TECHNISCHE UNIVERSITÄT WIEN

VIENNA UNIVERSITY OF TECHNOLOGY

DIPLOMARBEIT

3-erzeugte p-Gruppen, deren maximale Untergruppen alle 2-erzeugt sind

AUSGEFÜHRT AN DER
Institut für Analysis und Scientific Computing

UNTER DER ANLEITUNG VON
Ao.Univ.Prof. Mag.rer.nat. Dr.phil. Wolfgang Herfort

DURCH

Julian Wergieluk
Neubaugürtel 23/9B, 1150 Wien

Datum

Unterschrift (Student)

Inhaltsverzeichnis

Kurzfassung

In dieser Arbeit werden vor allem 2-Gruppen mit den im Titel angegebenen Eigenschaften untersucht. Erzeuger und Relationen für solche Gruppen, deren maximale Untergruppen H stets $d(H) = 2$ erfüllen, werden angegeben. Die Ergebnisse wurden ursprünglich von Yakov Berkovich in [BJ06] publiziert. Die hier angegebenen Beweismethoden scheinen kürzer zu sein.

Einleitung

In [BJ06] wurden vor allem in Kapitel 4 nicht 2-erzeugte Gruppen, deren sämtliche maximalen Untergruppen 2-erzeugt sind, untersucht. Zweck der vorliegenden Arbeit ist eine vereinfachte Darstellung folgender technisch relevanter Details:

- Ist G eine nilpotente 3-erzeugte Gruppe der Klasse 2 und Ordnung p^6, deren maximale Untergruppen 2-erzeugt sind, so erweist sich G als $\mathcal{A}_2$-Gruppe der Ordnung 2^6 mit sehr speziellen Relationen. Dieses in [BJ06] bewiesene Lemma wird hier auf die Klassifikation quadratischer Formen und den Satz von Chavalley-Warning zurückgeführt.

- Erweiterungen der im ersten Abschnitt beschriebenen Gruppen spielen eine wichtige Rolle bei der Klassifikation der $\mathcal{A}_2$-Gruppen, welche 2-Gruppen sind. Im zweiten Abschnitt werden die in [BJ06], Th. 4.2-4.4 beschriebene Gruppen untersucht. Die hier vorgestellten Beweise weichen gänzlich von der in [BJ06] angegebenen ab. Es werden Hall-Witt Identitäten benutzt, um mittels passender Automorphismen, die in den Gruppen geltende Relationen in eine Standardform zu bringen. Diese Methode scheint deutlich kürzer zu sein, als die in [BJ06] beschriebene.

Notation

Die in dieser Arbeit verwendete Notation wurde weitgehend an [Hup67] angelehnt.

G — endliche p-Gruppe der Ordnung $|G| = p^n$.
$\exp(G)$ — Exponent von G.
$c(G)$ — Nilpotenzklasse von G.
$d(G)$ — Anzahl der Elemente eines minimalen Erzeugendensystems von G.
$H \leq G$ — H ist Untergruppe von G.
$H \trianglelefteq G$ — H ist Normalteiler von G.
$[x, y] = x^{-1}y^{-1}xy$ — Kommutator von $x, y \in G$.
$[A, B] = \langle [a, b] \mid a \in A, b \in B \rangle$.
$G' = \langle [x, y] \mid x, y \in G \rangle = [G, G]$ — Kommutatoruntergruppe von G.
$K_1(G) = G$, $K_n(G) = [G, K_{n-1}(G)]$ — Glieder der absteigender Zentralreihe von G.
$\Phi(G)$ — Frattinigruppe von G, Durchschnitt aller maximalen Untergruppen.
$Z(G)$ — Zentrum von G.
$\Omega_1(G) = \langle x \in G \mid x^p = 1 \rangle$.
$\mho_1(G) = \langle x^p \mid x \in G \rangle$.
Γ_1 — Menge der maximalen Untergruppen von G.
E_{p^n} — elementar-abelsche Gruppe der Ordnung p^n.
C_{p^n} — zyklische Gruppe mit p^n Elementen.
$\mathbb{F}_p$ — der endliche Körper mit p Elementen.
$\mathbb{F}_p^*$ — multiplikative Gruppe von $\mathbb{F}_p$.
$\mathcal{A}_n$-Gruppe — p-Gruppe G, deren Untergruppen H folgende Bedingungen erfüllen: (i) alle H vom Index p^n sind abelsch. (ii) es existiert ein nichtabelsches $H \leq G$ mit Index p^{n-1}.

Kapitel 1

Gruppe der Ordnung p^6

1.1 Definition und einfache Eigenschaften

Lemma 1 *Sei G eine nilpotente p-Gruppe und $N \trianglelefteq G$. Falls $N \leq \Phi(G)$, dann ist $d(G/N) = d(G)$.*

Beweis. $G = \langle x_1, \ldots, x_{d(G/N)}, N\rangle = \langle x_1, \ldots, x_{d(G/N)}\rangle$. □

Lemma 2 *Sei G eine 3-erzeugte p-Gruppe mit der Eigenschaft, dass alle maximalen Untergruppen von G 2-erzeugt sind. Es gilt:*

1. *Für alle $H \in \Gamma_1$ gilt $\Phi(G) = \Phi(H)$.*
2. *G/G' ist elementar-abelsch.*
3. *$\mho_1(G) \leq G'$ und somit $\Phi(G) = G'$. Ist ferner $c(G) = 2$ so erhalten wir $\Phi(G) = G' \leq Z(G)$.*
4. *Für $c(G) = 2$ ist G' elementar-abelsch.*
5. *Falls $|G| \geq p^6$ gilt, dann sind alle maximalen Untergruppen von G nichtabelsch.*
6. *Für $|G| \geq p^5$ ist $Z(G) \leq \Phi(G)$ und $Z(G) = \Phi(G)$ falls $c(G) = 2$.*
7. *$\Omega_1(G) = \Phi(G)$.*
8. *Für $|G| = p^6$ ist jede Untergruppe K von G mit $[G : K] \geq p^2$ elementar-abelsch. G ist in diesem Fall eine $\mathcal{A}_2$-Gruppe.*

Beweis.

1. Wegen $d(G) = 3$ und $d(H) = 2$ für alle $H \in \Gamma_1(G)$, ist $|\Phi(G)| = |\Phi(H)| = p^3$. Maximalität von H impliziert $\Phi(G) \leq H$ und $\Phi(G) = H \cap \Phi(G) = H \cap G'G^p \leq \Phi(H) \Rightarrow \Phi(G) = \Phi(H)$.

2. G/G' ist abelsch und 3-erzeugt wegen $G' \leq \Phi(G)$. Für $H \in \Gamma_1(G)$ ist H/G' maximale Untergruppe von G/G' und $d(H/G') = 2$. G/G' ist also eine 3-erzeugte abelsche Gruppe, deren sämtliche maximalen Untergruppen 2-erzeugt sind. G/G' lässt sich wie folgt schreiben:

$$G/G' \cong C_{p^\alpha} \oplus C_{p^\beta} \oplus C_{p^\gamma}$$

   Wäre $\alpha > 1$ so wäre $H \cong pC_{p^\alpha} \oplus C_{p^\beta} \oplus C_{p^\gamma}$ echte 3-erzeugte Untergruppe von G/G'. Widerspruch. Es folgt $G/G' \cong E_{p^3}$.

3. Da G/G' elementar-abelsch ist, folgt $G^p \leq G'$ und damit $\Phi(G) = G'G^p = G'$. Mit $c(G) = 2$ gewinnen wir auch $\Phi(G) \leq Z(G)$.

4. Für beliebige $a, b \in G$ gilt $[a, b]^p = [a, b^p] = 1$ wegen $b^p \in G^p \leq G'$ und $c(G) = 2$. Es folgt $\exp G' = p$.

5. Angenommen, es gibt ein abelsches $H \in \Gamma_1(G)$. Dann ist $\Phi(H) = H'H^p = H^p = G' = \Phi(G)$. H ist 2-erzeugt, also ist H^p höchstens 2-erzeugt. Für $|G| \geq p^6$ ist aber $G' \cong E_{p^{|G|-3}}$. Widerspruch.

6. Angenommen, es existiert ein $z \in Z(G) \backslash \Phi(G)$. Aus dem Basissatz von Burnside folgt $G = \langle z, a, b\rangle$ mit geeigneten $a, b \in G$. Wir erhalten $\langle a, b\rangle \lhd G \Rightarrow G' = \langle z\rangle' \langle a, b\rangle' [\langle z\rangle, \langle a, b\rangle] \Rightarrow G' = \langle [a, b]\rangle$ im Widerspruch zu $G' \cong E_{p^{|G|-3}}$.

7. Angenommen, es existiert ein $x \in \Omega_1(G) \setminus \Phi(G)$. x ist in einer maximalen Untergruppe H von G enthalten und es existiert nach dem Basissatz von Burnside ein minimales Erzeugendensystem E von H mit $x \in E$. Aus $d(H) = 2$ folgt $H = \langle a, x\rangle$ und daher $\Phi(H) = \langle \langle x^p\rangle, \langle a^p\rangle, \langle [a, x]\rangle\rangle \cong E_{p^3} \Rightarrow x^p \neq 1$. Widerspruch.

