Norbert Klingen

Endliche Gruppen II

Konstruktive Gruppentheorie

Universität zu Köln WS 1988/89

Inhaltsverzeichnis

§5 Freie Gruppen

a. Heuristik, Definition

Sei G eine Gruppe und $A \subset G$ ein Erzeugendensystem. Dann haben wir die folgenden Beschreibungen der Elemente von G:

$$\begin{aligned} G &= \{ \prod_{i=1}^{r} a_i^{n_i} \mid r \in \mathbb{N},\, \underline{a} = (a_1, \ldots, a_r) \in A^r,\, \underline{n} = (n_i) \in \mathbb{Z}^r \} \\ &= \{ \prod_{i=1}^{r} a_i^{\varepsilon_i} \mid r \in \mathbb{N},\, \underline{a} = (a_i) \in A^r,\, \underline{\varepsilon} = (\varepsilon_i) \in \{\pm 1\}^r \} \\ &= \{ \prod_{i=1}^{r} a_i^{\varepsilon_i} \mid r \in \mathbb{N},\, \underline{a} = (a_i) \in A^r, \underline{\varepsilon} = (\varepsilon_i) \in \{\pm 1\}^r,\, a_i = a_{i+1} \Rightarrow \varepsilon_i = \varepsilon_{i+1} \} \end{aligned}$$

Diese Umformungen für die möglichen Darstellungen der Elemente von G durch ein Erzeugendensystem A gelten für *alle* Gruppen. Weitere Umformungen und evtl. Verkürzungen sind ohne zusätzliche spezielle Kenntnisse über G, genauer über Beziehungen zwischen den Erzeugenden, nicht allgemein möglich, denn es gibt (siehe Abschnitt b.) eine Gruppe $F(A)$ mit A als Erzeugendensystem, in der die letztgenannte Darstellung der Elemente *eindeutig* ist; dies ist die *freie Gruppe über A*. Das Erzeugendensystem A hat in ihr ähnliche Eigenschaften wie eine Basis in einem Vektorraum.

Bei der Definition einer freien Gruppe wollen wir uns jedoch an eine andere ('kategorietheoretische') Charakterisierung von Basen in Vektorräumen anlehnen. Hat eine Gruppe G die oben erwähnte eindeutige Darstellung ihrer Elemente durch die Erzeugenden, so kann man offenbar für jede beliebige Gruppe H und jede Auswahl von Elementen $\varphi(a) \in H$ $(a \in A)$ einen *Gruppenhomomorphismus* $\widetilde{\varphi}\colon G \to H$ definieren mit $\widetilde{\varphi}(a) = \varphi(a)$ für alle $a \in A$, indem man setzt

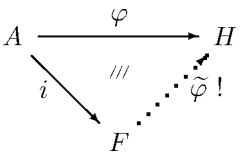
$$\widetilde{\varphi}\,(\prod_{i=1}^{r} a_i^{\varepsilon_i}) := \prod_{i=1}^{r} (\varphi(a_i))^{\varepsilon_i}.$$

Offenbar ist dieser Ansatz zwangsläufig und $\widetilde{\varphi}$ daher eindeutig bestimmt.

(5.1) Definition: Sei A eine nicht-leere Menge. Eine *freie Gruppe über A* ist eine Gruppe F zusammen mit einer Abbildung $i\colon A \to F$, die folgende Eigenschaft hat:

Für jede Gruppe H und jede Abbildung $\varphi\colon A \to H$ existiert *genau* ein Gruppen*homomorphismus* $\widetilde{\varphi}\colon F \to H$ mit

$$\widetilde{\varphi} \circ i = \varphi\,.$$



(5.2) Bemerkung: Sei A eine nicht-leere Menge.

a) Wie alle 'universellen Objekte' ist auch die freie Gruppe über A bis auf Isomorphie eindeutig bestimmt. Sie wird daher mit $F(A)$ bezeichnet.

b) Die zur freien Gruppe $F(A)$ gehörende Abbildung $i\colon A \to F(A)$ ist injektiv; man faßt daher stets A als Teilmenge von $F(A)$ auf.

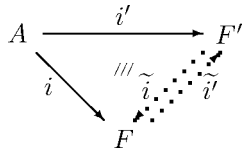
c) $F(A)$ wird von A erzeugt.

d) Gilt in einer von A erzeugten Gruppe F

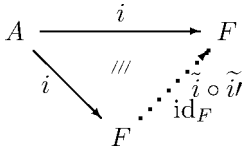
$$\prod_{i=1}^{r} a_i^{\varepsilon_i} \neq 1$$

für alle $r \in \mathbb{N}_+$, $\underline{a} = (a_i) \in A^r$, $\underline{\varepsilon} = (\varepsilon_i) \in \{\pm 1\}^r$ mit der Eigenschaft $a_i = a_{i+1} \Rightarrow \varepsilon_i = \varepsilon_{i+1}$, so ist F die freie Gruppe über A.

Beweis: a) Seien F, F' zwei freie Gruppen über A mit ihren Abbildungen $i\colon A \to F$, $i'\colon A \to F'$. Wir betrachten dann das nebenstehende kommutative Diagramm. Die universelle Eigenschaft von F sichert die Existenz des Homomorphismus $\widetilde{i'}\colon F \to F'$, während die universelle Eigenschaft von F' die Existenz von $\widetilde{i}\colon F' \to F$ liefert. Die Behauptung ist nun, daß diese Homomorphismen zueinander invers sind.



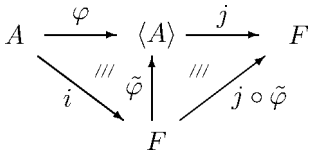
Zum Beweis von $\widetilde{i} \circ \widetilde{i'} = \mathrm{id}_F$ benutzt man die in (5.1) geforderte Eindeutigkeit für das nebenstehende Diagramm. Nach Konstruktion der Homomorphismen $\widetilde{i}$ bzw. $\widetilde{i'}$ ist das Diagramm kommutativ. Offensichtlich ist aber auch die Identität id_F ein Homomorphismus, der das Diagramm kommutativ ergänzt, so daß beide Homomorphismen übereinstimmen müssen: $\mathrm{id}_F = \widetilde{i} \circ \widetilde{i'}$.



Aus Symmetriegründen erhält man genauso $\widetilde{i'} \circ \widetilde{i} = \mathrm{id}_{F'}$, so daß die Homomorphismen $\widetilde{i}$ und $\widetilde{i'}$ zueinander inverse Isomorphismen sind: $F \simeq F'$.

Ad b): Sei $a \in A$ und $\varphi\colon A \to \mathbb{Z}/2\mathbb{Z}$ definiert durch $\varphi(a) = 1$, $\varphi(b) = 0$ für $b \neq a$. Der dadurch induzierte Gruppenhomomorphismus $\widetilde{\varphi}\colon F(A) \to \mathbb{Z}/2\mathbb{Z}$ bildet $i(a)$ auf 1, jedoch alle anderen $i(b)$ auf 0 ab, also folgt $i(a) \neq i(b)$ für $a \neq b$.

Ad c): Gemäß b) fassen wir A als Teilmenge von $F(A)$ und i als Inklusion auf. Sei nun $H = \langle A \rangle$ die von A erzeugte Untergruppe in F und φ die Inklusion $A \hookrightarrow \langle A \rangle$. Dann existiert ein Gruppenhomomorphismus $\widetilde{\varphi}\colon F \to \langle A \rangle$ mit $\varphi = \widetilde{\varphi} \circ i$. Bezeichnet $j\colon \langle A \rangle \to F$ die Inklusion, so ist das nebenstehende Diagramm kommutativ. Wegen $j \circ \varphi = i = \mathrm{id}_F \circ i$ wird das Gesamtdiagramm auch durch id_F kommutativ ergänzt. Aufgrund der Eindeutigkeitsforderung in Def. (5.1) folgt hieraus $\mathrm{id}_F = j \circ \widetilde{\varphi}$. Damit ist die Inklusion $j\colon \langle A \rangle \to F$ surjektiv und c) bewiesen.



Ad d): Die Voraussetzung ist gleichbedeutend mit der eindeutigen Darstellbarkeit aller Elemente von F in der Form $\prod_{i=1}^{r} a_i^{\varepsilon_i}$ mit den genannten Nebenbedingungen, jedoch einschließlich $r = 0$. Wie bereits in den heuristischen Vorüberlegungen erwähnt, hat F dann die universelle Eigenschaft (5.1), ist also die freie Gruppe über A.

b. Konstruktion freier Gruppen

(5.3) Satz: *Zu jeder Menge $A \neq \emptyset$ existiert eine freie Gruppe $F(A)$ über A. Sie ist bis auf Isomorphie eindeutig.*

Die Eindeutigkeit ist nach (5.2),a) klar. Zum Existenzbeweis *konstruieren* wir zu jeder Menge $A \neq \emptyset$ eine Gruppe $F(A)$, die von A erzeugt wird und die Bedingung in Bemerkung (5.2),d) erfüllt.

Die freie Halbgruppe. Zunächst konstruieren wir die *freie Halbgruppe* $H(B)$ über der Menge $B := A \dot\cup A'$, wobei $'\colon A \to A'$ eine Bijektion sei.
[Die Elemente a' von A' sollen später in $F(A)$ die Inversen der $a \in A$ liefern.]
Wir setzen

$$H(B) = \dot{\bigcup_{n \in \mathbb{N}}} B^n,$$

und definieren die *Verkettung* $*$ auf $H(B)$ durch

$$(b_1, \ldots, b_r) * (c_1, \ldots, c_s) = (b_1, \ldots, b_r, c_1, \ldots, c_s).$$

Dann ist diese Verknüpfung auf $H(B)$ assoziativ, und das eindeutig bestimmte Element in $B^0 = B^\emptyset$ (die leere Abbildung) ist neutrales Element, welches mit 1 bezeichnet wird. Die Elemente von B sind als B^1 in $H(B)$ enthalten, und es gilt:

> Jedes Element von $H(B)$ ist eindeutig darstellbar in der Form $w = b_1 * \ldots * b_r$ mit $r \in \mathbb{N}$ und $b_i \in B$. Man spricht daher von den Elementen von $H(B)$ als den 'Worten' über dem 'Alphabet' B.

Diese Eindeutigkeit der Darstellung aller $w \in H(B)$ impliziert, daß $H(B)$ die freie Halbgruppe über B ist, d.h. $B \to H(B)$ erfüllt die zu (5.1) analoge universelle Eigenschaft, wobei H über alle *Halb*gruppen variiert. Wir wollen dies hier jedoch nicht weiter ausführen.

Wir wollen nun vielmehr aus der freien Halbgruppe $H(B)$ die freie Gruppe $F(A)$ konstruieren. Wir setzen zunächst die Abbildung $':A \to A'$ fort zu einer Bijektion $':B \to B$ durch

$$B \ni b \mapsto \begin{cases} a' & \text{falls } b = a \in A, \\ a & \text{falls } b = a' \in A'. \end{cases}$$

Schließlich definieren wir für $w = b_1 * \ldots * b_s$ das Wort $w' = b'_s * \ldots * b'_1$. Dadurch wird $':H(B) \to H(B)$ eine selbstinverse Bijektion. Wir konstruieren nun $F(A)$ als Quotienten von $H(B)$ nach einer Kongruenzrelation '$\sim$', für die $b * b' \sim 1 \sim b' * b$ gilt. Wir definieren sukzessive

$$\begin{aligned} v \prec w :\iff & \bigvee_{u_1,u_2 \in H(B), b \in B} v = u_1 * u_2\,,\ w = u_1 * b * b' * u_2 \\ v \asymp w :\iff & \ v \prec w \ \vee\ v = w \ \vee\ w \prec v \\ v \sim w :\iff & \bigvee_{u_i \in H(B)} v = u_1 \asymp u_2 \asymp \ldots \asymp u_r = w. \end{aligned}$$

Damit ist '$\sim$' eine Kongruenzrelation auf $H(B)$ und die Menge der Kongruenzklassen

$$F(A) = H(B)/\!\sim$$

bzgl. repräsentantenweiser Verknüpfung eine Halbgruppe mit 1. Für $w \in H(B)$ bezeichne $\overline{w} \in F(A)$ die Restklasse und $\overline{v} \cdot \overline{w} := \overline{v * w}$ das Produkt in $F(A)$. Nun ist aber die Relation '$\sim$' gerade so definiert, daß jedes Element $\overline{w} \in F(A)$ das Element $\overline{w'}$ als Inverses besitzt und $F(A)$ daher eine *Gruppe* ist.

Wir wollen nun zeigen, daß die so konstruierte Gruppe $F(A)$ die Eigenschaft von Bemerkung (5.2),d) hat. Wir benutzen dazu, daß die Elemente von $F(A)$ in $H(B)$ eine Normalformdarstellung besitzen, die sog. *reduzierte Wortdarstellung* $w_\sigma \in H(B)$ von $\sigma \in F(A)$. Wir wollen ein Wort w in $H(B)$ *reduziert* nennen, wenn es kein Teilwort der Gestalt $b * b'$ für ein $b \in B$ enthält.

Wir zeigen nun die Existenz einer Funktion $\mathcal{N}: H(B) \to H(B)$, der sog. *Normalformfunktion*, mit folgenden Eigenschaften für alle Worte $w \in H(B)$:

i) $w = \mathcal{N}w \iff w$ ist reduziert.

ii) $\overline{v} = \overline{w} \iff \mathcal{N}v = \mathcal{N}w$.

Wir werden die Funktion explizit angeben und dabei zeigen, daß für jedes Argument ihr Wert in endlich vielen Schritten berechenbar ist. Wir definieren nämlich den *Reduktionsprozeß* für jedes Wort $w = b_1 * \ldots * b_s$ induktiv durch die Folge von Worten $w_0 = 1$ und für $w_{i-1} = c_1 * \ldots * c_t$

$$w_i = \begin{cases} w_{i-1} * b_i & \text{falls } b_i \neq c'_t, \\ c_1 * \ldots * c_{t-1} & \text{falls } b_i = c'_t. \end{cases}$$

Das Endergebnis w_s dieses Reduktionsprozesses ist die gesuchte Normalform $\mathcal{N}w$.

Wie man sofort sieht (d. h. induktiv beweist), sind die so definierten w_i reduziert, ist $w_i \sim b_1 * \ldots * b_i$, insbesondere also $\mathcal{N}w = w_s \sim w$, und es gilt $w_i = b_1 * \ldots * b_i \Leftrightarrow b_1 * \ldots * b_i$ reduziert. Damit hat $\mathcal{N}$ Eigenschaft i). Ebenso ist mit $\overline{w} = \overline{\mathcal{N}w}$ die Bedingung ii),'$\Leftarrow$' bewiesen. Die Umkehrung von ii) folgt, wenn wir gezeigt haben, daß äquivalente Worte dieselbe Normalform besitzen. Es genügt dabei zu zeigen

$$v \prec w \Rightarrow \mathcal{N}v = \mathcal{N}w,$$

denn dann vererbt sich diese Eigenschaft sukzessive auf die Relationen '$\asymp$' und '$\sim$'. ('$\sim$' ist die kleinste Äquivalenzrelation, die '$\prec$' enthält, und durch $v \approx w \iff \mathcal{N}v = \mathcal{N}w$ ist natürlich eine Äquivalenzrelation definiert.)

Sei $v = u_1 * u_2$, $w = u_1 * b * b' * u_2$. Da bei der Definition des Reduktionsprozesses der i-te Term w_i nur vom vorherigen Term w_{i-1} und dem i-ten Buchstaben b_i von w abhängt, folgt $w_r = (u_1)_r = v_r$, wenn r die Länge des Wortes u_1 ist. Aus denselben Gründen genügt es zu zeigen, daß $w_{r+2} = w_r$ ist.
Sei $w_r = c_1 * \ldots * c_s$ mit $c_i \in B$. Dann gilt nach Definition:
Ist $c'_s \neq b$, so ist $w_{r+1} = w_r * b$ und folglich $w_{r+2} = w_r$.
Ist $c'_s = b$, so ist $w_{r+1} = c_1 * \ldots * c_{s-1}$. Da w_r reduziert ist, folgt $c_{s-1} \neq c'_s = b$, also $c'_{s-1} \neq b'$ und daher $w_{r+2} = c_1 * \ldots * c_{s-1} * b' = c_1 * \ldots * c_{s-1} * c_s = w_r$.

Die so konstruierte *Normalformfunktion* liefert somit zu jedem Wort in $H(B)$ ein *äquivalentes reduziertes* Wort, das *eindeutig* und mit dem *Reduktionsprozeß* in endlich vielen Schritten *berechenbar* ist. Daher besitzt jedes Element $\sigma \in F(A)$ ein eindeutig bestimmtes reduziertes Urbild $w_\sigma \in H(B)$, die sog. *reduzierte Wortdarstellung* w_σ von σ.

Ist nun

$$\sigma = \prod_{i=1}^{r} a_i^{\varepsilon_i} \in F(A)\,,$$

so ist ein Urbild $w \in H(B)$ für σ gegeben durch

$$w = b_1 * \ldots * b_r$$

mit $b_i = a_i$ für $\varepsilon_i = 1$ und $b_i = a'_i$ im anderen Falle. Sind nun für das gegebene σ die Bedingungen von 5.2),d) erfüllt, so bedeutet dies gerade, daß w reduziert ist. Da w nicht das leere Wort e ist, kann $\overline{w} = \sigma$ nicht gleich $\overline{e} = 1$ sein. Damit ist Satz (5.3) vollständig bewiesen. □

Die im Beweis definierten Begriffe und Funktionen werden auch weiterhin eine wichtige Rolle spielen.

(5.4) Proposition: *Die freien Gruppen F_i über zwei Mengen A_i ($i = 1, 2$) sind genau dann isomorph, wenn die freien Erzeugendensysteme A_i gleichmächtig sind.*

Beweis: Ist $f\colon A_1 \to A_2$ eine Bijektion, so ist F_2 zusammen mit der Abbildung $A_1 \xrightarrow{f} A_2 \to F_2$ eine freie Gruppe über A_1, also nach (5.2),a) isomorph zu F_1.

Seien nun F_1 und F_2 isomorph. Dann stimmen in ihnen die Anzahlen $N_2(F_i)$ aller Untergruppen vom Index höchstens 2 überein. Diese Zahl $N_2(F)$ berechnet sich in der freien Gruppe $F = F(A)$ über A wie folgt. Untergruppen vom Index höchstens 2 sind notwendig Normalteiler, und damit treten sie gerade als Kerne der Homomorphismen $\varphi\colon F \to C_2$ auf. Da umgekehrt solche Homomorphismen durch ihren Kern eindeutig bestimmt sind, folgt:

$$N_2(F) = \#\{\, U \leq F \mid (F : U) \leq 2 \,\} = \#\{\, \varphi\colon F \to C_2 \mid \varphi \text{ Homomorphismus} \,\}\,.$$

Gemäß Definition (5.1) sind alle Homomorphismen von $F(A)$ nach C_2 eindeutig durch ihre Einschränkung auf A bestimmt, also ergibt sich die Formel

$$N_2(F) = \#\{\, \varphi\colon A \to C_2 \mid \varphi \text{ Abbildung} \,\} = \#\, {C_2}^A = 2^{\#A}\,.$$

Aus $N_2(F_1) = N_2(F_2)$ ergibt sich zunächst, daß beide 'Basen' A_i endlich oder beide unendlich sind. Sind beide endlich, so folgt aus $2^{\#A_1} = 2^{\#A_2}$ natürlich die Gleichheit $\#A_1 = \#A_2$. Sind beide A_i unendlich, so gilt $\#A_i \leq \#F_i \leq \#H(B_i) = \#B_i = \#A_i$, also $\#A_i = \#F_i$, und es folgt wiederum die Behauptung. □

Aufgrund dieser Proposition ist die Mächtigkeit eines freien Erzeugendensystems eine Invariante freier Gruppen, der sog. *Rang* der freien Gruppe.

c. Freiheitssatz von Schreier

Ziel dieses Abschnittes ist der Beweis von

(5.5) Satz: (Freiheitssatz von Schreier)

a) Untergruppen freier Gruppen sind frei.

b) Ist F frei von endlichem Rang n und $U \leq F$ eine Untergruppe von endlichem Index d, so ist U frei vom Rang $nd - (d-1) = d(n-1) + 1$.

Als ersten Beweisschritt untersuchen wir Erzeugungen von Untergruppen U in beliebigen Gruppen F. Dazu sei A ein Erzeugendensystem von F und S ein Repräsentantensystem der U-Nebenklassen in F mit $1 \in S$. Ein solches S bestimmt dann eine Funktion $\phi\colon F \to S$ durch die Vorschrift

$$\phi(x) \text{ ist das eindeutig bestimmte Element } \rho \in S \text{ mit } Ux = U\rho\,.$$

(5.6) Lemma: *Sei F eine beliebige Gruppe, A ein Erzeugendensystem von F, $U \leq F$ eine Untergruppe, $S \subset F$ ein volles Repräsentantensystem für die U-Nebenklassen (mit $1 \in S$) und ϕ die dadurch definierte Funktion.*
Dann ist ein Erzeugendensystem für U gegeben durch die Elemente

$$u_{\sigma,a} := \sigma a \phi(\sigma a)^{-1}\,, \quad \sigma \in S\,, a \in A\,.$$

Untergruppen von endlichem Index d in einer endlich erzeugten Gruppe mit n Erzeugenden sind somit endlich erzeugt mit nd Erzeugenden.

Beweis: Nach Definition von ϕ liegen die angegebenen Elemente $\sigma a \phi(\sigma a)^{-1}$ in U. Weiter sind die Inversen solcher Elemente darstellbar als

$$u_{\sigma,a}^{-1} = \phi(\sigma a) a^{-1} \sigma^{-1} = \rho a^{-1} \sigma^{-1} = \rho b \sigma^{-1} = \rho b \phi(\rho b)^{-1} = u_{\rho,b}$$

mit $\rho = \phi(\sigma a)$ und $b = a^{-1} \in A \cup A^{-1}$; wegen ρ, $\sigma \in S$ gilt nämlich

$$\rho = \phi(\sigma a) \iff U\sigma a = U\rho \iff U\sigma = U\rho a^{-1} \iff \sigma = \phi(\rho a^{-1}).$$

Die Behauptung des Lemmas ist also gleichwertig mit

$$U \subseteq \langle u_{\rho,b} \mid \rho \in S\,,\, b \in A \cup A^{-1} \rangle\,.$$

Sei nun $u = b_1 \cdot \ldots \cdot b_r \in U$ mit $b_i \in A \cup A^{-1}$. Wir definieren $\sigma_i = \phi(b_1 \cdot \ldots \cdot b_i)$ für $i = 0, \ldots, r$. Offenbar gilt $\sigma_0 = 1$ und wegen $u \in U$, $1 \in S$ auch $\sigma_r = \phi(u) = 1$. Damit erhält man

$$u = \sigma_0 u \sigma_r^{-1} = \sigma_0 b_1 \sigma_1^{-1} \cdot \sigma_1 b_2 \sigma_2^{-1} \cdot \ldots \cdot \sigma_{r-1} b_r \sigma_r^{-1}\,,$$

und u ist darstellbar als Produkt von Elementen der Form

$$\begin{aligned} \sigma_{i-1} b_i \sigma_i^{-1} &= \sigma_{i-1} b_i \phi(b_1 \cdot \ldots \cdot b_{i-1} b_i)^{-1} \\ &\overset{!}{=} \sigma_{i-1} b_i \phi(\phi(b_1 \cdot \ldots \cdot b_{i-1}) b_i)^{-1} \\ &= \sigma_{i-1} b_i \phi(\sigma_{i-1} b_i)^{-1}\,. \end{aligned}$$

Zum Beweis des Lemmas fehlt so lediglich der Nachweis der Gleichung '$\overset{!}{=}$': Offenbar gilt

$$Ua = U\phi(a) \Rightarrow Uab = U\phi(a)b \Rightarrow U\phi(ab) = U\phi(\phi(a)b)),$$

woraus nach Definition von ϕ die in der behaupteten Gleichung benutzte Formel $\phi(ab) = \phi(\phi(a)b)$ folgt. □

Um Satz (5.5) zu beweisen, benutzen wir ein Erzeugendensystem von U wie in Lemma (5.6), jedoch ausgehend von einem speziell gewählten Repräsentantensystem S:

(5.7) Lemma: *Sei $F = F(A)$ die freie Gruppe über A, $U \leq F$ eine Untergruppe.*
[Wir benutzen die Darstellung von F als Quotient der freien Halbgruppe $H(B)$ über $B = A \dot\cup A'$ und die Bezeichnungen aus dem Beweis von Satz (5.3).]
Dann existiert ein Repräsentantensystem S der U-Nebenklassen mit der folgenden Eigenschaft:

> *Ist $w = b_1 * \ldots * b_r \in H(B)$ $(b_i \in B)$ ein reduziertes Wort und $\overline{w} \in S$, so liegen auch alle durch die Wortanfänge $w_i = b_1 * \ldots * b_i$ von w gebildeten Elemente $\overline{w_i}$ $(i = 0, \ldots, r)$ in S.*

Beweis: Zur Konstruktion von S wählen wir eine *Wohlordnung* von $B = A \dot\cup A'$, d.h. eine Totalordnung, in der jede nicht-leere Teilmenge ein Minimum besitzt.
[Dies ist im Rahmen der üblicherweise zugrundegelegten Mengenlehre immer möglich; ist A höchstens abzählbar, so wählt man z.B. eine Abzählung von B durch $\mathbb{N}$ und überträgt so die Wohlordnung der natürlichen Zahlen auf B.]

Wir definieren dann eine Wohlordnung auf der freien Halbgruppe $H(B)$ wie folgt:

$$b_1 * \ldots * b_s < c_1 * \ldots * c_t \iff$$
$$s < t \text{ oder } s = t\ ,\ b_1 = c_1, \ldots, b_i = c_i\ ,\ b_{i+1} < c_{i+1} \text{ für ein } i \in \{0, \ldots, s-1\}.$$

Zur Definition des Repräsentantensystems S bzw. der entsprechenden Funktion ϕ wählen wir in jeder Nebenklasse Ux das 'kleinste' Element; genauer:

$$\phi(x) = \overline{m} \quad \text{mit} \quad m = \min\{w \in H(B) \mid \overline{w} \in Ux\}.$$

Da beliebige Wortdarstellungen in $H(B)$ für Elemente aus F länger, und damit im Sinne der definierten Ordnung größer als das entsprechende reduzierte Wort sind, ist $m = \min\{w \mid \overline{w} \in Ux\}$ ein reduziertes Wort in $H(B)$. Man kann $\phi(x)$ daher auch charakterisieren als das Element in Ux, dessen reduzierte Wortdarstellung kleiner ist als alle Wortdarstellungen von Elementen in Ux. S selbst ist als Wertemenge von ϕ definiert.

