Contributions to the Classification of Tame K^*-groups of Odd Type and Other Applications of 2-local Theory

Christine Altseimer

Dissertation
zur Erlangung des Doktorgrades
der Mathematischen Fakultät
der Albert-Ludwigs-Universität
Freiburg im Breisgau

August 1998

Dekan der mathematischen Fakultät:
Prof. Dr. Ludger Rüschendorf

Erster Referent:
Prof. Dr. Martin Ziegler

Zweiter Referent:
Prof. Dr. Alexandre V. Borovik

Datum der Promotion:
5. November 1998

Wer fertig ist, dem ist nichts recht zu machen,
ein Werdender wird immer dankbar sein.
(J. W. von Goethe)

Acknowledgments

My most grateful thanks go to Professor Alexandre Borovik at UMIST, who was my supervisor during the academic year 1996/97, and without whom nothing of this work would have been possible. He proposed the topics of the dissertation and was always there to give his ideas and advice freely. I warmly remember all our mathematical discussions at different places in and around Manchester, which gave me a deeper understanding of mathematical structures and a great enthusiasm to explore them.

I also thank Professor Martin Ziegler, who gave me the freedom to write a dissertation that is only losely connected with his mathematical interests, and who still gave me all the support I needed from him during these last years.

From time to time I was also able to discuss my work with other people, and I would like to thank them all in this place. Namely there were Laci Babai, Eamonn O'Brien, Markus Junker, William Kantor, Charles Leedham-Green, Frank Lübeck, Jürgen Müller and Akos Seress.

For the financial support during the last two years, I thank the Landesgraduiertenförderung Baden-Württemberg and the German Academic Exchange Service (DAAD, HSPII/AUFE).

Zusammenfassung

Involutionen spielen innerhalb der Gruppentheorie eine besonders interessante Rolle. Zum einen sind sie die denkbar einfachsten Studienobjekte und sind uns allen als Spiegelungen vertraut, zum anderen tragen die von ihnen definierten Strukturen einen sehr hohen Informationswert. So wurden beispielsweise viele endliche einfache Gruppen mit Hilfe der Zentralisatoren ihrer Involutionen charakterisiert und, im Falle der sporadischen Gruppen, gefunden; halbeinfache komplexe Lie Algebren lassen sich durch ihr Wurzelsystem klassifizieren, ein Wurzelsystem ist aber im wesentlichen nichts anderes als ein geschlossenes Spiegelsystem.

Diese Arbeit liefert eine Vielzahl von weiteren Beispielen, wie Involutionen die Struktur einer Gruppe bestimmen. Im Mittelpunkt steht dabei die 2-lokale Analyse von Gruppen, d.h. das Studium von Normalisatoren elementar-abelscher 2-Untergruppen.

Zunächst geht es um die Klassifikation der einfachen Gruppen von endlichem Morley-Rang. Gruppen von endlichem Morley-Rang können dabei als Gruppen mit einer "Dimension" [18] verstanden werden, d.h. als Verallgemeinerung algebraischer Gruppen. G. Cherlin [32] vermutete, daß die zwei Klassen von Gruppen im wesentlichen zusammenfallen und unendliche einfache Gruppen von endlichem Morley Rang algebraische Gruppen über algebraisch abgeschlossenen Körpern sind. Ein Schritt zum Beweis der Cherlinschen Vermutung ist die Klassifikation der zahmen Gruppen von endlichem Morley-Rang; das sind Gruppen, bei denen gewisse, modelltheoretische, Konstellationen von vorneherein ausgeschlossen werden. Der grundlegende Ansatz ist, mit einem minimalen Gegenbeispiel zur Cherlinschen Vermutung, einer K^*-Gruppe, zu arbeiten. Zahme K^*-Gruppen von endlichem Morley-Rang zerfallen natürlicherweise in zwei Klassen, die Gruppen von geradem und ungeradem Typ, je nachdem, ob die Sylow 2-Untergruppen denen der algebraischen Gruppen über einem Körper der Charakteristik 2 oder ungleich 2 gleichen.

Das Hauptresultat der Dissertation ist die Charakterisierung einfacher algebraischer Gruppen von Rang 2 über einem algebraisch abgeschlossenen Körper der Charakteristik ungleich 2 in der Klasse der zahmen K^*-Gruppen von endlichem Morley-Rang mit Hilfe von Zentralisatoren von Involutionen in Kapitel 4. So werden wir beweisen, daß eine einfache zahme K^*-Gruppe G von endlichem Morley-Rang isomorph zu $\mathrm{PSp}_4(K)$ oder $\mathrm{G}_2(K)$ ist, falls G eine Involution i enthält, so daß $C_G(i)^\circ/O(C_G(i))$ entweder isomorph zu $\mathrm{SL}_2(K) * \mathrm{SL}_2(K)$ oder zu $\mathrm{PSL}_2(K) \times K^*$ für einen algebraisch abgeschlossenen Körper K von Charakteristik 0 oder Charakteristik p für eine Primzahl $p \neq 2, 3$ ist.

Die Kapitel 2 und 3 dienen der technischen Vorbeitung dieser Sätze. In Kapitel 2 untersuchen wir quasiunipotente Gruppen, die in der Theorie der Gruppen von endlichem Morley-Rang die Rolle unipotenter Untergruppen einer algebraischen Gruppe übernehmen. Wir können zeigen, daß eine zahme auflösbare Gruppe G von endlichem Morley-Rang eine eindeutig bestimmte maximale quasiunipotente Untergruppe besitzt. Der zentrale Satz in Kapitel 3 besagt, daß eine stark eingebettete Untergruppe einer zahmen einfachen K^*-Gruppe G entweder auflösbar ist, oder G von ungeradem Typ und Prüfer 2-Rang 1 ist. Mit Hilfe dieses Satzes kann das Auftreten bestimmter Konfigurationen in zahmen einfachen K^*-Gruppen von ungeradem Typ ausgeschlossen werden.

Der zweite Teil der Arbeit beschäftigt sich mit der Frage, wie man zwei endliche einfache Gruppen unterscheiden kann, wenn man nur die Ordnungen von einer Menge zufälliger Elemente der Gruppe und von deren Produkten kennt. Die bisherigen Algorithmen haben im wesentlichen die Statistik der Elementordnungen benutzt. Der einzige Fall, der sich mit dieser Methode nicht behandeln läßt, ist die Unterscheidung zwischen $PSp_{2n}(q)$ und $\Omega_{2n+1}(q)$, da diese beiden Gruppen nicht nur diesselbe Ordnung haben, sondern im Prinzip auch dieselbe Statistik von Elementordnungen. Im 6. Kapitel stellen wir einen Algorithmus vor, der dieses Problem löst, indem er die Unterschiede in der Struktur von Konjugiertenklassen von Involutionen in diesen beiden Gruppen nützt. In Kapitel 5 werden hierzu die Ordnungen von stark realen Elementen in diesen beiden Gruppen bestimmt.

Contents

Introduction

Involutions of a group are special objects in many ways. On the one hand they are very easy to study and we all know them as reflections. On the other hand, the structure definable by involutions bears a great deal of information. Many finite simple groups have been characterized or, in the case of sporadic groups, even found by means of the centralizers of involutions. Semisimple complex Lie algebras can be classified by their root system, which is nothing else but a closed system of mirrors.

This thesis gives some new examples of how involutions determine the structure of groups. We will be mostly concerned with the 2-local analysis of groups, i.e. the study of normalizers of elementary abelian 2-subgroups. The first part of the thesis gives applications to groups of finite Morley rank, the second part an application to black box groups.

One of the great open problems in model theory is the Cherlin-Zil'ber conjecture. It states that an infinite simple group of finite Morley rank is isomorphic, as an abstract group, to an algebraic group over an algebraically closed field. This would imply that for simple groups the existence of a rank function obeying certain natural conditions would already suffice to obtain all its geometrical structure.

The original model theoretic approach to prove the Cherlin-Zil'ber conjecture was the following. Zil'ber has shown that we can interpret a field in a connected solvable non-nilpotent group of finite Morley rank. As it is of finite Morley rank such a field has to be algebraically closed by Macintyre's theorem. Hence there is always an algebraically closed field K interpretable in a simple infinite group G of finite Morley rank as long as none of its proper sections is a bad group. Here a *bad group* is a non-solvable group of finite Morley rank all of whose proper definable and connected subgroups are nilpotent. K will in general bear extra structure which is induced by G. If this structure is definable in K itself, then K is said to be *pure*. Hrushovski has shown that if a field K is interpretable in a simple group of finite Morley rank, we can interpret the group in K. If K is pure, then the group is already algebraic by a result of Hrushovski again. Zil'ber actually conjectured that all fields of finite Morley rank are pure, which would imply the Cherlin-Zil'ber conjecture for simple groups of finite Morley rank that do not interpret a bad group. However, Hrushovski constructed a field of finite Morley rank that is not pure. It is not known up to now if bad groups or fields in which non-algebraic groups can be interpreted exist.

Since then a new approach was proposed by Borovik, Cherlin and Nesin. Their idea is to apply the methods from the classification of finite simple groups (CFSG) to the context of groups of finite Morley rank. They believe that CFSG actually consists of several more or less independent theories. One theory, "sporadic", deals with "sporadic objects", the other "generic theory", describes structural properties of the majority of finite simple groups, namely, large groups of Lie type. If G is an affine algebraic group and $X \subseteq G$ an affine subvariety, then the the logarithm of the number of $GF(q)$-points of X is approximately $\dim X$ by a Lang-Weil type estimate [31]. If, for example, the center of G has dimension m, then the center of the corresponding finite group over $GF(q)$ has order approximately q^m. This enables one to some extent to deduce properties of finite simple groups from properties of simple algebraic groups. On the other hand much of the theory of groups of finite Morley rank is inspired be the part of CFSG that deals with large groups of Lie type.

To actually make this approach work we have to assume that no bad fields are interpretable in the group. A *bad field* is a ranked structure of the form $\langle K, +, \cdot, A \rangle$, where K is an algebraically closed field and A is a proper infinite multiplicative subgroup of K^*. If we call a group of finite Morley rank *tame* if none of its proper sections is a bad group and if it does not interpret a bad field, then the Cherlin-Zil'ber conjecture splits into three parts.

Conjecture 1 *Bad groups do not exist.*

Conjecture 2 *Bad fields do not exist.*

Conjecture 3 *A simple tame group of finite Morley rank is isomorphic to an algebraic group over an algebraically closed field.*

While a proof of the conjectures 1 and 2 is most likely to involve heavy model theory, it is hoped that the proof of Conjecture 3 can be achieved using ideas from finite group theory. The first of these is to analyse a minimal counterexample to Conjecture 3. A group of finite Morley rank is called a *K-group*, if every infinite simple definable and connected section of the group is an algebraic group over an algebraically closed field. A *K^*-group* is a group of finite Morley rank in which every proper definable subgroup is a K-group. In this inductive setting the conjecture reduces to the following:

Conjecture 4 *An infinite simple tame K^*-group is isomorphic to an algebraic group over an algebraically closed field.*

It is known [3] that an infinite simple tame K^*-group G is either of *even type*, meaning that its Sylow 2-subgroups are nilpotent, definable and of bounded exponent, or of *odd type*, meaning that the Sylow 2-subgroups are divisible abelian by finite. If G is of even type, Conjecture 4 would imply that G is isomorphic to an algebraic group over an algebraically closed field of characteristic 2. If G is of odd type, then G should be isomorphic to an algebraic group over an algebraically closed field of characteristic not 2. Depending on the type of the group, very different methods are required.

In this thesis we are dealing with the classification of simple tame K^*-groups of odd type. This case splits into three parts: Let G be a simple tame K^*-group of odd type. Either G is small, meaning that normal 2-rank of the group is less than 3, or G contains a proper 2-generated core or G satisfies the so-called B-conjecture and contains a classical involution. The last case could be almost completely described by A. Berkman in [15]. The second case should not appear at all and we will prove a partial result pointing in this direction in Chapter 3. Since, however, the amount of information which we have in the first case is extremly small, this is the most difficult part in the classification of simple tame K^*-groups of finite Morley rank. By Conjecture 4, we know what to expect.

Conjecture 5 *An infinite simple tame K^*-group G of odd type and normal 2-rank $n(G) \leq 2$ is isomorphic to one of the groups $\mathrm{PSL}_2(K)$, $\mathrm{PSL}_3(K)$, $\mathrm{PSp}_4(K)$, $\mathrm{G}_2(K)$ over some algebraically closed field K of characteristic not 2.*

We are mainly concerned with first approaches to prove this conjecture. In analogy with the CFSG, we attempted a characterization of the groups in question with the help of centralizers of involutions.

Chapter 2 and 3 provide the technical machinery which is used to prove the main classification results. Chapter 2 is dedicated to a thorough discussion of the concepts of quasi- and pseudounipotent. These are generalizations of unipotent subgroups of algebraic groups to the context of groups of finite Morley rank. The main result is, that if G is a solvable group of finite Morley rank which does not interpret a bad field then there exists exactly one maximal pseudounipotent (quasiunipotent) subgroup H (U) of G and H and U are characteristic subgroups. Especially maximal pseudounipotent (quasiunipotent) subgroups of a K-group of finite Morley rank which does not interpret a bad field are conjugate.

In Chapter 3 we discuss strongly embedded subgroups of a simple K^*-group of finite Morley rank and odd type that does not interpret a bad field. Strongly embedded subgroups should not exist in this context at all. As a first step we show that strongly embedded subgroups are solvable if the Prüfer 2-rank of G is greater than 1. This implies for example that G does not contain a proper 2-generated core, if G is of normal 2-rank greater than 2 and contains a non-solvable centralizer of an involution. In Section 3.2 we give an application of the Thompson rank formula, which we already proved in Section 1.1. This formula allows one to compute the Morley rank of a group of finite Morley rank with at least two conjugacy classes of involutions just using the structure of centralizers of involutions.

The main classification results are proved in Chapter 4. We give a partial characterization for PSL_3:

Theorem *Let G be a simple K^*-group of finite Morley rank that does not interpret a bad field. Assume that the centralizers of involutions of G are isomorphic to $\mathrm{GL}_2(K)$ for some algebraically closed field K of characteristic not 2. Then G is isomorphic to $\mathrm{PSL}_3(K)$, if there exists an involution i and a quasiunipotent subgroup $U \leq C_G(i)$ which is maximal in $C_G(i)$ but not maximal in G.*

For groups of larger dimension we achieve a better result.

Theorem *Let G be a simple K^*-group of finite Morley rank that does not interpret a bad field. Assume that G contains an involution i, such that either*

(i) $C_G(i)^\circ/O(C_G(i)) \cong \mathrm{SL}_2(K) * \mathrm{SL}_2(K)$, *where the two copies of* $\mathrm{SL}_2(K)$ *intersect nontrivially or*

(ii) $C_G(i)^\circ/O(C_G(i)) \cong \mathrm{PSL}_2(K) \times K^*$

for an algebraically closed field K of characteristic neither 2 nor 3. Then $G \cong \mathrm{PSp}_4(K)$ or $G \cong \mathrm{G}_2(K)$.

The second part of this thesis is concerned with algorithms for *black box groups*. A *black box group G* is a finite group whose elements are encoded as 0-1 strings of uniform length N, and the group operations are performed by an oracle (the "black box") at unit cost. Furthermore a set S of generators is given in this encoding. The main question is how much information about the group can be gained in time polynomial in N. Ideally one would like to be able to compute the composition series of the group or to identify all the simple components. This will in general be an unfeasible task.

If we, for example, consider a finite group G of Lie type of dimension n over a field of q elements, then G can be considered as a black box group since elements can be encoded by a tuple of length $N := n^2 \log(q)$. Assume that $q = 2^m$ for some large m. Then – by the Lang-Weil type estimate already mentioned – the share of 2-elements in G is about $1/q^2$ and the share of elements of even order is about $1/q$. If we thus generate elements of G randomly using the generating set S, we cannot expect to generate an element of even order in time polynomial in $n^2 \log(q)$. Hence G is a simple group that appears to be solvable by the Feit-Thompson theorem in our setting.

A more feasible task is to try to identify a black box group G, given the promise that it is simple. Much progress has been made recently to solve this problem. Most algorithms which have been developed in this context use the additional assumption, that the orders of elements of G are given.

The algorithms proposed so far are mainly based on the statistics of element orders of G. The crucial case was thus to distinguish $\mathrm{PSp}_{2n}(q)$ from $\Omega_{2n+1}(q)$ for q odd and $n \geq 3$, since not only the orders of these two groups coincide, but also the statistics of orders of elements is for all practical purposes the same in both groups. In Chapter 6 we present an algorithm to solve this problem. The algorithm uses the difference in the 2-local structure of symplectic and orthogonal groups. This is feasible in our context since at least one quarter of the elements of these groups has even order [39] and we can thus generate involutions in polynomial time.

Chapter 5 develops the theoretical background for this problem by investigating orders of strongly real elements in the two groups.

Chapter 1

Preliminaries

1.1 Groups of Finite Morley Rank

Since [18] and [19] give a very good and easily accessible introduction to groups of finite Morley rank, we are only going to introduce the most important notions and to discuss the recent developments. The original source of a result is not given if it can also be found in one of these two works. Citations are made accordingly. A collection of the basic properties of groups of finite Morley rank can also be found in [6].

1.1.1 Basic Properties

There are two equivalent ways to define groups of finite Morley rank. The first one is the original model theoretic definition by means of a topological rank on the Stone-space associated to the Boolean algebra of definable subsets of a model. The second one the axiomatic description as groups with a "dimension" by Borovik. Details of how these two definitions connect can be found in [50] and in [6] as well.

Note that the term "definable" always refers to definability in some ranked universe $\mathcal{U}$ (see [18] for definitions and discussion). Model-theoretically speaking a set definable in a group $\mathcal{G}= \langle G, *, 1, \cdots \rangle$ is a boolean combination of sets of the form $A/\equiv$ where $A \subset G^n$ for some $n \in \mathbb{N}$ and $\equiv$ is definable in $\mathcal{G}$.

One of the most important group theoretic consequences is that a group G of finite Morley rank satisfies the descending chain condition for definable subgroups by [18, 5.2]. This yields that a group G of finite Morley rank contains a unique minimal definable subgroup of finite index, which is called *the connected component G° of G*. G is called *connected* if $G = G^\circ$. As a further consequence every subset X of G is contained in a minimal definable subgroup, the *definable* *closure* $d(X)$ *of* X. Note, that in general $d(X) \neq dcl(X)$. For any subgroup Y of G we call $Y^\circ := Y \cap d(Y)^\circ$ *the connected component of* Y .

Crucial for the understanding of groups of finite Morley rank is the 2-structure of them. Sylow 2-subgroups of a group G of finite Morley rank are conjugate to each other by [18, 10.11]. If S is one of them, then $S^\circ = B * D$ is a central product of a definable connected nilpotent subgroup B of bounded exponent and a divisible abelian group D by [18, 6.22]. B and D are characteristic in S. Thus S is nilpotent-by-finite and $Z(S) \neq 1$ by [18, exc. 12, p. 14]. We say that G is of *even type* if $D = 1$ and that G is of *odd type* if $B = 1$.

Involutions can also be used for rank estimates. Let G be any group. Elements of order 2 are called *involutions* and the set of all involutions is denoted by $I(G)$. Let $x \in G$ be a nontrivial element. x is called *strongly real* if there exists an involution $i \in G$ such that $x^i = x^{-1}$. Let $Sr(G)$ be the set of strongly real elements of G. For $x \in Sr(G)$ we denote by $C^*_G(x)$ the *generalized centralizer of* x *in* G, where $C^*_G(x) := \{g \in G : \ x^g \in \{x, x^{-1}\}\}$. We have the following analogue to the Brauer-Fowler theorem.

Fact 1.1 (see [18] and also [6]) *Let G be a group of finite Morley rank containing an involution i. Then there exists a strongly real element $x = i^g i^h$ for some $g, h \in G$ such that*

$$rk(G) \leq 2\, rk(C_G(i)) + k(x) \leq 2\, rk(C_G(i)) + rk(C_G(x))$$

where $k(x) := rk(I(C_G(x))$ if $x \in I(G)$ and $k(x) := rk\big(I(C^*_G(x) \backslash I(C_G(x))\big)$ otherwise.

If a group G of finite Morley rank contains at least two conjugacy classes of involutions, the Morley rank of G can be computed locally by the following formula. The underlying fact is, that if two involutions $i, j \in G$ are not conjugate, then there exists an involution in $d(ij)$ by [18, 10.2].

Proposition 1.2 (Thompson Rank Formula) *Let G be a group of finite Morley rank with at least two distinct conjugacy classes $C_1 = u_1^G$ and $C_2 = u_2^G$ of involutions. Assume that there exists a definable function $f : C_1C_2 \longrightarrow I(G)$ such that $f(x^g) = f(x)^g$ for all $x \in C_1C_2$ and $g \in G$ and*

$$f(x) \in \{g \in G : \ g^y = g^{-1} \text{ for all } y \in I(C^*_G(x) \backslash C_G(x))\}.$$

Let $\rho(i) = rk\big(\{(c_1, c_2) \in C_1 \times C_2 : \ f(c_1c_2) = i\}\big)$ for all $i \in I(G)$. If $X_1, \cdots, X_k$ is a definable partition of $I(G)$ into sets such that ρ is constant on each X_j then

$$2\, rk(G) = C_G(u_1) + C_G(u_2) + \max_{1 \leq j \leq k} \big(\rho(j) + rk(X_j)\big)$$

If G has finitely many conjugacy classes of involutions, we may take the X_j to be these classes. In the case where G contains exactly two conjugacy classes of involutions we get the simple equation

$$rk(G) = \max\big\{r_1 + rk(C_G(u_2)), r_2 + rk(C_G(u_1))\big\}$$

where $r_j := rk\big(\{(\kappa,\lambda) : \ \kappa \in C_1 \cap C_G(u_j),\ \lambda \in C_2 \cap C_G(u_j) \text{ and } f(\kappa\lambda) = u_j\}\big)$ *for* $j = 1, 2$.

Proof. Define a function $\varphi : C_1 \times C_2 \longrightarrow I(G)$ such that $\varphi(\lambda, \kappa) = f(\lambda\kappa)$. Then φ is definable and $rk(\varphi^{-1}(i)) = \rho(i)$. By [1, 6.1]

$$rk(C_1 \times C_2) = \max_{1\leq j\leq k}\{\rho(j) + rk(X_j)\}.$$

Since $rk(C_j) = rk(G) - rk(C_G(u_j))$ for $j = 1, 2$ and $rk(C_1 \times C_2) = rk(C_1) + rk(C_2)$ the first claim follows. Furthermore ρ is constant on conjugacy classes since $f(x^g) = f(x)^g$. Consider now

$$\varphi^{-1}(u_j) = \big\{(\kappa, \lambda) \in C_1 \times C_2 : \ f(\kappa\lambda) = u_j\big\}$$

for $j = 1, 2$. Since λ and κ invert $\lambda\kappa$, u_j must be inverted as well by choice of f and hence $\lambda, \kappa \in C_G(u_j)$. The final equation now follows easily, noting that $k = 2$, $X_1 = C_1$ and $X_2 = C_2$ in this case. □

Altınel [1] has shown that if G is a group of even type, then $d(x)$ contains exactly on involution for all $x \in C_1C_2$ and we can choose f to be the following function: $f(x) = I(d(x))$ for all $x \in C_1C_2$. If G is a group of odd type we should be able to construct such a function f in many cases as well if we have enough information about the conjugacy classes of involutions. This is no great restriction, however, since the Thompson rank formula can only be applied if we have precise information about the centralizers of involutions (compare [55, 5.1]). Section 3.2 gives an example of how the formula can be used.

1.1.2 Tame K^*-Groups

This thesis is mainly concerned with tame K^*-groups of finite Morley rank. A group of finite Morley rank is called *tame* if none of its proper sections is a bad group and if it does not interpret a bad field. A *bad group* is a non-solvable group of finite Morley rank all of whose proper definable and connected subgroups are nilpotent and a *bad field* is a ranked structure of the form $\langle K, +, \cdot, A\rangle$, where K is an algebraically closed field and A is a proper infinite multiplicative subgroup of K^*. We call a group of finite Morley rank *K-group*, if every infinite simple definable and connected section of the group is an algebraic group over an algebraically closed field. A *K^*-group* is a group of finite Morley rank in which every proper definable subgroup is a K-group. To work with K^*-groups means to work with a minimal counter-example to the Cherlin-Zil'ber Conjecture. The most crucial distinction in the theory of tame K^*-groups is the following:

Fact 1.3 ([3]) *Let G be a simple tame K^*-group. Then G is either of odd type or of even type.*

We need to introduce some terminology. If E is a finite elementary abelian 2-group, its *2-rank* $m(E)$ is the minimal number of generators of E. If H is any subgroup of a group G of finite Morley rank and odd type, its *2-rank* $m(H)$ is the maximum of the 2-ranks of elementary abelian subgroups in H. Note that the 2-rank is well-defined, since elementary abelian subgroups of a group of odd type are finite. If H is definable and S is a Sylow 2-subgroup of H, then the *normal 2-rank* $n(H)$ is the maximum of the 2-ranks of elementary abelian normal subgroups of S. Also, the *Prüfer 2-* $pr(H)$ of a not necessarily definable subgroup H is the maximum of the Prüfer ranks of Prüfer 2-subgroups of H. (A *Prüfer p-group* is a product of a finite number of copies of the quasi-cyclic group $\mathbb{Z}(p^\infty)$; the number of copies is called its *Prüfer rank*). Obviously $pr(G) \leq n(G)$ and if G is a simple algebraic group over an algebraically closed field of characteristic not 2, equality holds.

Let S be a Sylow 2-subgroup in a group G of finite Morley rank. We define the *2-generated core* $\Gamma_{S,2}(G)$ as the definable closure of the group generated by all normalizers $N_G(U)$ of all subgroup $U \leq S$ with $m(U) \geq 2$.

A group G of finite Morley rank will be called *semi-simple* , if $G = G'$ and $G/Z(G)$ is the direct sum of n non-abelian simple subgroups for some $n \in \mathbb{N}$. If $n = 1$, then G is called *quasi-simple* . The only proper normal subgroups of a quasi-simple group are the central ones. Quasi-simple algebraic groups are traditionally called *simple algebraic groups.* By a *component* of G we mean a subnormal quasi-simple subgroup of G. Components are definable and there are only finitely many of them by [18, 7.10]. The *layer of* G, $L(G)$, is the product of all components of G. It is definable and normal in G.

The *Fitting subgroup* $F(G)$ is the group generated by all normal nilpotent subgroups of G. $F(G)$ is nilpotent by [18, 7.3]. The *generalized Fitting subgroup* $F^*(G)$ is taken to be $F^\circ(G) * L^\circ(G)$. Then $C^\circ_G(F^*(G)) \leq F^*(G)$. G satisfies the *B-conjecture*, if $C^\circ_G(i) = F^*(C_G(i))$ for any involution $i \in G$. Simple algebraic groups over an algebraically closed field of characteristic not 2 satisfy the B-conjecture.

Let $i \in G$ be an involution. A component $A \lhd L(C_G(i))$ is called *intrinsic* if $i \in Z(A)$. An involution is called *classical* if its centralizer contains an intrinsic component isomorphic to $\mathrm{SL}_2(K)$ for an algebraically closed field K.

Fact 1.4 (Trichotomy Theorem,[19]) *Let G be a simple tame K^*-group of odd type. Then one of the following statements is true.*

- $n(G) \leq 2$.
- *G has a proper 2-generated core.*
- *G satisfies the B-conjecture and contains a classical involution.*

The largest part of this thesis will be concerned with first approaches to prove Conjecture 4 for the first case. There is furthermore the outline of a proof in [18] that the second case of the Trichotomy Theorem cannot occur if $n(G) \geq 3$. We have proved this result in Corollary 3.15 under the additional assumptions that G contains a non-solvable centralizer of an involution.

Suppose now that z is a classical involution in a simple tame K^*-group G of odd type and that $M \cong SL_2(K)$ is an intrinsic component in $C_G(z)$. Let Ω stand for the collection of all conjugates of M in G. Form a graph $\mathcal{D}$ with vertex set Ω by joining a vertex J to L if $[J, L] = 1$.

