RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

ROLAND SCHMIDT

Untergruppenverbände involutorisch erzeugter Gruppen

Rendiconti del Seminario Matematico della Università di Padova, tome 63 (1980), p. 95-126

<http://www.numdam.org/item?id=RSMUP_1980__63__95_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 63 (1980)

Untergruppenverbände involutorisch erzeugter Gruppen.

ROLAND SCHMIDT (*)

Ziel dieser Note ist es, die Ergebnisse aus den Arbeiten [5], [6] und [7] über Projektivitäten endlicher involutorisch erzeugter Gruppen zu verbessern und auf unendliche Gruppen auszudehnen.

Es ist ziemlich klar (und wird in § 2 näher behandelt), daß die in diesen Arbeiten angewandte Methode—die Operation von Involutionen und ihrer Bilder unter Projektivitäten auf dem Untergruppenverband der Gruppe zu vergleichen — nicht sehr an der Endlichkeit der Gruppe hängt. Man muß nur die dort benutzten Hilfssätze über Bilder von Involutionen unter Projektivitäten, die für endliche Gruppen sehr einfach zu beweisen sind oder unmittelbar aus Suzukis Sätzen über singuläre Projektivitäten folgen, für beliebige Gruppen beweisen. Das tun wir in § 1 der Arbeit.

In § 3 behandeln wir mehrfach transitive Permutationsgruppen und zeigen, daß eine von Involutionen erzeugte dreifach transitive Permutationsgruppe vom Grade $\geqslant 4$ durch ihren Untergruppenverband bestimmt ist. Für zweifach transitive Permutationsgruppen können wir den Hauptsatz aus [5] nicht ganz auf unendliche Gruppen ausdehnen; wir beweisen aber ein Ergebnis (Satz 3.8), aus dem zum Beispiel folgt, daß die Gruppen $PSL(n, K)$ für $n \geqslant 3$ und beliebige Schiefkörper K durch ihren Untergruppenverband bestimmt sind.

(*) Indirizzo dell'A.: Mathematisches Seminar der Universität, 23 Kiel, Germania occidentale.

Die vorliegende Arbeit entstand aus Vorlesungen an der Universität von Trento im Oktober/November 1978. Für die Einladung dazu sowie die finanzielle Unterstützung sei Herrn Prof. Dr. G. Zacher sowie dem C.N.R. sehr herzlich gedankt.

In § 4 zeigen wir dasselbe für die Gruppen $PSL(2, K)$ und geben dann eine Anwendung unserer Methode des § 2 auf symplektische, orthogonale und unitäre Gruppen über Körpern.

1. – 2-reguläre und 2-singuläre Projektivitäten.

Eine *Projektivität* φ der Gruppe G auf die Gruppe H ist ein Isomorphismus des Untergruppenverbandes $\mathfrak{B}(G)$ von G auf den von H. Wir nennen φ 2-regulär, wenn φ Untergruppen der Ordnung 2 von G auf Untergruppen der Ordnung 2 in H abbildet; φ heißt *2-singulär*, wenn φ nicht 2-regulär ist. Eine *Diedergruppe* der Ordnung $2n$ ($n \in \mathbb{N} \cup \{\infty\}$) ist das semidirekte Produkt einer zyklischen Gruppe $\langle a \rangle$ der Ordnung n mit einer zyklischen Gruppe $\langle d \rangle$ der Ordnung 2 zum Automorphismus $a^d = a^{-1}$.

Wir wollen in diesem Abschnitt 2-singuläre Projektivitäten involutorisch erzeugter Gruppen studieren und untersuchen dazu zunächst die von zwei Involutionen erzeugten Gruppen, also die Diedergruppen.

LEMMA 1.1. *Sei* $n \in \mathbb{N} \cup \{\infty\}$, $G = \langle d, e \rangle$ *mit* $o(d) = o(e) = 2$ *und* $o(de) = n$ *eine Diedergruppe der Ordnung* $2n$, φ *eine Projektivität von* G *auf eine Gruppe* H *und sei* $\langle d \rangle^\varphi = \langle x \rangle$ *sowie* $\langle e \rangle^\varphi = \langle y \rangle$. *Dann gilt:*

(*a*) *Ist* $n = \infty$, *so ist* φ *2-regulär,* $\langle de \rangle^\varphi = \langle xy \rangle$ *und* $G^\varphi \simeq G$.

(*b*) *Ist* $n = p$ *eine Primzahl, so ist* G^φ *elementarabelsch der Ordnung* p^2 *oder nichtabelsch der Ordnung* pq, q *eine Primzahl mit* $q < p$.

(*c*) *Ist* n *weder* ∞ *noch eine Primzahl, so ist* $\langle de \rangle^\varphi$ *ein zyklischer Normalteiler der Ordnung* n *von* G^φ *und* $o(x) = o(y) = q$ *mit einer Primzahl* q. *Ist* $q = 2$, *so ist* φ *2-regulär,* $\langle de \rangle^\varphi = \langle xy \rangle$ *und* $G^\varphi \simeq G$. *Ist* $q > 2$, *so ist entweder* q *kein Teiler von* n *und* x *fixpunktfrei auf* $\langle de \rangle^\varphi$ *oder* $n = qn'$ *mit* $(n', q) = 1$.

BEWEIS. (*a*) Ist $n = \infty$, so ist $\langle de \rangle$ die einzige zyklische maximale Untergruppe von G. Da jede Projektivität zyklische Gruppen auf zyklische Gruppen abbildet [1, S. 6 und 7], ist also $\langle de \rangle^\varphi$ ein unendlich zyklischer Normalteiler von G^φ, etwa $\langle de \rangle^\varphi = \langle z \rangle$. Wäre $z^x = z$, so wäre $\langle xz \rangle$ eine unendlich zyklische Gruppe, deren Urbild $\langle xz \rangle^{\varphi^{-1}}$ Elemente der Ordnung 2 enthielte. Das geht nicht; es ist also $z^x = z^{-1}$. Da $o(x)$ eine Primzahl ist, folgt $o(x) = 2$, und G^φ ist eine unendliche

Diedergruppe. Die Untergruppen der Ordnung 2 von G sind die Komplemente zu $\langle de\rangle$, gehen bei φ über in die Komplemente zu $\langle de\rangle^\varphi$ in G^φ, also in Untergruppen der Ordnung 2. Damit ist φ 2-regulär und $\langle xy\rangle = \langle de\rangle^\varphi$, da $G^\varphi = \langle x, y\rangle = \langle xy, x\rangle$ ist.

(b) folgt aus [1, Theorem 11.2].

(c) Hier ist erneut $\langle de\rangle$ die einzige zyklische maximale Untergruppe von G, also $\langle de\rangle^\varphi = \langle z\rangle$ ein zyklischer Normalteiler von G^φ; ferner ist $o(x) = |G^\varphi : \langle z\rangle| = o(y)$ eine Primzahl q. Zu zeigen ist $o(z) = n$.

Sei zuerst $q = 2$. Dann ist G^φ von den Involutionen x and y erzeugt, also eine Diedergruppe der Ordnung $2m$ mit $m = o(xy)$ und $\langle xy\rangle = \langle z\rangle$, da $G^\varphi = \langle x, y\rangle = \langle xy, x\rangle$ ist. Offenbar ist m die Anzahl der minimalen Untergruppen von G^φ, die nicht in $\langle xy\rangle$ liegen, also $m = n$ und $G^\varphi \simeq G$. Daß φ 2-regulär ist, ist klar: Ist n ungerade, so sind die Untergruppen der Ordnung 2 von G gerade die Komplemente zu $\langle de\rangle$, deren Bilder also die Komplemente zu $\langle z\rangle$ und folglich von der Ordnung 2; ist n gerade, so enthält G Kleinsche Vierergruppen, und φ ist schon deshalb 2-regulär.

Sei nun $q > 2$. Ist $(o(z), q) = 1$, so ist x fixpunktfrei auf $\langle z\rangle$, da jeder Fixpunkt $z_1 \in \langle z\rangle$ mit $z_1 \neq 1$ eine zyklische Gruppe $\langle z_1 x\rangle$ liefern würde, deren Urbild $\langle z_1 x\rangle^{\varphi^{-1}}$ eine Diedergruppe wäre. Somit existieren genau $o(z)$ Komplemente zu $\langle z\rangle$ in G^φ. Die Anzahl der Komplemente zu $\langle de\rangle$ in G ist n; es folgt $o(z) = n$, was zu zeigen war. Sei schließlich q ein Teiler von $o(z)$ und Q^φ die q-Sylowgruppe von $\langle z\rangle$. Dann ist $Q^\varphi\langle x\rangle$ eine q-Sylowgruppe von G^φ, die durch die Projektivität φ^{-1} auf eine Gruppe abgebildet wird, die keine Primärgruppe ist. Nach [10, Theorem 12, S. 12] ist $Q^\varphi\langle x\rangle$ elementarabelsch. Da Q^φ zyklisch ist, folgt $|Q^\varphi| = q$. Somit ist $|Q\langle d\rangle| = 2q$ und $|Q| = q$, da $Q \trianglelefteq Q\langle d\rangle$. Sei R^φ das Komplement zu Q^φ in $\langle z\rangle$. Dann ist $R^\varphi\langle x\rangle$ Bild der Diedergruppe $R\langle d\rangle$ unter φ und $(|R^\varphi|, q) = 1$. Erneut ist x fixpunktfrei auf R^φ, und die Anzahl der Komplemente zu R^φ in $R^\varphi\langle x\rangle$ ist $|R^\varphi|$, die der Komplemente zu R in $R\langle d\rangle$ ist $|R|$, d.h. $|R^\varphi| = |R|$. Es folgt $o(z) = |R^\varphi||Q^\varphi| = |R|q = n$. Da $|Q^\varphi| = q$, ist schließlich $n = qn'$ mit $(n', q) = 1$.

Für das Folgende brauchen wir den Begriff der P-Gruppe [10, S. 11].

Definition 1.2. (a) Sei p eine Primzahl, $n \in \mathbb{N} \cup \{\infty\}$, $n \geqslant 2$. Die Gruppe G liegt in der Klasse $P(n, p)$, wenn G elementarabelsch der Ordnung p^n (bzw. G unendliche elementarabelsche p-Gruppe für $n = \infty$) ist oder $G = A\langle t\rangle$ gilt mit A elementarabelsch der Ordnung p^{n-1}

(bzw. A unendliche elementarabelsche p-Gruppe für $n = \infty$), t von der Ordnung q, q eine Primzahl, und $tat^{-1} = a^r$ für alle $a \in A$, $r^q \equiv 1(p)$, $r \not\equiv 1(p)$.

(*b*) G ist eine *P-Gruppe*, wenn $G \in P(n, p)$ für ein $n \in \mathbf{N} \cup \{\infty\}$ mit $n \geqslant 2$ und eine Primzahl p.

Die endlichen Gruppen mit 2-singulären Projektivitäten sind nach Suzukis Sätzen bekannt. Wir vermerken:

LEMMA 1.3. *Sei G eine endliche Gruppe und φ eine 2-singuläre Projektivität von G auf eine Gruppe H. Dann existiert ein normales 2-Komplement K in G mit zyklischer Faktorgruppe. Ist K^φ kein Normalteiler in G^φ, so ist $G = S \times T$ mit einer P-Gruppe S der Ordnung $2p^n$ ($p > 2$ eine Primzahl, $n \geqslant 1$) und $(|S|, |T|) = 1$.*

BEWEIS. Da φ 2-singulär ist, sind die 2-Sylowgruppen von G zyklisch. Nach Burnside besitzt G ein normales 2-Komplement K. Die letzte Behauptung folgt aus [9, Theorem 5 und Theorem 7].

Es scheint uns eine interessante Frage zu sein, ob Lemma 1.3 (in sinnvoll abgewandelter Form) auch für unendliche Gruppen gilt. Aber selbst die einfachste Vermutung, daß eine von Involutionen erzeugte Gruppe G mit einer 2-singulären Projektivität φ, die keine P-Gruppe ist, einen Normalteiler K mit $|G:K| = 2$ und $K^\varphi \trianglelefteq G^\varphi$ besitzt, dessen Elemente alle unendliche oder endliche ungerade Ordnung haben, konnten wir nicht beweisen. Eine unmittelbare Folgerung davon wäre, daß alle Untergruppen der Ordnung 2 von G durch φ auf Untergruppen der gleichen Ordnung q in G^φ abgebildet würden. Diese erheblich schwächere Aussage können wir beweisen, und sie wird für unsere weiteren Betrachtungen das zentrale Hilfsmittel sein. Um das zu tun, benötigen wir zwei einfache Hilfssätze, die wohl bekannt sind, deren Beweise wir aber zur Bequemlichkeit des Lesers kurz angeben.

HILFSSATZ 1.4. *Sei N ein Normalteiler der Gruppe G und G/N eine nicht-zyklische elementarabelsche 2-Gruppe. Ist φ eine Projektivität von G auf eine Gruppe H, so ist N^φ ein Normalteiler in G^φ und G^φ/N^φ eine elementarabelsche 2-Gruppe.*

BEWEIS. Sei M eine N enthaltende Untergruppe von G mit $|G:M| = 4$. Dann liegt jedes Element $g \in G$ in einer der drei M enthaltenden maximalen Untergruppen von G. Da φ^{-1} zyklische

Gruppen auf zyklische Gruppen abbildet, gilt das Entsprechende für G^φ: die Gruppe G^φ ist mengentheoretische Vereinigung dreier echter Untergruppen. Nach einem Satz von Scorza [11, S. 149] ist $M^\varphi \trianglelefteq G^\varphi$ und G^φ/M^φ eine Vierergruppe. Da N der Durchschnitt aller M mit $N \leqslant M$ und $|G:M| = 4$ ist, ist schließlich $N^\varphi \trianglelefteq G^\varphi$ und G^φ/N^φ eine elementarabelsche 2-Gruppe.

HILFSSATZ 1.5. *Sei p eine Primzahl und $G = \langle u\rangle \times \langle a\rangle$ mit $o(u) = \infty$, $o(a) = p$. Ist φ eine Projektivität von G auf eine Gruppe H, so ist H isomorph zu G.*

BEWEIS. Da $\langle a\rangle$ die einzige nichttriviale endliche Untergruppe in G ist, ist $\langle a\rangle^\varphi \trianglelefteq G^\varphi$; ferner natürlich $|\langle a\rangle^\varphi| = q$ eine Primzahl. Die Gruppe G besitzt genau p unendlich zyklische maximale Untergruppen, die sich in $\langle u^p\rangle$ schneiden. Da die Bilder dieser Gruppen auch zyklisch sind, ist $\langle u^p\rangle^\varphi \leqslant Z(G^\varphi)$ und folglich $\langle u^p, a\rangle = \langle u^p\rangle \times \langle a\rangle$ verbandsisomorph zu $\langle u^p, a\rangle^\varphi = \langle u^p\rangle^\varphi \times \langle a\rangle^\varphi$. Die erste Gruppe enthält genau p unendlich zyklische maximale Untergruppen, die sich in $\langle u^{p^2}\rangle$ schneiden, die zweite q; es folgt $p = q$ und $|\langle u^p\rangle^\varphi : \langle u^{p^2}\rangle^\varphi| = p$. Da der Faktorverband $[\langle u\rangle/\langle u^{p^2}\rangle]$ eine Kette ist, folgt $|\langle u\rangle^\varphi : \langle u^{p^2}\rangle^\varphi| = p^2$. Damit ist $\langle u\rangle^\varphi \trianglelefteq G^\varphi$, also $G^\varphi = \langle u\rangle^\varphi \times \langle a\rangle^\varphi \simeq G$.

