Gruppen mit einem BN-Paar vom Rang 1 oder 2

Inaugural-Dissertation

zur Erlangung des Doktorgrades
an den Naturwissenschaftlichen Fachbereichen
(Mathematik)

der Justus-Liebig-Universität Gießen

vorgelegt von
Heiko Wagner

Gießen 2003

D - 26

Dekan: Prof. Dr. Volker Metag (Gießen)

1. Berichterstatter: Prof. Dr. Franz Georg Timmesfeld (Gießen)
2. Berichterstatter: Prof. Dr. Thomas Meixner (Gießen)

Datum der Disputation: 16.01.2004

Inhaltsverzeichnis

Kapitel 1

Einleitung

Die Kennzeichnung der endlichen Gruppen mit einem (zerfallenden) BN-Paar gehört zu den zentralen Bestandteilen der *Klassifikation der endlichen einfachen Gruppen*. Die Gruppen mit BN-Paaren sind assoziiert zu geometrischen Strukturen – den von Tits in [35] eingeführten Gebäuden – und die Kennzeichnung der Gruppen mit einem BN-Paar vom Rang mindestens drei ist in der Klassifikation der sphärischen Gebäude von Tits [35] enthalten. Eine besondere Rolle spielt die Klassifikation der endlichen Gruppen mit einem BN-Paar vom Rang 1 und 2, die bei dem oben zitierten allgemeinen Resultat ausgenommen werden müssen. Die geometrische Struktur der assoziierten Gebäude ist in diesem Fall zu schwach, um die fast ausschließlich geometrischen Argumente von Tits zu verwenden.

Die Gruppen mit BN-Paaren vom Rang 1 sind zweifach transitive Permutationsgruppen und wurden unter der zusätzlichen Voraussetzung, dass das BN-Paar zerfallend ist, in den Jahren 1971 von Kantor & Seitz [20] sowie 1972 von Kantor, Hering & Seitz [21] klassifiziert. Eine Kennzeichnung der endlichen Gruppen mit einem zerfallenden BN-Paar vom Rang 2, welche treu auf dem zugehörigen Gebäude operieren, wurde zwischen 1973 und 1974 von Fong & Seitz in [12] und [13] vorgenommen. Besonders wichtig in den beiden Arbeiten ist es, Informationen über die Struktur der beiden standardmaximalparabolischen Untergruppen zu erhalten. Diese haben BN-Paare vom Rang 1 und Faktorgruppen dieser Gruppen sind somit zweifach transitive Permutationsgruppen. Hierin liegt nun die große Bedeutung in der Voraussetzung, dass das BN-Paar zerfallend ist. Dann besitzen die Stabilisatoren eines Punktes einen nilpotenten und auf den übrigen Punkten transitiven Normalteiler, so dass die Klassifikation von Kantor & Seitz [20] angewendet werden kann. Dieses Resultat liefert eine Einteilung der möglichen Strukturen der maximalparabolischen Untergruppen. Als erste Folge ist der nilpotente Normalteiler der Boreluntergruppe eine p-Gruppe. Die Strukturen der standardmaximalparabolischen Untergruppen beeinflussen sich gegenseitig und im weiteren Verlauf untersuchen Fong & Seitz langwierig, welche Paarungen die parabolischen Untergruppen in der obigen Einteilung eingehen können. Dies beinhaltet die Konstruktion von sogenannten Wurzeluntergruppen. Schließlich werden durch Berechnen von Kommutatorrelationen zwischen diesen Wurzeluntergruppen genügend Information über die Verknüpfungstabelle der betrachteten Gruppe gesammelt, um diese über Klassifikationssätze mit Lie-Typ-Gruppen zu klassifizieren.

Die beiden obigen Arbeiten von Fong & Seitz gehören trotz ihrer Bedeutung wohl aber wegen ihrer Komplexität zu den weniger gelesenen Arbeiten der endlichen Gruppentheorie. In der vorliegenden Arbeit beschäftigen wir uns unter anderem mit einer Revision dieser Arbeit, allerdings unter einer zusätzlichen Voraussetzung. Zu diesem Zweck nennen wir die endlichen einfachen Gruppen aus der Liste der Klassifikation die

bekannten endlichen, einfachen Gruppen. Sind die echten einfachen Abschnitte einer endlichen Gruppe G sämtlich bekannt, so heißt G eine $\mathcal{K}$-Gruppe. Wir betrachten hier endliche $\mathcal{K}$-Gruppen mit einem irreduziblen, zerfallenden BN-Paar, welche treu auf dem zugehörigen Gebäude operieren. Das (zweite) Hauptresultat in dieser Arbeit ist, dass das zugehörige Gebäude die *Moufangbedingung* erfüllt. Wir geben eine genaue Konstruktion der Wurzeluntergruppen innerhalb unserer Gruppe an und identifizieren diese mit den Wurzeluntergruppen des zugehörigen Gebäudes. Die Kennzeichnung der betrachteten Gruppen ist nun in der Klassifikation der Moufangpolygone von Tits & Weiss [36] enthalten.

Zwei Gründe sind verantwortlich für die Voraussetzung, dass wir hier $\mathcal{K}$-Gruppen betrachten werden. Zum einen ist diese Voraussetzung ausreichend für die Anwendung in der von Gorenstein, Lyons & Solomon [14] beschriebenen Revision der *Klassifikation der endlichen einfachen Gruppen*. Zum anderen macht diese Voraussetzung es möglich, die Klassifikation von zweifach transitiven Gruppen von Kantor & Seitz [20] zu ersetzen. Das Vorgehen zum Erhalt des oben formulierten Zieles wird zunächst dem von Fong & Seitz entsprechen. Die (Faktorgruppen) der maximalparabolischen Untergruppen sind zweifach transitive Permutationsgruppen, bei denen der Stabilisator eines Punktes einen nilpotenten und auf den übrigen Punkten transitiven Normalteiler besitzt. Eine zweifach transitive Permutationsgruppe besitzt einen eindeutig bestimmten Normalteiler, welcher einfach oder elementarabelsch ist. Dieser ist – sofern er einfach ist – nach Voraussetzung eine der bekannten einfachen Gruppen.

Um nun Aussagen über die Struktur der maximalparabolischen Untergruppen zu erhalten, klassifizieren wir (als erstes Hauptresultat) die endlichen, zweifach transitiven Gruppen G, bei denen der Stabilisator eines Punktes einen nilpotenten und auf den übrigen Punkten transitiven Normalteiler besitzt und für die $G_0 \leq G \leq Aut(G_0)$ für eine bekannte einfache Gruppe G_0 ist. (Für die sporadischen Gruppen G_0 zitieren wir geeignete Literatur.) Die Gruppe G_0 entspricht gerade dem im letzten Absatz erwähnten Normalteiler, (wenn dieser einfach ist). In den Beweis dieser Aussage fließen wesentlich Argumente aus der *Theorie der abstrakten Wurzeluntergruppen* von Timmesfeld [34] ein. In der Literatur existiert eine ähnliche Aussage von Curtis, Kantor & Seitz [11], wenn G_0 eine Lie-Typ-Gruppe ist. Der Beweis kommt ohne die Existenz von nilpotenten Normalteilern der Punktstabilisatoren aus, jedoch wird der Beweis in seinen Hauptbestandteilen mit charaktertheoretischen Argumenten geführt.

Mit Hilfe dieser Aussage ist es nun jedenfalls möglich, die Struktur der maximalparabolischen Untergruppen relativ genau zu bestimmen. Unter der erneuten Verwendung unseres ersten Hauptresultates erhalten wir dann die Folgerung, dass der nilpotente Normalteiler der Boreluntergruppe eine p-Gruppe ist. Eine weitere sehr wichtige Folgerung aus dem ersten Hauptsatz ist, dass der nilpotente Normalteiler des Stabilisators eines Punktes *regulär* auf den übrigen Punkten operiert. Die Identifikation der Wurzeluntergruppen des zugehörigen Gebäudes ist nun innerhalb der betrachteten Gruppe sehr leicht möglich. Das genaue Vorgehen beschreiben wir separat in den entsprechenden Kapiteln dieser Arbeit.

Zu Beginn der Arbeit stellen wir die notwendigen Begriffe, Notationen und einige wohlbekannte Tatsachen über Gebäude, Gruppen mit BN-Paaren und Lie-Typ-Gruppen bereit. Dieser Teil ist allerdings nur für den ungeübten Leser gedacht. Im dritten Kapitel befassen wir uns mit der Theorie der abstrakten Wurzeluntergruppen von Timmesfeld [34], die wir insbesondere im Zusammenhang mit Lie-Typ-Gruppen anwenden wollen. Hier bereiten wir den Beweis unseres ersten Hauptsatzes vor. Dieses Hauptresultat formulieren wir im vierten Kapitel, wogegen wir den Beweis wegen seines Umfangs auf die beiden nachfolgenden Kapitel verteilen. Im siebten Kapitel erhalten wir im Wesentlichen aus unserem ersten Hauptsatz die Klassifikation der endlichen zweifach transitiven Gruppen mit den zwei folgenden Eigenschaften: Der Stabilisator eines Punktes habe einen nilpotenten und auf den übrigen Punkten transitiven Normalteiler und der oben beschriebene eindeutig bestimmte Normalteiler sei eine *bekannte* Gruppe, wenn er einfach ist. Schließlich formulieren und beweisen wir im achten Kapitel unser zweites Hauptresultat. Anschließend finden wir noch drei Anhänge. Der erste enthält die Ordnungen der endlichen einfachen Lie-Typ-Gruppen, welche wir häufig vor Augen haben müssen, und die beiden übrigen stellen notwendige Berechnungen im Zusammenhang mit dem ersten Hauptsatz der Arbeit bereit. Die genaue Verwendung ist in den entsprechenden Kapiteln beschrieben.

Schließlich möchte ich verschiedenen Menschen meinen Dank ausdrücken. Herrn Prof. Dr. Franz-Georg Timmesfeld gilt mein besonderer Dank für die interessante Themenstellung der Dissertation, die Anregungen zu dieser Arbeit während vieler Gespräche und die gute Betreuung während der letzten Jahre. Mein besonderer Dank gilt auch Herrn Prof. Dr. Thomas Meixner für die vielen Diskussionen zum Thema dieser Dissertation und auch dafür, dass er stets ein offenes Ohr für mich hatte. Weiterhin möchte ich mich bei meinen Freunden und Kollegen Carola Klein, Anja Steinbach, Sergei Haller und Carsten Müller bedanken, die mich vielfältig unterstützt und auch oftmals zum Lachen gebracht haben. Mein letzter Dank gilt meiner Familie und meinen Freunden, die mich auf vielfältige Art und Weise unterstützt haben und manchmal meine Launen ertragen mussten.

Kapitel 2

Die endlichen einfachen Gruppen

Jede endliche einfache Gruppe ist isomorph zu einer zyklischen Gruppe von Primzahlordnung, einer alternierenden Gruppe A_n für $n \geq 5$, einer Lie-Typ-Gruppe oder einer der 26 sporadischen einfachen Gruppen. Die vertrautesten Vertreter der endlichen einfachen Gruppen sind die zyklischen und alternierenden Gruppen.

Unser Hauptinteresse gilt in diesem Kapitel den *endlichen* Chevalleygruppen und den *endlichen* getwisteten Chevalleygruppen, die wir als die Lie-Typ-Gruppen bezeichnen werden und als Gruppen von Automorphismen einfacher Lie-Algebren über einem endlichen Körper definieren. Zentraler Begriff in den nächsten Kapiteln ist der der (abstrakten) Wurzeluntergruppen, welchen wir hier definieren werden. Für die Beschreibung von Eigenschaften dieser Gruppen benötigen wir im nachfolgenden Kapitel die exakten Chevalley'schen Kommutatorrelationen innerhalb der Chevalleygruppen, weswegen wir hier relativ ausführlich sein werden.

Den Gruppen mit BN-Paaren gilt ab Kapitel 8 unser Hauptinteresse. Wie die Lie-Typ-Gruppen sind auch diese Gruppen zu einem Wurzelsystem assoziiert, mit welchen wir uns zuerst beschäftigen werden. Gruppen mit BN-Paaren operieren in natürlicher Weise auf einem als Gebäude bezeichneten geometrischen System. Mit der *Moufangbedingung* von Gebäuden definieren wir in diesem Kapitel den zentralen Begriff des achten Kapitels dieser Arbeit.

2.1 Wurzelsysteme

Sei V ein endlich-dimensionaler $\mathbb{R}$-Vektorraum mit positiv definitem Skalarprodukt $(\ ,\ ) : V \times V \longrightarrow \mathbb{R}$. Der *Senkrechtraum* zum Unterraum U von V sei

$$U^\perp := \{v \in V \mid (v, u) = 0 \text{ für alle } u \in U\}.$$

Für $r \in V^\sharp$ sei die orthogonale Abbildung w_r mit $w_r = id$ auf $\langle r \rangle^\perp$ und $r^{w_r} = -r$ die *Spiegelung entlang* r. Für $v \in V$ ist also

$$v^{w_r} = v - \frac{2(v, r)}{(r, r)} r.$$

Sei Φ eine endliche Teilmenge von V mit den Eigenschaften:

(1) $V = \langle \Phi \rangle$.

(2) Für $r, s \in \Phi$ ist $s^{w_r} \in \Phi$.

(3) Für $r \in \Phi$ und $\lambda \in \mathbb{R}$ ist $\lambda r \in \Phi$ genau dann, wenn $\lambda \in \{\pm 1\}$.

Dann heißt Φ ein *Wurzelsystem* in V und die Elemente von Φ heißen *Wurzeln*. Das Wurzelsystem Φ genügt der *kristallographischen Bedingung*, falls

$$\frac{2(r,s)}{(r,r)} \in \mathbb{Z}$$

für alle $r, s \in \Phi$. Ein Wurzelsystem heißt *unzerlegbar*, falls es nicht die disjunkte Vereinigung zweier nichtleerer, aufeinander senkrecht stehender Teilmengen ist.

Eine Teilmenge Π von Φ mit den Eigenschaften

(a) Π ist linear unabhängig.

(b) Jede Wurzel aus Φ läßt sich als Linearkombination mit lauter nichtnegativen oder nichtpositiven Koeffizienten von Elementen aus Π schreiben.

heißt *Fundamentalsystem* von Φ. Die Elemente von Π heißen *fundamentale Wurzeln* und $|\Pi|$ ist der *Rang* von Φ. Ferner heißen die Spiegelungen entlang der fundamentalen Wurzeln *fundamentale Spiegelungen*. Ein Vektorraum ist niemals die Vereinigung endlich vieler Unterräume, also ist

$$V_\Phi := V \setminus \bigcup_{r \in \Phi} \langle r \rangle^\perp \neq \emptyset.$$

Für $t \in V_\Phi$ setzen wir

$$\Phi_t^+ := \{r \in \Phi \mid (r,t) > 0\} \quad \text{und} \quad \Phi_t^- := \{r \in \Phi \mid (r,t) < 0\}$$

und erhalten $\Phi = \Phi_t^+ \dot\cup \Phi_t^-$. Wir nennen Φ_t^+ bzw. Φ_t^- *positives* bzw. *negatives* Wurzelsystem und deren Wurzeln entsprechend *positive* oder *negative Wurzeln*. Im folgenden verzichten wir auf den Index t, wenn wir von einem positiven bzw. negativen Wurzelsystem sprechen. Ist Φ^+ ein solches positives Wurzelsystem und Φ^- das korrespondierende negative Wurzelsystem, dann gibt es genau ein Fundamentalsystem Π in Φ^+ und es gibt kein weiteres positives Wurzelsystem, welches Π enthält. Jede positive Wurzel läßt sich eindeutig als Linearkombination von fundamentalen Wurzeln mit ausschließlich nichtnegativen Koeffizienten schreiben. Die beiden letzten Aussagen finden wir im Abschnitt (2.1) bei Carter [6].

Legen wir nun in Φ ein Fundamentalsystem fest, so läßt sich jede Wurzel r eindeutig als Linearkombination in Π schreiben. Die Summe der Koeffizienten dieser Linearkombination nennen wir *die Höhe* $h(r)$ der Wurzel r. Eine *höchste Wurzel* in Φ^+ ist eine positive Wurzel maximaler Höhe.

2.2 Weylgruppen von Wurzelsystemen

Jedes Wurzelsystem Φ ist per Definition invariant unter den Spiegelungen entlang seiner Wurzeln. Das Erzeugnis $W := W(\Phi)$ dieser Spiegelungen heißt die *Weylgruppe* von Φ und ist offenbar eine endliche Untergruppe von $O(V)$. Im folgenden legen wir ein

Fundamentalsystem $\Pi = \{r_i \mid i \in I\}$ im Wurzelsystem Φ fest. Gleichzeitig ist damit ein positives bzw. negatives Wurzelsystem Φ^+ bzw. Φ^- festgelegt.

Ist $J \subseteq I$, so heißt die Untergruppe

$$W_J := \langle w_{r_j} \mid j \in J \rangle$$

und jedes ihrer Konjugierten in W eine *parabolische Untergruppe* von W. Die Gruppe W_J nennen wir überdies eine *standardparabolische Untergruppe* von W. Nach (2.18) von CARTER [6] ist jede Wurzel in Φ Bild einer fundamentalen Wurzel unter W, und es ist $W = W_I$. Insbesondere ist jedes Element $w \in W$ ein Produkt von fundamentalen Spiegelungen. Die minimale Länge eines solchen Ausdrucks für w nennen wir die *Länge $\ell(w)$ von w*. Die Längen der Elemente von W hängen in folgender Weise mit dem Wurzelsystem zusammen. Wir finden dies in (2.2) und (2.2.6) bei CARTER [6].

(2.2.1) Lemma.

Die Länge von $w \in W$ ist die Anzahl der positiven Wurzeln, die von w auf negative Wurzeln abgebildet wird. Für jede fundamentale Wurzel r gilt weiterhin:

(a) $\ell(w_r w) = \ell(w) + 1$, *falls* $w^{-1}(r) \in \Phi^+$,

(b) $\ell(w_r w) = \ell(w) - 1$, *falls* $w^{-1}(r) \in \Phi^-$,

(c) $\ell(w w_r) = \ell(w) + 1$, *falls* $w(r) \in \Phi^+$,

(d) $\ell(w w_r) = \ell(w) - 1$, *falls* $w(r) \in \Phi^-$.

Ferner existiert eine Involution w_0 maximaler Länge mit $w_0(\Phi^+) = \Phi^-$.

2.3 Die Coxetergraphen von Weylgruppen

Ein *Coxetergraph* $\mathcal{G}$ ist ein Graph mit endlicher Eckenmenge, dessen Kanten $\{i, j\}$ die Markierungen $3 \leq q_{ij} \in \mathbb{N}$ tragen. Der Coxetergraph heißt *zusammenhängend*, wenn es zu je zwei Ecken i und j eine Folge von Ecken $i = i_1, \ldots, i_k = j$ gibt, so dass $\{i_s, i_{s+1}\}$ Kanten von $\mathcal{G}$ sind. Es ist üblich, die Markierung 3 wegzulassen und anstatt der Markierung 4 bzw. 6 eine Doppel- bzw. Dreifachkante zu zeichnen.

Ist Φ ein kristallographisches Wurzelsystem mit festgelegtem Fundamentalsystem $\Pi = \{r_i \mid i \in I\}$ und Weylgruppe W, dann können wir einen Coxetergraphen $\mathcal{G}(\Phi)$ zu Φ assoziieren. Die fundamentalen Wurzeln von Φ sind die Ecken des Graphen. Weiterhin sind zwei Ecken r_i und r_j über die Kante mit der Bezeichnung $p_{ij} := o(w_{r_i} w_{r_j})$ verbunden, wenn $p_{ij} \geq 3$. Ist $p_{ij} = 2$, so sind r_i und r_j nicht über eine Kante verbunden. Dies definiert offenbar einen Coxetergraphen. Die Gruppe W operiert transitiv auf den Fundamentalsystemen von Φ, so dass die Definition von $\mathcal{G}(\Phi)$ wohldefiniert ist.

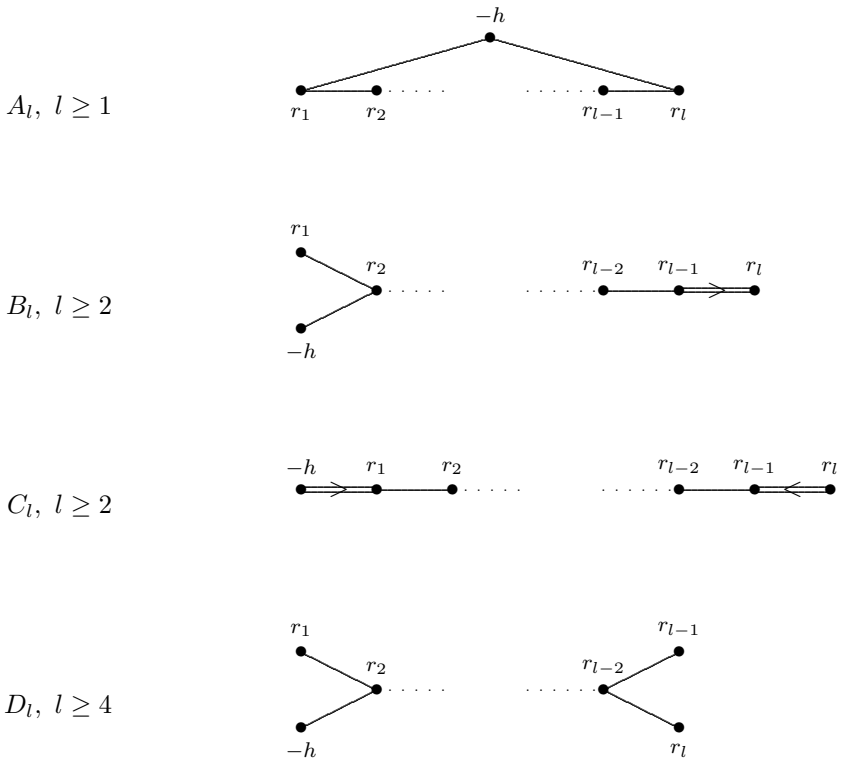

Abbildung 2.1: Die erweiterten klassischen Dynkindiagramme

Hauptsächlich interessieren uns die unzerlegbaren Wurzelsysteme, welche die kristallographische Bedingung erfüllen. Die Coxetergraphen solcher Wurzelsysteme sind zusammenhängend und es gilt überdies $p_{ij} \in \{1, 2, 3, 4, 6\}$. Dies finden wir in (2.8) und (2.9) bei HUMPHREYS [18]. Die Graphen mit diesen Eigenschaften sind dort in (2.7) vollständig klassiziert. Es gilt der

(2.3.1) Satz.

Die unzerlegbaren Wurzelsysteme, welche die kristallographische Bedingung erfüllen, sind die mit den Coxetergraphen A_l, B_l, D_l, E_6, E_7, E_8, F_4 oder G_2.

Beschriften wir die Ecken eines solchen Coxetergraphen mit den fundamentalen Wurzeln und zeichnen die Kanten als Bindungen, so heißt das resultierende Diagramm das *Dynkindiagramm* von Φ. Bei der Konstruktion der obigen Wurzelsysteme folgen wir der Notation von BOURBAKI [4] in Kapitel VI. Jedes solche Wurzelsystem enthält höchstens zwei Sorten von unterschiedlich langen Wurzeln. Die kürzeren Wurzeln heißen dann *kurze Wurzeln* und die längeren entsprechend *lange Wurzeln*. Haben alle Wurzeln dieselbe Länge, so nennen wir diese ebenfalls lange Wurzeln. Diese Information wird dem obigen Coxetergraph zugefügt, indem ein Pfeil zwischen zwei Wurzeln verschiedener Länge gesetzt wird. Bei sämtlichen der obigen Wurzelsysteme gibt es

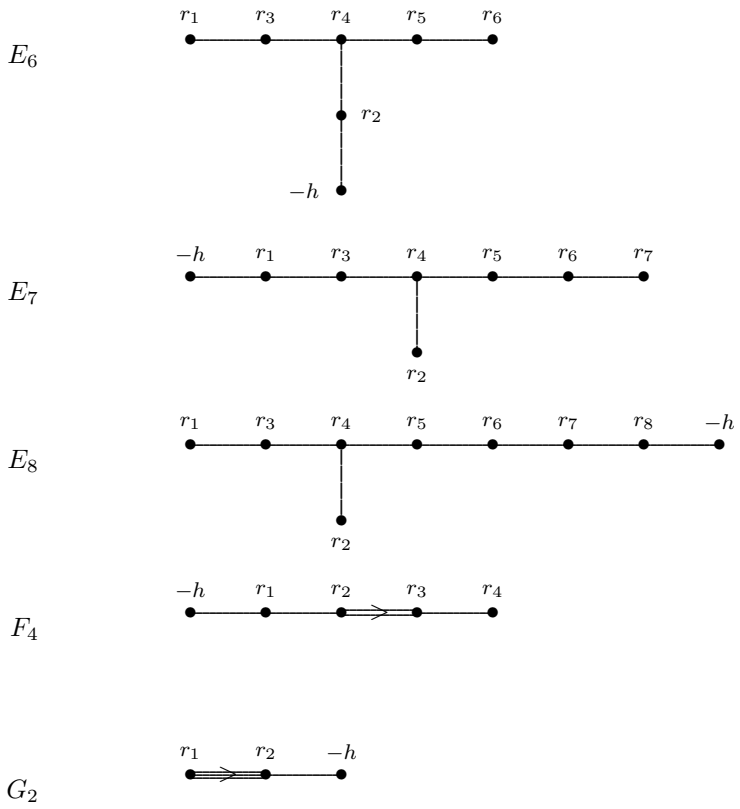

Abbildung 2.2: Die erweiterten Dynkindiagramme vom Ausnahmetyp

genau eine *höchste Wurzel* h in Φ^+, welche stets lang ist. Die negative höchste Wurzel $-h$ zeichnen wir im folgenden stets mit in das Diagramm ein und nennen das resultierende Diagramm das *erweiterte Dynkindiagramm*. Der *Typ* des Wurzelsystems Φ ist die Bezeichnung des zugehörigen Coxetergraphen.

(2.3.2) Das Wurzelsystem vom Typ BC_l.

Für die spätere Verwendung geben wir noch kurz eine Beschreibung des irreduzibeln Wurzelsystems vom Typ BC_l an. Sei $(e_1, \ldots, e_l)$ eine Orthonormalbasis von $\mathbb{R}^l$. Dann bilden die Wurzeln

$$\pm e_i, \pm 2e_i, \pm e_i \pm e_j, \text{ mit } i < j \text{ und } 1 \leq i, j \leq l$$

ein Wurzelsystem Φ vom Typ BC_l. Die fundamentalen Wurzeln sind

$$r_1 = e_1 - e_2, \ldots, r_{l-1} = e_{l-1} - e_l, r_l = e_l$$

und die positiven Wurzeln sind die Wurzeln

$$e_i = \sum_{k=i}^{l} r_k,\ 2e_i, \quad e_i - e_j = \sum_{k=i}^{j-1} r_k, \quad e_i + e_j = \sum_{k=i}^{j-1} r_k + 2\sum_{k=j}^{l} r_k.$$

Die höchste Wurzel ist gegeben durch $h = 2e_1$.

Abbildung 2.3: Das erweiterte Dynkindiagramm vom Typ BC_l

2.4 Gebäude und *BN*-Paare

Sind B und N zwei Untergruppen der endlichen Gruppe G mit den Eigenschaften

$(BN1)$ $G = \langle B, N\rangle$ und $H := B \cap N$ ist ein Normalteiler von N,

$(BN2)$ $W := N/H$ wird von n Involutionen $s_1, \ldots, s_n$ erzeugt,

$(BN3)$ $s_i B w \subseteq BwB \cup Bs_iwB$ für $s_i \in S$ und $w \in W$,

$(BN4)$ $s_i B s_i \neq B$ für alle $s_i \in S$,

so heißt G eine Gruppe mit einem *BN-Paar vom Rang n*. Gilt weiterhin $H = \bigcap_{n\in N} B^n$, dann nennen wir das BN-Paar *saturiert*. Ist zusätzlich $B = UH$ mit einem nilpotenten Normalteiler U von B, so nennen wir das BN-Paar ein *zerfallendes* BN-Paar.

Wir sind im folgenden flexibel bei der Auslegung der Elemente $w \in W$. Einmal fassen wir sie als Elemente in W auf, und ein anderes Mal wie in den beiden letzten Punkten als einen Repräsentanten eines solchen Elementes in N. Da nämlich H von N normalisiert wird, sind diese Punkte wohldefiniert. Die Gruppe W nennen wir die *Weylgruppe* des BN-Paares. Die *parabolischen Untergruppen* von G sind die Untergruppen, die ein Konjugiertes von B enthalten. Eine handlichere Darstellung und elementare Eigenschaften der parabolischen Untergruppen finden wir in (43.7) von Aschbacher [2]. Demnach sind die Konjugierten von

$$P_J := \langle B, s_j \mid j \in J\rangle = BW_JB$$

für $J \subseteq \{1, \ldots, n\}$ die parabolischen Untergruppen von G, wenn wir W_J wie im letzten Abschnitt definieren.

(2.4.1) Bemerkung.

Eine durch Erzeugende und Relationen definierte Gruppe

$$X = \langle w_i \mid i \in I,\ (w_iw_j)^{m_{ij}} = 1\rangle$$

mit $m_{ii} = 1$ und $m_{ij} \geq 2$ für $i \neq j$, heißt Coxetergruppe. *Die Weylgruppe eines BN-Paares vom Rang n ist eine solche Coxetergruppe und W ist assoziiert zu einem Wurzelsystem Φ vom Typ A_l, B_l, D_l, E_6, E_7, E_8, F_4, G_2 oder Φ besteht aus den Vektoren vom Ursprung zu den Ecken eines regelmäßigen* 16*-Ecks.*

Eine von zwei verschiedenen nilpotenten Gruppen A und B erzeugte Gruppe heißt eine *Rang* 1*-Gruppe*, wenn zu jedem Element $a \in A^\sharp$ ein $b \in B^\sharp$ existiert mit $A^b = B^a$ und umgekehrt. Die Konjugierten von A (und B) heißen die *unipotenten Untergruppen* von X. Die Einführung der Rang 1-Gruppen geht zurück auf Timmesfeld. In seinem Buch [34] finden wir in I (1.3), dass die Konzepte der Rang 1-Gruppen und der Gruppen mit zerfallendem BN-Paar vom Rang 1 äquivalent sind.

Ein *Kammersystem* $\mathcal{C}$ über einer Indexmenge I ist eine Menge $\mathcal{C}$ von *Kammern*, zusammen mit Partitionen $\mathcal{P}_i$ für $i \in I$. Für eine Kammer c sei $\Delta_i(c)$ die Äquivalenzklasse von $\mathcal{P}_i$, die c enthält. Wir bezeichnen diese als ein *Rang* 1*-Residuum* von c. Zwei Kammern c und d heißen *i-benachbart*, falls $d \in \Delta_i(c)$. Wir schreiben $c \overset{i}{\sim} d$. Eine *Galerie* vom Typ $(i_1, \ldots, i_k)$ ist eine Folge von Kammern $(c_0, \ldots, c_k)$ mit $c_{l-1} \overset{i_l}{\sim} c_l$ für $l \leq k$. Das Kammersystem $\mathcal{C}$ heißt *zusammenhängend*, wenn je zwei Kammern über eine Galerie verbunden sind. Weiterhin heißt $\mathcal{C}$ *dick*, wenn $|\Delta_i(c)| \geq 3$ für alle $i \in I$. Sei $\mathcal{D}$ ein weiteres Kammersystem über I. Ein *Isomorphismus* α von $\mathcal{C}$ nach $\mathcal{D}$ ist eine bijektive Abbildung von $\mathcal{C}$ nach $\mathcal{D}$ mit der Eigenschaft: Ist $c \overset{i}{\sim} d$ für $c, d \in \mathcal{C}$, so ist auch $c^\alpha \overset{i}{\sim} d^\alpha$.

(2.4.2) Beispiel.

Sei G eine Gruppe, B eine Untergruppe von G und $(P_i)_{i\in I}$ ein System von Untergruppen, die B enthalten. Dann sei $\mathcal{C} = \mathcal{C}(G, B, (P_i)_{i\in I})$ die Menge der Kammern Bg, $g \in G$ zusammen mit der i-Benachbartheit

$$Bg \overset{i}{\sim} Bh :\Longleftrightarrow P_i g = P_i h,$$

bzw. den zugehörigen Partitionen. Dann ist $\mathcal{C}$ ein Kammersystem über I.

Eine Coxetergruppe W wird erzeugt von Involutionen w_i mit $i \in I$. Bezeichnen wir mit m_{ij} die Ordnung von $w_i w_j$, so legt dies die Matrix $M = (m_{ij})$ fest. Ein *Coxetersystem* vom Typ M über I ist ein Kammersystem, dass isomorph zu $\mathcal{C}(W, \{1\}, \langle w_i \rangle_{i\in I})$ ist. Die Automorphismengruppe dieses Kammersystems ist isomorph zu W. Ein Coxetersystem heißt *sphärisch*, wenn $|W| < \infty$.

Ein *Gebäude* $\mathcal{B}$ über I vom Typ $M = M(I)$, ist ein zusammenhängendes Kammersystem über I zusammen mit einer Familie $\mathcal{F}$ von Untersystemen von $\mathcal{B}$ – den *Apartments von $\mathcal{B}$* – so dass gilt:

(B1) Jedes $\mathcal{A} \in \mathcal{F}$ ist ein Coxetersystem vom Typ M über I.

(B2) Zu jedem Paar c, d von Kammern existiert ein Apartment $\mathcal{A} \in \mathcal{F}$, welches $\{c, d\}$ enthält.

Sei nun $\mathcal{A} \in \mathcal{F}$ ein Apartment von $\mathcal{B}$ und $\Delta_i(c)$ ein Rang 1-Residuum von $\mathcal{B}$. Wir sagen, ein Rang 1-Residuum *liegt in* $\mathcal{A}$ genau dann, wenn $\Delta_i(c) \cap \mathcal{A} \neq \emptyset$.

(B3) Seien c und d Kammern von $\mathcal{B}$, bzw. c eine Kammer und $\Delta_i(d)$ ein Rang 1-Residuum von $\mathcal{B}$, die in den Apartments $\mathcal{A}$ und $\mathcal{A}'$ von $\mathcal{B}$ liegen. Dann existiert ein Isomorphismus $\sigma : \mathcal{A} \longrightarrow \mathcal{A}'$ der c und d, bzw. c und $\Delta_i(d)$ festläßt.

Das Axiom (B3) ist äquivalent zu dem Axiom (B3Tits) von Tits in [35]. Ein Gebäude heißt *sphärisch*, wenn alle Apartments (als Coxetersysteme) sphärisch sind. Der *Rang* von $\mathcal{B}$ ist $|I|$. Eine Familie $\mathcal{F}$ von Untersystemen von $\mathcal{B}$, die (B1) bis (B3) erfüllt, heißt *Apartment-System* von $\mathcal{B}$.

Ein sphärisches Gebäude ist durch seine Apartments assoziiert zu einer endlichen Coxetergruppe W und somit zu einem Wurzelsystem Φ. Die Wurzeln werden sich daher in den Apartments wiederfinden lassen. Wir betrachten dazu ein Apartment $\mathcal{A}$ von $\mathcal{B}$ und identifizieren es mit dem Coxeterkomplex $\mathcal{C}(W, \{1\}, \langle w_i \rangle_{i \in I})$. Eine *Spiegelung* w_r von $\mathcal{A}$ ist ein Konjugiertes von w_i für ein $i \in I$. Die *reflektierende Wand* M_r von w_r ist die Menge der echten Residuen von $\mathcal{A}$, die invariant unter w_r sind. Wir sagen, dass eine Galerie $(c_1, \ldots, c_m)$ von $\mathcal{A}$ die Wand M_r trifft, wenn die Kammern c_i und c_{i+1} von w_r vertauscht werden für ein $i \in \{1, \ldots, m-1\}$, d.h. wenn $\{c_i, c_{i+1}\} \in M_r$. Die Galerie trifft M_r genau k mal, wenn genau k der Paare $\{c_1, c_2\}, \ldots, \{c_{n-1}, c_n\}$ von w_r vertauscht werden, bzw. in M_r enthalten sind. Sind c und d zwei Kammern, so trifft jede Galerie zwischen c und d die Wand M_r entweder geradzahlig oder ungeradzahlig oft (vgl. (2.5) von Ronan [30]).

Legen wir nun eine Kammer c aus $\mathcal{A}$ fest, dann können wir $\mathcal{A}$ in zwei disjunkte Teilmengen r und $-r$ partitionieren, nämlich die Menge der Kammern x, bei der eine Galerie zwischen c und x die Wand M_r geradzahlig oft trifft, und entsprechend die Menge der Kammern y, bei der eine Galerie zwischen c und y die Wand M_r ungeradzahlig oft trifft. Die Mengen r und $-r$ heißen die durch w_r bestimmten *Wurzeln* von $\mathcal{A}$. Die Wurzeln r und $-r$ heißen *gegenüberliegend*. Die ausgezeichnete Kammer c spielt bei der Definition von r und $-r$ keine Rolle. Bei dem Übergang zu einer anderen Kammer erhalten wir die gleiche Partition. Weiterhin ist $r^{w_r} = -r$. Es gilt nun das folgende

(2.4.3) Lemma.

Sei $\mathcal{B}$ ein sphärisches Gebäude, $\mathcal{A}$ ein Apartment und W und Φ wie oben beschrieben. Dann sind die Operationen von W auf den Wurzeln von $\mathcal{A}$ und Φ äquivalent.

Das Gebäude $\mathcal{B}$ heißt *irreduzibel*, wenn das Wurzelsystem des oben beschriebenen Wurzelsystems Φ von $\mathcal{B}$ zusammenhängend ist. Dies ist offenbar genau dann der Fall, wenn Φ irreduzibel ist. Sei nun $\mathcal{B}$ ein dickes, irreduzibles und sphärisches Gebäude vom Rang

mindestens 2 und $\mathcal{A}$ ein Apartment. Für jede Wurzel r von $\mathcal{A}$ nennen wir die Gruppe

$$A_r := \{\sigma \in Aut(\mathcal{B}) \mid c^\sigma = c \text{ für alle } c \in \mathcal{B} \text{ mit } \Delta_i(c) \cap \mathcal{A} \text{ ist ein in } r \text{ enthaltenes Rang 1-Residuum von } \mathcal{A}, \text{ für ein } i \in I\}$$

die *Wurzeluntergruppe* von $Aut(\mathcal{B})$ bezüglich r. Da die Rang 1-Residuen von $\mathcal{A}$ stets von der Ordnung 2 sind, gilt offenbar auch

$$A_r = \{\sigma \in Aut(\mathcal{B}) \mid \sigma \text{ trivial auf } \Delta_i(c) \text{ mit } c \in r, \text{ falls } |\Delta_i(c) \cap r| = 2\}.$$

Mit $\mathcal{W}(r)$ bezeichnen wir im folgenden die Menge der Apartments von $\mathcal{B}$, welche die Wurzel r enthalten. Operiert A_r transitiv auf $\mathcal{W}(r)$ für jede Wurzel r eines Apartments $\mathcal{A}$, so heißt $\mathcal{B}$ ein *Moufanggebäude*. Ist der Rang von $\mathcal{B}$ mindestens 3, so ist $\mathcal{B}$ stets ein Moufanggebäude. Dies halten wir fest im folgenden Satz von Tits [37], den wir auch in I (4.7) bei Timmesfeld finden.

(2.4.4) Satz.

Sei $\mathcal{B}$ ein dickes, irreduzibles und sphärisches Gebäude vom Rang mindestens 2 und sei r eine Wurzel aus dem Apartment $\mathcal{A}$. Dann operiert A_r fixpunktfrei auf $\mathcal{W}(r)$. Ist der Rang von $\mathcal{B}$ mindestens 3, so operiert A_r transitiv auf $\mathcal{W}(r)$ und insbesondere ist $\mathcal{B}$ ein Moufanggebäude.

2.5 Lie-Algebren

Eine *Lie-Algebra* L ist ein Vektorraum über einem Körper k, auf dem eine bilineare Abbildung $[\ ,\ ] : L \times L \longrightarrow L$ mit folgenden Eigenschaften definiert ist:

(1) $[x, x] = 0$ für alle $x \in L$,

(2) $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$ für alle $x, y, z \in L$.

Die Abbildung $[\ ,\ ]$ heißt die *Lie-Multiplikation* auf L.

Für zwei Unterräume U und W von L definieren wir den Unterraum

$$[U, W] := \langle [u, w] \mid u \in U,\ w \in W \rangle.$$

Eine *Unteralgebra* der Lie-Algebra L ist ein unter der Lie-Multiplikation abgeschlossener Unterraum von L. Ist M eine Unteralgebra mit $[M, L] \leq M$, so heißt M ein *Ideal* von L. Besitzt L neben sich selbst und dem Nullraum keine weiteren Ideale, so heißt L eine *einfache Lie-Algebra*.

Um die Chevalleygruppen einzuführen, müssen wir zunächst die Chevalleybasen von einfachen Lie-Algebren über den komplexen Zahlen beschreiben. Wir beschreiben diese nur kurz und finden weitere Ausführungen in Kapitel 3 bei Carter [6]. Eine komplexe, einfache Lie-Algebra L operiert transitiv auf ihren Cartanunteralgebren, also

den Unteralgebren H mit $[H,H] = 0$ und der Eigenschaft: $[x,H] \leq H$ ist nur für $x \in H$ möglich. Die (gemeinsame) Dimension dieser Cartanunteralgebren nennen wir den üblicherweise mit l bezeicheten *Rang* von L. Weiterhin hat L eindimensionale Unterräume L_{r_i} mit $[H, L_{r_i}] = L_{r_i}$ und

$$L = H \oplus L_{r_1} \oplus \cdots \oplus L_{r_k}.$$

Jede einfache, komplexe Lie-Algebra L ist assoziiert zu einem unzerlegbaren kristallographischen Wurzelsystem Φ. Die Wurzeln lassen sich dabei mit Vektoren aus H identifizieren, derart, dass $L_{r_i} = L_r$ für eine Wurzel $r \in \Phi$ und H von einem Fundamentalsystem Π erzeugt wird. Dann ist

$$L = H \oplus \bigoplus_{r \in \Phi} L_r$$

und es können Vektoren $e_r \in L_r$ und $h_s \in H$ mit $r \in \Phi$ und $s \in \Pi$ gewählt werden, so dass

$$\{h_r \mid r \in \Pi\} \dot\cup \{e_r \mid r \in \Phi\}$$

eine Basis von L mit folgenden Eigenschaften ist:

(1) $[h_r, h_s] = 0$ für $r, s \in \Pi$,

(2) $[h_r, e_s] = \frac{2(r,s)}{(r,r)} e_s$ für $r \in \Pi$ und $s \in \Phi$,

(3) $[e_r, e_{-r}] = h_r$ für $r \in \Pi$,

(4) $[e_r, e_s] = 0$ für $r, s \in \Phi$ mit $r + s \notin \Phi$,

(5) $[e_r, e_s] = N_{rs} e_{r+s}$ für $r, s \in \Phi$ mit $r + s \in \Phi$. Die *Strukturkonstanten* N_{rs} sind dabei so wählbar, dass $N_{rs} = \pm(p^{rs} + 1)$, wobei p^{rs} die größte ganze Zahl p mit $s - pr \in \Phi$ ist.

Die Wahl der Vorzeichen der Strukturkonstanten ist dabei bis zu einem bestimmen Maß beliebig. (Genauere Informationen sind im Zusammenhang mit dieser Arbeit nicht wichtig, aber zu finden bei Carter [6].) Eine solche Basis nennen wir eine *Chevalleybasis* von L.

2.6 Die Chevalleygruppen

Sei L eine einfache, komplexe Lie-Algebra mit Chevalleybasis

$$\{h_r \mid r \in \Pi\} \dot\cup \{e_r \mid r \in \Phi\}$$

und sei $L_{\mathbb{Z}}$ die additiv geschriebene, abelsche Gruppe der ganzzahligen Linearkombination dieser Chevalleybasis. Die folgenden Ausführungen stehen in Kapitel 4 von Carter [6]. Das Lie-Produkt zweier Basisvektoren liegt offenbar in $L_{\mathbb{Z}}$, also ist diese Gruppe abgeschlossen unter der Lie-Multiplikation und damit eine *Lie-Algebra über* $\mathbb{Z}$.

Ist k ein beliebiger Körper, so bilden wir das Tensorprodukt

$$L_k := k \otimes L_{\mathbb{Z}}$$

der additiven Gruppen von k und $L_{\mathbb{Z}}$. Schreiben wir nun

$$\overline{h}_r := 1_k \otimes h_r \quad \text{und} \quad \overline{e}_r := 1_k \otimes e_r,$$

so ist L_k offenbar ein k-Vektorraum mit Basis

$$\overline{B} := \{\overline{h}_r \mid r \in \Pi\} \dot{\cup} \{\overline{e}_r \mid r \in \Phi\}.$$

Bei der Einführung der Chevalleybasis haben wir darauf Wert gelegt, dass die Multiplikationskonstanten A_{rs} und N_{rs} der Chevalleybasis stets ganzzahlig sind. Wir können daher leicht ein Lie-Produkt auf L_k definieren. Setzen wir für je zwei Elemente x und y der Chevalleybasis

$$[1_k \otimes x, 1_k \otimes y] := 1_k \otimes [x, y],$$

so liegt jeder solche Ausdruck wieder in L_k und durch bilineare Ausdehnung wird somit aus L_k eine Lie-Algebra über dem Körper k. Interpretieren wir die Multiplikationskonstanten der Chevalleybasis in natürlicher Weise im Primkörper von k, so sind dies offenbar gerade die Multiplikationskonstanten von L_k zur Basis $\overline{B}$.

Sei nun ad_{e_r} die lineare Abbildung von L definiert durch

$$ad_{e_r}(x) = [e_r, x]$$

für $x \in L$. Dann ist ad_{e_r} offenbar nilpotent und die Abbildung

$$a_r(\xi) := exp(\xi ad_{e_r}) = \sum_{i=0}^{\infty} \frac{(\xi ad_{er})^i}{i!}$$

ist für alle $\xi \in \mathbb{C}$ ein wohldefinierter Automorphismus von L. Die Eigenschaften der Lie-Multiplikation von L vererben sich also auf die der Lie-Multiplikation von L_k und so können wir leicht die Analoga der Abbildungen $a_r(\xi)$ auch für L_k definieren. Als lineare Abbildung hat $a_r(\xi)$ eine Darstellungsmatrix $A_r(\xi)$ bezüglich der Chevalleybasis. Die Operation auf der Chevalleybasis zeigt, dass die Einträge von der Form $a\xi^i$ für ganze Zahlen a und $i \geq 0$ sind. Dabei hängen die Zahlen a und i nur von der Wurzel r ab. Die Matrix $\overline{A}_r(t)$ erhalten wir, wenn wir in $A_r(\xi)$ jedes Element a im Primkörper von k auffassen und ξ durch t ersetzen. Damit definieren wir die lineare Abbildung $\overline{a}_r(t)$ mit Darstellungsmatrix $\overline{A}_r(t)$ bezüglich der Basis $\overline{B}$. Bei Carter [6] finden wir schließlich in (4.4.2), dass $\overline{a}_r(t)$ für alle $t \in k$ und $r \in \Phi$ ein Automorphismus von L_k ist.

Ist k der Körper der komplexen Zahlen, so stimmen die Elemente $a_r(t)$, h_r und e_r mit den Elementen $\overline{a}_r(t)$, $\overline{h}_r$ und $\overline{e}_r$ überein. Da für beliebige Körper k die Multiplikationskonstanten (über dem Primkörper) von L_k bezüglich $\overline{B}$ mit denen von L bezüglich der Chevalleybasis übereinstimmen, schreiben wir einfach $a_r(t)$ für $\overline{a}_r(t)$, h_r für $\overline{h}_r$ und e_r für $\overline{e}_r$.

Die *Chevalleygruppe $L(k)$ vom Typ L über dem Körper k* ist die von den Elementen $a_r(t)$ erzeugte Gruppe

$$L(k) := \langle a_r(t) \mid r \in \Phi,\ t \in k \rangle.$$

Ist der zugrunde liegende Körper k ein endlicher Körper $GF(q)$, so schreiben wir auch $L(k) = L(q)$. Von besonderem Interesse sind die Wurzeluntergruppen einer Chevalleygruppe $G := L(k)$. Zu jeder Wurzel $r \in \Phi$ sei die Untergruppe

$$A_r := \langle a_r(t) \mid t \in k \rangle$$

die *Wurzeluntergruppe* von G zur Wurzel r. Ist die Wurzel r eine lange Wurzel, so nennen wir A_r eine *lange Wurzeluntergruppe* und A_r heißt entsprechend *kurze Wurzeluntergruppe*, wenn r eine kurze Wurzel ist. Die Wurzeluntergruppe A_r heißt weiterhin *positive, negative oder fundamentale Wurzeluntergruppe*, wenn r eine positive, negative oder fundamentale Wurzel ist. Jede Wurzeluntergruppe von G ist isomorph zu $(k, +)$, denn es gilt

$$a_r(t)a_r(s) = a_r(t + s).$$

Die *unipotente Untergruppe U* von G ist das Erzeugnis der positiven Wurzeluntergruppen von G. Mit den Eigenschaften der Operationen der Wurzeluntergruppen auf der (Chevalley)basis von L_k ist es möglich, die Kommutatoren zwischen den Elementen der Wurzeluntergruppen exakt zu bestimmen. Die folgenden Relationen stehen in (5.2.2) bei Carter [6] und sind bekannt als

(2.6.1) Die Chevalley'schen Kommutatorrelationen.

Sind r und s linear unabhängige Wurzeln in Φ^+ und $u, t \in k$, so gilt

$$[a_s(u), a_r(t)] = \prod_{i,j>0} a_{ir+js}(c_{ijrs}(-t)^i u^j),$$

wobei das Produkt über alle Wurzeln der Form $ir + js$ nach aufsteigender Größe von $i + j$ gebildet wird. Die Konstanten c_{ijrs} sind gegeben durch

$$c_{i1rs} = M_{rsi}, \quad c_{1jrs} = (-1)^j M_{srj}, \quad c_{32rs} = \frac{1}{3} M_{r+s,r,2}, \quad c_{23rs} = -\frac{2}{3} M_{s+r,s,2},$$

mit

$$M_{rsi} = \pm \binom{p^{rs} + i}{i}.$$

Dabei ist jede der Konstanten c_{ijrs} eine der Zahlen ± 1, ± 2 oder ± 3.

Nach (6.3.1) von Carter [6] gibt es zu jeder Wurzel r einen Epimorphismus von $SL_2(k)$ auf die Untergruppe $\langle A_r, A_{-r} \rangle$ mit der Eigenschaft

$$\begin{pmatrix} 1 & t \\ & 1 \end{pmatrix} \longmapsto a_r(t) \quad \text{und} \quad \begin{pmatrix} 1 & \\ t & 1 \end{pmatrix} \longmapsto a_{-r}(t).$$

Mit Hilfe dieses Epimorphismus definieren wir für $\lambda \in k^*$ die Elemente $h_r(\lambda)$ und n_r in $\langle A_r, A_{-r}\rangle$ durch die Festlegungen

$$\begin{pmatrix} \lambda & \\ & \lambda^{-1} \end{pmatrix} \longmapsto h_r(\lambda) \quad \text{und} \quad \begin{pmatrix} & 1 \\ -1 & \end{pmatrix} \longmapsto n_r.$$

Ausgehend davon sei dann

$$H := \langle h_r(t) \mid r \in \Phi,\ t \in k^* \rangle$$

die *innere Diagonalgruppe* von G und

$$N := \langle H, n_r \mid r \in \Phi \rangle$$

die *monomiale Gruppe* von G. Ist W die Weylgruppe von Φ, so liefert die Ausdehnung der Abbildung $Hn_r \longmapsto w_r$ einen Isomorphismus von N/H auf W. Die Operationen von W auf Φ und der Menge der Wurzeluntergruppen sind äquivalent und es gilt $A_s^{n_r^{-1}} = A_{w_r(s)}$. Dies finden wir in (7.2.2) bei Carter [6].

Wir haben zu Beginn des Kapitels die Gruppen mit BN-Paaren eingeführt und die parabolischen Untergruppen definiert. Die monomiale Gruppe N der Chevalleygruppe $G = L(k)$ operiert auf der Menge der Wurzeluntergruppen mit Kern H. Insbesondere wird das Erzeugnis U der positiven Wurzeluntergruppen von H normalisiert und UH ist eine Gruppe die wir mit B bezeichnen. Ist der Körper k algebraisch abgeschlossen, so wird B auch als die *Borelgruppe* bezeichnet. Zusammen mit der monomialen Gruppe bildet B nach (7.2.4) und (8.2.1) von Carter [6] sogar ein *zerfallendes BN-Paar* der Chevalleygruppe G. Für jedes Element $w \in W$ sei

$$U_w^- := U \cap U^{w_0 w}.$$

Nach (8.4.4) von Carter [6] gilt dann

(2.6.2) Die Bruhat-Zerlegung.

Jedes Element $g \in G$ hat eine eindeutige Produktdarstellung der Form $g = uhwu'$ mit $u \in U$, $h \in H$, $w \in N$ und $u' \in U_w^-$.

Sei nun $\{r_1, \ldots, r_l\}$ ein Fundamentalsystem von Φ. Ferner sei Φ_J die Menge der Wurzeln, welche Linearkombinationen der fundamentalen Wurzeln r_j mit $j \in J$ sind. Desweiteren bezeichne $\overline{\Phi}_J := \Phi \setminus \Phi_J$. Ist M_J das Erzeugnis der Wurzeluntergruppen zu den positiven Wurzeln aus $\overline{\Phi}_J$, so ist

$$M_J = \prod_{r \in \Phi^+ \cap \overline{\Phi}_J} A_r$$

nach den Chevalley'schen Kommutatorrelationen das Produkt dieser Wurzeluntergruppen. Die Reihenfolge der Faktoren ist dabei beliebig. Die Produktdarstellung in der obigen Zerlegung ist eindeutig und daher ist

$$|M_J| = \prod_{r \in \Phi^+ \cap \overline{\Phi}_J} |A_r|.$$

Typ von G	k	α
A_l	$GF(q^2)$	$o(\alpha) = 2$
D_l	$GF(q^2)$	$o(\alpha) = 2$
E_6	$GF(q^2)$	$o(\alpha) = 2$
D_4	$GF(q^3)$	$o(\alpha) = 3$
B_2	$GF(2^{2m+1})$	$\varphi\alpha^2 = 1$
G_2	$GF(3^{2m+1})$	$\varphi\alpha^2 = 1$
F_4	$GF(2^{2m+1})$	$\varphi\alpha^2 = 1$

Tabelle 2.1: Der Körper k

Weiterhin sei L_J das Erzeugnis der Wurzeluntergruppen zu den Wurzeln aus Φ_J. Die Gruppe M_J nennen wir das *unipotente Radikal von* P_J und L_J heißt das *Levikomplement von* P_J. Nach (8.5.2) von CARTER [6] erhalten wir dann

(2.6.3) Die Levi-Zerlegung.

Es gilt $P_J = M_J L_J H$ *und* P_J *ist der Normalisator von* M_J.

Die Chevalleygruppen sind fast ausnahmslos einfache Gruppen. Wir finden in (11.1.2) bei CARTER [6] den

(2.6.4) Satz.

Die Chevalleygruppen sind bis auf die Ausnahmen $A_1(2)$, $A_1(3)$, $B_2(2)$ *und* $G_2(2)$ *einfache Gruppen. Die Gruppen* $A_1(2)$ *und* $A_1(3)$ *sind auflösbar und in den beiden übrigen Fällen ist die Kommutatorgruppe einfach.*

Bei den Automorphismen einer endlichen Chevalleygruppe unterscheiden wir zunächst vier Sorten von Abbildungen, nämlich die Inneren-, Diagonal-, Körper- und Graphautomorphismen. Alle drei Typen von Abbildungen sind sehr gut bei CARTER [6] beschrieben und wir verzichten hier auf eine nähere Betrachtung. Nach einem Resultat von STEINBERG in (12.5.1) von CARTER [6] gilt der

(2.6.5) Satz.

Jeder Automorphismus einer Chevalleygruppe über einem endlichen Körper ist ein Produkt eines Inneren-, Diagonal-, Körper- und Graphautomorphismus.

2.7 Die getwisteten Gruppen

Die getwisteten Gruppen werden als echte Untergruppen der Chevalleygruppen beobachtet und sie existieren nur in den Fällen, in denen das Dynkindiagramm der Chevalleygruppe eine nichttriviale Diagrammsymmetrie besitzt. Daher sei G im weiteren Verlauf eine Chevalleygruppe $L(k)$ über dem Körper k mit einem nichttrivialen Graphautomorphismus ν. Wir beschränken uns im folgenden auf die Einführung der endlichen getwisteten Gruppen. In dieser Situation werden an den Körper k gewisse Zusatzannahmen gestellt, die wir in Tabelle 2.1 darstellen. Insbesondere besitzt G einen Körperautomorphismus α mit der in der Tabelle angegebenen Eigenschaft, wobei φ die Frobeniusabbildung von k ist. Die Abbildung $\sigma := \alpha\nu$ ist dann ein Automorphismus von G, der die Gruppen U, U^{w_0}, H und N invariant läßt. Definieren wir nun $U^1 := C_U(\sigma)$ und $(U^{w_0})^1 := C_{U^{w_0}}(\sigma)$, so nennen wir die Gruppe

$$G^1 = \langle U^1, (U^{w_0})^1 \rangle$$

eine *getwistete Gruppe*. Eine getwistete Gruppe ist also eine echte Untergruppe einer Chevalleygruppe, welche elementweise von einem Automorphismus σ mit den obigen Eigenschaften festgelassen wird. Allerdings stimmen die Untergruppen G^1 und $C_G(\sigma)$ nicht notwendig überein.

Die Wurzeluntergruppen der getwisteten Gruppen sollen, wie dies entsprechend bei den Chevalleygruppen der Fall ist, zu den Wurzeln eines Wurzelsystems korrespondieren. Mit Hilfe geometrischer Eigenschaften der Gruppe $W^1 := C_W(\sigma)$ ist es möglich, eine Partition Φ^1 von Φ zu finden, so dass jedes Element von Φ^1 entweder nur positive oder nur negative Wurzeln von Φ enthält. Für $S \in \Phi^1$ ist

$$A_S := \prod_{r \in S} A_r$$

eine Gruppe, wobei die Faktoren in beliebiger Reihenfolge angeordnet sind. Ist G nicht vom Typ F_4, so ist Φ^1 mit einem Wurzelsystem wie in Tabelle 2.2 mit Weylgruppe W^1 zu identifizieren, und andernfalls besteht das Wurzelsystem aus den Vektoren vom Ursprung zu den Ecken eines gewöhnlichen 16-Ecks. Die Operationen von W^1 auf den Gruppen $\{A_S \mid S \in \Phi^1\}$ und dem entsprechenden Wurzelsystem sind äquivalent. Die Gruppen

$$A_S^1 := C_{A_S}(\sigma)$$

sind sämtlich nichttrivial und wir bezeichnen sie als die *Wurzeluntergruppen* der getwisteten Gruppe G^1.

Die Bezeichnung dieser Gruppen macht vermöge der Identifikation der Teilmengen S mit den Wurzeln aus Φ^1 Sinn. Die Bezeichnungen *lange, kurze, positive, negative* und *fundamentale* Wurzeluntergruppen vergeben wir wie bei den Chevalleygruppen entsprechend der Bezeichnung der korrespondierenden Wurzel. Sprechen wir im weiteren Verlauf von den Wurzeluntergruppen der getwisteten Gruppe, so bezeichnen wir diese ebenfalls mit A_r, wobei r dann aber eine Wurzel aus Φ^1 ist. Die Bezeichnung der

Typ von L	Typ von W^1
A_l, $l = 2k-1$	C_k
A_l, $l = 2k$	BC_k
D_l	B_{l-1}
E_6	F_4
D_4	G_2
B_2	A_1
F_4	$W \cong D_{16}$
G_2	A_1

Tabelle 2.2: Die Typen von W^1

getwisteten Gruppen G^1 halten wir in der Tabelle 2.3 fest. Die Ordnungen der Chevalleygruppen und der getwisteten Gruppen stellen wir im Anhang A dar. Dort finden wir auch die Isomorphismen einiger Lie-Typ-Gruppen zu den klassischen Gruppen.