Sei nun $w = b_1 * \ldots * b_r \in H(B)$ $(b_i \in B)$ ein reduziertes Wort und $\overline{w} \in S$. Dann ist $w = \min\{v \in H(B) \mid \overline{v} \in U\overline{w}\}$. Es genügt nun zu zeigen:

$$u := b_1 * \ldots * b_{r-1} = m := \min\{v \in H(B) \mid \overline{v} \in U\overline{u}\}.$$

Aus $U\overline{u} = U\overline{m}$ folgt $U\overline{w} = U\overline{u}\,\overline{b_r} = U\overline{m}\,\overline{b_r} = U\overline{m*b_r}$, und daher wegen der Minimalität von w die Abschätzung $u*b_r = w \leq m*b_r$. Diese impliziert angesichts der Definition der Ordnungsrelation $u \leq m$. Da nach Definition von m selbstverständlich $u \geq m$ gilt, folgt die Behauptung. □

Ziel der nun folgenden Überlegungen ist es zu zeigen, daß die in Lemma (5.6) konstruierten Erzeugenden $u_{\sigma,a} = \sigma a \phi(\sigma a)^{-1}$ $(\sigma \in S,\ a \in A)$ ein freies Erzeugendensystem von U bilden, wenn S gemäß Lemma (5.7) gewählt wird und die $u_{\sigma,a} = 1$ außer Betracht bleiben:

$$U \text{ ist die freie Gruppe über den Elementen } u_{\sigma,a} \text{ mit } \sigma \in S\,,\ a \in A\,,\ u_{\sigma,a} \neq 1\,.$$

Wir untersuchen nun gemäß (5.2),d) Potenzprodukte

$$u := \prod_{i=1}^{r} u_{\sigma_i,a_i}^{\varepsilon_i} \quad (r \geq 1\,,\ \sigma_i \in S\,,\ a_i \in A\,,\ \ u_{\sigma_i,a_i} \neq 1\,,\ \varepsilon_i \in \{\pm 1\})$$

und setzen voraus, daß für *kein* i gilt:

$$\sigma_{i+1} = \sigma_i \ \wedge\ a_{i+1} = a_i \ \wedge\ \varepsilon_{i+1} = -\varepsilon_i\,. \tag{1}$$

Wegen $u_{\sigma,a}^{-1} = u_{\phi(\sigma a),a^{-1}} = u_{\rho,b}$ mit $\rho = \phi(\sigma a) \in S, b = a^{-1} \in A \dot\cup A^{-1}$ hat u dann eine Darstellung der Form

$$u = \prod_{i=1}^{r} u_{\rho_i,b_i} \quad (r \geq 1\,,\ \rho_i \in S\,,\ b_i \in A \dot\cup A^{-1}\,,\ u_{\rho_i,b_i} \neq 1)\,.$$

Dabei berechnen sich die ρ_i, b_i gemäß

$$(\rho_i, b_i) = \begin{cases} (\sigma_i, a_i) & \text{falls } \varepsilon_i = +1, \\ (\phi(\sigma_i a_i), a_i^{-1}) & \text{falls } \varepsilon_i = -1, \end{cases} \tag{2}$$

Die Bedingung (1) ist dann äquivalent zu

$$b_{i+1} = b_i^{-1} \text{ und } \rho_{i+1} = \phi(\rho_i b_i)\,. \tag{3}$$

Begründung: Bedingung (1) ist symmetrisch in i und $i+1$. Dasselbe gilt wegen $\rho_{i+1} = \phi(\rho_i b_i) \iff \rho_i = \phi(\rho_{i+1} b_i^{-1}) = \phi(\rho_{i+1} b_{i+1})$ auch für (3). Aufgrund der Symmetrie können wir o. E. bei (1) $\varepsilon_i = +1$, $\varepsilon_{i+1} = -1$ und bei (3) $b_i \in A$, $b_{i+1} = b_i^{-1} \notin A$ voraussetzen. Dann folgt (3) aus (1) mittels (2):

$$\rho_{i+1} \underset{(2)}{=} \phi(\sigma_{i+1} a_{i+1}) \underset{(1)}{=} \phi(\sigma_i a_i) \underset{(2)}{=} \phi(\rho_i b_i)\,,\ b_{i+1} \underset{(2)}{=} a_{i+1}^{-1} \underset{(1)}{=} a_i^{-1} \underset{(2)}{=} b_i^{-1}\,.$$

Umgekehrt folgt aus $b_i \in A$, $b_{i+1} \notin A$ zunächst $\varepsilon_i = +1$, $\varepsilon_{i+1} = -1$. Damit ergibt sich $a_{i+1} \underset{(2)}{=} b_{i+1}^{-1} \underset{(3)}{=} b_i \underset{(2)}{=} a_i$. Daraus folgt dann weiter

$$\begin{aligned} &\phi(\sigma_{i+1} a_{i+1}) \underset{(2)}{=} \rho_{i+1} \underset{(3)}{=} \phi(\rho_i b_i) = \phi(\sigma_i a_{i+1}) \\ &\iff U\sigma_{i+1} a_{i+1} = U\sigma_i a_{i+1} \iff U\sigma_{i+1} = U\sigma_i \iff \sigma_{i+1} = \sigma_i\,. \end{aligned}$$

Wir setzen nun voraus, daß für *kein* i die Bedingung (3) erfüllt ist, und wollen dann zeigen, daß u nicht 1 sein kann. Wir untersuchen dafür die reduzierte Wortdarstellung von $u \in F(A)$ in der freien Halbgruppe $H(B)$ über $B := A \dot\cup A'$ und zeigen, daß diese nicht das leere Wort ist.
Wir führen folgende Bezeichnungen ein:
$\mathcal{N}(w)$ sei die reduzierte Normalform eines Wortes $w \in H(B)$,
$w_\sigma \in H(B)$ sei die reduzierte Wortdarstellung für $\sigma \in S$,
der Repräsentant für $b \in A \dot\cup A^{-1}$ in $H(B)$ werde ebenfalls mit b bezeichnet,
und schließlich sei $w'_\sigma = w_{\sigma^{-1}}$ die reduzierte Wortdarstellung für σ^{-1}.

(5.8) Hilfssatz: *Seien F, A, U, S und ϕ wie in (5.7). Es seien $b, c \in B$, $\sigma, \tau \in S$ und $\rho = \phi(\sigma b)$ bzw. $\omega = \phi(\tau c)$.*

a) *Ist $u_{\sigma,b} = \sigma b \phi(\sigma b)^{-1} = \sigma b \rho^{-1} \neq 1$, so ist $w_\sigma * b * w'_\rho$ die reduzierte Wortdarstellung für das Erzeugende $u_{\sigma,b}$, d. h. b kommt im reduzierten Wort vor.*

b) *Sind $u_{\sigma,b}$ und $u_{\tau,c}$ von 1 verschieden und ist für das Produkt $u_{\sigma,b}u_{\tau,c}$ Bedingung (3) nicht erfüllt, d. h. $b \neq c^{-1}$ oder $\tau \neq \phi(\sigma b) = \rho$, so ist $w_\sigma * b * \mathcal{N}(w'_\rho * w_\tau) * c * w'_\omega$ die reduzierte Wortdarstellung von $u_{\sigma,b}u_{\tau,c}$, d. h. b und c kommen im reduzierten Wort vor.*

Beweis: a) Ist $w_\sigma * b * w'_\rho$ nicht reduziert, so muß entweder der letzte 'Buchstabe' von w_σ oder der erste von w'_ρ gleich b' sein.

Im ersten Falle ist $w_\sigma = w_1 * b'$. Da S die Eigenschaft von Lemma (5.7) hat, ist $\overline{w_1} \in S$, also

$$\sigma b = \overline{w_\sigma * b} = \overline{w_1 * b' * b} = \overline{w_1} \in S\,.$$

Dies widerspricht der Voraussetzung $u_{\sigma,b} \neq 1$, denn nach Definition von ϕ und S gilt:

$$u_{\sigma,b} = 1 \iff \sigma b = \phi(\sigma b) \iff \sigma b \in S\,. \tag{4}$$

Im zweiten Fall schließt man wegen $u_{\sigma,b}^{-1} = u_{\rho,b^{-1}}$ genauso.

b) Angenommen, im Reduktionsprozeß für $w_\sigma{*}b{*}w'_\rho{*}w_\tau{*}c{*}w'_\omega$ lassen sich b oder c wegkürzen. Läßt sich c zuerst wegkürzen, so muß, da nach Teil a) die Worte $w_\sigma{*}b{*}w'_\rho$ und $w_\tau{*}c{*}w'_\omega$ reduziert sind, $w_\tau{*}c$ ein Anfang von w_ρ sein. Dann liegt aber τc in S und es ist $u_{\tau,c} = 1$, ein Widerspruch.

Genauso schließt man, wenn sich b zuerst wegkürzt. Schließlich bleibt die Möglichkeit, daß sich b und c gleichzeitig gegeneinander wegkürzen. Dies ist aber nur möglich, wenn $w_\rho = w_\tau$ und $b' = c$ sind, d. h. $b = c^{-1}$ und $\tau = \rho = \phi(\sigma b)$ ist, im Widerspruch zur Voraussetzung. □

Aus (5.8),b) folgt somit, daß das Element $u = \prod_{i=1}^{r} u_{\sigma_i,b_i}$ mit den genannten Nebenbedingungen nicht 1 sein kann, da seine reduzierte Wortdarstellung alle Faktoren b_i enthält. Damit ist U die freie Gruppe über den $u_{\sigma,a} \neq 1$ ($\sigma \in S$, $a \in A$) und Teil a) von Satz (5.5) ist bewiesen.

Zum Beweis von Satz (5.5),b) gilt es die Erzeugenden abzuzählen. Deren Anzahl ist

$$\#\{(\sigma,a) \in S \times A \mid u_{\sigma,a} \neq 1\} = \#S \cdot \#A - \#\{(\sigma,a) \in S \times A \mid u_{\sigma,a} = 1\}\,.$$

Wir setzen

$$D := \{(\sigma,a) \in S \times A \mid u_{\sigma,a} = 1\} \underset{(4)}{=} \{(\sigma,a) \in S \times A \mid \sigma a \in S\}\,,$$

so daß Satz (5.5), b) gleichbedeutend ist mit der Aussage $\#D = d-1 = \#S-1$. Wir konstruieren zum Beweis eine Bijektion $\theta : D \xrightarrow{\sim} S \setminus \{1\}$ durch die Zuordnung

$$D \ni (\sigma,a) \mapsto \theta(\sigma,a) = \begin{cases} \sigma & \text{falls } w_\sigma \text{ auf } a' \text{ endet,} \\ \sigma a & \text{falls } w_\sigma \text{ nicht auf } a' \text{ endet.} \end{cases}$$

Nach Definition von D gilt in beiden Fällen $\theta(\sigma,a) \in S$. Außerdem gilt nach Definition von θ in den entsprechenden Fällen:

$$w_{\theta(\sigma,a)} = \begin{cases} w_\sigma & \text{endet auf } a', \\ w_{\sigma a} = w_\sigma{*}a & \text{endet auf } a. \end{cases} \tag{5}$$

Dies zeigt, daß $w_{\theta(\sigma,a)}$ nicht leer, also $\theta(\sigma,a) \neq 1$ ist. Damit ist $\theta : D \to S\setminus\{1\}$ eine wohldefinierte Abbildung und man muß die Umkehrabbildung angeben. Mittels (5) kann man aus dem Element $\rho = \theta(\sigma,a) \in S$ das Element a ablesen, nämlich als letzten Buchstaben von ρ bzw. dessen Inverses, und damit die Umkehrabbildung wie folgt definieren:

$$S \setminus \{1\} \ni \rho \mapsto \begin{cases} (\rho, a) & \text{falls } w_\rho \text{ auf } a' \in A' \text{ endet,} \\ (\rho a^{-1}, a) & \text{falls } w_\rho \text{ auf } a \in A \text{ endet.} \end{cases}$$

Da für $\rho \neq 1$ das Wort w_ρ nicht leer ist, also mit irgendeinem Buchstaben aus $B = A \dot\cup A'$ endet, ist diese Zuordnung auf ganz $S\setminus\{1\}$ definiert. Wir zeigen zunächst, daß die zugeordneten Werte in D liegen. Im ersten Falle ist $\rho \in S$ und wegen $w_\rho = w_1{*}a'$ ist $\rho a = \overline{w_1} \in S$, denn w_1 ist ein Anfang von w_ρ. Im zweiten Fall endet ρ auf a, so daß mit gleicher Argumentation ρa^{-1} zu S gehört. Schließlich gehört $\rho a^{-1} \cdot a = \rho$ nach Voraussetzung zu S.

Damit ist eine Abbildung $S\setminus\{1\} \to D$ wohldefiniert, die offenbar zu θ invers ist. Dies beendet den Beweis von Satz (5.5). □

§6 Erzeugende und Relationen

a. Präsentierung von Gruppen

Wir wollen nun die freien Gruppen benutzen, um beliebige Gruppen zu beschreiben.

(6.1) Satz: *a) Jede Gruppe G ist Faktorgruppe einer freien Gruppe.*
b) Ist $E = \{\widetilde{a} \mid a \in A\}$ (A eine beliebige Indexmenge) ein Erzeugendensystem der Gruppe G, so existiert genau ein Gruppenepimorphismus $\varphi\colon F(A) \to G$ von der freien Gruppe über A auf die Gruppe G mit $\varphi(a) = \widetilde{a}$ für alle $a \in A$.

Dieser Satz ist nichts anderes als die definierende Eigenschaft (5.1) der freien Gruppe $F(A)$, lediglich mit der Zusatzaussage, daß φ surjektiv ist. Diese ist natürlich klar, da E die Gruppe G erzeugt und im Bild von φ liegt.

Für ein beliebiges Element $\sigma \in F(A)$ nennen wir $\widetilde{\sigma} := \varphi(\sigma)$ die *Interpretation* von σ in G. Wir benutzen dieselbe Notation für Worte $w \in H(B)$; also explizit: $\widetilde{w} := \widetilde{\widetilde{w}}$. Nun sind die Elemente $w \in H(B)$ Worte in endlich vielen a_i, a_j' mit $a_i, a_j \in A$; wir schreiben daher manchmal $w = w(a_1, \ldots, a_r)$. Da man die Interpretation von w in G erhält, indem man alle in w auftretenden a_i bzw. a_j' durch die $\widetilde{a}_i \in G$ bzw. $\widetilde{a}_j^{-1} \in G$ ersetzt und das Produkt in G interpretiert, schreibt man suggestiv $\widetilde{w} = w(\widetilde{a_1}, \ldots, \widetilde{a_r})$ und nennt dies auch die *Einsetzung* der $\widetilde{a}_i$ in w. [Dies ist völlig analog zur Definition des Einsetzungshomomorphismus bei Polynomringen.]

(6.2) Definition: Wird G von $E = \widetilde{A}$ erzeugt und ist $\varphi\colon F(A) \to G$ der obige Epimorphismus, so nennt man den Kern $\mathcal{N} := \operatorname{Ke}\varphi$ den *Relationennormalteiler* des gegebenen Erzeugendensystems E von G und die Elemente darin die *Relationen* zwischen den gegebenen Erzeugenden von G. Oft werden auch die (reduzierten) Repräsentanten dieser Relationen in der Worthalbgruppe $H(B)$ als Relationen bezeichnet.

In obiger Sprechweise sind Relationen also Elemente der freien Gruppe über A, deren Interpretation in G das Einselement ist, oder noch laxer gesagt, die Elemente der freien Gruppe $F(A)$, die 'in der Gruppe G zu 1 werden'. Mit Definition (6.2) ist eine mathematisch befriedigende Präzisierung des Relationenbegriffs gegeben.

Die freien Gruppen sind offenbar die Gruppen mit einem Erzeugendensystem ohne echte Relationen (d.h. ohne Relationen verschieden vom leeren Wort).

Man kann nun auf diese Weise Gruppen *konstruieren,* die einen vorgegebenen Satz von Erzeugenden haben und in denen beliebig vorgegebene Relationen gelten.

(6.3) Definition: Sei A eine nicht leere Menge und $\mathcal{R} \subseteq F(A)$ eine Teilmenge der freien Gruppe über A. Dann definieren wir *die von A erzeugte Gruppe mit den definierenden Relationen $\mathcal{R}$* als

$$G = \langle A \mid \mathcal{R} \rangle := F(A)/\langle\langle \mathcal{R} \rangle\rangle\,.$$

Wir nennen eine solche Beschreibung der Gruppe G eine *Präsentierung.* Eine Präsentierung heiße *endlich*, wenn Erzeugendensystem A und Relationensystem $\mathcal{R}$ endlich sind. Schließlich heißt eine Gruppe *endlich präsentierbar*, wenn sie eine endliche Präsentierung besitzt.

Präsentierte Gruppen besitzen die folgende universelle Eigenschaft:

(6.4) Proposition: *Sei $G = \langle A \mid \mathcal{R} \rangle$ eine präsentierte Gruppe, H eine Gruppe und darin ein Element $\tilde{a} \in H$ für jedes $a \in A$. Für diese Elemente $\tilde{a}$ seien in H alle Relationen $w \in \mathcal{R}$ für die $\tilde{a}$ erfüllt, das soll heißen:*

$$\bigwedge_{w = w(a_1, \ldots, a_r) \in \mathcal{R}} w(\widetilde{a_1}, \ldots, \widetilde{a_r}) = e_H \text{ in } H.$$

Dann gibt es genau einen Gruppenhomomorphismus $\varphi : G \to H$ mit $\varphi(a) = \tilde{a}$. Dieser ist ein Epimorphismus, wenn H von den $\tilde{a}$ ($a \in A$) erzeugt wird.

Der *Beweis* ist nichts anderes der Homomorphiesatz.

(6.5) Folgerung: *Sei $A \neq \emptyset$ und $\mathcal{R} \subseteq F(A)$ eine Menge von Relationen. Dann gilt: Das Normalteilererzeugnis $\langle\langle \mathcal{R} \rangle\rangle$ von $\mathcal{R}$ in $F(A)$ besteht genau aus den Relationen, die in all den Gruppen H mit einem Erzeugendensystem $\widetilde{A}$ erfüllt sind, in denen die gegebenen Relationen aus $\mathcal{R}$ gelten. $\langle\langle \mathcal{R} \rangle\rangle$ besteht also aus allen sich (zwangsläufig ergebenden) sog. Folgerelationen von $\mathcal{R}$.*

Beweis: Sei $w \in \langle\langle \mathcal{R} \rangle\rangle$ und H eine Gruppe mit den genannten Eigenschaften. Dann ist nach (6.4) H epimorphes Bild der präsentierten Gruppe $G = \langle A \mid \mathcal{R} \rangle$: $\varphi : G \twoheadrightarrow H$. Nach Definition 'gilt' w in G, d. h. unter der Abbildung $F(A) \twoheadrightarrow G$ gilt $w \mapsto 1_G$. Dann folgt aber erst recht $\varphi(w) = 1_H$ in H.
Ist umgekehrt $w \notin \langle\langle \mathcal{R} \rangle\rangle$, so ist die Interpretation $\widetilde{w}$ von w in $H := F(A)/\langle\langle \mathcal{R} \rangle\rangle$ gerade die Restklasse $\widetilde{w} = w\langle\langle \mathcal{R} \rangle\rangle$, also nicht 1. Damit ist H eine Gruppe, in der die Relationen aus $\mathcal{R}$ erfüllt sind, w aber nicht. □

Beispiel: Die Diedergruppe D_8 besitzt zwei Erzeugende a, b, für die $a^2 = b^4 = 1$ und $a^{-1}ba = b^{-1}$ gilt. Damit ist D_8 epimorphes Bild der Gruppe mit diesen Relationen als definierenden Relationen:

$$G := \langle a, b \mid a^2, b^4, ba^{-1}ba \rangle \twoheadrightarrow D_8 \,.$$

In diesem Falle gilt sogar Isomorphie, denn die in Frage stehende präsentierte Gruppe G hat *höchstens* die Ordnung 8. Dies beruht darauf, daß man aufgrund der Vertauschbarkeitsrelation $ba = ab^{-1}$ zunächst alle Elemente in G in der Form $a^i b^j$ darstellen und dann wegen $a^2 = 1$ und $b^4 = 1$ zusätzlich $0 \leq i \leq 1\,,\ 0 \leq j \leq 3$ erreichen kann.

Die Übereinstimmung $D_8 = \langle a, b \mid a^2, b^4, ba^{-1}ba \rangle$ bedeutet, daß sämtliche in D_8 geltenden Relationen *Folgerelationen* der drei genannten Relationen sind. Diese drei sind also *definierende* Relationen für D_8.

(6.6) Satz: *Alle endlichen Gruppen sind endlich präsentierbar.*

Beweis: Sei G eine endliche Gruppe und A irgendein (natürlich endliches) Erzeugendensystem von G. Wir betrachten die dadurch gegebene Präsentierung $\langle A \mid \mathcal{R} \rangle$ mit $\mathcal{R} = \operatorname{Ke} \varphi$ für einen Epimorphismus $\varphi\colon F(A) \to G$ gemäß Satz (6.1). Nun ist $\mathcal{R}$ beileibe nicht endlich, wohl aber endlich erzeugt gemäß Satz (5.5): $F(A)$ ist eine endlich erzeugte freie Gruppe, und $\mathcal{R}$ hat endlichen Index in $F(A)$, weil die Faktorgruppe die nach Voraussetzung endliche Gruppe G ist. Ein endliches Erzeugendensystem von $\mathcal{R}$ als Gruppe ist natürlich erst recht ein Erzeugendensystem von $\mathcal{R}$ als Normalteiler in $F(A)$, so daß Satz (6.6) bewiesen ist. □

Im Zusammenhang mit endlich präsentierten Gruppen stellen sich einige weitgehend ungelöste Probleme:

Wortproblem: Gibt es für eine gegebene endlich präsentierte Gruppe ein Verfahren, das in endlich vielen Schritten von *jedem* Wort in den Erzeugenden entscheidet, ob es die 1 der Gruppe darstellt?

Transformationsproblem: Gibt es ein Verfahren, das in endlich vielen Schritten von je zwei vorgelegten Worten in den Erzeugenden entscheidet, ob sie in der Gruppe konjugiert sind?

Isomorphieproblem: Man entscheide, ob zwei präsentierte Gruppen isomorph sind.

Das Wortproblem ist als Spezialfall im Transformationsproblem enthalten. Beide Probleme sind nur für unendliche Gruppen interessant. Das Wortproblem besitzt eine negative (!) Lösung (Novikov 1955; 4 Erzeugende, 32 Relationen, kein Entscheidungsverfahren). Während man für positive Antworten auf die Entscheidbarkeitsprobleme i. a. keine Präzisierung des Begriffes 'Verfahren' benötigt, muß man für ein negatives Resultat zunächst diesen Begriff fixieren (Church'sche These, Turing-Maschinen, math. Logik).

Die Lösbarkeit des Wortproblems ist gleichbedeutend mit der Existenz einer Normalformfunktion, wie wir sie bereits bei der Konstruktion der freien Gruppe kennengelernt haben.

Das Isomorphieproblem ist wohl das schwierigste der drei Probleme. Schon die Frage nach der Ordnung einer endlich präsentierten Gruppe, ja selbst die Frage, ob eine solche Gruppe

trivial, endlich oder unendlich ist, ist nicht so leicht zu beantworten. Von Nutzen kann dabei die Untersuchung abelscher Gruppen sein.

b. Freie abelsche Gruppen, freie Produkte

Ist G eine Gruppe, so bezeichne $G' = [G,G]$ die *Kommutatorgruppe* und $G^{\mathrm{ab}} = G/G'$ die *Faktorkommutatorgruppe.* Aus der universellen Eigenschaft der freien Gruppe folgert man sofort, daß $F(A)^{\mathrm{ab}}$ die freie abelsche Gruppe über A ist, d. h. daß die folgende universelle Eigenschaft erfüllt ist:

Ist $\varphi\colon A \to H$ eine Abbildung von A in eine abelsche Gruppe H, so existiert zunächst gemäß Definition (5.1) eine Fortsetzung zu einem Homomorphismus $\widetilde{\varphi}\colon F(A) \to H$. Dieser faktorisiert dann über einen Homomorphismus $\widehat{\varphi}\colon F(A)^{\mathrm{ab}} \to H$, da H abelsch ist. $\widehat{\varphi}$ ist dabei eindeutig bestimmt durch $\widehat{\varphi}(\bar{a}) = \varphi(a)$ für $a \in A$.

Nun hat aber die direkte Summe

$$\bigoplus_{a\in A} \mathbb{Z} = \{(n_a)_{a\in A} \mid n_a \in \mathbb{Z}\,,\ n_a = 0 \text{ für fast alle } a \in A\}$$

ebenfalls diese universelle Eigenschaft, denn eine Abbildung $\varphi : A \to H$ läßt sich bei *abelschem* H fortsetzen zu einem Homomorphismus

$$\hat{\varphi} : \bigoplus_{a\in A} \mathbb{Z}a \to H\,, \quad \hat{\varphi}((n_a)_{a\in A}) = \sum_{a\in A} n_a\varphi(a)$$

und diese Fortsetzung ist eindeutig. Da universelle Objekte eindeutig sind (vgl. Beweis von (5.2),a)), erhalten wir so die freie abelsche Gruppe

$$F(A)^{\mathrm{ab}} \simeq \bigoplus_{a\in A} \mathbb{Z}\,.$$

Bei endlichem A der Mächtigkeit n erhalten wir $\mathbb{Z}^n$ als freie abelsche Gruppe über A (wobei die $a \in A$ auf die kanonischen Basisvektoren abgebildet werden).

Wir studieren nun präsentierte Gruppen G und deren Faktorkommutatorgruppen $G^{\mathrm{ab}} = G/[G,G]$.

(6.7) Satz: *Sei $G = \langle A \mid \mathcal{R}\rangle$ eine präsentierte Gruppe. Dann gilt:*

a) $G^{\mathrm{ab}} = \langle A \mid \mathcal{R} \cup \mathcal{C}\rangle$ *mit* $\mathcal{C} = \{a^{-1}b^{-1}ab \mid a,b \in A\}$.

b) $G^{\mathrm{ab}} \simeq \bigoplus_{a\in A} \mathbb{Z}a \,/\, \langle \sum_{a\in A} m_{ra}a \mid r \in \mathcal{R}\rangle$,

mit der Exponentensumme m_{ra} des Erzeugenden a in der Relation $r \in F(A)$:

$m_{ra} =$ *Häufigkeit von a im Wort r − Häufigkeit von a^{-1} in r.*

c) Ist $A = \{a_1,\dots,a_n\}$ n-elementig, so lassen sich die Strukturkonstanten der endlich erzeugten abelschen Gruppe G^{ab} aus der Exponentensummenmatrix $M = (m_{ra})_{r\in\mathcal{R},a\in A}$ explizit ablesen:

$$G^{\mathrm{ab}} \simeq \mathbb{Z}^{n-d} \oplus \mathbb{Z}/\alpha_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/\alpha_d\mathbb{Z}$$

mit dem Rang d der Matrix M und den natürlichen Zahlen $\alpha_i \neq 0$ $(i = 1,\dots,d)$ definiert durch

$$\alpha_1 \cdot \ldots \cdot \alpha_i \text{ ist der ggT aller } i\text{-reihigen Unterdeterminanten von } M\,.$$

Beweis: a) Die Gruppe $H := \langle A \mid \mathcal{R} \cup \mathcal{C}\rangle$ ist epimorphes Bild von G, und da sie offenbar abelsch ist, gibt es einen Epimorphismus $\psi\colon G^{\mathrm{ab}} \to H$. Umgekehrt ist nach Proposition (6.4) G^{ab} epimorphes Bild von H. Die beiden Epimorphismen sind zueinander invers, da dies auf den Erzeugenden $a \in A$ gilt.

b) Gemäß a) gilt

$$G^{\mathrm{ab}} \simeq F(A)/\langle\langle \mathcal{R} \cup \mathcal{C} \rangle\rangle \simeq F(A)^{\mathrm{ab}}/\langle r^{\mathrm{ab}} \mid r \in \mathcal{R}\rangle$$

mit den Restklassen $r^{\mathrm{ab}} \in F(A)^{\mathrm{ab}}$ der Relationen $r \in \mathcal{R}$. Ist $r = \prod_{i=1}^{s} b_i = \prod_{i=1}^{t} a_i^{\nu_i} \in \mathcal{R}$, so gilt in der *abelschen* Gruppe $F(A)^{\mathrm{ab}}$ (bei additiver Schreibweise)

$$r^{\mathrm{ab}} = \sum_{i=1}^{s} \nu_i a_i = \sum_{a \in A} m_{ra} a$$

mit den oben definierten Exponentensummen $m_{ra} = \sum\limits_{a_i = a} \nu_i$. (Wegen der Injektivität der Abbildung $A \to F(A) \to F(A)^{\mathrm{ab}} \simeq \oplus_{a \in A} \mathbb{Z}$ identifizieren wir A mit den Erzeugenden dieser Gruppen.]

c) Wir führen für ganzzahlige Matrizen A vorübergehend die folgende Bezeichnung ein:

$$\mathrm{ggT}_i(A) := \text{ggT aller } i\text{-reihigen quadratischen Unterdeterminanten von } A\,.$$

Hat A den Rang d, so gibt es zu jedem $i \leq d$ eine i-reihige Unterdeterminante $\neq 0$, also gilt $\mathrm{ggT}_i(A) \neq 0 \iff i \leq \mathrm{rg}(A)$. Aufgrund des Laplace'schen Entwicklungssatzes ist jede i-reihige Unterdeterminante eine Linearkombination von $i-1$-reihigen Unterdeterminanten, so daß

$$\mathrm{ggT}_{i-1}(A) \mid \mathrm{ggT}_i(A)$$

gilt. Ist also $\mathrm{ggT}_i(M) = \alpha_1 \cdot \ldots \cdot \alpha_i$ gezeigt, so sind die α_i als sukzessive Quotienten der $\mathrm{ggT}_i(M)$ für $i \leq d = \mathrm{rg}(M)$ wohldefinierte natürliche Zahlen.