SATZ 1.6. *Sei G eine Gruppe und φ eine Projektivität von G auf die Gruppe H. Existieren Involutionen $a, b \in G$ mit $|\langle a\rangle^\varphi| \neq |\langle b\rangle^\varphi|$, so ist $G = S \times T$ mit einer von Involutionen erzeugten nichtabelschen P-Gruppe S und einer Gruppe T, für die $o(t)$ endlich und teilerfremd zu $o(s)$ für alle $s \in S$, $t \in T$ gilt.*

BEWEIS. Sei D die Menge der Involutionen in G und $S = \langle d | d \in D\rangle$. Ist $a \in D$, so ist natürlich $|\langle a\rangle^\varphi|$ eine Primzahl. Sei q die kleinste Primzahl, die unter den $|\langle a\rangle^\varphi|$ mit $a \in D$ auftritt. Wir untersuchen die Gruppen $\langle a, b\rangle$ und $\langle a, b, c\rangle$ mit $a, b, c \in D$.

(1) *Seien $a, b \in D$ mit $|\langle a\rangle^\varphi| = q$, $|\langle b\rangle^\varphi| = p$ und $q < p$. Dann ist $\langle a, b\rangle$ eine Diedergruppe der Ordnung $2p$ und $\langle a, b\rangle^\varphi$ eine nichtabelsche Gruppe der Ordnung pq.*

Denn $\langle a, b\rangle$ ist eine Diedergruppe der Ordnung $2r$ für ein $r \in \mathbf{N} \cup \{\infty\}$, die von φ so abgebildet wird, daß $\langle a\rangle^\varphi$ und $\langle b\rangle^\varphi$ verschiedene Ordnungen haben. Nach Lemma 1.1 ist r eine Primzahl und $\langle a, b\rangle^\varphi \in P(2, r)$. Da p und q die Ordnung von $\langle a, b\rangle^\varphi$ teilen, ist $\langle a, b\rangle^\varphi$ nichtabelsch der Ordnung pq, $r = p$ und $\langle a, b\rangle$ eine Diedergruppe der Ordnung $2p$.

(2) *Seien* $a, b \in D$ *mit* $|\langle a\rangle^\varphi| = q$, $|\langle b\rangle^\varphi| = p$ *und* $q < p$. *Ist* $c \in D$ *mit* $c \notin \langle a, b\rangle$, *so ist* $\langle a, b, c\rangle^\varphi$ *eine P-Gruppe der Ordnung* p^2q, $\langle a, b, c\rangle \in P(3, p)$ *und* $\langle ab, ac, bc\rangle$ *elementarabelsch der Ordnung* p^2.

Zum Beweis zeigen wir zuerst, daß $\langle a, b, c\rangle$ endlich ist. Ist $|\langle c\rangle^\varphi| = r > q$, so ist nach (1) $\langle a, c\rangle^\varphi$ eine nichtabelsche Gruppe der Ordnung rq und $\langle a, b\rangle^\varphi$ eine nichtabelsche Gruppe der Ordnung pq. Somit werden $\langle b\rangle^\varphi$ und $\langle c\rangle^\varphi$ von $\langle a\rangle^\varphi$ normalisiert, also auch $\langle b\rangle^\varphi \cup \langle c\rangle^\varphi = \langle b, c\rangle^\varphi$. Da $|\langle b\rangle^\varphi| = p > q \geqslant 2$, ist φ auf der Diedergruppe $\langle b, c\rangle$ nicht 2-regulär. Nach Lemma 1.1 ist $\langle b, c\rangle$ endlich, also auch $\langle b, c\rangle^\varphi$, damit ganz $\langle a, b, c\rangle^\varphi = \langle b, c\rangle^\varphi \langle a\rangle^\varphi$ und somit schließlich auch das Urbild $\langle a, b, c\rangle$. Ist $|\langle c\rangle^\varphi| = q$, so wird $\langle b\rangle^\varphi$ nach (1) von $\langle a\rangle^\varphi$ und von $\langle c\rangle^\varphi$ normalisiert. Somit müssen wir hier zeigen, daß $\langle a, c\rangle$ endlich ist; dann sind es auch $\langle a, c\rangle^\varphi$ und $\langle a, b, c\rangle^\varphi = \langle b\rangle^\varphi \langle a, c\rangle^\varphi$. Wäre aber $\langle a, c\rangle$ unendlich, so folgte $q = 2$ nach Lemma 1.1, und mit $\langle a\rangle^\varphi = \langle x\rangle$, $\langle b\rangle^\varphi = \langle y\rangle$ und $\langle c\rangle^\varphi = \langle z\rangle$ wären $\langle x, y\rangle$ und $\langle z, y\rangle$ nach (1) Diedergruppen der Ordnung $2p$. Es folgte $y^x = y^{-1} = y^z$, und damit wäre $xz \in C_{G^\varphi}(y)$, also $\langle xz, y\rangle$ das direkte Produkt der unendlich zyklischen Gruppe $\langle xz\rangle$ mit der Gruppe $\langle y\rangle$ der Ordnung p. Nach Hilfssatz 1.5 folgte $\langle xz, y\rangle \simeq \langle xz, y\rangle^{\varphi^{-1}}$, also $p = 2$, ein Widerspruch.

Damit ist $\langle a, b, c\rangle$ in allen Fällen eine endliche von Involutionen erzeugte Gruppe, auf der φ wegen $|\langle b\rangle^\varphi| = p > 2$ eine 2-singuläre Projektivität induziert. Besäße $\langle a, b, c\rangle$ ein normales 2-Komplement K mit $K^\varphi \trianglelefteq \langle a, b, c\rangle^\varphi$, so wären $\langle a\rangle^\varphi, \langle b\rangle^\varphi$ und $\langle c\rangle^\varphi$ Komplemente zu K^φ und hätten folglich die gleiche Ordnung; das ist aber nach Voraussetzung nicht der Fall. Nach Lemma 1.3 ist $\langle a, b, c\rangle$ eine P-Gruppe der Ordnung $2r^n$ mit einer Primzahl r. Da $c \notin \langle a, b\rangle$, ist $n = 2$, also $\langle a, b, c\rangle \in P(3, r)$ und folglich auch $\langle a, b, c\rangle^\varphi \in P(3, r)$ [1, Theorem 11.2]. Da p und q die Ordnung von $\langle a, b, c\rangle^\varphi$ teilen und $q < p$ gilt, ist $r = p$, $|\langle a, b, c\rangle^\varphi| = p^2q$ und somit schließlich $\langle a, b, c\rangle \in \in P(3, p)$. Offenbar liegen dann ab, ac, bc in dem Normalteiler der Ordnung p^2 von $\langle a, b, c\rangle$, und da a mit diesen drei Elementen ganz $\langle a, b, c\rangle$ erzeugt, ist $\langle ab, ac, bc\rangle$ elementarabelsch der Ordnung p^2.

(3) *Seien* $b, c \in D$ *mit* $|\langle b\rangle^\varphi| = p > q$, $|\langle c\rangle^\varphi| > q$ *und* $b \neq c$. *Dann ist* $\langle b, c\rangle^\varphi$ *elementarabelsch der Ordnung* p^2.

Ist nämlich $a \in D$ mit $|\langle a\rangle^\varphi| = q$, so ist $\langle a, b\rangle^\varphi$ nach (1) nichtabelsch der Ordnung pq und enthält folglich nur eine minimale Untergruppe mit von q verschiedener Ordnung, nämlich $\langle b\rangle^\varphi$. Somit ist $c \notin \langle a, b\rangle$, nach (2) also $\langle a, b, c\rangle^\varphi$ eine P-Gruppe der Ordnung p^2q.

Da $\langle c\rangle^\varphi$ nicht die Ordnung q hat, erzeugt es mit $\langle b\rangle^\varphi$ den elementarabelschen Normalteiler der Ordnung p^2 von $\langle a, b, c\rangle^\varphi$.

Sei nun b eine feste Involution in G mit $|\langle b\rangle^\varphi| = p > q$ und sei $A = \langle ab | a \in D\rangle$. Wir zeigen:

(4) *A ist eine elementarabelsche p-Gruppe.*

Wir müssen zeigen, daß alle Erzeugenden ab von A die Ordnung p haben und je zwei untereinander vertauschbar sind. Seien dazu $a, c \in D$ mit $a \neq b \neq c$. Hat $\langle a\rangle^\varphi$ oder $\langle c\rangle^\varphi$ die Ordnung q, etwa $|\langle a\rangle^\varphi| = q$, so ist $\langle a, b\rangle$ nach (1) eine Diedergruppe der Ordnung $2p$, also $o(ab) = p$. Ist $c \in \langle a, b\rangle$, so ist $\langle cb\rangle = \langle ab\rangle$ die Untergruppe der Ordnung p in $\langle a, b\rangle$, d.h. cb hat die Ordnung p und ist mit ab vertauschbar. Ist $c \notin \langle a, b\rangle$, so folgt nach (2), daß $\langle ab, ac, bc\rangle$ elementarabelsch der Ordnung p^2 ist; also haben auch dann ab und cb die Ordnung p und sind vertauschbar. — Sei nun $|\langle a\rangle^\varphi| > q$ und $|\langle c\rangle^\varphi| > q$. Nach (3) sind $\langle b, a\rangle^\varphi$ und $\langle b, c\rangle^\varphi$ elementarabelsch der Ordnung p^2, desgleichen dann $\langle a, c\rangle^\varphi$, falls $a \neq c$; somit sind $\langle a\rangle^\varphi$, $\langle b\rangle^\varphi$ und $\langle c\rangle^\varphi$ Untergruppen der Ordnung p in G^φ, die sich paarweise zentralisieren, also eine elementarabelsche Untergruppe der Ordnung p^3 oder p^2 von G^φ erzeugen. Dann ist $\langle a, b, c\rangle$ eine P-Gruppe der Ordnung $2p^2$ bzw. $2p$, und die Elemente ab und cb haben die Ordnung p und sind vertauschbar. Damit ist (4) bewiesen.

(5) *S ist eine P-Gruppe.*

Offenbar ist $S = \langle A, b\rangle$. Für $a \in D$ gilt $(ab)^b = ba = (ab)^{-1}$, b invertiert also alle Erzeugenden der abelschen Gruppe A. Damit wird ganz A invertiert, und $S = A\langle b\rangle$ ist eine P-Gruppe.

(6) *G enthält nur Elemente endlicher Ordnung.*

Für ein Element $g \in G$ unendlicher Ordnung wäre $S \cap \langle g\rangle = 1$, und mit $X = S\langle g\rangle$ wäre $X/A = S/A \times \langle g\rangle A/A$. Somit wäre $N = \langle g^2\rangle A \trianglelefteq X$ und X/N eine Vierergruppe. Nach Hilfssatz 1.4 wäre $N^\varphi \trianglelefteq X^\varphi$, damit $N^\varphi \cap S^\varphi = A^\varphi \trianglelefteq S^\varphi$, also $|\langle a\rangle^\varphi| = |S^\varphi : A^\varphi|$ für alle $a \in D$, im Widerspruch zur Voraussetzung.

(7) *Ist $g \in G \setminus S$ von Primzahlpotenzordnung, so ist $o(g)$ teilerfremd zu 2 und p sowie $g \in C_g(S)$.*

Sei $a \in D$ beliebig und $d \in D$ mit $|\langle a\rangle^\varphi| \neq |\langle d\rangle^\varphi|$. Da S eine P-Gruppe ist, ist $\langle a, d, g\rangle$ endlich. Da $|\langle a\rangle^\varphi| \neq |\langle d\rangle^\varphi|$ ist, liefert Lemma 1.3, daß $\langle a, d, g\rangle = S_1 \times T_1$ ist mit einer P-Gruppe S_1 der Ordnung $2p^m$ und $(|S_1|, |T_1|) = 1$. Da $S_1 \leqslant S$, ist $g \notin S_1$; da g Primzahlpotenzordnung hat, ist also $g \in T_1$. Damit ist $o(g)$ teilerfremd zu 2 und p und ferner $ag = ga$. Dies gilt für alle $a \in D$; es folgt $g \in C_G(S)$.

Für $T = C_G(S)$ ist nach (6) und (7) offenbar $G = ST$, ferner $S \cap T = Z(S) = 1$ und damit schließlich $G = S \times T$. Die Behauptungen über die Ordnungen der Elemente in T folgen ebenfalls aus (6) und (7). Damit ist Satz 1.6 bewiesen.

Es sei bemerkt, daß für eine Gruppe $G = S \times T$ mit der in Satz 1.6 angegebenen Struktur nach Suzuki [10, Theorem 4, S. 5] der Untergruppenverband $\mathfrak{V}(G)$ von G gleich dem direkten Produkt der Untergruppenverbände $\mathfrak{V}(S)$ und $\mathfrak{V}(T)$ ist und somit offenbar sogar Autoprojektivitäten φ von G existieren, die Untergruppen der Ordnung 2 von G auf Untergruppen verschiedener Ordnung (nämlich 2 und p) abbilden. Eine einfache Folgerung aus Satz 1.6 ist

KOROLLAR 1.7. *Existieren zwei vertauschbare Involutionen in der Gruppe G, so ist jede Projektivität von G 2-regulär.*

BEWEIS. Da die Gruppe G eine Vierergruppe U enthält, hat sie nicht die in Satz 1.6 angegebene Struktur. Nach Satz 1.6 existiert eine Primzahl q mit $|\langle a\rangle^\varphi| = q$ für alle Involutionen $a \in G$ und die Projektivität φ. Da $|U^\varphi| = 4$ ist, ist $q = 2$ und φ 2-regulär.

Wir wollen in § 2 die Operation von Involutionen und ihrer Bilder unter Projektivitäten auf dem Untergruppenverband einer Gruppe betrachten. Wir kümmern uns hier um die Fixpunkte dieser Operation. Das erste Lemma ist wegen einer Anwendung in § 3 allgemeiner formuliert; ist a eine Involution, so ist $U^{a^2} = U$ trivialerweise erfüllt.

LEMMA 1.8. *Sei G eine Gruppe, φ eine Projektivität von G auf eine Gruppe H, U eine maximale Untergruppe von G und $a \in G$ mit $U^a \neq U$ aber $U^{a^2} = U$. Ist $U^\varphi \trianglelefteq G^\varphi$, so ist $U \cap U^a \trianglelefteq G$, $(U \cap U^a)^\varphi \trianglelefteq G^\varphi$, $G/(U \cap U^a)$ nichtabelsch der Ordnung $2p$, p eine Primzahl, und $G^\varphi/(U \cap U^a)^\varphi \in P(2, p)$.*

BEWEIS. Sei $K = U \cap U^a$. Offenbar ist $a^2 \in N_G(U) = U$ und $a^2 \in N_G(U^a) = U^a$, also $a^2 \in K$. Ferner $K^a = (U \cap U^a)^a = U^a \cap U = K$. Ist also $V = K\langle a\rangle$, so ist $|V:K| = 2$ und $U \cap V = K$ sowie $V \cup U^a = G$.