8. Jede Untergruppe K von G mit Index $[G : K] = p^2$ ist maximal in einer maximalen Untergruppe H von G. K enthält $\Phi(H) = \Phi(G) \leq Z(G)$ wobei $\Phi(G) \cong E_{p^3}$ und muss daher elementar-abelsch sein. Weiters ist jede Untergruppe mit größerem Index wiederum in einer Untergruppe mit Index p^2 enthalten und daher auch elementar-abelsch.

□

Hilfssatz 3 (Zassenhaus, [Rot95]) *Sei G eine endliche Gruppe in der für alle $x, y \in G$ die Relation $x^n y^n = (xy)^n$ erfüllt ist. Für natürliches $n > 1$ definieren wir:*

$$\Pi_n(G) := \{x \in G \mid x^n = 1\} \quad \amalg_n(G) := \{x^n \mid x \in G\}.$$

Es gilt:

1. $\Pi_n(G) \trianglelefteq G$ *und* $\amalg_n(G) \trianglelefteq G$.
2. $|\amalg_n(G)| = [G : \Pi_n(G)]$.

Beweis.

1. Ist $x, y \in \Pi_n(G)$ so auch $xy \in \Pi_n(G)$, da $1 = x^n y^n = (xy)^n$. Analog erhält man $\amalg_n(G) \leq G$. Für $x \in \amalg_n(G)$ und $g \in G$ berechnen wir

   $$g^{-1} x^n g = (g^{-1} x g)^n \in \amalg_n(G).$$

   Ähnlich erhalten wir für $x \in \Pi_n(G)$:

   $$(g^{-1} x g)^n = g^{-1} x^n g = g^{-1} g = 1.$$

   Es folgt $x^g \in \Pi_n(G)$.

2. Die Abbildung

   $$.^n : G \to \Pi_n(G)\ ,\ x \mapsto x^n$$

   ist wegen der Voraussetzung $(xy)^n = x^n y^n\ \forall x, y \in G$ ein Homomorphismus mit Kern $\Pi_n(G)$, da

   $$x^n = y^n \Leftrightarrow (xy^{-1})^n = 1 \Leftrightarrow xy^{-1} \in \Pi_n(G).$$

Lemma 4 *Sei G eine 3-erzeugte p-Gruppe der Klasse 2 gegeben, deren sämtliche maximalen Untergruppen 2-erzeugt sind. Ist $p > 2$ dann gelten:*

$$\Omega_1(G) = \{x \in G \mid x^p = 1\} \quad \mho_1(G) = \{x^p \mid x \in G\} = G' = \Omega_1(G)$$

Beweis. G ist endliche Gruppe der Klasse 2 und somit erfüllt für $n = p$ die Voraussetzungen des Lemma 3. Es gilt daher

$$\Omega_1(G) = \Pi_p(G) = \langle x \in G \mid x^p = 1 \rangle$$
$$\mho_1(G) = \amalg_p(G) = \langle x^p \mid x \in G \rangle$$

und weiters

$$[G : \mho_1(G)] = |\Omega_1(G)| = |\Phi(G)| = p^3$$

und daher $\mho_1(G) = \Omega_1(G)$. □

Lemma 5 (Erzeugende Relationen) *Sei eine Gruppe G wie in Lemma 4 gegeben. Dann haben die von $G = \langle a, b, c\rangle$ erfüllten Relationen folgende Gestalt:*

$$\begin{array}{lll} x := c^p, & y := b^p, & z := a^p, \\ [b,c] = z, & [a,b] = x^\alpha y^\beta z^\kappa, & [a,c] = x^\gamma y^\delta z^\lambda \end{array}$$

mit $\alpha, \beta, \ldots \in \mathbb{F}_p$ und $\gamma\beta - \alpha\delta \neq 0$.

Beweis. Sei zunächst $p > 2$ vorausgesetzt. Die Gruppe G ist 3-erzeugt, also dürfen wir $G = \langle \tilde{a}, b, c\rangle$ ansetzen. Da $\exp G = p^2$ gilt und jedes Element der Ordnung p in $\Phi(G)$ liegt, erzeugen die Elemente $\{b, c\}$ eine maximale Untergruppe H von G. Für die Frattinigruppe von H ergibt sich:

$$\Phi(H) = \mho_1(H)H' = \langle b^p, c^p\rangle\langle [b,c]\rangle = \Phi(G) \cong E_{p^3}$$

somit ist $z := [b, c]$ ein nicht-triviales Element von $\Phi(G)$, das nicht in $\langle b^p, c^p\rangle$ liegen kann. Nach Lemma 4 ist $\Phi(G) = \mho_1(G) = \{x^p \mid x \in G\}$ und daher können wir ein Element $a \in G\backslash H$ finden, das $z = a^p$ erfüllt. Mit $G = \langle a, b, c\rangle$ ergibt sich

$$G' = \langle a^p, b^p, c^p\rangle = \langle [a,b], [a,c], [b,c]\rangle.$$

Wir legen $x := c^p$ und $y := b^p$ fest und erhalten

$$[a,b] = x^\alpha y^\beta z^\kappa, \quad [a,c] = x^\gamma y^\delta z^\lambda.$$

Wir können G' als einen 3-dimensionalen Vektorraum über dem endlichen Körper mit p Elementen ansehen. In diesem Kontext sind $\{x, y, z\}$ und $\{[a,b], [a,c], [b,c]\}$ Basen von G' und somit linear unabhängig. Diese Beobachtung, notiert in der Matrizenschreibweise

$$\begin{vmatrix} 0 & 0 & 1 \\ \alpha & \beta & \kappa \\ \gamma & \delta & \lambda \end{vmatrix} \neq 0$$

ergibt $\gamma\beta - \alpha\delta \neq 0$.

Für $p = 2$ zeigen wir zunächst, dass G' nur Kommutatoren enthalten kann. Da $G' = \langle [a,b], [a,c], [b,c]\rangle \leq Z(G)$ ist, lassen sich beliebige Elemente von G' in der Form

$$[a,b]^\alpha [a,c]^\beta [b,c]^\gamma \tag{1.1}$$

schreiben, wobei $\alpha, \beta, \gamma \in \mathbb{F}_2$. Sind nicht alle Exponenten in (1.1) gleich 1, so können wir uns der Formeln $[ab, c] = [a, c][b, c]$ oder $[a, bc] = [a, c][a, b]$ bedienen. Im Falle $\alpha = \beta = \gamma = 1$ setzen wir

$$[a,b][a,c][b,c] = [a^\lambda b^\mu c^\nu, a^\rho b^\sigma c^\tau]$$

an. Zerlegung des Kommutators auf der rechten Seite führt auf das Gleichungssystem

$$\begin{aligned} 1 &= \lambda\sigma + \mu\rho \\ 1 &= \lambda\tau + \nu\rho \\ 1 &= \mu\tau + \nu\sigma. \end{aligned}$$

Kurze Rechnung liefert eine der Lösungen: $\lambda = \nu = \sigma = \tau = 1$, $\mu = \rho = 0$.

Unser Ziel ist es nun, ein Erzeugendensystem $\langle a, b, c\rangle = G$ zu konstruieren, sodass $a^2 = [b, c]$ gilt. Wir behaupten zunächst, dass es in $G' \setminus \{1\}$ ein Element geben muss, das als Quadrat darstellbar ist. Wäre das Gegenteil der Fall, so hätten wir $x^2 = 1\ \forall x \in G$, da laut Lemma 2 $\mho_1(G) \leq G$ gilt. Es folgt $\exp G = 2$ und $1 = (xy)^2 = x^2y^2[x, y] = [x, y] \Rightarrow G' = 1$. Widerspruch. Es existiert also $k \in G' \setminus \{1\}$ mit $k = [b, c] = a^2$. Wegen $k \neq 1$ sind b und c modulo $\Phi(G)$ linear unabhängig und erzeugen eine maximale Untergruppe von G. Wäre $a \in \langle b, c\rangle$ so folgt $a = b^\beta c^\gamma [b, c]^\kappa$ und daher $(b^\beta c^\gamma [b, c]^\kappa)^2 = (b^2)^\beta (c^2)^\gamma [b, c] = a^2 = [b, c] \Rightarrow (b^2)^\beta (c^2)^\gamma = 1 \Rightarrow \beta \equiv \gamma \equiv 0\ (2) \Rightarrow a \in G'$. Widerspruch. Es gilt also $\langle a, b, c\rangle = G$. Der verbleibende Teil des Beweises wird genau wie im Fall $p > 2$ vollzogen. □

Lemma 6 (Maximale Untergruppen für $p > 2$) *Die in Lemma 4 beschriebene Gruppe $G = \langle a, b, c\rangle$ hat genau $p^2 + p + 1$ verschiedene maximale Untergruppen, wobei sich diese nach der Gestalt der Erzeuger folgendermaßen aufteilen lassen:*

$$\begin{aligned} H_{uv} &= \langle ac^u, bc^v\rangle \quad 0 \leq u, v \leq p - 1 \\ K_w &= \langle ab^w, c\rangle \quad 0 \leq w \leq p - 1 \\ L &= \langle b, c\rangle \end{aligned}$$

Diese Charakterisierung erlaubt nun genauere Beschreibung der Frattinigruppen:

	$\mho_1(M)$	M'	*Bedingung*
$\Phi(H_{uv})$	zx^u, yx^v	$x^{\gamma v+\alpha} y^{\delta v+\beta} z^{\lambda v-u+\kappa}$	$-u^2 + \delta v^2 + \lambda uv + \kappa u$ $+\beta v - \gamma v - \alpha \neq 0$
$\Phi(K_w)$	zy^w, x	$x^\gamma y^\delta z^{\lambda+w}$	$w^2 + \lambda w - \delta \neq 0$
$\Phi(L)$	x, y	z	

Die angegebenen Bedingungen drücken die in Lemma 2 bewiesene Relation $\Phi(M) \cong E_{p^3}$ aus.

