sind. Der Charakter $\chi_{\mathrm{reg}}^G : G \to K$ dieser Darstellung heißt *regulärer Charakter*. Es gilt

$$\chi_{\mathrm{reg}}^G(g) = \begin{cases} |G| & \text{falls } g = 1, \\ 0 & \text{sonst.} \end{cases}$$

Bezeichnung 4.7. Eine Funktion $f : G \to K$, die konstant auf Konjugationsklassen von G ist, heißt *Klassenfunktion* auf G. Wir bezeichnen mit $\mathrm{CF}_K(G)$ den Vektorraum der Klassenfunktionen auf G. Es seien $C_1, \dots, C_r$ die Konjugationsklassen von G. Dann ist die Dimension von $\mathrm{CF}_K(G)$ gleich r, denn die Funktionen $f_i : G \to K$, $i = 1, \dots, r$ definiert durch

$$f_i(g) = \begin{cases} 1 & \text{falls } g \in C_i, \\ 0 & \text{sonst,} \end{cases}$$

offensichtlich eine Basis von $\mathrm{CF}_K(G)$ bilden.

Bemerkung 4.8. Es seien $g_1, g_2 \in G$ zwei Elemente in derselben Konjugationsklasse, d. h. es gibt $h \in G$ mit $g_1 = hg_2h^{-1}$. Für jede Darstellung $\rho : G \to \mathrm{GL}_n(K)$ gilt (wegen $\mathrm{Spur}(A \cdot B) = \mathrm{Spur}(B \cdot A)$ für alle $A, B \in M_n(K)$, siehe LAAG):

$$\chi_\rho(g_1) = \mathrm{Spur}(\rho(g_1)) = \mathrm{Spur}(\rho(h)\rho(g_2)\rho(h^{-1})) = \mathrm{Spur}(\rho(h)\rho(g_2)\rho(h)^{-1}) = \mathrm{Spur}(\rho(g_2)) = \chi_\rho(g_2).$$

Damit haben wir gezeigt: Jeder Charakter $\chi : G \to K$ ist eine Klassenfunktion auf G.

Definition 4.9. Zwei Darstellungen $\rho : G \to \mathrm{GL}_n(K)$ und $\sigma : G \to \mathrm{GL}_m(K)$ heißen *äquivalent*, wenn es $n = m$ gilt und eine Matrix $T \in \mathrm{GL}_n(K)$ gibt mit

$$\sigma(g) = T\rho(g)T^{-1}, \quad \text{für alle } g \in G.$$

Bemerkung 4.10. Sind ρ und σ äquivalente Darstellungen, so gilt $\chi_\rho = \chi_\sigma$ (gleiches Argument wie oben).

Definition 4.11. Ein K-Vektorraum V mit $\dim(V) < \infty$ heißt *G-Modul*, falls es eine Operation von G auf V gibt, sodass für jedes feste $g \in G$ die Funktion

$$\varphi_g : V \to V, \quad v \mapsto g \cdot v$$

linear ist.

Bemerkung 4.12. Ist $\rho\colon G \to \mathrm{GL}_n(K)$, so ist $V = K^n$ ein G-Modul, wobei $g \cdot v = \rho(g)v$.

Umgekehrt seien V ein G-Modul und $\{v_1, \dots, v_n\}$ eine Basis von V. Dann erhalten wir eine Darstellung $\rho\colon G \to \mathrm{GL}_n(K)$, indem wir $\rho(g)$ gleich der Matrix von φ_g bezüglich $\{v_1, \dots, v_n\}$ setzen. Wählen wir eine andere Basis $\{v_1', \dots, v_n'\}$ von V, so erhalten wir eine Darstellung ρ', die äquivalent zu ρ ist.

Bis hier Woche 8

4.2 Lemma von Schur

Definition 4.13. Ein Teilraum $U \subset V$ eines G-Moduls V heißt *G-Untermodul*, falls $g \cdot u \in U$ für alle $g \in G$ und $u \in U$.

Offensichtlich sind $\{0\}$ und V immer G-Untermoduln von V.

Definition 4.14. Ein G-Modul V heißt *irreduzibel*, wenn $\{0\}$ und V die einzigen G-Untermoduln von V sind. Eine Darstellung $\rho\colon G \to \mathrm{GL}_n(K)$ heißt *irreduzibel*, falls der zugehörige G-Modul $V = K^n$ irreduzibel ist. Ein Charakter $\chi\colon G \to K$ heißt *irreduzibel*, wenn es eine irreduzible Darstellung $\rho\colon G \to \mathrm{GL}_n(K)$ gibt mit $\chi = \chi_\rho$.

Satz 4.15. *Jede Darstellung $\rho\colon G \to \mathrm{GL}_n(K)$ ist äquivalent zu einer Darstellung $\sigma\colon G \to \mathrm{GL}_n(K)$ mit folgender Gestalt:*

$$\sigma(g) = \begin{pmatrix} \sigma_1(g) & * & \dots & * \\ & \sigma_2(g) & * & * \\ & & \ddots & \vdots \\ 0 & & & \sigma_m(g) \end{pmatrix} \quad \textit{für alle } g \in G,$$

wobei $\sigma_i\colon G \to \mathrm{GL}_{n_i}(K)$ jeweils irreduzible Darstellungen sind und obige Matrix als Blockmatrix zu verstehen ist. Folglich ist dann auch $\chi_\rho = \chi_{\sigma_1} + \dots + \chi_{\sigma_m}$, d. h., jeder Charakter von G lässt sich als Summe von irreduziblen Charakteren darstellen.

Beweis per Induktion auf n. Ist $n = 1$, so gibt es nichts zu zeigen. Es sei also $n > 1$.

