Permutationsgruppen

Vorlesung im Sommersemester 2015

Benjamin Sambale

Vorwort

Das vorliegende Skript basiert auf einer Vorlesung im Sommersemester 2015 an der Friedrich-Schiller-Universität in Jena. Es handelt sich um eine $3 + 1$ Vorlesung für Masterstudenten der Mathematik. Zum Verständnis der Vorlesung werden nur Kenntnisse der „Algebra 1“ benötigt. Mit Kenntnissen der Gruppentheorie ließen sich daher einige Stellen des Skripts überspringen (zum Beispiel Definition 2.9). Im Anhang finden sich alternative Beweise zu einigen Sätzen und ergänzende Resultate. Ich bedanke mich bei Sebastian Uschmann für zahlreiche Fehlerhinweise und Verbesserungsvorschläge.

Folgende Quellen liegen dem Skript zu Grunde:

- Isaacs, *Finite group theory*, Graduate Studies in Mathematics Vol. 92, American Mathematical Society, Providence, RI, 2008
- Kurzweil und Stellmacher, *The theory of finite groups*, Universitext, Springer-Verlag, New York, 2004 (original auf deutsch)
- Wilson, *The finite simple groups*, Graduate Texts in Mathematics Vol. 251, Springer-Verlag, London, 2009
- Dixon und Mortimer, *Permutation groups*, Graduate Texts in Mathematics Vol. 163, Springer-Verlag, New York, 1996
- Passman, *Permutation groups*, Dover Publications, Inc., Mineola, NY, 2012 (1. Edition von 1968)
- Cameron, *Permutation groups*, London Mathematical Society Student Texts Vol. 45, Cambridge University Press, Cambridge, 1999
- Wielandt (übersetzt von Bercov), *Finite permutation groups*, Academic Press, London-New York, 1964
- Netto (übersetzt von Cole), *The theory of substitutions and its applications to algebra*, Chelsea Publishing Co., New York, 1964 (1. Edition von 1882)
- Burness, *Topics in Permutation Group Theory*, Skript von Young Algebraists' Conference, Lausanne, 2014, `http://seis.bristol.ac.uk/~tb13602/docs/permgroups_14.pdf`
- Müller, *Finite permutation groups*, Skript, 2013, `http://www.mathematik.uni-wuerzburg.de/~mueller/Teach/pg.pdf`
- Fawcett, *The O'Nan-Scott Theorem for Finite Primitive Permutation Groups, and Finite Representability*, Master thesis, Waterloo, 2009, `https://uwspace.uwaterloo.ca/bitstream/handle/10012/4534/Fawcett_Joanna.pdf`
- Cameron, *Proofs of some theorems of W. A. Manning*, Bull. London Math. Soc. 1 (1969), 349–352
- Cameron, Praeger, Saxl und Seitz, *On the Sims conjecture and distance transitive graphs*, Bull. London Math. Soc. 15 (1983), 499–506
- Chapman, *An elementary proof of the simplicity of the Mathieu groups M_{11} and M_{23}*, Amer. Math. Monthly 102 (1995), 544–545
- Guralnick, *Subgroups of prime power index in a simple group*, J. Algebra, 81 (1983), 304–311
- Guralnick und Wales, *Subgroups inducing the same permutation representation, II*, J. Algebra, 96 (1985), 94–13
- Jones, *Primitive permutation groups containing a cycle*, Bull. Aust. Math. Soc. 89 (2014), 159–165
- Lam und Leep, *Combinatorial structure on the automorphism group of S_6*, Exposition. Math. 11 (1993), 289–308

- Li, Lu und Marušič, *On primitive permutation groups with small suborbits and their orbital graphs*, J. Algebra 279 (2004), 749–770
- Liebeck, Praeger und Saxl, *A classification of the maximal subgroups of the finite alternating and symmetric groups*, J. Algebra 111 (1987), 365–383
- Liebeck und Saxl, *Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces*, Proc. London Math. Soc. 63 (1991), 266–314
- Maróti, *On the orders of primitive groups*, J. Algebra 258 (2002), 631–640
- Miller, *In a Simple Group of an Odd Composite Order every System of Conjugate Operators or Subgroups includes more than Fifty*, Proc. London Math. Soc. 33 (1900), 6–10
- Müller, *Permutation groups of prime degree, a quick proof of Burnside's theorem*, Arch. Math. (Basel) 85 (2005), 15–17
- Neumann, *Finite permutation groups, edge-coloured graphs and matrices*, in: Topics in group theory and computation, 82–118. Academic Press, London-New York, 1977.
- Dolfi, Guralnick, Praeger und Spiga, *On the maximal number of coprime subdegrees in finite primitive permutation groups*, arXiv:1203.2728v1
- Liebeck, Praeger und Saxl, *The classification of* $\frac{3}{2}$*-transitive permutation groups and* $\frac{1}{2}$*-transitive linear groups*, arXiv:1412.3912v1
- Wilson, *There is no* Sz(8) *in the Monster*, arXiv:1508.04996v1
- Cameron, *A note on Burnside's Theorem*, `http://www.maths.qmul.ac.uk/~pjc/permgps/burnside.html`
- Godfrey und Kociemba, *Rubik's Cube antisymmetry and the shrinking of Cube Space*, `http://cubezzz.homelinux.org/drupal/?q=node/view/22`
- Wikipedia, *Rank* 3 *permutation group*, `https://en.wikipedia.org/wiki/Rank_3_permutation_group`

Jena, 22. Dezember 2015, Benjamin Sambale

Inhaltsverzeichnis

1 Gruppenoperationen

Stets sei G eine endliche Gruppe und Ω eine nichtleere, endliche Menge.

Satz 1.1 (Wiederholung Algebra 1)**.**

(i) Für $H, K \leq G$ ist $HK \leq G$ genau dann, wenn $HK = KH$.

(ii) Für $H \leq G$ und $N \trianglelefteq G$ ist $NH \leq G$.

(iii) Für $H, K \leq G$ ist $|HK| = \frac{|H||K|}{|H \cap K|}$.

(iv) Für $H, K, L \leq G$ mit $H \leq L$ ist $HK \cap L = H(K \cap L)$ (Dedekind-Identität). □

Definition 1.2.

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

(ii) Die Elemente von $\mathrm{Sym}(\Omega)$ nennt man *Permutationen*. Wie üblich lässt sich jede Permutation σ als Produkt von disjunkten Zyklen $\sigma = \sigma_1 \ldots \sigma_s$ schreiben. Dabei sind die Zyklen σ_i bis auf „Rotation“ und Reihenfolge eindeutig. Hat σ_i die Länge l_i, so hat σ *Zyklentyp* $(l_1, \ldots, l_s)$. Es gilt $|\langle\sigma\rangle| = \mathrm{kgV}(l_1, \ldots, l_s)$. Zyklen der Länge 1 (d. h. *Fixpunkte* von σ) lässt man in dieser Darstellung oft weg. Zyklen der Länge 2 heißen *Transpositionen*. Jede Transposition ist eine *Involution*, d. h. ein Element der Ordnung 2.

(iii) Ist $\sigma \in \mathrm{Sym}(\Omega)$ ein Zyklus der Länge r, so setzt man $\mathrm{sgn}(\sigma) := (-1)^{r+1}$. Dies liefert einen Homomorphismus $\mathrm{sgn} : \mathrm{Sym}(\Omega) \to (\{\pm 1\}, \cdot)$, der *Signum* genannt wird.

(iv) Der Kern von sgn ist die *alternierende Gruppe* $\mathrm{Alt}(\Omega) \trianglelefteq \mathrm{Sym}(\Omega)$. Nach dem Homomorphiesatz gilt $|\mathrm{Sym}(\Omega) : \mathrm{Alt}(\Omega)| = 2$, falls $|\Omega| \geq 2$. Analog zu S_n definiert man A_n.

Definition 1.3. Eine *Operation* (engl. action) von G auf Ω ist ein Homomorphismus $f : G \to \mathrm{Sym}(\Omega)$. Wir schreiben ${}^g\omega := (f(g))(\omega) \in \Omega$ für $g \in G$ und $\omega \in \Omega$. Man sagt auch: G *operiert* auf Ω oder Ω ist eine *G-Menge*. Die Zahl $|\Omega|$ ist der *Grad* der Operation. Sofern die Operation im Kontext klar ist, werden wir im Folgenden manchmal Eigenschaften von Operationen auch den entsprechenden Gruppen zuordnen (z. B. der Grad von G).

Bemerkung 1.4.

(i) Für eine Operation $f : G \to \mathrm{Sym}(\Omega)$ gilt offenbar ${}^1\omega = \omega$ und ${}^g({}^h\omega) = {}^{gh}\omega$ für $g, h \in G$ und $\omega \in \Omega$. Seien nun umgekehrt Elemente ${}^g\omega \in \Omega$ für $g \in G$ und $\omega \in \Omega$ gegeben, sodass ${}^1\omega = \omega$ und ${}^g({}^h\omega) = {}^{gh}\omega$ gilt. Aus ${}^g\alpha = {}^g\beta$ folgt dann $\alpha = {}^1\alpha = {}^{g^{-1}g}\alpha = {}^{g^{-1}}({}^g\alpha) = {}^{g^{-1}}({}^g\beta) = \beta$. Also ist $f_g : \Omega \to \Omega$, $\omega \mapsto {}^g\omega$ eine Bijektion. Wegen $f_{gh}(\omega) = {}^{gh}\omega = {}^g({}^h\omega) = (f_g \circ f_h)(\omega)$ für $g, h \in G$ und $\omega \in \Omega$ ist $f : G \to \mathrm{Sym}(\Omega)$, $g \mapsto f_g$ ein Homomorphismus (also eine Operation).

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

Beispiel 1.5. Jede Gruppe G operiert *trivial* auf jeder Menge Ω durch $g \mapsto \mathrm{id}_\Omega$.

Definition 1.6. Eine Operation $f : G \to \mathrm{Sym}(\Omega)$ heißt *treu*, falls f injektiv ist. In diesem Fall ist G also zu einer Untergruppe von $\mathrm{Sym}(\Omega)$ isomorph. Man sagt dann: G ist eine *Permutationsgruppe* auf Ω.

Satz 1.7 (Cayley)**.** *Jede Gruppe G ist eine Permutationsgruppe auf sich selbst. Insbesondere ist G zu einer Untergruppe von $S_{|G|}$ isomorph.*

Beweis. Für $g, x \in G$ sei ${}^g x := gx$. Dann ist ${}^1x = x$ und ${}^{gh}x = (gh)x = g(hx) = {}^g({}^h x)$ für $g, h, x \in G$. Nach Bemerkung 1.4 operiert G also auf sich selbst durch Multiplikation von links. Operiert $g \in G$ trivial, so ist $g = {}^g 1 = 1$. Also ist die Operation treu. □

Bemerkung 1.8.

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

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

Definition 1.9. Für eine Operation $G \to \mathrm{Sym}(\Omega)$ ist

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

offenbar eine Äquivalenzrelation.

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

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

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

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

Beispiel 1.10.

(i) Sei $H \leq G$. Dann operiert H auf G durch Multiplikation von rechts, d. h. ${}^h x := xh^{-1}$ für $h \in H$ und $x \in G$. Die Bahnen sind dabei die Linksnebenklassen G/H. Außerdem operiert G transitiv auf G/H durch ${}^g(xH) := gxH$ für $g, x \in G$ (im Fall $H = 1$ ist dies die Operation aus Satz 1.7).

(ii) Jede Gruppe G operiert auf sich selbst durch *Konjugation*, d. h. ${}^g x := gxg^{-1}$ für $g, x \in G$. Die Bahnen sind dabei die *Konjugationsklassen* und der Stabilisator von $x \in G$ ist der *Zentralisator* $\mathrm{C}_G(x) := \{g \in G : gx = xg\}$. Zwei Elemente in der gleichen Konjugationsklasse heißen *konjugiert*. Der Kern der Operation ist das *Zentrum* $\mathrm{Z}(G) := \bigcap_{x \in G} \mathrm{C}_G(x) = \{g \in G : gx = xg \ \forall x \in G\}$ und das Bild ist die *innere Automorphismengruppe* $\mathrm{Inn}(G)$. Insbesondere ist $G/\mathrm{Z}(G) \cong \mathrm{Inn}(G) \leq \mathrm{Aut}(G) \leq \mathrm{Sym}(G)$.

Ist konkret $G = S_n$ und $x = (\alpha, \beta, \ldots)$, so ist ${}^g x = gxg^{-1} = ({}^g\alpha, {}^g\beta, \ldots)$. Die Konjugationsklassen von S_n sind also genau die Elemente vom gleichen Zyklentyp.

(iii) Jede Gruppe G operiert auf der Menge ihrer Untergruppen durch Konjugation, d. h. $gXg^{-1} := \{gxg^{-1} : x \in X\}$ für $g \in G$ und $X \leq G$. Die Bahnen heißen dabei wieder Konjugationsklassen und der Stabilisator von $X \leq G$ ist der *Normalisator* $\mathrm{N}_G(X) := \{g \in G : gX = Xg\}$. Die Bahnen der Länge 1 entsprechen den Normalteilern von G.

Bemerkung 1.11.

(i) Für $g \in G$ und $\omega \in \Omega$ ist

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

(ii) Ist Δ eine Bahn der Operation $G \to \mathrm{Sym}(\Omega)$, so erhält man durch Einschränken eine transitive Operation $G \to \mathrm{Sym}(\Delta)$ mit Kern $G_\Delta := \bigcap_{\delta \in \Delta} G_\delta \trianglelefteq G$. Insbesondere ist G/G_Δ eine transitive Permutationsgruppe. Wir schreiben auch $G_{\delta_1 \ldots \delta_k}$ anstelle von $G_{\{\delta_1, \ldots, \delta_k\}}$.

(iii) Sei G eine Permutationsgruppe auf Ω mit Bahnen $\Delta_1, \ldots, \Delta_s$. Dann ist die Abbildung $G \to \prod_{i=1}^s G/G_{\Delta_i}$ (direktes Produkt), $g \mapsto (gG_{\Delta_1}, \ldots, gG_{\Delta_s})$ ein Monomorphismus, denn $\bigcap_{i=1}^s G_{\Delta_i} = \{g \in G : {}^g\omega = \omega \ \forall \omega \in \Omega\} = 1$. Insbesondere ist G zu einer Untergruppe von $\prod_{i=1}^s G/G_{\Delta_i}$ isomorph. Die transitiven Permutationsgruppen verdienen daher besondere Beachtung.

Satz 1.12. *Für eine Operation von G auf Ω und $\omega \in \Omega$ ist die Abbildung $G/G_\omega \to {}^G\omega$, $gG_\omega \mapsto {}^g\omega$ bijektiv. Insbesondere ist $|{}^G\omega| = |G : G_\omega|$ und*

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

für ein Repräsentantensystem $\omega_1, \ldots, \omega_s$ für die Bahnen von G auf Ω.

Beweis. Für $g, h \in G$ gilt

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

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

Beispiel 1.13.

(i) In der Situation von Beispiel 1.10 erhält man

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

für ein Repräsentantensystem $x_1, \ldots, x_s$ für die Konjugationsklassen von G.

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

Satz 1.14 („Burnsides Lemma“)**.** *Sei s die Anzahl der Bahnen einer Operation $G \to \mathrm{Sym}(\Omega)$. Für $g \in G$ sei $f(g)$ die Anzahl der Fixpunkte von g. Dann gilt*

$$\boxed{s = \frac{1}{|G|} \sum_{g \in G} f(g).}$$

Beweis. Sei $\omega_1, \ldots, \omega_s$ ein Repräsentantensystem für die Bahnen von G. Nach Bemerkung 1.11 und Satz 1.12 ist

$$\frac{1}{|G|} \sum_{g \in G} f(g) = \frac{1}{|G|} \sum_{\omega \in \Omega} |G_\omega| = \frac{1}{|G|} \sum_{i=1}^{s} |{}^G\omega_i||G_{\omega_i}| = \frac{1}{|G|} \sum_{i=1}^{s} |G : G_{\omega_i}||G_{\omega_i}| = s.$$ □

Definition 1.15. Zwei Operationen $G \to \mathrm{Sym}(\Omega)$ und $G \to \mathrm{Sym}(\Omega')$ sind *isomorph* (oder *ähnlich*), falls es eine Bijektion $\varphi : \Omega \to \Omega'$ und ein $\alpha \in \mathrm{Aut}(G)$ mit ${}^{\alpha(g)}\varphi(\omega) = \varphi({}^g\omega)$ für $g \in G$ und $\omega \in \Omega$ gibt. Ggf. sind Ω und Ω' *isomorphe G-Mengen*. In den Anwendungen ist oft $\alpha = \mathrm{id}_G$.

Bemerkung 1.16. Wie üblich haben zwei isomorphe Operationen die gleichen Eigenschaften (trivial, treu, transitiv, ...). Man interessiert sich daher in der Regel nur für Operationen bis auf Isomorphie.

Satz 1.17. *Sei $\omega_1, \ldots, \omega_s$ ein Repräsentantensystem für die Bahnen einer Operation $f : G \to \mathrm{Sym}(\Omega)$. Dann ist f isomorph zu der Operation von G auf $\Delta := \bigsqcup_{i=1}^{s} G/G_{\omega_i}$ (disjunkte Vereinigung) durch Linksmultiplikation.*

Beweis. Nach Satz 1.12 ist die Abbildung $\varphi : \Delta \to \Omega$, $gG_{\omega_i} \mapsto {}^g\omega_i$ eine wohldefinierte Bijektion. Für $g \in G$ und $xG_{\omega_i} \in \Delta$ gilt außerdem ${}^g\varphi(xG_{\omega_i}) = {}^g({}^x\omega_i) = {}^{gx}\omega_i = \varphi(gxG_{\omega_i}) = \varphi({}^g(xG_{\omega_i}))$. □

Bemerkung 1.18. Man kann jede Operation von G also auch durch Angabe von Untergruppen beschreiben (je eine Untergruppe pro Bahn). Aufgabe 1.4 beschäftigt sich dabei mit der Eindeutigkeit.

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

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

Definition 1.20. Eine transitive Operation $G \to \mathrm{Sym}(\Omega)$ heißt *regulär*, falls $|G| = |\Omega|$ gilt.

Bemerkung 1.21. Sei $f : G \to \mathrm{Sym}(\Omega)$ regulär, und sei $\omega \in \Omega$. Da f transitiv ist, gilt $|G| = |\Omega| = |G : G_\omega|$, d. h. $G_\omega = 1$. Insbesondere ist f treu. Nach Satz 1.17 ist f isomorph zu der Operation aus Satz 1.7. Man kann also von „der“ regulären Operation von G sprechen.

Definition 1.22. Sei $f : G \to \mathrm{Sym}(\Omega)$ eine transitive, nicht-triviale Operation. Eine Teilmenge $\Delta \subseteq \Omega$ mit $1 < |\Delta| < |\Omega|$ heißt *Block* von f, falls für jedes $g \in G$ die Mengen ${}^g\Delta := \{{}^g\delta : \delta \in \Delta\}$ und Δ entweder gleich oder disjunkt sind. Existieren Blöcke, so heißt f *imprimitiv* und anderenfalls *primitiv*.

Bemerkung 1.23.

(i) Sei Δ ein Block einer Operation $G \to \mathrm{Sym}(\Omega)$, und sei $x \in G$. Dann ist sicher $|{}^x\Delta| = |\Delta|$. Für $g \in G$ gilt ${}^g({}^x\Delta) \cap {}^x\Delta = {}^{gx}\Delta \cap {}^x\Delta = {}^x({}^{x^{-1}gx}\Delta \cap \Delta) \in \{{}^x\Delta, \varnothing\}$. Daher ist auch ${}^x\Delta$ ein Block. Da G transitiv auf Ω operiert, ist $\mathcal{B} := \{{}^g\Delta : g \in G\}$ ein Partition von Ω. Insbesondere ist $|\Omega| = |\Delta||\mathcal{B}|$ und $\boxed{|\Delta| \mid |\Omega| \mid |G|.}$ Außerdem operiert G sicher transitiv auf $\mathcal{B}$.

(ii) Beachte: Für nicht-transitive Operationen sind Blöcke nicht definiert!

Beispiel 1.24.

(i) Nach Bemerkung 1.23 ist jede transitive Operation mit Primzahlgrad primitiv.

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

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

Definition 1.25. Eine Untergruppe $M \leq G$ heißt *maximal*, falls $M \neq G$ gilt und keine Untergruppe $H \leq G$ mit $M < H < G$ existiert.

Satz 1.26. *Eine transitive Operation $G \to \mathrm{Sym}(\Omega)$ ist genau dann primitiv, falls G_ω für ein (oder alle) $\omega \in \Omega$ eine maximale Untergruppe von G ist.*

Beweis. Sei zunächst Δ ein Block von G und $\omega \in \Delta$. Wir setzen $G_{(\Delta)} := \{g \in G : {}^g\Delta = \Delta\} \leq G$. Für $g \in G_\omega$ ist $\omega = {}^g\omega \in \Delta \cap {}^g\Delta \neq \varnothing$ und damit ${}^g\Delta = \Delta$. Dies zeigt $G_\omega \subseteq G_{(\Delta)}$. Wegen $|\Delta| > 1$ ist $G_\omega < G_{(\Delta)}$. Andererseits ist $G_{(\Delta)} < G$, da $G_{(\Delta)}$ nicht transitiv auf Ω operiert ($\Delta \neq \Omega$). Also ist G_ω nicht maximal. Sei nun $\omega' \in \Omega$ beliebig. Dann existiert ein $g \in G$ mit ${}^g\omega = \omega'$ und $G_{\omega'} = gG_\omega g^{-1}$. Somit ist kein Stabilisator maximal.

Sei nun umgekehrt G_ω nicht maximal für ein $\omega \in \Omega$. Im Fall $G_\omega = G$ operiert G trivial und damit nicht primitiv. Sei also $G_\omega < H < G$. Wir setzen $\Delta := {}^H\omega$. Wegen $G_\omega < H$ ist $|\Delta| > 1$. Außerdem ist $|\Delta| = |{}^H\omega| = |H : H_\omega| = |H : G_\omega| < |G : G_\omega| = |\Omega|$. Sei nun $g \in G$ mit $\delta \in \Delta \cap {}^g\Delta$. Dann existieren $h, h' \in H$ mit $\delta = {}^h\omega = {}^{gh'}\omega$. Es folgt $h^{-1}gh' \in G_\omega \subseteq H$ und $g \in H$. Also ist ${}^g\Delta = \Delta$ und die Operation ist imprimitiv. □

Satz 1.27. *Sei $G \to \mathrm{Sym}(\Omega)$ eine imprimitive Operation mit Block Δ, der maximal bzgl. Inklusion gewählt ist. Dann ist die Operation von G auf $\mathcal{B} := \{{}^g\Delta : g \in G\}$ primitiv.*

Beweis. Nehmen wir indirekt an, dass ein Block $\mathcal{C} \subseteq \mathcal{B}$ existiert. Wir können $\Delta \in \mathcal{C}$ annehmen. Setze $\Gamma := \bigcup_{C \in \mathcal{C}} C$. Dann ist $|\Delta| < |\Delta||\mathcal{C}| = |\Gamma| < |\Delta||\mathcal{B}| = |\Omega|$. Sei $g \in G$ und $\omega \in \Gamma \cap {}^g\Gamma$. Dann existieren $x, y \in G$ mit $\omega \in {}^x\Delta \cap {}^{gy}\Delta$. Also ist ${}^x\Delta = {}^{gy}\Delta \in \mathcal{C} \cap {}^g\mathcal{C}$ und ${}^g\mathcal{C} = \mathcal{C}$. Dies zeigt ${}^g\Gamma = \Gamma$. Also ist Γ ein Block von G, der Δ echt enthält. Dies widerspricht aber das Maximalität von Δ. □

Bemerkung 1.28.

Sei $G \neq 1$ eine Permutationsgruppe auf Ω. Nach Bemerkung 1.11 existiert ein Normalteiler $N_1 \trianglelefteq G$, sodass $G/N_1 \neq 1$ eine transitive Permutationsgruppe ist. Weiter existiert nach Satz 1.27 ein Normalteiler $N_2/N_1 \trianglelefteq G/N_1$, sodass $(G/N_1)/(N_2/N_1) \cong G/N_2$ (zweiter Isomorphiesatz) eine primitive Permutationsgruppe ist. Da auch N_2 treu auf Ω operiert, kann man diesen Prozess mit N_2 statt G wiederholen. Dies liefert eine Folge von Untergruppen $1 = G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_k = G$, sodass die Faktoren G_i/G_{i-1} primitive Permutationsgruppen sind. Im Unterschied zum Satz von Jordan-Hölder sind die Faktoren G_i/G_{i-1} aber in keiner Weise eindeutig. Wir werden später alle primitiven Permutationsgruppen klassifizieren (Satz 5.7). Zum Beispiel ist jede primitive Permutationsgruppe vom Grad 34 zu A_{34} oder S_{34} isomorph.

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

Aufgabe 1.2. Sei G eine abelsche, transitive Permutationsgruppe. Zeigen Sie, dass G regulär ist.

Aufgabe 1.3. Zeigen, Sie dass eine transitive Operation $G \to \mathrm{Sym}(\Omega)$ genau dann treu ist, wenn G_ω für $\omega \in \Omega$ keinen nicht-trivialen Normalteiler enthält.

Aufgabe 1.4. Seien $\varphi : G \to S_n$ und $\psi : G \to S_n$ zwei treue Operationen. Zeigen Sie:

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

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

Aufgabe 1.5. Seien $\varphi : G \to \mathrm{Sym}(\Omega)$ und $\psi : G \to \mathrm{Sym}(\Delta)$ Operationen, sodass für jede Untergruppe $H \leq G$ die Anzahl der Fixpunkte von H auf Ω gleich der Anzahl der Fixpunkte von H auf Δ ist. Zeigen Sie, dass φ und ψ isomorph sind. Gilt auch die Umkehrung?

Aufgabe 1.6. Sei $G \to \mathrm{Sym}(\Omega)$ eine imprimitive Operation und $\Delta \subseteq \Omega$ ein Block, der bzgl. Inklusion minimal ist. Zeigen Sie, dass $G_{(\Delta)} := \{g \in G : {}^g\Delta = \Delta\}$ primitiv auf Δ operiert.

Aufgabe 1.7. Sei $G \leq S_n$ regulär. Zeigen Sie: $\mathrm{C}_{S_n}(G) \cong G$.

Aufgabe 1.8.

(i) Sei $G \to \mathrm{Sym}(\Omega)$ eine transitive Operation mit $|\Omega| > 1$. Zeigen Sie, dass mindestens ein Element aus G keine Fixpunkte auf Ω hat.

(ii) Wählt man $g \in S_n$ zufällig und gleich verteilt, wie hoch ist die Wahrscheinlichkeit, dass g keine Fixpunkte hat?

Aufgabe 1.9. Sei $P \in \mathrm{Syl}_2(G)$ zyklisch. Zeigen Sie, dass ein Normalteiler $N \trianglelefteq G$ mit $G = NP$ und $N \cap P = 1$ existiert.

Aufgabe 1.10. Zeigen Sie, dass jede Gruppe der Ordnung 264 auflösbar ist.
Hinweis: Realisieren Sie ein Gegenbeispiel als Permutationsgruppe vom Grad 12.

Aufgabe 1.11. Seien P und Q verschiedene p-Sylowgruppen von G, sodass $|P \cap Q|$ möglichst groß ist. Dann ist $|\mathrm{Syl}_p(G)| \equiv 1 \pmod{|P : P \cap Q|}$.

Aufgabe 1.12. Sei G eine Permutationsgruppe vom Grad n mit r Bahnen. Zeigen Sie, dass man G mit $n - r$ Elementen erzeugen kann. Insbesondere lässt sich G immer mit $n - 1$ Elementen erzeugen.

Aufgabe 1.13. Bestimmen Sie alle endlichen Gruppen G, die zu keiner Untergruppe von $S_{|G|-1}$ isomorph sind.
Hinweis: Sie dürfen folgenden Satz verwenden: Eine p-Gruppe mit nur einer Untergruppe der Ordnung p ist zyklisch oder eine (verallgemeinerte) Quaternionengruppe für $p = 2$.

Aufgabe 1.14. Sei $H(n, k)$ die Anzahl der wesentlich verschiedenen Halsketten mit n Perlen aus k verschiedenen Farben. Zeigen Sie:

$$H(n,k) = \begin{cases} \dfrac{1}{2n}\displaystyle\sum_{d|n} \varphi(d)k^{n/d} + \frac{1}{4}(k+1)k^{n/2} & \text{falls } n \text{ gerade,} \\ \dfrac{1}{2n}\displaystyle\sum_{d|n} \varphi(d)k^{n/d} + \frac{1}{2}k^{(n+1)/2} & \text{falls } n \text{ ungerade.} \end{cases}$$

Aufgabe 1.15. Der Organisator der diesjährigen Konferenz über Permutationsgruppen beschließt folgendes Experiment durchzuführen: Die 80 Teilnehmer der Konferenz sollen in den ersten 80 Zimmern des Hotels „Harmonie“ untergebracht werden, aber bislang kennt keiner der Teilnehmer seine Zimmernummer. Die Teilnehmer werden nun nacheinander gebeten ihr Zimmer zu suchen, indem sie in maximal 40 der 80 Zimmer einen Blick werfen dürfen. In jedem Zimmer liegt eine personalisierte Konferenzmappe, sodass ersichtlich ist, wem das Zimmer zugeordnet wurde. Die Teilnehmer dürfen sich vor dem Experiment eine Strategie überlegen, aber während des Experiments in keiner Weise kommunizieren. Das Experiment gilt als erfolgreich, wenn jeder Teilnehmer sein eigenes Zimmer findet. Man überlege sich eine Strategie, bei der die Erfolgswahrscheinlichkeit mehr als 30% beträgt. Zum Vergleich: Öffnet jeder Teilnehmer 40 zufällige Türen, so ist die Wahrscheinlichkeit nur $2^{-80} < 10^{-24}$.

2 Abelsche Normalteiler in primitiven Gruppen

Satz 2.1. *Sei $G \to \mathrm{Sym}(\Omega)$ eine Operation, und sei $N \trianglelefteq G$ regulär. Für $\omega \in \Omega$ ist dann die Operation von G_ω auf Ω isomorph zur Operation auf N durch Konjugation.*

Beweis. Nach Voraussetzung ist die Abbildung $\varphi : N \to \Omega$, $x \mapsto {}^x\omega$ eine Bijektion. Für $g \in G_\omega$ und $x \in N$ gilt ${}^g\varphi(x) = {}^{gx}\omega = {}^{(gxg^{-1})g}\omega = {}^{gxg^{-1}}\omega = \varphi({}^g x)$. □

Satz 2.2. *Sei $G \to \mathrm{Sym}(\Omega)$ eine primitive Operation und $N \trianglelefteq G$. Dann operiert N trivial oder transitiv auf Ω.*

Beweis. Sei $\Delta \subseteq \Omega$ eine nicht-triviale Bahn von N (d. h. $|\Delta| > 1$). Für $g \in G$ ist dann ${}^g\Delta$ eine Bahn von $gNg^{-1} = N$. Also ist ${}^g\Delta \cap \Delta \in \{\Delta, \varnothing\}$. Die Primitivität von G liefert $\Delta = \Omega$, d. h. N ist transitiv. □

Definition 2.3.

(i) Ein Normalteiler $N \trianglelefteq G$ heißt *minimal*, falls $N \neq 1$ gilt und kein Normalteiler $M \trianglelefteq G$ mit $1 < M < N$ existiert.

(ii) Wir schreiben $G = N_1 \oplus \ldots \oplus N_k$ (*direkte Summe*), falls folgende Aussagen gelten:

(a) $N_i \trianglelefteq G$ für $i = 1, \ldots, k$,

(b) $G = N_1 \ldots N_k$,

(c) $N_i \cap N_1 \ldots N_{i-1} = 1$ für $i = 2, \ldots, k$.

Lemma 2.4. *Es gilt $G_1 \oplus \ldots \oplus G_k \cong G_1 \times \ldots \times G_k$.*

Beweis. Offenbar ist $G_i \cap G_j = 1$ für $i \neq j$. Für $x \in G_i$ und $y \in G_j$ gilt daher

$$\underbrace{(xyx^{-1})}_{\in G_j} y^{-1} = x \underbrace{(yx^{-1}y^{-1})}_{\in G_i} \in G_i \cap G_j = 1,$$

d. h. $xy = yx$. Sei nun $x_1 \ldots x_k = y_1 \ldots y_k$ für $x_i, y_i \in G_i$ $(i = 1, \ldots, k)$. Dann ist

$$x_k y_k^{-1} = x_1^{-1} y_1 \ldots x_{k-1}^{-1} y_{k-1} \in G_k \cap G_1 \ldots G_{k-1} = 1$$

und $x_k = y_k$. Wiederholt man die Rechnung mit $x_1 \ldots x_{k-1} = y_1 \ldots y_{k-1}$, so ergibt sich $x_i = y_i$ für $i = 1, \ldots, k$. Also lässt sich jedes Element in $G_1 \oplus \ldots \oplus G_k$ eindeutig in der Form $x_1 \ldots x_k$ mit $x_i \in G_i$ schreiben. Man sieht nun leicht, dass die Abbildung $\bigoplus_{i=1}^k G_i \to \prod_{i=1}^k G_i$, $x_1 \ldots x_k \mapsto (x_1, \ldots, x_k)$ ein Isomorphismus ist. □

Bemerkung 2.5.

(i) In manchen Büchern spricht man vom *inneren* und *äußeren* direkten Produkt (anstatt direkter Summe und direktem Produkt).

(ii) Offenbar ist $G_1 \oplus G_2 = G_2 \oplus G_1$. Sei nun $G = G_1 \oplus G_2 \oplus G_3$. Dann ist sicher $G_1 G_2 = G_1 \oplus G_2 \trianglelefteq G$ und $G = (G_1 \oplus G_2) \oplus G_3$. Sei nun umgekehrt $G = (G_1 \oplus G_2) \oplus G_3$. Dann ist $G_3 \subseteq \mathrm{C}_G(G_1 G_2)$. Dies zeigt $G_1, G_2 \trianglelefteq G$ und $G = G_1 \oplus G_2 \oplus G_3$. Direkte Summen sind also kommutativ und assoziativ.

Satz 2.6. *Jeder minimale Normalteiler $N \trianglelefteq G$ ist eine direkte Summe von isomorphen einfachen Gruppen.*

Beweis. Sei M ein minimaler Normalteiler von N. Für $g \in G$ ist $gMg^{-1} \trianglelefteq gNg^{-1} = N$. Sei $\widetilde{M}$ eine möglichst große direkte Summe von Konjugierten von M (im Zweifel $\widetilde{M} = M$). Nehmen wir $gMg^{-1} \not\subseteq \widetilde{M}$ für ein $g \in G$ an. Wegen $gMg^{-1} \cap \widetilde{M} \trianglelefteq N$ folgt $gMg^{-1} \cap \widetilde{M} = 1$ aus der Minimalität von gMg^{-1}. Also ist $gMg^{-1}\widetilde{M} = gMg^{-1} \oplus \widetilde{M}$ im Widerspruch zur Wahl von $\widetilde{M}$. Dies zeigt $\widetilde{M} = \langle gMg^{-1} : g \in G \rangle \trianglelefteq G$, und $N = \widetilde{M}$ ist eine direkte Summe von Gruppen, die zu M isomorph sind. Nehmen wir nun an, dass M einen Normalteiler $1 \neq K \trianglelefteq M$ besitzt. Wie in Lemma 2.4 ist $gMg^{-1} \subseteq \mathrm{C}_G(M) \subseteq \mathrm{C}_G(K)$ für $gMg^{-1} \neq M$. Dies zeigt $K \trianglelefteq N$, und die Minimalität von M liefert $K = M$. Also ist M einfach und die Behauptung ist bewiesen. □

Definition 2.7.

(i) Wir bezeichnen mit C_n eine (abstrakte) zyklische Gruppe der Ordnung $n \in \mathbb{N}$.

(ii) Eine abelsche Gruppe E heißt *elementarabelsch*, falls eine Primzahl p mit $x^p = 1$ für alle $x \in E$ existiert.

Bemerkung 2.8.

(i) Sei E elementarabelsch für eine Primzahl p. Dann kann man E wie folgt als Vektorraum über $\mathbb{F}_p$ auffassen:

$$\begin{aligned} x + y &:= xy && (x, y \in E), \\ (k + p\mathbb{Z}) \cdot x &:= x^k && (k + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p,\ x \in E). \end{aligned}$$

Man nennt $n := \dim_{\mathbb{F}_p} E$ den *Rang* von E. Insbesondere ist E eine direkte Summe von n Gruppen der Ordnung p, d. h. $E \cong C_p \times \ldots \times C_p =: C_p^n$. Umgekehrt ist jede solche Gruppe auch elementarabelsch. Jeder Automorphismus von E ist offenbar auch $\mathbb{F}_p$-linear. Dies zeigt $\mathrm{Aut}(E) \cong \mathrm{GL}(n, p)$.

(ii) Sei N ein minimaler Normalteiler einer auflösbaren Gruppe G. Dann ist auch N auflösbar (Algebra 1). Nach Satz 2.6 ist andererseits N eine direkte Summe von isomorphen einfachen Gruppen. Eine auflösbare einfache Gruppe hat bekanntlich Primzahlordnung. Somit ist N elementarabelsch.

Definition 2.9. Sei $\varphi : H \to \mathrm{Aut}(N)$ ein Homomorphismus für Gruppen H, N. Insbesondere operiert H auf N. Wir definieren eine Verknüpfung $*$ auf dem kartesischen Produkt $G := N \times H$ durch

$$\boxed{(x, g) * (y, h) := (x({}^g y), gh)} \qquad (x, y \in N,\ g, h \in H).$$

Man zeigt leicht, dass G damit zu einer Gruppe wird. Man nennt $G =: N \rtimes_\varphi H$ das *semidirekte Produkt* von N mit H.

Bemerkung 2.10.

(i) Ist die Operation φ im Kontext klar oder unwesentlich, so schreibt man auch $N \rtimes H$. Insbesondere wählt man im Fall $H \leq \mathrm{Aut}(N)$ oft die Inklusionsabbildung $\varphi : H \hookrightarrow \mathrm{Aut}(N)$.

(ii) Ist φ trivial, so ist offensichtlich $N \rtimes_\varphi H \cong N \times H$.

(iii) Im Gegensatz zum direkten Produkt kann man beim semidirekten Produkt die Faktoren nicht vertauschen.

(iv) Sei $G = N \rtimes_\varphi H$. Dann ist $N \cong \{(x, 1) : x \in N\} =: \widetilde{N} \trianglelefteq G$ und $H \cong \{(1, h) : h \in H\} =: \widetilde{H} \leq G$ mit $G = \widetilde{N}\widetilde{H}$ und $\widetilde{N} \cap \widetilde{H} = 1$.

(v) Nehmen wir nun umgekehrt an, dass G einen Normalteiler $N \trianglelefteq G$ und eine Untergruppe $H \leq G$ mit $G = NH$ und $N \cap H = 1$ enthält. Beschreibt $\varphi : H \to \mathrm{Aut}(N)$ die Operation durch Konjugation, so ist $G \cong N \rtimes_\varphi H$. Man kann also wieder von einem *inneren* und *äußeren* semidirekten Produkt sprechen.

Definition 2.11. Sei V ein n-dimensionaler Vektorraum über dem Körper $\mathbb{F}_q$ für eine Primzahlpotenz q. Für die Gruppe $(V, +)$ ist dann sicher $\mathrm{GL}(V) \leq \mathrm{Aut}(V)$ und

$$\mathrm{Aff}(V) := V \rtimes \mathrm{GL}(V) \qquad \cong \qquad \mathrm{Aff}(n, q) := \mathbb{F}_q^n \rtimes \mathrm{GL}(n, q)$$

ist die *affine Gruppe* vom Grad n über $\mathbb{F}_q$.

Satz 2.12. *Für einen endlich-dimensionalen $\mathbb{F}_q$-Vektorraum V wird $\mathrm{Aff}(V)$ durch*

$$\boxed{{}^{(v,f)}x := f(x) + v} \qquad (v, x \in V,\ f \in \mathrm{GL}(V))$$

zu einer Permutationsgruppe auf V.

Beweis. Für $x \in V$ und $(v,f),(w,g) \in \mathrm{Aff}(V)$ ist ${}^{(0,\mathrm{id}_V)}x = x$ und ${}^{(v,f)*(w,g)}x = {}^{(v+f(w),fg)}x = f(g(x)) + v + f(w) = {}^{(v,f)}(g(x)+w) = {}^{(v,f)}({}^{(w,g)}x)$. Dies zeigt, dass $\mathrm{Aff}(V)$ auf V operiert. Sei nun (v,f) im Kern dieser Operation. Für $0, x \in V$ ist dann $0 = {}^{(v,f)}0 = v$ und $x = {}^{(v,f)}x = f(x)$. Also ist $(v,f) = (0,\mathrm{id}_V)$ und die Operation ist treu. □

Bemerkung 2.13. In der Situation von Satz 2.12 operiert V durch *Translation* regulär auf sich selbst.

Satz 2.14. *Sei G eine primitive Permutationsgruppe vom Grad n mit abelschem Normalteiler $A \neq 1$. Dann ist $A = \mathrm{C}_G(A)$ der einzige minimale Normalteiler von G und $n = |A| = p^m$ für eine Primzahl p. Außerdem ist $G = A \rtimes G_\omega \cong \widetilde{G} \leq \mathrm{Aff}(m,p)$ mit $\mathbb{F}_p^m \trianglelefteq \widetilde{G}$ für $\omega \in \Omega$. Die Operation von G ist isomorph zur Operation aus Satz 2.12, wobei man G mit $\widetilde{G}$ identifiziert.*

Beweis. Nach Satz 2.2 operiert A transitiv auf Ω. Aufgabe 1.2 zeigt nun, dass A sogar regulär auf Ω operiert, d. h. $|A| = n$. Insbesondere ist A minimal und $|A| = p^m$ nach Satz 2.6. Da A abelsch ist, gilt $A \subseteq \mathrm{C}_G(A) =: C$. Sei $\omega \in \Omega$ fest. Für $a \in A$ ist $C_\omega = aC_\omega a^{-1} = C_{{}^a\omega}$. Da A transitiv ist, operiert C_ω trivial, d. h. $C_\omega = 1$. Nach Satz 1.19 hat man nun $C = AC_\omega = A$. Satz 1.19 liefert auch $G = AG_\omega$ und $A \cap G_\omega = A_\omega = 1$. Also ist G ein (inneres) semidirektes Produkt von A mit G_ω. Dabei gilt

$$G_\omega \cong G_\omega/G_\omega \cap A \cong G_\omega A/A = G/A = \mathrm{N}_G(A)/\mathrm{C}_G(A) \leq \mathrm{Aut}(A) \cong \mathrm{GL}(m,p)$$

nach Bemerkung 2.8. Dies liefert einen Monomorphismus $\Gamma : G \to \mathrm{Aff}(m,p)$ mit $\Gamma(A) = \mathbb{F}_p^m$. Man kann also $\widetilde{G} := \Gamma(G)$ setzen. Nach Satz 2.12 operiert G treu auf A durch ${}^{ag}x = agxg^{-1}$ für $a, x \in A$ und $g \in G_\omega$. Wir betrachten nun die Bijektion $\varphi : A \to \Omega$, $x \mapsto {}^x\omega$. Für $a, x \in A$ und $g \in G_\omega$ ist dann ${}^{ag}\varphi(x) = {}^{agx}\omega = {}^{agxg^{-1}g}\omega = {}^{agxg^{-1}}\omega = \varphi({}^{ag}x)$. Dies impliziert die letzte Behauptung. □

Satz 2.15 (Galois)**.** *Eine auflösbare Gruppe G ist genau dann eine primitive Permutationsgruppe, falls G (genau) einen minimalen Normalteiler N mit $\mathrm{C}_G(N) = N$ besitzt.*

Beweis. Sei zunächst G primitiv und $N \trianglelefteq G$ minimal. Nach Bemerkung 2.8 ist N abelsch und Satz 2.14 liefert die Behauptung.