G	G^1
$A_l(q^2)$	${}^2A_l(q)$
$D_l(q^2)$	${}^2D_l(q)$
$E_6(q^2)$	${}^2E_6(q)$
$D_4(q^3)$	${}^3D_4(q)$
$B_2(2^{2m+1})$	${}^2B_2(2^{2m+1})$
$G_2(3^{2m+1})$	${}^2G_2(3^{2m+1})$
$F_4(2^{2m+1})$	${}^2F_4(2^{2m+1})$

Tabelle 2.3: Die getwisteten Gruppen

Die Eigenschaften der Wurzeluntergruppen stimmen überwiegend mit denen der Chevalleygruppen überein. Wir finden diese in (13.5.2) bis (13.5.4), sowie (13.6.1) und (13.6.5) von Carter [6] und zählen diese hier nur noch auf. Die *Boreluntergruppe* $B^1 := B \cap G^1$ von G^1 ist das semidirekte Produkt von $H^1 := H \cap G^1$ mit der von den positiven Wurzeluntergruppen von G^1 erzeugten Gruppe U^1. Ferner bilden die Gruppen B^1 und $N^1 := N \cap G^1$ ein zerfallendes saturiertes BN-Paar mit Weylgruppe W^1 von G^1. Die unipotenten Radikale und Levikomplemente werden nun analog wie bei den Chevalleygruppen definiert und es gelten die selben Eigenschaften. In diesem Sinne ist auch die Bruhatzerlegung erfüllt. Schließlich wird die getwistete Gruppe G^1 von ihren fundamentalen Wurzeluntergruppen erzeugt. Abschließend finden wir in (14.4.1) von Carter [6] den

(2.7.1) Satz.

Die getwisteten Gruppen sind bis auf die Ausnahmen ${}^2A_2(2)$, ${}^2B_2(2)$, ${}^2G_2(3)$ *und* ${}^2F_4(2)$ *einfache Gruppen.*

Kapitel 3

Abstrakte Wurzeluntergruppen

Eine Menge Σ von nichttrivialen, abelschen Untergruppen einer Gruppe G heißt eine *Menge von abstrakten Wurzeluntergruppen* von G, wenn die folgenden Eigenschaften erfüllt sind:

(I) $G = \langle \Sigma \rangle$ und $\Sigma^g \subseteq \Sigma$ für alle $g \in G$.

(II) Für jedes Paar $A, B \in \Sigma$ gilt eine der folgenden Eigenschaften:

(a) $[A, B] = 1$.

(b) $\langle A, B \rangle$ ist eine Rang 1-Gruppe mit unipotenten Untergruppen A und B.

(c) $Z(\langle A, B \rangle) \geq [A, B] = [a, B] = [A, b] \in \Sigma$ für alle $a \in A^\sharp$ und $b \in B^\sharp$.

Ist Σ zusätzlich eine Konjugiertenklasse von G, dann heißt Σ eine *Klasse von abstrakten Wurzeluntergruppen*. Die Menge Σ heißt eine *Menge (bzw. Klasse) von k-Wurzeluntergruppen* für den festen Körper k, wenn in II (b) stets

$$\langle A, B \rangle \cong (P)SL_2(k)$$

gilt, und A und B (Bilder) von unipotenten Untergruppen von $SL_2(k)$ sind.

Tritt die Bedingung (c) in II *nicht* auf, so heißt Σ *ausgeartet*, und andernfalls *nichtausgeartet*. Ist $S \leq G$, so sei

$$S \cap \Sigma := \{A \in \Sigma \mid A \leq S\}.$$

Für jede Gruppe $A \in \Sigma$ legen wir folgende Bezeichnungen fest:

$$\begin{aligned} C_\Sigma(A) &:= \{B \in \Sigma \mid [A, B] = 1\}, \\ \Sigma_A &:= C_\Sigma(A) \setminus \{A\}, \\ \Lambda_A &:= \{B \in \Sigma_A \mid \Sigma \cap AB \text{ ist eine Partition von } AB\}, \\ \Psi_A &:= \{B \in \Sigma \mid [A, B] \in \Sigma\}, \\ \Omega_A &:= \{B \in \Sigma \mid \langle A, B \rangle \text{ ist eine Rang 1-Gruppe}\}, \\ D(\Sigma) &:= \{a \in A^\sharp \mid A \in \Sigma\}. \end{aligned}$$

Da Rang 1-Gruppen niemals nilpotent sind, schneiden sich Ω_A und Ψ_A trivial. Es folgt dann offenbar

$$\Sigma = \{A\} \dot\cup \Sigma_A \dot\cup \Psi_A \dot\cup \Omega_A. \tag{3.1}$$

Ein nützliches Hilfsmittel wird uns in dem Graphen $\mathcal{F}(\Delta)$ für $\Delta \subseteq \Sigma$ begegnen, dessen Ecken die Elemente aus Δ sind. Die Kanten sind die Paare $\{A, B\}$ mit $B \in \Omega_A$. Die obigen Definitionen stammen aus Kapitel II von Timmesfeld [34].

G	Σ	Typ
$A_1(k)$	A_h^G	ausgeartet
$C_2(2^f) \cong B_2(2^f)$	A_h^G,	ausgeartet
$C_l(2^f)$, $l > 2$	A_s^G, s kurz	nicht-ausgeartet
$C_l(k)$, $char(k) > 2$	A_h^G	ausgeartet
${}^2A_{2l}(k)$	$(A'_h)^G$	ausgeartet
${}^2A_{2l-1}(k)$	A_h^G	ausgeartet
Sonst	A_h^G	nicht-ausgeartet

Tabelle 3.1: Die Menge Σ

3.1 Notation und erste Resultate

Der Grund für die im Zusammenhang mit dieser Arbeit eingeführten abstrakten Wurzeluntergruppen liegt darin, dass jede endliche, (einfache) Lie-Typ-Gruppe bis auf wenige Ausnahmen eine Klasse von k-Wurzeluntergruppen besitzt. Hauptsächlich elementare Eigenschaften aus der Theorie der abstrakten Wurzeluntergruppen wird für die folgenden Kapitel nutzbringende Resultate liefern.

Für den Rest des Kapitels sei $k = GF(q)$ ein endlicher Körper und G eine von ${}^2F_4(k)$, ${}^2B_2(k)$ und ${}^2G_2(k)$ verschiedene Lie-Typ-Gruppe. Die Bezeichnungen innerhalb von G und dem zugehörigen Wurzelsystem Φ verwenden wir wie im vorangegangenen Kapitel. Weiterhin sei Σ wie in Tabelle 3.1.

In gerader Charakteristik identifizieren wir die Gruppe $C_l(k)$ für $l > 2$ mit der Gruppe $B_l(k)$. Diese beiden Gruppen sind isomorph derart, dass die kurzen Wurzeluntergruppen von $C_l(2^n)$ auf die langen Wurzeluntergruppen von $B_l(2^n)$ abgebildet werden. Insbesondere ist hier Σ das Urbild einer Klasse von abstrakten Wurzeluntergruppen in $B_l(2^n)$. Die auflösbaren Gruppen $A_1(2)$, $A_1(3)$, ${}^2A_2(2)$ und ${}^2B_2(2)$ werden wir im weiteren Verlauf nicht mehr betrachten, da sie für uns nicht von Interesse sein werden. Der folgende Satz ist wohlbekannt, aber kann auch aus II (5.20) von Timmesfeld [34] abgelesen werden.

(3.1.1) Satz.

Σ ist eine Klasse von k-Wurzeluntergruppen von $\langle\Sigma\rangle$.

Es ist wohlbekannt, dass die entsprechende Menge Σ ausgeartet ist oder nicht, aber wir finden dies auch beiläufig in den beiden übernächsten Abschnitten. Bis auf wenige Ausnahmen ist G eine einfache Gruppe und insbesondere ist Σ dann eine Klasse von abstrakten Wurzeluntergruppen von $G = \langle\Sigma\rangle$. Ist G eine der Gruppen $G_2(2)$ oder $B_2(2) \cong C_2(2)$, so ist $G' = \langle\Sigma\rangle$.

(3.1.2) Lemma.

Σ *ist eine* TI*-Menge.*

Beweis. Sei (B, N) das in Kapitel 2 eingeführte BN-Paar von G mit unipotenter Untergruppe U. Sind $A, C \in \Sigma$, so können wir A o.B.d.A. mit der abstrakten Wurzeluntergruppe zu A_h identifizieren. Dann ist $C = A^{b'wb}$ für geeigete $b, b' \in B$ und $w \in N$. Es folgt somit

$$A \cap C = A \cap A^{b'nb} = (A \cap A^n)^b.$$

Nun ist A^n in einer positiven Wurzeluntergruppe von G enthalten oder in U^{w_0}. In beiden Fällen folgt offensichtlich die Behauptung. □

Eine *isolierte Ecke* eines Graphen ist eine Ecke, die auf keiner Kante liegt. Ist A die abstrakte Wurzeluntergruppe zu A_h und B die zu A_{-h}, so ist $B \in \Omega_A$. Insbesondere enthält $\mathcal{F}(\Sigma)$ eine nichtisolierte Ecke und nach II (2.13) von Timmesfeld [34] erhalten wir daher das

(3.1.3) Lemma.

Der Graph $\mathcal{F}(\Sigma)$ *ist zusammenhängend.*

Der Normalisator der Wurzeluntergruppe A_h ist stets eine parabolische Untergruppe von G. Außer bei den linearen Gruppen ist dieser Normalisator stets maximalparabolisch. Dies sehen wir direkt aus dem erweiterten Dynkindiagramm und der Tatsache, dass $G = BNB$. Ebenso sehen wir dort, dass $N(A_h)$ bei den linearen Gruppen zweitmaximal ist. Es ist dann klar, dass die Gruppen A_h und die zugehörige abstrakte Wurzeluntergruppe denselben Normalisator haben, also hat jeder Normalisator $N(A)$ für $A \in \Sigma$ eine *Levizerlegung*

$$N(A) = M_A L_A H$$

mit unipotentem Radikal M_A und Levikomplement L_A. Eine der wichtigsten Eigenschaften der unipotenten Radikale M_A ist ihre reguläre Operation auf Ω_A. Die Fixpunktfreiheit dieser Operation können wir dabei durch die Eigenschaften des BN-Paares von G nachweisen, wenn M_A eine auf Ω_A transitive Untergruppe enthält. Für die Existenz der transitiven Untergruppe unterscheiden wir die Fälle, in denen Σ nichtausgeartet oder ausgeartet ist.

(3.1.4) Satz.

Für $A \in \Sigma$ *operiert* M_A *regulär auf* Ω_A*. Weiterhin ist* $M_A = \langle A, \Lambda_A \rangle$*, wenn* Σ *nichtausgeartet ist.*

(3.1.5) Bemerkung.

Für die Gruppen $G = G_2(2)$ und $C_2(2)$ ist G' fixpunktfrei, aber nicht mehr transitiv.

Beweis. Die Gruppe A sei o.B.d.A. die abstrakte Wurzeluntergruppe zur Gruppe A_h. Wir behandeln zuerst den Fall, dass G eine Gruppe vom Lie-Rang 1 ist. Dann ist $N(A)$ die Boreluntergruppe von G und aus der Bahnformel folgt

$$|\Sigma| = |G : N_G(A_h)| = |G : B| = |M_A| + 1.$$

Aus Ordnungsgründen folgt nun die Behauptung.

Sei nun G vom Lie-Rang mindestens 2 und Σ nicht-ausgeartet. Ist

$$M := \langle A, \Lambda_A \rangle,$$

so ist M/A nach III (2.6) von TIMMESFELD [34] eine abelsche Gruppe. Somit ist offenbar M eine p-Gruppe. Natürlich ist $M \trianglelefteq N(A)$ und somit in M_A enthalten, denn nach (47.5) von ASCHBACHER [2] ist $M_A = F(N(A))$. Sicherlich gibt es dann Elemente in Σ_A, die außerhalb von M liegen. Nach III (2.15) von TIMMESFELD [34] ist daher M transitiv auf Ω_A. Insbesondere ist auch M_A transitiv auf Ω_A.

Sei Σ ausgeartet und G habe mindestens den Lie-Rang 2. In III (1.6) von [34] finden wir eine auf Ω_A transitive Untergruppe M von M_A, also ist auch hier M_A transitiv auf Ω_A.

In den beiden letzten Fällen bleibt die Fixpunktfreiheit der Operation von M_A auf Ω_A zu zeigen. Sei dazu $B \in \Omega_A$ und $m \in M_A$ mit $B^m = B$. Da nun M_A transitiv auf Ω_A operiert, sei o.B.d.A. $B = A^{w_0}$ die abstrakte Wurzeluntergruppe zu A_{-h}. Dann ist $m \in M_A \cap N(B)$ und wir zeigen $M_A \cap N(B) = 1$. Nach (2.8.6) und dem Beweis von (2.8.2) in CARTER [7] gibt es eine Untergruppe N^* von N mit $G = N(A)N^*N(A)$ und

$$M_A \cap N(A)^n = (M_A \cap M_A^n)((L_AH)^n \cap M_A) \tag{3.2}$$

für alle $n \in N^*$. Ist W_J die Weylgruppe von $N(A)$, so ist nach (2.8.1) von CARTER [7] auch

$$w_0 \in N(A)nN(A) \cap N = W_JnW_J$$

für ein $n \in N^*$. Insbesondere gibt es $n_1, n_2 \in W_J$ mit $w_0 = n_1nn_2$. Wegen $n_1 \in N(A) \cap N(L_AH)$ liefert die Konjugation von (3.2) mit n_2 gerade

$$\begin{aligned} M_A \cap N(B) = M_A \cap N(A)^{w_0} &= (M_A \cap M_A^{w_0})((L_AH)^{w_0} \cap M_A) \\ &= (M_A \cap M_A^{w_0})(L_AH \cap M_A) = 1, \end{aligned}$$

wie gewünscht. Aus dem Frattiniargument folgt auch der zweite Teil der Behauptung. □

3.2 Unipotente Radikale

Wir starten in diesem Abschnitt mit der Bestimmung der Kommutatoren und Zentren der unipotenten Radikale M_A für $A \in \Sigma$, wobei in diesem Abschnitt Σ *nicht-ausgeartet* sei. Im folgenden sei o.B.d.A. A die abstrakte Wurzeluntergruppe zu A_h. Ist G eine Chevalleygruppe und B die abstrakte Wurzeluntergruppe zu A_{-h}, dann definiert die Konjugation mit den Diagonalelementen von $\langle A, B\rangle$ auf

$$V := M_A/Z(M_A) = \overline{M}_A$$

eine skalare Multiplikation über dem Körper k. Das Argument benutzt die exakten Chevalley'schen Kommutatorrelationen. Die Kommutatorbildung auf V liefert dann eine symplektische Form auf V, die mit obiger Skalarmultiplikation verträglich ist. Da in M_A gerade das Zentrum ausfaktorisiert wird, ist diese symplektische Form automatisch nicht-ausgeartet. Etwas umständlicher werden wir dann die gleiche Behauptung für die getwisteten Gruppen erhalten, allerdings ohne die Verwendung exakter Kommutatorrelationen.

3.2.1 Chevalleygruppen

Das prinzipielle Vorgehen bei den Chevalleygruppen ist stets dasselbe, weswegen wir nach einigen Beispielen weniger ausführlich werden. Für eine Wurzel $r \in \Phi$ sei $r^* = h - r$ und für jede Teilmenge L von Φ sei $L^* = \{r^* \mid r \in L\}$. Die Elemente aus der Diagonalgruppe von $\langle A, B\rangle$ bezeichnen wir mit $h(s)$ für $s \in k^*$.

(3.2.1.1) Die linearen Gruppen.

Sei G eine lineare Gruppe mit Wurzelsystem Φ vom Typ A_l mit $l > 1$. Wir haben auf Seite 18 von Kapitel 2 dargestellt, dass M_A das Produkt von positiven Wurzeluntergruppen ist. Durch Inspektion des Wurzelsystems sehen wir, dass M_A von A und den Wurzeluntergruppen zu den Wurzeln aus

$$\begin{aligned} L &:= \{e_1 - e_k \mid 2 \leq k \leq l\} \quad \text{und} \\ L^* &= \{e_k - e_{l+1} \mid 2 \leq k \leq l\} \end{aligned}$$

erzeugt wird, wobei $h = e_1 - e_{l+1}$. Ein Vergleich mit den Wurzeln von Φ zeigt sofort, dass die Vielfachensumme zweier Wurzeln aus L niemals eine Wurzel ist. Analog gilt dies auch für die Wurzeln aus L^* und für $r \in L$ ist sogar r^* die einzige Wurzel in L^*, so dass eine Vielfachensumme von r und r^* in Φ liegt. Dies ist vielmehr nur in der Form $r + r^* = h$ möglich. Aus den Chevalley'schen Kommutatorrelationen folgt daher für $t_1, t_2 \in K$ sofort

$$[a_r(t_1), a_{r^*}(t_2)] = a_h(c_{11rr^*}t_1t_2).$$

Hier ist $c_{11rr^*} = \pm(p^{rr^*} + 1)$, wobei p^{rr^*} die größte ganze Zahl p mit $r^* - pr \in \Phi$ ist. Es ist sehr leicht zu sehen, dass $p^{rr^*} = 0$ und daher gilt

$$[a_r(t_1), a_{r^*}(t_2)] = a_h(\pm t_1 t_2). \tag{3.3}$$

Es ist nun klar, dass M_A ein zentrales Produkt der Gruppen

$$\langle A_r, A_{r^*} \rangle = A_r A_h A_{r^*}$$

ist, und aus den Kommutatoridentitäten folgt leicht

$$M'_A = A = Z(M_A).$$

Offenbar ist nun

$$A_{hr} := \frac{2(h,r)}{(h,h)} = 1$$

für alle $r \in L \cup L^*$ und nach Kapitel 12 von CARTER [6] somit

$$a_r(t)^{h(s)} = a_r(s^{A_{rs}} t) = a_r(st)$$

für alle $t \in k$ und $s \in k^*$. Wir sehen damit leicht ein, dass V ein k-Vektorraum ist vermöge der Skalarmultiplikation

$$s \cdot v := v^{h(s)} \quad \text{und} \quad 0 \cdot v = 1$$

für $s \in k^*$ und $v \in V$. Sei weiterhin $f : V \times V \longrightarrow k$ mit

$$f(\overline{m}, \overline{n}) = c,$$

wenn $[m, n] = a_h(c)$. Dann ist f wegen $A = M'_A \leq Z(M_A)$ wohldefiniert und antisymmetrisch, da die Kommutatorabbildung antisymmetrisch ist. Mit den Kommutatoridentitäten und $M'_A \leq Z(M_A)$ sehen wir sofort, dass f auch die Addition auf V respektiert. Schließlich respektiert f wegen $A_{hh} = 2$ und (3.3) die skalare Multiplikation und offenbar ist nun V ein nicht-ausgearteter symplektischer k-Vektorraum.

(3.2.1.2) Die orthogonalen Gruppen $B_l(k)$.

Sei G eine orthogonale Gruppe $B_l(k)$ mit Wurzelsystem Φ vom Typ B_l. Durch Inspektion des Wurzelsystems sehen wir, dass M_A von A und den Wurzeluntergruppen zu den Wurzeln aus

$$\begin{aligned} L &:= \{e_1, e_1 \pm e_k \mid 3 \leq k \leq l\} \quad \text{und} \\ L^* &= \{e_2, e_2 \mp e_k \mid 3 \leq k \leq l\} \end{aligned}$$

erzeugt wird, wobei $h = e_1 + e_2$. Aus dem selben Grund wie in 3.2.1.1 ist für $t_1, t_2 \in k$ wieder

$$[a_r(t_1), a_{r^*}(t_2)] = a_h(c_{11rr^*} t_1 t_2).$$

Wir prüfen leicht nach, dass $p^{rr^*} = 0$ bis auf die Wurzel $r = e_1$. Hier ist $p^{rr^*} = 1$. In allen Fällen ist also M_A zentrales Produkt der Gruppen $\langle A_r, A_{r^*} \rangle$, wenn wir uns

daran erinnern, dass Σ für $B_2(k)$ in gerader Charakteristik ausgeartet ist. Aus den Kommutatoridentitäten folgt in ungerader Charakteristik

$$M'_A = A = Z(M_A).$$

In gerader Charakteristik ist $M'_A = A$ und $Z(M_A)$ offenbar von der Ordnung q^3.

Wir rechnen leicht nach, dass $A_{hr} = 1$ für alle Wurzeln $r \in L \cup L^*$. Völlig analog zu 3.2.1.1 folgt nun, dass V ein nicht-ausgearteter symplektischer k-Vektorraum ist.

(3.2.1.3) Die orthogonalen Gruppen $D_l(k)$.

Sei G eine orthogonale Gruppe $D_l(k)$ mit Wurzelsystem Φ vom Typ D_l. Durch Inspektion des Wurzelsystems sehen wir, dass M_A von A und den Wurzeluntergruppen zu den Wurzeln aus

$$L := \{e_1 \pm e_k \mid 3 \leq k \leq l\} \quad \text{und}$$
$$L^* = \{e_2 \mp e_k \mid 3 \leq k \leq l\}$$

erzeugt wird, wobei $h = e_1 + e_2$. Völlig analog zu 3.2.1.1 folgt nun, dass V ein nicht-ausgearteter symplektischer k-Vektorraum ist.

(3.2.1.4) Die Gruppen $E_6(k)$, $E_7(k)$ und $E_8(k)$.

Sei G eine der Gruppen $E_6(k)$, $E_7(k)$ oder $E_8(k)$ mit jeweiligem Wurzelsystem Φ vom Typ E_6, E_7 oder E_8. Jede Wurzel r ist eine Linearkombination der fundamentalen Wurzeln. Den i-ten Koeffizienten in dieser Darstellung bezeichnen wir mit r^i. In der obigen Reihenfolge sei nun i die Zahl 2, 1 oder 8 und L_i die Menge der positiven Wurzeln r mit $r^i = 1$. Durch Inspektion der Wurzelsysteme sehen wir, dass M_A von A und den Wurzeluntergruppen zu den Wurzeln aus L_i erzeugt wird. Durch leichtes Nachrechnen sehen wir $h^{w_{r_i}} = h - r_i \in L_i$. Zu jedem $r \in L_i$ gibt es ein $w \in W_{I\setminus\{i\}}$ mit $r = r_i^w$, denn L_i ist eine Bahn unter $W_{I\setminus\{i\}}$. Insbesondere ist dann $r^* = (h - r_i)^w \in L_i$. Die Wurzel h ist die einzige Wurzel mit 2 als i-tem Koeffizient, also ist r^* die einzige Wurzel in L_i, so dass die Vielfachensumme von r und r^* in Φ liegt. Wie in den vorangegangenen Fällen folgt nun für $t_1, t_2 \in k$ wieder

$$[a_r(t_1), a_{r^*}(t_2)] = a_h(\pm t_1 t_2).$$

Insbesondere ist M_A zentrales Produkt der Gruppen $\langle A_r, A_{r^*}\rangle$ für $r \in L_i$ und

$$M'_A = A = Z(M_A).$$

Wir rechnen nach, dass $A_{hr} = 1$ für alle Wurzeln $r \in L_i$. Völlig analog folgt nun, dass V ein nicht-ausgearteter symplektischer k-Vektorraum ist.

Die Wurzeln der Wurzelsysteme vom Typ E_6, E_7, E_8 sind etwas schwierig zu erfassen. Daher kann die Rechnung, dass $A_{hr} = 1$ für $r \in L_i$ unbefriedigend sein. In diesem Fall verweisen wir auf ein anderes Argument im Beweis zu (4.4) in der Arbeit von Curtis, Kantor & Seitz [11].

(3.2.1.5) Die Gruppen $F_4(k)$.

Sei G eine Gruppe $F_4(k)$ mit Wurzelsystem Φ vom Typ F_4. Durch Inspektion des Wurzelsystems sehen wir, dass M_A von A und den Wurzeluntergruppen zu den 14 Wurzeln aus

$$L := \{e_1, e_2, e_2 \pm e_3, e_2 \pm e_4, e_1 \pm e_3, e_1 \pm e_4, \frac{1}{2}(e_1 + e_2 \pm e_3 \pm e_4)\}$$

erzeugt wird, wobei $h = e_1 + e_2$. Zu jeder Wurzel $r \in L$ ist auch $r^* \in L$. Wir rechnen leicht nach, dass r^* die einzige Wurzel in L ist, so dass die Vielfachensumme von r und r^* in Φ liegt. Ferner ist dies nur in der Form $r + r^* = h$ möglich. Aus den Chevalley'schen Kommutatorrelationen erhalten wir für $t_1, t_2 \in k$ die Identität

$$[a_r(t_1), a_{r^*}(t_2)] = a_h(c_{11rr^*}t_1t_2).$$

Hierbei ist $c_{11rr*} = \pm 2$ für die Wurzeln $r = e_1$ und $\frac{1}{2}(e_1+e_2+e_3\pm e_4)$ (und entsprechend r^*). In den übrigen Fällen ist $c_{11rr^*} = \pm 1$. In allen Fällen folgt, dass M_A das zentrale Produkt der Gruppen $\langle A_r, A_{r^*}\rangle$ ist. Aus den Kommutatoridentitäten erhalten wir

$$M'_A = A = Z(M_A)$$

in ungerader Charakteristik und

$$M'_A = A < Z(M_A)$$

mit $Z(M_A)$ von der Ordnung q^7 in gerader Charakteristik.

Für alle Wurzeln $r \in L$ rechnen wir leicht $A_{hr} = 1$ nach, und daher ist V wieder ein nicht-ausgearteter symplektischer k-Vektorraum.

(3.2.1.6) Die Gruppen $G_2(k)$.

Sei schließlich G die Gruppe $G_2(q)$ mit Wurzelsystem Φ vom Typ G_2. Durch Inspektion des Wurzelsystems sehen wir, dass M_A von A und den Wurzeluntergruppen zu den Wurzeln aus

$$L := \{e_2 + e_3 - 2e_1, e_3 - e_1, e_1 + e_3 - 2e_2, e_3 - e_2\}$$

erzeugt wird, wobei $h = 2e_3 - e_2 - e_1$. Verfahren wir wie oben, so ist für $t_1, t_2 \in k$ gerade

$$[a_r(t_1), a_{r^*}(t_2)] = a_h(c_{11rr^*}t_1t_2)$$

für alle Wurzeln $r \in L$. Ferner ist $c_{11rr^*} = \pm 3$ für die Wurzel $r = e_3 - e_1$ (und entsprechend r^*). Für die übrigen Wurzeln ist $c_{11rr^*} = \pm 1$. Wie oben ist nun in von 3 verschiedener Charakteristik

$$M'_A = A = Z(M_A)$$

und in Charakteristik 3 ist

$$M'_A = A < Z(M_A)$$

G	Dimension von V
$A_l(q)$ für $l \geq 1$	$2l-2$
$B_l(q)$ für q ungerade	$4l-6$
$B_l(q)$ für q gerade und $l > 2$	$4l-8$
$D_l(q)$	$4l-8$
$E_6(q)$	20
$E_7(q)$	32
$E_8(q)$	56
$F_4(q)$, q ungerade	14
$F_4(q)$, q gerade	8
$G_2(q)$, $3 \nmid q$	4
$G_2(q)$, $3 \mid q$	2

Tabelle 3.2: Die Dimension von V

mit $Z(M_A)$ von der Ordnung q^3. Für alle $r \in L$ ist ferner $A_{hr} = 1$, und schließlich ist V auch hier ein nicht-ausgearteter symplektischer k-Vektorraum. Eine triviale Abänderung zeigt, dass M_A/A auch in Charakteristik 3 ein (symplektischer) k-Vektorraum ist.

Seien nun $A, B \in \Sigma$ zwei abstrakte Wurzeluntergruppen mit $B \in \Omega_A$. Nützlich für den ersten Teil der Arbeit ist unter anderem die Existenz einer zentralen Involution in

$$Y := \langle A, B \rangle,$$

natürlich nur, wenn k von ungerader Charakteristik ist. Dies ist stets der Fall, denn wir haben unabhängig von der Charakteristik des Körpers das folgende

(3.2.1.7) Lemma.

Es ist $Y \cong SL_2(k)$ und für $C \in \Lambda_A \cap \Psi_B$ ist $C[C,B]$ ein natürlicher $\mathbb{Z}Y$-Modul.

Beweis. Die in diesem Beweis benutzten Aussagen sind erste elementare Eigenschaften der Klassen von abstrakten Wurzeluntergruppen von Timmesfeld [34]. Dort finden wir in Kapitel II bei (2.15) und (2.19) eine abstrakte Wurzeluntergruppe C mit $C \in \Lambda_A \cap \Psi_B$, für die

$$N := \langle C^Y \rangle = C[C,B]$$

ein natürlicher $\mathbb{Z}\overline{Y}$-Modul ist mit

$$\overline{Y} := Y/C_Y(N) \cong SL_2(K) \quad \text{und} \quad C_Y(N) \leq Z(Y),$$

K ein Schiefkörper oder eine Caley-Divisionsalgebra. Wegen $C_Y(N) \leq Z(Y)$ ist die Behauptung nun klar. □

Ist k von ungerader Charakteristik, so besitzt also Y eine zentrale Involution i. Wir erhalten für diese Involution das

(3.2.1.8) Lemma.

Ist k von ungerader Charakteristik, so ist $C_{M_A}(i) = A$.

Beweis. Nach den obigen Punkten ist auch $\widetilde{M_A} := M_A/A$ stets ein k-Vektorraum, also ist die Aussage offenbar bewiesen, wenn dieser von i invertiert wird. Dies ist nach 3.1.4 der Fall, wenn $\widetilde{C}$ für alle $C \in \Lambda_A$ von i invertiert wird. Wegen der Zerlegung von Σ aus (3.1) liegt C in Ψ_B, Ω_B oder vertauscht mit B. Im letzten Fall wird Y von C zentralisiert und daher enthält $cA^\sharp$ für $c \in C^\sharp$ nach II (2.2) von Timmesfeld [34] keine Wurzelelemente. Dies ist offenbar ein Widerspruch.

Im zweiten Fall existiert nach II (2.11) von Timmesfeld [34] ein Element $D \in AC \cap \Psi_B$ mit $\widetilde{C} = \widetilde{D}$. Offenbar ist auch $D \in \Lambda_A$ und wir können o.B.d.A. $C \in \Lambda_A \cap \Psi_B$ wie im ersten Fall annehmen. Jetzt können wir die Behauptung im Beweis von 3.2.1.7 direkt ablesen. Nun ist nämlich $C[C, B]$ ein natürlicher $\mathbb{Z}Y$-Modul und insbesondere wird C und $\widetilde{C}$ von i invertiert. □

3.2.2 Getwistete Gruppen

Das Vorgehen im vorangegangenen Unterabschnitt hat die exakten Chevalley'schen Kommutatorrelationen ausgenutzt. Auch für die getwisteten Gruppen existieren die exakten Chevalley'schen Kommutatorrelationen, jedoch sind sie schwieriger zu erfassen. Die getwisteten Gruppen sind echte Untergruppen von Chevalleygruppen. Unter Verwendung der Aussage, dass V ein nicht-ausgearteter symplektischer Raum ist, lassen sich die Chevalley'schen Kommutatorrelationen hier umgehen, indem wir Eigenschaften von Timmesfelds [34] Theorie der abstrakten Wurzeluntergruppen benutzen. Hilfreich wird dabei das folgenden Lemma sein.

(3.2.2.1) Lemma.

Sei L ein Körper und W ein nicht-ausgearteter, symplektischer L-Vektorraum mit Form f und Basis $(w_i \mid i \in I)$. Ist k ein Unterkörper von L mit $f(w_i, w_j) \in k$ für $i, j \in I$, dann ist das k-Erzeugnis W_k von $(w_i \mid i \in I)$ ein nicht-ausgearteter symplektischer k-Vektorraum mit Form $f_{|W_k}$.

Beweis. Per Definition ist W_k ein k-Vektorraum und wegen $f(w_i, w_j) \in k$ ist $f' := f_{|W_k}$ eine symplektische Form von W_k. Ist $v \in W_k$ mit $f'(v, W_k) = 0$, so gilt insbesondere $f(v, w_i) = 0$ und somit auch $f(v, W) = 0$. Da f nicht-ausgeartet ist, folgt $v = 0$ und damit die Behauptung. □

Sei nun G eine der getwisteten Gruppen ${}^2E_6(k)$, ${}^2D_l(k)$ und ${}^3D_4(k)$, welche wir als echte Untergruppen von $E_6(L)$, $D_l(L)$ bzw. $D_4(L)$ mit $L = GF(q^2)$ oder entsprechend $GF(q^3)$ auffassen. Die entsprechende Chevalleygruppe bezeichnen wir mit G^*, und Σ^*

sei die zugehörige Klasse der k-Wurzeluntergruppen von G^*. Mit h sei aber weiterhin die höchste positive Wurzel im Wurzelsystem von G^* bezeichnet und A_h^* sei die abstrakte Wurzeluntergruppe zur Wurzel h in G^*. Verfolgen wir die Konstruktion der Wurzeluntergruppen von getwisteten Gruppen in (13.2) von CARTER [6], so ist dann $\{h\}$ ein Element der Partition Φ^1 von Seite 20, also ist insbesondere

$$C_{A_h^*}(\sigma) =: A \in \Sigma.$$

Wir beschreiben nun das weitere Vorgehen. Zunächst ist jede Untergruppe $B \in \Sigma$ in genau einer Untergruppe $B^* \in \Sigma^*$ enthalten, und die Elemente von $\Lambda_A \cap \Psi_B$ sind für $B \in \Omega_A$ in Elementen von $\Lambda_{A^*} \cap \Psi_{B^*}$ enthalten (und umgekehrt). Nach III (2.13) von TIMMESFELD [34] werden M_A bzw. M_A^* von A bzw. A^* und den beiden Mengen $\Lambda_A \cap \Psi_B$ bzw. $\Lambda_{A^*} \cap \Psi_{B^*}$ erzeugt, also ist insbesondere $M_A \leq M_{A^*}$. Insbesondere ist dann wegen $M'_{A*} = A^*$ auch leicht

$$M'_A = A.$$

Ein leichtes Abzählargument zeigt

$$|M_A/A| = q^d,$$

wobei d die Dimension des nicht-ausgearteten symplektischen L-Vektorraumes

$$V^* := M_A^*/A^* = \widetilde{M_{A^*}}$$

ist. Somit ist M_A Produkt von A mit d Untergruppen $C_i \in \Lambda_A \cap \Psi_B$. Wegen $|V^*| = (q^{|L:k|})^d$ ist V^* Produkt der d Gruppen $\widetilde{C}_i^*$, also können wir Elemente $1 \neq v_i \in C_i$ wählen, so dass $(\widetilde{v}_1, \ldots, \widetilde{v}_d)$ eine L-Basis von V^* ist. Die skalare Multiplikation ist dabei gegeben durch die Konjugation mit den Diagonalelementen aus

$$H^* = \{h(a) \mid a \in L^*\}$$

von $\langle A^*, B^* \rangle$, wobei o.B.d.A. $B^* = A_{-h}^*$.

Wir beachten hierbei Folgendes. Um $M_A \leq M_{A^*}$ zu erreichen, reicht es, die Elemente von Λ_A in Elementen von Λ_{A^*} wieder zu finden. Allerdings sind die Gruppen in Λ_{A^*} nicht notwendig invariant unter H^*, was zu Problemen bei der Konstruktion einer Skalarmultiplikation auf V führt. Der Grund für die Betrachtung der Menge $\Lambda_{A^*} \cap \Psi_{B^*}$ liegt in Lemma 3.2.1.7, nach welchem die Elemente dieser Menge H^*-invariant sind.

Wir definieren dann auf V eine skalare Multiplikation vermöge

$$a \cdot \overline{v} := \overline{v^{h(a)}} \quad \text{und} \quad 0 \cdot \overline{v} = 1$$

für $v \in M_A$ und $a \in k^*$. Da die Elemente $h(a)$ mit $a \in k$ in G liegen, ist diese Multiplikation wohldefiniert und V ist dann ein d-dimensionaler k-Vektorraum. Insbesondere ist dann $V \cong V_k^*$ aus 3.2.2.1. Der Vorteil der oben gewählten Basis ist nun, dass

$$f^*(\widetilde{v}_i, \widetilde{v}_j) \in k, \tag{3.4}$$

wobei f^* die nicht-ausgeartete symplektische Form von V^* aus den Punkten 3.2.1.3 bzw. 3.2.1.4 ist. Somit ist auch V ein nicht-ausgearteter symplektischer k-Vektorraum vermöge der Form $f : V \times V \longrightarrow k$ mit

$$f(\overline{v}, \overline{u}) = f^*(\widetilde{v}, \widetilde{u}),$$

für $v, u \in M_A$. Wir beachten hierbei, dass die Form f durch *Kommutatorbildung* entsteht. Insbesondere ist dann auch

$$A = Z(M_A).$$

(3.2.2.2) Lemma.

Jede abstrakte Wurzeluntergruppe von G ist in genau einer abstrakten Wurzeluntergruppe von G^* enthalten.

Beweis. Sei $B \in \Sigma$ und $g \in G$ mit $B = A^g$. Da g mit σ vertauscht, ist

$$B = C_{A^{*g}}(\sigma) \leq (A^*)^g \in \Sigma^*.$$

Da Σ eine TI-Menge ist, folgt die Behauptung. □

Die durch eine abstrakte Wurzeluntergruppe $B \in \Sigma$ eindeutig festgelegte abstrakte Wurzeluntergruppe in Σ^* bezeichnen wir im folgenden mit B^*. Nach obigem Lemma ist dies wohldefiniert. Bis auf weiteres sei nun

$$B \in \Omega_A.$$

Offenbar sind dann A^* und B^* nicht vertauschbar und es ist auch nicht $[A^*, B^*] \in \Sigma^*$, denn andernfalls wäre

$$[A, B] \leq C_{[A^*, B^*]}(\sigma) \in \Sigma.$$

Aus der Zerlegung (3.1) folgt nun $B^* \in \Omega_{A^*}$.

(3.2.2.3) Lemma.

Genau dann ist $C \in \Lambda_A \cap \Psi_B$, wenn $C^* \in \Lambda_{A^*} \cap \Psi_{B^*}$.

Beweis. Sei zuerst $C \in \Lambda_A \cap \Psi_B$. Wegen der Zerlegung (3.1) ist offenbar $C^* \in \Psi_{B^*}$ und es bleibt nur $C^* \in \Lambda_{A^*}$ zu zeigen. Sind A^* und C^* nicht vertauschbar, so ist C^* in Ψ_{A^*} oder in Ω_{A^*}. Im ersten Fall ist

$$\chi_a : c \longmapsto [a, c]$$

nach II (2.8) von Timmesfeld [34] für $a \in A^{*\sharp}$ ein Isomorphismus von C^* auf $[A^*, C^*] \in \Sigma^*$. Dies ist ein Widerspruch, wenn wir $a \in A$ wählen. Da der zweite Fall offenbar unmöglich ist, ist $C^* \in \Sigma_{A^*}$.

Somit ist C^* eine Ecke von $\mathcal{F}(C_{\Sigma^*}(A^*))$. Die isolierten Ecken dieses Graphen sind genau die Elemente aus $\Lambda_{A^*} \cup \{A^*\}$, also bleibt zu zeigen, dass C^* isoliert ist. Dies finden wir in III (2.6) von TIMMESFELD [34]. Angenommen C^* ist in diesem Graphen nicht isoliert. Dann gibt es ein $D^* \in \Omega_{C^*}$ mit $A^* \leq C(\langle C^*, D^* \rangle)$. Nach II (2.2) von TIMMESFELD [34] ist dann

$$aC^{*\sharp} \cap D(\Sigma^*) = \emptyset$$

für $1 \neq a \in A^*$. Wählen wir nun aber $a \in A^\sharp$ und $c \in C^\sharp$, so ist ac nach Voraussetzung in einer abstrakten Wurzeluntergruppe von Σ enthalten, und nach obigem Lemma auch in einer abstrakten Wurzeluntergruppe aus Σ^*. Dies ist ein Widerspruch, also ist C^* wie gewünscht isoliert im obigen Graphen.

Sei nun $C^* \in \Lambda_{A^*} \cap \Psi_{B^*}$. Dann sind A^* und C^* vertauschbar und jedes Element ac mit $a \in A$ und $c \in C$ liegt in einem Element von Σ^*. Da a und c von σ zentralisiert werden, liegt ac in einem Element von Σ und daher ist $C \in \Lambda_A$.

Die Abbildung

$$\chi_b : c \longmapsto [b, c]$$

ist für $b \in (B^*)^\sharp$ nach II (2.8) von TIMMESFELD [34] ein Isomorphismus von C^* auf $[B^*, C^*] \in \Sigma^*$. Daher ist offenbar notwendig $C \in \Psi_B$ und es folgt das Lemma. □

Wie oben beschrieben ist nun insbesondere $M'_A = A$ und wir können auf der elementarabelschen Gruppe V wie oben beschrieben eine skalare Multiplikation vermöge

$$a \cdot \overline{v} := \overline{v^{h(a)}} \quad \text{und} \quad 0 \cdot \overline{v} = 1$$

definieren, wobei $v \in M_A$ und $a \in k^*$. Wir erhalten leicht das

(3.2.2.4) Lemma.

V ist mit der oben definierten skalaren Multiplikation ein d-dimensionaler k-Vektorraum.

Beweis. Seien $0 \neq \lambda, \mu \in k$ und $v \in M_A$. Wegen $M_A \leq M_{A^*}$ ist

$$v^{h(\lambda+\mu)} \equiv v^{h(\lambda)} v^{h(\mu)} \mod A^*.$$

Die Elemente $h(a)$ normalisieren für $a \in k$ die Gruppe M_A, denn dies sind die Diagonalelemente von $\langle A, B \rangle$. Also ist $v^{h(\lambda+\mu)}, v^{h(\lambda)} v^{h(\mu)} \in M_A$. Natürlich ist $M_A \cap A^* = A$ und daher ist

$$v^{h(\lambda+\mu)} \equiv v^{h(\lambda)} v^{h(\mu)} \mod A.$$

Es folgt also

$$(\lambda + \mu)\overline{v} = \lambda\overline{v} + \mu\overline{v}.$$

Die übrigen Punkte sind klar, also folgt die Behauptung. □

Ist nun $(\widetilde{v}_1, \ldots, \widetilde{v}_d)$ die oben erläuterte Basis von V^*, so ist V wie gewünscht ein nichtausgearteter, symplektischer, d-dimensionaler k-Vektorraum. Wir halten die Dimension von V in Tabelle 3.3 fest.

G	Dimension von V
${}^3D_4(q)$	8
${}^2D_l(q)$	$4l-8$
${}^2E_6(q)$	20

Tabelle 3.3: Die Dimension von V

Seien nun wieder $A, B \in \Sigma$ zwei abstrakte Wurzeluntergruppen mit $B \in \Omega_A$ und

$$Y := \langle A, B \rangle.$$

Das folgende Lemma gilt offenbar auch für die getwisteten Gruppen, wenn wir benutzen, dass V ein k-Vektorraum ist. Völlig analog zu den Lemmata 3.2.1.7 und 3.2.1.8 erhalten wir das

(3.2.2.5) Lemma.

Es ist $Y \cong SL_2(k)$. Ist k von ungerader Charakteristik, so besitzt Y eine zentrale Involution i mit $C_{M_A}(i) = A$.

3.2.3 Gemeinsame Folgerungen

Für $A \in \Sigma$ ist nun in allen Fällen $V = M_A/Z(M_A)$ ein nicht-ausgearteter symplektischer Raum über dem Körper k. Die isotropen Unterräume sind bekanntlich höchstens von halber Dimension und da die Bilder der abelschen Untergruppen von M_A gerade isotrope Unterräume von V sind, erhalten wir das

(3.2.3.1) Lemma.

Sei M eine abelsche Untergruppe von M_A mit $A \cap M = 1$. Dann gilt $q^s \Big| |M_A : M|$, wobei $s = \frac{dim_k(V)}{2} + 1$ wie in Tabelle 3.4 ist.

Beweis. Die Dimension von V können wir in den Tabellen 3.2 und 3.3 auf den Seiten 30 und 35 ablesen. Im folgenden sei $Z := Z(M_A)$. Ist $M \cap A = 1$, so ist offenbar M eine abelsche Untergruppe von M_A und somit ist MZ/Z ein isotroper Unterraum von V. Ein solcher Unterraum hat höchstens die halbe Dimension von V. Insbesondere ist dann

$$|M_A : MZ| = |M_A/Z : MZ/Z| \geq q^{\frac{dim(V)}{2}}.$$

Dies formen wir um zu

$$|M_A : M| \geq q^{\frac{dim(V)}{2}} \cdot |Z : M \cap Z|.$$

Nach Voraussetzung ist $A(M \cap Z)/(M \cap Z)$ eine Untergruppe der Ordnung q von $Z/(M \cap Z)$. Da M_A eine p-Gruppe ist, folgt somit die Behauptung. □

G	s	$\lvert M_A\rvert$
$A_l(q)$ für $l \geq 2$	l	q^{2l-1}
$B_l(q)$ für q ungerade	$2l-2$	q^{4l-5}
$B_l(q)$ für q gerade und $l > 2$	$2l-3$	q^{4l-5}
$D_l(q)$	$2l-3$	q^{4l-7}
$E_6(q)$	11	q^{21}
$E_7(q)$	17	q^{33}
$E_8(q)$	29	q^{57}
$F_4(q)$, q ungerade	8	q^{15}
$F_4(q)$, q gerade	5	q^{15}
$G_2(q)$, $3 \nmid q$	3	q^5
$G_2(q)$, $3 \mid q$	2	q^5
${}^2E_6(q)$	11	q^{21}
${}^3D_4(q)$	5	q^9
${}^2D_l(q)$	$2l-3$	q^{4l-7}

Tabelle 3.4: Die Ordnung von M_A

3.3 Die unitären und symplektischen Gruppen

Wir ersetzen die Gruppen $PSU_l(k)$ und $PSp_{2n}(k)$ zunächst durch die Gruppen $SU_l(k)$ und $Sp_{2n}(k)$ und betrachten deren übliche Operation auf einem unitären bzw. symplektischen Vektorraum W über $GF(q^2)$ bzw. k als Isometriegruppe bezüglich einer (nicht-ausgearteten) hermiteschen bzw. alternierenden Form β. Genauer sei β eine σ-hermitesche Form für den involutorischen Körperautomorphismus von $GF(q^2)$, wenn W unitär ist und eine symplektische Form, wenn W symplektisch ist. Setzen wir bei den symplektischen Gruppen $2n = l$, so ist l in allen Fällen die Dimension von W. Ist l gerade, so ist W die orthogonale Summe von hyperbolischen Ebenen $W_1, \ldots, W_k$ und, falls W von ungerader Dimension ist, zusätzlich einem eindimensionalen, anisotropen Unterraum W_{k+1}. Ein hyperbolisches Paar von W_i bezeichnen wir mit (v_i, v_{l-i+1}). Ist W von ungerader Dimension, so sei der anisotrope Unterraum von dem normierten Vektor $v_{\frac{l+1}{2}}$ erzeugt. Die Darstellungsmatrizen der unitären Abbildungen schreiben wir in Zeilen bezüglich der Basis $(v_1, \ldots, v_l)$. Die zugehörige Gram'sche Matrix J hat dann die Form

$$\begin{pmatrix} & & & 1 \\ & & \cdot & \\ & \cdot & & \\ \cdot & & & \\ 1 & & & \end{pmatrix} \quad \text{bzw.} \quad \left(\begin{array}{ccc|ccc} & & & & & 1 \\ & & & & \cdot & \\ & & & \cdot & & \\ \hline & & & 1 & & \\ & & -1 & & & \\ \hline & \cdot & & & & \\ \cdot & & & & & \\ -1 & & & & & \end{array}\right). \tag{3.5}$$

Die Darstellungsmatrizen der unitären bzw. symplektischen Abbildungen sind nun die

Matrizen $M \in GL_l(q^2)$ bzw. $GL_l(q)$ mit

$$M^t J M^\sigma = J \quad \text{bzw.} \quad M^t J M = J. \tag{3.6}$$

Bei den symplektischen Gruppen mit $l > 2$ sei stets k von ungerader Charakteristik, da wir diese Gruppen sonst als orthogonale Gruppen auffassen. Sei nun $A \in \Sigma$ und $B \in \Omega_A$. Unser Ziel ist es, die Aussagen des vergangenen Abschnittes auch hier zu erhalten. Die folgenden Argumente finden wir in ähnlicher Form auch in Abschnitt 3 bei Curtis, Kantor & Seitz [11].

Die (Urbilder) von A und B sind o.B.d.A. die zu $(k,+)$ isomorphen Transvektionsgruppen zu den Punkten $\langle v_1 \rangle$ und $\langle v_l \rangle$. Die Matrizen dieser Transvektionen sind von der Form

$$\begin{pmatrix} 1 & & \\ & \ddots & \\ c & & 1 \end{pmatrix} \quad \text{bzw.} \quad \begin{pmatrix} 1 & & c \\ & \ddots & \\ & & 1 \end{pmatrix}$$

mit $c + c^\sigma = 0$ bei den unitären Matrizen und $c \in k$ bei den symplektischen Matrizen. Ist k von ungerader Charakteristik, so liegt die zentrale Involution von $\langle T_{v_1}, T_{v_l} \rangle$ offenbar nicht im Zentrum von $SU_l(q)$ bzw. $Sp_{2n}(q)$. Setzen wir

$$Y := \langle A, B \rangle,$$

so erhalten wir das

(3.3.1) Lemma.

Es ist $Y \cong SL_2(q)$.

Das unipotente Radikal M_A enthält sämtliche Matrizen der Form

$$\left(\begin{array}{c|c|c} 1 & & \\ \hline -a_{l-1}^\sigma & & \\ \vdots & I_{l-2} & \\ -a_2^\sigma & & \\ \hline -a_1^\sigma & a_2 \cdots a_{l-1} & 1 \end{array}\right) \quad \text{bzw.} \quad \left(\begin{array}{c|c|c} 1 & & \\ \hline -a_{l-1} & & \\ \vdots & & \\ -a_{k+1} & I_{l-2} & \\ a_k & & \\ \vdots & & \\ a_2 & & \\ \hline a_1 & a_2 \cdots a_{l-1} & 1 \end{array}\right) \tag{3.7}$$

mit

$$a_1 + a_1^\sigma = \beta(a_2 v_2 + \cdots + a_{l-1} v_{l-1}, a_2 v_2 + \cdots + a_{l-1} v_{l-1})$$

bei den unitären Matrizen. Wir rechnen dazu nach, dass diese Matrizen den Punkt (3.6) erfüllen und einen p-Normalteiler von $N(A)$ der Ordnung q^{2l-3} bzw. q^{l-1} bilden. Die Diagonalgruppe von Y enthält offenbar die Matrizen der Form

$$h(\lambda) := \left(\begin{array}{c|c|c} \lambda & & \\ \hline & I_{l-2} & \\ \hline & & \lambda^{-1} \end{array}\right)$$

für $\lambda \in k$. Für die unitären Matrizen folgt die Bedingung $\lambda \in k$ aus (3.6). Es ist nämlich notwendig $\lambda^{-1}\lambda^\sigma = 1$. Ist

$$m = \left(\begin{array}{c|c|c} 1 & & \\ \hline S & I_{l-2} & \\ \hline c & Z & 1 \end{array}\right) \in M_A,$$

so ist

$$m^{h(\lambda)} = \left(\begin{array}{c|c|c} 1 & & \\ \hline \lambda S & I_{l-2} & \\ \hline \lambda^2 c & \lambda Z & 1 \end{array}\right). \tag{3.8}$$

In ungerader Charakteristik ist $h(-1)$ die zentrale Involution i von Y und aus (3.8) lesen wir direkt ab:

(3.3.2) Folgerung.

Ist k von ungerader Charakteristik, so ist $C_{M_A}(i) = A$.

Für jede Matrix $m \in M_A$ in der Form von (3.7) sei

$$v_m := a_2 v_2 + \cdots + a_{l-1} v_{l-1}.$$

Die Operation von M_A auf W ist dann gegeben durch

$$\begin{aligned} v_1^m &= v_1, \\ v_l^m &= -a_1^\sigma v_1 + v_m + v_l \quad \text{bzw.} \quad v_l^m = a_1 v_1 + v_m + v_l \\ v^m &= v - \beta(v, v_m) v_1, \end{aligned}$$

für alle $v \in W_2 \perp \cdots \perp W_k \perp W_{k+1}$, wo auch stets v_m liegt. Hierbei sei $W_{k+1} = 0$, wenn W von gerader Dimension ist. Durch Nachrechnen sehen wir, dass der Kommutator $[m, n]$ für $n \in M_A$ die folgende Form hat:

$$[m, n] = \begin{pmatrix} 1 & & \\ & \ddots & \\ (v_m, v_n)' & & 1 \end{pmatrix}$$

mit

$$(v_m, v_n)' := \beta(v_n, v_m) - \beta(v_m, v_n).$$

Wir erhalten damit leicht das

(3.3.3) Lemma.

Für $G \neq PSp_4(2^f)$ ist $M_A' = A = Z(M_A)$.

Für $G = PSp_4(2^f)$ ist M_A offenbar elementarabelsch und für die folgenden Argumente schließen wir diese Gruppe aus. Nun ist

$$V := M_A/A = \overline{M}_A$$

eine elementarabelsche Gruppe. (Für $PSU_3(k)$ ist $x^p \in A$ für alle $x \in M_A$.) Definieren wir für $\lambda \in k^*$ und $m \in M_A$ die skalare Multiplikation

$$\lambda \cdot \overline{m} := \overline{m}^{h(\lambda)} \quad \text{und} \quad 0 \cdot \overline{m} = \overline{1}$$

auf V, so erhalten wir durch eine Matrizenrechnung das

(3.3.4) Lemma.

Ist G verschieden von $PSp_4(2^f)$, so ist V mit der oben definierten Skalarmultiplikation ein k-Vektorraum.

Nach (3.8) ist

$$v_{m^{h(\lambda)}} = \lambda v_m$$

für $\lambda \in k^*$ und $m \in M_A$. Nun ist λ invariant unter σ, also folgt insbesondere

$$(v_{m^{h(\lambda)}}, v_n)' = \beta(v_n, \lambda v_m) - \beta(\lambda v_m, v_n) = \lambda(v_m, v_n)'. \tag{3.9}$$

Sei $f : V \times V \longrightarrow k$ mit

$$f(\overline{m}, \overline{n}) = c,$$

wenn $[m, n] = a(c) \in A$. Genau wie in 3.2.1.1 ist nun f eine nicht-ausgeartete symplektische Form, also erhalten wir das

(3.3.5) Lemma.

Ist G verschieden von $PSp_4(2^f)$, so ist V bezüglich der Form f zusammen mit der Skalarmultiplikation aus 3.3.4 ein nicht-ausgearteter symplektischer k-Vektorraum.

Analog zu 3.2.3.1 erhalten wir das

(3.3.6) Lemma.

Sei G verschieden von $PSp_4(2^f)$ und M eine abelsche Untergruppe von M_A mit $A \cap M = 1$. Dann gilt $q^s \Big| |M_A : M|$, wobei $s = \frac{dim_k(V)}{2} + 1$ wie in Tabelle 3.5 ist.

G	s	$\lvert M_A\rvert$
$PSU_l(q)$	$l-1$	q^{2l-3}
$PSp_{2n}(q)$	n	q^{2n-1}

Tabelle 3.5: Die Ordnung von M_A

3.4 Wurzelinvolutionen

Unabhängig von der Charakteristik des der Gruppe G zugrunde liegenden Körpers bezeichnen wir mit D die Menge

$$D := D(\Sigma) = \{a \in A^\sharp \mid A \in \Sigma\}$$

der *langen Wurzelelemente* von G. Ist dieser Körper nun von gerader Charakteristik, so sind die Elemente von D natürlich Involutionen und wir nennen die Elemente aus D die *Wurzelinvolutionen* von G. Für eine Teilmenge Λ von D sei

$$\Lambda^2 := \{de \mid d, e \in \Lambda \text{ und } de = ed \neq 1\}.$$

(3.4.1) Lemma.

Das Produkt zweier Wurzelinvolution a und b erfüllt genau eine der drei Bedingungen

(a) $ab = ba$.

(b) ab hat ungerade Ordnung.

(c) ab hat die Ordnung 4 und $(ab)^2$ ist eine Wurzelinvolution.

Die drei Fälle korrespondieren in entsprechender Weise zu den drei Fällen (a), (b) und (c) von Seite 22.

Beweis. Seien a und b zwei Wurzelinvolutionen mit zugehörigen abstrakten Wurzeluntergruppen A und B. Es ist klar, dass der Fall (b) zu dem Fall (b) von Seite 22 korrespondiert, und dass der Fall (a) von Seite 22 den entsprechenden obigen Fall impliziert. Seien nun a und b vertauschbar. Wäre $A \in \Psi_B$, so wäre die Abbildung $\chi_a : B \longmapsto [a, b]$ für $a \in A^\sharp$ und alle $b \in B$ ein Isomorphismus von B auf $[A, B]$ und dies ist hier nicht der Fall. Insbesondere impliziert der Fall (a) den Fall (a) von Seite 22. Die Behauptung ist nun klar. □

(3.4.2) Lemma.

Sei $k = GF(q)$ mit $q = 2^f$ und $f \geq 2$. Seien $A, B, C \in \Sigma$ mit $A, B \in \Omega_C$ und $A \in \Omega_B$ und sei $K := \langle A, B, C\rangle$. Dann ist $K/O_2(K)$ isomorph zu einer der Gruppen $SL_2(k)$, $(P)SL_3(k)$, $(P)SU_3(k)$ oder einer Untergruppe von $(P)SL_3(q^3)$.

Beweis. Wir nehmen o.B.d.A. $O_2(K) = 1$ an. Sei $D_K = D \cap K$ und $\mathcal{F}(D_K)$ der Graph mit Eckenmenge D_K und Kanten der Form $\{a, b\}$ mit $o(ab)$ ungerade für $a, b \in D_K$. Nach IV (1.6) von TIMMESFELD [34] ist das Erzeugnis der isolierten Ecken ein 2-Normalteiler von K und demnach trivial. Weiterhin vertauschen daher verschiedene Zusammenhangskomponenten von $\mathcal{F}(D_K)$.

Sind a, b, c beliebige Elemente aus $A^\sharp$, $B^\sharp$ und $C^\sharp$, so liegen diese nach Voraussetzung in der selben Zusammenhangskomponente. Gäbe es ein Wurzelelement d in einer weiteren Komponente, dann ist d also mit A, B und C vertauschbar, ein Widerspruch wegen $O_2(K) = 1$. Insbesondere ist $\mathcal{F}(D_K)$ zusammenhängend und wegen $|A| > 2$ ist auch sicherlich $D_K \cap D_K^2 \neq \emptyset$. Nach IV (1.9) von TIMMESFELD [34] ist dann

$$K/Z_*(K) = \overline{K}$$

einfach. Dabei ist $Z_*(K)$ maximales Urbild von $Z(K/O_2(K)) \cong Z(K)$. Offenbar wird $\overline{K}$ von der Klasse von abstrakten Wurzeluntergruppen

$$\Delta := \overline{A}^{\overline{K}}$$

erzeugt. Nach den Klassifikationssätzen aus III §9 von TIMMESFELD [34] ist dann $\overline{K}$ eine Lie-Typ-Gruppe in gerader Charakteristik.

Sei $\overline{K}$ zunächst eine klassische Gruppe und V der zugehörige natürliche Modul. Wegen der Einfachheit von $\overline{K}$ operiert diese Gruppe trivial oder treu auf jedem Unterraum. Ist $\overline{K}$ eine lineare, unitäre oder symplektische Gruppe, so ist Δ eine Klasse von Transvektionsgruppen und die Kommutatoren $[V, \overline{D}]$ für $\overline{D} \in \Delta$ höchstens eindimensional. Somit operiert $\overline{K}$ treu auf dem höchstens dreidimensionalen Unterraum $[V, \overline{K}]$ und K ist die zentrale Erweiterung von $PSL_2(k)$, $PSL_3(k)$ oder $PSU_3(k)$.