Ist σ irreduzibel, gibt es wieder nichts zu zeigen. Dann können wir annehmen, dass es ein G-Untermodul $U \subseteq V$ von $V = K^n$ gibt mit $U \neq \{0\}$ und $U \neq V$. Nach dem Basisergänzungssatz der Linearen Algebra gibt es eine Basis $\{e_1, \dots, e_n\}$ von V, sodass $\{e_1, \dots, e_d\}$ eine Basis von U ist, wobei $d = \dim(U)$. Es sei ρ' die zu V gehörige Darstellung bezüglich $\{e_1, \dots, e_n\}$. Da $g \cdot u \in U$ für alle $u \in U$, hat jeder Matrix $\rho'(g)$ folgende Gestalt:

$$\rho'(g) = \left(\begin{array}{c|c} \rho_1'(g) & * \\ \hline 0 & \rho_2'(g) \end{array}\right),$$

wobei $\rho'_1 : G \to \mathrm{GL}_d(K)$ die zu U gehörige Darstellung bezüglich $\{e_1, \dots, e_d\}$. Außerdem gilt $\rho'_2(g) \in \mathrm{GL}_{n-d}(K)$ für alle g. Aus $\rho'(gh) = \rho'(g)\rho'(h)$ folgt $\rho'_2(gh) = \rho'_2(g)\rho'_2(h)$ für alle $g, h \in G$, d. h. $\rho'_2 : G \to \mathrm{GL}_{n-d}(K)$ ist auch eine Darstellung.

Nach Induktion gibt es Matrizen $T_1 \in \mathrm{GL}_d(K)$ und $T_2 \in \mathrm{GL}_{n-d}(K)$, sodass jeweils $T_1\rho'_1(g)T_1^{-1}$ und $T_2\rho'_2(g)T_2$ für alle $g \in G$ die gewünschte Blockdreiecksgestalt besitzen. Setzen wir

$$T = \left(\begin{array}{c|c} T_1 & 0 \\ \hline 0 & T_2 \end{array}\right) \quad \text{und} \quad \sigma(g) = T\rho'(g)T^{-1} \quad \text{für alle } g \in G,$$

so haben die Matrizen $\sigma(g)$ die gewünschte Form. □

Lemma 4.16 (Lemma von Schur)**.** *Es seien $\rho : G \to \mathrm{GL}_n(K)$ und $\sigma : G \to \mathrm{GL}_m(K)$ zwei irreduzible Darstellungen. Es sei A eine $m \times n$-Matrix mit*

$$A\rho(g) = \sigma(g)A \quad \textit{für alle } g \in G.$$

Dann ist entweder A die Null-Matrix oder es gilt $n = m$ und A ist invertierbar (insbesondere sind ρ und σ äquivalent).

Beweis. Nehmen wir an, dass $A \neq 0$ und lass uns Kern und Bild von A betrachten, d. h.

$$U = \mathrm{Ker}(A) = \{\, v \in K^n \mid Av = 0 \,\}, \quad W = \mathrm{Bild}(A) = \{\, w \in K^m \mid w = Av \text{ für ein } v \in V \,\}.$$

Wegen $A \neq 0$ gilt $U \neq K^n$ und $W \neq \{0\}$. Übrigens sind beide U und W G-Untermoduln von K^n bzw. K^m, denn es gilt

$$A(\rho(g)v) = (A\rho(g))v = (\sigma(g)A)v = \sigma(g)(Av)$$

für alle $g \in G$ und $v \in K^n$. Nach Voraussetzung sind die G-Moduln K^n und K^m irreduzibel, also muss $U = \{0\}$ und $W = K^m$ sein, d. h. $n = m$ und A ist invertierbar. □

Satz 4.17. *Angenommen, dass K algebraisch abgeschlossen ist, sei $\rho : G \to \mathrm{GL}_n(K)$ eine irreduzible Darstellung. Ist $A \in \mathrm{M}_n(K)$ mit $A\rho(g) = \rho(g)A$ für alle $g \in G$, so gilt $A = \lambda\mathbf{1}_n$ mit $\lambda \in K$.*

Beweis. Da K algebraisch abgeschlossen ist, hat das charakteristische Polynom von A eine Lösung in K, d. h. es existiert ein Eigenwert $\lambda \in K$ von A. Die Matrix $B = A - \lambda\mathbf{1}_n$ erfüllt auch $B\rho(g) = \rho(g)B$ für alle $g \in G$. Aus $\det(B) = 0$ folgt, dass B nicht invertierbar ist. Nach dem Lemma von Schur muss also $B = 0$ sein. □

Folgerung 4.18. *Angenommen, dass K algebraisch abgeschlossen und G endlich ist, seien $\rho : G \to \mathrm{GL}_n(K)$ eine irreduzible Darstellung und $C \subseteq G$ eine Konjugationsklasse. Dann gilt*

$$\sum_{x \in C} \rho(x) = \lambda\mathbf{1}_n,$$

mit $n\lambda = |C|\chi_\rho(g)$, wobei $g \in C$.

Beweis. Es sei $A = \sum_{x\in C} \rho(x)$. Dann gilt

$$A\rho(g) = \sum_{x\in C} \rho(x)\rho(g) = \sum_{x\in C} \rho(xg) = \sum_{y\in C} \rho(gy) = \rho(g) \sum_{y\in C} \rho(y) = \rho(g)A,$$

für jedes $g \in G$, denn läuft x über alle Elemente von C, so läuft auch $y = g^{-1}xg$ über alle Elemente von C. Aus Satz 4.17 folgt $A = \lambda \mathbf{1}_n$ mit $\lambda \in K$.

Es sei nun $g \in C$ fest. Dann gilt $\mathrm{Spur}(\rho(x)) = \chi_\rho(x) = \chi_\rho(g)$ für alle $x \in C$ (Bemerkung 4.8) und damit erhalten wir

$$n\lambda = \mathrm{Spur}(\lambda \mathbf{1}_n) = \mathrm{Spur}(\sum_{x\in C} \rho(x)) = \sum_{x\in C} \mathrm{Spur}(\rho(x)) = |C|\chi_\rho(g). \qquad \square$$

Folgerung 4.19. *Ist K algebraisch abgeschlossen und G abelsch ist, so hat jede irreduzible Darstellung $\rho : G \to \mathrm{GL}_n(K)$ Grad 1, d. h. $n = 1$.*

Beweis. Es sei $g \in G$ fest. Da G abelsch ist, gilt $\rho(x)\rho(g) = \rho(xg) = \rho(gx) = \rho(g)\rho(x)$ für jedes $x \in G$, also $\rho(g) = \lambda_g \mathbf{1}_n$ mit $\lambda_g \in K$ nach Satz 4.17. Es sei $V = K^n$ der zugehörige G-Modul. Wähle $v \in V \setminus \{0\}$ und sei $U \subseteq V$ der von v erzeugte Teilraum. Dann ist $\rho(g)v = \lambda_g v \in U$ für jedes g, d. h. U ist ein G-Untermodul. Da V nach Voraussetzung irreduzibel ist, muss $U = V$ sein, also $n = \dim(V) = 1$. $\square$

Satz 4.20 (Schur-Relationen)**.** *Es seien G eine Gruppe mit $|G| < \infty$ und $\rho : G \to \mathrm{GL}_n(K), \sigma : G \to \mathrm{GL}_m(K)$ zwei irreduzible Darstellungen. Sind ρ und σ nicht äquivalent, so gilt*

$$\sum_{g\in G} \rho(g)_{ij}\sigma(g^{-1})_{kl} = 0$$

für alle $1 \le i, j \le n$ und $1 \le k, l \le m$.