Fact 1.5 ([15]) *Let G be a simple tame K^*-group of finite Morley rank and odd type which satisfies the B-conjecture and contains a classical involution. Assume that the graph $\mathcal{D}$ is connected. Then G is isomorphic to one of the following groups:* $\mathrm{PSL}_n(K)$ *for* $n \geq 5$, $\mathrm{PSp}_{2n}(K)$ *for* $n \geq 3$, $\mathrm{PSO}_n(K)$ *for* $n \geq 9$, $\mathrm{E}_6(K)$, $\mathrm{E}_7(K)$, $\mathrm{E}_8(K)$, $\mathrm{F}_4(K)$, *where K is an algebraically closed field of odd or zero characteristic.*

The case where $\mathcal{D}$ is not connected is more difficult, since it is going to involve small groups like $\mathrm{PSL}_3(K)$.

1.2 Algebraic Groups

We do presuppose a basic knowledge of affine algebraic groups over an algebraically closed field. The standard reference is [42], where all necessary facts can be found easily.

In our context an algebraic group will always be the group of points over an algebraically closed field K of a linear algebraic group defined over K. If G is a semisimple algebraic group or connected sovable non-nilpotent algebraic group, then the field K can be interpreted in the *pure* group G by Zil'ber. In other cases (first of all, in the case of commutative groups) we usually have to postulate that the field K is definable in the universe $\mathcal{U}$.

Since we consider algebraic groups with a possibly richer structure inherited from the definable universe $\mathcal{U}$, we have two different concepts of "closed" subsets: "Zarisiki closed" and "definable". Therefore, if G is an algebraic group over a *definable* field K, Zariski closed subgroups are definable and the Zariski closure $\overline{H}$ of a subgroup $H < G$ contains the definable closure $d(H)$. If G is an algebraic group without extra structure, definable subsets are definable in G as a pure group and hence already Zariski closed.

We also have two versions of the connected component: the definable connected component and the Zariski closed identity component, the former being contained in the latter. Furthermore the Zariski closure of a definable connected group is Zariski connected. In most cases both do coincide though the proof usually requires some work. If we speak about connected algebraic groups in the following, we always mean Zariski connected groups.

Another important concept which transfers to groups of finite Morley rank is the concept of a Borel group. A subgroup $B \leq G$ of a group of finite Morley rank is called a *Borel subgroup* if it is maximal among the connected definable solvable subgroups of G. If G is an algebraic group over a definable field K and B a Borel subgroup in the sense of algebraic group theory, then B° is a Borel subgroup in the above sense. If on the other hand B is a Borel subgroup in the above sense, the Zariski closure $\overline{B}$ of B is a Borel subgroup in the sense of algebraic group theory by [42, 23.1]. Hence a Borel subgroup in the above sense has finite index in the Borel subgroup in the sense of algebraic group theory containing it.

Let furthermore G be any group. The group generated by all normal solvable subgroups $\sigma(G)$ is called the *solvable radical*. If G is a group of finite Morley rank, then $\sigma(G)$ is definable and solvable by [18, 7.3].

Proposition 1.6 *Let G be a K-group of finite Morley rank and B_1, B_2 be two Borel subgroups of G. Then B_1 and B_2 are conjugate.*

Proof. We may assume, that G is connected. The proposition holds if G is solvable. Let therefore G be nonsolvable and σ the solvable radical of G. Then $\sigma^\circ \leq B_n$ for $n = 1, 2$, as $\sigma^\circ B_n$ is a connected definable solvable subgroup of G. Set $\overline{X} := X\sigma/\sigma$ for all $X \leq G$. Then $\overline{G}$ is the direct product of finitely many simple algebraic groups A_i for $1 \leq i \leq m$ by [2]. Since σ is solvable, $H \leq G$ is solvable if and only if $\overline{H}$ is solvable. Hence $\overline{B}_n$ are definable connected solvable subgroups. Let $P_n \leq G$ such that $\overline{P}_n$ is a Borel subgroup containing $\overline{B}_n$ for $n = 1, 2$. Then P_n is a definable solvable subgroups containing B_n and $P_n^\circ = B_n$

for $n = 1, 2$. Especially $\overline{B}_n = \overline{P_n^\circ} = \overline{P}_n$ for $n = 1, 2$, as $\overline{P_n^\circ}$ is connected and $rk(\overline{P_n^\circ}) = rk(P_n^\circ) - rk(P_n^\circ \cap \sigma) = rk(P_n) - rk(\sigma) = rk(\overline{P}_n)$ by Lascar's equality. Thus $\overline{B}_n$ is a Borel subgroups of $\overline{G}$ for $n = 1, 2$. Consider the projections $\overline{B}_n^i$ of $\overline{B}_n$ onto A_i for $n = 1, 2$ and $1 \leq i \leq m$. By the above discussion $\overline{B}_n^i$ is the connected component of a Borel subgroup in the sense of algebraic group theory for all $n = 1, 2$ and $1 \leq i \leq m$. As Borel subgroups of connected algebraic groups are conjugate by [42, 21.3], there are $g_i \in A_i$ such that $(\overline{B}_1^i)^{g_i} = \overline{B}_2^i$ for $1 \leq i \leq m$. Therefore we can conclude that $(\overline{B}_1)^g = \overline{B}_2$ for $g := g_1 \cdots g_m$. Hence there exists $h \in G$, such that $B_1^h \leq B_2\sigma$. However $(B_2\sigma)^\circ = B_2$ and since B_1 is connected $B_1^h \leq B_2$. The claim follows since B_1 is maximal. □

Chapter 2 will be essentially devoted to an accurate treatment of algebraic implications of the existence of an extra structure on an algebraic group. The resulting technical complications seem to be unavoidable in work with K^*-groups of finite Morley rank, which explains the need for two different versions of the concept of an unipotent subgroup.

1.3 Chevalley Groups

All classical algebraic groups over a field K are *Chevalley groups*, i.e. they can be defined as the group of automorphism of a simple Lie algebra $\mathcal{L}_K$ over K. However, semisimple Lie algebras can be characterized by means of a *root system* by [41]. For the following compare [25] and [43].

Let V be a Euclidean space of dimension l. We denote by w_r the reflection in the hyperplane orthogonal to r. A finite subset Φ of non-zero vectors that spans V is called a *root system* in V, if it satisfies the following conditions: $w_r(s) \in \Phi$ and $2(r, s)/(r, r) \in \mathbb{Z}$ for all $r, s \in \Phi$ and additionally if $r, \lambda r \in \Phi$ for some $\lambda \in \mathbb{R}$, then $\lambda = \pm 1$. The elements of Φ are called *roots*. The *Weyl group* $W(\Phi)$ of Φ is the group generated by all reflections w_r for $r \in \Phi$.

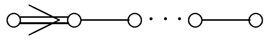
A subset Δ of Φ is called *fundamental system*, if it is linearly independent and every root in Φ is a linear combination of roots in Δ with coefficients which are either all non-negative or all non-positive. Fundamental systems always exist and their elements are called *simple roots*. The *rank* of a root system is the number of simple roots.

If $W := W(\Phi)$ is finite, we can characterize W by its *Dynkin diagram* Γ. The vertex set of Γ is the set of simple roots for some fixed fundamental system Δ. Let $m(\alpha, \beta) := o(w_\alpha w_\beta)$ for $\alpha \neq \beta$. Then $m(\alpha, \beta) \in \{2, 3, 4, 6\}$ and a pair of vertices $\alpha \neq \beta$ is joined by a single edge if $m(\alpha, \beta) = 2, 3$, by a double edge if $m(\alpha, \beta) = 4$ and a triple edge if $m(\alpha, \beta) = 6$. If Γ is connected, we call Φ *irreducible*. If Φ is irreducible at most two root lengths are possible and we label the graph by directing an arrow from long to short roots.

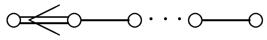
Fact 1.7 ([41]) *If Φ is an irreducible root system of rank n, its Dynkin diagram is one of the following:*

A_n, $n \geq 1$

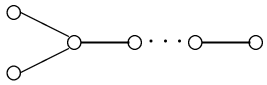
B_n, $n \geq 3$



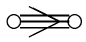
C_n, $n \geq 3$



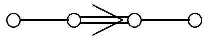
D_n, $n \geq 4$



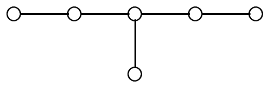
G_2



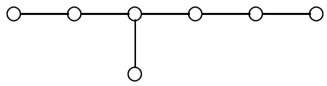
F_4



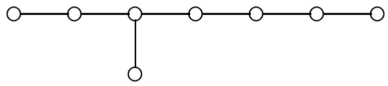
E_6



E_7



E_8



If we associate to every semisimple Lie algebra $\mathcal{L}$ a root system in the natural way, then two semisimple Lie algebras over the same field are isomorphic if and only if the corresponding Dynkin diagrams have the same type.

Fact 1.8 ([25]) *Let G be a Chevalley group over the Lie algebra $\mathcal{L}(K)$, where K is any field.*

(i) If $\mathcal{L}$ is of type A_n for $n \geq 1$, then G is isomorphic to $PSL_{n+1}(K)$.

(ii) If $\mathcal{L}$ is of type B_n for $n \geq 2$, then G is isomorphic to $P\Omega_{2n+1}(K, f)$, where f is the quadratic form $x_0^2 + x_1x_{-1} + \cdots x_nx_{-n}$.

(i) If $\mathcal{L}$ is of type C_n for $n \geq 3$, then G is isomorphic to $PSp_{2n}(K)$.

(ii) If $\mathcal{L}$ is of type D_n for $n \geq 4$, then G is isomorphic to $P\Omega_{2n}(K, f)$, where f is the quadratic form $x_1x_{-1} + \cdots x_nx_{-n}$.

Furthermore we can associate to every reductive algebraic group a Dynkin diagram, which is irreducible if G is simple. A *graph automorphism* of G is an automorphism of G which is induced by a nontrivial bijection on the Dynkin diagramm of G.

Fact 1.9 (see e.g. [37]) *Let G be a simple algebraic group that allows a nontrivial graph automorphism. Then G is of type A_n $(n \geq 2), D_n$ $(n \geq 4)$ or E_6. Furthermore $\Gamma \leq S_3$ if G is of type D_4 and $\Gamma \leq \mathbb{Z}_2$ in all other cases.*

Let Φ be a root system of rank n, Δ a fundamental system. The $\mathbb{Z}$-span P of Φ in V is called the *root lattice*. The root lattice is a free abelian group of rank n with basis Δ. Let Ξ be the group of K-characters of P for some field K. Then $\chi_{r,\lambda} \in \Xi$ for all $r \in \Phi$, $\lambda \in K^*$, where

$$\chi_{r,\lambda}(a) = \lambda^{2(r,a)/(r,r)} \text{ for all } r \in P.$$

Let $\mathcal{X}$ be the subgroup of Ξ generated by $\chi_{r,\lambda}$ for all $r \in \Phi$, $\lambda \in K^*$. If K is algebraically closed, then $\mathcal{X}$ is isomorphic to a maximal torus T of the corresponding Chevalley group G. Furthermore $W(\Phi) \cong N_G(T)/T$, the *Weyl group* of G. Thus statements about the action of the Weyl group of G on a maximal torus T can be translated into statements about characters of the root lattice and vice versa. One example is the following fact. Let $h : \mathcal{X} \longrightarrow \mathcal{T}$ be the isomorphism between $\mathcal{X}$ and T and $n : N_G(T) \longrightarrow W(\Phi)$ the homomorphism with kernel T, which induces the isomorphy between the two Weyl-groups.

Fact 1.10 ([25]) *Let $g \in N_G(T)$, $t \in T$, then $gtg^{-1} = h(\chi)$, where $\chi(r) = h^{-1}(t)(n(g)^{-1}(r))$ for all $r \in \Delta$.*

Let finally $H_r \leq T$ the subgroup of T generated by $h(\chi_{r,\lambda})$, $\lambda \in K^*$. One can associate, in a unique way, two one-dimensional unipotent subgroup X_r and X_{-r} of G with H_r such that $P := \langle X_r, X_{-r}\rangle \geq H_r$ and P is either isomorphic to $SL_2(K)$ or to $PSL_2(K)$. Furthermore H_r normalizes X_r and X_{-r} and there exists an element $g \in P$ such that $n(g) = w_r$. We call X_r and X_{-r} *root subgroups* of G.

1.4 Finite Groups of Lie type

The key to the study of finite groups of Lie type is that they are the fixed points of a special endomorphism, a *Frobenius map*, where G is a connected reductive algebraic group. A thorough discussion of this concept can be found in [27].

Let G be a linear algebraic group over an algebraically closed field of characteristic p. A homomorphism $F : G \longrightarrow G$ is called a *standard Frobenius map*, if there exists an injective homomorphism $i : G \longrightarrow GL(n, K)$ for some $n \in \mathbb{N}$, such that $i(F(G)) = F_q(i(g))$ for some $q = p^e$ and all $g \in G$ where $F_q(a_{ij}) = (a_{ij}^q)$. A homomorphism $F : G \longrightarrow G$ is called a *Frobenius map* if some power of F is a standard Frobenius map.

Notice that a Frobenius map is a surjective homomorphism of algebraic groups and that the set of fixed points G^F is a finite subgroup of G. Especially (G, F) is a σ-setup in the sense of Steinberg [52]. The basis of the theory is the following proposition:

Fact 1.11 ([52]) *Let G be a connected algebraic group and σ an endomorphism from G onto G with finitely many fixed points. Then the map $g \longrightarrow g^{-1}\sigma(g)$ is surjective.*

This setup allows us to deduce properties of finite groups of Lie type from analogous properties of algebraic groups. One of the key tools is the following Fact. Let A be a group on which F acts. $H^1(F, A)$ denotes A modulo the equivalence relation $\equiv$, where $a \equiv b$ iff $a = cbF(c)^{-1}$ for some $c \in A$. If $a, b \in A$ are equivalent we say that they are *F-conjugate*.

Fact 1.12 ([52]) *Let G be a connected linear algebraic group, F a Frobenius map, and M be a nonempty set, on which G and F act. If G permutes the elements of M transitively and $F(gm) = F(g)F(m)$ for all $g \in G$, $m \in M$, then M contains a point m fixed by F. If $A := C_G(m)$ is a Zariski-closed subgroup of G then G^F has $|H^1(F, A)|$ orbits on M^F. Furthermore $|H^1(F, A)| = |H^1(F, A/A^\circ)|$.*

If we apply this proposition to the set M of maximal tori of G, then we get the following result.

Corollary 1.13 *Let G be a connected reductive group and F a Frobenius map. G contains a maximal torus T fixed by F. There are $|H^1(F, W)|$ classes of maximal tori fixed by F under conjugation by G^F where $W = N_G(T)/T$ is the Weyl-group of G.*

Note that $T^{g^{-1}}$ is fixed by F iff $g^{-1}F(g) \in N_G(T)$. In this case we say that $(T^{g^{-1}})^F$ is a *maximal torus of* G^F *twisted by* $w := g^{-1}F(g)T \in W$.

To get hold of the intersection of tori we need the following definition. Let G be a connected reductive group with Frobenius map F and let T be an F-stable maximal torus of G. Then T is called *non-degenerate* if T is the only maximal torus of G containing T^F. This is equivalent to $T = C_G(T^F)^\circ$. If a maximal torus T is non-degenerate, we have good control over the Weyl-group of T^F, especially $(N_G(T))^F = N_{G^F}(T^F)$ and $N_G(T)^F/T^F \cong (N_G(T)/T)^F$ in this case.

For our purposes it is enough to consider the case, where G is a Chevalley group. Since F fixes every elements of the Weyl-group in this case, $H^1(F, W)$ corresponds to the conjugacy classes of W and we get the following order estimates.

Fact 1.14 ([52]) *Let G be a Chevalley group and F a standard Frobenius map. Let T be a maximal split torus, $w \in W = N_G(T)/T$ and T_w a maximal torus twisted by w. If q is the number of elements of the base field of G^F, then the characteristic polynomial of w evaluated at q gives the order of $(T_w)^F$. Furthermore $|N_G(T_w)^F/(T_w)^F| = |C_W(w)|$*

The characteristic polynomials of elements in the Weyl-group of Chevalley groups are given in [25]. We have thus a complete description of the orders of maximal tori in Chevalley groups.

1.5 Probabilistic Algorithms

The last decades of computations have seen several shortcomings of deterministic algorithms and have replaced them in many cases by *randomized algorithms*, i.e. algorithms which use random numbers. A further step is not only to consider algorithms which depend on random choices of elements of a certain sample but furthermore to consider algorithms where the outcome is only correct with a certain probability. The most famous application of these kinds of algorithms are primality testing algorithms.

Example (Strong Primality Test): Let n be any odd number. We want to know if n is prime.

- Take any base b where $1 \leq b < n$ is a natural number and test if $b^{n-1} = 1 \mod n$. If it is not, then n cannot be prime.
- Otherwise factor $n - 1 = 2^k m$, where m is odd.

- Consider the sequence $b^m, (b^m)^2, \cdots (b^m)^{2^k}$. If the sequence does not contain -1, then n cannot be prime. Otherwise b passes the test.

One can show that if n is not prime at least 1/2 of the bases fails the test [24]. Hence if we chose k bases randomly and all of them pass the test, then n is a prime number with probability greater than $1 - (\frac{1}{2})^k$.

The strong primality test is a so called *one-sided Monte-Carlo algorithm.* A *Monte Carlo algorithm* A is a randomized algorithm, where the result is only correct with a probability $1 - \epsilon$, where $0 \leq \epsilon < 1/2$. Assume that A has only *yes* and *no* as possible results. Then A is called *one-sided*, if the result *yes* is always correct. A *Las Vegas algorithm* is a randomized algorithm, which gives a result with probability $1-\epsilon$, where $0 \leq \epsilon < 1/2$. Here the result has to be always correct.

Let g be a function from $\mathbb{N}$ onto $\mathbb{R}^{+,0}$. The *Landau symbol* $O(g)$ is defined as

$$O(g) := \{f : \mathbb{N} \longrightarrow \mathbb{R}^{+,0} \,|\, \exists n_0 \in \mathbb{N},\ c > 0\ \forall n \geq n_0 : \quad 0 \leq f(n) \leq cg(n)\}.$$

Furthermore we say that an algorithm A with entries in E has complexity $O(f)$, if there exists $g \in O(f)$ such that the running time is bounded by $g(k(e))$ for all $e \in E$, where $k : E \longrightarrow \mathbb{N} \times \cdots \times \mathbb{N}$ measures the length of the input.

1.6 Black box groups

Black box groups were introduced by Babai and Szemerédi [9] as the ideal setting for some group computational problems and their importance has grown ever since. For the following compare [11] and [13].

A *black box group* G is a finite group whose elements are encoded as 0-1 strings of uniform length N, and the group operations are performed by an oracle (the "black box"). Moreover, a list of generators of the group is given in this encoding. Given strings representing $g, h \in G$, the black box can compute strings representing gh and g^{-1}, and decide whether $g = h$ at unit cost. We assume that not all strings need to correspond to group elements and that the encoding need not be unique.

Note that the upper bound on $|G|$ is 2^N. Furthermore, if we know the generating elements of a subgroup H, H is again a black box group with these generators. If moreover H is normal and *recognizable*, then G/H is a black box group as well with the same generators as G and all elements of H corresponding to the identity element. A subgroup H of a black box group G is said to be *recognizable*, if there exists a polynomial time algorithm which can decide if an element g of G is contained in H.

The classical examples of black box groups are permutation groups and matrix groups over finite fields. If G is a permutation group on n letters for some $n \in \mathbb{N}$, then any element can be encoded by at most $n \log(n)$ bits, and if $G \leq \mathrm{GL}_n(q)$ for $n \in \mathbb{N}$ and q any prime power, then elements can be encoded by strings of length $n^2 \log q$.

Sometimes it is necessary to strengthen the assumptions. A *grey box group* is a black box group with an additional oracle. Classically, a grey box group possesses an oracle that gives element orders or does linear algebra in case that the black box group is a matrix group.

The main question is, how much information about G can actually be gained in polynomial time. Can we for example, given the promise that G is a simple group and the name of a finite simple group A, decide if G is isomorphic to A?

There is a large joined effort to solve this and related questions. The most prominent results are by L. Babai, W. Kantor, P. Palfy and A. Seress. If G is a classical group, then the problem has been solved in [46]. Their algorithm even gives a presentation of the black box group G in question. The draw-back is, that their algorithm takes time polynomial in q. However, there are polynomial time algorithms as well.

Fact 1.15 ([47] and [12]) *Let G be a grey box group with order oracle isomorphic to a simple group of Lie type whose elements are encoded as strings of length N. Then there exists a Monte-Carlo algorithm which determines in time polynomial in N*

- *the size of the underlying field, the dimension and the type of the group, if G is known to be classical.*

- *the isomorphism type of the group, if the size of the underlying field is known.*

Both algorithms mentioned in Fact 1.15 rely on the result that finite simple groups of type B_n and C_n can be distinguished, which we will prove in Section 6.

As most group-theoretic algorithms for larger groups, many black box algorithms assume that they have random elements available, either from the uniform distribution or, as this is hardly feasible, at least from the *near uniform* distribution. A probability distribution over the finite set G is *ϵ-uniform* , if the probability of any particular element being selected is $(1 \pm \epsilon)/|G|$. The distribution is *near uniform*, if it is uniform for some $0 < \epsilon < 1$.

Fact 1.16 ([10]) *Let c and C be positive constants, and let $\epsilon = M^{-c}$. If G is a black box group of order at most M, then there is a Monte Carlo algorithm which constructs ϵ-uniformly distributed, independent random elements of G at a cost of $O(\log^5 M)$ group operations. The algorithm fails with probability $\leq M^{-C}$. If the algorithm succeeds, the cost for the construction of a single element after the initial preprocessing is $O(\log M)$.*

In practice, the algorithm from [29] is most widely used, since it is much faster. The theoretical analysis of this algorithm, however, is still missing and seems extremely difficult to achieve.

Part I

Groups of Finite Morley Rank

Chapter 2

Quasiunipotent Groups

One of the problems one encounters in the classification of simple tame K^*-groups is that one does not know how to generalize the concept of a unipotent subgroup of an algebraic group to groups of finite Morley rank. If all the proper simple sections of the group are algebraic groups over an algebraically closed field of characteristic p one can use p-groups. However, the algebraic groups that appear as simple sections could have characteristic 0 or they could even have different characteristics. Hence A. Berkman has introduced the concept of a quasiunipotent group and proved some basic results about them. To proceed further it became necessary to consider the more subtle notion of a pseudounipotent group as well. Both concepts capture some of the essential meaning of "unipotent". A. Berkman's work together with the results of this section have already been published in [7].

2.1 Basic properties

Let G be a group of finite Morley rank. An abelian divisible p-subgroup of G is called *p-torus*. A definable connected nilpotent subgroup $U \leq G$ is called *quasiunipotent* if U does not contain a p-torus for any prime number p. A definable connected nilpotent subgroup $H \leq G$ is called *pseudounipotent* (in G) if it satisfies the following condition: If $K \leq H$ is a definable connected subgroup of H which normalises a definable connected nilpotent subgroup $N \leq G$ then the product NK is nilpotent.

We will normally fix the group G; the word "pseudounipotent" in the subsequent text means "pseudounipotent in G".

Lemma 2.1 *Let G be a connected algebraic group over an algebraically closed* *field. Let U be a definable connected unipotent subgroup of G. Then U is quasiunipotent and pseudounipotent.*

Proof. Let U be a definable connected unipotent subgroup of G. Then U is nilpotent and since it does not contain a p-torus for any prime p, U is quasiunipotent.

Let $V \leq U$ be a definable connected subgroup of U and $N \leq G$ a connected definable nilpotent subgroup of G that is normalized by V. We show that VN is nilpotent. VN is a solvable connected group and the Zariski closure $\overline{VN}$ is thus a Zariski connected solvable algebraic group. Furthermore since the Zariski closure $\overline{N}$ of N is a Zariski connected and nilpotent algebraic group, $\overline{N} = W \times T$ is the direct product of its semisimple part T and its unipotent part W by [42, 19.2]. $\overline{VN}$ has, as a Zariski connected solvable algebraic group, a maximal normal unipotent subgroup H by [42, 19.3] which contains all unipotent elements. Thus $VW \leq H$ and as H is Zariski closed, already $\overline{V}W \leq H$. This implies that $\overline{VN} = \overline{V}(W \times T) = (\overline{V}W) \times T$ is nilpotent. Hence U is pseudounipotent in G. □

Fact 2.2 (Berkman [7]) *If G is a connected algebraic group that does not interpret any bad field then quasiunipotent subgroups of G are unipotent.*

In Corollary 2.14 we will furthermore prove that if G is a connected semisimple algebraic group that does not interpret a bad field, then pseudounipotent subgroups of G are unipotent.

Lemma 2.3 *Let G be a group of finite Morley rank, $H \leq G$ a definable subgroup of G and φ a definable automorphism of G.*

(i) A definable connected subgroup of a quasiunipotent subgroup of G is also quasiunipotent.

(ii) H is quasiunipotent if and only if $\varphi(H)$ is quasiunipotent.

(iii) If H is quasiunipotent it can be written as $H = B \times D$, where B and D are definable, B is of bounded exponent and D is torsion-free.

(iv) A definable connected subgroup of a pseudounipotent subgroup of G is also pseudounipotent.

(v) H is pseudounipotent if and only if $\varphi(H)$ is pseudounipotent.

(vi) If G is connected and nilpotent, then G is pseudounipotent.

(vii) *If H is pseudounipotent in G, then H is pseudounipotent in any definable subgroup K of G that contains H.*

Proof. (iii) follows by [18, 6.12], the rest is clear from the definitions. □

Fact 2.4 (Berkman [7]) *Let G be a group of finite Morley rank. Let U, V be definable subgroups of G and $N \lhd U$ a definable normal subgroup of U.*

(i) *If U is quasiunipotent, then U/N is also quasiunipotent.*

(ii) *If U/N and N are quasiunipotent and if U does not interpret a bad field, then U is quasiunipotent.*

(iii) *Assume that U and V are quasiunipotent and that U normalizes V. If UV does not interpret a bad field, then UV is quasiunipotent.*

To study pseudounipotent groups we need criteria for nilpotency.

Fact 2.5 ([38]) *Let G be any group. $H, K \leq G$ subgroups, such that $H \lhd K$. If H and K/H' are nilpotent, then K is nilpotent as well.*

Lemma 2.6 *Let G be a connected solvable group of finite Morley rank and $H \leq G$ a definable connected subgroup. Then the following are equivalent*

(i) *H is pseudounipotent*

(ii) *HG^n/G^n is pseudounipotent for all $n \geq 2$.*

(iii) *HG^n/G^n is pseudounipotent for some $n \geq 2$.*

Proof. $(iii) \to (i)$: Assume that $\overline{H} := HG^n/G^n$ is pseudounipotent for some $n \in \mathbb{N}$, $n \geq 2$ and let $K \leq H$ be a definable connected subgroup which normalises a definable connected nilpotent subgroup $N \leq G$. We have to show that NK is nilpotent. Let $\overline{K} := KG^n/G^n$ and $\overline{N} := NG^n/G^n$. Then $\overline{K}$ is a definable connected subgroup of $\overline{H}$ which normalises the definable connected nilpotent group $\overline{N}$. Since $\overline{H}$ is pseudounipotent $\overline{NK}$ is nilpotent. However G^{n-1} is nilpotent by [18, 9.9]. Thus NKG^n is nilpotent by Fact 2.5 and NK is nilpotent as well.