Ist $\overline{K}$ eine orthogonale Gruppe, so ist Δ eine Klasse von Siegeltransvektionsgruppen. Die obigen Kommutatoren sind dann höchstens zweidimensional und $\overline{K}$ operiert treu auf dem höchstens sechsdimensionalen Raum $[V, \overline{K}]$. Die einzigen möglichen Gruppen sind $\Omega_6^+(k) \cong PSL_4(k)$ und $\Omega_6^-(k) \cong PSU_4(q)$. Unter diesen Isomorphismen werden die Siegeltransvektionsgruppen jedoch auf Transvektionsgruppen abgebildet und dies ist wie im letzten Absatz nicht möglich.

Es bleiben die Gruppen vom Ausnahmetyp zu untersuchen. Die Gruppe $G_2(k)$ ist enthalten in $D_4(k)$ und die Wurzeluntergruppen von $G_2(k)$ sind Wurzeluntergruppen von $D_4(k)$. Somit tritt dieser Fall nicht ein. Die Gruppe ${}^3D_4(k)$ ist enthalten in $D_4(q^3)$ und jede Wurzeluntergruppe ist offenbar in genau einer Wurzeluntergruppe von $D_4(q^3)$ enthalten. Sind A^*, B^* und C^* die drei zu $\overline{A}$, $\overline{B}$ und $\overline{C}$ gehörenden Wurzeluntergruppen von $D_4(q^3)$, so erfüllen diese offenbar die Voraussetzungen des Lemmas und erzeugen paarweise eine zu $SL_2(q^3)$ isomorphe Untergruppe. Insbesondere ist $\overline{K} \leq SL_2(q^3)$. In den Abschnitten 4-6 von COOPERSTEIN [9] finden wir, dass die Gruppen $F_4(q)$, ${}^2E_6(q)$, $E_6(q)$, $E_7(q)$ und $E_8(q)$ nicht von den drei obigen Wurzeluntergruppen erzeugt werden können. Damit folgt schließlich das Lemma. □

3.5 Zentralisatoren von zentralen Involutionen

Die unipotente und monomiale Gruppe von G tragen hier die Bezeichnung U und N, unabhängig davon, ob G eine Chevalleygruppe oder eine getwistete Gruppe ist. In diesem Abschnitt sei k stets von ungerader Charakteristik, G verschieden von $PSL_2(k)$ und es sei daran erinnert, dass G nach Festlegung verschieden von $R(k)$ ist. Wir untersuchen hier den Zentralisator der zentralen Involution i von

$$Y := \langle A, B \rangle$$

mit $A, B \in \Sigma$ und $B \in \Omega_A$.

(3.5.1) Lemma.

Ist A die abstrakte Wurzeluntergruppe zur höchsten Wurzeluntergruppe A_h und B die zu A_{-h}, so gilt $C(i) = \langle C_U(i), C_N(i) \rangle$.

Beweis. Durch die Bruhat-Zerlegung läßt sich jedes Element $x \in G$ eindeutig in der Form $x = uhwu'$ darstellen, wobei $u \in U$, $h \in H$, $w \in W$ und $u' \in U_w^-$. Vertauschen nun i und x, so liefert die Konjugation mit i, dass

$$u^i h^i w^i u'^i = uhwu'.$$

Offenbar ist $i \in H$ und die Gruppen U, U_w^- und N sind H-invariant, also liefert die Eindeutigkeit der Bruhat-Zerlegung die Behauptung. □

(3.5.2) Lemma.

Die Konjugierten von Y unter $C(i)$ sind Normalteiler von $L_A Y$.

Beweis. Sei A o.B.d.A. die abstrakte Wurzeluntergruppe zur höchsten Wurzeluntergruppe A_h und B die zu A_{-h}. Die Gruppe U ist das Produkt der positiven Wurzeluntergruppen, also ist sicherlich $M_A \leq U \leq M_A L_A$ und daher nach der Dedekindidentität

$$U = M_A(U \cap L_A).$$

In den vorangegangenen Abschnitten haben wir gesehen, dass $C_{M_A}(i) = A$. Nun vertauscht L_A mit Y, also ist

$$C_U(i) = (U \cap L_A)A.$$

Die Involution w_0 maximaler Länge in W vertauscht jede positive mit ihrer negativen Wurzel, also ist L_A invariant unter Konjugation mit w_0 und es folgt

$$C_{U^{w_0}}(i) = (U^{w_0} \cap L_A)B.$$

Insbesondere ist dann

$$\langle C_U(i), C_{U^{w_0}}(i)\rangle \leq L_A Y.$$

Da U das Produkt der positiven Wurzeluntergruppen ist, erhalten wir damit

$$\langle C_{A_r}(i) \mid r \in \Phi\rangle \leq L_A Y.$$

Die umgekehrte Inklusion ist ebenfalls richtig, denn L_A vertauscht mit Y und es ist $A \leq Z_{M_A}$. Es gilt also stets

$$L_A Y = \langle C_{A_r}(i) \mid r \in \Phi\rangle.$$

Insbesondere wird $L_A Y$ von $C_N(i)$ normalisiert. Für $n \in C_N(i)$ ist also Y^n genau wie Y ein Normalteiler von $L_A Y$. Da $C_U(i) \leq L_A Y$, folgt mit 3.5.1 die Behauptung. □

3.6 Ein nützliches Lemma

In diesem letzten Abschnitt stellen wir noch ein von den Lie-Typ-Gruppen völlig unabhängiges Lemma vor.

(3.6.1) Lemma.

Sei $R = \langle x\rangle O_2(R)$ eine Gruppe mit $o(x) = 3$, $O_2(R) \neq 1$ und $R = \langle x^R\rangle$. Gilt zusätzlich für alle nicht mit x vertauschbaren $r \in R$:

(i) $\langle x, x^r\rangle \cong SL_2(3)$,

(ii) $C_{O_2(R)}(i_r) \leq N(\langle x, x^r\rangle)$, wobei i_r die zentrale Involution von $\langle x, x^r\rangle$ ist,

dann ist $R \cong SL_2(3)$.

Beweis. Sei R ein minimales Gegenbeispiel und $N := O_2(R)$ die offenbar einzige 2-Sylowgruppe von R. Insbesondere ist jede 2-Untergruppe von R in N enthalten. Wegen $O_2(R) \neq 1$, gibt es ein $r \in R$ mit

$$X_0 := \langle x, x^r\rangle \cong SL_2(3).$$

Ferner bezeichne Q die zu Q_8 isomorphe Untergruppe $O_2(X_0)$ und i die zentrale Involution von X_0. Offensichtlich ist $N \cap X_0 = Q$.

Nehmen wir an, dass $Q \trianglelefteq N$, so ist wegen $R = \langle x\rangle N$ auch $Q \trianglelefteq R$. Natürlich ist i die einzige Involution in Q, also sehen wir mit (ii), dass

$$N \leq C_N(i) \leq N(X_0)$$

und daher

$$[N, X_0] \leq N \cap X_0 = Q.$$

Ist nun $\overline{\ }$ der natürliche Homomorphismus von R auf R/Q, so vertauschen $\overline{N}$ und $\langle\overline{x}\rangle$. Demnach ist

$$\overline{R} = \langle\overline{x}^{\overline{R}}\rangle = \langle\overline{x}^{\overline{N}}\rangle = \langle\overline{x}\rangle,$$

und daher $N = Q$. Dann aber ist $X_0 = R$, ein Widerspruch.

Insbesondere ist dann

$$Q \lhd N_N(Q) < N.$$

Setzen wir $Q_1 := N_N(Q)$, so ist

$$\langle x^{N_N(Q_1)}\rangle \leq R = \langle x\rangle N.$$

Aus der Dedekindidentität folgt somit

$$\langle x^{N_N(Q_1)}\rangle = \langle x\rangle(\langle x^{N_N(Q_1)}\rangle \cap O_2(R)) = \langle x\rangle O_2(\langle x^{N_N(Q_1)}\rangle).$$

Daher erfüllt $\langle x^{N_N(Q_1)}\rangle$ offenbar die Voraussetzungen des Lemmas, wenn

$$\langle x^{N_N(Q_1)}\rangle \leq \langle x^{O_2(\langle x^{N_N(Q_1)}\rangle)}\rangle.$$

Da x auf der $3'$-Gruppe $N_N(Q_1)$ operiert, ist

$$N_N(Q_1) = C_{N_N(Q_1)}(x)[N_N(Q_1), x]$$

nach VII (7.12) von Kurzweil [24]. Da nun

$$[N_N(Q_1), x] \leq N \cap \langle x^{N_N(Q_1)}\rangle = O_2(\langle x^{N_N(Q_1)}\rangle),$$

ist die obige Forderung offenbar erfüllt.

Angenommen $N_N(Q_1) < N$. Dann ist

$$\langle x^{N_N(Q_1)}\rangle < \langle x\rangle N = R.$$

Da R ein minimales Gegenbeispiel war, folgt nun leicht

$$SL_2(3) \cong X_0 = \langle x^{N_N(Q_1)}\rangle$$

und damit

$$N_N(Q_1) \leq C_N(i) \leq N_N(X_0) \leq Q_1.$$

Da jedoch N und Q_1 nilpotent sind, kann Q_1 nicht sein eigener Normalisator sein. Insbesondere ist nun

$$N_N(Q_1) = N$$

Somit enthält Q_1 sämtliche Konjugierten von Q unter N, und da $Q_1 \leq C_N(i)$ ist dann nach (ii) auch

$$[Q^n, X_0] \leq N \cap X_0 = Q$$

für alle $n \in N$. Wegen $Q_1 < N$ finden wir ein $n \in N$ mit

$$Q^n \neq Q.$$

Setzen wir in die obige Ungleichung n^{-1} ein und konjugieren dies mit n, so folgt

$$[Q, X_0^n] \leq Q^n. \tag{3.10}$$

Insbesondere sind x und n nicht vertauschbar, denn mit Matrizen rechnen wir in $SL_2(3)$ leicht nach, dass

$$[Q, \langle x \rangle] = Q.$$

Folglich operiert $Y := \langle x, x^n \rangle$ auf QQ^n und insbesondere ist dann

$$Y \leq N(Z(QQ^n)).$$

Dabei ist $i \neq i^n$, denn andernfalls ist $n \in C_N(i) \leq N(X_0) \leq N(Q)$, ein Widerspruch. Somit können sich Q und Q^n nur trivial schneiden, denn sonst enthält $Q \cap Q^n$ in jedem Fall die zentrale Involution i von Q. Daher ist

$$Z(QQ^n) = Z(Q) \times Z(Q^n) = \langle i, i^n \rangle$$

und es ist klar, dass $\langle i, i^n \rangle \cong V_4$.
Als Folgerung erhalten wir nun, dass $Y/C_Y(\langle i, i^n \rangle)$ eine Untergruppe von $Aut(V_4) = \Sigma_3$ ist. Da diese jedoch keinen 2-Normalteiler hat, ist dann

$$\begin{aligned} O_2(Y) &\leq C_Y(\langle i, i^n \rangle) \leq C_N(\langle i, i^n \rangle) = C_N(i) \cap C_N(i^n) \\ &\leq N(X_0) \cap N(X_0^n) \leq N(Q) \cap N(Q^n). \end{aligned}$$

Da die 3-Sylowgruppen von Y in $O_2(Y)$ konjugiert sind, gibt es ein $m \in O_2(Y)$ mit

$$\langle x^n \rangle = \langle x \rangle^m.$$

Wegen $[Q, \langle x \rangle] = Q$ liefert Konjugation mit m und (3.10), dass auch

$$Q = Q^m = [Q, \langle x \rangle]^m = [Q, \langle x^n \rangle] \leq Q^n,$$

und dies ist ein Widerspruch. □

Kapitel 4

Zweifach transitive Permutationsgruppen

Die endlichen einfachen Gruppen aus der Liste der Klassifikation der endlichen einfachen Gruppen bezeichnen wir als die *bekannten* endlichen, einfachen Gruppen. Jede solche Gruppe ist dann isomorph zu einer zyklischen Gruppe von Primzahlordnung, einer alternierenden Gruppen, einer Lie-Typ-Gruppe oder einer sporadischen Gruppe.

(4.1) Hauptsatz.

Sei G_0 eine bekannte endliche, einfache Gruppe und G eine zweifach transitive Permutationsgruppe auf der Menge Ω mit $G_0 \leq G \leq Aut(G_0)$. Operiert $F(G_\alpha)$ transitiv auf $\Omega \setminus \{\alpha\}$, dann ist $F(G_\alpha)$ eine auf $\Omega \setminus \{\alpha\}$ reguläre p-Gruppe. Die Gruppe G_0 ist wie in Tabelle 4.1 und bis auf den Fall (f) mit $m = 28$ ist stets $F(G_\alpha) \leq G_0$ und G_0 zweifach transitiv auf Ω.

Der Beweis dieses Satzes ist recht umfangreich, weswegen ihn auf mehrere Kapitel verteilen. In diesem Kapitel werden wir nur noch einige Bezeichnungen festlegen und einige leichte Tatsachen festhalten. Offenbar kann G_0 niemals eine zyklische Gruppe sein. Ist G_0 eine alternierende Gruppe, so benutzen wir elementare Argumente von Maillet [25], um die Beispiele aus dem obigen Satz zu erhalten. Für die sporadischen Gruppen G_0 zitieren wir geeignete Literatur. Für die Gruppen G_0 vom Lie-Typ existiert bereits ein Beweis dieser Aussage unter der schwächeren Voraussetzung, dass G_α keinen auf $\Omega \setminus \{\alpha\}$ transitiven nilpotenten Normalteiler haben muss. Wir finden diese Aussage bei Curtis, Kantor & Seitz [11]. Allerdings ist der Beweis dieser Aussage in weiten Teilen von charaktertheoretischen Argumenten geprägt, und daher nur schwer zugänglich. Unser Beweis wird (weitestgehend) frei von diesen Argumenten bleiben und sich größtenteils der Theorie der abstrakten Wurzeluntergruppen bedienen. Manchmal müssen wir Listen maximaler Untergruppen von den Lie-Typ-Gruppen zitieren, welche keine Klasse von abstrakten Wurzeluntergruppen besitzen. Diese bedienen sich teilweise charaktertheoretischen Argumenten.

4.1 Notation

Die meisten Bezeichnungen übernehmen wir aus den vorangegangenen Kapiteln. Die Gruppen G und G_0 seien wie im Hauptsatz 4.1. Zusätzlich wählen wir ein Element

	G_0	G	$\lvert\Omega\rvert$
(a)	$PSL_2(q)$		$q+1$
(b)	$PSU_3(q)$		q^3+1
(c)	$Sz(q)$		q^2+1
(d)	$R'(q)$	$R(3)$ für $q=3$	q^3+1
(e)	$PSL_2(5) \cong PSL_2(4) \cong A_5$	G_0 oder $PGL_2(5) \cong P\Gamma L_2(4) \cong \Sigma_5$	5 oder 6
(f)	$R(3)' \cong PSL_2(8)$	$R(3) \cong P\Gamma L_2(8)$ (oder G_0 mit $m=9$)	9 oder 28
(g)	$PSL_3(2) \cong PSL_2(7)$	G_0 oder $Aut(PSL_3(2)) \cong PGL_2(7)$	8
(h)	$PSL_2(9) \cong Sp_4(2)' \cong A_6$	$G_0 \leq G \leq Aut(A_6) \cong P\Gamma L_2(9)$	10
(i)	$G_2(2)' \cong PSU_3(3)$	G_0 oder $G_2(2) \cong P\Gamma U_3(3)$	28

Tabelle 4.1: Die Gruppen G_0

$\alpha \in \Omega$ und legen folgende Notation fest:

$$\begin{aligned} \Omega^* &:= \Omega \setminus \{\alpha\}, \\ m &:= |\Omega|, \\ X &:= F(G_\alpha). \end{aligned}$$

Ist G_0 eine Lie-Typ-Gruppe, so sei zusätzlich

$$\begin{aligned} k &:= GF(q), \\ p &:= char(k), \\ p^f &:= q. \end{aligned}$$

4.2 Vorbereitende Aussagen

Ein häufig verwendetes Argument wird sein, dass X seinen Zentralisator enthält. Wir sagen dazu abkürzend, dass X *selbstzentralisierend* ist, obwohl X nicht notwendig abelsch ist. Ist $X = F^*(G_\alpha)$, so erfüllt X offenbar diese Eigenschaft. Dazu zeigen wir das folgende allgemeine Lemma, in dem $E(T)$ das Erzeugnis der quasieinfachen Subnormalteiler einer Gruppe T bezeichne.

(4.2.1) Lemma.

Sei Ω eine Menge mit $|\Omega| > 1$ und T eine endliche Permutationsgruppe auf Ω. Besitzt T einen auf Ω transitiven nilpotenten Normalteiler N mit $T = NE(T)$, so ist $N = T$.

Beweis. Angenommen $N < T$. Dann hat T insbesondere nichttriviale Komponenten. Da diese Komponenten quasieinfach sind, ist keine von ihnen in N enthalten und vertauschen daher mit N. Natürlich vertauscht dann N mit $E(T)$, und aus der Transitivität von N auf Ω folgt dann

$$E(T) \cap T_\alpha \leq \bigcap_{n \in N} T_\alpha^n = 1$$

für alle $\alpha \in \Omega$. Insbesondere ist T_α nilpotent, denn nun ist

$$T_\alpha \cong T_\alpha E(T)/E(T) \leq T/E(T) \cong N/N \cap E(T).$$

Nach dem Frattiniargument ist $T = T_\alpha N$. Da mit T_α auch jede Faktorgruppe nilpotent ist, ist auch

$$T_\alpha/(N \cap T_\alpha) \cong T_\alpha N/N = E(T)N/N \cong E(T)/(N \cap E(T))$$

nilpotent und daher auch auflösbar. Dies jedoch ist ein Widerspruch, denn $N \cap E(T)$ enthält keine Komponenten. □

Nun ist $F^*(G_\alpha) = XE(G_\alpha)$, und daher erhalten wir sofort die

(4.2.2) Folgerung.

Es ist $X = F^*(G_\alpha)$.

(4.2.3) Lemma.

Die Primteiler von $|X|$ *sind auch Teiler von* $m - 1$.

Beweis. Die Gruppe X ist das direkte Produkt ihrer r-Sylowgruppen. Insbesondere wird jede dieser r-Sylowgruppen X_r von X normalisiert. Folglich ist auch die Menge der Fixpunkte von X_r auf Ω invariant unter X. Da nun X transitiv auf Ω^* operiert, ist α notwendig der einzige Fixpunkt von X_r auf Ω. Zerlegen wir Ω^* in disjunkte Bahnen unter der Operation von X_r, so teilt r jede Bahnenlänge und es folgt das Lemma. □

(4.2.4) Lemma.

G_0 *operiert transitiv auf* Ω *und* $(G_0)_\alpha$ *ist eine maximale Untergruppe von* G_0.

Beweis. Als Normalteiler einer zweifach transitiven Gruppe operiert G_0 natürlich transitiv auf Ω. Die regulären Normalteiler von zweifach transitiven Permutationsgruppen sind elementarabelsch. Dies sehen wir beispielsweise in II (11.3) bei WIELANDT [40], und insbesondere operiert G_0 nicht regulär, denn G_0 ist offenbar nicht zyklisch.

Die nichtregulären, imprimitiven Normalteiler einer zweifach transitiven Permutationsgruppe sind nun aber nach II (12.3) von WIELANDT [40] gerade Frobeniusgruppen. Sicherlich ist G_0 als einfache Gruppe keine Frobeniusgruppe, denn diese normalisieren einen nichttrivialen Frobeniuskern. Daher ist G_0 primitiv auf Ω und es folgt die Behauptung. □

Kapitel 5

Zyklische, alternierende und sporadische Gruppen

In diesem Kapitel verwenden wir die Ergebnisse und Bezeichnungen aus dem vorangegangenen Kapitel. Wir befassen uns hier mit den Gruppen G, die die Voraussetzungen zu Hauptsatz 4.1 erfüllen und bei denen G_0 eine zyklische, alternierende oder sporadische Gruppe ist. Es ist dabei klar, dass G_0 niemals eine zyklische Gruppe ist.

Es gibt genau zehn Beispiele für zweifach transitive Gruppen G, bei denen G_0 eine sporadische Gruppe ist. Es sind die Gruppen M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, HS und Co_3 mit entsprechenden Permutationsgraden. Es übersteigt das Maß dieser Arbeit, hierfür eine Klassifikation vorzunehmen, weswegen wir uns auf die Angabe von geeigneter Literatur beschränken. Wir finden die obige Informationen in Tabelle (7.4) bei Cameron [5] oder bei Mortimer & Dixon [29] in Abschnitt 7.7 von Kapitel 7. Die Fittinguntergruppen der maximalen Punktstabilisatoren operieren nicht transitiv auf $m-1$ Ziffern und somit erfüllt keine der sporadischen Gruppen den Hauptsatz 4.1.

Die sämtlichen zweifach transitiven Darstellungen der symmetrischen und alternierenden Gruppen wurden um 1895 von Maillet [25] bestimmt. Die Originalarbeit von Maillet ist nicht gut lesbar, so dass wir seine Argumente weitestgehend ausführen. Durch die Existenz des nilpotenten Normalteilers X in G_α vereinfachen sich die Argumente etwas.

5.1 Alternierende Gruppen

Sei G_0 eine alternierende Gruppe A_n. Bis auf die Ausnahme $n = 6$ ist G stets eine der Gruppen A_n oder Σ_n und im Fall $n = 6$ besteht noch die Möglichkeit $G \cong \Sigma_6 : 2$.

(5.1.1) Lemma.

Ist $n \leq 6$, so ist G wie in (e) oder (h) von Hauptsatz 4.1.

Beweis. Sei zuerst $G = A_5$ oder Σ_5. Enthält X eine 3- oder 5-Sylowgruppe von G, so ist G_α wegen der Nilpotenz von X der Normalisator einer solchen und m ist die Anzahl der 3- oder 5-Sylowgruppen von G. Insbesondere ist $m = 10$ oder 6, wobei $m - 1$ im ersten Fall kein Teiler von $|G|$ ist. Wir erhalten damit den Punkt (e) aus 4.1 mit $m = 6$. Ist X nun eine 2-Gruppe, so ist m wegen der Transitivität von X auf Ω^* eine der Zahlen $2^i + 1$ mit $i \leq 3$. Für $i = 1$ enthält G_α notwendig genau eine

5-Sylowgruppe und $X = F(G_\alpha)$ hat dann einen 5-Anteil, ein Widerspruch. Der Fall $i = 3$ impliziert den Widerspruch $3^2 \mid |G|$, also ergibt sich schließlich (e) aus 4.1 mit $m = 5$.

Ist nun $G_0 = A_6$, dann enthält X wie oben keine 5-Untergruppe. Enthält X eine 3-Untergruppe, dann ist $m - 1 = 3^i 2^j$ mit $i \leq 2$ und $0 \leq j \leq 5$. Durch leichtes Nachrechnen ergibt sich für $j \geq 1$ stets $m \nmid |G|$, also ist $m = 4$ oder 10. Der Normalisator einer Untergruppe der Ordnung drei hat nicht den Index vier in G und somit erhalten wir den Fall (h) aus 4.1. Ist X eine 2-Gruppe, so ist m eine der Zahlen $2^i + 1$ mit $i \leq 5$. Die Fälle $i = 4, 5$ führen auf $m \nmid |G|$ und im Fall $i = 3$ enthält G_α wie oben genau eine 5-Sylowgruppe. Schließlich ist $i \neq 1, 2$, denn A_6 hat keine maximalen Untergruppen vom Index 3 oder 5. □

Wir haben dieses Resultat alleine aus der Betrachtung der Operation von G auf Ω erhalten. Für den offenen Fall $n > 6$ ist G stets eine der Gruppen Σ_n oder A_n und wir benutzen hier die treue Operation von G auf der Menge

$$N := \{1, \ldots, n\}.$$

Im weiteren Verlauf sei $n > 6$ und C die Konjugiertenklasse der 2-Zykel bzw. 3-Zykel, wenn $G = \Sigma_n$ bzw. A_n ist. Wir erhalten dann das folgende

(5.1.2) Lemma.

Es ist $\Omega = \alpha^C \cup \{\alpha\}$. Operiert G_α primitiv auf N, so ist $m - 1 \mid |C|$.

Beweis. Da G von C erzeugt wird, gibt es ein $c \in C$ mit $\alpha^c \neq \alpha$. Ist $\beta \in \Omega^*$ mit $\alpha^c \neq \beta$, so gibt es wegen der zweifachen Transitivität von G auf Ω ein $g \in G$ mit $(\alpha, \alpha^c)^g = (\alpha, \beta)$. Es folgt dann $\alpha^{c^g} = \beta$ und damit der erste Teil der Aussage.

Offenbar operiert G_α durch Konjugation transitiv auf der Menge

$$\{C \cap G_\alpha x \mid x \notin G_\alpha\}$$

und insbesondere sind die Mengen $C \cap G_\alpha x$ für alle $x \notin G_\alpha$ gleichmächtig von der Ordnung d. Operiert nun G_α primitiv auf den Ziffern N, so ist $G_\alpha \cap C = \emptyset$. Enthält nämlich eine primitive Untergruppe von Σ einen 2- bzw. 3-Zykel, so enthält diese nach (3.3A) von Mortimer & Dixon [29] die Gruppe A_n oder Σ_n. Somit folgt $|C| = d(|G : G_\alpha| - 1)$ und damit das Lemma. □

Aus der Operation von G auf Ω erhalten wir nun eine obere Schranke für den Index $|G : G_\alpha|$. Zusätzliche Information erhalten wir aus der Operation von G_α auf N, welche eine der drei folgenden Fälle erfüllt:

- G_α operiert primitiv auf N.
- G_α operiert transitiv und nicht primitiv auf N.

- G_α operiert nicht transitiv auf N.

In jedem der drei Fälle erhalten wir Abschätzungen von $|G : G_\alpha|$ nach unten, die bis auf Ausnahmen der oberen Schranke aus 5.1.2 widersprechen.

(5.1.3) Satz.

Für $n > 6$ ist G keine symmetrische Gruppe.

Beweis. Angenommen die Aussage ist falsch. Sei zuerst G_α primitiv auf N. Wir finden dann in (14.2) bei WIELANDT [40] die Abschätzung

$$m = |G : G_\alpha| \geq [\frac{n+1}{2}]!$$

von BOCHERT. Gleichzeitig gibt es nach 5.1.2 ein $d \in \mathbb{N}$ mit

$$m = 1 + \frac{|C|}{d} = 1 + \frac{1}{d}\binom{n}{2}$$

und daher

$$1 + \frac{1}{d}\binom{n}{2} \geq [\frac{n+1}{2}]!.$$

Für $n \neq 8$ ist dies ein Widerspruch und der Fall $n = 8$ ist nur für $d = 1$ möglich. Dies führt auf $m = 29$, aber $29 \nmid |G|$.

Sei nun G_α transitiv und nicht primitiv auf N. Dann enthält N einen Block Δ der Ordnung $2 \leq k \leq n-1$ für G_α. Wegen seiner Maximalität ist G_α notwendig der Stabilisator der Partition $\{\Delta^g \mid g \in G_\alpha\}$ von N und hat somit die Ordnung $k!l!$ mit $n = kl$. Mit 5.1.2 folgt

$$\frac{n!}{k!\ l!} \leq 1 + |C| \leq 1 + \binom{n}{2}.$$

Nun ist $n = kl \geq k + l$ und damit $l \leq n - k$. Aus der obigen Ungleichung wird daher

$$\binom{n}{k} \leq 1 + \binom{n}{2},$$

wobei sich hier natürlich k durch l ersetzen läßt. Dies ist für $k \geq 3$ nicht möglich. Für $k = 2$ ist $l \geq 4$ und dies ergibt ebenfalls einen Widerspruch.

Sei schließlich G_α nicht transitiv auf N. Dann hat G_α auf N eine Bahn Δ der Länge $2 \leq k \leq n-1$ und wegen der Maximalität von G_α ist dann notwendig

$$G_\alpha = Stab(\Delta) = \Sigma_k \times \Sigma_{n-k}.$$

Für $k \leq n - 2$ ist nach 5.1.2 insbesondere

$$\binom{n}{k} = |G : G_\alpha| \leq 1 + |\alpha^C| \leq 1 + \binom{n}{2} - \binom{n-k}{2} - \binom{k}{2}.$$

	$1+\frac{1}{3}n(n-1)(n-2)$	$1+\frac{1}{6}n(n-1)(n-2)$	$[\frac{n+1}{2}]!$
$n=7$	71	36	24
$n=8$	113	$3\cdot 19$	24
$n=9$	13^2	85	120
$n=10$	241	11^2	120

Tabelle 5.1: Konkrete Abschätzungen

Da die Fälle $k=2$ und $n-2$ offenbar äquivalent sind, ist dies für $k \leq n-2$ ein Widerspruch. Für $k=n-1$ ist schließlich $G_\alpha = \Sigma_{n-1}$ mit trivialer Fittinguntergruppe. Dies ist nach unserer Voraussetzung jedoch nicht möglich. □

(5.1.4) Satz.

Für $n>6$ ist G keine alternierend Gruppe.

Beweis. Angenommen die Aussage ist falsch. Sei zuerst G_α primitiv auf N. Dann liefert die Abschätzung von Bochert diesmal

$$m = |G : G_\alpha| \geq \frac{1}{2}[\frac{n+1}{2}]!.$$

Nach 5.1.2 gibt es dann wie eben ein $d \in \mathbb{N}$ mit

$$1+\frac{n(n-1)(n-2)}{3d} = 1+\frac{2}{d}\binom{n}{3} = m \geq [\frac{n+1}{2}]!.$$

Dies liefert für $n \geq 11$ sofort einen Widerspruch und für $d \geq 3$ ergibt sich sogar stets ein Widerspruch. Die Permutationsgrade in den übrigen Fällen sind in Tabelle 5.1 aufgeführt. Bis auf den Fall $n=7$ mit $d=2$ sind diese Grade kein Teiler der Ordnung von G. Im übrigen Fall ist offenbar G_α der Normalisator einer 5-Sylowgruppe und einer 7-Sylowgruppe, denn $m-1 \mid |X|$. Dies führt leicht zum Widerspruch.

Sei nun G_α transitiv und nicht primitiv auf N. Dann enthält N einen Block Δ der Ordnung $2 \leq k \leq n-2$ für G_α. Da G_α transitiv auf N operiert ist, ist G_α wegen seiner Maximalität der Stabilisator der Partition $\mathcal{P} = \{\Delta^g \mid g \in G_\alpha\}$ von N, also

$$G_\alpha = Stab_{\Sigma_n}(\mathcal{P}) \cap A_n.$$

Wegen $\Sigma_n = A_n \cdot Stab_{\Sigma_n}(\mathcal{P})$ folgt leicht

$$m = |G : G_\alpha| = \frac{n!}{k!l!}$$

für $n = kl > 6$. Sicher enthält C ein Element in G_α, also ist in 5.1.2 sogar $m \leq |C|$ und somit ist wie im letzten Satz

$$\binom{n}{k} \leq \frac{n!}{k!l!} \leq 2\binom{n}{3}.$$

Für $n \geq 11$ und $n-5 \geq k \geq 5$ ist dies wegen

$$2\binom{n}{3} \leq \binom{n}{4}$$

ein Widerspruch. Für alle übrigen Fälle führen wir die Ungleichung

$$\frac{n!}{k!l!} \leq 2\binom{n}{3}$$

durch leichte Rechnung zum Widerspruch, wenn wir $n = kl \geq k + l$ benutzen.

Sei schließlich G_α nicht transitiv auf N und Δ eine Bahn der Länge $2 \leq k \leq n-1$. Dann ist notwendig

$$G_\alpha = Stab(\Delta) = (\Sigma_k \times \Sigma_{n-k}) \cap A_n,$$

und wegen $\Sigma_n = (\Sigma_k \times \Sigma_{n-k})A_n$ folgt leicht

$$|G : G_\alpha| = \binom{n}{k}.$$

Wie im vorangegangenen Satz ergibt sich

$$\binom{n}{k} \leq 1 + 2\binom{n}{3}.$$

Dies liefert wie oben einen Widerspruch für $n \geq 11$ und $n-5 \geq k \geq 5$. In allen übrigen Fällen ist X zu klein, um transitiv auf Ω^* zu operieren. □

Kapitel 6

Lie-Typ-Gruppen

Im Anschluß an das vorangegangene Kapitel bleiben die Gruppen G aus dem Hauptsatz 4.1 zu betrachten, bei denen G_0 eine einfache Lie-Typ-Gruppe ist. Auch in diesem Kapitel verwenden wir die Ergebnisse und Festlegungen aus Kapitel 4. Im Vergleich zu dem letzten Kapitel ist dies der kompliziertere Teil des Beweises von 4.1. Wir spalten ihn in zwei Fälle auf, wobei der erste Fall – in dem X eine p-Sylowgruppe besitzt– auf die natürlichen Darstellungen der Gruppen vom Lie-Rang 1 führen wird. In der Tabelle A.2 von Anhang A sehen wir einige Gruppen vom Lie-Rang 1, die isomorph zu Lie-Typ-Gruppen in von p verschiedener Charakteristik sind. Hier werden wir die übrigen Fälle von 4.1 finden, wenn wir X als p'-Gruppe betrachten. Das genaue Vorgehen beschreiben wir in den entsprechenden Abschnitten.

6.1 Die natürlichen Darstellungen

Sei p *ein Primteiler von* $|X|$. Insbesondere ist G_α eine p-lokale Untergruppe von G. Nach Lemma 4.2.3 sind p und m teilerfremd und somit enthält $(G_0)_\alpha$ nach der Bahnformel den gesamten p-Anteil von G_0. Sei (B_0, N_0) das übliche BN-Paar von G_0 mit unipotenter Untergruppe U_0, Weylgruppe W_0 und $H_0 = B_0 \cap N_0$.

Enthält eine maximale Untergruppe von G_0 die Gruppe U_0, so ist sie nach (1.6) von Seitz [31] eine maximalparabolische Untergruppe von G_0 und daher können wir $(G_0)_\alpha$ o.B.d.A. als standardmaximalparabolische Untergruppe betrachten, die wir im folgenden mit P_J bezeichnen.

Als nilpotenter Normalteiler von P_J ist $X \cap G_0$ nach (47.5) von Aschbacher [2] im unipotenten Radikal U_J von P_J enthalten. Natürlich ist U_J charakteristisch in $(G_0)_\alpha$, also ist $U_J = X \cap G_0$. Es folgt

$$X/U_J \cong XG_0/G_0 \leq Out(G_0),$$

und daher auch

$$m - 1 \Big| \; |U_J| \cdot |Out(G_0)|. \tag{6.1}$$

Im weiteren Verlauf sei M das Erzeugnis der inneren, Körper- und Diagonalautomorphismen von G_0. Dann gilt

(6.1.1) Lemma.

Es ist $G \leq M$.

G_0	$I \setminus J$	m
$A_{2l-1}(q)$, $l \geq 2$	$\{l\}$	$\frac{\prod_{i=l+1}^{2l}(q^i-1)}{\prod_{i=1}^{l}(q^i-1)}$
$D_l(q)$, $l \geq 5$	$\{j\}$, $2 \leq j \leq l-3$	$\frac{(q^l-1)(q^{l-j}+1)\prod_{i=l-j+1}^{l-1}(q^{2i}-1)}{\prod_{i=1}^{j}(q^i-1)}$
$D_l(q)$	$\{1\}$ oder $\{3\}$, $\{4\}$ für $l=4$	$(q^{l-1}+1)\sum_{i=0}^{l-1} q^i$
$D_l(q)$	$\{l-2\}$	$\frac{(q^l-1)(q^{2(l-1)}-1)\prod_{i=1}^{l-2}(q^i+1)}{(q^2-1)^2}$
$E_6(q)$	$\{2\}$	$(q^4+1)(q^6+1)(q^3+1)\sum_{i=0}^{8} q^i$
$E_6(q)$	$\{4\}$	$\frac{(q^2+1)(q^3+1)^2(q^4+1)(q^5-1)(q^6+1)(q^9-1)}{(q^2-1)(q-1)}$

Tabelle 6.1: Die Ordnungen von Ω

Beweis. Angenommen $G \not\leq M$. Wegen $G_0 \leq G$ gibt es dann ein Element $g \in G$, welches das Produkt eines Diagonal- und Körperautomorphismus mit einem Diagrammautomorphismus σ ist. Die Diagonal- und Körperautomorphismen normalisieren die Wurzeluntergruppen von G_0, also ist insbesondere

$$P_J^g = P_J^\sigma$$

ebenfalls eine standardparabolische Untergruppe von G_0. Wir zeigen, dass P_J dann von σ normalisiert wird, was die Möglichkeiten für G_0 und P_J stark einschränkt. Die Operationen von G_0 auf Ω und den Nebenklassen von P_J sind äquivalent, also ist dann m bekannt und wir erhalten dann leicht einen Widerspruch.

Die Konjugierten von B_0 in G sind auch unter G_0 konjugiert, so dass wir aus dem Frattiniargument

$$G = G_0 N_G(B_0)$$

erhalten. Insbesondere ist

$$P_J^\sigma = P_J^{xy}$$

mit $x \in N_G(B_0)$ und $y \in G_0$. Da G_α maximal in G ist, gilt offensichtlich

$$G = G_0 G_\alpha = G_0 N_G(P_J).$$

Insbesondere gibt es dann aber ein $a \in N_G(P_J)$ und $b \in G_0$ mit $x = ab$. Es folgt

$$B_0 = B_0^x = B_0^{ab} \leq P_J^{ab} = P_J^b$$

und nach (43.7) von Aschbacher [2] ist daher $b \in P_J$. Insgesamt ist auch $x \in N_G(P_J)$, und $P_J^\sigma = P_J^y$. Daher sind P_J und P_J^σ in G_0 konjugiert und nach (43.7) bei Aschbacher [2] ist daher $P_J^\sigma = P_J$.

Die Inspektion der Dynkindiagramme schränkt die Möglichkeiten für G_0 und P_J auf die Fälle aus Tabelle 6.1 ein. Ist L_J das Levikomplement von P_J, so ist $|P_J| = |U_J L_J| \cdot |H_0 : H_0 \cap L_J|$. Da stets $|G_0 : P_J| \equiv 1 \mod q$, erhalten wir leicht die Einträge m aus Tabelle 6.1. Benutzen wir nun (6.1), so ergibt sich mit C.1 aus dem Anhang C ein Widerspruch. □

(6.1.2) Lemma.

G_0 hat den Lie-Rang 1 und P_J ist die Boreluntergruppe von G_0.

Beweis. Da nun $G \leq M$, läßt sich das BN-Paar (B_0, N_0) zu einem BN-Paar von G mit Weylgruppe $W \cong W_0$ ausdehen. Ferner ist G_α eine maximalparabolische Untergruppe mit Weylgruppe $W_J \cong (W_0)_J$. Wir finden diese Aussage in (2.6) von Curtis, Kantor & Seitz [11] oder in II (5.8) von Timmesfeld [34].

Da die Operation von G auf Ω zweifach transitiv ist, hat G_α genau zwei Doppelnebenklassen in G. Insbesondere besitzt W_J genau zwei Doppelnebenklassen in W, denn die Korrespondenz

$$G_\alpha w G_\alpha \longmapsto W_J w W_J$$

ist nach Abschnitt 43 von Aschbacher [2] eine bijektive Abbildung der Doppelnebenklassen von G_α in G auf die von W in W_J. Somit operiert auch W_0 zweifach transitiv auf den Nebenklassen von $(W_0)_J$ in W_0. Nach B.1 aus Anhang B ist dies nur für die linearen Gruppen (vom Typ A_l) und die Gruppen vom Lie-Rang 1 möglich. Ferner ist $(W_0)_J$ vom Typ A_{l-1}, also bleibt nur $l = 1$ zu zeigen.

Für $l > 1$ ist G_0 eine lineare Gruppe und dann ist

$$m = |G_0 : P_J| = \frac{q^{l+1} - 1}{q - 1} = \sum_{i=0}^{l} q^i.$$

Insbesondere ist q der p-Anteil von $m - 1$ und aus (6.1) erhalten wir dann $m - 1 \mid 2fq$, offenbar ein Widerspruch. □

(6.1.3) Satz.

G_0 ist wie in (a), (b) oder (c) aus Tabelle 4.1.

Beweis. Nun ist G_0 eine der Gruppen $PSL_2(q)$, $PSU_3(q)$, $Sz(q)$ oder $R'(q)$. Die Gruppen $PSL_2(2)$, $PSL_2(3)$ und $PSU_3(2)$ sind auflösbar und $R(3)'$ ist offenbar wie in (f) von 4.1, weswegen wir diese Fälle hier nicht mehr betrachten. Nun ist $P_J = B_0$ und nach der Bahnformel ist in obiger Reihenfolgt insbesondere

$$m = q + 1,\ q^3 + 1,\ q^2 + 1 \text{ oder } q^3 + 1.$$

Die Primteiler von $|X|$ sind nach 4.2.3 auch Teiler vom $m-1$, also ist X eine p-Gruppe. Offenbar wird

$$B_0 = (G_0)_\alpha$$

von G_α normalisiert und damit ist U_0 als Fittinguntergruppe von B_0 in X enthalten. Es bleibt zu zeigen, dass X nur innere Automorphismen auf G_0 induziert, denn dann ist $U_0 = X$ und es folgt aus Ordnungsgründen die Behauptung.

Dazu sei $x = ih\varphi \in X$ das Produkt eines inneren Automorphismus i, eines Diagonalautomorphismus h und eines Körperautomorphismus φ von G_0. Wegen $x, h, \varphi \in N(B_0)$ ist auch $i \in N(B_0) = B_0$ und somit $i = uh'$ mit $u \in U_0$ und $h' \in H$. Wir betrachten nun den Automorphismus

$$u^{-1}x = h'h\varphi \in X.$$

Sicherlich wird B_0/U_0 von X zentralisiert, denn

$$[X, B_0] \leq X \cap B_0 \leq F(B_0) = U_0.$$

Der Automorphismus $h'h$ zentralisiert sogar H_0, also muss der Körperautomorphismus φ auch die Faktorgruppe B_0/U_0 zentralisieren. Dies ist wegen $U_0 \cap H_0 = 1$ ganz sicher nur der Fall für $\varphi = 1$. Somit ist $u^{-1}x = h'h = 1$, denn andernfalls enthält X ein Element von p'-Ordnung, und dies wäre ein Widerspruch. □

6.2 Die nicht-natürlichen Darstellungen

Sei nun *p kein Teiler von $|X|$*. Wir verfahren hier in mehreren Schritten und erinnern uns zunächst an die Notation von Kapitel 3, die wir hier übernehmen werden. Bis auf Widerruf sei G_0 *verschieden von den Gruppen* ${}^2F_4(k)$, $Sz(q)$ und $R(q)$. Die einfache Lie-Typ-Gruppe G_0 hat dann eine Klasse von k-Wurzeluntergruppen Σ, wobei Σ die Menge aus Tabelle 3.1 auf Seite 23 sei.

Wir untersuchen zuerst den Fall, in dem G_α lange Wurzelelemente aus

$$D := D(\Sigma)$$

enthält. Es ist leicht zu sehen, dass dies höchstens für die Primzahlen $p = 2$ oder 3 möglich ist. Die Untersuchung dieser Fälle führt auf die Punkte (e) mit $m = 6$, (f) mit $m = 28$, sowie (h) und (i) in Hauptsatz 4.1.

Anschließend nehmen wir an, dass D fixpunktfrei auf Ω operiert. Wir erhalten dann bis auf Ausnahmen die Relation

$$m - 1 \quad \Big| \quad |G_0 : N_{G_0}(A)|(q-1)$$

für $A \in \Sigma$. Da G_α keine Wurzelelemente in D enthält, ist dann $M_A \cap G_\alpha$ eine abelsche Untergruppe von M_A für alle $\alpha \in \Omega$. In Kapitel 3 haben wir gezeigt, dass

$$q^s \quad \Big| \quad |M_A : M_A \cap G_\alpha|$$

für ein geeignetes s. Zerlegen wir Ω in Bahnen unter M_A, so ist $q^s \mid m$. Setzen wir dies in die obige Relation ein, so erhalten wir einen Widerspruch, wenn m keine p-Potenz ist. Die obige Relation gilt nicht in allen Fällen. Diese werden an geeigneter Stelle separat behandelt.

Es bleibt der Fall zu untersuchen, in denen m eine p-Potenz ist. Dann ist G_0 eine fahnentransitive Gruppe oder eine Gruppe vom Lie-Rang 1 und diese sind klassifiziert. Wir erhalten leicht die übrigen Fälle aus dem Hauptsatz.

6.2.1 Einleitende Aussagen

Wir nehmen in diesem Abschnitt an, dass D *nicht fixpunktfrei* auf Ω operiert. Da D invariant unter der auf Ω transitiven Gruppe G_0 ist, ist insbesondere auch

$$E := D \cap G_\alpha \neq \emptyset.$$

Die Menge D ist in Ausnahmefällen nicht invariant unter sämtlichen Automorphismen. Bei den Gruppen vom Typ B_2 und F_4 in gerader Charakteristik oder G_2 in Charakteristik 3 wird nämlich die Menge Σ der langen Wurzeluntergruppen auf die der kurzen Wurzeluntergruppen abgebildet. Unter Konjugation mit der p'-Gruppe X ist D und damit auch E jedoch abgeschlossen, wie wir im folgenden Lemma sehen.

(6.2.1.1) Lemma.

E ist X-invariant.

Beweis. Ist $e \in E$, so operiert die elementarabelsche p-Gruppe $\langle e \rangle$ auf dem p'-Normalteiler X von G_α. Für solche Operationen finden wir

$$X = [X, e]C_X(e)$$

in VII (7.12) von Kurzweil [24]. Offenbar ist nun $[X, e] \leq (G_0)_\alpha$ und da E unter Konjugation in $(G_0)_\alpha$ abgeschlossen ist, folgt die Aussage. □

(6.2.1.2) Notation.

Für jedes Element $d \in D$ bezeichne $E(d)$ die abstrakte Wurzeluntergruppe in Σ, die d enthält. Da Σ eine TI-Menge ist, ist diese Bezeichnung wohldefiniert.

(6.2.1.3) Lemma.

Für $e \in E$ gilt:

(a) Die Gruppe $\langle e^X \rangle = \langle e \rangle [X, e]$ ist auflösbar.

(b) Für $f \in e^X \setminus \{e\}$ ist $e^{-1}f$ von p'-Ordnung. Insbesondere ist $E(f) \in \Omega_{E(e)}$.

Beweis. Ist $f \in e^X$ verschieden von e, so ist $f = e^x$ für ein $x \in X$ und

$$e^{-1}f = [e, x] \in [X, e].$$

Insbesondere ist $\langle e^X \rangle = \langle e \rangle [X, e]$ mit auflösbaren p'-Normalteiler $[X, e]$, und das Lemma ist nun klar. □

(6.2.1.4) Lemma.

Enthält $A \in \Sigma$ ein langes Wurzelelement in G_α, so ist $A \cap G_\alpha$ die einzige Untergruppe der Ordnung p von $M_A \cap G_\alpha$.

Beweis. Ist $\langle t \rangle$ neben $\langle e \rangle \leq A \cap G_\alpha$ eine weitere Untergruppe der Ordnung p von $M_A \cap G_\alpha$, so ist $\langle e, t \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$, denn nach den Abschnitten 3.2 und 3.3 ist $A \leq Z(M_A)$. Für die Operation einer nicht zyklischen, abelschen p-Gruppe auf der p'-Gruppe X finden wir

$$X = \langle C_X(v) \mid v \in \langle e, t \rangle^\sharp \rangle$$

in VII (7.23) von KURZWEIL [24].

Angenommen $C_X(v) \not\leq C_X(e)$ für $v \in \langle e, t \rangle^\sharp$. Dann gibt es ein $x \in X$, dass mit v, aber nicht mit e vertauscht. Wegen $e \neq e^x$ ist $A^x \in \Omega_A$ nach 6.2.1.3, wird aber von $v \in M_A$ normalisiert. Dies ist ein Widerspruch, da M_A nach 3.1.4 regulär auf Ω_A operiert. Somit ist $X = C_X(e)$ und dies ist unmöglich, da X selbstzentralisierend ist. □

(6.2.1.5) Folgerung.

Enthält $A \in \Sigma$ ein langes Wurzelelement in G_α, so ist $M_A \cap G_\alpha$ zyklisch von der Ordnung p oder p^2 oder isomorph zur Quaternionengruppe der Ordnung acht.

Beweis. Die Gruppen, die genau eine Untergruppe der Ordnung p haben, sind nach (5.3.7) von KURZWEIL & STELLMACHER [23] gerade zyklisch oder in gerader Charakteristik isomorph zu einer Quaternionengruppe. In gerader Charakteristik ist nach Kapitel 3 und dem letzten Lemma

$$(M_A \cap G_\alpha)' \leq A \cap G_\alpha$$

von der Ordnung höchstens zwei und die Quaternionengruppe der Ordnung acht ist die einzige Quaternionengruppe mit Kommutatorgruppe der Ordnung zwei.

Ist $M_A \cap G_\alpha$ zyklisch, so ist

$$(M_A \cap G_\alpha)/(A \cap G_\alpha) \cong (M_A \cap G_\alpha)A/A \cong \mathbb{Z}_p \text{ oder } 1,$$

denn M_A/A ist elementarabelsch. Wegen $|A \cap G_\alpha| = p$ folgt nun die Behauptung. □

6.2.2 Weitere Aussagen

Zum Beginn des Abschnitts haben wir das weitere Vorgehen erläutert. Wir unterscheiden die Fälle, in denen die Elemente von D fixpunktfrei auf Ω operieren oder nicht. Wir werden Aussagen benötigen, die (teilweise) unabhängig von dieser Unterscheidung sind. Diese führen wir hier auf.

(6.2.2.1) Lemma.

Ist S eine p-Sylowgruppe von G und T eine p-Sylowgruppe von G_α mit $T \leq S$, so ist $|S : T|$ der p-Anteil von m.

Beweis. Offenbar ist

$$|G : S||S : T| = |G : T| = |G : G_\alpha||G_\alpha : T| = m \cdot |G_\alpha : T|,$$

und wir können die Behauptung direkt ablesen. □

(6.2.2.2) Folgerung.

Sei G_0 vom Lie-Rang mindestens zwei und verschieden von $Sp_4(2^f)$. Ist p^t der p-Anteil von m, dann gilt eine der folgenden Abschätzungen:

(a) Der Körper k hat gerade Charakteristik und $|M_A| \leq 2^{3+t}$ für $A \in \Sigma$.

(b) Der Körper k hat ungerade Charakteristik und $|M_A| \leq p^{2+t}$ für $A \in \Sigma$.

(c) Ist s wie in 3.2.3.1 und 3.3.6 von Kapitel 2, so ist $q^s \leq p^t$.

Beweis. Für $A \in \Sigma$ betten wir $M_A \cap G_\alpha$ in eine p-Sylowgruppe T von G_α ein. Ist $T \leq S$ eine p-Sylowgruppe von G, so ist nicht notwendig $M_A \leq S$, aber für ein Konjugiertes $B \in \Sigma$ ist $M_B \leq S$. Dann ist auch

$$M_B \cap G_\alpha \leq S \cap G_\alpha = T$$

und somit

$$|M_B : M_B \cap G_\alpha| \leq |S : T|.$$

Ist $B \cap E \neq \emptyset$, so folgen die beiden ersten Punkte aus 6.2.1.5 und obigem Lemma. Im Fall $B \cap E = \emptyset$ ist $M_B \cap G_\alpha$ abelsch und der dritte Punkt folgt aus 3.2.3.1 und 3.3.6. □

(6.2.2.3) Lemma.

Sei G_0 vom Lie-Rang 1 und ein $A \in \Sigma$ enthalte ein langes Wurzelelement in G_α. Ist p^t der p-Anteil von m, dann gilt eine der folgenden Abschätzungen:

(a) Der Körper k hat gerade Charakteristik und $|M_A| \leq 2^{3+t}$.

(b) Der Körper k hat ungerade Charakteristik und $|M_A| \leq p^{2+t}$.

Beweis. Seien T, S, A und B wie im Beweis des vorangegangenen Lemmas. Natürlich ist M_A eine p-Sylowgruppe von G_0 und operiert regulär auf $\Sigma \setminus \{A\} = \Omega_A$. Hier ist nun

$$M_A \cap G_\alpha \leq T \leq S = M_B,$$

also enthält M_B insbesondere ein Element in $A^\sharp$. Somit vertauscht A mit B und es folgt notwendig $A = B$. Ferner gilt nun

$$|M_A : M_A \cap G_\alpha| \leq |S : T|$$

und wir lesen sofort die Behauptung ab. □

(6.2.2.4) Lemma.

Für $A \in \Sigma$ ist A^G eine TI-Menge. Insbesondere ist $C(a) \leq N(A)$ und $M_A \trianglelefteq C(a)$ für $a \in A^\sharp$.

Beweis. Die Menge Σ wird von den Automorphismen von G_0 invariant gelassen, wenn G_0 keine der Gruppen vom Typ C_2 oder F_4 in gerader Charakteristik oder G_2 in Charakteristik 3 ist. Insbesondere ist dort A^G eine TI-Menge.

In den drei ausgeschlossenen Fällen gibt es einen Graphautomorphismus σ, der die Gruppe A auf eine kurze Wurzeluntergruppe A_s abbildet. Angenommen es ist $A^g \notin \Sigma$. Dann ist $g = id\tau\sigma$ das Produkt eines inneren, Diagonal-, Körper- und eines nichttrivialen Graphautomorphismus. Wir nehmen o.B.d.A. $A = A_h$ an. Da $\Sigma = A^{G_0}$ invariant unter $id\tau$ ist, ist

$$A^g \in A^{G_0\sigma} = A^{\sigma G_0} = A_s^{G_0}.$$

Insbesondere gibt es ein $x \in G_0$ mit $A^g = A_s^x$. Ist (B_0, N_0) das übliche BN-Paar von G_0, so gibt es $b, b' \in B_0$ und $w \in N_0$ mit $x = b'wb$. Nun ist $N_{G_0}(A)$ eine standardparabolische Untergruppe von G_0 und daher ist auch

$$N_{G_0}(A_s) = N_{G_0}(A)^\sigma$$

eine solche und A_s wird von B_0 normalisiert. Es folgt nun

$$A \cap A^g = A \cap A_s^x = A \cap A_s^{b'wb} = (A \cap A_{s^w})^b = 1,$$

denn entweder ist $A_{s^w} \in \Sigma$ oder enthalten in U^{w_0}.

In allen Fällen ist also A^G eine TI-Menge, und damit $C(a) \leq N(A)$ für $a \in A^\sharp$. Wegen $A \leq Z(M_A)$ ist $M_A \leq C(a)$ und da M_A charakteristisch in $N_{G_0}(A)$ ist, folgt die Behauptung. □

(6.2.2.5) Lemma.

Ist T eine nichttriviale X-invariante Untergruppe von G_α, so ist $N(T) \leq G_\alpha$.

Beweis. Bewegt $N(T)$ die Ziffer α, dann ist $N(T)$ wegen $X \leq N(T)$ transitiv auf Ω und somit ist $\alpha^{N(T)} = \Omega$ die Menge der Fixpunkte von T, ein Widerspruch. □

6.2.3 Der Fall $E \neq \emptyset$ mit $p > 3$

Operieren die Elemente von D fixpunktfrei auf Ω, dann können wir leicht den Hauptsatz beweisen, so wie wir es vorne angedeutet haben. Für $p > 3$ ist dies stets der Fall und sogar sehr einfach zu sehen. Ist nämlich $e \in E$, so enthält e^X nach der Bahnformel ein von e verschiedenes Wurzelelement f, denn die p'-Gruppe X ist selbstzentralisierend. Nach Lemma 6.2.1.3 erzeugen e und f eine auflösbare Untergruppe von $(P)SL_2(q)$ und $e^{-1}f$ ist kein Element von p-Potenzordnung. Nach der Dicksonliste ist dies nicht möglich und wir erhalten den

(6.2.3.1) Satz.

Ist $p > 3$, so operieren die Elemente von D fixpunktfrei auf Ω.

Für $p = 2$ oder 3 können wir das letzte Argument natürlich nicht verwenden. Dies zeigen die auftretenden Beispiele aus dem Hauptsatz, und auch nach der Dicksonliste enthält $(P)SL_2(q)$ auflösbare Untergruppen, die von zwei Involutionen bzw. Elementen der Ordnung drei erzeugt werden. Für $p = 2$ sind dies die Diedergruppen von 2-Potenzordnung und für $p = 3$ denken wir an die Untergruppen $PSL_2(3)$ und $SL_2(3)$, die ebenfalls auflösbar sind.

6.2.4 Der Fall $E \neq \emptyset$ mit $q = 2$

Im weiteren Verlauf sei $q = 2$ und $A \in \Sigma$ eine abstrakte Wurzeluntergruppe mit $A \leq G_\alpha$. Wir erhalten hier nur die Fälle (h) und (i) aus dem Hauptsatz 4.1 und arbeiten fast ausschließlich mit einfachen Eigenschaften zweifach transitiver Permutationsgruppen und Wurzelinvolutionen.

Natürlich wird A von einem einzigen langen Wurzelelement e erzeugt, dessen Fixpunktmenge auf Ω wir mit $Fix(e)$ bezeichnen werden. Die Konjugierten e^x von e unter X haben dann ebenfalls Mengen von Fixpunkten auf Ω, welche wir entsprechend mit $Fix(e^x)$ bezeichnen. Jede dieser Mengen enthält die Ziffer α und ist daher nichtleer. Wir beschreiben kurz das weitere Vorgehen. Zerlegen wir Ω in Bahnen unter A, dann hat A neben α stets mindestens einen zweiten Fixpunkt und

$$Fix(e^x)^* := Fix(e^x) \setminus \{\alpha\}$$

ist für alle $x \in X$ nichttrivial. Insbesondere ist dann Ω^* die Vereinigung der Mengen $Fix(e^x)^*$, denn X operiert transitiv auf Ω^*. Die Menge e^X enthält genau drei oder neun Involutionen.

Schneiden sich zwei der Fixpunktmengen aus der obigen Zerlegung nichttrivial, dann enthält e^X notwendig neun Involutionen. Die Menge $Fix(e)^*$ kann dann partitioniert werden in vier gleichgroße Fixpunktmengen von zu Σ_3 isomorphen Untergruppen von

$\langle e^X \rangle$. Die vier Fixpunktmengen sind in $C_X(e)$ konjugiert und nach der Bahnformel ist dann X von gerader Ordung, ein Widerspruch.

Schneiden sich die Fixpunktmengen $Fix(e^x)^*$ für alle $x \in X$ trivial, so ist M_A transitiv auf $Fix(e)$. Die Fixpunktmengen sind zueinander konjugiert und daher ist m eine der Zahlen $3 \cdot 2^l - 2$ oder $9 \cdot 2^l - 8$ für $l = |M_A : M_A \cap G_\alpha|$. Dies liefert den genauen 2-Anteil von m und mit 6.2.2.2 eine starke Abschätzung für die Ordnung von M_A. Leicht stoßen wir dann auf die beiden Beispiele aus dem Hauptsatz.

(6.2.4.1) Bemerkung.

Die zwei Gruppen $SL_2(2)$ und $PSU_3(2)$ sind auflösbare Gruppen und werden daher im folgenden nicht betrachtet. Wir können also stets annehmen, dass G_0 vom Lie-Rang mindestens zwei ist. Die Gruppen $G_2(2)'$ und $Sp_4(2)'$ betten wir in die Gruppen $G_2(2)$ und $Sp_4(2)$ ein und betrachten stattdessen auch diese Gruppen.

(6.2.4.2) Lemma.

Entweder ist $\langle e^X \rangle$ isomorph zu Σ_3 oder enthält genau neun Involutionen und wird von je zwei zu Σ_3 isomorphen Untergruppen erzeugt. Im letzten Fall ist M_A nicht abelsch.