Ist übrigens K algebraisch abgeschlossen und entweder $\mathrm{Char}(K) = 0$ oder $\mathrm{Char}(K) = p > 0$ und $p \nmid |G|$, so gilt $\mathrm{Char}(K) \nmid n$ und

$$\sum_{g\in G} \rho(g)_{ij}\rho(g^{-1})_{kl} = \delta_{il}\delta_{jk}\frac{|G|}{n}.$$

für alle $1 \le i, j, k, l \le n$, wobei δ_{ij} das Kronecker-Delta ist (d. h., $\delta_{ij} = 1$ falls $i = j$, sonst $\delta_{ij} = 0$).

Beweis. Es sei $M = E_{li}$ die $m \times n$-Matrix mit 1 an der Stelle (l, i) und 0 überall sonst. Setze $A = \sum_{g\in G} \sigma(g^{-1})M\rho(g)$. Für jedes $g \in G$ gilt dann

$$\begin{aligned} A\rho(g) &= \sum_{h\in G} \sigma(h^{-1})M\rho(h)\rho(g) = \sum_{h\in G} \sigma(h^{-1})M\rho(hg) \\ &= \sum_{y\in G} \sigma(gy^{-1})M\rho(y) = \sigma(g) \sum_{y\in G} \sigma(y^{-1})M\rho(y) = \sigma(g)A. \end{aligned}$$

Der (k, j)-Eintrag von A ist gleich

$$(A)_{kj} = \sum_{g\in G}\sum_{r=1}^{m}\sum_{s=1}^{n}\sigma(g^{-1})_{kr}(E_{li})_{rs}\rho(g)_{sj} = \sum_{g\in G}\sigma(g^{-1})_{kl}\rho(g)_{ij}. \tag{4.2}$$

Sind ρ und σ nicht äquivalent, so ist $A = 0$ nach dem Lemma von Schur (Lemma 4.16) und damit auch $(A)_{kj} = 0$. Aus (4.2) folgt also die erste Formel.

Nehmen wir nun an, dass K algebraisch abgeschlossen ist und entweder $\mathrm{Char}(K) = 0$ oder $\mathrm{Char}(K) = p > 0$ und $p \nmid |G|$. Übrigens sei $n = m$ und $\sigma = \rho$. Nach Satz 4.17 ist $A = \lambda \mathbf{1}_n$ für ein $\lambda \in K$. Mit der Regel $\mathrm{Spur}(AB) = \mathrm{Spur}(BA)$ (für $A, B \in M_n(K)$) folgt

$$n\lambda = \mathrm{Spur}(A) = \mathrm{Spur}\Big(\sum_{g\in G}\sigma(g^{-1})M\rho(g)\Big) = \sum_{g\in G}\mathrm{Spur}\left(\sigma(g^{-1})M\rho(g)\right) = \sum_{g\in G}\mathrm{Spur}(M) = |G|\delta_{li}.$$

Der Fall $l = i$ zeigt, dass $n \neq 0$ in K, d. h. $\mathrm{Char}(K) \nmid n$. Also gilt $\lambda = \delta_{il}|G|/n$. Aus (4.2) folgt nun

$$\sum_{g\in G}\rho(g)_{ij}\rho(g^{-1})_{kl} = (A)_{kj} = \lambda\delta_{kj} = \delta_{il}\delta_{jk}|G|/n. \qquad \square$$

4.3 Irreduzible Charaktere über $\mathbb{C}$

Lemma 4.21. *Es seien G eine endliche Gruppe und $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ eine Darstellung. Dann gilt*

$$\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)} \quad \textit{für alle } g \in G.$$

Beweis. Es sei $g \in G$ fest. Da die zyklische Untergruppe $H = \langle g\rangle$ abelsch ist, ist die Einschränkung von ρ auf $H = \langle g\rangle$ nach Satz 4.15 und Folgerung 4.19 äquivalent zu einer Darstellung $\sigma : H \to \mathrm{GL}_n(K)$ mit

$$\sigma(h) = \begin{pmatrix} \lambda_1(h) & * & \dots & * \\ & \lambda_2(h) & * & * \\ & & \ddots & \vdots \\ 0 & & & \lambda_n(h) \end{pmatrix} \quad \text{für alle } h \in H,$$

wobei $\lambda_i : H \to K^\times$ Homomorphismen sind (siehe Beispiel 4.2). Es sei $d = \mathrm{Ord}(g)$. Dann gilt $h^d = 1$ für alle $h \in H$ und damit $\lambda_i^d(h) = 1$ für alle $h \in H$. Insbesondere gilt $\lambda_i^d(g) = 1$, d. h., $\lambda_i(g)$ ist eine Einheitswurzel, und

$$\chi_\rho(g^{-1}) = \chi_\sigma(g^{-1}) = \lambda_1(g^{-1}) + \dots + \lambda_n(g^{-1}) = \lambda_1(g)^{-1} + \dots + \lambda_n(g)^{-1}.$$

Für jede Einheitswurzel $\zeta \in \mathbb{C}$ gilt $\overline{\zeta} = \zeta^{-1}$. Damit erhalten wir die gewünschte Formel. $\square$

Satz 4.22 (Orthogonalitätsrelationen)**.** *Es seien G eine endliche Gruppe und χ_ρ, χ_σ die Charaktere zweier irreduziblen Darstellungen $\rho\colon G \to \mathrm{GL}_n(\mathbb{C})$, $\sigma\colon G \to \mathrm{GL}_m(\mathbb{C})$. Dann gilt*

$$\sum_{g\in G} \chi_\rho(g)\overline{\chi_\sigma(g)} = \begin{cases} |G| & \text{falls } \chi_\rho = \chi_\sigma, \\ 0 & \text{sonst.} \end{cases}$$

Insbesondere sind zwei irreduzible Darstellungen ρ, σ genau dann äquivalent, wenn $\chi_\rho = \chi_\sigma$ gilt.