$(i) \to (ii)$: Let H be pseudounipotent and $n \in \mathbb{N}$, $n \geq 2$. Let furthermore $\overline{K}$ be a definable connected subgroup of $\overline{H} = HG^n/G^n$ which normalises the definable connected nilpotent group $\overline{N}$. We have to show that $\overline{NK}$ is nilpotent. Let K, N be the subgroups of G containing G^n such that $K/G^n = \overline{K}$ and $N/G^n = \overline{N}$. Set $K_1 := (K \cap H)^\circ$. Then $K = K \cap HG_n = (K \cap H)G_n \geq K_1G^n$. As

K is connected and K and $K_1 G^n$ have the same rank, already $K = K_1 G^n$. Furthermore K and N are connected groups since G^n is connected. They are nilpotent by Fact 2.5 since G^{n-1} is nilpotent by [18, 9.9]. As K normalises N, $K_1 \leq H$ normalises N as well and NK_1 is nilpotent by assumption. Hence $NK_1G^n/G^n = NK/G^n = \overline{NK}$ is nilpotent as well. □

Corollary 2.7 *Let G be a solvable connected group of finite Morley rank and $H \leq G$ a pseudounipotent subgroup. Then HG^n is pseudounipotent for all $n \geq 2$.*

Proof. Let $n \in \mathbb{N}$, $n \geq 2$. As H is pseudounipotent, HG^n/G^n is pseudounipotent by Lemma 2.6. Thus HG^n is pseudounipotent as well by Lemma 2.6 again, as G^n is connected by [18, 5.29]. □

Lemma 2.8 *Let G be any group, $H \leq G$ a subgroup. Then the following are equivalent:*

(i) H is nilpotent.

(ii) $HZ_m(G)/Z_m(G)$ is nilpotent for all $m \in \mathbb{N}$.

(iii) $HZ_m(G)/Z_m(G)$ is nilpotent for some $m \in \mathbb{N}$.

Thus $HZ_m(G)$ is nilpotent for all $m \in \mathbb{N}$ if H is nilpotent.

We give a short proof for this easy fact in lack of a suitable reference.

Proof. First note that (i) implies (ii) and that (ii) implies (iii). Hence it is only left to show that (iii) implies (i). We consider first the case where $H = G$. Let $m \in \mathbb{N}$ and $\overline{X} := XZ_m(H)/Z_m(H)$ for all $X \leq G$. Then

$$(*) \qquad H/Z_{m+n}(H) \cong \overline{H}/Z_n(\overline{H})$$

and

$$(**) \qquad Z_{m+n+1}(H)/Z_{m+n}(H) \cong Z_{n+1}(\overline{H})/Z_n(\overline{H})$$

for all $n \in \mathbb{N}$. We prove $(*)$ and $(**)$ by simultaneous induction on n. $(*)$ and $(**)$ are true for $n = 0$ since $Z_0(H) = 1$. For the induction step notice that

$$H/Z_{m+n+1}(H) \cong \big(H/Z_{m+n}(H)\big)/\big(Z_{m+n+1}(H)/Z_{m+n}(H)\big)$$

and hence by induction hypothesis

$$H/Z_{m+n+1}(H) \cong \big(\overline{H}/Z_n(\overline{H})\big)/\big(Z_{n+1}(\overline{H})/Z_n(\overline{H})\big) \cong \overline{H}/Z_{n+1}(\overline{H})$$

proving $(*)$. Especially

$$Z\big(H/Z_{m+n+1}(H)\big) \cong Z\big(\overline{H}/Z_{n+1}(\overline{H})\big) = Z_{n+2}(\overline{H})/Z_{n+1}(\overline{H})$$

and $(**)$ follows. Assume now that $\overline{H}$ is nilpotent. Then there exists $n \in \mathbb{N}$ such that $\overline{H} = Z_n(\overline{H})$. However this implies that $H = Z_{m+n}(H)$ by $(*)$ and H is nilpotent as well.

Let finally $H < G$ and assume that $HZ_m(G)/Z_m(G)$ is nilpotent for some $m \in \omega$. Since again by induction

$$\begin{aligned} Z_{n+1}(G) \cap H &= \big\{x \in H : [G,x] \leq Z_n(G)\big\} \\ &\leq \big\{x \in H : [H,x] \leq Z_n(G) \cap H\big\} \\ &\leq \big\{x \in H : [H,x] \leq H\big\} \\ &= Z_{n+1}(H) \end{aligned}$$

for all $n \in \mathbb{N}$,

$$\big(H/Z_m(G) \cap H\big)/\big(Z_m(H)/Z_m(G) \cap H\big) \cong H/Z_m(H)$$

is nilpotent and the claim follows. □

Lemma 2.9 *Let G be a group of finite Morley rank and H a connected definable subgroup. Then the following are equivalent*

(i) H is pseudounipotent

(ii) $HZ_n(G)/Z_n(G)$ is pseudounipotent for all $n \geq 2$.

(iii) $HZ_n(G)/Z_n(G)$ is pseudounipotent for some $n \geq 2$.

Proof. Similar to the proof of Lemma 2.6 using Lemma 2.8 instead of Fact 2.5. In proving $(i) \to (ii)$ we have to use the connected component of $Z_n(G)$, since $Z_n(G)$ need not be connected. The result then follows by rank considerations. □

Corollary 2.10 *Let G be a group of finite Morley rank and $H \leq G$ a pseudounipotent subgroup. Then $HZ_n(G)^\circ$ is pseudounipotent for all $n \in \mathbb{N}$. Especially $Z_n(G)^\circ$ is pseudounipotent for all $n \in \mathbb{N}$.*

Proof. Let $n \in \mathbb{N}$, $n \geq 2$. As H is pseudounipotent, $HZ_n(G)/Z_n(G)$ is pseudounipotent by Lemma 2.9. Thus $HZ_n(G)^\circ$ is pseudounipotent as well by Lemma 2.9 again. □

2.2 Maximal quasiunipotent groups

If B is a connected solvable algebraic group, the set of unipotent elements forms a maximal unipotent group and is characteristic in B. We are going to show that the analogue property holds for groups of finite Morley rank. We prove that a solvable group G of finite Morley rank contains a unique maximal quasiunipotent (pseudounipotent) subgroup $Q(G)$ respectively $P(G)$. Furthermore $Q(G)$ and $P(Q)$ are characteristic subgroups of G and $Q(G) \leq P(Q)$.

We call a quasiunipotent (pseudounipotent) subgroup U of a group G of finite Morley rank *maximal quasiunipotent (maximal pseudounipotent)*,if $U = V$ for all quasiunipotent (pseudounipotent) subgroups $U \leq V$ of G. Note that maximal quasiunipotent and maximal pseudounipotent subgroups exist by ascending chain condition on connected subgroups.

Proposition 2.11 *Let G be a group of finite Morley rank which does not interpret a bad field and $U \leq G$ a quasiunipotent subgroup. Then U is pseudounipotent.*

Proof. Let $U \leq G$ be a quasiunipotent subgroup of G and let $V \leq U$ be a definable connected subgroup that normalises the definable connected nilpotent subgroup $N \leq G$. VN is a connected solvable group. We show that VN is nilpotent. Set $F := F(VN)$. VN/F° is a divisible abelian group by [18, 9.21] and since $N \leq F^\circ$, $VN = VF^\circ$. As V is quasiunipotent it can be written as $V = B \times D$ where B and D are definable, B is of bounded exponent and D is torsion-free by Lemma 2.3. Thus $VN/F^\circ = VF^\circ/F^\circ \cong BD/(F^\circ \cap BD)$ is a divisible group and $B \leq F^\circ$. This implies that $VN = DF^\circ$.

Consider $\overline{VN} := VN/Z_m(VN)$, where $Z_m(VN)$ is the hyper-center of VN. Then $Z(\overline{VN}) = 1$ and $\overline{VN} = \overline{DF}^\circ$, where $\overline{D}$ is quasiunipotent by Fact 2.4. Furthermore $F(\overline{VN})$ is the direct product of a connected definable subgroup C of bounded exponent and a definable connected torsion-free subgroup T by [18, ex.3, p.148]. Thus $\overline{F}^\circ \leq F(\overline{VN})$ is quasiunipotent as well. Since G does not interpret a bad field, $\overline{VN}$ is quasiunipotent by Fact 2.4 and hence nilpotent. Thus VN is nilpotent by Lemma 2.8. □

Let G be a group of finite Morley rank. We call

$$Q(G) = \langle U \mid U \lhd G,\ U \text{ is quasiunipotent } \rangle$$

the *quasiunipotent radical of G* and

$$P(G) = \langle H \mid H \lhd G,\ H \text{ is pseudounipotent } \rangle$$

the *pseudounipotent radical of G* .

Lemma 2.12 *Let G be a group of finite Morley rank.*

(i) $Q(G)$ and $P(Q)$ are nilpotent groups.

(ii) $Q(G) = U_1 \cdots U_n$ and $P(G) = H_1 \cdots H_m$ are the products of finitely many normal quasiunipotent respectively pseudounipotent subgroups.

If G does not interpret a bad field then

(ii) $Q(G)$ is quasiunipotent,

(iii) $Q(G) \lhd P(G)$.

Proof. As $Q(G), P(G) \leq F(G)$, they are nilpotent by [18, 7.3]. They are products of finitely many normal quasiunipotent respectively pseudounipotent subgroups by Zil'bers indecomposability theorem [18, 5.28]. If finally G does not interpret a bad field, $Q(G)$ is quasiunipotent by Fact 2.4 and $Q(G) \lhd P(G)$ by Proposition 2.11. □

It is not known if $P(G)$ is pseudounipotent for every group of finite Morley rank.

Proposition 2.13 *Let G be a solvable group of finite Morley rank that does not interpret a bad field. Then $F(G)^\circ$ is the unique maximal pseudounipotent subgroup of G. Especially $P(G) = F(G)^\circ$ is pseudounipotent.*

Proof. We can take G to be connected, since all pseudounipotent groups are connected. The proof proceeds by induction on the solvable length of G. The claim is trivial if G is nilpotent. Let G be 2-step solvable and non-nilpotent. Consider $\overline{G} := G/Z_m(G)$ where $Z_m(G)$ is the hyper-center of G. Then $\overline{G}$ is a 2-step solvable connected centerless group of finite Morley rank. Furthermore $F(\overline{G})^\circ$ is a pseudounipotent subgroup of G by [18, ex.3, p.148] and Proposition 2.11. Since $\overline{G}' \leq F(\overline{G})^\circ$ by [18, 9.9], every subgroup of $\overline{G}$ which contains $F(\overline{G})^\circ$ is normal in G. Especially every maximal pseudounipotent subgroup of G containing $F(\overline{G})^\circ$ is equal to $F(\overline{G})^\circ$ and $F(\overline{G})^\circ$ is a maximal pseudounipotent group.

Let $K \leq \overline{G}$ be a pseudounipotent group. Since K normalises $F(\overline{G})^\circ$, $KF(\overline{G})^\circ$ is nilpotent and normal in $\overline{G}$. Hence $KF(\overline{G})^\circ \leq F(\overline{G})^\circ$ and $K \leq F(\overline{G})^\circ$. Thus $F(\overline{G})^\circ$ is the unique maximal pseudounipotent subgroup of $\overline{G}$. Since by Lemma 2.8 $\overline{F(G)} = F(\overline{G})$, Lemma 2.9 implies that $F(G)^\circ$ is the unique maximal pseudounipotent subgroup of G.

Let G be n-step solvable with $n \geq 3$. By induction $F(G/G^{n-1})^\circ$ is the unique maximal pseudounipotent subgroup of G/G^{n-1}. Let $H \leq G$ be such that $H/G^{n-1} = F(G/G^{n-1})^\circ$. Then $H = F(G)^\circ$ by Fact 2.5 since $G^{n-2} \leq G'$ is nilpotent by [18, 9.9]. $F(G)^\circ$ is thus the unique maximal pseudounipotent subgroup of G by Lemma 2.6. □

Corollary 2.14 *Let G be a connected algebraic group that does not interpret a bad field. The maximal pseudounipotent subgroups of G are $Z(G)^\circ U^\circ$, where U is the unipotent radical of a Borel subgroup. Thus, if G is semisimple, pseudounipotent and definable connected unipotent subgroups coincide.*

Proof. Let H be a maximal pseudounipotent subgroup of G and B a Borel subgroup of G in the sense of algebraic group theory containing H. Then $B = U \rtimes T$ by [42, 19.3], where U is the unipotent radical of B and T is a maximal torus. Thus $H \leq P(B)$ by Proposition 2.13. As on the other hand U° is pseudounipotent by Lemma 2.1 and Proposition 2.11, $U^\circ \leq P(B)$ as well. Since the Zariski closure $\overline{P(B)}$ of $P(B)$ is a Zariski connected nilpotent closed subgroup of B, it is the direct product of its unipotent part $U = \overline{U}^\circ$ and a semisimple part T_1. As $T_1 \leq C_B(U) = Z(B)$ and $Z(G) = Z(B)$ by [42, 22.2], $H \leq P(B) \leq UZ(G)$. However, $Z(G)^\circ U^\circ$ is pseudounipotent by Corollary 2.10, i.e. $H = Z(G)^\circ U^\circ$ by maximality of H. □

Lemma 2.15 *Let G be a nilpotent group of finite Morley rank that does not interpret a bad field. Then $Q(G)$ is the unique maximal quasiunipotent subgroup of G.*

Proof. We can take G to be connected since all quasiunipotent groups are connected. First assume that G is divisible. We prove the claim by induction on the solvable length of G. If G is abelian, then every quasiunipotent subgroup of G is normal in G and the claim follows by Lemma 2.12.

Assume that G is not abelian. G' is connected and torsionfree by [18, exc 5., p.102]. Hence G' is quasiunipotent. Furthermore $Q(G/G')$ is the unique maximal quasiunipotent subgroup of G/G' by induction hypothesis. Let $G' \leq H \leq G$ such that $H/G' = Q(G/G')$. Then H is a maximal quasiunipotent group by Fact 2.4, i.e. $H = Q(G)$.

Let finally G be a not necessarily divisible connected nilpotent group of finite Morley rank. Then $G = D{*}C$ where D is a definable connected characteristic and divisible subgroup of G and C is a definable connected characteristic subgroup of G of bounded exponent by [18, 6.8]. C is quasiunipotent. Hence $Q(G) = Q(D){*}C$ is the unique maximal quasiunipotent subgroup of G. □

Proposition 2.16 *Let G be a solvable group of finite Morley rank that does not interpret a bad field. Then $Q(G)$ is the unique maximal quasiunipotent subgroup of G.*

Proof. Let U be a maximal quasiunipotent subgroup of G. Then U is pseudounipotent by Proposition 2.11 and hence $U \leq P(G)$ by Proposition 2.13. However, as $P(G)$ is nilpotent by Proposition 2.13, it contains the unique maximal quasiunipotent subgroup $Q(P(G))$ by Lemma 2.15. Thus $U = Q(P(G))$ by maximality of U. Especially $Q(P(G)) = Q(G)$ is the unique maximal quasiunipotent subgroup of G. □

Corollary 2.17 *Let G be a K-group of finite Morley rank that does not interpret a bad field. If U_1, U_2 are two maximal quasiunipotent subgroups of G, then U_1 and U_2 are conjugate.*

Proof. Since U_1, U_2 are nilpotent, they are contained in Borel subgroups B_1 and B_2 of G respectively. Furthermore $U_n = Q(B_n)$ are characteristic subgroups of B_n for $n = 1, 2$ by Proposition 2.16. Since B_1 and B_2 are conjugate by Proposition 1.6, $Q(B_1) = U_1$ and $Q(B_2) = U_2$ are conjugate as well. □

2.3 Normalizers of quasiunipotent groups

The normalizer of a maximal unipotent subgroup U of a connected algebraic group G is $U \rtimes T$ for an algebraic torus T by [42, 19.3, 23.1, 30.4]. We are going to show that a similar result is valid for normalizers of maximal quasiunipotent subgroups in groups of finite Morley rank under the special assumptions that we will need in Chapter 4.

Proposition 2.18 *Let G be a simple K^*-group of finite Morley rank that does not interpret a bad field. Let T be a definable connected solvable subgroup. If Q is a nontrivial quasiunipotent subgroup of G that is normalised by T then there exists a maximal quasiunipotent subgroup $Q \geq V$ of G such that V is normalized by T.*

Proof. Let $1 \neq Q$ be a quasiunipotent subgroup of G that is normalized by T. Then QT is a definable connected solvable subgroup of $N_G(Q)$. Let B be a Borel subgroup of $N_G(Q)$ that contains QT. Then $Q(B)$ is the unique maximal quasiunipotent subgroup of B by Proposition 2.16 and $Q \leq Q(B) \lhd B$. Especially $Q(B)$ is normalized by T. Furthermore, as $N_G(Q)$ is a K-group, the Borel subgroups are conjugate by Proposition 1.6 and $Q(B)$ is a maximal quasiunipotent subgroup of $N_G(Q)$. Let $U \geq Q(B)$ be a maximal quasiunipotent subgroup of G. As U is nilpotent and connected either $U = Q$ or $N_U(Q)/Q$ is infinite by [18, 6.3]. As $N_U(Q) = Q(B)$, either Q is a maximal quasiunipotent subgroup of G, or there exists a quasiunipotent subgroup $Q(B)$ of $N_G(Q)$ which is strictly greater than Q

and normalized by T. We can now repeat our argument with $Q(B)$ instead of Q. After finitely many steps we arrive at a maximal quasiunipotent group V of G which is normalized by T by ascending chain condition on connected subgroups. □

Lemma 2.19 *Let G be an algebraic group that does not interpret a bad field. Let $H \leq G$ be a definable subgroup and $U \leq H$ a maximal quasiunipotent subgroup of H. Then $N_H(U)^\circ$ is solvable.*

Notice that if H is Zariski closed, Lemma 2.19 is an easy corollary of Lemma 2.2 and [43, 23.1 and 30.4].

Proof. Set $N := N_H(U)^\circ$. Assume that N is not solvable. Let σ be the solvable radical of N and $V \leq N$ a subgroup of N such that V/σ is a maximal quasiunipotent subgroup of N/σ. As N/σ is the direct sum of simple algebraic groups over algebraically closed fields by [2], V/σ is infinite. Furthermore V° is a connected solvable group with maximal quasiunipotent subgroup U by Proposition 2.16 as $U \leq \sigma$. Let $\overline{V}$ be the Zariski closure of V°. $\overline{V}$ is a Zariski connected solvable group. Let W be the unipotent radical of $\overline{V}$. Then $\overline{V} = W \rtimes T$ for some algebraic torus $T \leq \overline{V}$ by [42, 19.3]. Thus

$$T \cong \overline{V}/W \geq V^\circ W/W \cong V^\circ/(V^\circ \cap W)$$

As $(V^\circ \cap W)^\circ$ is quasiunipotent by Lemma 2.1 and $U \leq V^\circ \cap W$, $U = (V^\circ \cap W)^\circ$ by maximality of U. Thus $(V^\circ \cap W)/U$ is finite and

$$T \cong V^\circ/(V^\circ \cap W) \cong \big(V^\circ/U\big)/\big((V^\circ \cap W)/U\big).$$

As T is abelian, $[V^\circ/U, V^\circ/U] \leq (V^\circ \cap W)/U$. Since furthermore the commutator of a connected group is connected by [18, 5.29], V°/U is a connected abelian group. Especially V°/U is divisible by [18, 6.7], as T is divisible. Thus

$$V/\sigma = V^\circ\sigma/\sigma \cong V^\circ/(\sigma \cap V^\circ) \cong \big(V^\circ/U\big)/\big((\sigma \cap V^\circ)/U\big)$$

is a divisible quasiunipotent group and hence torsion-free by Lemma 2.3. Set $X := (V^\circ \cap \sigma)(V^\circ \cap W)$. Then $X \lhd V^\circ$ and

$$V^\circ/X \cong \big(V^\circ/(V^\circ \cap \sigma)\big)/\big(X/(V^\circ \cap \sigma)\big)$$

is torsion-free by [18, ex. 11, p. 93]. However,

$$V^\circ/X \cong \big(V^\circ/(V^\circ \cap W)\big)/\big(X/(V^\circ \cap W)\big)$$

is isomorphic to a connected definable section of the algebraic torus T. As G does not interpret a bad field, $V^\circ/X = 1$ and $V^\circ = X$. Especially

$$V^\circ\sigma/\sigma \cong V^\circ/(V^\circ \cap \sigma) \cong (V^\circ \cap W)/(V^\circ \cap W \cap \sigma)$$

is finite as $U \leq V^\circ \cap W \cap \sigma$. Contradiction. □

Let G be any group. $D \leq G$ is called *four-subgroup*, if D is an elementary abelian subgroup of order 4. We let $D^* := D\backslash\{1\}$ denote the set of involutions in D.

Proposition 2.20 *Let G be a K^*-group of finite Morley rank and odd type that does not interpret a bad field and V a maximal quasiunipotent group of G. Assume that V is normalized by a four-subgroup D such that $C_G(l)^\circ$ for all $l \in D^*$ is an algebraic group over an algebraically closed field and $D \leq C_G(D)^\circ$. Then $N_G(V)^\circ = V \rtimes T$, where $T \leq C_G(D)^\circ$ is an algebraic torus of $C_G(l)^\circ$ for all $l \in D^*$.*

Proof. By Fact 2.4, $Q \leq V$ for any quasiunipotent subgroup $Q \leq N_G(V)^\circ$ and V is the unique maximal quasiunipotent subgroup of $N_G(V)^\circ$. By [19, 5.14], $N_G(V)^\circ = \langle C_{N_G(V)}(l)^\circ |\ l \in D^*\rangle$ where $N_l := C_{N_G(V)}(l)^\circ$ is a connected definable subgroup of an algebraic group for all $l \in D^*$. Let U_l be a maximal quasiunipotent subgroup of N_l for all $l \in D^*$. As $U_l \leq V$, $U_l = V \cap C_G(l)^\circ$. Thus U_l is a characteristic subgroup of N_l for all $l \in D^*$ and $V = \langle U_l |\ l \in D^*\rangle$ by [19, 4.6].

Let $l \in D^*$. Then $N_l = N_{N_l}(U_l)$ is solvable by Lemma 2.19. Furthermore $D \leq N_l$, as D normalizes U and $D \leq C_G(D)^\circ$. Let $\overline{N_l}$ be the Zariski closure of N_l. As $\overline{N_l}$ is a Zariski connected solvable group, $N_l = W \rtimes T$ by [42, 19.3], where W is the unipotent radical of $\overline{N_l}$ and T a maximal torus. Since D consists of semisimple elements, we can chose T to contain D by [42, 19.4]. W° is a quasiunipotent subgroup of $C_G(l)^\circ$ by Lemma 2.1 and hence contained in U_l. Thus $\overline{N_l}^\circ \cap N_l = U_l \rtimes (T \cap N_l)$ since T is connected by [18, ex. 3, p. 78]. As G does not interpret a bad field, $T \cap N_l \leq T$ is an algebraic torus itself and actually $T \leq N_l$. Finally $T \leq C_G(D)^\circ$ and thus $T \leq N_k$ for all $k \in D^*$. This implies that $N_G(V)^\circ = \langle U_l |\ l \in D^*\rangle \rtimes T = V \rtimes T$. □

Corollary 2.21 *Let G be a K^*-group of finite Morley rank and odd type that does not interpret a bad field. Let B be a definable connected solvable subgroup of G. Assume that there exists a four-subgroup $D \leq B$ such that either*

(i) $C_B(l)^\circ$ is an algebraic group over an algebraically closed field for all $l \in D^*$ or

(ii) B is a Borel subgroup of G and $C_G(l)^\circ$ is an algebraic group over an algebraically closed field for all $l \in D^*$,

then there exists an algebraic torus T such that $B = Q(B) \rtimes T$.

Proof. B has connected Sylow 2-subgroups by [18, 9.29], especially $D \leq C_G(D)$ for any four-subgroup $D \leq B$. Furthermore $Q(B)$ is the unique maximal quasiunipotent subgroup of B by Proposition 2.16. If (i) holds then $B = N_B(Q(B))^\circ = Q(B) \rtimes T$ for an algebraic torus T by Proposition 2.20. If (ii) holds then $Q(B)$ is a maximal quasiunipotent subgroup of G as B is a Borel subgroup of G by Proposition 2.16. Thus $N_G(Q(B))^\circ = Q(B) \rtimes T$ for an algebraic torus T by Proposition 2.20. As $Q(B) \leq B$ this implies that $B = Q(B) \rtimes (B \cap T)$ and the claim follows since G does not interpret a bad field. □

Chapter 3

2-local Analysis

Let G be any group. A subgroup H is said to be a *local subgroup* if $H = N_G(A)$ for a nontrivial definable abelian subgroup $A \leq G$. If A is a p-group for some prime number p, H is said to be a *p-local subgroup*. In particular, the centralizer of an involution $t \in G$ is a 2-local subgroup because $C_G(t) = N_G(\langle t \rangle)$. As in the classification of finite simple groups, a great deal of information about groups of finite Morley rank can be deduced from information about centralizers of involutions and, especially in the odd type case, normalizers of the connected component of Sylow 2-subgroups.

3.1 Strongly embedded subgroups

One of the standard technics in the CFSG is to prove that a subgroup of a finite simple group G is either *strongly embedded* — and hence known by the classification result of H. Bender [14] — or already equals G. A proper definable subgroup M of a group G is said to be *strongly embedded* if it contains involutions and for every $g \in G \setminus M$, $M \cap M^g$ does not contain involutions. Altınel has shown in [2], that any simple tame K^*-group of even type that has a strongly embedded subgroup is isomorphic to $\mathrm{SL}_2(K)$ for an algebraically closed field K of characteristic 2. If Conjecture 3 is true, then this is the only place, where strongly embedded subgroups appear in the theory of simple tame K^*-groups. The main aim of this section is to prove the following partial result.

Theorem 3.1 *Let G be a simple K^*-group of odd type that does not interpret any bad field and such that $pr(G) \geq 2$. Let $M < G$ be a strongly embedded subgroup. Then M° is solvable.*

Corollary 3.2 *Let G be a simple tame K^*-group with a strongly embedded subgroup M. Then M is solvable or G is of odd type and Prüfer 2-rank* 1.

Proof. G is either of odd or of even type by Fact 1.3. If G is of odd type and $pr(G) \geq 2$, then M is solvable by Theorem 3.1. If G is of odd type, then M is solvable by [2]. □

Groups of finite Morley rank with a strongly embedded subgroup have only one conjugacy class of involutions by [18, 10.19]. Furthermore a proper subgroup M of a group G of finite Morley rank is strongly embedded if and only if M contains involutions, $C_G(t) \leq M$ for any $t \in I(M)$ and $N_G(S) \leq M$ for any Sylow 2-subgroup S of M by [2]. Their structural properties are discussed in [2] and slightly further explored in [6]. We can describe strongly embedded subgroups differently, if G is a connected K^*-group of finite Morley rank and odd type such that $pr(G) \geq 2$.

Proposition 3.3 *Let G be a connected K^*-group of finite Morley rank and odd type such that $pr(G) \geq 2$. Assume that $M < G$ is a strongly embedded subgroup of G. Then*

(i) $M^\circ = \langle C_G(t)^\circ |\, t \in D^* \rangle$ for any four-subgroup D of M and

(ii) M is a maximal proper definable subgroup of G.

Thus, if G is a K-group, then it cannot contain a strongly embedded subgroup.

Proof. Any Sylow 2-subgroup S of M is already a Sylow 2-subgroups of G by [2]. Thus there exists a four-subgroup $D \leq M$, as $pr(G) \geq 2$. Then $M^\circ = \langle C_M(t)^\circ |\, t \in D^* \rangle$ by [19, 5.14]. On the other hand $C_G(t)^\circ \leq M^\circ$ for all $t \in D^*$ as M is strongly embedded, which gives us that $M^\circ = \langle C_G(t)^\circ |\, t \in D^* \rangle$.

We show that M is a maximal proper definable subgroup of G. Let N be a definable subgroup of G such that $M \leq N < G$. Then N is strongly embedded as well by [2]. Hence $N^\circ = \langle C_G(t)^\circ : \ t \in D^* \rangle = M^\circ$ by [18, 5.14] again. Especially $N \leq N_G(M^\circ)$. Let $g \in N_G(M^\circ)$. Then $M^\circ \leq M \cap M^g$ contains involutions as $I(M) = I(M^\circ)$ by [2]. Since M is strongly embedded, this implies that $N_G(M^\circ) \leq M$ and hence $N = N_G(M^\circ) = M$.

As finally $G = \langle C_G(t)^\circ |\, t \in D^* \rangle$ for any four-subgroup $D \leq G$, if G is a K-group by [19, 5.14], G cannot contain a strongly embedded subgroup in this case. □

The reverse direction is true as well.