Nun zum Beweis von c): Es ist $F(A)^{\mathrm{ab}} \simeq \mathbb{Z}^n$ der freie $\mathbb{Z}$-Modul vom Rang n und der Untermodul

$$\langle \sum_{i=1}^{n} m_{r,a_i} a_i \mid r \in \mathcal{R} \rangle \simeq \langle (m_{r,a_1}, \ldots, m_{r,a_n}) \in \mathbb{Z}^n \mid r \in \mathcal{R}\rangle =: \mathcal{M}$$

wird erzeugt von den Zeilen der Matrix M. Nach dem Elementarteilersatz gibt es eine $\mathbb{Z}$-Basis $u_1, \ldots, u_n$ von $\mathbb{Z}^n$, $d \in \mathbb{N}$ und natürliche Zahlen $\alpha_1, \ldots, \alpha_d$, die sich sukzessive teilen, so daß $\alpha_1 u_1, \ldots, \alpha_d u_d$ eine $\mathbb{Z}$-Basis von $\mathcal{M} \leq \mathbb{Z}^n$ ist. Damit gilt

$$G^{\mathrm{ab}} \;\simeq\; \mathbb{Z}^n/\mathcal{M} \;\simeq\; \bigoplus_{i=1}^{n} \mathbb{Z}u_i \,/\, \bigoplus_{i=1}^{d} \mathbb{Z}\alpha_i u_i \;\simeq\; \bigoplus_{i=1}^{d} \mathbb{Z}/\alpha_i\mathbb{Z} \;\oplus\; \mathbb{Z}^{n-d}\,.$$

Dabei ist d offenbar der Rang von M. Man beachte jedoch, daß $\alpha_i = 1$ sein kann, so daß der entsprechende direkte Summand $\mathbb{Z}/\alpha_i\mathbb{Z} = \{0\}$ ist.

Nun zur Bestimmung der $\mathrm{ggT}_i(M)$ $(1 \leq i \leq d)$. Wir benutzen den Determinantenproduktsatz (in allgemeiner Form für nicht notwendig quadratische Faktoren $A \in M_{nm}$, $B \in M_{mn}$):

$$\det AB = \det\left((a_{ij})_{nm} \cdot (b_{jk})_{mn}\right) = \sum_{1 \leq j_1 < \ldots < j_n \leq m} \det(a_{i,j_\nu}) \cdot \det(b_{j_\nu,k})\,.$$

Ist $m < n$, so ist die Summe offensichtlich leer und es ergibt sich notwendig $\det AB = 0$; im Falle $m = n$ reduziert sich die Summe auf einen Summanden und man erhält den üblichen Determinantenproduktsatz $\det AB = \det A \cdot \det B$; im Fall $m > n$ summiert man über alle quadratischen n-reihigen Untermatrizen und multipliziert die entsprechenden Unterdeterminanten.
Der Vollständigkeit halber hier der Beweis: Es seien $z_j = (b_{jk})_k$ $(j = 1, \ldots, m)$ die Zeilen von

B. Da die Determinante alternierend und multilinear in den Zeilen ist, erhält man

$$\begin{aligned}\det(AB) &= \det\big(\sum_{j=1}^{m} a_{ij}z_j\big)_{1\le i\le n} = \sum_{j_1=1}^{m}\dots\sum_{j_n=1}^{m} a_{1j_1}\cdot\ldots\cdot a_{nj_n}\det(z_{j_\nu})\\ &= \sum_{1\le j_1<\ldots<j_n\le m}\ \sum_{\sigma\in S_n}\prod_{i=1}^{n} a_{ij_{\sigma(i)}}\cdot\det(z_{j_{\sigma(\nu)}})\\ &= \sum_{1\le j_1<\ldots<j_n\le m}\ \sum_{\sigma\in S_n}\prod_{i=1}^{n} a_{ij_{\sigma(i)}}\cdot\operatorname{sign}(\sigma)\det(z_{j_\nu})\\ &= \sum_{1\le j_1<\ldots<j_n\le m}\det(a_{ij_\nu})\det(b_{j_\nu k})\end{aligned}$$

Wendet man dies auf eine i-reihige Unterdeterminante von AB an, so erhält man für ganzzahlige Matrizen A, B:

$$\mathrm{ggT}_i(A)\mid\mathrm{ggT}_i(AB)\quad\text{und}\quad\mathrm{ggT}_i(B)\mid\mathrm{ggT}_i(AB)\,.$$

Weiter mit dem Beweis von c): Wir gehen von einer endlichen Zeilenzahl m von M aus (die Argumentation gilt aber auch allgemein). Es sei U_{nn} die Matrix mit der $\mathbb{Z}$-Basis u_i als Zeilen und

$$D_{dn} = \begin{pmatrix}\alpha_1 & \cdots & 0 & \cdots & 0\\ & \ddots & & & \vdots\\ 0 & \cdots & \alpha_d & \cdots & 0\end{pmatrix}.$$

Dann sind $\alpha_i u_i$ $(i=1,\dots d)$ die Zeilen von $D_{dn}U_{nn}$. Da die Zeilen von M aus den $\alpha_i u_i$ $\mathbb{Z}$-linear kombinierbar sind, gibt es eine ganzzahlige Matrix C mit $M_{mn} = C_{md}\cdot D_{dn}\cdot U_{nn}$. Nach obiger Vorüberlegung ist daher $\mathrm{ggT}_i(M)$ Vielfaches von $\mathrm{ggT}_i(D)$.

Umgekehrt schließt man genauso: Die $\alpha_i u_i$ sind Linearkombinationen der Zeilen von M, so daß eine ganzzahlige Matrix $\tilde{C}$ existiert mit $D_{dn}\cdot U_{nn} = \tilde{C}_{dm}\cdot M_{mn}$. Da die Zeilen von U_{nn} eine $\mathbb{Z}$-Basis des $\mathbb{Z}^n$ bilden, ist U *ganzzahlig* invertierbar, also $D_{dn} = \tilde{C}_{dm}\cdot M_{mn}\cdot\tilde{U}_{nn}$ mit einer *ganzzahligen* Matrix $\tilde{U}$. Wie oben folgt nun, daß $\mathrm{ggT}_i(D)$ ein Vielfaches von $\mathrm{ggT}_i(M)$ ist. Insgesamt ergibt sich die Behauptung $\mathrm{ggT}_i(D) = \mathrm{ggT}_i(M)$.

Nun ist $\mathrm{ggT}_i(D)$ der ggT aller i-fachen Produkte der α_ν. Wegen der Teilbarkeitsbeziehung $\alpha_i \mid \alpha_{i+1}$ heißt das $\mathrm{ggT}_i(D) = \alpha_1\cdot\ldots\cdot\alpha_i$, so daß die Behauptung von c) folgt:

$$\alpha_1\cdot\ldots\cdot\alpha_i = \mathrm{ggT}_i(D) = \mathrm{ggT}_i(M)\,.$$

Als unmittelbare, aber wichtige Folgerung aus Satz (6.7) halten wir fest

(6.8) Korollar:

a) *Eine endliche Gruppe hat in jeder endlichen Präsentierung mindestens soviele Relationen wie Erzeugende.*

b) *Ist $G = \langle a_1,\dots,a_n \mid r_1,\dots,r_n\rangle$ endlich präsentiert mit genausoviel Relationen wie Erzeugenden und M die n-reihige quadratische Exponentensummenmatrix, so gilt:*

$$\#G^{\mathrm{ab}} = \begin{cases}\infty & \textit{falls } \det M = 0,\\ |\det M| & \textit{sonst.}\end{cases}$$

Beweis: a) folgt unmittelbar aus Satz (6.7),c): Hat eine Gruppe weniger Relationen als Erzeugende, so ist natürlich auch der Rang d kleiner als die Erzeugendenzahl und nach (6.7),c) ist G^{ab} unendlich.

b) Wir können $d = n$ annehmen. Nach dem Beweis von (6.7),c) ist G^{ab} von der Ordnung $\alpha_1\dots\alpha_n$, und dies ist nach c) $\mathrm{ggT}_n(M) = |\det(M)|$. (Der ggT ist per definitionem eine natürliche Zahl.)

Beispiele: 1) $G = \langle a, b \mid a^2, b^4, b^a = b^{-1} \rangle$
Dies ist die schon früher besprochene Präsentierung der Diedergruppe[1)]. Die Exponentensummenmatrix dieser Präsentierung ist

$$M = \begin{pmatrix} 2 & 0 \\ 0 & 4 \\ 0 & 2 \end{pmatrix}.$$

Hieraus liest man sofort die in Satz (6.7) benötigten Invarianten ab:
$d = 2,\ \alpha_1\alpha_2 = \mathrm{ggT}(8, 4, 0) = 4,\ \alpha_1 = \mathrm{ggT}(0, 2, 4) = 2$, und erhält

$$G^{\mathrm{ab}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

2) $G = \langle x, y \mid x^5, y^3, (xy)^2 \rangle$
Wieder liest man ab

$$M = \begin{pmatrix} 5 & 0 \\ 0 & 3 \\ 2 & 2 \end{pmatrix}.$$

Offenbar ist der Rang $d = 2$, und damit G^{ab} endlich. Weiter ist $\alpha_1\alpha_2 = \mathrm{ggT}(15, 10, -6)$, also $\alpha_1\alpha_2 = 1$, so daß $\#G^{\mathrm{ab}} = 1$ ist. Dies bedeutet, die Gruppe G ist perfekt, d.h. $G = G' = [G, G]$. Insbesondere ist G nicht auflösbar. (In der Tat ist $G = A_5$ die alternierende Gruppe vom Grad 5.)

Wir wollen noch ein weiteres freies Objekt kennenlernen, das sich aus der freien Gruppe ableitet, die *freien Produkte* von Gruppen. Heuristische Intention ist dabei, zwei Gruppen zu einer Gruppe 'zusammenzusetzen', in der neben den Rechenregeln der Einzelfaktoren keine weiteren Beziehungen gelten. Dies wird realisiert durch folgende

(6.9) Definition: Seien G_1, G_2 Gruppen. Dann definiert man das *freie Produkt* von G_1 und G_2 durch

$$G_1 * G_2 = \langle A_1 \dot\cup A_2 \mid \mathcal{R}_1 \cup \mathcal{R}_2 \rangle$$

für beliebige Präsentierungen $G_i = \langle A_i \mid \mathcal{R}_i \rangle$ der gegebenen Gruppen (mit $A_1 \cap A_2 = \emptyset$).

Diese erfüllen die folgende universelle Eigenschaft, so daß das freie Produkt unabhängig von den gewählten Präsentierungen eindeutig durch die Gruppen G_i bestimmt ist.

(6.10) Satz: *a) Für jedes Paar φ_i $(i = 1, 2)$ von Gruppenhomomorphismen $\varphi_i \colon G_i \to H$ in eine Gruppe H gibt es genau einen Gruppenhomomorphismus $\varphi \colon G_1 * G_2 \to H$ mit $\varphi|_{G_i} = \varphi_i$ für $i = 1, 2$. Grob gesprochen: Man kann jedes Paar von Gruppenhomomorphismen $\varphi_i \colon G_i \to H$ 'zusammensetzen' zu einem Homomorphismus auf $G_1 * G_2$, und dieser ist eindeutig.*
b) Das freie Produkt $G_1 * G_2$ ist unabhängig von den Präsentierungen von G_1, G_2 bis auf Isomorphie eindeutig bestimmt.

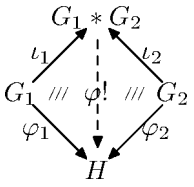
Beweis: Zur Rechtfertigung der Formulierungen zunächst eine Vorüberlegung. Wegen der Symmetrie betrachten wir nur $i = 1$. Die definierenden Relationen $\mathcal{R}_1$ von G_1 sind per definitionem auch in $G_1 * G_2$ erfüllt, so dass sich die Einbettung $A_1 \hookrightarrow A_1 \subset G_1 * G_2$ gemäß Prop. (6.4) zu einem Homomorphismus $\iota_1 : G_1 \to G_1 * G_2$ fortsetzt.

Umgekehrt läßt sich die Abbildung $\pi_1 : A_1 \dot\cup A_2 \to G_1$ mit $\pi_1(a) = a$ für $a \in A_1$ und $\pi_1(a) = e_{G_1}$ für $a \in A_2$ zu einem Homomorphismus $\pi_1 : G_1 * G_2 \to G_1$ fortsetzen, denn in G_1 sind die Relationen aus $\mathcal{R}_1$, die ja nur A_1 betreffen, erfüllt, während die Relationen aus $\mathcal{R}_2$ in G_1 trivialerweise erfüllt sind, wenn für $a \in A_2$ immer nur das neutrale Element e_{G_1} eingesetzt wird.

Man erkennt sofort $\pi_1 \circ \iota_1 = \mathrm{id}_{G_1}$, so daß ι_1 injektiv und π_1 surjektiv ist. Damit sind die Gruppen G_i (bis auf Isomorphie) im freien Produkt enthalten. Dies rechtfertigt die Formulierung von a).

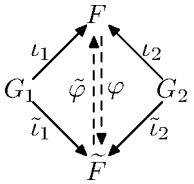
[1)] Dabei haben wir hier die Notation gelockert und die Relation $ba^{-1}ba \in F(A)$ suggestiv als die in G gültige Gleichheit $ba^{-1}ba = 1$ bzw. $b^a = b^{-1}$ notiert.

ad a): Man definiert zunächst φ auf $A_1 \dot\cup A_2$ durch $\varphi|_{A_i} = \varphi_i|_{A_i}$. Die Bilder von φ in H erfüllen dann die Relationen in $\mathcal{R}_1 \cup \mathcal{R}_2$, da diese jeweils nur die Erzeugenden in einem A_i betreffen und φ_i ein Homomorphismus auf $G_i = \langle A_i \mid \mathcal{R}_i\rangle$ ist. Damit induziert φ gemäß Proposition (6.4) einen Gruppenhomomorphismus $\varphi\colon G_1 * G_2 \to H$ mit den gewünschten Eigenschaften $\varphi \circ \iota_i = \varphi_i$, durch die er offenbar auch eindeutig bestimmt ist.



ad b): Aus dieser universellen Eigenschaft a) des direkten Produktes ergibt sich wie allgemein bei universellen Objekten die Eindeutigkeit bis auf Isomorphie (siehe etwa die Überlegungen in (5.2) zur Eindeutigkeit der freien Gruppe):

Sei $F = G_1 * G_2$ wie oben und jetzt $\tilde F = G_1 \tilde * G_2$ ein weiteres freies Produkt. Seien $\iota_i : G_i \to F$ wie oben und $\tilde\iota_i : G_i \to \tilde F$ die entsprechenden Einbettungen für $\tilde F$. Wir wenden nun a) an auf $H = \tilde F$ und $\varphi_i = \tilde\iota_i : G_i \to \tilde F$ und erhalten einen eindeutig bestimmten Homomorphismus $\varphi : F \to \tilde F$ mit $\tilde\iota_i = \varphi \circ \iota_i$ $(i = 1, 2)$. Genauso folgt aus a) die Existenz eines Homomorphismus $\tilde\varphi : \tilde F \to F$ mit $\iota_i = \tilde\varphi \circ \tilde\iota_i$. Hieraus folgt für die Verkettung



$$(\tilde\varphi \circ \varphi) \circ \iota_i = \tilde\varphi \circ \tilde\iota_i = \iota_i = \mathrm{id}_F \circ \iota_i \quad (i = 1, 2). \qquad (*)$$

Wendet man die Eindeutigkeitsaussage von a) auf F und $H = F$ mit $\varphi_i = \iota_i$ an, so folgt aus $(*)$ $\tilde\varphi \circ \varphi = \mathrm{id}_F$. Aus Symmetriegründen erhält man auch die umgekehrte Beziehung $\varphi \circ \tilde\varphi = \mathrm{id}_{\tilde F}$. Damit sind φ und $\tilde\varphi$ zueinander inverse Isomorphismen zwischen F und $\tilde F$. □

Das einfachste Beispiel sind freie Produkte zyklischer Gruppen C_n,C_m der Ordnung $n, m \in \mathbb{N}_+$. Diese sind für $n, m \geq 2$ unendlich; genauer gilt der folgende

(6.11) Satz: *Seien $n, m \in \mathbb{N}_+$ und $C_n = \langle x\rangle$, $C_m = \langle y\rangle$. Die Elemente von $C_n * C_m$ sind eindeutig darstellbar als Potenzprodukte von x und y, wobei sich die Basen x, y ständig abwechseln:*

$$y^\beta \cdot \prod_{i=1}^{s} x^{\nu_i} y^{\mu_i} \cdot x^\alpha \quad \textit{mit} \quad s \in \mathbb{N}\,,\ 0 < \nu_i < n\,,\ 0 < \mu_i < m\,,\ 0 \leq \alpha < n\,,\ 0 \leq \beta < m\,.$$

Der *Beweis* verläuft analog wie der Beweis von Satz (5.3): Man definiert in naheliegender Weise einen 'Reduktionsprozeß', der jedes Wort in endlich vielen Schritten in obige Normalform überführt und dabei die Interpretation in $C_n * C_m$ nicht ändert. Schließlich muß man zeigen, daß ein Wort in Normalform nur dann eine Relation in $\langle\langle x^n, y^m\rangle\rangle$ sein kann, wenn es leer ist. Um dies analog wie bei (5.3) beweisen zu können, gibt man zunächst eine ähnlich konstruktive Beschreibung der Kongruenzrelation modulo $\langle\langle x^n, y^m\rangle\rangle$. Dabei ist hier der Grundbaustein die Relation $(\sigma, \tau \in F = F(x, y))$

$$\sigma \prec \tau :\Longleftrightarrow \bigvee_{\rho_1, \rho_2 \in F, r \in \{x^n, y^m\}} \sigma = \rho_1\rho_2\,,\ \tau = \rho_1 r \rho_2.$$

Es sei noch angemerkt, daß Satz (6.11) bei entsprechender Modifizierung auch gilt, wenn eine der zyklischen Gruppen unendlich ist.

Beispiele: 1) *Das freie Produkt der zyklischen Gruppe C_2 mit sich*

$$C_2 * C_2 = \langle x, y \mid x^2, y^2\rangle$$

ist isomorph zur affinen Gruppe $\mathrm{Aff}(1, \mathbb{Z}) = \{ax + b \mid b \in \mathbb{Z}, a \in \mathbb{Z}^\times\}$.

Zunächst kann man das freie Produkt $C_2 * C_2$ als unendliche Diedergruppe

$$\langle u, v \mid u^2, v^u = v^{-1}\rangle$$

beschreiben mit $u := x$ und $v := xy$. Nach Satz (6.11) hat v unendliche Ordnung und alle Elemente besitzen eine eindeutige Normalformdarstellung der Gestalt $u^m v^n$ mit $m, n \in \mathbb{Z}, 0 \leq m \leq 1$. Die genannte affine Gruppe wird erzeugt von der Translation $v = x + 1$ und von

$u = -x$ ($x = \mathrm{id}_{\mathbb{Z}}$). Diese Erzeugenden erfüllen die definierenden Relationen der unendlichen Diedergruppe. Außerdem ist ein beliebiges Element

$$(-x)^m \circ (x+1)^n = (-1)^m x + (-1)^m n \in \mathrm{Aff}(1,\mathbb{Z}),\ 0 \le m \le 1, m, n \in \mathbb{Z}$$

nur dann gleich x, wenn $m = n = 0$ ist. Dies zeigt, daß die affine Gruppe als unendliche Diedergruppe präsentiert werden kann.
2) Man kann zeigen, daß das freie Produkt $C_2 * C_3$ isomorph ist zur Modulgruppe $\mathrm{PSL}_2(\mathbb{Z})$ aller gebrochen linearen Transformationen der oberen Halbebene

$$\frac{az+b}{cz+d} \ \text{ mit } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Die entsprechenden Erzeugenden der Ordnung 2 und 3 sind die Transformationen $S = -\frac{1}{z}$ und $U = ST = -\frac{1}{z+1}$ mit dem Element unendlicher Ordnung $T = SU = z + 1$, der Translation um 1.
3) Man kann freie Produkte benutzen, um für gewisse Präsentierungen nachzuweisen, daß sie unendliche Gruppen darstellen, nämlich:

(6.12) Bemerkung: Sei $G = \langle A \mid \mathcal{R} \rangle$ eine präsentierte Gruppe. Wir stellen die Relationen $r \in \mathcal{R}$ als Potenzprodukte

$$r = \prod_{i=1}^{s} a_i^{\nu_i(r)}$$

dar mit $\nu_i(r) \in \mathbb{Z} \setminus \{0\}$, $a_i \in A$ und $a_i \neq a_{i+1}$. Wir definieren dann für $a \in A$ den 'Exponenten-ggT' als

$$G(a) := \mathrm{ggT}\{\nu_i(r) \mid a_i = a, r \in \mathcal{R}\}.$$

Ist dieser für zwei verschiedene Erzeugende $a \neq b \in A$ ungleich 1, so ist G unendlich.

Der *Beweis* beruht einfach darauf, daß dann nach Proposition (6.4) das freie Produkt $C_n * C_m = \langle x \rangle * \langle y \rangle$ mit $n = G(a), m = G(b)$ ($C_0 = C_\infty = \mathbb{Z}$ gesetzt) Quotient von G ist: Die Elemente $\widetilde{a} = x, \widetilde{b} = y$ und $\widetilde{c} = 1$ für $c \in A \setminus \{a, b\}$ erzeugen $C_n * C_m$ und erfüllen die definierenden Relationen $r \in \mathcal{R}$ von G.

c. Automorphismen, Erweiterungen

In diesem Abschnitt wollen wir eine Reihe von Beispielgruppen durch Präsentierungen definieren. Dazu werden wir zuerst für spezielle Gruppenerweiterungen (siehe[2)] EGI, §3) Präsentierungen konstruieren. Zuvor jedoch eine kurze Bemerkung über Automorphismen präsentierter Gruppen:

(6.13) Bemerkung: Sei $G = \langle A \mid \mathcal{R} \rangle$ eine präsentierte Gruppe. Weiter seien $\hat{a} \in G$ ($a \in A$) andere Erzeugende von G. Dann sind äquivalent:

i) Die Zuordnung $a \mapsto \hat{a}$ induziert einen Automorphismus von G.

ii) Die Elemente $\hat{a} \in G$ ($a \in A$) erfüllen dieselben Relationen wie die Erzeugenden $a \in A$:

$$\bigwedge_{w \in H(B)} w(\hat{a}) = 1 \iff w(a) = 1\,.$$

Der *Beweis* ergibt sich unmittelbar aus Proposition (6.4).

Diese äquivalenten Bedingungen sind insbesondere erfüllt, wenn die $\hat{a}$ eine Permutation der Erzeugenden $a \in A$ bildet, unter der die Relationen invariant bleiben:

Beispiele: 1) $V_4 = \langle a, b \mid a^2, b^2, ab = ba \rangle$
Dieser Präsentierung der Klein'schen Vierergruppe sieht man sofort an, daß die Vertauschung der Erzeugenden die Relationen invariant läßt, also erhält man einen Automorphismus φ der

[2)] Verweise auf Teil I dieser Vorlesung werden mit EGI gekennzeichnet.

Ordnung 2, charakterisiert durch $a \mapsto b \mapsto a$. Wegen der Kommutativität der V_4 kann dies kein innerer Automorphismus sein. Formt man diese Präsentierung durch Einführung einer zusätzlichen Erzeugenden $c = ab$ um zu

$$V_4 = \langle a, b, c \mid a^2, b^2, c^2, abc \rangle,$$

so erkennt man einen Automorphismus der Ordnung 3, gegeben durch die zyklische Vertauschung $a \mapsto b \mapsto c \mapsto a$ dieser Erzeugenden. Der erstgenannte Automorphismus beschreibt sich in dieser zweiten Präsentierung als Vertauschung der Erzeugenden a und b bei Fixierung von c; insgesamt hat man somit die volle symmetrische Gruppe der drei Erzeugenden a, b, c, als Untergruppe von $\mathrm{Aut}V_4$.

Zum Nachweis der zweiten Präsentierung setzt man $c = ab$ und verifiziert

$$c^2 = abab = a^2b^2 = 1 \quad \text{und} \quad abc = c^2 = 1.$$

Dann folgert man aus dem zweiten Relationensatz den ersten:

$$ab = c^{-1} = c = b^{-1}a^{-1} = ba,$$

und hat die Gleichwertigkeit beider Präsentierungen bewiesen.

2) Die Quaternionengruppe Q_8

Wir zeigen zunächst

$$\begin{aligned} Q_8 &\simeq \langle a, b \mid a^2 = b^2, b^4, b^a = b^{-1} \rangle \\ &= \langle a, b \mid a^2 = b^2, b^a = b^{-1} \rangle \\ &\simeq \langle a, b, c \mid ab = c, bc = a, ca = b \rangle . \end{aligned}$$

Ist dies gezeigt, so entnimmt man der letzten Präsentierung, daß die Quaternionengruppe Q_8 einen Automorphismus der Ordnung 3 hat, wiederum gegeben durch zyklische Vertauschung der Erzeugenden a, b, c der letzten Präsentierung.

Es gilt zunächst, daß Q_8 die Relationen der erstgenannten Präsentierung erfüllt (siehe EGI, Satz (3.12)). Außerdem überlegt man sich wie bei der Präsentierung der Diedergruppe, daß die Gruppe $\langle a, b \mid a^2 = b^2, b^4, b^a = b^{-1} \rangle$ eine Darstellung ihrer Elemente in der Normalform $a^i b^j$ mit $0 \leq i < 2, 0 \leq j < 4$ besitzt und daher höchstens die Ordnung 8 hat.

Die Relation $b^4 = 1$ der ersten Präsentierung ergibt sich aus den beiden übrigen wie folgt:

$$b^{-2} = (b^2)^a = (a^2)^a = a^2 = b^2.$$

Für die dritte Präsentierung setze man $c = ab$ und verifiziere die genannten Relationen (die Relationen der sog. *Fibonacci-Gruppe* $F(2, 3)$):

$$bc = bab = ab^a b = a \quad \text{und} \quad ca = aba = a^2 b^a = b.$$

Umgekehrt folgt natürlich auch aus den letztgenannten Relationen für a, b, c sofort

$$a^2 = bca = b^2 \quad \text{und} \quad b^a b = a^{-1}bab = a^{-1}bc = 1.$$

Die in den beiden Beispielen durchgeführten Umformungen von Präsentierungen sind sog. *Tietze-Transformationen,* die den Isomorphietyp nicht ändern:

T1) Hinzufügen einer ableitbaren Relation:

$$r \in F(A),\ r \text{ gilt in } \langle A \mid \mathcal{R} \rangle \Longrightarrow \langle A \mid \mathcal{R} \rangle = \langle A \mid \mathcal{R} \cup \{r\} \rangle.$$

T2) Hinzufügen eines neuen Erzeugenden und einer Definition dieses Elementes durch die übrigen als zusätzliche Relation:

$$w \in F(A),\ z \notin A \Longrightarrow \langle A \mid \mathcal{R} \rangle \simeq \langle A, z \mid \mathcal{R}, z = w \rangle.$$

Die Rechtfertigung für diese Isomorphieaussagen liefert Proposition (6.4).
Zu den Tietze-Transformationen zählt man üblicherweise auch die Inversen der obigen Umformungen, also als Inverses zu T1):

T3) Weglassen einer Relation r, die aus den *übrigen* ableitbar ist.