Beweis. Es gilt $\chi_\rho(g) = \sum_{i=1}^n \rho(g)_{ii}$ und nach Lemma 4.21 $\overline{\chi_\sigma(g)} = \chi_\sigma(g^{-1}) = \sum_{k=1}^m \sigma(g^{-1})_{kk}$, also

$$\sum_{g\in G} \chi_\rho(g)\overline{\chi_\sigma(g)} = \sum_{i=1}^n \sum_{k=1}^m \sum_{g\in G} \rho(g)_{ii}\sigma(g^{-1})_{kk}. \tag{4.3}$$

Ist $\chi_\rho \neq \chi_\sigma$, dann sind ρ und σ nicht äquivalent nach Bemerkung 4.10. Daher ist $\rho(g)_{ii}\sigma(g^{-1})_{kk} = 0$ für alle $1 \leq i \leq n$ und $1 \leq k \leq m$ wegen der Schur-Relationen (Satz 4.20) und damit erhalten wir die Formel.

Ist $\chi_\rho = \chi_\sigma$, so erhalten wir aus den Schur-Relationen

$$\sum_{g\in G} \chi_\rho(g)\overline{\chi_\rho(g)} = \sum_{i=1}^n \sum_{k=1}^n \sum_{g\in G} \rho(g)_{ii}\rho(g^{-1})_{kk} = \sum_{i=1}^n \sum_{k=1}^n \delta_{ik}\delta_{ik}\frac{|G|}{n} = |G|.$$

Daher folgt die Formel. Insbesondere ist die Summe in (4.3) ungleich 0, also gibt es i, k mit $\sum_{g\in G} \rho(g)_{ii}\sigma(g^{-1})_{kk} \neq 0$. Nach Satz 4.20 sind dann ρ und σ äquivalent. □

Definition 4.23. Gegeben zwei Klassenfunktionen $f_1, f_2 \in \mathrm{CF}_{\mathbb{C}}(G)$ definieren wir

$$\langle f_1, f_2\rangle = \frac{1}{|G|}\sum_{g\in G} f_1(g)\overline{f_2(g)}.$$

Damit erhalten wir ein positiv-definites hermitesches Skalarprodukt $\langle\ ,\ \rangle\colon \mathrm{CF}_{\mathbb{C}}(G) \times \mathrm{CF}_{\mathbb{C}}(G) \to \mathbb{C}$, denn offensichtlich ist $\langle\ ,\ \rangle$ linear im ersten Argument, es gilt $\langle f_2, f_1\rangle = \overline{\langle f_1, f_2\rangle}$, $\langle f, f\rangle \in \mathbb{R}$ und $\langle f, f\rangle \geq 0$, mit Gleichheit nur für $f = 0$.

Bezeichnung 4.24. Wir bezeichen mit $\mathrm{Irr}(G)$ die Menge der irreduziblen Charaktere über $\mathbb{C}$ von G. Nach Bemerkung 4.8 gilt $\mathrm{Irr}(G) \subset \mathrm{CF}_{\mathbb{C}}(G)$ (Bezeichnung 4.7). Die Orthogonalitätsrelationen (Satz 4.22) lassen sich folgendermaßen schreiben:

$$\langle \chi, \chi'\rangle = \begin{cases} 1 & \text{falls } \chi = \chi', \\ 0 & \text{sonst.} \end{cases} \qquad \text{für alle } \chi, \chi' \in \mathrm{Irr}(G). \tag{4.4}$$

Insbesondere sind alle Elemente von $\mathrm{Irr}(G)$ orthogonal zueinander bezüglich dem Skalarprodukt $\langle\ ,\ \rangle$, also gilt $|\mathrm{Irr}(G)| \leq \dim \mathrm{CF}_{\mathbb{C}}(G)$. Wir werden demnächst sehen, dass eigentlich Gleichheit gilt.

Bemerkung 4.25. Es sei ψ ein beliebiger Charakter von G. Nach Satz 4.15 lässt sich ψ als Summe von irreduziblen Charaktern schreiben, also $\psi = \sum_{i=0}^{n} a_i \chi_i$ mit $a_i \in \mathbb{Z}_{\geq 0}$ und $\chi_i \in \mathrm{Irr}(G)$. Wegen (4.4) gilt

$$\langle \psi, \chi_i \rangle = \langle \sum_{j=0}^{n} a_j \chi_j, \chi_i \rangle = \sum_{j=0}^{n} a_j \langle \chi_j, \chi_i \rangle = a_i.$$

Beispiel 4.26. Es sei $\chi_{\mathrm{reg}}^G : G \to K$ der reguläre Charakter (Beispiel 4.6). Dann gilt

$$\langle \chi_{\mathrm{reg}}^G, \chi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{\mathrm{reg}}^G(g) \overline{\chi(g)} = \chi(1).$$

Insbesondere gilt

$$\chi_{\mathrm{reg}}^G = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1) \chi.$$

Folgerung 4.27. *Ein Charakter χ einer endlichen Gruppe G ist genau dann irreduzibel, wenn*

$$\langle \chi, \chi \rangle = 1.$$

Beweis. Schreibe $\chi = \sum_{i=0}^{n} a_i \chi_i$ mit $a_i \in \mathbb{Z}_{\geq 0}$ und $\chi_i \in \mathrm{Irr}(G)$. Wegen (4.4) gilt

$$\langle \chi, \chi \rangle = \sum_{i=1}^{n} a_i^2,$$

also $\langle \chi, \chi \rangle = 1$ genau dann, wenn $a_i = 1$ für ein i und $a_j = 0$ für $j \neq i$, d. h. $\chi = \chi_i \in \mathrm{Irr}(G)$. □

Bis hier Woche 9/10

Satz 4.28 (Orthogonalität der Spalten)**.** *Gegeben $g, h \in G$, sei $C \subseteq G$ die Konjugationsklasse von g und $H \leq G$ der Zentralisator von g (siehe Beispiel 1.37 für die Definition). Dann gilt*