Nehmen wir nun an, dass G einen minimalen Normalteiler N mit $\mathrm{C}_G(N) = N$ besitzt. Wir zeigen zunächst, dass ein Komplement $K \leq G$ von N existiert (d. h. $G = N \rtimes K$). Nach Bemerkung 2.8 ist N eine elementarabelsche p-Gruppe für eine Primzahl p. Im Fall $G = N$ ist $|G| = |N| = p$ und die reguläre Operation von G ist primitiv. Sei also $N < G$. Sei M/N ein minimaler Normalteiler von G/N. Dann ist M/N eine elementarabelsche q-Gruppe für eine Primzahl q. Nehmen wir zunächst $q = p$ an. Dann ist M ein p-Normalteiler von G, und M operiert durch Konjugation auf N. Die Bahnengleichung liefert

$$0 \equiv |N| \equiv |\mathrm{C}_N(M)| \pmod{p}.$$

Insbesondere ist $1 \neq \mathrm{C}_N(M) \trianglelefteq G$. Da N minimal ist, folgt $\mathrm{C}_N(M) = N$ und $M \subseteq \mathrm{C}_G(N) = N$. Dieser Widerspruch zeigt $q \neq p$. Sei $Q \in \mathrm{Syl}_q(M)$. Dann ist $M = QN$. Für $g \in G$ ist $gQg^{-1} \leq gMg^{-1} = M$. Nach Sylow existiert ein $h \in M$ mit $gQg^{-1} = hQh^{-1}$. Also operiert M transitiv auf den Konjugierten von Q in G. Nach Satz 1.19 ist also $G = \mathrm{N}_G(Q)M = \mathrm{N}_G(Q)QN = \mathrm{N}_G(Q)N$. Offenbar ist $\mathrm{N}_G(Q) \cap N \trianglelefteq \mathrm{N}_G(Q)$. Da N abelsch ist, gilt auch $\mathrm{N}_G(Q) \cap N \trianglelefteq N$. Insgesamt ist also $\mathrm{N}_G(Q) \cap N \trianglelefteq G$. Die Minimalität von N zeigt $\mathrm{N}_G(Q) \cap N \in \{1, N\}$. Nehmen wir an, dass der Fall $N \subseteq \mathrm{N}_G(Q)$ eintritt. Wie oben ist dann $G = \mathrm{N}_G(Q)N = \mathrm{N}_G(Q)$, also $Q \trianglelefteq G$. Aus Ordnungsgründen ist $N \cap Q = 1$ und damit $Q \subseteq \mathrm{C}_G(N) = N$. Widerspruch. Also ist $\mathrm{N}_G(Q) \cap N = 1$ und $G = N \rtimes K$ für $K := \mathrm{N}_G(Q)$.

Wir betrachten die Operation $\varphi : G \to \mathrm{Sym}(G/K)$ durch Linksmultiplikation. Bekanntlich ist φ transitiv. Die Elemente aus $\mathrm{Ker}(\varphi)$ lassen die triviale Nebenklasse $1K$ fest. Also ist $\mathrm{Ker}(\varphi) \subseteq K$ und $N \cap \mathrm{Ker}(\varphi) = 1$. Wegen $\mathrm{Ker}(\varphi) \subseteq \mathrm{C}_G(N) = N$ ist $\mathrm{Ker}(\varphi) = 1$ und φ ist treu. Der Stabilisator der trivialen Nebenklasse ist offenbar K. Nach Satz 1.26 genügt es zu zeigen, dass K maximal ist. Sei also $K < H \leq G$. Dann ist $1 \neq H \cap N \trianglelefteq H$ (anderenfalls wäre $|HN| > |G|$). Da N abelsch ist, gilt auch $H \cap N \trianglelefteq N$ und somit $H \cap N \trianglelefteq HN = HKN = G$. Die Minimalität von N impliziert wieder $N = H \cap N \subseteq H$. Also ist $G = KN \subseteq H$ und K ist maximal. □

Beispiel 2.16.

(i) Sei V eine elementarabelsche Gruppe und $G \leq \mathrm{Aff}(V)$ mit $V \trianglelefteq G$. Wir wollen untersuchen, wann die Operation $\varphi : G \to \mathrm{Sym}(V)$ aus Satz 2.12 primitiv ist. Nach Satz 2.14 muss dafür V ein minimaler Normalteiler sein. Nach Aufgabe 2.3 ist dies sogar hinreichend. Für den Stabilisator $G_0 = G \cap \mathrm{GL}(V)$ gilt also: G ist genau dann primitiv, falls die kanonische *Darstellung* $G_0 \hookrightarrow \mathrm{GL}(V)$ *irreduzibel* ist (vgl. Darstellungstheorie/Charaktertheorie).

(ii) Sei $V \cong C_p^n$. Man kann dann V als additive Gruppe des Körpers $\mathbb{F}_{p^n}$ auffassen. Für $\gamma \in \mathbb{F}_{p^n}^\times$ ist die Abbildung $f_\gamma : V \to V$, $v \mapsto \gamma v$ sicher linear und bijektiv. Also gibt es einen Monomorphismus $f : \mathbb{F}_{p^n}^\times \to \mathrm{Aut}(V) \cong \mathrm{GL}(n,p)$, $\gamma \mapsto f_\gamma$ mit Bild S. Nach Algebra 1 ist $S \cong \mathbb{F}_{p^n}^\times \cong C_{p^n-1}$. Sei $s \in S$ ein Erzeuger. Da jede nicht-triviale Potenz von s nur den trivialen Fixpunkt 0 auf V hat, entspricht s einem Zyklus der Länge $p^n - 1$ in $\mathrm{Sym}(V)$. Insbesondere operiert S transitiv auf $V \setminus \{0\}$. Nach (i) ist also $V \rtimes S$ eine primitive Permutationsgruppe. Man nennt S *Singer-Zyklus*. Im Fall $n = 1$ ist sicher $V \rtimes S = \mathrm{Aff}(V) \cong C_p \rtimes C_{p-1}$.

(iii) Sei V wie in (ii) die additive Gruppe von $\mathbb{F}_{p^n}$. Sei $F \in \mathrm{Aut}(V)$ der *Frobenius-Automorphismus* von $\mathbb{F}_{p^n}$, d. h. $F(x) = x^p$ für $x \in V$ (Algebra 1). Man beachte, dass x^p die Multiplikation des Körpers benutzt und nicht die Gruppenverknüpfung von V; insbesondere ist nicht unbedingt $x^p = 1$. Bekanntlich hat $\langle F \rangle$ die Ordnung n. Als Galois-Automorphismus muss F den Primkörper $\mathbb{F}_p$ festlassen (kleiner Satz von Fermat). Für $n \geq 2$ ist $V \rtimes \langle F \rangle$ also imprimitiv nach (i). Sei nun $f_\gamma \in S$ wie in (ii) und $v \in V$. Dann ist

$$(F \circ f_\gamma \circ F^{-1})(v) = F(\gamma F^{-1}(v)) = \gamma^p v = f_{\gamma^p}(v).$$

Dies zeigt $F \in \mathrm{N}_{\mathrm{Aut}(V)}(S)$. Da F nicht-triviale Fixpunkte im Primkörper hat, gilt auch $S \cap \langle F \rangle = 1$ und $S\langle F \rangle = S \rtimes \langle F \rangle =: \Gamma\mathrm{L}(1, p^n)$. Man nennt $\Gamma\mathrm{L}(1, p^n)$ die *semilineare Gruppe* vom Grad 1. Die auflösbare Gruppe $V \rtimes \Gamma\mathrm{L}(1, p^n) \cong C_p^n \rtimes (C_{p^n-1} \rtimes C_n)$ ist sicher primitiv, da S transitiv auf $V \setminus \{0\}$ operiert. Im Fall $n = p = 2$ ist $V \rtimes \Gamma\mathrm{L}(1, 4) = \mathrm{Aff}(2, 2) \cong S_4$.

Aufgabe 2.1. Sei G eine primitive Permutationsgruppe. Zeigen Sie: $\mathrm{Z}(G) = 1$ oder $|G|$ ist eine Primzahl.

Aufgabe 2.2. Sei G eine primitive Permutationsgruppe vom Grad n mit auflösbarem Normalteiler $N \neq 1$. Zeigen Sie, dass n eine Primzahlpotenz ist.

Aufgabe 2.3. Besitzt eine Permutationsgruppe G einen transitiven, abelschen, minimalen Normalteiler, so ist G primitiv.

3 Mehrfach transitive Gruppen

Definition 3.1. Eine Operation $G \to \mathrm{Sym}(\Omega)$ heißt (*scharf*) *k-transitiv*, falls $|\Omega| \geq k$ und für je zwei k-Tupel $(\alpha_1, \ldots, \alpha_k), (\beta_1, \ldots, \beta_k) \in \Omega^k$ von paarweise verschiedenen Elementen (genau) ein $g \in G$ mit ${}^g\alpha_i = \beta_i$ für $i = 1, \ldots, k$ existiert.

Beispiel 3.2.

(i) Die (scharf) 1-transitiven Operationen sind genau die transitiven (regulären) Operationen.

(ii) Jede (scharf) k-transitive Operation ist offenbar auch l-transitiv für $1 \leq l \leq k$, aber nicht unbedingt scharf l-transitiv.

(iii) Jede scharf k-transitive Operation ist treu.

(iv) Für $n \geq 2$ ist S_n scharf n-transitiv und scharf $(n-1)$-transitiv (auf $\{1, \ldots, n\}$).

(v) Sei $n \geq 3$ und $k := n - 2$. Für k-Tupel $(\alpha_1, \ldots, \alpha_k), (\beta_1, \ldots, \beta_k) \in \{1, \ldots, n\}^k$ mit paarweise verschiedenen Elementen sei $\{x, y\} = \{1, \ldots, n\} \setminus \{\alpha_1, \ldots, \alpha_k\}$ und $\{x', y'\} = \{1, \ldots, n\} \setminus \{\beta_1, \ldots, \beta_k\}$. Dann ist genau eine der beiden Permutationen

$$\begin{pmatrix} \alpha_1 & \cdots & \alpha_k & x & y \\ \beta_1 & \cdots & \beta_k & x' & y' \end{pmatrix} \qquad \text{oder} \qquad \begin{pmatrix} \alpha_1 & \cdots & \alpha_k & x & y \\ \beta_1 & \cdots & \beta_k & y' & x' \end{pmatrix}$$

in A_n. Also ist A_n scharf $(n-2)$-transitiv.

(vi) Für eine Primzahlpotenz q und $n \geq 2$ operiert $\mathrm{GL}(n, q)$ 2-transitiv auf der Menge der eindimensionalen Untervektorräume von $\mathbb{F}_q^n$.

Lemma 3.3. *Sei $\varphi : G \to \mathrm{Sym}(\Omega)$ eine transitive Operation, $\omega \in \Omega$ und $k \geq 2$. Genau dann ist φ (scharf) k-transitiv, wenn G_ω (scharf) $(k-1)$-transitiv auf $\Omega \setminus \{\omega\}$ operiert.*

Beweis. Sei G (scharf) k-transitiv, und seien $(\alpha_1, \ldots, \alpha_{k-1}), (\beta_1, \ldots, \beta_{k-1}) \in (\Omega \setminus \{\omega\})^{k-1}$ mit paarweise verschiedenen Elementen. Dann existiert (genau) ein $g \in G$ mit ${}^g\alpha_i = \beta_i$ für $i = 1, \ldots, k-1$ und ${}^g\omega = \omega$. Also ist $g \in G_\omega$ und G_ω ist (scharf) $(k-1)$-transitiv auf $\Omega \setminus \{\omega\}$.

Sei nun G_ω (scharf) $(k-1)$-transitiv auf $\Omega \setminus \{\omega\}$. Seien $(\alpha_1, \ldots, \alpha_k), (\beta_1, \ldots, \beta_k) \in \Omega^k$ mit paarweise verschiedenen Elementen. Da φ transitiv ist, existieren $x, y \in G$ mit ${}^x\alpha_k = \omega = {}^y\beta_k$. Dann sind ${}^x\alpha_i, {}^y\beta_i \in \Omega \setminus \{\omega\}$ für $i = 1, \ldots, k-1$. Es existiert also (genau) ein $h \in G_\omega$ mit ${}^{hx}\alpha_i = {}^y\beta_i$ für $i = 1, \ldots, k$. Für $g := y^{-1}hx \in G$ gilt also ${}^g\alpha_i = \beta_i$ für $i = 1, \ldots, k$. Ist h eindeutig, so auch g. Also ist G (scharf) k-transitiv. □

Lemma 3.4.

(i) Ist $G \to S_n$ k-transitiv, so ist $n(n-1)\ldots(n-k+1) \mid |G|$.

(ii) Ist $G \to S_n$ scharf k-transitiv, so ist $|G| = n(n-1)\ldots(n-k+1)$.

(iii) Ist $\varphi : G \to S_n$ k-transitiv und $|G| = n(n-1)\ldots(n-k+1)$, so ist φ scharf k-transitiv.

Beweis. Wir beweisen (i) und (ii) durch Induktion nach k. Im Fall $k = 1$ folgt die Behauptung aus Beispiel 1.13 und Definition 1.20. Sei nun $k \geq 2$. Dann ist G transitiv und nach Lemma 3.3 ist G_1 (scharf) $(k-1)$-transitiv. Außerdem ist $|G : G_1| = n$. Somit folgt die Behauptung aus der Induktionsvoraussetzung. Teil (iii) ergibt sich ebenfalls aus einer einfachen Induktion. □

Satz 3.5. *Jede 2-transitive Operation ist primitiv.*

Beweis. Sei $\varphi : G \to \mathrm{Sym}(\Omega)$ eine 2-transitive Operation. Nehmen wir an, dass es einen Block $\Delta \subseteq \Omega$ gibt. Seien $\alpha, \beta \in \Delta$ mit $\alpha \neq \beta$ und $\gamma \in \Omega \setminus \Delta$. Nach Voraussetzung existiert ein $g \in G$ mit ${}^g\alpha = \alpha$ und ${}^g\beta = \gamma$. Insbesondere ist $\varnothing \neq \Delta \cap {}^g\Delta \neq \Delta$. Widerspruch. □

Satz 3.6. *Sei $1 \neq N \trianglelefteq G$ und $\varphi : G \to \mathrm{Sym}(N \setminus \{1\})$ die Operation durch Konjugation. Dann gilt:*

(i) Ist φ transitiv, so ist N eine elementarabelsche p-Gruppe.

(ii) Ist φ sogar 2-transitiv, so ist $p = 2$ oder $|N| = 3$.

(iii) Ist φ sogar 3-transitiv, so ist $|N| = 4$.

(iv) φ ist nie 4-transitiv.

Beweis. Sei p ein Primteiler von $|N|$ und $x \in N$ ein Element der Ordnung p (Satz von Cauchy, Algebra 1). Ist φ transitiv, so ist jedes nicht-triviale Element von N zu x konjugiert. Insbesondere ist $y^p = 1$ für alle $y \in N$. Also ist N eine p-Gruppe (Satz von Cauchy) und damit auflösbar. Außerdem ist N ein minimaler Normalteiler. Aus Satz 2.6 folgt (i).

Sei nun φ 2-transitiv und $p \neq 2$. Dann ist $x^{-1} \neq x$. Für jedes $g \in G$ mit $gxg^{-1} = x$ ist auch $gx^{-1}g^{-1} = x^{-1}$. Daher ist $N = \{1, x, x^{-1}\}$. Dies zeigt (ii). Ist φ 3-transitiv, so muss also $p = 2$ gelten, da $|N \setminus \{1\}| \geq 3$. Sei $U := \{1, a, b, c\} \leq N$. Dann ist $c = ab$. Für ein $g \in G$ mit ${}^ga = a$ und ${}^gb = b$ muss also auch ${}^gc = c$ gelten. Dies zeigt $U = N$ und (iii) folgt. Wäre die Operation 4-transitiv, so wäre $|N \setminus \{1\}| \geq 4$ im Widerspruch zu (iii). □

Satz 3.7. *Für $n \geq 5$ ist A_n einfach.*

Beweis. Sei $1 \neq N \trianglelefteq G := A_n$. Nach Beispiel 1.24 operiert A_n treu und primitiv auf $\Omega := \{1, \ldots, n\}$. Daher operiert N transitiv auf Ω nach Satz 2.2. Wir argumentieren nun durch Induktion nach n. Sei $n = 5$ (vgl. Algebra 1). Dann ist $5 \mid |N|$. Da $|G/N|$ nicht mehr durch 5 teilbar ist, muss N alle Elemente der Ordnung 5 enthalten, d. h. alle 5-Zyklen. Jeder 5-Zyklus lässt sich eindeutig in der Form $(1, a, b, c, d)$ mit $\{a, b, c, d\} = \{2, 3, 4, 5\}$ schreiben. Also gibt es genau $4! = 24$ solche Elemente, und wir erhalten $|N| \geq 24$. Wegen $|N| \mid |G|$ bleiben nur die Möglichkeiten $|N| \in \{30, 60\}$. Also ist $|G/N|$ auch nicht mehr durch 3 teilbar, und N muss auch alle 3-Zyklen enthalten. Von diesen gibt es $\binom{5}{3} \cdot 2! = 20$ Stück. Also ist $|N| \geq 24 + 20 = 44$ und somit $N = G$.

Sei nun $n \geq 6$ und die Behauptung für $n - 1$ bereits gezeigt. Der Stabilisator $G_n = A_{n-1}$ ist nach Induktion einfach. Nach Satz 1.19 ist $G = NG_n$. Wir können also $G_n \not\subseteq N$ annehmen. Insbesondere ist $N \cap G_n \lhd G_n$ und damit $N_n = N \cap G_n = 1$. Also operiert N regulär auf Ω und $|N| = n$. Nach Beispiel 3.2 und Lemma 3.3 operiert G_n $(n-3)$-transitiv auf $\Omega \setminus \{n\}$. Nach Satz 2.1 ist diese Operation isomorph zur Operation auf $N \setminus \{1\}$ durch Konjugation. Satz 3.6 liefert nun $n = 6$ und $|N| = 4$. Dies widerspricht aber $|N| = n$. □

Satz 3.8. *Ist G eine einfache Gruppe der Ordnung 60, so ist $G \cong A_5$.*

Beweis. Wir konstruieren zunächst eine Untergruppe $H \leq G$ vom Index 5. Sei $P \in \mathrm{Syl}_2(G)$. Offenbar ist $\mathrm{N}_G(P) < G$. Im Fall $|G : \mathrm{N}_G(P)| = 3$ gäbe es einen nicht-trivialen Homomorphismus $G \to S_3$ im Widerspruch zur Einfachheit von G. Wir können also $\mathrm{N}_G(P) = P$ annehmen (anderenfalls setze man $H := \mathrm{N}_G(P)$). Schneiden sich je zwei verschiedene 2-Sylowgruppen trivial, so besitzt die Vereinigung aller 2-Sylowgruppen 46 Elemente. Andererseits muss es nach Sylow aber mindestens sechs 5-Sylowgruppen geben, die sich ebenfalls trivial schneiden. Dieser Widerspruch zeigt, dass es ein $Q \in \mathrm{Syl}_2(G)$ mit $|P \cap Q| = 2$ gibt. Dann ist $P, Q \leq \mathrm{N}_G(P \cap Q)$. Man kann also $H := \mathrm{N}_G(P \cap Q)$ wählen.

Die Operation auf den Nebenklassen G/H liefert nun einen Monomorphismus $G \to S_5$. Da A_5 die einzige Untergruppe der Ordnung 60 in S_5 ist (Aufgabe 3.4), folgt $G \cong A_5$. □

Satz 3.9. *Sei G eine auflösbare k-transitive Permutationsgruppe. Dann ist $k \leq 4$. Im Fall $k = 4$ ist $G \cong S_4$ und im Fall $k = 3$ ist $G \in \{S_3, S_4\}$. In beiden Fällen ist die Operation scharf k-transitiv.*

Beweis. Wir können $k \geq 2$ annehmen. Nach Satz 3.5 ist G auch primitiv. Sei N ein minimaler Normalteiler von G. Wie üblich operiert N regulär auf Ω. Nach Satz 2.1 ist die Operation von G_ω ($\omega \in \Omega$) auf Ω isomorph zur Operation auf N durch Konjugation. Andererseits operiert G_ω $(k-1)$-transitiv auf $\Omega \setminus \{\omega\}$ nach Lemma 3.3. Nun folgt $k \leq 4$ aus Satz 3.6. Im Fall $k = 4$ ist $|N| = 4$ und $G \leq \mathrm{Sym}(\Omega) \cong S_4$. Wegen $4 \cdot 3 \cdot 2 \mid |G|$ folgt $G \cong S_4$.

Sei nun $k = 3$. Nach Satz 3.6 ist $|N| = 3$ oder N ist eine elementarabelsche 2-Gruppe. Im ersten Fall ist sicher $G \cong S_3$. Sei nun $|N| = 2^n$ für ein $n \geq 2$. Wie oben operiert G_ω 2-transitiv und somit primitiv auf $\Omega \setminus \{\omega\}$. Da G_ω auflösbar ist, besitzt G_ω einen minimalen Normalteiler der Ordnung $2^n - 1$. Insbesondere ist $2^n - 1 = q^m$ für eine Primzahl $q \geq 3$. Ist m gerade, so erhält man den Widerspruch $0 \equiv 2^n = q^m + 1 \equiv 2 \pmod 4$. Also ist m ungerade. Außerdem ist

$$2^n = q^m + 1 = (q+1)(q^{m-1} - q^{m-2} \pm \ldots + 1).$$

Der Faktor $q^{m-1} - q^{m-2} \pm \ldots + 1$ ist eine Summe aus m vielen ungeraden Zahlen und ist daher ungerade. Dies zeigt $q^{m-1} - q^{m-2} \pm \ldots + 1 = 1$ und $q = 2^n - 1$ ist eine Mersenne-Primzahl. Nach Satz 2.14 ist G_ω zu einer Untergruppe von $\mathrm{Aff}(1, q)$ isomorph. Insbesondere ist $|G_\omega| \mid q(q-1)$. Andererseits ist $q(q-1) \mid |G_\omega|$ nach Lemma 3.4. Dies zeigt $G_\omega \cong \mathrm{Aff}(1, q)$ und $|G| = 2^n(2^n - 1)(2^n - 2)$. Also ist G sogar scharf 3-transitiv nach Lemma 3.4. Wir betrachten nun G_ω als Untergruppe von $\mathrm{Aut}(N) \cong \mathrm{GL}(n, 2)$. Sei $Q \in \mathrm{Syl}_q(G_\omega)$. Wegen $|\mathrm{GL}(n,2)| = (2^n - 1)(2^n - 2)\ldots(2^n - 2^{n-1})$ ist $Q \in \mathrm{Syl}_q(\mathrm{GL}(n, 2))$ und $|Q| = q$. Insbesondere ist Q zum Singer-Zyklus $S \leq \mathrm{GL}(n, 2)$ (Beispiel 2.16) konjugiert. Also ist

$$(2^n - 1)(2^n - 2) = |G_\omega| = |\mathrm{N}_{G_\omega}(Q)| \mid |\mathrm{N}_{\mathrm{GL}(n,2)}(Q)| = |\mathrm{N}_{\mathrm{GL}(n,2)}(S)|. \tag{3.1}$$

Wir berechnen nun $\mathrm{N}_{\mathrm{GL}(n,2)}(S)$. Sei dafür $S = \langle f_\gamma \rangle$ mit $\gamma \in \mathbb{F}_{2^n}^\times$. Sei außerdem $\Phi \in \mathrm{N}_{\mathrm{GL}(n,2)}(S)$ mit $a := \Phi(1)$, wobei man für die Definition von 1 wieder N mit $\mathbb{F}_{2^n}$ identifiziert. Dann existiert ein $k \in \mathbb{Z}$ mit $\Phi \circ f_\gamma = f_\gamma^k \circ \Phi$. Für $i, j \in \mathbb{Z}$ ist

$$(f_{a^{-1}} \circ \Phi)(\gamma^i \gamma^j) = (f_{a^{-1}} \circ \Phi \circ f_\gamma^{i+j})(1) = (f_{a^{-1}} \circ f_\gamma^{(i+j)k})(a) = \gamma^{(i+j)k} = (f_{a^{-1}} \circ \Phi)(\gamma^i)(f_{a^{-1}} \circ \Phi)(\gamma^j).$$

Da jedes nicht-triviale Element in $\mathbb{F}_{2^n}$ die Form γ^i hat, muss $f_{a^{-1}} \circ \Phi$ ein Körperautomorphismus sein. Bekanntlich wird $\mathrm{Aut}(\mathbb{F}_{2^n})$ vom Frobenius-Automorphismus F erzeugt (Algebra 1). Also ist $\Phi \in \Gamma\mathrm{L}(1, 2^n)$ und $\mathrm{N}_{\mathrm{GL}(n,2)}(S) = \Gamma\mathrm{L}(1, 2^n)$. Wegen (3.1) ist $2^n - 2 \mid n$ und daher $n = 2$. Also hat G Grad 4 und $G \cong S_4$ wegen $|G| = 24$. Die letzte Behauptung ist klar. □

Beispiel 3.10.

(i) Wir haben in Beispiel 2.16 gesehen, dass $\Gamma\mathrm{L}(1, p^n)$ transitiv auf $V \setminus \{0\}$ operiert, wobei V eine elementarabelsche p-Gruppe vom Rang n ist. Nach Satz 2.12 operiert $V \rtimes \Gamma\mathrm{L}(1, p^n)$ also 2-transitiv auf V. Betrachtet man nur den Singer-Zyklus S, so ist $V \rtimes S$ sogar scharf 2-transitiv nach Lemma 3.4.

(ii) Huppert hat umgekehrt gezeigt, dass bis auf endlich viele Ausnahmen jede auflösbare 2-transitive Permutationsgruppe G in $V \rtimes \Gamma\mathrm{L}(1, p^n)$ enthalten ist. In den Ausnahmen ist $G \leq \mathrm{Aff}(n, p)$ (Satz 2.14) mit $p^n \in \{3^2, 5^2, 7^2, 11^2, 23^2, 3^4\}$.

Satz 3.11. *Sei G eine scharf 2-transitive Permutationsgruppe vom Grad n. Dann ist $n = p^m$ für eine Primzahl p und $G \cong \widetilde{G} \leq \mathrm{Aff}(m, p)$ mit $\mathbb{F}_p^m \trianglelefteq \widetilde{G}$.*

Beweis. Die Operation $G \to \mathrm{Sym}(\Omega)$ sei scharf 2-transitiv mit $|\Omega| = n$. Nach Satz 3.5 ist G primitiv. Um Satz 2.14 anzuwenden, müssen wir einen abelschen Normalteiler konstruieren. Sei $\omega \in \Omega$. Nach Lemma 3.3 operiert G_ω regulär auf $\Omega \setminus \{\omega\}$. Für $\omega' \in \Omega \setminus \{\omega\}$ ist also $G_\omega \cap G_{\omega'} = 1$. Folglich hat jedes nicht-triviale Element in G höchstens einen Fixpunkt. Sei $N := G \setminus \bigcup_{\omega \in \Omega} G_\omega \cup \{1\}$ die Menge der fixpunktfreien Permutationen plus Identität. Da sich je zwei verschiedene Stabilisatoren trivial schneiden, ist $|N| = |G| - n(|G_\omega| - 1) = n(n-1) - n(n-2) = n$ nach Lemma 3.4. Sei p ein Primteiler von n, und sei $x \in G$ ein nicht-triviales p-Element. Dann ist x ein disjunktes Produkt von nicht-trivialen Zyklen, deren Längen durch p teilbar sind. Wegen $p \mid n$ ist die Anzahl der Fixpunkte von x auch durch p teilbar. Also ist x fixpunktfrei, d. h. $x \in N$. Sei $y \in \mathrm{C}_G(x) \cap G_\omega$ für ein $\omega \in \Omega$. Dann ist $y \in G_\omega \cap xG_\omega x^{-1} = G_\omega \cap G_{{}^x\omega} = 1$, da ${}^x\omega \neq \omega$. Dies zeigt $\mathrm{C}_G(x) \subseteq N$. Die Anzahl der Konjugierten von x in G ist also

$$|G : \mathrm{C}_G(x)| \geq \frac{|G|}{|N|} = \frac{n(n-1)}{n} = n - 1.$$

Da jedes Konjugierte von x (als p-Element) auch in N liegt, folgt $N = \{gxg^{-1} : g \in G\} \cup \{1\}$ und $N = \mathrm{C}_G(x) \leq G$. Sicher ist auch $N \trianglelefteq G$. Da N eine p-Gruppe ist, existiert ein m mit $n = |N| = p^m$. Wegen

$$\mathrm{Z}(N) = \bigcap_{g \in G} \mathrm{C}_G(gxg^{-1}) = \bigcap_{g \in G} g\,\mathrm{C}_G(x)g^{-1} = \bigcap_{g \in G} gNg^{-1} = N$$

ist N auch abelsch. Die Behauptung folgt nun aus Satz 2.14. □

Bemerkung 3.12.

(i) Man nennt G *Frobeniusgruppe*, falls eine Untergruppe $1 < H < G$ mit $H \cap gHg^{-1} = 1$ für alle $g \in G \setminus H$ existiert. Ggf. heißt H *Frobeniuskomplement* von G. In der Situation von Satz 3.11 zeigt man leicht, dass G eine Frobeniusgruppe mit Komplement G_ω ist. Mit dem Satz von Frobenius (siehe Charaktertheorie) vereinfacht sich obiger Beweis. Man kann außerdem zeigen, dass jede p-Sylowgruppe von G_ω für $p > 2$ zyklisch ist (im Fall $p = 2$ kommen noch *Quaternionengruppen* in Frage; vgl. Aufgabe 3.3).

(ii) Zassenhaus hat unter Verwendung von Fastkörpern gezeigt, dass jede scharf 3-transitive Permutationsgruppe zu einer von zwei unendlichen Familien gehört (vgl. Aufgabe 3.2). Wir zeigen im Folgenden, dass es neben S_n und A_n nur wenige scharf k-transitive Permutationsgruppen mit $k \geq 4$ gibt.

Satz 3.13 (Jordan). *Sei G eine scharf k-transitive Permutationsgruppe vom Grad n mit $k \geq 4$. Dann ist $G \in \{S_n, A_n\}$ oder $(n, k) \in \{(11, 4), (12, 5)\}$.*

Beweis (Tits). Wir können $G \leq S_n$ annehmen und argumentieren durch Induktion nach k.

Induktionsanfang: $k = 4$.
Nach Voraussetzung ist $n \geq k = 4$ und $|G| = n(n-1)(n-2)(n-3)$. Im Fall $n \leq 6$ ist $|G| \in \{n!, \frac{1}{2}n!\}$. Es folgt dann leicht $G \in \{S_n, A_n\}$ (Aufgabe 3.4). Nehmen wir nun $n = 7$ an. Dann ist $|S_7 : G| = 6$. Die Operation von S_7 auf den Nebenklassen S_7/G liefert einen Homomorphismus $f : S_7 \to S_6$ mit $1 \neq \mathrm{Ker}(f) \subseteq G$. Nach Aufgabe 3.4 kann der Normalteiler $\mathrm{Ker}(f)$ nicht existieren. Also ist $n \geq 8$.

Die 4-Transitivität liefert ein Element

$$x = (1, 2)(3)(4) \ldots \in G$$

(die Darstellung der Einerzyklen ist diesmal wichtig). Da G sogar scharf 4-transitiv ist, haben alle nicht-trivialen Elemente höchstens drei Fixpunkte. Da x^2 mindestens vier Fixpunkte hat, ist x eine Involution. Sei F die Menge der Fixpunkte von x. Dann ist $|F| \in \{2, 3\}$ je nachdem, ob n gerade oder ungerade ist. Offenbar operiert $H := G_1 \cap \mathrm{C}_G(x)$ auf F. Nehmen wir an, dass $y \in H$ dabei trivial operiert. Wegen ${}^y2 = {}^{yx}1 = {}^{xy}1 = {}^x1 = 2$ hat y dann mindestens die Fixpunkte $1, 2, 3, 4$. Also ist $y = 1$ und H operiert treu auf F. Insbesondere ist $|H| \leq |\mathrm{Sym}(F)| \leq 6$. Wir zeigen, dass H transitiv auf $\Delta := \{5, \ldots, n\} \setminus F \neq \varnothing$ operiert. Seien dafür $\alpha, \beta \in \Delta$. Die 4-Transitivität liefert ein Element $g \in G_1 \cap G_2$ mit ${}^g\alpha = \beta$ und ${}^g({}^x\alpha) = {}^x\beta$. Da $gxg^{-1}x^{-1}$ mindestens die Fixpunkte $1, 2, \beta, {}^x\beta$ hat, ist $gxg^{-1} = x$ und $g \in G_1 \cap \mathrm{C}_G(x) = H$. Also ist H transitiv und $n = 2 + |F| + |\Delta| \leq 2 + |F| + |H| \leq 11$. Ist n gerade, so ist $|F| = 2 \geq |H|$. Dies widerspricht aber $n \geq 8$. Wir können daher $n = 9$ annehmen. Dann ist aber $|\Delta| = 4 \nmid |H|$.

Induktionsschritt: $k \geq 5$.
Nach Lemma 3.3 operiert G_n scharf $(k-1)$-transitiv auf $\{1, \ldots, n-1\}$. Ist $|G_n| \in \{(n-1)!, \frac{1}{2}(n-1)!\}$, so ist $|G| \in \{n!, \frac{1}{2}n!\}$ und $G \in \{S_n, A_n\}$. Wir können also $G_n \notin \{S_{n-1}, A_{n-1}\}$ annehmen. Nach Induktion ist $(n, k) \in \{(12, 5), (13, 6)\}$. Sei also $n = 13$. Für $P \in \mathrm{Syl}_{13}(G)$ ist dann $|P| = 13$. Die 12! Zyklen der Länge 13 in S_{13} verteilen sich auf 11! Sylowgruppen. Also ist $|\mathrm{N}_{S_{13}}(P)| = 13 \cdot 12$. Wegen $\mathrm{N}_G(P) \leq \mathrm{N}_{S_{13}}(P)$ existiert ein $d \mid 12$ mit $|G : \mathrm{N}_G(P)| = 11 \cdot 10 \cdot 9 \cdot 8 \cdot d$. Nach Sylow ist $3d \equiv |G : \mathrm{N}_G(P)| \equiv 1 \pmod{13}$. Also ist $d \equiv 9 \pmod{13}$ und man erhält den Widerspruch $d \nmid 12$. □

Lemma 3.14. *Sei $G = \langle H, x\rangle$ eine Permutationsgruppe auf $\Omega \ni \omega$. Dabei operiere $H \leq G$ k-transitiv auf $\Omega \setminus \{\omega\}$ mit $k \geq 2$ und ${}^x\omega \neq \omega$. Es existiere $y \in H$ und $\alpha \in \Omega \setminus \{\omega\}$ mit ${}^y\alpha \neq \alpha$, $x^2 = y^2 = (xy)^3 = 1$ und $xH_\alpha x = H_\alpha$. Dann operiert G $(k+1)$-transitiv auf Ω und $G_\omega = H$.*

Beweis. Wegen $H \subseteq G_\omega$ ist G_ω k-transitiv auf $\Omega \setminus \{\omega\}$. Wegen ${}^x\omega \neq \omega$ ist G offenbar auch transitiv auf Ω. Aus Lemma 3.3 folgt, dass G $(k+1)$-transitiv operiert. Es bleibt zu zeigen: $G_\omega \subseteq H$.

Für $K := H \cup HxH$ ist $K^{-1} := \{g^{-1} : g \in K\} = K$ wegen $x^{-1} = x$. Sei $z \in H \setminus H_\alpha$. Wegen $k \geq 2$ operiert H_α transitiv auf $\Omega \setminus \{\omega, \alpha\}$. Also existiert ein $h \in H_\alpha$ mit ${}^{hz}\alpha = {}^y\alpha$. Es folgt $y^{-1}hz \in H_\alpha$ und $z \in H_\alpha y H_\alpha$. Dies zeigt $H = H_\alpha \cup H_\alpha y H_\alpha$. Die Relationen $x^2 = y^2 = (xy)^3 = 1$ implizieren $xyx = yxy$. Nach Voraussetzung erhalten wir

$$xHx = xH_\alpha x \cup xH_\alpha yH_\alpha x = H_\alpha \cup H_\alpha xyxH_\alpha = H_\alpha \cup H_\alpha yxyH_\alpha \subseteq H \cup HxH = K.$$

Für $g, g' \in HxH$ ist also $gg' \in HxHxH \subseteq HKH \subseteq K$. Dies zeigt $K \leq G$. Wegen $x \in K$ ist sogar $G = \langle H, x\rangle = K$. Für jedes $g \in G \setminus H \subseteq HxH$ ist also ${}^g\omega \neq \omega$. Dies zeigt die Behauptung. □

Lemma 3.15 (Witt)**.** *Sei H eine 2-transitive Permutationsgruppe auf $\Omega := \{4, \ldots, n\} \ni \omega$, und sei $x \in H \setminus H_\omega$ eine Involution. Seien $a, b, c \in \mathrm{N}_{S_n}(H_\omega)$ Involutionen mit*

$$a = (1,\omega)(2)(3)\ldots, \qquad b = (1,2)(3)(\omega)\ldots, \qquad c = (2,3)(1)(\omega)\ldots$$

und

$$(ax)^3 = (ba)^3 = (cb)^3 = 1, \qquad (xb)^2 = (xc)^2 = (ac)^2 = 1.$$

Dann ist $G := \langle H, a, b, c\rangle$ 5-transitiv auf $\{1, \ldots, n\}$ und $G_1 \cap G_2 \cap G_3 = H$.

Beweis. Nach Lemma 3.14 ist $K := \langle H, a\rangle$ 3-transitiv auf $\Omega \cup \{1\}$ und $K_1 = H$. Nach Satz 3.5 operiert H primitiv auf Ω. Insbesondere ist $H_\omega < H$ maximal und $H = \langle H_\omega, x\rangle$. Aus $x^2 = (xb)^2 = b^2 = 1$ folgt $xb = bx$. Insbesondere ist $bK_1b = bHb = \langle bH_\omega b, x\rangle = \langle H_\omega, x\rangle = H = K_1$. Eine weitere Anwendung von Lemma 3.14 zeigt, dass $L := \langle K, b\rangle$ 4-transitiv auf $\Omega \cup \{1, 2\}$ operiert mit $L_2 = K$. Aus den Relationen folgt nun wieder $ac = ca$ und $xc = cx$. Also ist

$$cL_2c = cKc = \langle cHc, a\rangle = \langle cH_\omega c, x, a\rangle = \langle H_\omega, x, a\rangle = K = L_2.$$

Eine dritte Anwendung von Lemma 3.14 ergibt schließlich, dass $G = \langle L, c\rangle$ 5-transitiv auf $\{1, \ldots, n\}$ operiert mit $G_3 = L$. Damit ist auch $G_1 \cap G_2 \cap G_3 = G_1 \cap L_2 = G_1 \cap K = K_1 = H$. □

Satz 3.16 (Mathieu)**.** *Sei*

$$a = (1,4)(7,8)(9,11)(10,12), \quad b = (1,2)(7,10)(8,11)(9,12), \quad c = (2,3)(7,12)(8,10)(9,11),$$
$$d = (4,5,6)(7,8,9)(10,11,12), \quad e = (4,7,10)(5,8,11)(6,9,12), \quad f = (5,7,6,10)(8,9,12,11),$$
$$g = (5,8,6,12)(7,11,10,9).$$

Dann ist $M_{12} := \langle a, b, c, d, e, f, g\rangle \leq S_{12}$ scharf 5-transitiv vom Grad 12 und $M_{11} := \langle a, b, d, e, f, g\rangle$ ist scharf 4-transitiv vom Grad 11.

Beweis. Da d die drei Zyklen von e permutiert, ist $E := \langle d, e\rangle$ elementarabelsch der Ordnung 9. Außerdem operiert E regulär auf $\Omega := \{4, \ldots, 12\}$. Offenbar ist $f^2 = g^2$ eine Involution und $fgf^{-1} = g^{-1}$. Für $Q := \langle f, g\rangle$ gilt also $\langle g\rangle \trianglelefteq Q$ und $|Q : \langle g\rangle| = 2$. Also ist $|Q| = 8$ (Q ist eine Quaternionengruppe). Eine Rechnung zeigt $fdf^{-1} = e$, $gdg^{-1} = (4,8,12)(11,6,7)(9,10,5) = de$, $fef^{-1} = d^{-1}$ und $geg^{-1} = (4,11,9)(8,6,10)(12,7,5) = de^{-1}$. Also ist $Q \subseteq \mathrm{N}_{S_{12}}(E)$ und $H := EQ \leq S_{12}$. Aus Ordnungsgründen ist $E \cap Q = 1$ und somit $|H| = |E||Q| = 9 \cdot 8$. Da E regulär auf Ω operiert, ist $H_4 = E_4Q = Q$. Man sieht leicht, dass Q transitiv auf $\Omega \setminus \{4\}$ operiert. Also ist H 2-transitiv auf Ω nach Lemma 3.3. Wegen $|H| = 9 \cdot 8$ und $|\Omega| = 9$ ist die Operation sogar scharf 2-transitiv. Wir wollen nun Lemma 3.15 mit $\omega = 4$ und

$$x := df^2d^{-1} = d(5,6)(7,10)(8,12)(9,11)d^{-1} = (4,6)(7,12)(8,11)(9,10) \in H \setminus H_4$$

anwenden. Dafür müssen wir zunächst $a, b, c \in \mathrm{N}_{S_{12}}(H_4) = \mathrm{N}_{S_{12}}(Q)$ zeigen:

$$afa^{-1} = g, \qquad aga^{-1} = a^2fa^{-2} = f, \qquad bfb^{-1} = f^{-1},$$
$$bgb^{-1} = (5,11,6,9)(7,12,10,8) = gf, \qquad cfc^{-1} = g^{-1}, \qquad cgc^{-1} = c^2f^{-1}c^{-2} = f^{-1}.$$

Die Relationen aus Lemma 3.15 überprüft man wie folgt:

$$ax = (1,4,6)(7,10,11)(8,9,12), \qquad ba = (1,4,2)(7,11,12)(8,10,9), \qquad cb = (1,3,2)(7,8,9)(10,12,11),$$
$$xb = (1,2)(4,6)(7,9)(10,12), \qquad xc = (2,3)(4,6)(8,9)(10,11), \qquad ac = (1,4)(2,3)(7,10)(8,12).$$

Also ist $G := \langle H, a, b, c\rangle = M_{12}$ 5-transitiv vom Grad 12 und $G_1 \cap G_2 \cap G_3 = H$. Da H scharf 2-transitiv auf Ω operiert, ist $G_1 \cap G_2 \cap G_3 \cap G_4 \cap G_5 = H_4 \cap H_5 = 1$. Dies zeigt, dass G sogar scharf 5-transitiv ist. Im Beweis von Lemma 3.15 ergab sich $G_3 = M_{11}$. Nach Lemma 3.3 ist M_{11} also scharf 4-transitiv vom Grad 11. □

Definition 3.17. Man nennt M_{11} und M_{12} die *Mathieugruppen* vom Grad 11 bzw. 12. Aus Lemma 3.4 ergibt sich $|M_{11}| = 11 \cdot 10 \cdot 9 \cdot 8 = 7.920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11$ und $|M_{12}| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 = 95.040 = 2^6 \cdot 3^3 \cdot 5 \cdot 11$.

Satz 3.18. *Die Gruppen M_{11} und M_{12} sind einfach.*

Beweis. Sei zunächst $G = M_{11}$ und $P \in \mathrm{Syl}_{11}(G)$. In S_{11} gibt es 10! Elemente der Ordnung 11, die sich auf 9! Sylowgruppen verteilen. Also ist $|\mathrm{N}_{S_{11}}(P)| = 11 \cdot 10$ und $|\mathrm{N}_G(P) : P| \mid 10$. Nach Sylow ist

$$5 \equiv 10 \cdot 9 \cdot 8 = \frac{|G|}{11} = |G : \mathrm{N}_G(P)||\mathrm{N}_G(P) : P| \equiv |\mathrm{N}_G(P) : P| \pmod{11}$$

und somit $|\mathrm{N}_G(P) : P| = 5$ und $|G : \mathrm{N}_G(P)| = 16 \cdot 9$. Sei nun $1 \neq N \trianglelefteq G$. Dann ist N transitiv und alle 11-Sylowgruppen von G liegen in N. Insbesondere ist $|N : \mathrm{N}_N(P)| = 16 \cdot 9$. Dies zeigt $|G : N| \leq 5$. Nehmen wir $|G : N| = 5$ an. Dann besitzt N genau $16 \cdot 9 \cdot 10$ Elemente der Ordnung 11. Die übrigen $|N|/11$ Elemente müssen dann den Stabilisator N_1 bilden. Insbesondere ist $N_1 = \ldots = N_{11}$. Dann kann N aber nicht treu operieren. Also ist $G = N$, und G ist einfach.

Sei nun $G = M_{12}$, und sei N ein minimaler Normalteiler von G. Nach Konstruktion ist $G_3 = M_{11}$ einfach und maximal in G, da G primitiv ist. Es folgt $G_3 \cap N \in \{1, G_3\}$. Wir können $N < G$ annehmen. Im Fall $G_3 \subseteq N$ ist $G_3 = N$ wegen der Maximalität von G_3. Dann kann N aber nicht transitiv operieren. Also ist $G_3 \cap N = 1$ und $|N| = |N : G_3 \cap N| = |NG_3 : G_3| = |G : G_3| = 12$. Dies widerspricht Satz 2.6. □

Bemerkung 3.19. Die Mathieugruppen M_{11} und M_{12} sind die beiden kleinsten *sporadisch* einfachen Gruppen. Dies sind 26 Ausnahmen, die nicht zu unendlichen Familien von einfachen Gruppen (wie A_n) gehören.

Satz 3.20. *Sei G eine scharf k-transitive Permutationsgruppe vom Grad n mit $k \geq 4$. Dann gilt eine der folgenden Aussagen:*

(i) $n \in \{k, k+1\}$ *und* $G \cong S_n$.

(ii) $n = k + 2$ *und* $G \cong A_n$.

(iii) $(n, k) = (11, 4)$ *und* $G \cong M_{11}$.

(iv) $(n, k) = (12, 5)$ *und* $G \cong M_{12}$.

In allen Fällen ist die Operation bis auf Isomorphie eindeutig.