Eine zum inversen Prozeß zu T2) (unter Verwendung von T1)) äquivalente Regel ist:

T4) Weglassen einer Erzeugenden z und einer unter den Relationen vorkommenden Definition von z durch die übrigen Erzeugenden, sowie *Ersetzung aller Vorkommen von z in den verbleibenden Relationen durch die Definition.*

So einfach und offensichtlich diese Tietze-Transformationen auch sind, es gilt nun:

(6.14) Satz: *Zwei endliche Präsentierungen $\langle X|\mathcal{R}\rangle$ und $\langle Y|\mathcal{S}\rangle$ beschreiben genau dann dieselbe Gruppe G, wenn eine endliche Folge von Tietze-Transformationen existiert, die die beiden Präsentierungen ineinander überführt.*

Beweis: $\Rightarrow$: Tietze-Transformationen ändern den Isomorphietyp nicht:
T1) Gilt r in $\langle A \mid \mathcal{R}\rangle$, so ist $r \in \langle\langle\mathcal{R}\rangle\rangle$ und folglich $\langle\langle\mathcal{R}\cup\{r\}\rangle\rangle = \langle\langle\mathcal{R}\rangle\rangle$. Dies ergibt die behauptete Gleichheit.
T2) Aus der universellen Eigenschaft präsentierter Gruppen ergeben sich Epimorphismen zwischen den beiden Präsentierungen, die sich als invers zueinander erweisen: Seien

$$\begin{array}{lllllll} \varphi_1: & F(A) & \twoheadrightarrow G_1 := & \langle A \mid \mathcal{R}\rangle & = & F(A)/\langle\langle\mathcal{R}\rangle\rangle & \text{und} \\ \varphi_2: F(A \dot\cup \{z\}) & \twoheadrightarrow G_2 := & \langle A, z \mid \mathcal{R}, z = w\rangle & = & F(A \dot\cup \{z\})/\langle\langle\mathcal{R}\cup\{z^{-1}w\}\rangle\rangle & & \end{array}$$

die per Definition gegebenen natürlichen Epimorphismen der Präsentierungen.

Wegen $\varphi_2(z) = \varphi_2(w) \in \langle\varphi_2(A)\rangle$ erzeugt $\varphi_2(A)$ ganz G_2 und erfüllt alle Relationen von $\mathcal{R}$, ist also ein epimorphes Bild von G_1: $\psi_1 : G_1 \twoheadrightarrow G_2$ mit $\psi_1(\varphi_1(a)) = \varphi_2(a)$. Wegen der Homomorphie gilt $\psi_1(\varphi_1(w)) = \varphi_2(w) = \varphi_2(z) \in G_2$.

Umgekehrt wird G_1 von $\varphi_1(A)$ und $\varphi_1(w)$ erzeugt und alle Relationen von $\mathcal{R}$ sind natürlich erfüllt. Aber auch die Relation $z = w$ von G_2 ist in G_1 erfüllt, wenn man für z $\varphi_1(w) \in G_1$ einsetzt. Damit erhält man den umgekehrten Epimorphismus $\psi_2 : G_2 \twoheadrightarrow G_1$ mit $\psi_2(\varphi_2(a)) = \varphi_1(a)$ und $\psi_2(\varphi_2(z)) = \varphi_1(w)$. Offenbar sind ψ_1 und ψ_2 invers zueinander.

Nun zur Umkehrung $\Leftarrow$ von (6.14). Es sei

$$G = \langle X \mid \mathcal{R}\rangle = \langle Y \mid \mathcal{S}\rangle.$$

Dann besitzen die Erzeugenden $y \in Y \subset G$ reduzierte Wortdarstellungen $w_y \in H(X \dot\cup X')$ bzgl. des Erzeugendensystems X; entsprechend seien umgekehrt $w_x \in H(Y \dot\cup Y')$ für $x \in X$ definiert. Dann erreicht man durch Tietze-Transformationen

$$\begin{aligned} \langle X \mid \mathcal{R}\rangle &\simeq \langle X \dot\cup Y \mid \mathcal{R},\ y = w_y\ (y \in Y)\rangle && (T2) \\ &= \langle X \dot\cup Y \mid \mathcal{R},\ y = w_y\ (y \in Y), \mathcal{S}, x = w_x\ (x \in X)\rangle. && (T1) \end{aligned}$$

Wegen der Symmetrie der letzten Präsentierung in X, Y und $\mathcal{R}, \mathcal{S}$ ist Satz (6.14) bewiesen. □

Wir wollen nun Präsentierungen von Gruppenerweiterungen untersuchen.

(6.15) Satz: *Es sei $G = \langle A \mid \mathcal{R}\rangle$ eine endlich präsentierte Gruppe und $C_d = \langle\sigma\rangle$ die zyklische Gruppe der Ordnung $d \in \mathbb{N}$. Für eine Gruppenerweiterung $G \hookrightarrow \hat G \twoheadrightarrow C_d$ von G mit C_d sei (siehe EGI §3) $\varphi = \alpha_\sigma$ der von σ auf G induzierte Automorphismus, $u_\sigma \in \hat G$ ein Repräsentant von $\sigma \in C_d$, $w_{\varphi(a)}$ die reduzierte Wortdarstellung für $\varphi(a) \in G$ $(a \in A)$ und w_ρ die von $\rho = u_\sigma^d \in G$.*

a) *Dann erhalten wir die folgende Präsentierung von* $\hat{G}$

$$\hat{G} = \langle A, x \mid \mathcal{R}\,,\ x^{-1}ax = w_{\varphi(a)}\,(a \in A)\,,\ x^d = w_\rho\,\rangle,$$

wobei $x \in \hat{G}$ *auf* $\sigma \in C_d$ *abgebildet wird.*

b) *Ist* φ *ein Automorphismus von* G *mit* $\varphi^d = \mathrm{id}_G$ *und* ρ *ein Element in* G*, das im Zentrum liegt und unter* φ *invariant ist, so beschreibt die Präsentierung aus a) eine Gruppenerweiterung* $G \hookrightarrow \hat{G} \twoheadrightarrow C_d$ *von* G *mit* C_d*, bei der* x *ein Urbild von* σ *ist.*

Beweis: a) Offenbar enthält die durch die Präsentierung gegebene Gruppe G^* die Gruppe G als Normalteiler. Der natürliche Epimorphismus $G^* \to G^*/G$ bildet x auf ein Element höchstens der Ordnung d ab, also hat die präsentierte Gruppe höchstens die Ordnung $\#G \cdot d$. Da nach Ansatz $\hat{G}$ die Relationen der Präsentierung erfüllt, ist $\hat{G}$ Quotient von G^*. Da $\hat{G}$ keine kleinere Ordnung als G^* hat, folgt die Behauptung.

Ad b): Hierfür genügt es, unter den gegebenen Voraussetzungen eine Gruppenerweiterung $\hat{G}$ von G mit C_d zu konstruieren, die die gegebenen definierenden Relationen erfüllt. Diese Gruppenerweiterung konstruieren wir gemäß EGI, Satz (3.3) aus dem Automorphismensystem

$$\alpha\colon C_d \to \mathrm{Aut}\,G\,,\ \sigma^i \mapsto \varphi^i$$

und dem α-Faktorensystem

$$f\colon C_d \times C_d \to G\,,\ (\sigma^i, \sigma^j) \mapsto \begin{cases} 1 & \text{für } 0 \le i, j < d,\ i + j < d, \\ \rho & \text{für } 0 \le i, j < d,\ i + j \ge d. \end{cases}$$

Die Normierungsbedingung (N): $f(1, \sigma^j) = f(\sigma^i, 1) = 1$, $\alpha_1 = \mathrm{id}$ ist nach Definition erfüllt. Da ρ und damit alle Werte von f im Zentrum von G liegen, fordert Bedingung (A) aus EGI Satz (3.1) daß α ein Homomorphismus ist. Wegen $\varphi^d = 1$ ist dies offenbar der Fall.

Da ρ und damit alle Werte von f unter φ invariant bleiben, nimmt die Bedingung (F) die Form

$$f(\sigma^{i+j}, \sigma^k) f(\sigma^i, \sigma^j) = f(\sigma^i, \sigma^{j+k}) f(\sigma^j, \sigma^k)$$

an. Nach Definition ist f symmetrisch, so daß beide Seiten bis auf eine Vertauschung der Indizes übereinstimmen. Es genügt also zu zeigen, daß die linke Seite *symmetrisch* in den Indizes ist. Wir berechnen nun

$$f(\sigma^{i+j}, \sigma^k) f(\sigma^i, \sigma^j) = \begin{cases} \rho \cdot \rho & \text{für } 2d \le i + j + k, \\ 1 \cdot 1 & \text{für } 0 \le i + j + k < d, \\ \rho & \text{sonst.} \end{cases}$$

Offenbar ist dies symmetrisch in i, j, k und die behauptete Gleichheit folgt.

Von der so konstruierten Gruppenerweiterung $\hat{G}$ führt der in a) beschriebene Prozeß zu der gegebenen Präsentierung: Zunächst gilt nach Wahl von α

$$\alpha_\sigma(a) = \varphi(a) \quad \text{für } a \in A\,,$$

und nach Wahl von f erhält man induktiv

$$u_\sigma^j = u_{\sigma^j} \text{ für } j < d \quad \text{und} \quad u_\sigma^d = u_{\sigma^d}\rho = \rho.$$

(6.16) Korollar: *Sei* $G = \langle A|\mathcal{R}\rangle$ *eine endliche abelsche Gruppe und* $d \in \mathbb{N}_+$ *eine natürliche Zahl. Dann sind sämtliche Gruppenerweiterungen* $\hat{G}$ *von* G *mit* C_d *gegeben durch*

$$\hat{G} = \langle A, x|\mathcal{R}\,,\ a^x = w_{\varphi(a)}(a \in A)\,,\ x^d = w_\rho\rangle$$

mit $\varphi \in \mathrm{Aut}(G)\,,\ \varphi^d = 1\,,\ \rho \in G\,,\ \varphi(\rho) = \rho$*. Der Epimorphismus* $\hat{G} \to C_d$ *mit Kern* G *ist dabei durch* $A \mapsto 1\,,\ x \mapsto \sigma$ *gegeben. Die semidirekten Produkte darunter sind die Gruppenerweiterungen mit* $\rho = 1$*.*

Beweis: Nach Satz (6.15),a) hat jede derartige Gruppenerweiterung eine solche Präsentierung mit $\varphi = \alpha_\sigma = (...)^{u_\sigma}$ und $\rho = u_\sigma^d$. Dann gilt

$$\varphi(\rho) = (u_\sigma^d)^{u_\sigma} = u_\sigma^d = \rho$$

und

$$\varphi^d = (...)^{u_\sigma^d} = (...)^\rho = \mathrm{id}_G,$$

da G abelsch ist.

Umgekehrt liefert jede derartige Präsentierung nach (6.15),b) eine Gruppenerweiterung des behaupteten Typs, da die Forderung $\rho \in \mathrm{Zentr}(G)$ wegen der Kommutativität von G natürlich erfüllt ist.

Der Zusatz für semidirekte Produkte ergibt sich mit denselben Überlegungen.

Beispiel: Zyklische Erweiterungen zyklischer Gruppen
$G = C_q = \langle a \rangle$ sei zyklisch von der Ordnung q, dann sind die Automorphismen φ von G gegeben durch $\varphi\colon a \mapsto a^\nu$ mit $\nu \in (\mathbb{Z}/q\mathbb{Z})^\times$. $\varphi^d = \mathrm{id}$ bedeutet $\nu^d \equiv 1 \bmod q$. Nach (6.16) erhält man alle Gruppenerweiterungen von C_q mit C_d in der Form

$$\langle a, x | a^q\,,\ x^d = a^\mu\,,\ a^x = a^\nu \rangle$$

mit $\nu^d \equiv 1 \bmod q$, $\mu\nu \equiv \mu \bmod q$. Durch Änderung des Erzeugenden a kann man o.E. erreichen, daß μ ein Teiler von q ist. Man erhält so die Nebenbedingungen

$$\mu | q\,,\ \nu \equiv 1 \bmod \frac{q}{\mu}\,,\ \nu^d \equiv 1 \bmod q.$$

Der Spezialfall $\mu = q$ bzw. $\rho = 1$ führt auf die semidirekten Produkte

$$\langle a, x | a^q\,,\ x^d\,,\ a^x = a^\nu \rangle \quad (\nu^d \equiv 1 \bmod q),$$

unter denen für $\nu = 1$ auch das direkte Produkt $C_q \times C_d$ vorkommt.

d. Gruppen kleiner Ordnung

Als weitere Anwendungsbeispiele wollen wir in diesem letzten Abschnitt Präsentierungen für alle Gruppen bestimmen, deren Ordnung Produkt von höchstens 3 Primzahlen ist:
Wir kennen bereits für eine Primzahl p die Gruppen der

$$\underline{\text{Ordnung } p}$$

Es gibt nur die zyklische:

$$C_p = \langle a \mid a^p \rangle.$$

$$\underline{\text{Ordnung } p^2}$$

Diese sind abelsch:

$$C_{p^2} = \langle a \mid a^{p^2} \rangle\,, \quad C_p \times C_p = \langle a, b \mid a^p, b^p, ab = ba \rangle.$$

$$\underline{\text{Ordnung } p^3}$$

Neben den drei abelschen Gruppen, deren Präsentierungen hier nicht mehr aufgeführt zu werden brauchen, gibt es zwei nicht-abelsche Gruppen dieser Ordnung (siehe EGI, Satz (3.15)), die man einheitlich für alle Primzahlen p folgendermaßen beschreiben kann (Übung):

$$A_{p^3} := \langle a, b, c \mid a^p, b^p, c^p, ab = ba, ac = ca, b^c = ba \rangle,$$
$$B_{p^3} := \langle a, b, c \mid a^p, b^p = c^p = a, ab = ba, ac = ca, b^c = ba \rangle.$$

Dabei ist für $p = 2$ $A_{2^3} = D_8$ die Diedergruppe und $B_{2^3} = Q_8$ die Quaternionengruppe.

Im folgenden seien $p < q < r$ Primzahlen.

Ordnung pq

Es sei $\hat{G}$ eine Gruppe der Ordnung pq. Aus den Sylowsätzen folgt für die Anzahl s_q der q-Sylowgruppen in $\hat{G}$: $s_q \equiv 1 \bmod q$ und $s_q | p$, also wegen $p < q$ $s_q = 1$. Dies bedeutet, daß die q-Sylowgruppe Normalteiler ist und $\hat{G}$ daher eine Gruppenerweiterung von C_q mit C_p. Wegen $p \neq q$ ist diese Gruppenerweiterung ein semidirektes Produkt (EGI, Satz von Zassenhaus (3.8)). Wir haben also für $\hat{G}$ die Präsentierung

$$\hat{G} = \langle\, a, x \mid a^q, x^p, a^x = w_{\varphi(a)} \,\rangle,$$

mit einem Automorphismus $\varphi \in \mathrm{Aut}(C_q)$, $\varphi^p = \mathrm{id}$. Nun ist $\mathrm{Aut}(C_q) \simeq \mathbb{F}_q^\times$ (siehe EGI, (3.13)) und somit jeder derartige Automorphismus φ gegeben durch $a \mapsto a^\nu$ mit $\nu \in \mathbb{Z}$, $\nu^p \equiv 1 \bmod q$. Also folgt nach Korollar (6.16)

$$\hat{G} = \langle a, x \mid a^q, x^p, a^x = a^\nu \rangle \quad (\nu^p \equiv 1 \bmod q).$$

Für $\nu = 1$ erhält man das (abelsche) direkte Produkt von C_q mit C_p. Die übrigen in Frage kommenden ν erzeugen die eindeutig bestimmte Untergruppe der Ordnung p in der zyklischen Gruppe $\mathbb{F}_q^\times$, sofern es überhaupt eine solche gibt, d.h. sofern p ein Teiler von $q-1$ ist. In diesem Falle gilt für zwei solche ν, μ stets $\mu \equiv \nu^i \bmod q$ und $\nu \equiv \mu^j \bmod q$ mit zu p teilerfremden Zahlen i und j. Man überprüft nun leicht, daß die Präsentierungen $\hat{G} = \langle a, x \mid a^q, x^p, a^x = a^\nu \rangle$ und $\hat{G} = \langle a, x \mid a^q, x^p, a^x = a^{\nu^i} \rangle$ isomorph sind, indem man x auf x^i abbildet. Wir finden also neben der abelschen Gruppe

$$C_q \times C_p \simeq C_{pq}$$

nur im Falle $p \mid q-1$ eine weitere nicht-abelsche Gruppe der Ordnung pq, nämlich das semidirekte Produkt

$$D_{pq} := \langle a, x \mid a^q, x^p, a^x = a^\nu \rangle \quad (\nu \not\equiv 1 \bmod q, \nu^p \equiv 1 \bmod q).$$

Diese Gruppe ist unabhängig vom gewählten ν mit den geforderten Eigenschaften. Ein solches ν, und also auch diese Gruppe, existiert nur für $p \mid q-1$.

Die Existenz dieser und der im folgenden auftretenden Gruppen ergibt sich aus (6.16) oder (6.15); sie wird dann jedoch nicht mehr explizit ausgesprochen. Außerdem werden wir im folgenden nur die nicht-abelschen Gruppen untersuchen, als nächstes die der

Ordnung pq^2

Wieder ist die q-Sylowgruppe Normalteiler in einer Gruppe $\hat{G}$ der betrachteten Ordnung, und diese daher eine Gruppenerweiterung einer Gruppe A der Ordnung q^2 mit der zyklischen Gruppe der Ordnung p. Wie schon erwähnt ist A abelsch, also $A = C_{q^2}$ oder $A = C_q \times C_q = \mathbb{F}_q^2$. Als teilerfremde Gruppenerweiterung ist $\hat{G}$ wieder ein semidirektes Produkt, so daß man die verschiedenen Operationen von C_p auf A zu bestimmen hat. Die triviale Operation führt zum direkten Produkt $C_p \times A$, welches abelsch ist. Die nichttrivialen Operationen von C_p auf A sind gegeben durch die verschiedenen Untergruppen von $\mathrm{Aut}(A)$ mit der Ordnung p.

$A = C_{q^2}$: Da die Automorphismengruppe $\mathrm{Aut}(C_{q^2}) = (\mathbb{Z}/q^2\mathbb{Z})^\times$ zyklisch ist (siehe EGI Satz (3.14)), findet man mit denselben Überlegungen wie im Falle der Gruppen der Ordnung pq als einzige nicht-abelsche Gruppe der Ordnung pq^2 die Gruppe

$$M_{pq^2} := \langle a, x \mid a^{q^2}, x^p, a^x = a^\nu \rangle \quad (\nu \not\equiv 1 \bmod q^2\,,\, \nu^p \equiv 1 \bmod q^2).$$

Diese ist unabhängig vom gewählten ν mit den geforderten Eigenschaften. Ein solches ν, und also auch diese Gruppe, existiert nur, falls p ein Teiler der Gruppenordnung $\#(\mathbb{Z}/q^2\mathbb{Z})^\times = \phi(q^2) = q(q-1)$ ist, also $p \mid q-1$ gilt.

$\underline{A = C_q \times C_q}$: Wir untersuchen die Untergruppen $\langle\varphi\rangle \leq \mathrm{Aut}(A) = \mathrm{GL}_2(\mathbb{F}_q)$ mit der Ordnung p.

1. Fall: φ ist diagonalisierbar mit doppeltem Eigenwert.
Also gilt bei entsprechender Basiswahl in $C_q \times C_q = \langle a, b \mid a^q, b^q, ab = ba\rangle$

$$\varphi(a) = a^\nu\,,\ \varphi(b) = b^\nu$$

mit $\nu \in \mathbb{Z}\,,\ \nu \not\equiv 1 \bmod q\,,\ \nu^p \equiv 1 \bmod q$. Dieser Fall tritt nur auf für $p \mid q-1$ und führt zu einer Gruppe

$$K_{pq^2} := \langle a, b, x | a^q, b^q, x^p, ab = ba, a^x = a^\nu, b^x = b^\nu\rangle$$

mit irgendeiner ganzen Zahl $\nu \not\equiv 1 \bmod q\,,\ \nu^p \equiv 1 \bmod q$. (Verschiedene Werte von ν führen zu verschiedenen Erzeugenden derselben Untergruppen, also zu derselben Operation von C_p auf A und damit zu derselben Gruppenerweiterung.)

2. Fall: φ ist diagonalisierbar mit 2 verschiedenen Eigenwerten.
Entweder ist einer der Eigenwerte 1: Dann erhält man analog wie eben die Gruppe

$$\langle a, b, x \mid a^q, b^q, x^p, ab = ba, a^x = a, b^x = b^\nu\rangle \simeq D_{pq} \times C_q$$

mit irgendeiner ganzen Zahl $\nu \not\equiv 1 \bmod q\,,\ \nu^p \equiv 1 \bmod q$. Diese Gruppe tritt nur auf für $p \mid q-1$ und ist wieder unabhängig von ν.
Oder beide Eigenwerte sind von 1 verschieden: Dann sind sie Potenzen voneinander (die Eigenwerte sind p-te Einheitswurzeln), und man erhält die Gruppen

$$L_{pq^2}(s) := \langle a, b, x \mid a^q, b^q, x^p, ab = ba, a^x = a^\nu, b^x = b^{\nu^s}\rangle$$

mit

$$\nu \not\equiv 1 \bmod q\,,\ \nu^p \equiv 1 \bmod q\,,\ s \not\equiv 0, 1 \bmod p.$$

Diese Gruppen existieren nur im Falle $p > 2\,,\ p \mid q-1$ und sind ebenfalls von ν unabhängig. Nun läßt aber auch eine Vertauschung der Basisvektoren a, b die Operation unverändert. Dabei gehen die Eigenwerte ν, ν^s über in $\nu^s =: \mu, \nu = \mu^{s^{-1}}$, also ändert sich s in sein Inverses $(\bmod p)$. Daher führen verschiedene Werte von s zu derselben Gruppenerweiterung genau dann, wenn sie in $\mathbb{F}_p^\times$ invers zueinander sind. Man erhält so für $p > 2\,,\ p \mid q-1$ genau $\frac{p-1}{2}$ nicht-isomorphe Gruppen dieses Typs $L_{pq^2}(s)$.

3. Fall: φ ist triangulierbar.
Dann besitzt φ bzgl. passender Basiswahl die Matrix

$$M = \begin{pmatrix} \nu & \alpha \\ 0 & \mu \end{pmatrix}$$

mit $\nu, \mu \in \mathbb{F}_q^\times\,,\ \alpha \in \mathbb{F}_q$. Wären ν, μ verschieden, so wäre φ diagonalisierbar (man wähle je einen Eigenvektor zu ν bzw. μ) und einer der ersten Fälle läge vor. Also folgt $\nu = \mu$. Aus $\varphi^p = 1$ ergibt sich dann

$$1 = M^p = \begin{pmatrix} \nu^p & p\nu^{p-1}\alpha \\ 0 & \nu^p \end{pmatrix},$$

also $p\nu^{p-1}\alpha = 0$. Wegen $\nu \in \mathbb{F}_q^\times$ und $\mathrm{char}(\mathbb{F}_q) = q \neq p$ ist dies nur für $\alpha = 0$ möglich, d.h. φ ist diagonalisierbar und einer der beiden ersten Fälle liegt vor.

4. Fall: φ ist nicht triangulierbar.
Dann hat das charakteristische Polynom von φ keine Wurzel in $k := \mathbb{F}_q$, aber als quadratisches Polynom zwei Wurzeln in dem einzigen quadratischen Erweiterungskörper $K := \mathbb{F}_{q^2}$ von $\mathbb{F}_q$. Wegen $p < q$ ist $q \neq 2$, also die Charakteristik der betrachteten Körper ungleich 2. Daher folgt $K = k(\sqrt{D})$ mit $D \in k^\times \setminus (k^\times)^2$. Es bezeichne im folgenden $z = c + d\sqrt{D} \mapsto \overline{z} = c - d\sqrt{D}$ den nicht-trivialen k-Automorphismus von $K = k(\sqrt{D})$. Da k endlich von der Mächtigkeit q ist,

ist dieser einzige nichttriviale Automorphismus notwendig der Frobeniusautomorphismus $\overline{z} = z^q$ (siehe Algebra-Vorlesung Satz III.2.15).

Seien nun $\alpha = a + b\sqrt{D}$ und $\overline{\alpha} = a - b\sqrt{D}$ die beiden Wurzeln des charakteristischen Polynoms von φ. Da diese nicht in $\mathbb{F}_q$ liegen, ist $b \neq 0$, und wegen $\operatorname{char} \mathbb{F}_q \neq 2$ sind dann die beiden Wurzeln verschieden.

Wie bei der Untersuchung von Endomorphismen reeller Vektorräume durch Übergang zur Komplexifizierung betrachten wir auch hier φ in natürlicher Weise als K-Automorphismus des K^2: Wir benutzen die Matrix von φ bzgl. der kanonischen Basis des k-Vektorraums k^2, um damit einen K-Automorphismus des K^2 zu definieren. Als K-Automorphismus ist φ dann diagonalisierbar, da das charakteristische Polynom 2 verschiedene Wurzeln in K hat. Sei $u \in K^2$ ein Eigenvektor von φ zum Eigenwert α, dann ist $\overline{u}$ Eigenvektor zum Eigenwert $\overline{\alpha}$ und $u, \overline{u}$ eine K-Basis des K^2, bzgl. der φ die Matrix

$$M_{u,\overline{u}}(\varphi) = \begin{pmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{pmatrix}$$

hat. Wegen $\varphi^p = 1$ und $\varphi \neq 1$ gilt auch $\alpha^p = 1, \alpha \neq 1$, so daß α eine primitive p-te Einheitswurzel aus $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ ist. Die folgenden Überlegungen sind von α unabhängig, da jede andere primitive p-te Einheitswurzel eine Potenz von α ist und daher zur entsprechenden Potenz von φ gehört. Dies ändert aber die Operation und damit die Gruppenerweiterung nicht.

Wir gehen nun über zur K-Basis

$$x = \frac{1}{2}(u + \overline{u}),\ y = \frac{1}{2\sqrt{D}}(u - \overline{u})$$

des K^2. Wegen $x, y \in k^2$ bilden diese Vektoren auch eine k-Basis des k^2. Bzgl. dieser Basis hat φ die Matrix

$$M_{x,y}(\varphi) = \begin{pmatrix} a & bD \\ b & a \end{pmatrix}.$$

Bzgl. der k-Basis $v = -\frac{1}{b}x, w = \frac{a}{b}x + y$ des k^2 finden wir dann die Matrix

$$M_{v,w}(\varphi) = \begin{pmatrix} 0 & a^2 - b^2D \\ -1 & 2a \end{pmatrix}.$$

Nun ist $2a = \alpha + \overline{\alpha} = \operatorname{Tr}_{K|k}(\alpha) = \alpha^q + \alpha$ die Spur und $a^2 - b^2D = \alpha\overline{\alpha} = \mathcal{N}_{K|k}(\alpha) = \alpha^{q+1}$ die Norm von α. Wegen $\alpha^p = 1$ ist auch $\mathcal{N}(\alpha)^p = 1$. Wäre nun $\mathcal{N}(\alpha) \neq 1$, so wäre dies eine primitive p-te Einheitswurzel in $k = \mathbb{F}_q$, und die p-te Einheitswurzel α läge auch in k, im Widerspruch zur Annahme in diesem 4. Fall. Wir folgern also $a^2 - b^2D = 1$ und erhalten für φ folgende Matrixdarstellung

$$\begin{pmatrix} 0 & 1 \\ -1 & \operatorname{Tr}\alpha \end{pmatrix}$$

mit einer primitiven p-ten Einheitswurzel $\alpha \in \mathbb{F}_{q^2}$, die nicht in $\mathbb{F}_q$ liegt. Diese existiert genau dann, wenn p ein Teiler von $\#\mathbb{F}_{q^2}^\times = q^2 - 1 = (q-1)(q+1)$, aber nicht von $\#\mathbb{F}_q^\times = q - 1$ ist, d.h. wenn $p \mid q + 1$ gilt. Wir finden somit in diesem 4. Fall die Gruppe

$$N_{pq^2} := \langle a, b, x \mid a^q, b^q, ab = ba, a^x = b, b^x = a^{-1}b^{\alpha^q + \alpha} \rangle$$

mit irgendeinem $\alpha \in \mathbb{F}_{q^2}^\times \setminus \mathbb{F}_q^\times$, $\alpha^p = 1$. Sie ist unabhängig von α. Solch ein α, und also auch diese Gruppe, existiert nur für $p \mid q + 1$.

Wir kommen nun zu den nicht-abelschen Gruppen der

$$\underline{\text{Ordnung } p^2q}$$

Wieder untersuchen wir die Anzahl s_q der q-Sylowgruppen. Wegen $p < q$ scheidet der Fall $s_q = p \equiv 1 \bmod q$ aus und der

1. Fall $s_q = p^2 \equiv 1 \bmod q$
ist nur möglich für $q = p + 1$, also für $p = 2, q = 3$ und somit $p^2q = 12$. Die 3-Sylowgruppen in einer Gruppe $\hat{G}$ dieser Ordnung sind zyklisch und verschiedene haben nur das neutrale Element gemeinsam. Aus $s_3 = 4$ folgt daher, daß $\hat{G}$ 8 Elemente der Ordnung 3 besitzt. Die übrigen 4 Elemente bilden gerade die 2-Sylowgruppe, die also eindeutig bestimmt und daher ein Normalteiler ist. $\hat{G}$ ist folglich semidirektes Produkt einer Gruppe A der Ordnung 4 mit der zyklischen Gruppe C_3 der Ordnung 3. Die nicht-abelschen darunter sind bestimmt durch Automorphismen $\varphi \in \mathrm{Aut}(A)$ von der Ordnung 3.