Proposition 3.4 *Let G be a connected K^*-group of finite Morley rank and odd type such that $pr(G) \geq 2$. Let $N := \langle C_G(l)^\circ |\, l \in D^* \rangle$ for a four-subgroup D of G. Then either N is normal in G or $N_G(N)$ is a strongly embedded subgroup of G.*

Proof. Assume that $M := N_G(N) < G$. Then M is a K-group which contains D and $M^\circ = N$ by [19, 5.14]. We are going to show that $C_G(t) \leq M$ for any $t \in I(M)$ and that $N_G(S) \leq M$ for any Sylow 2-subgroup S of M.

Let $t \in I(M)$ be any involution. Then t is contained in Sylow 2-subgroup S of M. As $Z(S) \neq 1$ by [18, 6.22], there exists $s \in S$ such that $D_1 := \langle t, s\rangle$ is a four-subgroup of S with $D_1 \cap Z(S) \neq 1$. Thus $M^\circ = \langle C_M(k)^\circ |\ k \in D_1^*\rangle$ by [19, 5.14]. Let $L := \langle C_G(k) |\ k \in D_1^*\rangle$. Then $C_G(t) \leq L$. We show that $L \leq M$. As $Z(S) \cap D_1 \neq 1$, $S \leq L$. Let $g \in M$ such that $D^g \leq S$. Then

$$L^\circ = \langle C_L(l)^\circ |\ l \in (D^g)^*\rangle \leq N^g = N.$$

by [19, 5.14] again. Thus $M^\circ \leq L^\circ \leq N = M^\circ$, $L^\circ = N$ and $L \leq N_G(N) = M$. Hence $C_G(t) \leq M$ for any involution $t \in M$.

Let furthermore S be any Sylow 2-subgroup of M. As $C_G(t) \leq M$ for all $t \in M$, $pr(M) = 2$. As $N_G(S) \leq N_G(S^\circ)$, it is sufficient to show that $N_G(S^\circ) \leq M$. Let $g \in N_G(S^\circ)$. Then either $g \in C_G(s) \leq M$ for some involution $s \in S^\circ$ or there exists an elementary abelian subgroup $E \leq S^\circ$ of order at least 4 such that $g \in N_G(E)$. Since $M^\circ = \langle C_G(l)^\circ :\ l \in E\backslash\{1\}\rangle$ by the first part of the proof, this implies that $g \in N_G(M^\circ) = M$. □

We are now able to exhibit two possible examples of strongly embedded subgroups.

Remark 3.5 *Let H be a K-group of odd type that contains an elementary abelian 2-subgroup E of order 8. Then*

$$H^\circ = \langle C_H(D)^\circ |\ D \leq E, [E : D] = 2\rangle.$$

Proof. Let $D_1 \leq E$ be a four-subgroup. Then $H^\circ = \langle C_H(i)^\circ |\ i \in D_1^*\rangle$ by [19, 5.14.]. However, $E \leq C_H(i)$ for any $i \in D_1^*$ and thus

$$C_H(i)^\circ = \langle C_H(D)^\circ |\ i \in D \leq E, [E : D] = 2\rangle$$

by [19, 5.14.] again. □

Proposition 3.6 *Let G be a simple K^*-group of odd type such that $pr(G) \geq 2$ and assume that G contains an elementary abelian subgroup E of order 8. If G contains a proper 2-generated core Γ, then G contains a strongly embedded subgroup $M := N_G(\Gamma^\circ)$.*

Proof. We may assume that $\Gamma = \Gamma_{S,2}$, where S is a Sylow 2-subgroup of G that contains E. As $pr(G) \geq 2$, $S \leq N_G(S^\circ) \leq \Gamma$ by definition and $\Gamma^\circ = \langle C_\Gamma(D)^\circ |\ D \leq E, [E : D] = 2\rangle$ by Remark 3.5. Since $N_G(D) \leq \Gamma$ for all four-subgroups $D \leq E$,

$$\Gamma^\circ = \langle C_G(D)^\circ |\ D \leq E, [E : D] = 2\rangle = \langle C_G(i)^\circ | i \in D_1^*\rangle$$

for any four-subgroup $D_1 \leq E$. The claim now follows by Proposition 3.4. □

To give the second example, we need some more definitions. Let G be a group of finite Morley rank. We say that G is a $2^\perp$-group if G does not contain involutions and we denote by $O(G)$ the *core of* G, the maximal normal definable connected $2^\perp$-subgroup of G. The core exists since the product of two normal definable $2^\perp$-subgroups is a $2^\perp$-subgroup itself by [18, ex. 11, p. 93]. Remember, that if G is a K-group that does not interpret a bad field, then $O(G)$ is nilpotent by [19, 5.8].

It is well known that in a simple algebraic group G over an algebraically closed field of characteristic not 2 we have $O(C_G(i)) = 1$ for any involution $i \in G$. This should also hold in a simple tame K^*-group G of odd type. In Corollary 3.16 we prove this conjecture in a special case.

Let G be a group of finite Morley rank and θ a function from $I(G)$ into the set of definable subgroups of G. We say that θ is a *signalizer functor for* G if $\theta(s) \leq O(C_G(s))$ is a connected definable normal subgroup of $C_G(s)$ for all $s \in I(G)$ and if furthermore for any commuting involutions $s, t \in G$

$$\theta(t) \cap C_G(s) = \theta(s) \cap C_G(t).$$

In particular, θ is a signalizer functor for any simple K^*-group G of odd type if $\theta(t) = O(C_G(t))$ for any involution $t \in G$ by [18, B.29]. A signalizer functor θ is called *complete*, if for any elementary abelian subgroup $E \leq G$ of order ≥ 8 the subgroup $\theta(E) = \langle \theta(t), t \in E\backslash\{1\}\rangle$ is a connected $2^\perp$-subgroup and $C_{\theta(E)}(s) = \theta(s)$ for any $s \in E^*$. We call θ *nilpotent* if all the subgroups $\theta(t)$ for $t \in I(H)$ are nilpotent.

Fact 3.7 ([17]) *Any nilpotent signalizer functor θ on a group G of finite Morley rank is complete.*

Proposition 3.8 *Let G be a simple K^*-group of odd type that does not interpret a bad field. Assume that $pr(G) \geq 2$ and that G contains an elementary abelian subgroup E of order 8. Let θ be the signalizer functor defined by $\theta(s) = O(C_G(s))$ for all $s \in I(G)$. Then either $O(C_G(s)) = 1$ for all $s \in E^*$ or $N_G\big(N_G(\theta(E))\big)$ is a strongly embedded subgroup of G.*

Proof. As G does not interpret a bad field, θ is a nilpotent signalizer functor and thus complete by Fact 3.7. Hence $\theta(E)$ is nilpotent. Let D be any four-subgroup of E. As D acts on $\theta(E)$ by a definable group automorphism

$$\theta(E) = \langle C_{\theta(E)}(t),\ t \in D^* \rangle$$

by [19, 4.6]. Since θ is complete this implies that

$$\theta(E) = \langle O(C_G(t)),\ t \in D^* \rangle$$

In particular $N_G(D) \leq N_G(\theta(E))$. Thus

$$N_G(\theta(E))^\circ = \langle C_G(D)^\circ |\ D \leq E, [E : D] = 2 \rangle = \langle C_G(i)^\circ | i \in D_1^* \rangle$$

for any four-subgroup $D_1 \leq E$ by Remark 3.5. The claim now follows by Proposition 3.4. $\square$

To prove Theorem 3.1, we need the following crucial fact about centralizers of involutions, which is also one of the main tools to classify groups of small Prüfer 2-rank.

Fact 3.9 ([19]) *Let G be a simple K^*-group of finite Morley rank and odd type that does not interpret a bad field. Let $i \in I(G)$. Then $C_G(i)^\circ/O(C_G(i))$ is a central product of an abelian divisible group T and a semisimple group H all of whose components are simple algebraic groups over algebraically closed fields of characteristic different from 2.*

Lemma 3.10 *Let H be a group of finite Morley rank. For any $X \leq H$ and $h \in H$ let $\overline{X} := XO(H)/O(H)$ and $\overline{t} := tO(H)$.*

(i) If $t \in I(H)$ then $\overline{t} \in I(\overline{H})$ and if $\overline{s} \in I(\overline{H})$ then there exists an involution in $sO(H)$.

(ii) $O(\overline{H}) = 1$.

(iii) Let $t, s \in I(H)$. If $[\overline{t}, \overline{s}] = 1$, then there exists $u \in I(sO(H))$ such that $[t, u] = 1$.

(iv) Let $t \in I(H)$. Then $I(tO(H)) = t^{O(H)}$. Especially $t, s \in I(H)$ are conjugate in H if and only if $\overline{t}, \overline{s}$ are conjugate in $\overline{H}$.

Proof. Let $t \in I(H)$. Since $O(H)$ is a $2^{\perp}$-subgroup of H, $t \notin O(H)$ and $\overline{t}$ is an involution in $\overline{H}$. Since furthermore $sO(H)$ contains a 2-element by [18, ex 11, p.93] if $\overline{s}$ is an involution, (i) follows.

To show (ii), let $B \geq O(H)$ be such that $\overline{B} = O(\overline{H})$. Then B is a definable, connected normal subgroup of H since $O(H)$ and $O(\overline{H})$ are definable and connected. Furthermore B cannot contain an involution by (i) and $B = O(H)$ by maximality of $O(H)$.

Let $t, s \in I(H)$. If $[\overline{t}, \overline{s}] = 1$, then

$$\overline{s} \in C_{\overline{H}}(\overline{t}) = \overline{C_H(t)} \cong C_H(t)/(C_H(t) \cap O(H))$$

by [3, 2.52], i.e. we can find an involution $u \in C_H(t)$ such that $\overline{s} = \overline{u}$ which gives us (iii).

Let finally $to \in I(tO(H))$. Then to and t cannot commute with an involution in the definable closure of their product since $d(tot) = d(o^t) \leq O(H)$. Thus they must be conjugate in $O(H)$ by [18, 10.2]. □

Lemma 3.11 *Let H be a group of finite Morley rank and odd type. Let S be a Sylow 2-subgroup of H and $N \lhd H$ a definable solvable subgroup. Then $S^\circ N/N$ is the connected component of a Sylow 2-subgroup of H/N.*

Proof. Let P be a Sylow 2-subgroup of H/N that contains $S^\circ N/N$. Let furthermore F be a subgroup of H which contains N such that $F/N = d(P^\circ)$. Then F is a definable solvable group and $S^\circ \leq F$. Thus S° is the connected component of a Sylow 2-subgroup of F and $S^\circ N/N$ is the connected component of a Sylow 2-subgroup of $F/N = d(P^\circ)$ by [5]. Hence $S^\circ N/N = P^\circ$ and the claim follows. □

Lemma 3.12 *Let G be a simple K^*-group of finite Morley rank and odd type that does not interpret a bad field. Let $i \in G$ be an involution and $C := C_G(i)^\circ/O(C_G(i)) = H * T$ as in Fact 3.9. If Q is a Sylow 2-subgroup of H and S a Sylow 2-subgroup of C that contains Q, then $S^\circ = Q^\circ R$ where R is the Sylow 2-subgroup of T. Especially $pr(C) = pr(H) + pr(T)$, were either T is trivial or $pr(T) \geq 1$.*

Proof. Since C is the central product of H and T, $H \cap T \leq Z(H) \leq Z(C)$ and $H \cap T$ is finite, as H is semisimple. Let Q be a Sylow 2-subgroup of H and S a Sylow 2-subgroup of C that contains Q. Since T is a central subgroup of C, the Sylow 2-subgroup R of T is contained in S and $Q * R \leq S$. T is as a divisible group connected by [18, ex. 3, p. 78]. Thus R is connected as well by [18, 9.29] and $Q^\circ R \leq S^\circ$.

As T is abelian $S^\circ T/T$ is the connected component of a Sylow 2-subgroup of C/T by Lemma 3.11 where $S^\circ T/T \cong S^\circ/(S^\circ \cap T) = S^\circ/R$. On the other hand $Q^\circ(H\cap T)/(H\cap T) \cong Q^\circ/(Q^\circ \cap T)$ is the connected component of a Sylow 2-subgroup of $H/(H\cap T)$ by Lemma 3.11 again. As $C/T = HT/T \cong H/(H\cap T)$ actually $S^\circ/R \cong Q^\circ/(Q^\circ \cap T) = Q^\circ/(Q^\circ \cap R) \cong Q^\circ R/R$ and $S^\circ = Q^\circ R$. As $pr(C) = pr(S)$, $pr(H) = pr(Q)$ and $pr(T) = pr(R)$ this implies that $pr(C) = pr(H) + pr(T)$.

Assume now that $pr(T) = 0$. As R is connected, $R = 1$. Especially $T \leq O(C)$. However $O(C) = 1$ by Lemma 3.10 and T is trivial. □

Proposition 3.13 *Let G be a simple K^*-group of odd type that does not interpret a bad field. Then $N_G(P^\circ)$ is solvable-by-finite for any Sylow 2-subgroup P of G.*

Proof. Since P° is a 2-torus $|N_G(P^\circ)/C_G(P^\circ)| < \infty$ by [18, 6.16]. Hence it is enough to show that $C_G(P^\circ)^\circ$ is solvable.

Let $i \in P^\circ$ be any involution. As P is infinite by [19], i exists. We write $\overline{X} = XO(C_G(i))/O(C_G(i))$ for any subgroup $X \leq C_G(i)$. If $C := \overline{C_G(i)^\circ}$ is solvable, the claim follows, since $C_G(P^\circ) \leq C_G(i)$. Assume now that C is not solvable. Then $C = H * T$ by Fact 3.9, where T is an abelian divisible group and H is a nontrivial semisimple group all of whose components H_n for $1 \leq n \leq k$ are simple algebraic groups over algebraically closed fields of characteristic different from 2. $\overline{P}^\circ$ is the connected component of a Sylow 2-subgroup of C by Lemma 3.11. Thus $\overline{P}^\circ = Q^\circ R$, where Q is a Sylow 2-subgroup of H and R the Sylow 2-subgroup of T by Lemma 3.12. Let Q_n for $1 \leq n \leq k$ be the projections of Q° onto H_n. As Q° consists of commuting 2-elements, Q_n is an abelian 2-group and hence contained in a maximal torus T_n of H_n for all $1 \leq n \leq k$ by [42, 15.4]. As Q_n are the connected components of Sylow 2-subgroups of the simple algebraic groups H_n for all $1 \leq n \leq k$, $C_H(Q^\circ) = T$, where $T := T_1 \cdots T_k$. Thus $C_H(\overline{P}^\circ) = T$ as well and $\overline{C_{C_G(i)^\circ}(P^\circ)} \leq C_C(\overline{P}^\circ)$ is abelian. Hence $C_{C_G(i)^\circ}(P^\circ)^\circ$ is a connected solvable group. However, $C_G(P^\circ)^\circ \leq C_G(i)^\circ$ and $C_G(P^\circ)^\circ \leq C_{C_G(i)^\circ}(P^\circ)^\circ$ is solvable. □

We need one more result to prove Theorem 3.1.

Lemma 3.14 *Let N be a group of finite Morley rank and $H \lhd N$ a definable normal subgroup such that H° is a $2^\perp$-group. Then $N^\circ = C_N(i)^\circ H^\circ$ for all involutions $i \in H$.*

Notice that the Lemma reduces to the Frattini argument [18, 10.12], if $\langle i \rangle$ is a Sylow 2-subgroup of H.

Proof. Let $i \in I(H)$. Then $H^\circ = C_{H^\circ}(i)H^-$ where H^- is the set of elements of H° inverted by i by [18, ex. 14, p. 73]. Furthermore

$$(*) \quad rk(H^\circ) = rk(C_{H^\circ}(i)) + rk(H^-).$$

We claim that $H^- = ii^{H^\circ} = iI(iH^\circ)$. Let $h \in H^-$. As H° is as a $2^\perp$-group 2-divisible by [18, ex. 11, p. 72], there exists an element $d \in H^\circ$ such that $h = d^2$. On the other hand $h^i = h^{-1}$ and thus already $d = d^{-1}$ by [18, ex. 12, p. 72]. Thus $d \in H^-$ and $t = d^2 = [i,d] \in ii^{H^\circ}$. Furthermore for all $d \in H^\circ$, $ii^d \in iI(iH^\circ)$ as $i^d = i[i,d] \in iH^\circ$. The claim follows since $iI(iH^\circ)$ is a subset of H° inverted by i.

i^N on the other hand is the disjoint union of finitely many sets $I(j_kH^\circ)$ for $1 \le k \le d$ where $d \le |H/H^\circ|$ and $j_k \in i^N$. Thus we may assume that $rk(i^N) = rk(I(iH^\circ)) = rk(H^-)$ and

$$(**) \quad rk(N) = rk(C_N(i)) + rk(i^N) = rk(C_N(i)) + rk(H^-).$$

(*) and (**) imply that

$$rk(N) = rk(C_N(i)) + rk(H^\circ) - rk(C_N(i) \cap H^\circ) = rk(C_N(i)H^\circ).$$

Hence $N^\circ = C_N(i)^\circ H^\circ$ for any involution $i \in N$. □

Proof of Theorem 3.1. Let σ be the solvable radical of M°. Since M does not interpret a bad field $O(M^\circ)$ is nilpotent and hence, as a definable connected subgroup, contained in σ°. Notice that, since $O(M^\circ)$ is characteristic in M°, $O(M^\circ) \le O(M) \le M^\circ$ and thus $O(M^\circ) = O(M)$. As furthermore M is a strongly embedded K-group

$$O(C_G(t)) = O(C_M(t)) \le O(M) \le \sigma^\circ$$

for all involutions $t \in M$ by [19]. σ° is a characteristic subgroup of M° and hence normal in M. Since M contains one conjugacy class of involutions as a strongly embedded subgroup by [18, 10.19], this implies that either $I(M) \subseteq \sigma^\circ$ or σ° does not contain involutions.

(a) If σ° contains involutions, then M° is solvable.

Proof. Assume that $I(M) \subseteq \sigma^\circ$. Let S_1 be a Sylow 2-subgroup of σ° and $S \ge S_1$ a Sylow 2-subgroup of M. Then S is a Sylow 2-subgroup of G by [2]. Furthermore S_1 is connected by [18, 9.29] and thus a divisible subgroup of the abelian group S°. Hence S_1 has a complement B in S° by the theorem of Baer [34, 15.1]. As, however, all involutions are contained in σ°, B has to be trivial,

$S_1^\circ = S^\circ$ and S° is a Sylow 2-subgroup of σ°. By the Frattini argument [18, 10.12] $M = N_M(S^\circ)\sigma^\circ$. Since $N_M(S^\circ)/C_M(S^\circ)$ is finite by [18, 6.16], $M^\circ = C_M(S^\circ)^\circ\sigma^\circ$. However $C_G(S^\circ)^\circ$ is solvable by Corollary 3.13. Thus M° is already solvable and $M^\circ = \sigma^\circ$. □

(b) If σ contains involutions, then either $I(M)$ is finite or M° is solvable.

Proof. We may assume by (a) that σ° is a $2^\perp$-group and that $I(M) \subseteq \sigma$ as σ is normal in M. As $M^\circ = C_G(i)^\circ\sigma^\circ$ for any involution $i \in M$ by Lemma 3.14,

$$\overline{M}^\circ := M^\circ/\sigma^\circ \cong C_G(i)^\circ/(C_G(i)^\circ \cap \sigma^\circ) = C_G(i)^\circ/O(C_G(i))$$

for any involution $i \in M$. Since $I(M) = I(M^\circ)$ by [2], $\{i\sigma^\circ | i \in I(M)\} \subseteq Z(\overline{M}^\circ)$. If $I(M)$ is infinite, then $M^\circ = \sigma$, since M° would otherwise contain infinitely many commuting involutions by Lemma 3.10. Hence M° is solvable in this case. □

(c) If $I(M)$ is finite, then either $pr(G) = 1$ or M° is solvable.

Proof. If $I(M)$ is finite, then $M^\circ = C_G(i)^\circ$ for any involution $i \in M$ as $rk(M) = rk(C_G(i)) + rk(I(M))$. Hence $M^\circ/O(M)$ is a central product of an abelian divisible group T and a semisimple group H all of whose components are algebraic groups over algebraically closed fields of characteristic not 2 by Fact 3.9. We assume that M° is not solvable. Then $O(M) = \sigma^\circ$ by (a) and $T = 1$, as T is connected. Let $L_1, \cdots, L_k$ be the components of $M^\circ/O(M) = H$. By Lemma 3.10 all involutions of H are central in H. Especially $|I(L_l)| = 2^{pr(L_l)-1}$, as $Z(L_l)$ is the intersection of all maximal tori in L_l for $1 \leq l \leq k$ by [42, ex. 2, p. 162] and $|I(H)| = 2^{pr(H)-1}$, as $Z(H)$ is the intersection of all maximal tori in H by [42, ex. 2, p. 162] again. Let $g \in M$. As g acts as automorphism on $M^\circ/O(M)$, for all $1 \leq l \leq k$ there exists $1 \leq s \leq k$ such that $L_l^g = L_s$ by [18, 7.1] and thus $I(L_l)^g = I(L_s)$. If $i_1 \in I(L_1)$, then $I(M^\circ/O(M)) = i_1^M = \{I(L_1), \cdots, I(L_k)\}$ since M, and hence $M/O(M)$ by Lemma 3.10, contains one conjugacy class of involutions. Set $p := pr(L_1)$. Then $pr(H) = kp$ and $|\{I(L_1), \cdots, I(L_k)\}| \leq k2^{p-1}$. This can only happen for $k = 1$, since $|I(H)| = 2^{kp-1} > k2^{p-1} \geq |i_1^M|$ for $k > 1$. Hence H is already quasi-simple. However, the only quasi-simple algebraic group in which all involutions are central is $\mathrm{SL}_2(K)$ for an algebraically closed field of characteristic not 2. (Compare e.g. [37]). As $pr(H) = pr(M^\circ/O(M)) = pr(M^\circ)$ by Lemma 3.11, the claim follows. □

Suppose that σ does not contain involutions. Then M° is not solvable since $pr(M) = pr(G) \geq 2$ and $1 \neq \overline{M} := M/\sigma$ contains one conjugacy class of involutions as in the proof of Lemma 3.10. As furthermore M is a K-group $\overline{M^\circ}$ is the direct sum of simple algebraic groups over algebraically closed fields of characteristic not 2 by [2]. Let $L_1, \cdots, L_k$ be the components of $\overline{M}^{\circ}$. As L_l contains involutions for any $1 \leq l \leq k$, $\overline{M}$ acts transitively on the components and all components are isomorphic by [18, 7.10].

We claim that L_1 contains one conjugacy class of involutions. For assume that i, j in $I(L_1)$ are not conjugate in L_1. Then there exists $m \in \overline{M}$ such that $i^m = j$. As $\overline{M^\circ}$ is the direct product of conjugates of L_1, this implies that $L_1^m = L_1$. Thus $C_{L_1}(i)^m = C_{L_1}(j)$. However, non-conjugate involutions of simple algebraic groups have non-isomorphic centralizers of involutions by [37, 4.3]. Contradiction.

The only simple algebraic groups with one conjugacy class of involutions are $\mathrm{PSL}_2(K), \mathrm{PSL}_3(K)$ or $\mathrm{G}_2(K)$ for an algebraically closed field K of characteristic not 2. Hence we may assume that $\overline{M}^{\circ}$ is isomorphic to a direct sum of copies of these groups. On the other hand $M^\circ = C_G(i)^\circ H$ for a connected $2^\perp$-group H which can be chosen independently from $i \in I(M)$ by [2, 3.10] since M is strongly embedded. Hence $\overline{M}^{\circ}$ is the product of the centralizer of the involution $\overline{\imath}$ and a Borel subgroup B of $\overline{M}^{\circ}$ in the sense of algebraic group theory which contains the connected nilpotent group $H\sigma/\sigma$. As H is independent from $i \in I(M)$, we can choose i such that $\overline{\imath} \in B$. Let $B = U \rtimes T$, where U is the unipotent radical of B and T a maximal torus which contains $\overline{\imath}$ by [42, 19.3]. Let U_l be the projections of U into L_l and T_l be the projections of T into L_l for $1 \leq l \leq k$. Then $\overline{\imath} = i_1 \cdots i_k$ where $i_l \in I(T_l)$ and thus $T_l \leq C_{L_l}(i_l)$ for $1 \leq l \leq k$. Hence $\dim L_l \leq \dim C_{L_l}(i_l) + \dim U_l$ for $1 \leq l \leq k$. We may assume that $i_1 \neq 1$.

If $L_1 \cong \mathrm{PSL}_2(K)$, then $\dim L_1 = 3$, $\dim C_{L_1}(i_1) = 1$ and $\dim U_1 = 1$.

If $L_1 \cong \mathrm{PSL}_3(K)$, then $\dim L_1 = 8$, $\dim C_{L_1}(i_1) = 4$ and $\dim U_1 = 3$.

If $L_1 \cong \mathrm{G}_2(K)$, then $\dim L_1 = 14$, $\dim C_{L_1}(i_1) = 6$ and $\dim U_1 = 6$.

Thus none of these cases can occur. Contradiction. □

Corollary 3.15 *Let G be a simple K^*-group of odd type that does not interpret a bad field. Assume that $pr(G) \geq 2$ and that G contains an elementary abelian subgroup of order 8. If there exists an involution $i \in G$ such that $C_G(i)$ is not solvable, then G does not contain a proper 2-generated core.*

Proof. Assume that G does contain a proper 2-generated core. Then G contains a strongly embedded subgroup M by Proposition 3.6. If there exists an involution $i \in G$ such that $C_G(i)$ is not solvable, we may assume that $i \in M$, as

G contains only one conjugacy class of involutions. Then $C_G(i) \leq M$ since M is strongly embedded and M is not solvable. Contradiction to Theorem 3.1. □

Corollary 3.16 *Let G be a simple K^*-group of odd type that does not interpret a bad field. Assume that $pr(G) \geq 2$ and that G contains an elementary abelian subgroup of order 8. If there exists an involution $i \in G$ such that $C_G(i)$ is not solvable, then $O(C_G(t)) = 1$ for all $t \in E^*$.*

Proof. By Proposition 3.8 either $O(C_G(t)) = 1$ for all $t \in E^*$ or G contains a strongly embedded subgroup M. The second case cannot occur, however, as in the proof of Corollary 3.15, which implies the claim. □

Corollary 3.17 *Let G be a simple K^*-group of odd type that does not interpret a bad field. Assume that $pr(G) \geq 2$. If there exists an involution $i \in G$ such that $C_G(i)$ is not solvable, then $G = \langle C_G(k)^\circ |\ k \in D_1^* \rangle$ for any four-subgroup $D_1 \leq G$.*

Proof. $D_1 \leq G$ be a four-subgroup of G and set $M := \langle C_G(k)^\circ |\ k \in D_1^* \rangle$. By Proposition 3.4 either $G = N_G(M)$ or M is a strongly embedded subgroup. Since G cannot contain a strongly embedded subgroup as in the proof of Corollary 3.15, $G = M$ as G is simple. □

3.2 Thompson Rank Formula

In this section we give an application of the Thompson rank formula and prove the following theorem.

Theorem 3.18 *Let C_1, C_2 be the nonisomorphic centralizers in $\mathrm{PSp}_4(K)$ of two involutions where K is an algebraically closed field of characteristic not 2. Let G be a group of finite Morley rank that contains involutions i and j such that $C_G(i) \cong C_1$ and $C_G(j) \cong C_2$. Set $k := \max\{rk(Z(C_G(u_1))), rk(Z(C_G(u_2)))\}$. Then $rk\ G = 10\ k$.*

The proof of this theorem is quite easy and involves only computations in C_1 and C_2. We proceed in the following way. First we describe C_1 and C_2. We show that G contains exactly two conjugacy classes of involutions. This information allows us to construct a function f as in Proposition 1.2, and finally to compute

$$r_w := rk\big(\{(\kappa, \lambda) :\ \kappa \in i^G \cap C_G(w),\ \lambda \in j^G \cap C_G(w) \text{ and } f(\kappa\lambda) = w\}\big)$$

for $w = i, j$. This gives us the Morley rank of G by Proposition 1.2.