Beweis. Im Fall $G \cong S_n$ ist $|G| = n!$. Andererseits ist $|G| = n(n-1)\ldots(n-k+1)$. Dies zeigt $n \in \{k, k+1\}$. Der Fall $G \cong A_n$ ist analog. Da S_n und A_n die einzigen Untergruppen der Ordnung $n!$ bzw. $n!/2$ in S_n sind, ist die Operation bis auf Isomorphie eindeutig (Aufgabe 1.4). Nach Satz 3.13 können wir also $(n, k) \in \{(11, 4), (12, 5)\}$ annehmen.

Sei zunächst $G \leq S_{11}$ eine scharf 4-transitive Permutationsgruppe. Um zu zeigen, dass G in S_{11} zu M_{11} konjugiert ist (Aufgabe 1.4), genügt es zu zeigen, dass G bis auf Umnummerierung der Ziffern $1, \ldots, 11$ eindeutig bestimmt ist. Wie in Satz 3.18 zeigt man, dass G einfach ist. Im Fall $G \not\leq A_{11}$ wäre $1 \neq G \cap A_{11} \lhd G$ im Widerspruch zur Einfachheit von G. Also ist $G \leq A_{11}$. Wegen $|G| = 11 \cdot 10 \cdot 9 \cdot 8$ enthält G einen 11-Zyklus, sagen wir

$$x := (1, \ldots, 11).$$

Dann ist $P := \langle x\rangle \in \mathrm{Syl}_{11}(G)$. Wie in Satz 3.18 ist $|\mathrm{N}_G(P)| = 11 \cdot 5$ und $\mathrm{N}_G(P) = \mathrm{N}_{A_{11}}(P)$. Sei also

$$y := (1,4,5,9,3)(2,8,10,7,6) \in \mathrm{N}_G(P)$$

mit $yxy^{-1} = x^4$. Dann ist $Q := \langle y \rangle \in \mathrm{Syl}_5(G)$. Man sieht leicht, dass $\mathrm{C}_{A_{11}}(Q) = \langle (1,4,5,9,3), (2,8,10,7,6) \rangle$ gilt. Wegen $25 \nmid |G|$ ist $\mathrm{C}_G(Q) = Q$. Wie üblich ist $\mathrm{N}_G(Q)/Q \leq \mathrm{Aut}(Q) \cong (\mathbb{Z}/5\mathbb{Z})^\times \cong C_4$. Andererseits ist $|G : \mathrm{N}_G(Q)| \equiv 1 \pmod 5$ nach Sylow. Es folgt $|\mathrm{N}_G(Q)| = 20$ und $\mathrm{N}_G(Q)/Q$ ist zyklisch. Wir wählen ein Element $z \in \mathrm{N}_G(Q)$ der Ordnung 4 mit $zyz^{-1} = y^2$. Dann ist $z(1,4,5,9,3)z^{-1} \in \{(1,5,3,4,9), (2,10,6,8,7)\}$. Nehmen wir zunächst an, dass der zweite Fall eintritt. Dann hat z keine Fixpunkte auf $\{1, \ldots, 10\}$. Da $z^2 \neq 1$ höchstens drei Fixpunkte hat, muss z Zyklentyp $(4,4,2)$ haben. Insbesondere ist z eine ungerade Permutation im Widerspruch zu $G \leq A_{11}$. Also ist $z(1,4,5,9,3)z^{-1} = (1,5,3,4,9)$ und $z(2,8,10,7,6)z^{-1} = (2,10,6,8,7)$. Indem man z durch ein zy^i ersetzt, kann man

$$z = (3,9,4,5)z' \qquad \text{mit} \qquad z' \in \{(2,10,8,6), (2,6,10,7), (6,7,8,10), (2,8,7,10), (2,7,6,8)\}.$$

annehmen. Wir zeigen, dass die letzten drei von diesen fünf Möglichkeiten nicht in Frage kommen. Dafür berechnet man:

$$\begin{aligned} x^{-1}(3,9,4,5)(6,7,8,10) &= (1,11,10,5,2)(3,8,9), \\ x((3,9,4,5)(2,8,7,10))^2 &= (1,2,8,11)(3,5,10,9,6,7), \\ x(3,9,4,5)(2,7,6,8) &= (1,2,8,3,10,11)(4,6,9,5). \end{aligned}$$

Man sieht sofort, dass geeignete nicht-triviale Potenzen dieser Elemente mehr als drei Fixpunkte haben. Also ist $z = (3,9,4,5)(2,10,8,6)$ oder $z = (3,9,4,5)(2,6,10,7)$. Wir betrachten nun

$$g := (1,7,5,2,3,10,4,6,9,8) \in S_{11}.$$

Dann ist $gxg^{-1} = x^8$ und damit $g \in \mathrm{N}_{S_{11}}(P)$. Außerdem bildet g durch Konjugation den zweiten Kandidaten von z auf den ersten ab. Nach Konjugation mit g können wir also

$$z = (3,9,4,5)(2,10,8,6)$$

annehmen (dabei bleibt die bereits gefundene Gruppe $\mathrm{N}_G(P) = \mathrm{N}_{A_{11}}(P) \trianglelefteq \mathrm{N}_{S_{11}}(P)$ erhalten). Also enthält G die Untergruppe $H := \langle x, y, z \rangle = \langle \mathrm{N}_G(P), \mathrm{N}_G(Q) \rangle$ mit $11 \cdot 5 \cdot 4 \mid |H|$. Wegen $|H : \mathrm{N}_G(P)| = |H : \mathrm{N}_H(P)| \equiv 1 \pmod{11}$ und $|H : \mathrm{N}_G(P)| \mid |G : \mathrm{N}_G(P)| = 9 \cdot 16$ können wir $|H| = 11 \cdot 5 \cdot 12$ annehmen (anderenfalls ist $H = G$). Dies liefert aber den Widerspruch $33 = |H : \mathrm{N}_G(Q)| = |H : \mathrm{N}_H(Q)| \equiv 1 \pmod 5$. Also ist $G = H$ eindeutig bestimmt.

Sei schließlich $G \leq S_{12}$ scharf 5-transitiv. Dann ist G_{12} scharf 4-transitiv. Nach dem eben Gezeigten ist $G_{12} \cong M_{11}$. Durch Konjugation können wir annehmen, dass $G_{12} = \langle x, y, z \rangle$ wie oben gegeben ist. Die 5-Transitivität liefert nun ein Element

$$g := (2)(3,4)(5,9)\ldots \in G.$$

Wegen $g \in G_2 \cong M_{11} \leq A_{11}$ ist g ein disjunktes Produkt von vier Transpositionen. Insbesondere hat g genau vier Fixpunkte. Da $gz^2 \neq 1$ die Fixpunkte $3,4,5,9$ hat, hat g die Fixpunkte $2,6,8,10$. Dies ergibt drei Möglichkeiten:

$$g \in \{(3,4)(5,9)(1,7)(11,12),\ (3,4)(5,9)(1,11)(7,12),\ (3,4)(5,9)(1,12)(7,11)\}.$$

In den ersten beiden Fällen ist

$$\begin{aligned} y(3,4)(5,9)(1,7)(11,12) &= (1,6,2,8,10,7,4)(3,5)(11,12), \\ x^3(3,4)(5,9)(1,11)(7,12) &= (1,3,7,12,10,2,5)(4,6,9,8,11). \end{aligned}$$

Wegen $7 \nmid |G|$ ist also

$$g = (3,4)(5,9)(1,12)(7,11) \in G$$

und aus der Maximalität von G_{12} folgt $G = \langle x, y, z, g \rangle$. □

Bemerkung 3.21. Man kann Lemma 3.15 auch verwenden, um die größeren einfachen Mathieugruppen M_{22}, M_{23} und M_{24} zu konstruieren (siehe Theorem 21.10 in [Passman]). Dabei ist $H = \mathrm{PSL}(3,4) := \mathrm{SL}(3,4)/\mathrm{Z}(\mathrm{SL}(3,4))$ eine Permutationsgruppe auf den 21 eindimensionalen Untervektorräumen von $\mathbb{F}_4^3$. Da man heutzutage die Existenz und Eigenschaften dieser Gruppen leicht mit Computer verifizieren kann, verzichten wir auf einen theoretischen Beweis. Manchmal definiert man noch die Mathieugruppen M_{10}, $M_9 \cong C_3^2 \rtimes Q_8$, $M_{21} \cong \mathrm{PSL}(3,4)$ und $M_{20} \cong C_2^4 \rtimes A_5$ als Stabilisator von M_{11} (bzw. M_{10}, M_{22}, M_{21}). Diese liefern aber keine sporadisch einfachen Gruppen. Mit Hilfe der Klassifikation der endlichen einfachen Gruppen (CFSG) kann man folgenden Satz beweisen.

Satz 3.22. *Sei G eine 4-transitive Permutationsgruppe. Dann gilt eine der folgenden Aussagen:*

(i) $G \cong S_n$ *mit* $n \geq 4$.

(ii) $G \cong A_n$ *mit* $n \geq 6$.

(iii) $G \in \{M_{11}, M_{23}\}$ *und die Operation ist nicht 5-transitiv.*

(iv) $G \in \{M_{12}, M_{24}\}$ *und die Operation ist 5-transitiv, aber nicht 6-transitiv.* □

Aufgabe 3.1. Zeigen Sie, dass eine transitive Permutationsgruppe G auf Ω genau dann 2-transitiv ist, falls $G = G_\omega \cup G_\omega g G_\omega$ für $\omega \in \Omega$ und $g \in G \setminus G_\omega$ gilt.

Aufgabe 3.2. Zeigen Sie, dass $\mathrm{SL}(2, 2^n)$ scharf 3-transitiv auf der Menge der eindimensionalen Untervektorräume von $\mathbb{F}_{2^n}^2$ operiert.

Aufgabe 3.3. Sei G eine scharf 2-transitive Permutationsgruppe auf Ω. Zeigen Sie, dass G_ω für $\omega \in \Omega$ höchstens eine Involution besitzt. Im Fall $|G_\omega| \equiv 0 \pmod 2$ ist also $\mathrm{Z}(G_\omega) \neq 1$.

Aufgabe 3.4. Bestimmen Sie alle Normalteiler von S_n.

Aufgabe 3.5. Zeigen Sie, dass A_5 eine primitive Permutationsgruppe vom Grad 5, 6 und 10 ist.

Aufgabe 3.6. Zeigen Sie: Sind $H, K \leq \mathrm{Aut}(N)$ konjugiert in $\mathrm{Aut}(N)$, so ist $N \rtimes H \cong N \rtimes K$.

Aufgabe 3.7. Zeigen Sie, dass die unendliche Gruppe $A_\infty := \bigcup_{i=1}^{\infty} A_i$ einfach ist.

Aufgabe 3.8. Sei $\varphi : G \to \mathrm{Sym}(\Omega)$ eine Operation.

- φ heißt *k-primitiv* für $k \geq 1$, falls φ primitiv ist und im Fall $k > 1$ ein Stabilisator G_ω $(k-1)$-primitiv auf $\Omega \setminus \{\omega\}$ operiert.
- φ heißt *$\frac{1}{2}$-transitiv*, falls $|\Omega| = 1$ oder alle Bahnen von G die gleiche Länge > 1 haben.
- φ heißt *$(k + \frac{1}{2})$-transitiv* für $k \geq 1$, falls $|\Omega| \geq k + 1$, G transitiv operiert und G_ω für ein $\omega \in \Omega$ $(k - \frac{1}{2})$-transitiv auf $\Omega \setminus \{\omega\}$ operiert.
- φ heißt *semiregulär* (oder *frei*), falls $G_\omega = 1$ für alle $\omega \in \Omega$.
- φ heißt *quasiprimitiv*, falls jeder nicht-triviale Normalteiler von G transitiv operiert.

Zeigen Sie für $G \neq 1$:

(i) $(k+1)$-transitiv $\Longrightarrow$ k-primitiv $\Longrightarrow$ k-transitiv $(k \geq 1)$

(ii) $(k + \frac{1}{2})$-transitiv $\Longrightarrow$ k-transitiv $\Longrightarrow$ $(k - \frac{1}{2})$-transitiv $(k \geq 1)$

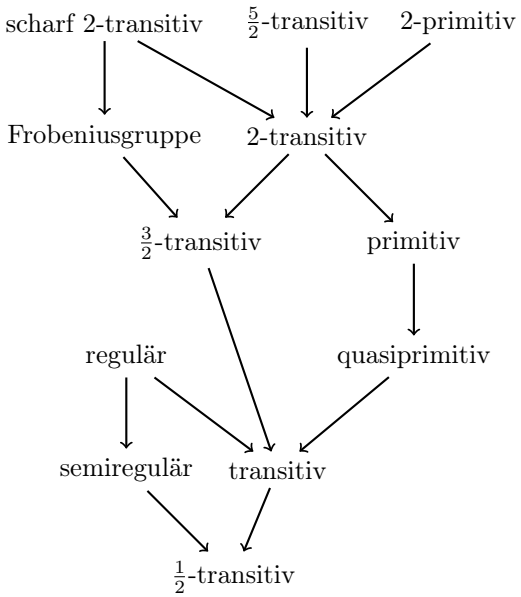
(iii) regulär $\Longrightarrow$ semiregulär $\Longrightarrow$ $\frac{1}{2}$-transitiv

(iv) primitiv+treu $\Longrightarrow$ quasiprimitiv $\Longrightarrow$ transitiv

(v) $\frac{3}{2}$-transitiv $\not\Longrightarrow$ primitiv $\not\Longrightarrow$ $\frac{3}{2}$-transitiv

(vi) Sei φ transitiv und $N \trianglelefteq G$. Dann operiert N trivial oder $\frac{1}{2}$-transitiv.

(vii) Ist H ein Frobeniuskomplement in G, so operiert G $\frac{3}{2}$-transitiv auf G/H.



Aufgabe 3.9. Sei $1 \neq N \trianglelefteq G$ und $\varphi : G \to \mathrm{Sym}(N \setminus \{1\})$ die Operation durch Konjugation. Zeigen Sie:

(i) Ist φ $\frac{3}{2}$-transitiv oder primitiv, so ist N eine elementarabelsche 2-Gruppe oder $|N| = 3$.

(ii) Ist φ 2-primitiv, so ist $|N| \in \{3, 4\}$.

(iii) Ist φ $\frac{5}{2}$-transitiv, so ist $|N| = 4$.

4 Konstruktion primitiver Gruppen mit vorgegebenem Sockel

Satz 4.1 (Baer)**.** *Sei G eine primitive Permutationsgruppe. Dann gilt eine der folgenden Aussagen:*

(i) G hat genau einen minimalen Normalteiler N und $\mathrm{C}_G(N) = N$ ist regulär.

(ii) G hat genau einen minimalen Normalteiler N und $\mathrm{C}_G(N) = 1$.

(iii) G hat genau zwei minimale Normalteiler N und $M = \mathrm{C}_G(N) \cong N$ und beide sind regulär.

Beweis. Die Gruppe G operiere treu und primitiv auf Ω. Sei N ein minimaler Normalteiler von G. Nehmen wir zunächst $\mathrm{C}_G(N) = 1$ an. Für einen weiteren minimalen Normalteiler M wäre $N \cap M = 1$ und $M \subseteq \mathrm{C}_G(N) = 1$. Also gilt (ii) und wir können nun $\mathrm{C}_G(N) \neq 1$ annehmen. Im Fall $N \subseteq \mathrm{C}_G(N)$ ist N abelsch und (i) gilt nach Satz 2.14. Es genügt also den Fall $M := \mathrm{C}_G(N) \trianglelefteq G$ mit $N \cap M = 1$ zu untersuchen. Sei $\omega \in \Omega$ und $y \in N$. Dann ist $M_\omega = yM_\omega y^{-1} = M_{y\omega}$. Da N transitiv auf Ω operiert, ist $M_\omega = 1$ und M ist regulär. Ist nun K ein minimaler Normalteiler von G mit $K \leq M$, so ist K transitiv und $|\Omega| \leq |K| \leq |M| = |\Omega|$. Dies zeigt, dass $M = K$ minimal ist. Die gleiche Argumentation mit M anstelle von N liefert einen regulären minimalen Normalteiler $\mathrm{C}_G(M)$ mit $N \subseteq \mathrm{C}_G(M)$. Also ist auch $N = \mathrm{C}_G(M)$ regulär. Ist nun K ein dritter minimaler Normalteiler, so ist $K \cap N = 1$ und man erhält den Widerspruch $K \subseteq \mathrm{C}_G(N) = M$. Es bleibt zu zeigen, dass N und M isomorph sind. Dafür betrachten wir den Stabilisator $S := (NM)_\omega$ in NM. Es gilt $S \cap N = N_\omega = 1 = M_\omega = S \cap M$ und $NM = NS = MS$ nach Satz 1.19. Also ist

$$N \cong N/N \cap M \cong NM/M = MS/M \cong S/S \cap M \cong S \cong S/S \cap N \cong NS/N = NM/N \cong M/M \cap N \cong M. \quad \square$$

Definition 4.2. Das Produkt aller minimalen Normalteiler von G bezeichnet man als *Sockel* $\mathrm{Soc}(G)$.

Bemerkung 4.3. Nach Satz 2.6 und Satz 4.1 ist der Sockel einer primitiven Permutationsgruppe eine direkte Summe isomorpher einfacher Gruppen. Wir konstruieren nun primitive Permutationsgruppen mit vorgegebenem Sockel. Ist $\mathrm{Soc}(G)$ nichtabelsch, so ist $\mathrm{C}_G(\mathrm{Soc}(G)) = 1$ nach Satz 4.1. Also ist $G \cong \mathrm{N}_G(\mathrm{Soc}(G))/\mathrm{C}_G(\mathrm{Soc}(G)) \leq \mathrm{Aut}(\mathrm{Soc}(G))$.

Lemma 4.4. *Sei $G = T_1 \oplus \ldots \oplus T_k$ mit nichtabelschen einfachen Gruppen $T_1 \cong \ldots \cong T_k$. Sei $\pi_i : G \to T_i$ die i-te Projektion.*

(i) Sei $H \leq G$ mit $\pi_i(H) = T_i$ für $i = 1, \ldots, k$. Dann existiert eine Partition $\{1, \ldots, k\} = I_1 \dot\cup \ldots \dot\cup I_l$, sodass $H = D_1 \oplus \ldots \oplus D_l$ mit $D_i \leq \bigoplus_{j \in I_i} T_j$ und $\mathrm{Ker}(\pi_j) \cap D_i = 1$ für alle $j \in I_i$. Insbesondere ist $H \cong T_1^l$.

(ii) Jeder Normalteiler von G hat die Form $\bigoplus_{i \in I} T_i$ für ein $I \subseteq \{1, \ldots, k\}$.

(iii) $T_1, \ldots, T_k$ sind die einzigen minimalen Normalteiler von G.

Beweis.

(i) Induktion nach k: Der Fall $k = 1$ ist klar. Sei also $k \geq 2$. Sei $I \subseteq \{1, \ldots, k\}$ minimal mit der Eigenschaft $D := H \cap \bigoplus_{i \in I} T_i \neq 1$. Im Fall $\mathrm{Ker}(\pi_j) \cap D \neq 1$ für ein $j \in I$ wäre $H \cap \bigoplus_{i \in I \setminus \{j\}} T_i \neq 1$ im Widerspruch zur Minimalität von I. Also ist $\mathrm{Ker}(\pi_i) \cap D = 1$ für alle $i \in I$. Außerdem ist $D \trianglelefteq H$ wegen $T_i \trianglelefteq G$. Wir können also $I_1 := I$ und $D_1 := D$ setzen. Im Fall $|I| = k$ sind wir fertig. Sei also $|I| < k$ und o. B. d. A. $1 \in I$. Für $i \in I$ ist $\pi_i(D) \trianglelefteq \pi_i(H) = T_i$ nach Voraussetzung. Da T einfach ist, folgt $\pi_i(D) = T_i$. Sei nun $x \in H$ beliebig und $x_1 := \prod_{i \in I} \pi_i(x)$. Wir wollen $x_1 \in D$ zeigen. Nehmen wir $x_1 \notin D$ an. Wegen $\pi_1(D) = T_1$ existiert ein $y \in D$ mit $\pi_1(xy) = 1$. Ersetzt man also x durch xy, so kann man $\pi_1(x) = 1$ annehmen. Sei o. B. d. A. $2 \in I$ und $\pi_2(x) \neq 1$. Wegen $\mathrm{Z}(T_2) = 1$ existiert ein $z \in T_2 \setminus \mathrm{C}_G(\pi_2(x))$. Sei $y \in D$ mit $\pi_2(y) = z$. Wegen $D \trianglelefteq H$ gilt $w := xyx^{-1}y^{-1} \in D$. Allerdings ist $\pi_1(w) = 1$ und $\pi_2(w) \neq 1$ im Widerspruch zu

$\mathrm{Ker}(\pi_1) \cap D = 1$. Wir also gezeigt, dass $\prod_{i\in I} \pi_i(x) \in D$ für alle $x \in H$ gilt. Für $\overline{D} := \bigcap_{i\in I} \mathrm{Ker}(\pi_i) \cap H \trianglelefteq H$ ist also $H = D\overline{D}$ und $D \cap \overline{D} = 1$. Für $j \in \{1, \dots, k\} \setminus I$ ist sicher $\pi_j(\overline{D}) = \pi_j(H) = T_j$. Man kann also die Induktionsvoraussetzung auf $\overline{D}$ anwenden. Damit folgt die erste Behauptung. Da $\pi_j : D_i \to T_j$ für $j \in I_i$ ein Isomorphismus ist, folgt auch die zweite Behauptung.

(ii) Sei $g \in N \trianglelefteq G$ mit $\pi_i(g) \neq 1$ für ein $i \in \{1, \dots, k\}$. Wegen $\mathrm{Z}(T_i) = 1$ existiert ein $x \in T_i \setminus \mathrm{C}_G(\pi_i(g))$. Es folgt $1 \neq x\pi_i(g)x^{-1}\pi_i(g)^{-1} = xgx^{-1}g^{-1} \in N \cap T_i$. Also ist $1 \neq N \cap T_i \trianglelefteq T_i$, und die Einfachheit von T_i zeigt $T_i \subseteq N$. Dies liefert die Behauptung.

(iii) Folgt aus (ii). □

Bemerkung 4.5. Untergruppen H wie in Lemma 4.4(i) nennt man *subdirekte Produkte*.

Lemma 4.6. *Seien $N_1, \dots, N_k$ paarweise verschiedene Normalteiler von G mit $\bigcap_{i=1}^{k} N_i = 1$, sodass $G/N_1 \cong \dots \cong G/N_k =: S$ nichtabelsch und einfach ist. Dann ist $G \cong S^k$.*

Beweis. Der Fall $k = 1$ ist klar. Sei $k \geq 2$ und $M := \bigcap_{i=1}^{k-1} N_i$. Für $H \leq G$ sei $\overline{H} := HM/M$. Dann ist $\overline{G}/\overline{N_i} \cong G/N_i \cong S$ für $i = 1, \dots, k-1$. Nach Induktion ist also $\overline{G} \cong S^{k-1}$. Nach Lemma 4.4 hat $\overline{G}$ nur $k-1$ maximale Normalteiler. Insbesondere ist $M \neq 1$ (anderenfalls müsste N_k mit einem N_i mit $i < k$ übereinstimmen). Wegen $1 \neq MN_k/N_k \trianglelefteq G/N_k \cong S$ ist $G = MN_k \cong M \times N_k \cong G/N_k \times \overline{G} \cong S^k$. □

Definition 4.7. Sei G eine primitive Permutationsgruppe.

(i) G ist vom *Typ* (A), falls $\mathrm{Soc}(G)$ (elementar)abelsch ist. Ggf. ist $G \leq \mathrm{Aff}(\mathrm{Soc}(G))$ („A“ steht für „affin“).

(ii) G ist vom *Typ* (F), falls $\mathrm{Soc}(G)$ nichtabelsch, einfach und nicht-regulär ist. Ggf. ist $G \leq \mathrm{Aut}(\mathrm{Soc}(G))$ („F“ steht für „fast einfach“ (engl. almost simple)).

Beispiel 4.8. Wir haben in Beispiel 2.16 bereits gesehen, welche Untergruppen von $\mathrm{Aff}(n, p)$ tatsächlich primitiv sind. Beispiele für Typ (F) sind durch A_n und S_n $(\leq \mathrm{Aut}(A_n))$ mit $n \geq 5$ gegeben. Sei nun G eine beliebige nichtabelsche einfache Gruppe. Durch die Operation auf den Nebenklassen einer maximalen Untergruppe wird G zu einer primitiven Permutationsgruppe vom Typ (F).

Definition 4.9. Seien G, H Gruppen und $A \leq G$. Sei $\varphi : A \to \mathrm{Aut}(H)$ ein Homomorphismus (und damit eine Operation), und sei $\mathcal{R}$ ein Repräsentantensystem für G/A. Für $x \in G$ sei $\overline{x} \in \mathcal{R}$ mit $xA = \overline{x}A$. Sei $\widehat{H} := \{f : \mathcal{R} \to H\}$. Durch $(fg)(r) := f(r)g(r)$ für $f, g \in \widehat{H}$ und $r \in \mathcal{R}$ wird $\widehat{H}$ zu einer Gruppe mit $\widehat{H} \cong \prod_{r\in\mathcal{R}} H = H^{|G:A|}$. Für $f \in \widehat{H}$ und $x \in G$ definieren wir ${}^x f \in \widehat{H}$ durch

$$\boxed{({}^x f)(r) := {}^{r^{-1}x\overline{x^{-1}r}}\Big(f\big(\overline{x^{-1}r}\big)\Big)}$$

für $r \in \mathcal{R}$. Dabei ist $x^{-1}rA = \overline{x^{-1}r}A$ und $r^{-1}x\overline{x^{-1}r} \in A$. Für $x, y \in G$ und $r \in \mathcal{R}$ ist

$$\begin{aligned}({}^x({}^y f))(r) &= {}^{r^{-1}x\overline{x^{-1}r}}\Big(({}^y f)\big(\overline{x^{-1}r}\big)\Big) = {}^{r^{-1}x\overline{x^{-1}r}\cdot(\overline{x^{-1}r})^{-1}y\overline{y^{-1}x^{-1}r}}\Big(f\big(\overline{y^{-1}x^{-1}r}\big)\Big)\\ &= {}^{r^{-1}xy\overline{(xy)^{-1}r}}\Big(f\big(\overline{(xy)^{-1}r}\big)\Big) = ({}^{xy} f)(r).\end{aligned}$$

Offenbar ist auch ${}^1 f = f$. Dies beschreibt also eine Operation $\psi : G \to \mathrm{Sym}(\widehat{H})$. Da A durch Automorphismen auf H operiert, sieht man leicht, dass auch $\psi : G \to \mathrm{Aut}(\widehat{H})$ gilt. Wir können also $H \wr_\varphi G := \widehat{H} \rtimes_\psi G$ definieren. Man nennt $H \wr_\varphi G$ das *verschränkte Kranzprodukt* (engl. twisted wreath product) von H mit G. Ist φ trivial, so spricht man auch nur vom *Kranzprodukt* und schreibt $H \wr G$, wobei man G als Permutationsgruppe auf G/A auffasst. Ist umgekehrt G eine transitive Permutationsgruppe auf Ω, so setzt man oft $A := G_\omega$ für ein $\omega \in \Omega$ in der Definition von $H \wr G$. Nach Satz 1.17 kann man dann $\mathcal{R}$ mit Ω identifizieren. Ist sogar $A = 1$, so nennt man $H \wr G$ manchmal *Standard-Kranzprodukt*.

Lemma 4.10. *Der Isomorphietyp von $H \wr_\varphi G$ hängt nicht von der Wahl von $\mathcal{R}$ ab.*

Beweis. Sei $\mathcal{R}'$ ein weiteres Repräsentantensystem für G/A. Für $r \in \mathcal{R}$ existiert dann genau ein $r' \in \mathcal{R}'$ mit $rA = r'A$. Sei $\widehat{H}' := \{f : \mathcal{R}' \to H\}$. Dann existiert eine Bijektion $\widehat{H} \to \widehat{H}'$, $f \mapsto f'$ mit $f'(r') := {}^{r'^{-1}r}(f(r))$. Dabei ist $(fg)' = f'g'$ und

$$({}^{x}f)'(r') = {}^{r'^{-1}r}(({}^{x}f)(r)) = {}^{r'^{-1}x\overline{x^{-1}r}}\Big(f\big(\overline{x^{-1}r}\big)\Big) = {}^{r'^{-1}x(\overline{x^{-1}r})'}\Big(f'\big((\overline{x^{-1}r})'\big)\Big) = ({}^{x}f')(r')$$

für $x \in G$ (beachte: $(\overline{x^{-1}r})'A = \overline{x^{-1}r}A = x^{-1}rA = x^{-1}r'A = \overline{x^{-1}r'}A$). Wir betrachten nun die Bijektion $\Psi : \widehat{H} \rtimes G \to \widehat{H}' \rtimes G$, $(f, x) \mapsto (f', x)$. Für $(f, x), (g, y) \in \widehat{H} \rtimes G$ gilt

$$\begin{aligned}\Psi((f,x) * (g,y)) &= \Psi(f({}^{x}g), xy) = ((f({}^{x}g))', xy) = (f'({}^{x}g)', xy)\\ &= (f'({}^{x}g'), xy) = (f', x) * (g', y) = \Psi(f,x) * \Psi(g,y).\end{aligned}$$

Also ist Ψ ein Isomorphismus. □

Bemerkung 4.11.

(i) Offenbar ist $|H \wr_\varphi G| = |H|^{|G:A|}|G|$.

(ii) Im Fall $A = G$ ist $H \wr_\varphi G \cong H \rtimes_\varphi G$.

(iii) Ist S nichtabelsch und einfach, so ist $\mathrm{Aut}(S^k) \cong \mathrm{Aut}(S) \wr S_k$ nach Aufgabe 4.4. Für eine primitive Permutationsgruppe G mit nichtabelschem Sockel gilt also stets $G \leq \mathrm{Aut}(S) \wr S_k$ für eine nichtabelsche einfache Gruppe S und $k \geq 1$.

Definition 4.12. Eine primitive Permutationsgruppe G ist vom *Typ* (V) („V“ steht für „verschränkt“), falls $G = S \wr_\varphi P$ mit folgenden Eigenschaften:

(i) S ist nichtabelsch und einfach,

(ii) $\varphi : A \to \mathrm{Aut}(S)$ mit $\mathrm{Inn}(S) \subseteq \varphi(A)$,

(iii) P operiert treu auf P/A,

(iv) P ist ein Stabilisator von G.

Lemma 4.13. *Sei G vom Typ (V) mit $n := |P : A|$. Dann ist $n \geq 6$, G hat Grad $|S|^n$ und $\mathrm{Soc}(G) = \widehat{S}$ ist regulär.*

Beweis. Wegen $S \cong S/\mathrm{Z}(S) \cong \mathrm{Inn}(S) \leq \varphi(A) \cong A/\mathrm{Ker}(\varphi)$ kann A nicht auflösbar sein. Andererseits ist P zu einer Untergruppe von S_n isomorph. Da A als Stabilisator sogar in S_{n-1} liegt, ist $n \geq 6$. Der Grad von G ist $|G : P| = |\widehat{S}| = |S|^n$. Wegen $\widehat{S} \cap P = 1$, operiert $\widehat{S}$ regulär auf G/P. Sei $\mathcal{R}$ ein Repräsentantensystem für P/A. Für $r \in \mathcal{R}$ sei $T_r := \{f : \mathcal{R} \to S : f(s) = 1 \ \forall s \neq r\} \cong S$. Dann ist $\widehat{S} = \bigoplus_{r\in\mathcal{R}} T_r$. Für $f \in T_r$, $s \in \mathcal{R}$ und $x \in P$ ist $({}^{x}f)(s) = {}^{\cdots}(f(\overline{x^{-1}s}))$ und ${}^{x}f \in T_{\overline{xr}}$. Also operiert P transitiv durch Konjugation auf $\{T_r : r \in \mathcal{R}\}$. Aus Lemma 4.4 folgt nun leicht, dass $\widehat{S}$ ein minimaler Normalteiler von G ist.

Sei nun $(f, x) \in \mathrm{C}_G(\widehat{S})$ mit $f \in \widehat{S}$ und $x \in P$. Dann operiert x trivial auf $\{T_r : r \in \mathcal{R}\}$. Wie oben operiert x dann auch trivial auf P/A und nach Voraussetzung ist $x = 1$. Dies zeigt $\mathrm{C}_G(\widehat{S}) = \mathrm{Z}(\widehat{S}) \cong \mathrm{Z}(S^n) \cong \mathrm{Z}(S)^n = 1$. Daher ist $\widehat{S}$ der einzige minimale Normalteiler und $\mathrm{Soc}(G) = \widehat{S}$. □

Bemerkung 4.14. Im Allgemeinen ist es schwer zu sehen, welche verschränkten Kranzprodukte nach obiger Bauart tatsächlich primitive Operationen liefern. Im kleinstmöglichen Fall ist $S \cong A_5$ und $|P : A| = 6$. Hier hat G also Grad $60^6 > 10^{10}$ (Aufgabe 4.6). Diese Beispiele wurden ursprünglich von O'Nan und Scott übersehen und erst durch Aschbacher gefunden.

Definition 4.15. Eine primitive Permutationsgruppe G ist vom *Typ* (D) („D“ steht für „diagonal“), falls $G \leq \mathrm{Aut}(S) \wr S_k$ mit folgenden Eigenschaften:

(i) S ist nichtabelsch und einfach,

(ii) $k \geq 2$,

(iii) $B := \widehat{\mathrm{Inn}(S)} \trianglelefteq G$ mit $B \cong S^k$,

(iv) Für $(f,x) \in G$ mit $f \in \widehat{\mathrm{Aut}(S)}$ ist f konstant modulo $\mathrm{Inn}(S)$,

(v) $D := \{(f,x) \in G : f \text{ konstant}\} \leq G$ ist ein Stabilisator,

(vi) $k = 2$ oder $P := \{x \in S_k : \exists\, f \in \widehat{\mathrm{Aut}(S)} : (f,x) \in G\} \leq S_k$ ist primitiv (auf $\{1,\dots,k\}$).

Lemma 4.16. *Eine Gruppe $G \leq \mathrm{Aut}(S) \wr S_k$, die die Bedingungen* (i)–(vi) *von Typ (D) erfüllt, operiert treu und primitiv auf G/D.*

Beweis. Wir zeigen zunächst, dass G treu auf G/D operiert. Nehmen wir an, dass D einen minimalen Normalteiler $N \trianglelefteq G$ enthält. Dann ist $N \cap B = 1$ nach Lemma 4.4. Also ist $N \leq \mathrm{C}_G(B)$ und $N \leq \widehat{\mathrm{Aut}(S)}$. Nach Aufgabe 4.1 ist $\mathrm{C}_{\mathrm{Aut}(S)}(\mathrm{Inn}(S)) = 1$. Dies liefert den Widerspruch $N = 1$. Also operiert G treu auf G/D und es bleibt zu zeigen, dass D maximal in G ist.

Sei indirekt $D < M < G$. Für ein $(f,x) \in G$ sei $f_1 \in \widehat{\mathrm{Aut}(S)}$ mit $f_1(i) := f(1)$ für $i = 1,\dots,k$. Nach Voraussetzung ist dann $ff_1^{-1} \in B$ und $(f,x) = ff_1^{-1}(f_1,x) \in BD$. Dies zeigt $G = BD$ und $D \cap B < M \cap B < B$. Sei zunächst $k = 2$. Dann gibt es eine Funktion $f \in M \cap B$ mit $f(1) \neq f(2)$. Nach Multiplikation mit einer geeigneten Funktion aus $D \cap B$ können wir $f(1) = 1$ annehmen. Sei $B_i := \{g \in B : g(j) = 1\ \forall j \neq i\} \trianglelefteq B$ ähnlich wie in Lemma 4.13. Sei $C \subseteq B_2$ die Konjugationsklasse von f in B_2. Dann lässt sich jedes Element in C in der Form gfg^{-1} mit $g \in D \cap B$ schreiben. Also ist $C \subseteq M \cap B$. Da $B_2 \cong \mathrm{Inn}(S) \cong S$ einfach ist, gilt $B_2 = \langle C \rangle \leq M \cap B$. Analog ist $B_1 \leq M \cap B$ und man hat den Widerspruch $B = B_1B_2 \leq M$.

Sei nun $k \geq 3$ und damit P primitiv. Sei $M_i \trianglelefteq M \cap B$ der Kern der Projektion $\pi_i : M \cap B \to B_i$ für $i = 1,\dots,k$. Wegen $D \cap B \leq M \cap B$ ist $(M \cap B)/M_i \cong \pi_i(M \cap B) = B_i \cong S$. Außerdem ist offenbar $\bigcap M_i = 1$. Sind die M_i paarweise verschieden, so liefert Lemma 4.6 den Widerspruch $|M \cap B| = |S|^k = |B|$. Nehmen wir nun an, dass alle M_i gleich sind. Dann ist $M_1 = \bigcap M_i = 1$ und $|M \cap B| = |\pi_1(M \cap B)| = |S| = |D \cap B|$. Dies ist also auch ausgeschlossen. Für $V := \{1 \leq i \leq k : M_i = M_1\}$ gilt daher $1 < |V| < k$ (o. B. d. A.). Sei $x \in P$. Wegen $G = BD$ existiert ein $g \in D$, sodass x von g induziert wird. Dann ist $gM_ig^{-1} = M_{x^i}$ für $i = 1,\dots,k$, da $M \cap B \trianglelefteq M$. Sei nun $i \in V \cap {}^xV$. Dann ist $M_i = M_1 = M_{x^{-1}i}$. Für ein beliebiges $j \in V$ ist daher $M_{x^j} = gM_jg^{-1} = gM_1g^{-1} = gM_{x^{-1}i}g^{-1} = M_i = M_1$. Dies zeigt ${}^xV = V$. Also ist V ein Block von P im Widerspruch zur Primitivität von P. □

Beispiel 4.17. Für jede nichtabelsche einfache Gruppe S und $k \geq 2$ ist $\mathrm{Inn}(S) \wr S_k \cong S \wr S_k$ vom Typ (D) nach Lemma 4.16. Außerdem ist S^2 vom Typ (D).

Lemma 4.18. *Sei G vom Typ (D). Dann hat G Grad $|S|^{k-1}$ und $\mathrm{Soc}(G) = B$. Im Fall $k = 2$ und $P = 1$ hat G zwei minimale Normalteiler. Anderenfalls ist B selbst minimal.*

Beweis. Nach Satz 2.2 ist B transitiv. Aus Satz 1.19 folgt $G = BD$. Dies zeigt $|G : D| = |BD : D| = |B : B \cap D| = |\mathrm{Inn}(S)|^{k-1} = |S|^{k-1}$. Ist $P \neq 1$, so operiert P wie im Beweis von Lemma 4.13 transitiv auf den k Faktoren von B. Es folgt leicht, dass B dann ein minimaler Normalteiler ist. Gäbe es einen weiteren minimalen Normalteiler, so wäre B regulär nach Satz 4.1. Dies geht aus Ordnungsgründen nicht. Also ist $\mathrm{Soc}(G) = B$. Im Fall $k = 2$ und $P = 1$ ist B das Produkt zweier minimaler Normalteiler, die auch in G normal sind. □

Definition 4.19. Eine primitive Permutationsgruppe G ist vom *Typ (P)* („P“ steht für „Produkt“), falls $G \leq H \wr S_k$ mit folgenden Eigenschaften:

(i) H ist eine primitive Permutationsgruppe auf Δ vom Typ (F) oder (D),

(ii) $k \geq 2$,

(iii) $B := \widehat{\mathrm{Soc}(H)} \trianglelefteq G$ mit $B \cong S^{ks}$ für eine nichtabelsche einfache Gruppe S und $s \geq 1$,

(iv) Für $\delta \in \Delta$ ist $K := \{(f,x) \in G : f \in \widehat{H_\delta}\} \leq G$ ein Stabilisator von G,

(v) $P := \{x \in S_k : \exists\, f \in \widehat{H} : (f,x) \in G\} \leq S_k$ ist transitiv (auf $\{1,\dots,k\}$).

Bemerkung 4.20. In der Situation von Definition 4.19 operiert G auf Δ^k wie folgt: Für $g = (f, x) \in G$ und $\delta_1, \ldots, \delta_k \in \Delta$ sei

$$\boxed{{}^g(\delta_1, \ldots, \delta_k) := ({}^{f(1)}\delta_{x^{-1}1}, \ldots, {}^{f(k)}\delta_{x^{-1}k}).}$$

Da $\mathrm{Soc}(H)$ transitiv auf Δ operiert, ist G auch transitiv auf Δ^k. Für $\delta_1 = \ldots = \delta_k =: \delta$ erhält man dabei gerade den angegebenen Stabilisator.

Lemma 4.21. *Eine Gruppe $G \leq H \wr S_k$, die die Bedingungen* (i)–(v) *von Typ* (P) *erfüllt, operiert treu und primitiv auf G/K.*

Beweis. Aus Bemerkung 4.20 folgt leicht, dass G treu operiert. Sei $K < M \leq G$. Wegen $H = \mathrm{Soc}(H)H_\delta$ ist $G = BK$. Dies zeigt $K \cap B < M \cap B$. Wähle $f \in M \cap B$ mit $f(i) \notin H_\delta$ für ein $i \in \{1, \ldots, k\}$. Da H vom Typ (F) oder (D) ist, ist $\mathrm{Soc}(H)$ nicht regulär, d. h. $\mathrm{Soc}(H)_\delta = \mathrm{Soc}(H) \cap H_\delta \neq 1$. Es folgt $\mathrm{N}_H(\mathrm{Soc}(H)_\delta) = H_\delta$. Also existiert ein $h \in \mathrm{Soc}(H)_\delta$ mit $f(i)hf(i)^{-1} \notin \mathrm{Soc}(H)_\delta$. Wegen $\mathrm{Soc}(H) \trianglelefteq H$ ist dann $f(i)hf(i)^{-1} \notin H_\delta$. Sei $f_1 \in B \cap K \subseteq M$ mit $f_1(i) = h$ und $f_1(j) = 1$ für alle $j \neq i$. Sei weiter $f_2 := f_1 f f_1^{-1} f^{-1} \in B \cap M$ mit $f_2(i) = hf(i)h^{-1}f(i)^{-1} \notin H_\delta$. Die Maximalität von H_δ zeigt $H = \langle H_\delta, f_2(i)\rangle$. Wegen $B \cap K \leq M$ ist daher $B_i := \{g \in B : g(j) = 1\ \forall j \neq i\} \leq M$. Sei nun $j \in \{1, \ldots, k\}$ beliebig. Da P transitiv auf $\{1, \ldots, k\}$ operiert, existiert ein $x \in P$ mit ${}^x i = j$. Wegen $G = BK$ ist x durch ein Element $g \in K \subseteq M$ induziert. Folglich ist auch $B_j = B_{{}^x i} = gB_i g^{-1} \leq M$ und somit $B \leq M$. Dies zeigt $G = BK = M$ und K ist maximal in G. Die Behauptung folgt mit Satz 1.26. □

Beispiel 4.22. Für jede Gruppe H vom Typ (F) oder (D) und jedes $k \geq 2$ hat $H \wr S_k$ Typ (P).

Lemma 4.23. *Sei G vom Typ (P). Hat H Grad d, so hat G Grad d^k. Außerdem ist* $\mathrm{Soc}(G) = B$.

Beweis. Der Grad von G ergibt sich aus Bemerkung 4.20. Für $i = 1, \ldots, k$ sei wie bisher $B_i := \{f \in B : f(j) = 1\ \forall j \neq i\} \trianglelefteq B$. Nach Satz 4.1 ist $\mathrm{C}_H(\mathrm{Soc}(H)) = 1$. Es folgt leicht, dass auch $\mathrm{C}_{\widehat{H}}(B) = 1$ gilt. Sei nun $(f, x) \in \mathrm{C}_G(B)$ mit $f \in \widehat{H}$ und $x \in S_k$. Dann operiert x trivial $\{B_i : i = 1, \ldots, k\}$, und es folgt $x = 1$. Somit ist auch $f \in \mathrm{C}_{\widehat{H}}(B) = 1$ und $\mathrm{C}_G(B) = 1$. Also liegt jeder minimale Normalteiler von G in B, d. h. $\mathrm{Soc}(G) \subseteq B$. Nach Voraussetzung ist $B = T_1 \oplus \ldots \oplus T_{ks}$ mit nichtabelschen einfachen Gruppen $T_1 \cong \ldots \cong T_{ks}$. Nach Lemma 4.4 ist $\mathrm{Soc}(G) = \bigoplus_{i \in I} T_i$ für eine Teilmenge $I \subseteq \{1, \ldots, ks\}$. Im Fall $\mathrm{Soc}(G) < B$ hätte man daher den Widerspruch $\mathrm{C}_G(\mathrm{Soc}(G)) \neq 1$. □

Bemerkung 4.24. Für Typ (F), (D) und (P) ist $\mathrm{Soc}(G)$ offenbar nicht regulär.

Aufgabe 4.1. Sei $\mathrm{Z}(G) = 1$. Zeigen Sie: $\mathrm{C}_{\mathrm{Aut}(G)}(\mathrm{Inn}(G)) = 1$.

Aufgabe 4.2. Beschreiben Sie die Struktur von $\mathrm{C}_{S_n}(\sigma)$ für $\sigma \in S_n$ mit Hilfe von Kranzprodukten.