Beweis. Lemma 2 können wir entnehmen, dass 2-erzeugte Untergruppen von G entweder p^2 oder p^5 Elemente haben können, wobei die p^2-elementigen zur Gänze in $\Phi(G)$ enthalten sind. Daraus lässt sich ableiten, dass jede zweielementige modulo $\Phi(G)$ linear unabhängige Menge $E \subset G \setminus \Phi(G)$ eine maximale Untergruppe erzeugt. Die Faktorgruppe $G/\Phi(G)$ ist isomorph zu E_{p^3} und somit ein 3-dimensionaler Vektorraum über den Körper $\mathbb{F}_p$ mit p Elementen. Maximale Untergruppen von G werden kanonisch auf 2-dimensionale Unterräume von $G/\Phi(G)$ abgebildet. Die Suche nach allen maximalen Untergruppen der Gruppe G kann also auf das Auffinden aller 2-dimensionalen Unterräume in $G/\Phi(G)$ zurückgeführt werden. Diese wiederum sind umkehrbar eindeutig durch ihre orthogonalen Komplemente, also durch eindimensionalen Unterräume festgelegt:

$$L \perp \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\rangle \quad K_w \perp \left\langle \begin{pmatrix} -w \\ 1 \\ 0 \end{pmatrix} \right\rangle \quad H_{uv} \perp \left\langle \begin{pmatrix} -u \\ -v \\ 1 \end{pmatrix} \right\rangle \quad u, v, w \in \mathbb{F}_p$$

Auf obiger Überlegung stützt sich die Berechnung von Erzeugendensystemen der Frattinigruppen. Wir fangen mit $\Phi(H_{uv})$ an:

$$\begin{aligned}
\mho_1(H_{uv}) &= \langle (ac^u)^p, (bc^v)^p \rangle = \langle a^p (c^p)^u, b^p (c^v)^p \rangle = \langle zx^u, yx^v \rangle \\
H'_{uv} &= \langle ac^u, bc^v \rangle' = \langle [ac^u, bc^v] \rangle = \langle [a, bc^v][c^u, bc^v] \rangle = \\
&= \langle [a, c^v][a, b][c^u, c^v][c^u b] \rangle = \langle (x^\gamma y^\delta z^\lambda)^v x^\alpha y^\beta z^\kappa z^{-u} \rangle = \\
&= \langle x^{\gamma v + \alpha} y^{\delta v + \beta} z^{\lambda v - u + \kappa} \rangle \\
\mho_1(K_w) &= \langle (ab^w)^p, c^p \rangle = \langle zy^w, x \rangle \\
K_w &= \langle ab^w, c \rangle' = \langle [ab^w, c] \rangle = \langle [a, c][b^w, c] \rangle = \langle x^\gamma y^\delta z^{\lambda + w} \rangle \\
L^p &= \langle b^p, c^p \rangle = \langle x, y \rangle \\
L' &= \langle b, c \rangle' = \langle [b, c] \rangle = \langle z \rangle
\end{aligned}$$

Aus $\Phi(H_{uv}) = \mho_1(H_{uv}) H'_{uv} \cong E_{p^3}$ erhalten wir

$$\begin{vmatrix} u & v & \gamma v + \alpha \\ 0 & 1 & \delta v + \beta \\ 1 & 0 & \lambda v - u + \kappa \end{vmatrix} = -u^2 + \delta v^2 + \lambda uv + \kappa u + \beta v - \gamma v - \alpha \neq 0.$$

Ähnlich für $\Phi(K_w)$ ergibt sich

$$\begin{vmatrix} 1 & 0 & \gamma \\ 0 & w & \delta \\ 0 & 1 & \lambda + w \end{vmatrix} = w^2 + \lambda w - \delta \neq 0.$$

□

Ähnliche Überlegungen können auch im Falle $p = 2$ durchgeführt werden. Die Rechnungen verlaufen hier anders, weil sich die Formel

$$(ab)^p = a^p b^p [a,b]^{\binom{p}{2}} = a^p b^p \tag{1.2}$$

für $p = 2$ zu

$$(ab)^2 = a^2 b^2 [a,b] \tag{1.3}$$

reduziert.

Wir notieren

$$\begin{aligned}
\Phi(H_{uv}) &= \langle (ac^u)^2, (bc^v)^2, [ac^u, bc^v] \rangle \\
(ac^u)^2 &= ac^u ac^u = a^2 (c^2)^u [a,c]^u = x^{u(1+\gamma)} y^{\delta u} z^{1+\lambda u} \\
(bc^v)^2 &= b^2 (c^2)^v [b,c]^v = x^v y z^v \\
[ac^u, bc^v] &= [a,c]^v [a,b][b,c]^u = (x^\gamma y^\delta z^\lambda)^v x^\alpha y^\beta z^\kappa z^u = \\
&= x^{\gamma v + \alpha} y^{\delta v + \beta} z^{\lambda v + \kappa + u} \\
\Phi(K_w) &= \langle (ab^w)^2, c^2, [ab^w, c] \rangle = \\
(ab^w)^2 &= a^2 (b^2)^w [a,b]^w = z y^w (x^\alpha y^\beta z^\kappa)^w = x^{\alpha w} y^{w(1+\beta)} z^{\kappa w + 1} \\
c^2 &= x \\
[ab^w, c] &= [a,c][b,c]^w = x^\gamma y^\delta z^{\lambda + w}
\end{aligned}$$

und daraus

$$\begin{aligned}
\Phi(H_{uv}) &= \langle x^{u(1+\gamma)} y^{\delta u} z^{1+\lambda u}, x^v y z^v, x^{\gamma v + \alpha} y^{\delta v + \beta} z^{\lambda v + \kappa + u} \rangle \\
\Phi(K_w) &= \langle x^{\alpha w} y^{w(1+\beta)} z^{\kappa w + 1}, x, x^\gamma y^\delta z^{\lambda + w} \rangle \\
\Phi(L) &= \langle x, y, z \rangle .
\end{aligned}$$

$\Phi(H_{uv}) \cong E_{2^3}$ ist äquivalent zu

$$\begin{vmatrix} u(1+\gamma) & v & \gamma v + \alpha \\ v\delta & 1 & \delta v + \beta \\ 1 + u\lambda & v & \lambda v - u + \kappa \end{vmatrix} \neq 0 \quad \forall u, v \in \mathbb{F}_2 \iff$$

$$\begin{aligned}
(\delta\gamma - \delta\lambda) v^3 + \\
((\delta\lambda - \delta\gamma) u + \delta - \delta\kappa + \delta\alpha) v^2 + \\
((\lambda - \beta - \gamma\beta + \lambda\beta) u + \beta - \gamma) v + \\
(-1 - \gamma) u^2 + (\gamma\kappa + \kappa - \lambda\alpha) u - \alpha = 1 \quad \forall u, v \in \mathbb{F}_2 .
\end{aligned} \tag{1.4}$$

$\Phi(K_w) \cong E_{2^3}$ bedeutet

$$\begin{vmatrix} \alpha w & 1 & \gamma \\ w(1+\beta) & 0 & \delta \\ w\kappa + 1 & 0 & \lambda + w \end{vmatrix} \neq 0 \quad \forall w \in \mathbb{F}_2$$

oder

$$-(\beta+1)w^2 + (-\lambda - \lambda\beta + \delta\kappa)w + \delta = 1 \quad \forall w \in \mathbb{F}_2. \tag{1.5}$$

$\Phi(L) = \langle x, y, z \rangle \cong E_{2^3}$ gilt bei beliebiger Wahl der Koeffizienten $\alpha, \beta, \ldots \in \mathbb{F}_2$.