3.2.1 Structure of G

We may assume that $C_G(i) = (L_1 * L_2)\langle u\rangle$ where $L_n \cong \mathrm{SL}_2(K)$ for $n = 1, 2$, u is an involution in G such that $L_1^u = L_2$, and furthermore $L_1 \cap L_2 = Z(L_1) = Z(L_2) = \langle i\rangle$. Set $L := L_1L_2$. Then $C_G(j) \cong (\mathrm{GL}_2(K)/\langle -I\rangle) \rtimes \langle w\rangle$ where $-I = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and w is an involution in G such that w acts as an inverse-transpose automorphism on $GL_2(K)$, i.e.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^w = (ad - bc)^{-1} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

for any $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$. For the structure of centralizers of involutions in this case compare [57]. General information about centralizers of groups of Lie type is available in [37].

Since both i and j are contained in the connected component of a Sylow 2-subgroup of G and as Sylow 2-subgroups are conjugate, we may assume that $i, j \in S^\circ$, where S is a Sylow 2-subgroup of G. Let $D := \langle i, j\rangle$ and $T := C_G(D)^\circ$. Since D contains a central involution by [18, ex. 12, p. 14], $S \leq C_G(i)$.

To apply the Thompson rank formula we need precise information about the distribution of conjugacy classes of involutions in $C_G(i)$ and $C_G(j)$. Let us first consider $C_G(i)$. As all elements of order 4 are conjugate in $\mathrm{SL}_2(K)$, $I(L) = j^L \cup i$ as in [57]. Furthermore $I(Lu) = u^{L_1} \cup iu^{L_1}$, as $lu \in I(G)$ for $l \in L$ if and only if $l^u = l$ or $l^u = il$, i.e. if and only if $l = l_1l_1^u$ or $l = il_1l_1^u$ for $l_1 \in L_1$.

Set now $R := C_G(j)^\circ$. Elements of R can be represented by elements of $\mathrm{GL}_2(K)$ where the two matrices A and $-A$ are identified. Then $I(R) = j \cup i^R \cup (ij)^R$, depending on the determinant of the corresponding matrix. Let $v \in R$ such that v corresponds to $V := \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Then $A^V = det(A)A^w$ for all $A \in GL_2(K)$. As furthermore for $A := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$

$$AA^V = \begin{pmatrix} -det(A) + b(b-c) & a(c-b) \\ d(b-c) & -det(A) + c(c-b) \end{pmatrix},$$

gw is an involution for $g \in R$, if and only if g is represented by one of the following matrices:

$$\begin{pmatrix} a & b \\ b & d \end{pmatrix} \text{ or } \begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix}$$

where we can choose $a, b, d \in K$ such that the determinants are unequal to 0. It is now easy to see that $I(Rw) = w^R \cup (vw)^R$.

Lemma 3.19 *$C_G(i)$ contains four conjugacy classes of involutions represented by $\{i, j, u, iu\}$ and $C_G(j)$ contains five conjugacy classes of involutions represented by $\{j, i, ij, w, vw\}$. Furthermore $i^G \cap C_G(i) = i \cup (iu)^{L_1}$, $j^G \cap C_G(i) = j^L \cup u^{L_1}$, $j^G \cap C_G(j) = j \cup (ij)^R \cup w^R$ and $i^G \cap C_G(j) = i^R \cup (vw)^R$. Especially G contains exactly two conjugacy classes of involutions.*

Proof. We have already finished the proof of the first part of the lemma. As $C_G(D) = T \rtimes \langle v, w\rangle$ where $\langle v, w\rangle$ is a four-subgroup and w inverts T, $w \in L$ and w is conjugate to j in $C_G(i)$. Let $w = w_1w_2$, where $w_1 \in L_1T$, $w_2 \in L_2T$. As $w_1, w_2 \in N_G(T)$, $w_2^u = w_1t$ for some $t \in T$ and $j^{w_1} = ij$. We may assume that $u \in R$. For if $u \notin R$, then $uw = uw^u = uw_1^uw_2^u = w_1uw_1t \in R$ and $(uw)^{w_1} \in uT \cap R^{w_1} = uT \cap C_G(ij)^\circ$, i.e. $u \in C_G(ij)^\circ$. Especially u is conjugate to i or ij in $C_G(j)$ and the same is true for iu. Let $D_1 = \langle u, j\rangle$. Then D_1 is conjugate to D in $C_G(j)^\circ$ and u and ju belong to different conjugacy classes. This implies that ju and iu are conjugate. Hence $det(J) = -1$, where J is the matrix corresponding to i. As $det(V) = 1$, v has to be conjugate to ij in R and vi conjugate to i. We may hence assume that u is conjugate to j and ui to i. On the other hand $vw \in C_G(i)\backslash L$. This implies that vw and vwi are not conjugate. Thus $vwi \in C_G(j)\backslash R$ is conjugate to w and hence to j and vw is conjugate to i. □

Lemma 3.20 *The following rank equations are valid.*

- $k = rk(C_G(i, j, u))$.
- $rk(C_G(i)) = 6k$, $rk(C_G(j)) = 4k$.
- $rk(u^{C_G(i)}) = rk((iu)^{C_G(i)}) = 3k$ *and* $rk(j^{C_G(i)}) = 2k$.
- $rk(i^{C_G(j)}) = rk((ij)^{C_G(j)}) = 2k$ *and* $rk(w^{C_G(j)}) = 3k$, $rk((vw)^{C_G(j)}) = k$.

Proof. Since $Z(L)$ is finite, $k = rk(Z(R))$ by definition. However $Z(R) = C_G(i, j, u)^\circ$. Projection gives us that a torus T_1 in L_1 has Morley rank k. Let T_1 be contained in a Borel subgroup B of L_1. Then $rk(L_1) = rk(T_1) + 2\,rk(U_1)$, where U_1 is the unipotent radical of B by the Bruhat decomposition of L_1 [42, 28.3]. Since T_1 acts transitively on $U_1\backslash\{1\}$ with finite 1-point stabilizers $rk(L_1) = 3k$. Hence $rk(C_G(i)) = rk(L_1) + rk(L_1^u) = 6k$ and $rk(C_G(D)) = 2k$. R is the direct product of $Z(R)$ with $\mathrm{PSL}_2(K)$ where the torus in $\mathrm{PSL}_2(K)$ has Morley rank k again. Thus $rk(C_G(j)) = k + 3k = 4k$ using similar arguments. The remaining equalities are easily seen. □

We are now in a position to show that there is a definable function f from $i^G j^G$ to $I(G)$ such that $f(x^g) = f(x)^g$ for all $g \in G$ and

$$f(x) \in \{g \in G |\ g^y = g^{-1} \text{ for all } y \in I(C^*_G(x))\}.$$

The basic idea is that the definable closure of such an element x contains at least one involution by [18, 10.2] and all we have to do is to distinguish one in a definable way. Let $x \in i^G j^G$. If $x \in I(G)$ set $f(x) = x$. If $x \notin I(G)$, let

$$H_x := \{g \in Z(C_G(x)) |\ g^y = g^{-1} \text{ for all } y \in I(C^*_G(x) \backslash C_G(x))\}.$$

H_x is an abelian group. Furthermore $d(x) \leq \langle x \rangle H_x^\circ$, since $x \in H_x$ and $D_x := \langle x \rangle H_x^\circ$ contains an involution. If H_x° contains involutions, let E_x be the maximal elementary abelian 2-subgroup of H_x°. Let S_0 be the Sylow 2-subgroup of H_x°. Since S_0 is connected by [18, 9.29], E_x is conjugate to a subgroup of D. Assume now that H_x° is a $2^\perp$-group. Let $k := |D_x/H_x^\circ|$. Since H_x° is 2-divisible as a $2^\perp$-group by [18, ex. 11, p. 72], there exists $h \in H_x^\circ$ such that $x^k = h^2$. Since k is even, $i_x := x^{k/2}h^{-1}$ is the unique involution in D_x. Furthermore i_x is definable as there exists $m \in \mathbb{N}$ such that $|H_x/H_x^\circ| < m$ for all $x \in i^G j^G \backslash I(G)$ by [18, B.5].

- If $I(H_x^\circ) \neq \emptyset$ set $f(x) = C_G(N_G(E_x)) \cap I(H_x^\circ)$.
- If $I(H_x^\circ) = \emptyset$, set $f(x) = i_x = I(D_x)$.

f is definable. We need to show that f is well-defined. Assume that H_x° contains exactly one involution λ. Then

$$f(x) = C_G(N_G(E_x)) \cap I(H_x^\circ) = C_G(N_G(\langle \lambda \rangle)) \cap \{\lambda\} = \lambda.$$

If H_x contains more than one involution, E_x is conjugate to D and we only need to compute $C_D(N_G(D))$. However $C_D(N_G(D)) = \langle i \rangle$ and f is well-defined in both cases. Let $g \in G$. Then $H_x^g = H_{x^g}$ and $D_x^g = D_{x^g}$. Furthermore

- $f(x)^g = x^g = f(x^g)$ in case that $x \in I(G)$,
- $f(x)^g = C_G(N_G(E_x^g)) \cap I((H_x^\circ)^g) = f(x^g)$ in case that $I(H_x^\circ) \neq \emptyset$,
- $f(x)^g = I(D_x)^g = I(D_{x^g}) = f(x^g)$ in case that $I(H_x^\circ) = \emptyset$.

Thus $f(x)^g = f(x^g)$ for all $g \in G$.

To finish the proof of our theorem, the only thing left to do is to compute r_i and r_j. Up to now we have the following approximations:

$$r_j \leq rk(i^G \cap C_G(j)) + rk(j^G \cap C_G(j)) = 5\ k.$$

Furthermore

$$r_i \le rk(i^G \cap C_G(i)) + rk(j^G \cap C_G(i)) = 4\ k$$

and

$$rk(G) = max\{4\ k + r_i, 6\ k + r_j\} \le 11\ k.$$

3.2.2 Computing r_i and r_j

To compute r_i and r_j, it is sufficient to consider the function f on its restriction to $C_G(i)$ and $C_G(j)$ respectively. Let $\kappa \in i^G$, $\lambda \in j^G$. If $x = \kappa\lambda \in C_G(s)$ for $s = i, j$ is not an involution, then

$$H_x = \{g \in Z(C_G(x)) :\ g^\kappa = g^{-1}\} \le C_G(s),$$

since $s \in C_G(x)$ and $C_G^*(x) = \kappa C_G(x) = \lambda C_G(x)$.

We are going to compute r_j first because it is a better candidate for an actual maximum. Since $f(x) = x$ if $x \in I(G)$ and furthermore $f(x^g) = f(x)^g$ it is enough to consider the following four cases:

(i) $x = i(ij)^g$ for all $g \in R$.

(ii) $x = iw^g$ for all $g \in R$.

(iii) $x = (vw)^g(ij)$ for all $g \in R$.

(iv) $x = (vw)^g w = g^{-1}vg^w$ for all $g \in R$.

The easiest case is case (iv). If g corresponds to $A \in GL_2(K)$, then x corresponds to $A^{-1}VA^w = det(A)^{-1}V$. Set $b := det(A)^{-1}$ and let $t \in Z(R)$ such that $x = vt$. Then $d(x) = \langle v\rangle d(t^2)$ and x has order either even or infinite. Furthermore $d(x) \le C_G(D)$.

If $b = 1$, then $x = v$ and $f(x) = v$. Otherwise $x \notin I(G)$. As $E := \langle i, j, v\rangle \le C_G(x)$, $H_x \le Z(C_G(x)) \le C_G(E) = Z(R)\langle v\rangle$. As w inverts x and T and centralizes v, $H_x = Z(C_G(x))$ and $H_x^\circ \le Z(R) \cong K^*$. Let $s \in H_x$ be any involution. Then $C_G(x) \le C_G(s)$, where $C_G(s)$ is either isomorphic to C_1 or C_2. This implies that $Z(C_G(x))$ is isomorphic to an infinite Zariski closed subgroup of the algebraic group $\mathrm{PSp}_4(K)$. Thus $H_x^\circ = Z(R)$ and $f(x) = j$ for all $x = (vw)^g w^h$, where $g, h \in R$ and $det(A) \ne 1$ for $A \in GL_2(K)$ corresponding to g.

Especially $r_j \geq k + 3\,k = 4\,k$ by Lemma 3.20 and $10\,k \leq rk(G) \leq 11\,k$. Note that this implies by virtue of Lemma 3.20 that the only case which is left to compute is case (ii).

Let $Z := \{z \in R |\ z^i = z^{-1}\}$. Then $H_x^\circ \leq C_Z(x)$. Let $z \in Z$. Then either $z = j$, $z = ij$ or z corresponds to a matrix in

$$\{\left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right) \mid ut - vw = \epsilon,\ u = \epsilon t \text{ where } \epsilon = 1, -1\}$$

Let $x = rw$ for $r \in R$ such that r corresponds to $R := \left(\begin{smallmatrix} a & b \\ -b & -d \end{smallmatrix}\right)$. Note that if either $a = d = 0$ or $b = 0$ then x is an involution. In this case $f(x) = x$. Let from now on $ab \neq 0$ or $bd \neq 0$. As $z^{-1}xz = x$ if and only if $z^{-1}xwz^w = xw$, we can do our computations completely within R.

$ad \neq 0$: Set $\rho := ad^{-1}$. Let first $z \in Z$ correspond to $\left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right)$ where $ut - vw = 1$. Then either $z = ij$ or $u = t$. Then $z^{-1}xz = x$ iff the following equations are satisfied:

$$\begin{aligned} -at^2 + dv^2 &= -\epsilon a \qquad & -b + awt - duv &= -\epsilon b \\ -aw^2 + du^2 &= \epsilon d \qquad & b + awt - duv &= \epsilon b \end{aligned}$$

where $\epsilon = 1$ or $\epsilon = -1$. Since however $b \neq 0$ the case $\epsilon = -1$ can never hold. Furthermore $ij \notin C_Z(x)$ and we may assume that $u = t$. Hence $u(aw - dv) = 0$. If $u = 0$ then $v^2 = -\rho$. On the other hand $v = \rho w$ if $u \neq 0$.

Let now $z \in Z$ correspond to $\left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right)$ where $ut - vw = -1$. Then either $z = i$, $z = j$ or $u = -t$. Then $z^{-1}xz = x$ iff the following slightly modified equations are satisfied:

$$\begin{aligned} -at^2 + dv^2 &= \epsilon a \qquad & b + awt - duv &= \epsilon b \\ -aw^2 + du^2 &= -\epsilon d \qquad & -b + awt - duv &= -\epsilon b \end{aligned}$$

where $\epsilon = 1$ or $\epsilon = -1$. Since $b \neq 0$ the case $\epsilon = -1$ again cannot hold. As $i \notin C_Z(x)$, $j \in C_Z(x)$ we may assume that $u = -t$. Then either $u = t = 0$ and $v^2 = \rho$ or $v = -\rho w$. If however $v = -\rho w$ then

$$-1 + \rho w^2 = u^2 = -1 + vw = -1 - \rho w^2$$

and $v = 0 = w$. Contradiction. Hence H_x° corresponds to $\{\left(\begin{smallmatrix} u & \rho w \\ w & u \end{smallmatrix}\right) \mid u^2 - \rho w^2 = 1\}$ and $f(x)$ corresponds to $\left(\begin{smallmatrix} 0 & -w^{-1} \\ w & 0 \end{smallmatrix}\right)$ where $w^2 = -\rho^{-1}$.

$a = 0$: Using similar arguments H_x° is a unipotent subgroup normalized by T and containing x^2. As x^2 corresponds to $\left(\begin{smallmatrix} 1 & 0 \\ 2db^{-1} & 1 \end{smallmatrix}\right)$ the involution in D_x is gw, where g corresponds to $\left(\begin{smallmatrix} 0 & b \\ -b & 0 \end{smallmatrix}\right)$. Thus $f(x) = gw$.

$d = 0$: $f(x) = gw$ as well.

As $f(x) = j$ never occurs in this case, $r_j = 4\,k$ and $rk(G) = 10\,k$. $\square$

Chapter 4

Groups of Small Prüfer 2-rank

In this chapter we are dealing with the classification of tame simple K^*-groups of odd type where the normal 2-rank of the group is small. Due to Conjecture 4, the following should hold.

Conjecture 6 *An infinite simple tame K^*-group G of odd type and normal 2-rank $n(G) \leq 2$ is isomorphic to one of the groups $\mathrm{PSL}_2(K)$, $\mathrm{PSL}_3(K)$, $\mathrm{PSp}_4(K)$, $\mathrm{G}_2(K)$ over an algebraically closed field K of characteristic not 2.*

The basic idea is to construct a BN-pair of G out of information about the centralizers of involutions in G. Two subgroups B and N of a group G are said to be a *BN-pair of G* if the following conditions hold.

BN1. $G = \langle B, N \rangle$ and $T := B \cap N \lhd N$.

BN2. $W := N/T$ is generated by a nonempty set S of involutions.

BN3. $v_i B v \subseteq BvB \cup Bv_i vB$ for all $v_i \in N$ such that $v_i T \in S$ and all $v \in N$.

BN4. $vBv \neq B$ for all $v \in N$ such that $vT \in S$.

The group W is called the *Weyl group* of G. The cardinality of the set S of generators of W, which may be infinite, is called the *Tits rank* of the BN-pair. A conjugate P of a proper subgroup of G that contains B is called *parabolic subgroup.* Finally a BN-pair is called *split* BN-pair if $B = U \rtimes T$ for some normal subgroup U of B. The standard example of a BN-pair, is the pair of subgroups (B, N) of a semisimple algebraic group over an algebraically closed field, where B is a Borel subgroup, $T \leq B$ a maximal torus and $N := N_G(T)$. For further information about BN-pairs see [42].

As an immediate consequence of the results about quasiunipotent groups in Chapter 2 a very important theorem by DeBonis and Nesin [33] can be generalized to the characteristic 0 case. We need the following version.

Theorem 4.1 *Let G be an infinite, simple K^*-group of finite Morley rank that does not interpret a bad field and which has a BN-pair (B, N) of Tits rank 2. Assume further that $B = UT$ is solvable where $U \lhd B$ is the maximal quasiunipotent subgroup of B and $T := B \cap N$. Then $G \simeq \mathrm{PSL}_3(K)$, $\mathrm{PSp}_4(K)$ or $\mathrm{G}_2(K)$ for some algebraically closed field K.*

Virtually no changes in the proof of the corresponding result in [33] are needed.

Sketch of the proof. As G has Tits rank 2, G contains two parabolic subgroups P_1 and P_2. For $i = 1, 2$, set $R_i = \bigcap_{g \in P_i} B^g$. Then P_i/R_i is called a Levi factor of G. By [33, Theorem 1] the two Levi factors of G are infinite simple algebraic groups over algebraically closed fields, since otherwise there would exist a definable normal subgroup V of U such that $U/V \cong K^*$ for some algebraically closed field K by [33, Section 6]. This cannot be the case since U/V is quasiunipotent by Fact 2.4. Since B is solvable the proofs of [33, Lemma 22 and Proposition 23] give us that the Levi factors are actually 3-transitive permutation groups isomorphic to $\mathrm{PSL}_2(K_i)$ for some algebraically closed fields K_i $(i = 1, 2)$ acting on the corresponding projective lines. The rest of the proof can be copied from [33] noting that in the proof of [33, Lemma 24 i] "p-subgroup" has to be replaced by "quasiunipotent subgroup". □

We are still far from a complete classification of tame K^*-groups of small Prüfer 2-rank. In the following we will restrict ourselves to the case where $pr(G) = 2$ and the centralizers of four-subgroups are minimal in the following sense.

Proposition 4.2 *Let G be a simple K^*-group of odd type that does not interpret any bad field. Assume that $pr(G) = 2$ and let D be the four-subgroup which is contained in the connected component of a Sylow 2-subgroup S of G. Set $O_D := \bigcap_{l \in D^*} O(C_G(l))$. If $T_0 := C_G(D)^\circ/O_D \cong K^* \times K^*$ for some algebraically closed field of characteristic not 2, then $C_G(i)^\circ/O(C_G(i))$ is isomorphic to one of the following groups for any $i \in D^*$.*

(i) $K^* \times K^*$.

(ii) $\mathrm{GL}_2(K)$

(iii) $\mathrm{PSL}_2(K) \times K^* \cong \mathrm{GL}_2(K)/\langle -I \rangle$ *where* $-I = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

(iv) $\mathrm{SL}_2(K) * \mathrm{SL}_2(K)$ *where the two copies of* $\mathrm{SL}_2(K)$ *intersect non-trivially.*

If $C_G(i)^\circ/O(C_G(i))$ is isomorphic to one of the groups in (iii) or (iv), then $O(C_G(l)) = 1$ for all $l \in D^*$.

Proof. Let $i \in D^*$, then $C := C_G(i)^\circ/O(C_G(i))$ is a central product of an abelian divisible group T and a semisimple group H all of whose components are simple algebraic groups over algebraically closed fields of characteristic different from 2 by Fact 3.9. Furthermore $pr(C) = 2$ by Lemma 3.11 and $pr(H) = pr(C) - pr(T)$ by Lemma 3.12. Thus H is the central product of simple algebraic groups of Prüfer 2-rank less than or equal to 2 by [42, 27.5].

Set $C_k := C_G(k)$ and $O_k := O(C_k)$ for all $k \in I(G)$. Let θ be the signalizer functor defined by $\theta(s) := O_s$ for all $s \in I(G)$. Then $O_i \cap C_j = O_j \cap C_i = O_j \cap O_i = O_D$ for all $j \in D^*$, $j \neq i$. Hence

$$C_i \cap C_j/O_D \cong (C_i \cap C_j)O_i/O_i \cong (C_i \cap C_j)O_j/O_j.$$

Thus by [3, 2.52] $(C_i \cap C_j)/O_D \cong C_{C_i/O_i}(jO_i) \cong C_{C_j/O_j}(iO_j)$. This implies that $T \leq C_C(jO_i) \cong C_G(D)/O_D = T_0$ and either $T = 1$, $T \cong K^*$ or $T \cong T_0$, since T is connected and G does not interpret a bad field.

Thus (i) holds, if $pr(T) = 2$, as in this case $H = 1$ and $T \cong T_0$. If $pr(T) = 1$, then $T \cong K^*$ and $pr(H) = 1$. Hence H is of type $A_1(K)$, i.e. $H \cong \mathrm{SL}_2(K)$ or $H \cong \mathrm{PSL}_2(K)$. If $C = H \times T$, then $H \cong \mathrm{PSL}_2(K)$, as $C_C(jO_i) \cong T_0$ for any involution $j \in H$. Thus $C \cong \mathrm{GL}_2(K)/\langle -I \rangle$ in this case. If on the other hand $C = H * T$, where $H \cap T$ is non-trivial, then $H \cong \mathrm{SL}_2(K)$ and $C \cong \mathrm{GL}_2(K)$.

If finally $pr(H) = 2$, then T is trivial by Lemma 3.12 and H is of type $A_1(K) \times A_1(K)$, $A_2(K)$, $C_2(K)$ or $\mathrm{G}_2(K)$. However, H has to contain a central involution. Thus H cannot be of type $A_2(K)$ or $\mathrm{G}_2(K)$ and it cannot be isomorphic to $\mathrm{PSp}_4(K)$. As furthermore $C_C(jO_i) \cong T_0$ for any $j \in D \backslash \langle i \rangle$, H cannot be isomorphic to $\mathrm{Sp}_4(K)$ either. Hence H is of type $A_1(K) \times A_1(K)$, contains the central involution i and $C_C(jO_i) \cong T_0$ for any other involution j. Especially $C \cong \mathrm{SL}_2(K) * \mathrm{SL}_2(K)$, where the two copies of $\mathrm{SL}_2(K)$ intersect in $\langle i \rangle$.

If C is isomorphic to the group in (iii) or (iv), then $C_G(i)^\circ$ contains an elementary abelian subgroup E of order 8 which contains D by Lemma 3.10 as C does. Thus $O(C_G(i)) = 1$ by Corollary 3.16. □

We expect that all simple tame K^*-groups of odd type and Prüfer 2-rank 2 fulfill the assumptions of Proposition 4.2.

Conjecture 7 *Let G be a simple tame K^*-group of odd type and Prüfer 2-rank 2. Let $i \in G$ be any involution and $C := C_G(i)^\circ/O(C_G(i))$.*

(1) If $C \cong \mathrm{GL}_2(K)$, then $G \cong \mathrm{PSL}_3(K)$

(2) If $C \cong \mathrm{PSL}_2(K) \times K^*$, then $G \cong \mathrm{PSp}_4(K)$.

(3) If $C \cong \mathrm{SL}_2(K) * \mathrm{SL}_2(K)$, where the two copies of $\mathrm{SL}_2(K)$ intersect non-trivially, then $G \cong \mathrm{PSp}_4(K)$ or $G \cong \mathrm{G}_2(K)$.

Furthermore one of these three cases holds.

We are going to prove cases (2) and (3) of the conjecture. We furthermore have a partial result of case (1), if $O(C_G(i)) = 1$. To prove the complete case (1) seems to be extremely challenging and one will probably need new methods. It should furthermore be difficult to exclude case (i) from Proposition 4.2, as we do not have any information about normalizers of maximal tori and conjugacy classes of involutions in this case.

4.1 $\mathrm{PSL}_3(K)$

The aim of this section is to prove the following result which is a partial analog to the result in finite group theory by Brauer [22] and a first step in proving case (1) of Conjecture 7. The main difficulty will probably be to show that cores of centralizers of involutions of a group G are trivial, if G does not contain an elementary abelian subgroups of order 8.

Theorem 4.3 *Let G be a simple K^*-group of finite Morley rank that does not interpret a bad field. Assume that the centralizers of involutions of G are isomorphic to $\mathrm{GL}_2(K)$ for some algebraically closed field K of characteristic not 2. Then G is isomorphic to $\mathrm{PSL}_3(K)$, if there exists an involution i and a quasiunipotent subgroup $U \leq C_G(i)$ which is maximal in $C_G(i)$ but not maximal in G.*

We strongly believe, that G is always isomorphic to $\mathrm{PSL}_3(K)$ and this is the result one would need for the classification program. At the moment we just have the following partial information.

Proposition 4.4 *Let G be a simple K^*-group of finite Morley rank that does not interpret a bad field. Assume that the centralizers of involutions of G are isomorphic to $\mathrm{GL}_2(K)$ for some algebraically closed field K of characteristic not 2 and that a maximal quasiunipotent subgroup $U \leq C_G(i)$ is maximal in G for some $i \in I(G)$. Set $f := rk(Z(C_G(i))$.*

(i) $C_G(x)^\circ$ is abelian for all $1 \neq x \in G \backslash I(G)$.

(ii) Either $G = \bigcup_{i \in G} C_G(i)$ and $rk(G) = 8f$ or there exists a maximal quasiunipotent group V which is not conjugate to U such that $rk(G) = rk(U) + 7f + r$ for some $0 \leq r \leq f$ and furthermore $8f < rk(G) < 11f$ in this case.

4.1.1 Basic results

Let G be a group as in Theorem 4.4. Let S be a Sylow 2-subgroup of G. By [18, 6.22] S contains a central involution k and hence $S \leq C_k$. Let D be a four-subgroup in S°. Since $C_G(l)$ contains only two conjugacy classes of involutions for every $l \in D^*$, all involutions in D must be conjugate and $N_G(D)/C_G(D) \cong S_3$. D is characteristic in S° and Sylow 2-subgroups of groups of finite Morley rank are conjugate. Thus four-subgroups in the connected component of a Sylow 2-subgroup must be conjugate to D and hence all four-subgroups of G are conjugate to each other.

Proposition 4.5 *$G = \langle C_G(l) | l \in D^* \rangle$ and $Z(C_G(i)) \cap Z(C_G(j)) = 1$ for $i, j \in D^*$ and $i \neq j$.*

Proof. $G = \langle C_G(l) | l \in D^* \rangle$ by Corollary 3.17. Since j and ij are conjugate in $C_G(i)$, $Z(C_G(i)) \cap Z(C_G(j)) = Z(C_G(i)) \cap Z(C_G(ij)) = Z(G) = 1$. □

Let $T := C_G(D)$ and U a quasiunipotent subgroup of G that is normalized by T. Then $U = \langle C_U(l)^\circ | l \in D^* \rangle$ due to [19, 4.6] and U is called *n-dimensional* where $n = |\{l \in D^* | C_U(l) \neq 1\}|$. There are exactly 6 one-dimensional unipotent subgroups which are normalized by T, since there are exactly two in $C_G(l)$ for each $l \in D^*$. Furthermore $N_G(T)$ acts transitively on them. Assume that $D = \langle i_0, i_1 \rangle$ and let $X \leq C_G(i_0)$ be a one-dimensional quasiunipotent subgroup which is normalized by T. Let $i_2 := i_0 i_1$ and write $\overline{x} := xT$ for all $x \in N_G(T)$.