Da $U^\varphi \trianglelefteq G^\varphi$ ist, erhalten wir $K^\varphi = U^\varphi \cap (U^a)^\varphi \trianglelefteq (U^a)^\varphi$ und $K^\varphi = U^\varphi \cap V^\varphi \trianglelefteq V^\varphi$, also $K^\varphi \trianglelefteq (U^a)^\varphi \cup V^\varphi = G^\varphi$. $(U^a)^\varphi / K^\varphi$ ist isomorph zu G^φ / U^φ, und folglich ist K^φ maximal in $(U^a)^\varphi$. Die Projektivität $\varphi^{-1} a \varphi$ von G^φ bildet $(U^a)^\varphi$ auf U^φ und K^φ auf $K^\varphi ab$; es ist also K^φ auch maximal in U^φ, und folglich sind $|G^\varphi / U^\varphi|$ und $|U^\varphi / K^\varphi|$ Primzahlen. Da mindestens drei Zwischengruppen zwischen G und K existieren, ist G^φ / K^φ nicht zyklisch, also $G^\varphi / K^\varphi \in P(2, p)$ für eine Primzahl p.

Nach Hilfssatz 1.4 ist G^φ / K^φ keine Vierergruppe, also $p > 2$. Da $K^a = K$ ist, operiert a auf den p von $V = K\langle a \rangle$ verschiedenen Untergruppen zwischen G und K und zwar in Bahnen der Länge 1 und 2, da $a^2 \in K$. Somit existiert $W \neq V$ mit $K < W < G$ und $W^a = W$, also $W \trianglelefteq G$. Es folgt $K = W \cap U \trianglelefteq U$, $K = W \cap U^a \trianglelefteq U^a$, also $K \trianglelefteq U \cup U^a = G$. Nun induziert φ^{-1} eine Projektivität von G^φ / K^φ auf G/K; es ist also G/K nichtabelsch der Ordnung $2p$. Damit ist Lemma 1.8 bewiesen.

Wir benötigen einen weiteren einfachen Hilfssatz.

HILFSSATZ 1.9. *Ist $G = U\langle a \rangle$, $a^2 = 1$ und haben alle Elemente $u^{-a}u$ mit $u \in U$ endliche ungerade Ordnung, so ist $U = C_U(a)\, U_0$ mit $U_0 = \{u \in U \mid u^a = u^{-1}\}$.*

BEWEIS. Ist $u \in U$, so ist $(u^{-a}u)^a = u^{-1}u^a = (u^{-a}u)^{-1}$, also $u^{-a}u \in U_0$. Da $o(u^{-a}u)$ ungerade ist, existiert ein $v \in \langle u^{-a}u \rangle$ mit $v^2 = u^{-a}u$. Dann ist $v \in U_0$ und $(uv^{-1})^a = u^a v = uv^{-1}$, also $u = (uv^{-1})v \in C_U(a)\, U_0$. Das war zu zeigen.

SATZ 1.10. *Sei G eine Gruppe und φ eine Projektivität von G auf eine Gruppe H mit der folgenden Eigenschaft.*

(*) *Es gibt eine Primzahl q, so daß $|\langle a \rangle^\varphi| = q$ gilt für jede Involution $a \in G$.*

Ist dann $a \in G$ eine Involution, $\langle a \rangle^\varphi = \langle x \rangle$ und $U \leqslant G$ mit $U^a = U$, so ist $(U^\varphi)^x = U^\varphi$.

BEWEIS. Ist $a \in U$, so ist offenbar $x \in U^\varphi$, also $(U^\varphi)^x = U^\varphi$. Sei also $a \notin U$ und sei zuerst $q = 2$. Wäre dann $(U^\varphi)^x \neq U^\varphi$, so wendeten wir Lemma 1.8 an auf die Gruppe $\langle U, a \rangle^\varphi$, die Projektivität φ^{-1} und die Involution x. Mit $K = U^\varphi \cap (U^\varphi)^x$ wäre dann $\langle U, a \rangle^\varphi / K$ nichtabelsch der Ordnung $2p$ für eine Primzahl p und $\langle U, a \rangle^\varphi / K^{\varphi^{-1}} \in P(2, p)$, also auch nichtabelsch der Ordnung $2p$. Für $u \in U$ ist a^u eine Involution, also $|\langle a^u \rangle^\varphi K / K| = 2$. Es folgt $|U^\varphi / K| = p$, also $U^\varphi \trianglelefteq \langle U, a \rangle^\varphi$ im Widerspruch zu $(U^\varphi)^x \neq U^\varphi$.

Sei nun $q \neq 2$ und sei $U_0 = \{u \in U | u^a = u^{-1}\}$. Dann gilt:

(1) *$C_U(a)$ und U_0 enthalten nur Elemente endlicher ungerader Ordnung; ferner ist $U = C_U(a)\, U_0$.*

Wäre nämlich $u \in C_U(a)$ mit $o(u) = \infty$, so wäre $\langle u, a\rangle = \langle u\rangle \times \langle a\rangle$, und aus Hilfssatz 1.5 folgte $q = 2$. Wäre $u \in U_0$ mit $o(u) = \infty$, so wäre $\langle u, a\rangle$ eine unendliche Diedergruppe, was nach Lemma 1.1 unmöglich ist. Wäre schließlich $u \in C_U(a)$ oder $u \in U_0$ mit gerader Ordnung, so existierte eine Vierergruppe in G, woraus $q = 2$ folgen würde. Offenbar ist $u^{-a}u \in U_0$ für alle $u \in U$; aus Hilfssatz 1.9 folgt also $U = C_U(a)\, U_0$.

(2) *$C_U(a)^\varphi$ wird von x zentralisiert.*

Da nämlich $u \in C_U(a)$ ungerade Ordnung hat, ist $\langle u, a\rangle$ zyklisch, also auch $\langle u, a\rangle^\varphi$ zyklisch, und folglich wird $\langle u\rangle^\varphi$ von x zentralisiert. Da $C_U(a)^\varphi$ von diesen $\langle u\rangle^\varphi$ erzeugt wird, folgt die Behauptung.

(3) *Ist $u \in U_0$, so ist $(\langle u\rangle^\varphi)^x = \langle u\rangle^\varphi$.*

Denn $\langle u, a\rangle$ ist eine Diedergruppe der Ordnung $2m$ mit $m = o(u)$. Ist $m = p$ eine Primzahl, so ist $\langle u, a\rangle^\varphi \in P(2, p)$, also entweder elementarabelsch der Ordnung p^2 oder nichtabelsch der Ordnung pr, $p > r$. Im ersten Falle ist offensichtlich $(\langle u\rangle^\varphi)^x = \langle u\rangle^\varphi$, im zweiten folgt aus der Voraussetzung (*), daß $r = q$ und $|\langle u\rangle^\varphi| = p$, also auch $\langle u\rangle^\varphi \trianglelefteq \langle u, a\rangle^\varphi$ ist. Ist aber m keine Primzahl, so folgt die Behauptung aus Lemma 1.1.

Nach (1) wird U^φ von $C_U(a)^\varphi$ und den $\langle u\rangle^\varphi$ mit $u \in U_0$ erzeugt. Da x alle diese Gruppen normalisiert, folgt schließlich $(U^\varphi)^x = U^\varphi$.

Die Sätze 1.6 und 1.10 liefern sofort das folgende

KOROLLAR 1.11. *Sei G eine Gruppe, die nicht die in Satz 1.6 angegebene Struktur hat, und sei φ eine Projektivität von G auf eine Gruppe H. Ist $a \in G$ eine Involution, $\langle a\rangle^\varphi = \langle x\rangle$ und $U \leqslant G$ mit $U^a = U$, so ist $(U^\varphi)^x = U^\varphi$.*

Eine von Involutionen erzeugte Gruppe hat genau dann die in Satz 1.6 angegebene Struktur, wenn sie eine nichtabelsche P-Gruppe ist. Somit gilt

KOROLLAR 1.12. *Sei G eine von Involutionen erzeugte Gruppe, die keine P-Gruppe ist, und sei φ eine Projektivität von G auf eine Gruppe H.*

(*a*) *Ist $a \in G$ eine Involution, $\langle a\rangle^\varphi = \langle x\rangle$ und $U \leqslant G$ mit $U^a = U$, so ist $(U^\varphi)^x = U^\varphi$.*

(*b*) *Ist $N \trianglelefteq G$, so ist $N^\varphi \trianglelefteq G^\varphi$.*

2. – Involutionen und Konjugiertenklassen.

Wir wollen nun die Methode aus den Arbeiten [5], [6] und [7] auf unendliche Gruppen verallgemeinern. Das folgende Lemma beschreibt sie in ihrer allgemeinsten und einfachsten Form.

LEMMA 2.1. *Sei G eine Gruppe, D eine Menge von Involutionen in G, Δ eine Menge von Untergruppen von G und φ eine Projektivität von G auf eine Gruppe H mit den folgenden Eigenschaften.*

(1) $G = \langle d | d \in D\rangle$.

(2) $\Delta^g = \Delta$ (*d.h.* $U^g \in \Delta$ *für alle* $U \in \Delta$, $g \in G$).

(3) *Für* $d \in D$, $U \in \Delta$ *und* $\langle d\rangle^\varphi = \langle x\rangle$ *gilt* $(U^\varphi)^x = (U^d)^\varphi$.

(*a*) *Dann ist* $G/\bigcap_{U\in\Delta} N_G(U)$ *isomorph zu* $H/\bigcap_{U\in\Delta} N_H(U^\varphi)$.

(*b*) *Sei* $\bigcap_{U\in\Delta} N_G(U) = 1$. *Ist G endlich oder $D^G = D$, so ist H isomorph zu G.*

BEWEIS. (*a*) Für $h \in H$ und $U \leqslant G$ sei $U^{\psi(h)}$ definiert durch $U^{\psi(h)} = U^{\varphi h \varphi^{-1}}$. Für $d \in D$, $U \in \Delta$ und $\langle x\rangle = \langle d\rangle^\varphi$ gilt $U^{\psi(x)} = U^d \in \Delta$. Da H von diesen x erzeugt wird, ist also $\Delta^{\psi(h)} = \Delta$ für alle $h \in H$.

Sei nun ν die Permutationsdarstellung von G auf Δ mit $U^{\nu(g)} = U^g$ ($g \in G$) und μ die von H auf Δ mit $U^{\mu(h)} = U^{\psi(h)}$ ($h \in H$) für $U \in \Delta$. Nach (3) ist $\nu(d) = \mu(x)$ für $d \in D$ und $\langle x\rangle = \langle d\rangle^\varphi$; da G von diesen Involutionen erzeugt wird, folgt $G^\nu = H^\mu$, also wegen $\operatorname{Kern}\nu = \bigcap_{U\in\Delta} N_G(U)$ und $\operatorname{Kern}\mu = \bigcap_{U\in\Delta} N_H(U^\varphi)$ schließlich die Behauptung.

(*b*) Nach (*a*) ist G isomorph zu $H/\bigcap_{U\in\Delta} N_H(U^\varphi)$. Ist G endlich, so folgt $H \simeq G$, da die endliche Gruppe H keine Projektivität auf eine echte Faktorgruppe besitzen kann.

Sei nun $D^G = D$ und sei $K^\varphi = \operatorname{Kern}\mu \neq 1$. Für $d \in D$ und $\langle x\rangle = \langle d\rangle^\varphi$ ist $\mu(x) = \nu(d)$, also $o(\mu(x)) = 2$. Damit ist $o(x) = 2$. Wäre G eine P-Gruppe, so folgte $G^\varphi \simeq G$, was wir zeigen wollen. Sei also G keine P-Gruppe. Dann ist auch G^φ keine P-Gruppe und wird von Involutionen erzeugt. Nach Satz 1.6 sind φ und φ^{-1} 2-regulär, und nach Korollar 1.12 ist $K = (\operatorname{Kern}\mu)^{\varphi^{-1}} \trianglelefteq G$.

Da $Z(G) = 1$ und $G = \langle d | d \in D\rangle$ ist, existiert ein $d \in D$ mit $C_K(d) \neq K$. Sei $u \in K$ mit $u^d \neq u$ und sei $v = u^{-d}u$. Dann ist $v^d = u^{-1}u^d = v^{-1}$ und somit $\langle v, d\rangle$ eine Diedergruppe der Ordnung $2m$ mit $m = o(v) \neq 1$. Da $K \trianglelefteq G$ ist, liegt v in K und hat somit von 2 verschiedene Ordnung; denn sonst wäre $v \in \bigcap_{U\in\Delta} N_G(U)$ nach Satz 1.10. Damit sind d und $e = d^v$ zwei verschiedene Involutionen aus D (hier wird $D^G = D$ benutzt) mit $de \in \langle v\rangle \leqslant K$. Sei $\langle d\rangle^\varphi = \langle x\rangle$ und $\langle e\rangle^\varphi = \langle y\rangle$. Da φ 2-regulär ist, ist $\langle de\rangle^\varphi = \langle xy\rangle$ (s. Lemma 1.1 oder Hilfssatz 1 aus [7]) und somit $xy \in \operatorname{Kern}\mu$. Für $U \in \Delta$ ist $U^d \in \Delta$ nach (2) und somit $U^\varphi = (U^\varphi)^{x^v} = ((U^d)^\varphi)^v = (U^{de})^\varphi$, also $U = U^{de}$. Damit ist $de \in \bigcap_{U\in\Delta} N_G(U) = 1$, also $d = e$. Das ist ein Widerspruch; es folgt $K = 1$, also $G^\varphi \simeq G$.

Wir konnten nicht entscheiden, ob die Voraussetzung «G endlich oder $D^G = D$» in (b) notwendig ist; in den üblichen Anwendungen von Lemma 2.1 ist aber immer $D^G = D$. Der folgende Satz verallgemeinert den Haupthilfssatz (Lemma 2.1) aus [6] auf unendliche Gruppen. Da man aber über Bilder von Konjugiertenklassen in unendlichen Gruppen relativ wenig weiß, ist er wohl nicht so nützlich wie Lemma 2.1 in [6].

Satz 2.2. *Sei G eine Gruppe, D eine Menge von Involutionen in G und Δ eine Menge von Untergruppen von G mit den folgenden Eigenschaften.*

(1) $G = \langle d | d \in D\rangle$ *und* $G \notin P(n, 3)$ *für alle* $n \in \mathbf{N} \cup \{\infty\}$.

(2) $\Delta^G = \Delta$ *und* $\bigcap_{U\in\Delta} N_G(U) = 1$.

(3) *Sei* $a \in D$, $U \in \Delta$. *Dann ist* $V^a = V$ *für alle* $V \in \Delta \setminus \{U, U^a\}$ *mit* $U \cap U^a \leqslant V \leqslant \langle U, U^a\rangle$.

Ist dann φ eine Projektivität von G auf eine Gruppe H mit

(4) $(\Delta^\varphi)^H = \Delta^\varphi$,

so ist H isomorph zu G.

BEWEIS. Die Aussage (3) gilt wegen $\Delta^g = \Delta$ offenbar für alle $a \in D^g$. Indem wir D durch D^g ersetzen haben wir also zusätzlich $D = D^g$. Nach Lemma 2.1, (*b*) ist somit nur zu zeigen, daß (3) aus Lemma 2.1 für D und Δ gilt. Wir zeigen zuerst

(5) *G ist keine P-Gruppe.*

Angenommen, G wäre eine P-Gruppe, also $G \in P(n, p)$ für eine Primzahl p und ein $n \in \mathbf{N} \cup \{\infty\}$. Nach (1) und (2) existiert ein $U \in \Delta$ und ein $a \in D$ mit $U^a \neq U$. Es ist also G nicht abelsch; sei P der elementarabelsche p-Normalteiler vom Index 2 in G. Dann sind alle Untergruppen von P normal in G, und folglich ist $|U : U \cap P| = 2$ und $\langle U, a\rangle / U \cap P = \langle U, U^a\rangle / U \cap U^a$ eine Diedergruppe der Ordnung $2p$. Damit liegen zwischen $U \cap U^a$ und $\langle U, U^a\rangle$ genau p zueinander konjugierte Untergruppen, die nach (2) alle in Δ enthalten sind und von denen a genau eine normalisiert, nämlich $\langle a\rangle(U \cap P)$. Aus (3) folgt $p = 3$ im Widerspruch zu (1). Damit ist (5) gezeigt.