Mit Hilfe der Gleichungen (1.4) und (1.5) können wir nun versuchen, die möglichen Werte der Koeffizienten $\alpha, \beta, \ldots \in \mathbb{F}_2$ zu ermitteln. Einsetzen von $w = 0$ bzw. $u = 0, v = 0$ in (1.4) bzw. (1.5) liefert $\delta = 1$ und $\alpha = 1$ und durch das Auswerten aller verbleibenden Kombinationen der Werte u, v, w erhalten wir Gleichungssystem

$$\begin{aligned} -\beta - \lambda - \lambda\beta + \kappa &= 1 \\ \gamma\beta + 1 &= 1 \\ -\lambda + 1 - \kappa + \beta &= 1 \\ -\gamma + \gamma\kappa + \kappa - \lambda &= 1 \\ -\gamma\beta + \lambda\beta + \gamma\kappa &= 1 \end{aligned}$$

welches zwei Lösungen besitzt:

$$\begin{aligned} &\beta = 0,\ \gamma = 1,\ \kappa = 1,\ \lambda = 0 \\ &\tilde{\beta} = 1,\ \tilde{\gamma} = 0,\ \tilde{\kappa} = 0,\ \tilde{\lambda} = 1 \end{aligned}$$

Diese führen uns auf folgendes Paar erzeugender Relationen

$$[a, b] = a^2c^2, \quad [a, c] = b^2c^2 \tag{1.6}$$

$$[\tilde{a}, \tilde{b}] = \tilde{b}^2\tilde{c}^2, \quad [\tilde{a}, \tilde{c}] = \tilde{a}^2\tilde{b}^2 \tag{1.7}$$

Jede Gruppe mit einem Erzeugendensystem der (1.6) erfüllt, besitzt ein Erzeugendensystem das der Relationen (1.7) genügt und umgekehrt. Geht man nämlich von (1.6) aus und setzt $\tilde{b} := bc$ so ergibt sich

$$\begin{aligned} [a, \tilde{b}] &= [a, bc] = [a, b][a, c] = \\ &= a^2c^2b^2c^2 = a^2c^2\tilde{b}^2[b, c] = a^2c^2\tilde{b}^2a^2 = \tilde{b}^2c^2 \\ [a, c] &= b^2c^2 = \tilde{b}^2[b, c] = a^2\tilde{b}^2. \end{aligned}$$

Wir fassen unsere Ergebnisse zusammen:

Lemma 7 (Erzeugende Relationen im Falle $p = 2$) *Die in Lemma 4 beschriebene 2-Gruppe $G = \langle a, b, c\rangle$ genügt den Relationen*

$$[a, b] = a^2c^2, \quad [a, c] = b^2c^2, \quad [b, c] = a^2.$$

□

1.2 Quadratische Formen

Die in diesem Abschnitt vorgeführte Darstellung der quadratischen Funktionen wurde an [Bol01] angelehnt. Für die ausführliche Beschreibung der Theorie der quadratischen Formen sei auf [Ser96] verwiesen.

Im folgenden wird mit $\mathbf{V}$ stets ein n-dimensionaler Vektorraum über einem Körper $\mathbb{K}$ der Charakteristik $p \neq 2$ bezeichnet.

Definition 8 *Unter einer* Quadratischen Funktion *verstehen wir eine Abbildung $Q : \mathbf{V} \to \mathbb{K}$ folgender Bauart:*

$$Q(v) = q(v - h) + l(v - h) + c \tag{1.8}$$

$q : \mathbf{V} \to \mathbb{K}$ ist dabei eine quadratische Form, $l \in \mathbf{V}^*$ eine Linearform, $c \in \mathbb{K}$ und $h \in \mathbf{V}$.

Der Vektor h in (1.8) kann auch durch einen anderen Vektor $k \in \mathbf{V}$ ersetzt werden.

$$\begin{aligned} Q(v) &= q(v - k + (k - h)) + l(v - k + (k - h)) + c = \\ &= q(v - k) + l(v - k) + \\ &\quad + 2b_q(v - k, k - h) + q(k - h) + l(k - h) + c \end{aligned} \tag{1.9}$$

Mit b_q bezeichnen wir die mit q assoziierte symmetrische Bilinearform, die mit Hilfe der Spaltformel

$$b_q(v, w) = q(w + v) - q(w) - q(v)$$

gewonnen werden kann. Nach (1.9) notieren wir $Q(v) = q(v-k)+\tilde{l}(v-k)+\tilde{c}$ mit

$$\begin{aligned} \tilde{l} &= l(v - k) + 2b_q(v - k, k - h) \in \mathbf{V}^* \\ \tilde{c} &= q(k - h) + l(k - h) + c = Q(k) \in \mathbb{K}. \end{aligned}$$

Beim Übergang $h \to k$ bleibt also die quadratische Form q unberührt.

Lemma 9 *Sei $b : \mathbf{V} \times \mathbf{V} \to \mathbb{K}$ eine Bilinearform und eine Abbildung*

$$d_b : \mathbf{V} \to \mathbf{V}^*, v \mapsto b(., v)$$

gegeben. d_b ist genau dann eine Bijektion, wenn b nicht ausgeartet ist.

Beweis.

1. Ist b ausgeartet, so existiert $w \in \mathbf{V} \setminus \{0\}$ mit $b(., v) \equiv 0 \Rightarrow \ker d_b \neq \{0\} \Rightarrow d_b$ nicht injektiv.

2. Sei b nicht ausgeartet, $(b_1, \ldots, b_n)$ eine Basis von $\mathbf{V}$ und $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ beliebig. Es gilt $\alpha_1 b(., b_1) + \cdots + \alpha_n b(., b_n) = 0 \iff b(., \alpha_1 b_1 + \cdots + \alpha_n b_n) = 0 \iff \alpha_1 b_1 + \cdots + \alpha_n b_n = 0 \iff \alpha_i = 0 \; \forall i \Rightarrow \dim d_b(\mathbf{V}) = \dim \mathbf{V} = \dim \mathbf{V}^* \Rightarrow d_b$ ist Bijektion.

Ist q in (1.8) nicht ausgeartet, so gibt es stets ein $h_0 \in \mathbf{V}$ mit

$$Q(v) = q(v - h_0) + Q(h_0).$$

Auf einem Vektorraum $\mathbf{V}$ mit einer quadratischen Form q kann stets mit Hilfe der assoziierten Bilinearform b_q ein Skalarprodukt erklärt werden. Dieses induziert eine Orthogonalitätsrelation auf $\mathbf{V}$ und auf der Menge aller Unterräume von $\mathbf{V}$. $\mathbf{V}$ heißt *orthogonale innere direkte Summe* $U_1 \oplus \ldots \oplus U_k$ der Unterräume $U_1, \ldots, U_k$ wenn $\mathbf{V}$ direkte Summe der (U_i) ist und diese paarweise orthogonal sind. q eingeschränkt auf einen Unterraum U von $\mathbf{V}$ ist wieder eine quadratische Form.

Ist umgekehrt $(U_i, q_i)_i$ eine endliche Familie von Vektorräumen mit quadratischen Formen so kann auf $U_1 \times \ldots \times U_k$ eine quadratische Form $(q_1 \oplus \ldots \oplus q_k)(u_1, \ldots, u_k) := q_1(u_1) + \ldots + q_k(u_k)$ erklärt werden. In dem so konstruierten Vektorraum $U_1 \oplus \ldots \oplus U_k$ sind die Unterräume U_i paarweise orthogonal.

Definition 10 *Quadratische Form $q : \mathbf{V} \to \mathbb{K}$* repräsentiert *$a \in \mathbb{K}^*$, wenn es ein $v \in \mathbf{V} \setminus \{0\}$ mit $q(v) = a$ gibt.*

Lemma 11 *Sei $q : \mathbf{V} \to \mathbb{K}$ nicht ausgeartete quadratische Form, $a \in \mathbb{K}^*$ beliebig und $h : \mathbb{K} \to \mathbb{K}$ eine nicht ausgeartete quadratische Form die $-a$ auf $\mathbb{K}$ repräsentiert. Dann sind folgende Aussagen äquivalent:*

1. *q repräsentiert a.*

2. *$q \oplus h$ repräsentiert* 0.

Beweis.

1. q repräsentiert a so gibt es ein $v \in \mathbf{V} \setminus \{0\}$ mit $q(v) = a \Rightarrow (q \oplus h)(v, x) = 0$ wobei $h(x) = -a$ nach Voraussetzung.

2. Umgekehrt sei $(v, x) \in \mathbf{V} \oplus \mathbb{K} \setminus \{(0, 0)\}$ mit $(q \oplus h)(v, x) = q(v) + h(x) = 0$ gegeben. Ist $x \neq 0$ so folgt $h(x) \neq 0$. Sei $h(y) = -a$ und $y = \alpha x \Rightarrow -a = h(y) = h(\alpha x) = \alpha^2 h(x) \Rightarrow (1/\alpha^2) q(v) = g(v/\alpha) = h(x) = a$. Fall $x = 0$ ist gleichbedeutend mit $q(v) = 0$. Für alle $x, y \in \mathbf{V}$ sei $xy := b_q(x, y)$ festgelegt. q ist nicht ausgeartet so $\exists z \in \mathbf{V} \setminus \{0\} : vz = 1$. Sei $y = 2z - q(z)v$ so erhalten wir $q(y) = 4q(z) - 4q(z)vz + q(z)^2 q(v) = 0$ und $vy = b_q(v, 2z - q(z)v) = 2b_q(v, z) + q(z)q(v) = 2$. Wir skalieren y sodass $vy = 1$ gilt und berechnen $q(v + \frac{a}{2}y) = q(v) + ab_q(v, y) + q(\frac{a}{2}y) = a$.

1.3 Satz von Chavalley-Warning

Für diesen Abschnitt sei q eine feste Potenz einer Primzahl $p \neq 2$ und $\mathbb{F}_q$ der endliche Körper mit q Elementen. Für jedes Polynom $f \in \mathbb{K}[X_1, \ldots, X_n]$ über einem Körper $\mathbb{K}$ definieren wir

$$S(f) := \sum_{x \in \mathbb{K}^n} f(x) \in \mathbb{K}.$$

Lemma 12 ([Ser96], S. 5) *Für jedes $n \in \mathbb{N}$ gilt für $X^n \in \mathbb{F}_q[X]$:*

$$S(X^n) = \sum_{x \in \mathbb{F}_q} x^n = \begin{cases} -1 & \text{falls } n \geq 1 \text{ und } (q-1) | n \\ 0 & \text{sonst} \end{cases}$$

Beweis. Wir vereinbaren $0^0 = 1$ und betrachten folgende Fälle.