Lemma 4.6 *(i) $W := N_G(T)/T \cong S_3$ is a finite group of order 6, which is generated by $\overline{w}_1$ and $\overline{w}_2$, where w_n is an involution in $N_G(T) \backslash T \cap C_G(i_n)$ for $n = 1, 2$. The other elements of W are $\overline{1}$, $\overline{w}_0 = \overline{w}_1^{\overline{w}_2} = \overline{w}_2^{\overline{w}_1}$, $\overline{y} = \overline{w}_2 \overline{w}_1$ and $\overline{y}^2 = \overline{y}^{-1} = \overline{w}_1 \overline{w}_2$.*

(ii) $w_0 T X w_0 \subseteq T X w_0 X$.

(iii) $\langle T, X, X^{w_0} \rangle = C_G(i_0)$.

Proof. (i) follows directly from the definitions. As $C_G(i_0)$ is a reductive algebraic group of rank 1, it has a BN-pair (B_1, N_1), where $B_1 := TX$ and $N_1 = \langle w_0, T \rangle$. Hence $w_0 T X w_0 \subseteq TX \cup T X w_0 X = T X w_0 X$ and $C_G(i_0) = \langle B, N \rangle = \langle T, X, X^{w_0} \rangle$ which proves (ii) and (iii). □

Lemma 4.7 *Let $X_1 := X$, $X_2 := X_1^{w_0}$ and $X_n^{(\lambda)} := X_n^{y^\lambda}$ for any $n = 1, 2$ and $\lambda \in \mathbb{Z}$. Then*

(i) $X_n^{(\lambda)} = X_n^{(\lambda+3)}$ for all $n = 1, 2$ and $\lambda \in \mathbb{Z}$.

(ii) $(X_1^{(\lambda)})^{w_\kappa} = X_2^{(2\lambda-\kappa)}$ *for* $\kappa, \lambda = 0, 1, 2$.

(iii) i_λ *centralizes* $X_n^{(\lambda)}$ *and inverts* $X_n^{(\lambda-1)}$ *and* $X_n^{(\lambda+1)}$ *for* $\lambda = 0, 1, 2$ *and* $n = 1, 2$.

Proof. Since X is normalized by T and $N_G(T)/T \cong S_3$, (i) follows. Furthermore $\overline{y}$ is inverted by $\overline{w}_\lambda$ for $\lambda = 0, 1, 2$, $\overline{y^\lambda} = \overline{w_\lambda w_0}$ and hence

$$\overline{y^\kappa w_\lambda y^{\lambda-2\kappa} w_0} = \overline{y^{3\kappa-\lambda} w_\lambda w_0} = \overline{y^{-\lambda} y^\lambda} = \overline{1}$$

for $\lambda, \kappa = 0, 1, 2$ which proves (ii). Elementary computations in $\mathrm{GL}_2(K)$ show finally that i_0 centralizes X_n and that i_1, i_2 invert X_n for $n = 1, 2$. □

By Proposition 2.18 there exists a maximal quasiunipotent subgroup U of G that contains X_1 and is normalized by T. There are only four possible cases.

Lemma 4.8 *Let* U *be a maximal quasiunipotent subgroup of* G *that contains* X_1 *and is normalized by* T*. Then one of the following holds.*

(1) U *is 3-dimensional.*

  (a) $Z(U)$ *is 3-dimensional. Then* $U = X_1 X_1^{(1)} X_1^{(2)}$

  (b) $Z(U)$ *is 1-dimensional. Without loss of generality* $Z(U) = X_1$ *and* $U = X_1\langle X_2^{(1)}, X_2^{(2)}\rangle$.

(2) U *is 2-dimensional. We may assume that* $U = X_1 \times X_2^{(2)}$.

(3) U *is 1-dimensional and* $U = X_1$.

Proof. $U = \langle C_U(l)^\circ | l \in D^*\rangle$ due to [19, 4.6]. Thus U is generated by at k one-dimensional quasiunipotent subgroups for $1 \le k \le 3$ as T acts transitively on $X_1 \backslash \{1\}$. As U is nilpotent, $Z(U)$ is infinite and $Z(U)^\circ = \langle C_{Z(U)}(l)^\circ | l \in D^*\rangle$ by [19, 4.6] again. As furthermore T acts transitively on $X \backslash \{1\}$, either $C_{Z(U)}(l)^\circ = C_U(l)^\circ$ or $C_{Z(U)}(l)^\circ = 1$ for all $l \in D^*$. We may assume that $X_1 \le Z(U)$ by conjugating with an element from $N_G(T)$.

If U is 1-dimensional, then obviously $U = X_1$. Let thus U be at least 2-dimensional. If $X_1^{(\lambda)} \le U$ for some $\lambda = 1, 2$, then $X_1 = X_1^{\lambda-\lambda} \le C_G(X_1^{-\lambda})$ and $X_1^{(k)} \le C_G(X_1)$ for all $k = 0, 1, 2$. Hence $(X_2^k) \cap U = 1$ for all $k = 0, 1, 2$, since otherwise $w_k \in C_G(i_k) \le N_G(X_1)$ by Lemma 4.6. Thus $U = X_1 X_1^{(1)} X_1^{(2)}$ in this case and $Z(U)$ is 3-dimensional.

Assume therefore that $X_1 < U \le X_1\langle X_2^{(1)}, X_2^{(2)}\rangle$. If U is 2-dimensional, then $U = X_1 \times X_2^{(k)}$ for some $k = 1, 2$ and we are in case (2). If U is 3-dimensional, $U = X_1\langle X_2^{(1)}, X_2^{(2)}\rangle$. These are all possible cases. □

Lemma 4.9 *If X_1 centralizes $Y := \langle X_2^{(1)}, X_2^{(2)}\rangle$, then $Y^{w_k} \subseteq TYw_kX_2^{(k)}$ for $k = 1, 2$.*

Proof. Let $k \in \{1, 2\}$. Since X_1 is connected there exists $n \in \mathbb{N}$ such that $Y = (X_2^{(k)}X_2^{(-k)})^n$ by Zil'bers indecomposability theorem [18, 5.28]. Set $Y_m = (X_2^{(k)}X_2^{(-k)})^m$ for all $1 \leq m \leq n$. We proceed by induction on m. Then by Lemma 4.7 and Lemma 4.6

$$(Y_1)^{w_k} = X_1^{(2k-k)}X_1^{-2k-k} = X_1^{(k)}X_1 \subseteq TX_2^{(k)}w_kX_2^{(k)}X_1.$$

Since X_1 centralizes $X_2^{(k)}$ by assumption

$$Y_1^{w_k} \subseteq TX_2^{(k)}X_1^{w_k}w_kX_2^{(k)} = TY_1w_kX_2^{(k)}.$$

Furthermore by induction hypothesis

$$Y_{m+1}^{w_k} = Y_mX_2^{(k)}X_2^{(-k)} \subseteq T(Y_mw_kX_2^{(k)})(X_2^{(k)}X_2^{(-k)}w_kX_2^{(k)})$$

and hence

$$Y_{m+1}^{w_k} \subseteq TY_mY_1^{w_k}X_2^{(k)} \subseteq TY_{m+1}w_kX_2^{(k)}$$

which gives us the claim. □

Theorem 4.10 *Assume that there exists a maximal quasiunipotent Q of G which is normalized by T and 3-dimensional and non-abelian. Then G is a split BN-pair of Tits rank 2, where $B = N_G(Q)^\circ$, $N := N_G(T)$ and $\overline{w_1}, \overline{w_2}$ are generators of the Weyl group.*

Proof. We may assume by Lemma 4.8 that $Q = X_1Y$, where X_1 centralizes $Y = \langle X_2^{(1)}, X_2^{(2)}\rangle$. Then $B = Q \rtimes T$ by Proposition 2.20 and $B \leq N_G(Z(Q)) = N_G(X_1)$. We first show BN1. $G = \langle C_G(k)^\circ |\ k \in D^*\rangle$ by Proposition 4.5. As $\langle N, X_1\rangle \geq C_G(i)^\circ$ by Lemma 4.6 and N operates transitively on D^*, $G = \langle B, N\rangle$. Furthermore $B \cap N = T \lhd N$, since $B = Q \rtimes T$, as desired. BN2 follows from the fact that $\langle \overline{w}_1, \overline{w}_2\rangle = N_G(T)/T$ by Lemma 4.7. Let $S := \{\overline{w}_1, \overline{w}_2\}$ and $W := N/T$.

We prove BN3. We have to show that $vBw \subseteq BvwB \cup BvB$ for all $v, w \in N$ such that $\overline{v} \in W$ and $\overline{w} \in S$. By Lemma 4.9 and Lemma 4.7

$$w_1B = TX_1^{w_1}Y^{w_1}w_1 \subseteq TX_2^{(2)}Yw_1X_2^{(1)}w_1 = TX_2^{(2)}YX_1^{(1)} \subseteq BX_1^{(1)}$$

and

$$w_2B = TX_1^{w_2}Y^{w_2}w_2 \subseteq TX_2^{(1)}YX_1^{(2)} \subseteq BX_1^{(2)}.$$

Hence

$$\begin{array}{rcl} w_1Bw_1 & \subseteq & Bw_1(X_1^{(1)})^{w_1} = Bw_1X_2^{(1)} \subseteq Bw_1B, \\ w_1By^2 & \subseteq & By^2(X_1^{(1)})^{y^2} = By^2X_1 \subseteq By^2B, \\ w_1Bw_0 & \subseteq & Bw_0(X_1^{(1)})^{w_0} = Bw_0X_2^{(2)} \subseteq Bw_0B \end{array}$$

as well as

$$\begin{array}{rcl} w_2Bw_2 & \subseteq & Bw_2(X_1^{(2)})^{w_2} = Bw_2X_2^{(2)} \subseteq Bw_2B, \\ w_2By & \subseteq & By(X_1^{(2)})^{y} = ByX_1 \subseteq By^2B, \\ w_2Bw_0 & \subseteq & Bw_0(X_1^{(2)})^{w_0} = Bw_0X_2^{(1)} \subseteq Bw_0B \end{array}$$

proving BN3 in these cases. For the other cases just note that

$$w_1By = (w_1Bw_1)w_0 \subseteq B(w_1Bw_0) \subseteq Bw_0B = Bw_1yB$$

and

$$w_1Bw_2 = (w_1Bw_1)y^2 \subseteq B(w_1By^2) \subseteq By^2B = Bw_1w_2B$$

as well as

$$w_2By^2 = (w_2Bw_2)w_0 \subseteq B(w_2Bw_0) \subseteq Bw_0B = Bw_2y^2B$$

and

$$w_2Bw_1 = (w_2Bw_2)y \subseteq B(w_2By) \subseteq ByB = Bw_2w_1B$$

yielding the claim as $wB1 \subseteq Bw1B$ for all $w \in N$.

We finally prove BN4. Assume that $B = B^{w_k}$ for some $k = 1, 2$. Then $(X_2^{(k)})^{w_k} = X_1^{(k)} \leq B \leq N_G(X_1)$ and $w_k \in C_G(i_k) \leq N_G(X_1)$. Contradiction. Hence $B \neq B^{w_k}$ for $k = 1, 2$ and we have proved everything. □

4.1.2 3- and 2-dimensional case

Assume from now on that all maximal quasiunipotent subgroup of G that are normalized by T are abelian. We are first going to show that U cannot be 2-dimensional.

We call $t \in T$ *regular point of* T iff $C_G(t) = T$ and denote the set of regular points by $R(T)$. An element $g \in G$ is called *regular point* iff it is conjugate to an element of $R(T)$. Set furthermore $T[w_k] := \{t \in T |\ t^{w_k} = t^{-1}\}$ for all $k = 0, 1, 2$.

Lemma 4.11 *$R(T)$ is a generic subset of T. In particular there are 3 different kinds of points in T.*

(a) The set of regular points $R(T)$.

(b) The set of central points $X := \bigcup_{l \in D^*} Z(C_G(l))$.

(c) The finite group $C_T(y)$, where $y \in N_G(T)$, such that $y^3 \in T$.

Finally, $C_G(t) = T\langle y \rangle$ for $t \in C_T(y)$.

Proof. Let $t \in T \backslash X$. Then $C_G(t)^\circ = \langle C_{C_G(t)}(l)^\circ | l \in D^* \rangle$ by [19, 5.14]. Since $t \notin X$, $C_G(t) \cap C_G(l) = T$ for $l \in D^*$ and hence $C_G(t)^\circ = T$. Let $x \in C_G(t) \backslash T$. Then $x \in N_G(T)$. However $x \notin I(N_G(T))$, since for $x \in I(N_G(T))$: $C_G(x) \cap T \subseteq X$. Thus $t \in C_T(y) \cup R(T)$ and $C_G(t) = T\langle y \rangle$ for $t \in C_T(y)$.

We finally show that $C_T(y)$ is a finite group. Let $t \in C_T(y)$. We may assume that $y = w_2 w_1$. Then

$$(tt^{w_2})^y = tt^{w_1} \in Z(C_G(i_2))^y \cap Z(C_G(i_1)) = Z \cap Z(C_G(i_1)) = 1$$

by Proposition 4.5. Hence $t^{w_2} = t^{w_1} = t^{-1}$ and $C_T(y) \leq T[w_1]$. As $T[w_1] \cong K^*$ and G does not interpret a bad field, $C_T(y)$ is either finite or equals $T[w_1]$. However $C_T(y) < T[w_1]$ since $i_1 \notin C_T(y)$ and the claim follows. □

Lemma 4.12 *Let $H \leq C_G(i_0)$ be a definable subgroup that contains T. Then either $H = T$, $H = X_1 T$, $H = X_2 T$ or $H = C_G(i_0)$.*

Proof. First assume that H is solvable. Then $T \leq H$ is contained in a Borel subgroup – in the sense of algebraic group theory – of $C_G(i_0)$ by [42, 23.1]. There are exactly two of them, namely $X_1 T$ and $X_2 T$. Since T operates transitively on $X_n \backslash \{1\}$ for $n = 1, 2$ either $H = T$ or $H = X_n T$ for $n = 1, 2$. If H is non-solvable then H° / σ is isomorphic to $\mathrm{PSL}_2(K)$ for an algebraically closed field K where σ is the solvable radical of H° by [2]. Since σ is solvable and normalized by H, $\sigma = Z(C_G(i_0))$ which forces H to be equal to $C_G(i_0)$. □

Proposition 4.13 *There is a maximal quasiunipotent subgroup V of G that is normalized by T such that $C_G(X_1) = V \rtimes Z(C_G(i_0))$.*

Proof. Set $Z := Z(C_G(i_0))$. We show first that $C_G(X_1)^\circ = V \rtimes Z$. Let V be a maximal quasiunipotent subgroup that is normalized by T and contains X_1. V exists by Proposition 2.18. V is – as maximal quasiunipotent subgroup normalized by T – abelian and hence contained in $C_G(X_1)$. On the other hand

$N_G(X_1)^\circ = \langle N_k |\ k = 0,1,2\rangle$ by [19, 5.14], where $N_k := C_{N_G(X_1)}(i_k)^\circ$ for $k = 0,1,2$. Let $k \in \{0,1,2\}$. Since $X_1^{w_k} = X_2^{(-k)}$ by Lemma 4.7, $T \leq N_k < C_G(k)$. Thus either $N_k = T$ or $N_k = TX_n^{(k)}$ for $n = 1$ or $n = 2$ by Lemma 4.12. Especially $N_G(X_1)^\circ \leq TX_1\langle X_n^{(1)}, X_n^{(2)}\rangle$ for $n = 1,2$ by Lemma 4.8.

We show that $N_G(X_1^\circ)$ is solvable. Assume that $N_G(X_1)^\circ$ is not solvable. Then $N_G(X_1)^\circ = TX_1\langle X_2^{(1)}, X_2^{(2)}\rangle$ by Lemma 4.8. Let σ be the solvable radical of $N_G(X_1)^\circ$. Then $X_1 \leq \sigma$. $\overline{N} := N_G(X_1)^\circ/\sigma$ is the direct product of simple algebraic groups over algebraically closed fields by [2], i.e. $\overline{N} \cong PSL(2,K)$, as G does not interpret any bad field. Let S be the Sylow 2-subgroup of T. Then $S\sigma/\sigma \cong S/(\sigma \cap S)$ is a Sylow 2-subgroup of $\overline{N}$ by Lemma 3.11. As $pr(T) = 2$ and $pr(\overline{N}) = 1$, this implies that $\sigma \cap S$ is infinite and hence that $T_0 := (\sigma \cap T)^\circ \cong K^*$, as T does not interpret a bad field. $\sigma^\circ = X_1 \rtimes T_0 \leq C_G(i_0)^\circ$ is normalized by $X_2^{(k)}$ for $k = 1,2$. Thus $T_0^g \leq C_G(i_0)^\circ$ for any $g \in N_G(X_1)^\circ$ and hence $i_0^{X_2^{(1)}} \cup i_0^{X_2^{(2)}} \subseteq C_G(T_0)$. This implies by Lemma 4.11 that $T_0 \leq Z(C_G(i_1)) \cap Z(C_G(i_2))$. Contradiction, as $Z(C_G(i_1)) \cap Z(C_G(i_2)) = 1$ by Proposition 4.5.

Hence $N_G(X_1)^\circ$ is solvable and V is normal in $N_G(X_1)^\circ$ by Proposition 2.16. Thus $N_G(X_1)^\circ \leq N_G(V)^\circ = V \rtimes T$ by Proposition 2.20 and $N_G(X_1)^\circ = V \rtimes T$. Especially $C_G(X_1)^\circ = V \rtimes (T \cap C_G(X_1)^\circ) = V \rtimes Z$.

We finally claim that $C_G(X_1)$ is connected. Let $x \in C_G(X_1)$. Then $X_1 \leq C_G(i_0^x)$ and hence

$$(*) \quad i_0^x \in Z(C_G(i_0^x)) \leq C_G(X_1)^\circ = V \rtimes Z.$$

Since $Z \cap Z(C_G(i_k)) = 1$ for $k = 1,2$ by Proposition 4.5, Z acts freely on $X_n^{(k)} \backslash \{1\}$ for $n,k = 1,2$. Thus $X_n^{(k)} \rtimes Z = X_n^{(k)} \cup \bigcup_{u \in X_n^{(k)}} Z^u$ for $n,k = 1,2$ by [18, ex.11, p.98]. As V is abelian, this gives us that $V \rtimes Z = V \cup \bigcup_{u \in V} X_1 Z^u$. By $(*)$ $i_0^x \in VZ$ and as i_0^x is an involution it cannot be contained in V. This means that $i_0^x \in X_1 Z^v$ for some $v \in V$. However, X_1 is a $2^\perp$-group that is centralized by Z^v and thus $i_0^x \in Z^v = Z(C_G(i_0^v))$. Hence $i_0^x = i_0^v$ and $vx^{-1} \in C_G(i_0) \cap C_G(X_1) = ZX_1 \leq C_G(X_1)^\circ$. Especially $x \in C_G(X_1)^\circ$ and the claim is proved. □

Corollary 4.14 X_1 *is contained in exactly one maximal quasiunipotent subgroup, namely* $Q(C_G(X_1))$.

Proof. $V := Q(C_G(X_1))$ is a maximal quasiunipotent subgroup that contains X_1 by Proposition 4.13. Let $W \geq X_1$ be another maximal quasiunipotent subgroup of G. As W is nilpotent, $Z(W)$ is infinite by [18, 6.2]. Then $1 \neq Z(W)^\circ \leq Q(C_G(X_1)) = V$ and since V is abelian, $V, W \leq C_G(Z(W)^\circ)$. As $C_G(Z(W)^\circ)$ is a K-group, V and W are conjugate by Proposition 2.16. Thus W is abelian as well and $W = Z(W)^\circ \leq V$. By the maximality of W, $V = W$. □

Theorem 4.15 *Let U be a maximal quasiunipotent subgroup of G that is normalized by T. Then U is not 2-dimensional.*

Proof. Assume that U is 2-dimensional. Thus without loss of generality $U = X_1 \times X_2^{(2)}$ by Lemma 4.8 and U is normalized by $w_1 \in C_G(i_1)$. Let $V = C_U(w_1)$. Then $V = \{uu^{w_1} | \, u \in X_1\}$. Furthermore since U is the direct product of $X_1, X_2^{(2)}$ there is a definable bijection $\phi : X_1 \longrightarrow V$ where $\phi(u) = uu^{w_1}$. Hence V is connected and $rk(V) = rk(X_1)$. Thus V is a maximal quasiunipotent subgroup of $C_G(w_1)$ and

$$w_1 \in C_G(V) = U \rtimes Z(C_G(w_1)) \leq N_G(U)^\circ$$

by Proposition 4.13. However $N_G(U)^\circ = U \rtimes T$ by Proposition 2.20. Thus $w_1 = u_0 u_2 t$ for $u_0 \in X_1$, $u_2 \in X_2^{(2)}$, $t \in T$ and $i_2 = i_0^{w_1} = i_0^{u_2 t}$. Since $u_2 t \in C_G(i_2)$ we conclude that $i_0 = i_2$. Contradiction. □

It is slightly more difficult to show that U is not 3-dimensional.

Lemma 4.16 *Let $i \in I(G)$ be an involution of G. Then*

(i) $N_G(C_G(i)) = C_G(i)$,

(ii) $C_G(z) = C_G(i)$ *for any* $z \in Z(C_G(i))$ *and*

(iii) the only strongly real element in $Z(C_G(i))$ *is* i.

Proof. Let $i \in I(G)$. If $x \in N_G(C_G(i))$ then $C_G(i) = C_G(i^x)$ and since $I(Z(C_G(i))) = \{i\}$, $i = i^x$ and $x \in C_G(i)$. Let furthermore $z \in Z(C_G(i))$. Then $C_G(z)^\circ = \langle C_{C_G(z)}(l)^\circ | \, l \in D^* \rangle$ by [19, 5.14]. Let $l \in D^* \backslash \{i\}$ then $z \notin Z(C_G(l))$ due to Proposition 4.5 and hence $(C_G(z) \cap C_G(l))^\circ = T \leq C_G(i)$ by Lemma 4.11. Thus $C_G(z)^\circ = C_G(i)$ and (i) implies that $C_G(z) = C_G(i)$. Let finally $x \in Z(C_G(i))$ be strongly real. Then there exists an involution $w \in I(G)$ such that $x^w = x^{-1}$, i.e. w normalises $C_G(x) = C_G(i)$ by (ii). Hence $w \in C_G(i)$ by (i) and $x = x^{-1}$ is an involution. □

Proposition 4.17 *Let $u \in X_1$ be a unipotent element and $z \in Z(C_G(i_0))$. Then $C_G(zu)^\circ$ is solvable and $C_G(u)^\circ = C_G(X_1)$*

Proof. Let $N := C_G(zu)^\circ$ and $Z := Z(C_G(i_0))$. Then $Z \leq N$. Furthermore N cannot contain a four-subgroup D, since $C_G(D)$ does not contain unipotent elements. Hence any Sylow 2-subgroups of N is connected and contains a single involution and N has Prüfer 2-rank 1. N contains thus only one conjugacy class of involutions as the Sylow 2-subgroups of N are conjugate. Let σ be the solvable radical of N and S a Sylow 2-subgroup of σ. By the Frattini argument [18, 10.12] $N = N_N(S)\sigma$. Assume that $S \neq 1$. Then $I(N) \leq \sigma$ and we may assume that $i_0 \in S$. Thus $N_N(S) = C_N(i_0) = X_1 \rtimes Z$ is solvable and $N = \sigma$.

We assume from now on that σ does not contain involutions. Let $\overline{N} := N/\sigma$. As $pr(\overline{N}) = 1$ by Lemma 3.11, $\overline{N} \cong \mathrm{PSL}_2(K)$ for some algebraically closed field K of characteristic not 2 by [2]. As σ is a $2^{\perp}$-group, $\overline{ZX_1} = \overline{C_N(i_0)} = C_{\overline{N}}(\overline{i}_0)$ by [3, 2.52]. The centralizers of involutions in $\mathrm{PSL}_2(K)$ where K is an algebraically closed field of characteristic not 2 are finite extensions of tori and thus $X_1 \leq \sigma$. As σ is solvable it contains a unique maximal quasiunipotent subgroup $Q(\sigma)$. Let V be a maximal quasiunipotent subgroup of G that contains $Q(\sigma)$. Then $X_1 \leq V^g$ for all $g \in N$ as $X_1 \leq Q(\sigma)$. Thus $V^g \leq C_G(X_1)$ for all $g \in N$ as V is abelian. However, $C_G(X_1) = V \rtimes Z$ by Proposition 4.13 and Corollary 4.14. Thus $V = V^g$ for all $g \in N$. Hence $N \leq N_G(V)^\circ = V \rtimes T$ by Proposition 2.20 and N is solvable. Contradiction.

Let $z = 1$, then $N = C_G(u)^\circ \geq C_G(X_1) = V \rtimes Z$. As N is solvable, $V = Q(N)$ by Proposition 2.16. Thus $N \leq N_G(V)^\circ = V \rtimes Z$ by Proposition 2.20 which implies the claim. □

Remark 4.18 *Let $g \in C_G(i)$ for some $i \in I(G)$, then g is conjugate to an element in T or $Z(C_G(i_0))X_1$.*

Proof. As G has one conjugacy class of involutions, we may assume that $g \in C_G(i_0)$. As $C_G(i_0)$ is isomorphic to a connected algebraic group all elements of $C_G(i_0)$ are conjugate to an element in the Borel-subgroup $B = X_1T$ of $C_G(i_0)$. However $B = Z(C_G(i_0))X_1 \cup \bigcup_{u \in X_1} T^u$ of $C_G(i_0)$ and we are done. □

Corollary 4.19 *Let $g \in G$. Then either $C_G(g) = C_G(i)$ for some $i \in I(G)$ or $C_G(g)^\circ$ is solvable.*

Proof. If $C_G(g)$ is a $2^{\perp}$-group, then $C_G(g)^\circ$ is nilpotent by [18, B1]. Hence we may assume that $g \in C_G(i)$ for some $i \in I(G)$. Then g is conjugate to an element in T or $Z(C_G(i_0)X_1$ by Remark 4.18. Thus either $g \in Z(C_G(k))$ for some $k \in I(T)$ and $C_G(g) = C_G(i)$ by Lemma 4.16 or $C_G(g)^\circ$ is solvable by Proposition 4.17 and Lemma 4.11 □

Lemma 4.20 *Let N be a nilpotent $2^{\perp}$-group of finite Morley rank and w a definable involutive automorphism. Let $V \leq N$ be an abelian group such that $V \cap V^w = 1$. Then $rk(C_N(w)) \geq rk(V)$.*

Proof. Without loss of generality $N = \langle V, V^w\rangle$. The proof proceeds by induction on the nilpotency class of N.

If N is abelian, $W := \{vv^w \mid v \in V\} \subseteq C_N(w)$. Then N is the direct product of V and V^w and we get a definable bijection $\phi : X_1 \longrightarrow V$ by $\phi(u) = uu^{w_1}$. Hence W is connected and $rk(V) = rk(W) \leq rk(C_N(w))$.