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(g) \overline{\chi(h)} = \begin{cases} |H| & \text{falls } h \in C, \\ 0 & \text{sonst.} \end{cases}$$

Beweis. Es sei $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_r\}$. Für $1 \leq k \leq r$ setze $n_k = \chi_k(1)$ und sei $\rho_k : G \to \mathrm{GL}_{n_k}(\mathbb{C})$ eine irreduzible Darstellung mit $\chi_k = \chi_{\rho_k}$. Es sei χ_{reg}^G die reguläre Darstellung. Nach Beispiel 4.6 gilt

$$\sum_{x \in C} \chi_{\mathrm{reg}}^G(xh^{-1}) = \begin{cases} |G| & \text{falls } h \in C, \\ 0 & \text{sonst.} \end{cases}.$$

Außerdem gilt nach Beispiel 4.26 für jedes $x \in C$

$$\begin{aligned} \chi_{\mathrm{reg}}^G(xh^{-1}) &= \sum_{k=1}^{r} \chi_k(1) \chi_k(xh^{-1}) = \sum_{k=1}^{r} n_k \operatorname{Spur}\left(\rho_k(xh^{-1})\right) \\ &= \sum_{k=1}^{r} n_k \sum_{i=1}^{n_k} \left(\rho_k(x)\rho_k(h^{-1})\right)_{ii} = \sum_{k=1}^{r} \sum_{i,j=1}^{n_k} n_k \rho_k(x)_{ij} \rho_k(h^{-1})_{ji}. \end{aligned}$$

Andererseits ist nach Folgerung 4.18 $\sum_{x\in C}\rho_k(x) = \lambda_k \mathbf{1}_{n_k}$ mit $\lambda_k = |C|\chi_k(g)/n_k$. Damit können wir obige Rechnung wie folgt fortsetzen:

$$\begin{aligned}\sum_{x\in C}\chi^G_{\mathrm{reg}}(xh^{-1}) &= \sum_{k=1}^{r}\sum_{i,j=1}^{n_k} n_k\Big(\sum_{x\in C}\rho_k(x)\Big)_{ij}\rho_k(h^{-1})_{ji} = \sum_{k=1}^{r}\sum_{i,j=1}^{n_k} n_k\lambda_k\delta_{ij}\rho_k(h^{-1})_{ji}\\ &= \sum_{k=1}^{r}\sum_{i=1}^{n_k} n_k\lambda_k\rho_k(h^{-1})_{ii} = \sum_{k=1}^{r} n_k\lambda_k\chi_k(h^{-1}) = |C|\sum_{k=1}^{r}\chi_k(g)\chi_k(h^{-1}).\end{aligned}$$

Es gilt $|H| = |G|/|C|$ wegen des Bahnensatzes und $\chi_k(h^{-1}) = \overline{\chi_k(h)}$ nach Lemma 4.21. Dies ergibt also die Behauptung. □

Bemerkung 4.29. Es sei $\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_r\}$ mit $\chi_i : G \to \mathrm{GL}_{n_i}(\mathbb{C})$. Wählen wir $g = h = 1$ in Satz 4.28, so erhalten wir mit Bemerkung 4.3

$$\sum_{i=1}^{r} n_i^2 = |G|.$$

Folgerung 4.30. *Für jede endliche Gruppe G bildet $\mathrm{Irr}(G)$ eine Orthonormalbasis von $\mathrm{CF}_{\mathbb{C}}(G)$ bezüglich $\langle\ ,\ \rangle$. Insbesondere ist $|\mathrm{Irr}(G)|$ gleich der Anzahl der Konjugationsklassen von G und für jedes $F \in \mathrm{CF}_{\mathbb{C}}(G)$ gilt*

$$f = \sum_{\chi\in\mathrm{Irr}(G)}\langle f, \chi\rangle\chi.$$

Beweis. Es seien $C_1, \dots, C_s$ die Konjugationsklassen von G und $\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_r\}$. Wähle ein festes Repräsentantensystem $g_1, \dots, g_s$ mit $g_i \in C_i$. Für $1 \le i \le s$ sei $f_i : G \to \mathbb{C}$ definiert durch $f_i(g) = 1$ falls $g \in C_i$, sonst $f_i(g) = 0$. Offensichtlich ist $\{f_1, \dots, f_s\}$ eine Basis von $\mathrm{CF}_{\mathbb{C}}(G)$. Nun lässt sich Satz 4.28 (mit $h = g_i$) folgendermaßen umschreiben:

$$|H_i|f_i = \sum_{j=1}^{r}\overline{\chi_j(g_i)}\chi_j,$$

wobei H_i der Zentralisator von g_i ist. D. h., $\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_r\}$ ist auch ein Erzeugendensystem für $\mathrm{CF}_{\mathbb{C}}(G)$. Zusammen mit Bezeichnung 4.24 bedeutet das $r = |\mathrm{Irr}(G)| = \dim \mathrm{CF}_{\mathbb{C}}(G) = s$. □

Definition 4.31. Es sei G eine endliche Gruppe mit Konjugationsklassen $C_1, \dots, C_r$ und $\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_r\}$. Es sei $g_1, \dots, g_r$ ein Repräsentantensystem mit $g_i \in C_i$ für jedes i. Die *Charaktertafel* von G ist die quadratische Matrix

$$X(G) = (\chi_i(g_j)) \in \mathrm{M}_r(\mathbb{C}).$$

Da $\mathrm{Irr}(G)$ eine Basis von $\mathrm{CF}_{\mathbb{C}}(G)$ ist, gilt $\det(X(G)) \neq 0$.

Bemerkung 4.32. Obwohl viele Eigenschaften einer Gruppe G aus ihrer Charatertafel abgelesen werden können, lässt sich eine Gruppe im Allgemeinen nicht von ihrer Charaktertafel rekonstruieren. Zum Beispiel sind die Charaktertafeln der Diedergruppe mit 8 Elementen D_8 und der Quaternionengruppe Q_8 gleich (siehe Übungen).