1. Ist $n \geq 1$ und $q - 1$ Teiler von n, so ergibt sich

$$S(X^n) = \sum_{x \in \mathbb{F}_q} x^n = \sum_{x \in \mathbb{F}_q} x^{(q-1)k} = \sum_{x \in \mathbb{F}_q^*} 1^k + 0^n = (q-1) \cdot 1 = -1$$

   da $\mathbb{F}_q^*$ zyklische Gruppe der Ordnung $q - 1$ ist.

2. Ist $n \geq 1$ und nicht durch $q - 1$ teilbar so gilt für ein $y \in \mathbb{F}_q^*$ mit $y^n \neq 1$

$$S(X^n) = \sum_{x \in \mathbb{F}_q} x^n = \sum_{x \in \mathbb{F}_q} y^n x^n = y^n S(X^n).$$

   Daraus folgt $S(X^n) = 0$.

3. Für $n = 0$ berechnen wir

$$S(X^n) = \sum_{x \in \mathbb{F}_q} x^0 = q \cdot 1 = 0.$$

Lemma 13 (Chevalley-Warning, [Ser96], S. 5) *Sei eine Polynomfamilie*

$$f_i \in \mathbb{F}_q[X_1, \ldots, X_n]$$

mit der Eigenschaft

$$\sum_i \operatorname{grad} f_i < n$$

gegeben und bezeichne mit V die Menge der gemeinsamen Nullstellen von (f_i) in $\mathbb{F}_q$. Es gilt

$$|V| \equiv 0 \ (p).$$

Beweis. Wir definieren

$$P = \prod_i (1 - f_i^{q-1}).$$

Für $x \notin V$ gibt es ein f_i mit $f_i(x) \in \mathbb{F}_q^*$ woraus $f_i(x)^{q-1} = 1$ und $P(x) = 0$ folgt. Wenn x Nullstelle aller f_i ist, dann erhalten wir $P(x) = \prod_i 1 = 1$. Somit ist P die charakteristische Funktion der Nullstellenmenge V. Daraus ergibt sich $|V| \equiv S(P)$ modulo p. Aus $\sum_i \operatorname{grad} f_i < n$ erhalten wir $\operatorname{grad} P < (q-1)n$. Betrachten wir beliebigen Term $\alpha X^{u_1} \cdot \ldots \cdot X^{u_n}$ von P. Wegen $\sum u_i < n(q-1)$ können wir mindestens einen Exponenten $u_j < q-1$ finden. Wir nehmen o.B.d.A. $j = 1$ an und erhalten

$$\begin{aligned} S(X^{u_1} \cdot \ldots \cdot X^{u_n}) &= \sum_{(x_1,\ldots,x_n) \in \mathbb{F}_q^n} x_1^{u_1} \cdot \ldots \cdot x_n^{u_n} = \\ &= \sum_{(x_2,\ldots,x_n) \in \mathbb{F}_q^{n-1}} x_2^{u_2} \cdot \ldots \cdot x_n^{u_n} \sum_{x_1 \in \mathbb{F}_q} x_1^{u_1} = 0. \end{aligned}$$

Daraus ergibt sich $S(P) = 0$ modulo p. □

Unmittelbare Konsequenz des obigen Satzes ist

Lemma 14 *Alle quadratischen Formen in mindestens 3 Variablen über dem Körper $\mathbb{F}_q$ haben eine Nullstelle in $\mathbb{F}_q^*$.*

1.4 Existenz

Lemma 15 (Nichtexistenz im Falle $p > 2$) *Für $p > 2$ gibt es keine wie in Lemma 4 beschriebene Gruppe.*

Beweis. Laut Lemma 6 ist die Existenz einer solchen Gruppe G äquivalent zur Unlösbarkeit der Gleichungen

$$-u^2 + \delta v^2 + \lambda uv + \kappa u + \beta v - \gamma v - \alpha = 0 \tag{1.10}$$

$$w^2 + \lambda w - \delta = 0 \tag{1.11}$$

für jede Wahl der Koeffizienten $\alpha, \beta, \gamma, \delta, \kappa, \lambda \in \mathbb{F}_p$. Gleichung (1.11) ist unlösbar genau dann, wenn die Diskriminante

$$\lambda^2 + 4\delta \tag{1.12}$$

kein Quadrat in $\mathbb{F}_p$ ist. Nehmen wir an, das ist der Fall. (1.12) ist zugleich die Diskriminante der quadratischen Form $q(u, v) := -u^2 + \delta v^2 + \lambda uv$ in (1.10) und diese ist in Folge dessen nicht ausgeartet. Daraus folgt, wir können $h, k \in \mathbb{F}_p$ finden, sodass sich (1.10) in der Form

$$q(u - h, v - k) = c \in \mathbb{F}_p \tag{1.13}$$

schreiben lässt. Da $q(u, v)$ eine quadratische Form zweiten Grades ist, folgt die Lösbarkeit von (1.13) für beliebige Wahl von $\alpha, \beta, \ldots \in \mathbb{F}_p$. □

Kapitel 2

Gruppen der Ordnung 2^7 und 2^8

2.1 Eigenschaften und Rechenregeln

Lemma 16 (Kommutatoridentitäten) *Sei G eine Gruppe und $[a,b,c] := [[a,b],c]$. Es gelten folgende Identitäten:*

1. $[a,bc] = [a,c][a,b]^c = [a,c][a,b][a,b,c]$
   $[ab,c] = [a,c]^b[b,c] = [a,c][a,c,b][b,c]$
2. $[ab,c] = [a,c]^b[b,c] = [a,c][a,c,b][b,c]$
3. $[a,b] = [b,a]^{-1}$
4. $[a,b]^m = [a^m,b] = [a,b^m]$ $\forall m \in \mathbb{Z}$ *falls* $[x,y]$ *mit* x *und* y *vertauschbar.*

Wenn G zusätzlich von der Klasse 3 ist, dann gelten

5. $[a,b,c][b,c,a][c,a,b] = 1$ *(Spezialfall der* Hall-Witt-*Identität)*
6. $[a,[b,c]] = [c,a,b][a,b,c]$
7. $[a,b,c]^m = [a,b,c^m] = [[a,b]^m,c]$
8. $[x,[a,b]]^m = [x^m,[a,b]] = [x,[a,b]^m]$

Lemma 17 $[K_i(G), K_j(G)] \leq K_{i+j}(G)$ $\forall i,j \in \mathbb{N}$.

Die Beweise der Lemmata 16 und 17 sowie ausführliche Diskussion der Kommutatoruntergruppen findet man in [Hup67].

Im Lemma 7 wurden die erzeugenden Relationen der 2-Gruppe aus Lemma 4 wie folgt angegeben:

$$[a,b] = a^2c^2, \quad [a,c] = b^2c^2, \quad [b,c] = a^2.$$

In diesem Kapitel verwenden wir eine andere, aus [BJ06] stammende Form der Relationen:

$$[a,b] = c^2, \quad [a,c] = b^2c^2, \quad [b,c] = a^2b^2$$

Lemma 18 *Sei G eine 3-erzeugte p-Gruppe der Klasse 3, deren maximale Untergruppen alle 2-erzeugt sind. Es gelten folgende Aussagen:*

1. *Wir kürzen $K_n(G)$ mit K_n ab und notieren einfachste Folgerungen: $1 \leq K_3 \leq Z(G) \leq K_2$ sowie $K_3 < K_2$ und $K_4 = 1$.*
2. *G' ist abelsch.*

Sei noch zusätzlich vorausgesetzt, dass G/K_3 isomorph zu der in Lemma 4 beschriebenen 2-Gruppe ist, so lässt sich folgendes über G aussagen:

3. *Es gilt $\mho_1(G/K_3) \leq \Phi(G/K_3) = \Omega_1(G/K_3) = (G/K_3)' = G'/K_3 = Z(G/K_3)$ und $\mho_1(G/K_3) = \mho_1(G)/K_3$.*
4. *Für alle $x \in G'$ gilt $x^p \in K_3$.*
5. *K_3 ist elementar-abelsch.*
6. $\exp G \leq p^2$.
7. *G' ist elementar-abelsch.*

Beweis.

1. Gilt wegen $c(G) = 3$.
2. Aus Lemma 17 folgt $G'' = [K_2, K_2] \leq K_4 = 1$.
3. $\Phi(G/K_3) = \Omega_1(G/K_3) = (G/K_3)' = Z(G/K_3)$ ist unmittelbare Konsequenz der früheren Untersuchungen. Die übrigen Aussagen folgen, da für einen beliebigen Homomorphismus φ einer Gruppe H $\varphi(H') = (\varphi H)'$ und $\varphi(H^p) = (\varphi H)^p$ gilt.
4. Wegen Lemma 2 ist G'/K_3 elementar-abelsch, also $x^p \equiv 1$ modulo K_3. Es folgt $x^p \in K_3$.
5. Für $k \in G'$ und $a \in G$ ist $[k,a] \in K_3$ und $[k,a]^p = [k,a^p] = [k^p,a] = 1$ wegen Lemma 17 und $k^p \in K_3$.