Ist $A = C_4$ zyklisch, so ist $\mathrm{Aut}(A) = (\mathbb{Z}/4\mathbb{Z})^\times \simeq C_2$, ein solches φ existiert also nicht. Ist $A = C_2 \times C_2 = \mathbb{F}_2^2$ die Kleinsche Vierergruppe, so hat $\mathrm{Aut}(A) = \mathrm{GL}_2(\mathbb{F}_2)$ die Ordnung $(2^2 - 1)(2^2 - 2) = 6$ und besitzt daher nur eine Untergruppe der Ordnung 3. Einer der beiden Automorphismen der Ordnung 3 von

$$A = C_2 \times C_2 = \langle a, b \mid a^2, b^2, ab = ba \rangle$$

ist gegeben durch $a \mapsto b \mapsto ab \mapsto a$ (vgl. Beispiel 1) nach Bemerkung (6.13)). Die einzige nicht-abelsche Gruppe in diesem Fall ist daher

$$A_4 \simeq \langle a, b, x \mid a^2, b^2, ab = ba, a^x = b, b^x = ab \rangle,$$

die alternierende Gruppe vierten Grades.

2. Fall $s_q = 1$
In diesem Fall ist die q-Sylowgruppe Normalteiler in $\hat{G}$ und die Faktorgruppe eine Gruppe der Ordnung p^2. Diese besitzt einen Normalteiler vom Index p, also ist $\hat{G}$ eine Gruppenerweiterung einer Gruppe H der Ordnung pq mit der zyklischen Gruppe C_p. Mit denselben Überlegungen ergibt sich, daß *jede* Untergruppe H der Ordnung pq Normalteiler in $\hat{G}$ ist.

2.1 Eine Untergruppe H der Ordnung pq ist abelsch
Dann ist $H \simeq C_p \times C_q$. Ein Automorphismus $\varphi \in \mathrm{Aut}(H)$ läßt die direkten Faktoren C_p und C_q von H invariant, induziert durch Einschränkung also Automorphismen $\varphi_p \in \mathrm{Aut}(C_p)$ bzw. $\varphi_q \in \mathrm{Aut}(C_q)$ mit $\varphi_p^p = 1$ und $\varphi_q^p = 1$. Da die Ordnung $\#\,\mathrm{Aut}(C_p) = p - 1$ zu p prim ist, folgt $\varphi_p = 1$. Also ist der Automorphismus φ von $H = \langle a, b \mid a^p, b^q, ab = ba \rangle$ gegeben durch

$$\varphi(a) = a\,,\ \varphi(b) = b^\nu \quad \text{für ein } \nu \in \mathbb{Z}\,,\ \nu^p \equiv 1 \bmod q.$$

Da nur nicht-abelsche Gruppen betrachtet werden, ist $\varphi \neq 1$, d.h. $\nu \not\equiv 1 \bmod q$. Gemäß (6.16) sind die Präsentierungen der möglichen Gruppen $\hat{G}$ durch φ und ein Element $\rho \in H$ mit $\varphi(\rho) = \rho$ bestimmt. Die Fixgruppe von φ ist gerade die p-Sylowgruppe C_p von H, also folgt $\rho = 1$ oder ρ ist ein Erzeugendes von $C_p = \langle a \rangle$, o.E. also $\rho = a$.

Dies führt zu den folgenden Möglichkeiten für nicht-abelsche Gruppen der Ordnung p^2q im Falle 2.1:

$$\begin{aligned} C_p \times D_{pq} &\simeq \langle a, b, x \mid a^p, b^q, x^p, ab = ba, a^x = a, b^x = b^\nu \rangle \quad \text{und} \\ G_{p^2q} : \quad &= \langle a, b, x \mid a^p, b^q, x^p = a, ab = ba, a^x = a, b^x = b^\nu \rangle\,, \end{aligned}$$

jeweils mit irgendeiner ganzen Zahl $\nu \not\equiv 1 \bmod q\,,\ \nu^p \equiv 1 \bmod q$. Beide Gruppen existieren nur im Falle $p \mid q - 1$.

2.2 Keine Untergruppe der Ordnung pq ist abelsch.
Die einzige nicht-abelsche Gruppe der Ordnung pq ist D_{pq}. Damit ist $\hat{G}$ eine Gruppenerweiterung von $H = D_{pq}$ mit der zyklischen Gruppe C_p. Gemäß Satz (6.15) erhalten wir aus der Präsentierung $D_{pq} = \langle a, b \mid a^q, b^p, a^b = a^\mu \rangle$ ($\mu \not\equiv 1, \mu^p \equiv 1 \bmod q$) eine Präsentierung für $\hat{G}$

$$\hat{G} = \langle a, b, x \mid a^q, b^p, x^p = \rho, a^b = a^\mu, a^x = \varphi(a), b^x = \varphi(b) \rangle,$$

wobei x Repräsentant eines Erzeugenden von C_p ist. Wir untersuchen nun die verschiedenen Möglichkeiten für $\rho = x^p \in D_{pq}$ und $\varphi = (\ldots)^x \in \mathrm{Aut}(D_{pq})$.

Die q-Sylowgruppe $C_q = \langle a \rangle$ von D_{pq} ist eindeutig bestimmt, also eine charakteristische Untergruppe, so daß φ durch Einschränkung ein $\varphi_q \in \mathrm{Aut}(C_q) \simeq \mathbb{F}_q^\times$ induziert. Damit ergibt sich $\varphi(a) = a^\nu$ für eine ganze Zahl $\nu \in \mathbb{Z}$, $q \nmid \nu$.

Wir unterscheiden nun die verschiedenen möglichen Ordnungen von $\rho = x^p \in D_{pq}$. (D_{pq} enthält nur Elemente der Ordnung $1, p, q$.)

Fall 2.2.1 $\rho = 1$
In diesem Falle gilt $\varphi^p = (\ldots)^\rho = \mathrm{id}$ und somit $\nu^p \equiv 1 \bmod q$. Wäre $\varphi = 1$, so wäre $\hat{G}$ das direkte Produkt $D_{pq} \times C_p$ und enthielte daher mit $C_q \times C_p$ eine abelsche Untergruppe der Ordnung pq entgegen der Annahme in diesem Fall 2.2.

Also ist $\varphi \neq 1$ und $\nu \not\equiv 1 \bmod q$, d.h. μ und ν sind primitive p-te Einheitswurzeln in $\mathbb{F}_q^\times$, also Potenzen voneinander: $\mu = \nu^s$ für ein $s \in \mathbb{F}_p^\times$. Daraus folgt für das Element $y = b^{-1}x^s \in \hat{G}$: $y \notin D_{pq}$, $a^y = a$. Die von a und y erzeugte Untergruppe $\langle a, y \rangle$ von $\hat{G}$ ist somit abelsch, und da p die Ordnung von y teilt ($\#\hat{G}/D_{pq} = p$), enthielte $\hat{G}$ eine abelsche Untergruppe der Ordnung pq, im Widerspruch zur Annahme in diesem Fall 2.2.

Fall 2.2.2 $\mathrm{ord}\,\rho = q$
Dann hat x die Ordnung pq, wieder im Widerspruch zur Voraussetzung 2.2.

Fall 2.2.3 $\mathrm{ord}\,\rho = p$
Dann gilt $D_{pq} = \langle a, b \rangle = \langle a, \rho \rangle$ und wir können in obiger Präsentierung für $\hat{G}$ o.E. $\rho = b$ annehmen und erhalten

$$\hat{G} = \langle a, b, x \mid a^q, b^p, x^p = b, a^b = a^\mu, a^x = a^\nu, b^x = b \rangle,$$

mit $\mu, \nu \in \mathbb{Z}$, $\mu \not\equiv 1 \bmod q$, $\mu^p \equiv 1 \bmod q$. Wegen $x^p = b$ muß natürlich $\nu^p \equiv \mu \bmod q$ gelten und wir erhalten die Gruppe

$$H_{p^2q} := \langle a, x \mid a^q, x^{p^2}, a^x = a^\nu \rangle$$

für irgendein $\nu \in \mathbb{Z}$, $\nu^p \not\equiv 1 \bmod q$, $\nu^{p^2} \equiv 1 \bmod q$. Diese Gruppe ist ein semidirektes Produkt $C_q \rtimes C_{p^2}$; sie existiert genau im Falle $p^2 \mid q - 1$ und ist wiederum vom gewählten ν mit den geforderten Eigenschaften unabhängig.

Die Bestimmung von Präsentierungen für die Gruppen der

$$\underline{\text{Ordnung } pqr}$$

erfolgt mit denselben Methoden (Übung) und führt zu den Gruppen

$$\begin{aligned}
C_{pqr} &= \langle a \mid a^{pqr} \rangle, \\
C_r \times D_{pq} &\simeq \langle a, b, x \mid a^r, b^q, x^p, ab = ba, a^x = a, b^x = b^\nu \rangle \\
&\quad \text{mit } \nu \not\equiv 1, \nu^p \equiv 1 \bmod q, \text{ nur möglich falls } p \mid q-1; \\
G_{pqr}(s) &:= \langle a, b, x \mid ab = ba, a^x = a^\mu, b^x = b^{\nu^s} \rangle \, (s = 1, \ldots, p-1) \\
&\quad \text{mit } \nu \not\equiv 1, \nu^p \equiv 1 \bmod q\,,\ \mu \not\equiv 1, \mu^p \equiv 1 \bmod r, \\
&\quad \text{nur möglich falls } p \mid q-1, p \mid r-1; \\
H_{pqr} &:= \langle a, b \mid a^r, b^{pq}, a^b = a^\nu \rangle \\
&\quad \text{mit } \nu^p \not\equiv 1, \nu^q \not\equiv 1, \nu^{pq} \equiv 1 \bmod r, \text{ nur möglich falls } pq \mid r-1.
\end{aligned}$$

Die Notation für die in diesem Abschnitt eingeführten Gruppen entspricht der von J. Neubüser benutzten.

§7 Permutationsgruppen

Eine *Permutationsgruppe* auf einer Menge Ω ist eine Untergruppe der vollen *symmetrischen Gruppe* $\mathcal{S}(\Omega)$ über Ω:

$$G \leq \mathcal{S}(\Omega) := \{\sigma \mid \sigma\colon \Omega \to \Omega \text{ Bijektion } \}$$

mit der Hintereinanderausführung $\circ$ als Gruppenverknüpfung. Allgemeiner versteht man unter einer *Permutationsdarstellung* einer Gruppe G einen Gruppenhomomorphismus $P\colon G \to \mathcal{S}(\Omega)$ von G in die symmetrische Gruppe $\mathcal{S}(\Omega)$ über einer Menge Ω. $P(G)$ ist dann eine Permutationsgruppe auf Ω. Eine Permutationsdarstellung P von G auf Ω induziert durch die Festsetzung $\sigma.\omega := P(\sigma)(\omega)$ $(\sigma \in G, \omega \in \Omega)$ eine Operation von G auf Ω, d. i. eine Abbildung

$$G \times \Omega \to \Omega\,, \quad (\sigma, \omega) \mapsto \sigma.\omega$$

mit den Eigenschaften

$$1_G.\omega = \omega\,,\ (\sigma\tau).\omega = \sigma.(\tau.\omega) \quad (\sigma, \tau \in G, \omega \in \Omega).$$

Umgekehrt bestimmt jede derartige Operation eine Permutationsdarstellung.
Operiert G auf Ω, so auch auf der Potenzmenge $\mathcal{P}(\Omega)$ durch

$$\Omega \supseteq B \mapsto \sigma.B := \{\sigma.b \mid b \in B\}.$$

Als übung präzisiere man den Begriff eines Homomorphismus/Isomorphismus zwischen Operationen von Gruppen auf (verschiedenen) Mengen bzw. zwischen Permutationsdarstellungen bzw. Permutationsgruppen.

a. Primitive Permutationsgruppen

Die folgenden Begriffsbildungen für Operationen von Gruppen auf Mengen sind in natürlicher Weise auch auf Permutationsdarstellungen bzw. Permutationsgruppen anwendbar.

(7.1) Definition: Die Gruppe G operiere auf der Menge Ω.

a) Die Operation heißt *transitiv* auf Ω genau dann, wenn für alle $\omega, \omega' \in \Omega$ ein $\sigma \in G$ existiert mit $\sigma.\omega = \omega'$.

b) Eine Teilmenge $B \subseteq \Omega$ heißt *Block* unter der Operation von G auf Ω (kurz G-Block), wenn gilt:

$$\sigma.B = B \ \vee \ \sigma.B \cap B = \emptyset \quad \text{für alle } \sigma \in G.$$

[Offenbar sind Ω, $\emptyset$ und die einpunktigen Mengen $\{\omega\}$ $(\omega \in \Omega)$ Blöcke bzgl. jeder Operation auf Ω, die sog. trivialen Blöcke.]

c) Die Operation heißt *primitiv* auf Ω, wenn sie transitiv ist und nur die trivialen Blöcke hat, d. h. Blöcke mit mindestens 2 Elementen notwendig ganz Ω sind.

(7.2) Beispiel: (Imprimitive Permutationsgruppe) Sei Ω eine endliche Menge, zerlegt in k disjunkte Mengen B_j $(j = 1, \ldots, k)$ von *gleicher* Mächtigkeit b, also $\#\Omega = k \cdot b$. Wir betrachten nun die Gruppe $\mathcal{S}(B_1|\ldots|B_k)$ aller Permutationen der symmetrischen Gruppe $\mathcal{S}(\Omega)$, die diese *Partition* (B_j) von Ω 'respektieren', d.h.

$$\mathcal{S}(B_1|\ldots|B_k) := \{\sigma \in \mathcal{S}(\Omega) \mid \bigwedge_i \bigvee_j \sigma B_i = B_j\}.$$

Man erkennt sofort, daß diese Permutationsgruppe $G = \mathcal{S}(B_1|\ldots|B_k)$ transitiv auf Ω operiert. Die Mengen B_j sind G-Blöcke der Länge b, so daß G für $1 < b < \#\Omega$ imprimitiv ist.

Die Elemente von G permutieren definitionsgemäß die k Blöcke B_j, also hat man eine natürliche Permutationsdarstellung $p\colon G \to \mathcal{S}_k$ gegeben durch

$$p(\sigma)(i) = j \iff \sigma B_i = B_j.$$

Der Kern dieser Darstellung p

$$\operatorname{Ke} p = \{\sigma \in \mathcal{S}(\Omega) \mid \sigma B_j = B_j \text{ für alle } j\}$$

ist offensichtlich isomorph zur Gruppe

$$(\mathcal{S}_b)^k = \underbrace{\mathcal{S}_b \times \ldots \times \mathcal{S}_b}_{k-\text{mal}},$$

da man auf jedem Block B_j unabhängig beliebige Permutationen $\sigma_j \in \mathcal{S}_b \simeq \mathcal{S}(B_j)$ vorschreiben kann. Damit ist $\mathcal{S}(B_1|\ldots|B_k)$ eine Gruppenerweiterung des Normalteilers $(\mathcal{S}_b)^k$ mit $\mathcal{S}_k$

$$(\mathcal{S}_b)^k \hookrightarrow \mathcal{S}(B_1|\ldots|B_k) \twoheadrightarrow \mathcal{S}_k \qquad (*)$$

und hat die Ordnung

$$\#\mathcal{S}(B_1|\ldots|B_k) = (b!)^k \cdot k!.$$

Diese Gruppe ist ein Kranzprodukt, wie in EGI, Definition (3.6) definiert:

(7.3) Proposition: *$G = \mathcal{S}(B_1|\ldots|B_k)$ ist das Kranzprodukt*

$$\mathcal{S}_b \wr \mathcal{S}_k := (\mathcal{S}_b)^k \rtimes \mathcal{S}_k = \underbrace{\mathcal{S}_b \times \ldots \times \mathcal{S}_b}_{k-\text{mal}} \rtimes \mathcal{S}_k,$$

wobei die Operation von $\mathcal{S}_k$ auf $(\mathcal{S}_b)^k$ durch Permutation der k Faktoren gegeben ist.

Beweis: Um zu zeigen, daß die Gruppenerweiterung $(*)$ ein semidirektes Produkt ist, muß man nachweisen, daß ein Komplement existiert und dieses wie beschrieben auf dem Kern operiert (siehe EGI, Proposition (3.5)).

Wir wählen dazu feste Abzählungen $B_j = \{\omega_{ij} \mid 1 \le i \le b\}$ der B_j, wodurch Ω mit $\{1, \ldots, b\} \times \{1, \ldots, k\}$ identifiziert wird. Ein $\sigma = (\sigma_1, \ldots, \sigma_k) \in (\mathcal{S}_b)^k$ operiere entsprechend dieser Abzählung auf Ω durch $\sigma(\omega_{ij}) = \omega_{\sigma_j(i),j}$. Daneben induziert jede Permutation $\tau \in \mathcal{S}_k$ ein $\hat{\tau} \in G$ definiert durch $\hat{\tau}(\omega_{ij}) = \omega_{i\tau(j)}$. Dieses $\hat{\tau} \in G$ ist ein Urbild von $\tau \in \mathcal{S}_k$ bzgl. der Gruppenerweiterung $(*)$ und liefert ein Komplement $U = \{\hat{\tau} \mid \tau \in \mathcal{S}_k\}$ von $(\mathcal{S}_b)^k$ in G. Die Gruppenerweiterung $(*)$ ist somit ein semidirektes Produkt, und wir müssen nun nur noch die Operation der Faktorgruppe auf dem Kern bestimmen:
In der folgenden Rechnung identifizieren wir Ω mit $\{1, \ldots, b\} \times \{1, \ldots, k\}$ vermöge der Abzählung $(i, j) \mapsto \omega_{ij}$. Dann gilt für $(\sigma_1, \ldots, \sigma_k) \in (\mathcal{S}_b)^k \hookrightarrow G$ und $\tau \in \mathcal{S}_k$:

$$\begin{aligned}
(\sigma_1, \ldots, \sigma_k)^\tau(i, j) &= \hat{\tau}^{-1} \circ (\sigma_1, \ldots, \sigma_k) \circ \hat{\tau}\,(i, j) \\
&= \hat{\tau}^{-1} \circ (\sigma_1, \ldots, \sigma_k)(i, \tau(j)) \\
&= \hat{\tau}^{-1}(\sigma_{\tau(j)}(i), \tau(j)) \\
&= (\sigma_{\tau(j)}(i), j) \\
&= (\sigma_{\tau(1)}, \ldots, \sigma_{\tau(k)})(i, j),
\end{aligned}$$

also wie behauptet

$$(\sigma_1, \ldots, \sigma_k)^\tau = (\sigma_{\tau(1)}, \ldots, \sigma_{\tau(k)}).$$

□

Wir wollen im folgenden nun zeigen, daß jede imprimitive Permutationsgruppe $G \leq \mathcal{S}(\Omega)$ in einem solchen Kranzprodukt enthalten ist, genauer gilt

(7.4) Proposition: *Es sei $P\colon G \to \mathcal{S}(\Omega)$ eine transitive Permutationsdarstellung. $B \subseteq \Omega$ sei ein G-Block und $H := \mathrm{Stab}_G(B) := \{\sigma \in G \mid \sigma B = B\}$ die Stabilisatorgruppe[3] des Blockes B. Dann gilt:*

a) *Die Bilder σB ($\sigma \in G$) des Blockes B sind ebenfalls G-Blöcke und bilden eine Klasseneinteilung von Ω; die Anzahl der verschiedenen σB ist genau der Gruppenindex $(G : H)$. Die Gruppe H operiert transitiv auf B.*

b) *Sind G und Ω endlich, so gilt:*

$$n := \#\Omega = b \cdot k \text{ mit } b := \#B \mid \#H\,,\ k := \#\{\sigma B \mid \sigma \in G\} = (G : H).$$

c) *Sind unter den Voraussetzungen von b) $B_1, \ldots, B_k$ die verschiedenen unter den Blöcken σB ($\sigma \in G$), so bildet die Permutationsdarstellung $P\colon G \to \mathcal{S}(\Omega)$ die Gruppe G in das Kranzprodukt $\mathcal{S}(B_1|\ldots|B_k)$ ab.*

Der *Beweis* ist eine einfache Übung (vgl. EGI, Abschnitt 2.a.).

(7.5) Korollar: *Operiert eine Gruppe G transitiv auf einer Menge Ω, deren Mächtigkeit eine Primzahl ist, so ist die Operation primitiv.*

Eine Übersicht über die möglichen Blöcke einer Permutationsgruppe gibt der folgende

(7.6) Satz: *Es operiere G transitiv auf Ω und es sei $G_\omega = \mathrm{Fix}_G(\omega)$ die Fixgruppe einer Ziffer $\omega \in \Omega$. Dann gilt:*

a) *Die Zuordnungen*

$$G_\omega \leq H \leq G \mapsto B := H.\omega \quad \text{und} \quad \omega \in B \text{ Block } \mapsto H := \mathrm{Stab}_G(B)$$

sind zueinander inverse, inklusionstreue Bijektionen zwischen den Obergruppen von G_ω und den G-Blöcken B, die ω enthalten.
Die verschiedenen Zerlegungen von Ω in G-Blöcke gemäß (7.4), a) entsprechen daher bijektiv den Obergruppen H von G_ω.

b) *Genau dann operiert G primitiv auf Ω, wenn die Fixgruppe G_ω einer beliebigen Ziffer $\omega \in \Omega$ eine maximale Untergruppe in G ist.*

Beweis: a) rechnet man leicht nach. Gemäß a) sind dann die G-Blöcke B, die ω enthalten, genau die Bahnen $H\omega$ von ω unter einer Obergruppe H von G_ω. Da deren Länge gerade $\#B = \#H\omega = (H : H_\omega) = (H : G_\omega)$ ist, folgt die Behauptung von b).

(7.7) Proposition:

a) *Operiert G transitiv auf Ω und ist N ein Normalteiler in G, so bilden die N-Bahnen Blöcke bzgl. G. Diese haben alle dieselbe Länge $l \geq 2$, es sei denn N operiert trivial.*

b) *Normalteiler $N \neq \{\mathrm{id}\}$ in primitiven Permutationsgruppen $G \leq \mathcal{S}(\Omega)$ operieren transitiv auf Ω.*

[3] Man unterscheide dies von der Fixgruppe, bestehend aus den $\sigma \in G$, die B *elementweise* festhalten!

Beweis: a) Ist $\omega \in \Omega$ und $N\omega$ die Bahn von ω unter N, so ist für alle $\sigma \in G$ offenbar $\sigma N\omega = N^{\sigma^{-1}}\sigma\omega = N\sigma\omega$ wieder eine Bahn unter N, also disjunkt zu $N\omega$ oder damit identisch. Die N-Bahnen sind also G-Blöcke. Da G auf Ω und damit auch auf ihren Blöcken transitiv operiert, sind diese von gleicher Länge l. $l = 1$ bedeutet, daß N alle PUnkte festläßt.

b) Wäre nun in einer primitiven Permutationsgruppe $G \leq \mathcal{S}(\Omega)$ ein Normalteiler N nicht transitiv, so wären die N-Bahnen $N\omega \neq \Omega$, also als Blöcke der primitiven Gruppe G einpunktig und $N = \{\mathrm{id}_\Omega\}$, im Widerspruch zur Voraussetzung. □

b. Mehrfach transitive Permutationsgruppen

Eine wichtige Klasse von primitiven Permutationsgruppen sind die mehrfach transitiven Gruppen im Sinne der folgenden

(7.8) Definition: Eine Gruppe G operiert *k-fach transitiv* auf Ω, wenn $1 \leq k \leq \#\Omega$ ist und für je zwei k-Tupel $(\omega_1, \ldots, \omega_k)$, $(\omega'_1, \ldots, \omega'_k)$ von verschiedenen Elementen in Ω (d.h. $\omega_i \neq \omega_j$, $\omega'_i \neq \omega'_j$, für $i \neq j$) ein $\sigma \in G$ existiert mit $\sigma(\omega_i) = \omega'_i$ für $i = 1, \ldots, k$.
Existiert jeweils *genau ein* solches σ, so nennt man die Operation *scharf k-fach transitiv.*
Statt k-fach transitiv sagt man oft auch einfach *k-transitiv.*

(7.9) Proposition: *Operiert eine Gruppe G 2-fach transitiv, so auch primitiv.*

Beweis: Sei $B \subseteq \Omega$ ein G-Block mit mindestens 2 Elementen, etwa $a, b \in B$, $a \neq b$. Da G 2-fach transitiv operiert, existiert zu jedem $c \in \Omega, c \neq a$ ein $\sigma \in G$ mit $\sigma a = a$ und $\sigma b = c$. Da B ein Block ist, und $a \in \sigma B \cap B$ gilt, muß $\sigma B = B$ sein, und folglich gilt $c \in \sigma B = B$. Dies heißt, daß ganz Ω in B liegt; G operiert damit definitionsgemäß primitiv.

(7.10) Proposition: *Die Gruppe G operiere auf der Menge Ω.*

a) Dann sind für eine natürliche Zahl $1 < k \leq \#\Omega$ äquivalent:

i) G operiert (scharf) k-fach transitiv auf Ω.

ii) G operiert transitiv auf Ω und die Fixgruppe $G_\omega = \mathrm{Fix}_G(\omega)$ irgendeiner Ziffer $\omega \in \Omega$ operiert (scharf) (k-1)-fach transitiv auf $\Omega \setminus \{\omega\}$.

b) Operiert G k-fach transitiv auf n Elementen ($k \leq n$), so gilt

$$n(n-1) \cdot \ldots \cdot (n-k+1) \mid \#G.$$

Die Operation ist genau dann scharf k-fach transitiv, wenn die Gleichheit gilt.

Beweis: a) i)⇒ii) ist eine einfache Übung.
ii) ⇒ i): Seien $(\omega_1, \ldots, \omega_k)$, $(\omega'_1, \ldots, \omega'_k)$ k-Tupel von verschiedenen Elementen in Ω. Da G transitiv ist, existieren $\sigma, \sigma' \in G$ mit $\sigma\omega_k = \omega = \sigma'\omega'_k$. Da σ, σ' Bijektionen sind, sind die Elemente $\sigma\omega_i$ $(i = 1, \ldots, k)$ untereinander verschieden, insbesondere $\sigma\omega_i \neq \sigma\omega_k = \omega$ für $i = 1, \ldots, k-1$. Gleiches gilt für σ' und die ω'_i, so daß nach Voraussetzung ii) ein $\tau \in G_\omega$ existiert mit $\tau(\sigma\omega_i) = \sigma'\omega'_i$ für $i = 1, \ldots, k-1$. Dann hat $\rho := \sigma'^{-1} \circ \tau \circ \sigma \in G$ die gewünschte Eigenschaft $\rho\omega_i = \omega'_i$ für $i = 1, \ldots, k$. ρ ist durch diese Eigenschaft eindeutig bestimmt, wenn τ eindeutig ist.

b) folgt induktiv aus a): Der Induktionsanfang $k = 1$ ist klar nach der Bahngleichung (2.5) aus EGI: $(G : G_\omega) = \#\Omega = n$, und scharf 1-transitiv bedeutet insbesondere $G_\omega = \{\mathrm{id}\}$.

Sei nun $k \geq 2$. Die Fixgruppe G_ω einer Ziffer ω ist (scharf) $(k-1)$-fach transitiv auf $n-1$ Elementen, also gilt nach Induktionsannahme

$$(n-1)(n-2)\ldots(n-k+1) \mid \#G_\omega,$$

mit Gleichheit genau im Falle scharf $(k-1)$-fach transitiver Operation. Da G transitiv auf n Elementen operiert, gilt $(G : G_\omega) = n$, so daß insgesamt die Behauptung b) folgt. □

(7.11) Beispiele: 1) Simple Beispiele für mehrfach transitive Permutationsgruppen sind natürlich die symmetrische Gruppe $\mathcal{S}_n$, die scharf n-fach transitiv ist, und die alternierende Gruppe A_n, die für $n \geq 3$ scharf $(n-2)$-fach transitiv ist (Übung). Offensichtlich ist jede $(n-1)$-fach transitive Gruppe auf n Elementen bereits die symmetrische Gruppe $\mathcal{S}_n$.