Beweis. Sei $\langle e^X \rangle$ nicht isomorph zu Σ_3. Die Menge der Involutionen von $\langle e^X \rangle$ ist nach 6.2.1.3 (a) offenbar gerade e^X und die selbstzentralisierende Gruppe X ist von ungerader Ordnung. Insbesondere gibt es also $d, e, f \in e^X$ mit

$$e \notin \langle d, f \rangle \cong \Sigma_3.$$

Für je zwei verschiedene Involutionen $x, y \in e^X$ gilt $\langle x, y \rangle \cong \Sigma_3$ und insbesondere

$$x^y = y^x.$$

Aus dieser Gleichung, die wir im weiteren Verlauf immer wieder verwenden, sehen wir, dass die Gruppe $\langle d, e, f \rangle$ nur die Involutionen e, f, e^f, d, e^d, f^d, e^{fd}, d^{fe} und d^{ef} von $\langle d, e, f \rangle$ enthält. Wegen

$$\begin{aligned}
(d^{fe})^d &= f^{ded} = f^{e^d} = (e^d)^f = e^{df}, & (d^{ef})^e &= d^{f^e} = f^{ed} = e^{fd},\\
(d^{ef})^d &= e^{dfd} = f^{de} = d^{fe}, & (e^d)^f &= d^{ef},\\
(f^d)^e &= d^{fe}, & (f^d)^f &= d,\\
(e^{fd})^e &= f^{ede} = f^{d^e} = d^{ef}, & (e^{fd})^f &= e^{f^d} = f^{de} = d^{fe}.
\end{aligned}$$

ist die Menge dieser Involutionen nämlich offenbar invariant unter d, e und f. Die Gruppe $\langle d, e, f \rangle$ hat nach 6.2.1.3 die Ordnung $2l$ mit ungeradem l. Daher sind ihre Involutionen zueinander konjugiert und insbesondere sind die obigen neun Involutionen sämtliche Involutionen von $\langle d, e, f \rangle$. Wir beachten dabei, dass die obigen Involutionen paarweise verschiedenen sein müssen, denn $3 \mid l$.

Da M_A regulär auf Ω_e operiert, gibt es ein $a \in M_A$ mit

$$f^a = d.$$

Wäre $a^2 = 1$, so vertauscht a die Involutionen f und d und zentralisiert somit die dritte Involution d^f in $\langle d, f\rangle$. Nach Wahl von d ist aber

$$d^f \in e^X \setminus \{e\} \subseteq \Omega_e,$$

ein Widerspruch zu 6.2.1.3. Da nun M_A/A elementarabelsch ist, ist $x^2 \in A$ für alle $x \in M_A$. Insbesondere ist

$$a^2 = e \tag{6.2}$$

und M_A ist nicht (elementar)abelsch.

Liegt nun keine Involution von e^X außerhalb von $\langle d, e, f\rangle$, so folgt offensichtlich die Behauptung. Angenommen es gibt ein $\ell \in e^X$ mit

$$\ell \notin \langle d, e, f\rangle.$$

Seien dann $b, c \in M_A$ mit

$$f^b = d^f \quad \text{und} \quad f^c = \ell.$$

Genau wie in (6.2) sehen wir

$$a^2 = b^2 = c^2 = e. \tag{6.3}$$

und ganz ähnlich folgt

$$(a^{-1}b)^2 = (a^{-1}c)^2 = (b^{-1}c)^2 = e.$$

Andernfalls vertauscht etwa $a^{-1}c$ die Involutionen d und ℓ und zentralisiert demnach $\ell^d \in e^X$. Dies ist wie oben wegen $\ell \notin \langle d, e, f\rangle$ ein Widerspruch.

Insbesondere sind a, b und c paarweise nicht vertauschbar, sonst ist etwa

$$(a^{-1}b)^2 = a^{-2}b^2 = e^2 = 1.$$

Somit ist

$$(ab)^2 = (ac)^2 = (bc)^2 = e,$$

denn andernfalls ist etwa

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

ein Widerspruch. Aus $(ab)^2 = e$ folgern wir

$$a^b = b^3ab = b^2bab = a^2bab = a(ab)^2 = ae = a^3$$

und damit

$$b^a = b^3 \quad \text{sowie analog} \quad c^a = c^3. \tag{6.4}$$

Wir erhalten

$$(bc)^a = b^a c^a = b^3 c^3 = bece = bce^2 = bc,$$

also vertauscht a mit bc. Wegen $(bc)^2 = e$ ist somit

$$((ab)c)^2 = (a(bc))^2 = 1$$

und wegen $(ab)^{-1} = abe$ vertauscht c mit ab. Somit vertauscht auch c^{-1} mit ab und es folgt

$$(c^{-1}ab)^2 = 1.$$

Folglich vertauscht $c^{-1}ab$ die Involutionen ℓ und $f^{ab} = d^b$. Wir berechnen noch d^b. Nach Wahl von b ist $fb = bd^f$ und somit

$$d^{bd^f e} = d^{fbe} = (d^f)^{be} = (d^f)^{b^{-1}} = f.$$

Es folgt

$$d^b = f^{ed^f} = e^{fd^f} = e^{df}.$$

Die Involution $c^{-1}ab$ vertauscht also e^{df} und ℓ und diese liegen in e^X. Daher ist auch $\ell^{e^{df}} \in e^X$ und diese Involution wird von $c^{-1}ab$ zentralisiert. Nun ist aber nach Wahl von ℓ auch

$$\ell^{e^{df}} \in e^X \setminus \{e\},$$

und dort hat M_A keine Fixpunkte. Dies ist ein Widerspruch. □

(6.2.4.3) Lemma.

Es ist $Fix(e)^* \neq \emptyset$.

Beweis. Operiert A fixpunktfrei auf Ω^*, so hat dort jede Bahn von A die Länge 2. Insbesondere ist dann $m-1$ gerade und dies ist ein Widerspruch, da X von ungerader Ordnung ist. □

(6.2.4.4) Lemma.

Es ist $\Omega^* = \dot{\bigcup}_{x \in X} Fix(e^x)^*$.

Beweis. Wegen der Transitivität von X auf Ω^* ist

$$\Omega^* = \bigcup_{x \in X} Fix(e^x)^*.$$

Ist die Vereinigung nicht disjunkt, so gibt es ein $e \neq f \in e^X$ mit

$$\emptyset \neq Fix(e)^* \cap Fix(f)^* = Fix(\langle e, f \rangle)^*.$$

Somit enthält e^X genau neun Involutionen, denn andernfalls ist

$$\langle e, f \rangle = \langle e^X \rangle$$

invariant unter X und somit wäre $\Omega^* = Fix(e)^* \cap Fix(f)^*$. Die Gruppe Σ_3 wird von je zwei ihrer drei Involutionen erzeugt, also enthält $\langle e^X \rangle$ offenbar genau vier zu Σ_3 isomorphe Untergruppen, die das Element e enthalten. Wir bezeichnen diese Gruppen im weiteren Verlauf mit Σ_3^i für $i = 1, \ldots, 4$. Die Fixpunktmengen dieser Gruppen bezeichnen wir wie üblich mit $Fix(\Sigma_3^i)$ und entsprechend ist

$$Fix(\Sigma_3^i)^* = Fix(\Sigma_3^i) \setminus \{\alpha\}.$$

Die vier Gruppen sind in M_A konjugiert und somit sind die vier Fixpunktmengen $Fix(\Sigma_3^i)^*$ sämtlich nichttrivial. Wir zeigen nun, dass $C_X(e)$ transitiv auf $\{Fix(\Sigma_3^i)^* \mid i = 1, \ldots, 4\}$ operiert. Nach der Bahnformel ist dann X von gerader Ordnung, ein Widerspruch. Wir beachten, dass $C_X(e)$ auf obiger Menge operiert.

Wählen wir o.B.d.A $\beta \in Fix(\Sigma_3^1)^*$ und $\gamma \in Fix(\Sigma_3^2)^*$, so gibt es ein $y \in X$ mit $\gamma^y = \beta$ und somit ist

$$\beta \in Fix(\Sigma_3^1)^* \cap Fix((\Sigma_3^2)^y)^*.$$

Demnach ist also

$$(\Sigma_3^2)^y = \Sigma_3^1,$$

denn sonst ist

$$Fix(\Sigma_3^1)^* \cap Fix((\Sigma_3^2)^y)^* = Fix(\langle e^X \rangle)^* = \emptyset.$$

Insbesondere ist e^y eine der drei Involutionen von Σ_3^1, welche wir hier mit e, e^x und e^{xe} bezeichnen. Ist $y \notin C_X(e)$, so ist entweder $e^y = e^x$ oder e^{xe}. Wir nutzen im folgenden aus, dass $u^w = w^u$ für je zwei Involutionen u und w in Σ_3 die dritte Involution ist.

Im ersten Fall ist dann offenbar $e^{y(e^{xe}e)} = e$ und

$$ye^{xe}e = y[e, x] \in C_X(e).$$

Wegen

$$(\Sigma_3^2)^{ye^{xe}e} = \Sigma_3^1$$

folgt dann die Behauptung. Im zweiten Fall ist $e^{ye} = e^x$ und daher wie eben $e^{yee^{xe}} = e$. Nun ist

$$yee^{xe} = y[x, e] \in C_X(e),$$

und wie eben folgt dann die Behauptung. □

(6.2.4.5) Folgerung.

Die Operation von M_A auf $Fix(e)$ ist transitiv und $Fix(e)$ hat eine 2-Potenzordnung.

Beweis. Wählen wir $\beta, \gamma \in Fix(e)^*$, so gibt es ein $x \in X$ mit $\beta = \gamma^x$. Es folgt

$$\beta \in Fix(e)^* \cap Fix(e^x)^*$$

und somit $x \in C_X(e)$. Insbesondere ist $C_X(e)$ transitiv auf $Fix(e)^*$. Nun ist A nach 6.2.1.4 die einzige Untergruppe der Ordnung zwei von $M_A \cap G_\alpha$. Insbesondere ist

$$M_A \not\leq G_\alpha,$$

denn sonst ist notwendig G_0 vom Lie-Rang 1, was aber hier nicht der Fall ist. Daher ist auch $C(e) \not\leq G_\alpha$ und wegen der Transitivität von $C_X(e)$ auf $Fix(e)^*$ ist dann $C(e)$ sogar zweifach transitiv auf $Fix(e)$. Nach 6.2.2.4 ist $M_A \trianglelefteq C(e)$ und somit transitiv auf $Fix(e)$, wie gewünscht. □

(6.2.4.6) Bemerkung.

Offenbar gilt diese Folgerung in beliebiger Charakteristik, wenn sich die Fixpunktmengen $Fix(e^x)^*$ für $x \in X$ trivial schneiden und wenn $M_A \not\leq G_\alpha$. Wir werden dieser Folgerung im Fall der Charakteristik 3 wieder begegnen.

Wir haben nun genügend Informationen gesammelt, um die möglichen Gruppen anzugeben. Der Hilfssatz 6.2.4.5 liefert

$$|Fix(e)| = |M_A : M_A \cap G_\alpha| =: 2^l.$$

und damit nach 6.2.1.5 insbesondere auch

$$2^{l+1} \leq |M_A| \leq 2^{l+3}. \tag{6.5}$$

(6.2.4.7) Satz.

Enthält e^X genau drei Involutionen, so ist $G_0 \cong Sp_4(2)'$ wie in (h) von 4.1.

Beweis. Enthält e^X genau drei Involutionen, so verbessert sich die obige Abschätzung denn M_A operiert regulär auf Ω_e und daher operiert $M_A \cap G_\alpha$ offenbar fixpunktfrei auf $e^X \setminus \{e\}$. Dies liefert dann sogar

$$|M_A| = 2^{l+1}.$$

Nach 6.2.4.5 ist $m-1 = 3\cdot 2^l - 3$ und dies liefert den genauen 2-Anteil 2^t von $m = 3\cdot 2^l - 2$. Dieser ist offenbar 2 für $l \geq 2$ und 2^2 für $l = 1$, wobei $l = 1$ offenbar nicht möglich ist.

Sei G_0 zunächst verschieden von $Sp_4(2)'$. Gilt die erste Abschätzung

$$2^{l+1} = |M_A| \leq 2^{3+t}$$

aus 6.2.2.2, so ist dies nur für $l = 2$ möglich. Die einzige Möglichkeit ist $G_0 \cong PSL_3(2)$ mit $m = 10$. Wir haben die Ordnungen von M_A in den Tabellen 3.4 und 3.5 angegeben. Da $SL_3(2)$ keinen 5-Anteil hat, ist dies jedoch nicht möglich. Es bleibt die dritte Abschätzung aus 6.2.2.2 zu untersuchen, in der $s \leq t \leq 1$ gilt. Dies führt wieder auf den oben ausgeschlossenen Fall $G_0 \cong PSL_3(2)$.

Es bleibt der Fall $G_0 = Sp_4(2)' \cong A_6$ zu untersuchen. Die Gruppe $(G_0)_\alpha$ enthält die zu Σ_3 isomorphe Untergruppe $\langle e^X \rangle$ und somit ist

$$3 \cdot 2^l - 2 = m = |G_0 : (G_0)_\alpha| \Big| \; 2^2 \cdot 3 \cdot 5.$$

l	t	m	$\lvert M_A\rvert$
1	1	10	2^3
2	2	28	2^3
2	2	28	2^5
3	6	64	2^5
4	3	$136 = 2^3 \cdot 17$	2^5

Tabelle 6.2: Die Möglichkeiten für m

Dies ist offenbar nur für $m = 4$ oder 10 möglich. Da A_6 keine maximale Untergruppe vom Index 4 besitzt, bleibt nur $m = 10$. Wegen $|Out(G_0)| = 2^2$ ist $X \leq G_0$ und es folgt sofort, dass X regulär auf neun Ziffern operiert, wie gewünscht. □

(6.2.4.8) Satz.

Enthält e^X genau neun Involutionen, so ist $G_0 \cong G_2(2)'$ wie in (i) von 4.1.

Beweis. In diesem Fall ist M_A nicht abelsch und somit $G_0 \neq Sp_4(2)'$. Genau wie eben folgt

$$m = 9 \cdot 2^l - 8,$$

und dies liefert den genauen 2-Anteil 2^t von m. Wir betrachten zuerst den Fall, in dem die erste Abschätzung

$$2^{l+1} \leq |M_A| \leq 2^{3+t} \tag{6.6}$$

aus 6.2.2.2 gilt. Für $l \geq 5$ ist $t = 3$ und daher $2^6 = |M_A|$. Dies ist niemals der Fall und somit $l \leq 4$. Benutzen wir die Tatsache, dass $M_A \cap G_\alpha$ von der Ordnung höchstens 2^3 ist, so erhalten wir für die Zahlen $1 \leq l \leq 3$ allein aus (6.5) eine Abschätzung für $|M_A|$. Für $l = 4$ benutzen wir zusätzlich (6.6) und erhalten insgesamt Tabelle 6.2.

Die einzige Gruppe mit $|M_A| = 2^3$ ist $SL_3(2)$ von der Ordnung $2^3 \cdot 3 \cdot 7$. Dies schließt den Fall $l = 1$ aus, denn m teilt die Ordnung von G_0. Außerdem ist $Out(G_0)$ von der Ordnung 2 und damit $X \leq G_0$. Da nun X transitiv auf 3^3 Ziffern operieren muss, schließt dies auch den Fall $l = 2$ aus.

Die einzigen Gruppen mit $|M_A| = 2^5$ sind die Gruppen $SL_4(2)$, $G_2(2)$ und $PSU_4(2)$. Für $l = 3$ sind aus Ordnungsgründen wie oben nur die Gruppen $SL_4(2)$ bzw. $G_2(2)$ möglich. Hier ist jedoch $m = 2^6$ der 2-Anteil von G_0 bzw. G, und somit ist $(G_0)_\alpha$ bzw. G_α eine $2'$-Gruppe, ein Widerspruch.

Für $l = 4$ teilt m nicht die Ordnungen der aufgeführten Gruppen und $l = 2$ ist nur für $G_0 = G_2(2)'$ möglich. Schließlich ist der Fall $l = 2$ nur für $G = G_2(2)$ möglich. Insbesondere ist dann X regulär auf 27 Ziffern.

Es bleibt die dritte Abschätzung aus 6.2.2.2 zu untersuchen. Hier gilt $s \leq t$. Allerdings müssen wir nur noch die Fälle $l \geq 4$ betrachten, denn die übrigen Fälle haben nur (6.5)

benötigt. Für $l \geq 4$ ist also $s \leq 3$ und damit $|M_A| \leq 2^5$. Nach (6.5) ist $|M_A| \geq 2^{l+1}$ und damit $l = 4$ und $|M_A| = 2^5$. Auch diesen Fall haben wir oben bereits ausgeschlossen und es folgt die Behauptung. □

6.2.5 Der Fall $E \neq \emptyset$ mit $p = 2$ und $q > 2$

Sei k von gerader Charakteristik mit $q > 2$ und $E \neq \emptyset$. Das Ziel dieses Abschnittes ist die Identifikation der Fälle (e) und (f) mit $m = 6$ und 28 aus dem Hauptsatz 4.1. Ein leichtes Studium dieser beiden Beispiele zeigt, dass $(G_0)_\alpha$ eine Diedergruppe ist und vielmehr erzeugt wird von e^X, wenn e ein langes Wurzelelement innerhalb von $PSL_2(4)$ oder $PSL_2(8)$ ist. Daher untersuchen wir den Fall, in denen

$$D_e := \langle e^X \rangle$$

für alle $e \in E$ keine Diedergruppe ist getrennt von dem entsprechenden Fall, in dem es ein $e \in E$ gibt, so dass D_e eine Diedergruppe ist. Wir benutzen dabei ständig die Eigenschaften der Wurzelinvolutionen aus D bzw. E, die wir in Abschnitt 3.4 von Kapitel 3 angegeben haben.

Wir beschreiben nun den ersten Fall. Ist D_e keine Diedergruppe für $e \in E$, so sehen wir leicht ein, dass $ee^x = [e, x]$ für $x \in X$ eine 3-Potenzordnung hat. Insbesondere sind $[X, e]$ und $[X, E]$ auch 3-Gruppen. Nehmen wir dann an, dass X eine r-Sylowgruppe P enthält mit $r \neq 2, 3$, so folgt leicht, dass E von P zentralisiert wird. Als Folgerung erhalten wir, dass P auf denjenigen Gruppen $\langle E(e), E(f) \rangle$, $e, f \in E$, die isomorph zu $SL_2(q)$ sind, operiert. Eine genauere Untersuchung dieser Operation zeigt, dass P die Ordnung r hat und dass $q = 2^r$. Ist x ein Erzeuger von P und fassen wir diesen als Automorphismus von G_0 auf, dann können wir x in die Nebenklasse $G_0\varphi$ konjugieren, wobei φ ein Körperautomorphismus ist. Der Satz von Lang [15] sagt aus, dass ein solches Element von Primzahlordnung konjugiert zu einem Körperautomorphismus von G_0 ist. Da P von x erzeugt wird, können wir annehmen, dass P die Körperautomorphismengruppe von G_0 ist. Insbesondere ist dann

$$R := \langle a_r(1) \mid r \in \Phi \rangle \leq C_{G_0}(P) \leq G_\alpha,$$

wenn Φ das Wurzelsystem von G_0 ist. Somit enthält G_α alle langen Wurzelelemente von R, und dies wird nur möglich sein, wenn R den Lie-Rang 1 hat. Da G_0 denselben Lie-Typ hat, ist auch G_0 eine Gruppe vom Lie-Rang 1, und dies schließen wir leicht aus.

Daher ist X eine 3-Gruppe und folglich $m-1$ eine 3-Potenz, womit wir den 2-Anteil von m abschätzen können. Wie im Fall $q = 2$ liefert dies eine Abschätzung für die Ordnung von M_A für $A \in \Sigma$, womit wir leicht sehen, dass diese Fälle niemals eintreten können. Der zweite Fall führt mit elementaren Argumenten auf die beiden oben aufgeführten Beispiele aus dem Hauptsatz 4.1.

6.2.5.1 Einleitende Aussagen

In diesem Unterabschnitt beweisen wir zuerst zwei Aussagen, die unabhänig von der genauen Struktur von D_e und damit unabhängig von den zwei angekündigten Fällen sind. Beide Aussagen setzen nur voraus, dass E nichtleer ist und benutzen Eigenschaften der Wurzelinvolutionen aus D.

(6.2.5.1.1) Lemma.

Es ist $E \cap E^2 = \emptyset$.

Beweis. Angenommen $e, f, ef = fe \in E$. Wir konstruieren ein Produkt von langen Wurzelelementen, dass eine von 2 und 4 verschiedene gerade Ordnung hat, was nicht möglich ist. Nach Wahl von e und f ist $\langle e, f\rangle$ eine elementarabelsche 2-Gruppe, die auf der $2'$-Gruppe X operiert. Daher ist

$$X = \langle C_X(e), C_X(f), C_X(ef)\rangle$$

nach VII (7.23) von KURZWEIL [24]. Wäre nun $C_X(e) = C_X(f)$, dann wäre $X = C_X(ef)$, und dies ist ein Widerspruch, da die $2'$-Gruppe X selbstzentralisierend ist. Insbesondere gibt es o.B.d.A. ein $x \in X$, dass mit e aber nicht mit f vertauscht. Nach 6.2.1.1 ist E invariant unter Konjugation mit X, also ist

$$z := (ef)f^x = e[f, x]$$

ein Produkt zweier langer Wurzelelemente. Dabei vertauscht e mit $1 \neq [f, x] \in X$ und z hat somit die Ordnung $2s$ mit ungeradem s, wie gewünscht. □

(6.2.5.1.2) Folgerung.

Sind $e, f \in E$ verschieden, so ist ef von ungerader Ordnung.

Beweis. Hat ef keine ungerade Ordnung, so vertauschen e und f oder ef ist von der Ordnung vier und $(ef)^2$ ist wieder eine Wurzelinvolution. Im letzten Fall ist natürlich $(ef)^2 = (fe)^2 \in D$, also ist

$$e(ef)^2 = e^f = (fe)^2 e \in E \cap E^2,$$

ein Widerspruch und somit sind e und f vertauschbar. Ist $\overline{\ }$ der natürliche Homomorphismus von $\langle e^X, f^X\rangle$ auf $\langle e^X, f^X\rangle X/X$, so gilt demnach

$$\overline{[e^X, f^X]} = 1,$$

da wir etwa schon mehrfach gesehen haben, dass $D_e \leq \langle e\rangle X$. Für $x \in X$ ist dann insbesondere

$$(e^x f)^2 = [e^x, f] \in X$$

und somit $e^x f$ von der Ordnung $2s$ mit ungeradem s. Dies ist nur möglich für $s = 1$, also vertauschen e^x und f und es folgt notwendig $[E(f), E(e^x)] = 1$ für alle $x \in X$. Nach 6.2.2.5 ist dann aber

$$E(f) \leq N(D_e) \leq G_\alpha$$

und dies ist unmöglich, da nach 6.2.1.4 gerade $E(f) \cap G_\alpha$ von der Ordnung zwei ist und hier $E(f)$ mindestens vier Elemente hat. □

6.2.5.2 Die nichtauftretenden Situationen

In den Beispielen aus dem Hauptsatz ist D_e stets eine Diedergruppe für alle $e \in E$. Wir schließen in diesem Unterabschnitt eine andere Möglichkeit aus. Sei also D_e *keine Diedergruppe* für alle $e \in E$. Dies wird in gerader Charakteristik der komplizierteste Teil des Beweises sein. Wir erhalten zuerst das folgende

(6.2.5.2.1) Lemma.

$[X, E]$ *ist eine* 3*-Gruppe.*

Beweis. Sei $e^x \in e^X$ verschieden von $e \in E$. Die Involutionen von D_e sind nach 6.2.1.3 die von

$$e^X =: \{e, e_2, e_3, \ldots, e_n\}$$

mit $e_2 := e^x$. Da D_e keine Diedergruppe ist, gibt es ein i, so dass

$$\langle e, e^x, \ldots, e_i\rangle =: \langle a, b\rangle$$

eine Diedergruppe und $H := \langle a, b, e_{i+1}\rangle$ keine Diedergruppe ist. Produkte von Elementen aus e^X haben ungerade Ordnung, also ist $E(a), E(b) \in \Omega_{E(e_{i+1})}$ und $E(a) \in \Omega_{E(b)}$. Wegen $H \leq D_e$ ist $O_2(H) = 1$ und nach 3.4.2 aus Kapitel 3 ist dann H eine Untergruppe von $SL_2(q)$, $SL_3(q)$, $SL_3(q^3)$ oder $SU_3(q)$. Nach der Liste der Untergruppen dieser Gruppen ist H isomorph zu $3^2\mathbb{Z}_2$, $3^{1+2}\mathbb{Z}_2$ oder eine Diedergruppe, wobei wir den letzten Fall ausgeschlossen haben. Insbesondere ist $[e, x] = ee^x$ von 3-Potenzordnung. Da X nilpotent ist, hat X und jede Untergruppe von X genau eine 3-Sylowgruppe. Daraus folgt die Behauptung. □

Der Beweis zeigt, dass G insbesondere verschieden von $Sp_4(q)$ ist, denn dort wäre $H \leq SL_2(q)$. Im folgenden zeigen wir, dass X notwendig eine 3-Gruppe sein muss. *Angenommen* X *ist keine* 3*-Gruppe.* Dann gibt es eine r-Sylowuntergruppe P von X mit $r > 3$. Eine r-Sylowgruppe von X ist wegen der Nilpotenz von X charakteristisch in X und somit ein Normalteiler von G_α. Insbesondere ist $[P, E] \leq P \cap [X, E] = 1$ und es gilt das

(6.2.5.2.2) Lemma.

Es ist $P \leq C_X(E)$.

Als Folgerung aus 6.2.2.4 erhalten wir das

(6.2.5.2.3) Lemma.

Ist $A \cap E \neq \emptyset$ für $A \in \Sigma$, so ist $P \leq N(A)$.

Seien nun $A, B \in \Sigma$ zwei abstrakte Wurzeluntergruppen mit Wurzelelement e bzw. f in E und $B \in \Omega_A$. Solche Wurzeluntergruppen existieren, wenn wir etwa $e \in E$ und $f \in e^X$ verschieden von e wählen. Die Gruppe P operiert nun auf $Y := \langle A, B\rangle$ und wir nehmen folgende Identifikationen vor:

$$A = \left\{ \begin{pmatrix} 1 & \\ t & 1 \end{pmatrix} \mid t \in GF(q) \right\} \equiv \{a(t) \mid t \in GF(q)\},$$
$$B = \left\{ \begin{pmatrix} 1 & t \\ & 1 \end{pmatrix} \mid t \in GF(q) \right\} \equiv \{b(t) \mid t \in GF(q)\},$$
$$e = a(1).$$

Möglich sind diese Identifikationen, da A transitiv auf den von A verschiedenen 2-Sylowgruppen von Y operiert und die Diagonalgruppe H_Y von Y transitiv auf $A^\sharp$ und $B^\sharp$ operiert. Mit Matrizen rechnen wir nämlich leicht nach, dass H_Y (wegen $p = 2$) fixpunktfrei auf $A^\sharp$ operiert, und daher nach der Bahnformel auch transitiv operiert. Wir untersuchen nun die Operation von P auf Y.

(6.2.5.2.4) Lemma.

P operiert treu auf Y.

Beweis. Wir haben oben gezeigt, dass P auf A, B und somit auch auf Y operiert. Es reicht also zu zeigen, dass P treu auf A operiert. Wäre dies nicht der Fall, so wäre $C_P(A)$ ein nichttrivialer Normalteiler von P. Da X direktes Produkt seiner Sylowgruppen ist, ist $C_P(A)$ auch invariant unter X und mit 6.2.2.5 ist dann

$$A \leq N(C_P(A)) \leq G_\alpha.$$

Dies ist ein Widerspruch, da e nach 6.2.1.4 das einzige Wurzelelement von A in G_α ist. □

(6.2.5.2.5) Lemma.

Es ist $q = p^r$ und $P \cong Aut(k)$. Ferner ist $\langle e, f\rangle \cong \Sigma_3$.

Beweis. Nach 6.2.5.2.4 ist $x \in P$ das Produkt eines inneren Automorphismus y mit einem Körperautomorphismus φ von Y. Offenbar ist dann

$$y = x\varphi^{-1} \in N_Y(A) \cap N_Y(B) =: H_Y = \{h(c) \mid c \in k^*\}$$

mit Fixpunkt $e = a(1)$. Wegen $a(1)^{h(c)} = a(c^2)$ für $c \in k^*$ ist dann notwendig $y = 1$ und folglich ist P eine Untergruppe von $Aut(k)$ und insbesondere abelsch.

Insbesondere wird $\langle x \rangle$ von P und daher auch von X normalisiert und es folgt

$$\langle e \rangle \leq A \cap C(x) \leq A \cap G_\alpha = \langle e \rangle = \langle a(1) \rangle$$

nach 6.2.2.5 und 6.2.1.4. Somit ist $\mathbb{Z}_2$ der Fixörper von x und schließlich $Aut(k) = \langle x \rangle$. Da x beliebig in P gewählt war, beweist dies die Aussage. □

(6.2.5.2.6) Lemma.

Es ist $P \not\leq G_0$.

Beweis. Andernfalls ist sogar

$$P \leq N_{G_0}(A) = M_A L_A H_0,$$

wobei wir A mit der abstrakten Wurzeluntergruppe zu A_h identifizieren. Die Gruppe A wird von $M_A L_A$ zentralisiert, also operiert ein erzeugendes Element von P wie ein Element $h \in H_0$ (nichttrivial) auf A. In Carter [6] finden wir ein $c \in k^*$ mit $a(t)^h = a(ct)$ für alle $t \in k$. Da e ein Fixpunkt von P ist, ist $c = 1$ und A wird von P zentralisiert, ein Widerspruch, denn P operiert treu auf A. □

(6.2.5.2.7) Lemma.

P ist konjugiert zur Körperautomorphismengruppe von G_0.

Beweis. Es bezeichne $\overline{\ }$ den natürlichen Homomorphismus von $Aut(G_0)$ auf die äußere Automorphismengruppe $Out(G_0)$. Jeder Automorphismus ist Produkt eines inneren-, Diagonal, Körper- und Graphautomorphismus. Da die Graphautomorphismen von G_0 von der Ordnung 2 oder 3 sind, ist

$$1 \neq \overline{P} \leq \overline{HAut(k)} =: \overline{M},$$

wobei H die Gruppe der äußeren Diagonalautomorphismen von G_0 ist.

Die Ordnung der Gruppe $\overline{H}$ ist ein Teiler von 2, 3, 2^2 oder $q \pm 1$. Letzteres lesen wir aus dem Atlas [8] ab. Da r eine von 2 und 3 verschiedene Primzahl ist, gilt

$$2^r \equiv 2 \mod r$$

nach dem kleinen Satz von Fermat. Insbesondere ist also

$$r \nmid 2^r - 1 = q - 1$$

und auch

$$r \nmid (2^r - 2) + 3 = 2^r + 1 = q + 1.$$

Somit schneiden sich $\overline{H}$ und $\overline{Aut(k)}$ trivial und daher ist $\overline{P}$ als r-Sylowgruppe von $\overline{HAut(k)}$ zu $\overline{Aut(k)}$ konjugiert. Wird P von x und $Aut(k)$ von φ erzeugt, so ist x nach Konjugation und obigem Lemma enthalten in der Nebenklasse $G_0\varphi$. Nach dem Satz von Lang (vgl. (7.2) von Gorenstein & Lyons [15]) ist dann x zu φ konjugiert, wie gewünscht. □

(6.2.5.2.8) Bemerkung.

Die obige Aussage liefert, dass wir P als Körperautomorphismengruppe von G_0 auffassen können, indem wir P auf die Körperautomorphismengruppe konjugieren. Der Diagonalautomorphismus von B_2 bzw. F_4 in gerader Charakteristik bildet die langen auf die kurzen Wurzelelemente ab. Da aber P und die Körperautomorphismengruppe in der von G_0 und den Körper- und Diagonalautomorphismen erzeugten Gruppe konjugiert sind, ist gewährleistet, dass auch weiterhin D und E nur lange Wurzelelemente enthalten.

Ist Φ das Wurzelsystem von G_0 und

$$R := \langle a_r(1) \mid r \in \Phi \rangle,$$

dann ist R eine Lie-Typ-Gruppe über dem Primkörper vom gleichen Typ wie G_0. Nach obiger Bemerkung gilt nun o.B.d.A. sogar

$$R \leq C_{G_0}(P) \leq G_\alpha,$$

wobei wir die hintere Abschätzung aus 6.2.2.5 erhalten. Insbesondere sind nun die langen Wurzelelemente von R sämtlich in E enthalten, denn

$$D \cap R \leq D \cap G_\alpha = E.$$

Die Elemente von E sind nun aber nach 6.2.5.1.2 paarweise nicht vertauschbar, also ist Φ ein Wurzelsystem vom Typ A_1. Nun sind R und G_0 offenbar vom gleichen Lie-Typ, also ist G_0 eine der Gruppen $SL_2(k)$ oder $PSU_3(k)$. Dabei ist G_0 verschieden von $SL_2(k)$, denn sonst ist $C_{G_0}(P) = SL_2(2) = D_6$, ein Widerspruch.

Es bleibt also nur der Fall, in dem $G_0 = PSU_3(k)$. Wir zeigen zuerst, dass $C_{G_0}(P) = PSU_3(2)$. Sei dazu $x \in P$ die Frobeniusabbildung von k und σ der Automorphismus $a \longmapsto a^q$ von $GF(q^2)$. Dann ist $Z := Z(SU_3(k))$ die Menge der Matrizen aI_3 mit $a^3 = 1$ und $aa^\sigma = a^{q+1} = 1$. Da r ungerade ist, sehen wir leicht, dass Z von der Ordnung $(3, q+1) = 3$ ist. Ist $\overline{A}$ eine Matrix in $C_{G_0}(P)$, so gilt notwendig

$$A^x = aA$$

für ein a mit $aI_3 \in Z$. Ist b ein Eintrag von A, so ist also

$$b^2 = b^x = ab.$$

Insbesondere nehmen die Einträge von A also nur die Werte 0 oder a an, und es folgt nun offenbar

$$C_{G_0}(P) = PSU_3(2).$$

Sei S die zu $GF(3)^2$ isomorphe 3-Sylowgruppe von $PSU_3(2)$. Eine Matrizenrechnung zeigt

$$C_{G_0}(S) = S,$$

und daher ist $|N_{G_0}(S)|$ wegen

$$N_{G_0}(S)/C_{G_0}(S) \leq GL_2(3)$$

höchstens ein Teiler von $2^4 \cdot 3^3$. Nun ist P wegen der Nilpotenz von X charakteristisch in X und somit wird P von G_α normalisiert. Insbesondere ist

$$(G_0)_\alpha \leq N_{G_0}(C_{G_0}(P)) \leq N_{G_0}(S).$$

Benutzen wir die Bahnformel, so erhalten wir

$$m = |G_0 : (G_0)_\alpha| \geq \frac{|G_0|}{2^4 \cdot 3^3} = \frac{q^3(q^2-1)(q^3+1)}{2^4 \cdot 3^4}.$$

Anderseits ist $X \cap G_0$ eine $2'$-Untergruppe von $N_{PSU_3(q)}(S)$, also ist $|X \cap G_0| \leq 3^3$. Weiterhin ist die Ordnung

$$X/(X \cap G_0) \cong XG_0/G_0 \leq Out(G_0)$$

ein Teiler von $6r$. Da die $2'$-Gruppe X transitiv auf Ω^* operiert, ist

$$m \leq |X| + 1 \leq 3^4 r + 1.$$

Setzen wir beide Abschätzungen zusammen, so ergibt sich

$$2^{3r}(2^{2r}-1)(2^{3r}+1) \leq (3^4 r + 1)2^4 3^4$$

und dies ist wegen $r \geq 5$ offenbar ein Widerspruch.

Somit war unsere letzte Annahme, dass X eine r-Sylowgruppe mit $r > 3$ enthält, falsch. Notwendig ist nun X eine 3-Gruppe und insbesondere ist m wegen der Transitivität von X auf Ω^* von der Form

$$m = 3^s + 1.$$

Nun ergibt sich die fast triviale

(6.2.5.2.9) Folgerung.

Der 2-Anteil von m ist 2 oder 2^2.

Beweis. Wäre $8 \mid m = 3^s+1$, so wäre wegen $3^s+1 = 3^2(3^{s-2}+1)-8$ auch $8 \mid 3^{s-2}+1$. Sukzessive erhalten wir $8 \mid 3+1$ oder $8 \mid 3^2+1$, ein Widerspruch. □

Wir können nun direkt die Abschätzungen für $|M_A|$ aus 6.2.2.2 benutzen und erhalten, dass G_0 höchstens eine der linearen Gruppen $PSL_2(2^f)$ mit $2 \leq f \leq 5$ oder die Gruppe $PSp_4(q)$ ist. Letztere haben wir bereits ausgeschlossen, also bleiben nur die obigen linearen Gruppen mit $m = 3^s + 1$. Eine Inspektion der Dicksonliste zeigt, dass dies nur für die Gruppen $PSL_2(4)$ mit $m = 3^2+1$, $PSL_2(8)$ mit $m = 3^3+1$ möglich ist. In beiden Fällen ist $(G_0)_\alpha$ eine Diedergruppe und wir sehen leicht, dass $D_e = (G_0)_\alpha$, ein Widerspruch. Somit war auch unsere erste Annahme falsch und wir haben gezeigt, dass dieser Fall nicht eintritt.

6.2.5.3 Die auftretenden Beispiele

Wie in den entsprechenden Beispielen aus dem Hauptsatz *sei nun D_e eine Diedergruppe* für ein $e \in E$. Relativ leicht werden wir hier die Beispiele aus dem Hauptsatz erhalten. In D_e ist e^X nach 6.2.1.3 die Menge der Involutionen und diese sind in D_e zueinander konjugiert. Daher gibt es eine von e verschiedene Involution $f \in e^X$ mit $D_e = \langle e, f\rangle$. In den Beispielen ist G_0 gerade die Gruppe

$$Y := \langle E(e), E(f)\rangle \cong SL_2(q),$$

und wir erhalten zunächst das

(6.2.5.3.1) Lemma.

X normalisiert Y und Y operiert transitiv auf Ω. Insbesondere ist $X \leq Aut(Y)$.

Beweis. Da in $\langle e, f\rangle$ sämtliche Involutionen konjugiert sind, gibt es zu $x \in X$ ein $y \in Y$ mit $e^x = e^y$. Nach 6.2.2.4 ist A^G eine TI-Menge und E ist invariant unter Konjugation mit X. Daher ist

$$E(e)^x = E(e^x) = E(e^y) = E(e)^y \leq Y.$$

Analog ist $E(f)^x \leq Y$ und daher operiert X auf Y. Insbesondere ist XY eine Gruppe. Sicherlich ist $Y \not\leq G_\alpha$, denn $|E(e)| > 2$ und e ist nach 6.2.1.4 das einzige Wurzelelement von $E(e)$ in G_α. Es ist nun wegen $X \leq G_\alpha$ klar, dass die Gruppe XY zweifach transitiv auf Ω operiert und somit muss auch Y wenigstens transitiv auf Ω sein. Insbesondere stabilisiert $C_X(Y)$ ziffernweise die Menge $\alpha^Y = \Omega$. Somit ist $C_X(Y) = 1$ und es folgt die Behauptung. □

Insbesondere ist

$$XAut(k)/Aut(k) \cong X/(X \cap Aut(k))$$

eine nilpotente $2'$-Untergruppe von

$$Aut(Y)/Aut(k) \cong Y$$

und nach der Dicksonliste somit zyklisch der Ordnung $s \mid q \pm 1$. Für $q = 2^f$ gilt also offensichtlich

$$|X| \Big| (q \pm 1) \cdot |X \cap Aut(k)| \leq (q+1)f. \tag{6.7}$$

Wegen $1 \neq [e, X] \leq X \cap Y$ ist $X \cap Y$ ein nichttrivialer nilpotenter $2'$-Normalteiler von Y_α und nach der Dicksonliste zyklisch mit

$$|X \cap Y| \Big| q \pm 1.$$

Die Normalisatoren dieser zyklischen Untergruppen sind die Diedergruppen $D_{2(q\pm1)}$, also ist

$$Y_\alpha \leq N_Y(X \cap Y) \cong D_{2(q\pm1)}. \tag{6.8}$$

Damit folgt schließlich der

(6.2.5.3.2) Satz.

Es ist $G_0 = Y$ wie in 4.1 (e) mit $m = 6$ oder (f) mit $m = 28$.

Beweis. Durch die Abschätzung aus (6.8) erhalten wir

$$|Y : Y_\alpha| \geq \frac{q(q-1)}{2},$$

denn $|Y| = q(q^2 - 1)$. Nun operiert Y transitiv auf Ω, also liefert die Bahnformel zusammen mit (6.7) die Abschätzung

$$\frac{q(q-1)}{2} - 1 \leq |Y : Y_\alpha| - 1 = m - 1 \leq |X| \leq (q+1)f. \tag{6.9}$$

Für $q > 8$ ist $f < \frac{q-2}{2}$ und dies führt sofort zu einem Widerspruch.

Ist $q = 4$, so ist $Aut(k)$ eine Gruppe der Ordnung 2 und daher ist $X \cap Aut(k) = 1$. Verfeinern wir die Abschätzung (6.9) mit (6.7), so erhalten wir

$$5 \leq |Y : Y_\alpha| - 1 \leq |X| \leq 5.$$

Da Y transitiv auf Ω operiert, ist also $m = 6$ und X regulär auf 5 Ziffern. Der 2-Anteil von m ist 2, also erhalten wir nach 6.2.2.2 gerade $|M_{E(e)}| \leq 2^4$ oder $G_0 = Sp_4(4)$. Letzteres jedoch wie oben wegen $|e^X| \geq 3$ nicht möglich. Wie im vorangegangenen Abschnitt ist dies wegen $q = 4$ nur für $G_0 = Y$ möglich.

Im Fall $q = 8$ erhalten wir aus (6.9) nun

$$27 \leq |Y : Y_\alpha| - 1 \leq |X| \leq 27.$$

Wie eben ist also $m = 28$ und X regulär auf 27 Ziffern. Ferner ist

$$Y_\alpha \cong D_{18}.$$

Der 2-Anteil von m ist 2^2, also folgt wie eben $|M_{E(e)}| \leq 2^5$ oder $G_0 = PSp_4(8)$, wobei letzteres offenbar nicht möglich ist. Wegen $q = 8$ führt dies nur auf den Fall $G_0 = Y$. Die Behauptung ist nun wieder klar. □

6.2.6 Der Fall $E \neq \emptyset$ mit $p = 3$

Wir nehmen wieder $E \neq \emptyset$ an und werden in diesem Abschnitt anders als im Fall der geraden Charakteristik von k keine weiteren Beispiele für den Hauptsatz erhalten. Sei $e \in E$ und $A := E(e)$. Die Gruppe $\langle e^X \rangle = \langle e \rangle [X, e]$ bezeichnen wir wieder mit D_e. Obwohl D keine Menge von Wurzelinvolutionen ist, wird das Vorgehen dem aus dem Fall $q = 2$ ähnlich sein. Wir übernehmen die Bezeichnungen der Fixpunktmengen von dort.

(6.2.6.1) Lemma.

Für $e^x \in e^X \setminus \{e\}$ ist $\langle e, e^x \rangle \cong (P)SL_2(3)$. Insbesondere ist $[X, e] = O_2(D_e)$ und $D_e = \langle e \rangle O_2(D_e)$.

Beweis. Ist $e^x \in e^X \setminus \{e\}$, dann ist $\langle e, e^x \rangle \leq D_e$ offenbar eine auflösbare Untergruppe von

$$\langle A, A^x \rangle \cong \begin{cases} PSL_2(k), & \text{wenn } G_0 \cong PSL_2(k), \\ SL_2(k), & \text{sonst.} \end{cases}$$

Die Elemente e und e^x sind von der Ordnung drei und

$$e^2 e^x = [e, x] \in X$$

hat eine $3'$-Ordnung. Nach der Dicksonliste ist dann $\langle e, e^x \rangle$ die Gruppe $SL_2(3)$ bzw. $PSL_2(3)$. Insbesondere ist $[e, x] = e^2 e^x$ von 2-Potenzordnung und wegen der Nilpotenz von X ist $[X, e]$ eine 2-Gruppe. □

(6.2.6.2) Lemma.

Für $G_0 \ncong PSL_2(k)$ ist $D_e \cong SL_2(3)$ und für $G_0 \cong PSL_2(k)$ ist $D_e \cong PSL_2(3)$.

Beweis. Ist $G_0 \cong PSL_2(k)$, so lesen wir die Behauptung direkt aus der Dicksonliste ab und es bleiben die übrigen Gruppen zu betrachten. Wir überprüfen einfach die Voraussetzungen zu 3.6.1. Nach 3.2.2.5 und 3.3.1 besitzt jede Gruppe

$$Y = \langle A, A^x \rangle \cong SL_2(k)$$

mit $e^x \in e^X \setminus \{e\}$ eine zentrale Involution i_x und es bleibt offenbar nur noch zu zeigen, dass $\langle e, e^x\rangle$ von $C_{O_2(D_e)}(i_x)$ normalisiert wird, denn $\langle e, e^x\rangle \cong SL_2(3)$ nach 6.2.6.1.

Nach der Dedekindidentität ist

$$Y \cap D_e = Y \cap \langle e\rangle O_2(D_e) = \langle e\rangle (Y \cap O_2(D_e)),$$

und nach der Dicksonliste ist dann sofort

$$Y \cap D_e = \langle e, e^x\rangle. \tag{6.10}$$

Sei nun $z \in C_{O_2(D_e)}(i_x) \leq X$. Nach 3.5.2 ist dann $Y^z \trianglelefteq L_A Y$.

Für $q = 3$ operiert $\langle e\rangle$ auf der Menge der vier 3-Sylowgruppen von Y^z und normalisiert daher mindestens eine davon. Nach der Bahnformel wird eine solche Untergruppe P (der Ordnung 3) sogar von e zentralisiert. Wegen $Y^z \leq D_e$ wird P von e^u für ein $u \in X$ erzeugt und

$$e^2 e^u = [e, u] \in [X, e]$$

ist von der Ordnung 1 oder 3. Da X eine $3'$-Gruppe ist, erhalten wir $e = e^u \in Y^z$. Wegen $D_e = D_{e^x}$ folgt analog $e^x \in Y^z$ und daher $Y = Y^z$, wie gewünscht. (Hier ist sogar $Y = \langle e, e^x\rangle$.)

Sei nun $q > 3$. Dann sind Y und Y^z Komponenten von $L_A Y$ und verschiedene Komponenten vertauschen miteinander. Ist $Y \neq Y^z$, so ist insbesondere

$$e^2 e^z = [e, z] \in [X, z]$$

von der Ordnung 1 oder 3. Da X eine $3'$-Gruppe ist, folgt $e = e^z$ und analog $e^x = (e^x)^z$, wie gewünscht. Ist $Y = Y^z$, so normalisiert z nach (6.10) die Gruppe $\langle e, e^x\rangle$. Die Behauptung ist damit bewiesen. □

Wir sind nun in der Lage, die Sätze über die Fixpunktmengen aus dem Fall $q = 2$ auf diese Situation zu übertragen, um den genauen 3-Anteil von m anzugeben. In allen Fällen ist nun

$$D_e = \langle e, e^x\rangle \cong (P)SL_2(3)$$

für alle $x \in X$ invariant unter X. Wegen der Transitivität von X auf Ω^* ist Ω^* die *disjunkte* Vereinigung der vier Mengen $Fix(e^x)^*$ für $x \in X$.

Als Voraussetzung für die Anwendung von 6.2.4.6 brauchen wir noch $M_A \not\leq G_\alpha$. Dies ist offenbar stets erfüllt, wenn G_0 verschieden von $PSL_2(3)$ ist, denn $A \cap G_\alpha$ ist die einzige Untergruppe der Ordnung 3 von $M_A \cap G_\alpha$. Der Fall $G_0 = PSL_2(3)$ tritt aber offensichtlich nicht auf.

Daher operiert M_A transitiv auf $Fix(e)$ und diese Menge hat daher 3-Potenzordnung. Es folgt schließlich

$$m = 4 \cdot 3^l - 3$$

mit $3^l = |M_A : M_A \cap G_\alpha|$, und der 3-Anteil von m ist somit 3 oder 3^2. Wir beachten dabei, dass $|M_A \cap G_\alpha| \leq 3^2$.

Ist G_0 eine lineare Gruppe, so ist nach 6.2.2.3 gerade $|M_A| \leq 3^4$ und dies führt nur auf die linearen Gruppen $PSL_2(3^f)$ mit $2 \leq f \leq 4$ und $m = 9, 33$ oder 105. In den beiden letzten Fällen ist ein Primteiler von m oder $m-1$ kein Teiler von $|G_0|$ bzw. $|G|$, also ist nur der Fall $m = 9$ zu betrachten. Hier ist aber m der 3-Anteil von G_0, ein Widerspruch, da $(G_0)_\alpha$ das Wurzelelement e der Ordnung 3 enthält.

Sei nun G_0 keine lineare Gruppe. Dann hat D_e eine zentrale Involution i. Insbesondere ist $X \leq C(i)$ und nach 6.2.2.5 auch $A \leq C(i) \leq G_\alpha$. Nach 6.2.1.4 führt uns dies sofort auf den Fall $q = 3$. Der 3-Anteil von m ist wieder 3 oder 3^2 und daher ist $|M_A| \leq 3^4$ oder $s \leq 2$ nach 6.2.2.2. Somit ist G_0 eine der Gruppen $PSL_3(3)$, $PSU_3(3)$ oder $P\Omega_5(3) \cong PSp_4(3)$ ist. Dort ist M_A von der Ordnung 3^3 und dies führt auf die Fälle $m = 33$ oder 9. Im ersten Fall ist $11 \nmid |G_0|$, ein Widerspruch. Für $m = 9$ ist $|M_A \cap G_\alpha| = 3^2$. Bei den Gruppen $PSL_3(3)$ und $PSU_3(3)$ ist 3^3 gerade der 3-Anteil von $|G_0|$ und daher hat m wegen $m = |G_0 : (G_0)_\alpha|$ den 3-Anteil 3, ein Widerspruch. Schließlich hat $PSp_4(3)$ keine transitive Permutationsdarstellung vom Grad 9.

Insbesondere war unsere erste Annahme falsch und somit enthält G_α keine langen Wurzelelemente von G_0. Natürlich hätten wir m im Fall $G_0 \cong PSL_2(k)$ direkt aus der Dicksonliste ablesen können. Da obige Argumente aber anwendbar waren, hat uns dies aber etwas Rechnung erspart.

6.2.7 Fixpunktfreie Elemente

Schließlich bleibt die Situation zu betrachten, in der die Wurzelelemente aus D fixpunktfrei auf Ω operieren. Wir betrachten ab hier wieder den Körper k in beliebiger Charakteristik p. Das Ziel dieses Abschnittes ist es, für die Gruppe $A \in \Sigma$ bis auf eine Ausnahme die Relation

$$m - 1 \mid |G_0 : N_{G_0}(A)| \cdot (q-1)$$

zu beweisen. Für die folgenden Argumente sei A o.B.d.A. die abstrakte Wurzeluntergruppe zur höchsten Wurzeluntergruppe A_h. Unabhängig davon zeigen wir aber zunächst das

(6.2.7.1) Lemma.

Sei Ω eine endliche Menge der Ordnung m und sei G eine zweifach transitive Permutationsgruppe auf Ω mit einem fixpunktfreien Element x. Dann ist $m - 1 \mid |G : C(x)|$.

Beweis. Die Operationen von G_α auf Ω^* und $\{G_\alpha h \mid h \notin G_\alpha\}$ sind äquivalent. Da G_α transitiv auf Ω^* operiert, sind insbesondere die Mengen $x^G \cap G_\alpha h$ mit $h \notin G_\alpha$ konjugiert und damit von gleicher Ordnung.
Nun ist

$$G = \dot{\bigcup_{h \in G}} G_\alpha h.$$

Nach Voraussetzung ist x fixpunktfrei auf Ω, also ist offenbar $x^G \cap G_\alpha = \emptyset$. Demnach erhalten wir

$$x^G = \dot{\bigcup_{h \notin G_\alpha}} (x^G \cap G_\alpha h).$$

Wegen $|G : G_\alpha| = m$ ist nun klar, dass

$$(m-1) \cdot |x^G \cap G_\alpha h| = |x^G| = |G : C(x)|,$$

wie gewünscht. □

Wir wenden uns nun wieder der ursprünglichen Situation zu. Nach Voraussetzung operiert $a \in A^\sharp$ fixpunktfrei auf Ω. Verwenden wir nun 6.2.7.1, so erhalten wir sofort $m-1 \mid |G : C(a)|$. Wir haben in 6.2.2.4 gezeigt, dass $C(a) \leq N(A)$, also formen wir dies um zu

$$m-1 \mid |G : N(A)| \cdot |N(A) : C(a)|. \tag{6.11}$$

Wir erreichen nun leicht unser Ziel, wenn wir die beiden Faktoren auf der rechten Seite untersuchen. Die Gruppen vom Typ F_4 oder B_2 in gerader Charakteristik und G_2 in Charakteristik 3 fassen wir zur Menge $\mathfrak{S}$ zusammen. Ist $G_0 \notin \mathfrak{S}$, so ist Σ invariant unter G und daher $A^G = A^{G_0}$. Ist $G_0 \in \mathfrak{S}$, so ist Σ entweder invariant unter G_0, oder

$$A^G = A^{G_0} \dot{\cup} A_s^{G_0}$$

für eine kurze Wurzel s. Aus der Bahnformel folgt das

(6.2.7.2) Lemma.

Es ist $|G : N(A)| \mid 2 \cdot |G_0 : N_{G_0}(A)|$. *Der Faktor* 2 *taucht höchstens für die Gruppen* $G_0 \in \mathfrak{S}$ *auf.*

(6.2.7.3) Lemma.

Es ist $|N(A) : C(a)| \mid q-1$.

Beweis. Im weiteren Verlauf sei B die abstrakte Wurzeluntergruppe zu A_{-h} und $Y = \langle A, B \rangle$. Nach der Bahnformel erhalten wir sofort

$$|N(A) : C(a)| = |a^{N(A)}| = |a^{N(A)} \cap A|.$$

Nun ist offenbar $a^{N(A)} \cap A$ invariant unter Konjugation mit $N_Y(A)$ und wir können diese Menge in disjunkte Bahnen unter $N_Y(A)$ zerlegen. Mit Matrizen rechnen wir nun in

$$(P)SL_2(k) \cong Y$$

für $b \in a^{N(A)} \cap A$ leicht nach, dass

$$|b^{N_Y(A)}| = |N_Y(A) : C_Y(b)| = \frac{q-1}{ggT(2, q-1)}.$$

Nun hat $A^\sharp$ nur $q-1$ Elemente, also enthält $b^{N_Y(A)} = a^{N(A)} \cap A$ genau $\frac{q-1}{ggT(2,q-1)}$ Elemente oder $a^{N(A)} \cap A$ ist die Vereinigung von zwei Bahnen der Länge $\frac{q-1}{2}$. In jedem Fall aber folgt die Behauptung. □

Setzen wir die beiden letzten Lemmata mit (6.11) zusammen, so erreichen wir schließlich unser Ziel. Der Faktor 2 in Lemma 6.2.7.2 spielt dabei einzig für die Gruppe vom Typ G_2 in Charakteristik 3 eine Rolle. Für die anderen Gruppen in $\mathfrak{S}$ ist nämlich X eine $2'$-Gruppe und somit enthält $m-1$ keinen Faktor 2. Wir erhalten also die

(6.2.7.4) Folgerung.

Es ist $m-1 \mid 2(q-1) \cdot |G_0 : N_{G_0}(A)|$. *Der Faktor* 2 *taucht höchstens auf, wenn* G_0 *vom Typ* G_2 *in Charakteristik* 3 *ist.*

6.2.8 Fahnentransitive Untergruppen

Die Relation aus Folgerung 6.2.7.4 wird zeigen, dass wir keine weiteren Beispiele für den Hauptsatz 4.1 erhalten, wenn m keine p-Potenz ist. Ist m jedoch eine p-Potenz, so ist diese Relation völlig nutzlos und wir müssen diesen Fall separat behandeln. Wir erhalten das

(6.2.8.1) Lemma.

Ist m *eine* p*-Potenz, so ist* G_0 *wie in (e), (f) oder (g) von Hauptsatz 4.1.*

Den Beweis erhalten wir leicht, wenn wir die beiden folgenden Fälle unterscheiden.

(6.2.8.2) Die Gruppen $PSL_2(k)$ und $PSU_3(k)$.

Aus der Liste der maximalen Untergruppen dieser Gruppen in Bloom [3], Hartley [16], Mitchell [28], Walter [39] und der Dicksonliste sehen wir, dass höchstens die Gruppen aus Tabelle 6.3 auftauchen können. Der Fall (a) ist offenbar der Fall (e) mit $m = 5$ aus dem Hauptsatz 4.1. In (c) wäre $X \cap (G_0)_\alpha = 1$, was offenbar nicht möglich ist, da X selbstzentralisierend ist. In (d) ist $X \cap (G_0)_\alpha \leq V_4$ und $Out(G_0) = 2$, also ist X eine 2-Gruppe. Wegen $m-1 \mid |X|$ ist dies nicht möglich.

(6.2.8.3) Die Gruppen vom Lie-Rang mindestens 2.

Sei G_1 die von G_0, den Körperautomorphismen und Diagonalautomorphismen von G_0 erzeugte Untergruppe. Ist $G_0 \leq G^* \leq G_1$, so besitzt G^* eine BN-Paar mit einer Boreluntergruppe B. Eine Untergruppe L von G^* mit $G^* = BL$ nennen wir eine

	G_0	$(G_0)_\alpha$	m
(a)	$PSL_2(5)$	A_4	5
(c)	$PSL_2(11)$	A_5	11
(d)	$PSL_2(7)$	Σ_4	7

Tabelle 6.3: Die Gruppen G_0 vom Lie-Rang 1 mit m als p-Potenz

fahnentransitive Untergruppe von G^*. Die Gruppen (vom irreduziblen Typ und vom Lie-Rang mindestens 2) mit fahnentransitiven Untergruppen sind von SEITZ [31] klassifiziert worden, wobei in dieser Klassifikation von SEITZ allerdings Fälle fehlen. Eine korrigierte Liste finden wir etwa in (2.1) und (2.2) bei MEIXNER [27]. Wir zeigen, dass $(G_0)_\alpha$ eine fahnentransitive Untergruppe von G_0 ist.

Da G_0 transitiv auf Ω operiert, enthält $|(G_0)_\alpha|$ nach der Bahnformel den kompletten p'-Anteil von $|G_0|$. Sicherlich ist U_0 eine p-Sylowgruppe von $(G_0)_\alpha$, also ist wegen

$$|U_0(G_0)_\alpha| = \frac{|U_0||(G_0)_\alpha|}{|(G_0)_\alpha \cap U_0|}$$

auch

$$G_0 = U_0(G_0)_\alpha.$$

Insbesondere ist $(G_0)_\alpha$ eine fahnentransitive Untergruppe von G_0. Wir können nun die oben zitierte Klassifikation verwenden, wobei wir natürlich nur die fahnentransitiven Untergruppen einfacher Gruppen auflisten. Nach dieser ist entweder

$$G_0 = \langle U_0^{G_0} \rangle \leq (G_0)_\alpha$$

– was offenbar nicht möglich ist – oder $G_0 = PSL_3(2) \cong PSL_2(7)$ mit $(G_0)_\alpha = 7 \cdot 3$ oder $G_0 = PSp_4(3)$ mit $(G_0)_\alpha = 2^4 \cdot A_5$. Im zweiten Fall ist $m = 3^3$ und dies ist wegen $m - 1 \mid |X|$ nicht möglich. Der erste Fall führt leicht auf den Fall (g) aus dem Hauptsatz 4.1.