6. Angenommen $\exp G \geq p^3 \Rightarrow \exists C \leq G$ mit $C \cong C_{p^3}$. Da $x^{p^2} \in K_3 \; \forall x \in G$ und K_3 elementar-abelsch folgt $K_3 \cap C \cong C_p$ und $C/K_3 \cong C_{p^2}$ in G/K_3. Jede Untergruppe $H \leq G/K_3$ der Ordnung p^2 ist nach Lemma 2 elementar-abelsch. Widerspruch.

7. Nachdem $G' = \langle [a,b], [a,c], [b,c], K_3 \rangle$ kommutativ vom Exponent höchstens 2^2 ist, kann jedes Element aus G' in der Form $[a,b]^\alpha [a,c]^\beta [b,c]^\gamma k_3$ mit $\alpha, \beta, \gamma \in \mathbb{F}_4$ und $k_3 \in K_3$ dargestellt werden. Wir berechnen

$$\begin{aligned}([a,b]^\alpha [a,c]^\beta [b,c]^\gamma k_3)^2 = \\ = ((c^2\mu)^\alpha (b^2c^2\nu)^\beta (a^2b^2\kappa)^\gamma k_3)^2 = ((c^4)^\alpha (b^4c^4)^\beta (a^4b^4)^\gamma) = 1\end{aligned}$$

$\Rightarrow \exp G' = 2$.

Lemma 19 (Weitere Kommutatoridentitäten) *Sei G eine p-Gruppe wie in Lemma 18 gegeben, wobei zusätzlich $p = 2$ festgesetzt wird. Für $x, y, z, a, b \in G$, $r, s, t \in G'$ und $k, l \in K_3$ sind folgende Identitäten erfüllt:*

1. $[xk, yl] = [x, y]$
2. $[xr, ys, zt] = [x, y, z]$
3. $[xy, a, b] = [x, a, b][y, a, b]$
   $[a, xy, b] = [a, x, b][a, y, b]$
   $[a, b, xy] = [a, b, x][a, b, y]$
4. $[x, y^2] = [x, y, y] \quad [x^2, y] = [x, y, x]$

Beweis.

1. Wegen $k, l \in K_3 \leq Z(G)$ erhalten wir $[xk, yl] = k^{-1}x^{-1}l^{-1}y^{-1}xkyl = k^{-1}kl^{-1}l[x, y]$.

2. Wir berechnen zuerst

$$[x, y, zt] = [x, y, t][x, y, z][x, y, z, t] = [x, y, z]$$

mit $[x, y, t], [x, y, z, t] \in K_4$. Analog ist

$$[xr, y, z] = [[x, y]^r [r, y], z] = [x, y, z]^{[r,y]} [r, y, z] = [x, y, z]$$

und

$$[x, ys, z] = [ys, x, z] = [y, x, z] = [x, y, z].$$

3.

$$\begin{aligned}[xy,a,b] &= [[xy,a],b] = [[x,a][y,a]k,b] = [[x,a][y,a],b] = \\ &= [x,a,b]^{[y,a]}[y,a,b] = [x,a,b][y,a,b] \\ [a,xy,b] &= [xy,a,b] = [x,a,b][y,a,b] = [a,x,b][a,x,b] \\ [a,b,xy] &= [a,b,y][a,b,x]^y = [a,b,x] = [a,b,y]\end{aligned}$$

4.

$$\begin{aligned}[x,y^2] &= [x,y][x,y][x,y,y] = [x,y,y] \\ [x^2,y] &= [x,y][x,y,x][x,y] = [x,y,x]\end{aligned}$$

□

Wir legen für den Rest des Kapitels fest, dass mit G, wenn nichts anderes gesagt wird, stets eine 3-erzeugte 2-Gruppe der Klasse 3 gemeint ist, mit der Eigenschaften, dass alle maximalen Untergruppen 2-erzeugt sind und $G/K_3(G)$ isomorph zu der in Lemma 2 beschriebenen Gruppe der Ordnung 2^6 ist.

Aufgrund dieser Definition und Lemma 2 erhalten wir folgende Relationen

$$1 = a^4 = b^4 = c^4, \quad [a,b] = c^2\mu, \quad [a,c] = b^2c^2\nu, \quad [b,c] = a^2b^2\kappa \qquad (2.1)$$

mit $\mu, \nu, \kappa \in K_3(G) =: K_3$.

2.2 Berechnung der höheren Kommutatoren

Wir listen zunächst alle Kommutatoren der Ordnung 3, die mit Hilfe der Elemente a, b, c erzeugbar sind. Da G eine 2-Gruppe und G' elementarabelsch ist, erhalten wir $[a,b] = [b,a]^{-1} = [b,a]$ was den Schluss $[x,y,z] = [y,x,z]$ für beliebige $x, y, z \in G$ nach sich zieht und uns erlaubt nur solche Kommutatoren zu betrachten, deren erste 2 Symbole der lexikographischen Ordnung genügen. Bei der Untersuchungen bedienen wir uns primär der

Relationen (2.1) und der Kommutatoridentitäten des Lemma 16.

$$
\begin{aligned}
&[a,b,c] = [c^2k_3,c] = [c^2,c] = 1\\
&[a,c,b] = [b^2c^2k_3,b] = [b^2c^2,b]^{k_3}[k_3,b] = [b^2,b]^{c^2}[c^2,b] = [c^2,b] = [b,c^2]\\
&[b,c,a] = [a^2b^2k_3,a] = [a^2b^2,a] = [a^2,a]^{b^2}[b^2,a] = [a,b^2]\\
&[a,b,a] = [c^2k_3,a] = [c^2,a] = [a,c^2] = [a^2,b]\\
&[a,b,b] = [c^2,b] = [b,c^2] = [a,b^2]\\
&[a,c,a] = [a^2,c] = [b^2c^2,a] = [b^2,a][c^2,a] = [a,b,b][a,c,c]\\
&[a,c,c] = [b^2c^2,c] = [b^2,c][b^2,c,c^2][c^2,c] = [b^2,c]\\
&[b,c,b] = [b^2,c] = [c,b,b] = [b,[b,c]] = [b,a^2b^2] =\\
&\qquad = [b,b^2][b,a^2][b,a^2,b^2] = [a^2,b]\\
&[b,c,c] = [a^2b^2,c] = [a^2,c][a^2,c,b^2][b^2,c] = [a^2,c][b^2,c] = [b,c^2]
\end{aligned}
$$

Aus diesen Berechnungen sind nun folgende Gleichungen ablesbar:

$$
\begin{aligned}
&[a,b,c] = 1\\
&[a,c,b] = [a,b,b] = [b,c,a] = [b,c,c]\\
&[a,b,a] = [a,c,c] = [b,c,b]\\
&[a,c,a][b,c,c][b,c,b] = 1
\end{aligned}
\tag{2.2}
$$

wobei die letzte eine Folgerung der HALL-WITT-Identität ist. Obige Gleichungen teilen uns die dreifachen mit a,b,c erzeugten Kommutatoren in drei Klassen auf, die nicht verschieden zu sein brauchen. Multiplizieren wir zwei Elemente aus diesen Klassen, so erhalten wir auf Grund der letzten Identität aus (2.2) entweder einen Repräsentanten aus einer der übrigen Klassen oder 1. Daraus leiten wir ab, dass $K_3 = \{1,[a,b,a],[a,c,a],[b,c,c]\}$ und daher höchstens von der Ordnung 2^2 ist. Für diese Elemente wollen wir Abkürzungen einführen:

$$m := [a,b,a], \quad k := [a,c,a], \quad l := [b,c,c].$$

2.3 Wechsel des Erzeugendensystems von G

Wir entwickeln nun zwei auf der Menge aller Erzeugendensysteme wirkende Transformationen, mit der Zielsetzung, zusätzliche Informationen über die Gruppenstruktur zu erhalten und die Relationen (2.1) präziser zu formulieren.

Transformation T7

Diese Transformation wird durch die Abbildung

$$(a, b, c) \to (b, c, ac) =: (a', b', c')$$

vermittelt. $\{a, b, c\}$ ist genau dann ein Erzeugendensystem von G, wenn $\{a\Phi(G), b\Phi(G), c\Phi(G)\}$ die Faktorgruppe $G/\Phi(G)$ erzeugt. $G/\Phi(G)$ ist elementar-abelsch von Ordnung 2^3 und somit isomorph zu $\mathbb{F}_2^3$. Wir können $\{a, b, c\}$ mit Vektoren der kanonischen Basis von $\mathbb{F}_2^3$ identifizieren und auf diese Transformation T7 anzuwenden:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} =: A$$

Die Spaltenvektoren von A entsprechen genau der transformierten Elementen (a', b', c') und A kann als die Koordinatenmatrix der von T7 vermittelten linearen Bijektion interpretiert werden. Aus diesen Überlegungen ist es ersichtlich, dass (a', b', c') ebenfalls ein Erzeugendensystem von G ist und da A von der Ordnung 7 ist, muss auch T7 von dieser Ordnung sein.