2) Eine abelsche transitive Permutationsgruppe $G \leq \mathcal{S}(\Omega)$ ist scharf 1-fach transitiv (*regulär*), insbesondere gilt $\#G = \#\Omega$.

Beweis: Da $G \leq \mathcal{S}(\Omega)$ transitiv ist, sind die Fixgruppen beliebiger $\omega \in \Omega$ untereinander konjugiert, also im abelschen Falle gleich. Damit folgt $G_\omega = \bigcap_{\omega' \in \Omega} G_{\omega'} = \{\mathrm{id}_\Omega\}$, und G ist scharf 1-fach transitiv. Der Zusatz folgt aus Proposition (7.10),b).

3) Sei $\Omega = \mathbb{P}^1(K)$ die projektive Gerade über einem Körper K. Darauf operiert die Gruppe $\mathrm{PGL}_2(K)$ der gebrochen-linearen Abbildungen

$$z \mapsto \frac{az+b}{cz+d}\,, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K).$$

[Man identifiziert $\Omega = \mathbb{P}^1(K) = K \cup \{\infty\}$ und rechnet mit ∞ in üblicher Weise.]

- Diese Operation von $\mathrm{PGL}_2(K)$ auf Ω ist scharf 3-transitiv.
- Ist K ein endlicher Körper mit p^f Elementen, so folgt daraus gemäß Proposition (7.10),b):

$$\#\mathrm{PGL}_2(K) = \#\mathrm{PGL}(2, p^f) = (p^f+1)p^f(p^f-1).$$

Beweis: Offenbar operiert $G := \mathrm{PGL}_2(K)$ transitiv auf $\Omega = K \cup \{\infty\}$. Die Fixgruppe G_∞ von ∞ ist die Gruppe der linearen Abbildungen $z \mapsto az+b$ $(a, b \in K, a \neq 0)$. Diese ist transitiv auf $\Omega \setminus \{\infty\} = K$. Schließlich bestimmt man in G_∞ die Fixgruppe der 0. Diese besteht genau aus den 'Drehstreckungen' $z \mapsto az$ $(a \in K^\times)$ und ist als abelsche Gruppe scharf 1-fach transitiv auf $K^\times = \Omega \setminus \{\infty, 0\}$. □

4) Mit Beispiel 3) verwandt ist die *affine Gruppe* $\mathrm{AGL}_d(K)$ über einem Körper. Diese ist definiert als Gruppe

$$\mathrm{AGL}_d(K) = \{K^d \ni v \mapsto Av + b \mid A \in \mathrm{GL}_d(K)\,, b \in K^d\}$$

der affinen Abbildungen des Vektrorraums K^d.

In ihrer natürlichen Operation auf K^d ist $G := \mathrm{AGL}_d(K)$ 2-fach transitiv, denn schon die Untergruppe $T = \{v \mapsto v+b \mid b \in K^d\}$ aller Translationen operiert transitiv, und die Fixgruppe der 0 $G_0 = \{v \mapsto Av \mid A \in \mathrm{GL}_d(K)\}$ ist offensichtlich transitiv auf $K^d \setminus \{0\}$.

Zugleich ist durch die Gruppen T und G_0 die Struktur von $\mathrm{AGL}_d(K)$ erfaßt: Wegen $T \cap G_0 = \{\mathrm{id}\}$ und $G = T \cdot G_0$ ist G semidirektes Produkt von T mit G_0.

Nun ist T isomorph zur Additionsgruppe des Vektorraumes K^d, während G_0 zur allgemeinen linearen Gruppe $\mathrm{GL}_d(K)$ isomorph ist. Unter diesen Isomorphismen geht die durch Konjugation in G gegebene Operation von G_0 auf T genau in die natürliche Operation von $\mathrm{GL}_d(K) = \mathrm{Aut}(K^d)$ auf dem Vektorraum K^d über: $A \circ (v \mapsto v+b) \circ A^{-1} = (v \mapsto v + Ab)$. Fazit:

- $\mathrm{AGL}_d(K)$ ist das semidirekte Produkt des Vektorraumes K^d mit seiner Automorphismengruppe $\mathrm{GL}_d(K)$ bzgl. der natürlichen Operation.

5) Höher transitive Gruppen, die nicht die entsprechende alternierende Gruppe umfassen, zu konstruieren, ist schwierig. Es gilt nämlich der folgende

Satz: *Die einzigen mindestens 4-fach transitiven Gruppen vom Grade n, die nicht die alternierende Gruppe $\mathcal{A}_n$ umfassen, sind die folgenden vier Mathieugruppen:*

M_{24}: 5-fach transitiv vom Grad 24; Ordnung $24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48 = 244823040$,

M_{12}: scharf 5-fach transitiv vom Grad 12; Ordnung $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 = 95040$,

und darin die jeweiligen Fixgruppen einer Ziffer:

M_{23}: 4-fach transitiv vom Grad 23; Ordnung $23 \cdot 22 \cdot 21 \cdot 20 \cdot 48 = 10200960$,

M_{11}: scharf 4-fach transitiv vom Grad 11; Ordnung $11 \cdot 10 \cdot 9 \cdot 8 = 7920$.

Insbesondere ist eine mindestens 6-fach transitive Permutationsgruppe die alternierende oder symmetrische Gruppe.

Der *Beweis* dieses Satzes beruht auf der Klassifikation der endlichen einfachen Gruppen. Siehe dazu P. J. Cameron: Finite permutation groups and finite simple groups, Bull. London Math. Soc. **13** (1981) 1–22.

c. Normalteiler in primitiven Permutationsgruppen

In diesem Abschnitt wollen wir ein wenig erläutern, wie die Klassifikation der endlichen einfachen Gruppen bei einem Resultat über Permutationsgruppen ins Spiel kommt. Der Schlüssel dazu sind die minimalen Normalteiler. Der folgende Satz zeigt, wie die Untersuchung der minimalen Normalteiler zu Strukturaussagen führen kann:

(7.12) Satz: *Sei $G \leq \mathcal{S}(\Omega)$ eine primitive Permutationsgruppe und N ein minimaler Normalteiler. Ist dieser auflösbar* (etwa wenn G selbst auflösbar ist)*, so gilt:*

a) *$N \simeq \mathbb{F}_p^d$ ist elementar-abelsch und operiert regulär auf Ω,*

b) *der Grad $\#\Omega$ von G ist eine Primzahlpotenz p^d,*

c) *G ist semidirektes Produkt von N mit der Fixgruppe G_ω einer Ziffer $\omega \in \Omega$, und*

d) *bei geeigneter Identifizierung von Ω mit $\mathbb{F}_p^d$ ist G als Permutationsgruppe in der affinen Gruppe $\mathrm{AGL}_d(\mathbb{F}_p) = \mathrm{AGL}(d,p)$ enthalten.*

Beweis: a): Als minimaler Normalteiler ist N selbst charakteristisch einfach, also nach EGI, Satz (4.13) direktes Produkt $N = T_1 \times \ldots \times T_d$ von untereinander isomorphen einfachen Gruppen $T_i \simeq T$. Da N auflösbar sein soll, ist T zyklisch von Primzahlordnung, etwa $T \simeq \mathbb{F}_p$, und folglich $N \simeq \mathbb{F}_p^d$ elementar-abelsch. Da G primitiv ist, operiert der Normalteiler N transitiv auf Ω (Proposition (7.7),b)), als abelsche Gruppe also regulär (siehe (7.11) Beispiel 2)).

ad b): Insbesondere gilt dann $\#\Omega = \#N = p^d$.

ad c): Sei $\omega \in \Omega$ fest gewählt und $U = G_\omega$ die entsprechende Fixgruppe. Wegen der regulären Operation von N auf Ω gilt

$$N \cap U = N \cap G_\omega = N_\omega = 1.$$

Wegen der Transitivität von N gibt es zu jedem $\sigma \in G$ ein $\tau \in N$ mit $\sigma\omega = \tau\omega$, also $\tau^{-1}\sigma \in G_\omega = U$ und folglich ist $G = NU$. Damit ist U ein Komplement zu N in G und c) folgt.

ad d): Da N regulär auf Ω operiert, ist die Abbildung $N \to \Omega, \rho \mapsto \rho\omega$ eine Bijektion, mittels der wir Ω mit dem d-dimensionalen $\mathbb{F}_p$-Vektorraum N identifizieren. Dabei operiert dann $N \leq G$ auf $N \simeq \mathbb{F}_p^d$ durch Translation, während die Operation von $U = G_\omega$ auf $N \simeq \mathbb{F}_p^d$ gerade die in c) erwähnte Operation auf N durch Konjugation innerhalb G ist: Es gilt nämlich für $\tau \in N$ und $\sigma \in U = G_\omega$

$$\sigma(\tau\omega) = \sigma\tau\sigma^{-1}(\sigma\omega) = \sigma\tau\sigma^{-1}(\omega).$$

Da G als Permutationsgruppe treu auf Ω operiert, gilt dies auch für diese Operation von U auf N durch Konjugation, d. h. U ist Untergruppe von $\mathrm{Aut}(N) = \mathrm{GL}_d(p)$ und G wird als Permutationsgruppe isomorph zum semidirekten Produkt $\mathbb{F}_p^d \rtimes U \leq \mathrm{AGL}(d,p)$ mit der in Beispiel (7.11), 4) beschriebenen Operation auf $\mathbb{F}_p^d$.

Zum Schluß des Beweises sei angemerkt, daß c) für jeden Normalteiler $N \triangleleft G$ gilt, der regulär auf Ω operiert.

Daß die durch Konjugation innerhalb G gegebene Operation von U auf N treu ist, bedeutet, daß der Kern dieser Operation, der Zentralisator von N in U trivial ist. Dies ergibt sich auch aus der schärferen Aussage $C_G(N) = N$ des nachfolgenden Lemmas, das wir später noch mehrfach benötigen werden:

(7.13) Lemma: *Sei $N \leq \mathcal{S}(\Omega) =: \mathcal{S}$ eine transitive Permutationsgruppe und $C_{\mathcal{S}}(N) := \{\tau \in \mathcal{S} \mid \bigwedge_{\rho \in N} \tau\rho = \rho\tau\}$ sein Zentralisator. Dann gilt:*

a) *Der Zentralisator $C := C_{\mathcal{S}}(N)$ von N in der vollen symmetrischen Gruppe $\mathcal{S}$ hat triviale Fixgruppen $C_\omega = 1$ und seine Ordnung $\#C$ teilt daher $\#\Omega$.*

b) *Ist N zusätzlich abelsch, so folgt $N = C_{\mathcal{S}}(N)$.*

Beweis: Ad a): Sei $\sigma \in C_\omega$ und $\omega' \in \Omega$ beliebig. Da N transitiv operiert, gibt es ein $\tau \in N$ mit $\omega' = \tau\omega$. Dann gilt wegen $\sigma \in C_{\mathcal{S}}(N)$, also $\sigma\tau = \tau\sigma$ natürlich

$$\sigma\omega' = \sigma\tau\omega = \tau\sigma\omega = \tau\omega = \omega',$$

und folglich ist σ die Identität. Wegen $C_\omega = 1$ haben alle C-Bahnen die Länge $\#C$, so daß $\#\Omega$ ein Vielfaches von $\#C$ sein muß.

Ad b): Ist N abelsch, so gilt natürlich $N \leq C_{\mathcal{S}}(N) = C$. Als abelsche, transitive Gruppe ist N regulär, also $\#N = \#\Omega$, und aus a) folgt dann $\#N = \#\Omega \geq \#C$ und damit die Behauptung. □

Aus Satz (7.12) über Permutationsgruppen kann man nun leicht das folgende Korollar über maximale Untergruppen beliebiger auflösbarer Gruppen entnehmen, welches ein entsprechendes Resultat (EGI, (2.13)) für nilpotente Gruppen verallgemeinert.

(7.14) Korollar: *Maximale Untergruppen auflösbarer Gruppen haben Primzahlpotenzindex.*

Beweis: Sei G eine auflösbare Gruppe und U eine maximale Untergruppe. Dann liefert die Operation von G auf den Nebenklassen von U eine transitive, und wegen der Maximalität von U sogar primitive Permutationsdarstellung $p\colon G \to \mathcal{S}_n$ mit $n = (G : U)$. Mit G ist auch die Permutationsgruppe $p(G) \leq \mathcal{S}_n$ auflösbar. Nach Satz (7.12) ist dann der Grad $n = (G : U)$ eine Primzahlpotenz. □

Nachdem wir in (7.12) primitive Permutationsgruppen mit einem auflösbaren minimalen Normalteiler betrachtet haben, wollen wir nun die 2-fach transitiven Gruppen auch im nicht-auflösbaren Fall studieren.

(7.15) Satz: (Burnside) *Sei $G \leq \mathcal{S}(\Omega)$ eine 2-fach transitive Permutationsgruppe auf Ω.*

a) *Dann besitzt G genau einen minimalen Normalteiler N.*

b) *Für diesen minimalen Normalteiler N in G gibt es die folgenden Alternativen:*

   1) *N operiert regulär, ist elementar abelsch, und die Eigenschaften aus Satz (7.12) gelten,*

   oder

   2) *N operiert primitiv, ist eine nicht-abelsche einfache Gruppe,*
   und es gilt $N \lhd G \leq \mathrm{Aut}(N)$, wobei die Einbettung von G in $\mathrm{Aut}(N)$ durch die Konjugationsoperation von G auf N gegeben ist.

Beweis: Wir zeigen zunächst (für beliebige Normalteiler $N \lhd G$)

$$N \text{ operiert regulär} \Longrightarrow N \text{ elementar-abelsch.} \qquad (A)$$

Operiert N regulär, so kann N mit Ω identifiziert werden, und die Operation von G_ω auf N wird dann die Konjugation in G (siehe Beweis von (7.12),c),d)). Da G nach Voraussetzung 2-fach transitiv auf Ω operiert, ist die Operation von G_ω auf $N \setminus \{1\}$ noch transitiv. Da G_ω durch

Gruppenautomorphismen operiert, müssen alle Elemente von $N \setminus \{1\}$ dieselbe Ordnung haben, die dann eine Primzahl p sein muß. Damit ist N eine p-Gruppe mit nicht-trivialem Zentrum $\mathrm{Zentr}(N)$. Dieses ist als charakteristische Untergruppe von $N \triangleleft G$ Normalteiler in G, also unter der Operation von G_ω invariant: $G_\omega.\mathrm{Zentr}(N) \subset \mathrm{Zentr}(N)$. Wegen der Transitivität von G_ω auf $N \setminus \{1\}$ folgt dann für ein $1 \neq \sigma \in \mathrm{Zentr}(N)$ $G_\omega.\sigma = N \setminus \{1\} \subset \mathrm{Zentr}(N)$; N ist somit p-elementar-abelsch und (A) ist bewiesen.

a) Wir nehmen nun an, es gibt zwei verschiedene minimale Normalteiler N und M in G. Dann gilt $[N, M] \leq N \cap M = 1$ und die Elemente aus N und M kommutieren elementweise. Also liegt $1 \neq M$ im Zentralisator $N' := C_G(N) \leq C := C_{\mathcal{S}}(N)$. Nach Lemma (7.13),a) ist dann $M_\omega \leq N'_\omega \leq C_\omega = 1$ für $\omega \in \Omega$.

Zentralisatoren von Normalteilern sind als Kerne der Konjugation von G selbst Normalteiler. Also operiert $1 \neq N' \triangleleft G$ wegen der Primitivität von G transitiv auf Ω und damit regulär. Gleiches gilt für den minimalen Normalteiler M, also $\#M = \#N' = \#\Omega$ und wegen $M \leq N'$ dann $M = N'$. Nach (A) ist also $M = N'$ abelsch, nach (7.13),b) folgt dann $M = C_{\mathcal{S}}(M)$.

Wegen der Symmetrie von N und M erhält man genauso $N = M' := C_G(M) \leq C_{\mathcal{S}}(M) = M$, und damit einen Widerspruch zur Annahme $N \neq M$ und der Minimalität von M. □

b) Wir zeigen nun:

$$N \text{ operiert regulär oder primitiv.} \tag{B}$$

Wäre N weder regulär noch primitiv, so wäre N gemäß nachfolgender Proposition (7.16) eine *Frobeniusgruppe,* die gemäß anschließendem Satz (7.17) eine echte charakteristische Untergruppe besäße. N ist als minimaler Normalteiler in G aber bekanntlich charakteristisch einfach.

(7.16) Proposition: *Sei $G \leq \mathcal{S}(\Omega)$ 2-fach transitiv und N ein nicht trivialer Normalteiler. Ist N nicht primitiv auf Ω, so ist die Fixgruppe $N_{\omega\omega'}$ verschiedener Punkte $\omega, \omega' \in \Omega$ trivial:*

$$N_{\omega\omega'} = \{1\}.$$

[Die nicht regulären Gruppen mit dieser Eigenschaft sind die sog. *Frobeniusgruppen.]*

Beweis: Da nach Voraussetzung N imprimitiv auf Ω ist, gilt

$$\Omega = \dot{\bigcup_{1 \leq i \leq k}} B_i$$

mit N-Blöcken $B_i = \{\omega_{ij} \mid j = 1, \ldots, m\}$ der Mächtigkeit $1 < m < n := \#\Omega$. Für $\omega := \omega_{11}$ bildet N_ω den Block B_1 in sich ab. Nun ist nach Voraussetzung G_ω transitiv auf $\Omega \setminus \{\omega\}$ und $N_\omega = N \cap G_\omega$ Normalteiler in G_ω, also sind alle N_ω-Bahnen in $\Omega \setminus \{\omega\}$ als G_ω-Blöcke gleich lang. Ist diese Länge 1, so ist $N_\omega = \{1\}$ und die Behauptung gezeigt.

Seien nun also alle von $\{\omega\}$ verschiedenen N_ω-Bahnen von der Länge $l > 1$. (Man sagt: N ist $\frac{1}{2}$-*transitiv*.) Dann folgt aber $m = \#B_1 \equiv 1 \bmod l$, da N_ω den Block B_1 in sich abbildet und dieser ω enthält. Insbesondere sind l und m teilerfremd.

Wir betrachten nun die Mengen $N_\omega B_i$; diese sind Vereinigung von Blöcken B_j, also gilt

$$m \mid \#N_\omega B_i. \tag{1}$$

Andererseits ist

$$N_\omega B_i = \bigcup_{j=1}^{m} N_\omega \omega_{ij} \tag{2}$$

Vereinigung von N_ω-Bahnen, die im Falle $i > 1$ wegen $\omega_{ij} \neq \omega$ alle die Länge l haben, also erhält man

$$l \mid \#N_\omega B_i \quad \text{für } i > 1. \tag{3}$$

Wegen der Teilerfremdheit von l und m folgt damit sogar

$$lm \mid \#N_\omega B_i \quad \text{für } i > 1. \tag{4}$$

Dies bedeutet aber, daß die Vereinigung in (2) disjunkt sein muß, und daher gilt:

$$\bigwedge_{i>1} \bigwedge_{j} N_{\omega_{11}}\omega_{ij} \cap B_i = \{\omega_{ij}\}. \tag{5}$$

Diese Überlegungen gelten für jedes ω_{kl} statt ω_{11} genauso, also folgt

$$\bigwedge_{k\neq i,l,j} N_{\omega_{kl}}\omega_{ij} \cap B_i = \{\omega_{ij}\}. \tag{6}$$

Hieraus entnehmen wir nun

$$\rho \in N_{\alpha\beta} \wedge \alpha \in B_i \wedge \beta \notin B_i \implies \rho|_{B_i} = \mathrm{id}_{B_i}. \tag{7}$$

Denn zunächst gilt wegen der Block-Eigenschaft von B_i:

$$\rho(\alpha) = \alpha \in B_i \implies \rho B_i = B_i,$$

und damit folgt (7) aus (6):

$$\rho\{\omega_{ij}\} \underset{(6)}{=} \rho(N_\beta\omega_{ij} \cap B_i) = \rho N_\beta\omega_{ij} \cap \rho B_i = N_\beta\omega_{ij} \cap B_i \underset{(6)}{=} \{\omega_{ij}\}.$$

Insbesondere für $i = 1$ erhält man

$$\bigwedge_{\omega'\notin B_1} \bigwedge_{2\leq j\leq m} N_{\omega\omega'} \leq \mathrm{Fix}_N(B_1) := \{\sigma \in N \mid \bigwedge_{\alpha\in B_1} \sigma\alpha = \alpha\} \leq N_{\omega\omega_{1j}}. \tag{8}$$

Da alle N_ω-Bahnen außer $\{\omega\}$ die gleiche Länge l haben, folgt, daß auch alle Fixgruppen $N_{\omega\omega'}$ mit $\omega \neq \omega'$ gleichmächtig sind, so daß in (8) jeweils die Gleichheit gilt. Da es mindestens zwei Blöcke B_i gibt, folgt daraus die Behauptung:

$$\bigwedge_{\omega'\neq\omega} N_{\omega\omega'} = \{\mathrm{id}\}.$$

Die Struktur der Frobeniusgruppen klärt der folgende Satz. Er wird mit darstellungstheoretischen Methoden[4)] bewiesen (siehe dazu die Vorlesung über Darstellungstheorie, §4 e.).

(7.17) Satz: (Frobenius) *Sei G eine transitive Permutationsgruppe auf Ω mit $G_\omega \neq 1$ und $G_{\omega\omega'} = 1$ für alle $\omega \neq \omega'$, also eine Frobeniusgruppe. Dann bilden die fixpunktfreien Permutationen von G zusammen mit der Identität einen Normalteiler*

$$H := \{\sigma \in G \mid \bigwedge_{\omega\in\Omega} \sigma(\omega) \neq \omega\} \cup \{\mathrm{id}\} \lhd G,$$

und dieser operiert regulär auf Ω. Daher gilt außerdem

a) $G = H \rtimes G_\omega$ ist semidirektes Produkt von H mit G_ω.

b) $\#H = \#\Omega \equiv 1 \bmod \#G_\omega$.

c) H ist charakteristische Untergruppe von G.

Wir kommen zurück zum Beweis von Satz (7.15),b). Wie schon früher erwähnt (siehe Beweis von Satz (7.12),a) bzw. EGI, Satz (4.13)), ist der minimale Normalteiler N direktes Produkt $N = T_1 \times \ldots \times T_d$ von isomorphen einfachen Gruppen $T_i \simeq T$ $(i = 1, \ldots, d)$. Wir unterscheiden nun die beiden Fälle (1) N auflösbar und (2) N nicht auflösbar. Es gilt zunächst

$$\text{(1) } N \text{ auflösbar} \iff T \text{ abelsch} \iff N \text{ abelsch} \iff N \leq C_G(N) \iff C_G(N) \neq 1\,.$$

[4)] die nicht mehr in diese Vorlesung aufgenommen werden konnten

Für die letzte Äquivalenz beachte man, daß $C_G(N) \neq 1$ als Normalteiler den nach a) einzigen minimalen Normalteiler N enthalten muß. Für auflösbares N folgt aus (7.12) die Alternative (1) von Satz (7.15),b).

Liege also nun der komplementäre Fall (2) vor:

$$(2)\ N \text{ nicht auflösbar} \iff T \text{ nicht-abelsch} \iff N \text{ nicht abelsch} \iff C_G(N) = 1\,.$$

Nach (A) ist dann N nicht regulär und nach (B) primitiv. Damit sind die Normalteiler $T_i \lhd N$ transitiv. Wir wollen nun zeigen, dass $d = 1$ und damit $N = T$ nicht abelsch einfach ist.

Angenommen $d \geq 2$. Dann ist $1 \neq T_2 \leq C_N(T_1) \leq C := C_{\mathcal{S}}(T_1)$ und damit nach Lemma (7.13) $(T_2)_\omega \leq C_\omega = 1$. Also gilt $\#T = \#T_2 = \#\Omega =: n$ und $\#N = n^d$. Da N transitiv operiert, ist $(N : N_\omega) = n$ und daher $\#N_\omega = n^{d-1}$ für $\omega \in \Omega$.

Nun ist $N_\omega = G_\omega \cap N \lhd G_\omega$ und G_ω transitiv auf $\Omega \setminus \{\omega\}$, also haben nach Prop. (7.7) alle N_ω-Bahnen in $\Omega \setminus \{\omega\}$ gleiche Länge $l \geq 2$, so daß l ein Teiler von $\#(\Omega \setminus \{\omega\}) = n - 1$ ist und daher l, n teilerfremd sind.

Als Bahnenlänge von N_ω ist l aber auch ein Teiler von $\#N_\omega = n^{d-1}$. Dies ergibt für $d \geq 2$ einen Widerspruch zur Teilerfremdheit von l und n, also ist $d = 1$ und $N = T$ eine nicht-abelsche einfache Gruppe.

Da im Fall (2) $C_G(N) = 1$ ist, hat die Operation von G auf N durch Konjugation einen trivialen Kern, d. h. $G \leq \mathrm{Aut}(N)$. □

Damit ist Satz (7.15) vollständig auf Satz (7.17) zurückgeführt. Dieser sollte im Kap. III über Darstellungstheorie bewiesen werden.

d. Transitive Untergruppen kleineren Grades

Ist G eine Permutationsgruppe auf Ω, $\Omega_1 \subseteq \Omega$ eine Teilmenge von Ω und U eine Untergruppe von G, so führen wir folgende Bezeichnung ein:

$$U|_{\Omega_1} := \{\sigma|_{\Omega_1} \mid \sigma \in U\}.$$

Dies ist eine Menge von Abbildungen $\Omega_1 \to \Omega$; genau dann ist es eine Permutationsgruppe $\leq \mathcal{S}(\Omega_1)$, wenn Ω_1 U-stabil ist.

Wir beweisen zunächst das folgende nützliche Primitivitätskriterium

(7.18) Proposition: *Sei G eine transitive Permutationsgruppe auf Ω. Es seien $U_1, U_2 \leq G$ Untergruppen mit $G = \langle U_1, U_2\rangle$ und $\Omega_i \subset \Omega$ $(i = 1, 2)$ U_i-Bahnen mit $\Omega = \Omega_1 \cup \Omega_2$. Sind dann die Permutationsgruppen $U_i|_{\Omega_i} \leq \mathcal{S}(\Omega_i)$ (i=1,2) primitiv, so ist G primitiv auf Ω.*

Beweis: Wegen der Transitivität von $G = \langle U_1, U_2\rangle$ auf Ω gilt

$$\Omega_1 \cap \Omega_2 \neq \emptyset, \tag{$*$}$$

denn wäre $\Omega = \Omega_1 \dot\cup \Omega_2$ disjunkt, so wäre Ω_1 nicht nur unter U_1 stabil, sondern wegen $\Omega_1 = \Omega \setminus \Omega_2$ auch unter U_2, also unter ganz G. Da G aber transitiv auf Ω operieren soll, folgt $\Omega_1 = \Omega$ und $\Omega_2 = \emptyset$, im Widerspruch zu den Voraussetzungen.

Nach $(*)$ muß eine der beiden Mengen Ω_i die Bedingung $\#\Omega_i > \#\Omega/2$ erfüllen, und die Behauptung ergibt sich aus nachfolgendem

(7.19) Hilfssatz: *Sei $G \leq \mathcal{S}(\Omega)$ eine transitive Permutationsgruppe auf Ω und $U \leq G$ eine Untergruppe. Es sei $\Omega_1 \subseteq \Omega$ ein U-Orbit und $U|_{\Omega_1}$ primitiv auf Ω_1. Ist dann $\#\Omega_1 > \#\Omega/2$, so operiert G primitiv auf Ω.*

Beweis: Es sei B ein Block für G mit $1 \leq \#B < \#\Omega$. Dann ist $B_1 := B \cap \Omega_1$ ein Block für $U|_{\Omega_1}$: Sei nämlich $\tau \in U$ und $B_1 \cap \tau B_1 \neq \emptyset$. Dann gilt erst recht $B \cap \tau B \neq \emptyset$ und damit $B = \tau B$. Also erhält man

$$\tau B_1 = \tau(B \cap \Omega_1) = \tau B \cap \tau\Omega_1 = B \cap \Omega_1 = B_1.$$

Damit ist $B_1 = \Omega_1 \cap B$ ein $U|_{\Omega_1}$-Block, also gilt nach Voraussetzung entweder $B_1 = \Omega_1$ oder $\#B_1 \leq 1$. Im ersten Falle folgt $\Omega_1 \subseteq B$ und damit

$$\#\Omega/2 < \#\Omega_1 \leq \#B < \#\Omega,$$

im Widerspruch zu $\#B \mid \#\Omega$.