6.2.9 Der Fall $E = \emptyset$

In diesem letzten Unterabschnitt untersuchen wir die Operation der unipotenten Radikale M_A für $A \in \Sigma$ auf Ω. Wir nehmen nun an, dass D *fixpunktfrei auf* Ω *operiert* und dass m *keine p-Potenz ist.*

(6.2.9.1) Die von $G_2(3^f)$, $F_4(2^f)$ und $Sp_4(2^f)$ verschiedenen Gruppen.

Das folgende Argument ist für alle Gruppen das selbe. Wir zerlegen die Menge Ω unter der Operation von M_A in Bahnen der Länge

$$|\alpha^{M_A}| = |M_A : M_A \cap G_\alpha|.$$

G_0	Anhang	s	$\lvert G_0 : N_{G_0}(A_h)\rvert \cdot (q-1)$
$A_l(q)$	C.2	l	$\frac{(q^l-1)(q^{l+1}-1)}{q-1}$
$B_l(q)$, $l \geq 2$, q ungerade	C.3	$2l-2$	$\frac{(q^{2l}-1)(q^{2l-2}-1)}{q^2-1}$
$B_l(q)$, $l > 2$, q gerade	C.3	$2l-3$	$\frac{(q^{2l}-1)(q^{2l-2}-1)}{q^2-1}$
$C_l(q)$, $l \geq 2$, q ungerade	C.15	l	$q^{2l}-1$
$D_l(q)$, $l \geq 4$	C.4	$2l-3$	$\frac{(q^l-1)(q^{l-1}+1)(q^{l-1}-1)(q^{l-2}+1)}{q^2-1}$
$E_6(q)$	C.5	11	$\frac{(q^4+1)(q^9-1)(q^{12}-1)}{q^3-1}$
$E_7(q)$	C.6	17	$\frac{(q^{14}-1)(q^6+1)(q^{18}-1)}{q^4-1}$
$E_8(q)$	C.7	29	$\frac{(q^{10}+1)(q^{24}-1)(q^{30}-1)}{q^6-1}$
$F_4(q)$	C.8	8	$(q^4+1)(q^{12}-1)$
$G_2(q)$, $3 \nmid q$	C.9	3	q^6-1
${}^2E_6(q)$	C.10	11	$\frac{(q^4+1)(q^9+1)(q^{12}-1)}{q^3+1}$
${}^3D_4(q)$	C.11	5	$(q^2-1)(q^8+q^4+1)$
${}^2D_l(q)$, $l \geq 4$	C.12	$2l-3$	$\frac{(q^l+1)(q^{l-1}+1)(q^{l-1}-1)(q^{l-2}-1)}{q^2-1}$
${}^2A_{l-1}(q)$, l gerade	C.13	$l-1$	$\frac{(q^l-1)(q^{l-1}+1)}{q+1}$
${}^2A_{l-1}(q)$, l ungerade	C.14	$l-1$	$\frac{(q^l+1)(q^{l-1}-1)}{q+1}$

Tabelle 6.4: Die Zahlen $\lvert G_0 : N_{G_0}(A_h)\rvert \cdot (q-1)$

Nun ist wegen $M_A' \leq A$ stets $M_A \cap G_\alpha$ eine abelsche Untergruppe von M_A und somit ist

$$q^s \mid |M_A : M_A \cap G_\alpha|$$

für die Zahlen s aus den Tabellen 3.2 und 3.5 von Kapitel 3 bzw. $s = 1$ für die Gruppe $G_0 = PSL_2(q)$. Insbesondere ist $m = q^s x$, wobei $1 \neq x$ keine p-Potenz ist. Setzen wir diese Informationen in 6.2.7.4 ein, so folgt

$$q^s x - 1 \mid (q-1) \cdot |G_0 : N_{G_0}(A)|. \tag{6.12}$$

Die Indizes geben wir in Tabelle 6.4 an. Mit Anhang C sehen wir nun sofort, dass (6.12) nicht erfüllt sein kann.

(6.2.9.2) Die Gruppen $G_2(3^f)$ und $F_4(2^f)$.

Die Menge Δ der kurzen Wurzeluntergruppen ist unter dem Diagrammautomorphismus zu Σ konjugiert und somit eine Klasse von k-Wurzeluntergruppen von G_0. Insbesondere können wir annehmen, dass G_α auch keine kurzen Wurzelelemente enthält, die wir

zur Menge $D(\Delta)$ zusammenfassen. Nun ist $V = M_A/A$ ein natürlicher Modul für $L_A \cong Sp_6(2^f)$ oder $SL_2(3^f)$ und somit ist L_A transitiv auf $V^\sharp$. Natürlich ist dann $Z(M_A) = A(Z(M_A) \cap D(\Delta))$ und insbesondere $Z(M_A) \cap G_\alpha$ von der Ordnung höchstens q. Da G_α nämlich weder lange noch kurze Wurzelelemente enthält, sind die Elemente von $Z(M_A) \cap G_\alpha$ Produktelemente ab mit $a \in A^\sharp$ und $b \in Z(M_A)^\sharp \cap D(\Delta)$. Zu a ist dabei b eindeutig bestimmt, denn $A \leq Z(M_A)$.

Da $(M_A \cap G_\alpha)Z(M_A)/Z(M_A)$ ein isotroper Unterraum von $M_A/Z(M_A)$ ist, folgt im Beweis zu 3.2.3.1 leicht

$$|M_A : M_A \cap G_\alpha| \geq q^{\frac{dim(V)}{2}} |Z(M_A) : Z(M_A) \cap G_\alpha|$$

und dies liefert die Abschätzung $q^4 \mid m$ bzw. $q^{10} \mid m$. Dies liefert offenbar wie oben einen Widerspruch.

(6.2.9.3) Die Gruppen $Sp_4(2^f)$.

Den Fall $G_0 = Sp_4(2)' \cong A_6$ haben wir bereits im letzten Kapitel komplett behandelt, weswegen wir im folgenden stets $q > 2$ annehmen. Die Wurzeln r_1 und r_2 seien die fundamentalen Wurzeln des Wurzelsystems C_2 von Seite 9, und weiterhin seien $A_1 = A_{2r_1+r_2}$ und $A_2 = A_{r_1+r_2}$. Mit den Chevalley'schen Kommutatorrelation sehen wir $Z(S) = A_1A_2$ für eine 2-Sylowgruppe $S = A_{r_1}A_1A_2A_{r_2}$ von G_0.

Das Problem wird auch hier wieder sein, eine günstige obere Schranke für $M_{A_1} \cap G_\alpha$ oder alternativ $M_{A_2} \cap G_\alpha$ anzugeben. Wie im letzten Punkt enthält nun G_α auch keine kurzen Wurzelelemente, und daher ist offenbar

$$|A_1A_2 \cap G_\alpha| \leq q.$$

Angenommen, beide Gruppen $M_{A_i} \cap G_\alpha$ haben mindestens die Ordnung $4q$. Dann gilt für $i = 1, 2$ also

$$|M_{A_i} \cap G_\alpha : A_1A_2 \cap G_\alpha| \geq 4,$$

wobei hier $M_{A_1} = A_1A_2A_{r_1}$ und $M_{A_2} = A_1A_2A_{r_2}$. Insbesondere existieren in $M_{A_i} \cap G_\alpha$ Elemente der Form $x_{ij}a_{r_i}(t_{ij})$ für $j \leq 3$ und $i \leq 2$ mit $x_{ij} \in (A_1A_2)^\sharp$ und $t_{ij} \in k^*$ für festes i paarweise verschieden. Kommutatorbildung liefert nun wegen $x_{ij} \in Z(S)$ mit den Chevalley'schen Kommutatorrelationen zwei verschiedene Elemente

$$z_k := [x_{11}a_{r_1}(t_{11}), x_{2k}a_{r_2}(t_{2k})] = a_{r_1+r_2}(t_{11}t_{2k})a_{2r_1+r_2}(t_{11}^2t_{2k}),$$

mit $k = 1, 2$. Die zu V_4 isomorphe Gruppe $\langle z_1, z_2 \rangle$ operiert teilerfremd auf X und daher ist

$$X = \langle C_X(z) \mid z \in \langle z_1, z_2 \rangle^\sharp \rangle$$

nach VII (7.23) von Kurzweil [24]. Sei nun V der symplektische Vektorraum von Seite 36. Eine leichte Rechnung in der Operation von G_0 auf V zeigt, dass für $z = ab \in AB$ mit $a \in A^\sharp$ und $b \in B^\sharp$ gerade

$$C_V(z) = \ell$$

eine Gerade einer maximalen Fahne von V ist. Demnach ist X im Normalisator G_ℓ einer parabolischen Untergruppe von G_0 enthalten, welche der Stabilisator von ℓ ist. Da X transitiv auf Ω^* operiert, ist entweder $G_\ell \leq G_\alpha$ oder G_ℓ ist zweifach transitiv auf Ω. Im ersten Fall ist X wegen $X = F^*(G_\alpha)$ eine 2-Gruppe, und dies ist nach Voraussetzung ein Widerspruch. Im zweiten Fall ist jeder minimale (nicht einfache) Normalteiler von G_ℓ regulär auf Ω und somit ist m eine 2-Potenz, was wir im letzten Abschnitt behandelt hatten.

Insbesondere ist o.B.d.A. $|M_{A_1} \cap G_\alpha| \leq 2q$. Die Zerlegung von Ω in Bahnen unter der Operation von M_{A_1} liefert wie in den obigen Punkten $m - 1 = \frac{q^2}{2}x - 1$, wobei $1 \neq x$ eine p-Potenz ist. Dies ist nach C.16 aus Anhang C wie in den obigen Punkten nicht möglich, also ist G_0 keine symplektische Gruppe.

6.2.10 Die Ree- und Suzukigruppen und ${}^2F_4(k)$

Die Lie-Typ-Gruppen besitzen bis auf Ausnahmen eine Klasse von abstrakten Wurzeluntergruppen. Mit überwiegend abstraken Argumenten haben wir diese Gruppen in den vorangegangenen Abschnitten behandelt. Die Gruppen $G_0 := {}^2F_4(k)'$ und $Sz(k)$ für $k = GF(2^{2l+1})$, sowie $R(k)$ für $k = GF(3^{2n+1})$ besitzen keine solche Klasse von abstrakten Wurzeluntergruppen und die bereits benutzten Argumente lassen sich nicht ohne weiteres auf diese Gruppen ausdehnen. Unser Vorgehen wird daher hier ein anderes sein. Der Fall $G_0 = R'(3) \cong SL_2(8)$ führt mit der Dicksonliste direkt auf den Fall (f) in 4.1. Der Fall $G_0 = Sz(2)$ tritt wegen $X = F^*(G_\alpha)$ offensichtlich nicht ein. Für den Fall $G_0 = {}^2F_4(2)'$ entnehmen wir die maximalen Untergruppen aus dem Atlas [8], und erkennen, dass auch dieser Fall nicht eintritt.

In den übrigen Fällen interessieren wir uns für eine Liste der maximalen Untergruppen von G_0, um den Grad m der Permutationsdarstellung von G_0 auf Ω zu berechnen. Die maximale Untergruppe G_α von G ist dann höchstens die Erweiterung von $(G_0)_\alpha$ mit einem Körperautomorphismus und somit ist die Ordnung von G_α abschätzbar. Wir sehen dann aus Ordnungsgründen bzw. aus der Tatsache $X = F^*(G_\alpha)$ leicht, dass G_α nicht transitiv auf $m - 1$ Ziffern operieren kann. Uns interessieren hier aber nur die *lokalen Untergruppen* von G_0, also die maximalen Untergruppen mit auflösbarem Normalteiler, denn da X *selbstzentralisierend* ist, ist $X \cap (G_0)_\alpha$ ein *nichttrivialer*, nilpotenter Normalteiler von $(G_0)_\alpha$. Andernfalls sind $(G_0)_\alpha$ und X vertauschbar und damit $(G_0)_\alpha = 1$, im Widerspruch zur Maximalität von $(G_0)_\alpha$. Insbesondere ist $(G_0)_\alpha$ eine r-lokale Untergruppe von G_0 für eine Primzahl r, also eine maximale Untergruppe mit r-Normalteiler. Die im folgenden angegebenen Listen der maximalen Untergruppen verwenden teilweise den *Klassifikationssatz der endlichen einfachen Gruppen.* Aber dieser wird ausschließlich zur Bestimmung der nicht-lokalen Untergruppen eingesetzt, was uns hier nicht berührt.

Wir starten mit den Gruppen ${}^2F_4(k)$ und zitieren hier eine Arbeit von Malle [26]. Diese Arbeit benutzt eine Klassifikation der maximalen Tori von G_0 und der Konju-

giertenklassen der (halbeinfachen) Elemente von G_0.

Eine Klassifikation dieser maximalen Tori und Konjugiertenklassen finden wir bei SHINODA [32]. Die folgenden Bezeichnungen und Resultate übernehmen wir aus dieser Arbeit. Jeder maximale Torus von G_0 ist konjugiert zu einem von elf maximalen Tori $T_1, \ldots, T_{11}$, und Repräsentanten $t_0, \ldots, t_{17}$ der halbeinfachen Konjugiertenklassen können in diesen Tori gewählt werden. Die Normalisatoren und Zentralisatoren dieser Tori und Elemente finden wir in den Tabellen III und IV bei SHINODA [32].

Es gibt nur eine einzige Konjugiertenklasse von Elementen der Ordnung 3, nämlich die halbeinfache Klasse mit Repräsentant t_4. Dies führt direkt auf die Klassifikation der 3-lokalen Untergruppen. Jede solche Untergruppe L ist der Normalisator eines Elementes der Ordnung drei oder einer elementarabelschen Gruppe E der Ordnung neun. Im ersten Fall ist o.B.d.A. $L = N_{G_0}(\langle t_4 \rangle)$ und es ist $C_{G_0}(t_4) \cong 3 \cdot U_3(q)$. Dies führt leicht auf

$$L \cong 3 \cdot U_3(q) : 2.$$

Im zweiten Fall kann E in den maximalen Torus T_8 eingebettet werden, und es folgt $L = N_{G_0}(T_8)$.

Auch die Klassifikation der r-lokalen Untergruppen mit $r > 3$ steht eng im Zusammenhang mit den obigen maximalen Tori und den halbeinfachen Klassen von G_0. Die Ordnung der Weylgruppe enthält nicht den Primteiler r, also kann jedes direkte Produkt zyklischer r-Gruppen in einem maximalen Torus eingebettet werden. Ist E eine elementarabelsche r-Gruppe, so ist diese insbesondere in einem Torus $T \cong k^* \times k^*$ enthalten und somit ist offensichtlich E zyklisch der Ordnung r oder isomorph zu $\mathbb{Z}_r \times \mathbb{Z}_r$. Im ersten Fall ist ein Erzeuger von E konjugiert zu einem der Elemente t_1, t_2, t_5, t_7 oder t_9 mit Normalisatoren in Tabelle IV von SHINODA [32], oder $C_{G_0}(E)$ ist ein maximaler Torus T von G_0. Da r und die Ordnung der Weylgruppe teilerfremd sind, ist $N_{G_0}(E) \leq N_{G_0}(T)$ und es gilt offenbar Gleichheit. Es bleibt der Fall $E \cong \mathbb{Z}_r \times \mathbb{Z}_r$. Wieder ist $N_{G_0}(E) \leq N_{G_0}(T)$ für einen maximalen Torus T. Nicht alle Normalisatoren der elf maximalen Tori sind maximal und dies führt insgesamt auf die Liste der r-lokalen Untergruppen von G_0, die wir in den Propositionen (1.2) und (1.3) bei MALLE [26] finden.

(6.2.10.1) Satz.

Jede r-lokale Untergruppe von G_0 ist konjugiert zu einer der folgenden Untergruppen:

(1) $N_{G_0}(\langle t_4 \rangle) \cong 3 \cdot U_3(q) : 2$.

(2) $N_{G_0}(T_8) \cong (\mathbb{Z}_{q+1} \times \mathbb{Z}_{q+1}) : GL_2(3)$.

(3) $N_{G_0}(\langle t_1 \rangle) \cong (\mathbb{Z}_{q-1} : 2) \times {}^2B_2(q)$.

(4) $N_{G_0}(\langle t_2 \rangle) \cong (\mathbb{Z}_{q-1} : 2) \times L_2(q)$.

(5) $N_{G_0}(\langle t_5 \rangle) \cong (\mathbb{Z}_{q+1} : 2) \times L_2(q)$.

m	$\lvert G_\alpha\rvert \leq$
$\frac{1}{2}q^9(q-1)(q^2+1)(q^6+1)$	$2q^4(q^2-1)(q^3+1)$
$\frac{1}{48}q^{12}(q-1)^2(q^2+1)(q^6+1)(q^2-q+1)$	$48q(q+1)^2$
$\frac{1}{2}q^{10}(q+1)(q^2+1)(q^3+1)(q^6+1)$	$2q^3(q-1)^2(q^2+1)$
$\frac{1}{2}q^{11}(q^2+1)(q^3+1)(q^6+1)$	$2q^2(q-1)(q^2-1)$
$\frac{1}{2}q^{11}(q-1)(q^2+1)(q^2-q+1)(q^6+1)$	$2q^2(q+1)(q^2-1)$
$\geq \frac{1}{8}q^8(q^2-1)(q^3+1)(q^6+1)$	$8q^4(q-1)(q^2+1)$
$\geq \frac{1}{8}q^8(q^2-1)(q^3+1)(q^6+1)$	$8q^4(q-1)(q^2+1)$
$\frac{1}{16}q^{12}(q-1)(q^2+1)(q^3+1)(q^6+1)$	$16q(q-1)^2$
$\geq \frac{1}{384}q^{10}(q-1)(q^3+1)(q^4-1)(q^6+1)$	$384q^3$
$\geq \frac{1}{384}q^{10}(q-1)(q^3+1)(q^4-1)(q^6+1)$	$384q^3$
$\geq \frac{1}{36}q^{10}(q-1)(q^3+1)(q^4-1)(q^6+1)$	$36q^2$
$\geq \frac{1}{36}q^{10}(q-1)(q^3+1)(q^4-1)(q^6+1)$	$36q^2$

Tabelle 6.5: Permutationsgrade von ${}^2F_4(k)$

(6) $N_{G_0}(\langle t_7\rangle) \cong (\mathbb{Z}_{q-\sqrt{2q}+1} : 4) \times {}^2B_2(q)$.

(7) $N_{G_0}(\langle t_9\rangle) \cong (\mathbb{Z}_{q+\sqrt{2q}+1} : 4) \times {}^2B_2(q)$.

(8) $N_{G_0}(T_1) \cong (\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}) : D_{16}$.

(9) $N_{G_0}(T_6) \cong (\mathbb{Z}_{q-\sqrt{2q}+1} \times \mathbb{Z}_{q-\sqrt{2q}+1}) : [96]$.

(10) $N_{G_0}(T_7) \cong (\mathbb{Z}_{q+\sqrt{2q}+1} \times \mathbb{Z}_{q+\sqrt{2q}+1}) : [96]$.

(11) $N_{G_0}(T_{10}) \cong (\mathbb{Z}_{q^2-\sqrt{2}q^{\frac{3}{2}}+q-\sqrt{2q}+1} \times \mathbb{Z}_{q^2-\sqrt{2}q^{\frac{3}{2}}+q-\sqrt{2q}+1}) : 12$.

(12) $N_{G_0}(T_{11}) \cong (\mathbb{Z}_{q^2+\sqrt{2}q^{\frac{3}{2}}+q+\sqrt{2q}+1} \times \mathbb{Z}_{q^2+\sqrt{2}q^{\frac{3}{2}}+q+\sqrt{2q}+1}) : 12$.

Der Grad m der Permutationsdarstellung von G_0 auf Ω läßt sich nun mit der Bahnformel leicht ablesen oder abschätzen, wenn wir die offensichtlichen Abschätzungen

$$q \pm \sqrt{2q} + 1 \leq 2q$$
$$q^2 \pm \sqrt{2}q^{\frac{3}{2}} + q \pm \sqrt{2q} + 1 \leq 3q^2$$

benutzen. Die Gruppe G_α ist nach der Arbeit von Malle die Erweiterung von $(G_0)_\alpha$ mit einem Körperautomorphismus, dessen Ordnung wir mit q abschätzen. Es ergeben sich die Zahlen in Tabelle 6.5, aus denen wir ohne weiteren Kommentar erkennen, dass G_α nicht transitiv auf $m-1$ Ziffern operieren kann. Somit erfüllt keine der Reegruppen ${}^2F_4(k)$ den Hauptsatz 4.1.

Wir kommen nun zu den Reegruppen $R(k)$ für $k \neq GF(3)$ und zitieren hier eine Untergruppenliste aus Satz (C) von Kleidman [22], aus der wir natürlich nur die nicht-einfachen Gruppen angeben müssen. Dann ist $(G_0)_\alpha$ eine der Gruppen $[q^3] : \mathbb{Z}_{q-1}$, $2 \times L_2(q)$, $(2^2 \times D_{(1/2)(q+1)}) : 3$, $2^3 : 7 : 3$ oder $\mathbb{Z}_{q\pm\sqrt{3q}+1} : \mathbb{Z}_6$. Da X eine $3'$-Gruppe ist, ist der erste Fall unmöglich. In den übrigen Fällen schätzen wir G_α wieder mit $|(G_0)_\alpha|f$

ab, und aus der Tatsache $X = F^*(G_\alpha)$ folgt offensichtlich, dass keine der Reegruppen den Satz 4.1 erfüllt.

Schließlich zitieren wir für die Suzukigruppen den Satz 9 in der Arbeit von SUZUKI [33] und erhalten, dass $(G_0)_\alpha$ eine parabolische Untergruppe, eine Diedergruppe der Ordnung $2(q-1)$, oder $\mathbb{Z}_{q\pm\sqrt{2q}+1} : 4$ ist. Alle Fälle treten offenbar mit den gleichen Argumenten wie oben nicht auf.

Kapitel 7

Zweifach transitive Permutationsgruppen II

Eine endliche, zweifach transitive Permutationsgruppe besitzt stets einen eindeutig bestimmten minimalen Normalteiler, welcher (entweder) einfach oder elementarabelsch ist. Einführendes zu diesem Thema finden wir etwa in dem Buch von MORTIMER & DIXON [29]. Im Wesentlichen erhalten wir daraus und aus dem Hauptsatz 4.1 den folgenden

(7.1) Satz.

Sei G eine endliche, zweifach transitive Permutationsgruppe auf der Menge Ω und X ein auf $\Omega \setminus \{\alpha\}$ transitiver, nilpotenter Normalteiler von G_α. Weiterhin sei der oben beschriebene Normalteiler N eine bekannte Gruppe, wenn N einfach ist. Dann gilt einer der folgenden Fälle:

(a) $\langle X^G \rangle$ ist eine einfache Lie-Typ-Gruppe vom Lie-Rang 1 und X ist eine auf $\Omega \setminus \{\alpha\}$ reguläre p-Gruppe.

(b) $G = R(3) = R(3)'X$ und X ist eine auf $\Omega \setminus \{\alpha\}$ reguläre p-Gruppe.

(c) N operiert regulär auf Ω. Ferner ist $\langle X^G \rangle = NX$ scharf 2-fach transitiv auf Ω und X operiert regulär auf $\Omega \setminus \{\alpha\}$.

(d) N operiert regulär auf Ω. Ferner gilt $\langle X^G \rangle = G = NX$ und $|G| = 2r^2(r^2-1)$ für eine Mersenne'sche Primzahl r. Weiterhin ist $G_\alpha = X$ von der Ordnung $2(r^2-1)$ und $|G_{\alpha,\beta}| = 2$.

Ist N einfach und nicht zyklisch, dann ist wegen der Minimalität von N natürlich $C_G(N) = 1$ und daher offenbar $G \leq Aut(N)$. Aus dem Hauptsatz 4.1 erhalten wir dann sofort die ersten beiden Punkte des obigen Satzes, denn bis auf den Fall (f) von 4.1 ist stets $X \leq N$ und N ist nach Voraussetzung eine bekannte einfache Gruppe. Insbesondere müssen wir uns im folgenden nur noch mit dem Fall beschäftigen, in dem N eine elementarabelsche r-Gruppe für eine Primzahl r ist. In diesem Fall ist $N = C_G(N)$ und daher $G/N \leq Aut(N)$. Zunächst aber ist klar, dass N als abelscher Normalteiler einer zweifach transitiven Gruppe natürlich regulär operieren muss.

(7.2) Lemma.

N operiert regulär auf Ω.

Wir unterscheiden nun die Fälle, in denen G_α *regulär* oder *nicht regulär* auf $N^\sharp$ operiert. Dies führt leicht auf die beiden übrigen Fälle aus dem obigen Satz. Wie üblich sei im folgenden wieder $\Omega^* := \Omega \setminus \{\alpha\}$ für ein $\alpha \in \Omega$.

(7.3) Lemma.

Operiert X regulär auf Ω^*, so ist G wie in (c) von 7.1.

Beweis. Wegen $X \trianglelefteq G_\alpha$ ist auch $NX \trianglelefteq NG_\alpha = G$ und daher

$$\langle X^G \rangle \leq \langle (NX)^G \rangle = NX.$$

Eine Gruppe operiert scharf zweifach transitiv auf Ω, wenn sie regulär auf der Menge

$$\chi := \{(\gamma, \delta) \mid \gamma, \delta \in \Omega \text{ und } \gamma \neq \delta\}$$

operiert. Wir zeigen, dass $\langle X^G \rangle$ transitiv und NX fixpunktfrei auf χ operiert. Aus dem Frattiniargument folgt dann offenbar die Behauptung, denn die übrigen Punkte von (c) haben wir bereits gezeigt oder vorausgesetzt.

Seien dazu γ und δ verschieden in Ω mit $\gamma \neq \alpha$. Nun ist $G = NG_\alpha$ und N ist regulär auf Ω, also gibt es ein $g \in N$ mit $\alpha^g \neq \alpha, \gamma$. Da X transitiv auf Ω^* operiert, gibt es ein $x \in X$ mit

$$(\gamma^{g^{-1}})^x = \alpha^{g^{-1}}$$

und somit ist

$$(\gamma, \delta)^{x^g} = (\alpha, \delta^{x^g}).$$

Nun ist X transitiv auf Ω^*, also ist offenbar $\langle X^G \rangle$ und daher auch NX transitiv auf χ. Es bleibt somit nur die Fixpunktfreiheit von NX auf χ nachzuweisen.

Seien dazu γ und δ wie oben und $g \in NX$ mit

$$(\gamma, \delta)^g = (\gamma, \delta).$$

Da NX transitiv auf Ω operiert, können wir o.B.d.A. annehmen, dass $\gamma = \alpha$. Schreiben wir $g = xg_0$ mit $g_0 \in N$ und $x \in X$, so ist insbesondere $\alpha = \alpha^g = \alpha^{g_0}$ und somit $g_0 = 1$, denn N operiert fixpunktfrei auf Ω. Somit ist aber auch $\delta = \delta^g = \delta^x$ und daher $x = 1$, denn auch X operiert fixpunkfrei auf Ω^*. Dies beweist das Lemma. □

(7.4) Lemma.

Operiert X nicht regulär auf Ω^*, so ist N von der Ordnung r^2 für eine Mersenne'sche Primzahl r.

Beweis. Die Operationen von G_α auf Ω^* und $N^\sharp$ sind äquivalent, denn N operiert regulär auf Ω. Nach Huppert [19] ist daher N notwendig nicht von der Ordnung 2^6, denn dann operiert X fixpunktfrei auf $N^\sharp$.

Ist die Ordnung r^a von N nicht das Quadrat einer Mersenne'schen Primzahl und verschieden von 2^6, so gibt es nach ZSIGMONDY [41] eine Primzahl s mit $s \mid r^a - 1$ und $s \nmid r^b - 1$ für alle $1 \leq b < a$. Nun operiert X transitiv auf $N^\sharp$, also ist $X = S \times O_{s'}(X)$ für die s-Sylowgruppe S von X. Zu jedem Element $x \in S$ existiert wegen der Nilpotenz von S eine Zentralreihe

$$\langle x \rangle = S_0 \lhd S_1 \lhd \ldots \lhd S_k = S.$$

Da die Operationen von G_α auf Ω^* und $N^\sharp$ äquivalent sind, ist stets $C_N(S_i) < N$. Nun ist N ein minimaler Normalteiler von $G = NG_\alpha$, also ist $C_N(S) = 1$ und daher

$$C_S(n) < S = S_k$$

für $n \in N^\sharp$. Zerlegen wir die Operation von S_k auf $C_N(S_{k-1})$ in Bahnen, so ist

$$s \mid |C_N(S_{k-1})^\sharp| = r^b - 1$$

für $b \leq a$. Wegen $C_N(S_{k-1}) < N$ ist $b = 0$ und $C_N(S_{k-1}) = 1$. Sukzessive Anwendung des obigen Arguments liefert $C_N(S_0) = 1$, also operiert S fixpunktrei auf $N^\sharp$.

Die Gruppe S operiert nun für $y \in O_{s'}(X)$ auf der Menge $C_N(y)^\sharp$ und wir zerlegen diese in Bahnen der Länge $|S : C_S(n)| = |S|$. Insbesondere ist wieder $s \mid r^b - 1$ für $b < a$ und daher $C_N(y) = 1$. Somit operiert auch $O_{s'}(X)$ fixpunktfrei auf $N^\sharp$ bzw. Ω^* und daher offensichtlich auch X, denn S und $O_{s'}(X)$ haben teilerfremde Ordnung. Dies liefert den gewünschten Widerspruch. □

(7.5) Lemma.

Operiert X nicht regulär auf Ω^*, so ist G wie in (d) von 7.1.

Beweis. Die Gruppe N ist nun eine elementarabelsche r-Gruppe der Ordnung r^2 für eine Mersenne'sche Primzahl und wir können N als zweidimensionalen $\mathbb{Z}_r$-Vektorraum V auffassen. Da die Operationen von G_α auf Ω^* und $N^\sharp$ äquivalent sind, ist $G_\alpha \leq GL(V)$. Insbesondere enthält $GL(V)$ die auf $V^\sharp$ transitive und nilpotente Gruppe X. Aus der Liste der Untergruppen von $GL_2(r)$ sehen wir, dass $Z := Z(GL_2(r)) \leq X$ und X/Z eine Diedergruppe der Ordnung $D_{2(r+1)}$ ist.

Für $r > 3$ ist X/Z maximal in $PGL_2(r)$ und $X = G_\alpha$ oder $G_\alpha = GL_2(r)$ hat einen nilpotenten Normalteiler X, wobei letzteres offenbar nicht eintreten kann. Auch für $r = 3$ ist $X = G_\alpha$. Hier ist nämlich $GL_2(3)$ von der Ordnung $2^4 \cdot 3$ und X transitiv (aber nicht fixpunktfrei) auf 8 Vektoren. Notwendig ist also X eine 2-Sylowgruppe von $GL_2(3)$ und dort sein eigener Normalisator. In jedem Fall ist also $X = G_\alpha$ maximal in G, und somit $\langle X^G \rangle = G$. Schließlich folgt

$$|G| = |NX| = |N| \cdot |X| = r^2 \cdot |Z| \cdot |D_{2(r+1)}| = 2r^2(r^2 - 1),$$

und außerdem

$$|G_\alpha : G_{\alpha,\beta}| = |\beta^{G_\alpha}| = m - 1 = r^2 - 1.$$

Dies beweist schließlich das Lemma. □

Kapitel 8

Gruppen mit einem BN-Paar vom Rang 2

Ein BN-Paar einer (endlichen) Gruppe G nennen wir *irreduzibel*, wenn die zugehörige Weylgruppe ein zusammenhängendes Dynkindiagramm hat. Zu jeder Gruppe mit einem irreduziblen BN-Paar (vom Rang $n \geq 2$) korrespondiert ein irreduzibles Gebäude $\mathcal{B}$, welches für $n \geq 3$ nach 2.4.4 die *Moufangbedingung* erfüllt. Ist hingegen $n = 2$, so müssen wir Zusatzannahmen an das BN-Paar stellen, damit auch hier das korrespondierende Gebäude die Moufangbedingung erfüllt. Bevor wir den Hauptsatz dieses Kapitels formulieren können, benötigen wir einige Notation.

Sei G eine endliche Gruppe mit einem irreduziblen BN-Paar (B, N) vom Rang n und U ein nilpotenter Normalteiler von B mit $B = UH$, wobei $H = B \cap N$. Obwohl der Hauptsatz dieses Kapitels nur den Fall $n = 2$ behandeln wird, beschränken wir den Rang n zunächst nicht, denn die ersten folgenden Abschnitte kommen ohne eine solche Beschränkung aus. Weiterhin werde die Weylgruppe W des BN-Paares von den Involutionen $s_1, \ldots, s_n$ erzeugt. Mit W assoziieren wir ein (in Kapitel 2 beschriebenes) irreduzibles Wurzelsystem Φ, oder $W \cong D_{16}$ und Φ ist die Menge der Vektoren vom Ursprung zu den Ecken eines regulären 16-Ecks. Schließlich sei $\{r_1, \ldots, r_n\}$ ein Fundamentalsystem von Φ. Sei $\mathcal{B}$ das auf Seite 12 eingeführte zu G korrespondierende Gebäude

$$\mathcal{B} := \mathcal{C}(G, B, (P_i)_{i \in I}),$$

und sei $\mathcal{A}$ das Apartment

$$\mathcal{A} := \{Bw \mid w \in W\}$$

von $\mathcal{B}$. Für $n = 2$ ist $\mathcal{B}$ ein verallgemeinertes m-Eck mit $m \in \{3, 4, 6, 8\}$. Innerhalb der Gruppe G legen wir für $w \in W$ und $i \leq n$ noch die Bezeichnungen

$$\begin{aligned} B_w &:= B \cap B^w, & B_{r_i} &:= B \cap B^{w_0 s_i}, & B_w^- &:= B \cap B^{w_0 w}, \\ U_w &:= U \cap B_w, & B_{r_i} &:= U \cap B_{r_i}, & U_w^- &:= U \cap B_w^-, \\ K_i &:= \bigcap_{x \in P_i} B^x, & L_i &:= \langle U^{P_i} \rangle, \end{aligned}$$

fest und beachten die Wohldefiniertheit dieser Festlegungen. Die beiden letzten Festlegungen benutzen wir nur für den Fall $n = 2$, in dem P_i die beiden standardmaximalparabolischen Untergruppen von G sind. In diesem Fall nennen wir die Untergruppen U_{r_i} (und ihre Konjugierten) die *Wurzeluntergruppen* von G. Wir identifizieren die fundamentalen Wurzeln r_i mit gleichnamigen Wurzeln in $\mathcal{A}$ (welche die Kammer B enthalten) und bezeichnen die zugehörigen Wurzeluntergruppen von $\mathcal{B}$ mit A_{r_i} für $i \leq 2$. Die Rechtfertigung für die Bezeichnung der Gruppen U_{r_i} als Wurzeluntergruppen von G wird deutlich in dem folgenden Hauptsatz.

Sind die echten einfachen Abschnitte einer endlichen Gruppe G *bekannt*, so heißt G eine $\mathcal{K}$-Gruppe. Es gilt nun der

(8.1) Hauptsatz.

Sei G eine endliche $\mathcal{K}$-Gruppe mit einem irreduziblen BN-Paar vom Rang 2, welche treu auf dem korrespondierenden Gebäude $\mathcal{B}$ operiert. Weiterhin sei U ein nilpotener Normalteiler von B mit $B = UH$, wobei $H = B \cap N$. Dann gilt $U_{r_i} = A_{r_i}$ für $i \leq 2$ und $\mathcal{B}$ ist ein Moufanggebäude.

In den Jahren 1973 und 1974 haben Fong & Seitz in ihren Arbeiten *Groups with a BN-Pair of Rank* 2, I & II in [12] und [13] endliche Gruppen mit BN-Paaren vom Rang 2 klassifiziert. Die exakten Voraussetzungen waren die treue Operation von G auf $\mathcal{B}$ und die Bedingung $G = \langle U^G \rangle$. Auf die Voraussetzung, dass G eine $\mathcal{K}$-Gruppe ist, wurde verzichtet.

Das weitere Vorgehen sei wie folgt beschrieben. Im letzten Abschnitt werden wir den Hauptsatz beweisen und werden dort zunächst (ohne die Notation zu ändern) das BN-Paar aus dem Hauptsatz durch ein saturiertes BN-Paar ersetzen und U durch $F(B)$ ersetzen. Dass dies prinzipiell möglich ist, sehen wir im ersten Abschnitt. Die beiden nachfolgenden Abschnitte zeigen erste elementare Eigenschaften. Wichtig für die Konstruktion der Wurzeluntergruppen von G ist die Identität $U_w = U \cap U^w$ für $w \in W$. Diese erhalten wir nach dem dritten Abschnitt, wenn U eine p-Gruppe ist. Mit diesem Punkt werden wir uns im fünften Abschnitt befassen, in welchem wir $n = 2$ voraussetzen. Hier kommt die Voraussetzung ins Spiel, dass G eine $\mathcal{K}$-Gruppe ist. Die parabolischen Untergruppen P_i operieren zweifach transitiv auf $\Delta_i(B)$ und K_i ist offenbar der Kern dieser Operation. Ist $\overline{\ }$ jeweils der natürliche Homomorphismus von P_i auf P_i/K_i, so enthält der Stabilisator der Kammer B den auf $\Delta_i(B)\setminus\{B\}$ transitiven Normalteiler $\overline{U}$. Insbesondere erfüllt $\overline{P}_i$ die Voraussetzung zu 7.1 und wir können die Gruppe $\overline{P}_i$ und die normale Hülle $\overline{L}_i$ von $\overline{U}$ beschreiben. Der Satz 7.1 ist für uns von großer Bedeutung, denn erst hiermit werden wir zeigen, dass U eine p-Gruppe ist. Eine weitere Folge von 7.1 wird eine reguläre Operation von $\overline{U}$ auf $\Delta_i(B)$ sein, was wir in den beiden vorletzten Abschnitt sehen.

Schließlich können wir die Gruppen U_{r_i} mit den fundamentalen Wurzeluntergruppen A_{r_i} des Apartments $\mathcal{A}$ identifizieren und außerdem wird A_{r_i} regulär auf $\mathcal{W}(r_i)$ operieren. Insbesondere wird dann $U \cap H = 1$ sein, und somit stimmt das BN-Paar mit dem ersetzten BN-Paar überein, wenn wir die Konstruktion des saturierten BN-Paares aus dem ersten Abschnitt verfolgen. Da W transitiv auf den Wurzeln von $\mathcal{A}$ operiert, ist dann die Moufangbedingung „innerhalb von $\mathcal{A}$“ erfüllt. Die Moufangbedingung für $\mathcal{B}$ ist deswegen und nach Axiom (B3) offenbar erfüllt.

Die ersten fünf Abschnitte sind in ähnlicher Form in der ersten oben zitierten Arbeit von Fong & Seitz zu finden, worauf wir in den entsprechenden Abschnitten nicht jedesmal hinweisen werden. Wir geben diese Abschnitte der Vollständigkeit halber an,

und um zu sehen, was genau in den Beweis des obigen Satzes eingeht.

8.1 Ein saturiertes BN-Paar

Sei G eine Gruppe mit einem BN-Paar (B, N) vom Rang n, und es sei $H = B \cap N$. Wir zeigen mit elementaren Argumenten, wie wir das vorhandene BN-Paar zu einem saturierten BN-Paar erweitern können. Dazu sei

$$H_1 := \bigcap_{n \in N} B^n.$$

Dann wird H_1 von N normalisiert und $N_1 := H_1 N$ ist eine Gruppe. Wir erhalten nun das

(8.1.1) Lemma.

Es ist (B, N_1) ein saturiertes BN-Paar vom Rang n von G, und die zugehörige Weylgruppe ist isomorph zu W. Ist U ein Normalteiler von B mit $B = UH$, so ist $B = UH_1$.

Beweis. Natürlich ist $H \leq H_1 \leq B$ und somit erhalten wir aus der Dedekindidentität sofort

$$B \cap N_1 = B \cap H_1 N = H_1(B \cap N) = H_1$$

und der Punkt $(BN1)$ ist nun offenbar erfüllt. Weiterhin ist

$$N_1/H_1 = NH_1/H_1 \cong N/(N \cap H_1) = N/H = W,$$

und es ist auch $(BN2)$ erfüllt. Sind $s_1, \ldots, s_n$ Urbilder der Erzeuger von W, so sind dies auch Urbilder der Erzeuger von N_1/H_1 und die Punkte $(BN3)$ und $(BN4)$ sind nun trivialerweise erfüllt. Somit ist (B, N_1) ein BN-Paar von G und wegen

$$\bigcap_{n \in N_1} B^n = \bigcap_{n \in N} B^n = H_1,$$

ist dieses sogar saturiert. Der Rest der Behauptung ist nun klar. □

Häufig wird es von Nutzen sein, wenn G ein triviales Zentrum hat. Dies ist automatisch erfüllt, wenn G treu auf dem Gebäude $\mathcal{B}$ operiert.

(8.1.2) Lemma.

Operiert G treu auf $\mathcal{B}$, so ist $Z(G) = 1$.

Beweis. Da die parabolische Untergruppe B von $Z(G)$ normalisiert wird, ist $Z(G) \leq B$. Insbesondere ist $Z(G) \leq \bigcap_{g \in G} B^g$, und dies ist offenbar der nach Voraussetzung triviale Kern der Operation von G auf $\mathcal{B}$. □

8.2 Eigenschaften von Gruppen mit BN-Paaren

In diesem Abschnitt sei G eine endliche Gruppe mit einem saturierten, irreduziblen BN-Paar (B, N) vom Rang n. Wir zeigen hier erste elementare Eigenschaften der Gruppen mit BN-Paaren, die im wesentlichen aus der Bruhatzerlegung folgen. In (8.2.3) und (8.2.4) bei CARTER [6] finden wir

(8.2.1) Die Bruhatzerlegung.

Es gelten die folgenden Eigenschaften:

(a) $G = \bigcup_{w \in W} BwB$.

(b) Sind $w, w' \in W$ *mit* $BwB = Bw'B$, *dann gilt* $w = w'$.

(c) Ist $w \in W$ *und* $i \leq n$ *mit* $\ell(s_i w) > \ell(w)$, *so ist* $s_i Bw \subseteq Bs_i wB$.

(8.2.2) Folgerung.

Ist $w \in W$ *und* $i \leq n$ *mit* $\ell(s_i w) > \ell(w)$, *so gilt:*

(a) $B^{s_i} \cap B^{w^{-1}} \leq B$.

(b) $B_{s_i w} \leq B_w$.

(c) $B = B_{w^{-1}} B_{s_i} = B_{s_i} B_{w^{-1}}$.

Beweis. Den ersten Punkt erhalten wir im wesentlichen aus dem Punkt $(BN3)$ und der Bruhatzerlegung. Es gilt nämlich offenbar

$$\begin{aligned} B^{s_i} \cap B^{w^{-1}} &= s_i B s_i \cap wBw^{-1} \\ &\leq s_i B s_i \cap BwBw^{-1} \\ &\subseteq (B \cup Bs_i B) \cap BwBw^{-1} \\ &= (B \cap BwBw^{-1}) \cup (Bs_i B \cap BwBw^{-1}), \end{aligned} \tag{8.1}$$

also folgt die Behauptung, wenn $Bs_i B \cap BwBw^{-1} = \emptyset$. Ist dies nicht der Fall, so liefert die Multiplikation mit w von rechts

$$\emptyset \neq Bs_i Bw \cap BwB \subseteq Bs_i wB \cap BwB,$$

wenn wir Punkt (c) von 8.2.1 benutzen. Offenbar folgt nun $w = s_i w$ aus der Bruhatzerlegung. Dies ist ein Widerspruch und es folgt (a). Direkt hieraus sehen wir dann

$$B_{s_i w}^{w^{-1}} = (B \cap B^{s_i w})^{w^{-1}} = B^{s_i} \cap B^{w^{-1}} \leq B,$$

woraus unmittelbar der Teil (b) abzulesen ist.

Nutzen wir schließlich Punkt (c) von 8.2.1, so erhalten wir aus (8.1) zunächst

$$B = s_i(s_iBw)w^{-1} \subseteq s_i(Bs_iw)Bw^{-1} = B^{s_i}B^{w^{-1}}.$$

Sei nun $b = xy \in B$ mit $x \in B^{s_i}$ und $y \in B^{w^{-1}}$. Nach (8.1) folgt dann

$$x = by^{-1} \in BwBw^{-1} \cap s_iBs_i \subseteq B.$$

Damit ist offenbar auch $y \in B$ und Teil (c) ist nun offensichtlich. □

(8.2.3) Folgerung.

Ist $n = 2$ und operiert G treu auf $\mathcal{B}$, so enthält P_i keinen Normalteiler von G für $i = 1, 2$.

Beweis. Angenommen P_i enthält den Normalteiler N. Nach Umnummerieren nehmen wir o.B.d.A. $i = 1$ an. Da G treu auf $\mathcal{B}$ operiert, enthält B keine Normalteiler von G und wegen $P_1 = B \cup Bs_1B$ ist daher

$$N \cap Bs_1B \neq \emptyset.$$

Da N invariant unter s_2 ist, ist auch

$$N \cap s_2Bs_1Bs_2 \neq \emptyset.$$

Nach der Bruhatzerlegung und $(BN3)$ ist

$$s_2Bs_1Bs_2 \subseteq s_2Bs_1s_2B \subseteq Bs_1s_2B \cup Bs_2s_1s_2B.$$

Insbesondere ist eine der Mengen $N \cap Bs_1s_2B$ oder $N \cap Bs_2s_1s_2B$ nichtleer und wegen $N \leq B \cup Bs_1B$ ist daher

$$Bs_1s_2B = Bs_1B \quad \text{oder} \quad Bs_2s_1s_2B = Bs_1B.$$

Somit ist $s_1s_2 = s_1$ oder $s_1s_2s_1 = s_2$, ein Widerspruch. □

(8.2.4) Lemma.

Für $w \in W$ und $i \leq n$ gelten die folgenden Aussagen:

(a) $B_{w_0} = H$ und $B = B_{r_i}B_{s_i}$. Insbesondere ist $B_{r_i} \not\leq H$.

(b) Ist $\ell(ws_i) > \ell(w)$, dann gilt $B_{r_i} \leq B_w$, $B^-_{ws_i} = B_{r_i}(B^-_w)^{s_i}$ und $B_{r_i} \cap (B^-_w)^{s_i} = H$.

(c) Ist $\ell(ws_i) < \ell(w)$, dann gilt $B_{r_i} \not\leq B_w$, $B_{r_i} \cap B_w = H$, $B^-_w = B_{r_i}(B^-_{ws_i})^{s_i}$ und $B_{r_i} \cap (B^-_{ws_i})^{s_i} = H$.

(d) $B = B^-_wB_w$ und $B_w \cap B^-_w = H$. Insbesondere gilt $B_{r_i} \cap B_{s_i} = H$.

(e) $G = \bigcup_{w \in W} BwB^-_w$ und $|BwB^-_w : B| = |B^-_w : H|$.

Beweis. Sei $w \in W$ von w_0 verschieden. Sei $w_1 = w$ und $w_{i+1} = s_{j_i} w_i$, wobei $j_i \in \{1, \ldots, n\}$ so gewählt ist, dass $w_i^{-1}(r_{j_i}) > 0$ ist. Ein solches j_i existiert, falls $w_0 \neq w_i$, denn w_0 ist das einzige Element in W, das sämtliche fundamentale Wurzeln auf negative Wurzeln abbildet. Nach 2.2.1 ist

$$\ell(w_{i+1}) = \ell(s_{j_i} w_i) = \ell(w_i) + 1,$$

also bricht die Folge in einem Element w_k ab, da es ein Element maximaler Länge gibt. Offenbar ist $w_k = w_0$, denn w_k bildet die fundamentalen Wurzeln auf negative Wurzeln ab. Aus Teil (b) von 8.2.2 erhalten wir sofort $B_{w_{i+1}} \leq B_{w_i}$ für $i \leq k-1$ und somit auch $B_{w_0} \leq B_w$. Nach Voraussetzung ist unser BN-Paar saturiert, also ergibt sich aus

$$H \leq B_{w_0} \leq \bigcap_{w \in W} B_w = \bigcap_{w \in W} B^w = H$$

offenbar der erste Teil von (a). Den zweiten Teil erhalten wir aus (c) von 8.2.2. Es ist nämlich $\ell(s_i(s_i w_0)) = \ell(w_0) > \ell(s_i w_0)$ und daher

$$B = B_{(s_i w_0)^{-1}} B_{s_i} = B_{w_0 s_i} B_{s_i} = B_{r_i} B_{s_i}.$$

Für $w \in W$ ist $\ell(w)$ die Anzahl der positiven Wurzeln, die von w auf negative Wurzeln abgebildet wird, also ist $\ell(w_0 w) = \ell(w_0) - \ell(w)$. Ist nun $w \in W$ mit $\ell(w s_i) > \ell(w)$, so ist

$$\ell(w_0 s_i w^{-1}) = \ell(w_0) - \ell(s_i w^{-1}) = \ell(w_0) - \ell(w s_i) = \ell(w_0) - \ell(w) - 1.$$

Sei nun $s_{i_1} \cdots s_{i_k}$ ein minimaler Ausdruck für $w_0 s_i w^{-1}$. Wir definieren eine Folge $w_1, \ldots, w_{k+1}$ in W durch

$$w_j := s_{i_j} \cdots s_{i_k} w$$

für $j = 1, \ldots, k$ und $w_{k+1} = w$. Es folgt

$$\ell(w_j) = 1 + \ell(w_{j+1}) \tag{8.2}$$

für alle $j \leq k$. Andernfalls gilt $\ell(w_j) < 1 + \ell(w_{j+1})$ für ein $j = 1, \ldots, k$ und in der Verwendung mit (8.2) ergibt sich sukzessive

$$\begin{aligned} \ell(w_0) - 1 = \ell(w_0 s_i) = \ell(w_1) < \ell(w) + k = \ell(w) + \ell(w_0 s_i w^{-1}) \\ = \ell(w) + \ell(w_0) - \ell(w) - 1 = \ell(w_0) - 1, \end{aligned}$$

ein Widerspruch. Daher gilt

$$\ell(w_j) > \ell(w_{j+1})$$

für $j \leq k$ und aus (b) von 8.2.2 lesen wir mit

$$B_{r_i} = B_{w_1} \leq B_{w_2} \leq \ldots \leq B_{w_{k+1}} = B_w$$

den ersten Teil von (b) ab. Wegen $\ell(w s_i) > \ell(w)$ ist auch

$$\begin{aligned} \ell((w_0 w s_i) s_i) = \ell(w_0 w) = \ell(w_0) - \ell(w) > \ell(w_0) - \ell(w) - 1 \\ = \ell(w_0) - \ell(w s_i) = \ell(w_0 w s_i), \end{aligned}$$

also erhalten wir aus dem ersten Teil von (b) sofort

$$B_{r_i} \leq B_{w_0 w s_i} = B^-_{w s_i}.$$

Mit der Dedekindidentität und (a) folgt

$$\begin{aligned} B^-_{ws_i} &= B^-_{ws_i} \cap B = B^-_{ws_i} \cap (B_{r_i} B_{s_i}) \\ &= B_{r_i}(B^-_{ws_i} \cap B_{s_i}) = B_{r_i}(B^{s_i} \cap B^{w_0 w} \cap B)^{s_i}. \end{aligned}$$

Nun gilt wegen $\ell(w_0 w) > \ell(w_0 w s_i)$ auch

$$\ell(s_i(s_i w^{-1} w_0)) = \ell(w^{-1} w_0) = \ell(w_0 w) > \ell(w_0 w s_i) = \ell(s_i w^{-1} w_0)$$

und mit (a) von 8.2.2 folgt $B^{s_i} \cap B^{w_0 w s_i} \leq B$. Damit ist auch

$$B \cap B^{w_0 w} \leq B \cap B^{s_i}$$

und schließlich

$$B^{s_i} \cap B^{w_0 w} \cap B = B \cap B^{w_0 w} = B^-_w. \tag{8.3}$$

Wir erhalten

$$B^-_{ws_i} = B_{r_i}(B^-_w)^{s_i}.$$

Aus (8.3) und aus (a) ergibt sich

$$H \leq B_{r_i} \cap (B^-_w)^{s_i} = B \cap B^{w_0 s_i} \cap B^{s_i} \cap B^{w_0 w s_i} \leq (B^{w_0} \cap B)^{s_i} = H^{s_i} = H,$$

und wir haben Teil (b) gezeigt.

Sicherlich ist $H \leq B_{r_i} \cap B_w$ und umgekehrt ist

$$B_{r_i} \cap B_w = B \cap B^{w_0 s_i} \cap B^w = (B^{s_i} \cap B^{w_0} \cap B^{w s_i})^{s_i}.$$

Nun ist

$$\ell(s_i w^{-1}) = \ell(w s_i) < \ell(w) = \ell(w s_i s_i) = \ell(s_i(s_i w^{-1})),$$

also erhalten wir aus (a) von 8.2.2 die Abschätzung $B^{s_i} \cap B^{w s_i} \leq B$. Damit ist

$$B_{r_i} \cap B_w \leq (B \cap B^{w_0})^{s_i} = H^{s_i} = H,$$

also gilt $B_{r_i} \cap B_w = H$. Insbesondere ist $B_{r_i} \not\leq B_w$, denn sonst ist $B_{r_i} = H$ und $B = B_{s_i}$ in (a) wird von s_i normalisiert, ein Widerspruch. Der Rest von (c) folgt nun direkt aus (b).

Sei schließlich $w \in W$ beliebig mit minimalem Ausdruck $s_{i_1} \cdots s_{i_k}$. Dann ist $s_{i_k} \cdots s_{i_1}$ ein minimaler Ausdruck für w^{-1}. Insbesondere gilt dann

$$\ell(s_{i_k} \cdots s_{i_j}) > \ell(s_{i_k} \cdots s_{i_{j+1}}). \tag{8.4}$$

Für $i = 1, \ldots, k$ sei

$$w_j := w_0 s_{i_k} \cdots s_{i_j}$$

und $w_{k+1} := w_0$. Dann gilt $w_{j+1} = w_j s_{i_j}$ für $j \leq k$ und somit

$$\ell(w_k s_{i_k}) = \ell(w_{k+1}) = \ell(w_0) > \ell(w_0) - 1 = \ell(w_0 s_{i_k}) = \ell(w_k).$$

Nach (8.4) ist außerdem

$$\begin{aligned}\ell(w_j s_{i_j}) = \ell(w_{j+1}) = \ell(w_0 s_{i_k} \cdots s_{i_{j+1}}) &= \ell(w_0) - \ell(s_{i_k} \cdots s_{i_{j+1}}) \\ &> \ell(w_0) - \ell(s_{i_k} \cdots s_{i_j}) = \ell(w_j).\end{aligned}$$

für $j \leq k-1$ und aus (b) sehen wir insgesamt

$$B^-_{w_{j+1}} = B^-_{w_j s_{i_j}} = B_{r_{i_j}} (B^-_{w_j})^{s_{i_j}}$$

für $j \leq k$. Wir erhalten damit

$$\begin{aligned}B &= B^-_{w_0} \\ &= B^-_{w_{k+1}} \\ &= B_{r_{i_k}} (B^-_{w_k})^{s_{i_k}} \\ &= B_{r_{i_k}} B^{s_{i_k}}_{r_{i_{k-1}}} (B^-_{w_{k-1}})^{s_{i_{k-1}} s_{i_k}} \\ &= \dots \\ &= B_{r_{i_k}} B^{s_{i_k}}_{r_{i_{k-1}}} B^{s_{i_{k-1}} s_{i_k}}_{r_{i_{k-2}}} \cdots B^{s_{i_2} \cdots s_{i_k}}_{r_{i_1}} (B^-_{w_1})^{s_{i_1} \cdots s_{i_k}} \\ &= B_{r_{i_k}} B^{s_{i_k}}_{r_{i_{k-1}}} B^{s_{i_{k-1}} s_{i_k}}_{r_{i_{k-2}}} \cdots B^{s_{i_2} \cdots s_{i_k}}_{r_{i_1}} (B^-_{w_0 w^{-1}})^w \\ &= B_{r_{i_k}} B^{s_{i_k}}_{r_{i_{k-1}}} B^{s_{i_{k-1}} s_{i_k}}_{r_{i_{k-2}}} \cdots B^{s_{i_2} \cdots s_{i_k}}_{r_{i_1}} B_w.\end{aligned}$$

Ist nun $w'_j := s_{i_1} \cdots s_{i_j}$ für $j \leq k-1$, so gilt offenbar

$$\ell(w'_{j+1}) = \ell(w'_j s_{i_{j+1}}) > \ell(w'_j).$$

Mit (b) erhalten wir

$$B^-_w = B^-_{w'_{k-1} s_{i_k}} = B_{r_{i_k}} (B^-_{w'_{k-1}})^{s_{i_k}} = \dots = B_{r_{i_k}} B^{s_{i_k}}_{r_{i_{k-1}}} \cdots B^{s_{i_2} \cdots s_{i_k}}_{r_{i_1}}.$$

Damit gilt also $B = B^-_w B_w$. Mit (a) folgt

$$B_w \cap B^-_w = B \cap B^w \cap B^{w_0 w} = B \cap (B \cap B^{w_0})^w = B \cap H = H$$

und insbesondere auch $B_{r_i} \cap B_{s_i} = B_{s_i} \cap B^-_{s_i} = H$.

Aus der Bruhatzerlegung erhalten wir mit (d) leicht

$$G = \bigcup_{w \in W} BwB = \bigcup_{w \in W} BwB_w B^-_w = \bigcup_{w \in W} BwB^-_w.$$

Für $x, y \in B^-_w$ gilt ferner

$$Bwx = Bwy \iff (xy^{-1})^{w^{-1}} \in B \iff xy^{-1} \in B^w \cap B^-_w = H \iff Hx = Hy,$$

und damit ist (e) klar. □

Im weiteren Verlauf sei $G_{r_i} := \langle B_{r_i}, s_i \rangle$ für $i \leq n$.

(8.2.5) Satz.

Für $i \leq n$ operiert G_{r_i} zweifach transitiv auf den Nebenklassen von B_{r_i}.

Beweis. Der folgende Beweis stammt von TITS. Die Behauptung ist richtig, wenn G_{r_i} genau zwei Doppelnebenklassen von B_{r_i} enthält. Nach 8.2.4 ist $B = B_{r_i}B_{s_i}$, also ist

$$P_i = B \cup Bs_iB = B \cup B_{r_i}s_iB,$$

da B_{s_i} von s_i normalisiert wird. Offenbar gilt

$$\ell(s_i^{w_0}) = \ell(w_0) - \ell(s_iw_0) = \ell(w_0) - \ell(w_0s_i) = \ell(w_0) - (\ell(w_0) - 1) = 1,$$

also ist $s_i^{w_0} = s_j$ für ein $j \leq n$. Wir zeigen nun

$$P_i \cap P_j^{w_0} = B_{r_i} \cup B_{r_i}s_iB_{r_i}.$$

Dann ist die Doppelnebenklassenzerlegung auf der rechten Seite eine Gruppe, und die Behauptung ist klar. Es ist nun

$$P_j^{w_0} = B^{w_0} \cup B^{w_0}s_iB^{w_0} = B^{w_0} \cup s_iB^{w_0s_i}B^{w_0} \subseteq s_iB^{w_0} \cup B^{w_0s_i}B^{w_0},$$

denn nach $(BN3)$ gilt

$$s_iB^{w_0s_i} = s_iB^{s_jw_0} = s_i(s_jBs_j)^{w_0} \subseteq s_i(B \cup Bs_jB)^{w_0} = s_iB^{w_0} \cup B^{w_0s_i}B^{w_0}.$$

Umgekehrt ist $s_i \in P_j^{w_0}$ und $B^{w_0} \leq P_j^{w_0}$, also gilt offenbar

$$P_j^{w_0} = s_iB^{w_0} \cup B^{w_0s_i}B^{w_0}.$$

Nach (d) von 8.2.4 gilt

$$B^{w_0s_i} = (B^-_{s_iw_0})^{w_0s_i}(B_{s_iw_0})^{w_0s_i} = (B^{w_0s_i} \cap B^{w_0})(B \cap B^{w_0s_i}) \subseteq B^{w_0}B_{r_i},$$

also ist auch

$$P_j^{w_0} \subseteq s_iB^{w_0} \cup B_{r_i}B^{w_0}.$$

Wegen $B_{r_i} \leq B^{w_0s_i} \leq P_j^{w_0}$ gilt wie oben die umgekehrte Inklusion, also ist

$$P_j^{w_0} = s_iB^{w_0} \cup B_{r_i}B^{w_0}.$$

Angenommen $B \cap s_iB^{w_0} \neq \emptyset$. Dann gibt es $b, c \in B$ mit $b = s_ic^{w_0}$, also

$$w_0s_i^{-1}b = cw_0 \in Bw_0s_i^{-1}B \cap Bw_0B = Bw_0s_iB \cap Bw_0B.$$

Nach der Bruhatzerlegung ist dann aber $w_0s_i = w_0$, ein Widerspruch. Daher ist

$$B \cap s_iB^{w_0} = \emptyset$$

und mit der Dedekindidentität folgt

$$B \cap P_j^{w_0} = B \cap B_{r_i}B^{w_0} = B_{r_i}(B \cap B^{w_0}) = B_{r_i}H = B_{r_i}.$$

Wegen $s_i B_{r_i} \subseteq P_j^{w_0}$ ist somit

$$B_{r_i} s_i B \cap P_j^{w_0} = B_{r_i} s_i B_{r_i}$$

und wir erhalten schließlich

$$P_i \cap P_j^{w_0} = (B \cup B_{r_i} s_i B) \cap P_j^{w_0} = (B \cap P_j^{w_0}) \cup (B_{r_i} s_i B \cap P_j^{w_0}) = B_{r_i} \cup B_{r_i} s_i B_{r_i},$$

wie gewünscht. □

Abschließend sei G eine endliche Gruppe mit einem *saturierten BN-Paar vom Rang* 2. Wir definieren dann zwei natürliche Zahlen t_i durch

$$|P_i : B| = t_i + 1$$

für $i = 1, 2$ und erhalten wegen $B = B_{r_i} B_{s_i}$ und $B_{r_i} \cap B_{s_i} = H$ leicht $t_i = |B_{r_i} : H|$. Durch die wiederholte Anwendung von Lemma 8.2.4 erhalten wir das

(8.2.6) Lemma.