Let now $Z := Z(N)$ and denote by $\overline{X} := XZ/Z$ for all $X \leq N$. Since V is abelian, VZ is abelian as well and we can apply the first part of the proof to $VZ \cap V^w \leq VZ \cap V^wZ$. Hence

$$(*) \quad rk\big(C_{VZ\cap V^wZ}(w)\big) \geq rk(VZ \cap V^w).$$

Furthermore since $\overline{V} \cap \overline{V}^w \lhd \overline{N}$ and $\big(\overline{V}/(\overline{V}\cap\overline{V}^w)\big) \cap \big(\overline{V}^w/(\overline{V}\cap\overline{V}^w)\big) = 1$, we get by induction hypothesis and Lascar's equality

$$(**) \quad rk\big(C_{\overline{N}/(\overline{V}\cap\overline{V}^w)}(w)\big) \geq rk\big(\overline{V}/(\overline{V}\cap\overline{V}^w)\big) = rk\big(VZ/(VZ\cap V^wZ)\big).$$

Since N is a $2^{\perp}$-group [3, 2.44] implies that

$$rk(C_{\overline{N}}(w)) = rk(\overline{C_N(w)}) = rk(C_N(w)) - rk(C_Z(w))$$

and using the same argument again

$$\begin{aligned} rk(C_{\overline{N}/(\overline{V}\cap\overline{V}^w)}(w)) &= rk(C_{\overline{N}}(w)) - rk(C_{\overline{V}\cap\overline{V}^w}(w)) \\ &= rk(C_N(w)) - rk(C_{VZ\cap V^wZ}(w)). \end{aligned}$$

Therefore

$$\begin{aligned} rk(C_N(w)) &= rk(C_{\overline{N}/(\overline{V}\cap\overline{V}^w)}(w)) + rk(C_{VZ\cap V^wZ}(w)) \\ &\geq rk(VZ) - rk(VZ\cap V^wZ) + rk(VZ\cap V^w) \end{aligned}$$

by $(*)$ and $(**)$. As $VZ \cap V^wZ = (VZ\cap V^w)Z$, [18, ex.18, p.66] implies that

$$\begin{aligned} rk(VZ\cap V^wZ) &= rk(VZ\cap V^w) + rk(Z) - rk(V^w \cap Z) \\ &= rk(VZ\cap V^w) + rk(V^wZ) - rk(V) \end{aligned}$$

and $rk(C_N(w)) \geq rk(VZ) + rk(V) - rk(V^wZ) = rk(V)$. □

Theorem 4.21 *Let $X_1 \leq U$ be a maximal quasiunipotent subgroup of G that is normalized by T. Then U is not abelian and 3-dimensional.*

Proof. Assume that U is abelian and 3-dimensional. Thus U is normalized by $y := w_2w_1$ as $U = X_1 \times X_1^{(1)} \times X_1^{(2)}$ by Lemma 4.8. Set $N := C_G(y)^{\circ}$. N is solvable by Corollary 4.19 since $y \in Sr(G)\backslash I(G)$ and hence cannot be contained in the center of $C_G(\lambda)$ for some $\lambda \in I(G)$ by Lemma 4.16. Let $V_1 = C_U(y)$, $V_2 = V_1^{w_1}$. Obviously $V_1 = \{uu^yu^{y^2} \mid u \in X_1\}$. Furthermore since U is the direct product of $X_1, X_1^{(1)}, X_1^{(2)}$ we get a definable bijection $\phi : X_1 \longrightarrow V_1$ via $\phi(u) = uu^yu^{y^2}$ and hence V_1 is quasiunipotent with $rk(V_1) = rk(X_1)$. Since $V_1, V_2 \leq Q(N)$ by Proposition 2.16 and $V_1 \cap V_2 \leq U \cap U^{w_1} = 1$, $rk(C_{Q(N)}(w_1)) \geq rk(V_1)$ by Lemma 4.20. As all quasiunipotent subgroups of centralizers of involutions are conjugate $rk(C_{Q(N)}(w_1)) = rk(V_1)$ and $V_3 := C_{Q(N)}(w_1) \leq Q(N)$ is a maximal quasiunipotent subgroup of $C_G(w_1)$. Let $W := Q(C_G(V_3))$ be the unique maximal quasiunipotent subgroup that contains V_3 as in Corollary 4.14. W is conjugate to U and thus abelian. Furthermore $Q(N) \leq W$ as $V_3 \leq Q(N)$ and hence $V_1, V_2 \leq W$. This implies that $V_2 \leq C_G(V_1)$.

As $C_G(V_1)$ is solvable by Corollary 4.19, it contains a unique maximal quasiunipotent subgroup which has to be $U = W$ by the maximality of U and W. Hence $V_2 \leq U$. Contradiction. □

This finishes the proof of Theorem 4.3 by Theorem 4.1 and Theorem 4.15.

4.1.3 1-dimensional case

Assume from now on, that all maximal quasiunipotent subgroup of G which are normalized by T are one-dimensional. We won't be able to exclude this case completely. However, there is a great deal of information available.

Proposition 4.22 $N_G(X_1) = X_1 \rtimes T$

Proof. $N_G(X_1)^\circ = C_G(X_1) = X_1 \times Z(C_G(i_0))$ by Proposition 4.13 and Proposition 2.20. Thus $C_G(X_1)$ is a connected normal abelian subgroup of $N_G(X_1)$. Furthermore $C_G(X_1) \cap C_G(i_1) = \langle i_0 \rangle$. As i_1 inverts X_1 by Lemma 4.7, i_1^n inverts X_1 for all elements $n \in N_G(X_1)$. Thus $i_1^{N_G(X_1)} \subseteq I(i_1C_G(X_1)) = i_1^{X_1} \cup i_0i_1^{X_1}$. Especially $[i_1, N_G(X_1)] \subseteq \langle i_0 \rangle X_1 \leq C_G(X_1)$. Hence $N_G(X_1) = C_G(X_1)C_{N_G(X_1)}(i_1)$ by [18, ex. 10, p. 98] and $C_{N_G(X_1)}(i_1)^\circ \leq C_G(X_1)$. Thus $C_{N_G(X_1)}(i_1) = T$ by Lemma 4.12 and the claim follows. □

Corollary 4.23 *Let $x \in C_G(X_1) \backslash Z(C_G(i_0))$. Then $C_G(x) = C_G(X_1)$.*

Proof. As $C_G(X_1)$ is abelian, $C_G(X_1) \leq C_G(x)$. Furthermore $C_G(x)^\circ$ is solvable by Proposition 4.17 and hence $C_G(x)^\circ \leq N_G(X_1) = X_1 \rtimes T$ by Proposition 2.16 and Proposition 4.22. This implies that $C_G(x) \leq N_G(X_1)$ as well and $C_G(x) = (X_1 \rtimes T) \cap C_G(x) = X_1 \rtimes (T \cap C_G(x)) = X_1 \rtimes Z(C_G(i_0)) = C_G(X_1)$. □

Lemma 4.24 *If $x \in C_G(i_0)\backslash\{1\}$, then either* *(i)* $C_G(x) < C_G(i_0)$ *is a connected abelian group,*

(ii) $C_G(x) = (T\langle y\rangle)^g$ *for some* $g \in C_G(i_0)$ *or*

(iii) $C_G(x) = C_G(k)$ *for some* $k \in I(C_G(i_0))$.

Proof. By Remark 4.18 we only have to prove the claim for elements of $Z(C_G(i_0))X_1$ and T. Let $x \in Z(C_G(i_0))X_1 \backslash Z(C_G(i_0))$. Then $C_G(x) = X_1 \rtimes Z(C_G(i_0))$ is a connected abelian group by Proposition 4.23. If $x \in T$, then the claim follows by Lemma 4.11. □

Let H be a group of finite Morley rank. A definable subset $X \subseteq H$ is called *generic* if $rk(X) = rk(H)$.

Proposition 4.25 *The definable set* $C := \bigcup_{k\in I(G)} C_G(k)$ *is generic in* G.

Proof. Consider the definable map $\phi : G \times C_G(i_0) \to C$ with $\phi(g, c) = c^g$. Let $c \in C_G(i_0)$ and compute the Morley rank of the fiber of c.

$$\begin{aligned}\phi^{-1}(c) &= \big\{(h, x) \in G \times C_G(i_0)|\ x^h = c\big\}\\ &= \big\{(h, x)|\ x := c^{h^{-1}} \in C_G(i_0),\ h \in G\big\}.\end{aligned}$$

Therefore

$$(*) \quad rk(\phi^{-1}(c)) = rk\big(\{h \in G|\ i_0^h \in C_G(c)\}\big) = rk\big(I(C_G(c)) + rk(C_G(i_0)\big)$$

since $i_0^{g_1} = i_0^{g_2}$ if and only if $g_1C_G(i_0) = g_2C_G(i_0)$. Consider the definable subset $Y := \big\{x \in C|\ rk(\phi^{-1}(x)) = rk(C_G(i_0))\big\}$.

Claim: $\phi^{-1}(Y)$ is generic in $G \times C_G(i_0)$.
By $(*)$ it is enough to show, that $W := \{x \in C_G(i_0)|\ rk(I(C_G(x))) = 0\}$ is a generic subset of $C_G(i_0)$. As $\bigcup_{x\in C_G(i_0)} R(T)^x \subseteq W$ and $R(T) \cap R(T)^x = \emptyset$ for all $x \in C_G(i_0)\backslash N_G(T)$, we have

$$rk(W) \geq rk(\bigcup_{x\in C_G(i_0)} R(T)^x) = rk(C_G(i_0)) + rk(R(T) - rk(T)) = rk(C_G(i_0))$$

by Lemma 4.11. □

By additivity of Morley rank this implies that

$$rk(G) + rk(C_G(i_0)) = rk(\phi^{-1}(Y)) = rk(Y) + rk(C_G(i_0)).$$

Thus $rk(C) \geq rk(Y) = rk(G)$ and C is generic in G. □ □

Remark 4.26 *The proof of Lemma 4.25 actually shows that the set of regular points is generic in G.*

Let $x \in G$. We call x *visible* iff $x \in \bigcup_{i\in I(G)} C_G(i)$ and *invisible* iff x is not visible. We call a definable connected subgroup $H \leq G$ *visible*, iff $H \leq C_G(i)$ for an involution $i \in I(G)$ and *invisible*, if $H\backslash\{1\}$ consists of invisible elements. Notice, that a connected definable subgroup consisting of visible elements need not be visible. $Inv(G)$ denotes the definable set of all invisible elements. We are going to show that all invisible elements are strongly real.

Proposition 4.27 *(i) Let $x \in G$ be visible. Then $C_G(x)^\circ$ is an infinite visible group.*

(ii) Let $x \in G$ be invisible. Then $C_G(x)^\circ$ is an infinite invisible group.

(iii) Let U be an infinite invisible group. Either $N_G(U)$ contains an involution i, in which case U is abelian and inverted by i, or $N_G(U)^\circ$ is invisible.

(iv) Let U be invisible. If there exists a strongly real element $ij \in U$ for some $i, j \in I(G)$, then U is abelian and inverted by i.

(v) Two maximal invisible groups are either equal or have trivial intersection.

(vi) $rk\big(\bigcup_{g\in G} U^g\big) = rk(G) - rk(N_G(U)/U)$ for any maximal invisible group U.

(vii) Invisible elements are strongly real, i.e. $Inv(G) \subseteq Sr(G)$.

Proof. (i) follows directly from Lemma 4.24.

(ii) Let $x \in G$ be invisible and $K := C_G(x)^\circ$. Then x^G consists of invisible elements and $rk(x^G) = rk(G) - rk(K)$. Since $\bigcup_{i\in I(G)} C_G(i)$ is generic in G by Proposition 4.25, $rk(K) > 0$ and K is infinite. Furthermore K is as a connected $2^\perp$-group nilpotent by [19, 5.8]. Assume that K contains a non-trivial visible element g. As $Z(K)$ is infinite by [18, 6.2], $1 \neq Z(K)^\circ \leq C_G(g)^\circ$ is visible by (i). Especially $K \leq C_G(Z(K)^\circ)$ is visible by (i) again. As K is thus a connected $2^\perp$-subgroup of $C_G(s)$ for some $s \in I(G)$, K is unipotent and $C_G(K)$ is connected by Proposition 4.23. Especially $C_G(K)$ is visible by (i). Contradiction to $x \in C_G(K)$.

(iii) Let U be an infinite invisible group. Assume that $N_G(U)$ contains an involution w. Since $C_U(w) = 1$, w inverts U by [18, ex.15, p.79] and U is an abelian group consisting of strongly real elements. Otherwise $N_G(U)^\circ$ is a connected $2^\perp$-group and therefore nilpotent by by [19, 5.8]. Then U contains infinitely many central elements of $N_G(U)^\circ$ by [18, ex.5, p.98] and $A := (U \cap Z(N_G(U)^\circ))^\circ$ is an infinite invisible group. Furthermore $N_G(U)^\circ \leq C_G(A)^\circ$ which proves the claim by (ii).

(iv) Let $i, j \in I(G)$ such that $ij \in U$. Then $1 \neq Z(U)^\circ \leq C_G(ij)^\circ$ by [18, 6.2]. As $C_G(ij)^\circ$ is invisible by (ii) and normalized by i, $C_G(ij)^\circ$ is inverted by i and abelian by (iii). Thus there exists an involution $k \in I(G)$ such that $ik \in Z(U)^\circ$. Especially $U \leq C_G(ik)^\circ$ is abelian and inverted by i as well.

(v) Let A and B be two maximal invisible groups and assume that $1 \neq g \in A \cap B$. Assume that A is abelian. Then $A = C_G(g)^\circ$ by (i) and the maximality of A. On the other hand $1 \neq Z(B)^\circ \leq C_G(g)^\circ$ by [18, 6.2] and $B = C_G(Z(B)^\circ)^\circ = A$ by (ii) and maximality of A and B again.

We may hence assume by (iv) that A and B do not contain strongly real elements. We are going to show that $A = B$. As before $1 \neq Z(A)^\circ \leq C_G(g)^\circ$ and hence $Z(C_G(g)^\circ)^\circ \leq C_G(Z(A)^\circ)^\circ = A$ by (i) and maximality of A. Using the same argument $Z(C_G(g)^\circ)^\circ \leq B$ and $A \cap B$ is infinite by [18, 6.2]. If $A \neq B$, then $A > (A \cap B)^\circ$ and $(A \cap B)^\circ$ is a definable invisible subgroup of infinite index. Hence $N_A((A \cap B)^\circ)/(A \cap B)^\circ$ is infinite by [18, 6.3]. Let $B_1 \geq N_G((A \cap B)^\circ)^\circ$ be a maximal invisible subgroup. B_1 exists by (iii) as A does not contain strongly real elements. Then $rk(A \cap B_1) > rk(A \cap B)$. If $A > (A \cap B_1)^\circ$ then there exists a maximal invisible group $B_2 \geq N_G((A \cap B_1)^\circ)^\circ$ such that $rk(A \cap B_2) > rk(A \cap B_1)$. Iterating this process we eventually arrive at a maximal invisible subgroup $B_n \geq N_G((A \cap B_{n-1})^\circ)^\circ$ such that $A = (A \cap B_n)^\circ$ by ascending chain condition on connected subgroups. Hence $A = B_n$ by maximality of A. Assume that $B_{n-1} > (A \cap B_{n-1})^\circ$. Then $(A \cap B_{n-1})^\circ$ has infinite index in $N_{B_{n-1}}((A \cap B_{n-1})^\circ)^\circ \leq A \cap B_{n-1}$ by [18, 6.3]. This would imply that $rk((A \cap B_{n-1})^\circ) < rk(A \cap B_{n-1})$. Contradiction. Thus $B_{n-1} = A$ already. We can repeat the argument until we arrive at $A = B$.

(vi) As $U \cap U^g = 1$ if and only if $g \in G \backslash N_G(U)$ by (v),

$$\begin{aligned} rk\Big(\bigcup_{g \in G} U^g\Big) &= rk(G) - rk(N_G(U)) + rk(U) \\ &= rk(G) - rk(N_G(U)/U). \end{aligned}$$

by the additivity of Morley rank and Lascar's equality.

(vii) Assume that G contains an invisible element x which is not strongly real. Then there exists by (ii) an infinite maximal invisible group $A \geq C_G(x)^\circ$, such that $A = N_G(A)^\circ$ by (iii), as x is not strongly real. Thus $\bigcup_{g \in G} A^g$ is generic in G by (vi). Contradiction to Proposition 4.25. $\square$

Corollary 4.28 *Let $U \leq G$ be a maximal invisible group and $u \in U$. Then $C_G(u)$ is abelian, inverted by i and $I(C_G^*(u)) = iC_G(u) = i^{C_G(u)}$. Furthermore $U = C_G(u)^\circ$.*

Proof. Let U be a maximal invisible group. U consists of strongly real elements by Proposition 4.27 (vii). Thus U is abelian and inverted by an involution i by Proposition 4.27 (iv). Let $u \in U$ be a nontrivial element.

Assume that $C_G(i) \cap C_G(u)$ is not trivial. Then, conjugating with a suitable element of G, there exists a nontrivial element $g \in C_G(i_0) \cap C_G(v)$ for some invisible element v that is inverted by i_0. As $v \in C_G(g)$, $C_G(g)$ is conjugate in $C_G(i_0)$ to $T\langle y\rangle$ by Lemma 4.24. However $T\langle y\rangle$ does not contain an element that is inverted by i_0. Contradiction.

Thus i acts fixed-point free on $C_G(u)$, $C_G(u)$ is abelian, inverted by i and $I(C_G^*(u)) = iC_G(u) = i^{C_G(u)}$ by [18, 10.5]. As finally U is abelian $U \leq C_G(u)^\circ$. However, $C_G(u)^\circ$ is invisible by Proposition 4.27 (ii) and thus $U = C_G(u)^\circ$ by maximality of U. □

Corollary 4.29 *Let $u \in G$ be invisible. Then $C_G(u)\backslash\{1\}$ consists of invisible elements and $C_G(u)^\circ$ is a maximal invisible group.*

Proof. As $C_G(u)^\circ$ is an infinite invisible group by Proposition 4.27 (ii), u is contained in a maximal invisible group $U \geq C_G(u)^\circ$. Thus $U = C_G(u)^\circ$ and $C_G(u)$ is abelian by Corollary 4.28. Let $v \in C_G(u)\backslash\{1\}$. Then $U \leq C_G(v)^\circ$ and v cannot be visible by Proposition 4.27 (i). Hence v is invisible and the claim follows. □

We are going to estimate the Morley rank of G. Let $f := rk\big(Z(C_G(i_0))\big)$.

Lemma 4.30 $rk(C_G(i_0)) = 4f$.

Proof. Since $C_G(i_0) \cong \mathrm{GL}_2(K)$ for an algebraically closed field K, $C_G(i_0)$ has a Bruhat decomposition $C_G(i_0) = B \cup Bw_0B$, where $B = TX_1$ by [42, 28.3]. Thus

$$rk(C_G(i)) = rk(BwB) = rk(X_1^w X_1 T).$$

By Proposition 4.5 $T = Z(C_G(i_0))Z(C_G(i_1))$ and thus $rk(T) = 2f$. Furthermore $Z(C_G(i_1))$ acts transitively on $X_1\backslash\{1\}$ and $rk(X_1) = f$. Hence

$$rk(X_1^w X_1 T) = 2rk(X_1) + rk(T) = 4f$$

which proves the claim □

We need a precise description of strongly real elements. Let

$$\begin{aligned} X_s &:= \bigcup\nolimits_{g\in G} T[w_0]^g, \\ X_u &:= \bigcup\nolimits_{g\in G} (\langle i_0\rangle X_1\backslash\{i_0\})^g. \end{aligned}$$

Lemma 4.31 *If $x \in Sr(C_G(i_0))$, then either $I(C^*_G(x)) \subseteq C_G(l)$ for some $l \in I(C_G(i_0))$ or $x \in C_T(y)$. Furthermore $I(G) \cup X_s \cup X_u$ is the set of strongly real visible elements of G.*

Proof. Let $x \in C_G(i_0)$. By Remark 4.18 we may assume that either $x \in T$ or $x \in Z(C_G(i_0))X_1$. If $x \in T$, then x is an involution or $C_G(x)^\circ = T$ by Lemma 4.16. If $x \in I(T)$, then $C^*_G(x) = C_G(x)$. Assume that x is not an involution and let i invert x. Then $i, ix \in I(N_G(T))$ and $x \in \bigcup_{1\leq n\leq 3} T[w_n]$ by Lemma 4.64. If $x \in Z(C_G(i_0))X_1$ then either $x \in Z(C_G(i_0))$ and $x = i_0$ by Lemma 4.16 or $C_G(x) = Z(C_G(i_0))X_1$ by Lemma 4.23. If i inverts x thus $i \in N_G(X_1) = TX_1$ by Lemma 4.22. Hence $x \in \langle i_0\rangle X_1$.

The second part of the Lemma follows as a visible element $x \in Sr(G)$ is a strongly real element of $C_G(s)$ for some involution $s \in I(G)$. □.

Lemma 4.32 *$rk(X_s) = rk(G) - f$ and $rk(X_u) = rk(G) - 2f$.*

Proof. First note that $rk(T[w_0]) = rk(T) - rk(Z(C_G(i_0)) = f$. Consider $\psi : G \times T[w_0] \to X_s$ where $\psi(g,t) = t^g$. If $x \in T[w_0]$, then

$$\psi^{-1}(x) := \{(t,g) \in T[w_0] \times G | \ t^g = x\},$$

and

$$\begin{aligned} rk(\psi^{-1}(x)) &= rk\big(\{g \in G| \ x^{g^{-1}} \in T[w_0]\}\big) \\ &= rk\big(\{g \in G| \ x \in T[w_0] \cap T[w_0]^g\}\big). \end{aligned}$$

However if $x \in T[w_0] \cap T[w_0]^g$ then $T[w_0], T[w_0]^g \leq C_G(x)^\circ$. If $x \notin \langle i_0\rangle$, then $C_G(x)^\circ = T$ by Lemma 4.11. This implies that $C_G(T[w_0]) = T = T^{g^{-1}}$ and hence $g \in N_G(T)$. Thus

$$rk(\psi^{-1}(x)) = rk(N_G(T)) = rk(T) = 2f$$

and $rk(G) + rk(T[w_0]) = rk(X_s) + 2f$ by additivity of Morley rank. Hence $rk(X_s) = rk(G) - f$.

Finally $(\langle i_0\rangle X_1 \backslash \{i_0\}) \cap (\langle i_0\rangle X_1 \backslash \{i_0\})^g \neq 1$ if and only if $g \in N_G(X_1)$ by Lemma 4.23. Thus

$$rk(X_s) = rk(G) - \big(rk(N_G(X_1)) + rk(X_1)\big) = rk(G) - rk(T) = rk(G) - 2f$$

as $N_G(X_1) = X_1 \rtimes T$ by Proposition 4.22. □

Proposition 4.33 *$rk(G) \geq 8f$, $rk(I(i_0X_s)) = 4f$ and $rk(I(i_0X_u)) = 3f$.*

Proof. We are going to use the standard technique for rank estimates from the proof of Fact 1.1. Consider $\varphi : I(G) \times I(G) \longrightarrow G$ where $\varphi((\lambda,\kappa)) = \lambda\kappa$ for all $\lambda, \kappa \in I(G)$. Then $X_s \cup X_u \subseteq \varphi(I(G) \times I(G))$ and

$$(*) \quad rk(I(G)) = rk(i_0^G) = rk(G) - rk(C_G(i_0)) = rk(G) - 4f$$

by Lemma 4.30. Let $t \in T[w_0] \backslash \{1, i_0\}$. As

$$\begin{aligned} rk\big(\varphi^{-1}(t)\big) &= rk\big(\{\lambda \in I(G) | t^\lambda = t^{-1}\}\big) = rk\big(I(C_G^*(t) \backslash C_G(t))\big) \\ &= rk\big(I(w_0 T)\big) = rk\big(T[w_0]\big) = f, \end{aligned}$$

$rk\big(\varphi^{-1}(X_s)\big) = rk(X_s) + rk\big(T[w_0]\big) = rk(G)$ by Lemma 4.32. By additivity of Morley rank we can hence conclude that

$$rk(G) \leq rk\big(I(G) \times I(G)\big) = 2\, rk(G) - 8f$$

by $(*)$. Thus $rk(G) \geq 8f$. Furthermore

$$\varphi^{-1}(X_s) = \big\{(\kappa, \lambda) \in I(G) \times I(G) | \lambda \in \kappa X_s\big\}$$

and thus $rk\big(\varphi^{-1}(X_s)\big) = rk\big(I(G)\big) + rk\big(I(i_0 X_s)\big)$. As $rk\big(\varphi^{-1}(X_s)\big) = rk(G)$ the second part of the claim follows by $(*)$ again.

Finally let $u \in X_u$ be a nontrivial element. Then

$$\begin{aligned} rk\big(\varphi^{-1}(X_u)\big) &= rk\big(X_u\big) + rk\big(I(C_G^*(u) \backslash C_G(u))\big) \\ &= rk\big(X_u\big) + rk\big(X_1\big) = rk(G) - f \end{aligned}$$

by Lemma 4.23 and Lemma 4.32. As $rk\big(\varphi^{-1}(X_s)\big) = rk\big(I(G)\big) + rk\big(I(i_0 X_u)\big)$ the claim follows by $(*)$. □

Corollary 4.34 *Let $i \in I(G)$. Then $rk\big(\{j \in I(G) |\ ij$ is visible $\}\big) = 4f$.*

Proof. If ij is visible for $ij \in I(G)$, then $ij \in I(G) \cup X_s \cup X_f$ by Lemma 4.31. If $ij \in I(G)$, then $j \in I(C_G(i))$. Since $rk\big(I(C_G(i))\big) = 2f$, the claim follows by Proposition 4.33. □

It is more difficult to get an upper bound for $rk(G)$.

Lemma 4.35 *Let $i, j \in I(G)$.*

(i) If ij is invisible, then $C_G(i) \cap C_G(j) = 1$.

(ii) If ij is visible, then $C_G(i) \cap C_G(j)$ contains an involution.

Proof. If ij is invisible, then $C_G(ij)\backslash\{1\}$ consists of invisible elements by Corollary 4.29. As $C_G(i) \cap C_G(j) \leq C_G(ij)$ thus $C_G(i) \cap C_G(j) = 1$.

Assume now ij is visible. Then either $i, j \in I(C_G^*(ij)) \subseteq C_G(s)$ for some involution $s \in I(G)$ or ij is conjugate to an element in $C_T(y)$ by Lemma 4.31. Assume that ij is centralized by y. Then $j \in N_G(C_G(ij)^\circ) = N_G(T)$ by Lemma 4.11. Hence $j = i(ij) \in iT \cap N_G(T) \leq C_G(l)$ for some involution $l \in D^*$ by Lemma 4.64. Thus there always exists an involution $s \in I(G)$ such that $i, j \in C_G(s)$ and the claim follows. □

Lemma 4.36 *Let $H \leq T$ be an infinite definable subgroup such that $H \cong K^*$. Then either $H = T[w_0]$, $H = Z(C_G(i_0))$ or $T = HH^{w_0}$ and $rk(H) = f$.*

Proof. Since $H, H^{w_0} \leq T$, either $H = H^{w_0}$ or $H \cap H^{w_0}$ is finite as G does not interpret a bad field. Assume that w_0 normalises H. If $C_H(w_0)$ is finite, then w_0 inverts H and $H = T[w_0]$. Thus $rk(H) = f$ in this case. If $C_H(w_0)$ is infinite, then $C_H(w_0) = H = Z(C_G(i_0))$ since G does not interpret a bad field and $rk(H) = f$ again. If on the other hand w_0 does not normalize H, $H \cap H^{w_0}$ is finite and $rk(HH^{w_0}) = 2\, rk(H)$. Furthermore $C_{HH^{w_0}}(w_0) = \{hh^{w_0} |\ h \in H\} = Z(C_G(i_0))$. Especially as $H \cap H^{w_0}$ is finite, $rk(H) = f$ again and $T = HH^{w_0}$ is this case. □

Proposition 4.37 *Let U be maximal invisible group and i an involution that inverts U. Then*

(i) *$N_G(U) = C_G(U) \rtimes H$ where $H = C_G(i) \cap N_G(U)$. Furthermore $H = C_G(i) \cap C_G(j)C_G(U)$ for all $j \in I(N_G(U))$.*

(ii) *$H \cap H^u = 1$ for all $u \in C_G(U)$.*

(iii) *$rk(\bigcup_{g\in G} U^g) = rk(G) - rk(H)$ and H is infinite.*

(iv) *$H^\circ \cong K^*$, $H^\circ < C_G(D)$ for some four-subgroup $D \leq C_G(i)$ and U contains a subgroup $A \cong K^+$ on which H acts transitively. Especially $rk(H) = f$.*

(v) *$N_G(U)^\circ = U \rtimes H^\circ$ is a 2-step solvable centerless group and $(N_G(U)^\circ)' = U$ is either a p-subgroup of bounded exponent, if $char(K) = p$, or a torsion-free divisible group, if $char(K) = 0$.*

(vi) *$N_G(U)^\circ = U \cup \bigcup_{c\in U} H^c$ and $Uh = h^U$ for all $h \in H\backslash\{1\}$. Especially $H \cap H^u = 1$ for all $u \in U$.*

(vii) *If $M \leq N_G(U)^\circ$ is such that $M \cap U = 1$, then M is contained in $(H^\circ)^x$ for some $x \in U$.*

Proof. We first show (i). Since any involution that normalizes $C_G(U)$ already inverts it,

$$(*) \quad i^{N_G(U)} \subseteq I(N_G(U)) = iC_G(U) = i^{C_G(U)}$$

by Corollary 4.28. Hence $N_G(U) \subseteq C_G(k)C_G(U)$ for all $k \in I(N_G(U))$. Furthermore $[N_G(U), i] \subseteq C_G(U)$ and $N_G(U) = C_G(U) \rtimes C_{N_G(U)}(i)$ by [18, ex. 9, p. 98]. Let $H := C_{N_G(U)}(i)$. Then $H \subseteq C_G(i) \cap C_G(j)C_G(U)$ for all $j \in I(N_G(U))$. On the other hand $C_G(i)C_G(U) \cap C_G(j)C_G(U) \subseteq N_G(U)$ and hence $N_G(U) = C_G(i)C_G(U) \cap C_G(j)C_G(U)$ and (i) follows.