Wir untersuchen, wie sich die Werte von μ, ν, κ unter T7 verändern.

$$\begin{aligned}
\mu' &= [a', b']c'^2 = [b, c](ac)^2 = [b, c]acac = [b, c]a^2c[a, c]c = \\
&= [b, c]a^2c^2[a, c][a, c, c] = a^2b^2[b, c]b^2c^2[a, c][a, b, a] = \kappa\nu m \\
\nu' &= [a', c']b'^2c'^2 = [b, ac]c^2(ac)^2 = [b, c][a, b][b, a, c]c^2(ac)^2 = \\
&= [b, c][a, b][a, b, c]c^2a^2c[a, c]c = [b, c][a, b]c^2a^2c^2[a, c][a, c, c] = \\
&= [a, b]c^2[b, c]a^2b^2[a, c]b^2c^2[a, c, c] = \mu\kappa\nu m \\
\kappa' &= [b', c']a'^2b'^2 = [c, ac]b^2c^2 = [c, c][c, a][c, a, c]b^2c^2 = \\
&= [a, c]b^2c^2[a, c, c] = \nu m
\end{aligned}$$

Somit erhalten wir $(\mu, \nu, \kappa) \to (\kappa\nu m, \mu\kappa\nu m, \nu m) =: (\mu', \nu', \kappa')$. Es gilt insbesondere $\mu', \nu', \kappa' \in K_3$ und die neuen Erzeuger a', b', c' erfüllen wieder die Relationen (2.2). Weiters ist

$$\begin{aligned}
m' &= [a', b', a'] = [b, c, b] = m \\
k' &= [a', c', c'] = [b, ac, ac] = [b, a, c][b, c, ac] = \\
&= [b, a, a][b, a, c][b, c, a][b, c, c] = [a, b, a][a, b, c][b, c, a][b, c, c] = \\
&= [a, b, a] = k \\
l' &= [b', c', c'] = [c, ac, ac] = [c, a, ac][c, c, ac] = \\
&= [c, a, a][c, a, c] = [a, c, a][c, a, c] = [b, c, c] = l.
\end{aligned}$$

Transformation T-G

Eine weitere Transformation sei durch folgende Vorschrift definiert:

$$(a,b,c) \to (af, bg, ch) \quad f,g,h \in G'$$

Sie wirkt sich folgendermaßen auf die Elemente μ, ν, κ aus:

$$\begin{aligned}
\mu' &= [a',b']c'^2 = [af,bg](ch)^2 = [a,bg][a,f,bg][f,bg](ch)^2 = \\
&= [a,g][a,b][a,b,g][a,f,b][f,g][f,b][f,b,g](ch)^2 = \\
&= [a,g][a,b][b,f](ch)^2 = [a,g][b,f][c,h][a,b]c^2 = \\
&= [a,g][b,f][c,h]\mu \\
\nu' &= [a',c']b'^2c'^2 = [af,ch](bg)^2(ch)^2 = \\
&= [a,ch][a,ch,f][f,ch](bg)^2(ch)^2 = \\
&= [a,h][a,c][a,c,h][f,h][f,c][f,c,h](bg)^2(ch)^2 = \\
&= [a,h][c,f][a,c](bg)^2(ch)^2 = [a,h][c,f][a,c]b^2[b,g]c^2[c,h] = \\
&= [a,h][c,f][b,g][c,h][a,c]b^2c^2 = [a,h][b,g][c,fh]\nu \\
\kappa' &= [b',c']a'^2b'^2 = [bg,ch](af)^2(bg)^2 = \\
&= [b,ch][g,ch][b,ch,g](af)^2(bg)^2 = \\
&= [b,h][b,c][b,c,h][g,h][g,c][g,c,h][b,c,g][b,h,g](af)^2(bg)^2 = \\
&= [b,h][b,c][g,c]a^2[a,f]b^2[b,g] = [a,f][b,gh][c,g]\kappa
\end{aligned} \tag{2.3}$$

Als Hilfsüberlegung wollen wir nun dreifache Kommutatoren von der Bauart $[u,w]$ mit $u \in \{a,b,c\}$ und $w \in G'$ näher ansehen. Nach Lemma 18 ist G' elementar-abelsch und daher lässt sich beliebiger Kommutator w aus G' in der Form $w = [a,b]^\xi[a,c]^\eta[b,c]^\zeta$ schreiben, wobei $\xi,\eta,\zeta \in \{0,1\}$ ist. Wir wollen die Abhängigkeit des Kommutators $[u,w]$ von der Exponenten ξ,η,ζ genauer studieren.

Bei der Berechnungen erweist sich folgende, für alle $x,a,b,c \in G$ geltende Identität als sehr nützlich:

$$[x,abc] = [x,c][x,ab][x,ab,c] = [x,c][x,b][x,a][x,a,b][x,a,c][x,b,c].$$

Nun gilt unter der Voraussetzung $x = [a,b]^\xi[a,c]^\eta[b,c]^\zeta$ folgendes:

$$\begin{aligned}
[a,x] &= [a,[a,b]^\xi[a,c]^\eta[b,c]^\zeta] = [a,[b,c]^\zeta][a,[a,c]^\eta][a,[a,b]^\xi] = \\
&= [c,a,b]^\zeta[a,b,c]^\zeta[c,a,a]^\eta[a,a,c]^\eta[b,a,a]^\xi[a,a,b]^\xi = \\
&= l^\zeta k^\eta m^\xi = k^\zeta m^\zeta k^\eta m^\xi = k^{\eta+\zeta}m^{\xi+\zeta} \\
[b,x] &= [b,[a,b]^\xi[a,c]^\eta[b,c]^\zeta] = [b,[b,c]^\zeta][b,[a,c]^\eta][b,[a,b]^\xi] = \\
&= [c,b,b]^\zeta[b,b,c]^\zeta[c,b,a]^\eta[b,a,c]^\eta[b,b,a]^\xi[b,a,b]^\xi = \\
&= m^\zeta l^\eta l^\xi = m^\zeta l^{\xi+\eta} = m^{\xi+\eta+\zeta}k^{\xi+\eta} \\
[c,x] &= [c,[a,b]^\xi[a,c]^\eta[b,c]^\zeta] = [c,[b,c]^\zeta][c,[a,c]^\eta][c,[a,b]^\xi] = \\
&= [c,c,b]^\zeta[c,b,c]^\zeta[c,c,a]^\eta[c,a,c]^\eta[b,c,a]^\xi[c,a,b]^\xi = \\
&= m^\eta l^\zeta = m^\eta(km)^\zeta = m^{\eta+\zeta}k^\zeta
\end{aligned}$$

Mit Hilfe dieser Ergebnisse und der Identitäten (2.3) können wir μ', ν', κ' als Potenzprodukte der Elemente m, k und μ, ν, κ darstellen. Es gelten zunächst folgende Darstellungen:

$$\begin{aligned}
f &= [a,b]^{\xi_f}[a,c]^{\eta_f}[b,c]^{\zeta_f} \\
g &= [a,b]^{\xi_g}[a,c]^{\eta_g}[b,c]^{\zeta_g} \\
h &= [a,b]^{\xi_h}[a,c]^{\eta_h}[b,c]^{\zeta_h}
\end{aligned}$$

Dann erhalten wir:

$$\begin{aligned}
\mu' &= [a,g][b,f][c,h]\mu = k^{\zeta_g+\eta_g}m^{\zeta_g+\xi_g}m^{\zeta_f+\eta_f+\xi_f}k^{\eta_f+\xi_f}m^{\eta_h+\zeta_h}k^{\zeta_h}\mu = \\
&= k^{\eta_f+\xi_f+\zeta_g+\eta_g+\zeta_h}m^{\zeta_f+\eta_f+\xi_f+\zeta_g+\xi_g+\eta_h+\zeta_h}\mu \\
\nu' &= [a,h][b,g][c,fh]\nu = \\
&= k^{\zeta_h+\eta_h}m^{\zeta_h+\xi_h}m^{\zeta_g+\eta_g+\xi_g}m^{\eta_f+\eta_h+\zeta_f+\zeta_h}k^{\zeta_f+\zeta_h}\nu = \\
&= m^{\eta_f+\zeta_f+\xi_g+\eta_g+\zeta_g+\xi_h+\eta_h}k^{\zeta_f+\xi_g+\eta_g+\eta_h}\nu \\
\kappa' &= [a,f][b,gh][c,g]\kappa = \\
&= k^{\zeta_f+\eta_f}m^{\zeta_f+\xi_f}m^{\zeta_g+\zeta_h+\eta_g+\eta_h+\xi_g+\xi_h}k^{\eta_g+\eta_h+\xi_g+\xi_h}m^{\eta_g+\zeta_g}k^{\zeta_g}\kappa = \\
&= m^{\xi_f+\zeta_f+\xi_g+\eta_g+\zeta_g+\xi_h+\eta_h+\zeta_h}k^{\eta_f+\zeta_f+\xi_g+\eta_g+\zeta_g+\xi_h+\eta_h}\kappa
\end{aligned} \tag{2.4}$$

2.4 Erzeugende Relationen in genauerer Fassung

Ziel dieses Abschnitts ist es, die Relationen (2.1) mit Hilfe der zuvor entwickelten Transformationen T7 und T-G auf die Form

$$1 = a^4 = b^4 = c^4, \quad [a,b] = c^2k^\epsilon, \quad [a,c] = b^2c^2k^\epsilon, \quad [b,c] = a^2b^2 \tag{2.5}$$

mit $\epsilon \in \{0,1\}$ zu bringen. Wir geben zunächst zwei nützliche Spezialfälle der Transformation T-G an.