Ist $|W| = 2m$ mit geradem m, so gilt:

(a) Tauchen s_1 und s_2 genau a_1- bzw. a_2-mal in einem minimalen Ausdruck von $w \in W$ auf, so ist $|B_w^- : H| = t_1^{a_1} t_2^{a_2}$. Insbesondere ist $|B : H| = (t_1 t_2)^{\frac{m}{2}}$.

(b) $|G| = |H|(t_1 + 1)(t_2 + 1)(t_1 t_2)^{\frac{m}{2}} \frac{(t_1 t_2)^{\frac{m}{2}} - 1}{t_1 t_2 - 1}$.

(8.2.7) Bemerkung.

Auch für $|W| = 6$ ist $|B : H|$ Produkt von Potenzen von t_i für $i \leq 2$.

Beweis. Sei $w \in W$ mit minimalem Ausdruck $s_{i_1} \cdots s_{i_k}$. Für $j \leq k$ definieren wir die Elemente $w_j = s_{i_1} \cdots s_{i_j}$ und sehen sofort

$$\ell(w_j s_{i_{j+1}}) = \ell(w_{j+1}) > \ell(w_j),$$

für $j \leq k - 1$. Wenden wir nun (b) von 8.2.4 an, so ist

$$B_{r_{i_{j+1}}} \cap (B_{w_j}^-)^{s_{i_{j+1}}} = H,$$

sowie

$$B_{w_{j+1}}^- = B_{r_{i_{j+1}}} (B_{w_j}^-)^{s_{i_{j+1}}}$$

für $j \leq k$. Durch wiederholte Anwendung von (b) aus 8.2.4 erhalten wir damit

$$\begin{aligned}
|B_w^-| &= |B_{w_{k-1}s_{i_k}}^-| \\
&= |B_{r_{i_k}}(B_{w_{k-1}}^-)^{s_{i_k}}| \\
&= \frac{|B_{r_{i_k}}||B_{w_{k-1}}^-|}{|H|} \\
&= \dots \\
&= \frac{|B_{r_{i_k}}||B_{r_{i_{k-1}}}| \cdots |B_{r_{i_1}}|}{|H|^{k-1}} \\
&= |H||B_{r_{i_k}} : H| \cdots |B_{r_{i_1}} : H|.
\end{aligned}$$

Ist m gerade, so sind a_1 und a_2 wohldefiniert und es folgt der erste Teil der Behauptung.

Nach (e) von 8.2.4 ist offenbar

$$|G| = |B|(\sum_{w \in W} |B_w^- : H|).$$

Da $w_0 = (s_1 s_2)^{\frac{m}{2}} = (s_2 s_1)^{\frac{m}{2}}$ das eindeutig bestimmte längste Element in W ist und sämtliche Elemente von W von der Form $s_1 s_2 s_1 \dots$ oder $s_2 s_1 s_2 \dots$ sind, folgt aus dem ersten Teil

$$\sum_{w \in W} |B_w^- : H| = (\sum_{\substack{i,j=0 \\ |i-j|=1}}^{\frac{m}{2}} t_1^i t_2^j + (t_1 t_2)^{\frac{m}{2}} + 1 + 2 \sum_{i=1}^{\frac{m}{2}-1} (t_1 t_2)^i).$$

Wir rechnen leicht nach, dass

$$\begin{aligned}
&(\sum_{\substack{i,j=0 \\ |i-j|=1}}^{\frac{m}{2}} t_1^i t_2^j + (t_1 t_2)^{\frac{m}{2}} + 1 + 2 \sum_{i=1}^{\frac{m}{2}-1} (t_1 t_2)^i)(t_1 t_2 - 1) \\
&\quad = (t_1 t_2)^{\frac{m}{2}+1} + t_1^{\frac{m}{2}+1} t_2^{\frac{m}{2}} + t_1^{\frac{m}{2}} t_2^{\frac{m}{2}+1} + (t_1 t_2)^{\frac{m}{2}} - t_1 t_2 - t_1 - t_2 - 1 \\
&\quad = (t_1 + 1)(t_2 + 1)((t_1 t_2)^{\frac{m}{2}} - 1),
\end{aligned}$$

und dies liefert die Behauptung. □

8.3 Schnitte von Konjugierten von U

In diesem Abschnitt sei G eine endliche Gruppe mit einem irreduziblen, saturierten BN-Paar (B, N) vom Rang n. Weiterhin sei $U := O_p(B) = F(B)$ mit $B = UH$ und $H = B \cap N$. Die Gruppen B_w können wir im folgenden auch mit Hilfe ihrer Untergruppen U_w ausdrücken. Benutzen wir nämlich die Dedekindidentität, so erhalten wir unmittelbar

$$B_w = HU \cap B^w = H(U \cap B^w) = HU_w.$$

Wir erhalten nun mit elementaren Argumenten das

(8.3.1) Lemma.

Es ist $O_p(H) = U \cap H$ und für $w \in W$ ist $U_w = U \cap U^w$.

Beweis. Offenbar ist $U \cap H \leq O_p(H)$. Umgekehrt ist $UO_p(H)$ ein p-Normalteiler von B und somit gilt auch

$$U \cap H = O_p(H).$$

Aus (d) von 8.2.4 sehen wir außerdem

$$U \cap H \leq U \cap B_w \cap B_w^- \leq U_w.$$

Wegen $B_w = HU_w$ ist $U_w \leq O_p(B_w)$ und aus der Dedekindidentität folgt

$$O_p(B_w) = (H \cap O_p(B_w))U_w \leq O_p(H)U_w = U_w,$$

also auch $U_w = O_p(B_w)$.

Offenbar folgt nun aus der Dedekindidentität

$$B_w = B \cap HU^w = H(B \cap U^w) \tag{8.5}$$

und es ist

$$V_w := B \cap U^w \leq O_p(B_w) = U_w.$$

Die Gruppe $O_p(H)$ wird von w normalisiert, also ist $O_p(H) \leq U \cap U^w$ und somit folgt aus (8.5) mit der Dedekindidentität

$$U_w = O_p(B_w) \leq O_p(H)V_w = V_w.$$

Insbesondere ist

$$U_w = V_w = V_w \cap U = U^w \cap B \cap U = U^w \cap U,$$

und das Lemma ist bewiesen. □

8.4 Überlagerungsgruppen

Eine *Überlagerungsgruppe* einer Gruppe L ist eine Gruppe $\hat{L}$ mit $\hat{L}/Z \cong L$ für eine Untergruppe $Z \leq Z(\hat{L}) \cap \hat{L}'$. Die Gruppe Z ist der *Kern* der Überlagerung. In diesem Abschnitt sei G eine endliche Gruppe mit einem irreduziblen, saturierten BN-Paar (B, N) vom Rang 2. Ferner sei $U := O_p(B) = F(B)$ mit $B = UH$ und $H = B \cap N$. Dann erhalten wir das

(8.4.1) Lemma.

Für $i = 1, 2$ ist $L_i/(U \cap K_i)$ eine Überlagerungsgruppe von L_iK_i/K_i. Weiterhin ist der Kern $(L_i \cap K_i)/(U \cap K_i)$ eine p'-Gruppe.

Beweis. Wir zeigen zunächst, dass $U \cap K_i = O_p(K_i)$ für $i = 1, 2$. Offenbar ist K_i ein Normalteiler von B. Nun ist $O_p(K_i)$ charakteristisch in K_i, also ist auch $O_p(K_i) \trianglelefteq B$. Insbesondere ist dann nach Voraussetzung

$$O_p(K_i) \leq O_p(B) \cap K_i = U \cap K_i.$$

Ferner ist $U \cap K_i$ eine p-Gruppe, die von K_i normalisiert wird, also ist auch

$$U \cap K_i = O_p(K_i).$$

Insbesondere ist $U \cap K_i$ charakteristisch in K_i und daher ist $Y := L_i/(U \cap K_i)$ eine Gruppe. Wir zeigen zunächst, dass

$$(K_i \cap L_i)/(U \cap K_i) \leq Z(L_i/(U \cap K_i)).$$

Sicherlich ist

$$[U, K_i] \leq U \cap K_i = O_p(K_i)$$

und Konjugation mit s_i liefert

$$[U^{s_i}, K_i] \leq O_p(K_i)^{s_i} = O_p(K_i).$$

Da $O_p(K_i)$ von U und U^{s_i} normalisiert wird, berechnen wir mit den Kommutatoridentitäten, dass

$$[L_i, K_i] \leq O_p(K_i) = U \cap K_i,$$

denn offenbar ist $L_i = \langle U, U^{s_i} \rangle$. Wir erhalten somit

$$[(K_i \cap L_i)/(U \cap K_i), L_i/(U \cap K_i)] \leq [K_i, L_i](U \cap K_i)/(U \cap K_i) = 1,$$

also ist

$$(K_i \cap L_i)/(U \cap K_i) \leq Z(L_i/(U \cap K_i)).$$

Insbesondere ist dann $(K_i \cap L_i)/(U \cap K_i)$ abelsch.

Angenommen

$$p \mid |(K_i \cap L_i)/(U \cap K_i)|.$$

Dann enthält $(K_i \cap L_i)/(U \cap K_i)$ eine p-Untergruppe S, und das Urbild $\widetilde{S}$ von S in $K_i \cap L_i$ ist eine p-Untergruppe von $K_i \cap L_i$, welche nicht in $U \cap K_i$ enthalten ist. Da $(K_i \cap L_i)/(U \cap K_i)$ abelsch ist, erhalten wir

$$S \trianglelefteq (K_i \cap L_i)/(U \cap K_i),$$

und insbesondere ist $\widetilde{S}(U \cap K_i)$ ein p-Normalteiler von $K_i \cap L_i$. Wegen $O_p(K_i) = U \cap K_i$ ist dies ein Widerspruch. Somit ist also $(K_i \cap L_i)/(U \cap K_i)$ eine p'-Gruppe.

Da Y/Y' abelsch ist, ist Y/Y' eine p-Gruppe, denn U und U^{s_i} sind p-Gruppen. Angenommen

$$(K_i \cap L_i)/(U \cap K_i) \not\leq Y',$$

dann ist $((K_i \cap L_i)/(U \cap K_i))Y'/Y'$ keine p-Gruppe, aber eine Untergruppe von Y/Y', ein Widerspruch. Damit gilt

$$(K_i \cap L_i)/(U \cap K_i) \leq Y'.$$

Mit den Isomorphiesätzen erhalten wir nun

$$(L_i/(U \cap K_i))/((K_i \cap L_i)/(U \cap K_i)) \cong L_i/(K_i \cap L_i) \cong L_iK_i/K_i,$$

und damit gilt die Behauptung. □

8.5 Eine Sylowuntergruppe der Borelgruppe

Sei G eine endliche $\mathcal{K}$-Gruppe mit einem irreduziblen, saturierten BN-Paar (B, N) vom Rang 2. Weiterhin sei $B = UH$ mit $U = F(B)$ und $H = B \cap N$ und G operiere treu auf $\mathcal{B}$. Die parabolischen Untergruppen $P_i = B \cup Bs_iB$ operieren offenbar zweifach transitiv auf den Kammern aus

$$\Omega_i := \{Bx \mid x \in P_i\} = \{B\} \cup \{Bs_iu \mid u \in U\}$$

von $\mathcal{B}$ und der Stabilisator B der Kammer $\alpha := B$ hat den auf

$$\Omega_i^* := \Omega_i \setminus \{\alpha\}$$

transitiven und nilpotenten Normalteiler U. Offenbar ist Ω_i ein Rang 1-Residuum der Kammer B im Gebäude $\mathcal{B}$. Der Kern der Operation ist die Gruppe K_i, und $\overline{P}_i$ erfüllt die Voraussetzung zu dem Hauptsatz 7.1, wobei $\overline{\ }$ jeweils der natürliche Homorphismus von P_i auf P_i/K_i ist. Den folgenden Satz erhalten wir sofort aus 7.1. Wir beachten dabei, dass der eindeutig bestimmte minimale Normalteiler von $\overline{P}_i$ nach Voraussetzung eine *bekannte* einfache Gruppe ist, wenn er nicht zyklisch ist.

(8.5.1) Satz.

Für $i = 1, 2$ gilt einer der folgenden Fälle:

(A) $\overline{L}_i$ ist ein einfacher Normalteiler von $\overline{P}_i$ und eine Lie-Typ Gruppe vom Rang 1.

(B) $\overline{P}_i = R(3) = R(3)'\overline{U}$.

(C) $\overline{L}_i$ operiert scharf zweifach transitiv auf Ω_i.

(D) $\overline{P}_i$ hat einen auf Ω_i regulären Normalteiler $\overline{N}_i$. Ferner gilt $\overline{L}_i = \overline{P}_i = \overline{N}_i\overline{U}$ und $|\overline{P}_i| = 2r_i^2(r_i^2 - 1)$ für eine Mersenne'sche Primzahl r_i. Weiterhin ist $\overline{B} = \overline{U}$, $|\overline{U}| = 2(r_i^2 - 1)$ und $|\overline{B}_{s_i}| = 2$.

In den ersten drei Fällen operiert $\overline{U}$ regulär auf Ω_i^* und in den ersten beiden Fällen ist $\overline{U}$ eine p_i-Gruppe für eine Primzahl p_i.

(8.5.2) Lemma.

Im Fall (D) ist $|U_{s_i} : U \cap K_i| = 2$ und ansonsten ist $U_{s_i} = U \cap K_i \trianglelefteq U$ für $i \leq 2$.

Beweis. Offenbar ist in jedem Fall

$$U \cap K_i \leq U \cap B \cap B^{s_i} = U_{s_i}.$$

Gelten die Fälle (A), (B) oder (C), so operiert $\overline{U}$ regulär auf Ω_i^* und daher ist $\overline{U}_{s_i} = 1$, denn U_{s_i} fixiert die Kammer Bs_i. Insbesondere gilt der letzte Teil des Lemmas. Im Fall (D) sehen wir aus 8.5.1 direkt $|B_{s_i} : K_i| = 2$ und $B = UK_i$, und dies beweist das Lemma. □

Wir sind nun in der Lage zu zeigen, dass U eine p-Gruppe ist. Es reicht zu zeigen, dass $|B : H|$ eine p-Potenz ist. Dies sehen wir leicht in dem folgenden

(8.5.3) Lemma.

Ist $|B : H|$ eine p-Potenz für eine Primzahl p, so ist U eine p-Gruppe.

Beweis. Die Gruppe U ist nilpotent, also ist $U = O_p(U) \times O_{p'}(U)$. Nach Voraussetzung ist $|U : U \cap H|$ eine p-Potenz, also ist notwendig $O_{p'}(U) \leq U \cap H$. Sei nun $g \in G = BNB$. Dann gibt es $x, y \in B$ und ein $n \in N$ mit $g = xny$. Sicherlich ist $O_{p'}(U) \trianglelefteq B$ und es folgt

$$O_{p'}(U)^{g^{-1}} = O_{p'}(U)^{n^{-1}x^{-1}} \leq H^{x^{-1}} \leq B.$$

Insbesondere ist $O_{p'}(U) \leq \bigcap_{g \in G} B^g = 1$, denn G operiert treu auf $\mathcal{B}$. □

Angenommen, es gibt eine ungerade Primzahl p mit $p \mid |B_{r_2} : H|$. Die folgenden Lemmata zeigen, dass dann $|B_{r_1} : H|$ eine p-Potenz ist. Vertauschen wir dann in den folgenden Lemmata die Rollen der Gruppen B_{r_1} und B_{r_2}, so sind $|B_{r_1} : H|$ und $|B_{r_2} : H|$ beides p-Potenzen. Gibt es keine solche Primzahl, so sind die beiden Indizes dann offenbar 2-Potenzen. In 8.2.6 haben wir bereits gesehen, dass $|B : H|$ Produkt von Potenzen dieser Indizes ist. Zusammen mit dem obigen Lemma folgt dann, dass U eine p-Gruppe ist.

(8.5.4) Lemma.

Es ist $O_p(U_{r_2}) \leq O_p(K_1)$.

Beweis. Nach Voraussetzung ist offenbar $p \mid |U_{r_2} : U_{r_2} \cap H|$ und wegen der Nilpotenz von U ist dann offenbar $O_p(U_{r_2})$ die nichttriviale p-Sylowgruppe von U_{r_2}. Natürlich ist $\ell(s_1 s_2) > l(s_1)$, also ist $B_{r_2} \leq B_{s_1}$ nach 8.2.4. Insbesondere ist dann

$$U_{r_2} = U \cap B_{r_2} \leq U \cap B_{s_1} = U_{s_1}.$$

Gilt für $i = 1$ der Fall (D), so ist $|U_{s_1} : U \cap K_1| = 2$. Nach unserer Annahme ist p ungerade, also ist $O_p(U_{r_2}) \leq U \cap K_1$. In allen anderen Fällen ist $U_{s_1} = U \cap K_1$ und somit gilt stets

$$O_p(U_{r_2}) \leq U \cap K_1.$$

Nun ist $U \cap K_1$ nilpotent, also enthält $O_p(U \cap K_1)$ offenbar sämtliche Elemente von p-Potenzordnung von $U \cap K_1$ und somit ist

$$O_p(U_{r_2}) \leq O_p(U \cap K_1).$$

Natürlich ist $O_p(K_1) \trianglelefteq B$, also folgt $O_p(K_1) \trianglelefteq F(B) = U$ und daher

$$O_p(K_1) \leq O_p(U \cap K_1).$$

Die umgekehrte Inklusion ist klar, denn $U \cap K_1 \trianglelefteq K_1$. Daher gilt auch $O_p(U \cap K_1) = O_p(K_1)$, und dies beweist das Lemma. □

Die Gruppe $G_{r_1} = \langle B_{r_1}, s_1 \rangle$ operiert nach 8.2.5 zweifach transitiv auf der Menge χ der Nebenklassen von B_{r_1} in G_{r_1} mit Kern

$$T_1 := \bigcap_{x \in G_1} B_{r_1}^x.$$

Wegen $B_{r_1} = HU_{r_1}$ ist

$$G_{r_1} = B_{r_1} \cup B_{r_1} s_i U_{r_1}$$

und der Stabilisator von B_{r_1} enthält den auf den von B_{r_1} verschiedenen Nebenklassen transitiven nilpotenten Normalteiler U_{r_1}. Wir können also den Hauptsatz 7.1 aus Kapitel 7 auf die Permutationsgruppe

$$\overline{G}_{r_1} := G_{r_1}/T_1$$

anwenden und erhalten direkt das

(8.5.5) Lemma.

Ist $\overline{M}_1 = \langle \overline{U}_{r_1}^{\overline{G}_{r_1}} \rangle$, *so gilt einer der folgenden Fälle:*

(I) Es ist $\overline{M}_1$ *ein einfacher Normalteiler von* $\overline{G}_{r_1}$.

(II) Es ist $\overline{G}_{r_1} = R(3) = R(3)'\overline{U}_{r_1}$.

(III) Es ist $\overline{M}_1$ *scharf zweifach transitiv auf* χ *und enthält einen auf* χ *regulären Normalteiler* $\overline{N}_1$ *mit* $\overline{M}_1 = \overline{N}_1\overline{U}_{r_1}$.

(IV) $\overline{G}_{r_1}$ *hat einen auf* χ *regulären Normalteiler* $\overline{N}_1$ *mit* $\overline{M}_1 = \overline{N}_1\overline{U}_{r_1}$ *und* $\overline{B}_{r_1} = \overline{U}_{r_1}$. *Ferner ist dann* $|\overline{U}_{r_1} \cap \overline{U}_{r_1}^{s_1}| = 2$.

In den ersten drei Fällen operiert $\overline{U}$ *regulär auf* $\chi \setminus \{B_{r_1}\}$.

(8.5.6) Lemma.

Für $i \leq 2$ *enthält die Gruppe* $\langle U_{r_i}^{G_{r_i}} \rangle$ *einen Repräsentanten von* s_i.

Beweis. Nach (8.2.5) und unserer Vorbemerkung ist offenbar

$$G_{r_i} = B_{r_i} \cup B_{r_i} s_i B_{r_i} = B_{r_i} \cup U_{r_i} s_i H U_{r_i}.$$

Angenommen $\langle U_{r_i}^{G_{r_i}} \rangle \leq B_{r_i}$. Dann ist natürlich $U_{r_i}^{s_i} \leq B \cap B^{w_0} = H$, ein Widerspruch zu (a) von 8.2.4. Somit ist

$$\langle U_{r_i}^{G_{r_i}} \rangle \cap U_{r_i} s_i H U_{r_i} \neq \emptyset$$

und $s_i H$ enthält ein Element in $\langle U_{r_i}^{G_{r_i}} \rangle$, wie gewünscht. □

(8.5.7) Lemma.

Es ist $O_{p'}(U_{r_1}) \leq T_1$.

Beweis. Sei $C_1 := C_{G_{r_1}}(O_p(K_1)))$, dann ist sicherlich $C_1 \trianglelefteq G_{r_1}$. Angenommen $O_{p'}(U_{r_1}) \not\leq T_1$. Dann ist insbesondere

$$\overline{C}_1 \cap \overline{M}_1 \trianglelefteq \overline{M}_1 \tag{8.6}$$

ein nichttrivialer Normalteiler von $\overline{M}_1$, denn es gilt

$$[O_{p'}(U_{r_1}), O_p(K_1)] \leq [O_{p'}(U), O_p(K_1)] \leq O_{p'}(U) \cap O_p(K_1) = 1. \tag{8.7}$$

Wir zeigen zuerst, dass C_1 einen Repräsentanten von s_1 enthält.

Im Fall (I) ist dies leicht zu sehen, denn hier ist $\overline{M}_1$ einfach und somit enthalten in $\overline{C}_1$. Nach 8.5.6 enthält nun C_1 einen Repräsentanten von s_1.

Im Fall (II) ist $\overline{M}_1 \cap \overline{C}_1 = R(3)'$ und enthält eine – und nach (8.6) alle – 2-Sylowgruppen von $\overline{M}_1$. Dies ist der Fall (f) aus 4.1 mit $|\chi| = 28$. Insbesondere ist jeder Zweipunktstabilisator von der Ordnung 2. Nach 8.5.6 ist $s_1 \in M_1$ wählbar und daher $\overline{s_1}^2 \in \overline{M}_1 \cap \overline{H}$. Somit stabilisiert $\overline{s}_1^2$ die Punkte B_{r_1} und $B_{r_1} s_1$ und daher ist $\overline{s}_1$ von der Ordnung 2 oder 4. In jedem Fall ist dann $\overline{s}_1$ in einer 2-Sylowgruppe von $\overline{M}_1$ enthalten. Nach 8.2.4 ist nun

$$T_1 \leq B_{r_1} \cap B_{r_1}^{s_1} \leq B \cap B^{w_0} = H,$$

also enthält C_1 einen Repräsentanten von s_1.

In den beiden übrigen Fällen ist dies schwieriger zu sehen. Wir wählen wieder einen Repräsentanten von s_1 in M_1 und es ist wieder $\overline{s}_1^2$ im Stabilisator der Punkte B_{r_1} und $B_{r_1} s_1$ von $\overline{M}_1$. Wegen der Regularität des Normalteilers $\overline{N}_1$ aus (III) und (IV) und der Dedekindidentität ist dies gerade $\overline{U}_{r_1} \cap \overline{U}_{r_1}^{s_1}$. In (III) ist diese Gruppe natürlich trivial und $\overline{s}_1$ ist von der Ordnung 2. In (IV) ist diese Gruppe von der Ordnung 2 und $\overline{s}_1$ ist von der Ordnung 2 oder 4. In allen Fällen ist also wieder $\overline{s}_1$ in einer 2-Sylowgruppe von $\overline{M}_1$ enthalten. Somit enthält C_1 wie in (II) einen Repräsentanten von s_1, wenn $\overline{M}_1 \cap \overline{C}_1$ eine 2-Sylowgruppe von $\overline{M}_1$ enthält.

In den Fällen (III) und (IV) ist $\overline{N}_1$ ein minimaler Normalteiler von $\overline{G}_{r_1}$. Daher ist $\overline{C}_1 \cap \overline{N}_1 = 1$ oder $\overline{N}_1 \leq \overline{C}_1$. Im ersten Fall zentralisieren sich $\overline{C}_1$ und $\overline{N}_1$ gegenseitig

und dies ist ein Widerspruch, da $\overline{N}_1$ in $\overline{G}_{r_1}$ sein eigener Zentralisator ist. Dies hatten wir im Anschluß an 7.1 vermerkt. Insbesondere ist also

$$\overline{N}_1 \leq \overline{C}_1.$$

Weiterhin ist $\overline{M}_1 = \overline{N}_1\overline{U}_{r_1}$ und p ist eine ungerade Primzahl. Somit enthält

$$O_2(\overline{U}_{r_1})\overline{N}_1 \leq \overline{C}_1$$

nach (8.7) eine 2-Sylowgruppe von $\overline{M}_1$, denn wegen der Nilpotenz von $\overline{U}_{r_1}$ ist $O_2(\overline{U}_{r_1})$ die 2-Sylowgruppe von $\overline{U}_{r_1}$.

In jedem Fall enthält also C_1 einen Repräsentanten von s_1 und damit können wir leicht den Widerspruch zu unserer Annahme vom Anfang herleiten. Nun ist nämlich

$$\ell(s_2s_1s_2) > \ell(s_2s_1)$$

und nach 8.2.4 gilt dann

$$B_{r_2} \leq B_{s_2s_1} = (B^-_{w_0s_1s_2})^{s_2s_1}.$$

Konjugation mit s_1 liefert

$$B_{r_2}^{s_1} \leq (B^-_{w_0s_1s_2})^{s_2}$$

und wegen $\ell(w_0s_1s_2) < \ell(w_0s_1)$ folgt mit (c) von 8.2.4 schließlich

$$B_{r_2} \cap (B^-_{w_0s_1s_2})^{s_2} = H.$$

Wir haben nun oben gezeigt, dass $O_p(K_1)$ von s_1h zentralisiert wird für ein $h \in H$ und dies gilt nach 8.5.4 auch für $O_p(U_{r_2})$. Somit wird $O_p(U_{r_2})$ von s_1 normalisiert und insbesondere ist

$$O_p(U_{r_2}) \leq U \cap B_{r_2} \cap B_{r_2}^{s_1} \leq U \cap B_{r_2} \cap (B^-_{w_0s_1s_2})^{s_2} = U \cap H.$$

Da aber $O_p(U_{r_2})$ die p-Sylowgruppe von U_{r_2} ist, folgt $p \nmid |U_{r_2} : U_{r_2} \cap H|$, ein Widerspruch zu unserer Annahme von Seite 107. □

Insbesondere ist nun endlich

$$O_{p'}(U_{r_1}) \leq U_{r_1} \cap T_1 \leq U_{r_1} \cap H$$

und wie gewünscht ist

$$|B_{r_1} : H| = |U_{r_1} : U_{r_1} \cap H|$$

eine p-Potenz. Wie bereits erklärt erhalten wir nun den

(8.5.8) Satz.

U ist eine p-Gruppe.

8.6 Projektive Ebenen

Sei G wie im letzten Abschnitt. Insbesondere ist nun $U = O_p(B) = F(B)$. Beide Gruppen L_i erfüllen nach 8.5.1 jeweils einen der vier Fälle (A)-(D) und es ist unser Ziel, denn Fall (D) auszuschließen. Wir betrachten hier den Fall $|W| = 6$ separat von den übrigen Fällen, denn dieser würde in dem nachfolgenden Abschnitt immer wieder zu technischen Schwierigkeiten führen. Nun ist $\mathcal{B}$ eine projektive Ebene und nach den Arbeiten von Higman & MacLaughlin [17] und Abe [1] ist G isomorph zu einer Untergruppe von $P\Gamma L_3(q)$, welche $PSL_3(q)$ enthält. Hierbei ist q eine p-Potenz. Unter diesem Isomorphismus wird P_1 auf den Stabilisator eines Punktes und P_2 auf den einer Geraden abgebildet, die diesen Punkt enthält. Insbesondere wird $B = P_1 \cap P_2$ auf den Stabilisator eines inzidenten Punkt-Geradenpaares abgebildet. Die Gruppen P_i/K_i sind daher Untergruppen von $P\Gamma L_2(q)$ und insbesondere sind die Gruppen L_i notwendig vom Typ (A) oder (C). Im Hinblick auf 8.5.1 erhalten wir das

(8.6.1) Lemma.

Für $|W| = 6$ und $i = 1, 2$ operiert UK_i/K_i regulär auf Ω_i^*.

8.7 Die nichtreguläre Operationen

Sei G wie im Abschnitt 8.5 und somit auch wieder $U = O_p(B) = F(B)$. Weiterhin sei $|W| > 6$. Wie im letzten Abschnitt erfüllen die Gruppen L_i nach 8.5.1 jeweils einen der vier Fälle (A)-(D) und wie eben werden wir den Fall (D) ausschließen. Im Hinblick auf 8.5.1 ist unser Ziel das folgende

(8.7.1) Lemma.

Für $i = 1, 2$ operiert UK_i/K_i regulär auf Ω_i^*.

Wir führen einen Widerspruchsbeweis in mehreren Schritten und dafür sei o.B.d.A. L_2 vom Typ (D). Im weiteren Verlauf des Abschnittes sei dazu $\widetilde{\ }$ bzw. $\overline{\ }$ der natürliche Homomorphismus von P_i auf P_i/K_i für $i = 1$ bzw. 2. Es gilt dann das

(8.7.2) Lemma.

Die Gruppe U ist eine 2-Gruppe und es gelten die folgenden Aussagen:

(a) Es ist $\overline{L}_2 \cong \mathbb{Z}_3^2 \cdot \overline{U}$, wobei $\overline{U}$ isomorph zu einer 2-Sylowuntergruppe von $GL_2(3)$ ist.

(b) Ist L_1 vom Typ (A), so ist $\widetilde{L}_1$ eine der einfachen Gruppen $SL_2(q)$, $Sz(q)$ oder $PSU_3(q)$.

(c) Ist L_1 vom Typ (C), so ist $\widetilde{L}_1$ isomorph zu einer der Gruppen $SL_2(2)$, $Sz(2)$ oder $PSU_3(2)$, oder $\widetilde{U}$ ist zyklisch der Ordnung 8 oder 16 ist.

Beweis. Wegen der Wahl von L_2 und 8.5.8 ist U eine 2-Gruppe der Ordnung $2(t^2-1)$ für eine Mersenne'sche Primzahl $t := 2^\alpha - 1$. Somit ist $t^2 - 1$ eine 2-Potenz und eine triviale Rechnung ergibt $t = 3$. Insbesondere ist $\overline{L}_2$ wie im obigen Lemma. Der Parameter t_2 aus 8.2.6 ist damit auch festgelegt durch

$$t_2 = 2^3.$$

Sei nun L_1 vom Typ (C). Hier ist der eindeutig bestimmte, minimale Normalteiler $\widetilde{N}$ von $\widetilde{L}_1$ scharf zweifach transitiv auf Ω_1 und nach 8.5.1 ist daher

$$|\widetilde{L_1}| = r^s(r^s - 1)$$

mit einer ungeraden Primzahl r und $r^s - 1 = 2^b$. Nach (1K) von Fong & Seitz [12] ist t_1 von der Form 2^j mit $(j, 3) = 1$ und $|j - 3| \leq 2$ oder 2^{3j} mit $|j - 1| \leq 2$. Eine triviale Rechnung ergibt die möglichen Werte für r und s. Entweder ist $s = 1$ und b eine 2-Potenz oder $s = 2$ und $b = r = 3$. Wegen $\widetilde{U} \leq Aut(\widetilde{N})$ ist nun $\overline{L}_1$ eine der Gruppen $SL_2(2)$, $Sz(2)$, $PSU_3(2)$ ist, oder $\overline{U}$ zyklisch der Ordnung 8 oder 16. □

Wir legen für den Rest des Abschnittes die Notation

$$U_i := U \cap K_i$$

für $i = 1, 2$ fest. Nach einleitenden Aussagen zeigen wir

$$C_{L_i}(U_i) \leq U_i$$

für $i = 1, 2$. Ist $\widetilde{L}_1$ keine lineare Gruppe, dann besitzt diese Gruppe genau wie $\overline{L}_2$ keinen FF-Modul. Wegen $C_{L_i}(U_i) \leq U_i$ lassen sich diese Fälle dann mit Hilfe von Standard-Amalgamargumenten behandeln, welche zur Entstehungszeit der am Anfang des Kapitels aufgeführten Arbeiten von Fong & Seitz noch nicht bekannt waren. Wir werden aber hierauf nicht weiter eingehen und behandeln nur noch den Fall, in dem $\widetilde{L}_1$ eine lineare Gruppe ist.

8.7.1 Einleitende Eigenschaften

(8.7.1.1) Lemma.

Es ist $H \cap K_1 \cap K_2 = 1$.

Beweis. Fixiert ein Automorphismus σ von $\mathcal{B}$ eine zur Kammer b gegenüberliegende Kammer und die Kammern aus $\Delta_1(b) \cup \Delta_2(b)$, so ist $\sigma = id$. Dies sehen wir aus I (4.8) bei Timmesfeld [34]. Die Kammern Bw_0 und B sind gegenüberliegend und H stabilisert sogar das ganze Apartment $\mathcal{A}$, also folgt offenbar die Behauptung. □

(8.7.1.2) Lemma.

Es ist $K_1 = U \cap K_1 = U_{s_1}$.

Beweis. Angenommen, K_1 enthält ein Element σ ungerader Ordnung. Sei $\sigma = uh$ für $u \in U$ und $h \in H$ geeignet. Wegen $\overline{B} = \overline{U}$ ist $\sigma \in K_1 \cap K_2$ und insbesondere $u \neq 1$. Dann ist aber $h^{-1}\sigma = u^h$ von 2-Potenzordnung k und da $K_1 \cap K_2$ von H normalisiert wird ist dann

$$h^{-k} \in H \cap K_1 \cap K_2 = 1.$$

Insbesondere ist h von 2-Potenzordnung, und dies ist wegen $U\sigma = Uh$ ein Widerspruch. Mit 8.5.2 folgt nun die Behauptung. □

(8.7.1.3) Lemma.

Es ist $L_2 \cap K_2 = U_2$.

Beweis. Wegen $\overline{L_2} \cong 3^2 \cdot 2^4$ ist $\overline{L_2}$ isomorph zu jeder ihrer Überlagerungsgruppen mit $2'$-Kern. Dies finden wir in (4D) von Fong & Seitz [12]. Aus 8.4.1 folgt sofort das Lemma. □

(8.7.1.4) Lemma.

Es gelten die folgenden Eigenschaften:

(a) B *ist auflösbar.*

(b) Die $2'$*-Untergruppen von* H *sind Untergruppen von* K_2.

(c) Es ist $|H \cap K_1| \leq 2$.

(d) Ist L_1 *nicht vom Typ (D), so ist* $O_2(H) = U \cap H = H \cap K_1$

Beweis. Im ersten Teil müssen wir nur den Fall betrachten, in dem P_1 nicht auflösbar ist. Nach 8.5.1 ist HK_1/K_1 auflösbar und da K_1 nun auflösbar ist, ist (a) klar. Der Teil (b) folgt sofort aus $\overline{B} = \overline{U}$. Nach 8.7.1.1 ist

$$H \cap K_1 \cong (H \cap K_1)/(H \cap K_1 \cap K_2) \cong (H \cap K_1)K_2/K_2 \leq U_{s_2}K_2/K_2 \cong \mathbb{Z}_2,$$

denn nach 8.7.1.2 und 8.2.4 ist

$$H \cap K_1 \leq U \cap H = U_{s_i} \cap U_{r_i}.$$

Dies beweist (c) und es bleibt der letzte Teil zu zeigen. Dieser ist mit 8.3.1 klar, denn hier gilt $K_1 = U_{s_1}$. □

(8.7.1.5) Lemma.

Ist L_1 vom Typ (A), dann gilt:

(a) $H \cap L_1$ besitzt genau eine nichttriviale $2'$-Halluntergruppe H_0.

(b) H_0 ist N-invariant.

(c) Es ist $C_U(H_0) \leq K_1$ und insbesondere $U = K_1U_2$.

(d) $P_2 = (K_2 \cap L_1)N_{P_2}(H_0)$.

Beweis. Nach 8.5.1 ist $\widetilde{L}_1$ eine der einfachen Gruppen $PSL_2(q)$, $PSU_3(q)$ oder $Sz(q)$. Insbesondere ist jeder Zweipunktstabilisator von $\widetilde{L}_1$ eine $2'$-Gruppe. Wegen $K_1 \leq L_1$ ist

$$\begin{aligned}\widetilde{H} \cap \widetilde{L}_1 = \widetilde{H \cap L_1} &\cong (H \cap L_1)/(H \cap L_1 \cap K_1) \\ &= (H \cap L_1)/O_2(H)\end{aligned}$$

ein solcher Stabilisator von $2'$-Ordnung und daher ist

$$H \cap L_1 = H_0O_2(H)$$

für eine $2'$-Halluntergruppe H_0. Nun ist $|H \cap L_1 : H_0| \leq 2$, also ist sogar

$$H \cap L_1 = H_0 \times O_2(H)$$

und H_0 ist die einzige $2'$-Halluntergruppe von $H \cap L_1$.

Offenbar ist dann H_0 auch invariant unter s_1 und H. Nun ist $H_0 \leq K_2$ und (ein Repräsentant von) s_2 liegt in L_2 nach 8.7.1.4 und 8.5.6. Nach 8.7.1.3 ist $L_2 \cap K_2 = U \cap K_2$ und daher

$$[H_0, s_2] \leq H \cap L_2 \cap K_2 = H \cap U \cap K_2 = H \cap K_1 \cap K_2 = 1,$$

nach 8.7.1.1 und 8.7.1.4. Damit folgt sofort (b).

Sicherlich operiert $(H \cap L_1)K_1/K_1$ fixpunktfrei auf U/K_1 und daher ist $C_U(H_0) \leq K_1$. Offenbar operiert nun H_0 teilerfremd auf U und daher ist

$$U = C_U(H_0)[U, H_0] \leq K_1(U \cap K_2)$$

und es folgt (c).

Es bleibt der letzte Punkt zu zeigen. Die Gruppe $K_2 \cap L_1$ ist wegen $s_2 \in L_2$ und

$$[K_2 \cap L_1, s_2] \leq K_2 \cap L_2 = K_2 \cap U \leq K_2 \cap L_1$$

offenbar ein Normalteiler von P_2. Ferner operiert $K_2 \cap L_1$ transitiv auf seinen $2'$-Halluntergruppen und aus dem Frattiniargument folgt die Behauptung, denn H_0 ist wegen

$$K_2 \cap L_1 \leq UH \cap L_1 = U(H \cap L_1)$$

und $H_0 \leq K_2$ eine solche $2'$-Halluntergruppe. □

(8.7.1.6) Lemma.

Es ist $R_2 := \langle U_{r_2}, U_{r_2}^{s_2}\rangle \cong \mathbb{Z}_3^2 \cdot S$ *mit einer auf* $(\mathbb{Z}_3^2)^\sharp$ *transitiven Untergruppe* S *von einer 2-Sylowgruppe von* $GL_2(3)$. *Weiterhin ist* $[R_2, H_0] = 1 = R_2 \cap H_0$, *wenn* L_1 *vom Typ (A) ist.*

Beweis. Offenbar ist $K_2 \leq B_{s_2}$ und nach 8.2.5 und 8.2.4 ist daher

$$R_2 \cap K_2 \leq (B_{r_2} \cap B_{s_2}) \cup (B_{r_2} s_2 B_{r_2} \cap B_{s_2}) = B_{r_2} \cap B_{s_2} = H.$$

Nun ist offenbar $R_2 \leq L_2$ und daher

$$R_2 \cap K_2 \leq L_2 \cap K_2 = U \cap K_2.$$

Mit 8.7.1.4 folgt zusammen

$$R_2 \cap K_2 \leq U \cap H \cap K_2 = H \cap K_1 \cap K_2 = 1$$

und insbesondere ist

$$R_2 \cong R_2K_2/K_2 \leq \overline{L}_2.$$

Offenbar operiert R_2 wegen $U = U_{s_i} U_{r_i}$ zweifach transitiv auf $\Delta_2(B)$ und der erste Teil der Behauptung läßt sich nun leicht ablesen. Ist L_1 vom Typ (A), so folgt

$$[R_2, H_0] \leq R_2 \cap K_2 = 1.$$

Schließlich ist

$$H_0 \cap L_2 \leq H_0 \cap K_2 \cap L_2 = H_0 \cap U_2 = 1,$$

und es folgt das Lemma. □

8.7.2 Zentralisatoren von U_i in L_i

(8.7.2.1) Lemma.

Ist L_1 *vom Typ (A), so ist* $C_{L_1}(K_1) \leq K_1$.

Beweis. In diesem Fall ist L_1/K_1 einfach und daher ist offenbar $F(L_1) = K_1$ und $F^*(L_1) = K_1$ oder L_1. Im ersten Fall folgt offenbar die Behauptung und im zweiten Fall ist $L_1 = K_1 * E(L_1)$. Nach 8.7.1.5 gilt $C_U(H_0) \leq K_1$. Wir zeigen die umgekehrte Inklusion. Ist $h \in H_0$, so ist $h = ue$ für $u \in K_1$ und $e \in E(L_1)$. Da u und e vertauschen, u von 2-Potenzordnung und h von $2'$-Ordnung ist, gilt notwendig $u = 1$. Daher wird $H_0 \leq E(L_1)$ von K_1 zentralisiert und es folgt $C_U(H_0) = K_1$. Insbesondere ist damit

$$C_{U_2}(H_0) = K_1 \cap K_2.$$

Nach 8.7.1.5 (c) und wegen $U_2 = L_2 \cap K_2$ ist somit $K_1 \cap K_2 \trianglelefteq P_2$ und daher

$$G = \langle P_2, E(L_1)\rangle \leq N(K_1 \cap K_2).$$

Es folgt notwendig $K_1 \cap K_2 = 1$ und daher ist

$$U_{s_1} = K_1 \cong K_1K_2/K_2 \leq B/K_2$$

höchstens von der Ordnung 2^4. Wegen $|U \cap H| \leq 2$ führt dies mit 8.2.6 durch eine leichte Rechnung zu einem Widerspruch. □

(8.7.2.2) Folgerung.

Ist L_1 vom Typ (A), so ist $K_1 \cap K_2 \not\trianglelefteq P_2$.

Beweis. Die Gruppe $H_0 \leq K_2$ operiert teilerfremd auf K_1. Daher ist

$$[K_1, H_0] = [K_1, H_0, H_0] \leq [K_1 \cap K_2, H_0] \leq [K_1, H_0]$$

und es folgt Gleichheit. Ist die Behauptung falsch, dann ist $[K_1 \cap K_2, H_0] = [K_1, H_0]$ nach 8.7.1.5 invariant unter Konjugation mit N. Da die Kammer B von $[K_1, H_0]$ fixiert wird, wird daher das Apartment $\mathcal{A} = \{Bw \mid w \in W\}$ kammernweise fixiert. Wegen

$$[K_1, H_0] \leq K_1 \cap K_2$$

folgt dann $[K_1, H_0] = 1$ aus I (4.8) bei Timmesfeld [34]. Dies ist das selbe Argument wie in 8.7.1.1 und liefert einen Widerspruch zu obigem Lemma. □

(8.7.2.3) Lemma.

Ist L_1 vom Typ (C), so ist $C_{L_1}(K_1) \leq K_1$.

Beweis. Hier ist $\widetilde{L}_1$ Produkt eines elementarabelschen Normalteilers mit $\widetilde{U}$. Sei N das Urbild dieses Normalteilers in P_1. Offenbar ist $\widetilde{F(L_1)}$ enthalten in $F(\widetilde{L}_1)$ und da $\widetilde{U}$ transitiv auf $\widetilde{N}^\sharp$ operiert, ist dann $F(L_1) = K_1$ oder $F(L_1) = K_1 * N$. Da L_1 auflösbar ist, ist $F^*(L_1) = F(L_1)$, also folgt im ersten Fall die Behauptung. Im zweiten Fall ist $N \trianglelefteq P_1$ und daher $N(N) = P_1$. Andernfalls ist $N \trianglelefteq G$, ein Widerspruch zu 8.2.3.

Wir betrachten zuerst die Fälle, in denen $\widetilde{L}_1$ eine der Gruppen $SL_2(2)$ oder $3^2 \cdot \mathbb{Z}_8$ ist. Im ersten Fall ist $\widetilde{L}_1 = \widetilde{P}_1$, und da K_1 eine 2-Gruppe ist, ist N eine 3-Sylowgruppe von P_1. Im anderen Fall erhalten wir das selbe Resultat, denn

$$\widetilde{P}_1/\widetilde{N} \leq Aut(\widetilde{N}) = V_4.$$

Insbesondere ist N eine 3-Sylowgruppe von G, denn andernfalls betten wir N in eine größere 3-Gruppe ein, die N normalisiert, ein Widerspruch zu $N(N) = P_1$. Nach den Ordnungsformeln aus 8.2.6 sind die 3-Sylowgruppen wegen $|W| > 6$ von der Ordnung mindestens 3^3 und dies ist erneut ein Widerspruch.

Ist $\widetilde{L}_1 \cong PSU_3(2)$, so ist N von der Ordnung 3^2 und der 3-Anteil von P_1 ist 3^2 oder 3^3, denn

$$\widetilde{P}_1/\widetilde{N} \leq Aut(\widetilde{N}) = GL_2(3).$$

Im ersten Fall folgt wie oben der Widerspruch. Sei also T eine 3-Sylowgruppe der Ordnung 3^3 von P_1. Hier ist in 8.2.6 gerade t_1t_2 kein Quadrat, also ist $|W| \neq 12$ nach dem Satz von Feit & Higman [38]. Insbesondere ist dann T nach 8.2.6 keine 3-Sylowgruppe von G. Daher wird T von einer Gruppe T_1 der Ordnung 3^4 normalisiert. Ist dann $t \in T_1 \setminus (T_1 \cap P_1)$, so ist

$$T = NN^t = N^tN^{t^2}.$$

Insbesondere ist

$$Z(T) = N \cap N^t \cong \mathbb{Z}_3$$

invariant unter T_1. Andererseits ist $Z(T) \trianglelefteq P_1$ und somit

$$G = \langle P_1, T_1 \rangle \leq N(Z(T)),$$

offenbar ein Widerspruch.

Es bleiben die Fälle zu untersuchen, in denen $\widetilde{L}_1$ eine der Gruppen $Sz(2)$ oder $\mathbb{Z}_{17} \cdot \mathbb{Z}_{16}$ ist. Sei dazu $\mathcal{A} = \{Bw \mid w \in W\}$ ein Apartment in $\mathcal{B}$. Dabei ist $\mathcal{A}$ nach dem Satz von Feit & Higman [38] ein 4-Eck oder ein 8-Eck, denn bei den 6-Ecken ist das Produkt der Parameter $t_i = \Delta_i(B) \setminus \{B\}$ ein Quadrat. Aus pragmatischen Gründen benutzen wir die Notation der Gebäude von Tits & Weiss [36], in der das Gebäude ein bipartiter Graph mit den Ecken P_ix mit $i = 1, 2$ und $g \in G$ ist. Dabei ist $\{P_1x, P_2y\}$ eine Kante genau dann, wenn $P_1x \cap P_2y \neq \emptyset$. Seien nun $x_4 = P_1$, $x_3 = P_2$ und $x_2 = P_1s_2$ drei Kammern auf einem 2-Pfad. Mit $G_x^{[i]}$ bezeichnen wir den (punktweisen) Stabilisator der Ecken vom Abstand höchstens 2 von x. Dann ist offenbar $K_1 \leq G_{x_4}^{[1]}$ und $K_2 \leq G_{x_3}^{[1]}$. Nach unserer Annahme enthält $F(L_1)$ einen auf $\Delta(x_4)$ transitiven Normalteiler, der K_1 zentralisiert. Insbesondere ist

$$K_1 \cap K_2 \leq G_{x_4}^{[2]}$$

und somit auch

$$K_1^{s_2} \cap K_2 \leq G_{x_2}^{[2]}.$$

Somit fixiert $K_1 \cap K_2 \cap K_1^{s_2}$ einen Pfad der Länge 5.

Ist $n = 4$, so fixiert diese Gruppe ein ganzes Apartment und somit ist wieder

$$K_1 \cap K_2 \cap K_1^{s_2} = 1$$

nach I (4.8) von Timmesfeld [34]. Wegen $K_1 \cap K_2 = K_1 \cap U_2$ ist nun andererseits

$$U_2/(K_1 \cap K_2) \cong \widetilde{U}_2 \leq \widetilde{U},$$

und daher $|U_2 : K_1 \cap K_2| \leq 2^i$ mit $i = 2$ bzw. 4, wenn $\widetilde{L}_1$ isomorph zu $Sz(2)$ bzw. $\mathbb{Z}_{17} \cdot \mathbb{Z}_{16}$ ist. Nach der Produktformel für Untergruppen ist nun

$$|U_2|^2 \leq 2^{2i} \cdot |K_1 \cap K_2| \cdot |K_1^{s_2} \cap K_2| \leq 2^{2i} \cdot |U_2|,$$

und somit $|U_2| \leq 2^4$ bzw. 2^8. Nach 8.5.2 und wegen $|U_{s_2} : U_2| = 2$ ist aber $|U_2| \geq 2^8$ bzw. 2^{10}, ein Widerspruch.

Im Fall $n = 8$ bilden wir die Ecke x_3 unter N auf eine Ecke x_5 ab, und erhalten einen 8-Pfad $(x_0, x_1, \ldots, x_8)$, welcher punktweise von $K_1 \cap K_2 \cap K_1^{s_2}$ fixiert wird. Wir beachten dabei, dass die Kammern wegen $n = 8$ paarweise verschieden sind. Nach Konstruktion ist

$$K_1 \cap K_2 \cap K_1^{s_2} \leq G_{x_i}^{[1]}$$

für $i = 1, \ldots, 7$ und insbesondere in einer Wurzeluntergruppe von $\mathcal{B}$ enthalten. Da diese aber fixpunktfrei auf den Residuen einer Ecke operieren, ist somit

$$|K_1 \cap K_2 \cap K_1^{s_2}| \leq 2^2 \text{ bzw. } 2^3.$$

Nun ist wie eben $|K_1 \cap K_2| \geq \frac{|U_2|}{2^i}$ für $i = 2$ bzw. 4. Mit der Ungleichung

$$|U_2| \geq \frac{|K_1 \cap K_2| \cdot |K_1^{s_2} \cap K_2|}{|K_1 \cap K_1^{s_2} \cap K_2|}$$

erhalten wir

$$2^2|U_2| \geq |K_1 \cap K_2|^2 \geq \frac{|U_2|^2}{2^{2i}}$$

und umgeformt

$$|U_2| \leq 2^{2i+2}.$$

Dies ist nach der üblichen Ordnungsformel offenbar ein Widerspruch, und es folgt das Lemma. □

(8.7.2.4) Lemma.

Ist L_1 vom Typ (D), so ist $C_{L_1}(K_1) \leq K_1$.

Beweis. Hier ist $\widetilde{L}_1 = \widetilde{P}_1 \cong 3^2 \cdot 2^4$, und genau wie im letzten Lemma ist $F^*(L_1) = K_1$ oder $F^*(K_1) = K_1 * N$ mit $\widetilde{N} = O_3(\widetilde{N}_1)$. Im ersten Fall folgt die Behauptung und im zweiten Fall ist N wieder eine 3-Sylowgruppe von G, denn 3^2 ist hier der 3-Anteil von P_1. Dies ist aus Ordnungsgründen ein Widerspruch. □

(8.7.2.5) Lemma.

Es ist $C_{L_2}(U_2) \leq U_2$.

Beweis. Natürlich ist L_2 auflösbar und daher ist $F^*(L_2) = F(L_2)$. Sei N das Urbild von $O_3(\overline{L}_2)$ in L_2. Da $\overline{U}$ transitiv auf $\overline{N}^\sharp$ operiert, ist $F^*(L_2) = U_2$ oder $F^*(L_2) = N \times U_2$. Im ersten Fall folgt offenbar die Behauptung und im zweiten Fall ist $N(N) = P_2$ wie im Beweis zu 8.7.2.3. Ist K_2 eine $3'$-Gruppe, so ist 3^2 eine 3-Sylowgruppe von P_2 und daher auch wieder von G, ein Widerspruch.

Ist K_2 keine $3'$-Gruppe, so ist wegen $\widetilde{K}_2 \leq \widetilde{B}$ entweder L_1 vom Typ (A), oder $\widetilde{L}_1 \cong PSU_3(2)$. Im ersten Fall ist $[K_1, H_0] = [K_1 \cap K_2, H_0]$ invariant unter s_1. Wegen $N \leq C(U_2)$ und $P_2 = NB$ sowie $K_1 \cap K_2 \leq U_2$ ist dann obiger Kommutator wegen

8.7.1.5 auch invariant unter s_2. Wie im Beweis zu 8.7.2.2 folgt dann $[K_1, H_0] = 1$, ein Widerspruch wegen $C_{L_1}(K_1) \leq K_1$.

Ist $\widetilde{L}_1 \cong PSU_3(2)$, so ist der 3-Anteil von B/K_1 höchstens von der Ordnung 3 und daher ist $|K_2|_3 = 3$. Somit ist $|P_2|_3 = 3^3$, und die Behauptung folgt wie im Beweis zu 8.7.2.3 im Fall $\widetilde{L}_1 \cong PSU_3(2)$. □

8.7.3 Moduln und FF-Moduln

Sei X eine endliche Gruppe und V ein treuer $\mathbb{Z}_pX$-Modul. Besitzt X eine elementarabelsche p-Untergruppe A mit $|V : C_V(A)| \leq |A|$, so nennen wir V einen *failure-factorisation-Modul* von X oder kurz *FF-Modul*. In diesem Unterabschnitt werden wir wie zu Beginn des Abschnittes angekündigt zeigen, dass die Gruppen vom Typ (A) - (D) bis auf die linearen Gruppen keinen FF-Modul haben.

(8.7.3.1) Lemma.

Sei $X = R_2$ oder $\overline{L}_2$ und V ein kX-Modul für einen Körper k (mit von 3 verschiedener Charakteristik). Operiert $O_3(X)$ nichttrivial auf V, so ist $dim_k(V) \geq 8$.

Beweis. Natürlich besitzt V eine X-Kompositionsreihe und X operiert dann irreduzibel auf jedem Hauptfaktor dieser Reihe. Wegen $char(k) \neq 3$ operiert $O_3(X)$ nichttrivial auf einem dieser Hauptfaktoren und somit ist V o.B.d.A. ein irreduzibler kX-Modul. Da $O_3(X)$ teilerfremd auf V operiert, wird V von den Zentralisatoren $C_V(d)$, $d \in O_3(X)^\sharp$ erzeugt. Sind $d, e \in O_3(X)^\sharp$ mit $e \neq d, d^2$, so ist

$$C_V(d) \cap C_V(e) = C_V(O_3(X))$$

invariant unter X und wegen der Irreduziblität der Operation somit trivial. Insbesondere gibt es vier solcher $kO_3(X)$-Untermoduln, die in S zueinander konjugiert sind, wobei S eine 2-Sylowgruppe von X ist.

Zu einer Involution $z \in S$ wählen wir eine Basis (a, b) von $O_3(X)$ derart, dass a und $-a$ von z vertauscht werden, sowie b und $-b$ von z vertauscht oder festgelassen werden. Die Existenz einer solchen Basis erhalten wir durch leichtes Nachrechnen in der Operation der Untergruppe $S \leq GL_2(3)$ auf $O_3(X)$. Wir betrachten nun die offenbar nichttriviale Operation von a auf $C_V(b)$. Hat a auf $C_V(b)$ einen Eigenvektor zum Eigenwert λ, so ist

$$\lambda v^z = (v^z)^a = v^{zaz^2} = v^{a^2z} = \lambda^2 v^z,$$

und daher ist dann $\lambda = 1$.

Insbesondere ist jeder nichttriviale $O_3(X)$-Untermodul von $C_V(e)$ für $e \in O_3(X)^\sharp$ mindestens zweidimensional. Außerdem sind verschiedene Zentralisatoren $C_V(e)$ nicht

$O_3(X)$-isomorph und daher liegen die irreduziblen $O_3(X)$-Untermoduln von verschiedenen Zentralisatoren in verschiedenen homogenen $O_3(X)$-Komponenten von V. Nach dem Satz von CLIFFORD [2] ist V aber die direkte Summe der $O_3(X)$-Komponenten, und insbesondere ist V nun mindestens achtdimensional. □

(8.7.3.2) Lemma.

Sei X vom Typ (A) - (D), aber verschieden von $PSL_2(q)$. Dann hat X keinen FF-Modul.

Beweis. Für die unitären Gruppen und die Suzukigruppen erhalten wir die Aussage direkt bei COOPERSTEIN [10] und es bleiben die übrigen Gruppen zu betrachten. Sei S im folgenden eine 2-Sylowgruppe von X. Angenommen, X hat einen FF-Modul V. Dann enthält S eine elementarabelsche Untergruppe A mit $|V : C_V(A)| \leq |A|$.

Sei zuerst X wie im Fall (D), und damit offenbar auch $|A| \leq 4$. Wir betrachten zuerst den Fall $|A| = 2$, in dem $C_V(A)$ eine *Hyperebene* ist. Offenbar gibt es dann ein $d \in O_3(X)$ mit $A^d \neq A$ und insbesondere ist

$$[a, d] =: e \in O_3(X)^\sharp.$$

Somit ist

$$C_V(e) \geq C_V(A) \cap C_V(A^d) \equiv H_1 \cap H_2$$

und $C_V(e)$ enthält einen Unterraum der Codimension 2. Offenbar ist $C_V(e)$ keine Hyperebene, also ist

$$C_V(e) = C_V(A) \cap C_V(A^d) \leq C_V(A).$$

Offenbar ist nun

$$O_3(X) = \langle e, f \rangle$$

für ein geeignetes $f \in O_3(X)$. Da S transitiv auf $O_3(X)^\sharp$ operiert, ist $O_3(X)$ der Schnitt von vier Hyperebenen und daher

$$codim(C_V(O_3(X))) \leq 4.$$

Nach dem letzten Lemma ist insbesondere $C_V(O_3(X)) \neq 0$ und wir können die Operation von X auf dem Modul

$$\overline{V} := V/C_V(O_3(X))$$

mit $C_{\overline{V}}(O_3(X)) = 0$ betrachten. Da e teilerfremd auf V operiert, ist $\overline{C_V(e)} = C_{\overline{V}}(e)$. Ferner ist $C_{\overline{V}}(e)$ der Schnitt der beiden Hyperebenen $\overline{H}_i$ und somit von der Codimension 2. Wie eben ist $C_{\overline{V}}(O_3(X))$ höchstens von der Codimension 4, ein Widerspruch.