Aufgabe 4.3. Zeigen Sie, dass S_n treu und transitiv auf den k-elementigen Teilmengen von $\{1, \ldots, n\}$ mit $1 \leq k < n$ operiert. Wann ist die Operation primitiv?

Aufgabe 4.4. Sei S nichtabelsch und einfach. Zeigen Sie $\mathrm{Aut}(S^k) \cong \mathrm{Aut}(S) \wr S_k$ für $k \in \mathbb{N}$.

Aufgabe 4.5. Sei $P \in \mathrm{Syl}_p(S_{p^n})$ für ein $n \geq 1$. Zeigen Sie:

$$P \cong \underbrace{C_p \wr \ldots \wr C_p}_{n \text{ Stück}}$$

(es spielt dabei keine Rolle, wie man Klammern setzt). Wie sehen die p-Sylowgruppen von S_m für ein beliebiges m aus?

Aufgabe 4.6. Zeigen Sie, dass es eine primitive Permutationsgruppe vom Typ (V) mit $S = A_5$ und $|P : A| = 6$ gibt.
Hinweis: Man kann Lemma 4.6 benutzen.

Aufgabe 4.7. Finden Sie eine primitive Permutationsgruppe vom Grad n für $n = 5, \ldots, 33$, die nicht zu A_n oder S_n isomorph ist.

5 Der Satz von Aschbacher-O'Nan-Scott

Bemerkung 5.1. Wir wollen zeigen, dass die Typen (A), (F), (V), (D) und (P) alle primitiven Permutationsgruppen beschreiben. Dies erfordert einige Vorüberlegungen.

Lemma 5.2. *Sei G eine primitive Permutationsgruppe auf Ω. Sei $\mathrm{Soc}(G) = T_1 \oplus \ldots \oplus T_k$ für nichtabelsche einfache Gruppen $T_1, \ldots, T_k$ mit $k \geq 2$. Sei $\pi_i : \mathrm{Soc}(G) \to T_i$ die i-te Projektion. Für ein $\omega \in \Omega$ und ein $i \in \{1, \ldots, k\}$ gelte $\pi_i(\mathrm{Soc}(G)_\omega) = T_i$. Dann ist G vom Typ (D) oder (P).*

Beweis. Nach Bemerkung 4.3 ist $T_1 \cong \ldots \cong T_k$.

Schritt 1: $\pi_j(\mathrm{Soc}(G)_\omega) = T_j$ für $j = 1, \ldots, k$.
Nach Lemma 4.4 operiert G durch Konjugation auf $\mathcal{T} := \{T_1, \ldots, T_k\}$. Jede Bahn entspricht dabei einem minimalen Normalteiler von G. Nach Satz 4.1 hat G höchstens zwei minimale Normalteiler. Nach Satz 1.19 ist $G = \mathrm{Soc}(G)G_\omega$. Also hat auch G_ω höchstens zwei Bahnen auf $\mathcal{T}$. Sei $g \in G_\omega$. Wegen $\mathrm{Soc}(G)_\omega = \mathrm{Soc}(G) \cap G_\omega \trianglelefteq G_\omega$ ist $g\pi_i(\mathrm{Soc}(G)_\omega)g^{-1} = \pi_j(\mathrm{Soc}(G)_\omega)$ für ein $j \in \{1, \ldots, k\}$. Hat G nur einen minimalen Normalteiler, so folgt die Behauptung aus der Voraussetzung $\pi_i(\mathrm{Soc}(G)_\omega) = T_i$. Nehmen wir nun an, dass G zwei minimale Normalteiler N und M hat. O. B. d. A. sei $T_i \subseteq N$ (Lemma 4.4). Nach Satz 1.19 ist

$$G = G_\omega N \leq \mathrm{N}_G\Big(\bigoplus_{j=1}^{k} \pi_j(\mathrm{Soc}(G)_\omega)\Big),$$

d. h. $\bigoplus_{j=1}^{k} \pi_j(\mathrm{Soc}(G)_\omega) \trianglelefteq G$ und $\pi_j(\mathrm{Soc}(G)_\omega) \in \{1, T_j\}$ für alle j. Da N regulär operiert, ist $\mathrm{Soc}(G)_\omega \nsubseteq N$. Also ist

$$\bigoplus_{j=1}^{k} \pi_j(\mathrm{Soc}(G)_\omega) = NM = \mathrm{Soc}(G)$$

und die Behauptung folgt.

Nach Lemma 4.4 existiert eine Partition $\{1, \ldots, k\} = I_1 \,\dot\cup\, \ldots \,\dot\cup\, I_l$, sodass $\mathrm{Soc}(G)_\omega = D_1 \oplus \ldots \oplus D_l$ mit $D_j \leq \bigoplus_{s \in I_j} T_s$ und $\mathrm{Ker}(\pi_s) \cap D_j = 1$ für alle $s \in I_j$.

Schritt 2: G_ω operiert transitiv auf $\{D_1, \ldots, D_l\}$.
Nach Lemma 4.4 sind die $D_1 \cong \ldots \cong D_l \cong T_1$ die einzigen minimalen Normalteiler von $\mathrm{Soc}(G)_\omega$. Also werden die D_j von G_ω permutiert. Die Behauptung ist klar, falls G nur einen minimalen Normalteiler hat. Hat G zwei minimale Normalteiler N und M, so kann kein D_j in N (oder M) liegen, da sonst $D_j \subseteq N \cap G_\omega = 1$ wäre. Man sieht leicht, dass G_ω also auch in diesem Fall transitiv operiert.

Fall 1: $l = 1$.
Schritt 3: $k = 2$ oder G operiert primitiv auf $\mathcal{T}$.
Es ist $\mathrm{Soc}(G)_\omega \cong T_1$. Hat G zwei minimale Normalteiler N und M, so ist $|N| = |N : N \cap \mathrm{Soc}(G)_\omega| = |N\,\mathrm{Soc}(G)_\omega : \mathrm{Soc}(G)_\omega| = |\mathrm{Soc}(G) : \mathrm{Soc}(G)_\omega| = |T_1|^{k-1}$. Andererseits ist auch $|T_1|^k = |\mathrm{Soc}(G)| = |N||M| = |N|^2 = |T_1|^{2(k-1)}$, und es folgt $k = 2$. Sei nun $k \geq 3$. Dann hat G nur einen minimalen Normalteiler. Wir haben bereits gesehen, dass G transitiv auf $\mathcal{T}$ operiert. Nehmen wir an, dass G imprimitiv mit Blockzerlegung $\mathcal{B}_1 \,\dot\cup\, \ldots \,\dot\cup\, \mathcal{B}_b = \{1, \ldots, k\}$ ist. Sei $\pi_{\mathcal{B}_j} : \mathrm{Soc}(G) \to \bigoplus_{s \in \mathcal{B}_j} T_s$ die Projektion für $j = 1, \ldots, b$. Wir betrachten die Untergruppe

$$H := \{x \in \mathrm{Soc}(G) : \exists\, y_1, \ldots, y_b \in \mathrm{Soc}(G)_\omega \text{ mit } \pi_{\mathcal{B}_j}(x) = \pi_{\mathcal{B}_j}(y_j) \text{ für } j = 1, \ldots, b\} \leq \mathrm{Soc}(G).$$

Wegen $1 < b < k$ und $l = 1$ sieht man leicht, dass $\mathrm{Soc}(G)_\omega < H < \mathrm{Soc}(G)$ gilt. Für $x \in H$, $g \in G_\omega$ und $y_j \in \mathrm{Soc}(G)_\omega$ mit $\pi_{\mathcal{B}_j}(x) = \pi_{\mathcal{B}_j}(y_j)$ existiert ein $j' \in \{1, \ldots, b\}$ mit $\pi_{\mathcal{B}_j}(gxg^{-1}) = \pi_{\mathcal{B}_j}(gy_{j'}g^{-1})$. Wegen $\mathrm{Soc}(G)_\omega \trianglelefteq G_\omega$ folgt $gxg^{-1} \in H$ und $HG_\omega = G_\omega H \leq G$. Dann ist

$$|G_\omega| < |HG_\omega| < |G_\omega||\mathrm{Soc}(G) : G_\omega \cap H| = |G_\omega||\mathrm{Soc}(G) : \mathrm{Soc}(G) \cap G_\omega| = |\mathrm{Soc}(G)G_\omega| = |G|.$$

Dies widerspricht der Maximalität von G_ω.

Schritt 4: G ist vom Typ (D).
Konjugation liefert die bekannte Einbettung $G \hookrightarrow \mathrm{Aut}(\mathrm{Soc}(G))$. Indem wir T_j mit $\mathrm{Inn}(T_j)$ identifizieren, können wir also $G \leq \mathrm{Aut}(\mathrm{Soc}(G))$ annehmen. Nach Aufgabe 4.4 ist $\mathrm{Aut}(\mathrm{Soc}(G)) \cong \mathrm{Aut}(T_1) \wr S_k$. Wir müssen zeigen, dass man eine isomorphe Operation findet, sodass der Stabilisator wie in Typ (D) gegeben ist. Es gibt Isomorphismen $\varphi_j : T_1 \to T_j$ für $j = 2, \ldots, k$, sodass $\mathrm{Soc}(G)_\omega = D_1 = \{(x, \varphi_2(x), \ldots, \varphi_k(x)) : x \in T_1\}$. Sei $\varphi : T_1^k \to \mathrm{Soc}(G)$ der Isomorphismus mit $\varphi(x_1, \ldots, x_k) = (x_1, \varphi_2(x_2), \ldots, \varphi_k(x_k))$ für $x_1, \ldots, x_k \in T_1$. Dann bildet φ die diagonale Untergruppe $\{(x, \ldots, x) : x \in T_1\}$ genau auf $\mathrm{Soc}(G)_\omega$ ab. Offenbar induziert φ einen Isomorphismus $\widehat{\varphi} : \mathrm{Aut}(T_1^k) \to \mathrm{Aut}(\mathrm{Soc}(G))$, $\gamma \mapsto \varphi\gamma\varphi^{-1}$. Indem wir G durch $\widehat{\varphi}^{-1}(G)$ ersetzen, können wir $\mathrm{Soc}(G)_\omega = \{(x, \ldots, x) : x \in T_1\}$ annehmen. Diese Eigenschaft bleibt unter dem Isomorphismus $\mathrm{Aut}(T_1^k) \cong \mathrm{Aut}(T_1) \wr S_k$ erhalten. Sei ab jetzt also $G \leq \mathrm{Aut}(T_1) \wr S_k$. Sei $(f, x) \in G_\omega$ mit $f \in \widehat{\mathrm{Aut}(T_1)}$ und $x \in S_k$. Nehmen wir an, dass f nicht konstant ist. Dann existiert ein $f_1 \in \mathrm{Soc}(G)_\omega$, sodass $(f, x)f_1(f, x)^{-1} = ff_1f^{-1}$ nicht konstant ist (Aufgabe 4.1). Dies widerspricht aber $\mathrm{Soc}(G)_\omega \trianglelefteq G_\omega$. Die Maximalität von G_ω zeigt also $G_\omega = \{(f, x) \in G : f \text{ konstant}\}$ wie gewünscht. Es bleibt zu zeigen, dass Eigenschaft (iv) in Definition 4.15 gilt. Nehmen wir indirekt an, dass ein Element $(f, x) \in G$ mit $f(1) \not\equiv f(2) \pmod{\mathrm{Inn}(T_1)}$ existiert. Sei $H := \langle \mathrm{Soc}(G), (f, x)\rangle = \mathrm{Soc}(G)\langle (f, x)\rangle$. Nach Satz 1.19 ist $H = \mathrm{Soc}(G)H_\omega$. Es existiert also ein Element $f_1 \in \mathrm{Soc}(G)$ mit $(f_1f, x) = f_1(f, x) \in H_\omega \subseteq G_\omega$. Wegen $f_1(1)f(1) \equiv f(1) \not\equiv f(2) \equiv f_1(2)f(2) \pmod{\mathrm{Inn}(T_1)}$ kann f_1f aber nicht konstant sein. Dieser Widerspruch zeigt, dass f für alle $(f, x) \in G$ konstant modulo $\mathrm{Inn}(T_1)$ ist. Damit ist G vom Typ (D) und der Fall $l = 1$ ist erledigt.

Fall 2: $l \geq 2$.
Schritt 5: G ist vom Typ (P).
O. B. d. A. sei $I_1 = \{1, \ldots, t\}$. Nach Schritt 2 ist $k = lt$. Im Fall $t = 1$ wäre $\mathrm{Soc}(G) \subseteq G_\omega$ im Widerspruch zu Satz 2.2. Also ist $t \geq 2$. Sei $K := \bigoplus_{j=1}^{t} T_j$ und $N := \mathrm{N}_G(K)$. Sicher ist $K_\omega = \mathrm{Soc}(G)_\omega \cap K = D_1$. Sei $Y < N$ maximal mit $N_\omega \, \mathrm{C}_G(K) \subseteq Y$. Offenbar ist $D_1 \subseteq Y \cap K$. Nehmen wir $D_1 < Y \cap K$ an. Dann ist $G = \langle G_\omega, Y \cap K\rangle$. Da G_ω die Untergruppen $D_1, \ldots, D_l$ permutiert und $N_\omega \leq \mathrm{N}_G(Y \cap K)$ gilt, ist $\langle g(Y \cap K)g^{-1} : g \in G_\omega\rangle \trianglelefteq G$. Es folgt nun $K = Y \cap K \subseteq Y$ aus Lemma 4.4. Dies führt aber zum Widerspruch $N = N_\omega \, \mathrm{Soc}(G) \subseteq N_\omega K \, \mathrm{C}_G(K) \subseteq Y$ nach Satz 1.19. Also ist $Y \cap K = D_1$. Es folgt $Y \cap \mathrm{Soc}(G) = D_1 \oplus T_{t+1} \oplus \ldots \oplus T_k$. Außerdem ist $Y = Y \cap \mathrm{Soc}(G)N_\omega = (Y \cap \mathrm{Soc}(G))N_\omega$ (Dedekind-Identität). Für $L \leq N$ sei $L^* := L \, \mathrm{C}_G(K)/\, \mathrm{C}_G(K)$ das Bild der Konjugationsoperation auf K. Damit hat man $Y^* = D_1^* N_\omega^* = N_\omega^*$ wegen $D_1 \subseteq N_\omega$. Sei $H := N^*$ und $\Delta := H/N_\omega^*$. Da Y maximal in N ist, ist auch N_ω^* maximal in H. Also operiert H primitiv auf Δ. Wir untersuchen nun $\mathrm{Soc}(H)$. Da $K^* \cong K$ die direkte Summe minimaler Normalteiler von H sein muss, ist $K^* \subseteq \mathrm{Soc}(H)$. Wegen $\mathrm{C}_H(K^*) = \mathrm{C}_G(K)/\, \mathrm{C}_G(K) = 1$ ist also $\mathrm{Soc}(H) = K^* \cong K$. Für $\delta := 1N_\omega^* \in \Delta$ ist $H_\delta = N_\omega^*$. Es folgt

$$H_\delta \cap \mathrm{Soc}(H) = N_\omega^* \cap K^* = Y^* \cap K^* = (Y \cap K)^* = D_1^* \cong D_1 \cong T_1.$$

Insbesondere enthält H_δ keinen nicht-trivialen Normalteiler von H. Also operiert H auch treu auf Δ. Nach dem ersten Teil des Beweises hat H also Typ (D). Wir werden nun zeigen, dass G in $H \wr S_l$ enthalten ist. Dafür können wir H als Untergruppe von $\mathrm{Aut}(K)$ auffassen. Wir haben bereits gesehen, dass G_ω transitiv auf $\{D_1, \ldots, D_l\}$ durch Konjugation operiert. Ein Stabilisator ist dabei $\mathrm{N}_G(D_1) \cap G_\omega = N_\omega$. Sei $\mathcal{R} = \{r_1, \ldots, r_l\}$ ein Repräsentantensystem für G_ω/N_ω mit ${}^{r_j}D_1 = D_j$ für $j = 1, \ldots, l$. Wegen $|G_\omega : N_\omega| = |G_\omega N : N| = |G_\omega \, \mathrm{Soc}(G)N : N| = |G : N|$ ist $\mathcal{R}$ auch ein Repräsentantensystem für G/N. Sei $K_j := {}^{r_j}K$ für $j = 1, \ldots, l$. Dann operiert G auch transitiv auf $\{K_1, \ldots, K_l\}$. Für $g \in G$ definieren wir $\overline{g} \in \mathcal{R}$ durch $gN = \overline{g}N$. Wir betrachten die Abbildung

$$\Psi : G \to H \wr S_l, \; g \mapsto (f_g, \sigma_g),$$

wobei $f_g(j) \in H \leq \mathrm{Aut}(K)$ die Konjugation mit $r_j^{-1}g\overline{g^{-1}r_j} \in N$ beschreibt und σ_g die Operation von g auf $\{K_1, \ldots, K_l\}$. Es gilt

$${}^{r_{\sigma_g(j)}^{-1}gr_j}K = {}^{r_{\sigma_g(j)}^{-1}g}K_j = {}^{r_{\sigma_g(j)}^{-1}}K_{\sigma_g(j)} = K$$

und damit $\overline{gr_j} = r_{\sigma_g(j)}$ für $j = 1, \ldots, l$. Für $g, h \in G$ beschreibt $(f_g({}^{\sigma_g}f_h))(j)$ die Konjugation mit

$$r_j^{-1}g\overline{g^{-1}r_j} \cdot r_{\sigma_g^{-1}(j)}^{-1}h\overline{h^{-1}r_{\sigma_g^{-1}(j)}} = r_j^{-1}gh\overline{h^{-1}g^{-1}r_j}.$$

Also ist $\Psi(g) * \Psi(h) = (f_g, \sigma_g) * (f_h, \sigma_h) = (f_g({}^{\sigma_g}f_h), \sigma_g\sigma_h) = (f_{gh}, \sigma_{gh}) = \Psi(gh)$, und Ψ ist ein Homomorphismus. Sei nun $g \in \mathrm{Ker}(\Psi)$. Dann ist $\sigma_g = 1$ und $g \in N$. Außerdem ist $r_j^{-1}gr_j = r_j^{-1}g\overline{g^{-1}r_j} \in \mathrm{C}_G(K)$ und $g \in \mathrm{C}_G(K_j)$ für $j = 1, \ldots, l$. Dies zeigt $g \in \mathrm{C}_G(K_1 \ldots K_l) = \mathrm{C}_G(\mathrm{Soc}(G)) = 1$. Also ist Ψ injektiv. Sei $g \in \mathrm{Soc}(G)$.

Dann ist $\sigma_g = 1$ und $f_g(j)$ ist die Konjugation mit $r_j^{-1}\overline{gg^{-1}r_j} = r_j^{-1}gr_j \in \mathrm{Soc}(G) \subseteq K\,\mathrm{C}_G(K)$. Dies zeigt $\widehat{\mathrm{Soc}(H)} = \Psi(\mathrm{Soc}(G)) \trianglelefteq \Psi(G)$. Um zu zeigen, dass G vom Typ (P) ist, müssen wir noch $\Psi(G_\omega)$ bestimmen. Es gilt $\mathcal{R} \subseteq G_\omega$. Für $g \in G_\omega$ und $j = 1, \ldots, l$ ist also $r_j^{-1}\overline{gg^{-1}r_j} \in N_\omega$. Also ist $\Psi(G_\omega) \subseteq \{(f, x) \in \Psi(G) : f \in \widehat{H_\delta}\} =: X$, wobei $\delta := N_\omega^* \in \Delta$ wie oben. Man sieht leicht, dass X eine Untergruppe von $\Psi(G)$ ist. Aus der Maximalität von G_ω folgt also $X = \Psi(G_\omega)$ oder $X = \Psi(G)$. Im zweiten Fall wäre $\mathrm{Soc}(H) \subseteq H_\delta$ im Widerspruch zu Satz 2.2. Also ist $\Psi(G_\omega) = X$, und G ist vom Typ (P). □

Satz 5.3 („SCHREIERs Vermutung"). *Für jede einfache Gruppe S ist* $\mathrm{Out}(S) := \mathrm{Aut}(S)/\mathrm{Inn}(S)$ *auflösbar.* □

Bemerkung 5.4.

(i) Bislang kennt man keinen Beweis von Satz 5.3, der ohne die CFSG auskommt (der Beweis der CFSG selbst hat mehr als 10.000 Seiten).

(ii) Für einfache abelsche Gruppen S ist $\mathrm{Out}(S) = \mathrm{Aut}(S)$ bekanntlich sogar zyklisch. Wir werden später sehen, dass Satz 5.3 auch für A_n gilt (Satz 5.13). Man kann auch zeigen, dass $\mathrm{Out}(M_{11}) = 1$ und $|\mathrm{Out}(M_{12})| = 2$ gilt (ohne Beweis).

(iii) Im nächsten Lemma wird Satz 5.3 (leider) benutzt.

Lemma 5.5. *Sei G eine primitive Permutationsgruppe mit einfachem nichtabelschem Sockel. Dann ist G vom Typ (F).*

Beweis. Sei $T := \mathrm{Soc}(G)$. Wir müssen nur zeigen, dass T nicht regulär operiert. Nehmen wir das Gegenteil an, d. h. $T_\omega = 1$ für ein $\omega \in \Omega$ (wobei G auf Ω operiert). Wegen $G_\omega \cong G_\omega T/T \leq \mathrm{Aut}(T)/\mathrm{Inn}(T)$ ist G_ω auflösbar nach Satz 5.3. Sei N ein minimaler Normalteiler von G_ω. Dann ist N eine elementarabelsche p-Gruppe. Es gilt $G_\omega \leq G_\omega\,\mathrm{C}_G(N) \leq G$. Im Fall $G = G_\omega\,\mathrm{C}_G(N)$ wäre $N \trianglelefteq G$ im Widerspruch zu Satz 2.2. Also ist $\mathrm{C}_G(N) \subseteq G_\omega$ und $\mathrm{C}_T(N) = 1$. Die Bahnengleichung liefert $|T| \equiv 1 \pmod p$. Insbesondere ist $p \nmid |T|$. Wir betrachten $H := TN = T \rtimes N$. Sei q ein Primteiler von $|T|$. Jede q-Sylowgruppe Q von H liegt dann in T. Nach Satz 1.19 ist also $H = T\,\mathrm{N}_H(Q)$. Insbesondere ist $|N| \;\big|\; |\mathrm{N}_H(Q)|$. Wegen $N \in \mathrm{Syl}_p(H)$ können wir $N \leq \mathrm{N}_H(Q)$ annehmen, indem wir Q durch ein Konjugiertes ersetzen. Sei nun $\widetilde{Q} \in \mathrm{Syl}_q(H)$ beliebig mit $N \leq \mathrm{N}_H(\widetilde{Q})$. Dann existiert ein $x \in T$ mit $x\widetilde{Q}x^{-1} = Q$. Folglich ist $N, xNx^{-1} \leq \mathrm{N}_H(Q)$. Nach Sylow existiert ein $y \in \mathrm{N}_T(Q)$ mit $yNy^{-1} = xNx^{-1}$. Für jedes $g \in N$ ist $(x^{-1}ygy^{-1}x)g^{-1} \in N \cap T = 1$. Also gilt sogar $x^{-1}y \in \mathrm{C}_T(N) = 1$ und wir erhalten $\widetilde{Q} = x^{-1}Qx = y^{-1}Qy = Q$. Somit ist Q die einzige q-Sylowgruppe von H, die von N normalisiert wird. Für $g \in \mathrm{N}_G(N)$ normalisiert $N = gNg^{-1}$ auch $gQg^{-1} \in \mathrm{Syl}_q(T)$. Folglich ist $g \in \mathrm{N}_G(Q)$ und $G_\omega \leq \mathrm{N}_G(N) \leq \mathrm{N}_G(Q)$. Damit erhält man $G_\omega < G_\omega Q < G$ im Widerspruch zur Maximalität von G_ω. □

Lemma 5.6. *Sei G eine primitive Permutationsgruppe auf Ω. Sei $\mathrm{Soc}(G) = T_1 \oplus \ldots \oplus T_k$ für nichtabelsche einfache Gruppen $T_1, \ldots, T_k$ mit $k \geq 2$. Sei $\pi_i : \mathrm{Soc}(G) \to T_i$ die i-te Projektion. Für ein $\omega \in \Omega$ und alle $i \in \{1, \ldots, k\}$ gelte $\pi_i(\mathrm{Soc}(G)_\omega) \neq T_i$. Dann ist G vom Typ (V) oder (P).*

Beweis. Sei $R_i := \pi_i(\mathrm{Soc}(G)_\omega)$ für $i = 1, \ldots, k$.

Schritt 1: $\mathrm{Soc}(G)$ ist ein minimaler Normalteiler und $R_1 \cong \ldots \cong R_k$.
Wie in Lemma 5.2 hat G_ω höchstens zwei Bahnen auf $\mathcal{T} := \{T_1, \ldots, T_k\}$. Nehmen wir an, dass es zwei Bahnen sind. Diese entsprechen zwei minimalen (regulären) Normalteilern N und M von G. Sei o. B. d. A. $N = T_1 \ldots T_{k/2}$. Da N regulär operiert, ist $\mathrm{Soc}(G)_\omega \neq 1$. Nach Umnummerierung können wir $R_1 \neq 1$ annehmen. Wie in Lemma 5.2 ist $G_\omega R_1 \ldots R_{k/2} \leq \mathrm{N}_G(R_1 \ldots R_{k/2})$. Wegen $G_\omega \cap R_1 \subseteq N_\omega = 1$ ist $G_\omega < G_\omega R_1 \ldots R_{k/2}$. Die Maximalität von G_ω zeigt daher $R_1 \ldots R_{k/2} \trianglelefteq G$. Lemma 4.4 liefert den Widerspruch $R_1 = T_1$. Also ist $\mathrm{Soc}(G)$ der einzige minimale Normalteiler und G_ω operiert transitiv auf $\mathcal{T}$. Damit folgt auch $R_1 \cong \ldots \cong R_k$.

Sicher ist $\mathrm{Soc}(G)_\omega \subseteq R_1 \ldots R_k$. Wie oben ist $G_\omega R_1 \ldots R_k < G$ und damit $R_1 \ldots R_k \leq G_\omega R_1 \ldots R_k = G_\omega$. Dies zeigt $\mathrm{Soc}(G)_\omega = R_1 \ldots R_k$. Sei $N := \mathrm{N}_G(T_1)$. Für $L \leq N$ sei $L^* := L\,\mathrm{C}_G(T_1)/\mathrm{C}_G(T_1)$. Nach Satz 1.19 ist $N = \mathrm{Soc}(G)N_\omega$. Dies zeigt $N^* = T_1^* N_\omega^*$.

Fall 1: $T_1^* \leq N_\omega^*$.
Hier ist $N^* = N_\omega^*$. Nehmen wir $R_1 \neq 1$ an. Dann ist

$$T_1 = \langle xR_1x^{-1} : x \in T_1\rangle \leq \langle xR_1x^{-1} : x \in N_\omega\rangle \leq G_\omega.$$

Dieser Widerspruch liefert $R_1 = 1$ und $\mathrm{Soc}(G)_\omega = 1$ nach Schritt 1. Sei $\varphi : N_\omega \to \mathrm{Aut}(T_1)$ die Operation durch Konjugation. Dann ist $\mathrm{Ker}(\varphi) = \mathrm{C}_G(T_1) \cap G_\omega$ und $\mathrm{Inn}(T_1) \cong T_1^* \leq N_\omega^* \cong \varphi(N_\omega)$. Sei Y der Kern der Operation $G \to \mathrm{Sym}(\mathcal{T})$.

Schritt 2: $Y = \mathrm{Soc}(G)$.
Offenbar operiert Y auf jeden T_i. Dies liefert einen Monomorphismus $Y \to \mathrm{Aut}(T_1) \times \ldots \times \mathrm{Aut}(T_k)$. Insbesondere ist $Y/\mathrm{Soc}(G) \leq \mathrm{Out}(T_1)^k$ auflösbar nach Satz 5.3. Damit ist auch $Y_\omega \cong Y_\omega \mathrm{Soc}(G)/\mathrm{Soc}(G)$ auflösbar. Somit ist $\varphi(Y_\omega)$ ein auflösbarer Normalteiler von $\varphi(N_\omega)$. Dann ist $\varphi(Y_\omega) \cap \mathrm{Inn}(T_1) = 1$ und $\varphi(Y_\omega)$ zentralisiert $\mathrm{Inn}(T_1)$. Für $t \in T_1$ und $x \in Y_\omega$ ist also $\varphi(t) = \varphi(xtx^{-1})$. Dies zeigt $x \in \mathrm{C}_G(T_1)$ und $Y_\omega \subseteq \mathrm{C}_G(T_1)$. Da Y unabhängig von T_1 ist, gilt auch $Y_\omega \subseteq \mathrm{C}_G(T_i)$ für $i = 1, \ldots, k$. Also ist $Y_\omega \subseteq \mathrm{C}_G(\mathrm{Soc}(G)) = 1$. Aus $\mathrm{Soc}(G) \subseteq Y$ folgt nun die Behauptung.

Wegen $Y = \mathrm{Soc}(G)$ operiert G_ω also treu und transitiv auf $\mathcal{T}$. Dabei ist N_ω gerade ein Stabilisator.

Schritt 3: $G \cong T_1 \wr_\varphi G_\omega$ ist vom Typ (V).
Sei $\mathcal{R} := \{r_1, \ldots, r_k\}$ ein Repräsentantensystem für G_ω/N_ω mit ${}^{r_i}T_1 = T_i$ für $i = 1, \ldots, k$. Jedes $g \in G$ lässt sich eindeutig in der Form $g = g_1 \ldots g_k x_g$ mit $g_i \in T_i$ und $x_g \in G_\omega$ schreiben. Wir definieren

$$\Psi : G \to T_1 \wr_\varphi G_\omega,\ g \mapsto (f_g, x_g)$$

mit $f_g(r_i) := r_i^{-1} g_i r_i$. Offensichtlich ist Ψ bijektiv mit $\Psi(G_\omega) = G_\omega$. Für $g, h \in G$ müssen wir zeigen, dass $f_g({}^{x_g} f_h) = f_{gh}$ gilt. Seien $r_i, r_j \in \mathcal{R}$ mit $x_g^{-1} r_i N_\omega = r_j N_\omega$. Dann ist einerseits

$$f_g(r_i)({}^{x_g} f_h)(r_i) = r_i^{-1} g_i r_i ({}^{r_i^{-1} x_g r_j}(f_h(r_j))) = r_i^{-1} g_i r_i \cdot r_i^{-1} x_g r_j \cdot r_j^{-1} h_j r_j \cdot r_j^{-1} x_g^{-1} r_i = r_i^{-1} g_i x_g h_j x_g^{-1} r_i.$$

Wegen $x_g \in r_i N_\omega r_j^{-1}$ ist andererseits $x_g h_j x_g^{-1} \in T_i$ und

$$gh = (g_1 \ldots g_k x_g)(h_1 \ldots h_k x_h) = \ldots g_i x_g h_j x_g^{-1} \ldots x_g x_h.$$

Insgesamt ist also

$$\Psi(g)\Psi(h) = (f_g, x_g) * (f_h, x_h) = (f_g({}^{x_g} f_h), x_g x_h) = (f_{gh}, x_{gh}) = \Psi(gh).$$

Also ist Ψ ein Isomorphismus. Wir haben auch bereits gesehen, dass alle Bedingungen von Definition 4.12 erfüllt sind. Somit ist G vom Typ (V).

Fall 2: $T_1^* \not\leq N_\omega^*$.
Die Argumentation ist hier ähnlich wie im zweiten Fall im Beweis von Lemma 5.2. Sei $Y < N$ maximal mit $N_\omega \mathrm{C}_G(T_1) \leq Y$. Sicher ist $R_1 \leq Y \cap T_1$. Nehmen wir $R_1 < Y \cap T_1$ an. Dann ist $G = \langle G_\omega, Y \cap T_1 \rangle$. Wegen $N_\omega \leq \mathrm{N}_G(Y \cap T_1)$ ist $\langle g(Y \cap T_1)g^{-1} : g \in G_\omega \rangle \trianglelefteq G$. Es folgt nun $T_1 = Y \cap T_1 \subseteq Y$ aus Lemma 4.4. Dies führt zum Widerspruch $N = N_\omega T_1 \mathrm{C}_G(T_1) \subseteq Y$. Also ist $Y \cap T_1 = R_1$. Es folgt

$$\begin{aligned} Y = Y \cap N &= Y \cap \mathrm{Soc}(G) N_\omega = Y \cap T_1 \ldots T_k N_\omega = (Y \cap T_1) T_2 \ldots T_k N_\omega \\ &= R_1 T_2 \ldots T_k N_\omega = T_2 \ldots T_k N_\omega \leq \mathrm{C}_G(T_1) N_\omega \leq Y \end{aligned}$$

(Dedekind-Identität). Insbesondere ist $\mathrm{C}_G(T_1)N_\omega = Y$ eine maximale Untergruppe von N. Sei $H := N^*$ und $\Delta := H/N_\omega^*$. Da $N_\omega^* = Y^*$ maximal in N^* ist, operiert H primitiv auf Δ. Sicher ist $T_1 \cong T_1^* \leq \mathrm{Soc}(H)$. Wegen $\mathrm{C}_H(T_1^*) = 1$ ist auch $\mathrm{Soc}(H) = T_1^*$. Somit kann N_ω^* keinen nicht-trivialen Normalteiler von H enthalten ($T_1^* \not\leq N_\omega^*$). Insbesondere ist die Operation von H auf Δ auch treu. Nach Lemma 5.5 ist H vom Typ (F).

Schritt 4: $G \leq H \wr S_k$ ist vom Typ (P).
Wir wissen bereits, dass G transitiv auf $\mathcal{T}$ operiert. Dabei ist N ein Stabilisator. Wir wählen ein Repräsentantensystem $\mathcal{R} := \{r_1, \ldots, r_k\}$ für G_ω/N_ω mit ${}^{r_i}T_1 = T_i$ für $i = 1, \ldots, k$. Wegen $|G_\omega : N_\omega| = |G_\omega N : N| = |G_\omega \mathrm{Soc}(G) N : N| = |G : N|$ ist $\mathcal{R}$ auch ein Repräsentantensystem für G/N. Für $g \in G$ sei $\overline{g} \in \mathcal{R}$ mit $gN = \overline{g}N$. Wie in Lemma 5.2 betrachten wir H als Untergruppe von $\mathrm{Aut}(T_1)$. Sei nun

$$\Psi : G \to H \wr S_k,\ g \mapsto (f_g, \sigma_g),$$

wobei $f_g(i) \in \mathrm{Aut}(T_1)$ die Konjugation mit $r_i^{-1} g \overline{g^{-1} r_i} \in N$ beschreibt und $\sigma_g \in S_k$ die Operation von g auf $\mathcal{T}$. Es gilt

$${}^{r_{\sigma_g(i)}^{-1} g r_i} T_1 = {}^{r_{\sigma_g(i)}^{-1} g} T_i = {}^{r_{\sigma_g(i)}^{-1}} T_{\sigma_g(i)} = T_1$$

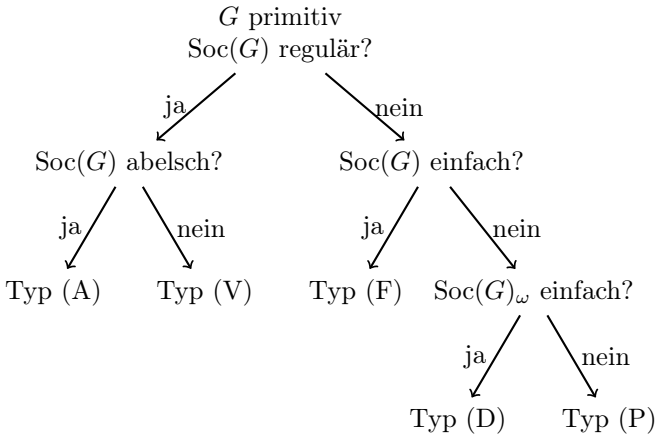
und $\overline{gr_i} = r_{\sigma_g(i)}$ für $i = 1, \dots, k$. Für $g, h \in G$ beschreibt $(f_g({}^{\sigma_g} f_h))(i)$ die Konjugation mit

$$r_i^{-1} g \overline{g^{-1} r_i} \cdot r_{\sigma_g^{-1}(i)}^{-1} h \overline{h^{-1} r_{\sigma_g^{-1}(i)}} = r_i^{-1} g h \overline{h^{-1} g^{-1} r_i}.$$

Also ist $\Psi(g) * \Psi(h) = (f_g, \sigma_g) * (f_h, \sigma_h) = (f_g({}^{\sigma_g} f_h), \sigma_g \sigma_h) = (f_{gh}, \sigma_{gh}) = \Psi(gh)$, und Ψ ist ein Homomorphismus. Sei nun $g \in \operatorname{Ker}(\Psi)$. Dann ist $\sigma_g = 1$ und $g \in N$. Außerdem ist $r_i^{-1} g r_i = r_i^{-1} g \overline{g^{-1} r_i} \in \mathrm{C}_G(T_1)$ und $g \in \mathrm{C}_G(T_i)$ für $i = 1, \dots, k$. Dies zeigt $g \in \mathrm{C}_G(T_1 \dots T_k) = \mathrm{C}_G(\operatorname{Soc}(G)) = 1$. Also ist Ψ injektiv. Sei $g \in \operatorname{Soc}(G)$. Dann ist $\sigma_g = 1$ und $f_g(i)$ ist die Konjugation mit $r_i^{-1} g \overline{g^{-1} r_i} = r_i^{-1} g r_i \in \operatorname{Soc}(G) \subseteq T_1 \, \mathrm{C}_G(T_1)$. Dies zeigt $\widehat{\operatorname{Soc}(H)} = \widehat{T_1^*} = \Psi(\operatorname{Soc}(G)) \trianglelefteq \Psi(G)$. Um zu zeigen, dass G vom Typ (P) ist, müssen wir noch $\Psi(G_\omega)$ bestimmen. Es gilt $\mathcal{R} \subseteq G_\omega$. Für $g \in G_\omega$ ist also $r_i^{-1} g \overline{g^{-1} r_i} \in N_\omega$. Somit ist $\Psi(G_\omega) \subseteq \{(f, x) \in \Psi(G) : f \in \widehat{H_\delta}\} =: X$, wobei $\delta := N_\omega^* \in \Delta$. Man sieht leicht, dass X eine Untergruppe von $\Psi(G)$ ist. Aus der Maximalität von G_ω folgt also $X = \Psi(G_\omega)$ oder $X = \Psi(G)$. Im zweiten Fall wäre $\operatorname{Soc}(H) \subseteq H_\delta$ im Widerspruch zu Satz 2.2. Also ist $\Psi(G_\omega) = X$, und G ist vom Typ (P). □

Satz 5.7 (Aschbacher-O'Nan-Scott)**.** *Jede primitive Permutationsgruppe ist von genau einem der Typen (A), (F), (V), (D) oder (P).*

Beweis. Sei G eine primitive Permutationsgruppe. Ist $\operatorname{Soc}(G)$ abelsch, so ist G vom Typ (A). Sei also $\operatorname{Soc}(G)$ nichtabelsch. Ist $\operatorname{Soc}(G)$ einfach, so ist G vom Typ (F) nach Lemma 5.5. Sei nun $\operatorname{Soc}(G)$ nicht-einfach. Dann gilt entweder die Voraussetzung von Lemma 5.2 oder Lemma 5.6. Also ist G vom Typ (D), (P) oder (V). Da die Fälle in den Beweisen von Lemma 5.2 und Lemma 5.6 sich gegenseitig ausschließen, kann auch nur genau ein Typ gelten. □



Bemerkung 5.8.

(i) Eine abstrakte Gruppe kann durchaus treue primitive Operationen zulassen, die zu verschiedenen Typen gehören. Zum Beispiel kann man $A_5 \wr S_2$ als Permutationsgruppe vom Typ (D) und (P) realisieren (siehe Beispiel 4.17 und Beispiel 4.22).

(ii) Man kennt keinen Beweis von Satz 5.7, der ohne die CFSG auskommt.

(iii) Sei n der Grad der primitiven Permutationsgruppe G. Dann ist offenbar

$$n \geq \begin{cases} 2 & \text{Typ (A)}, \\ 5 & \text{Typ (F)}, \\ 25 & \text{Typ (P)}, \\ 60 & \text{Typ (D)}, \\ 60^6 & \text{Typ (V)}. \end{cases}$$

In den letzten beiden Fällen ist außerdem n gerade nach Feit-Thompson („Gruppen ungerader Ordnung sind auflösbar“).

(iv) Für jede Primzahl $p \geq 5$ gibt es nach Beispiel 1.24 und Beispiel 3.2(vi) stets primitive Permutationsgruppen vom Grad p und $p+1$, die nicht zu S_n oder A_n isomorph sind. Cameron, Neumann und Teague haben umgekehrt gezeigt, dass die Grade n, von denen es primitive Permutationsgruppen außer A_n und S_n gibt, etwa doppelt so häufig wie Primzahlen sind. Nach dem Primzahlsatz ist die Anzahl dieser Grade zwischen 1 und m ungefähr $\frac{2m}{\log m}$ (ohne Beweis). Die Anzahl aller primitiven Permutationsgruppen vom Grad n kann man für kleine n unter `https://oeis.org/A000019` nachschlagen.

(v) Für Typ (F) kann man a priori nicht viel über die Operation sagen (nicht einmal der Grad ist eindeutig, siehe Aufgabe 3.5). Nach Satz 5.3 ist allerdings $G/\operatorname{Soc}(G)$ auflösbar. Da die primitiven Operationen in Korrespondenz zu den maximalen Untergruppen von G stehen, muss man sich mit der Bestimmung der maximalen Untergruppen von (fast) einfachen Gruppen beschäftigen. Für die sporadisch einfache *Monstergruppe* M ist die Klassifikation der maximalen Untergruppen beispielsweise noch offen. Wir betrachten im Folgenden den Fall $\operatorname{Soc}(G) = A_n$.

Lemma 5.9. *Für $n \geq 3$ ist $A_n = \langle (1,2,3), \ldots, (1,2,n) \rangle$.*

Beweis. Wir argumentieren durch Induktion nach n. Der Fall $n = 3$ ist klar. Sei nun $n \geq 4$. Es genügt zu zeigen, dass $A_n = \langle A_{n-1}, (1,2,n) \rangle =: H$ gilt. Sei indirekt $\sigma \in A_n \setminus H$. Dann existiert ein $k \neq n$ mit ${}^{\sigma}k = n$. Wähle $\tau \in A_{n-1}$ mit ${}^{\tau}1 = k$. Dann ist $\sigma\tau(1,2,n) \in A_{n-1}$ und wir erhalten den Widerspruch $\sigma \in H$. □

Lemma 5.10. *Sei $G \leq \operatorname{Sym}(\Omega)$ mit genau einem minimalen Normalteiler. Dann existiert eine Bahn $\Delta \subseteq \Omega$, sodass G treu auf Δ operiert.*

Beweis. Seien $\Delta_1, \ldots, \Delta_s$ die Bahnen von G. Seien K_i die Kerne der Operationen $G \to \operatorname{Sym}(\Delta_i)$. Da G treu auf Ω operiert, ist $K_1 \cap \ldots \cap K_s = 1$. Ist K_i nicht-trivial, so ist $\operatorname{Soc}(G) \subseteq K_i$ nach Voraussetzung. Folglich existiert ein i mit $K_i = 1$. □

Bemerkung 5.11. Nach Aufgabe 3.4 gilt die Voraussetzung von Lemma 5.10 für alle symmetrischen und alternierenden Gruppen.

Lemma 5.12. *Sei $n \geq 4$ und $A_{n-1} \cong H \leq A_n$. Dann ist $H = \operatorname{Alt}(\{1, \ldots, n\} \setminus \{i\})$ für ein $i \in \{1, \ldots, n\}$ oder $n = 6$.*

Beweis. O. B. d. A. sei $n \geq 5$. Nach Lemma 5.10 operiert H treu auf einer Bahn $\Delta \subseteq \{1, \ldots, n\}$. Wegen $|H| = (n-1)!/2$ ist $|\Delta| \geq n-1$. Wir können also annehmen, dass H transitiv auf $\{1, \ldots, n\}$ operiert. Insbesondere ist $n \mid |H| \mid (n-1)!$. Daher dürfen wir $n \geq 8$ voraussetzen.

Sei $f : A_{n-1} \to H$ ein Isomorphismus, und sei $\sigma \in A_{n-1}$ ein 3-Zyklus. Offenbar ist A_{n-4} zu einer Untergruppe von $\mathrm{C}_{A_{n-1}}(\sigma)$ isomorph. Insbesondere besitzt auch $\mathrm{C}_H(f(\sigma))$ eine Untergruppe $C \cong A_{n-4}$. Sei $f(\sigma)$ das disjunkte Produkt von k vielen 3-Zyklen. Offenbar permutiert C die Bahnen von $f(\sigma)$ (einschließlich trivialer Bahnen). Der Kern dieser Operation ist eine 3-Gruppe und damit trivial. Es gibt also einen Monomorphismus $\varphi : C \to S_{n-2k}$. Wegen $|C| = (n-4)!/2$ folgt $k \leq 2$. Im Fall $k = 2$ ist φ transitiv und man erhält den Widerspruch $n = 3k = 6$. Also ist auch $f(\sigma)$ ein 3-Zyklus.