Wir nehmen nun an, daß (3) aus Lemma 2.1 nicht gilt. Nach (1) und (5) ist G von Involutionen erzeugt und keine P-Gruppe. Nach Satz 1.6 existiert eine Primzahl q mit $|\langle a\rangle^\varphi| = q$ für alle Involutionen $a \in G$. Wir zeigen:

(6) *$q \neq 2$ und $U^\varphi \trianglelefteq G^\varphi$ für alle $U \in \Delta$.*

Sei dazu $U \in \Delta$, $a \in D$, $\langle a\rangle^\varphi = \langle x\rangle$. Ist $U^a = U$, so folgt $(U^\varphi)^x = U^\varphi = (U^a)^\varphi$ nach Satz 1.10. Ist $U^a \neq U$, so ist $(U \cap U^a)^a = U \cap U^a$ und $\langle U, U^a\rangle^a = \langle U, U^a\rangle$, also $\big((U \cap U^a)^\varphi\big)^x = (U \cap U^a)^\varphi$ und $\big(\langle U, U^a\rangle^\varphi\big)^x = \langle U, U^a\rangle^\varphi$, erneut nach Satz 1.10. Nach (4) operiert x auf der Menge der V^φ mit $V \in \Delta$ und $U \cap U^a \leqslant V \leqslant \langle U, U^a\rangle$, und nach (3) und Satz 1.10 läßt x alle von U^φ und $(U^a)^\varphi$ verschiedenen V^φ fest, d.h. operiert auf $\{U^\varphi, (U^a)^\varphi\}$. Wäre $q = 2$, so wäre G^φ von Involutionen erzeugt, keine P-Gruppe und folglich $(U^\varphi)^x \neq U^\varphi$, da sonst nach Korollar 1.12 angewandt auf φ^{-1} offenbar $U^a = U$ gelten müßte. Es folgte $(U^\varphi)^x = (U^a)^\varphi$, also (3) von Lemma 2.1 für alle $U \in \Delta$, $a \in D$, im Widerspruch zu unserer Annahme. Damit ist $q \neq 2$ gezeigt. Nun operiert das Element x der Ordnung q auf der zweielementigen Menge $\{U^\varphi, (U^a)^\varphi\}$. Es folgt $(U^\varphi)^x = U^\varphi$, erneut für alle $U \in \Delta$ und $a \in D$, also schließlich $U^\varphi \trianglelefteq G^\varphi$, da $G = \langle a \mid a \in D\rangle$.

(7) *Es ist $q = 3$. Ist $U \in \Delta$ nicht normal in G, so existiert genau ein Normalteiler U_0 vom Index 2 in U; es ist $U_0 \trianglelefteq G$, $U_0^\varphi \trianglelefteq G^\varphi$ und* $|U^\varphi : U_0^\varphi| = 3$.

Sei $U \in \Delta$ nicht normal in G und sei $a \in D$ mit $U^a \neq U$. Nach Lemma 1.8 angewandt auf $\langle U, a\rangle = \langle U, U^a\rangle$ ist $\langle U, U^a\rangle/U \cap U^a$ nichtabelsch der Ordnung $2p$ und $\langle U, U^a\rangle^\varphi/(U \cap U^a)^\varphi \in P(2, p)$ für eine Primzahl p. Da U^φ und $(U^a)^\varphi$ Normalteiler in $\langle U, U^a\rangle^\varphi$ sind, ist $\langle U, U^a\rangle^\varphi/(U \cap U^a)^\varphi$ elementarabelsch, und wegen $|\langle U, U^a\rangle^\varphi : U^\varphi| = |\langle x\rangle|$ ist $p = q$. Wieder sind alle q Untergruppen V mit $U \cap U^a < V < \langle U, U^a\rangle$ und $|V : U \cap U^a| = 2$ konjugiert zu U, liegen also in Δ, und nur $\langle a\rangle(U \cap U^a)$ wird von a normalisiert. Aus (3) folgt $q = 3$.

Offenbar ist $U_0 = U \cap U^a \trianglelefteq U$ mit $|U : U_0| = 2$, ferner $|U^\varphi : U_0^\varphi| = q = 3$ und $U_0^\varphi = U^\varphi \cap (U^a)^\varphi \trianglelefteq G^\varphi$ nach (6). Wäre U_1 ein weiterer Normalteiler vom Index 2 in U, so wäre $U/(U_0 \cap U_1)$ eine Vierergruppe, desgleichen $U^\varphi/(U_0 \cap U_1)^\varphi$ nach Hilfssatz 1.4; es ist aber $|U^\varphi : U_0^\varphi| = 3$. Somit ist U_0 der einzige Normalteiler vom Index 2 in U. Zu zeigen bleibt, daß $U_0 \trianglelefteq G$ ist. Ist aber $d \in D$ mit $U^d = U$, so ist $U_0^d = U_0$, da U_0 eine charakteristische Untergruppe von U ist; ist $U^d \neq U$, so ist $U \cap U^d$ nach dem eben Bewiesenen ein Normalteiler vom Index 2 in U, also $U \cap U^d = U_0$ und damit $U_0^d = U_0$. Da $G = \langle d | d \in D\rangle$ ist, folgt $U_0 \trianglelefteq G$.

(8) *Ist $U \in \Delta$ und $g \in G$ mit $U^g \neq U$, so ist $\langle U, U^g\rangle/U_0$ nichtabelsch der Ordnung* 6 *und $\langle U, U^g\rangle^\varphi/U_0^\varphi$ elementarabelsch der Ordnung* 9.

Offenbar ist U nicht normal in G; es existiert also der Normalteiler U_0 mit den in (7) angegebenen Eigenschaften. Da $U_0 \trianglelefteq G$ ist, ist $U_0 \trianglelefteq U^g$ mit $|U^g : U_0| = 2$. Nach (6) und (7) sind also U^φ/U_0^φ und $(U^g)^\varphi/U_0^\varphi$ Normalteiler von G^φ/U_0^φ der Ordnung 3. Somit ist $\langle U, U^g\rangle^\varphi/U_0^\varphi$ elementarabelsch der Ordnung 9 und dann $\langle U, U^g\rangle/U_0$ nichtabelsch der Ordnung 6.

(9) *Für $g \in G$ ist $o(g) \in \{1, 2, 3\}$; für $h \in G^\varphi$ ist $o(h) \in \{1, 3\}$.*

Wir nehmen dazu zuerst an, G enthielte ein Element g unendlicher Ordnung. Nach (2) existiert ein $U \in \Delta$ mit $g^6 \notin N_G(U)$, und nach (8) ist $\langle U, U^g\rangle/U_0$ nichtabelsch der Ordnung 6. Ist $U^{g^2} \leqq \langle U, U^g\rangle$, so ist $\langle U, U^g\rangle^g = \langle U^g, U^{g^2}\rangle = \langle U, U^g\rangle$, und g operiert auf $\langle U, U^g\rangle/U_0$. Es folgt $U^{g^6} = U$ im Widerspruch zur Wahl von U. Somit ist $U^{g^2} \nleqq \langle U, U^g\rangle$. Wegen $\langle U, U^g, U^{g^2}\rangle \leqq \langle U, g\rangle$ ist

$$\langle U, U^g, U^{g^2}\rangle^\varphi/U^\varphi \leqq U^\varphi\langle g\rangle^\varphi/U^\varphi \simeq \langle g\rangle^\varphi/(U^\varphi \cap \langle g\rangle^\varphi),$$

also zyklisch. Aber $\langle U, U^g\rangle^\varphi/U^\varphi$ und $\langle U, U^{g^2}\rangle^\varphi/U^\varphi$ sind zwei verschiedene Normalteiler der Ordnung 3, die in $\langle U, U^g, U^{g^2}\rangle^\varphi/U^\varphi$ enthalten

sind. Mit diesem Widerspruch ist gezeigt, daß Elemente unendlicher Ordnung in G (und damit auch in G^φ) nicht vorkommen.

Sei nun $g \in G$ mit $o(g) = p^n$, p eine Primzahl, $n \in \mathbb{N}$, und sei $\langle h\rangle = \langle g\rangle^\varphi$. Zu $f \in \langle g\rangle$ mit $o(f) = p$ existiert wegen (2) ein $U \in \Delta$ mit $f \notin N_G(U)$. Dann ist $U \cap \langle g\rangle = 1$ und wegen $U^\varphi \trianglelefteq G^\varphi$ somit $\langle U, g\rangle^\varphi / U^\varphi \simeq \langle g\rangle^\varphi = \langle h\rangle$, also $[\langle U, g\rangle^\varphi / U^\varphi]$ und damit auch $[\langle U, g\rangle / U]$ eine Kette der Länge n. Nach (8) ist sowohl $\langle U, U^f\rangle / U_0$ als auch $\langle U, U^g\rangle / U_0$ nichtabelsch der Ordnung 6, und wegen $U, U^f, U^g \leqslant \langle U, g\rangle$ ist $\langle U, U^f\rangle = \langle U, U^g\rangle$ die Untergruppe von $\langle U, g\rangle$, in der U maximal ist. Somit ist $o(f) = |U_0\langle f\rangle : U_0| = 2$ oder 3 und $U^g = U^f$ oder $U^g = U^{f^2}$, also $g^{-1}f$ *bzw.* $g^{-1}f^2$ in $N_{\langle U,g\rangle}(U)$ enthalten. Dieser Normalisator ist U, da U nicht normal in $\langle U, U^g\rangle$ und $[\langle U, g\rangle / U]$ eine Kette ist; es folgt $g = f$ oder $g = f^2$, also $n = 1$. Da $\langle U, U^g\rangle^\varphi / U_0^\varphi$ elementarabelsch der Ordnung 9 ist, ist schließlich $o(h) = |\langle U, U^g\rangle^\varphi / U^\varphi| = 3$. Damit ist die Behauptung (9) für Elemente von Primzahlpotenzordnung gezeigt. Jedes Element endlicher Ordnung ist Produkt vertauschbarer Elemente von Primzahlpotenzordnung. Somit ist jedes von 1 verschiedene Element in G^φ von der Ordnung 3, und dann können auch in G keine Elemente von der Ordnung 6 enthalten sein. Damit ist (9) bewiesen.

(10) *Sind* $u, v \in G$ *mit* $o(u) = 3 = o(v)$, *so ist* $o(uv) = 3$ *oder* 1.

Denn nach (9) käme ansonsten nur $o(uv) = 2$ in Frage. Dann wären auch $(uv)^u$ und $(uv)^v$ Involutionen, und es folgte

$$(uv)^v(uv)^u = v^{-1}uvvu^{-1}uvu = v^{-1}u^{-1} = (uv)^{-1} = uv\,.$$

Somit wäre $\langle (uv)^u, (uv)^v\rangle$ eine Kleinsche Vierergruppe, und aus Korollar 1.7 folgte $q = 2$, ein Widerspruch.

Nach (10) ist $A = \{u \in G \mid o(u) = 3 \text{ oder } 1\}$ ein Normalteiler von G. Sind $d, e \in D$ mit $d \neq e$, so ist $\langle d, e\rangle$ nach (9) nichtabelsch der Ordnung 6, also $de \in A$. Wegen $G = \langle d \mid d \in D\rangle$ ist $G = A\langle d\rangle$ und nach Hilfssatz 1.9 ist $A = C_A(d)A_0$ mit $A_0 = \{u \in A \mid u^d = u^{-1}\}$. Nach (9) ist $C_A(d) = 1$, also $A = A_0$ abelsch und somit schließlich $G \in P(m, 3)$ für ein m. Das ist ein Widerspruch zur Voraussetzung (1), womit Satz 2.2 bewiesen ist.

Eine weitere Situation, in der man (3) von Lemma 2.1 nachweisen kann, ist die folgende.

LEMMA 2.3. *Sei G eine Gruppe, φ eine Projektivität von G auf eine Gruppe H, $d \in G$ eine Involution und U eine Untergruppe von G.*

Existiert ein Isomorphismus α von $\langle U, d\rangle$ auf $\langle U, d\rangle^\varphi$ mit $X^\alpha = X^\varphi$ für alle $X \leqslant \langle U, d\rangle$, so ist $(U^\varphi)^x = (U^d)^\varphi$ für $x \in H$ mit $\langle x\rangle = \langle d\rangle^\varphi$.

BEWEIS. Offenbar ist $\langle d\rangle^\varphi = \langle x\rangle = \langle d\rangle^\alpha$, also $d^\alpha = x$. Dann folgt $(U^d)^\varphi = (U^d)^\alpha = d^\alpha U^\alpha d^\alpha = (U^\alpha)^x = (U^\varphi)^x$, was zu zeigen war.

Wir wollen Lemma 2.3 anwenden auf die Situation, in der $\Delta = \{\langle d\rangle \mid d \in D\}$ ist. Dazu benötigen wir

LEMMA 2.4. *Sei $G = S \times T$, $S = \langle d, e\rangle$ mit Involutionen d und e und T eine zu S isomorphe oder eine unendliche Diedergruppe. Ist dann φ eine Projektivität von G auf eine Gruppe H, $\langle d\rangle^\varphi = \langle x\rangle$ und $U = \langle e\rangle$, so ist $(U^\varphi)^x = (U^d)^\varphi$.*

BEWEIS. Ist $T \simeq S$, so existiert nach [7, Lemma 3] ein Isomorphismus α von G auf G^φ mit $X^\alpha = X^\varphi$ für alle $X \leqslant G$, und nach Lemma 2.3 ist $(U^\varphi)^x = (U^d)^\varphi$. Ist T eine unendliche Diedergruppe, so zeigt der Beweis zu [7, Korollar 4], daß ein Isomorphismus α von $S = \langle U, d\rangle$ auf S^φ existiert mit $X^\alpha = X^\varphi$ für alle $X \leqslant S$. Erneut folgt $(U^\varphi)^x = (U^d)^\varphi$ aus Lemma 2.3.

Das folgende Ergebnis verallgemeinert Satz 2.4 aus [6] und verbessert den Satz aus [7].

SATZ 2.5. *Sei F eine Untergruppe der Gruppe G mit den folgenden Eigenschaften.*

(1) *$Z(F) = 1$ und $F \notin P(n, 3)$ für alle $n \in \mathbf{N} \cup \{\infty\}$.*

(2) *F wird erzeugt von einer Menge D von Involutionen mit $D^F = D$.*

(3) *Seien $d, e \in D$ und $S = \langle d, e\rangle$. Ist $o(de) \notin \{1, 2, 3, 4, \infty\}$, so existiert eine zu S oder zu einer unendlichen Diedergruppe isomorphe Untergruppe T von $C_G(S)$ mit $S \cap T = 1$.*

Ist dann φ eine Projektivität von G auf eine Gruppe H, so ist F^φ isomorph zu F.

BEWEIS. Wir zeigen, daß die Voraussetzungen von Lemma 2.1 für F, die Einschränkung ψ von φ auf F, D und $\Delta = \{\langle d\rangle \mid d \in D\}$ erfüllt sind. Das ist für (1) und (2) nach Voraussetzung so; zu zeigen bleibt (3) von Lemma 2.1. Dann folgt wegen $\bigcap_{U \in \Delta} N_F(U) = \bigcap_{d \in D} C_F(d) = Z(F) = 1$ und $D^F = D$ aus Lemma 2.1, (*b*) die Behauptung.