Es bleibt der Fall $|A| = 4$, in dem wir mit Matrizen leicht nachrechnen, dass A die zentrale Involution z von S enthält. Insbesondere ist $codim(C_V(z)) = 2$, sonst sind wir im ersten Fall. Genau wie oben ist nun

$$C_V(z) \cap C_V(z^d) \leq C_V(e)$$

für geeignete $d, e \in O_3(X)^\sharp$. Insbesondere ist $codim(C_V(e)) \leq 4$ und sicherlich ist $C_V(e)$ keine Hyperebene. Weiterhin ist $codim(C_V(e)) < 4$, denn sonst ist

$$C_V(e) \leq C_V(z),$$

und Konjugation mit S liefert $C_V(d) \leq C_V(z)$ für alle $d \in O_3(X)^\sharp$. Da $O_3(X)$ teilerfremd auf V operiert und nicht zyklisch ist, erhalten wir

$$V = \langle C_V(f) \mid f \in O_3(X)^\sharp \rangle \leq C_V(z),$$

ein Widerspruch.

Somit bleiben die Fälle, in denen $C_V(e)$ von der Codimension 2 oder 3 ist. Hier ist $C_V(e)$ der Schnitt von zwei bzw. drei Hyperebenen und daher $C_V(O_3(X))$ wie oben der Schnitt von maximal sechs Hyperebenen. Insbesondere ist $codim(C_V(O_3(X))) \leq 6$ und somit $C_V(O_3(X)) \neq 0$. Ausfaktorisieren von $C_V(O_3(X))$ aus V liefert wie oben einen Widerspruch.

Sei schließlich X wie in (C). Dann ist natürlich $|A| = 2$ und A enthält die zentrale Involution von S. Es folgt wie oben, dass

$$C_V(A) \cap C_V(A^d) = C_V(e)$$

von der Codimension 2 in V ist, für geeignete $d, e \in O_{2'}(X)$. Da S transitiv auf $O_{2'}(X)^\sharp$ operiert, enthält $C_V(A)$ sämtliche Unterräume $C_V(f)$ mit $f \in O_{2'}(X)^\sharp$. Der Fall $X = \mathbb{Z}_{17} \cdot \mathbb{Z}_{16}$ tritt offensichtlich nicht ein, also ist $O_{2'}(X) = O_3(X)$ nicht zyklisch und operiert teilerfremd auf V. Insbesondere ist

$$V = \langle C_V(f) \mid f \in O_3(X)^\sharp \rangle \leq C_V(A),$$

ein Widerspruch. □

8.7.4 Lineare Gruppen

Wie angekündigt schließen wir nur noch aus, dass $\widetilde{L}_1$ eine lineare Gruppe ist. Sei dazu

$$N_2 := \bigcap_{x \in P_2} (K_1 \cap U_2)^x.$$

Nach den letzten Abschnitten können wir nun $C_{L_i}(U_i) \leq U_i$ für $i = 1, 2$ verwenden und erhalten die beiden folgenden Sätze.

(8.7.4.1) Satz.

Es ist $\widetilde{L}_1 \ncong PSL_2(q)$ für $q > 2$.

Beweis. Angenommen die Behauptung ist falsch. Wegen $U = K_1U_2$ ist

$$U_2/(K_1 \cap K_2) \cong U/K_1$$

elementarabelsch und wir sehen leicht, dass auch die Gruppe U_2/N_2 elementarabelsch ist. Ferner operiert $O_3(R_2)$ nichttrivial auf U_2/N_2, denn andernfalls ist $[U_2, O_3(R_2)] \leq N_2$ und dann insbesondere

$$[K_1 \cap U_2, O_3(R_2)] \leq K_1 \cap U_2.$$

Dann aber ist $K_1 \cap U_2 \trianglelefteq P_2$, denn R_2 enthält einen Repräsentanten von s_2. Dies ist ein Widerspruch zu 8.7.2.2, also operieren die Gruppen $H_0 \times R_2$ und $O_3(R_2)$ nichttrivial auf U_2/N_2.

Natürlich operiert H_0R_2 irreduzibel auf jedem Hauptfaktor einer H_0R_2-Kompositionsreihe von U_2/N_2 und $O_3(R_2)$ muss offenbar nichttrivial auf einem Hauptfaktor $\widehat{U}_2$ operieren. Nun operiert $\widetilde{H}_0$ fixpunktfrei auf $\widetilde{U}$, also ist insbesondere $C_{U_2}(x) \leq K_1 \cap U_2$ für alle $x \in H_0^\sharp$. Da H_0 invariant unter s_2 ist, ist dann auch $C_{U_2}(x) \leq N_2$ für alle $x \in H_0^\sharp$. Insbesondere operiert H_0 (elementweise) fixpunktfrei auf U_2/N_2. Da H_0 teilerfremd auf U_2/N_2 operiert, operiert dann H_0 auch fixpunktfrei auf dem Hauptfaktor $\widehat{U}_2$.

Insgesamt ist dann $H_0 \leq End_{H_0R_2}(\widehat{U}_2)$ nach dem Lemma von Schur ein Körper und hat somit mindestens $|H_0| + 1 \geq q$ Elemente. Da $O_3(R_2)$ nichttrivial auf $\widehat{U}_2$ operiert, ist $\widehat{U}_2$ mindestens von der Dimension 8 über diesem Körper und es folgt

$$|\widehat{U}_2| \geq q^8.$$

Nach der Ordnungsformel aus 8.2.6 ist aber

$$|U : U \cap H| \leq (2^3 q)^{\frac{|W|}{4}}.$$

Dies ist für $q > 4$ ein Widerspruch, wenn wir beachten, dass nach dem Satz von Feit & Higman [38] für $q = 8$ gerade $|W| \neq 12$.

Für den Fall $q = 4$ führt dieses Argument nur auf die Möglichkeit $|W| = 16$. Insbesondere ist dann

$$|U_{s_2} : U \cap H| = (2^2)^4 \cdot (2^3)^3 = 2^{17}.$$

Wegen $|U_{s_2} : U_2| = 2$ ist daher U_2 von der Ordnung 2^{16} bzw. 2^{17} und dies ist genau dann der Fall, wenn $|U \cap H| = 1$ bzw. 2.

Die Gruppe R_2 können wir in obiger Argumentation auch durch die Gruppe $\overline{L}_2$ ersetzen, denn stets ist U_2 wegen $U_2' \leq N_2$ im Kern der entsprechenden Operation und $H_0 \cap L_2 = 1$. Wegen $[H_0, L_2] \leq L_2 \cap K_2 = U_2$ vertauschen die Gruppen H_0 und $\overline{L}_2$ in der obigen Operation.

Wir starten nun mit dem Fall $|U_2| = 2^{17}$ mit $U_2' \neq 1$. Dann ist natürlich auch $|N_2| = 2$ und $\widehat{U}_2 = U_2/N_2$. Insbesondere ist U_2 extraspeziell und für $Z := Z(U)$ ist

$$Z = Z(U_2) \leq Z(U_1)$$

wegen $C_{L_i}(U_i) \leq U_i$ für $i \leq 2$. Da Z von K_1 zentralisiert wird und $\overline{L}_1$ genau fünf 2-Sylowgruppen hat, ist

$$V_1 := \langle Z^{L_1} \rangle \leq U$$

offenbar eine elementarabelsche Gruppe der Ordnung höchstens 2^5. Die nichttrivialen A_5-Moduln sind mindestens vierdimensional und es ist leicht zu sehen, dass V_1 ein vierdimensionaler, orthogonaler $\widetilde{L}_1$-Modul ist. Wir beachten hierbei, dass V_1 von $K_1 \trianglelefteq L_1$ zentralisiert wird. Daher ist

$$V_1 \not\leq U_2,$$

denn andernfalls ist

$$[V_1, U_2] \leq U_2' = Z,$$

und U_2 operiert (modulo K_1) als Transvektionsgruppe zu Z auf V_1. Daher ist auch aus Ordnungsgründen

$$0 < Z < [V_1, U_2] = V_1 \cap U_2 < V_1$$

und $|[V_1, U_2]| = 2^3$. Insbesondere ist dann $\overline{V}_1$ ein Normalteiler von $\overline{U}$, und enthält somit die zentrale Involution von $\overline{U}$. Daher ist

$$W := \langle \overline{V}_1^{P_2} \rangle \leq \langle \overline{V}_1, \overline{V}_1^d, \overline{V}_1^e \rangle$$

mit $\langle e, d \rangle = O_3(\overline{L}_2)$, und daher ist $[U_2/Z, W]$ ein höchstens sechsdimensionaler und $\overline{L}_2$-invarianter Unterraum von U_2/Z. Dies ist ein Widerspruch zur Irreduziblität der Operation.

Sei nun $|U_2| = 2^{17}$ mit $U_2' = 1$. Ist $|N_2| = 2$, dann können wir Z in der obigen Argumentation durch N_2 ersetzen. Es ist nämlich $[N_2, P_2] = 1$ und daher operiert $\widetilde{L}_1$ nichttrivial auf $V_1 := \langle N_2^{L_1} \rangle$. Da N_2 von K_2 zentralisiert wird, ist wie oben $2^4 \leq |V_1| \leq 2^5$. Auch hier ist $V_1 \not\leq U_2$, sonst zentralisiert $\widetilde{U}$ die Gruppe V_1 und daher auch $N_2^{s_1}$. Insbesondere operiert dann $\widetilde{U}^{s_1}$ trivial auf N_2 und daher ganz $\overline{L}_1$. Somit ist $N_2 \trianglelefteq \langle P_2, L_1 \rangle = G$, ein Widerspruch. Der Kommutator $[V_1, U_2]$ hat die Ordnung 2^3 und wie oben produziert dies einen echten Untermodul von U_2/N_2, ein Widerspruch.

Ist $N_2 = 1$, so ist U_2 elementarabelsch und da $O_3(\overline{U}_2)$ teilerfremd auf U_2 operiert, ist

$$U_2 = [U_2, O_3(\overline{L}_2)] \oplus C_{U_2}(O_3(\overline{L}_2))$$

und $N := C_{U_2}(O_3(\overline{L}_2))$ ist von der Ordnung 2. Offenbar gilt wieder $[P_2, N] = 1$ und $V_1 = \langle N^{L_1} \rangle \not\leq U_2$ und wie oben können wir Z durch N ersetzen, was uns den Widerspruch liefert.

Sei schließlich U_2 elementarabelsch der Ordnung 2^{16}. Zuerst sei die Gruppe $U_1 \cap U_2$ nicht s_1-invariant. Zu einer Involution $\overline{t} \in \overline{U_1 \cap U_2^{s_1}}$ wählen wir dann $d \in O_3(\overline{L}_2)$, so dass d von $\overline{t}$ invertiert wird. Dann ist

$$C_{U_2}(\overline{t}) \cap C_{U_2}(\overline{t}^d) \leq C_{U_2}(d)$$

höchstens von der Ordnung 2^4, denn nach dem Beweis von 8.7.3.1 und dem Satz von Clifford ist U_2 die direkte Summe von den Zentralisatoren $C_{U_2}(d_i)$ für vier geeignete Elemente in $O_3(\overline{L}_2)$. Somit ist

$$\frac{|C_{U_2}(\overline{t})| \cdot |C_{U_2}(\overline{t}^d)|}{|C_{U_2}(\overline{t}) \cap C_{U_2}(\overline{t}^d)|} \leq |U_2| = 2^{16},$$

und umgeformt

$$|C_{U_2}(\overline{t})| \leq 2^{10}.$$

Ist nun

$$V := (U_1 \cap U_2) \cap (U_1 \cap U_2^{s_1}),$$

so ist wegen $U_2' = 1$ auch

$$V \leq C_{U_2}(\overline{t})$$

und daher $|V| \leq 2^{10}$. Andererseits ist $|U_1 \cap U_2| = 2^{14}$, denn $|U_2/U_1 \cap U_2| = 2^2$. Es folgt

$$\frac{|U_1 \cap U_2| \cdot |U_1 \cap U_2^{s_1}|}{|V|} \leq |U_1| = 2^{18},$$

und somit $|V| \geq 2^{10}$. Insbesondere ist $|V| = 2^{10}$ und somit ist $\overline{U_1 \cap U_2^{s_1}} \cong V_4$. Die obige Argumenation können wir für jede der drei Involutionen $\overline{t}_i$, $i \leq 3$ dieser Gruppe durchführen, also ist $V = C_{U_2}(\overline{t}_i)$. Nun ist aber auch

$$O_3(\overline{L}_2) = \langle C_{O_3(\overline{L}_2)}(\overline{t}_i) \mid i \leq 3 \rangle,$$

also ist V offenbar $O_3(\overline{L}_2)$-invariant. Offenbar ist dann V ein $H_0\overline{L}_2$-Modul und dies ist ein Widerspruch.

Sei nun $U_1 \cap U_2$ invariant unter s_1. Dann operiert $\widetilde{L}_1$ auf $U_1/(U_1 \cap U_2) \cong \widetilde{U}$ und

$$U_2 \leq C_{L_1}(U_1 \cap U_2) \trianglelefteq P_1$$

Daher wird $U_1 \cap U_2$ von einem Element x der Ordnung 5 von L_1 zentralisiert. Nun ist auch $[\overline{U}, x] = 1$. Dies sehen wir leicht ein, da die Elemente der Ordnung 4 von $\overline{U}$ und neben der zentralen Involution auch die übrigen vier Involutionen zentralisiert werden müssen. Daher ist $x \in C_{L_1}(U_1) \leq U_1$, und dies ist ein Widerspruch. □

(8.7.4.2) Satz.

Es ist $\widetilde{L}_1 \ncong SL_2(2)$.

Beweis. Angenommen die Behauptung ist falsch. In 8.2.6 ist dann offenbar $t_1 = 2$ und $t_2 = 2^3$, und dies ist nach (1K) von Fong & Seitz [12] nur für $|W| = 12$ möglich. Insbesondere ist dann

$$|U_{s_2} : U \cap H| = 2^9.$$

Wegen $|U_{s_2} : U_2| = 2$ ist U_2 von der Ordnung 2^8 bzw. 2^9 und dies ist genau dann der Fall, wenn $|U \cap H| = 1$ bzw. 2. Wegen $C_{L_2}(U_2) \leq U_2$ operiert R_2 natürlich nichttrivial auf dem Modul $U_2/\Phi(U_2)$ und daher ist U_2 nach 8.7.3.1 entweder elementarabelsch und ein irreduzibler R_2-Modul der Ordnung 2^8, oder extraspeziell der Ordnung 2^9 oder elementarabelsch der Ordnung 2^9.

Sei zuerst U_2 extraspeziell. Wegen $C_{L_i}(U_i) \leq U_i$ ist dann

$$Z := Z(U) = Z(U_2) \leq Z(U_1).$$

Nun hat $\widetilde{L}_1$ genau drei 2-Sylowgruppen und Z wird von K_1 zentralisiert. Für

$$V_1 := \langle Z^{L_1} \rangle \leq U$$

ist V_1 ein natürlicher $\widetilde{L}_1$-Modul und $|V_1| = 2^2$. Wir beachten hierbei, dass V_1 von $K_1 \trianglelefteq L_1$ zentralisiert wird. Insbesondere ist $[V_1, U_2] \leq Z$ und U_2/Z wird somit von $\langle V_1^{P_2} \rangle$ zentralisiert. Ist $V_1 \not\leq U_2$, dann ist $\langle V_1^{P_2} \rangle \trianglelefteq P_2$ wegen $F(L_2) = U_2$ keine 2-Gruppe. Da auch Z von $\langle V_1^{P_2} \rangle$ zentralisiert wird, ist $V_1 \leq C_{L_2}(U_2) \leq U_2$, ein Widerspruch. Somit ist in jedem Fall

$$Z^{s_1} \leq V_1 \leq U_2$$

und insbesondere ist

$$(U_2^{s_1} \cap L_2)U_2/U_2 \cong (U_2^{s_1} \cap L_2)/(U_2 \cap U_2^{s_1})$$

eine elementarabelsche Untergruppe von L_2/U_2. Wir zeigen, dass diese Gruppe von der Ordnung mindestens 2^3 ist, was dann offenbar ein Widerspruch ist.

Nun ist

$$|U_2^{s_1} : U_2^{s_1} \cap U_1| = |U_2^{s_1} K_1/K_1| = 2,$$

denn wegen $|U : U_1| = 2$ ist $U = U_1U_2$. Somit ist auch

$$|U_2^{s_1} \cap L_2| \geq |U_2^{s_1} \cap U_1| = 2^8.$$

Insbesondere ist

$$(U_2 \cap U_2^{s_1})' \leq Z \cap Z^{s_1} = 1,$$

also ist $U_2 \cap U_2^{s_1}$ abelsch. Die maximalen abelschen Untergruppen von U_2 haben nach (5.1.9) von Kurzweil & Stellmacher [23] die Ordnung 2^5 und somit ist obige Gruppe mindestens von der Ordnung 2^3, ein Widerspruch.

Ist U_2 abelsch, dann können wir die Gruppe R_2 in obiger Argumentation durch $\overline{L}_2$ ersetzen, da nun U_2 im Kern der Operation liegt. Sei nun $|U_2| = 2^9$ mit $U_2' = 1$. Dann ist

$$U_2 = C_{U_2}(O_3(\overline{L}_2)) \oplus [U_2, O_3(\overline{L}_2)]$$

und $N := C_{U_2}(O_3(\overline{L}_2))$ ist von der Ordnung 2. Insbesondere ist $[N, P_2] = 1$, also ist wegen der Operation von $\widetilde{L}_1$ auf

$$V_1 := \langle N^{L_1} \rangle$$

gerade $2^2 \leq |V_1| \leq 2^3$. Natürlich ist $V_1 \not\leq U_2$, denn andernfalls sind N und N^{s_1} invariant unter $\widetilde{U}$. Dann ist aber N invariant unter $\widetilde{L}_1$ und daher $N \leq N(P_2, L_1) = G$, ein Widerspruch. Somit ist $[V_1, U_2] \leq V_1 \cap U_2$ höchstens von der Ordnung 2^2 und $\overline{V}_1$ enthält die zentrale Involution von $\overline{U}$, denn V_1 wird von U normalisiert. Daher ist $|[V_1, U_2]| = 2^4$, ein Widerspruch.

Sei schließlich U_2 elementarabelsch der Ordnung 2^8. Da U_2 in diesem Fall ein irreduzibler $\overline{L}_2$-Modul ist, ist

$$U_2 = \oplus_{i=1}^4 C_{U_2}(d_i)$$

für $d_i \in O_3(\overline{L}_2)$, $i \leq 4$ geeignet. Wir sehen dies im Beweis zu 8.7.3.1. Zuerst sei die Gruppe $U_1 \cap U_2$ nicht s_1-invariant. Zu einer Involution $\overline{t} \in \overline{U_1 \cap U_2^{s_1}}$ wählen wir $d \in O_3(\overline{L}_2)$, so dass d von $\overline{t}$ invertiert wird. Dann ist

$$C_{U_2}(\overline{t}) \cap C_{U_2}(\overline{t}^d) \leq C_{U_2}(d)$$

höchstens von der Ordnung 2^2. Somit ist

$$\frac{|C_{U_2}(\overline{t})| \cdot |C_{U_2}(\overline{t}^d)|}{|C_{U_2}(\overline{t}) \cap C_{U_2}(\overline{t}^d)|} \leq |U_2| = 2^8,$$

und umgeformt

$$|C_{U_2}(\overline{t})| \leq 2^5.$$

Ist nun

$$V := (U_1 \cap U_2) \cap (U_1 \cap U_2^{s_1}),$$

so ist wegen $U_2' = 1$ auch

$$V \leq C_{U_2}(\overline{t})$$

und daher $|V| \leq 2^5$. Sei nun

$$H := (U_1 \cap U_2)(U_1 \cap U_2^{s_1}).$$

Dann ist wegen $|U_1 \cap U_2| = 2^7$ gerade

$$|H| = \frac{|U_1 \cap U_2| \cdot |U_1 \cap U_2^{s_1}|}{|V|} \leq |U_1| = 2^{11},$$

und somit $|V| \geq 2^3$. Insgesamt bleiben daher die Fälle $2^3 \leq |V| \leq 2^5$ zu untersuchen, oder anders ausgedrückt die Fälle, in denen $2^2 \leq |H/(U_1 \cap U_2)| \leq 2^4$ ist.

Ist $|H/(U_1 \cap U_2)| \geq 2^3$, dann ist HU_2/U_2 ein elementarabelscher Normalteiler von $\overline{U}_2$, ein Widerspruch. Ist nun $|H/(U_1 \cap U_2)| = 2^2$, so ist $V = C_{U_2}(\overline{t})$ für die zentrale Involution $\overline{t} \in \overline{U_1 \cap U_2^{s_1}}$ von $\overline{U}$. Aber dann ist $|C_{U_2}(\overline{t})| = 2^4$.

Sei nun $U_1 \cap U_2$ invariant unter s_1. Dann operiert $\overline{L}_1$ auf $U_1/(U_1 \cap U_2) \cong \overline{U}$ und

$$U_2 \leq C_{L_1}(U_1 \cap U_2) \trianglelefteq P_1$$

Daher wird $U_1 \cap U_2$ von einem Element x der Ordnung 3 von L_1 zentralisiert. Die Operation von x auf $\overline{U}$ zeigt leicht $[\overline{U}, x] = 1$. Da x von ungerader Ordnung ist, folgt $x \in C_{L_1}(U_1) \leq U_1$, und dies ist ein Widerspruch. □

8.8 Die Moufangbedingung

In diesem letzten Abschnitt erfülle die endliche Gruppe G schließlich die Voraussetzungen des Hauptsatzes 8.1. Wir erinnern uns daran, dass G eine endliche $\mathcal{K}$-Gruppe mit einem BN-Paar (B, N) vom Rang 2 ist. Weiterhin besitzt B einen nilpotenten

Normalteiler U mit $B = UH$ und $H = B \cap N$ und G operiert treu auf $\mathcal{B}$. In den vorherigen Abschnitten haben wir gesehen, dass an das BN-Paar weitere Voraussetzungen gestellt wurden. Diese sind hier erfüllt, wenn wir unser BN-Paar (ohne die Notation zu verändern) durch das saturierte BN-Paar aus dem ersten Abschnitt und U durch die Fittinguntergruppe von B ersetzen.

Die folgenden Argumente zeigen, dass die Wurzeluntergruppen U_{r_i} mit den Wurzeluntergruppen A_{r_i} übereinstimmen. Vielmehr ist A_{r_i} regulär auf $\mathcal{W}(r_i)$ und wegen

$$U \cap H = U_{r_i} \cap U_{s_i}$$

ist dann $U \cap H = 1$. Es ist nun klar, dass das neue BN-Paar mit dem BN-Paar vom Anfang übereinstimmt, und schließlich folgt der Hauptsatz, wie zu Beginn des Abschnittes erläutert.

Wir beschränken die folgenden Argumente nur auf die Betrachtung der Wurzeluntergruppe A_{r_1}, um überflüssig komplizierte Notation zu vermeiden. Für die Wurzeluntergruppe A_{r_2} verlaufen die Argumente völlig analog. Im Apartment

$$\mathcal{A} = \{Bw \mid w \in W\}$$

ist die reflektierende Wand von $w_{r_1} = s_1$ offenbar gegeben durch

$$M_{r_1} = \{\{B, Bs_1\}, \{Bw_0, Bw_0s_1\}\}.$$

Die Wurzeln von $\mathcal{A}$ sind bis auf ein Vorzeichen eindeutig bestimmt. Für die folgenden Argumente sollten wir uns aber festlegen, und so sei r_1 die Wurzel von $\mathcal{A}$, welche die Kammer B enthält. Bevor wir den Hauptsatz beweisen können, benötigen wir noch einige Notationen.

Da $\mathcal{A}$ ein m-Eck ist, hat w_0s_1 einen minimalen Ausdruck der Form

$$w_0s_1 = \begin{cases} (s_2s_1)^{\frac{m}{2}-1}s_2 \equiv s_{11}\cdots s_{1k}, & \text{für } m > 3 \\ s_1s_2 \equiv s_{11}s_{12}, & \text{für } m = 3. \end{cases}$$

Für $l \leq k$ sei dann

$$w_l := s_{1l}\cdots s_{1k},$$

wenn im letzten Fall $k = 2$ ist. In allen Fällen ist dann $w_1 = w_0s_1$ und $w_k = s_2$ und gemäß unserer obigen Festlegung ist die Wurzel r_1 die Galerie

$$r_1 = (B, Bw_k, Bw_{k-1}, \ldots, Bw_1) = (B, Bs_2, Bs_1s_2, Bs_2s_1s_2, \ldots, Bw_0s_1)$$

im Apartment $\mathcal{A}$.

(8.8.1) Lemma.

Es ist $U_{r_1} = U \cap U^{w_1} \cap \ldots \cap U^{w_k}$.

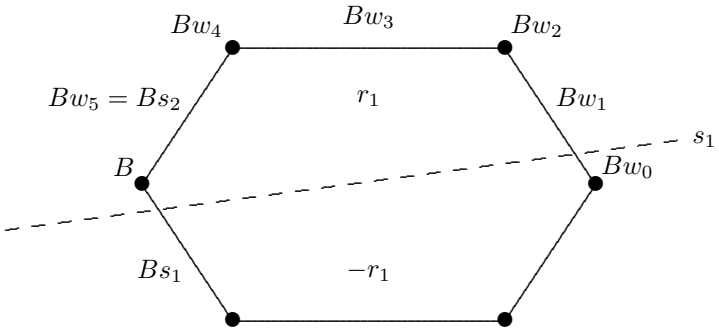

Abbildung 8.1: Das Apartment $\mathcal{A}$ mit $m = 6$

Beweis. Aus der Definition der Elemente w_l sehen wir für $l \leq k-1$ sofort

$$U_{w_l} = U_{s_{i_l} w_{l+1}} = U \cap B_{s_{i_l} w_{l+1}} \leq U \cap B_{w_{l+1}} = U_{w_{l+1}},$$

denn nach 8.2.2 ist $\ell(s_{i_l} w_{l+1}) > \ell(w_{l+1})$. Sukzessive Anwendung ergibt

$$U_{r_1} = U_{w_1} \leq \bigcap_{l=1}^{k} U_{w_l}$$

und die umgekehrte Inklusion ist offensichtlich. Nach 8.3.1 ist nun $U_w = U \cap U^w$ für alle $w \in W$, denn nach 8.5.8 ist U eine p-Gruppe. Dies beweist das Lemma. □

(8.8.2) Satz.

Es ist $A_{r_1} = U_{r_1}$ und A_{r_1} operiert regulär auf $\mathcal{W}(r_1)$.

Beweis. Die Gruppe A_{r_1} besteht offenbar aus den Automorphismen von $\mathcal{B}$, welche trivial auf den Rang 1-Residuen $\Delta_i(c)$ mit $c \in r_1$ und $|\Delta_i(c) \cap r_1| = 2$ operieren. Diese Residuen sind offenbar die Mengen $\Delta_i(Bw_l)$ mit $i \leq 2$ und $l \geq 2$. Wir können uns dies anhand der Abbildung 8.1 vor Augen führen.

Nach 8.8.1 ist nun $U_{r_1} \leq U^{w_l}$, und U_{r_1} fixiert neben B_{w_l} mindestens eine weitere Kammer in $\Delta_i(B_{w_l})$, nämlich eine von Bw_{l-1} oder Bw_{l+1} (mit $w_{k+1} := 1$). Die Gruppen $U^{w_l} K_i^{w_l} / K_i^{w_l}$ operieren aber nach den beiden letzten Abschnitten regulär auf $\Delta_i(Bw_l) \setminus \{Bw_l\}$, und daher ist $U_{r_1} \leq K_i^{w_l}$. Dies ist der Kern der Operation von $P_i^{w_l}$ auf $\Delta_i(Bw_l)$, also ist insbesondere

$$U_{r_1} \leq A_{r_1},$$

denn es ist $U_{r_1} \leq Aut(\mathcal{B})$.

Verwenden wir nun 8.2.4, so ist nach der Dedekindidentität

$$U = U \cap B_1 B_{s_1} = U \cap U_{r_1} B_{s_1} = U_{r_1}(U \cap B_{s_1}) = U_{r_1} U_{s_1}.$$

Nun wird $U_{s_1} = U \cap U^{s_1}$ von s_1 normalisiert und daher ist

$$\Delta_1(B) \setminus \{B\} = \{Bs_1x \mid x \in U_{r_1}\}$$

und U_{r_1} operiert transitiv auf $\Delta_1(B) \setminus \{B\}$. Bei I (4.6) von TIMMESFELD [34] finden wir, dass zwei gegenüberliegende Kammern in genau einem Apartment enthalten sind, also operiert U_{r_1} auch transitiv auf $\mathcal{W}(r_1)$. Der Satz folgt nun direkt aus dem Frattiniargument, denn die Gruppe A_{r_1} operiert fixpunktfrei auf $\mathcal{W}(r_1)$. □

Anhang A

Die Ordnungen der endlichen Lie-Typ-Gruppen

In diesem Kapitel geben wir die Ordnungen der endlichen Lie-Typ-Gruppen und einige Isomorphismen zwischen Lie-Typ-Gruppen an. Wir finden diese Informationen in den Tabellen I und II bei Gorenstein, Lyons & Solomon [14].

Gruppe	Andere Namen	Ordnung
$A_l(q)$ (1)	$PSL_{l+1}(q)$	$\frac{1}{(l+1,q-1)} q^{\binom{l+1}{2}} \prod_{i=2}^{l+1}(q^i-1)$
${}^2A_l(q)$ (1)	$PSU_{l+1}(q)$	$\frac{1}{(l+1,q+1)} q^{\binom{l+1}{2}} \prod_{i=2}^{l+1}(q^i-(-1)^i)$
$B_l(q)$ (2)	$P\Omega_{2l+1}(q)$	$\frac{1}{(2,q-1)} q^{l^2} \prod_{i=1}^{l}(q^{2i}-1)$
${}^2B_2(q)$ (1),(3)	$Sz(q)$	$q^2(q-1)(q^2+1)$
$C_l(q)$ (2)	$PSp_{2l}(q)$	$\frac{1}{(2,q-1)} q^{l^2} \prod_{i=1}^{l}(q^{2i}-1)$
$D_l(q)$	$P\Omega^+_{2l}(q)$	$\frac{1}{(4,q^l-1)} q^{l(l-1)}(q^l-1) \prod_{i=1}^{l-1}(q^{2i}-1)$
${}^2D_l(q)$	$P\Omega^-_{2l}(q)$	$\frac{1}{(4,q^l+1)} q^{l(l-1)}(q^l+1) \prod_{i=1}^{l-1}(q^{2i}-1)$
${}^3D_4(q)$		$q^{12}(q^2-1)(q^8+q^4+1)(q^6-1)$
$E_6(q)$		$\frac{1}{(3,q-1)} q^{36}(q^2-1)(q^5-1)(q^6-1)(q^8-1)(q^9-1)(q^{12}-1)$
${}^2E_6(q)$		$\frac{1}{(3,q+1)} q^{36}(q^2-1)(q^5+1)(q^6-1)(q^8-1)(q^9+1)(q^{12}-1)$
$E_7(q)$		$\frac{1}{(2,q-1)} q^{63}(q^2-1)(q^6-1)(q^8-1)(q^{10}-1)(q^{12}-1)$ $(q^{14}-1)(q^{18}-1)$
$E_8(q)$		$q^{120}(q^2-1)(q^8-1)(q^{12}-1)(q^{14}-1)(q^{18}-1)(q^{20}-1)$ $(q^{24}-1)(q^{30}-1)$
$F_4(q)$		$q^{24}(q^2-1)(q^6-1)(q^8-1)(q^{12}-1)$
${}^2F_4(q)$ (2),(3)		$q^{12}(q-1)(q^3+1)(q^4-1)(q^6+1)$
$G_2(q)$ (2)		$q^6(q^2-1)(q^6-1)$
${}^2G_2(q)$ (2),(4)	$R(q)$	$q^3(q-1)(q^3+1)$

Tabelle A.1: Die endlichen Lie-Typ-Gruppen und ihre Ordnungen

Anmerkungen zu Tabelle A.1.

(1) $A_1(2)$, $A_1(3)$, ${}^2A_2(2)$ und ${}^2B_2(2)$ sind auflösbar.

(2) Für $G = B_2(2) = C_2(2)$, $G_2(2)$, ${}^2G_2(3)$ und ${}^2F_4(2)$ ist G' einfach und der Index in G ist $2, 2, 3$ bzw. 2.

(3) Nur für $q = 2^{2n+1}$.

(4) Nur für $q = 3^{2n+1}$.

$B_2(q) \cong C_2(q)$
$B_l(2^m) \cong C_l(2^m)$
$A_5 \cong A_1(4) \cong A_1(5)$
$A_1(7) \cong A_2(2)$
$A_1(8) \cong {}^2G_2(3)'$
$A_6 \cong A_1(9) \cong B_2(2)' \cong C_2(2)'$
${}^2A_2(3) \cong G_2(2)'$
$A_8 \cong A_3(2)$
${}^2A_3(2) \cong B_2(3) \cong C_2(3)$

Tabelle A.2: Isomorphismen zwischen Lie-Typ-Gruppen

Anhang B

Zweifach transitive Weylgruppen

Eine Gruppe G operiert genau zweifach transitiv auf einer Menge, wenn der Stabilisator einer Ziffer genau zwei Doppelnebenklassen in G hat. Die im folgenden Satz aufgeführten Weylgruppen sind die Weylgruppen der unzerlegbaren Wurzelsysteme, welche die kristallographische Bedingung erfüllen, oder des Wurzelsystems, dessen Wurzeln die Vektoren vom Ursprung zu den Ecken eines regelmäßigen 16-Eckes sind. Wir übernehmen für den Rest des Abschnittes die Bezeichnungen aus den Abschnitten 2.1, 2.2 und 2.3 von Kapitel 2.

(B.1) Satz.

Sei W eine Weylgruppe vom Typ A_l, B_l, C_l, D_l, E_6, E_7, E_8, F_4, G_2 oder eine Diedergruppe der Ordnung 16. *Ist W^* eine parabolische Untergruppe von W und operiert W zweifach transitiv auf den Nebenklassen von W^* in W, so ist W vom Typ A_l und W^* vom Typ A_{l-1}.*

Wir gehen in mehreren Schritten vor und fassen $W^* = W_J$ o.B.d.A. als standardparabolische Untergruppe auf. Da W zweifach transitiv auf den Nebenklassen von W_J in W operiert, ist W_J eine maximalparabolische Untergruppe von W. Das einzige Element von $I \setminus J$ bezeichnen wir mit i und setzen $w_i := w_{r_i}$. Insbesondere ist dann

$$W = W_J \dot{\cup} W_J w_i W_J,$$

denn W_J hat wegen der zweifach transitiven Operation genau zwei Doppelnebenklassen in W. Offenbar haben $W_J w_i W_J$ und $W_J^{w_i} W_J$ die gleiche Mächtigkeit, also ist

$$|W| = |W_J| \left(1 + \frac{|W_J|}{|W_J^{w_i} \cap W_J|}\right). \tag{B.1}$$

Für die weiteren Argumente ist es nützlich, die Dynkindiagramme der Weylgruppen vor Augen zu haben. Wir verweisen dazu auf die Abbildungen 2.1 und 2.2 auf den Seiten 9 und 10. Wir erhalten zunächst das folgende

(B.2) Lemma.

Ist W vom Typ A_l, so ist W_J vom Typ A_{l-1}.

Beweis. Ist $i = 1$ oder l, so ist W_J wie in der Behauptung, und wir rechnen leicht nach, das diese Fälle tatsächlich eintreten. Angenommen i ist verschieden von 1 und l. Dies ist natürlich nur für $l \geq 3$ möglich. Nach dem Dynkindiagramm ist

$$W_J = W_{\{1,\ldots,i-1\}} \times W_{\{i+1,\ldots,l\}} \cong W(A_{i-1}) \times W(A_{l-i}),$$

Coxetergraph	Ordnung von W
A_l	$(l+1)!$
B_l	$2^l l!$
D_l	$2^{l-1} l!$
E_6	$2^7 \cdot 3^4 \cdot 5$
E_7	$2^{10} \cdot 3^4 \cdot 5 \cdot 7$
E_8	$2^{14} \cdot 3^5 \cdot 5^2 \cdot 7$
F_4	$2^7 \cdot 3^2$
G_2	12

Tabelle B.1: Die Ordnungen der Weylgruppen

also

$$|W_J| = i!(l+1-i)!.$$

Die Gruppen $W_{\{1,\dots,i-2\}}$ und $W_{\{i+2,\dots,l\}}$ werden von w_i zentralisiert, also ist

$$W(A_{i-2}) \times W(A_{l-i-1}) \cong W_{\{1,\dots,i-2\}} \times W_{\{i+2,\dots,l\}} \leq W_J^{w_i} \cap W_J,$$

wobei wir $W(A_0) = 1$ setzen. Daher ist

$$|W_J^{w_i} \cap W_J| \geq (i-1)!(l-i)!.$$

Mit (B.1) erhalten wir

$$\begin{aligned}(l+1)! = |W| &\leq i!(l+1-i)! \left(1 + \frac{i!(l+1-i)!}{(i-1)!(l-i!)}\right) \\ &= i!(l+1-i)!(1+i(l+1-i)).\end{aligned}$$

Division durch $i!(l+1-i)!$ ergibt

$$\binom{l+1}{i} \leq 1 + i(l+1-i). \tag{B.2}$$

Wir schätzen zunächst die rechte Seite weiter ab. Das Polynom $1 + x(l+1-x)$ hat ein Maximum an der Stelle $x = \frac{l+1}{2}$. Wegen $i \in \{2, \dots, l-1\}$ folgt

$$\frac{l(l+1)}{2} = \binom{l+1}{2} \leq \binom{l+1}{i} \leq 1 + \frac{l+1}{2}\left(l+1-\frac{l+1}{2}\right) = 1 + \frac{(l+1)^2}{4},$$

und daher $2l(l+1) \leq 4 + l^2 + 2l + 1$. Wir formen dies um zu $l^2 - 5 \leq 0$. Dies ist ein Widerspruch. □

(B.3) Lemma.

W ist nicht vom Typ B_l und C_l.

Beweis. Es reicht natürlich, die Weylgruppe vom Typ B_l zu betrachten. Mit (B.1) folgt sofort, dass W nicht vom Typ B_2 ist. Sei daher $l \geq 3$. Ist $i = 1$, so ist W_J vom

Typ B_{l-1}. Setzen wir $W(B_1) := \mathbb{Z}_2$, dann enthält $W_J \cap W_J^{w_i}$ wie eben eine Weylgruppe vom Typ B_{l-2} und daher ist

$$|W_J^{w_i} \cap W_J| \geq 2^{l-2}(l-2)!.$$

Eingesetzt in (B.1) ergibt sich

$$2^l l! = |W| \leq 2^{l-1}(l-1)! \left(1 + \frac{2^{l-1}(l-1)!}{2^{l-2}(l-2)!}\right) = 2^{l-1}(l-1)!(1+2(l-1)).$$

Division durch $2^{l-1}(l-1)!$ ergibt $2l \leq 2l-1$, ein Widerspruch.

Ist $i = l$, dann ist W_J vom Typ A_{l-1} und $W_J \cap W_J^{w_i}$ enthält eine Weylgruppe vom Typ A_{l-2}. Mit (B.1) erhalten wir

$$2^l l! = |W| \leq l! \left(1 + \frac{l!}{(l-1)!}\right) = (l+1)!,$$

also auch $2^l \leq l+1$, ein Widerspruch.

Ist nun $i \neq 1$ oder l, so ist W_J vom Typ $A_{i-1} \times B_{l-i}$. Setzen wir $W(A_0) = W(B_0) = 1$, so enthält $W_J \cap W_J^{w_i}$ eine Untergruppe vom Typ $A_{i-2} \times B_{l-i-1}$. Eingesetzt in (B.1) ergibt sich

$$\begin{aligned} 2^l l! = |W| &\leq 2^{l-i}(l-i)!i! \left(1 + \frac{2^{l-i}(l-i)!i!}{2^{l-(i+1)}(l-(i+1))!(i-1)!}\right) \\ &= 2^{l-i}(l-i)!i!(1+2i(l-i)). \end{aligned}$$

Division durch $2^{l-i}(l-i)!i!$ ergibt

$$2^i \binom{l}{i} \leq 1 + 2i(l-i). \tag{B.3}$$

Wir sehen, dass das Polynom $1 + 2x(l-x)$ maximal ist für $x = \frac{l}{2}$. Wegen $i \geq 2$ folgt für $i \neq l-1$ aus (B.3), dass

$$2l(l-1) = 2^2 \binom{l}{2} \leq 2^i \binom{l}{i} \leq 1 + 2\frac{l}{2}(l - \frac{l}{2}) = 1 + \frac{l^2}{2}.$$

Wir erhalten $3l^2 - 4l - 2 \leq 0$, und damit $l = 1$, ein Widerspruch. Für $i = l-1$ führt (B.3) direkt zum Widerspruch. □

(B.4) Lemma.

W ist nicht vom Typ D_l.

Beweis. Mit $W(D_2)$ bezeichnen wir die Gruppe vom Typ $A_1 \times A_1$ und mit $W(D_3)$ die Gruppe $W(A_3)$. Ist $i = 1$, so ist W_J vom Typ D_{l-1} und $W_J \cap W_J^{w_i}$ enthält eine Weylgruppe vom Typ D_{l-2}. Eingesetzt in (B.1) folgt

$$2^{l-1} l! = |W| \leq 2^{l-2}(l-1)! \left(1 + \frac{2^{l-2}(l-1)!}{2^{l-3}(l-2)!}\right) = 2^{l-2}(l-1)!(2l-1).$$

Division durch $2^{l-2}(l-1)!$ ergibt $2l \leq 2l-1$, ein Widerspruch.

Ist $i \in \{l-1, l\}$, dann können wir aus Symmetriegründen o.B.d.A. annehmen, dass $i = l$. Dann ist W_J vom Typ A_{l-1} und $W_J \cap W_J^{w_i}$ enthält eine Untergruppe vom Typ $A_{l-3} \times A_1$. Eingesetzt in (B.1) folgt

$$2^{l-1}l! = |W| \leq l! \left(1 + \frac{l!}{2(l-2)!}\right) = l! \left(1 + \frac{l(l-1)}{2}\right).$$

Division durch $\frac{l!}{2}$ ergibt $2^l \leq 2 + l(l-1)$, offenbar ein Widerspruch.

Ist $i \in \{2, \ldots, l-2\}$, so ist W_J vom Typ $A_{i-1} \times D_{l-i}$ und $W_J \cap W_J^{w_i}$ enthält eine Untergruppe vom Typ $A_{i-2} \times D_{l-(i+1)}$, wenn wir $W(D_1) = 1$ setzen. Es folgt

$$|W_J^{w_i} \cap W_J| \geq 2^{l-(i+2)}(i-1)!(l-(i+1))!.$$

Eingesetzt in (B.1) folgt also

$$\begin{aligned} 2^{l-1}l! &= |W| \\ &\leq 2^{l-(i+1)}i!(l-i)! \left(1 + \frac{2^{l-(i+1)}i!(l-i)!}{2^{l-(i+2)}(i-1)!(l-(i+1))!}\right) \\ &= 2^{l-(i+1)}i!(l-i)!(1+2i(l-i)). \end{aligned}$$

Division durch $2^{l-(i+1)}i!(l-i)!$ ergibt die Ungleichung (B.3). □

(B.5) Lemma.

W ist nicht vom Typ E_6.

Beweis. Aus Symmetriegründen müssen wir nur die Fälle $i = 1, 2, 3, 4$ betrachten. Ist $i = 1$, dann ist W_J vom Typ D_5 und $W_J \cap W_J^{w_i}$ enthält eine Weylgruppe vom Typ A_4. Mit (B.1) folgt daher

$$51840 = 2^7 \cdot 3^4 \cdot 5 = |W| \leq 2^4 \cdot 5!(1 + \frac{2^4 \cdot 5!}{5!}) = 32640,$$

ein Widerspruch.

Ist $i = 2$, dann ist W_J vom Typ A_5 und $W_J \cap W_J^{w_i}$ enthält eine Untergruppe vom Typ $A_2 \times A_2$. Eingesetzt in (B.1) folgt

$$51840 = |W| \leq 6!(1 + \frac{6!}{36}) = 15120,$$

ein Widerspruch.

Ist $i = 3$, dann ist W_J vom Typ $A_1 \times A_4$ und $W_J \cap W_J^{w_i}$ enthält eine Untergruppe vom Typ $A_1 \times A_2$. Eingesetzt in (B.1) folgt

$$51840 = |W| \leq 240(1 + \frac{240}{12}) = 5040,$$

ein Widerspruch.

i	Typ von W_J	$\lvert W_J\rvert$
1	D_6	23040
2	A_6	5040
3	$A_1 \times A_5$	1440
4	$A_1 \times A_2 \times A_3$	288
5	$A_4 \times A_2$	720
6	$D_5 \times A_1$	3840
7	E_6	51840

Tabelle B.2: Die möglichen Ordnungen von W_J

Ist $i = 4$, dann ist W_J vom Typ $A_1 \times A_2 \times A_2$ und $W_J \cap W_J^{w_i}$ enthält eine Untergruppe vom Typ $A_1 \times A_1$. Eingesetzt in (B.1) folgt

$$51840 = |W| \leq 72(1 + \frac{72}{4}) = 1368,$$

ein Widerspruch. □

(B.6) Lemma.

W ist nicht vom Typ E_7.

Beweis. Aus dem Dynkindiagramm der Weylgruppe vom Typ E_7 sehen wir, dass $W_J \cap W_J^{w_i}$ unabhängig von i eine Untergruppe vom Typ $A_1 \times A_2$ hat. Mit (B.1) folgt somit

$$2903040 = |W| \leq |W_J| + \frac{|W_J|^2}{12},$$

und dies formen wir um zu

$$|W_J| > 5896.$$

Nach Tabelle B.2 müssen wir nur noch die Fälle $i = 1$ und 7 genauer betrachten.

Für $i = 1$ enthält $W_J \cap W_J^{w_i}$ eine Untergruppe vom Typ A_5. Eingesetzt in (B.1) folgt

$$2903040 = |W| \leq 2^5 \cdot 6!(1 + \frac{2^5 \cdot 6!}{6!}) = 760320,$$

ein Widerspruch. Ist $i = 7$, so enthält $W_J \cap W_J^{w_i}$ eine Untergruppe vom Typ D_5 und mit (B.1) folgt

$$2903040 = |W| \leq 51840(1 + \frac{51840}{2^4 \cdot 5!}) = 1451520,$$

ein Widerspruch. □

(B.7) Lemma.

W ist nicht vom Typ E_8.

i	Typ von W_J	$\lvert W_J\rvert$
1	D_7	322560
2	A_7	40320
3	$A_1 \times A_6$	10080
4	$A_1 \times A_2 \times A_4$	1440
5	$A_4 \times A_3$	2880
6	$D_5 \times A_2$	11520
7	$E_6 \times A_1$	103680
8	E_7	2903040

Tabelle B.3: Die möglichen Ordnungen von W_J

Beweis. Offenbar enthält $W_J \cap W_J^{w_i}$ stets eine Untergruppe vom Typ $A_1 \times A_3$, $A_1 \times A_2 \times A_2$ oder D_5 und ist somit mindestens von der Ordnung 48. Eingesetzt in (B.1) erhalten wir

$$696729600 = |W| \leq |W_J| + \frac{|W_J|^2}{48},$$

und damit leicht

$$|W_J| > 182850.$$

Nach Tabelle B.3 müssen wir nur noch die Fälle $i = 1$ und 8 genauer betrachten.

Für $i = 1$ enthält $W_J \cap W_J^{w_i}$ eine Untergruppe vom Typ A_6. Eingesetzt in (B.1) folgt

$$696729600 = |W| \leq 2^6 \cdot 7!(1 + \frac{2^6 \cdot 7!}{7!}) = 20966400,$$

ein Widerspruch. Für $i = 8$ enthält $W_J \cap W_J^{w_i}$ eine Weylgruppe vom Typ E_6. Mit (B.1) folgt

$$696729600 = |W| \leq 2903040(1 + \frac{2903040}{51840}) = 165473280,$$

ein Widerspruch. □

(B.8) Lemma.

W ist nicht vom Typ F_4.

Beweis. Aus Symmetriegründen müssen wir nur die Fälle $i = 1, 2$ betrachten. Ist $i = 1$, dann ist W_J vom Typ B_3 und $W_J \cap W_J^{w_i}$ enthält eine Untergruppe vom Typ A_2. Mit (B.1) folgt

$$1152 = 2^7 \cdot 3^2 = |W| \leq 2^3 \cdot 3!(1 + \frac{2^3 \cdot 3!}{3!}) = 432,$$

ein Widerspruch.

Ist $i = 2$, dann ist W_J vom Typ $A_1 \times A_2$ und mit (B.1) folgt

$$1152 = |W| \leq 12 \cdot (1 + 12) = 156,$$

ein Widerspruch. □

(B.9) Lemma.

W ist keine Diedergruppe der Ordnung 16 *und nicht vom Typ* G_2.

Beweis. Hier ist W_J vom Typ A_1 und die Behauptung folgt direkt mit (B.1). □

Anhang C

Einige zahlentheoretische Lemmata

In diesem Abschnitt sammeln wir einige recht technische Rechnungen. Die Rechnungen sind in vielen Fällen sehr ähnlich, weswegen wir diese nach ausführlichen Beispielen etwas verkürzt darstellen werden. Im ganzen Kapitel sei $q = p^f$ eine Potenz der Primzahl p.

(C.1) Lemma.

Sei y eine p-Potenz und seien m und v wie in der Tabelle C.1. Dann ist $m-1$ kein Teiler von yv.

	v	m
(a)	$2(q-1)f$	$\frac{\prod_{i=l+1}^{2l}(q^i-1)}{\prod_{i=1}^{l}(q^i-1)}$, $l \geq 2$
(b)	$2^3 f$	$\frac{(q^l-1)(q^{l-j}+1)\prod_{i=l-j+1}^{l-1}(q^{2i}-1)}{\prod_{i=1}^{j}(q^i-1)}$, $2 \leq j \leq l-3$, $l \geq 5$
(c)	$2^3 f$	$(q^{l-1}+1)\sum_{i=0}^{l-1} q^i$
(d)	$2^3 f$	$\frac{(q^l-1)(q^{2(l-1)}-1)\prod_{i=1}^{l-2}(q^i+1)}{(q^2-1)^2}$
(e)	$2(q-1)f$	$(q^4+1)(q^6+1)(q^3+1)\sum_{i=0}^{8} q^i$
(f)	$2(q-1)f$	$\frac{(q^2+1)(q^3+1)^2(q^4+1)(q^5-1)(q^6+1)(q^9-1)}{(q^2-1)(q-1)}$

Tabelle C.1: Die Zahlen m und v

Beweis. Wir zeigen zunächst, dass $m-1$ den p-Anteil q hat. Nehmen wir dann an, dass unsere Behauptung falsch ist, so folgt $m-1 \mid qv$ und hier benötigen wir sogar nur noch $m-1 \leq qv$, um einen Widerspruch zu erhalten.

Im Fall (c) und (e) läßt sich der p-Anteil von $m-1$ direkt ablesen. Für die übrigen Fälle betrachten wir stellvertretend den Fall (b). Hier ist

$$m-1 = \frac{(q^l-1)(q^{l-j}+1)\prod_{i=l-j+1}^{l-1}(q^{2i}-1) - \prod_{i=1}^{j}(q^i-1)}{\prod_{i=1}^{j}(q^i-1)}$$

und das Ausmultiplizieren des Zählers impliziert auch hier die Behauptung. Wir haben nun in jedem Fall $m-1 \leq qv$ und damit auch

$$m \leq qv+1 \leq 2qv.$$

Bis auf den Fall (b) ist dies offensichtlich ein Widerspruch oder führt durch eine leichte Rechnung zum Widerspruch. In (b) ist

$$m = \frac{(q^l-1)(q^{l-j}+1)\prod_{i=l-j+1}^{l-1}(q^{2i}-1)}{\prod_{i=1}^{j}(q^i-1)} \leq 2^4 fq.$$

Umgeformt ist dann

$$(q^l-1)(q^{l-j}+1)\prod_{i=l-j+1}^{l-1}(q^{2i}-1) \leq 2^4 fq\prod_{i=1}^{j}(q^i-1) \leq 2^4 fq\prod_{i=l-j+1}^{l-1}(q^{2i}-1)$$

und somit

$$(q^l-1)(q^{l-j}+1) \leq 2^4 fq,$$

ein Widerspruch wegen $l \geq 5$. □

Für den Rest des Abschnittes sei $1 \neq x$ eine natürliche Zahl, die keine p-Potenz ist. Die folgenden Rechnungen sind teilweise sehr aufwändig, aber dennoch elementarer Natur. Für zwei teilerfremde ganze Zahlen a, b benutzen wir häufig, dass auch $a+b$ und b teilerfremd sind.

(C.2) Lemma.

Es ist $q^l x - 1 \nmid \frac{(q^l-1)(q^{l+1}-1)}{q-1}$ *mit* $l \in \mathbb{N}$.

Beweis. Angenommen

$$q^l x - 1 \mid \frac{(q^l-1)(q^{l+1}-1)}{q-1}. \tag{C.1}$$

Wir behandeln zuerst den Fall $l = 1$. Dann gibt es ein $y \in \mathbb{N}$ mit

$$(qx-1)y = q^2-1.$$

Offenbar ist dann auch

$$y \equiv 1 \mod q,$$

und daher gibt es ein $z \in \mathbb{Z}$ mit

$$0 \leq y = zq+1.$$

Da $x \neq 1$ keine p-Potenz ist, ist offenbar $z \geq 1$ und daher ist

$$q^2-1 = (q-1)(q+1) < (qx-1)(zq+1) = q^2-1,$$

ein Widerspruch.

Sei nun $l \geq 2$. Nach (C.1) gibt es dann ein $y \in \mathbb{N}$ mit

$$(q-1)(q^l x-1)y = (q^l-1)(q^{l+1}-1). \tag{C.2}$$

Offenbar gilt dann auch

$$-(q-1)y \equiv 1 \mod q^l,$$

und daher gibt es ein $z \in \mathbb{Z}$ mit

$$0 \leq (q-1)y = zq^l - 1. \tag{C.3}$$

Es ist klar, dass $z \geq 1$. Setzen wir (C.3) in (C.2) ein, dann erhalten wir

$$(q^l x - 1)(zq^l - 1) = (q^l - 1)(q^{l+1} - 1). \tag{C.4}$$

Wir zeigen, dass $x > q$. Aus (C.4) sehen wir, dass

$$q^l x - 1 \mid (q^l - 1)(q^{l+1} - 1)x.$$

Offenbar ist

$$q^{l+1}x - x = x(q^l x - 1) + (q - x)q^l x,$$

also ist auch

$$q^l x - 1 \mid (q^l - 1)(q - x)q^l x.$$

Wegen $ggT(q^l x - 1, q^l x) = 1$ folgt

$$q^l x - 1 \mid (q^l - 1)(q - x).$$

Dann ist auch

$$q^l x - 1 \mid (q - x)(q^l - 1)x = (q - x)(q^l x - 1) + (q - x)(1 - x),$$

und schließlich

$$q^l x - 1 \mid (q - x)(1 - x). \tag{C.5}$$

Angenommen $x \leq q$. Dann ist auch $x < q$ und wegen $x > 1$ ist dann $(q-x)(1-x) < 0$. Aus (C.5) folgt

$$2q^l - 1 \leq q^l x - 1 \leq (q - x)(x - 1) < (q - 2)^2,$$

ein Widerspruch wegen $l \geq 2$. Wir haben gezeigt, dass

$$x > q.$$

Wir erhalten damit aus (C.4)

$$(q^{l+1} - 1)(q^l - 1) < (q^l x - 1)(q^l z - 1) = (q^{l+1} - 1)(q^l - 1),$$

ein Widerspruch zu unserer ersten Annahme. Daher gilt die Behauptung. □

(C.3) Lemma.

Es ist $q^{2l-3}x - 1 \nmid \frac{(q^{2l}-1)(q^{2l-2}-1)}{q^2-1}$ *mit* $3 \leq l \in \mathbb{N}$. *Ferner ist* $q^2 x - 1 \nmid q^4 - 1$.

Beweis. Angenommen

$$q^{2l-3}x - 1 \mid \frac{(q^{2l}-1)(q^{2l-2}-1)}{q^2-1}, \quad l \geq 3.$$

Dann gibt es ein $y \in \mathbb{N}$ mit

$$(q^2-1)(q^{2l-3}x-1)y = (q^{2l}-1)(q^{2l-2}-1). \tag{C.6}$$

Offenbar ist dann

$$-(q^2-1)y \equiv 1 \mod q^{2l-3},$$

und daher gibt es ein $z \in \mathbb{Z}$ mit

$$0 \leq (q^2-1)y = zq^{2l-3} - 1. \tag{C.7}$$

Es ist klar, dass

$$z \geq 1.$$

Setzen wir nun (C.7) in (C.6) ein, so erhalten wir

$$(q^{2l-3}x-1)(zq^{2l-3}-1) = (q^{2l}-1)(q^{2l-2}-1). \tag{C.8}$$

Wir zeigen, dass $x > q^4$. Aus (C.8) sehen wir, dass

$$q^{2l-3}x - 1 \mid (q^{2l-2}-1)(q^{2l}-1)x = (q^{2l-2}-1)(q^{2l}x - x). \tag{C.9}$$

Offenbar ist

$$q^{2l}x - x = x(q^{2l-3}x-1) + (q^3-x)q^{2l-3}x,$$

also ist nach (C.9) auch

$$q^{2l-3}x - 1 \mid (q^{2l-2}-1)(q^3-x)q^{2l-3}x.$$

Wegen $ggT(q^{2l-3}x-1, q^{2l-3}x) = 1$ ist daher

$$q^{2l-3}x - 1 \mid (q^{2l-2}-1)(q^3-x).$$

Wir sehen damit, dass

$$q^{2l-3}x - 1 \mid (q^{2l-2}-1)(q^3-x)x = (q^3-x)q(q^{2l-3}x-1) + (q^3-x)(q-x).$$

Schließlich ergibt sich

$$q^{2l-3}x - 1 \mid (q-x)(q^3-x).$$

Sei zunächst $l \geq 4$. Ist $x \leq q$, so ist auch $x < q$ und daher

$$q^5 - 1 < q^{2l-3}x - 1 \leq (q-x)(q^3-x) < q^4,$$

ein Widerspruch. Daher ist $x > q$. Ist nun $x < q^3$, so ist

$$(q-x)(q^3-x) < 0$$

und daher

$$q^6 - 1 < q^{2l-3}x - 1 \leq (x-q)(q^3-x) < (q^3-q)^2 < (q^3-1)^2,$$

ein Widerspruch und insbesondere ist $x > q^3$. Nehmen wir schließlich an, dass $x \leq q^4$, so ist

$$\begin{aligned} q^8 - 1 < q^{2l-3}x - 1 &\leq (q-x)(q^3-x) = (x-q)(x-q^3) \\ &\leq (q^4-q)(q^4-q^3) = q^4(q^3-1)(q-1) < q^7(q-1), \end{aligned}$$

erneut ein Widerspruch. Somit ist $x \geq q^4 + 1$ und mit (C.8) folgt schließlich

$$(q^{2l+1} + q^{2l-3} - 1)(q^{2l-3} - 1) \leq (q^{2l-3}x - 1)(zq^{2l-3} - 1) = (q^{2l} - 1)(q^{2l-2} - 1)$$

und dies formen wir um zu

$$q^{4l-6} - 2q^{2l-3} - q^{2l+1} \leq -(q^{2l-2} + q^{2l}) \leq 0,$$

ein Widerspruch. Also gilt die Behauptung für $l \geq 4$.