1. Setzen wir in (2.4) $g = h = 1$ und $\zeta_f = 0$, so erhalten wir

$$\begin{aligned}\mu' &= k^{\eta_f+\xi_f} m^{\eta_f+\xi_f} \mu \\ \nu' &= m^{\eta_f} \nu \\ \kappa' &= m^{\xi_f} k^{\eta_f} \kappa.\end{aligned}$$

   Wegen $\kappa \in K_3 = \langle k, m\rangle$ können wir Exponenten $\sigma, \tau \in \mathbb{F}_2$ finden mit $\kappa = m^\sigma k^\tau$. Die Festlegung $\xi_f := \sigma$ und $\eta_f := \tau$ führt auf

$$(\mu, \nu, \kappa) \to ((mk)^{\sigma+\tau}\mu, m^\tau \nu, 1). \tag{2.6}$$

2. Es ist auch möglich T-G so einzuschränken, dass $\kappa = \kappa'$ gilt. Dazu muss zunächst

$$\begin{aligned}\xi_f + \zeta_f + \xi_g + \eta_g + \zeta_g + \xi_h + \eta_h + \zeta_h &= 0 \\ \eta_f + \zeta_f + \xi_g + \eta_g + \zeta_g + \xi_h + \eta_h &= 0\end{aligned}$$

   gelten. Das Einsetzen in (2.1) ergibt

$$\begin{aligned}\mu' &= m^{\eta_f+\zeta_g+\xi_h} \mu \\ \nu' &= k^{\eta_f+\zeta_g+\xi_h} \nu \\ \kappa' &= \kappa\end{aligned}$$

   und daraus

$$(\mu, \nu, \kappa) \to (m\mu, k\nu, \kappa). \tag{2.7}$$

Anwendung von (2.6) auf (μ, ν, κ) führt auf $(\mu_1, \nu_1, 1)$ und weiters mit (2.7) erreichen wir entweder $(\mu_2, 1, 1)$ oder $(\mu_2, m, 1)$. Tripel von der Form $(\mu, 1, 1)$ umfasst Spezialfälle $(k, 1, 1)$ und $(mk^\alpha, 1, 1)$ mit $\alpha \in \{0, 1\}$. Umformungen von $(k, 1, 1)$ führen auf

$$(k,1,1) \xrightarrow{\text{T7}} (km,k,k) \xrightarrow{\text{T7}} (km,k,k) \xrightarrow[\sigma=0,\tau=1]{\text{T-G}} \cdots$$

$$\to (1,mk,1) \xrightarrow{\text{T7}} (k,k,k) \xrightarrow[\sigma=0,\tau=1]{\text{T-G}} (m,mk,1) \xrightarrow{\text{T-G}} \cdots$$

$$\to (1,m,1) \xrightarrow{\text{T7}} (1,1,1).$$

Unter Berücksichtigung obiger Ergebnisse kann $(mk^\alpha, 1, 1)$ wie folgt behandelt werden:

$$\begin{array}{ccccccc}
(mk^\alpha,1,1) & \xrightarrow{\text{T7}} & (m,k^\alpha,1) & \xrightarrow{\alpha=0} & (m,1,m) & \xrightarrow[\sigma=1,\tau=0]{\text{T-G}} & (k,1,1) \\
 & & \downarrow{\scriptstyle \alpha=1} & & & & \downarrow{\scriptstyle \cdots} \\
 & & (m,k,m) & & \xrightarrow[\sigma=1,\tau=0]{\text{T-G}} & & (k,k,1) \qquad (1,1,1)
\end{array}$$

Schließlich kommen wir zu $(\mu, m, 1)$.

$$\begin{array}{ccccccc}
 & & (1,mk,1) & \xrightarrow{\cdots} & (1,1,1) & & \\
 & & \uparrow & & & & \\
(\mu,m,1) & \xrightarrow{\text{T7}} & (1,\mu,1) & \longrightarrow & (1,m,1) & \xrightarrow{\cdots} & (1,1,1) \\
 & & \downarrow & & & & \\
 & & (1,k,1) & & & & \\
 & & \downarrow{\scriptstyle \text{T7}} & & & & \\
 & & (km,km,km) & \xrightarrow[\sigma=\tau=1]{\text{T-G}} & (km,k,1) & \xrightarrow{\cdots} & (1,1,1)
\end{array}$$

Lemma 20 *Ist $K_3(G) \cong E_2$ so gilt $\mu = \nu = \kappa = 1$.*

Beweis. Es gelte $(\mu, \nu, \kappa) = (k, k, 1)$ und $k \neq 1$. Falls $m \neq 1$ so ist notwendigerweise $m = k$ und wir erhalten

$$(k,k,1) \xrightarrow{\text{T-G}} (1,1,1).$$

Im Falle $m = 1$ ist

$$(k,k,1) \xrightarrow{\text{T-G}} (k,1,k) \xrightarrow{\text{T7}} (1,1,1).$$

□

Lemma 21 *Das Zentrum von G fällt mit $K_3(G)$ zusammen.*

Beweis. Da $c(G) = 3$, gilt klarerweise $K_3 \leq Z(G)$. Wir wählen nun ein beliebiges Element $x \in Z(G)$ und zeigen $x \in K_3$. Wegen

$$G = \langle [a,b], [a,c], [b,c], K_3 \rangle \tag{2.8}$$

können wir x in der Form $x = [a,b]^\alpha[a,c]^\beta[b,c]^\gamma k_3$ mit $k_3 \in K_3$ schreiben. x kommutiert mit allen Elementen der Gruppe, insbesondere mit Erzeugern:

$$\begin{aligned}[x,a] &= [a,b,a]^\alpha[a,c,a]^\beta[b,c,a]^\gamma = 1\\ [x,b] &= [a,b,b]^\alpha[a,c,b]^\beta[b,c,b]^\gamma = 1\\ [x,c] &= [a,b,c]^\alpha[a,c,c]^\beta[b,c,c]^\gamma = 1.\end{aligned}$$

Daraus erhalten wir

$$\begin{aligned}m^\alpha k^\beta l^\gamma &= m^\alpha k^\beta m^\gamma k^\gamma = m^{\alpha+\gamma}k^{\beta+\gamma} = 1\\ l^\alpha l^\beta m^\gamma &= (mk)^{\alpha+\beta}m^\gamma = m^{\alpha+\beta+\gamma}k^{\alpha+\beta} = 1\\ 1^\alpha m^\beta l^\gamma &= m^\beta(mk)^\gamma = m^{\beta+\gamma}k^\gamma = 1\end{aligned}$$

Es sei zunächst $K_3 \cong E_4$. In diesem Fall gilt $m \neq 1$, $k \neq 1$ und $l = mk \neq 1$. Durch Aufmultiplizieren der obigen Gleichungen erhalten wir $m^\gamma k^\alpha = 1$ und daraus $\gamma = \alpha = 0 \Rightarrow m^\beta = 1 \Rightarrow \beta = 0 \Rightarrow x \in K_3$. Ist $K_3 \cong E_2$, so haben wir drei Fälle zu untersuchen. Gilt $k \neq 1$ und $m = 1$, so folgt

$$\begin{aligned}k^{\beta+\gamma} = 1 &\Rightarrow \beta = 0\\ k^{\alpha+\beta} = 1 &\Rightarrow \alpha = 0\\ k^\gamma = 1 &\Rightarrow \gamma = 0.\end{aligned}$$

$k \neq 1$ und $m = k$ impliziert

$$\begin{aligned}k^{\alpha+\beta} &= 1\\ k^\gamma &= 1\\ k^\beta &= 1.\end{aligned}$$

Schließlich $k = 1 \Rightarrow m \neq 1 \Rightarrow$

$$\begin{aligned}m^{\alpha+\gamma} &= 1\\ m^{\alpha+\beta+\gamma} &= 1\\ m^{\beta+\gamma} &= 1\end{aligned}$$

$\Rightarrow \beta = 0 \Rightarrow \gamma = 0 \Rightarrow \alpha = 0 \Rightarrow x \in K_3$. □

Literaturverzeichnis

[BJ06] Berkovich, Yakov und Zvonimir Janko: *Structure of finite p-groups with given subgroups.* Arad, Zvi (ed.) et al., Ischia group theory 2004. Proceedings of a conference in honor of Marcel Herzog, Naples, Italy, March 31–April 03, 2004. Providence, RI: American Mathematical Society (AMS); Ramat Gan: Bar-Ilan University. Contemporary Mathematics 402. Israel Mathematical Conference Proceedings, 13-93 (2006)., 2006.

[Bol01] Bolthausen, Erwin: *Lineare Algebra und Geometrie I und II Wintersemester 2000/2001 und Sommersemester 2001.* September 2001. `http://mathweb.unizh.ch/vorlesungen/lineare-algebra/skript.pdf` [Online; Stand 31. Juli 2007].

[Hup67] Huppert, Bertram: *Endliche Gruppen I*, Band 134 der Reihe *Grundlehren der mathematischen Wissenschaften.* Springer-Verlag, Berlin, Heidelberg, New York, 1967.

[Rot95] Rotman, Joseph J.: *An Introduction to the Theory of Groups*, Band 148 der Reihe *Graduate Texts in Mathematics.* Springer-Verlag, 4. Auflage, 1995.

[Ser96] Serre, Jean-Pierre: *A Course in Arithmetic*, Band 7 der Reihe *Graduate Texts in Mathematics.* Springer-Verlag, 5. Auflage, 1996.