Sei also $d \in D$, $U = \langle e\rangle \in \Delta$, $\langle d\rangle^\psi = \langle x\rangle$ und sei $S = \langle d, e\rangle$. Ist $o(de) \notin \{1, 2, 3, 4, \infty\}$, so ist $(U^\psi)^x = (U^d)^\psi$ nach Lemma 2.4. Ist

$o(de) = 1$ oder 2, so ist offenbar $(U^a)^\psi = U^\psi = (U^\psi)^x$. Ist $o(de) = 4$, so sind S und S^ψ Diedergruppen der Ordnung 8, und d sowie x vertauschen jeweils die beiden von $\Phi(S)$ bzw. $\Phi(S^\psi)$ verschiedenen Untergruppen in $\langle e, e^a\rangle$ bzw. $\langle e, e^a\rangle^\psi$. Ist $o(de) = \infty$, so sind S und S^ψ unendliche Diedergruppen, in denen es jeweils genau 2 Untergruppen der Ordnung 2 gibt, die mit d bzw. x ganz S bzw. S^ψ erzeugen, nämlich $U = \langle e\rangle$ und $U^a = \langle ded\rangle$ bzw. deren Bilder unter ψ, und die dann von d bzw. x vertauscht werden müssen. In beiden Fällen folgt ebenfalls $(U^a)^\psi = (U^\psi)^x$. Sei schließlich $o(de) = 3$. Dann ist F nach Voraussetzung (1) keine P-Gruppe, und nach Satz 1.6 existiert eine Primzahl q mit $|\langle a\rangle^\psi| = q$ für alle Involutionen $a \in F$. Da $\langle d, e\rangle$ eine Diedergruppe der Ordnung 6 ist, ist $q = 2$ oder $q = 3$. Wäre $q = 3$, so wäre nach Lemma 1.1 und Korollar 1.7 offenbar $o(ab) = 3$ für alle $a, b \in D$ mit $a \neq b$, und folglich wären $\langle a\rangle^\psi$ und $\langle b\rangle^\psi$ vertauschbare Untergruppen der Ordnung 3 in F^ψ. Da F^ψ von diesen Untergruppen erzeugt wird, wäre F^ψ eine elementarabelsche 3-Gruppe, was wegen (1) unmöglich ist. Somit ist $q = 2$ und $\langle d, e\rangle^\psi$ eine Diedergruppe der Ordnung 6, in der $\langle x\rangle$ die beiden anderen Untergruppen U^ψ und $(U^a)^\psi$ der Ordnung 2 vertauscht. Es folgt $(U^\psi)^x = (U^a)^\psi$, womit (3) von Lemma 2.1 in allen Fällen bewiesen ist.

Offenbar kann man unseren Satz 2.5 gut in der Situation anwenden, daß F ein direkter Faktor von G mit genügend großem Komplement ist; man vergleiche [7]. Wir werden in § 4 aber auch einige Anwendungen angeben, bei denen $F = G$ ist.

3. – Mehrfach transitive Permutationsgruppen.

Wir wollen in diesem Abschnitt zeigen, daß alle involutorisch erzeugten dreifach transitiven und gewisse zweifach transitive Permutationsgruppen vom Grad $\geqslant 4$ durch ihren Untergruppenverband bestimmt sind. Dazu benutzen wir Lemma 2.1 und müssen uns folglich um die Voraussetzungen dieses Lemmas sowie der Hilfssätze aus § 1 kümmern. Die benutzten grundlegenden Eigenschaften unendlicher Permutationsgruppen findet man in [8], Kapitel 10 und 11.

LEMMA 3.1. *Sei G eine zweifach transitive Permutationsgruppe auf der Menge Ω. Ist G eine P-Gruppe, so ist $|\Omega| = 3$ und G die symmetrische Gruppe auf Ω.*

BEWEIS. Der Stabilisator G_α eines Punktes $\alpha \in \Omega$ ist eine maximale Untergruppe und enthält keinen nichttrivialen Normalteiler von G. Es folgt $|G| = pq$ mit Primzahlen p und q; sei $p > q$. Da G zweifach transitiv ist, wird $q = p-1$, also $p = 3$ und $q = 2$.

LEMMA 3.2. *Sei G eine zweifach transitive Permutationsgruppe auf der Menge Ω und sei $|\Omega| \geqslant 4$. Ist φ eine Projektivität von G auf eine Gruppe H und $\alpha \in \Omega$, so ist G_α^φ kein Normalteiler in G^φ. Ist $\Delta = \{G_\alpha \mid \alpha \in \Omega\}$, so ist also $\bigcap_{U \in \Delta} N_G(U) = 1$ und $\bigcap_{U \in \Delta} N_H(U^\varphi) = 1$.*

BEWEIS. Da G zweifach transitiv ist, ist G_α eine maximale Untergruppe von G; ferner existiert ein $\beta \in \Omega$ mit $\beta \neq \alpha$ sowie ein $a \in G$ mit $\alpha^a = \beta$ und $\beta^a = \alpha$. Es folgt $G_\alpha^a = G_\beta \neq G_\alpha$ und $G_\alpha^{a^2} = G_\beta^a = G_\alpha$. Wäre $G_\alpha^\varphi \trianglelefteq G^\varphi$, so wäre nach Lemma 1.8 dann $G_\alpha \cap G_\alpha^a \trianglelefteq G$ und $G/(G_\alpha \cap G_\alpha^a)$ eine P-Gruppe. Da G_α keinen nichttrivialen Normalteiler enthält, folgte $G_\alpha \cap G_\alpha^a = 1$, und G wäre eine P-Gruppe im Widerspruch zu Lemma 3.1. Damit ist G_α^φ nicht normal in G^φ. Da G_α maximal in G ist, folgt $N_G(G_\alpha) = G_\alpha$ und $N_H(G_\alpha^\varphi) = G_\alpha^\varphi$ und somit $\bigcap_{U \in \Delta} N_G(U) = \bigcap_{\alpha \in \Omega} G_\alpha = 1$ und $\bigcap_{U \in \Delta} N_H(G_\alpha^\varphi) = \bigcap_{\alpha \in \Omega} G_\alpha^\varphi = (\bigcap_{\alpha \in \Omega} G_\alpha)^\varphi = 1$.

Der folgende Hilfssatz zeigt, daß bei dreifach transitiven Permutationsgruppen G vom Grade $\geqslant 4$ die Stabilisatoren G_α und G_β im Faktorverband $[G/G_{\alpha\beta}]$ zu erkennen sind.

LEMMA 3.3. *Sei G eine dreifach transitive Permutationsgruppe auf der Menge Ω mit $|\Omega| \geqslant 4$ und seien $\alpha, \beta \in \Omega$ mit $\alpha \neq \beta$. Dann existieren genau drei Untergruppen X von G mit $G_{\alpha\beta}$ maximal in X, nämlich G_α, G_β und eine dritte X mit $|X : G_{\alpha\beta}| = 2$.*

BEWEIS. Da G dreifach transitiv ist, ist $G_{\alpha\beta}$ maximal in G_α und G_β. Ferner existiert ein $g \in G$ mit $\alpha^g = \beta$ und $\beta^g = \alpha$. Dann ist $g \notin G_{\alpha\beta}$, $g^2 \in G_{\alpha\beta}$ und $(G_{\alpha\beta})^g = G_{\alpha\beta}$, also $|\langle g, G_{\alpha\beta}\rangle : G_{\alpha\beta}| = 2$. Da $g \notin G_\alpha$ und $g \notin G_\beta$, ist also $\langle g, G_{\alpha\beta}\rangle$ eine dritte Untergruppe von G, in der $G_{\alpha\beta}$ maximal ist.

Sei nun X eine beliebige Untergruppe von G, in der $G_{\alpha\beta}$ maximal ist. Wir nehmen $G_\alpha \neq X \neq G_\beta$ an und müssen dann $X = \langle g, G_{\alpha\beta}\rangle$ zeigen. Da $G_{\alpha\beta}$ maximal in G_α und G_β ist, folgt $X_\alpha = X \cap G_\alpha = G_{\alpha\beta} = X \cap G_\beta = X_\beta$. Wäre X transitiv auf Ω, so existierte ein $x \in X$ mit $\alpha^x = \beta$, also $(G_{\alpha\beta})^x = X_\alpha^x = X_\beta = G_{\alpha\beta}$. Damit wäre $X_\alpha = G_{\alpha\beta} \trianglelefteq X$, wegen der Transitivität von X also $G_{\alpha\beta} = 1$, ein Widerspruch, da $G_{\alpha\beta}$ transitiv auf $\Omega \setminus \{\alpha, \beta\}$ und $|\Omega| \geqslant 4$ ist. Damit ist X intransitiv auf Ω. Da $G_{\alpha\beta} \leqslant X$ aber transitiv auf $\Omega \setminus \{\alpha, \beta\}$ ist, folgt $\alpha^x = \beta$ und $\beta^x = \alpha$

für jedes $x \in X \setminus G_{\alpha\beta}$. Dann ist offenbar $xg \in G_{\alpha\beta}$, also $x \in \langle g, G_{\alpha\beta}\rangle$. Es folgt $X = \langle g, G_{\alpha\beta}\rangle$, was zu zeigen war.

SATZ 3.4. *Jede dreifach transitive Permutationsgruppe vom Grade $\geqslant 4$, die von Involutionen erzeugt wird, ist durch ihren Untergruppenverband bestimmt.*

BEWEIS. Sei G dreifach transitiv auf der Menge Ω, $|\Omega| \geqslant 4$, sei D die Menge der Involutionen in G, $\Delta = \{G_\alpha | \ \alpha \in \Omega\}$ und sei φ eine Projektivität von G auf eine Gruppe H. Wir wollen zeigen, daß (1)-(3) von Lemma 2.1 erfüllt sind. Dabei sind (1) und (2) vorausgesetzt; zu zeigen ist (3).

Sei dazu $d \in D$, $U = G_\alpha \in \Delta$ und $\langle d\rangle^\varphi = \langle x\rangle$. Ist $d \in U$, so ist $x \in U^\varphi$, also $(U^\varphi)^x = U^\varphi = (U^d)^\varphi$. Sei also $d \notin U$, d.h. $d = (\alpha\beta) \ldots$ mit $\alpha \neq \beta \in \Omega$. Dann ist $G_\alpha^d = G_\beta$ und $G_{\alpha\beta}^d = G_{\alpha\beta}$. Nach Lemma 3.1 ist G keine P-Gruppe und nach Korollar 1.12 somit $(G_{x\beta}^\varphi)^x = G_{\alpha\beta}^\varphi$. Nach Lemma 3.3 existieren genau drei Untergruppen in H, in denen $(G_{\alpha\beta})^\varphi$ maximal ist, nämlich G_α^φ, G_β^φ und $\langle d, G_{\alpha\beta}\rangle^\varphi$, und die folglich von x irgendwie permutiert werden müssen. Nach Lemma 3.2 ist $(G_\alpha^\varphi)^x \neq G_\alpha^\varphi$, und wegen $x \in \langle d, G_{\alpha\beta}\rangle^\varphi$ folgt schließlich $(G_\alpha^\varphi)^x = G_\beta^\varphi = (G_\alpha^d)^\varphi$. Damit ist (3) von Lemma 2.1 bewiesen. Aus Lemma 2.1 und 3.2 folgt $H \simeq G$.

Aus Satz 3.4 folgt sofort, daß alle symmetrischen und alternierenden Gruppen vom Grade $\geqslant 4$ durch ihren Untergruppenverband bestimmt sind.

KOROLLAR 3.5. *Sei Ω eine Menge mit $|\Omega| \geqslant 4$ und sei A eine unendliche Kardinalzahl. Dann sind*

$$\mathrm{Sym}(\Omega, A) = \{g \in \mathrm{Sym}(\Omega) \text{ mit } |\{\alpha \in \Omega | \ \alpha^g \neq \alpha\}| < A\}$$

und Alt (Ω) *durch ihren Untergruppenverband bestimmt.*

BEWEIS. Daß die alternierende Gruppe vom Grade 4 durch ihren Untergruppenverband bestimmt ist, ist leicht zu sehen und wohlbekannt. Alle anderen betrachteten Gruppen sind offenbar dreifach transitiv und von Involutionen erzeugt [8, S. 306].

Bekanntlich ist für jeden Körper K die zweidimensionale projektive lineare Gruppe $PGL(2, K)$ von Involutionen erzeugt und dreifach transitiv auf der Menge der eindimensionalen Teilräume eines zweidimensionalen Vektorraumes über K [8, S. 278]. Es folgt:

KOROLLAR 3.6. *Ist K ein Körper mit $|K|\geqslant 3$, so ist $PGL(2, K)$ durch ihren Untergruppenverband bestimmt.*

Wir kommen nun zu zweifach transitiven Permutationsgruppen. Hier können wir — wie in [5] im endlichen Fall — nur für spezielle Gruppen zeigen, daß sie durch ihren Untergruppenverband bestimmt sind. Immerhin werden aber die Gruppen $PSL(n, K)$ für $n\geqslant 3$ und beliebige Schiefkörper durch unsere Sätze erfaßt. Wir benötigen einen Hilfssatz, den wir etwas allgemeiner formulieren.

LEMMA 3.7. *Sei G eine Permutationsgruppe auf einer Menge Ω, von Involutionen erzeugt, keine P-Gruppe, und sei φ eine Projektivität von G auf eine Gruppe H. Seien $\alpha, \beta, \gamma \in \Omega$, $d = (\alpha\beta)(\gamma)\ldots$ eine Involution aus G, $\langle x\rangle = \langle d\rangle^\varphi$, $s = (\alpha)(\beta\gamma)\ldots$ ein Element aus G und sei $F = \langle s, G_{\alpha\beta}\rangle$. Dann gilt (a) oder (b).*

(a) *$(F^\varphi)^x = F^\varphi$, $o(x) = 3$, $G_{\alpha\beta} \trianglelefteq F$ und $|F : G_{\alpha\beta}| = 2$.*

(b) *$(F^\varphi)^x = (F^d)^\varphi$ und $o(x) = 2$.*

BEWEIS. Zunächst einmal ist $(G_{\alpha\beta})^d = G_{\alpha\beta}$ und nach Korollar 1.12 folglich $(G^\varphi_{\alpha\beta})^x = G^\varphi_{\alpha\beta}$. Zu behandeln ist also $\langle s\rangle$. Sei dazu $T = G_{\alpha\beta\gamma}$. Dann sind offenbar $d, s \in N_G(T)$, $s^2 \in T$, $sd = (\alpha\beta\gamma)\ldots$, also $(sd)^3 \in T$, und folglich ist $\langle s, d, T\rangle/T$ eine Diedergruppe der Ordnung 6. Damit sind d und d^s Involutionen, die mit T zusammen $\langle s, d, T\rangle$ erzeugen; nach Korollar 1.12 ist $T^\varphi \trianglelefteq \langle s, d, T\rangle^\varphi$. Nun induziert φ eine Projektivität von $\langle s, d, T\rangle/T$ auf $\langle s, d, T\rangle^\varphi/T^\varphi$, und folglich ist $\langle s, d, T\rangle^\varphi/T^\varphi$ elementarabelsch der Ordnung 9 oder eine Diedergruppe der Ordnung 6.