Es bleibt der Fall $l = 3$, in dem wir aus (C.7) sofort

$$q^2 - 1 \mid zq^3 - 1 = zq^3 - q^2 + q^2 - 1 = q^2(zq-1) + (q^2-1)$$

einsehen. Insbesondere ist

$$q^2 - 1 \mid (zq-1)q^2$$

und wegen $ggT(q^2-1, q^2) = 1$ somit

$$q^2 - 1 \mid zq - 1$$

und auch

$$z \geq q.$$

Für $z = q$ ist $y = q^2 + 1$ in (C.7) und daher $x = q^3$ in (C.6), ein Widerspruch. Somit ist

$$z = q + a$$

mit $a \geq 1$ und somit

$$q^2 - 1 \mid zq - 1 = (q^2-1) + aq.$$

Da $ggT(q, q^2-1) = 1$, ist nun

$$q^2 - 1 \mid a$$

und somit

$$z = q + b(q^2-1)$$

mit $b \geq 1$. Eingesetzt in (C.7) ergibt sich dann

$$y = \frac{zq^3 - 1}{q^2 - 1} = \frac{(q^4-1) + (q^2-1)q^3 b}{q^2-1} = q^3 b + q^2 + 1. \tag{C.10}$$

Aus (C.6) folgt dann

$$(q^6-1)(q^2+1) = (q^3x-1)(q^3b+q^2+1) = q^3x(q^3b+q^2+1) - q^3b - (q^2+1).$$

Dies formen wir um zu

$$q^3x(q^3b+q^2+1) = q^6(q^2+1) + q^3b$$

und Division durch q^3 ergibt

$$x(q^3b+q^2+1) = q^3(q^2+1) + b,$$

was wir umformen zu

$$q^3(bx-1) = q^5 + b - (q^2+1)x.$$

Insbesondere ist

$$q^3 \mid b - (q^2+1)x$$

und somit

$$1 \leq b = cq^3 + (q^2+1)x \tag{C.11}$$

für ein $c \in \mathbb{Z}$. Wir betrachten zuerst den Fall, in dem $c \leq -q$. Angenommen $x < q^2$. Dann ist

$$0 < b = cq^3 + (q^2+1)x \leq -q^4 + (q^2+1)x \leq -q^4 + (q^2+1)(q^2-1) = -1,$$

ein Widerspruch. Somit ist $x \geq q^2+1$ und eingesetzt in (C.6) ergibt sich zusammen mit (C.10) folgendes:

$$(q^6-1)(q^2+1) = (q^3x-1)(q^3b+q^2+1) \geq (q^5+q^3-1)(q^3+q^2+1).$$

Dies formen wir um zu

$$0 \geq q^7 + 2q^5,$$

ein Widerspruch.

Sei nun $-1 \geq c > -q$. Angenommen $x < -cq$. Dann folgt wie eben

$$0 < b = cq^3 + (q^2+1)x \leq cq^3 + (q^2+1)(-cq-1) = -cq - q^2 - 1 \leq -1,$$

ein Widerspruch. Somit ist

$$x \geq -cq \geq q$$

und damit nach (C.11) auch

$$b = cq^3 + (q^2+1)x \geq cq^3 - (q^2+1)cq = -cq \geq q.$$

Setzen wir nun $x \geq q+1$ und $b \geq q$ in (C.6) ein, so folgt

$$(q^6-1)(q^2+1) = (q^3x-1)(q^3b+q^2+1) \geq (q^4+q^3-1)(q^4+q^2+1).$$

Dies formen wir leicht um zu

$$0 \geq q^7 + q^5 + q^3$$

und erhalten einen Widerspruch.

Sei nun $c \geq 0$. Dann ist

$$b = cq^3 + (q^2+1)x \geq q^2 + 1.$$

Wegen $x > 1$ ist dann in (C.6) schließlich auch

$$\begin{aligned}(q^6-1)(q^2+1) &= (q^3x-1)(q^3b+q^2+1) > (q^3-1)(q^5+q^3+q^2+1)\\ &= (q^3-1)(q^3+1)(q^2+1) = (q^6-1)(q^2+1),\end{aligned}$$

ein Widerspruch. Insgesamt folgt also auch für $l = 3$ die Behauptung.

Es bleibt der zweite Teil der Behauptung zu zeigen. Angenommen

$$q^2x - 1 \mid q^4 - 1.$$

Dann gibt es ein $y \in \mathbb{N}$ mit

$$(q^2x-1)y = q^4 - 1 \tag{C.12}$$

und es folgt

$$y \equiv 1 \mod q^2.$$

Somit existiert ein $z \geq 0$ mit

$$y = zq^2 + 1.$$

Es ist $z \geq 1$, da sonst $x = q^2$, und dies ist unmöglich. Eingesetzt in (C.12) ergibt sich schließlich mit

$$(q^4-1) = (q^2-1)(q^2+1) < (q^2x-1)(q^2z+1) = q^4 - 1$$

ein Widerspruch. Somit gilt insgesamt die Behauptung. □

(C.4) Lemma.

Es ist $q^{2l-3}x - 1 \nmid \frac{(q^l-1)(q^{l-1}+1)(q^{l-1}-1)(q^{l-2}+1)}{q^2-1}$ *mit* $4 \leq l \in \mathbb{N}$.

Beweis. Angenommen

$$q^{2l-3}x - 1 \mid \frac{(q^l-1)(q^{l-1}+1)(q^{l-1}-1)(q^{l-2}+1)}{q^2-1}, \quad l \geq 4.$$

Dann gibt es ein $y \in \mathbb{N}$ mit

$$\begin{aligned}(q^2-1)(q^{2l-3}x-1)y &= (q^l-1)(q^{l-1}+1)(q^{l-1}-1)(q^{l-2}+1)\\ &= (q^{2l-2}+q^l-q^{l-2}-1)(q^{2l-2}-1).\end{aligned} \tag{C.13}$$

Offenbar gilt dann auch

$$-(q^2-1)y \equiv -(q^l - q^{l-2} - 1) \mod q^{2l-3},$$

und daher gibt es ein $z \in \mathbb{Z}$ mit

$$0 \leq (q^2-1)y = zq^{2l-3} + q^l - q^{l-2} - 1. \tag{C.14}$$

Angenommen $z < 0$. Wegen $l \geq 4$ folgt dann

$$q^{2l-3} \leq -zq^{2l-3} \leq q^l - q^{l-2} - 1 < q^l,$$

ein Widerspruch. Daher ist $z \geq 0$. Angenommen $z = 0$. Dann sehen wir aus (C.14), dass

$$q^2 - 1 \mid q^l - q^{l-2} - 1 = q^{l-2}(q^2-1) - 1,$$

ein Widerspruch. Wir haben gezeigt, dass

$$z \geq 1.$$

Setzen wir nun (C.14) in (C.13) ein, so erhalten wir

$$(q^{2l-3}x - 1)(zq^{2l-3} + q^l - q^{l-2} - 1) = (q^l - 1)(q^{l-2} + 1)(q^{2l-2} - 1). \tag{C.15}$$

Wir zeigen, dass $x < q^2$. Angenommen $q^2 \leq x$. Dann ist auch $q^2 + 1 \leq x$ und mit (C.15) und $z \geq 1$ folgt

$$\begin{aligned}(q^{2l-3}(q^2+1) - 1)q^{2l-3} &\leq (q^{2l-3}x - 1)(zq^{2l-3} + q^l - q^{l-2} - 1) \\ &= (q^l - 1)(q^{l-2} + 1)(q^{2l-2} - 1) \\ &< q^{3l-2}(q^{l-2} + 1).\end{aligned} \tag{C.16}$$

Division durch q^{2l-3} ergibt

$$q^{2l-3}(q^2+1) - 1 < q^{l+1}(q^{l-2} + 1),$$

und daher

$$q^{2l-3} - 1 < q^{l+1},$$

ein Widerspruch für $l \geq 5$. Für $l = 4$ sehen wir aus der zweiten Zeile von (C.16), dass

$$q^{10}(q^2+1) - q^5 = (q^5(q^2+1) - 1)q^5 \leq (q^4 - 1)(q^2 + 1)(q^6 - 1).$$

Wir formen dies um zu

$$q^5 \geq (q^2+1)(q^{10} - (q^4 - 1)(q^6 - 1)) = (q^2 + 1)(q^6 + q^4 - 1),$$

ein Widerspruch.
Wir haben nun

$$x < q^2$$

gezeigt und zeigen noch, dass $x > q$. Nach (C.13) gilt

$$q^{2l-3}x - 1 \mid (q^{l-2} + 1)(q^l - 1)(q^{2l-2} - 1)x.$$

Offenbar ist

$$q^{2l-2}x - x = x(q^{2l-3}x - 1) + (q - x)q^{2l-3}x,$$

also ist auch

$$q^{2l-3}x - 1 \mid (q^{l-2} + 1)(q^l - 1)(q - x)q^{2l-3}x.$$

Wegen $ggT(q^{2l-3}x - 1, q^{2l-3}x) = 1$ ist somit

$$q^{2l-3}x - 1 \mid (q^{l-2} + 1)(q^l - 1)(q - x)$$

und daher auch

$$\begin{aligned} q^{2l-3}x - 1 \mid\ & (q^{l-2} + 1)(q^l - 1)(q - x)q^{l-3}x \\ &= (q - x)(q^{l-2} + 1)(q^{2l-3}x - q^{l-3}x) \\ &= (q - x)(q^{l-2} + 1)(q^{2l-3}x - 1) - (q - x)(q^{l-2} + 1)(q^{l-3}x - 1). \end{aligned}$$

Schließlich folgt

$$q^{2l-3}x - 1 \mid (q^{l-2} + 1)(q^{l-3}x - 1)(q - x). \tag{C.17}$$

Angenommen $x < q$. Dann folgt wegen $x > 1$ aus (C.17), dass

$$\begin{aligned} 2q^{2l-3} - 1 \leq q^{2l-3}x - 1 &\leq (q^{l-2} + 1)(q^{l-3}x - 1)(q - x) \\ &\leq (q^{l-2} + 1)q^{l-2}q \leq q^{2l-3} + q^{l-1}, \end{aligned}$$

ein Widerspruch. Wir haben gezeigt, dass

$$x > q.$$

Mit (C.17) folgt nun

$$q^{2l-3}x - 1 \leq (x - q)(q^{l-2} + 1)(q^{l-3}x - 1) < (x - q)(q^{l-2} + 1)q^{l-3}x,$$

also folgt auch

$$q^{2l-3}x \leq (x - q)(q^{l-2} + 1)q^{l-3}x.$$

Mit $x \leq q^2$ und Division durch $q^{l-3}x$ folgt schließlich

$$q^l \leq (q^2 - q)(q^{l-2} + 1) = q^l - q^{l-1} + q^2 - q,$$

wegen $l \geq 4$ ein Widerspruch zu unserer ersten Annahme. □

(C.5) Lemma.

Es ist $q^{11}x - 1 \nmid \frac{(q^4+1)(q^9-1)(q^{12}-1)}{q^3-1}$.

Beweis. Angenommen

$$q^{11}x - 1 \mid \frac{(q^4 + 1)(q^9 - 1)(q^{12} - 1)}{q^3 - 1}.$$

Dann gibt es ein $y \in \mathbb{N}$ mit

$$(q^3-1)(q^{11}x-1)y = (q^4+1)(q^9-1)(q^{12}-1). \tag{C.18}$$

Offenbar gilt dann auch

$$-(q^3-1)y \equiv -(q^4+1)(q^9-1) \mod q^{11},$$

und daher gibt es ein $z' \in \mathbb{Z}$ mit

$$0 \leq (q^3-1)y = z'q^{11} + (q^4+1)(q^9-1) = zq^{11} + (q^4+1)(q^9-1) - q^{13}, \tag{C.19}$$

wobei $z = z' + q^2$. Wir zeigen zunächst, dass $z \geq 0$. Angenommen $z < 0$. Dann folgt

$$q^{11} \leq -zq^{11} \leq (q^4+1)(q^9-1) - q^{13} = q^9 - q^4 - 1,$$

ein Widerspruch und somit ist $z \geq 0$. Setzen wir (C.19) in (C.18) ein, so erhalten wir

$$(q^{11}x-1)(zq^{11} + (q^4+1)(q^9-1) - q^{13}) = (q^4+1)(q^9-1)(q^{12}-1). \tag{C.20}$$

Angenommen $z = 0$. Dann erhalten wir aus (C.20)

$$(q^{11}x-1)(q^9-q^4-1) = (q^4+1)(q^9-1)(q^{12}-1),$$

und folglich

$$q^9 - q^4 - 1 \mid (q^4+1)(q^9-1)(q^{12}-1).$$

Offenbar ist $ggT(q^4, q^9-1) = 1$, also ist nach unserer Vorbemerkung auch

$$ggT((q^9-1) - q^4, q^9-1) = 1.$$

Analog folgt $ggT((q^4+1) - q^9, q^4+1) = 1$ und daher

$$q^9 - q^4 - 1 \mid q^{12} - 1 = q^3(q^9 - q^4 - 1) + (q^7 + q^3 - 1),$$

und somit

$$q^9 - q^4 - 1 \mid q^7 + q^3 - 1,$$

offenbar ein Widerspruch. Daher ist

$$z \geq 1. \tag{C.21}$$

Wir zeigen nun, dass $x < q^4$. Angenommen $x \geq q^4 + 1$. Aus (C.20) und (C.21) folgt dann

$$\begin{aligned}(q^{11}(q^4+1) - 1)q^{11} &\leq (q^{11}x - 1)(zq^{11} + (q^4+1)(q^9-1) - q^{13}) \\ &= (q^4+1)(q^9-1)(q^{12}-1) \\ &< (q^4+1)q^{21}.\end{aligned}$$

Division durch q^{11} liefert offensichtlich einen Widerspruch. Daher ist

$$x < q^4. \tag{C.22}$$

Nach (C.20) ist

$$q^{11}x - 1 \mid (q^4+1)(q^9-1)(q^{12}-1)x = (q^4+1)(q^9-1)(q^{12}x - x).$$

Offenbar ist

$$q^{12}x - x = x(q^{11}x - 1) + (q-x)q^{11}x,$$

also ist

$$q^{11}x - 1 \mid (q^4+1)(q^9-1)(q-x)q^{11}x.$$

Wegen $ggT(q^{11}x - 1, q^{11}x) = 1$ ist dann

$$q^{11}x - 1 \mid (q^4+1)(q^9-1)(q-x),$$

und somit auch

$$\begin{aligned} q^{11}x - 1 \mid{}& (q^4+1)(q^9-1)(q-x)q^2x \\ &= (q^4+1)(q-x)(q^{11}x - q^2x) \\ &= (q^4+1)(q-x)(q^{11}x - 1) - (q^4+1)(q-x)(q^2x-1). \end{aligned}$$

Schließlich folgt

$$q^{11}x - 1 \mid (q^4+1)(q^2x-1)(q-x). \tag{C.23}$$

Angenommen $x < q$. Mit (C.23) folgt dann

$$2q^{11} - 1 \leq q^{11}x - 1 \leq (q^4+1)(q^2x-1)(q-x) \leq (q^4+1)q^4,$$

ein Widerspruch. Insbesondere ist

$$x > q.$$

Nun ist nach (C.23) und (C.22)

$$\begin{aligned} q^{11}x - 1 &\leq (x-q)(q^4+1)(q^2x-1) < (x-q)(q^4+1)q^2x \\ &\leq (q^4-1)(q^4+1)q^2x = (q^8-1)q^2x, \end{aligned}$$

und somit auch

$$q^{11}x \leq (q^8-1)q^2x.$$

Division durch q^2x liefert

$$q^9 \leq q^8 - 1,$$

ein Widerspruch zu unserer ersten Annahme. Daher gilt die Behauptung. □

(C.6) Lemma.

Es ist $q^{17}x - 1 \nmid \frac{(q^{14}-1)(q^6+1)(q^{18}-1)}{q^4-1}$.

Beweis. Angenommen

$$q^{17}x - 1 \mid \frac{(q^{14}-1)(q^6+1)(q^{18}-1)}{q^4-1}.$$

Dann gibt es ein $y \in \mathbb{N}$ mit

$$(q^4-1)(q^{17}x-1)y = (q^{14}-1)(q^6+1)(q^{18}-1). \tag{C.24}$$

Offenbar gilt dann auch

$$-(q^4-1)y \equiv -(q^{14}-1)(q^6+1) \mod q^{17},$$

und daher gibt es ein $z' \in \mathbb{Z}$ mit

$$0 \leq (q^4-1)y = z'q^{17} + (q^{14}-1)(q^6+1) = zq^{17} + (q^{14}-1)(q^6+1) - q^{20}, \tag{C.25}$$

wobei $z = z' + q^3$. Angenommen $z < 0$. Mit (C.25) folgt dann

$$q^{17} \leq -zq^{17} \leq (q^{14}-1)(q^6+1) - q^{20} = q^{14} - q^6 - 1,$$

ein Widerspruch. Insbesondere ist $z \geq 0$. Setzen wir (C.25) in (C.24) ein, so erhalten wir

$$(q^{17}x-1)(zq^{17} + (q^{14}-1)(q^6+1) - q^{20}) = (q^{14}-1)(q^6+1)(q^{18}-1). \tag{C.26}$$

Angenommen $z = 0$. Dann erhalten wir aus (C.26)

$$(q^{17}x-1)(q^{14}-q^6-1) = (q^{14}-1)(q^6+1)(q^{18}-1),$$

und folglich

$$q^{14} - q^6 - 1 \mid (q^{14}-1)(q^6+1)(q^{18}-1).$$

Offenbar ist $ggT(q^6, q^{14}-1) = 1$, also ist nach unserer Vorbemerkung auch

$$ggT((q^{14}-1) - q^6, q^{14}-1) = 1.$$

Analog folgt $ggT((q^6+1) - q^{14}, q^6+1) = 1$ und daher

$$q^{14} - q^6 - 1 \mid q^{18} - 1 = q^4(q^{14} - q^6 - 1) + (q^{10} + q^4 - 1),$$

und somit

$$q^{14} - q^6 - 1 \mid q^{10} + q^4 - 1,$$

offenbar ein Widerspruch. Wir haben gezeigt, dass

$$z \geq 1. \tag{C.27}$$

Angenommen $x \geq q^6 + 1$. Aus (C.26) und (C.27) folgt dann

$$\begin{aligned}(q^{17}(q^6+1) - 1)q^{17} &\leq (q^{17}x-1)(zq^{17} + (q^{14}-1)(q^6+1) - q^{20}) \\ &= (q^{14}-1)(q^6+1)(q^{18}-1) \\ &< (q^6+1)q^{32}.\end{aligned}$$

Division durch q^{17} liefert offensichtlich einen Widerspruch. Daher ist

$$x < q^6. \tag{C.28}$$

Nach (C.26) ist

$$q^{17}x - 1 \mid (q^6+1)(q^{14}-1)(q^{18}-1)x. = (q^6+1)(q^{14}-1)(q^{18}x - x)$$

Offenbar ist

$$q^{18}x - x = x(q^{17}x - 1) + (q-x)q^{17}x,$$

also ist

$$q^{17}x - 1 \mid (q^6+1)(q^{14}-1)(q-x)q^{17}x.$$

Wegen $ggT(q^{17}x-1, q^{17}x) = 1$ ist dann

$$q^{17}x - 1 \mid (q^6+1)(q^{14}-1)(q-x),$$

und somit auch

$$\begin{aligned} q^{17}x - 1 \mid (q^6+1)(q^{14}-1)(q-x)q^3x \\ &= (q^6+1)(q-x)(q^{17}x - q^3x) \\ &= (q^6+1)(q-x)(q^{17}x-1) - (q^6+1)(q-x)(q^3x-1). \end{aligned}$$

Schließlich folgt

$$q^{17}x - 1 \mid (q^6+1)(q^3x-1)(q-x). \tag{C.29}$$

Angenommen $x < q$. Mit (C.29) erhalten wir

$$2q^{17} - 1 \leq q^{17}x - 1 \leq (q^6+1)(q^3x-1)(q-x) \leq (q^6+1)q^4q = (q^6+1)q^5,$$

ein Widerspruch. Insbesondere ist

$$x > q.$$

Nun ist nach (C.29) und (C.28)

$$\begin{aligned} q^{17}x - 1 \leq (x-q)(q^6+1)(q^3x-1) < (x-q)(q^6+1)q^3x \\ \leq (q^6-1)(q^6+1)q^3x = (q^{12}-1)q^3x, \end{aligned}$$

und somit auch

$$q^{17}x \leq (q^{12}-1)q^3x.$$

Division durch q^3x liefert

$$q^{14} \leq q^{12} - 1,$$

ein Widerspruch zu unserer ersten Annahme. Daher gilt die Behauptung. □

(C.7) Lemma.

Es ist $q^{29}x - 1 \nmid \frac{(q^{10}+1)(q^{24}-1)(q^{30}-1)}{q^6-1}$.

Beweis. Angenommen

$$q^{29}x - 1 \mid \frac{(q^{10}+1)(q^{24}-1)(q^{30}-1)}{q^6-1}.$$

Dann gibt es ein $y \in \mathbb{N}$ mit

$$(q^6-1)(q^{29}x-1)y = (q^{10}+1)(q^{24}-1)(q^{30}-1). \tag{C.30}$$

Offenbar gilt dann auch

$$-(q^6-1)y \equiv -(q^{10}+1)(q^{24}-1) \mod q^{29},$$

und daher gibt es ein $z' \in \mathbb{Z}$ mit

$$0 \leq (q^6-1)y = z'q^{29} + (q^{10}+1)(q^{24}-1) = zq^{29} + (q^{10}+1)(q^{24}-1) - q^{34}, \tag{C.31}$$

wobei $z = z' + q^5$. Angenommen $z < 0$. Mit (C.31) folgt dann

$$q^{29} \leq -zq^{29} \leq (q^{10}+1)(q^{24}-1) - q^{34} = q^{24} - q^{10} - 1,$$

ein Widerspruch und es ist $z \geq 0$. Setzen wir (C.31) in (C.30) ein, so erhalten wir

$$(q^{29}x-1)(zq^{29} + (q^{10}+1)(q^{24}-1) - q^{34}) = (q^{10}+1)(q^{24}-1)(q^{30}-1). \tag{C.32}$$

Angenommen $z = 0$. Aus (C.32) erhalten wir dann

$$(q^{29}x-1)(q^{24}-q^{10}-1) = (q^{10}+1)(q^{24}-1)(q^{30}-1),$$

und folglich

$$q^{24}-q^{10}-1 \mid (q^{10}+1)(q^{24}-1)(q^{30}-1).$$

Offenbar ist $ggT(q^{10}, q^{24}-1) = 1$, also ist nach unserer Vorbemerkung auch

$$ggT((q^{24}-1) - q^{10}, q^{24}-1) = 1.$$

Analog folgt $ggT((q^{10}+1) - q^{24}, q^{10}+1) = 1$ und daher

$$q^{24}-q^{10}-1 \mid q^{30}-1 = q^6(q^{24}-q^{10}-1) + (q^{16}+q^6-1),$$

und somit

$$q^{24}-q^{10}-1 \mid q^{16}+q^6-1,$$

offenbar ein Widerspruch und es folgt

$$z \geq 1. \tag{C.33}$$

Angenommen $x \geq q^{10}+1$. Aus (C.32) und (C.33) folgt dann

$$\begin{aligned}(q^{29}(q^{10}+1)-1)q^{29} &\leq (q^{29}x-1)(zq^{29} + (q^{10}+1)(q^{24}-1) - q^{34}) \\ &= (q^{10}+1)(q^{24}-1)(q^{30}-1) \\ &< (q^{10}+1)q^{54}.\end{aligned}$$

Division durch q^{29} liefert offensichtlich einen Widerspruch und es ist

$$x < q^{10}. \tag{C.34}$$

Nach (C.32) ist

$$q^{29}x - 1 \mid (q^{10}+1)(q^{24}-1)(q^{30}-1)x = (q^{10}+1)(q^{24}-1)(q^{30}x - x)$$

Offenbar ist

$$q^{30}x - x = x(q^{29}x - 1) + (q - x)q^{29}x,$$

also ist

$$q^{29}x - 1 \mid (q^{10}+1)(q^{24}-1)(q-x)q^{29}x.$$

Wegen $ggT(q^{29}x - 1, q^{29}x) = 1$ ist dann

$$q^{29}x - 1 \mid (q^{10}+1)(q^{24}-1)(q-x),$$

und somit auch

$$\begin{aligned} q^{29}x - 1 \mid{}& (q^{10}+1)(q^{24}-1)(q-x)q^5x \\ &= (q^{10}+1)(q^{29}x - q^5x)(q-x) \\ &= (q^{10}+1)(q-x)(q^{29}x-1) - (q^{10}+1)(q-x)(q^5x-1). \end{aligned}$$

Schließlich folgt

$$q^{29}x - 1 \mid (q^{10}+1)(q^5x-1)(q-x). \tag{C.35}$$

Angenommen $x < q$. Dann ist

$$2q^{29} - 1 \leq q^{29}x - 1 \leq (q^{10}+1)(q^5x-1)(q-x) < q^{11}q^6q = q^{18},$$

ein Widerspruch. Insbesondere ist

$$x > q,$$

und nach (C.35) und (C.34) ist dann

$$q^{29}x - 1 \leq (x-q)(q^{10}+1)(q^5x-1) < (q^{10}-1)(q^{10}+1)q^5x = (q^{20}-1)q^5x,$$

und somit

$$q^{29}x \leq (q^{20}-1)q^5x.$$

Division durch q^5x liefert

$$q^{24} \leq q^{20} - 1,$$

ein Widerspruch zu unserer ersten Annahme. Daher gilt die Behauptung. □

(C.8) Lemma.

Es ist $q^7x - 1 \nmid (q^4+1)(q^{12}-1)$.

Beweis. Angenommen

$$q^7x - 1 \mid (q^4 + 1)(q^{12} - 1).$$

Dann gibt es ein $y \in \mathbb{N}$ mit

$$(q^7x - 1)y = (q^4 + 1)(q^{12} - 1). \tag{C.36}$$

Offenbar gilt dann auch

$$-y \equiv -(q^4 + 1) \mod q^7,$$

und daher gibt es ein $z \in \mathbb{Z}$ mit

$$0 \leq y = zq^7 + q^4 + 1. \tag{C.37}$$

Offenbar ist $z \geq 0$. Setzen wir (C.37) in (C.36) ein, so erhalten wir

$$(q^7x - 1)(zq^7 + q^4 + 1) = (q^4 + 1)(q^{12} - 1). \tag{C.38}$$

Ist $z = 0$, dann ist $x = q^5$, ein Widerspruch. Daher haben wir

$$z \geq 1. \tag{C.39}$$

Angenommen $x \geq q^3 + 1$. Aus (C.38) und (C.39) erhalten wir

$$(q^7(q^3 + 1) - 1)q^7 < (q^7x - 1)(zq^7 + q^4 + 1) = (q^4 + 1)(q^{12} - 1) < (q^4 + 1)q^{12}.$$

Division durch q^7 liefert offenbar einen Widerspruch, also ist

$$x < q^3. \tag{C.40}$$

Nach (C.36) ist

$$q^7x - 1 \mid (q^4 + 1)(q^{12} - 1)x. \tag{C.41}$$

Offenbar ist

$$q^{12}x - x = (q^7x - 1)x + (q^5 - x)q^7x,$$

also erhalten wir aus (C.41), dass

$$q^7x - 1 \mid (q^4 + 1)(q^5 - x)q^7x.$$

Wegen $ggT(q^7x - 1, q^7x) = 1$ ist

$$q^7x - 1 \mid (q^4 + 1)(q^5 - x),$$

also gibt es mit (C.40) ein $v \geq 0$ mit

$$q^7xv - v = (q^7x - 1)v = (q^4 + 1)(q^5 - x) = -x(q^4 + 1) + q^5 + q^9. \tag{C.42}$$

Wir formen dies um zu

$$v + q^5 = (q^4 + 1)x + q^7(xv - q^2). \tag{C.43}$$

Angenommen $xv > q^2$. Dann ist $xv - q^2 \geq 1$ und aus (C.43) folgt

$$v + q^5 \geq (q^4 + 1)x + q^7 > q^7,$$

und somit

$$v > q^7 - q^5 = q^5(q^2 - 1) > q^5.$$

Setzen wir dies in (C.42) ein, dann ist

$$q^{10} > (q^4 + 1)(q^5 - x) = (q^7x - 1)v > (q^7x - 1)q^5 > (q^7 - 1)q^5 > q^{11},$$

ein Widerspruch. Da x keine p-Potenz ist, gilt also

$$xv < q^2.$$

Mit (C.40), (C.43) und wegen $v \geq 0$ folgt schließlich

$$q^7 + q^3 = (q^4 + 1)q^3 > (q^4 + 1)x = v + q^5 + q^7(q^2 - xv) \geq q^5 + q^7,$$

ein Widerspruch zu unserer ersten Annahme. Daher gilt die Behauptung. □

(C.9) Lemma.

Es ist $q^3x - 1 \nmid 2(q^6 - 1)$.

Beweis. Angenommen

$$q^3x - 1 \mid 2(q^6 - 1).$$

Dann gibt es ein $y \in \mathbb{N}$ mit

$$(q^3x - 1)y = 2(q^6 - 1). \tag{C.44}$$

Offenbar gilt dann auch

$$-y \equiv -2 \mod q^3,$$

und daher gibt es ein $z \in \mathbb{Z}$ mit

$$0 \leq y = zq^3 + 2. \tag{C.45}$$

Es ist klar, dass $z \geq 1$, denn sonst ist $z = 0$ und damit $x = q^3$. Setzen wir (C.45) in (C.44) ein, dann erhalten wir

$$(q^3x - 1)(zq^3 + 2) = 2(q^6 - 1).$$

Mit $x \geq 2$ folgt nun

$$2q^6 + 3q^3 - 2 = (2q^3 - 1)(q^3 + 2) \leq (q^3x - 1)(q^3z + 2) = 2q^6 - 2,$$

ein Widerspruch zu unserer ersten Annahme. Daher gilt die Behauptung. □

(C.10) Lemma.

Es ist $q^{11}x - 1 \nmid \frac{(q^4+1)(q^9+1)(q^{12}-1)}{q^3+1}$.

Beweis. Angenommen

$$q^{11}x - 1 \mid \frac{(q^4+1)(q^9+1)(q^{12}-1)}{q^3+1}.$$

Dann gibt es ein $y \in \mathbb{N}$ mit

$$(q^3+1)(q^{11}x-1)y = (q^4+1)(q^9+1)(q^{12}-1). \tag{C.46}$$

Offenbar gilt dann auch

$$-(q^3+1)y \equiv -(q^4+1)(q^9+1) \mod q^{11},$$

und daher gibt es ein $z' \in \mathbb{Z}$ mit

$$0 \leq (q^3+1)y = z'q^{11} + (q^4+1)(q^9+1) = zq^{11} + (q^4+1)(q^9+1) - q^{13}, \tag{C.47}$$

wobei $z = z' + q^2$. Angenommen $z < 0$. Mit (C.47) folgt dann

$$q^{11} \leq -zq^{11} \leq (q^4+1)(q^9+1) - q^{13} = q^9 + q^4 + 1,$$

offenbar ein Widerspruch und es ist $z \geq 0$.

Setzen wir (C.47) in (C.46) ein, so erhalten wir

$$(q^{11}x-1)(zq^{11} + (q^4+1)(q^9+1) - q^{13}) = (q^4+1)(q^9+1)(q^{12}-1). \tag{C.48}$$

Angenommen $z = 0$. Dann erhalten wir aus (C.48)

$$(q^{11}x-1)(q^9+q^4+1) = (q^4+1)(q^9+1)(q^{12}-1),$$

und folglich

$$q^9 + q^4 + 1 \mid (q^4+1)(q^9+1)(q^{12}-1).$$

Offenbar ist $ggT(q^4, q^9+1) = 1$, also ist nach unserer Vorbemerkung auch

$$ggT((q^9+1)+q^4, q^9+1) = 1.$$

Analog folgt $ggT((q^4+1)+q^9, q^4+1) = 1$ und daher

$$q^9 + q^4 + 1 \mid q^{12} - 1 = q^3(q^9+q^4+1) - (q^7+q^3+1),$$

und somit

$$q^9 + q^4 + 1 \mid q^7 + q^3 + 1,$$

offenbar ein Widerspruch, und es folgt

$$z \geq 1. \tag{C.49}$$

Angenommen $x \geq q^4 + 1$. Aus (C.48) und (C.49) folgt dann

$$\begin{aligned}(q^{11}(q^4+1)-1)q^{11} &< (q^{11}x-1)(zq^{11} + (q^4+1)(q^9+1) - q^{13}) \\ &= (q^4+1)(q^9+1)(q^{12}-1) \\ &< (q^4+1)(q^9+1)q^{12}.\end{aligned}$$

Division durch q^{11} liefert

$$q^{11}(q^4+1)-1 < q(q^4+1)(q^9+1)$$

und daher

$$q^{11}(q^4+1) \leq q(q^4+1)(q^9+1).$$

Division durch $q(q^4+1)$ liefert

$$q^{10} \leq q^9+1,$$

ein Widerspruch. Daher ist

$$x < q^4. \tag{C.50}$$

Nach (C.48) ist

$$q^{11}x-1 \mid (q^4+1)(q^9+1)(q^{12}-1)x = (q^4+1)(q^9+1)(q^{12}x-x).$$

Offenbar ist

$$q^{12}x-x = x(q^{11}x-1)+(q-x)q^{11}x,$$

also ist

$$q^{11}x-1 \mid (q^4+1)(q^9+1)(q-x)q^{11}x.$$

Wegen $ggT(q^{11}x-1, q^{11}x) = 1$ ist dann

$$q^{11}x-1 \mid (q^4+1)(q^9+1)(q-x),$$

und somit auch

$$\begin{aligned} q^{11}x-1 \mid{}& (q^4+1)(q^9+1)(q-x)q^2x \\ &= (q^4+1)(q-x)(q^{11}x+q^2x) \\ &= (q^4+1)(q-x)(q^{11}x-1)+(q^4+1)(q-x)(q^2x+1). \end{aligned}$$

Schließlich folgt

$$q^{11}x-1 \mid (q^4+1)(q^2x+1)(q-x). \tag{C.51}$$

Angenommen $x < q$. Mit (C.51) ist dann

$$2q^{11}-1 \leq q^{11}x-1 \leq (q^4+1)(q^2x+1)(q-x) < (q^4+1)q^4q = q^9+q^5,$$

ein Widerspruch. Somit ist

$$x > q.$$

Mit (C.51) und (C.50) ist also

$$\begin{aligned} q^{11}x-1 &\leq (x-q)(q^4+1)(q^2x+1) \leq (x-q)(q^4+1)q^3x \\ &< (q^4-1)(q^4+1)q^3x = (q^8-1)q^3x. \end{aligned}$$

Daher gilt auch

$$q^{11}x \leq (q^8-1)q^3x,$$

und Division durch q^3x liefert

$$q^8 \leq q^8-1,$$

ein Widerspruch zu unserer ersten Annahme. Daher gilt die Behauptung. □

(C.11) Lemma.

Es ist $q^5x - 1 \nmid (q^2-1)(q^8+q^4+1)$.

Beweis. Angenommen

$$q^5x - 1 \mid (q^2-1)(q^8+q^4+1).$$

Dann gibt es ein $y \in \mathbb{N}$ mit

$$(q^5x-1)y = (q^2-1)(q^8+q^4+1). \tag{C.52}$$

Offenbar gilt dann auch

$$-y \equiv (q^2-1)(q^4+1) \mod q^5,$$

und daher gibt es ein $z \in \mathbb{Z}$ mit

$$0 \leq y = zq^5 - (q^2-1)(q^4+1). \tag{C.53}$$

Aus (C.53) sehen wir, dass

$$zq^5 \geq (q^2-1)(q^4+1) > (q^2-1)q^4 = q^6 - q^4,$$

und damit erhalten wir leicht

$$z \geq q. \tag{C.54}$$

Setzen wir nun (C.53) in (C.52) ein, dann ergibt sich

$$(q^5x-1)(zq^5 - (q^2-1)(q^4+1)) = (q^2-1)(q^8+q^4+1). \tag{C.55}$$

Angenommen $x \geq q^2+1$. Es ist leicht einzusehen, dass

$$q^3 \leq q^4 - q^2 + 1,$$

also erhalten wir aus (C.55) und (C.54) die Abschätzung

$$\begin{aligned}
(q^7+q^5-1)q^3 &= (q^5(q^2+1)-1)q^3 \\
&\leq (q^5(q^2+1)-1)(q^4-q^2+1) \\
&= (q^5(q^2+1)-1)(q^6-(q^2-1)(q^4+1)) \\
&\leq (q^5x-1)(zq^5-(q^2-1)(q^4+1)) \\
&= (q^2-1)(q^8+q^4+1) \\
&\leq q^2(q^8+q^4+1).
\end{aligned}$$

Division durch q^2 liefert

$$q^8+q^6-q \leq q^8+q^4+1,$$

ein Widerspruch, und es folgt

$$x < q^2. \tag{C.56}$$

Wegen (C.55) ist

$$q^5x - 1 \mid (q^2-1)(q^8+q^4+1)(q^4-1)x = (q^2-1)(q^{12}-1)x. \tag{C.57}$$

Offenbar gilt

$$q^{12}x - x = x(q^5x-1) + (q^7-x)q^5x,$$

also ist wegen (C.57)

$$q^5x - 1 \mid (q^2-1)(q^7-x)q^5x.$$

Wegen $ggT(q^5x-1, q^5x) = 1$ ist dann auch

$$q^5x - 1 \mid (q^2-1)(q^7-x). \tag{C.58}$$

Wegen $x < q^2$ existiert insbesondere ein $v \geq 0$ mit

$$q^5xv - v = (q^5x-1)v = (q^2-1)(q^7-x) = q^9 - q^7 - x(q^2-1). \tag{C.59}$$

Wir formen dies um zu

$$q^7 + x(q^2-1) = v + q^5(q^4 - xv). \tag{C.60}$$

Angenommen $q^4 - xv = q^2$. Dann ist

$$v = (q^2-1)x,$$

und eingesetzt in (C.59) folgt

$$(q^5x-1)(q^2-1)x = (q^2-1)(q^7-x).$$

Somit ist

$$q^5x^2 - x = q^7 - x$$

und daher $x = q$, ein Widerspruch. Angenommen $q^4 - xv \leq q^2 - 1$. Wegen $x \geq 2$ folgt aus (C.60), dass

$$q^7 + q^2 \leq q^7 + x(q^2-1) = v + q^5(q^4 - xv) \leq v + q^5(q^2-1) = v + q^7 - q^5.$$

Daher ist $q^5 + q^2 \leq v$ und eingesetzt in (C.59) folgt wegen $q^5 \leq q^5x - 1$, dass

$$q^5(q^5+q^2) \leq (q^5x-1)v = (q^2-1)(q^7-x) \leq q^9,$$

ein Widerspruch. Wir haben somit

$$q^4 - xv \geq q^2 + 1,$$

und aus (C.60) und (C.56) erhalten wir mit $v \geq 0$ die Abschätzung

$$\begin{aligned} q^7 + q^4 - q^2 = q^7 + q^2(q^2-1) &\geq q^7 + x(q^2-1) = v + q^5(q^4 - xv) \\ &\geq q^5(q^2+1) = q^7 + q^5, \end{aligned}$$

ein Widerspruch zu unserer ersten Annahme. Daher gilt die Behauptung. □

(C.12) Lemma.

Es ist $q^{2l-3}x - 1 \nmid \frac{(q^l+1)(q^{l-1}+1)(q^{l-1}-1)(q^{l-2}-1)}{q^2-1}$ *mit* $4 \leq l \in \mathbb{N}$.

Beweis. Angenommen

$$q^{2l-3}x - 1 \mid \frac{(q^l+1)(q^{l-1}+1)(q^{l-1}-1)(q^{l-2}-1)}{q^2-1}, \quad l \geq 4.$$

Dann gibt es ein $y \in \mathbb{N}$ mit

$$\begin{aligned}(q^2-1)(q^{2l-3}x-1)y &= (q^l+1)(q^{l-1}+1)(q^{l-1}-1)(q^{l-2}-1) \\ &= (q^{2l-2}-q^l+q^{l-2}-1)(q^{2l-2}-1).\end{aligned} \tag{C.61}$$

Sei zunächst $l \geq 5$. Offenbar ist dann auch

$$-(q^2-1)y \equiv -(q^{l-2}-q^l-1) \mod q^{2l-3},$$

und daher gibt es ein $z \in \mathbb{Z}$ mit

$$0 \leq (q^2-1)y = zq^{2l-3} + q^{l-2} - q^l - 1. \tag{C.62}$$

Da $q^{l-2} - q^l - 1 < 0$ ist offenbar

$$z \geq 1.$$

Setzen wir nun (C.62) in (C.61) ein, so erhalten wir

$$(q^{2l-3}x-1)(zq^{2l-3}+q^{l-2}-q^l-1) = (q^l+1)(q^{l-2}-1)(q^{2l-2}-1). \tag{C.63}$$

Angenommen $x > q^2$. Dann folgt aus (C.63), dass

$$\begin{aligned}(q^{2l-3}(q^2+1)-1)(q^{l-3}-1)q^l &= (q^{2l-3}(q^2+1)-1)(q^{2l-3}-q^l) \\ &\leq (q^{2l-3}x-1)(zq^{2l-3}+q^{l-2}-q^l-1) \\ &= (q^l+1)(q^{l-2}-1)(q^{2l-2}-1) \\ &= (q^{2l-2}-q^l+q^{l-2}-1)(q^{2l-2}-1) \\ &< q^{2l-2}q^{2l-2} \\ &= q^{4l-4},\end{aligned} \tag{C.64}$$

also auch

$$(q^{2l-3}(q^2+1)-1)(q^{l-3}-1) < q^{3l-4}. \tag{C.65}$$

Ausmultiplizieren der linken Seite ergibt

$$q^{3l-6} - q^{2l-3} - q^{2l-1} - q^{l-3} \leq 0.$$

Division durch q^{l-3} und Addition von 1 liefert

$$q^l(q^{l-3}-1-q^2) = q^{2l-3} - q^l - q^{l+2} \leq 1,$$

ein Widerspruch für $l > 5$. Ist $l = 5$, so liefern die drei ersten Zeilen aus (C.64) gerade

$$(q^7(q^2+1)-1)(q^2-1)q^5 \leq (q^5+1)(q^3-1)(q^8-1) = (q^5+1)(q^3-1)(q^4+1)(q^2+1)(q^2-1)$$

und somit

$$(q^9 + q^7 - 1)q^5 \leq (q^5 + 1)(q^3 - 1)(q^4 + 1)(q^2 + 1).$$

Ausmultiplizieren führt auf

$$0 \leq -q^{11} + q^{10} - 2q^6 + 2q^5 - 2q^4 - 2q^3 - 1,$$

ein Widerspruch. Damit ist

$$x \leq q^2 - 1 \tag{C.66}$$

für $l \geq 5$.

Wir zeigen nun, dass $x > q$. Nach (C.63) gilt

$$q^{2l-3}x - 1 \mid (q^{l-2} - 1)(q^l + 1)(q^{2l-2} - 1)x. \tag{C.67}$$

Offenbar ist

$$q^{2l-2}x - x = x(q^{2l-3}x - 1) + (q - x)q^{2l-3}x,$$

also ist auch

$$q^{2l-3}x - 1 \mid (q^{l-2} - 1)(q^l + 1)(q - x)q^{2l-3}x.$$

Wegen $ggT(q^{2l-3}x - 1, q^{2l-3}x) = 1$ ist somit

$$q^{2l-3}x - 1 \mid (q^{l-2} - 1)(q^l + 1)(q - x)$$

und daher auch

$$\begin{aligned} q^{2l-3}x - 1 \mid (q^{l-2} - 1)(q^l + 1)(q - x)q^{l-3}x \\ = (q - x)(q^{l-2} - 1)(q^{2l-3}x + q^{l-3}x) \\ = (q - x)(q^{l-2} - 1)(q^{2l-3}x - 1) + (q - x)(q^{l-2} - 1)(q^{l-3}x + 1) \end{aligned}$$

Schließlich folgt

$$q^{2l-3}x - 1 \mid (q^{l-2} - 1)(q^{l-3}x + 1)(q - x). \tag{C.68}$$

Angenommen $x < q$. Dann ist

$$\begin{aligned} 2q^{2l-3} - 1 &\leq q^{2l-3}x - 1 \\ &\leq (q^{l-2} - 1)(q^{l-3}x + 1)(q - x) \\ &< q^{l-2}(q^{l-3}(q - 1) + 1)q \\ &< q^{l-2}q^{l-2}q \\ &= q^{2l-3}, \end{aligned}$$

ein Widerspruch. Wir haben gezeigt, dass

$$x > q.$$

Schließlich folgt mit (C.68), dass

$$q^{2l-3}x - 1 \leq (q^{l-2} - 1)(q^{l-3}x + 1)(x - q) < q^{l-2}x(q^{l-3}x + 1),$$

also auch

$$q^{2l-3}x \leq q^{l-2}x(q^{l-3}x + 1).$$

Division durch $q^{l-2}x$ liefert wegen $x > q$ und (C.66) schließlich

$$q^{l-1} \leq q^{l-3}x + 1 \leq q^{l-3}(q^2 - 1) + 1 = q^{l-1} - q^{l-3} + 1,$$

ein Widerspruch. Für $l \geq 5$ gilt daher die Behauptung.

Es bleibt der Fall $l = 4$. Aus (C.61) sehen wir sofort

$$(q^5x - 1)y = (q^4 + 1)(q^6 - 1). \tag{C.69}$$

Offenbar ist dann auch

$$-y \equiv -(q^4 + 1) \mod q^5,$$

und daher gibt es ein $z \in \mathbb{Z}$ mit

$$0 \leq y = zq^5 + q^4 + 1$$

und offenbar $z \geq 1$. Eingesetzt in (C.69) erhalten wir

$$(q^5x - 1)(zq^5 + q^4 + 1) = (q^4 + 1)(q^6 - 1).$$

Wegen $x > 1$ folgt

$$q^5(q^5 + q^4 + 1) < (q^5x - 1)(zq^5 + q^4 + 1) = (q^4 + 1)(q^6 - 1) < (q^4 + 1)q^6,$$

und Division durch q^5 liefert

$$q^5 + q^4 + 1 < (q^4 + 1)q = q^5 + q,$$

ein Widerspruch. Damit gilt insgesamt die Behauptung. □

(C.13) Lemma.

Es ist $q^{l-1}x - 1 \nmid \frac{(q^l-1)(q^{l-1}+1)}{q+1}$ *für* $l \geq 4$.

Beweis. Angenommen

$$q^{l-1}x - 1 \mid \frac{(q^l - 1)(q^{l-1} + 1)}{q + 1}, \quad l \geq 4.$$

Dann gibt es ein $y \in \mathbb{N}$ mit

$$(q + 1)(q^{l-1}x - 1)y = (q^l - 1)(q^{l-1} + 1). \tag{C.70}$$

Offenbar gilt dann auch

$$-(q + 1)y \equiv -1 \mod q^{l-1},$$

und daher gibt es ein $z \in \mathbb{Z}$ mit

$$q + 1 \leq (q + 1)y = zq^{l-1} + 1 \tag{C.71}$$

und es ist offenbar

$$z \geq 1.$$

Setzen wir (C.71) in (C.70) ein, so folgt

$$(q^{l-1}x - 1)(q^{l-1}z + 1) = (q^l - 1)(q^{l-1} + 1). \tag{C.72}$$

Wir zeigen, dass $x > q$. Aus (C.72) sehen wir, dass

$$q^{l-1}x - 1 \mid (q^{l-1} + 1)(q^l - 1)x = (q^{l-1} + 1)(q^l x - x). \tag{C.73}$$

Offenbar ist

$$q^l x - x = x(q^{l-1}x - 1) + (q - x)q^{l-1}x,$$

also ist nach (C.73) auch

$$q^{l-1}x - 1 \mid (q^{l-1} + 1)(q - x)q^{l-1}x.$$

Wegen $ggT(q^{l-1}x - 1, q^{l-1}x) = 1$ ist daher

$$q^{l-1}x - 1 \mid (q^{l-1} + 1)(q - x).$$

Wir sehen damit, dass

$$\begin{aligned} q^{l-1}x - 1 \mid (q^{l-1} + 1)(q - x)x \\ &= (q^{l-1}x + x)(q - x) \\ &= (q^{l-1}x - 1)(q - x) + (1 + x)(q - x). \end{aligned}$$

Schließlich ergibt sich

$$q^{l-1}x - 1 \mid (1 + x)(q - x).$$

Angenommen $x < q$. Dann folgt

$$2q^{l-1} - 1 \leq q^{l-1}x - 1 \leq (1 + x)(q - x) \leq q(q - 1) = q^2 - q,$$

ein Widerspruch. Daher ist

$$x > q.$$

Aus (C.72) folgt damit schließlich

$$(q^l - 1)(q^{l-1} + 1) < (q^{l-1}x - 1)(q^{l-1}z + 1) = (q^l - 1)(q^{l-1} + 1),$$

ein Widerspruch zu unserer ersten Annahme. Daher gilt die Behauptung. □

(C.14) Lemma.

Es ist $q^{l-1}x - 1 \nmid \frac{(q^l+1)(q^{l-1}-1)}{q+1}$ *für* $l \geq 3$.

Beweis. Angenommen

$$q^{l-1}x - 1 \mid \frac{(q^l + 1)(q^{l-1} - 1)}{q + 1}, \quad l \geq 3.$$

Dann gibt es ein $y \in \mathbb{N}$ mit

$$(q + 1)(q^{l-1}x - 1)y = (q^l + 1)(q^{l-1} - 1). \tag{C.74}$$

Offenbar gilt dann auch

$$-(q + 1)y \equiv -1 \mod q^{l-1},$$

und daher gibt es ein $z \in \mathbb{Z}$ mit

$$q + 1 \leq (q + 1)y = zq^{l-1} + 1 \tag{C.75}$$

und

$$z \geq 1.$$

Setzen wir (C.75) in (C.74) ein, so folgt

$$(q^{l-1}x - 1)(q^{l-1}z + 1) = (q^l + 1)(q^{l-1} - 1). \tag{C.76}$$

Wir zeigen, dass $x > q$. Aus (C.76) sehen wir, dass

$$q^{l-1}x - 1 \mid (q^{l-1} - 1)(q^l + 1)x = (q^{l-1} - 1)(q^l x + x). \tag{C.77}$$

Offenbar ist

$$q^l x + x = -x(q^{l-1}x - 1) + (x + q)q^{l-1}x,$$

also ist nach (C.77) auch

$$q^{l-1}x - 1 \mid (q^{l-1} - 1)(x + q)q^{l-1}x.$$

Wegen $ggT(q^{l-1}x - 1, q^{l-1}x) = 1$ ist daher

$$q^{l-1}x - 1 \mid (q^{l-1} - 1)(q + x).$$

Wir sehen damit, dass

$$\begin{aligned} q^{l-1}x - 1 \mid (q^{l-1} - 1)(q + x)x \\ &= (q^{l-1}x - x)(q + x) \\ &= (q^{l-1}x - 1)(q + x) + (1 - x)(q + x). \end{aligned}$$

Schließlich ergibt sich

$$q^{l-1}x - 1 \mid (1 - x)(q + x).$$

Wegen $x > 1$ ist also

$$q^{l-1}x - 1 \leq (x - 1)(q + x).$$

Angenommen $x < q$. Dann folgt

$$2q^{l-1} - 1 \leq q^{l-1}x - 1 \leq (q + x)(x - 1) \leq 2q(q - 1) = 2q^2 - 2q,$$

ein Widerspruch. Daher ist

$$x > q.$$

Aus (C.76) folgt schließlich

$$\begin{aligned} q^{2l-1} - q^{l-1} + q^l - 1 &= (q^l - 1)(q^{l-1} + 1) < (q^{l-1}x - 1)(q^{l-1}z + 1) \\ &= (q^l + 1)(q^{l-1} - 1) = q^{2l-1} + q^{l-1} - q^l - 1. \end{aligned}$$

Wir formen dies um zu

$$2q^l < 2q^{l-1},$$

ein Widerspruch zu unserer ersten Annahme. Daher gilt die Behauptung. □

(C.15) Lemma.

Es ist $q^l x - 1 \nmid q^{2l} - 1$ *mit* $l \geq 2$.

Beweis. Angenommen

$$q^l x - 1 \mid q^{2l} - 1.$$

Dann gibt es ein $y \in \mathbb{N}$ mit

$$(q^l x - 1)y = q^{2l} - 1. \tag{C.78}$$

Offenbar ist dann auch

$$-y \equiv -1 \mod q^l,$$

und daher gibt es ein $z \in \mathbb{Z}$ mit

$$0 \leq y = zq^l + 1 \tag{C.79}$$

und

$$z \geq 0.$$

Setzen wir nun (C.79) in (C.78) ein, so erhalten wir

$$(q^l x - 1)(zq^l + 1) = q^{2l} - 1. \tag{C.80}$$

Ist $z = 0$, dann ist $x = q^l$, ein Widerspruch, und somit ist

$$z \geq 1.$$

Wegen $x > 1$ folgt daher mit (C.80), dass

$$q^{2l} - 1 = (q^l - 1)(q^l + 1) < (q^l x - 1)(zq^l + 1) = q^{2l} - 1,$$

ein Widerspruch zu unserer ersten Annahme. Daher gilt die Behauptung. □

(C.16) Lemma.

Es ist $\frac{q^2}{2}x - 1 \nmid q^4 - 1$ *für* $q = 2^f$ *mit* $f > 1$.

Beweis. Angenommen

$$2^{2f-1}x - 1 \mid 2^{4f} - 1.$$

Dann gibt es ein $y \in \mathbb{N}$ mit

$$(2^{2f-1}x - 1)y = 2^{4f} - 1. \tag{C.81}$$

Offenbar ist dann auch

$$y \equiv 1 \mod 2^{2f-1},$$

und daher gibt es ein $z \in \mathbb{Z}$ mit

$$0 \leq y = z2^{2f-1} + 1 \tag{C.82}$$

und

$$z \geq 0.$$

Setzen wir nun (C.82) in (C.81) ein, so erhalten wir

$$(2^{2f-1}x - 1)(2^{2f-1}z + 1) = 2^{4f} - 1.$$

Ist $z = 0$, dann ist x eine 2-Potenz, ein Widerspruch. Für $z = 1$ liefert die Division von $2^{4f} - 1$ durch $2^{2f-1} + 1$ einen Rest 3, was nur für $f = 1$ möglich ist. Daher ist $z \geq 2$ und wegen $x > 2$ folgt nun

$$2^{4f} - 1 = (2^{2f} - 1)(2^{2f} + 1) < (2^{2f-1}x - 1)(2^{2f-1}z + 1) = 2^{4f} - 1,$$

ein Widerspruch. □

Literaturverzeichnis

[1] Abe, E.: Finite Groups admittting Bruhat decompositions of type A_n. Tohoku Math. J. **16** (1964)

[2] Aschbacher, M.: Finite Group Theory. Cambridge University Press (1986)

[3] Bloom, D.M.: The Subgroups of $PSL_3(q)$ for odd q. Trans. Amer. Math. Soc. **127** (1967)

[4] Bourbaki, N.: Groupes et algebres de Lie. Chapitres 4,5 et 6 Elements de Mathematique (1968)

[5] Cameron, P.J.: Permutation Groups. Cambridge University Press, London Mathematical Society Student Texts **45** (1999)

[6] Carter, R.W.: Simple Groups of Lie-Type. J.Wiley & Sons (1972)

[7] Carter, R.W.: Finite Groups of Lie-Type. J.Wiley & Sons (1985)

[8] Conway, J., *et al.* : Atlas of Finite Groups. Clarendon Press, Oxford (1985)

[9] Cooperstein, B.N.: The Geometry of Root Subgroups in Exceptional Groups I. Geometriae Dedicata **8** (1979)

[10] Cooperstein, B.N.: An enemies list for factorization theorems. Comm. Alg. **6** (1978)

[11] Curtis, C.W., Kantor, W.M., Seitz, G.M.: The 2-Transitive Permutation Representations of the Finite Chevalley Groups. Transact. AMS **218** (1976)

[12] Fong, P., Seitz, M.: Groups with a (B, N)-Pair of Rank 2 I. Invent. math. **21** (1973)

[13] Fong, P., Seitz, M.: Groups with a (B, N)-Pair of Rank 2 II. Invent. math. **24** (1974)

[14] Gorenstein, D., Lyons, R., Solomon, R.: The Classification of the Finite Simple Groups. Mathematical Surveys an Monographs, Vol. **40**, No.1, AMS (1994)

[15] Gorenstein, D., Lyons, R.: The local structure of finite groups of characteristic 2-type. Memoirs of the AMS, **276** (1983)

[16] Hartley, R.W.: Determination of the Ternary Collineation Groups whose Coefficients lie in the $GF(2^n)$. Ann. of Math. **27** (1926)

[17] Higman, D.G., McLaughlin, J.: Geometric ABA-Groups. Illinois J. Math. **5** (1961)

[18] Humphreys, J.E.: Reflection Groups and Coxeter Groups. Cambridge studies in advanced mathematics **29** (1990)

[19] Huppert, B.: Zweifach transitive auflösbare Permutationsgruppen. Math. Z. **68** (1957)

[20] Kantor, W.M., Seitz, G.M.: Some results on 2-transitive groups. Invent. Math. **13** (1971)

[21] Kantor, W.M., Hering, C., Seitz, G.M.: Finite Groups with a split BN-pair of rank 1. Journal of Algebra **20** (1972)

[22] Kleidman, P.B.: The maximal subgroups of the Chevalley Groups $G_2(q)$ with q odd, the Ree Groups ${}^2G_2(q)$, and Their Automorphism Groups. Journal of Algebra **117** (1988)

[23] Kurzweil, H., Stellmacher, B.: Theorie der endlichen Gruppen. Springer (1998)

[24] Kurzweil, H.: Endliche Gruppen. Springer (1977)

[25] Maillet, E.: Sur les isomorphes holoédriques et transitivs des groupes symétriques ou alternés. J. Math. Pures Appl. **5** (1895)

[26] Malle, G.: The maximal subgroups of ${}^2F_4(q^2)$. Journal of Algebra **139** (1991)

[27] Meixner, T.: Tits Chamber Systems in Charakteristic 3. Geom. Dedicata **35** (1990)

[28] Mitchell, H.H.: Determination of the Ordinary and Modular Ternary Collineation Groups. Trans. Amer. Math. Soc. **12** (1911)

[29] Mortimer, B., Dixon, J.D.: Permutation Groups. Springer (1996)

[30] Ronan, M.: Lectures on Buildings. Academic Press (1989)

[31] Seitz, M.: Flag-transitive subgroups of Chevalley groups. Annals of Mathematics **97** (1973), Correction unpublished

[32] Shinoda, K.: Conjugacy classes of the finite Ree groups. Journal of the Fac. of Science Tokyo, Sect. IA **22** (1975)

[33] Suzuki, M.: On a Class of Doubly Transitive Groups. Ann. of Math. (2) **75** (1962)

[34] Timmesfeld, F.G.: Abstract Root Subgroups and Simple Groups of Lie-Type. Birkhäuser (2001)

[35] Tits, J.: Buildings of spherical type and finite BN-Pairs. Lecture Notes in Mathematics., vol **386**, Springer (1974)

[36] Tits, J., Weiss, R.: Moufang Polygons. Springer (2002)

[37] Tits, J.: Endliche Spiegelungsgruppen, die als Weylgruppen auftreten. Invent. Math. **43** (1977)

[38] Van Maldeghem, H.: Generalized Polygons. Birkhäuser (1998)

[39] Walter, J.H.: Finite Groups with abelian Sylow 2-Groups of Order 8. Invent. Math. **2** (1967)

[40] Wielandt, H.: Finite Permutation Groups. Academic Press (1964)

[41] Zsigmondy, K.: Zur Theorie der Potenzreste. Monatshefte Math. Phys. **3** (1892)