Sei $f((1,2,3)) = (\alpha, \beta, \gamma)$ und $f((1,2,4)) = (\delta, \epsilon, \varphi)$. Im Fall $\{\alpha, \beta, \gamma\} \cap \{\delta, \epsilon, \varphi\} = \varnothing$ wäre

$$A_4 \cong \langle (1,2,3), (1,2,4) \rangle \cong \langle f((1,2,3)), f((1,2,4)) \rangle$$

abelsch. Im Fall $|\{\alpha, \beta, \gamma\} \cap \{\delta, \epsilon, \varphi\}| = 1$ würde $\langle f((1,2,3)), f((1,2,4)) \rangle$ transitiv auf der 5-elementigen Menge $\{\alpha, \beta, \gamma\} \cup \{\delta, \epsilon, \varphi\}$ operieren. Also ist $|\{\alpha, \beta, \gamma\} \cap \{\delta, \epsilon, \varphi\}| = 2$, und $\langle f((1,2,3)), f((1,2,4)) \rangle$ kann nur vier Ziffern bewegen. Durch Induktion nach k sieht man, dass $\langle f((1,2,3)), \ldots, f((1,2,k)) \rangle$ höchstens k Ziffern bewegen kann. Also ist $H = f(A_{n-1}) = \langle f((1,2,3)), \ldots, f((1,2,n-1)) \rangle$ (Lemma 5.9) nicht transitiv. Dies war aber bereits ausgeschlossen. □

Satz 5.13 (Hölder)**.** *Es gilt $\operatorname{Aut}(A_6) \cong S_6 \rtimes C_2$ und $\operatorname{Aut}(A_n) \cong S_n$ für $4 \leq n \neq 6$.*

Beweis. Offenbar operiert S_n durch Konjugation auf A_n mit Kern $\mathrm{C}_{S_n}(A_n) = 1$ (beachte: $\mathrm{C}_{S_n}(A_n) \trianglelefteq S_n$). Dies liefert einen Monomorphismus $\Psi : S_n \to \mathrm{Aut}(A_n)$. Sei $H_i := \mathrm{Alt}(\{1,\dots,n\} \setminus \{i\})$ für $i = 1,\dots,n$. Sei zunächst $n \neq 6$. Nach Lemma 5.12 operiert dann $\mathrm{Aut}(A_n)$ auf $\{H_1,\dots,H_n\}$. Dies liefert einen Homomorphismus $\Gamma : \mathrm{Aut}(A_n) \to S_n$. Sei $f \in \mathrm{Ker}(\Gamma)$ und $g \in A_n$. Dann ist $H_{f(g)i} = f(g)H_i f(g)^{-1} = f(g)f(H_i)f(g)^{-1} = f(gH_ig^{-1}) = f(H_{gi}) = H_{gi}$ und $f(g) = g$. Also ist Γ injektiv. Damit sind Ψ und Γ sogar Isomorphismen. Sei nun $n = 6$.

Schritt 1: $\Psi(S_6) < \mathrm{Aut}(A_6)$.
Offenbar operiert A_5 treu und transitiv auf seinen sechs 5-Sylowgruppen durch Konjugation. Dies liefert einen Monomorphismus $f : A_5 \to S_6$. Im Fall $f(A_5) \nsubseteq A_6$ wäre $1 \neq f(A_5) \cap A_6 \lhd f(A_5)$ im Widerspruch zur Einfachheit von $f(A_5) \cong A_5$. Also ist $f(A_5) \leq A_6$. Da f transitiv ist, gilt $f(A_5) \neq H_i$ für $i = 1,\dots,6$. Die Operation von A_6 auf den Nebenklassen $A_6/f(A_5)$ liefert einen Monomorphismus $\varphi : A_6 \to S_6$. Wie eben ist $\varphi(A_6) = A_6$, d. h. $\varphi \in \mathrm{Aut}(A_6)$. Da $f(A_5)$ der Stabilisator der trivialen Nebenklasse ist, muss $\varphi(f(A_5)) = H_i$ für ein $i \in \{1,\dots,6\}$ gelten. Insbesondere ist $\varphi \notin \Psi(S_6)$.

Schritt 2: $|\mathrm{Out}(A_6)| = 4$.
Seien $\varphi, \psi \in \mathrm{Aut}(A_6) \setminus \Psi(S_6)$. Offenbar bildet jeder Automorphismus Konjugationsklassen auf Konjugationsklassen ab. Mit Beispiel 1.10 sieht man leicht, dass die Menge der 3-Zyklen eine Konjugationsklasse C von A_6 bildet. Gilt $\varphi(C) = C$, so sieht man wie im Beweis von Lemma 5.12, dass φ die Untergruppen H_i permutiert. Dann wäre aber $\varphi \in \Psi(S_6)$. Also muss $\varphi(C) = \psi(C)$ die Konjugationsklasse der Elemente vom Zyklentyp $(3,3)$ sein, denn dies sind die einzigen weiteren Elemente der Ordnung 3. Es folgt $(\varphi\psi)(C) = C$ und $\varphi\psi \in \Psi(S_6)$. Dies impliziert die Behauptung.

Schritt 3: $\mathrm{Aut}(A_6) \cong S_6 \rtimes C_2$.
Als Untergruppe vom Index 2 ist $\Psi(S_6) \trianglelefteq \mathrm{Aut}(A_6)$. Es genügt also ein Element $\varphi \in \mathrm{Aut}(A_6) \setminus \Psi(S_6)$ der Ordnung 2 zu finden. Sei zunächst $\varphi \in \mathrm{Aut}(A_6) \setminus \Psi(S_6)$ beliebig, und sei $x := (1,2,3,4,5) \in A_6$. Dann ist auch $\varphi(x)$ ein 5-Zyklus und daher in S_6 zu x konjugiert (Beispiel 1.10). Ersetzt man also φ durch ein geeignetes Element aus der Nebenklasse $\varphi\Psi(S_6)$, so kann man $\varphi(x) = x$ annehmen. Also existiert ein $y \in \mathrm{C}_{S_6}(x)$ mit $\varphi^2 = \Psi(y)$. Da S_6 genau $6 \cdot 4!$ Zyklen der Länge 5 besitzt, ist $|\mathrm{C}_{S_6}(x)| \leq 5$ und damit $y \in \mathrm{C}_{S_6}(x) = \langle x \rangle$. Dies zeigt $|\langle\varphi\rangle| \in \{2, 10\}$. Also hat $\varphi^5 \in \mathrm{Aut}(A_6) \setminus \Psi(S_6)$ die Ordnung 2. □

Bemerkung 5.14. Offenbar ist $\mathrm{Out}(A_6) \cong C_2^2$ (aber $\mathrm{Aut}(A_6) \ncong A_6 \rtimes C_2^2$). Die Untergruppen von $\mathrm{Aut}(A_6)$ der Ordnung 720 sind S_6, $\mathrm{PGL}(2,9) := \mathrm{GL}(2,9)/\mathrm{Z}(\mathrm{GL}(2,9))$ und M_{10} (ohne Beweis). Nach Aufgabe 5.1 gilt außerdem $\mathrm{Aut}(S_n) \cong \mathrm{Aut}(A_n)$ für $n \geq 4$.

Satz 5.15 (O'Nan-Scott)**.** *Für eine Untergruppe $1 \neq G \leq S_n$ gilt eine der folgenden Aussagen:*

(i) $G \leq S_k \times S_{n-k}$ *mit* $1 \leq k < \frac{n}{2}$ (*bis auf Isomorphie*).

(ii) $G \leq S_k \wr S_l$ *mit* $n = kl$ *und* $k, l \geq 2$ (*bis auf Isomorphie*).

(iii) G *ist primitiv auf* $\{1,\dots,n\}$.

Beweis. Nehmen wir zunächst an, dass G intransitiv auf $\Omega := \{1,\dots,n\}$ operiert. Sei $\Delta \subseteq \{1,\dots,n\}$ eine Bahn von G mit $k := |\Delta| \leq \frac{n}{2}$. Dann ist $G \leq \mathrm{Sym}(\Delta) \oplus \mathrm{Sym}(\Omega \setminus \Delta) \cong S_k \times S_{n-k}$. Sei nun $k = \frac{n}{2}$. Dann ist G in einer transitiven Gruppe der Form $S_k \wr S_2$ enthalten wie wir gleich sehen werden.

Sei also nun G transitiv und imprimitiv auf Ω. Dann existiert eine Blockzerlegung $\Omega = \Delta_1 \dot\cup \dots \dot\cup \Delta_l$ mit $|\Delta_i| = k$ und $n = kl$. Sei $H := \{x \in G : {}^x\Delta_1 = \Delta_1\} \leq G$. Da G transitiv auf $\{\Delta_1,\dots,\Delta_l\}$ operiert, ist $|G : H| = l$. Sei $\mathcal{R} = \{r_1,\dots,r_l\}$ ein Repräsentantensystem für G/H mit ${}^{r_i}\Delta_1 = \Delta_i$. Für $g \in G$ sei $\overline{g} \in \mathcal{R}$ mit $gH = \overline{g}H$. Wir betrachten die Abbildung

$$\Psi : G \to S_k \wr S_l,\ g \mapsto (f_g, \sigma_g),$$

wobei $f_g(i) \in S_k$ die Operation von $r_i^{-1}g\overline{g^{-1}r_i} \in H$ auf Δ_1 beschreibt und σ_g die Operation von g auf $\{\Delta_1,\dots,\Delta_l\}$. Wie üblich ist $\overline{gr_i} = r_{\sigma_g(i)}$. Für $g, h \in G$ beschreibt $(f_g({}^{\sigma_g}f_h))(i)$ die Konjugation mit

$$r_i^{-1}g\overline{g^{-1}r_i} \cdot r_{\sigma_g^{-1}(i)}^{-1}h\overline{h^{-1}r_{\sigma_g^{-1}(i)}} = r_i^{-1}gh\overline{h^{-1}g^{-1}r_i}.$$

Also ist $\Psi(g) * \Psi(h) = (f_g, \sigma_g) * (f_h, \sigma_h) = (f_g({}^{\sigma_g}f_h), \sigma_g\sigma_h) = (f_{gh}, \sigma_{gh}) = \Psi(gh)$, und Ψ ist ein Homomorphismus. Sei $g \in \mathrm{Ker}(\Psi)$. Dann ist $\sigma_g = 1$ und $g \in H$. Außerdem operiert $r_i^{-1}g\overline{g^{-1}r_i} = r_i^{-1}gr_i$ trivial auf Δ_1 für $i = 1,\dots,l$.

Also operiert g trivial auf Δ_i für $i = 1, \ldots, l$. Dies impliziert $g = 1$, und Ψ ist injektiv. Man kann also G als Untergruppe von $S_k \wr S_l$ auffassen. □

Bemerkung 5.16.

(i) Man kann leicht zeigen, dass die Untergruppen $S_k \times S_{n-k}$ $(1 \leq k < \frac{n}{2})$ und $S_k \wr S_l$ $(n = kl,\ k, l \geq 2)$ tatsächlich maximal in S_n sind (vgl. Aufgabe 4.3). Außerdem sind die maximalen Untergruppen im Fall (iii) von Satz 5.15 nie vom Typ (V) (ohne Beweis).

(ii) Sei G eine primitive Permutationsgruppe vom Typ (F) mit $\mathrm{Soc}(G) \cong A_n$. Im Fall $n \neq 6$ kann man $G \in \{A_n, S_n\}$ nach Satz 5.13 annehmen (man beachte, dass n nicht unbedingt der Grad von G ist!). Der Stabilisator G_ω ist maximal in G. Nach Satz 5.15 gilt einer der folgenden Fälle:

(a) $G_\omega \cong S_k \times S_{n-k}$ oder $G_\omega \cong (S_k \times S_{n-k}) \cap A_n$.

(b) $G_\omega \cong S_k \wr S_l$ oder $G_\omega \cong (S_k \wr S_l) \cap A_n$.

(c) G_ω ist eine primitive Permutationsgruppe vom Grad n.

Im ersten Fall ist die Operation von G isomorph zur Operation auf den k-elementigen Teilmengen von $\{1, \ldots, n\}$. Insbesondere ist $\binom{n}{k}$ der Grad der Operation. Im zweiten Fall ist die Operation isomorph zur Operation auf allen Partitionen von $\{1, \ldots, n\}$ mit l gleichgroßen Teilen. Hier ist der Grad gegeben durch $n!/(k!^l \cdot l!)$. Schließlich kann man im dritten Fall Satz 5.7 auf G_ω anwenden. In der Regel ist dann G_ω deutlich kleiner als G (siehe Satz 6.14).

Beispiel 5.17.

(i) Nach Aufgabe 1.1 sind die primitiven Permutationsgruppen vom Grad ≤ 4 gegeben durch S_2, A_3, S_3, A_4 und S_4 jeweils mit den natürlichen Operationen. Sei nun $G \leq S_5$ primitiv vom Grad 5. Nach Bemerkung 5.8 ist G vom Typ (A) oder (F). Für Typ (A) erhält man die Gruppen C_5, $C_5 \rtimes C_2$ und $C_5 \rtimes C_4 \cong \mathrm{Aff}(1, 5)$ aus Satz 2.15. Sei nun G vom Typ (F). Dann ist $\mathrm{Soc}(G) \cong A_5$, da keine andere nichtabelsche einfache Gruppe in S_5 enthalten ist. Also ist $G \in \{A_5, S_5\}$ mit der natürlichen Operation.

(ii) Sei nun $G \leq S_6$ primitiv vom Grad 6. Da 6 keine Primzahlpotenz ist, muss G vom Typ (F) sein. Dabei gibt es die offensichtlichen Möglichkeiten $G \in \{S_6, A_6\}$ mit der natürlichen Operation. Sei nun $\mathrm{Soc}(G) \neq A_6$. Wie üblich ist $\mathrm{Soc}(G) \subseteq A_6$ und $|A_6 : \mathrm{Soc}(G)| \geq 6$, denn anderenfalls könnte die einfache Gruppe A_6 nicht treu auf den Nebenklassen $A_6/\mathrm{Soc}(G)$ operieren. Also ist $|\mathrm{Soc}(G)| \leq 60$ und $\mathrm{Soc}(G) \cong A_5$. Nach Bemerkung 5.16 ist $G \in \{S_5, A_5\}$, und G_ω ist primitiv vom Grad 5. Wegen $|G : G_\omega| = 6$ folgt leicht, dass G_ω der Normalisator einer 5-Sylowgruppe in G ist. Insbesondere ist auch hier die Operation eindeutig (siehe Aufgabe 1.4).

(iii) Die treue, 2-transitive Operation von $G := \mathrm{GL}(3, 2)$ auf $\mathbb{F}_2^3 \setminus \{0\}$ liefert eine primitive Permutationsgruppe vom Grad 7. Nach Satz 2.14 kann G nicht auflösbar sein. Wegen $60 \nmid 168 = |G|$ muss G also einfach sein. Somit ist G vom Typ (F).

Bemerkung 5.18. Die primitiven Permutationsgruppen vom Grad $< 2^{12}$ sind vollständig klassifiziert und im Computeralgebrasystem MAGMA verfügbar. In GAP kann man derzeit auf die primitiven Permutationsgruppen vom Grad < 2500 zugreifen.

Satz 5.19 (Burnside)**.** *Jede 2-transitive Permutationsgruppe ist vom Typ (A) oder (F).*

Beweis. Sei G eine 2-transitive Permutationsgruppe auf Ω. Besitzt G einen regulären Normalteiler $N \trianglelefteq G$, so operiert G_ω transitiv auf $N \setminus \{1\}$ nach Satz 2.1. Nach Satz 3.6 ist N abelsch und G ist vom Typ (A). Wir können also annehmen, dass G keinen regulären Normalteiler besitzt. Insbesondere ist G nicht vom Typ (V). Sei nun $G \leq H \wr S_k$ vom Typ (P), wobei H auf Δ operiert. Wir benutzen die Operation von G auf $\Omega := \Delta^k$ wie in Bemerkung 4.20. Für $\omega := (\delta, \ldots, \delta) \in \Omega$ ist $G_\omega = \{(f, x) \in G : f \in \widehat{H_\delta}\}$. Wir müssen zeigen, dass G_ω nicht transitiv auf $\Omega \setminus \{\omega\}$ operiert. Für $\delta \neq \gamma \in \Delta$ gibt es tatsächlich kein Element aus G_ω, welches $(\gamma, \delta, \ldots, \delta)$ auf $(\gamma, \ldots, \gamma)$ abbildet. Sei schließlich G vom Typ (D) mit $\mathrm{Soc}(G) \cong S^k$. Dann ist $|\Omega| = |S|^{k-1}$. Nach Aufgabe 3.8 operiert $N := \mathrm{Soc}(G)_\omega \trianglelefteq G_\omega$ $\frac{1}{2}$-transitiv auf $\Omega \setminus \{\omega\}$, d. h. alle Bahnen von N haben die gleiche Länge $l \mid |N| = |S|$. Da $\mathrm{Soc}(G)$ nicht regulär ist, gilt $N \neq 1$ und $l > 1$. Dies liefert den Widerspruch

$$0 \equiv |S|^{k-1} = |\Omega| \equiv 1 \pmod{l}.$$ □

Bemerkung 5.20.

(i) Man kann Satz 5.19 auch ohne Schreiers Vermutung beweisen (siehe Anhang, Satz A.1).

(ii) Wir haben in Satz 3.11 bereits gesehen, dass für scharf 2-transitive Permutationsgruppen nur Typ (A) in Frage kommt.

(iii) Mit Hilfe der CFSG lassen sich alle 2-transitiven (sogar $\frac{3}{2}$-transitiven) Permutationsgruppen angeben (vgl. Anhang, Satz A.8 und Abschnitt 7.7 in [Dixon-Mortimer]). Dies verallgemeinert also Satz 3.22. Im Folgenden werden wir uns daher verstärkt den primitiven Permutationsgruppen zuwenden, die nicht 2-transitiv sind.

Aufgabe 5.1.

(i) Zeigen Sie: $\mathrm{Aut}(S_n) \cong \mathrm{Aut}(A_n)$ für $n \geq 4$.

(ii) Zeigen Sie, dass $\varphi \in \mathrm{Aut}(S_6)$ mit

$$\varphi((1,2)) = (1,5)(2,3)(4,6), \qquad \varphi((1,3)) = (1,4)(2,6)(3,5), \qquad \varphi((1,4)) = (1,3)(2,4)(5,6),$$
$$\varphi((1,5)) = (1,2)(3,6)(4,5), \qquad \varphi((1,6)) = (1,6)(2,5)(3,4)$$

ein äußerer Automorphismus der Ordnung 2 ist.

(iii) Zeigen Sie: $\mathrm{Aut}(A_6) \ncong A_6 \rtimes C_2^2$.

Aufgabe 5.2. Finden Sie eine endliche Gruppe, die zwei nicht-isomorphe, primitive, treue Operationen vom gleichen Grad zulässt.
Hinweis: Alle Hilfsmittel sind erlaubt (Internet, Computer, ...).

6 Jordan-Mengen

Bemerkung 6.1. Nachdem wir im letzten Kapitel die Untergruppenstruktur von primitiven Permutationsgruppen gut verstanden haben, werden wir in diesem Kapitel die Eigenschaften der Elemente untersuchen.

Satz 6.2. *Sei Ω eine transitive G-Menge, und sei $H \leq G$ primitiv auf $\Delta \subseteq \Omega$ mit $|\Delta| > |\Omega|/2$. Dann ist G primitiv auf Ω.*

Beweis. Sei Γ ein Block von G auf Ω. Für $h \in H$ ist ${}^h(\Gamma \cap \Delta) = {}^h\Gamma \cap \Delta$. Aus der Primitivität von H folgt also $|\Gamma \cap \Delta| \leq 1$ oder $\Delta = \Gamma \cap \Delta \subseteq \Gamma$. Im letzten Fall wäre $|\Delta| \leq |\Omega|/2$, da $|\Gamma|$ ein echter Teiler von $|\Omega|$ sein muss. Also ist $|\Gamma \cap \Delta| \leq 1$. Da Ω die disjunkte Vereinigung der Blöcke ${}^g\Gamma$ ist, erhält man den Widerspruch $|\Delta| \leq |\Omega|/|\Gamma| \leq |\Omega|/2$. □

Definition 6.3. Sei Ω eine transitive G-Menge. Eine Teilmenge $\Delta \subsetneq \Omega$ heißt *Jordan-Menge*, falls G_Δ transitiv auf $\Omega \setminus \Delta$ operiert. Ist G_Δ sogar primitiv auf $\Omega \setminus \Delta$, so ist Δ eine *starke Jordan-Menge*.

Beispiel 6.4.

(i) Die leere Menge ist offensichtlich eine Jordan-Menge ($G_\varnothing = G$).

(ii) Ist Δ eine (starke) Jordan-Menge, so auch ${}^g\Delta$ für $g \in G$, denn $G_{{}^g\Delta} = gG_\Delta g^{-1}$.

Lemma 6.5. *Seien Δ und Γ (starke) Jordan-Mengen der transitiven G-Menge Ω mit $\Delta \cup \Gamma \neq \Omega$. Dann ist auch $\Delta \cap \Gamma$ eine (starke) Jordan-Menge.*

Beweis. Nach Voraussetzung liegt $\Omega \setminus \Delta$ in einer Bahn Λ_1 unter $G_{\Delta\cap\Gamma}$ ($\supseteq G_\Delta$). Analog liegt auch $\Omega \setminus \Gamma$ in einer Bahn Λ_2 von $G_{\Delta\cap\Gamma}$. Wegen $(\Omega \setminus \Delta) \cap (\Omega \setminus \Gamma) = \Omega \setminus (\Delta \cup \Gamma) \neq \varnothing$ ist $\Lambda_1 = \Lambda_2$, und $G_{\Delta\cap\Gamma}$ ist transitiv auf $(\Omega\setminus\Delta)\cup(\Omega\setminus\Gamma) = \Omega\setminus(\Delta\cap\Gamma)$. Also ist $\Delta\cap\Gamma$ eine Jordan-Menge. Nehmen wir nun an, dass Δ und Γ starke Jordan-Mengen sind. O. B. d. A. sei $|\Delta| \leq |\Gamma|$. Wegen $(\Omega\setminus\Delta)\cap(\Omega\setminus\Gamma) \neq \varnothing$ ist $|\Omega\setminus\Delta| > |(\Omega\setminus\Delta)\cup(\Omega\setminus\Gamma)|/2 = |\Omega\setminus(\Delta\cap\Gamma)|/2$. Nach Satz 6.2 ist $G_{\Delta\cap\Gamma}$ primitiv auf $\Omega \setminus (\Delta \cap \Gamma)$. □

Satz 6.6. *Sei Δ eine (starke) Jordan-Menge der primitiven G-Menge Ω mit $1 \leq |\Delta| \leq |\Omega| - 2$. Dann ist G 2-transitiv (2-primitiv, siehe Aufgabe 3.8).*

Beweis. Ist $|\Delta| = 1$, so sind wir fertig. Sei nun $|\Delta| \geq 2$ und Δ minimal gewählt. Wir setzen

$$\Gamma := \begin{cases} \Delta & \text{falls } |\Delta| \leq \frac{|\Omega|}{2}, \\ \Omega \setminus \Delta & \text{sonst.} \end{cases}$$

Dann ist $2 \leq |\Gamma| \leq |\Omega|/2$. Da Γ kein Block sein kann, existiert ein $g \in G$ mit $0 < |{}^g\Gamma \cap \Gamma| < |\Gamma|$. Insbesondere ist $\Delta \cup {}^g\Delta \neq \Omega$. Nach Lemma 6.5 ist $\Delta \cap {}^g\Delta$ eine (starke) Jordan-Menge im Widerspruch zur Minimalität von Δ (beachte: $(\Omega \setminus \Gamma) \cap (\Omega \setminus {}^g\Gamma) = \Omega \setminus (\Gamma \cup {}^g\Gamma) \neq \varnothing$). □

Satz 6.7 (Jordan)**.** *Sei Δ eine starke Jordan-Menge der primitiven G-Menge Ω mit $|\Delta| \leq |\Omega| - 2$. Dann ist G $(|\Delta| + 1)$-transitiv auf Ω.*

Beweis. Im Fall $\Delta = \varnothing$ ist nichts zu zeigen. Sei also $\Delta \neq \varnothing$. Wir argumentieren durch Induktion nach $|\Omega|$. Sei $\omega \in \Delta$. Offenbar ist $G_\Delta = (G_\omega)_{\Delta\setminus\{\omega\}}$. Nach Satz 6.6 ist G 2-primitiv. Somit ist G_ω primitiv auf $\Omega \setminus \{\omega\}$. Sicher ist G_Δ auch primitiv auf $(\Omega \setminus \{\omega\}) \setminus (\Delta \setminus \{\omega\}) = \Omega \setminus \Delta$. Außerdem ist $|\Delta \setminus \{\omega\}| \leq |\Omega \setminus \{\omega\}| - 2$. Nach Induktion ist daher G_ω $|\Delta|$-transitiv auf $\Omega \setminus \{\omega\}$. Die Behauptung folgt nun aus Lemma 3.3. □

Lemma 6.8. *Sei $G \leq S_n$ primitiv. Enthält G einen 3-Zyklus, so ist $G \in \{S_n, A_n\}$.*

Beweis. Sei $g = (\alpha, \beta, \gamma) \in G$ und $\Delta := \{1, \dots, n\} \setminus \{\alpha, \beta, \gamma\}$. Wegen $g \in G_\Delta$ operiert G_Δ transitiv und damit primitiv auf $\{1, \dots, n\} \setminus \Delta = \{\alpha, \beta, \gamma\}$. Nach Satz 6.7 ist G $(n-2)$-transitiv. Insbesondere ist $\frac{n!}{2} \leq |G|$ (Lemma 3.4) und die Behauptung folgt. □

Lemma 6.9. *Sei $\sigma \in S_n$ ein Zyklus der Länge n. Dann ist $\mathrm{C}_{S_n}(\sigma) = \langle \sigma \rangle$.*

Beweis. Die $(n-1)!$ Zyklen der Länge n sind nach Beispiel 1.10 alle in S_n konjugiert. Also ist $|\mathrm{C}_{S_n}(\sigma)| \leq n$. Umgekehrt ist sicher $\langle \sigma \rangle \leq \mathrm{C}_{S_n}(\sigma)$ (vgl. Aufgabe 4.2). □

Satz 6.10. *Sei $G \leq S_n$ eine primitive Permutationsgruppe, und sei $p \leq n-3$ eine Primzahl. Enthält G einen p-Zyklus, so ist $G \in \{S_n, A_n\}$.*

Beweis. Nach Lemma 6.8 können wir $p \neq 3$ annehmen. Sei $g \in G$ ein p-Zyklus und $\Delta := \{\omega \in \Omega : {}^g\omega = \omega\}$ mit $\Omega := \{1, \dots, n\}$. Nach Satz 6.7 ist G $|\Delta|$-transitiv auf Ω. Sei $H := \{h \in G : {}^h\Delta = \Delta\}$. Dann ist die Operation $\varphi : H \to \mathrm{Sym}(\Delta)$ surjektiv, d. h. $H/G_\Delta \cong \mathrm{Sym}(\Delta)$. Da G_Δ treu auf $\Omega \setminus \Delta$ operiert, ist $P := \langle g \rangle \in \mathrm{Syl}_p(G_\Delta)$. Wegen $G_\Delta \trianglelefteq H$ folgt nun $H = G_\Delta \, \mathrm{N}_H(P)$ aus Satz 1.19 wie üblich. Bekanntlich ist $\mathrm{N}_H(P)/\mathrm{C}_H(P) \leq \mathrm{Aut}(P)$ abelsch. Insbesondere ist $\mathrm{C}_H(P)G_\Delta \trianglelefteq H$ mit abelscher Faktorgruppe

$$H/\mathrm{C}_H(P)G_\Delta \cong \mathrm{N}_H(P)/(\mathrm{N}_H(P) \cap \mathrm{C}_H(P)G_\Delta) = \mathrm{N}_H(P)/\mathrm{C}_H(P)(\mathrm{N}_H(P) \cap G_\Delta).$$

Also ist $\mathrm{Alt}(\Delta) \subseteq \varphi(\mathrm{C}_H(P)G_\Delta)$. Wegen $|\Delta| = n - p \geq 3$ existiert ein $x \in \mathrm{C}_H(P)$, sodass $\varphi(x)$ ein 3-Zyklus ist. Betrachten wir nun die Operation $\psi : H \to \mathrm{Sym}(\Omega \setminus \Delta)$. Nach Lemma 6.9 ist $\psi(x) \in \mathrm{C}_{\mathrm{Sym}(\Omega\setminus\Delta)}(\psi(g)) = \langle \psi(g) \rangle$. Insbesondere ist $\psi(x^p) = 1$, d. h. x^p operiert trivial auf $\Omega \setminus \Delta$. Wegen $p \neq 3$ ist auch $\varphi(x^p)$ ein 3-Zyklus. Also ist x^p ein 3-Zyklus auf Ω und die Behauptung folgt aus Lemma 6.8. □

Beispiel 6.11. Sei $G \leq S_n$ transitiv mit $n \geq 8$. Nach Bertrands Postulat aus der Zahlentheorie existiert stets eine Primzahl p mit $n/2 < p < n-2$. Ist $p \mid |G|$, so enthält G einen p-Zyklus. Nach Satz 6.2 ist G primitiv, und nach Satz 6.10 folgt $G \in \{S_n, A_n\}$.

Bemerkung 6.12. Jones hat mit Hilfe der CFSG gezeigt, dass Satz 6.10 richtig bleibt, wenn p keine Primzahl ist.

Lemma 6.13. *Seien $x, y \in S_n$, sodass es genau ein $\omega \in \{1, \dots, n\}$ mit ${}^x\omega \neq \omega \neq {}^y\omega$ gibt. Dann ist $xyx^{-1}y^{-1}$ ein 3-Zyklus.*

Beweis. Nach Voraussetzung ist ${}^{ab}\omega = {}^b\omega$ für $a \in \{x^{\pm 1}, y^{\pm 1}\}$ und $b \in \{x^{\pm 1}, y^{\pm 1}\} \setminus \{a^{\pm 1}\}$. Insbesondere ist ${}^x\omega \neq {}^y\omega$. Wir zeigen, dass $z := xyx^{-1}y^{-1}$ der 3-Zyklus $(\omega, {}^x\omega, {}^y\omega)$ ist. Dafür genügt es zu zeigen, dass z jedes $\alpha \in \{1, \dots, n\} \setminus \{\omega, {}^x\omega, {}^y\omega\}$ festlässt. Dies ist klar, falls α von x und y nicht bewegt wird. Wird α von x bewegt, so bleiben α und ${}^{x^{-1}}\alpha$ fest unter y. Also ist ${}^z\alpha = \alpha$. Der Fall ${}^y\alpha \neq \alpha$ ist analog. □

Satz 6.14 (Bochert)**.** *Sei $G \leq S_n$ eine primitive Permutationsgruppe mit $A_n \not\subseteq G$. Dann ist*

$$|G| \leq n(n-1)\dots(n - \lfloor n/2 \rfloor + 1).$$

Beweis. Wähle $\Delta \subseteq \Omega := \{1, \dots, n\}$ minimal mit $G_\Delta = 1$ (im Zweifel $\Delta = \Omega$). Nehmen wir $|\Delta| > n/2$ an. Wegen $|\Omega \setminus \Delta| < n/2 < |\Delta|$ existiert ein $1 \neq x \in G_{\Omega\setminus\Delta}$. Sei $\omega \in \Delta$ mit ${}^x\omega \neq \omega$. Nach Wahl von Δ existiert auch ein $1 \neq y \in G_{\Delta\setminus\{\omega\}}$. Nach Lemma 6.13 ist $xyx^{-1}y^{-1} \in G$ ein 3-Zyklus und Lemma 6.8 liefert einen Widerspruch. Also ist $|\Delta| \leq n/2$. Sei $S := S_n$. Dann ist

$$|S : G| \geq \frac{|S_\Delta G|}{|G|} = |S_\Delta : S_\Delta \cap G| = |S_\Delta| = |\mathrm{Sym}(\Omega \setminus \Delta)| = (n - |\Delta|)! \geq (n - \lfloor n/2 \rfloor)!$$

und die Behauptung folgt. □

Bemerkung 6.15. Maróti hat mit Hilfe der CFSG gezeigt, dass die Ungleichung $|G| < 50n^{\sqrt{n}}$ in der Situation von Satz 6.14 gilt. Eine Teilmenge $\Delta \subseteq \Omega$ mit $G_\Delta = 1$ nennt man im Englischen *base*.

Beispiel 6.16. Wir hatten in Beispiel 5.17 bereits gesehen, dass $G := \mathrm{GL}(3,2)$ eine einfache primitive Permutationsgruppe vom Grad 7 ist. Nach Satz 6.14 hat jede primitive Permutationsgruppe vom Grad 7, die nicht zu A_7 oder S_7 isomorph ist, Ordnung $\leq 7 \cdot 6 \cdot 5 = 210$. Also ist G die einzige solche Gruppe mit Sockel $\mathrm{GL}(3,2)$ (dennoch ist $G < \mathrm{Aut}(G)$, siehe Beispiel 8.14(ii)). Wir befassen uns nun mit der Eindeutigkeit dieser Operation.

Lemma 6.17.

(i) Je zwei einfache Untergruppen von S_7 der Ordnung 168 sind konjugiert.

(ii) $\mathrm{GL}(3,2)$ *ist bis auf Isomorphie die einzige einfache Gruppe der Ordnung* 168.

Beweis.

(i) Sei $G \leq S_7$ einfach mit $|G| = 168$. Wie üblich ist $G \leq A_7$. Ähnlich wie in Satz 3.20 zeigen wir, dass G bis auf Permutation der Ziffern eindeutig ist. O. B. d. A. sei

$$x := (1, \ldots, 7) \in G$$

und $P := \langle x \rangle \in \mathrm{Syl}_7(G)$. Nach Sylow ist $|\mathrm{N}_G(P)| = 21$. Die 7-Zyklen in A_7 verteilen sich auf 5! viele 7-Sylowgruppen. Also ist $|\mathrm{N}_{A_7}(P)| = 21$ und $\mathrm{N}_G(P) = \mathrm{N}_{A_7}(P)$. Wir können also

$$y := (2,3,5)(4,7,6) \in \mathrm{N}_G(P)$$

wählen. Dann ist $Q := \langle y \rangle \in \mathrm{Syl}_3(G)$. Offenbar ist $\mathrm{C}_G(Q) \leq \mathrm{C}_{A_7}(Q) = \langle (2,3,5), (4,7,6) \rangle$ und $\mathrm{C}_G(Q) = Q$. Wegen $|\mathrm{Aut}(Q)| = 2$ ist $|\mathrm{N}_G(Q)| \leq 6$. Nach Sylow ist $|\mathrm{N}_G(Q)| = 6$. Sei $z \in \mathrm{N}_G(Q)$ eine Involution. Indem man z durch zy^i für ein $i \in \{0,1,2\}$ ersetzt, kann man

$$z \in \{(3,5)(4,7), (3,5)(6,7), (3,5)(4,6)\}$$

annehmen. Der letzte Fall ist ausgeschlossen wegen $(3,5)(4,6)x^2 = (1,5,7,2,6) \notin G$. Betrachte nun $g := (2,4,3,7,5,6) \in S_7$. Dann ist $gxg^{-1} = x^3$ und $g \in \mathrm{N}_{S_7}(P)$. Wir können also G mit g konjugieren ohne $\mathrm{N}_G(P) = \mathrm{N}_{A_7}(P)$ zu verändern. Dabei wird die erste Möglichkeit für z auf die zweite abgebildet. Man kann also

$$z = (3,5)(6,7)$$

annehmen. Sei nun $H := \langle x, y, z \rangle$. Wegen $|G : H| \leq 4$ ist $H = G$.

(ii) Sei G eine einfache Gruppe der Ordnung 168. Nach (i) genügt es zu zeigen, dass G eine Untergruppe der Ordnung 24 besitzt. Sei $P \in \mathrm{Syl}_3(G)$. Nach Sylow ist $|\mathrm{N}_G(P)| \in \{6, 24, 42\}$. Im letzten Fall kann G nicht treu auf den vier Nebenklassen $G/\mathrm{N}_G(P)$ operieren. Dies widerspricht also der Einfachheit von G. Im zweiten Fall wären wir fertig. Nehmen wir also $|\mathrm{N}_G(P)| = 6$ an. Sei $Q \in \mathrm{Syl}_2(G)$. Hier kann man analog $\mathrm{N}_G(Q) = Q$ annehmen. Gibt es eine weitere 2-Sylowgruppe S mit $|Q \cap S| = 4$, so ist $Q, S \subseteq \mathrm{N}_G(Q \cap S)$ und es besteht nur die Möglichkeit $|\mathrm{N}_G(Q \cap S)| = 24$. Schneiden sich je zwei 2-Sylowgruppen trivial, so gibt es $7 \cdot 21 = 147$ viele 2-Elemente und es ist kein Platz mehr für die $2 \cdot 28 = 56$ Elemente der Ordnung 3. Wir können somit annehmen, dass $|Q \cap S| = 2$ ein maximal großer Sylowschnitt ist (vgl. Aufgabe 1.11). Bekanntlich ist $\mathrm{Z}(Q) \neq 1$ (Algebra 1). Man sieht daher leicht, dass $4 \mid |\mathrm{N}_G(Q \cap S)|$ gilt. Besitzt $\mathrm{N}_G(Q \cap S)$ nur eine 2-Sylowgruppe R, so ist $Q \cap S < \mathrm{N}_Q(Q \cap S) \leq Q \cap R$ und $R \leq Q$ nach Wahl von S. Analog ist aber auch $Q \cap S < \mathrm{N}_S(Q \cap S) \leq S \cap R \leq S \cap Q$ und man hat einen Widerspruch. Also hat $\mathrm{N}_G(Q \cap S)$ mehrere 2-Sylowgruppen und es gilt $|\mathrm{N}_G(Q \cap S)| \in \{12, 24, 28\}$. Im letzten Fall wäre wie üblich $G \leq S_6$, aber 6! ist nicht durch 7 teilbar. Wir können daher $|\mathrm{N}_G(Q \cap S)| = 12$ annehmen. Wegen $|\mathrm{N}_G(P)| = 6$ hat $\mathrm{N}_G(Q \cap S)$ genau vier 3-Sylowgruppen. Es ist daher nur Platz für eine 2-Sylowgruppe. Widerspruch. □

Beispiel 6.18. Nach Lemma 6.17 und Aufgabe 1.4 ist die Operation der primitiven Gruppe $\mathrm{GL}(3,2)$ vom Grad 7 bis auf Isomorphie eindeutig. Sei nun $G \notin \{A_7, S_7\}$ eine beliebige primitive Permutationsgruppe vom Grad 7 und Typ (F). Dann ist $7 \mid |\mathrm{Soc}(G)| \mid \frac{7!}{2} = |A_7|$ und $|G| \leq 210$ nach Satz 6.14. Nach Satz 6.10 ist sogar $|\mathrm{Soc}(G)| \mid 2^3 \cdot 3^2 \cdot 7$. Also besitzt $\mathrm{Soc}(G)$ genau acht 7-Sylowgruppen und es folgt $|\mathrm{Soc}(G)| = 168$. Nach Lemma 6.17 ist $\mathrm{Soc}(G) \cong \mathrm{GL}(3,2)$ und Beispiel 6.16 impliziert $G = \mathrm{Soc}(G)$. Also ist $\mathrm{GL}(3,2)$ die einzige primitive Permutationsgruppe vom Grad 7 und Typ (F) mit nicht-alternierendem Sockel ist. Die entsprechenden Gruppen vom Typ (A) kann man leicht mit Satz 2.14 angeben: C_7, $C_7 \rtimes C_2$, $C_7 \rtimes C_3$ und $C_7 \rtimes C_6 \cong \mathrm{Aff}(1,7)$.

Aufgabe 6.1. Zeigen Sie, dass die Voraussetzung $p \leq n - 3$ in Satz 6.10 notwendig ist.

Aufgabe 6.2. Bestimmen Sie die primitiven Permutationsgruppen vom Grad 8 und Typ (A).

Aufgabe 6.3. Bestimmen Sie die primitiven Permutationsgruppen G mit $\mathrm{Soc}(G) \cong A_7$ und klassifizieren Sie deren Operationen bis auf Isomorphie.

Aufgabe 6.4.

(i) Sei M eine maximale Untergruppe einer auflösbaren endlichen Gruppe G. Zeigen Sie, dass $|G : M|$ eine Primzahlpotenz ist.

(ii) Sei umgekehrt G eine beliebige endliche Gruppe, in der der Index jeder maximalen Untergruppe eine Primzahlpotenz ist. Ist G dann auflösbar?

Aufgabe 6.5. Sei $1 \neq \sigma \in S_n$ mit $n \neq 4$. Zeigen Sie, dass ein $\tau \in S_n$ mit $\langle \sigma, \tau \rangle = S_n$ existiert. Warum ist der Fall $n = 4$ eine Ausnahme?

Aufgabe 6.6. Welcher der beiden folgenden Zustände eines Schiebepuzzles lässt sich in die richtige Reihenfolge bringen? (Man darf das leere Feld mit einem vertikal oder horizontal benachbarten Feld vertauschen.)

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

1	2	3	4
5	6	7	8
9	10	11	12
14	15	13	

7 Transitive Gruppen mit Primzahlgrad

Definition 7.1. Sei K ein Körper. Mittels des Ringhomomorphismus $\mathbb{Z} \to K$, $1 \mapsto 1$ können wir die ganzen Zahlen mit Elementen in K identifizieren (im Allgemeinen aber nicht injektiv). Sei $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein Polynom. Dann ist $f' := \sum_{i=1}^{n} i a_i X^{i-1} \in K[X]$ die (*erste*) *Ableitung* von f. Für $k \geq 2$ definieren wir induktiv die *k-te Ableitung* $f^{(k)} := (f^{(k-1)})'$. Außerdem sei $f^{(0)} := f$.

Bemerkung 7.2.

(i) In der Algebra muss man zwischen einem Polynom in $K[X]$ und der entsprechenden Funktion $K \to K$ unterscheiden. Beispielsweise entspricht $X^2 + X \in \mathbb{F}_2[X]$ der Nullabbildung.

(ii) Für $K = \mathbb{F}_p$ ist $(X^p)' = 0$.

(iii) Für $f, g \in K[X]$ und $\alpha, \beta \in K$ ist sicher $(\alpha f + \beta g)' = \alpha f' + \beta g'$.

(iv) Für $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ und $\alpha \in K$ ist

$$f(X+\alpha) = \sum_{i=0}^{n} a_i (X+\alpha)^i = \sum_{i=0}^{n} a_i \sum_{k=0}^{i} \binom{i}{k} \alpha^{i-k} X^k = \sum_{k=0}^{n} \left(\sum_{i=k}^{n} a_i \binom{i}{k} \alpha^{i-k} \right) X^k \in K[X].$$

Für $g \in K[X]$ und $\beta, \gamma \in K$ ist dann sicher $(\beta f + \gamma g)(X+\alpha) = \beta f(X+\alpha) + \gamma g(X+\alpha)$ und $(fg)(X+\alpha) = f(X+\alpha)g(X+\alpha)$. Außerdem ist

$$\begin{aligned} f(X+\alpha)' &= \sum_{k=1}^{n} \left(k \sum_{i=k}^{n} a_i \binom{i}{k} \alpha^{i-k} \right) X^{k-1} = \sum_{k=0}^{n-1} \left(\sum_{i=k}^{n-1} (i+1) a_{i+1} \frac{k+1}{i+1} \binom{i+1}{k+1} \alpha^{i-k} \right) X^k \\ &= \sum_{k=0}^{n-1} \left(\sum_{i=k}^{n-1} (i+1) a_{i+1} \binom{i}{k} \alpha^{i-k} \right) X^k = \sum_{i=0}^{n-1} (i+1) a_{i+1} (X+\alpha)^i = f'(X+\alpha). \end{aligned}$$

Dies entspricht einem Spezialfall der Kettenregel aus der Analysis.

Lemma 7.3. *Sei p eine Primzahl und $\varnothing \neq U \subsetneq \mathbb{F}_p^\times$. Sei $\sigma \in \mathrm{Sym}(\mathbb{F}_p)$ mit der Eigenschaft*

$$x - y \in U \Longrightarrow \sigma(x) - \sigma(y) \in U$$

für $x, y \in \mathbb{F}_p$. Dann existieren $\alpha, \beta \in \mathbb{F}_p$ mit $\sigma(x) = \alpha x + \beta$ für alle $x \in \mathbb{F}_p$.

Beweis. Durch wiederholte Anwendung von σ sieht man, dass $x - y \in U \iff \sigma(x) - \sigma(y) \in U$ gilt. Insbesondere kann man U durch $\mathbb{F}_p^\times \setminus U$ ersetzen. Wir können daher $|U| \leq (p-1)/2$ annehmen. Sei nun $x \in \mathbb{F}_p$ fest. Für $u \in U$ ist dann sicher $(u+x) - x \in U$ und somit $\sigma(u+x) - \sigma(x) \in U$. Für verschiedene u sind auch $\sigma(u+x) - \sigma(x)$ verschieden, da σ bijektiv ist. Also ist $U = \{\sigma(u+x) - \sigma(x) : u \in U\}$ und $\{\sigma(x+u) : u \in U\} = \{\sigma(x) + u : u \in U\}$. Für $m \in \mathbb{N}$ ist daher

$$\sum_{u \in U} \sigma(x+u)^m = \sum_{u \in U} (\sigma(x) + u)^m. \tag{7.1}$$

Bekanntlich existiert ein Polynom $f \in \mathbb{F}_p[X]$ vom Grad $n \leq p-1$ mit $f(x) = \sigma(x)$ für alle $x \in \mathbb{F}_p$ (Stichwort: Interpolation, Lagrange-Polynom). Es genügt zu zeigen, dass $n = 1$ gilt. Sei m maximal mit $nm \leq p-1$.