Im ersten Fall ist $o(x) = |\langle d, T\rangle^\varphi : T^\varphi| = 3$ und $(\langle s, T\rangle^\varphi)^x = \langle s, T\rangle^\varphi$, wegen $F = \langle s, G_{\alpha\beta}\rangle = \langle\langle s, T\rangle, G_{\alpha\beta}\rangle$ also schließlich $(F^\varphi)^x = F^\varphi$. Damit ist F maximal in $\langle d, F\rangle$ und nach Lemma 1.8 dann $F \cap F^d \trianglelefteq \langle d, F\rangle$ und $\langle d, F\rangle/(F \cap F^d)$ nichtabelsch der Ordnung $2p$ für eine Primzahl p. Da $F \leqslant G_\alpha$, ist $F^d \leqslant G^d_\alpha = G_\beta$, also $F \cap F^d = G_{\alpha\beta}$ und somit $G_{\alpha\beta} \trianglelefteq F$ und $|F : G_{\alpha\beta}| = 2$, da F nicht normal in $\langle d, F\rangle$ ist. Damit sind alle Aussagen in (a) gezeigt.

Im zweiten Fall ist $\langle sd, T\rangle^\varphi/T^\varphi$ erneut nach Korollar 1.12 der Normalteiler der Ordnung 3 der Diedergruppe $\langle s, d, T\rangle^\varphi/T^\varphi$. Damit ist $o(x) = |\langle d, T\rangle^\varphi : T^\varphi| = 2$, und die Involution x vertauscht die beiden x nicht enthaltenden Untergruppen der Ordnung 2 in $\langle s, d, T\rangle^\varphi/T^\varphi$. Also ist $(\langle s, T\rangle^\varphi)^x = \langle s^d, T\rangle^\varphi = (\langle s, T\rangle^d)^\varphi$ und wegen $F = \langle\langle s, T\rangle, G_{\alpha\beta}\rangle$ dann auch $(F^\varphi)^x = (F^d)^\varphi$. Das war zu zeigen.

SATZ 3.8. *Ist G eine zweifach transitive Permutationsgruppe auf der Menge Ω, $|\Omega| \geqslant 4$, mit den Eigenschaften* (1)-(3), *so ist G durch ihren Untergruppenverband bestimmt.*

(1) *G ist von Involutionen erzeugt, die Fixpunkte auf Ω haben.*

(2) *Sind $\alpha, \beta, \gamma \in \Omega$ paarweise verschieden, so existiert ein $s \in G$ mit $s = (\alpha)(\beta\gamma) \ldots$.*

(3) *Es gilt* (*a*), (*b*) *oder* (*c*).

(*a*) *G ist endlich.*

(*b*) *Für alle $\alpha \in \Omega$ ist G_α eine Rang-3-Gruppe.*

(*c*) *Für $\alpha, \beta, \gamma \in \Omega$ ist das s aus* (2) *so wählbar, daß $G_\alpha = \langle s, G_{\alpha\beta}\rangle$ gilt* (*das ist z.B. der Fall, wenn G zweifach primitiv ist*).

BEWEIS. Sei φ eine Projektivität von G auf eine Gruppe H, D die Menge der Involutionen mit Fixpunkten in G und $\Delta = \{G_\alpha : \alpha \in \Omega\}$. Wir wollen zeigen, daß (1)-(3) von Lemma 2.1 erfüllt sind. Dabei sind (1) und (2) vorausgesetzt; zu zeigen ist (3). Aus Lemma 2.1 und 3.2 folgt dann $H \simeq G$.

Sei dazu $d \in D$, $U = G_\alpha \in \Delta$ und $\langle d\rangle^\varphi = \langle x\rangle$. Ist $d \in U$, so ist $(U^\varphi)^x = U^\varphi = (U^d)^\varphi$; sei also $d \notin U$, d.h. $d = (\alpha\beta)(\gamma) \ldots$ mit paarweise verschiedenen $\alpha, \beta, \gamma \in \Omega$. Nach (2) existiert ein $s \in G$ mit $s = (\alpha)(\beta\gamma) \ldots$; sei $F = \langle s, G_{\alpha\beta}\rangle$. Nach Lemma 3.1 ist G keine P-Gruppe, und folglich gilt (*a*) oder (*b*) aus Lemma 3.7.

Erfüllt G die Voraussetzung (3*c*), so wählen wir s so, daß $F = \langle s, G_{\alpha\beta}\rangle = G_\alpha$ ist. Nach Lemma 3.2 ist dann $(F^\varphi)^x \neq F^\varphi$, nach Lemma 3.7 also $(G_\alpha^\varphi)^x = (G_\alpha^d)^\varphi$, was zu zeigen war.

Erfüllt G die Voraussetzung (3*a*), so existiert nach [5, Satz 2] ein $\delta \in \Omega$ mit $(G_\alpha^\varphi)^x = G_\delta^\varphi$, und es folgt $(F^\varphi)^x \leqslant (G_\alpha^\varphi)^x = G_\delta^\varphi$. Wäre also $(F^\varphi)^x = F^\varphi$, so wäre $F \leqslant G_\alpha \cap G_\delta = G_{\alpha\delta}$, wegen $|F| > |G_{\alpha\beta}|$ dann $\delta = \alpha$, ein Widerspruch zu Lemma 3.2. Nach Lemma 3.7 ist also $(F^\varphi)^x = (F^d)^\varphi$ und damit $F^d \leqslant G_\beta \cap G_\delta = G_{\beta\delta}$. Da $|F| > |G_{\alpha\beta}|$, folgt diesmal $\delta = \beta$, d.h. $(G_\alpha^\varphi)^x = G_\beta^\varphi = (G_\alpha^d)^\varphi$.

Wir nehmen nun an, daß G die Voraussetzung (3*b*) erfüllt. Sei $V \leqslant G$ mit $(G_\alpha^\varphi)^x = V^\varphi$; nach Lemma 3.2 ist $V \neq G_\alpha$. Gilt dann (*a*) von Lemma 3.7, so ist $G_{\alpha\beta} \leqslant F \leqslant V$ und $G_{\alpha\beta} = (G_{\alpha\beta})^s = G_{\alpha\gamma}$, d.h. $G_{\alpha\beta}$ läßt γ fest. Nach Voraussetzung hat $G_{\alpha\beta}$ genau 4 Transitivitätsgebiete auf Ω, und die sind dann $\{\alpha\}, \{\beta\}, \{\gamma\}$ und $\Omega \setminus \{\alpha, \beta, \gamma\} = \Gamma$. Wir betrachten die Transitivitätsgebiete von V auf Ω. Wegen $G_{\alpha\beta} \leqslant V$ sind das Vereinigungen der vier Transitivitätsgebiete von $G_{\alpha\beta}$. Da

$d \in G_\gamma$, ist $(G_\gamma^\varphi)^x = G_\gamma^\varphi$ und nach Korollar 1.12 ist $(G_{\alpha\beta}^\varphi)^x = G_{\alpha\beta}^\varphi$. Es folgt

$$V_\gamma^\varphi = (V \cap G_\gamma)^\varphi = V^\varphi \cap G_\gamma^\varphi = (G_\alpha^\varphi)^x \cap (G_\gamma^\varphi)^x = (G_\alpha^\varphi \cap G_\gamma^\varphi)^x =$$

$$= (G_{\alpha\gamma}^\varphi)^x = (G_{\alpha\beta}^\varphi)^x = G_{\alpha\beta}^\varphi ,$$

also $V_\gamma = G_{\alpha\beta}$. Ist Λ die γ enthaltende Bahn von V auf Ω, so ist wegen $G_{\alpha\beta} < F < V$ dann $|\Lambda| = |V : G_{\alpha\beta}| \geqslant 4$, also $\Lambda \cap \Gamma \neq \emptyset$ und damit $\Gamma \subseteq \Lambda$. Da $s = (\alpha)(\beta\gamma) \ldots \in F \leqslant V$, ist auch $\beta \in \Lambda$. Da $V \neq G_\alpha$, ist $\Omega \setminus \{\alpha\}$ keine Bahn von V und damit schließlich $\Lambda = \Omega$. Sei $v \in V$ mit $\gamma^v = \alpha$. Dann ist $G_{\alpha\beta}^v = V_\gamma^v = V_\alpha \geqslant F$; das geht nicht, da $G_{\alpha\beta}$ genau vier Bahnen und V_α wegen $s = (\alpha)(\beta\gamma) \ldots \in F$ höchstens drei Bahnen auf Ω hat.

Damit gilt (b) von Lemma 3.7, also $(F^\varphi)^x = (F^d)^\varphi$ und $o(x) = 2$. Ist $F = G_\alpha$, so sind wir fertig; sei also $F \neq G_\alpha$. Nach Satz 1.6 ist φ 2-regulär, also G^φ von Involutionen erzeugt und keine P-Gruppe. Nach Korollar 1.12 ist $(G_\alpha \cap V)^d = G_\alpha \cap V$ da $(G_\alpha^\varphi \cap V^\varphi)^x = G_\alpha^\varphi \cap V^\varphi$ gilt. Es folgt $G_\alpha \cap V \leqslant G_\alpha \cap G_\alpha^d = G_{\alpha\beta}$, andererseits ist $(G_{\alpha\beta}^\varphi)^x = G_{\alpha\beta}^\varphi$, also $G_{\alpha\beta} \leqslant G_\alpha \cap V$ und somit schließlich $G_{\alpha\beta} = G_\alpha \cap V = V_\alpha$. Wir betrachten wieder die Bahnen von V auf Ω. Die von $G_{\alpha\beta}$ seien $\{\alpha\}$, $\{\beta\}$, Γ_1 und Γ_2 mit $\gamma \in \Gamma_1$. Da $s^d = (\beta)(\alpha\gamma) \ldots \in F^d \leqslant V$, ist $\Gamma_1 \subseteq \Lambda$, wenn Λ die Bahn von α unter V ist. Wäre $\Lambda = \{\alpha\} \cup \Gamma_1$, so wäre $V_\alpha = G_{\alpha\beta}$ transitiv auf $\Lambda \setminus \{\alpha\}$, also V zweifach transitiv auf Λ. Das ist nicht der Fall, da $V_\alpha < F^d < V$ und somit V nicht einmal primitiv auf Λ ist. Wäre $\beta \in \Lambda$, so existierte ein $v \in V$ mit $\alpha^v = \beta$ und somit $G_{\alpha\beta}^v = V_\alpha^v = V_\beta \geqslant F^d$. Das geht nicht, da V_β wegen $s^d = (\beta)(\alpha\gamma) \ldots \in V$ höchstens drei, $G_{\alpha\beta}$ aber vier Bahnen auf Ω hat. Da Λ Vereinigung von Bahnen von $G_{\alpha\beta}$ sein muß, bleibt als einzige Möglichkeit $\Lambda = \{\alpha\} \cup \Gamma_1 \cup \Gamma_2$. Dann ist $\Omega \setminus \Lambda = \{\beta\}$ eine Bahn von V, also $V = G_\beta = G_\alpha^d$, was zu zeigen war.

4. – Anwendungen auf lineare Gruppen.

Wir wollen die Ergebnisse der Paragraphen 2 und 3 benutzen, um zu zeigen, daß eine Reihe von linearen Gruppen durch ihren Untergruppenverband bestimmt ist.

SATZ 4.1. *Ist K ein Schiefkörper und $n \geqslant 3$, so ist die Gruppe $PSL(n, K)$ durch ihren Untergruppenverband bestimmt.*

BEWEIS. Wir zeigen, daß die Permutationsdarstellung von $G = PSL(n, K)$ auf der Menge Ω der eindimensionalen Teilräume des n-dimensionalen K-Vektorraumes V die Voraussetzungen von Satz 3.8 erfüllt. Bekanntlich ist G zweifach transitiv auf Ω und einfach [2, S. 39], ferner natürlich $|\Omega| \geqslant 4$. Seien $\alpha = \langle u \rangle$, $\beta = \langle v \rangle$ und $\gamma = \langle w \rangle$ paarweise verschieden aus Ω. Sind u, v, w linear unabhängig, so existiert eine Involution $\sigma \in SL(V)$ mit $u^\sigma = -u$, $v^\sigma = w$, $w^\sigma = v$, und das Bild s von σ unter dem natürlichen Epimorphismus von $SL(V)$ auf G erfüllt (2). Sind u,v,w linear abhängig, also bei geeigneter Wahl von u etwa $u = av + w$ mit $0 \neq a \in K$, so existiert wegen $n \geqslant 3$ eine Involution $\sigma \in SL(V)$ mit $v^\sigma = a^{-1}w$ und $w^\sigma = av$, also $u^\sigma = u$. Damit ist (2) gezeigt, ferner, daß Involutionen mit Fixpunkten in G existieren. Da G einfach ist, folgt (1). Ähnlich leicht sieht man, daß $\{\alpha\}$, $\{\beta\}$, $\Gamma_1 = \{\gamma = \langle w \rangle : w \in \langle u, v \rangle, \gamma \neq \alpha, \beta\}$ und $\Gamma_2 = \{\gamma = \langle w \rangle : w \notin \langle u, v \rangle\}$ die Transitivitätsgebiete von $G_{\alpha\beta}$ auf Ω sind. Damit gilt (3b) von Satz 3.8, und Satz 4.1 ist bewiesen.

Für die Gruppen $PSL(2, K)$ liefert Satz 3.8 nicht mehr als partielle Resultate, da seine Voraussetzungen nur für spezielle Schiefkörper erfüllt sind. (Ist etwa K ein Körper und -1 kein Quadrat in K, so enthält $PSL(2, K)$ überhaupt keine Involution mit Fixpunkt.) Wir wollen zeigen, daß aber auch diese Gruppen durch ihren Untergruppenverband bestimmt sind, und wenden dazu Lemma 2.1 direkt an. Wir benötigen einige Ergebnisse über Transvektionen, die wir kurz zusammenstellen.

HILFSSATZ 4.2. *Sei K ein Schiefkörper, V ein zweidimensionaler K-Vektorraum, $G = PSL(V) = SL(V)/Z$ mit $Z = Z(SL(V))$ und Ω die Menge der eindimensionalen Teilräume von V. Für $\alpha = \langle v \rangle \in \Omega$ sei $T(\alpha)$ die Menge der projektiven Transvektionen zur Hyperebene α, d.h. $T(\alpha) = \{\tau Z : \tau \in SL(V)$, τ trivial auf $\langle v \rangle$ und $V/\langle v \rangle\}$. Ist $\beta = \langle w \rangle \in \Omega$ mit $\beta \neq \alpha$, so gilt (wobei Matrizen die zugehörigen Abbildungen immer bezüglich der Basis $\{v, w\}$ von V darstellen):*

(*a*) $T(\alpha) = \left\{ \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} Z : a \in K \right\}$ *ist isomorph zur additiven Gruppe $(K, +)$ von K.*

(*b*) $G_\alpha = T(\alpha) G_{\alpha\beta}$, $T(\alpha) \cap G_{\alpha\beta} = 1$, $T(\alpha) \trianglelefteq G_\alpha$.