Beispiel 4.33 (Zyklische Gruppen)**.** Es sei $G = \langle g \rangle$ eine zyklische Gruppe der Ordnung $d = \mathrm{Ord}(g) < \infty$. Es sei $\chi : G \to K$ ein irreduzibler Charakter und $\rho : G \to \mathrm{GL}_n(K)$ eine Darstellung mit $\chi = \chi_\rho$. Da G abelsch ist, gilt $n = 1$ nach Folgerung 4.19, also ist $\chi(g) = \lambda(g)$ für jedes $g \in G$, wobei $\lambda : G \to K^\times$ ein Homomorphismus ist. Aus $g^d = 1$ folgt $\lambda(g)^d = \lambda(g^d) = \lambda(1) = 1$, d. h. $\zeta = \chi(g)$ ist eine d-Einheitswurzel.

Ist nun ζ_d eine primitive d-Einheitswurzel, so erhalten wir d irreduzible Charaktere $\chi_0, \dots, \chi_{d-1}$ definiert durch

$$\chi_i : G \to K, \quad g^j \mapsto \zeta_d^{ij}.$$

Jedes Element liegt in einer Konjugationsklassen für sich. Mit Folgerung 4.30 bedeutet das, dass es genau d irreduzible Charaktere gibt, d. h. $\mathrm{Irr}(G) = \{\chi_0, \dots, \chi_{d-1}\}$.

Als Beispiel erstellen wir die Charaktertafeln für $d = 2, 3, 4$.

Z_2	1	g
χ_0	1	1
χ_1	1	-1

Z_3	1	g	g^2
χ_0	1	1	1
χ_1	1	ζ_3	ζ_3^2
χ_2	1	ζ_3^2	ζ_3

Z_4	1	g	g^2	g^3
χ_0	1	1	1	1
χ_1	1	i	-1	$-i$
χ_2	1	-1	1	-1
χ_3	1	$-i$	-1	i

Beispiel 4.34 (Charaktertafel von S_3)**.** Es sei $G = S_3$. Nach Aufgabe 1.49 gibt es drei Konjugationsklassen in S_3 mit Repräsentanten id, (1 2) und (1 2 3). Also gibt es drei irreduzible Charaktere: $\mathrm{Irr}(S_3) = \{\chi_1, \chi_2, \chi_3\}$. Wir kennen schon zwei, nämlich den trivialen Charakter $\chi_1 \equiv 1$ und den Signum $\chi_2 = \mathrm{sgn}$. Um den dritten Charakter zu bestimmen, benutzen wir Satz 4.28 mit $g = h = \mathrm{id}$. Das ergibt

$$\chi_1(g)\overline{\chi_1(h)} + \chi_2(g)\overline{\chi_2(h)} + \chi_3(g)\overline{\chi_3(h)} = 1 + 1 + |\chi_3(\mathrm{id})|^2 = 6.$$

Da $\chi_3(\mathrm{id}) \in \mathbb{N}$ (Bemerkung 4.3), muss $\chi_3(\mathrm{id}) = 2$ sein.

Alle $g \in S_3 \setminus \{\mathrm{id}\}$ sind nicht zu id konjugiert, also folgt aus Satz 4.28 mit $h = \mathrm{id}$

$$\chi_1(g) + \chi_2(g) + 2\chi_3(g) = 0.$$

Damit erhalten wir $\chi_3((1\ 2)) = 0$ und $\chi_3((1\ 2\ 3)) = -1$. Die Charaktertafel von S_3 ist also folgendermaßen gegeben:

S_3	id	(1 2)	(1 2 3)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Bis hier Woche 11

Bezeichnung 4.35. Es seien G eine endliche Gruppe und $C, C' \subseteq G$ zwei Konjugationsklassen. Für $g \in G$ definieren wir

$$\alpha_{C,C'}(g) := |\{ (x, y) \in C \times C' \mid xy = g \}|.$$

Bezeichnung 4.36. Es sei G eine endliche Gruppe mit $\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_r\}$. Es seien $C_1, \dots, C_r$ die Konjugationsklassen von G mit Repräsentanten $g_1 \in C_1, \dots, g_r \in C_r$. Für $1 \leq i \leq r$ definieren wir die Matrizen

$$Z_i := (\alpha_{C_i,C_j}(g_l))_{1 \leq j,l \leq r} \in \mathrm{M}_r(\mathbb{N}).$$

Daraufhin setzen wir $\omega_k(C_l) := |C_l|\chi_k(g_l)/\chi_k(1)$ und $v_k := (\omega_k(C_1), \dots, \omega_k(C_r))^{\mathrm{t}} \in \mathbb{C}^r$ für $1 \leq k, l \leq r$.

Lemma 4.37. *(a) Jeder Vektor v_k ist ein Eigenvektor von Z_i zum Eigenwert $\omega_k(C_i)$.*
(b) Die Vektoren $\{v_1, \dots, v_r\}$ bilden eine Basis von $\mathbb{C}^r$.
(c) Ist $v \in \mathbb{C}^r$ ein gemeinsamer Eigenvektor von $Z_1, \dots, Z_r$, so gibt es ein $k \in \{1, \dots, r\}$ und ein $c \in \mathbb{C}$ mit $v = cv_k$.

Beweis. (a) Es sei k fest. Aus Folgerung 4.18 wissen wir, dass $\sum_{g \in C_l} \rho(g) = \omega_k(C_l)\mathbf{1}_n$, wobei $n = \chi_k(1)$. Es gilt

$$\begin{aligned}\omega_k(C_i)\omega_k(C_j)\mathbf{1}_n &= \Big(\sum_{x \in C_i} \rho(x)\Big)\Big(\sum_{y \in C_j} \rho(y)\Big) = \sum_{(x,y) \in C_i \times C_j} \rho(xy) \\ &= \sum_{g \in G} \alpha_{C_i,C_j}(g)\rho(g) = \sum_{l=1}^{r} \alpha_{C_i,C_j}(g_l)\Big(\sum_{g \in C_l} \rho(g)\Big) = \sum_{l=1}^{r} \alpha_{C_i,C_j}(g_l)\omega_k(C_l)\mathbf{I}_n,\end{aligned}$$

wobei die vorletzte Gleichung daher kommt, dass α_{C_i,C_j} eine Klassenfunktion ist. In Matrizenform heißt das genau, dass v_k ein Eigenvektor von Z_i zum Eigenwert $\omega_k(C_i)$ ist.