Wegen Gleichung 7.1 hat das Polynom $\sum_{u \in U} f(X+u)^m - \sum_{u \in U} (f(X) + u)^m$ mindestens p Nullstellen und Grad $\leq p-1$. Nach Algebra 1 ist also

$$\sum_{u \in U} f(X+u)^m = \sum_{u \in U} (f(X) + u)^m.$$

Für $k \geq 1$ sei $S(k) := \sum_{u \in U} u^k$. Aus dem binomischen Satz folgt dann

$$\sum_{u \in U} \big(f(X+u)^m - f(X)^m\big) = \sum_{u \in U} \sum_{k=1}^{m} \binom{m}{k} u^k f(X)^{m-k} = \sum_{k=1}^{m} \binom{m}{k} S(k) f(X)^{m-k}.$$

Wegen $nm \leq p-1$ hat die l-te Ableitung $(f(X)^m)^{(l)}$ den Grad $mn-l$. Insbesondere existieren $\alpha_0, \ldots, \alpha_{nm} \in \mathbb{F}_p$ mit

$$X^{nm} = \sum_{l=0}^{nm} \alpha_l \big(f(X)^m\big)^{(l)}.$$

Dies impliziert

$$\begin{aligned}
\sum_{u \in U} \big((X+u)^{nm} - X^{nm}\big) &= \sum_{u \in U} \Big(\sum_{l=0}^{nm} \alpha_l \big(f(X+u)^m\big)^{(l)} - \sum_{l=0}^{nm} \alpha_l \big(f(X)^m\big)^{(l)} \Big) \\
&= \sum_{l=0}^{nm} \alpha_l \sum_{u \in U} \Big(\big(f(X+u)^m\big)^{(l)} - \big(f(X)^m\big)^{(l)} \Big) \\
&= \sum_{l=0}^{nm} \alpha_l \sum_{k=1}^{m} \binom{m}{k} S(k) \big(f(X)^{m-k}\big)^{(l)}
\end{aligned}$$

nach Bemerkung 7.2. Sei $r \geq 1$ minimal mit $S(r) \neq 0$. Im Fall $r \leq nm$ liefert ein Gradvergleich $nm - r \leq n(m-r)$, und die Behauptung folgt (man beachte, dass $\binom{nm}{r} \neq 0$ wegen $p > nm$). Sei nun $r \geq nm+1$. Nach Wahl von m ist $2r \geq 2nm \geq n(m+1) \geq p$ und $S(i) = 0$ für $i = 1, \ldots, (p-1)/2$. Sei $U = \{u_1, \ldots, u_k\}$. Bekanntlich ist die Vandermonde-Matrix $(u_j^{i-1})_{i,j=1,\ldots,k}$ invertierbar. Da die Determinante linear in den Spalten ist und $0 \notin U$ gilt, ist auch $M := (u_j^i)_{i,j=1,\ldots,k}$ invertierbar. Wegen $k = |U| \leq (p-1)/2$ ist aber $Mv = 0$ für $v = (1, \ldots, 1)$. Widerspruch. □

Satz 7.4 (Burnside)**.** *Sei G eine transitive Permutationsgruppe vom Primzahlgrad p. Dann ist G 2-transitiv oder $G \cong C_p \rtimes C_d$ für einen echten Teiler d von $p-1$.*

Beweis (Müller). Wir können $G \leq \mathrm{Sym}(\mathbb{F}_p)$ annehmen. Sei außerdem G nicht 2-transitiv. Wegen der Transitivität ist $p \mid |G|$ und es gibt ein Element $\sigma \in G$ der Ordnung p. Indem man G geeignet in $\mathrm{Sym}(\mathbb{F}_p)$ konjugiert, kann man annehmen, dass $\sigma(x) = x+1$ für alle $x \in \mathbb{F}_p$ gilt. Seien $x, y \in \mathbb{F}_p$ mit $x \neq y$ fest. Wir definieren $U := \{\tau(x) - \tau(y) : \tau \in G\} \subseteq \mathbb{F}_p^\times$. Sind nun $x', y' \in \mathbb{F}_p$ mit $x' - y' \in U$, so existiert ein $\tau \in G$ mit $x' - y' = \tau(x) - \tau(y)$. Also existiert auch ein $i \in \{0, \ldots, p-1\}$ mit $\sigma^i(\tau(x)) = \tau(x) + i = x'$ und $\sigma^i(\tau(y)) = \tau(y) + i = y'$. Für alle $\rho \in G$ ist also $\rho(x') - \rho(y') = (\rho\sigma^i\tau)(x) - (\rho\sigma^i\tau)(y) \in U$. Da G nicht 2-transitiv ist, existieren $x', y' \in \mathbb{F}_p$ mit $x' \neq y'$ und $(\tau(x), \tau(y)) \neq (x', y')$ für alle $\tau \in G$. Das gleiche Argument wie eben zeigt $x' - y' \notin U$. Insbesondere ist U eine echte Teilmenge von $\mathbb{F}_p^\times$. Nach Lemma 7.3 hat jedes Element in G die Form $x \mapsto \alpha x + \beta$ mit $\alpha, \beta \in \mathbb{F}_p$. Also liegt G im Bild der Operation $\mathrm{Aff}(1,p) \to \mathrm{Sym}(\mathbb{F}_p)$ von Satz 2.12. Dies zeigt $G \cong C_p \rtimes C_d$ mit $d \mid p-1$. Im Fall $d = p-1$ wäre G (scharf) 2-transitiv. □

Bemerkung 7.5.

(i) Burnsides ursprünglicher Beweis von Satz 7.4 war eine der ersten Anwendungen der Charaktertheorie (siehe Anhang, Satz A.3).

(ii) Zusammen mit Satz 5.19 (oder Satz 5.7) folgt, dass jede primitive Permutationsgruppe mit Primzahlgrad Typ (A) oder (F) hat.

(iii) Guralnick und Wales haben mit Hilfe der CFSG gezeigt, dass für eine primitive Permutationsgruppe G vom Grad $2p$ (p Primzahl) eine der folgenden Aussagen gilt:

  (a) G ist 2-transitiv.

  (b) $p = 5$ und $G \in \{A_5, S_5\}$ (vgl. Beispiel 8.27(ii)).

Aufgabe 7.1. Sei $G \leq S_p$ transitiv für eine Primzahl p. Zeigen Sie, dass $G/\mathrm{Soc}(G)$ zyklisch ist.

8 Subgrade

Bemerkung 8.1. Sei $G \leq \mathrm{Sym}(\Omega)$ primitiv, aber nicht 2-transitiv (vgl. Bemerkung 5.20). Dann operiert G_ω für $\omega \in \Omega$ nicht transitiv auf $\Omega \setminus \{\omega\}$. Wir werden im Folgenden sehen, dass die Primitivität trotzdem starke Einschränkungen an die Bahnen(längen) von G_ω liefert.

Definition 8.2. Sei $G \leq \mathrm{Sym}(\Omega)$ transitiv und $\omega \in \Omega$. Die Anzahl der Bahnen von G_ω auf Ω ist der *Rang* von G. Sei $\Delta \subseteq \Omega \setminus \{\omega\}$ eine Bahn von G_ω. Wir bezeichnen das Bild der Operation $G_\omega \to \mathrm{Sym}(\Delta)$ mit G_ω^Δ. Außerdem ist $|\Delta|$ ein *Subgrad* (engl. subdegree) von G. Sei $\delta \in \Delta$. Dann existiert ein $g \in G$ mit ${}^g\omega = \delta$. Offenbar ist ${}^{g^{-1}}\omega \in \Omega \setminus \{\omega\}$. Wir bezeichnen die Bahn von ${}^{g^{-1}}\omega$ unter G_ω mit Δ^*.

Lemma 8.3. *In der Situation von Definition 8.2 gilt:*

(i) Die Subgrade von G hängen nicht von der Wahl von ω ab.

(ii) Δ^* hängt nicht von der Wahl von δ oder g ab.

(iii) $|\Delta^*| = |\Delta|$ und $(\Delta^*)^* = \Delta$.

(iv) Ist $|G|$ ungerade, so ist $\Delta \neq \Delta^*$.

(v) Ist G primitiv und nicht-regulär, so ist $|\Delta| > 1$.

Beweis.

(i) Sei $\omega' \in \Omega$. Dann existiert ein $g \in G$ mit ${}^g\omega = \omega'$. Offenbar ist die Abbildung $\Delta \mapsto {}^g\Delta$ eine Bijektion zwischen den Bahnen von G_ω und den Bahnen von $G_{\omega'} = gG_\omega g^{-1}$.

(ii) Seien $\delta, \delta' \in \Delta$ und $g, g' \in G$ mit ${}^g\omega = \delta$ und ${}^{g'}\omega = \delta'$. Dann existiert ein $h \in G_\omega$ mit ${}^h\delta = \delta'$. Also ist ${}^{g'^{-1}hg}\omega = \omega$ und $g'^{-1}hg \in G_\omega$. Daher sind ${}^{g^{-1}}\omega$ und ${}^{g'^{-1}}\omega$ in der gleichen Bahn von G_ω.

(iii) Es gilt $|\Delta| = |G_\omega : G_\omega \cap G_\delta| = |G_\omega : G_\omega \cap G_{g\omega}| = |G_\omega : G_{g^{-1}\omega} \cap G_\omega| = |\Delta^*|$. Die zweite Aussage folgt leicht aus (ii).

(iv) Sei $\Delta = \Delta^*$. Dann existiert ein $h \in G_\omega$ mit ${}^{hg}\omega = {}^{g^{-1}}\omega$. Also vertauscht hg die Elemente ω und ${}^{g^{-1}}\omega$. Folglich ist $2 \mid |\langle hg \rangle| \mid |G|$.

(v) Sei G primitiv. Gilt $\Delta = \{\delta\}$, so ist $G_\omega \subseteq G_\delta$ und $G_\omega = G_\delta$ wegen der Transitivität. Für $g \in G$ mit ${}^g\omega = \delta$ ist also $g \in \mathrm{N}_G(G_\omega)$. Da G_ω maximal ist, folgt $\mathrm{N}_G(G_\omega) = G$ und $G_\omega \trianglelefteq G$. Satz 2.2 liefert $G_\omega = 1$, d. h. G ist regulär. □

Beispiel 8.4.

(i) Sei G eine primitive Permutationsgruppe vom Grad 9 und ungerader Ordnung. Offenbar sind dann auch die Subgrade $d_1, \ldots, d_k$ ungerade. Da 9 keine Primzahl ist, kann G nicht regulär sein. Nach Lemma 8.3 ist $d_i \geq 3$ und $8 = d_1 + \ldots + d_k$. Außerdem treten die d_i in Paaren auf. Das dies nicht aufgeht, kann G nicht existieren.

(ii) Offenbar hat eine Permutationsgruppe genau dann Rang 2, wenn sie 2-transitiv ist. Sei nun $G \leq S_n$ 4-transitiv. Dann operiert G sicher auch transitiv auf der Menge P_2 der zweielementigen Teilmengen von $\{1, \ldots, n\}$. Sei $H \leq G$ der Stabilisator von $\{1, 2\}$. Dann werden die nicht-trivialen Bahnen von H auf P_2 durch $\{1, 3\}$ und $\{3, 4\}$ repräsentiert. Bezüglich dieser Operation hat G also Rang 3. Mit Hilfe der CFSG kann man alle primitiven Permutationsgruppen mit Rang 3 bestimmen. Es treten dabei nur die Typen (A), (F) und (P) auf (siehe Anhang, Satz A.6).

(iii) Sei S eine nichtabelsche einfache Gruppe und $G = S^2$ vom Typ (D). Nach Satz 2.1 entsprechen die Bahnen des Stabilisators $D := \{(x, x) : x \in S\} \cong S$ genau den Konjugationsklassen von S.

Definition 8.5. Sei $G \leq \mathrm{Sym}(\Omega)$ transitiv. Dann operiert G durch ${}^g(\alpha, \beta) = ({}^g\alpha, {}^g\beta)$ auf $\Omega \times \Omega$. Die entsprechenden Bahnen heißen *Orbitale*. Für ein festes $\omega \in \Omega$ ist die Abbildung $\Delta \mapsto \{\alpha \in \Omega : (\omega, \alpha) \in \Delta\} =: \Delta(\omega)$ offenbar eine Bijektion zwischen der Menge der Orbitale und der Menge der Bahnen von G_ω. Das *triviale* Orbital $\{(\alpha, \alpha) : \alpha \in \Omega\}$ geht dabei auf die triviale Bahn $\{\omega\}$. Für ein Orbital Δ sei $\mathcal{G}_\Delta$ der gerichtete Graph mit Knotenmenge Ω und Pfeilmenge Δ. Für eine Bahn $\Delta(\omega)$ von G_ω sei $\mathcal{G}_{\Delta(\omega)} := \mathcal{G}_\Delta$.

Bemerkung 8.6. Sei Δ ein Orbital von G und $\omega \in \Omega$. Dann ist $\Delta^* := \{(\alpha, \beta) \in \Omega \times \Omega : (\beta, \alpha) \in \Delta\}$ ein Orbital mit $\Delta^*(\omega) = \Delta(\omega)^*$ nach Aufgabe 8.2.

Beispiel 8.7. Sei G eine transitive Permutationsgruppe mit ungeradem Grad n. Sei Δ ein nicht-triviales Orbital, sodass auch der entsprechende Subgrad $|\Delta(\omega)|$ ungerade ist. Dann ist $|\Delta| = n|\Delta(\omega)|$ ungerade und $\Delta^* \neq \Delta$. Die ungeraden Subgrade müssen hier also in Paaren auftreten.

Satz 8.8 (Higman)**.** *Eine transitive Operation $G \to \mathrm{Sym}(\Omega)$ ist genau dann primitiv, falls $\mathcal{G}_\Delta$ für jedes nicht-triviale Orbital zusammenhängend ist.*

Beweis. Nehmen wir zunächst an, dass $\mathcal{G}_\Delta$ für jedes nicht-triviale Orbital zusammenhängend ist. Sei $\Gamma \subseteq \Omega$ mit $1 < |\Gamma| < |\Omega|$. Wähle $\alpha, \beta \in \Gamma$ mit $\alpha \neq \beta$. Dann existiert ein nicht-triviales Orbital Δ mit $(\alpha, \beta) \in \Delta$. Da $\mathcal{G}_\Delta$ zusammenhängend ist, existiert ein $g \in G$ mit ${}^g\alpha \in \Gamma$ und ${}^g\beta \notin \Gamma$. Insbesondere ist $\varnothing \neq \Gamma \cap {}^g\Gamma \neq \Gamma$. Dies zeigt, dass G primitiv ist.

Sei nun umgekehrt G primitiv und Δ ein nicht-triviales Orbital. Sei $\omega \in \Omega$, und sei $\Gamma \subseteq \Omega$ die Menge der Punkte, die man durch einen Pfad in $\mathcal{G}_\Delta$ von ω erreichen kann. Wir lassen dabei auch Pfade der Länge 0 zu, d. h. $\omega \in \Gamma$. Da Δ nicht trivial ist, gilt $|\Gamma| > 1$. Sei $(\alpha, \beta) \in \Delta$ und $g \in G$ mit ${}^g\alpha = \beta$. Dann ist $({}^{g^i}\alpha, {}^{g^{i+1}}\alpha) = ({}^{g^i}\alpha, {}^{g^i}\beta) \in \Delta$ für $i = 1, \ldots, |\langle g \rangle| - 1$. Somit erhält man einen Pfad von β nach α in $\mathcal{G}_\Delta$. Dies zeigt, dass Γ eine Zusammenhangskomponente des *ungerichteten* Graphen $\mathcal{G}_\Delta$ ist. Insbesondere ist auch ${}^g\Gamma$ eine Zusammenhangskomponente und es folgt $\Gamma \cap {}^g\Gamma \in \{\varnothing, \Gamma\}$. Die Primitivität von G zeigt $\Gamma = \Omega$, d. h. $\mathcal{G}_\Delta$ ist zusammenhängend. □

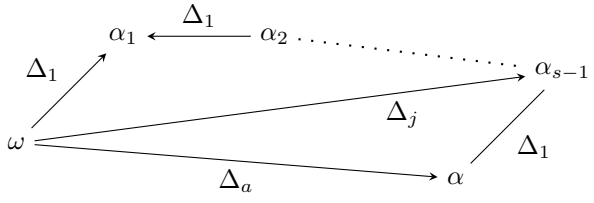
Bemerkung 8.9. Für 2-transitive Operationen ist $\mathcal{G}_\Delta$ offensichtlich sogar vollständig.

Satz 8.10 (Neumann)**.** *Sei G eine nicht-reguläre, primitive Permutationsgruppe auf Ω mit Subgraden $d_1 \leq \ldots \leq d_k$. Dann ist $d_{i+1} \leq d_i(d_1 - 1)$ für $i = 1, \ldots, k-1$.*

Beweis. Seien $\Delta_1, \ldots, \Delta_k$ die nicht-trivialen Orbitale von G und $\omega \in \Omega$ mit $|\Delta_i(\omega)| = d_i \geq 2$ für $i = 1, \ldots, k$. Sei $i \in \{1, \ldots, k-1\}$ fest, und sei

$$\Gamma := \{(\alpha, \beta) \in \Omega \times \Omega : \exists\, \gamma \in \Omega : (\alpha, \gamma), (\beta, \gamma) \in \Delta_1\}.$$

Sicher ist Γ eine Vereinigung von Orbitalen. Sei $(\alpha, \omega) \in \Delta_1$. Dann existiert ein $h \in G_\omega$ mit $\alpha \neq {}^h\alpha =: \beta$. Also ist $(\alpha, \beta) \in \Gamma$, und Γ enthält ein nicht-triviales Orbital. Nach Satz 8.8 sind also alle Elemente aus Ω durch einen Pfad aus Γ verbunden. Für $\alpha \in \Omega$ gibt es somit einen Pfad $\omega = \alpha_0, \ldots, \alpha_s = \alpha$ mit $(\alpha_j, \alpha_{j+1}) \in \Delta_1$ (bzw. $(\alpha_{j+1}, \alpha_j) \in \Delta_1$), falls j gerade (bzw. ungerade) ist. Wir wählen $a > i$, $\alpha \in \Delta_a(\omega)$ und diesen Pfad, sodass s möglichst klein ist. Dann ist $s \geq 2$. Außerdem ist $(\omega, \alpha_{s-1}) \in \Delta_j$ für ein $j \leq i$ nach Wahl von α.



Sei o. B. d. A. s ungerade (anderenfalls ersetze man im Folgenden Δ_1 durch Δ_1^*, siehe Bemerkung 8.6). Dann ist $(\alpha_{s-1}, \alpha_{s-2}) \in \Delta_1$ und es gibt höchstens $d_1 - 1$ Elemente $\gamma \in \Delta_a(\omega)$ mit $(\alpha_{s-1}, \gamma) \in \Delta_1$ (nach Wahl von α ist $\gamma = \alpha_{s-2}$ nicht zulässig). Für jedes $\gamma \in \Delta_a(\omega)$ existiert ein $h \in G_\omega$ mit $\gamma = {}^h\alpha$. Somit gibt es einen Pfad $\omega = {}^h\omega = {}^h\alpha_0, \ldots, {}^h\alpha_s = {}^h\alpha = \gamma$. Dabei ist ${}^h\alpha_{s-1} \in \Delta_j(\omega)$ (siehe oben). Für γ gibt es daher nur $|\Delta_j(\omega)|(d_1 - 1)$ Möglichkeiten. Dies zeigt $d_{i+1} \leq d_a \leq d_j(d_1 - 1) \leq d_i(d_1 - 1)$. □

Satz 8.11 (Weiss). *Sei G eine nicht-reguläre, primitive Permutationsgruppe auf Ω mit Subgraden $d_1 \leq \ldots \leq d_k$. Sind $d_i < d_j$ teilerfremd, so existiert ein l mit $d_j < d_l \mid d_i d_j$. Insbesondere ist $\mathrm{ggT}(d_i, d_k) \neq 1$ für $i = 1, \ldots, k$.*

Beweis. Seien $\Delta_1, \ldots, \Delta_k$ die nicht-trivialen Orbitale von G und $\omega \in \Omega$ mit $|\Delta_i(\omega)| = d_i \geq 2$ für $i = 1, \ldots, k$. Sei

$$\Gamma := \{(\alpha, \beta) \in \Omega \times \Omega : \exists\, \gamma \in \Omega : (\alpha, \gamma) \in \Delta_j,\ (\gamma, \beta) \in \Delta_i\}.$$

Wir wollen zeigen, dass Γ ein Orbital ist. Seien dazu $(\alpha, \beta), (\alpha', \beta') \in \Gamma$. Dann existieren $\gamma, \gamma' \in \Omega$ mit $(\alpha, \gamma), (\alpha', \gamma') \in \Delta_j$ und $(\gamma, \beta), (\gamma', \beta') \in \Delta_i$. Ersetzt man (α, β) durch ${}^g(\alpha, \beta)$ für ein geeignetes $g \in G$, so kann man $\gamma = \gamma'$ annehmen. Nach Voraussetzung sind $|G_\gamma : G_{\gamma\alpha}| = |\Delta_j^*(\gamma)| = d_j$ und $|G_\gamma : G_{\gamma\beta}| = d_i$ teilerfremd. Insbesondere ist $|G_\gamma : G_{\gamma\alpha\beta}|$ durch $d_i d_j$ teilbar. Dies bedeutet, dass G_γ transitiv auf $\Delta_j^*(\gamma) \times \Delta_i(\gamma)$ operiert. Also existiert ein $g \in G_\gamma$ mit ${}^g(\alpha, \beta) = (\alpha', \beta')$, und Γ ist ein Orbital.

Wir berechnen nun $|\Gamma(\omega)|$. Es gibt d_j viele Elemente $\gamma \in \Omega$ mit $(\omega, \gamma) \in \Delta_j$. Für jedes solche γ gibt es d_i viele Elemente $\alpha \in \Delta_i(\gamma)$. Ein Element $\alpha \in \Gamma(\omega)$ wird auf diese Weise allerdings mehrfach gezählt. Sei

$$N := |\{\gamma \in \Omega : (\omega, \gamma) \in \Delta_j,\ (\gamma, \alpha) \in \Delta_i\}|.$$

Offenbar hängt N nicht von der Wahl von α ab und es gilt $|\Gamma(\omega)| = d_i d_j / N$. Wählt man also $\Delta_l := \Gamma$, so bleibt nur $d_l > d_j$ zu zeigen. Sicher ist $d_l \geq d_j$. Nehmen wir $d_l = d_j$ an. Dann ist $N = d_i$ und $\Delta_i^*(\alpha) \subseteq \Delta_j(\omega)$ für jedes $\alpha \in \Gamma(\omega)$. Sei

$$\Lambda := \{(\alpha, \beta) \in \Omega \times \Omega : \exists\, \gamma \in \Omega : (\alpha, \gamma), (\beta, \gamma) \in \Delta_i^*\}.$$

Wie im Beweis von Satz 8.10 enthält Λ ein nicht-triviales Orbital Ψ. Sei $\alpha \in \Gamma(\omega)$ und $\beta \in \Psi(\alpha)$. Dann existiert ein $\gamma \in \Omega$ mit $(\alpha, \gamma), (\beta, \gamma) \in \Delta_i^*$. Wegen $\Delta_i^*(\alpha) \subseteq \Delta_j(\omega)$ ist $(\omega, \gamma) \in \Delta_j$. Dies zeigt $\beta \in \Gamma(\omega)$. Folglich enthält $\Gamma(\omega)$ eine Zusammenhangskomponente von $\mathcal{G}_\Psi$ im Widerspruch zu Satz 8.8. □

Beispiel 8.12. Die sporadisch einfache *Janko-Gruppe* J_1 der Ordnung 175.560 ist primitiv vom Grad 266 mit Subgraden 11, 12, 110, 132.

Bemerkung 8.13. Mit Hilfe der CFSG haben Dolfi, Guralnick, Praeger und Spiga gezeigt, dass von je drei Subgraden einer primitiven, nicht-regulären Permutationsgruppe mindestens zwei einen gemeinsamen Teiler haben.

Beispiel 8.14.

(i) Aus Satz 8.11 folgt sofort, dass jede primitive Permutationsgruppe vom Grad 8 entweder regulär oder 2-transitiv ist. Da 8 keine Primzahl ist, kann es keine solchen regulären primitiven Gruppen geben. Nehmen wir also an, dass G 2-transitiv vom Grad 8 ist. Dann ist G_ω eine primitive Permutationsgruppe vom Grad 7. Nach Beispiel 6.18 gibt es somit folgende Möglichkeiten:

$$|G| \in \{8 \cdot 7,\ 8 \cdot 14,\ 8 \cdot 21,\ 8 \cdot 42,\ 8 \cdot 168,\ 8!/2,\ 8!\}.$$

Die letzten beiden Ordnungen korrespondieren sicherlich mit A_8 und S_8. Nach Aufgabe 6.2 sind die Gruppen vom Typ (A) gegeben durch

$$C_2^3 \rtimes C_7,\ C_2^3 \rtimes \Gamma\mathrm{L}(1,8) \cong C_2^3 \rtimes (C_7 \rtimes C_3),\ \mathrm{Aff}(3,2) \cong C_2^3 \rtimes \mathrm{GL}(3,2).$$

Jede Gruppe der Ordnung $8 \cdot 14$ ist auflösbar und müsste daher auch vom Typ (A) sein. Eine solche primitive Permutationsgruppe vom Grad 8 kann es also nicht geben.

(ii) Wir konstruieren nun Gruppen G vom Typ (F) mit $|G| \in \{168, 336\}$. Sei $G := \mathrm{GL}(3,2)$. Wir haben in Lemma 6.17 bereits gesehen, dass G acht 7-Sylowgruppen besitzt. Sei $P \in \mathrm{Syl}_7(G)$. Da G einfach ist, ist die Operation auf $G/\,\mathrm{N}_G(P)$ treu. Wäre $\mathrm{N}_G(P)$ nicht maximal, so hätte G eine echte Untergruppe vom Index ≤ 4. Also ist G eine primitive Permutationsgruppe vom Grad 8 und Typ (F). Betrachten wir die Abbildung $\varphi : G \to G$, $g \mapsto (g^{-1})^{\mathrm{T}}$, wobei g^{T} die Transponierte von g bezeichnet. Offenbar ist φ ein Automorphismus von G. Nehmen wir an, dass φ der von $x \in G$ induzierte innere Automorphismus ist. Für

$$a := \begin{pmatrix} 1 & . & . \\ . & . & 1 \\ . & 1 & . \end{pmatrix}, \qquad b := \begin{pmatrix} . & 1 & . \\ 1 & . & . \\ . & . & 1 \end{pmatrix}$$

ist $\varphi(a) = a$ und $\varphi(b) = b$. Also ist $x \in \mathrm{C}_G(\langle a, b\rangle)$. Es folgt leicht, dass $x = \left(\begin{smallmatrix} s & t & t \\ t & s & t \\ t & t & s \end{smallmatrix}\right)$ mit $s, t \in \mathbb{F}_2$. Da x invertierbar ist, muss $x = 1$ gelten. Man sieht aber leicht, dass φ nicht trivial ist (beachte Bild einer Dreiecksmatrix). Dies zeigt $\varphi \in \mathrm{Aut}(G) \setminus \mathrm{Inn}(G)$. Offenbar hat φ die Ordnung 2. Sei $\widehat{G} := G \rtimes \langle\varphi\rangle \leq \mathrm{Aut}(G)$. Dann ist auch $P \in \mathrm{Syl}_7(\widehat{G})$ und $\mathrm{N}_G(P) \subseteq \mathrm{N}_{\widehat{G}}(P)$. Nach Sylow ist $|\widehat{G} : \mathrm{N}_{\widehat{G}}(P)| \equiv 1 \pmod 7$. Es folgt $|\widehat{G} : \mathrm{N}_{\widehat{G}}(P)| = 8$. Wie immer operiert $\widehat{G}$ transitiv auf den Nebenklassen. Sei K der Kern dieser Operation. Dann ist $K \subseteq \mathrm{N}_{\widehat{G}}(P)$ und $K \cap G = 1$. Dies zeigt $|K| \leq 2$. Im Fall $|K| = 2$ wäre $K \subseteq \mathrm{Z}(\widehat{G})$ im Widerspruch zu Aufgabe 4.1. Also ist $K = 1$, und G operiert treu. Sei nun $\mathrm{N}_{\widehat{G}}(P) < H \leq \widehat{G}$. Dann hat H mehrere 7-Sylowgruppen, also mindestens acht. Es folgt $H = \widehat{G}$. Somit ist $\mathrm{N}_{\widehat{G}}(P)$ maximal in $\widehat{G}$, und $\widehat{G}$ ist eine primitive Permutationsgruppe vom Grad 8 und Typ (F).

(iii) Sei $G \leq S_8$ primitiv vom Typ (F) mit $\mathrm{Soc}(G) < A_8$. Nach (i) ist $|\mathrm{Soc}(G)| = 2^a \cdot 3 \cdot 7$ mit $a \in \{3, 4, 6\}$. Für $P \in \mathrm{Syl}_7(\mathrm{Soc}(G))$ hat $\mathrm{N}_{\mathrm{Soc}(G)}(P) \leq \mathrm{N}_{A_8}(P)$ höchstens Ordnung 21. Dies schließt den Fall $a = 4$ aus. Nehmen wir nun $a = 6$ an. Wie in Lemma 6.17 findet man dann eine Untergruppe $H \leq \mathrm{Soc}(G)$ mit $|H| = 2^5 \cdot 3$. Wegen der Einfachheit von $\mathrm{Soc}(G)$ ist H maximal und $\mathrm{Soc}(G)$ ist eine primitive Permutationsgruppe vom Grad 14. Dies widerspricht aber Aufgabe 8.11. Also ist $|\mathrm{Soc}(G)| = 2^3 \cdot 3 \cdot 7$ und $\mathrm{Soc}(G) \cong \mathrm{GL}(3, 2)$ nach Lemma 6.17. Im Fall $G = \mathrm{Soc}(G)$ ist die Operation bis auf Isomorphie eindeutig, denn ein Stabilisator ist zu $\mathrm{N}_G(P)$ konjugiert (Aufgabe 1.4). Sei nun $G \neq \mathrm{Soc}(G)$. Offenbar ist $\mathrm{N}_G(P) \leq \mathrm{N}_{S_8}(P)$ und $|\mathrm{N}_{S_8}(P)| = 42$. Da $\mathrm{Soc}(G)$ alle 7-Sylowgruppen von G besitzt, ist $|G| = 16 \cdot 3 \cdot 7$. Nach (i) gilt für den Stabilisator $G_8 \cong \mathrm{GL}(3, 2)$. Nach Lemma 6.17 ist G_8 bis auf Konjugation eindeutig. Wir können also $P = \langle(1, \ldots, 7)\rangle \leq G_8$ annehmen. Wegen $\mathrm{N}_G(P) = \mathrm{N}_{S_8}(P)$ ist dann auch $G = \langle G_8, \mathrm{N}_G(P)\rangle$ bis auf Konjugation eindeutig. Wir haben also die Gruppe $\widehat{G}$ aus (ii) gefunden. Zusammen mit Beispiel 6.18 haben wir alle primitiven Permutationsgruppen vom Grad ≤ 8 klassifiziert. In allen Fällen ist die Operation bis auf Isomorphie eindeutig (vgl. Aufgabe 5.2).

Grad	Gruppen
2	S_2
3	A_3, S_3
4	A_4, S_4
5	C_5, $C_5 \rtimes C_2$, $\mathrm{Aff}(1, 5)$, A_5, S_5
6	A_5, S_5, A_6, S_6
7	C_7, $C_7 \rtimes C_2$, $C_7 \rtimes C_3$, $\mathrm{Aff}(1, 7)$, $\mathrm{GL}(3, 2)$, A_7, S_7
8	$C_2^3 \rtimes C_7$, $C_2^3 \rtimes \Gamma\mathrm{L}(1, 8)$, $\mathrm{Aff}(3, 2)$, $\mathrm{GL}(3, 2)$, $\mathrm{GL}(3, 2) \rtimes C_2$, A_8, S_8

Satz 8.15 (Jordan). *Es existiert eine Funktion $f : \mathbb{N} \to \mathbb{N}$ mit folgender Eigenschaft: Ist $G \leq S_n$ primitiv mit $A_n \nsubseteq G$ und bewegt $g \in G \setminus \{1\}$ genau k Ziffern, so ist $n \leq f(k)$.*

Beweis. Sei $\omega \in \Delta := \{1 \leq \alpha \leq n : g \notin G_\alpha\}$. Wegen der Primitivität ist $G = \langle G_\omega, g\rangle$. Also muss g jede Bahn von G_ω verändern. Dies zeigt, dass der Rang von G höchstens k ist. Nach Satz 8.10 genügt es einen Subgrad zu finden, der durch eine Funktion in k beschränkt ist. Sei $\Gamma := \Delta \setminus \{\omega\}$. Nehmen wir an, dass ein $x \in G_\omega$ mit ${}^x\Gamma \cap \Gamma = \varnothing$ existiert. Nach Lemma 6.13 ist dann $g(xgx^{-1})g^{-1}(xg^{-1}x^{-1})$ ein 3-Zyklus im Widerspruch zu Satz 6.10. Für jedes $x \in G_\omega$ existiert also ein $\gamma_x \in \Gamma$ mit ${}^x\gamma_x \in \Gamma$. Für ein festes $\gamma \in \Gamma$ gibt es höchstens $|\Gamma||G_{\omega\gamma}|$ Elemente $x \in G_\omega$ mit $\gamma_x = \gamma$. Also ist

$$|G_\omega| \leq |\Gamma| \sum_{\gamma \in \Gamma} |G_{\omega\gamma}| \leq |\Gamma|^2 \max_{\gamma \in \Gamma} |G_{\omega\gamma}|$$

und es existiert ein $\gamma \in \Gamma$ mit $|G_\omega : G_{\omega\gamma}| \leq |\Gamma|^2 = (k-1)^2$. □

Bemerkung 8.16. Nach Satz 6.10 kann man $f(p) := p+2$ für jede Primzahl p wählen. Andererseits ist $f(4) := 8$ optimal (siehe Anhang, Satz A.4). Liebeck und Saxl haben mit Hilfe der CFSG gezeigt, dass $f(k) := \left(\frac{k}{2} + 1\right)^2$ für alle $k \in \mathbb{N}$ funktioniert. Die minimale Zahl k für alle $g \in G \setminus \{1\}$ nennt man im Englischen *minimal degree* (oder veraltet *class*) von G.

Lemma 8.17 (Rudio). *Sei $G \leq \mathrm{Sym}(\Omega)$ primitiv, $\varnothing \neq \Delta \subsetneq \Omega$ und $\alpha, \beta \in \Omega$ mit $\alpha \neq \beta$. Dann existiert ein $g \in G$ mit ${}^g\alpha \in \Delta$ und ${}^g\beta \notin \Delta$.*

Beweis. Sei

$$\Gamma := \bigcap_{\substack{g\in G,\\ \alpha\in {}^g\Delta}} {}^g\Delta.$$

Da G transitiv ist, gilt $\alpha \in \Gamma \subsetneq \Omega$. Sei $h \in G$ mit $\alpha \in {}^h\Gamma = \bigcap {}^{hg}\Delta$. Aus $\alpha \in {}^g\Delta$ folgt dann $\alpha \in {}^{hg}\Delta$ für alle $g \in G$. Also ist $\Gamma \subseteq {}^h\Gamma$ und damit $\Gamma = {}^h\Gamma$. Sei nun $h \in G$ beliebig mit $\gamma \in \Gamma \cap {}^h\Gamma \neq \varnothing$. Dann existiert ein $x \in G$ mit ${}^x\gamma = \alpha$. Also ist $\alpha \in \Gamma \cap {}^x\Gamma \cap {}^{xh}\Gamma$. Nach dem eben Gezeigten folgt ${}^x\Gamma = \Gamma = {}^{xh}\Gamma$. Daher ist auch ${}^h\Gamma = \Gamma$. Wir haben also gezeigt, dass $\Gamma \cap {}^h\Gamma \in \{\Gamma, \varnothing\}$ für alle $h \in G$ gilt. Da G primitiv ist, folgt $\Gamma = \{\alpha\}$. Dies impliziert die Behauptung. □

Definition 8.18. Eine *Sektion* von G ist eine Gruppe S mit $S \cong H/N$ für $N \trianglelefteq H \leq G$.

Satz 8.19 (Jordan)**.** *Sei $G \leq \mathrm{Sym}(\Omega)$ primitiv und $\omega \in \Omega$. Sei $\Delta \subseteq \Omega \setminus \{\omega\}$ eine Bahn von G_ω. Jede einfache Sektion von G_ω ist dann auch eine Sektion von G_ω^Δ. Insbesondere ist G_ω auflösbar, falls G_ω^Δ auflösbar ist.*

Beweis. Sei S eine einfache Sektion von G_ω. Wir wählen $H \leq G_\omega$ minimal mit $S \cong H/N$ für ein $N \trianglelefteq H$. Sei $\alpha \in \Delta$ und $\Gamma := \{\gamma \in \Omega : H \subseteq G_\gamma\}$. Sicher ist $\omega \in \Gamma \subsetneq \Omega$, da H nicht trivial operieren kann. Nach Lemma 8.17 existiert ein $g \in G$ mit $\omega \in {}^g\Gamma$ und $\alpha \notin {}^g\Gamma$. Also existiert ein $\gamma \in \Gamma$ mit $\omega = {}^g\gamma$ und $H \leq G_\gamma$. Ersetzt man also H durch $gHg^{-1} \leq G_\omega$, so kann man annehmen, dass H nicht-trivial auf Δ operiert. Sei K der Kern der Operation $H \to \mathrm{Sym}(\Delta)$. Nehmen wir $K \nsubseteq N$ an. Da S einfach ist, gilt $H = NK$. Also ist $S \cong H/N = KN/N \cong K/N \cap K$, und die Wahl von H impliziert $K = H$. Dieser Widerspruch zeigt $K \subseteq N$, und die Behauptung folgt. □

Definition 8.20. Für eine Primzahl p ist $\mathrm{O}^{p'}(G) := \langle \mathrm{Syl}_p(G)\rangle \leq G$ das *p'-Residuum* von G.

Bemerkung 8.21. Offenbar ist $\mathrm{O}^{p'}(G) \trianglelefteq G$ und $G/\mathrm{O}^{p'}(G)$ ist eine p'-Gruppe (d. h. $p \nmid |G/\mathrm{O}^{p'}(G)|$). Ist umgekehrt $N \trianglelefteq G$ mit p'-Faktorgruppe G/N, so enthält N eine p-Sylowgruppe von G und nach Sylow ist $\mathrm{O}^{p'}(G) \leq N$. Somit ist $\mathrm{O}^{p'}(G)$ der kleinste Normalteiler mit p'-Faktorgruppe.

Satz 8.22. *Sei $G \leq \mathrm{Sym}(\Omega)$ primitiv und $\omega \in \Omega$. Ist p ein Primteiler von $|G_\omega|$, so ist $p \mid |G_\omega^\Delta|$ für jede Bahn $\Delta \subseteq \Omega \setminus \{\omega\}$ von G_ω. Ist p ein Subgrad von G, so ist p der kleinste Subgrad und $p^2 \nmid |G_\omega|$. Ist zusätzlich $p = 2$, so ist $|G_\omega| = 2$ und $G \cong D_{2q} := C_q \rtimes C_2$ (Diedergruppe) für eine ungerade Primzahl q.*

Beweis. Die erste Aussage folgt aus Satz 8.19. Seien nun $d_1 \leq \ldots \leq d_k$ die Subgrade und $d_i = p$. Sei $\Delta_1 \subseteq \Omega \setminus \{\omega\}$ eine Bahn von G_ω mit $|\Delta_1| = d_1$. Nach Satz 8.19 ist dann $p \mid |G_\omega^{\Delta_1}| \mid d_1!$ und es folgt $d_i = p \leq d_1 \leq d_i$.

Sei nun K der Kern der Operation $G_\omega \to \mathrm{Sym}(\Delta_1)$, d. h. $K = G_\omega \cap G_{\Delta_1}$. Dann ist $|G_\omega/K| = |G_\omega^{\Delta_1}| \mid p!$ und $|G_\omega : G_{\omega\alpha}| = p$ für ein $\alpha \in \Delta_1$. Dies zeigt $p \nmid |G_{\omega\alpha}/K|$ und $N := \mathrm{O}^{p'}(G_{\omega\alpha}) \leq K$. Also ist $\mathrm{O}^{p'}(K) \subseteq N$. Für $P \in \mathrm{Syl}_p(K)$ und $g \in G_\omega$ ist auch ${}^gP \in \mathrm{Syl}_p(K)$. Dies zeigt $\mathrm{O}^{p'}(K) \trianglelefteq G_\omega$ und $N = \mathrm{O}^{p'}(K)$. Die Bahn von ω unter G_α hat ebenfalls die Länge $|G_\alpha : G_{\alpha\omega}| = |G_\omega : G_{\omega\alpha}| = p$. Vertauscht man also die Rollen von ω und α, so ergibt sich $N \trianglelefteq G_\alpha$ und $N \trianglelefteq \langle G_\omega, G_\alpha\rangle = G$. Da $N \leq G_\omega$ nicht transitiv auf Ω operieren kann, ist $N = 1$ nach Satz 2.2. Also ist $G_{\omega\alpha}$ eine p'-Gruppe und es folgt $p^2 \nmid |G_\omega|$.

Sei schließlich $d_1 = d_i = p = 2$. Dann ist $|G_\omega^{\Delta_1}| = 2$. Nach dem ersten Teil des Beweises ist G_ω eine 2-Gruppe. Andererseits ist $4 \nmid |G_\omega|$ nach dem eben Gezeigten. Also ist $|G_\omega| = 2$. Nach Aufgabe 2.1 kann G keine 2-Gruppe sein. Die Maximalität von G_ω zeigt daher $G_\omega \in \mathrm{Syl}_2(G)$. Nach Aufgabe 1.9 existiert ein Normalteiler $N \trianglelefteq G$ mit $G = N \rtimes G_\omega$. Sei q ein Primteiler von $|N|$. Dann ist die Anzahl der q-Sylowgruppen von N ungerade. Die Bahnengleichung zeigt $G_\omega \leq \mathrm{N}_G(Q)$ für ein $Q \in \mathrm{Syl}_q(N)$. Die Maximalität von G_ω impliziert $G = QG_\omega$ und $N = Q$. Das gleiche Argument zeigt, dass N ein minimaler Normalteiler von G ist. Also ist N elementarabelsch. Sei $G_\omega = \langle x\rangle$. Nach Satz 2.1 hat x keine Fixpunkte auf $N \setminus \{1\}$. Für $1 \neq y \in N$ ist $(xy)^2 \in N$ und $x(xy)^2x^{-1} = y(xyx^{-1}) = (xyx^{-1})y = (xy)^2$. Dies zeigt $xyx^{-1} = y^{-1}$ und $G_\omega\langle y\rangle \leq G$. Da G_ω maximal ist, folgt $N = \langle y\rangle$. Dies zeigt die Behauptung. □

Bemerkung 8.23. Man kennt auch alle primitiven Permutationsgruppen mit Subgrad 3 oder 4 (ohne Beweis).

Satz 8.24 (Manning)**.** *Sei $G \leq \mathrm{Sym}(\Omega)$ primitiv und $\omega \in \Omega$. Seien $\Delta_1, \ldots, \Delta_k$ die Bahnen von G_ω auf $\Omega \setminus \{\omega\}$, sodass $G_\omega^{\Delta_i}$ für $i = 1, \ldots, r < k$ primitiv ist. Dann operiert G_ω treu auf $\Delta_{r+1} \cup \ldots \cup \Delta_k$.*

Beweis. Wir können sicher annehmen, dass G nicht regulär ist. Sei $\Delta := \Delta_1 \cup \ldots \cup \Delta_r$, $\Delta' := \Delta_{r+1} \cup \ldots \cup \Delta_k$ und $N := G_\omega \cap G_{\Delta'}$. Wir müssen $N = 1$ zeigen. Nehmen wir das Gegenteil an. Dabei können wir annehmen, dass N nicht-trivial auf Δ_i für $i = 1, \ldots, r$ operiert (anderenfalls verkleinere man r). Offenbar ist $1 \neq NG_{\Delta_i}/G_{\Delta_i} \trianglelefteq G_\omega^{\Delta_i}$. Da $G_\omega^{\Delta_i}$ primitiv ist, operiert N transitiv auf Δ_i für $i = 1, \ldots, r$.