Also ist für alle Blöcke σB der Schnitt $\sigma B \cap \Omega_1$ höchstens einpunktig. Da die Blöcke σB ganz Ω überdecken, muß es daher mindestens $\#\Omega_1$ verschiedene davon geben und man erhält

$$\#B\#\Omega_1 \leq \#\Omega < 2\#\Omega_1,$$

woraus $\#B = 1$ folgt. G ist also primitiv.

(7.20) Satz: (Jordan) *Es sei $G \leq \mathcal{S}(\Omega)$ primitiv und $\Omega = \Omega_1 \dot\cup \Omega_2$ eine disjunkte Zerlegung von Ω mit $2 \leq \#\Omega_1$ und $1 \leq \#\Omega_2$.*
Operiert die Fixgruppe $G_{\Omega_2} = \{\rho \in G \mid \rho|_{\Omega_2} = \mathrm{id}_{\Omega_2}\}$ transitiv auf Ω_1, so gilt:

a) G ist 2-fach transitiv auf Ω.

b) Ist G_{Ω_2} sogar primitiv auf Ω_1, so ist G 2-fach primitiv, d. h. G_ω ist primitiv.

Der *Beweis* erfolgt durch Induktion über $\#\Omega_2$. Im Fall $\#\Omega_2 = 1$ ist nichts zu zeigen. Sei also nun $\#\Omega_2 \geq 2$.

1. Fall: $\#\Omega_2 < \#\Omega/2$, also $\#\Omega_1 > \#\Omega/2$. Dann folgt

$$\bigwedge_{\sigma \in G} \sigma\Omega_1 \cap \Omega_1 \neq \emptyset. \tag{1}$$

Wegen der Transitivität von G_{Ω_2} auf Ω_1, und daher der von $\sigma G_{\Omega_2}\sigma^{-1}$ auf $\sigma\Omega_1$, folgt aus (1) für alle $\sigma \in G$

$$H := \langle G_{\Omega_2}, \sigma G_{\Omega_2}\sigma^{-1}\rangle \text{ operiert transitiv auf } \Omega_1' := \Omega_1 \cup \sigma\Omega_1. \tag{2}$$

Das Komplement $\Omega_2' := \Omega \setminus \Omega_1' = \Omega_2 \cap \sigma\Omega_2$ wird offensichtlich von H fixiert, also gilt $H \leq G_{\Omega_2'}$ und wir erhalten aus (2) für jedes σ

$$\Omega = \Omega_1' \dot\cup \Omega_2' \quad \text{und} \quad G_{\Omega_2'} \text{ operiert transitiv auf } \Omega_1'\,. \tag{3}$$

Weiter gilt offensichtlich

$$2 \leq \#\Omega_1' \quad \text{und} \quad \#\Omega_2' \leq \#\Omega_2. \tag{4}$$

Wir wollen nun $\sigma \in G$ so wählen, daß

$$1 \leq \#\Omega_2' < \#\Omega_2 \tag{5}$$

gilt und die Induktionsvoraussetzung für $\Omega = \Omega_1' \dot\cup \Omega_2'$ angewendet werden kann. Dazu benutzen wir das nachfolgende

(7.21) Lemma: *Sei $G \leq \mathcal{S}(\Omega)$ eine primitive Permutationsgruppe, $\emptyset \neq \Omega_0 \subsetneq \Omega$ und $a \neq b$ beliebige Elemente in Ω. Dann gibt es ein $\sigma \in G$ mit $a \in \sigma\Omega_0$ und $b \notin \sigma\Omega_0$.*

Wir stellen den Beweis vorläufig zurück und wenden das Lemma zunächst auf $\Omega_0 = \Omega_2$ und zwei verschiedene Elemente $a, b \in \Omega_2$ an. (Es ist $\#\Omega_2 \geq 2$!) Für ein $\sigma \in G$ mit den Eigenschaften aus Lemma (7.21) gilt dann (5), denn $a \in \Omega_2'$ und $b \in \Omega_2 \setminus \Omega_2'$.

Ad (7.20) a): Wegen (3)–(5) sind die Voraussetzungen von (7.20) für die Zerlegung $\Omega = \Omega_1' \dot\cup \Omega_2'$ erfüllt. Außerdem gilt $\#\Omega_2' < \#\Omega_2$, so daß nach Induktionsvoraussetzung die Behauptung folgt.

Ad (7.20) b): Hier schließen wir genauso, nachdem wir gezeigt haben:

$$H := \langle G_{\Omega_2}, \sigma G_{\Omega_2}\sigma^{-1}\rangle \text{ operiert primitiv auf } \Omega_1' := \Omega_1 \cup \sigma\Omega_1. \tag{6}$$

Aus der Voraussetzung von b) folgt dies aber genau mit Proposition (7.18), angewendet auf die nach (2) transitive Permutationsgruppe $H|_{\Omega_1'}$.

Wir kommen nun zum *2. Fall* von (7.20): $\#\Omega \leq 2\#\Omega_2$, also $2\#\Omega_1 \leq \#\Omega$.

Jetzt wenden wir Lemma (7.21) an auf $\Omega_0 = \Omega_1$ und zwei verschiedene Elemente $a, b \in \Omega_1$. (Hier wird die Voraussetzung $\#\Omega_1 \geq 2$ von Satz (7.20) benutzt.) Sei also $\sigma \in G$ mit $a \in \sigma\Omega_1$ und $b \notin \sigma\Omega_1$. Dann folgt $a \in \Omega_1 \cap \sigma\Omega_1 \neq \emptyset$, so daß wieder gilt:

$$H := \langle G_{\Omega_2}, \sigma G_{\Omega_2} \sigma^{-1} \rangle \text{ operiert transitiv auf } \Omega_1' := \Omega_1 \cup \sigma\Omega_1. \tag{7}$$

Aus $\Omega_1 \cap \sigma\Omega_1 \neq \emptyset$ folgt

$$1 < \#\Omega_1 \leq \#\Omega_1' = \#(\Omega_1 \cup \sigma\Omega_1) < 2\#\Omega_1 \leq \#\Omega. \tag{8}$$

Wegen $b \in \Omega_1$ und $b \notin \sigma\Omega_1$ gilt $\Omega_1 \subsetneq \Omega_1'$, also mit $\Omega_2' := \Omega \setminus \Omega_1'$

$$1 \leq \#\Omega_2' < \#\Omega_2, \tag{9}$$

so daß man wie im ersten Fall weiterschließt.

Wir kommen nun zum *Beweis* von Lemma (7.21). Für das gegebene Ω_0 und $a \in \Omega$ setzen wir

$$B := \bigcap_{\substack{\sigma \in G \\ a \in \sigma\Omega_0}} \sigma\Omega_0 \,.$$

Wegen der Transitivität von G gibt es wenigstens ein σ mit $a \in \sigma\Omega_0$, so daß tatsächlich ein Durchschnitt gebildet wird und $a \in B \neq \Omega$ gilt. Wir zeigen nun, daß B ein G-Block ist. Wegen der Primitivität von G muß dann $B = \{a\}$ sein und die Behauptung folgt.

Wir müssen für beliebige $\tau \in G$ zeigen: $B \cap \tau B \neq \emptyset \implies B = \tau B$. Wir zeigen zunächst

$$a \in B \cap \tau B \implies B = \tau B \,. \tag{1}$$

Beweis: $a \in \tau B = \bigcap_{\sigma\Omega_0 \ni a} \tau\sigma\Omega_0$ bedeutet

$$a \in \sigma\Omega_0 \implies a \in \tau\sigma\Omega_0. \tag{2}$$

Also werden bei der Durchschnittsbildung in $\tau B = \bigcap_{\sigma\Omega_0 \ni a} \tau\sigma\Omega_0$ nur Mengen $\tau\sigma\Omega_0 =: \rho\Omega_0$ erfaßt, für die $a \in \rho\Omega_0$ gilt, so daß der Durchschnitt über *alle* solche $\rho\Omega_0$ noch kleiner ist:

$$\tau B = \bigcap_{\sigma\Omega_0 \ni a} \tau\sigma\Omega_0 \supset \bigcap_{\rho\Omega_0 \ni a} \rho\Omega_0 = B. \tag{3}$$

Da B und τB gleichmächtig sind, folgt die Behauptung $B = \tau B$ von (1).

Im allgmeinen Fall wählen wir zu $c \in B \cap \tau B$ ein $\rho \in G$ mit $\rho c = a$, also

$$a \in B \cap \rho B \cap \rho\tau B. \tag{4}$$

Mit (1) folgt dann daraus $\rho B = B$ und $\rho\tau B = B$, also $B = \tau B$, womit Lemma (7.21) bewiesen ist. □

So wie man mehrfache Transitivität rekursiv über die Fixgruppen einzelner Ziffern beschreiben kann (siehe Prop. (7.10),a)), so definiert man die sog. *mehrfach primitiven* Permutationsgruppen rekursiv durch:

1-fach primitiv bedeutet dasselbe wie primitiv,

und für $n \geq 2$ heißt G n-fach primitiv, wenn G transitiv und die Fixgruppe G_ω irgendeiner Ziffer ω $(n-1)$-fach primitiv ist.

Aus Prop. (7.9) entnimmt man die Implikationen

$$(k+1)\text{-fach primitiv} \implies k\text{-fach primitiv} \implies k\text{-fach transitiv.}$$

(7.22) Satz: (Jordan) *Sei G eine primitive Permutationsgruppe auf Ω und Ω_1 eine Teilmenge mit $1 < \#\Omega_1 =: m < n := \#\Omega$. Operiert nun $G_{\Omega\setminus\Omega_1}$ primitiv auf Ω_1, so operiert G sogar $(n-m+1)$-fach primitiv auf Ω.*

Beweis: Wir schließen induktiv über $\#\Omega - \#\Omega_1 = n - m$.
Nach (7.20),b) folgt aus den Voraussetzungen in jedem Falle: G ist 2-fach primitiv. Für $n-m = 1$ ist daher nichts mehr zu zeigen.

Sei nun $n-m \geq 2$ und $\omega \in \Omega\setminus\Omega_1$. $G' := G_\omega$ operiert primitiv auf $\Omega' := \Omega\setminus\{\omega\}$ und $\Omega_1 \subset \Omega'$. Wegen $m \leq n-2$ gilt außerdem

$$1 < \#\Omega_1 = m < \#\Omega' = n-1\,.$$

Schließlich gilt

$$G'_{\Omega'\setminus\Omega_1} = G_{\{\omega\}\cup\Omega'\setminus\Omega_1} = G_{\Omega\setminus\Omega_1}\,.$$

Nach Voraussetzung operiert $G_{\Omega\setminus\Omega_1}$ primitiv auf Ω_1, so daß alle Voraussetzungen von (7.22) für G', Ω', Ω_1 erfüllt sind. Wegen $\#\Omega' - \#\Omega_1 = n-1-m < n-m$ folgt aus der Induktionsvoraussetzung, daß $G' = G_\omega$ $(n-1-m)$-fach primitiv auf Ω', also G $(n-m)$-fach primitiv auf Ω operiert. □

(7.23) Korollar: *G operiere primitiv auf n Objekten und enthalte einen p-Zyklus für eine Primzahl p. Dann ist G $(n-p+1)$-fach primitiv.*
Speziell: Ist $p = 2$, so ist G die volle symmetrische Gruppe: $G = \mathcal{S}_n$.
Ist $p = 3$, so umfaßt G die alternierende Gruppe: $G \supseteq A_n$.

Beweis: Sei $\sigma \in G$ ein p-Zyklus und Ω_1 seine Bahn, also $\#\Omega_1 = p$. σ operiert transitiv, nach (7.5) also primitiv auf Ω_1. Wegen $\sigma\,|_{\Omega\setminus\Omega_1} = \mathrm{id}$, also $\sigma \in G_{\Omega\setminus\Omega_1}$ sind die Voraussetzungen von (7.22) erfüllt, und die Behauptung folgt.

Der erste Zusatz ist ebenfalls klar, denn für $p = 2$ ist G $(n-1)$-fach transitiv. Bei Operation auf n Objekten muß G dann aber n-fach transitiv und damit $\mathcal{S}_n$ sein.

Sei nun $p = 3$, also G $(n-2)$-fach transitiv auf n Elementen und folglich $n!/2$ ein Teiler von $\#G$ (Proposition (7.10),b)). Ist $n \geq 5$, so ist G 3-fach transitiv, so daß mit dem 3-Zyklus σ *sämtliche* 3-Zyklen in G liegen. Da diese die alternierende Gruppe A_n erzeugen, ist die Behauptung gezeigt. Es bleibt nun nur noch der Fall $n = 4$ zu untersuchen. Wäre $N := G \cap A_4 \subsetneq A_4$, so hätte N die Ordnung 6 (wegen $(\mathcal{S}_4 : G) \leq 2$) und wäre Normalteiler in $\mathcal{S}_4$. Damit wäre die 3-Sylowgruppe von N als charakteristische Untergruppe von N Normalteiler in $\mathcal{S}_4$, aber $\mathcal{S}_4$ hat mehrere 3-Sylowgruppen. Also muß $N = A_4$, d. h. $A_4 \subseteq G$ gelten.

Es sei angemerkt, daß man unter Benutzung der Einfachheit von A_n für $n \geq 5$ bereits aus der Tatsache $(\mathcal{S}_n : G) = 2$ folgern kann, daß $G = A_n$ ist. Es gilt sogar der folgende interessante

Satz: (Bochert) *Ist $G \leq \mathcal{S}_n$ eine primitive Permutationsgruppe und der Index $(\mathcal{S}_n : G) < [(n+1)/2]!$, so umfaßt G bereits die alternierende Gruppe A_n.*

Zum *Beweis* siehe etwa B. Huppert, Endliche Gruppen I, Kap. II, Satz (4.6).

§8 Matrixgruppen

a. Transvektionen

Bekanntlich sind die alternierenden Gruppen $\mathcal{A}_n$ für $n \geq 5$ einfache Gruppen (siehe Vorlesung Algebra, Satz (2.7). Weitere unendliche Serien einfacher Gruppen liefern die Matrixgruppen über endlichen Körpern.

Es sei K ein Körper, $M_n(K)$ der Ring der quadratischen $n \times n$-Matrizen und $\mathrm{GL}_n(K) := M_n(K)^\times$ die Einheitengruppe, die *allgemeine lineare* Gruppe n-ten Grades über dem Körper K. Nun ist $\det : \mathrm{GL}_n(K) \to K^\times$ ein Epimorphismus, dessen Kern die *spezielle lineare* Gruppe $\mathrm{SL}_n(K)$ ist. Es bezeichne E_n die n-reihige Einheitsmatrix. Dann bilden die *Skalarmatrizen* αE_n ($\alpha \in K^\times$) das Zentrum von $\mathrm{GL}_n(K)$. Die Faktorgruppe $\mathrm{PGL}_n(K) := \mathrm{GL}_n(K)/\mathrm{Zentr}(\mathrm{GL}_n(K))$ ist die *projektive allgemeine* Gruppe n-ten Grades; sie ist die Gruppe der projektiven Selbstabbildungen des $(n-1)$-dimensionalen projektiven Raumes $\mathbb{P}^{n-1}K$. Das Bild von $\mathrm{SL}_n(K)$ unter der natürlichen Abbildung $\mathrm{GL}_n(K) \to \mathrm{PGL}_n(K)$ wird mit $\mathrm{PSL}_n(K)$ bezeichnet, die *projektive spezielle* Gruppe n-ten Grades über K. Wir haben dann das folgende kommutative Diagramm von Gruppenhomomorphismen mit exakten[5)] Zeilen und Spalten:

$$\begin{array}{ccccc}
\mu_n(K) & \hookrightarrow & K^\times & \overset{(\ldots)^n}{\twoheadrightarrow} & K^{\times n} \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{SL}_n(K) & \hookrightarrow & \mathrm{GL}_n(K) & \overset{\det}{\twoheadrightarrow} & K^\times \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{PSL}_n(K) & \hookrightarrow & \mathrm{PGL}_n(K) & \overset{\overline{\det}}{\twoheadrightarrow} & K^\times/K^{\times n}
\end{array}$$

Darin bezeichnet $\mu_n(K)$ die Gruppe *der in K enthaltenen* n-ten Einheitswurzeln und $\overline{\det}$ den durch die Determinante induzierten Epimorphismus $\mathrm{PGL}_n(K) \twoheadrightarrow K^\times/K^{\times n}$. Ist nun $K = \mathbb{F}_q = \mathbb{F}_{p^f}$ ein endlicher Körper, so sind alle auftretenden Gruppen endlich, und man liest aus diesem Diagramm leicht das folgende Resultat ab. Dabei schreibt man statt $\mathrm{GL}_n(\mathbb{F}_{p^f})$ kurz $\mathrm{GL}(n, p^f)$.

(8.1) Proposition: *Es gilt für eine beliebige Primzahl p und natürliche Zahlen $n, f \in \mathbb{N}$:*

a) $\#\mathrm{GL}(n,p^f) = \prod_{i=0}^{n-1}(p^{nf} - p^{if}) = (p^{nf}-1)(p^{nf}-p^f)\ldots(p^{nf}-p^{(n-1)f})$.

b) $\#\mathrm{SL}(n,p^f) = \#\mathrm{PGL}(n,p^f) = \#\mathrm{GL}(n,p^f)/(p^f-1) = p^{(n-1)f}\prod_{i=0}^{n-2}(p^{nf}-p^{if})$.

c) $\#\mathrm{PSL}(n,p^f) = \#\mathrm{SL}(n,p^f)/\mathrm{ggT}(n,p^f-1)$.

Beweis: Wir zählen zunächst die Elemente der im Zentrum des obigen Diagramms stehenden allgemeinen linearen Gruppe $\mathrm{GL}(n,p^f)$ folgendermaßen ab: Eine Matrix A in $\mathrm{GL}(n,p^f)$ ist eindeutig durch n linear unabhängige Vektoren $a_1, \ldots, a_n$ (etwa die Zeilen) gegeben. Dabei kann a_1 beliebig in $\mathbb{F}_q^n \setminus \{0\}$ gewählt werden, dann wählt man a_2 beliebig in $\mathbb{F}_q^n \setminus \langle a_1\rangle$, und allgemein a_{i+1} beliebig in $\mathbb{F}_q^n \setminus \oplus_{j=1}^{i}\mathbb{F}_q a_j$. Dies ergibt genau die Behauptung a).

Den Rest liest man aus obigem kommutativem Quadrat ab:
Für b) beachtet man $\#\mathrm{SL}(n,p^f) = \#\mathrm{GL}(n,p^f)/\#\mathbb{F}_q^\times = \#\mathrm{GL}(n,p^f)/(p^f-1)$, während man für c) $\#\mu_n(\mathbb{F}_q)$ zu berechnen hat. $\mu_n(\mathbb{F}_q)$ ist die Menge der Elemente in $\mathbb{F}_q^\times$, deren Ordnung n teilt, deren Ordnung also $\mathrm{ggT}(n, q-1)$ teilt. Nun ist $\mathbb{F}_q^\times$ zyklisch von der Ordnung $q-1$ (siehe Algebra, Satz II.3.8) und darin gibt es genau eine Untergruppe der Ordnung $\mathrm{ggT}(n,q-1)$, die dann mit $\mu_n(\mathbb{F}_q)$ übereinstimmt: $\#\mu_n(\mathbb{F}_q) = \mathrm{ggT}(n,q-1)$. Die Exaktheit der ersten Spalte des Diagramms liefert dann c).

[5)] Wir erinnern an EGI Def. (3.2): Eine Sequenz von Gruppenhomomorphismen $H \overset{\varphi}{\to} G \overset{\psi}{\to} \mathfrak{g}$ heißt exakt, wenn φ injektiv, ψ surjektiv und $\mathrm{Ke}\,\psi = \mathrm{Im}\,\varphi$ ist. Bei endlichen Gruppen folgt nach dem Homomorphiesatz $\#G = \#H \cdot \#\mathfrak{g}$.

Man entnimmt dem obigen Diagramm außerdem, daß bis auf $\mathrm{PSL}(n, p^f)$ alle genannten Matrixgruppen nichttriviale Normalteiler besitzen. Wir wollen im folgenden $\mathrm{PSL}(n, p^f)$ genauer untersuchen. Ein wichtiges Hilfsmittel sind dabei spezielle Erzeugende der speziellen linearen Gruppe $\mathrm{SL}(n, p^f)$, die sog. *Transvektionen*.

(8.2) Definition: Eine *Transvektion* eines endlich-dimensionalen K-Vektorraumes V ist ein Endomorphismus t, zu dem eine Hyperebene $H \subset V$ existiert, so daß gilt:

a) $t\,|_H = \mathrm{id}$, und

b) der von t auf $\bar{V} := V/H$ induzierte Endomorphismus $\bar{t}$ ist ebenfalls die Identität: $\bar{t} = \mathrm{id}_{\bar{V}}$.

Offenbar sind Transvektionen Automorphismen von V mit der Determinante 1, liegen also in $\mathrm{SL}(V)$. Die Transvektionen zu einer festen Hyperebene H bilden eine zu H isomorphe abelsche Untergruppe von $\mathrm{SL}(V)$, denn: Ergänzt man eine Basis $v_1, \ldots, v_{n-1}$ von H durch einen Vektor v_n zu einer Basis von V, so ist jede Transvektion t mit $t\,|_H = \mathrm{id}$ durch $t(v_n)$ festgelegt. Wegen $\bar{t} = \mathrm{id}$ gilt $v_n - t(v_n) =: a_t \in H$ und die Zuordnung $t \mapsto a_t$ liefert den behaupteten Isomorphismus: $a_{s \circ t} = a_s + a_t$.

Eine nützliche Beschreibung von t durch a_t erhält man, indem man eine Linearform $\mu : V \to K$ mit H als Kern und $\mu(v_n) = 1$ wählt. Dann beschreibt sich t wie folgt: $t(v) = v - \mu(v)a_t$. Die Gesamtheit der Transvektionen zu $H = \mathrm{Ke}\ \mu$ ist also gegeben durch

$$t_{\mu,a} : V \to V\ ,\ v \mapsto t_{\mu,a}(v) = v - \mu(v)a,$$

wobei a ganz H durchläuft.

Aus der Definition entnimmt man außerdem sofort, daß die Konjugierten von Transvektion unter beliebigen Automorphismen von V wieder Transvektionen sind. Es gilt folgende explizite Formel für μ und a wie oben und $\sigma \in \mathrm{GL}(V)$:

$$t^{\sigma}_{\mu,a} = \sigma^{-1} \circ t_{\mu,a} \circ \sigma = t_{\mu \circ \sigma, \sigma^{-1} a}$$

(8.3) Satz: *Sei V ein endlich-dimensionaler Vektorraum über einem Körper K. Dann wird die spezielle lineare Gruppe $\mathrm{SL}(V)$ von den Transvektionen erzeugt.*

Beweis: Der Beweis erfolgt durch Induktion über $n = \dim V$. O. E. sei $n \geq 2$. Es bezeichne $\mathcal{T}$ die von allen Transvektionen erzeugte Untergruppe von $\mathrm{SL}(V)$. Diese ist, wie oben bemerkt, Normalteiler in $\mathrm{SL}(V)$. Sei nun $\sigma \in \mathrm{SL}(V)$ beliebig vorgegeben. Dann gilt

$$\bigvee_{\tau \in \mathrm{SL}(V)} \bigvee_{0 \neq v \in V} \mathcal{T}\sigma = \mathcal{T}\tau \wedge \tau(v) = v. \tag{1}$$

Zum Beweis von (1) betrachten wir zunächst den *1. Fall:* $v, \sigma v$ linear unabhängig für ein $v \in V$. Wir wählen dann eine Linearform μ auf V mit

$$\mu(\sigma v - v) = 0\ ,\ \mu(\sigma v) = 1. \tag{2}$$

Zu diesem μ betrachten wir die Transvektion $t := t_{\mu, \sigma v - v}$ und erhalten

$$t(\sigma v) = \sigma v - \mu(\sigma v)(\sigma v - v) = v, \tag{3}$$

so daß $\tau = t \circ \sigma$ und der Vektor v die Bedingungen in (1) erfüllen.

Im *2. Fall:* $\sigma v \in Kv$ für alle $v \in V$ wähle man zu einem beliebigen $v \in V \setminus \{0\}$ einen davon linear unabhängigen Vektor w. Da σ ein Automorphismus von V ist, folgt

$$\sigma w \notin Kv. \tag{4}$$

Ist nun μ eine Linearform von V mit $\mu(v) = 1$ und $\mu(w) = 0$, und $t = t_{\mu,w}$, so gilt

$$\sigma t(v) = \sigma(v - \mu(v)w) = \sigma(v - w) \notin Kv.$$

Damit liegt für $\sigma \circ t$ der 1. Fall vor und es gilt

$$\mathcal{T}\sigma t = \mathcal{T}\tau\,,\ \tau v = v. \tag{5}$$

Wegen $t \in \mathcal{T}$ und der Normalteilereigenschaft von $\mathcal{T}$ gilt $\mathcal{T}\sigma t = \mathcal{T}\sigma$, so daß aus (5) die Behauptung (1) folgt.

Seien nun $\tau \in \mathrm{SL}(V)$ und $v_1 := v \in V$ gemäß (1) gewählt. Dann induziert τ auf $\bar{V} := V/\langle v_1\rangle$ einen Automorphismus $\bar{\tau} \in \mathrm{SL}(\bar{V})$. Ist $n = 2$, also $\bar{V}$ 1-dimensional, so ist $\bar{\tau} = \mathrm{id}$ und τ damit eine Transvektion. Damit folgt $\sigma \in \mathcal{T}$. Sei nun also $n > 2$. Nach Induktionsvoraussetzung gibt es Transvektionen $\overline{t_i}$ von $\bar{V}$ mit $\bar{\tau} = \prod \overline{t_i}$. Zu jedem $\overline{t_i}$ gibt es Hyperebenen $\overline{H_i} = \mathrm{Ke}\ \overline{\mu_i}$, $\overline{\mu_i} : \bar{V} \to K$ und Vektoren $\overline{w_i} \in \overline{H_i}$ mit

$$\overline{t_i}(\bar{v}) = \bar{v} - \overline{\mu_i}(\bar{v})\overline{w_i}. \tag{6}$$

Seien H_i das volle Urbild von $\overline{H_i}$ unter dem Epimorphismus $p_1 : V \twoheadrightarrow \bar{V} = V/\langle v_1\rangle$, $w_i \in V$ irgendwelche Urbilder von $\overline{w_i} \in \bar{V}$ unter p_1 und $\mu_i = \overline{\mu_i} \circ p_1$ die natürliche Liftung von $\overline{\mu_i}$ auf V. Also ist $H_i = \mathrm{Ke}\ \mu_i$ eine Hyperebene in V, die v_1 und w_i enthält. Wir wählen nun die Transvektionen $t_i := t_{\mu_i,w_i}$ und erhalten:

$$t_i \in \mathcal{T} \text{ induziert auf } \bar{V} \text{ die Transvektion } \overline{t_i}. \tag{7}$$

Setzt man also

$$\rho := (\prod t_i)^{-1}\tau \in \mathcal{T}\tau, \tag{8}$$

so gilt

$$\rho(v_1) = v_1 \quad \text{und} \quad \bar{\rho} = \mathrm{id}_{\bar{V}}. \tag{9}$$

Ergänzt man v_1 zu einer Basis $v_1, \ldots, v_n$ von V, so existieren gemäß (9) $\beta_j \in K$ $(j = 2, \ldots, n)$ mit

$$\rho(v_1) = v_1 \quad \text{und} \quad \bigwedge_{j=2}^{n} \rho(v_j) = v_j - \beta_j v_1. \tag{10}$$

Dieses ρ ist nun selbst ein Produkt von Transvektionen: Sind $x_i : V \to K$ die Koordinatenfunktionen zur Basis v_i von V, so gilt:

$$\rho = \prod_{j=2}^{n} t_{x_j,\beta_j v_1}, \tag{11}$$

wie man leicht nachrechnet. Damit erhält man

$$\mathcal{T}\sigma \underset{(1)}{=} \mathcal{T}\tau \underset{(8)}{=} \mathcal{T}\rho \underset{(11)}{=} \mathcal{T},$$

also die Behauptung $\sigma \in \mathcal{T}$ von Satz (8.3). □

(8.4) Lemma: *Sei K ein Körper und $n \in \mathbb{N}_+$. Dann gilt: Beliebige Transvektionen $\neq \mathrm{id}$ sind in $\mathrm{GL}_n(K)$, für $n \geq 3$ sogar in $\mathrm{SL}_n(K)$ konjugiert.*

Beweis: Seien zwei Transvektionen $t_{\mu,a}$, $t_{\mu',a'}$ mit den üblichen Eigenschaften für μ, μ' und a, a' gegeben. Sind beide von der Identität verschieden, so gilt $a \neq 0 \neq a'$. Wir ergänzen nun a zu einer Basis $a_1 = a, a_2, \ldots, a_{n-1}$ von $H := \mathrm{Ke}\ \mu$ und wählen einen Vektor $b \in K^n$ mit $\mu(b) = 1$. Entsprechend verfahren wir mit den 'gestrichenen' Größen. Nun können wir ein $\sigma \in \mathrm{GL}_n(K)$ wählen mit $\sigma(a') = a$, $\sigma H' = H$ und $\sigma b' = b$. Für $n \geq 3$ ist σ mit diesen Eigenschaften offenbar bereits in $\mathrm{SL}_n(K)$ wählbar. Wegen $\sigma H' = H$ gilt $\mu \circ \sigma = \lambda\mu'$ für ein $\lambda \in K$. Nun gilt aber $1 = \mu(b) = \mu(\sigma b') = \lambda\mu'(b') = \lambda$, also $\mu \circ \sigma = \mu'$ und daher

$$t^{\sigma}_{\mu,a} = t_{\mu\circ\sigma,\sigma^{-1}a} = t_{\mu',a'}.$$

b. Die einfachen Gruppen $\mathrm{PSL}(n, p^f)$

Aufgrund der Resultate des vorigen Abschnittes bilden die Transvektionen in $\mathrm{SL}_n(K)$ eine ausgezeichnete Konjugationsklasse von Erzeugenden. Diese ist das wichtige Hilfsmittel in den folgenden Beweisen.