(b) Es sei M die Matrix mit Spalten gegeben durch $v_1, \dots, v_r$. Betrachte die Diagonalmatrizen $D_1 = \mathrm{Diag}(\chi_1(1)^{-1}, \dots, \chi_r(1)^{-1})$ und $D_2 = \mathrm{Diag}(|C_1|, \dots, |C_r|)$. Dann gilt $M = D_1 X(G) D_2$. Da $\det(X(G)) \neq 0$ ist auch $\det(M) \neq 0$.

(c) Nach Voraussetzung gibt es $\lambda_1, \dots, \lambda_r \in \mathbb{C}$ mit $Z_i v = \lambda_i v$ für $1 \leq i \leq r$. Nach (b) können wir v als Linearkombination $v = c_1 v_1 + \dots + c_r v_r$ mit $c_k \in \mathbb{C}$ schreiben. Dann gilt

$$\sum_{k=1}^{r} \lambda_i c_k v_k = \lambda_i v = Z_i v = \sum_{k=1}^{r} c_k Z_i v_k = \sum_{k=1}^{r} c_k \omega_k(C_i) v_k.$$

Also folgt $\lambda_i c_k = c_k \omega_k(C_i)$ für $1 \leq i, k \leq r$. Angenommen, es gäbe Indizes $k \neq l$ mit $c_k \neq 0$ und $c_l \neq 0$, dann folgte $\omega_k(C_i) = \lambda_i = \omega_l(C_i)$ für alle i, Widerspruch zu (b). □

Algorithmus 4.38. Input: eine endliche Gruppe G. Output: die Charaktertafel $X(G)$.

Beschreibung. 1. Schritt. Bestimme alle Konjugationsklassen $C_1, \dots, C_r$ von G sowie die Matrizen $Z_1, \dots, Z_r$. (Dies geschiet allein durch Rechnungen mit Elementen von G.)

2. Schritt. Für jedes Z_i berechne die Eigenwerte und die zugehörigen Eigenräume. Bilde die Durchschnitte dieser Eigenräume und wähle daraus r linear unabhängige Vektoren $u_1, \dots, u_r \in \mathbb{C}^r$, sodass jedes u_k ein gemeinsamer Eigenvektor von $Z_1, \dots, Z_r$ ist.

3. Schritt. Berechne die Werte $\chi_k(g_i)$ aus den Komponenten von u_k wie im Folgenden erklärt. Bemerke: Ist $u_k = (u_{k,1}, \dots, u_{k,r})^{\mathrm{t}}$, so ist

$$u_{k,i} = c_k \omega_k(C_i) = \frac{c_k |C_i| \chi_k(g_i)}{\chi_k(1)} \quad \text{mit } c_k \in \mathbb{C}. \tag{4.5}$$

Aus $C_1 = \{1\}$ folgt $\omega_k(C_1) = |C_1| = 1$, also $c_k = u_{k,1}$. Außerdem berechnen wir die (positive reelle) Zahl $\alpha = \sum_{i=1}^{r} |u_{k,i}|^2 / |C_i|$. Dann gilt

$$\alpha = \frac{|c_k|^2}{\chi_k(1)^2} \sum_{i=1}^{r} |C_i| \chi_k(g_i) \overline{\chi_k(g_i)} = \frac{|c_k|^2}{\chi_k(1)^2} |G|.$$

Also ist $|c_k| / \chi_k(1) = \pm\sqrt{\alpha / |G|}$. Da wir c_k bereits kennen, legt dies $\pm\chi_k(1)$ fest und damit auch $\chi_k(1)$ selbst (da dies positiv ist, siehe Bemerkung 4.3). Nun kann $\chi_k(g_i)$ aus (4.5) gewonnen werden. □

Beispiel 4.39 (Charaktertafel von A_5)**.** Man rechnet nach, dass es fünf Konjugationsklassen in A_5 gibt, mit Repräsentanten id, (1 2)(3 4), (1 2 3), (1 2 3 4 5) bzw. (1 3 5 2 4). Die Matrix Z_1 ist gleich der Einheitsmatrix $\mathbf{1}_5$. Mit GAP können wir die weiteren Matrizen Z_2, Z_3, Z_4, Z_5 berechnen. Insbesondere gilt

$$Z_4 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 4 & 3 & 5 & 0 \\ 0 & 4 & 3 & 5 & 5 \\ 0 & 4 & 3 & 1 & 1 \\ 12 & 0 & 3 & 1 & 5 \end{pmatrix}$$

Das charakteristische Polynom von Z_4 ist $X(X-12)(X+3)(X^2-4X-16)$, d. h., wir haben hier bereits fünf verschiedene Eigenwerte, nämlich 0, 12, -3 und $2 \pm 2\sqrt{5}$, jeweils mit einem Eigenraum der Dimension 1. Um $X(\mathrm{A}_5)$ überhaupt erst zu bestimmen, bräuchten wir also nur Eigenvektoren zu diesen fünf Eigenwerten von Z_4 zu berechnen und dann wie im 3. Schritt vorzugehen. Um einfach nur zu zeigen, dass $X(\mathrm{A}_5)$ die folgende Matrix ist, brauchen wir nur die Gleichungen $\langle \chi_k, \chi_k \rangle = 1$, und $Z_4 v_k = \omega_k(C_4) v_k$ für $1 \le k \le 5$ nachzurechnen, mit v_k wie in Bezeichnung 4.36.

4.4 Aufgaben

Aufgabe 4.40. Gegeben seien die folgenden Matrizen in $\mathrm{GL}_2(\mathbb{C})$:

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

A_5	id	(1 2)(3 4)	(1 2 3)	(1 2 3 4 5)	(1 3 5 2 4)
χ_1	1	1	1	1	1
χ_2	3	-1	0	$(1+\sqrt{5})/2$	$(1-\sqrt{5})/2$
χ_3	3	-1	0	$(1-\sqrt{5})/2$	$(1+\sqrt{5})/2$
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

Dann ist $Q_8 = \{\pm E, \pm I, \pm J, \pm K\}$ eine Untergruppe von $GL_2(\mathbb{C})$ mit $|Q_8| = 8$, und heißt *Quaternionengruppe*. Zeige, dass diese Matrixdarstellung irreduzibel ist.