Schritt 1: $\Delta_i \subseteq \Delta \Longleftrightarrow \Delta_i^* \subseteq \Delta$.
Sei $g \in G$ mit ${}^g\omega \in \Delta'$. Dann ist $N \leq G_{{}^g\omega}$ und $g^{-1}Ng \leq G_\omega$. Es genügt zu zeigen, dass ${}^{g^{-1}}\omega \in \Delta'$ gilt. Nehmen wir das Gegenteil an. Dann ist $gNg^{-1} \not\leq G_\omega$. Die Maximalität von G_ω zeigt $G = \langle G_\omega, gNg^{-1}\rangle$. Sei o. B. d. A. $|\Delta_r| \geq |\Delta_i|$ für $i = 1, \ldots, r$. Wegen $N \leq G_{{}^g\omega}$ liegt Δ_r in einer Bahn Γ von $G_{{}^g\omega}$. Im Fall $\Delta_r = \Gamma$ wäre Δ_r eine Bahn von $\langle G_\omega, G_{{}^g\omega}\rangle = G$. Also ist $\Delta_r \subsetneq \Gamma$. Nach Wahl von Δ_r operiert gNg^{-1} ($\trianglelefteq G_{{}^g\omega}$) trivial auf Γ und somit auch auf Δ_r. Also ist Δ_r eine Bahn von $\langle G_\omega, gNg^{-1}\rangle = G$. Widerspruch.

Wir betrachten nun die Graphen $\mathcal{G}$ und $\mathcal{G}'$, die durch Vereinigung von $\mathcal{G}_{\Delta_i}$ mit $i = 1, \ldots, r$ bzw. $i = r+1, \ldots, k$ entstehen. Nach Schritt 1 können wir $\mathcal{G}$ und $\mathcal{G}'$ als ungerichtete Graphen auffassen.

Schritt 2: $\mathcal{G}$ ist vollständig.
Nach Satz 8.8 ist $\mathcal{G}$ zusammenhängend. Seien (α, β) und (β, γ) Kanten in $\mathcal{G}$ mit $\alpha \neq \gamma$. Wir müssen zeigen, dass auch (α, γ) eine Kante in $\mathcal{G}$ ist. Ist dies nicht der Fall, so ist (α, γ) eine Kante von $\mathcal{G}'$. Sei $g \in G$ mit ${}^g\omega = \alpha$. Dann ist $gNg^{-1} \trianglelefteq G_\alpha$. Also liegt β in einer nicht-trivialen Bahn Γ_1 von gNg^{-1}. Sei nun $h \in G$ mit ${}^h\alpha = \gamma$. Dann ist $hgNg^{-1}h^{-1} \trianglelefteq G_\gamma$. Also liegt β auch in einer nicht-trivialen Bahn Γ_2 von $hgNg^{-1}h^{-1}$. Da (α, γ) eine Kante von $\mathcal{G}'$ ist, ist $hgNg^{-1}h^{-1} \leq G_\alpha$. Nach dem ersten Teil des Beweises ist Γ_1 auch eine Bahn von G_α. Dies zeigt $\Gamma_2 = {}^{hgNg^{-1}h^{-1}}\beta \subseteq {}^{G_\alpha}\beta = \Gamma_1$. Analog ist auch $\Gamma_1 \subseteq \Gamma_2$. Also ist $\Gamma_1 = \Gamma_2$ eine Bahn von G_α und von G_γ. Somit ist Γ_1 auch eine Bahn von $\langle G_\alpha, G_\gamma\rangle = G$. Widerspruch.

Da $\mathcal{G}$ vollständig ist, kann $\mathcal{G}'$ überhaupt keine Kante haben. Dies widerspricht aber der Voraussetzung $r < k$. □

Satz 8.25. *Sei $G \leq \mathrm{Sym}(\Omega)$ primitiv mit regulärem Normalteiler $N \trianglelefteq G$ (z. B. $N = \mathrm{Soc}(G)$ für Typ (A) oder (V)). Dann operiert G_ω für $\omega \in \Omega$ treu auf jeder nicht-trivialen Bahn.*

Beweis. Nach Satz 2.1 ist die Operation von G_ω auf Ω isomorph zur Operation auf N durch Konjugation. Sei $\Delta \subseteq N$ eine nicht-triviale Bahn. Dann ist $G_\omega \leq \mathrm{N}_G(\langle\Delta\rangle)$. Wegen $N_\omega = 1$ ist $G_\omega < G_\omega\langle\Delta\rangle \leq G$. Die Maximalität von G_ω liefert $\langle\Delta\rangle = N$. Operiert $g \in G_\omega$ also trivial auf Δ, so auch auf N. Dies zeigt $g = 1$ und die Behauptung folgt. □

Satz 8.26 (Manning)**.** *Sei $G \leq \mathrm{Sym}(\Omega)$ primitiv und $\omega \in \Omega$. Sei $d \geq 3$ der größte Subgrad. Operiert G_ω 2-transitiv auf einer Bahn der Länge d, so ist G 3-transitiv.*

Beweis. Es genügt zu zeigen, dass $|\Omega| = d + 1$ gilt. Sei Δ ein Orbital mit $|\Delta(\omega)| = d$, sodass G_ω 2-transitiv auf $\Delta(\omega)$ operiert. Seien $\alpha, \beta \in \Delta(\omega)$ mit $\alpha \neq \beta$. Dann gibt es ein Orbital Γ mit $(\alpha, \beta) \in \Gamma$. Da G_ω 2-transitiv auf $\Delta(\omega)$ operiert, bilden je zwei verschiedene Punkte aus $\Delta(\omega)$ einen Pfeil in $\mathcal{G}_\Gamma$. Insbesondere ist $\Gamma^* = \Gamma$. Außerdem ist $\Delta(\omega) \setminus \{\alpha\} \subseteq \Gamma(\alpha)$ und $|\Gamma(\alpha)| \geq d - 1$. Im Fall $|\Gamma(\alpha)| = d - 1$ wären die Subgrade $d - 1$ und d teilerfremd, und nach Satz 8.11 kann d nicht der größte Subgrad sein. Dieser Widerspruch zeigt $\Gamma(\alpha) = \Delta(\omega) \setminus \{\alpha\} \cup \{\gamma\}$ für ein $\gamma \in \Omega$. Da G_ω 2-transitiv auf $\Delta(\omega)$ operiert, operiert $G_{\omega\alpha}$ noch transitiv auf $\Delta(\omega) \setminus \{\alpha\} = \Gamma(\alpha) \setminus \{\gamma\}$. Wegen $G_{\omega\alpha} \subseteq G_\alpha$ ist sicher $G_{\omega\alpha} \subseteq G_{\alpha\gamma}$. Dies zeigt, dass auch G_α 2-transitiv auf $\Gamma(\alpha)$ operiert. Wegen $d \geq 3$ gibt es Punkte $\beta, \delta \in \Delta(\omega) \setminus \{\alpha\} = \Gamma(\alpha) \setminus \{\gamma\}$ mit $\beta \neq \delta$. Nach Definition von Γ ist $(\beta, \delta) \in \Gamma$. Da G_α 2-transitiv auf $\Gamma(\alpha)$ operiert, bilden je zwei verschiedene Punkte aus $\Gamma(\alpha)$ einen Pfeil von $\mathcal{G}_\Gamma$. Aus Symmetriegründen bilden, für ein beliebiges $\beta \in \Omega$, je zwei verschiedene Punkte von $\Gamma(\beta)$ einen Pfeil von $\mathcal{G}_\Gamma$. Nehmen wir nun indirekt an, dass $\Gamma(\alpha) \cup \{\alpha\} \neq \Omega$ gilt. Da $\mathcal{G}_\Gamma$ nach Satz 8.8 zusammenhängend ist, existieren $\beta \in \Gamma(\alpha) \cup \{\alpha\}$ und $\delta \notin \Gamma(\alpha) \cup \{\alpha\}$ mit $(\beta, \delta) \in \Gamma$. Dann ist $\delta \in \Gamma(\beta)$ und es folgt $\alpha \neq \beta$. Also ist $\beta \in \Gamma(\alpha)$ und damit auch $\alpha \in \Gamma(\beta)$ wegen $\Gamma^* = \Gamma$. Nach dem eben Gezeigten ist also $(\alpha, \delta) \in \Gamma$. Dies widerspricht aber $\delta \notin \Gamma(\alpha)$. □

Beispiel 8.27.

(i) Sei $G \leq \mathrm{Sym}(\Omega)$ primitiv vom Grad 9, aber nicht 2-transitiv. Seien $d_1 \leq \ldots \leq d_k$ die Subgrade von G. Der Fall $d_1 = 2$ ist nach Satz 8.22 ausgeschlossen, da 9 keine Primzahl ist. Nach Satz 8.11 ist außerdem $(d_1, d_2) = (3, 5)$ unmöglich. Also ist $d_1 = d_2 = 4$. Sei $\Delta \subseteq \Omega \setminus \{\omega\}$ eine Bahn von G_ω. Nehmen wir zunächst an, dass G_ω^Δ keine 2-Gruppe ist. Dann ist offenbar $G_\omega^\Delta \in \{A_4, S_4\}$ bis auf Isomorphie. Dies widerspricht aber Satz 8.26. Also ist G_ω^Δ eine 2-Gruppe ist. Nach Satz 8.22 ist auch G_ω eine 2-Gruppe. Nach Aufgabe 8.10 (oder Burnsides $p^a q^b$-Satz) ist G auflösbar. Also operiert G_ω treu auf Δ nach Satz 8.25. Dies zeigt $G_\omega \leq D_8$ bis auf Isomorphie, wobei D_8 die Diedergruppe der Ordnung 8 ist. Insbesondere ist $|G| \leq 72$. Wir konstruieren ein Beispiel. Sei $V := \mathbb{F}_3^2$ und $C \leq \mathrm{Aut}(V)$ eine Untergruppe des Singer-Zyklus mit $C \cong C_4$. Die Bahnen von C auf $V \setminus \{0\}$ haben dann Länge 4. Insbesondere kann C keine Untergruppe der Ordnung 3 von V festhalten. Also ist die Gruppe $V \rtimes C$ primitiv mit Subgraden $4, 4$. Da C die Multiplikation mit -1 enthält, gilt außerdem $\Delta = \Delta^*$ (vgl. Aufgabe 8.3). Ist nun F der Frobenius-Automorphismus auf $\mathbb{F}_9$, so gilt $C\langle F\rangle \cong D_8$ (vgl. Beispiel 2.16). Da F nicht-triviale Fixpunkte auf V hat, kann $C\langle F\rangle$ nicht transitiv operieren. Dies liefert ein weiteres Beispiel $V \rtimes C\langle F\rangle$.

(ii) Sei $G \leq \mathrm{Sym}(\Omega)$ primitiv vom Grad 10, aber nicht 2-transitiv. Da 10 keine Primzahlpotenz ist, ist G nicht auflösbar. Seien $d_1 \leq \ldots \leq d_k$ die Subgrade von G. Wie üblich ist $d_1 \geq 3$. Nach Satz 8.11 ist $d_1 = 3$. Für eine entsprechende Bahn Δ ist also $G_\omega^\Delta \in \{A_3, S_3\}$. Im ersten Fall ist $|G_\omega| = 3$ und G wäre auflösbar. Also ist G_ω^Δ primitiv. Nach Satz 8.26 ist $d_1 = d_2 = d_3 = 3$ ausgeschlossen. Somit gilt $d_1 = 3$ und $d_2 = 6$. Nach Satz 8.24 ist $G_\omega \leq S_6$. Nach Satz 8.22 ist außerdem $|G_\omega| = 2^a \cdot 3$ und $|G| = 2^{a+1} \cdot 3 \cdot 5$ mit $a \leq 4$. Da 3 und 5 nur einmal die Gruppenordnung teilen, ist $\mathrm{Soc}(G)$ einfach, d. h. G ist vom Typ (F). Offenbar ist dann $|\mathrm{Soc}(G)| = 2^b \cdot 3 \cdot 5$ mit $2 \leq b \leq 5$. Wir werden zeigen, dass $b = 2$ und $\mathrm{Soc}(G) \cong A_5$ gilt. Sei dafür $P \in \mathrm{Syl}_2(\mathrm{Soc}(G))$. Im Fall $|\mathrm{Soc}(G) : \mathrm{N}_{\mathrm{Soc}(G)}(P)| = 5$ ist die Behauptung richtig. Nehmen wir also $\mathrm{N}_{\mathrm{Soc}(G)}(P) = P$ an. Nach Aufgabe 1.11 existiert ein $Q \in \mathrm{Syl}_2(\mathrm{Soc}(G))$ mit $|P : P \cap Q| = 2$. Offenbar besitzt dann $\mathrm{N}_{\mathrm{Soc}(G)}(P \cap Q)$ mindestens die beiden 2-Sylowgruppen P und Q. Also ist $|\mathrm{Soc}(G) : \mathrm{N}_{\mathrm{Soc}(G)}(P \cap Q)| = 5$ und die Behauptung folgt. Nach Satz 5.13 ist nun $G \in \{A_5, S_5\}$. In beiden Fällen hat die Operation auf den zweielementigen Teilmengen von $\{1, \ldots, 5\}$ die gewünschte Eigenschaft (vgl. Bemerkung 5.16).

(iii) Die primitiven Permutationsgruppen vom Grad 11 und 13, die nicht 2-transitiven sind, lassen sich leicht mit Satz 7.4 angeben. Nach Aufgabe 8.11 gibt es keine entsprechenden Gruppen vom Grad 12 oder 14 (vgl. Bemerkung 7.5). Für Grad 15 hat man wieder Beispiele durch die Operation von A_6 oder S_6 auf den zweielementigen Teilmengen von $\{1, \ldots, 6\}$.

Bemerkung 8.28. Mit Hilfe der CFSG konnten Cameron, Praeger, Saxl und Seitz zeigen, dass es bei vorgegebenem Subgrad nur endlich viele Möglichkeiten für G_ω gibt (Sims' Vermutung). Für Typ (A) und (V) folgt dies aus Satz 8.25. Für Typ (D) gilt sogar ein stärkeres Ergebnis (siehe Anhang, Satz A.7).

Definition 8.29. Eine Untergruppe $H \leq G$ heißt *subnormal*, falls es eine Folge $H \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_k = G$ gibt.

Bemerkung 8.30. Subnormalität ist der transitive Abschluss der Normalteilerrelation. Man verwendet daher manchmal das Symbol $\trianglelefteq\trianglelefteq$.

Lemma 8.31. *Für jede subnormale Untergruppe $H \leq G$ gilt* $\mathrm{Soc}(G) \leq \mathrm{N}_G(H)$.

Beweis. Wir argumentieren durch Induktion nach $|G : H|$. Der Fall $H = G$ ist klar. Sei nun $H < G$. Sei N ein minimaler Normalteiler von G. Wir müssen $N \leq \mathrm{N}_G(H)$ zeigen. Nach Voraussetzung existiert ein Normalteiler $K \lhd G$, sodass H subnormal in K ist. Wegen $K \cap N \trianglelefteq G$ gilt $N \leq K$ oder $NK = N \oplus K$. Im zweiten Fall ist $N \leq \mathrm{C}_G(K) \leq \mathrm{C}_G(H) \leq \mathrm{N}_G(H)$. Sei also $N \leq K$. Sei L ein minimaler Normalteiler von K mit $L \leq N$. Nach Induktion ist $L \leq \mathrm{N}_K(H)$. Für $x \in G$ ist xLx^{-1} sicher auch ein minimaler Normalteiler von K. Also ist auch $xLx^{-1} \leq \mathrm{N}_K(H)$. Offenbar ist $\langle xLx^{-1} : x \in G\rangle \trianglelefteq G$ und damit $N = \langle xLx^{-1} : x \in G\rangle \leq \mathrm{N}_K(H) \leq \mathrm{N}_G(H)$. □

Lemma 8.32. *Sei $H \leq G$ mit $HxHx^{-1} = xHx^{-1}H$ für alle $x \in G$. Dann ist H subnormal in G.*

Beweis. Wir benutzen wieder Induktion nach $|G : H|$. Im Fall $H \trianglelefteq G$ ist die Behauptung klar. Sei also $x \in G$ mit $xHx^{-1} \neq H$. Wir setzen $K := HxHx^{-1} \leq G$. Dann ist $|G : K| < |G : H|$. Für $y \in G$ ist $yKy^{-1}K = KyKy^{-1}$, denn nach Voraussetzung sind sicher alle Konjugierten von H paarweise vertauschbar. Nach Induktion ist K subnormal in G. Im Fall $x \in K$ wäre $1 \in K = Kx = HxH$ und somit $x \in H$. Also ist $x \notin K$. Dies impliziert $|K : H| < |G : H|$. Nach Induktion ist also H subnormal in K. Insgesamt ist daher H subnormal in G. □

Satz 8.33 (Wielandt). *Sei $G \leq \mathrm{Sym}(\Omega)$ primitiv und $\omega \in \Omega$. Sei $\Gamma \subseteq \Omega \setminus \{\omega\}$ mit $\Delta \subseteq \Gamma$ oder $\Delta^* \subseteq \Gamma$ für jede nicht-triviale Bahn Δ von G_ω. Dann operiert G_ω treu auf Γ.*

Beweis. Wir müssen zeigen, dass $N := G_\omega \cap G_\Gamma$ trivial ist. Offenbar ist $N \trianglelefteq G_\omega$. Sei $g \in G$. Im Fall $g \in G_\omega$ ist N sicher mit $gNg^{-1} = N$ vertauschbar. Sei nun ${}^g\omega \in \Delta$ für eine nicht-triviale Bahn Δ von G_ω. Im Fall $\Delta \subseteq \Gamma$ gilt $N \leq G_{{}^g\omega}$ und $g^{-1}Ng \leq G_\omega$. Also ist N mit $g^{-1}Ng$ vertauschbar. Sicher ist dann N auch mit gNg^{-1} vertauschbar. Sei schließlich $\Delta^* \subseteq \Gamma$. Dann ist ${}^{g^{-1}}\omega \in \Gamma$ und $gNg^{-1} \leq G_\omega$. Für alle $g \in G$ ist also $NgNg^{-1} = gNg^{-1}N$. Nach Lemma 8.32 ist N subnormal in G. Also ist $\mathrm{Soc}(G) \leq \mathrm{N}_G(N)$ nach Lemma 8.31. Im Fall $N \neq 1$ ist $\mathrm{N}_G(N) = G_\omega$, da G_ω maximal ist. Dann kann $\mathrm{Soc}(G)$ aber nicht transitiv operieren. Dieser Widerspruch zeigt $N = 1$. □

Satz 8.34 (Rietz). *Sei $G \leq \mathrm{Sym}(\Omega)$ primitiv und $\omega \in \Omega$. Sei $\Delta \subseteq \Omega \setminus \{\omega\}$ eine Bahn von G_ω, sodass G_ω^Δ regulär ist und $G_{\omega\delta} = G_{\omega\gamma}$ für gewisse $\delta, \gamma \in \Delta^*$ mit $\delta \neq \gamma$. Dann ist $G_\omega \cong G_\omega^\Delta$.*

Beweis. Sei $\alpha \in \Delta$. Da G_ω^Δ regulär ist, gilt $G_{\omega\alpha} = G_\omega \cap G_\Delta \trianglelefteq G_\omega$. Im Fall $G_{\omega\alpha} \trianglelefteq G$ ist $G_{\omega\alpha} = 1$ und wir sind fertig. Wir können daher $\mathrm{N}_G(G_{\omega\alpha}) = G_\omega$ annehmen. Sei $g \in G$ mit ${}^g\omega = \alpha$ und ${}^{g^{-1}}\omega = \delta \in \Delta^*$. Dann ist $G_\delta = g^{-1}G_\omega g = g^{-1}\,\mathrm{N}_G(G_{\omega\alpha})g = \mathrm{N}_G(G_{\delta\omega})$. Also ist $\mathrm{N}_G(G_{\omega\delta}) \cap G_\omega = G_{\omega\delta}$. Nach Voraussetzung existiert ein $\gamma \in \Delta^* \setminus \{\delta\}$ mit $G_{\omega\delta} = G_{\omega\gamma}$. Außerdem existiert ein $h \in G_\omega$ mit ${}^h\delta = \gamma$. Dann ist aber $h \in \mathrm{N}_{G_\omega}(G_{\omega\delta}) \setminus G_{\omega\delta}$. Widerspruch. □

Bemerkung 8.35. Burnside und andere haben Anfang des 20. Jahrhunderts die obigen Methoden benutzt, um zu zeigen, dass viele Gruppen ungerader Ordnung auflösbar sind. Dies wurde 1963 von Feit und Thompson in voller Allgemeinheit bewiesen (allerdings mit deutlich schwierigeren Methoden). Wir skizzieren den Anfang dieser Entwicklung anhand eines minimalen Gegenbeispiels (dabei dürfen wir Satz 5.7 nicht verwenden, denn Satz 5.3 basiert implizit auf Feit-Thompson). Dafür benötigen wir einen Spezialfall von Burnsides Verlagerungssatz.

Lemma 8.36. *Sei p eine Primzahl und $P < G$ eine maximale Untergruppe mit $|P| = p$. Dann ist G nicht einfach.*

Beweis. Wir können sicher $P \in \mathrm{Syl}_p(G)$ und $\mathrm{N}_G(P) = P$ annehmen. Nach Aufgabe 1.9 ist $p > 2$. Sei $\mathcal{R}$ ein Repräsentantensystem für G/P. Für $g \in G$ sei $\overline{g} \in \mathcal{R}$ mit $gP = \overline{g}P$. Wir betrachten die Abbildung $\varphi : G \to P$, $g \mapsto \prod_{r\in\mathcal{R}} (gr)^{-1}\overline{gr}$. Da P abelsch ist, kommt es in dem Produkt nicht auf die Reihenfolge der Faktoren an. Für $g, h \in G$ ist $\overline{ghr}P = ghrP = g\overline{hr}P = \overline{g\overline{hr}}P$ und somit

$$\varphi(gh) = \prod_{r\in\mathcal{R}} (ghr)^{-1}\overline{ghr} = \prod_{r\in\mathcal{R}} (hr)^{-1}\overline{hr}(\overline{hr})^{-1}g^{-1}\overline{g\overline{hr}} = \prod_{r\in\mathcal{R}} (hr)^{-1}\overline{hr}(g\overline{hr})^{-1}\overline{g\overline{hr}} = \varphi(g)\varphi(h).$$

Also ist φ ein Homomorphismus. Sei nun $1 \neq x \in P$. Im Fall $xgP = gP$ ist $g^{-1}xg \in P$ und $g \in \mathrm{N}_G(P) = P$. Also hat x nur den trivialen Fixpunkt P auf G/P. Wir wählen ein Repräsentantensystem $\mathcal{S} \subseteq \mathcal{R}$ für die nicht-trivialen Bahnen von P auf G/P. Man kann dann $\mathcal{R} := \{x^i s : s \in \mathcal{S},\ i = 0, \ldots, p-1\} \cup \{1\}$ setzen. Dann ist $(x(x^i s))^{-1}\overline{x(x^i s)} = 1$ für $s \in \mathcal{S}$ und $i = 0, \ldots, p-1$. Also ist $\varphi(x) = x^{-1}\overline{x} = x^{-1}$. Insbesondere ist φ nicht trivial. Die Behauptung folgt. □

Satz 8.37 (Miller). *Sei G eine nichtabelsche einfache Gruppe ungerader Ordnung und $H < G$. Dann ist $|G : H| > 50$.*

Beweis. Wie üblich operiert G transitiv und treu auf G/H. Ist die Operation nicht primitiv, so kann man H durch eine größere echte Untergruppe ersetzen. Wir können also annehmen, dass G eine primitive Permutationsgruppe vom Grad $n := |G : H| < 50$ ist. Nach Satz 7.4 ist n keine Primzahl. Sei d ein Subgrad von G. Nehmen wir $d \in \{3, 5, 17\}$ an. Nach Satz 7.4 ist $G_\omega^\Delta \cong C_d$ für eine entsprechende Bahn Δ von G_ω (dieses Argument funktioniert allgemeiner für jede Fermatprimzahl). Nach Satz 8.22 ist auch $G_\omega \cong C_d$. Da G_ω maximal ist, ist $G_\omega \in \mathrm{Syl}_d(G)$. Dies widerspricht aber Lemma 8.36. Wir können daher annehmen, dass alle Subgrade mindestens 7 sind. Nach Lemma 8.3 treten die Subgrade außerdem in Paaren auf (entsprechend (Δ, Δ^*)). Also ist $n \geq 15$. Gibt es zwei verschiedene Subgrade, so sind diese 9 und 15 nach Satz 8.11 (in allen anderen Fällen ist $n > 50$). Sei Δ eine Bahn von G_ω der Länge 9. Nach Beispiel 8.4 ist G_ω^Δ imprimitiv. Es folgt leicht, dass G_ω^Δ eine 3-Gruppe ist (genauer ist $G_\omega^\Delta \leq C_3 \wr C_3$, vgl. Beweis von Satz 5.15). Nach Satz 8.22 ist auch G_ω eine 3-Gruppe und es kann keine Bahn der Länge 15 geben. Widerspruch.

Wir können daher annehmen, dass alle Subgrade identisch sind. Insbesondere hat n die Form $n = 1 + 2kl$ mit $k \geq 1$, $l \geq 7$ und $l \equiv 1 \pmod 2$. Induktiv genügt es jeweils eine echte Untergruppe mit kleinerem Index zu konstruieren.

(a) $n = 15$. Hier gibt es zwei Bahnen Δ und Δ^* mit $|\Delta| = 7$. Nach Satz 8.33 und Satz 7.4 ist $G_\omega \cong G_\omega^\Delta \in \{C_7, C_7 \rtimes C_3\}$ und $|G| \in \{3^a \cdot 5 \cdot 7\}$ mit $a \leq 2$. Der Normalisator einer 3-Sylowgruppe hat dann Index 7.

(b) $n = 27$. Hier sind die Subgrade $13, 13$. Wie üblich folgt $|G| = 3^a \cdot 13$ mit $a \leq 4$. Eine 3-Sylowgruppe hat dann aber Index 13 und wir sind fertig.

(c) $n = 39$. Hier sind die Subgrade $19, 19$. Es ergibt sich $|G| = 3^a \cdot 13 \cdot 19$ mit $a \leq 3$. Die Anzahl der 13-Sylowgruppen ist dann 27.

(d) $n = 45$. Hier sind die Subgrade $11, 11, 11, 11$. Wie üblich ist $|G| = 3^2 \cdot 5^a \cdot 11$ mit $a \leq 2$. Die Anzahl der 5-Sylowgruppen ist 11 und wir sind fertig. □

Beispiel 8.38. Sei G eine Gruppe der Ordnung $42.525 = 3^5 \cdot 5^2 \cdot 7$ und $P \in \mathrm{Syl}_3(G)$. Wir wollen zeigen, dass G nicht einfach ist. Nach Satz 8.37 können wir $\mathrm{N}_G(P) = P$ annehmen. Wie üblich operiert P auf $\mathrm{Syl}_3(G)$. Der Stabilisator von $Q \in \mathrm{Syl}_3(G) \setminus \{P\}$ ist dabei $P \cap Q$. Wegen $|G : \mathrm{N}_G(P)| = 5^2 \cdot 7 \equiv 4 \pmod 9$ existiert ein $Q \in \mathrm{Syl}_3(G)$ mit $|P : P \cap Q| = 3$. Bekanntlich ist dann $P, Q \leq \mathrm{N}_G(P \cap Q)$ (vgl. Aufgabe 8.5). Also ist $|G : \mathrm{N}_G(P \cap Q)| \leq 25$ und die Behauptung folgt. Induktiv erhält man leicht, dass G sogar auflösbar ist.

Bemerkung 8.39. Satz 8.37 wurde von Burnside und Rietz auf die Schranke $|G : H| \geq 243$ verbessert. Zusammen mit elementaren Methoden der abstrakten Gruppentheorie kann man dann zeigen, dass jede Gruppe ungerader Ordnung kleiner 1.000.000 auflösbar ist.

Aufgabe 8.1. Bestimmen Sie die Subgrade der Operation von S_7 auf den dreielementigen Teilmengen von $\{1, \ldots, 7\}$.

Aufgabe 8.2. Sei $G \leq \mathrm{Sym}(\Omega)$ transitiv, und sei Δ ein nicht-triviales Orbital von G. Zeigen Sie, dass $\{(\alpha, \beta) \in \Omega \times \Omega : (\beta, \alpha) \in \Delta\}$ das Orbital von $\Delta(\omega)^*$ ist.

Aufgabe 8.3. Sei $G \leq \mathrm{Sym}(\Omega)$ transitiv. Zeigen Sie, dass $|G|$ genau dann gerade ist, falls ein nicht-triviales Orbital Δ mit $\Delta^* = \Delta$ existiert.

Aufgabe 8.4. Sei G eine transitive Permutationsgruppe mit ungeradem Grad, sodass auch alle Subgrade ungerade sind. Zeigen Sie, dass $|G|$ ungerade ist.

Aufgabe 8.5. Zeigen Sie, dass jede Untergruppe einer p-Gruppe subnormal ist.

Aufgabe 8.6. Sei $G \leq \mathrm{Sym}(\Omega)$ primitiv und nicht-regulär mit k paarweise teilerfremden Subgraden. Zeigen Sie, dass der Rang von G mindestens 2^k ist.

Aufgabe 8.7. Sei $G \leq \mathrm{Sym}(\Omega)$ primitiv und $\omega \in \Omega$. Für eine Bahn Δ von G_ω, sei $|G_\omega^\Delta| = |\Delta| \neq 1$ eine Primzahlpotenz. Zeigen Sie: $G_\omega \cong G_\omega^\Delta$.

Aufgabe 8.8. Sei $G \to \mathrm{Sym}(\Omega)$ transitiv vom Rang r, und sei $f(g)$ die Anzahl der Fixpunkte von $g \in G$ in Ω. Zeigen Sie:

$$r = \frac{1}{|G|} \sum_{g \in G} f(g)^2.$$

Aufgabe 8.9. Sei $G := \langle (1,2,3,4,5,6), (3,5)(4,6) \rangle \leq S_6$.

(i) Bestimmen Sie die Struktur von G ($|G|$, Normalteiler etc.)

(ii) Bestimmen Sie die Subgrade von G.

(iii) Finden Sie heraus, ob G primitiv ist.

Aufgabe 8.10. Zeigen Sie, dass jede Gruppe der Ordnung $2^n \cdot 3^2$ mit $n \geq 1$ auflösbar ist.
Hinweis: Betrachten Sie den Schnitt zweier 2-Sylowgruppen.

Aufgabe 8.11. Zeigen Sie, dass jede primitive Permutationsgruppe vom Grad 12 oder 14 2-transitiv ist.
Hinweis: Für Grad 14 zeigen Sie, dass $|G| = 2^a \cdot 3 \cdot 7$ mit $a \leq 5$ gilt und betrachten Sie anschließend den Normalisator einer 7-Sylowgruppe.

Aufgabe 8.12. Sei $G \leq \mathrm{Sym}(\Omega)$ transitiv vom Grad 100, sodass G_ω einfach ist mit Subgraden 22 und 77. Zeigen Sie, dass G einfach ist.
Bemerkung: Die sporadisch einfache *Higman-Sims-Gruppe* HS der Ordnung 44.352.000 besitzt diese Eigenschaften mit $G_\omega \cong M_{22}$.

Anhang

Satz A.1 (= Satz 5.19)**.** *Jede 2-transitive Permutationsgruppe ist vom Typ (A) oder (F).*

Beweis (*ohne Schreiers Vermutung*). Sei $G \to \mathrm{Sym}(\Omega)$ treu und 2-transitiv vom Grad n. Wir können annehmen, dass $N := \mathrm{Soc}(G)$ nichtabelsch ist. Wie üblich operiert N transitiv. Nehmen wir zunächst an, dass N imprimitiv ist. Sei $\Delta \subseteq \Omega$ ein Block von N mit $|\Delta|$ minimal. Für $g \in G$ und $x \in N$ ist dann ${}^g\Delta \cap {}^{xg}\Delta = {}^g(\Delta \cap {}^{g^{-1}xg}\Delta) \in \{\varnothing, {}^g\Delta\}$. Also ist auch ${}^g\Delta$ ein Block von N. Außerdem gilt

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

Da $|\Delta|$ minimal ist, folgt ${}^g\Delta = \Delta$ oder $|\Delta \cap {}^g\Delta| \leq 1$. Seien $\alpha, \beta \in \Omega$ beliebig mit $\alpha \neq \beta$. Da G 2-transitiv operiert, existiert ein $g \in G$ mit $\alpha, \beta \in {}^g\Delta$. Für $\gamma \in \Omega \setminus {}^g\Delta$ existieren $h_1, h_2 \in G$ mit $\alpha, \gamma \in {}^{h_1}\Delta$ und $\beta, \gamma \in {}^{h_2}\Delta$. Im Fall ${}^{h_1}\Delta = {}^{h_2}\Delta$ wäre $\alpha, \beta \in {}^{h_1}\Delta \cap {}^g\Delta = {}^g\Delta$ und somit $\gamma \in {}^g\Delta$. Also ist ${}^{h_1}\Delta \cap {}^{h_2}\Delta = \{\gamma\}$. Für $x \in N_{\alpha\beta}$ gilt dann ${}^x\{\gamma\} = {}^x({}^{h_1}\Delta \cap {}^{h_2}\Delta) = {}^{h_1}\Delta \cap {}^{h_2}\Delta = \{\gamma\}$, da ${}^{h_1}\Delta$ und ${}^{h_2}\Delta$ Blöcke von N sind. Also operiert $N_{\alpha\beta}$ trivial auf $\Omega \setminus {}^g\Delta$. Insbesondere ist $N_{\alpha\beta} \subseteq N_{\alpha\gamma}$. Da G 2-transitiv ist, existiert ein $a \in G$ mit $aN_{\alpha\beta}a^{-1} = N_{{}^a\alpha{}^a\beta} = N_{\alpha\gamma}$. Dies zeigt $N_{\alpha\beta} = N_{\alpha\gamma}$. Wie eben operiert $N_{\alpha\gamma}$ trivial auf $\Omega \setminus {}^{h_1}\Delta$. Wegen ${}^g\Delta \cap {}^{h_1}\Delta = \{\alpha\}$ operiert $N_{\alpha\beta}$ also trivial auf Ω. Es folgt $N_\alpha \cap N_\beta = N_{\alpha\beta} = 1$.

Wir folgen nun den Beweis von Satz 3.11. Sei $M := N \setminus \bigcup_{\omega\in\Omega} N_\omega \cup \{1\}$. Da sich je zwei verschiedene Stabilisatoren trivial schneiden, ist $|M| = |N| - |N : N_\omega|(|N_\omega| - 1) = n$. Sei p ein Primteiler von n und $x \in N$ ein nicht-triviales p-Element. Dann operiert x fixpunktfrei und es folgt $x \in M$. Die Anzahl der Tripel (α, β, y) mit $\alpha, \beta \in \Omega$, $y \in M \setminus \{1\}$ und ${}^y\alpha = \beta$ ist offenbar $n(n-1)$, denn für jedes y und jedes α ist β eindeutig bestimmt. Andererseits gibt es genau $n(n-1)$ Paare (α, β) mit $\alpha \neq \beta$. Für jedes solche Paar gibt es daher genau ein $y \in M$ mit ${}^y\alpha = \beta$. Sei nun $z \in M \setminus \{1\}$ beliebig und ${}^z\alpha = \gamma$. Wegen der 2-Transitivität existiert ein $g \in G$ mit ${}^g\alpha = \alpha$ und ${}^g\beta = \gamma$. Also ist $gyg^{-1} \in M$ mit ${}^{gyg^{-1}}\alpha = \gamma$. Dies zeigt $gyg^{-1} = z$. Somit sind alle nicht-trivialen Elemente von M zu x konjugiert. Insbesondere ist n eine Potenz von p. Sei $P \in \mathrm{Syl}_p(N)$. Wie oben gezeigt ist dann $P \subseteq M$. Wegen $|M| = n \mid |N|$ ist andererseits $|P| \geq |M|$. Dies zeigt $M = P \leq N$. Offenbar ist M auch ein p-Normalteiler von N. Dies widerspricht aber Bemerkung 4.3 und Lemma 4.4.

Wir haben also gezeigt, dass N primitiv ist. Nach Bemerkung 4.3 ist $N = S_1 \oplus \ldots \oplus S_r$ mit einfachen Gruppen $S_1 \cong \ldots \cong S_r$. Nach Satz 4.1 ist $r \leq 2$. Im Fall $r = 1$ folgt die Behauptung aus Lemma 5.5. Sei also $r = 2$. Dann ist S_1 regulär und $|N| = n^2$. Wir betrachten $1 \neq N_\omega \trianglelefteq G_\omega$ für ein $\omega \in \Omega$. Da G 2-transitiv ist, operiert G_ω transitiv auf $\Omega \setminus \{1\}$. Nach Aufgabe 3.8 haben alle Bahnen von N_ω auf $\Omega \setminus \{1\}$ die gleiche Länge $l \mid |N_\omega| = n$. Dies liefert den Widerspruch $0 \equiv n = |\Omega| \equiv 1 \pmod{l}$. □

Lemma A.2 (= Lemma 5.12)**.** *Sei $n \geq 4$ und $A_{n-1} \cong H \leq A_n$. Dann ist $H = \mathrm{Alt}(\{1, \ldots, n\} \setminus \{i\})$ für ein $i \in \{1, \ldots, n\}$ oder $n = 6$.*

Beweis (*mit Bertrands Postulat*). O. B. d. A. sei $n \geq 5$. Nach Lemma 5.10 operiert H treu auf einer Bahn $\Delta \subseteq \{1, \ldots, n\}$. Wegen $|H| = (n-1)!/2$ ist $|\Delta| \geq n - 1$. Wir können also annehmen, dass H transitiv auf $\{1, \ldots, n\}$ operiert. Insbesondere ist $n \mid |H| \mid (n-1)!$. Wir können daher $n \geq 8$ voraussetzen. Dann liefert Beispiel 6.11 aber einen Widerspruch. □

Satz A.3 (= Satz 7.4)**.** *Sei G eine transitive Permutationsgruppe vom Primzahlgrad p. Dann ist G 2-transitiv oder $G \cong C_p \rtimes C_d$ für einen echten Teiler d von $p - 1$.*

Beweis (*mit Charaktertheorie*). Wir können annehmen, dass $G \leq S_p$ nicht 2-transitiv ist. Insbesondere ist $G \ngeq \mathrm{Aff}(1, p) \cong C_p \rtimes C_{p-1}$. Es genügt zu zeigen, dass G vom Typ (A) ist. Da G transitiv ist, gilt $p \mid |G|$. Sei $P = \langle x \rangle \in \mathrm{Syl}_p(G)$. Dann ist $\mathrm{C}_G(P) \leq \mathrm{C}_{S_p}(x) = P$. Sei $y \in G$ beliebig. Ist die Ordnung von y durch p teilbar,

so erzeugt eine gewisse Potenz von y eine p-Sylowgruppe von G. Wegen $\mathrm{C}_G(P) = P$ hat y dann selbst Ordnung p. Jedes Element in G ist also ein p-Element oder ein p'-Element.

Sei nun π der Permutationscharakter von G, d. h. $\pi(g)$ ist die Anzahl der Fixpunkte von $g \in G$. Nach Satz 1.14 ist $(\pi, 1_G)_G = 1$. Sei χ ein irreduzibler Bestandteil von $\pi - 1_G$. Nach Aufgabe 8.8 ist $(\pi, \pi)_G > 2$ und $s := \chi(1) < (\pi - 1_G)(1) = p - 1$. Die Einschränkung π_P entspricht dem regulären Charakter auf P, denn x hat keine Fixpunkte. Also ist $\chi(x)$ die Summe von s paarweise verschiedenen nicht-trivialen p-ten Einheitswurzeln. Insbesondere ist $\chi(x) \notin \mathbb{Q}$. Sei $\zeta \in \mathbb{C}$ eine primitive $|G|$-te Einheitswurzel, und sei $\mathcal{G}$ die Galoisgruppe des Kreisteilungskörpers $\mathbb{Q}(\zeta)$ über $\mathbb{Q}$. Dann existiert ein $\gamma \in \mathcal{G}$ mit ${}^\gamma\chi \neq \chi$. Da π rational ist, muss auch ${}^\gamma\chi$ ein irreduzibler Bestandteil von $\pi - 1_G$ sein. Da $\mathcal{G}$ transitiv auf den nicht-trivialen p-ten Einheitswurzeln operiert, sind alle irreduziblen Bestandteile von $\pi - 1_G$ algebraisch konjugiert zu χ. Insbesondere ist $s \mid p - 1$. Für jedes $\gamma \in \mathcal{G}$ mit ${}^\gamma(\chi_P) = \chi_P$ ist auch ${}^\gamma\chi = \chi$. Dies zeigt $\mathbb{Q}(\chi) = \mathbb{Q}(\chi(x)) \subseteq \mathbb{Q}(\zeta^{|G|/p})$ und $t := [\mathbb{Q}(\chi) : \mathbb{Q}] = (p-1)/s$.

Für ein p'-Element $y \in G$ gilt

$$\chi(y) \in \mathbb{Q}(\chi) \cap \mathbb{Q}(\zeta^{|G|/|\langle y\rangle|}) \subseteq \mathbb{Q}(\zeta^{|G|/p}) \cap \mathbb{Q}(\zeta^{|G|/|\langle y\rangle|}) = \mathbb{Q}$$

(siehe Lemma 10.12 in Charaktertheorie). Als ganz-algebraische Zahl gilt sogar $\chi(y) \in \mathbb{Z}$. Also ist $\pi(y) = 1 + t\chi(y)$ und $\chi(y) \in \{0, \dots, s\}$. Im Fall $\chi(y) = s$ ist $\pi(y) = 1 + st = p$ und $y = 1$. Für einen irreduziblen Bestandteil $\psi \neq \chi$ von $\pi - 1_G$ gilt

$$\sum_{i=1}^{p-1} \chi(x^i) = |P|(\chi_P, 1_P)_P - \chi(1) = -s,$$
$$\sum_{i=1}^{p-1} \chi(x^i)\overline{\psi}(x^i) = |P|(\chi_P, \psi_P)_P - \chi(1)^2 = -s^2.$$

Dies zeigt

$$0 = |G|(\chi, \psi - s1_G)_G = |G : \mathrm{N}_G(P)| \sum_{i=1}^{p-1} \chi(x^i)(\overline{\psi}(x^i) - s) + \sum_{y \in G_{p'}} \chi(y)(\chi(y) - s)$$
$$= \sum_{y \in G_{p'} \setminus \{1\}} \chi(y)(\chi(y) - s),$$

wobei $G_{p'}$ die Menge der p'-Elemente bezeichnet. Für jedes $y \in G_{p'} \setminus \{1\}$ gilt also $\chi(y) = 0$ und $\pi(y) = 1$. Also ist

$$|G| = |G|(\pi, 1_G)_G = \sum_{g \in G} \pi(g) = p + |G_{p'}| - 1.$$

Somit ist P die einzige p-Sylowgruppe in G und $P \trianglelefteq G$. Dies zeigt, dass G vom Typ (A) ist. □

Satz A.4. *Sei $G \leq S_n$ primitiv mit $n \geq 9$. Bewegt ein Element aus G genau vier Ziffern, so ist $G \in \{S_n, A_n\}$.*

Beweis. Ist $g \in G$ ein 4-Zyklus, so hat g^2 Zyklentyp $(2, 2)$. Nach Konjugation dürfen wir also annehmen, dass

$$x := (1, 2)(3, 4) \in G$$

gilt. Sei $y := (\alpha, \beta)(\gamma, \delta) \in G$ beliebig. Gilt $|\{\alpha, \beta, \gamma, \delta\} \cap \{1, 2, 3, 4\}| = 1$, so ist $(xy)^2$ ein 3-Zyklus (vgl. Lemma 6.13) und die Behauptung folgt aus Satz 6.10. Im Fall $|\{\alpha, \beta, \gamma, \delta\} \cap \{1, 2, 3, 4\}| = 3$ ist xy entweder ein 3-Zyklus oder ein 5-Zyklus. Wieder folgt die Behauptung aus Satz 6.10. Wir können also stets $|\{\alpha, \beta, \gamma, \delta\} \cap \{1, 2, 3, 4\}| \in \{0, 2, 4\}$ annehmen.

Schritt 1: G enthält zwei Elemente der Form $(\alpha, \beta)(\gamma, \delta)$ und $(\alpha, \gamma)(\beta, \delta)$.
Offenbar ist

$$N := \langle g \in G \mid g \text{ hat Zyklentyp } (2, 2)\rangle \trianglelefteq G.$$

Nach Satz 2.2 ist N transitiv. Also existiert ein $y := (1, \alpha)(\beta, \gamma) \in G$ mit $\alpha \neq 2$. Im Fall $\alpha \in \{3, 4\}$ ist $\beta, \gamma \geq 5$ und $(xy)^2 \in \{(1, 3)(2, 4), (1, 4)(2, 3)\}$. Sei also $y = (1, 5)(\beta, \gamma)$ mit $|\{\beta, \gamma\} \cap \{2, 3, 4\}| = 1$. Ist $y = (1, 5)(2, 6)$, so ist $(xy)^2 = (1, 2)(5, 6)$ und die Behauptung ist erfüllt. Wir können daher

$$y = (1, 5)(3, 6)$$

annehmen. Dann hat $\langle x, y\rangle$ die beiden Bahnen $\{1, 2, 5\}$ und $\{3, 4, 6\}$. Da N transitiv ist, existiert ein $z \in N$ vom Zyklentyp $(2, 2)$, welches die Menge $\{1, 2, 5\}$ nicht festhält. Nach Konjugation mit x oder y, können wir $z := (1, \alpha)(\beta, \gamma)$ mit $\alpha \notin \{2, 5\}$ annehmen. Ein Vergleich mit x führt wie eben zu $z = (1, \alpha)(3, \gamma)$ oder $z = (1, \alpha)(4, \gamma)$. Ein analoger Vergleich mit y führt zu $z = (1, 7)(3, 8)$ oder $z = (1, 7)(4, 6)$. Im zweiten Fall ist $(xyz)^2 = (1, 5)(2, 7)$ und die Behauptung folgt wie oben (Analyse von y). Sei also

$$z = (1, 7)(3, 8).$$

Dann hat $\langle x, y, z\rangle$ aber immer noch zwei Bahnen und man kann den Prozess wiederholen. Da nur endlich viele Ziffern zur Verfügung stehen, erhält man schließlich Elemente der gesuchten Form.