(*c*) *Für $1 \neq S \leqslant T(\alpha)$ ist $N_G(S) \leqslant G_\alpha$.*

(*d*) *Ist das Zentrum $Z(K)$ von K unendlich und ist S eine Untergruppe von $T(\alpha)$ mit endlicher oder zyklischer Faktorgruppe $T(\alpha)/S$, so ist $C_G(S) = T(\alpha)$.*

BEWEIS. (*a*) und (*b*) sind wohlbekannt; *s.* [2, S. 4]. Da $T(\alpha) \cap \cap G_{\alpha\beta} = 1$ ist, hat S nur den einen Fixpunkt α auf Ω, der dann unter $N_G(S)$ festbleiben muß. Es folgt $N_G(S) \leqslant G_\alpha$, also (*c*). Zum Beweis von (*d*) sei $\mu\colon (K, +) \to T(\alpha)$ der Isomorphismus aus (*a*) mit $a^\mu = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} Z$ für $a \in K$ und sei $L = S^{\mu^{-1}}$. Dann ist $(K, +)/L$ zyklisch oder endlich, nach Voraussetzung aber $(Z(K), +)$ unendlich und damit nicht zyklisch. Es folgt $L \cap Z(K) \neq 0$. Nach (*c*) ist $C_G(S) \leqslant G_\alpha$, also $C_G(S) = T(\alpha)(C_G(S) \cap G_{\alpha\beta})$ nach (*b*). Zu zeigen ist $C_G(S) \cap G_{\alpha\beta} = 1$. Sei dazu $g = \begin{pmatrix} b & 0 \\ 0 & c \end{pmatrix} Z \in C_G(S) \cap G_{\alpha\beta}$. Für $a \in L$ folgt aus $a^\mu g = g a^\mu$ durch einfache Rechnung $ab = ca$. Da $L \cap Z(K) \neq 0$ folgt $b = c$ und dann $ab = ba$ für alle $a \in L$. Für $0 \neq x \in K$ ist $Lx = \{ax\colon a \in L\}$ eine zu L isomorphe Untergruppe von $(K, +)$. Wäre $L \cap Lx = 0$, so wäre Lx mit $(K, +)/L$ endlich oder zyklisch, also auch L endlich oder zyklisch. Das geht nicht, da $(K, +)$ entweder eine unendliche elementarabelsche p-Gruppe ist oder die additive Gruppe der rationalen Zahlen enthält. Somit ist $L \cap Lx \neq 0$. Sind dann $a_1, a_2 \in L$ mit $0 \neq a_1 = a_2 x$, so ist b vertauschbar mit a_1 and a_2, also auch mit x. Da x beliebig war, folgt $b \in Z(K)$ und damit $g = 1$. (Unser Beweis funktioniert offenbar auch, wenn $T(\alpha)/S$ endlich erzeugt ist, doch brauchen wir (*d*) nur in der angegebenen schwächeren Form.)

HILFSSATZ 4.3. *Mit den Voraussetzungen und Bezeichnungen von* 4.2 *sei* $r \in Z(K)$ *mit* $r \neq 0$ *und* $r^n \neq 1$ *für alle* $n \in \mathbb{N}$ *und sei* $g = \begin{pmatrix} r^{-1} & 0 \\ 0 & r \end{pmatrix} Z \in G_{\alpha\beta}$. *Ist* U *eine abelsche Untergruppe von* G *mit* $U^g = U$, *so ist* $U \leqslant G_\alpha$ *oder* $U \leqslant G_\beta$.

BEWEIS. Wir zeigen, daß jedes Element von U entweder in G_α oder in G_β liegt. Da U nicht die mengentheoretische Vereinigung zweier echter Untergruppen sein kann, folgt dann $U \leqslant G_\alpha$ oder $U \leqslant G_\beta$.

Sei dazu $u = \begin{pmatrix} a & b \\ c & d \end{pmatrix} Z \in U$. Zu zeigen ist $b = 0$ oder $c = 0$; wir nehmen also an, es wäre

(1) $b \neq 0 \neq c$.

Mit g normalisiert auch $g^n = \begin{pmatrix} r^{-n} & 0 \\ 0 & r^n \end{pmatrix} Z$ die Gruppe U, und alle r^n sind nach Voraussetzung verschieden ($n \in \mathbb{N}$). Das Polynom $x^{12} -$

$-x^{10}-x^8+x^4+x^2-1$ hat höchstens 12 Nullstellen im Körper $Z(K)$. Wir können also annehmen, daß gilt

(2) $r^{12}-r^{10}-r^8+r^4+r^2-1\neq 0$.

Da U von g normalisiert wird, liegt $u^g=\begin{pmatrix} a & r^2b \\ r^{-2}c & d \end{pmatrix}Z$ in U, und da U abelsch ist, folgt $uu^g=u^gu$. Rechnet man die Matrizen aus, so erhält man:

(3) *Es existiert ein* $s\in Z(K)$ *mit* $s\neq 0$, *so daß gilt*

(*a*) $a^2+r^{-2}bc=s(a^2+r^2bc)$,

(*b*) $r^2ab+bd=s(ab+r^2bd)$,

(*c*) $ca+r^{-2}dc=s(r^{-2}ca+dc)$,

(*d*) $r^2cb+d^2=s(r^{-2}cb+d^2)$.

Wendet man dasselbe Verfahren auf g^2 an Stelle von g an, so erhält man mit (3):

(4) *Es existiert ein* $t\in Z(K)$ *mit* $t\neq 0$, *so daß gilt*

(*a*) $a^2+r^{-4}bc=t(a^2+r^4bc)$,

(*b*) $r^4ab+bd=t(ab+r^4bd)$,

(*c*) $ca+r^{-4}dc=t(r^{-4}ca+dc)$,

(*d*) $r^4cb+d^2=t(r^{-4}cb+d^2)$.

Aus (3) folgt, daß auch a und d von 0 verschieden sind. Denn wäre $a=0$, so folgte aus (3*a*) und (1), daß $s=r^{-4}$ ist, und aus (3*b*) dann $d=0$. Aber (3*d*) lieferte damit $cb=0$, einen Widerspruch. Für $d=0$ schließt man entsprechend. Somit

(5) $a\neq 0\neq d$.

Aus (3*a*) folgt $(1-s)a^2=(r^2s-r^{-2})bc$, aus (4*a*) folgt $(1-t)a^2=(r^4t-r^{-4})bc$ und aus diesen beiden Gleichungen mit (1) und (5) dann

(6) $s\neq 1$

und

(7) $(1-s)(r^4t-r^{-4})=(1-t)(r^2s-r^{-2})$.

Benutzt man in derselben Weise die Gleichungen (3b) und (4b), so erhält man $(r^2-s)ab = (r^2s-1)bd$ und $(r^4-t)ab = (r^4t-1)bd$ und daraus

$$(8)\quad s \neq r^{-2}$$

und

$$(9)\quad (r^4t-1)(r^2-s) = (r^2s-1)(r^4-t)$$

Die Gleichungen (7) und (9) liefern eine quadratische Gleichung für s, deren höchster Koeffizient $r^{10}-r^8-r^6+r^2+1-r^{-2}$ nach (2) von 0 verschieden ist. Somit existieren höchstens zwei Lösungen für s in $Z(K)$. Aber offensichtlich lösen $s_1 = 1$, $t_1 = 1$ und $s_2 = r^{-2}$, $t_2 = r^{-4}$ die Gleichungen (7) und (9). Es folgt $s = 1$ oder $s = r^{-2}$ im Widerspruch zu (6) und (8).

Satz 4.4. *Ist K ein Schiefkörper mit $|K| > 2$, so ist die Gruppe $PSL(2, K)$ durch ihren Untergruppenverband bestimmt.*

Beweis. Wir benutzen weiter die Bezeichnungen von Hilfssatz 4.2. Ist K endlich, so folgt die Behauptung aus [5, Korollar 3]; wir können also annehmen, daß K unendlich ist. Sei φ eine Projektivität von $G = PSL(V)$ auf eine Gruppe H, D die Menge der Involutionen in G und $\Delta = \{G_\alpha : \alpha \in \Omega\}$. Dann sind wieder (1) und (2) von Lemma 2.1 erfüllt, und es genügt (3) zu zeigen; aus Lemma 2.1 und 3.2 folgt $H \simeq G$.

Sei dazu $d \in D$, $U = G_\alpha \in \Delta$ und $\langle d\rangle^\varphi = \langle x\rangle$. Ist $d \in U$, so ist $(U^\varphi)^x = U^\varphi = (U^d)^\varphi$. Sei also $d \notin U$, d.h. $d = (\alpha\beta)\ldots$ mit $\alpha \neq \beta \in \Omega$. Wir betrachten die Autoprojektivität $\psi = \varphi x \varphi^{-1}$ von G und haben $G_\alpha^\psi = G_\beta$ zu zeigen. Da G keine P-Gruppe ist, gilt nach Korollar 1.12 wieder $(G_{\alpha\beta}^\varphi)^x = G_{\alpha\beta}^\varphi$, also $G_{\alpha\beta}^\psi = G_{\alpha\beta}$. Zu untersuchen ist $T(\alpha)^\psi = T$. Wir zeigen, daß es ein $\gamma \in \Omega$ gibt mit $T \leqslant G_\gamma$ und $G_{\alpha\beta} \leqslant G_\gamma$. Dann folgt $G_\alpha^\psi = \langle T, G_{\alpha\beta}\rangle \leqslant G_\gamma$, also $G_\alpha^\psi = G_\gamma$, da beides maximale Untergruppen von G sind. Da $G_{\alpha\beta}$ keinen von α und β verschiedenen Punkt aus Ω fest läßt, ist $\gamma = \alpha$ oder $\gamma = \beta$. Aus Lemma 3.2 folgt $G_\alpha^\psi = G_\beta$, was zu zeigen war.

Sei zuerst Char $K = 0$.

Dann ist $T(\alpha) \simeq (K, +)$ abelsch und torsionsfrei und damit jedes verbandsisomorphe Bild von $T(\alpha)$ eine torsionsfreie Gruppe mit modularem Untergruppenverband, also abelsch [10, S. 19]. Insbesondere ist T abelsch. Wir zeigen, daß T von $G_{\alpha\beta}$ normalisiert wird. Da

$T(\alpha) \trianglelefteq G_\alpha$ ist, ist T modular in $G_\alpha^\psi \geqslant G_{\alpha\beta}$. Ist also $g \in G_{\alpha\beta}$, so ist nach [4, (2.1) und (2.7)] der Faktorverband $[T/T \cap T^g] \simeq [\langle T, T^g\rangle/T^g]$ wegen $\langle T, T^g\rangle \leqslant \langle T, g\rangle$ isomorph zu einem Intervall im Verband $[\langle T^g, g\rangle/T^g] \simeq [\langle g\rangle/\langle g\rangle \cap T^g]$, also isomorph zum Untergruppenverband einer Untergruppe von $\langle g\rangle/\langle g\rangle \cap T^g$. Somit ist $S = (T \cap T^g)^{\psi^{-1}} = T(\alpha) \cap (T^g)^{\psi^{-1}}$ normal in $T(\alpha)$ mit zyklischer Faktorgruppe $T(\alpha)/S$. Nach Hilfssatz 4.2, (*d*) ist $C_G(S) = T(\alpha)$, also die abelsche Gruppe $(T^g)^{\psi^{-1}}$ in $T(\alpha)$ enthalten. Es folgt $T^g \leqslant T$, also schließlich $G_{\alpha\beta} \leqslant N_G(T)$. Nach Hilfssatz 4.3 ist $T \leqslant G_\alpha$ oder $T \leqslant G_\beta$, was zu zeigen war.

Sei nun Char $K = p > 0$.

Dann ist $T(\alpha) \simeq (K, +)$ eine unendliche elementarabelsche p-Gruppe und damit $T \in P(\infty, p)$ nach [1, Theorem 11.2]. Für $g \in G_{\alpha\beta}$ ist wieder $[T/T \cap T^g]$ isomorph zum Untergruppenverband einer Untergruppe von $\langle g\rangle/\langle g\rangle \cap T^g$. Ist also $o(g)$ endlich, so ist $T \cap T^g$ eine maximale Untergruppe von T; ist $o(g)$ unendlich, so ist $\langle g\rangle \cap T^g = 1$ und dann $T \leqslant T^g$, genauso $T^g \leqslant T$ also schließlich $T = T^g$. Wir unterscheiden zwei Fälle.

I) *Die multiplikative Gruppe* $Z(K)^*$ *des Körpers* $Z(K)$ *ist eine Torsionsgruppe.*

Dann ist auch $Z = Z(SL(V))$ eine Torsionsgruppe, und jede Untergruppe $P \leqslant SL(V)$ mit $|P/Z| = p$ enthält ein Element σ der Ordnung p. Bekanntlich (s. [2, S. 97]) ist σ eine Transvektion. Damit besteht die p-Sylowgruppe A von T aus projektiven Transvektionen, die nach Hilfssatz 4.2 einen gemeinsamen Fixpunkt $\gamma \in \Omega$ haben. Somit ist $A \leqslant T(\gamma)$ und nach 4.2, (*c*) dann $T \leqslant G_\gamma$. Ist $g \in G_{\alpha\beta}$ mit $o(g) = m < \infty$, so ist $T \cap T^{g^i}$ maximal in T und folglich $S = \bigcap_{i=1}^{m} A^{g^i} \neq 1$ und $g \in N_G(S) \leqslant G_\gamma$, erneut nach 4.2, (*c*). Ebenso ist $g \in N_G(A) \leqslant G_\gamma$ für $g \in G_{\alpha\beta}$ mit $o(g) = \infty$. Es folgt $G_{\alpha\beta} \leqslant G_\gamma$, was zu zeigen war.

II) $Z(K)^*$ *enthält ein Element* r *unendlicher Ordnung.*

Dann hat auch $g = \begin{pmatrix} r^{-1} & 0 \\ 0 & r \end{pmatrix} Z \in G_{\alpha\beta}$ unendliche Ordnung, und es gilt $T^g = T$, also auch $A^g = A$, wenn A wieder die p-Sylowgruppe von T ist. Nach Hilfssatz 4.3 ist $A \leqslant G_\alpha$ oder $A \leqslant G_\beta$. Sei $\gamma = \alpha$ oder $\gamma = \beta$ so, daß $A \leqslant G_\gamma$. Ist $T \leqslant G_\gamma$, so sind wir fertig; sei also $T \nleqslant G_\gamma$ und damit $T \neq A$. Sei $X = G_\alpha^\psi \cap G_\gamma$. Da $g \in Z(G_{\alpha\beta})$ unendliche Ordnung hat, wird $G_{\alpha\beta}$ von seinen Elementen unendlicher Ordnung er-

zeugt. Die normalisieren alle T, und damit ist $T \trianglelefteq G_\alpha^\psi$ und $G_\alpha^\psi = TG_{\alpha\beta}$. Es folgt $X = (T \cap X)G_{\alpha\beta} = AG_{\alpha\beta}$ und $A \trianglelefteq X$; genauso ist $X = (T(\gamma) \cap X)\, G_{\alpha\beta} = BG_{\alpha\beta}$ mit $B = T(\gamma) \cap X \trianglelefteq X$. Wäre $A \cap B \neq 1$, so wäre $T \leqslant N_G(A \cap B) \leqslant G_\gamma$ nach Hilfssatz 4.2, (c), was nach Annahme nicht der Fall sein soll. Somit ist $A \cap B = 1$ und AB eine elementarabelsche p-Gruppe. Ist Q die p-Sylowgruppe der P-Gruppe $(AB)^{\psi^{-1}}$, so ist offenbar $|T(\alpha) : Q \cap A^{\psi^{-1}}| \leqslant p^2$ und nach Hilfssatz 4.2, (d) dann $Q \leqslant C_G(Q \cap A\psi^{-1}) = T(\alpha)$. Damit ist $|B^{\psi^{-1}}| \leqslant p^3$, also B endlich. Das geht nicht, da $X = BG_{\alpha\beta}$ und $|X : G_{\alpha\beta}|$ unendlich ist. Mit diesem Widerspruch ist $T \leqslant G_\gamma$ gezeigt and Satz 4.4 bewiesen.