(8.5) Satz: *Sei K ein Körper und n eine natürliche Zahl. Ist $n \geq 3$ oder $n = 2$, $\#K > 3$, so gilt:*

$$\mathrm{GL}_n(K)' = \mathrm{SL}_n(K)' = \mathrm{SL}_n(K),$$

wobei $(...)'$ die Kommutatorgruppe bezeichne. Insbesondere ist $\mathrm{SL}_n(K)$ als perfekte Gruppe nicht auflösbar.

Beweis: Es ist $\mathrm{GL}_n(K)/\mathrm{SL}_n(K) \simeq K^\times$ abelsch, also

$$\mathrm{SL}_n(K)' \leq \mathrm{GL}_n(K)' \leq \mathrm{SL}_n(K), \tag{1}$$

so daß nur

$$\mathrm{SL}_n(K) \subseteq \mathrm{SL}_n(K)' \tag{2}$$

nachzuweisen ist. Wegen Satz (8.3) muß man also zeigen, daß jede Transvektion in der Kommutatorgruppe $\mathrm{SL}_n(K)'$ liegt. Da $\mathrm{SL}_n(K)'$ Normalteiler in $\mathrm{GL}_n(K)$ ist, genügt nach Lemma (8.4) der Nachweis, daß mindestens eine Transvektion $\neq \mathrm{id}$ in der Kommutatorgruppe $\mathrm{SL}_n(K)'$ liegt.

1. Fall: $n \geq 3$. Wir wählen eine Hyperebene H in $V := K^n$ und eine Linearform $\mu : V \to K$ mit $H = \mathrm{Ke}\ \mu$. Wegen $\dim H \geq 2$ kann man Vektoren $a_1, a_2 \in H$ wählen mit $a_1, a_2 \neq 0$ und $a_1 + a_2 \neq 0$. Dann gilt

$$t_{\mu,a_1} \circ t_{\mu,a_2} = t_{\mu,a_1+a_2} \tag{3}$$

und alle drei Transvektionen sind von der Identität verschieden.

Nun sind nach Lemma (8.4) je zwei Transvektionen $t, t' \neq \mathrm{id}$ in $\mathrm{SL}_n(K)$ konjugiert, ihre Restklassen in $\mathrm{SL}_n(K)^{\mathrm{ab}} = \mathrm{SL}_n(K)/\mathrm{SL}_n(K)'$ also gleich. Gemäß (3) ist diese Restklasse also ihr eigenes Quadrat und daher trivial.

2. Fall: $n = 2$ und $\#K > 3$. Sei zunächst $t \neq \mathrm{id}$ eine beliebige Transvektion. Dann existiert eine Basis v_1, v_2 von $V = K^2$ mit

$$tv_1 = v_1 \quad \text{und} \quad tv_2 = v_2 + v_1. \tag{4}$$

Wegen $\#K > 3$ können wir ein $d \in K$ wählen mit $0 \neq d^2 \neq 1$. Sei nun $\sigma \in \mathrm{SL}_2(K)$ definiert durch

$$\sigma v_1 = dv_1\,,\ \sigma v_2 = d^{-1}v_2. \tag{5}$$

Dann gilt

$$t^{-1}\sigma t\sigma^{-1}(v_1) = v_1 \text{ und } t^{-1}\sigma t\sigma^{-1}(v_2) = t^{-1}(v_2 + d^2v_1) \underset{(4)}{=} v_2 + (d^2 - 1)v_1. \tag{6}$$

Definiert man die Linearform $\mu : V \to K$ durch $\mu(v_1) = 0, \mu(v_2) = 1$, so ergibt sich aus (6)

$$t' := t_{\mu,(1-d^2)v_1} = t^{-1}\sigma t\sigma^{-1} \in \mathrm{SL}_2(K)'. \tag{7}$$

Wegen $d^2 \neq 1$ ist somit t' eine Transvektion $\neq \mathrm{id}$, die in $\mathrm{SL}_2(K)'$ liegt.

In beiden Fällen ist also eine Transvektion $t \neq \mathrm{id}$ in $\mathrm{SL}_n(K)'$ gefunden und Satz (8.5) bewiesen. □

Die Voraussetzungen von Satz (8.5) sind nicht entbehrlich, denn die Gruppen $\mathrm{SL}(2, 2)$ und $\mathrm{SL}(2, 3)$ sind auflösbar: Gemäß Proposition (8.1) hat $\mathrm{SL}(2, 2)$ die Ordnung 6, ist also auflösbar. (Es gilt $\mathrm{SL}(2, 2) \simeq S_3$.) Ebenfalls nach (8.1) hat die Gruppe $\mathrm{SL}(2, 3)$ die Ordnung 24 und als Faktorgruppe die Gruppe $\mathrm{PSL}(2, 3)$ von der Ordnung 12. Nun operiert $\mathrm{PSL}(2, 3)$ treu auf den 4 Punkten von $\mathbb{P}^1(\mathbb{F}_3)$ (den 4 Geraden von $\mathbb{F}_3^2$), ist also eine Permutationsgruppe vom Grade 4

und daher mit S_4 auflösbar. (Es gilt $\mathrm{PSL}(2,3) \simeq \mathcal{A}_4$, und damit ist $\mathrm{SL}(2,3)$ eine Erweiterung von C_2 mit der Gruppe $\mathcal{A}_4$.)

Zur Vorbereitung des Einfachheitsnachweises für die Gruppen $\mathrm{PSL}(n, p^f)$ (außer $\mathrm{PSL}(2,2)$ und $\mathrm{PSL}(2,3)$) bemerken wir:

(8.6) Bemerkung: *Es sei K ein Körper, q eine Primzahlpotenz und $n \geq 2$. Dann gilt:*

a) Die Gruppen $\mathrm{PSL}_n(K)$ operieren 2-fach transitiv auf dem projektiven Raum $\mathbb{P}^{n-1}K$.

b) $\mathrm{PSL}(n,q)$ operiert 2-fach transitiv auf den $(q^n-1)/(q-1) = 1 + q + \cdots + q^{n-1}$ Punkten von $\mathbb{P}^{n-1}\mathbb{F}_q$.

Beweis: Zwei verschiedene Punkte a_1, a_2 in $\mathbb{P}^{n-1}K$ sind nichts anderes als zwei verschiedene Geraden im K^n. Zu zwei Paaren von verschiedenen Geraden im K^n gibt es natürlich einen Automorphismus des K^n, der das eine Paar in das andere überführt. Damit ist a) bewiesen. Für b) hat man lediglich die Geraden im $\mathbb{F}_q$-Vektorraum $\mathbb{F}_q^n$ abzuzählen: $\mathbb{F}_q^n \setminus \{0\}$ ist disjunkte Vereinigung von Geraden ohne Nullpunkt, und jede Gerade ohne Nullpunkt besteht aus $q-1$ Punkten. Also erhält man die angegebene Zahl $\#(\mathbb{F}_q^n \setminus \{0\})/(q-1) = (q^n-1)/(q-1)$ von Geraden in $\mathbb{F}_q^n$.

Der angestrebte Beweis der Einfachheit der $\mathrm{PSL}(n,q)$ beruht auf dem nachfolgenden Einfachheitskriterium von Iwasawa.

(8.7) Lemma: (Iwasawa) *Eine primitive Permutationsgruppe G auf einer Menge Ω ist einfach, wenn folgende Bedingungen erfüllt sind:*

α) G ist perfekt, d. h. $G = G'$.

β) Es gibt einen auflösbaren Normalteiler $T \lhd G_\omega$ in der Fixgruppe irgendeiner Ziffer $\omega \in \Omega$, dessen sämtliche Konjugierten in G ganz G erzeugen:

$$\langle T^\sigma \mid \sigma \in G \rangle = G\,.$$

Beweis: Sei $1 \neq N \lhd G$ ein nicht-trivialer Normalteiler in G. Da G als primitiv vorausgesetzt ist, operiert N transitiv auf Ω (Prop. (7.7)), es gilt daher

$$G = NG_\omega = G_\omega N\,. \tag{1}$$

Wegen $T \lhd G_\omega$ erhalten wir daher aus Voraussetzung β)

$$G = \langle T^\sigma \mid \sigma \in G_\omega N \rangle = \langle T^\sigma \mid \sigma \in N \rangle \leq NT \leq G. \tag{2}$$

Da N Normalteiler ist, also $Nt = tN$ für alle $t \in T$, folgt unmittelbar $(NT)' \leq NT'$, so daß die Kommutatorreihe von G wegen der Auflösbarkeit von T bis N hinabsteigt:

$$G^{(k)} = (NT)^{(k)} \leq NT^{(k)} = N \quad \text{für ein } k \in \mathbb{N}. \tag{3}$$

Da nach Voraussetzung α) aber G perfekt ist, folgt $G = G^{(k)} \leq N$, womit die Einfachheit von G bewiesen ist. □

Wir kommen nun zum Hauptresultat dieses Abschnittes.

(8.8) Satz: *Außer* $\mathrm{PSL}(2,2)$ *und* $\mathrm{PSL}(2,3)$ *sind alle Gruppen* $\mathrm{PSL}(n,p^f)$ *einfach.*

Beweis: Wir wenden Lemma (8.7) auf $G = \mathrm{PSL}(n,p^f)$ mit seiner natürlichen, nach (8.6) und (7.9) primitiven, Operation auf $\Omega = \mathbb{P}^{n-1}\mathbb{F}_q$ $(q = p^f)$ an. Die Voraussetzung $\alpha)$ von (8.7) ist für G gemäß Satz (8.5) erfüllt. Für $\beta)$ wählen wir $a \in \mathbb{P}^{n-1}\mathbb{F}_q$ und $0 \neq w \in V := \mathbb{F}_q^n$ einen Repräsentanten von a. Es sei $T \leq G_a$ das Bild der folgenden Gruppe von Transvektionen

$$T(w) := \{t_{\mu,w} \mid \mu \in \mathrm{Hom}(V,K)\,,\ \mu(w) = 0\} \leq \mathrm{SL}(n,p^f)$$

unter der kanonischen Abbildung $\mathrm{SL}(n,p^f) \twoheadrightarrow \mathrm{PSL}(n,p^f)$. Wegen $t_{\mu,w} \circ t_{\mu',w} = t_{\mu+\mu',w}$ sind $T(w)$ und T abelsch. Aus $t_{\mu,w}^{\sigma} = t_{\mu\circ\sigma,\sigma^{-1}w}$ und $t_{\lambda\mu,w} = t_{\mu,\lambda w}$ für $\lambda \in \mathbb{F}_q$ folgert man, daß T Normalteiler in G_a ist. Schließlich erhält man daraus auch

$$\langle T(w)^{\sigma} \mid \sigma \in \mathrm{SL}(n,p^f)\rangle = \langle T(\sigma^{-1}w) \mid \sigma \in \mathrm{SL}(n,p^f)\rangle \underset{((8.3))}{=} \mathrm{SL}(n,p^f).$$

Die Konjugierten von T in G erzeugen daher G und die Voraussetzungen von Lemma (8.7) sind erfüllt. □

Die Gruppen $\mathrm{PSL}(n,p^f)$ stellen somit neben den alternierenden Gruppen eine zweite unendliche Serie von endlichen einfachen, nicht-abelschen Gruppen dar. Die genannten Gruppen sind im wesentlichen voneinander verschieden; die nachfolgend beschriebenen Isomorphien sind die einzigen zwischen ihnen (o. Beweis).

(8.9) Satz: *Zwischen den Gruppen* $\mathrm{PSL}(d,p^f)$ *und* $\mathcal{A}_n$ *bestehen folgende (und nur folgende) Isomorphien:*

a) $\mathrm{PSL}(2,2) \simeq \mathrm{SL}(2,2) \simeq \mathrm{GL}(2,2) \simeq S_3$.

b) $\mathrm{PSL}(2,3) \simeq \mathcal{A}_4$.

c) $\mathrm{PSL}(2,4) \simeq \mathrm{PSL}(2,5) \simeq \mathcal{A}_5$, *die einzige einfache Gruppe der Ordnung 60.*

d) $\mathrm{PSL}(2,7) \simeq \mathrm{PSL}(3,2)$ *ist die einzige einfache Gruppe der Ordnung 168.*

e) $\mathrm{PSL}(4,2) \simeq \mathcal{A}_8$.

f) $\mathrm{PSL}(2,9) \simeq \mathcal{A}_6$.

Beweis: Wir weisen nur die Existenz der behaupteten Isomorphien nach.
Alle in a) genannten Gruppen haben die Ordnung 6 und sind nicht abelsch.
b) $\mathrm{PSL}(2,3)$ hat die Ordnung 12 und liegt in S_4 (siehe oben).
c) $\mathrm{PSL}(2,4)$ und $\mathrm{PSL}(2,5)$ sind einfache Gruppen der Ordnung 60. Wir zeigen nun im nachfolgenden Satz (8.10), daß eine einfache Gruppe der Ordnung 60 isomorph zur alternierenden Gruppe $\mathcal{A}_5$ ist.
d) $\mathrm{PSL}(3,2)$ und $\mathrm{PSL}(2,7)$ sind einfache Gruppen der Ordnung 168, so daß die Behauptung ebenfalls aus Satz (8.10) folgt.

Die Beweise von e) und f) wollen wir hier nicht ausführen. e) kann z. B. bewiesen werden, indem man in $\mathrm{PSL}(4,2)$ 6 Matrizen angibt, die die Relationen der folgenden Präsentierung der $\mathcal{A}_8$ erfüllen:

$$\mathcal{A}_8 \simeq \langle x_1,\ldots,x_6 \mid x_1^3\,,\ x_i^2\,(2 \leq i \leq 6)\,,\ (x_ix_{i+1})^3\,,\ (x_ix_j)^2\,(i+1<j)\rangle.$$

Siehe etwa Huppert, Endliche Gruppen I, Kap. II, Satz 2.5.

Für f) benutzt man die vollständige Bestimmung aller Untergruppen der Gruppen $\mathrm{PSL}(2,p^f)$ gemäß Dickson (Huppert, l. c., Kap. II, Hauptsatz 8.27). Demzufolge besitzt $\mathrm{PSL}(2,9)$ eine

Untergruppe isomorph zu $\mathcal{A}_5$, also eine treue Permutationsdarstellung vom Grade 6. Wegen $\#\mathrm{PSL}(2,9) = 360$ muß dann $\mathrm{PSL}(2,9)$ mit $\mathcal{A}_6$ übereinstimmen.

(8.10) Satz: *a)* $\mathcal{A}_5$ *ist bis auf Isomorphie die einzige einfache Gruppe der Ordnung 60.*
b) $\mathrm{PSL}(2,7)$ *ist bis auf Isomorphie die einzige einfache Gruppe der Ordnung 168.*

Beweis: a) Sei G eine einfache Gruppe der Ordnung 60. Wir wollen einen Isomorphismus auf die alternierende Gruppe $\mathcal{A}_5$ konstruieren. Dazu genügt es zu zeigen:

$$G \text{ besitzt eine Untergruppe } U \text{ vom Index 5.} \qquad (*)$$

Ist nämlich U eine solche Untergruppe, so hat wegen der Einfachheit von G die Permutationsdarstellung auf den Nebenklassen von U trivialen Kern, also ist G isomorph zu einer Untergruppe vom Index 2 in S_5, und damit zu $\mathcal{A}_5$ (siehe Bemerkung nach Korollar (7.22)). [Mit denselben Überlegungen folgt, daß G keine echte Untergruppe mit einem Index ≤ 4 besitzen kann.]

Zum Beweis von $(*)$ betrachten wir für einen beliebigen Primteiler p von $60 = \#G$ den Normalisator $N_G(P)$ einer p-Sylowgruppe P von G. Wegen der Einfachheit von G sind diese Normalisatoren *echte* Untergruppen. Wäre nun $(*)$ falsch, so folgte für die Anzahl N_p der p-Sylowgruppen in G

$$N_p = (G : N_G(P)) > 5. \qquad (1)$$

Aus dem Sylowsatz $N_p \equiv 1 \bmod p$ und $N_p \mid 60$ erhält man dann

$$N_5 = 6\,,\ N_3 = 10 \ \text{ und } \ N_2 = 15. \qquad (2)$$

Angenommen zwei verschiedene 2-Sylowgruppen P_1, P_2 haben nicht-trivialen Schnitt

$$1 \neq D = P_1 \cap P_2. \qquad (3)$$

Wegen $\#P_i = 4$ sind die P_i abelsch, also $1 \neq D \lhd T := \langle P_1, P_2\rangle$, so daß T nicht ganz G sein kann. T enthält mehr als eine 2-Sylowgruppe, also mindestens 3 (Sylowsatz), und es folgt $\#T \geq (T\colon N_T(P_1)) \cdot \#P_1 \geq 12$, so daß G doch eine echte Untergruppe vom Index ≤ 5 besäße.

Die Annahme (3) war also falsch, so daß je zwei verschiedene 2-Sylowgruppen von G trivialen Durchschnitt haben. Damit enthält G $N_2 \cdot (4-1) = 45$ Elemente von 2-Potenzordnung $\neq 1$. Da G außerdem $N_5 \cdot (5-1) = 24$ Elemente der Ordnung 5 und $N_3 \cdot (3-1) = 20$ Elemente der Ordnung 3 enthält, kann G nicht die Ordnung 60 haben.

b) Sei G eine einfache Gruppe der Ordnung $\#G = 168 = 2^3 \cdot 3 \cdot 7$. Die Gruppe $\mathrm{PSL}(2,7)$ operiert 2-fach transitiv auf den 8 Punkten von $\mathbb{P}^1\mathbb{F}_7$. Wir wollen nun G ebenfalls als Untergruppe der S_8 darstellen und dann zeigen, daß bei passender Numerierung der 8 Punkte G mit $\mathrm{PSL}(2,7)$ übereinstimmt.

Da G einfach ist, hat G mehrere 7-Sylowgruppen, also ist nach üblichen Schlüssen deren Anzahl $N_7 = 8$. G besitzt daher eine transitive und – wegen der Einfachheit von G – treue Permutationsdarstellung vom Grade 8: $G \leq S_\Omega$ mit $\#\Omega = 8$.

Sei $P_7 = \langle\sigma\rangle$ eine 7-Sylowgruppe in G und $N_G(P_7) =: N$ der Normalisator. Dann gilt $(G : N) = N_7 = 8$ und folglich $\#N = 3 \cdot 7$. Als Element der Ordnung 7 operiert σ notwendig als 7-Zyklus auf den 8 Punkten von Ω, hat also genau einen Fixpunkt, der mit ∞ bezeichnet werden soll. Auch der Normalisator N muß dann diesen einzigen Fixpunkt ∞ von P_7 festlassen, operiert daher ebenfalls transitiv auf den verbleibenden 7 Punkten von $\Omega \setminus \{\infty\}$, die mit $\{0, 1, \ldots, 6\}$ bezeichnet werden sollen. Da N gerade den Index 8 hat, ist $N = G_\infty$ die volle Fixgruppe des Punktes ∞ in G. Als auflösbare transitive Permutationsgruppe von Primzahlgrad 7 ist N semidirektes Produkt von $P_7 \simeq \mathbb{F}_7$ mit der Fixgruppe $N_0 = \mathrm{Fix}_N(0)$ der Ziffer 0 in N, und diese ist Untergruppe von $\mathrm{Aut}\,\mathbb{F}_7 = \mathbb{F}_7^\times$ (Satz (7.12)).

Wegen $\#N_0 = 3$ ist diese Untergruppe gerade die Gruppe $\mathbb{F}_7^{\times 2} = \{1, 2, 4\}$ der Quadrate in $\mathbb{F}_7^\times$. Damit kann N als Permutationsgruppe identifiziert werden mit der folgenden Untergruppe von $\mathrm{AGL}(1,7)$:

$$N = \{\alpha x + \beta \in \mathrm{AGL}(1,7) \mid \alpha \in \mathbb{F}_7^{\times 2},\ \beta \in \mathbb{F}_7\}.$$

Nun ist $\mathrm{AGL}(1,7)$ Untergruppe in $\mathrm{PGL}(2,7)$, und zwar gerade die Fixgruppe des Punktes $\infty \in \mathbb{P}^1\mathbb{F}_7$. N läßt sich dann innerhalb $\mathrm{PGL}(2,7)$ beschreiben als

$$N = \{\varphi \in \mathrm{PGL}(2,7) \mid \varphi(\infty) = \infty \wedge \overline{\det}\,\varphi = \bar{1}\} = \{\varphi \in \mathrm{PSL}(2,7) \mid \varphi(\infty) = \infty\},$$

d. h. als Fixgruppe des Punktes ∞ in $\mathrm{PSL}(2,7)$.

Wir haben also Ω mit $\mathbb{P}^1\mathbb{F}_7 = \{0,\ldots,6,\infty\}$ und dadurch dann $N = G_\infty$ mit $\mathrm{PSL}(2,7)_\infty$ identifiziert. Wir wollen nun zeigen, daß die beiden Untergruppen G und $\mathrm{PSL}(2,7)$ von S_Ω übereinstimmen.

Sei $\tau = 2x \in \mathrm{PSL}(2,7)_\infty = N$. Dann ist $\langle\tau\rangle = P_3$ eine 3-Sylowgruppe in G. Sei $H := N_G(P_3)$ ihr Normalisator in G. Wir zeigen, daß der Index $N_3 := (G : H)$ durch 7 teilbar ist: Andernfalls wäre 7 eine Teiler von $\#H$, es gäbe also ein Element $\rho \in H$ der Ordnung 7. Dieses Element operiert durch Konjugation auf P_3; wegen $\#P_3 = 3$ und $\operatorname{ord}\rho = 7$ muß ρ trivial operieren. (Ließe ρ ein Element in P_3 nicht fest, so müßte ρ eine Bahn der Länge 7 haben.) Also sind ρ und τ vertauschbar, ihr Produkt hätte daher die Ordnung 21. Ein solches Element gibt es aber in der symmetrischen Gruppe S_8 nicht. Also war die Annahme falsch, und es gilt

$$7 \mid N_3 \mid 2^3 \cdot 7.$$

Zusammen mit $N_3 \equiv 1 \bmod 3$ (Sylowsätze) erhält man folgende Möglichkeiten:

$$N_3 = 7 \vee N_3 = 28.$$

Nehmen wir $N_3 = 7$ an, d. h. G hätte genau 7 verschiedene 3-Sylowgruppen. Aber bereits $N = \mathbb{F}_7 \cdot {\mathbb{F}_7^\times}^2$ hat 7 verschiedene 3-Sylowgruppen und wird von diesen erzeugt. Damit würde N von allen 3-Sylowgruppen von G erzeugt, wäre folglich Normalteiler in G, im Widerspruch zur Einfachheit von G.

Also gilt $N_3 = 28$ und daher $\#H = 6$. Sei α eine Involution in H.

1. Fall: $\tau^\alpha = \tau$. Dann ist $\tau\alpha \in H$ ein Element der Ordnung 6, also H zyklisch. Daher ist $\langle\tau\rangle$ die einzige Untergruppe der Ordnung 3 in H, und somit $H = N_G(\langle\tau\rangle) = N_G(H)$ sein eigener Normalisator. Damit enthält die Gruppe G folgende Elemente:

- $28 \cdot 2 = 56$ Elemente der Ordnung 6 in den 28 Konjugierten von H;
- $28 \cdot 2 = 56$ Elemente der Ordnung 3 in den 28 3-Sylowgruppen;
- $8 \cdot 6 = 48$ Elemente der Ordnung 7 in den 8 7-Sylowgruppen.

Damit bleiben in G nur noch 8 Elemente, die dann notwendig die einzige 2-Sylowgruppen bilden müssen. Wegen der Einfachheit von G ist dies nicht möglich.

2. Fall: $\tau^\alpha = \tau^{-1}$. Daraus folgt, daß α die Fixpunktmenge $\{0,\infty\}$ von $\tau = 2x$ in sich abbildet. Also gilt $\alpha(\mathbb{F}_7^\times) = \mathbb{F}_7^\times$, und aus $\alpha\tau = \tau^{-1}\alpha$ folgt für alle $\omega \in \mathbb{F}_7^\times \subset \mathbb{P}^1\mathbb{F}_7$

$$\alpha(2\omega) = \alpha \circ \tau(\omega) = \tau^{-1}(\alpha(\omega)) = \frac{1}{2}\alpha(\omega).$$

Als Element der Ordnung 2 läßt $\alpha \in G$ keinen Punkt von $\mathbb{P}^1\mathbb{F}_7$ fest, da die Fixgruppe eines beliebigen Punktes die Ordnung 21 hat. Also gilt in $\mathbb{F}_7$

$$1 \neq \alpha(1)\,,\ 2 \neq \alpha(2) = \frac{1}{2}\alpha(1)\,,\ 4 \neq \alpha(4) = \frac{1}{4}\alpha(1).$$

Daraus entnimmt man $\alpha(1) \neq 1, 4, 2$, oder mit anderen Worten

$$\alpha(1) \notin {\mathbb{F}_7^\times}^2. \qquad (*)$$

Man erhält also für α die folgende Zyklendarstellung:

$$\alpha = (0, \infty)\,(1, \alpha(1))\,(2, \alpha(1)/2)\,(4, \alpha(1)/4).$$

Daraus folgt unmittelbar

$$\alpha = \frac{\alpha(1)}{x} \in \mathrm{PGL}(2, 7).$$

Wegen $(*)$ ist $-\alpha(1) \in {\mathbb{F}_7^\times}^2$, also

$$\alpha = \frac{\alpha(1)}{x} \in \mathrm{PSL}(2, 7).$$

Wir betrachten nun die erzeugte Untergruppe $U := \langle \sigma, \tau, \alpha \rangle \subseteq G \cap \mathrm{PSL}(2, 7)$. Diese hat mindestens die Ordnung 42, also in G höchstens den Index 4. Dann besitzt G einen Normalteiler S (den Kern der Permutationsdarstellung von G auf den Nebenklassen von U), der in U liegt und in G höchstens den Index $4! = 24$ hat. Dies ist wegen der Einfachheit von G nur möglich, wenn $G = U$ gilt. Damit ist G Untergruppe der $\mathrm{PSL}(2, 7)$, wegen übereinstimmender Ordnungen also $G = \mathrm{PSL}(2, 7)$, und Satz (8.10) ist bewiesen. □