Aufgabe 4.41. Es sei $\chi \in \mathrm{Irr}(G)$. Zeige: Ist $\lambda \in \mathrm{Irr}(G)$ mit $\lambda(1) = 1$, so gilt $\chi\lambda \in \mathrm{Irr}(G)$.

Aufgabe 4.42. Es sei G eine endliche Gruppe.

(a) Die Gruppe G operiert auf sich selbst durch Konjugation. Bestimme den Charakter des zugehörigen Permutationsmoduls.

(b) Zeige: Die Summe der Einträge in einer Zeile der Charaktertafel von G ist in $\mathbb{N}_0$.

Aufgabe 4.43. Es sei $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_r\}$ und es seien $C_1, \ldots, C_r$ die Konjugationsklassen von G. Zeige:

$$\overline{\det(X(G))} = \pm\det(X(G)) \quad \text{und} \quad \det(X(G))^2 = \pm\frac{|G|^r}{|C_1| \cdot |C_2| \cdot \ldots \cdot |C_r|}.$$

Finde jeweils Beispiele mit $\det(X(G))^2 > 0$ bzw. $\det(X(G))^2 < 0$.

Aufgabe 4.44. (a) Zeige: Ist $N \trianglelefteq G$ ein Normalteiler und $\sigma : G/N \to GL_n(\mathbb{C})$ eine irreduzible Matrixdarstellung, so ist auch $\hat{\sigma} : G \to GL_n(\mathbb{C})$, $g \mapsto \sigma(gN)$, eine irreduzible Matrixdarstellung.

(b) Bestimme die Charaktertafel der Kleinschen Vierergruppe V_4.

(c) Bestimme die Charaktertafel einer nicht-abelschen Gruppe der Ordnung 8. (Hinweis: Zeige, dass $G/Z(G) \cong V_4$ sein muss.)

(d) Bestimme die Charaktertafel der alternierenden Gruppe A_4. (Hinweis: Die Gruppe A_4 hat einen Normalteiler der Ordnung 4.)

Aufgabe 4.45. Es sei G eine endliche Gruppe und $\rho : G \to GL_n(\mathbb{C})$ eine Darstellung mit Charakter χ. Zeige:

(a) Die Menge $N = \{\, g \in G \mid \rho(g) = \lambda \mathbf{1}_n \text{für ein } \lambda \in \mathbb{C} \,\}$ ist ein Normalteiler von G.

(b) Es gilt $g \in N$ genau dann, wenn $\chi(1) = |\chi(g)|$.

(c) Für jedes $g \in G$ der Ordnung $d = \mathrm{Ord}(g) \geq 1$ ist das charakteristische Polynom von $\rho(g)$ durch die Werte $\chi(g^i)$ für $0 \leq i \leq d-1$ bestimmt. (Hinweis: Betrachte die Eigenwerte von $\rho(g)$.)

Aufgabe 4.46. Es sei G eine endliche Gruppe, in der es ein Element $t \in G$ der Ordnung 2 gibt. Es sei $\chi \in \mathrm{Irr}(G)$ beliebig. Zeige:

(a) Es gilt $\chi(t) \in \mathbb{Z}$. Ist $\chi(1) = 2$, welches sind die Möglichkeiten für $\chi(t)$? (Betrachte die Eigenwerte von $\rho(t)$, wobei $\rho\colon G \to \mathrm{GL}_n(\mathbb{C})$ eine Darstellung mit Charakter χ ist.)
(b) Es sei G nicht-abelsch und einfach. Ist χ nicht der triviale Charakter, so gilt $\chi(1) > 2$.

Aufgabe 4.47. Es sei G eine endliche, nicht-abelsche, einfache Gruppe, in der es ein Element $t \in G$ der Ordnung 2 gibt mit Zentralisator H der Ordnung $|H| = 4$. Ziel dieser Aufgabe ist es, zu zeigen, dass $G \cong \mathrm{A}_5$ gilt.

(a) Es sei C die Konjugationsklasse von t und betrachte die in Bezeichnung 4.35 definierte Funktion $\alpha_{C,C}\colon G \to \mathbb{C}$. Zeige: Sind $x, y \in C$ mit $t = xy$, so folgt $x, y \in H$; schließe damit, dass $\alpha_{C,C}(t) \leq 2$ gilt. Kann man den genauen Wert von $\alpha_{C,C}(t)$ bestimmen?
(b) zeige mit Hilfe der Spalten-Orthogonalität der Charaktertafel, dass es genau 4 irreduzible Charaktere $\chi_1, \chi_2, \chi_3, \chi_4$ von G gibt mit Wert ± 1 auf t, und alle anderen irreduziblen Charaktere haben Wert 0 auf t. (Wie oft kommen die Werte $+1$ und -1 jeweils vor?) Schließe weiterhin:

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(t)^3}{\chi(1)} = \sum_{i=1}^{4} \frac{\pm 1}{\chi_i(1)} > \frac{1}{3}.$$

(c) Kombiniere nun (a) und (b) mit der Charakterformel für $\alpha_{C,C}$, um zu zeigen, dass $|G| < 96$ gilt. Versuche anschließend, die diversen Terme in obigen Abschätzungen zu präzisieren um zu schließen, dass $|G| = 60$ und damit $G \cong \mathrm{A}_5$ gelten muss.

Bemerkung 4.48. Obige Übung ist ein Spezialfall eines viel allgemeineren Satzes, nämlich: Es sei G eine endliche, nicht-abelsche, einfache Gruppe. Nach dem Satz von Feit–Thompson ist $|G|$ gerade; nach dem Satz von Cauchy gibt es also ein $t \in G$ der Ordnung 2. Es sei $n = |H|$, wobei H der Zentralisator von t ist. Dann besagt der Satz von Brauer–Fowler (1955), dass G isomorph zu einer Untergruppe von S_{n^2-1} ist, es damit nur endlich viele Möglichkeiten für G bis auf Isomorphie gibt. Die obige Übung zeigt also, dass es im Fall $n = 4$ sogar nur genau eine Möglichkeit gibt.

Bis hier Woche 12

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

[4] 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

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

[6] Serre J.P., *Linear representations of finite groups*, Graduate Texts in Mathematics, vol. 42, Springer-Verlag, 1977.

[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