Für lineare Gruppen mit Form liefert Satz 2.5 die folgenden Ergebnisse.

SATZ 4.5. *Sei K ein Körper mit Char $K \neq 2$.*

(A) Sei V ein nicht-singulärer symplektischer K-Vektorraum mit dim $V \geqslant 12$ und sei $G = PSp(V)$.

(B) Sei V ein nicht-singulärer orthogonaler K-Vektorraum mit ind $V \geqslant 6$ und -1 ein Quadrat in K; sei $G = P\Omega(V)$.

(C) Sei V ein nicht-singulärer orthogonaler K-Vektorraum mit ind $V \geqslant 12$ und sei $G = P\Omega(V)$.

(D) Sei V ein nicht-singulärer unitärer K-Vektorraum mit ind $V \geqslant 6$ und sei $G = PSU(V)$.

In jedem der Fälle A-D ist die Gruppe G durch ihren Untergruppenverband bestimmt.

BEWEIS. Sei $\tilde{G} = Sp(V)$ in Fall A, $\tilde{G} = \Omega(V)$ in den Fällen B und C sowie $\tilde{G} = SU(V)$ im Fall D, so daß also in allen Fällen $G = \tilde{G}/Z$ mit $Z = Z(\tilde{G})$ gilt. Unsere Voraussetzungen liefern bekanntlich die Existenz hyperbolischer Ebenen in V, d.h. von Teilräumen H von V mit $H = \langle u, v\rangle$, $(u, u) = 0 = (v, v)$ und $(u, v) = 1$ [3, S. 53].

Sei $\mathfrak{M}$ die Menge der hyperbolischen Ebenen in V in den Fällen A, B und D; im Fall C sei $\mathfrak{M}$ die Menge der Teilräume von V, die orthogonale Summe zweier hyperbolischer Ebenen sind. Für $H \in \mathfrak{M}$ sei σ_H die Involution in $GL(V)$ mit $x^{\sigma_H} = -x$ für $x \in H$ und $x^{\sigma_H} = x$ für $x \in H^\perp$. Da $V = H \perp H^\perp$, ist σ_H wohldefiniert und liegt offenbar in $\tilde{G}$ (s. [3, (20.4) und (20.6)] für den orthogonalen Fall). Sei schließlich $D = \{\sigma_H Z : H \in \mathfrak{M}\}$. Wir wollen zeigen, daß D die Voraussetzungen von Satz 2.5 mit $F = G$ erfüllt. Da die betrachteten Gruppen einfach sind, sind (1) und (2) von Satz 2.5 erfüllt; zu zeigen ist also (3).

Seien dazu $d = \sigma_{H_1} Z$, $e = \sigma_{H_2} Z$ aus D mit $d \neq e$, sei zur Abkürzung $\sigma_{H_i} = \sigma_i$ und sei $S = \langle d, e \rangle$. Wir zeigen:

(*) Es existieren nicht ausgeartete Teilräume X und Y von V und eine Isometrie ϱ auf V mit

(1) $H_1 + H_2 \leqslant X$,

(2) $X \perp Y$,

(3) $X^\varrho = Y$.

Dann sind wir fertig; denn für $T = S^\varrho$ gilt natürlich zunächst einmal $T \simeq S$. Ferner ist wegen $H_1 + H_2 \leqslant X$ offenbar $X^\perp \leqslant H_1^\perp \cap H_2^\perp$, und somit ist $X^{\sigma_i} = X$ und $x^{\sigma_i} = x$ für alle $x \in X^\perp$ $(i = 1, 2)$. Entsprechendes gilt für die $\sigma_i^\varrho = \tau_i$: es ist $Y^{\tau_i} = Y$ und $y^{\tau_i} = y$ für alle $y \in Y^\perp$ $(i = 1, 2)$. Da $V = X \perp Y \perp W$ mit $W = X^\perp \cap Y^\perp$, sind die σ_i mit den τ_j vertauschbar, und folglich ist $T = \langle \tau_1 Z, \tau_2 Z \rangle \leqslant C_G(S)$. Schließlich ist $S \cap T = 1$; denn ist $\mu = \sigma_1^i \sigma_2^j = \tau_1^k \tau_2^l \zeta$ mit $\zeta \in Z$, also $\zeta = c \cdot id$ mit geeignetem $c \in K$, so ist $v^\mu = v^{\sigma_1^i \sigma_2^j} = v$ für $v \in Y \perp W$ und $v^\mu = v^{\tau_1^k \tau_2^l \zeta} = v^\zeta = cv$ für $v \in X \perp W$. Ist also $W \neq 0$, so folgt $c = 1$ und $v^\mu = v$ für alle $v \in V$, d.h. $S \cap T = 1$. Ist aber $W = 0$, so folgt $\dim X \geqslant 6$ (bzw. $\dim X \geqslant 12$ im Fall C), also $X \cap H_1^\perp \cap H_2^\perp \neq 0$. Für $x \in X \cap H_1^\perp \cap H_2^\perp$ ist $cx = x^\mu = x^{\sigma_1^i \sigma_2^j} = x$, und somit ist erneut $c = 1$ und $S \cap T = 1$. Damit hat T alle in (3) von Satz 2.5 geforderten Eigenschaften.

Zu zeigen bleibt (*). Da $V = H_1 \perp H_1^\perp$, ist

$$H_1 + H_2 = H_1 \perp (H_1^\perp \cap (H_1 + H_2)) = H_1 \perp U$$

mit $U = H_1^\perp \cap (H_1 + H_2)$. Offenbar ist $\dim U \leqslant 2$ in den Fällen A, B, D und $\dim U \leqslant 4$ im Fall C. Wir betrachten zuerst den Fall, daß U eine Orthogonalbasis besitzt, d.h. $U = \langle u_1 \rangle \perp \ldots \perp \langle u_r \rangle$. Nach [3, 9.11] existieren $s = \operatorname{ind} V$ hyperbolische Ebenen E_i und ein Teilraum V_0 von V, so daß $V = E_1 \perp \ldots \perp E_s \perp V_0$, und auf Grund unserer Voraussetzungen ist $s \geqslant 2r + 2$ (bzw. $s \geqslant 2r + 4$ im Fall C). Nach [3, 9.9] existieren $v_i \in E_i$ mit $(v_i, v_i) = (u_i, u_i)$ $(i = 1, \ldots, r)$. Dann ist offenbar $U_0 = \langle v_1 \rangle \perp \ldots \perp \langle v_r \rangle \perp E_{r+1}$ (bzw. $U_0 = \langle v_1 \rangle \perp \ldots \perp \langle v_r \rangle \perp E_{r+1} \perp E_{r+2}$ im Fall C) isometrisch zu $U \perp H_1 = H_1 + H_2$, und nach dem Satz von Witt [3, 14.3] existiert eine Isometrie ν auf V mit $U_0^\nu = U \perp H_1$. Setzen wir $X = (E_1 \perp \ldots \perp E_{r+1})^\nu$ und $Y = (E_{r+2} \perp \ldots \perp E_{2(r+1)})^\nu$ (bzw $X = (E_1 \perp \ldots \perp E_{r+2})^\nu$ und $Y = (E_{r+3} \perp \ldots \perp E_{2(r+2)})^\nu$ im Fall C), so

ist offenbar $H_1 + H_2 \leqslant X$, $X \perp Y$, X nicht ausgeartet und isometrisch zu Y. Nach dem Satz von Witt existiert eine Isometrie ϱ auf V mit $X^\varrho = Y$. Damit ist (*) gezeigt, falls U eine Orthogonalbasis besitzt. Besitzt aber U keine Orthogonalbasis, so ist U symplektisch [3, S. 47 und 48] und wegen dim $U \leqslant 2$ dann eine hyperbolische Ebene. Somit ist $X = H \perp U = H_1 + H_2$ nicht ausgeartet und folglich $V = X \perp X^\perp$. Ist Y Summe zweier hyperbolischer Ebenen in $X^\perp$, so sind (1) und (2) von (*) erfüllt, und der Satz von Witt liefert das in (3) geforderte ϱ. Damit ist Satz 4.5 bewiesen.

Hat der Körper K die Charakteristik 2, so können wir mit Transvektionen arbeiten und erhalten etwas bessere Ergebnisse.

SATZ 4.6. *Sei K ein Körper mit Char $K = 2$.*

(A) Sei V ein nicht-singulärer symplektischer K-Vektorraum mit dim $V > 2$, falls $K = GF(2)$; sei $G = PSp(V) = Sp(V)$.

(B) Sei V ein nicht-singulärer unitärer K-Vektorraum mit ind $V \geqslant 2$ und sei $G = PSU(V)$.

(C) Sei V ein nicht-singulärer orthogonaler K-Vektorraum, also $g: V \to K$ eine quadratische Form auf V mit zugehöriger nicht-singulärer symplektischer Form $(\ ,\ )$, sei ind $V \geqslant 6$ und $G = P\Omega(V)$.

In jedem der Fälle A-C ist die Gruppe G durch ihren Untergruppenverband bestimmt.

BEWEIS. Wir definieren $\tilde{G}$ und Z wie im Beweis zu Satz 4.5 und setzen $D = \{\sigma Z: \sigma \text{ Transvektion in } \tilde{G}\}$. Zu zeigen sind wieder (1)-(3) von Satz 2.5 für D, wobei wir im Fall A dim $V \geqslant 4$ voraussetzen können; denn $PSp(2, K) \simeq PSL(2, K)$ [2, S. 46] ist nach Satz 4.4 durch ihren Untergruppenverband bestimmt. Ferner ist $PSp(4, 2) \simeq S_6$ bekanntlich (oder nach Satz 3.4) durch ihren Untergruppenverband bestimmt; in allen anderen Fällen ist G einfach und somit wieder (1) und (2) von Satz 2.5 trivialerweise erfüllt. Man beachte dabei im Fall C, daß wegen ind $V > 0$ die quadratische Form g jeden Wert in K annimmt und somit Transvektionen in $\tilde{G}$ existieren; in allen Fällen hat eine Transvektion σ in $\tilde{G}$ die Form $x^\sigma = x + \lambda(x, v)v$ mit geeignetem $\lambda \in K$, $v \in V$. Dabei ist immer $(v, v) = 0$ [2, S. 25] und $g(v) \in (K^*)^2$ im Fall C. Zu zeigen ist (3) von Satz 2.5.

Seien dazu $d = \sigma_1 Z$, $e = \sigma_2 Z$ aus D mit $d \neq e$, also etwa σ_i Transvektionen zu $v_i \in V$. Ist $(v_1, v_2) = 0$, so ist $o(de) = 2$ und nichts zu zeigen. Ist aber $(v_1, v_2) \neq 0$, so ist $X = \langle v_1, v_2 \rangle$ in den Fällen A und B

eine hyperbolische Ebene, und es existiert wegen $\dim V \geqslant 4$ bzw. ind $V \geqslant 2$ eine hyperbolische Ebene Y und ein Teilraum W von V, so daß $V = X \perp Y \perp W$. Ferner existiert eine Isometrie ϱ von V mit $X^\varrho = Y$. Setzen wir wieder $S^\varrho = T$ und $\sigma_i^\varrho = \tau_i$, so ist $T \simeq S$ und $T \leqslant C_G(S)$, da die σ_i auf $Y \perp W$ und die τ_i auf $X \perp W$ die Identität bewirken; ist ferner $\mu = \sigma_1^i \sigma_2^j = \tau_1^k \tau_2^l \zeta$ mit $\zeta = c \cdot id \in Z$, so bewirkt μ auf $Y \perp W$ die Identität und auf $X \perp W$ Multiplikation mit c. Ist also $W \neq 0$, so folgt $c = 1$ und $S \cap T = 1$; ist aber $W = 0$, so ist $\dim V = 4$ und dann $1 = \det \zeta = c^4$, also $c = 1$ und erneut $S \cap T = 1$. Damit hat T die geforderten Eigenschaften.

Im Fall C existiert nach Voraussetzung ein total-singulärer Teilraum U der Dimension 6 in V. Dann ist $\dim (U \cap X^\perp) \geqslant 4$; es existieren also hyperbolische Ebenen H_i $(i = 1, \ldots, 4)$ und ein Teilraum W von $X^\perp$, so daß $V = X \perp H_1 \perp \ldots \perp H_4 \perp W$ ist (wobei $\perp$ sich auf die symplektische Form $(\ ,\ )$ bezieht; vergl. [3, 10.10]). Da $X^{\sigma_i} = X$ und $x^{\sigma_i} = x$ für $x \in X^\perp$, ist $\langle \sigma_1, \sigma_2 \rangle$ isomorph zu einer Untergruppe von $SL(2, K)$. Seien τ_1, τ_2 Involutionen in $O(V)$, die auf $H_1 \perp H_2$ eine zu $\langle \sigma_1, \sigma_2 \rangle$ isomorphe Gruppe erzeugen [2, S. 68], auf $H_3 \perp H_4$ genauso wie auf $H_1 \perp H_2$ und auf $X \perp W$ trivial operieren. Nach [3, 20.6] sind $\tau_1, \tau_2 \in \tilde{G}$; sei $T = \langle \tau_1 Z, \tau_2 Z \rangle$. Da $\dim V \geqslant 12$, ist $W \neq 0$, und da alle σ_i, τ_j trivial auf W operieren, ist $\langle \sigma_1, \sigma_2 \rangle \cap Z = 1 = \langle \tau_1, \tau_2 \rangle \cap Z$. Somit ist $T \simeq \langle \tau_1, \tau_2 \rangle \simeq \langle \sigma_1, \sigma_2 \rangle \simeq S$, ferner offenbar $T \leqslant C_G(S)$ und $T \cap S = 1$. Damit hat T die gewünschten Eigenschaften, und Satz 4.6 ist bewiesen.

LITERATURVERZEICHNIS

[1] R. Baer, *The significance of the system of subgroups for the structure of the group*, Amer. J. Math., **61** (1939), pp. 1-44.

[2] J. Dieudonné, *La géométrie des groupes classiques*, Berlin-Heidelberg-New York, Springer, 1971.

[3] B. Huppert, *Geometric algebra*, Lecture notes, University of Illinois at Chicago Circle, 1968/69.

[4] R. Schmidt, *Modulare Untergruppen endlicher Gruppen*, Illinois J. Math., **13** (1969), pp. 358-377.

[5] R. Schmidt, *Untergruppenverbände zweifach transitiver Permutationsgruppen*, Math. Zeitschrift, **144** (1975), pp. 161-168.

[6] R. Schmidt, *Untergruppenverbände endlicher einfacher Gruppen*, Geometriae Dedicata, **6** (1977), pp. 275-290.

[7] R. SCHMIDT, *Untergruppenverbände direkter Produkte von Gruppen*, Archiv Math., **30** (1978), pp. 229-235.
[8] W. R. SCOTT, *Group theory*, Englewood Cliffs, Prentice-Hall, 1964.
[9] M. SUZUKI, *On the lattice of subgroups of finite groups*, Trans. Amer. Math. Soc., **70** (1951), pp. 345-371.
[10] M. SUZUKI, *Structure of a group and the structure of its lattice of subgroups*, Ergebnisse der Mathematik Band **10**, Berlin-Göttingen-Heidelberg, Springer, 1956.
[11] G. ZAPPA, *Fondamenti di Teoria dei gruppi - I*, Roma, Edizioni Cremonese, 1965.

Manoscritto pervenuto in redazione il 20 agosto 1979.