Schritt 2: $G \in \{S_n, A_n\}$.
Nach Schritt 1 dürfen wir $H := \langle (1, 2)(3, 4), (1, 3)(2, 4)\rangle \leq G$ voraussetzen. Also ist $\{5, \ldots, n\}$ eine Jordan-Menge und G ist 2-transitiv nach Satz 6.6. Nach dem Beweis von Satz 8.15 können wir $n \in \{9, 10\}$ annehmen. Der Stabilisator G_n ist transitiv auf $\{1, \ldots, n-1\}$. Wegen $N_n \trianglelefteq G_n$ ist N $\frac{3}{2}$-transitiv (Aufgabe 3.8). Nach der 2-Transitivität von G können wir $x := (1, 5)(2, 6) \in G$ annehmen (die Fälle $(1, 5)(3, 6)$ und $(1, 5)(4, 6)$ sind symmetrisch). Damit operiert $\langle H, x\rangle \leq N$ transitiv auf $\{1, \ldots, 6\}$. Somit ist der Stabilisator N_n nicht nur $\frac{1}{2}$-transitiv, sondern sogar transitiv. Folglich ist N 2-transitiv und damit primitiv. Da $\{1, 2\}$ kein Block von N ist, existiert ein $y := (\alpha, \beta)(\gamma, \delta) \in N$ mit $\alpha \in \{1, 2\}$ und $\beta, \gamma, \delta \notin \{1, 2\}$. Da y mit $(1, 2)(3, 4)$ und mit x jeweils zwei Ziffern gemeinsam haben muss, bewegt y nur eine zusätzliche Ziffer, sagen wir 7. Also ist $\langle H, x, y\rangle$ transitiv auf $\{1, \ldots, 7\}$ und enthält somit einen 7-Zyklus. Nach Satz 6.10 können wir also $n = 9$ annehmen. Da der 7-Zyklus zwei Fixpunkte hat, ist N sogar 3-transitiv. Da $\langle H, x\rangle$ drei Fixpunkte hat, ist N sogar 4-transitiv. Dann ist aber $(1, 2)(3, 5) \in N$ und die Behauptung folgt wie zu Beginn des Beweises. □

Beispiel A.5. Sei $G := \mathrm{Aff}(3, 2) \leq S_8$. Dann ist der Stabilisator $G_0 \cong \mathrm{GL}(3, 2)$ einfach und damit in A_7 enthalten. Folglich enthält G Elemente vom Zyklentyp $(2, 2)$. Dies zeigt, dass die Schranke $n \geq 9$ in Satz A.4 optimal ist.

Satz A.6. *Sei G eine primitive Permutationsgruppe vom Rang 3. Dann gilt eine der folgenden Aussagen:*

(i) G ist vom Typ (A) oder (F).

(ii) $G \leq H \wr S_2$ ist vom Typ (P), wobei H 2-transitiv vom Typ (F) ist.

Beweis. Wie üblich operiere G auf Ω. Nehmen wir zunächst an, dass G einen regulären Normalteiler N besitzt. Dann hat der Stabilisator G_ω zwei Bahnen auf $N \setminus \{1\}$. Nach dem Satz von Cauchy ist $|N|$ durch höchstens zwei verschiedene Primzahlen teilbar. Nach Burnsides $p^a q^b$-Satz ist N auflösbar und G ist vom Typ (A) (vgl. Aufgabe 2.2). Wir können im Folgenden also annehmen, dass G keine regulären Normalteiler besitzt. Insbesondere ist G nicht vom Typ (V). Sei nun $G \leq \mathrm{Aut}(S) \wr S_k$ vom Typ (D). Sei $B := \mathrm{Soc}(G) \cong S^k$. Bekanntlich ist dann $B_\omega \cong S$ eine diagonale Untergruppe. Die Nebenklassen von G_ω nach G werden daher durch die Elemente $(g_1, \ldots, g_{k-1}, 1) \in B$ mit $g_i \in S$ für $i = 1, \ldots, k-1$ repräsentiert. Sei $(\widehat{x}, y) \in G_\omega$ mit $\widehat{x} = (x, \ldots, x) \in \widehat{\mathrm{Aut}(S)}$ und $y \in S_k$. Für $g \in S$ ist dann

$$(\widehat{x}, y)(g, 1, \ldots, 1)G_\omega = (\widehat{x}, y)(g, 1, \ldots, 1)(\widehat{x}, y)^{-1}G_\omega = (1, \ldots, 1, xgx^{-1}, 1, \ldots, 1)G_\omega.$$

Zwei Nebenklassen $(g, 1, \ldots, 1)G_\omega$ und $(h, 1, \ldots, 1)G_\omega$ liegen also nur dann in der gleichen Bahn, falls g unter $\mathrm{Aut}(S)$ zu h oder h^{-1} konjugiert ist (im zweiten Fall muss $k = 2$ gelten). Nach Voraussetzung hat $|S|$ dann aber wieder nur zwei Primteiler und Burnsides $p^a q^b$-Satz liefert einen Widerspruch.

Sei nun $G \leq H \wr S_k$ vom Typ (P), wobei H auf Δ operiert. Wir benutzen die Operation von Bemerkung 4.20 auf Δ^k. Sei $K \leq G$ der Stabilisator von $(\delta, \ldots, \delta) \in \Delta^k$. Im Fall $k \geq 3$ hätte K mindestens drei nicht-triviale Bahnen auf Δ^k repräsentiert durch $(\alpha, \ldots, \alpha)$, $(\delta, \alpha, \ldots, \alpha)$ und $(\delta, \delta, \alpha, \ldots, \alpha)$ für ein $\alpha \in \Delta \setminus \{\delta\}$. Also ist $k = 2$. Für $\alpha, \beta \in \Delta \setminus \{\gamma\}$ sind außerdem (δ, α) und (δ, β) in einer Bahn unter K. Also operiert H_δ transitiv auf $\Delta \setminus \{\gamma\}$ und H ist 2-transitiv. Nach Definition ist H vom Typ (F) oder (D). Nach Satz 5.19 muss H vom Typ (F) sein. □

Satz A.7. *Für jedes $d \in \mathbb{N}$ gibt es nur endlich viele primitive Permutationsgruppen vom Typ (D) mit Subgrad d.*

Beweis. Sei S eine nichtabelsche einfache Gruppe und $G \leq \mathrm{Aut}(S) \wr S_k$ primitiv auf Ω vom Typ (D) mit Subgrad d. Es genügt zu zeigen, dass der Grad $|S|^{k-1}$ durch eine Funktion in d beschränkt ist. Wie in Satz A.6 lässt sich Ω durch die Elemente $(g_1, \ldots, g_{k-1}, 1) \in \mathrm{Soc}(G)$ realisieren. Sei Δ eine Bahn von G_ω der Länge d und $(g_1, \ldots, g_{k-1}, 1) \in \Delta$. Für $\widehat{x} = (x, \ldots, x) \in \mathrm{Soc}(G)_\omega$ ist dann

$$\widehat{x}(g_1, \ldots, g_{k-1}, 1)G_\omega = (xg_1x^{-1}, \ldots, xg_{k-1}x^{-1}, 1)G_\omega.$$

Also besitzt S eine nichttriviale Konjugationsklasse K mit $|K| \leq d$. Da S treu auf K operiert, folgt $|S| \leq d!$. Wir müssen nun k abschätzen. Sei $N \trianglelefteq G_\omega$ der Kern der Operation auf Δ. Im Fall $\mathrm{Soc}(G)_\omega \leq N$ wäre $g_i \in \mathrm{Z}(S) = 1$ für $i = 1, \ldots, k-1$. Da $\mathrm{Soc}(G)_\omega \trianglelefteq G_\omega$ einfach ist, gilt also $\mathrm{Soc}(G)_\omega \cap N = 1$. Insbesondere ist jedes Elemente von N mit jedem Element von $\mathrm{Soc}(G)_\omega$ vertauschbar.

Nach Definition vom Typ (D) und Satz 1.19 operiert G_ω primitiv auf den k Faktoren von $\mathrm{Soc}(G)$. Der Kern dieser Operation ist $\widehat{\mathrm{Aut}(S)} \cap G_\omega$. Nach dem eben Gezeigten operiert N also treu auf den k Faktoren. Wir können also $N \leq S_k$ annehmen. Als Normalteiler einer primitiven Gruppe ist N transitiv. Sei $1 \leq i \leq k-1$ beliebig und $\Gamma := \{j : h_j = h_i \ \forall (h_1, \ldots, h_{k-1}, 1) \in \Delta\}$. Da G_ω primitiv ist, folgt $\Gamma = \{i\}$. Dies zeigt, dass N sogar regulär auf den k Faktoren von $\mathrm{Soc}(G)$ operiert. Für jedes $h = (h_1, \ldots, h_{k-1}, 1) \in \Delta$ und $x \in N$ gilt $(h_1, \ldots, h_{k-1}, 1)G_\omega = (h_{x^{-1}1}, \ldots, h_{x^{-1}k})G_\omega$ (setze $h_k = 1$). Also ist die Abbildung $\varphi_h : N \to S$, $x \mapsto h_i^{-1}h_{x^{-1}i}$ unabhängig von i. Für $x, y \in N$ gilt

$$\varphi_h(xy) = h_i^{-1}h_{y^{-1}x^{-1}i} = h_i^{-1}h_{x^{-1}i}h_{x^{-1}i}^{-1}h_{y^{-1}x^{-1}i} = \varphi_h(x)\varphi_h(y),$$

d. h. φ_h ist ein Homomorphismus. Sei $x \in \bigcap_{h\in\Delta} \mathrm{Ker}(\varphi_h)$. Für Indizes $i \neq j$ existiert wie oben gezeigt stets ein $h \in \Delta$ mit $h_i \neq h_j$. Folglich ist ${}^xi \neq j$ und $x = 1$. Daher ist der kanonische Homomorphismus $N \to \prod_{h\in\Delta} N/\mathrm{Ker}(\varphi_h)$ injektiv und $k = |N| \leq |S|^d \leq d!^d$. □

Satz A.8 (Maillet)**.** *Sei $G \leq S_n$ 2-transitiv mit alternierendem Sockel. Dann gilt eine der folgenden Aussagen:*

(i) $n \geq 5$ *und* $G \in \{A_n, S_n\}$.

(ii) $n = 6$ *und* $G \in \{A_5, S_5\}$.

(iii) $n = 10$ *und* $A_6 \leq G \leq \mathrm{Aut}(A_6)$.

(iv) $n = 15$ *und* $G \in \{A_7, A_8\}$.

Beweis. Zur besseren Unterscheidung der Mengen nehmen wir an, dass G 2-transitiv auf Ω operiert ($|\Omega| = n$). Sei $\mathrm{Soc}(G) = A_k$ mit $k \geq 5$. O. B. d. A. sei $k < n$. Nehmen wir zunächst $k \neq 6$ an. Nach Satz 5.13 ist $G \in \{A_k, S_k\}$.

Fall 1: $G = S_k$.
Nach Bemerkung 5.16 gibt es für G_ω drei Fälle. Ist Ω die Menge der l-elementigen Teilmengen von $\{1, \ldots, k\}$ für $2 \leq l < \frac{k}{2}$, so wäre die Operation nicht 2-transitiv. Sei nun Ω die Menge der Partitionen von $\{1, \ldots, k\}$ mit $l \geq 2$ gleichgroßen Teilen. Sei zunächst $l \geq 3$ und sei $\omega \in \Omega$ fest. Dann gibt es $\alpha, \beta \in \Omega$, sodass α und ω (bzw. β und ω) genau eine (bzw. keine) Menge gemeinsam haben. Offenbar können dann α und β nicht in der gleichen Bahn unter G_ω liegen. Also ist $l = 2$ und damit $k \geq 8$. Wir können $\omega = \{\{1, \ldots, \frac{k}{2}\}, \{\frac{k}{2}+1, \ldots, k\}\}$ wählen. Offenbar sind dann

$$\{\{1, 2, \ldots, \tfrac{k}{2}-1, k\}, \{\tfrac{k}{2}+1, \ldots, k-1, \tfrac{k}{2}\}\},$$
$$\{\{1, 2, \ldots, \tfrac{k}{2}-2, k-1, k\}, \{\tfrac{k}{2}+1, \ldots, k-2, \tfrac{k}{2}-1, \tfrac{k}{2}\}\}$$

nicht in der gleichen Bahn unter G_ω. Es verbleibt daher nur die Möglichkeit, dass G_ω primitiv auf $\{1, \ldots, k\}$ operiert. Nach Satz 6.14 ist dann $n \geq \lfloor \frac{k+1}{2} \rfloor !$. Sei $x := (1, 2) \in G$ und sei $\omega \in \Omega$ mit $x \notin G_\omega$. Da G_ω transitiv auf $\Omega \setminus \{\omega\}$ operiert, hat x mindestens $n-1$ Konjugierte unter G_ω. Andererseits ist $|G : \mathrm{C}_G(x)| = \binom{k}{2}$. Dies zeigt

$$\Big\lfloor \frac{k+1}{2} \Big\rfloor ! \leq n \leq 1 + \frac{k(k-1)}{2}.$$

Wir zeigen durch Induktion nach k, dass dies für $k \geq 9$ falsch ist. Dafür brauchen wir nur die geraden k betrachten. Offenbar ist die Ungleichung für $k = 10$ nicht erfüllt. Induktion liefert

$$\Big(\frac{k+2}{2}\Big)! = \frac{k+2}{2}\Big(\frac{k}{2}\Big)! > \frac{k+2}{2}\Big(1 + \frac{k(k-1)}{2}\Big) \geq 1 + \frac{(k+2)k(k-1)}{4} \geq 1 + \frac{(k+2)(k+1)}{2}.$$

Also ist $k \in \{5, 8\}$. Im Fall $k = 8$ ist $|G_\omega| \leq 8 \cdot 168$ nach Beispiel 8.14. Dann ist aber $n \geq 30 > 1 + 8 \cdot 7/2$. Also ist $k = 5$. Nach Beispiel 5.17 ist dann $|G_\omega| = 20$ und $n = 6$, denn G_ω ist maximal in G. Man kann dann Ω mit der Menge der 5-Sylowgruppen von G identifizieren. Da eine feste 5-Sylowgruppe die anderen fünf Sylowgruppen transitiv permutiert, ist die Operation tatsächlich 2-transitiv (siehe auch Satz 8.11).

Fall 2: $G = A_k$.
Operiert G auf den l-elementigen Teilmengen oder auf den Partitionen von $\{1, \ldots, k\}$ mit l gleichgroßen Teilen, so lässt sich die Operation zu S_k fortsetzen. Nach Fall 1 kann dann G nicht 2-transitiv operieren. Nehmen wir nun an, dass G_ω primitiv vom Grad k ist. Die Betrachtung des Elements $x := (1, 2, 3) \in G$ führt dann zur schwächeren Ungleichung

$$\frac{1}{2}\Big\lfloor \frac{k+1}{2} \Big\rfloor ! \leq n \leq 1 + 2\binom{k}{3} = 1 + \frac{k(k-1)(k-2)}{3}.$$

Wir zeigen, dass dies für $k \geq 13$ falsch ist. Es genügt wieder die geraden k zu betrachten. Der Fall $k = 14$ ist klar. Induktion liefert nun

$$\frac{1}{2}\Big(\frac{k+2}{2}\Big)! > \frac{k+2}{2}\Big(1 + \frac{k(k-1)(k-2)}{3}\Big) \geq 1 + \frac{(k+2)k(k-1)(k-2)}{6} \geq 1 + \frac{(k+2)(k+1)k}{3}.$$

Also ist $k \in \{12, 10, 9, 8, 7, 5\}$. Sei $k = 12$. Dann ist $n \in \{360, \ldots, 441\}$. Enthält G_ω eine p-Sylowgruppe mit $3 \leq p \leq 7$, so liegt auch ein p-Zyklus in G_ω im Widerspruch zu Satz 6.10. Also ist $105 = 3 \cdot 5 \cdot 7 \mid n$. Dies liefert $n = 420$. Dann ist aber $n - 1 \nmid |G|$ und G ist nicht 2-transitiv. Sei nun $k = 10$. Dann ist $n \in \{60, \ldots, 241\}$ und es folgt $n \in \{105, 210\}$. Wieder ist $n - 1 \nmid |G|$. Im Fall $k = 9$ ist $n \in \{60, \ldots, 169\}$ und $15 \mid n$. In allen Fällen ist $n - 1 \nmid |G|$. Nehmen wir nun $k = 8$ an. Hier ergibt sich analog $n = 15$. Also ist $G_\omega \cong \mathrm{Aff}(3, 2)$ nach Beispiel 8.14. Wegen Satz 8.22 ist jeder Subgrad mindestens 7. Nach Aufgabe 8.4 können die Subgrade nicht 7, 7 sein. Also ist G tatsächlich 2-transitiv. Im Fall $k = 7$ gibt es ebenfalls nur die Möglichkeit $n = 15$. Sei schließlich $k = 5$. Dann gibt es wieder die 2-transitive Operation auf den 5-Sylowgruppen von G.

Fall 3: $k = 6$.
Sei zunächst $G = A_6$. Die Operation auf den Partitionen von $\{1, \ldots, 6\}$ mit zwei gleichgroßen Teilen hat Grad $n = 10$. Nach Beispiel 8.27 ist diese Operation tatsächlich 2-transitiv. Dies entspricht auch der Operation auf den 3-Sylowgruppen von G. Ist G_ω hingegen primitiv, so ergibt sich nur die Möglichkeit $n = k$. Sei nun $A_6 < G \leq \mathrm{Aut}(A_6)$. Dann operiert G sicher auch 2-transitiv auf den 3-Sylowgruppen von A_6. Wir müssen zeigen, dass es keine weiteren Möglichkeiten gibt. Die einzigen weiteren Grade n mit $n(n-1) \mid |G|$ sind $n \in \{9, 16\}$. Im Fall $n = 9$ ist auch $|A_6 : A_6 \cap G_\omega| = 9$. Dies widerspricht Bemerkung 5.16. Sei also $n = 16$. Dann ist $|G_\omega A_6 : A_6| = |G_\omega : G_\omega \cap A_6| \leq 2$ und G_ω ist nicht maximal. □

Bemerkung A.9.

(i) Sei $n = 6$ und $G = S_5$. Dann ist $|G_\omega| = 20$ und G_ω ist 2-transitiv vom Grad 5 nach Satz 7.4. Also ist G sogar scharf 3-transitiv. Sei nun $n = 10$ und $A_6 \leq G \leq \mathrm{Aut}(A_6)$. Im Fall $G = A_6$ kann G aus Ordnungsgründen nicht 3-transitiv sein. Sei nun $|G| = 720$. Dann ist G_ω der Normalisator einer 3-Sylowgruppe P von G. Für $\delta \in \Omega \setminus \{\omega\}$ ist $|G_{\omega\delta}| = 8$ und $P_\delta = 1$, d. h. P operiert regulär auf $\Omega \setminus \{\omega\}$. Die Operation von $G_{\omega\delta}$ auf $\Omega \setminus \{\omega, \delta\}$ ist also isomorph zur Operation auf $P \setminus \{1\}$. Da P auch eine 3-Sylowgruppe von A_6 ist, besteht $P \setminus \{1\}$ aus vier 3-Zyklen und vier Elementen vom Zyklentyp $(3, 3)$. Wie im Beweis von Satz 5.13 existiert ein äußerer Automorphismus von A_6, der 3-Zyklen auf Elemente vom Zyklentyp $(3, 3)$ abbildet. Für $G \neq S_6$ ist G also scharf 3-transitiv auf Ω (für $G = M_{10}$ wissen wir das bereits). Offenbar ist auch $G = \mathrm{Aut}(A_6)$ 3-transitiv vom Grad 10.

Im Fall $n = 15$ und $G \in \{A_7, A_8\}$ ist die Operation aus Ordnungsgründen nicht 3-transitiv.

(ii) Man kann $A_8 \cong \mathrm{GL}(4, 2)$ zeigen. Die 2-transitive Operation von A_8 vom Grad 15 entspricht dabei der Operation von $\mathrm{GL}(4, 2)$ auf $\mathbb{F}_2^4 \setminus \{0\}$.

Satz A.10 (Wielandt). *Jede $\frac{3}{2}$-transitive Permutationsgruppe ist primitiv oder eine Frobeniusgruppe.*

Beweis. Sei $G \leq \mathrm{Sym}(\Omega)$ $\frac{3}{2}$-transitiv, aber nicht primitiv. Dann ist $|\Omega| > 2$. Sei $\omega \in \Omega$ fest, und sei $\Omega = \Delta_1 \dot\cup \ldots \dot\cup \Delta_k$ eine Blockzerlegung mit $\omega \in \Delta_1$. Nach Voraussetzung zerfällt $\Omega \setminus \{\omega\}$ in Bahnen der Länge $m > 1$ unter G_ω. Da G_ω auf Δ_1 operiert, ist $l := |\Delta_1| \equiv 1 \pmod m$. Insbesondere sind m und l teilerfremd. Sei $2 \leq i \leq k$ und $\Gamma := \bigcup_{\delta \in \Delta_i} {}^{G_\omega}\delta = \bigcup_{g \in G_\omega} {}^g\Delta_i$. Dann ist $|\Gamma|$ durch m und l teilbar, also auch durch ml. Dies zeigt

${}^{G_\omega}\delta \cap \Delta_i = \{\delta\}$ für alle $\delta \in \Delta_i$. Für $g \in G_{\omega\delta}$ und $\gamma \in \Delta_i$ gilt ${}^g\gamma = {}^g({}^{G_\omega}\gamma \cap \Delta_i) = {}^{G_\omega}\gamma \cap {}^g\Delta_i = {}^{G_\omega}\gamma \cap \Delta_i = \{\gamma\}$. Es folgt $G_{\omega\delta} \leq G_{\Delta_i}$. Vertauscht man die Rollen von ω und δ, so ergibt sich $G_{\omega\delta} \leq G_{\Delta_1}$. Für $\omega' \in \Delta_1 \setminus \{\omega\}$ ist also $G_{\omega\delta} \leq G_{\omega\omega'}$ und $|G_\omega : G_{\omega\delta}| = m = |G_\omega : G_{\omega\omega'}|$. Somit ist auch $G_{\omega\delta} = G_{\omega\omega'}$. Variiert man nun i und δ, so ergibt sich $G_{\omega\alpha} \leq G_\Omega = 1$ für alle $\alpha \in \Omega \setminus \{\omega\}$. Sei $H := G_\omega$ und $g \in G \setminus H$. Dann ist $H \cap gHg^{-1} = G_\omega \cap G_{g\omega} = G_{\omega({}^g\omega)} = 1$. Also ist H ein Frobeniuskomplement in G. □

Satz A.11. *Die Zustände des Zauberwürfels (Rubik's Cube) bilden eine Permutationsgruppe G vom Grad 48 mit folgenden Eigenschaften:*

(i) $G \leq (C_3 \wr S_8) \times (C_2 \wr S_{12})$.

(ii) $|G| = 2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11 = 43.252.003.274.489.856.000$.

(iii) $|\mathrm{Z}(G)| = 2$.

Beweis. Jede der sechs Seiten des Würfels besteht aus neun Einzelflächen. Die relative Position der sechs Seitenmittelflächen zueinander verändert sich durch Verdrehen des Würfels aber nicht. Man kann diese Flächen also fixieren (zum Beispiel: oben: weiß, vorn: rot). Somit kann man G als Permutationsgruppe auf den $6 \cdot 8 = 48$ verbleibenden Flächen realisieren. Wir werden im Folgenden Zustände und Zugfolgen miteinander identifizieren. Offenbar wird G dann von den 90°-Drehungen um die sechs Seiten erzeugt. Man sieht leicht, dass man die 24 Eckflächen transitiv permutieren kann. Analog lassen sich auch die 24 Kantenflächen transitiv permutieren. Umgekehrt ist es unmöglich eine Eckfläche in eine Kantenfläche zu überführen. Also hat G zwei Bahnen der Länge 24. Die Operation auf beiden Bahnen ist imprimitiv, da die drei Flächen einer Ecke einen Block bilden (bzw. die zwei Flächen einer Kante). Man beachte, dass man diese drei Flächen nur zyklisch permutieren kann. Mit Bemerkung 1.11 und Satz 5.15 erhält man einen Monomorphismus

$$\Gamma : G \to (C_3 \wr S_8) \times (C_2 \wr S_{12}), \tag{A.1}$$

dessen Bild wir bestimmen werden.

Wir zerlegen den Würfel gedanklich in 27 kleinere Würfel, von denen uns nur die acht Eckwürfel E und die 12 Kantenwürfel K interessieren. Wir bestimmen zunächst das Bild der transitiven Operation

$$\varphi : G \to \mathrm{Sym}(E).$$

Sei x die Hintereinanderausführung zweier Drehungen benachbarter Seiten um 90° im Uhrzeigersinn. Dann ist $\varphi(x)$ ein 5-Zyklus, denn $(1,2,3,4)(2,1,5,6) = (1,5,6,3,4)$. Nach Satz 6.2 ist φ sogar primitiv, und nach Satz 6.10 ist $A_8 \leq \varphi(G)$. Da eine 90°-Drehung um eine Seite einen 4-Zyklus auf E bewirkt, muss φ sogar surjektiv sein.

Sei nun $G_1 := \mathrm{Ker}(\varphi)$ und

$$\psi : G_1 \to \mathrm{Sym}(K).$$

Wegen $(1,2,3,4)(1,5,6,7) = (1,5,6,7,2,3,4)$ bewirkt x auf K einen 7-Zyklus. Insbesondere ist auch $\psi(x^5)$ ein 7-Zyklus (beachte: $x^5 \in G_1$). Wählt man für x andere Seiten zum Drehen, so folgt leicht, dass auch ψ surjektiv ist. Mit Satz 6.2 und Satz 6.10 erhält man $A_{12} \leq \psi(G_1)$. Die 90°-Drehungen bewirken sowohl auf E als auch auf K eine ungerade Permutation. Daher sind die Elemente in G_1 gerade Permutationen auf K. Dies zeigt $\psi(G_1) = A_{12}$.

Sei nun $G_2 := \mathrm{Ker}(\psi)$. Dies sind also genau die Zustände, bei denen die 27 Einzelwürfel an der richtigen Stelle liegen, aber verdreht sein können. Wegen (A.1) ist $\Gamma(G_2) \leq C_3^8 \times C_2^{12}$ und $G_2 \cong C_3^a \times C_2^b$ mit $a \leq 8$ und $b \leq 12$. Wir nummerieren die Eckflächen mit $EF := \{1, \ldots, 24\}$, sodass $\{3k-2, 3k-1, 3k\}$ für $k = 1, \ldots, 8$ eine Ecke beschreibt, wobei die drei Eckflächen im Uhrzeigersinn nummeriert werden. Hier trifft man also eine nicht-kanonische Wahl. Dies hängt damit zusammen, dass die Untergruppe S_8 in $C_3 \wr S_8$ nicht eindeutig ist. Sei $\gamma : G \to \mathrm{Sym}(EF)$ und

$$o : G \to \mathbb{Z}/3\mathbb{Z}, \qquad g \mapsto \sum_{k=1}^{8} {}^{\gamma(g)}(3k) \pmod 3$$

(dies beschreibt die „Gesamt-Orientierung" der Ecken). Seien $g, h \in G$ und ${}^{\gamma(h)}(3k) = 3h_k - l_k$ mit $h_k \in \{1, \ldots, 8\}$ und $l_k \in \{0, 1, 2\}$ für $k = 1, \ldots, 8$. Dann ist

$$o(gh) = \sum_{k=1}^{8} {}^{\gamma(gh)}(3k) = \sum_{k=1}^{8} {}^{\gamma(g)}(3h_k - l_k) \equiv \sum_{k=1}^{8} {}^{\gamma(g)}(3h_k) - l_k \equiv o(g) + o(h) \pmod 3,$$

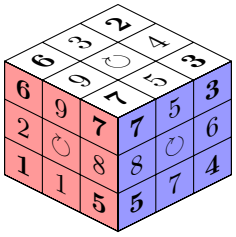
d. h. o ist ein Homomorphismus. Für eine 90°-Drehung g ist allerdings $o(g) = 0$. Also ist $o(g) = 0$ für alle $g \in G$. Es ist daher unmöglich nur eine Ecke zu verdrehen, d. h. $a \leq 7$. Wir zeigen nun $a = 7$.

Dafür beobachten wir, dass x die Orientierung, aber nicht die Position einer bestimmten Ecke e verändert. Also verändert auch $x^{35} \in G_2$ und x^{70} die Orientierung von e. Umgekehrt kippt x^{70} keine Kante. Sei Γ_1 die Projektion von $\Gamma(G_2)$ auf die erste Komponente. Wegen $o(x^{70}) = 0$ ist $\Gamma_1(x^{70})$ nicht konstant. Sei also $\Gamma_1(x^{70}) = (a_1, \ldots, a_8) \in (\mathbb{Z}/3\mathbb{Z})^8$ mit $a_1 \neq a_2$. Es existiert ein $g \in G$ mit $\varphi(g) = (1, 2)$. Dann ist

$$\Gamma_1(gx^{70}g^{-1}x^{-70}) = \Gamma_1(gx^{70}g^{-1})\Gamma_1(x^{-70}) = (a_2, a_1, a_3, \ldots, a_8) - (a_1, \ldots, a_8) = \pm(1, 2, 0, \ldots, 0).$$

Man sieht nun leicht: $|\langle gx^{70}g^{-1} : g \in G\rangle| = 3^7$, d. h. $a = 7$ (dies entspricht dem *Standard-Modul* von S_8 über $\mathbb{F}_3$).

Wir zeigen schließlich $b = 11$. Eine 90°-Drehung bewirkt zwei 4-Zyklen, also eine gerade Permutation auf den Kantenflächen. Es ist also unmöglich nur eine Kante zu kippen, d. h. $b \leq 11$. Sei y die Hintereinanderausführung von 90°-Drehungen im Uhrzeigersinn um die folgenden Seiten: vorn, rechts, oben (in dieser Reihenfolge).



Dann ist $\varphi(y) = (1, 2, 3, 4, 5)(6, 7)$ und $\psi(y) = (1, \ldots, 8)$. Also ist $y^{40} \in G_2$ und $y^{120} \in \mathrm{Ker}(\Gamma_1)$. Beobachtet man den Verlauf einer Kante, so stellt man fest, dass y^8 mindestens eine Kante kippt. Umgekehrt bewegt y drei Kanten gar nicht. Ist also Γ_2 die Projektion von $\Gamma(G_2)$ auf die zweite Komponente, so ist $\Gamma_2(y^{120})$ nicht konstant. Es folgt wie oben, dass $|\langle gy^{120}g^{-1} : g \in G\rangle| = 2^{11}$ gilt. Insgesamt ist

$$|G| = |G/G_1||G_1/G_2||\Gamma_1(G_2)||\Gamma_2(G_2)| = 8! \cdot 12! \cdot 3^7 \cdot 2^{10} = 43.252.003.274.489.856.000.$$

Sei schließlich $1 \neq z \in \mathrm{Z}(G)$. Dann ist $\varphi(z) \in \mathrm{Z}(S_8) = 1$ und $\psi(z) \in \mathrm{Z}(A_{12}) = 1$, d. h. $z \in G_2$. Außerdem müssen $\Gamma_1(z)$ und $\Gamma_2(z)$ konstant sein. Wegen $o(z) = 0$ ist $z \in \mathrm{Ker}(\Gamma_1)$. Also ist z der Zustand, bei dem alle Kanten gekippt sind. Dies ist offensichtlich auch ein zentrales Element in G. □

Bemerkung A.12. Man kann den Beweis von Satz A.11 auch als (langwierigen) Lösungsalgorithmus verwenden. Man versucht dabei einen vorgegebenen Zustand $g \in G$ so zu manipulieren, dass er zunächst in G_1 und dann in G_2 liegt. Man erhält außerdem, dass ein Element $(a, \sigma, b, \tau) \in ((\mathbb{Z}/3\mathbb{Z})^8 \rtimes S_8) \times ((\mathbb{Z}/2\mathbb{Z})^{12} \rtimes S_{12})$ genau dann in G liegt, falls $\sum_{i=1}^{8} a_i = \sum_{i=1}^{12} b_i = 0$ und $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\tau)$ gilt. Zerlegt man den Würfel in seine Einzelteile und baut diese zufällig wieder zusammen, so ist der Würfel mit einer Wahrscheinlichkeit von $11/12 \approx 92\%$ nicht mehr lösbar. Viel schlimmer ist es jedoch, wenn man die Aufkleber entfernt und permutiert.

Satz A.13. *Bis auf Symmetrie besitzt der Zauberwürfel genau* 901.083, 404.981.813.616 *verschiedene Zustände.*

Beweis. Sei G die Gruppe des Zauberwürfels wie in Satz A.11. Wir wenden Satz 1.14 mit der Symmetriegruppe des Würfels $W \cong S_4 \times C_2$ an. Sind zwei Symmetrien in W konjugiert, so stimmen sie in der Anzahl der Fixpunkte auf G offenbar überein. Da die Rotationsgruppe S_4 genau 5 Konjugationsklassen hat, besitzt W genau 10 Konjugationsklassen:

- 1 – Identität
- d_4 – 90°-Drehung um die x-Achse
- d_4^2 – 180°-Drehung um die x-Achse
- d_3 – 120°-Drehung um eine Raumdiagonale
- d_2 – 180°-Drehung um eine Gerade durch gegenüberliegende Kantenmittelpunkte
- s – Punktspiegelung am Mittelpunkt des Würfels

- sd_4^2 – Spiegelung an der xy-Ebene
- sd_2 – Spiegelung diagonal durch eine Seitenmitte
- sd_4, sd_3 – Kompositionen

Realisiert man die Elemente in W als Permutationen auf den 48 Seitenflächen, so sind G und W beide in $X := (S_3 \wr S_8) \times (C_2 \wr S_{12})$ enthalten (man beachte den Faktor S_3). Für $x \in W$ ist die Anzahl der Fixpunkte also gerade $|\mathrm{C}_G(x)|$. Wir schreiben $x = (x_e, x_k) \in X$. Seien G_e und G_k die Bilder der entsprechenden Projektion von G. Für $x \in W$ und $g \in G$ gilt $g \in \mathrm{C}_G(x)$ genau dann, wenn $g_e \in \mathrm{C}_{G_e}(x_e)$ und $g_k \in \mathrm{C}_{G_k}(x_k)$. Wir können also die Ecken und Kanten getrennt betrachten. Sei $x_e = (x_e^o, x_e^p) \in S_3^8 \rtimes S_8$ und $x_k = (x_k^o, x_k^p) \in C_2^8 \rtimes S_{12}$. Für die Definition von x_e^o und x_k^o muss man wieder eine nicht-kanonische Wahl treffen. Solange x fest ist, funktioniert aber oft $x_e^o = 1 \in S_3^8$ bzw. $x_k^o = 1 \in C_2^{12}$. Für $i \in \{e, k\}$ gilt nun

$$\begin{aligned} g_i \in \mathrm{C}_G(x_i) &\iff x_i^o x_i^p g_i^o g_i^p = g_i^o g_i^p x_i^o x_i^p \iff x_i^o (x_i^p g_i^o (x_i^p)^{-1}) x_i^p g_i^p = g_i^o (g_i^p x_i^o (g_i^p)^{-1}) g_i^p x_i^p \\ &\iff x_i^p g_i^p = g_i^p x_i^p \ \wedge \ x_i^o (x_i^p g_i^o (x_i^p)^{-1}) = g_i^o (g_i^p x_i^o (g_i^p)^{-1}). \end{aligned}$$

Im Fall $x_i^o = 1$ verkürzt sich die zweite Bedingung zu $x_i^p g_i^o = g_i^o x_i^p$. Wir machen eine Tabelle, wobei für x_i^p nur der Zyklentyp angeben ist. Für die Werte von x_e^o in S_3 benutzen wir $\sigma := (1,2,3)$ und $\tau := (1,2)$.

$x \in W$	$\lvert^W x\rvert$	x_e^o	x_e^p	x_k^o	x_k^p	$\lvert\mathrm{C}_{G_e}(x_e)\rvert$	$\lvert\mathrm{C}_{G_k}(x_k)\rvert$	$\lvert\mathrm{C}_G(x)\rvert$
1	1	1	1	1	1	$8! \cdot 3^7$	$12! \cdot 2^{11}$	$\lvert G\rvert$
d_4	6	1	4^2	1	4^3	$4^2 \cdot 2 \cdot 3$	$4^3 \cdot 3! \cdot 2^3$	$2^{14} \cdot 3^2$
d_4^2	3	1	2^4	1	2^6	$2^4 \cdot 4! \cdot 3^3$	$2^6 \cdot 6! \cdot 2^6$	$2^{22} \cdot 3^6 \cdot 5$
d_3	8	$(\sigma, \sigma^2, 1^{(6)})$	3^2	1	3^4	$3^2 \cdot 2 \cdot 3^3$	$3^4 \cdot 4! \cdot 2^3$	$2^6 \cdot 3^{10}$
d_2	6	1	2^4	$(-1,-1,1^{(10)})$	2^5	$2^4 \cdot 4! \cdot 3^3$	$2^6 \cdot 5! \cdot 2^6$	$2^{21} \cdot 3^5 \cdot 5$
s	1	$(\tau^{(8)})$	2^4	1	2^6	$2^4 \cdot 4! \cdot 3^4$	$2^6 \cdot 6! \cdot 2^6$	$2^{22} \cdot 3^7 \cdot 5$
sd_4	6	$(\tau^{(8)})$	4^2	1	4^3	$4^2 \cdot 2 \cdot 3^2$	$4^3 \cdot 3! \cdot 2^3$	$2^{14} \cdot 3^3$
sd_4^2	3	$(\tau^{(8)})$	2^4	1	2^4	$2^4 \cdot 4! \cdot 3^4$	$2^4 \cdot (4!)^2 \cdot 2^7$	$2^{23} \cdot 3^7$
sd_3	8	$(\sigma\tau, \tau^{(7)})$	$(2,6)$	1	6^2	$6 \cdot 3^2$	$6^2 \cdot 2 \cdot 2^2$	$2^5 \cdot 3^5$
sd_2	6	$(\tau^{(8)})$	2^2	$(-1,-1,1^{(10)})$	2^5	$2^3 \cdot 4! \cdot 3^2$	$2^6 \cdot 5! \cdot 2^6$	$2^{20} \cdot 3^4 \cdot 5$

Wir erläutern beispielhaft den Fall $x = sd_3$. Man sieht leicht, dass $x_e^p = (1,2)(3,\dots,8)$ gilt. Da x eine Spiegelung enthält, wird die Orientierung aller Ecken um eine Transposition verändert. Für die Ecken $3,\dots,8$ kann man die Orientierung offenbar gleich wählen, zum Beispiel τ. Da x^2 die Orientierung der ersten Ecke immer noch verändert, können die Orientierungen der ersten beiden Ecken nicht gleich sein, also zum Beispiel $x_e^o = (\sigma\tau, \tau, \dots, \tau)$. Nach der oben angegebenen Bedingung ist $g_e^p \in \mathrm{C}_{G_e}(x_e^p) = \langle (1,2), (3,\dots,8) \rangle$. Nehmen wir ${}^{g_e^p}1 = 2$ an. Sei $g_e^o = (\sigma^i, \sigma^j, *, \dots, *)$. Dann gilt

$$(\sigma\tau, \tau, \dots, \tau)(\sigma^j, \sigma^i, *, \dots, *) = (\sigma^i, \sigma^j, *, \dots, *)(\tau, \sigma\tau, \tau, \dots, \tau).$$

Es folgt $\sigma^{1-j}\tau = \sigma\tau\sigma^j = \sigma^i\tau$ und $\sigma^{-i}\tau = \tau\sigma^i = \sigma^{j+1}\tau$. Dieser Widerspruch zeigt $g_i^p \in \langle (3,\dots,8) \rangle$. Eine ähnliche Rechnung zeigt nun $g_e^o = (\sigma^i, \sigma^{-i}, \sigma^j, \sigma^{-j}, \sigma^j, \sigma^{-j}, \sigma^j, \sigma^{-j})$ mit $i, j \in \{0,1,2\}$. Dadurch ist automatisch gewährleistet, dass die Gesamt-Orientierung der Ecken 0 ist. Es gilt also $|\mathrm{C}_{G_e}(x_e)| = 6 \cdot 3^2$. Analog ist $x_k^p = (1,\dots,6)(7,\dots,12)$ und $x_k^o = 1$. Es folgt $g_k^p \in \mathrm{C}_{G_k}(x_k) \cong C_6 \wr C_2$ und $x_k^o = ((-1)^i, \dots, (-1)^i, (-1)^j, \dots, (-1)^j)$ mit $i, j \in \{0,1\}$. Dadurch ist auch gewährleistet, dass eine gerade Anzahl von Kanten gekippt wird. Also ist $|\mathrm{C}_{G_k}(x_k)| = 6^2 \cdot 2 \cdot 2^2$. Beachtet man nun, dass G Index 2 in $G_e \times G_k$ hat, so folgt $|\mathrm{C}_G(x)| = 2^5 \cdot 3^5$. Satz 1.14 lieft nun die gesuchte Anzahl. □

Bemerkung A.14. Man kann Satz A.13 auch leicht mit GAP bewerkstelligen (siehe `http://www.gap-system.org/Doc/Examples/rubik.html`). Hat man eine Lösung für einen Zustand des Zauberwürfels gefunden, so ergibt sich daraus leicht eine Lösung (der gleichen Länge) für alle symmetrischen Zustände. Satz A.13 reduziert also die Suche nach (kurzen) Lösungen ungefähr um den Faktor 48. Eine Lösung für $g \in G$ liefert auch eine Lösung für g^{-1} (der gleichen Länge). Dies reduziert die Anzahl weiter ungefähr um den Faktor 2 auf 450.541.810.590.509.978.

Satz A.15. *Im schlechtesten Fall benötigt man mindestens* 18 *Züge, um einen vorgegebenen Zustand des Zauberwürfels zu lösen. Ein Zug sei hierbei eine Drehung um eine Seite um* 90°, 180° *oder* 270°.

Beweis. Wir zählen wie viele Zustände man mit weniger als 18 Zügen höchstens erreichen kann. Nach 0 Zügen hat man den Ausgangszustand. Für den ersten Zug gibt es $z_1 := 3 \cdot 6 = 18$ Möglichkeiten. Im zweiten Zug macht es keinen Sinn die gleiche Seite noch einmal zu drehen. Es gibt nun also noch 15 Möglichkeiten. Sind die ersten beiden Drehungen um gegenüberliegende Seiten, so spielt die Reihenfolge dieser Züge keine Rolle. Mit zwei Zügen erreicht man also maximal $z_2 := 18 \cdot 15 - 9 \cdot 3 = 3^5$ Zustände. Sei nun $n \geq 3$. Man hat dann 12 Möglichkeiten für den n-ten Zug, falls dieser nicht um die gleiche Achse wie der $(n-1)$-te Zug erfolgen soll. Dreht man jedoch um die gleiche Achse, so sollte der $(n-1)$-te Zug nicht auf der gleichen Achse wie der $(n-2)$-te Zug sein. Zusätzlich spielt dann die Reihenfolge von Zug n und Zug $n-1$ keine Rolle. Dies zeigt $z_n := 12z_{n-1} + 18z_{n-2}$. Die Lösung dieser Rekursionsgleichung ist

$$z_n = \frac{3+\sqrt{6}}{4}(6+3\sqrt{6})^n + \frac{3-\sqrt{6}}{4}(6-3\sqrt{6})^n$$

(vgl. Fibonacci-Zahlen). Schließlich ist

$$1 + \sum_{i=1}^{17} z_i = \frac{90+33\sqrt{6}}{116}(6+3\sqrt{6})^{17} + \frac{90-33\sqrt{6}}{116}(6-3\sqrt{6})^{17} - \frac{16}{29} < 43.252.003.274.489.856.000. \qquad \square$$

Bemerkung A.16. Der sogenannte *Superflip* $s \in \mathrm{Z}(G) \setminus \{1\}$ benötigt 20 Züge und dies ist auch die Höchstzahl für alle Zustände, d. h. *God's Number* ist 20 (siehe `http://www.cube20.org/`). Aus mathematischer Sicht ist dies der Durchmesser des entsprechenden Cayley-Graphen. Der Beweis erforderte erheblichen Computereinsatz.

Stichwortverzeichnis