(ii) is a direct consequence of Corollary 4.35, as $H \cap H^u \leq C_G(i) \cap C_G(i^u)$ and $ii^u \in C_G(U)$ is invisible by Corollary 4.29.

(iii) follows since by Corollary 4.28 $rk(C_G(U)) = rk(U)$ and thus by Proposition 4.27

$$rk(\bigcup_{g\in G} U^g) = rk(G) - rk(N_G(U)/U) = rk(G) - rk(H).$$

Especially $rk(H) > 0$ by Lemma 4.25.

To prove (iv), let $B \leq H$ a Borel subgroup of H and $A \leq U$ a B-minimal group. Then B' centralizes A by [18, 9.8]. However, $C_H(x) \leq C_G(i) \cap C_G(U) = 1$ for all $x \in U\backslash\{1\}$ by Corollary 4.29. Hence $B' = 1$ and B is abelian. Since H is a K-group all Borel subgroups are conjugate by Proposition 1.6. Hence H does not contain connected solvable non-nilpotent definable subgroups. Thus $H^\circ \leq C_G(i) \cong \mathrm{GL}_2(K)$ has to be solvable already and hence abelian. As $C_H(A) = 1$, $A \cong K^+$ and $H^\circ \cong K^*$ for some algebraically closed field K by [18, 9.1], since G does not interpret a bad field. As $H \leq C_G(i)$, $H^\circ < C_G(D)$ for some four-subgroup $D \leq C_G(i)$. Furthermore H operates transitively on $A\backslash\{1\}$, i.e. $rk(A) = rk(H) = f$ by Lemma 4.36.

We show (v). Since H° is abelian, $(N_G(U)^\circ)' \leq U$ and $N_G(U)^\circ$ is a 2-step solvable centerless group. As furthermore $U = [i, U] = (N_G(U)^\circ)'$ by equation $(*)$, U is quasiunipotent by [18, ex. 3, p. 148]. U is thus the direct sum of a definable subgroup of bounded exponent B and a definable divisible torsion-free subgroup D, both of which are characteristic in U by Lemma 2.3. Since however H°-minimal subgroups of U are isomorphic to K^+, either $B = 1$ and U is a divisible torsion-free group or $D = 1$ and U is a p-group, where $p = char(K)$.

(vi) follows from [18, ex. 8, ex. 11, p. 98] as $U \cap C_G(h) = 1$ for all $h \in H\backslash\{1\}$ by Corollary 4.29.

We finally show (vii). M is abelian, since $[M, M] \leq G' \cap M = U \cap M = 1$. Thus $M \leq C_G(m)$ for all $m \in M$. Set $V := UM \cap H^\circ$ and let $v \in V$. Since $C_{N_G(U)^\circ}(v) = H^\circ$, $C_{UM}(v) \leq V$. On the other hand $v \in Um$ for some $m \in M$

and thus $m \in vU = v^U$ by (vi). Thus there exists $u \in U$ such that $v = m^u$ and $M^u \leq C_{UM}(m)^u = C_{UM}(v) \leq V \leq H^\circ$. Especially $M \leq (H^\circ)^{u^{-1}}$. □

Proposition 4.38 *Either G consists of visible elements and $rk(G) = 8f$ or there exist a maximal invisible subgroup U such that*

$$7f + rk(U) \leq rk(G) < 8f + rk(U).$$

Furthermore

$$rk(G) = rk(U) + 7f + rk(B/\equiv)$$

where

$$B := \{g \in Inv(G)|\, rk(C_G(g)) = rk(U)\}$$

and $b_1 \equiv b_2$ if there exists $g \in G$ such that $b_1 \in C_G(b_2)^g$.

Proof. We are again using the technique from the proof of Fact 1.1. Let $\varphi : I(G) \times I(G) \longrightarrow G$ be defined by $\varphi((x, y)) = xy$. Then $2\,rk\big(I(G)\big) = max_{1\leq n\leq k}\{B_n + a_n\}$ by [1, 6.1], where

$$B_n := \{g \in \varphi(I(G) \times I(G))|\, rk(\varphi^{-1}(g)) = a_n\}$$

and $0 \leq a_n \leq 2\,rk(I(G))$. Now $rk\big(\varphi^{-1}(1)\big) = rk\big(I(G)\big)$,

$$rk\big(\varphi^{-1}(g)\big) = rk\big(I(C_G(g)\big) = 2f \text{ if } g \in I(G)$$

and

$$rk\big(\varphi^{-1}(g)\big) = rk\big(I(C^*_G(g)\backslash C_G(g))\big) \text{ for } g \in Sr(G)\backslash I(G).$$

If g is invisible then $rk\big(\varphi^{-1}(g)\big) = rk(C_G(g))$ as $C_G(g)^\circ$ is a maximal invisible group by Corollary 4.29 which is inverted by an involution $i \in I(G)$. If $g \in Sr(G)\backslash I(G)$ is visible, then $g \in X_s \cup X_u$ by Lemma 4.31 and thus $rk(\varphi^{-1}(g)) = f$ as in Proposition 4.33. Let $m := rk(I(G))$. Hence, if we set $a_n := nf$ for $1 \leq n \leq k := 2f^{-1}I(G)$, then

$$B_1 \subseteq X_s \cup X_u \cup Inv(G),\ B_2 \subseteq I(G) \cup Inv(G),\ B_m \subseteq 1 \cup Inv(G)$$

and $B_n \subseteq Inv(G)$ for all $3 \leq n \leq k$, $n \neq m$. By Proposition 4.37 either $rk(Inv(G) \cap B_n) = 0$ or $rk(Inv(G) \cap B_n) \geq rk(G) - f$ for all $1 \leq n \leq k$. If

$Inv(G) = \emptyset$ then $2\,rk(I(G)) = f + (rk(G) - f)$ by Lemma 4.32. In this case $rk(G) = 8f$. If $Inv(G) \neq \emptyset$ then $2\,rk(I(G)) = rk(U) + rk(B)$ where

$$B := \{g \in Inv(G)|\; rk(C_G(g)) = rk(U)\}.$$

Especially $rk(G) = rk(U) + 8f + (rk(B) - rk(G))$. By Lemma 4.25 and Proposition 4.37 $rk(G) - f \leq rk(B) < rk(G)$. Define an equivalence relation $\equiv$ on B via $b_1 \equiv b_2$ if $b_1 \in \bigcup_{g\in G} C_G(b_2)^g$. Since $rk[b]_\equiv = rk(G) - f$ for all $b \in B$ by Proposition 4.37

$$rk(B/\equiv) = rk(B) - rk(G) + f = rk(G) - rk(U) - 7f < f$$

and $rk(G) = rk(U) + 7f + rk(B/\equiv)$. □

Lemma 4.39 *Let $i \in I(G)$. Then $\{j \in I(G)|\; ij$ is invisible$\}$ is either empty or generic in $I(G)$.*

Proof. Assume there exists $j \in I(G)$ such that ij is invisible. Then $U := C_G(ij)^\circ$ is a maximal invisible group by Corollary 4.29. We may assume by Proposition 4.38 that $rk(G) = 7f + rk(U) + rk(B/\equiv)$ and thus

$$rk(I(G)) = rk(G) - rk(C_G(i)) = 3f + rk(U) + rk(B/\equiv).$$

We are going to show that $J := \{j \in I(G)|\; ij \in B\}$ is generic in $I(G)$. To do this we define an equivalence relation $\simeq$ on J via $j_1 \simeq j_2$ if there exists $g \in G$ such that $C_G(ij_1) = C_G(ij_2)^g$. We claim that

$$i^{C_G(ij_1)C_G(i)} \subseteq [j_1]_\simeq.$$

for all $j_1 \in J$. For let $c \in C_G(ij_1)$, $x \in C_G(i)$, then $ii^{cx} = (ii^c)^x = (c^{-i}c)^x = c^{2x} \in C_G(ij_1)^x$ by Corollary 4.28 and thus $C_G(ii^{cx}) = C_G(ij_1)^x$ as both groups are abelian.

We compute the Morley rank of $[j]_\simeq$. Consider $\phi : UC_G(i) \longrightarrow i^{UC_G(i)}$ where $\phi(x) = i^x$. Let $u_n \in U$, $c_n \in C_G(i)$ for $n = 1, 2$. Then $i^{u_1c_1} = i^{u_2c_2}$ if and only if

$$(*) \quad ii^{u_1c_1c_2^{-1}} = ii^{u_2} \in U \cap U^{c_1c_2^{-1}}.$$

However $(*)$ is only the case if $c_1c_2^{-1} \in N_G(U) \cap C_G(i)$. Set $h := c_1c_2^{-1}$. Then $i^{u_1hu_2^{-1}} = i$ by assumption and therefore $i = i^{u_1u_2^{-h^{-1}}h} = i$. This implies that $u_1u_2^{-h^{-1}} \in C_G(i) \cap U = 1$ and $u_1^h = u_2$. Especially $rk(\phi^{-1}(x)) = rk(N_G(U) \cap C_G(i)) = f$ for all $x \in UC_G(i)$ by Proposition 4.37. Hence by additivity of Morley rank

$$\begin{aligned} rk(i^{UC_G(i)}) &= rk(UC_G(i)) - f = rk(U) + rk(C_G(i)) - f \\ &= rk(I(G)) - rk(B/\equiv). \end{aligned}$$

This implies that $rk(J) \geq rk(J/\simeq) + (rk(I(G)) - rk(B/\equiv))$ and it is only left to show that $rk(J/\simeq) \geq rk(B/\equiv)$. Define $\psi : J \longrightarrow B/\equiv$ by $\psi(j) = [ij]_\equiv$. Then $\psi(j_1) = \psi(j_2)$ iff $ij_2 \in C_G(ij_1)^g$ for some $g \in G$ iff $j_1 \simeq j_2$. Thus $rk(\psi^{-1}([ij]_\equiv)) = rk([j]_\simeq)$ and $rk(J/\simeq) = rk(B/\equiv)$ since ψ is surjective. □

Let U be a maximal invisible subgroup as in Proposition 4.38. Let $N := N_G(U)^\circ$ and H a complement of U in N. Define as in [18, 14.5] for all $w \in I(G \backslash N)$

$$H[w] := \{n \in N |\ n^w = n^{-1}\}$$

$$X := \{w \in I(G \backslash N) |\ H[w] \neq 1\}$$

$$X' := \{w \in I(G \backslash N) |\ H[w] = 1\}$$

Lemma 4.40 *Let $w \in I(G \backslash N)$. Then $H[w]$ is an abelian subgroup of N and is contained in some complement H of U.*

Proof. As $U \cap U^w = 1$ by Corollary 4.28, $U^w \cap N$ is contained in H^u for some $u \in U$ by Proposition 4.37. Thus $U^w \cap N = 1$ since U^w is invisible and $H^u \leq C_G(k)$ for an involution $k \in N$. Thus $(N \cap N^w) \cap U = 1$ as well and $H[w] \subseteq N \cap N^w$ is contained in a complement of U in N by Proposition 4.37. This implies that $H[w]$ consists of commuting elements and $H[w]$ is hence a subgroup of N. □

Corollary 4.41 *Let $w \in I(G \backslash N)$. Then $H[w]$ is either finite or a complement of U in N.*

Proof. $H[w] \leq H$ for some complement H of U by Lemma 4.40. As $H \cong K^*$ by Proposition 4.37 and G does not interpret a bad field, either $H[w]$ is finite or already equals H. □

Proposition 4.42 *$rk(X') = rk(I(G))$ and $rk(U) \leq 3f$.*

Proof. $I(G) = I(N) \cup X \cup X'$ and

$$rk(I(N)) = rk(U) < rk(U) + 3f + r = rk(G) - 4f = rk(I(G)).$$

To show, that X' is generic in $I(G)$, it is therefore enough to prove that $rk(X) < rk(I(G))$. By Lemma 4.40 there exists a complement of U in N which contains $H[w]$. Let $I_u := \{w \in X |\ H[w] \leq H^u\}$ for all $u \in U$. Then $rk(X) = \bigcup_{u \in U} I_u \leq rk(U) + rk(I_1)$ as $H[w^u] = H[w]^u$ for all $u \in U$. However $w \in I_1$ only if w

inverts an element $t \in H$. Thus $rk(I_1) \leq rk(I(C_G^*(t))) \leq 2f$ by Lemma 4.24 and $rk(X) \leq rk(U) + 2f < rk(I(G))$. Hence

$$rk(G) - 4f = rk(I(G)) = rk(X') \leq rk(G/N) = rk(G) - (rk(U) + f)$$

since for $w_1, w_2 \in X'$: $w_1 N = w_2 N$ if and only if $w_1 w_2 \in H[w_1] = 1$. This implies that $rk(U) \leq 3f$. □

Corollary 4.43 *Either $G = \bigcup_{g \in G} C_G(i)^g$ and $rk(G) = 8f$ or there exists an invisible element and $8f < rk(G) < 11f$.*

Proof. Assume that G does not contain invisible elements. Then $rk(G) = 8f$ by Proposition 4.38. Assume now that G contains an invisible element u which is inverted by $i \in I(G)$. Then $\{j \in I(G) | \ ij \text{ is invisible}\}$ is generic in $I(G)$ by Lemma 4.39. On the other hand $rk(\{j \in I(G) | \ ij \text{ is visible}\}) = 4f$ by Lemma 4.34. As G is connected and thus $deg(I(G)) = deg(i^G) = 1$, $rk(I(G)) > 4f$ in this case. Furthermore $rk(I(G)) = rk(G) - rk(C_G(i)) = 3f + rk(U) + rk(B/\equiv)$ by Proposition 4.38. Hence $rk(U) + rk(B/\equiv) > f$ and $rk(G) > 8f$. As however $rk(G) < 8f + rk(U)$ by Proposition 4.37 and $rk(U) \leq 3f$ by Proposition 4.42, $rk(G) < 11f$ and everything is proven. □

4.2 $\mathrm{PSp}_4(K)$ and $\mathrm{G}_2(K)$

The aim of this section is to prove cases (2) and (3) of Conjecture 7.

Theorem 4.44 *Let G be a simple K^*-group of finite Morley rank that does not interpret a bad field. Assume that G contains an involution i, such that either*

(i) $C_G(i)^\circ / O(C_G(i)) \cong \mathrm{SL}_2(K) * \mathrm{SL}_2(K)$ where the two copies of $\mathrm{SL}(2, K)$ intersect non-trivially or

(ii) $C_G(i)^\circ / O(C_G(i)) \cong \mathrm{PSL}(2, K) \times K^*$

for an algebraically closed field K of characteristic neither 2 nor 3. Then $G \cong \mathrm{PSp}_4(K)$ or $G \cong \mathrm{G}_2(K)$.

4.2.1 Basic Results

We are first going to show, that case (ii) of Theorem 4.44 implies case (i).

Lemma 4.45 *Let G be a K^*-group of finite Morley rank. Assume that there exist two definable subgroups $N, H \leq G$ such that $N \lhd H$ and $\overline{H} := H/N$ is a proper simple section of G allowing no graph automorphisms. Then $N_G(H) = C_{N_G(H)}(\overline{H})H$.*

Proof. Let $g \in N_G(H)$ and set $R := d(g)$. $R \leq N_G(H)$ acts on $\overline{H}$. As G is a K^*-group and H is a proper simple section, H is a simple algebraic group over an algebraically closed field. Consider the semidirect product $\overline{H} \rtimes R/C_R(\overline{H})$. Then, viewing $R/C_R(\overline{H})$ as a subgroup of $Aut(\overline{H})$, $R/C_R(\overline{H}) \leq Inn(\overline{H})\Gamma$, where Γ are the graph automorphisms of $\overline{H}$ by [18, 8.4]. As $\Gamma = 1$, either $g \in C_{N_G(H)}(\overline{H})$ or there exists an $h \in H$ such that $x^g \in x^h N$ for all $x \in H$ and $gh^{-1} \in C_{N_G(H)}(\overline{H})$. Thus $g \in C_{N_G(H)}(\overline{H})H$. □

Lemma 4.46 *Let H be a group of finite Morley rank, such that H° is a reductive algebraic group and let $\overline{H}^\circ := H^\circ/Z(H^\circ)$. Then $C_{C_H(Z(H^\circ))}(H^\circ) = C_{C_H(Z(H^\circ))}(\overline{H}^\circ)$.*

Proof. Let $g \in C_H(\overline{H}^\circ) \cap C_H(Z(H^\circ))$. As H° is reductive, $\overline{H}^\circ$ is a simple group by [42, 27.5] and $m := o(\overline{g}) < |H/H^\circ|$. Set $z_x := x^{-1}x^g \in Z(H^\circ)$ for all $x \in H^\circ$. Then, as $x^g = xz_x$, $x = x^{g^m} = xz_x^m$ and $o(z_x)|m$ for all $x \in H^\circ$. On the other hand $(x^m)^g = (xz_x)^m = x^m z_x^m$ and $g \in C_H(x^m)$ for all $x \in H^\circ$. Especially $C_P(g) = P$, for any maximal torus P of H°, since maximal tori are divisible. As finally H° is a reductive algebraic group, $H^\circ = \langle P^h |\ h \in H^\circ\rangle \leq C_H(g)$ by [42, ex. 12, p. 162] and $g \in C_H(H^\circ)$. □

Theorem 4.47 *Let G be a simple K^*-group of finite Morley rank that does not interpret a bad field. Assume that G contains an involution i, such that $C_G(i)^\circ/O(C_G(i)) \cong \mathrm{PSL}_2(K) \times K^*$ where K is an algebraically closed field of characteristic not 2. Then G contains an involution j, such that $C_G(j)^\circ \cong \mathrm{SL}_2(K) * \mathrm{SL}_2(K)$.*

Proof. Let S be Sylow 2-subgroup of G that contains i and $D \leq S^\circ$ a four-subgroup. We may assume that $i \in D$ by Proposition 4.2. Set $T := C_G(D)^\circ$. Hence $O(C_G(t)) = 1$ for all $t \in D^*$ by Proposition 4.2 again. Furthermore $G = \langle C_G(k)^\circ |\ k \in D_1^*\rangle$ for any four-subgroup $D_1 \leq G$ by Corollary 3.17. Set $T := C_G(D)^\circ$ and let $u \in (C_G(D) \cap C_G(i)^\circ)\backslash T$. Then $C_T(u) = Z(C_G(i)^\circ)$.

Assume that $C_G(j)^\circ \cong \mathrm{GL}_2(K)$ for some $j \in D^*$. Then there exists an involution $w \in C_G(j)^\circ \cap N_G(D)$ such that $i^w = ij$. Then $uu^w = w^u w \in C_G(D) \cap C_G(j)^\circ = T$. Furthermore, as u centralises $Z(C_G(i)^\circ)$, u^w centralises $Z(C_G(i)^\circ)$

as well. On the other hand $C_T(u^w) = C_T(u)^w = Z(C_G(ij)^\circ)$. Contradiction as $Z(C_G(ij)^\circ) \neq Z(C_G(i)^\circ)$.

Assume that $C_G(j)^\circ \cong \mathrm{PSL}_2(K) \times K^*$ for some $j \in D^*$, $j \neq i$. Let $v \in C_{C_G(j)^\circ}(D) \backslash T$ be an involution. As $C_T(v)^\circ = Z(C_G(j)^\circ)$, $v \in C_G(i) \backslash C_G(i)^\circ$. Let $C := C_G(i)^\circ$ and $\overline{C} := C/Z(C)$. By Lemma 4.45 $C_G(i) = C_{C_G(i)}(\overline{C})C$.

v normalises $Z(C) \cong K^*$ and G does not interpret a bad field. Thus v either inverts $Z(C)$ or centralizes it by [18, 10.5]. Since $C_T(v) = Z(C_G(j)^\circ)$, the second case cannot occur and v inverts $Z(C)$. Let $x \in C$, such that $xv \in C_{C_G(i)}(\overline{C})$. Then $x \in N_G(D) \cap C = T\langle u \rangle$ and xv inverts $Z(C)$. As u inverts $Z(C_G(j)^\circ)$ as above, yv inverts T for all $y \in uT$. Hence $x \in T$, since $xv \in C_{C_G(i)}(\overline{C})$. Furthermore we may assume that $x \in Z(C_G(j)^\circ)$, as $T = Z(C_G(j)^\circ)Z(C)$. Thus $(xv)^2 = x^2 \in C_C(\overline{C}) = Z(C) \cap Z(C_G(j)^\circ) = 1$ by Lemma 4.46 and $x \in \langle j \rangle$. Then $[xv, C] \subseteq Z(C)$ and $C = Z(C) * C_C(xv)$ by [18, ex. 10, p. 98] where $Z(C) \cap C_C(xv) = \langle i \rangle$. Set $H := C_C(xv)^\circ$. As $C \cong \mathrm{PSL}_2(K) \times K^*$, $H \cong \mathrm{PSL}_2(K)$ and $C = Z(C) \times H$. As $x \in \langle j \rangle$, $xv \in I(C_G(D))$. Thus $D_1 := \langle i, xv \rangle$ is a four-subgroup and $G := \langle C_G(k) |\ k \in D_1^* \rangle$. Furthermore $H \leq C_G(D_1)$. As H is a normal subgroup of $C_G(i)^\circ$ and G is simple, H cannot be a normal subgroup of both $C_G(ux)$ and $C_G(uxi)$. As ux and uxi are conjugate to involutions in D by Lemma 3.19, this implies that $C_G(k) \cong \mathrm{SL}(2, K) * \mathrm{SL}(2, K)$ for $k = ux$ or $k = uxi$ by Proposition 4.2.

As finally $G = \langle C_G(k)^\circ |\ k \in D^* \rangle$, it is impossible that $C_G(k)^\circ$ is abelian for all $k \in D \backslash \langle i \rangle$. This implies the claim by Proposition 4.2. □

Thus Theorem 4.44 basically consists of two parts. The first one is a partial analogue of the result of Wong [57] in finite group theory. It will appear in [8] and be proven in Section 4.2.

Theorem 4.48 *Let C_1 and C_2 be the non-isomorphic centralizers in $\mathrm{PSp}_4(K)$ of two involutions where K is an algebraically closed field of characteristic not 2. Let G be a K^*-group of finite Morley rank that does not interpret a bad field. Assume that G contains two involutions i and j such that $C_G(i) \cong C_1$ and $C_G(j) \cong C_2$. Then $G \cong \mathrm{PSp}_4(K)$.*

The corresponding result for $\mathrm{G}_2(K)$ is the following theorem, which will be proven in Section 4.3.

Theorem 4.49 *Let C be the centralizer in $\mathrm{G}_2(K)$ of an involutions where K is an algebraically closed field of characteristic not 2. Let G be a K^*-group of finite Morley rank that does not interpret a bad field. Assume that G contains one conjugacy class i^G of involutions such that $C_G(i) \cong C$. Then $G \cong \mathrm{G}_2(K)$ if $char(K) \neq 3$.*

The rest of the subsection is devoted to the proof that Theorems 4.48 and 4.49 imply Theorem 4.44.

Let G be a group as in Theorem 4.44. By Theorem 4.47 there exists an involution $i \in G$, such that $C_G(i)^\circ / O(C_G(i)) \cong L_1 * L_2$ where $L_n \cong \mathrm{SL}_2(K)$ for an algebraically closed field K of characteristic neither 2 nor 3 and $n = 1, 2$. We may assume that $i \in C_G(i)^\circ$ by Lemma 4.2. Thus $L_1 \cap L_2 = \langle \overline{\imath} \rangle$. Let S be a Sylow 2-subgroup of $C_G(i)$, D a four-subgroup such that $D \leq S^\circ$ and set $T := C_G(D)^\circ$. Then D contains a central involution of S by [18, ex. 12, p. 14] which means that i is central in S, since j and ij are conjugate in S for $j \in D \backslash \langle i \rangle$.

Proposition 4.50 *$G = \langle C_G(k)^\circ |\ k \in D_1^* \rangle$ for any four-subgroup $D_1 \leq G$ and $O(C_G(k)) = 1$ for all $k \in D^*$.*

Proof. $O(C_G(t)) = 1$ for all $t \in D^*$ by Proposition 4.2 and $G = \langle C_G(k)^\circ |\ k \in D_1^* \rangle$ for any four-subgroup $D_1 \leq G$ by Corollary 3.17. □

Corollary 4.51 *$C_G(k)^\circ$ is nonabelian for all $k \in D^*$.*

Proof. Assume that $C_G(j)^\circ$ is abelian for some $j \in D^*$. Then $C_G(j)^\circ \leq C_G(i)^\circ$ since $i \in C_G(j)^\circ$. As furthermore j and ij are conjugate, $G = C_G(i)^\circ$ by Proposition 4.50. Contradiction. □

Corollary 4.52 *Let $j \in D^*$. If i and j are not conjugate in G, then $C_G(j)^\circ \cong \mathrm{PSL}_2(K) \times K^*$.*

Proof. Let $j \in D^*$ be not conjugate to i. Then j is conjugate to ij in $C_G(i)^\circ$. Now $C_G(j)^\circ$ is not abelian by Corollary 4.51. Furthermore $C_G(D)^\circ \cong K^* \times K^*$ and there are only three possibilities by Proposition 4.2, namely $C_G(j)^\circ \cong \mathrm{GL}_2(K)$, $C_G(j)^\circ \cong \mathrm{PSL}_2(K) \times K^*$ or $C_G(j)^\circ \cong \mathrm{SL}_2(K) * \mathrm{SL}_2(K)$. The first and third case cannot occur since i and ij are not conjugate, which proves the claim. □

We have to distinguish two different cases:

(i) $C_G(i)$ is connected.

(ii) $C_G(i)$ is not connected.

We are going to show that $G \cong \mathrm{G}_2(K)$ in the first case and $G \cong \mathrm{PSp}_4(K)$ in the second case. Assume from now on that $D = \langle i, j \rangle$.

Lemma 4.53 *If $C_G(i)$ is connected, then G contains one conjugacy class of involutions.*

Proof. $S \leq C_G(i)$, since $i \in Z(S)$. As Sylow 2-subgroups of G are conjugate, and $C_G(i)$ contains only two conjugacy classes of involutions i and $j^{C_G(i)}$ by Lemma 3.19, it is enough to show that i and j are conjugate.

Assume that j is not conjugate to i and let $w \in N_G(T)$ such that $D\langle w\rangle$ is an elementary abelian 2-subgroup of order 8. Then $C_G(D) = T\langle w\rangle$ and w inverts T. As i and ij are not conjugate in G, $C_G(j)^\circ \cong \mathrm{PSL}_2(K) \times K^*$ by Corollary 4.52. Let $u \in (N_G(T) \cap C_G(j)^\circ)\backslash T$ be an involution. Then $u \in C_G(D)$, i.e. since $C_G(D) = T\langle w\rangle$, $u = tw$ for some $t \in T$. Thus u has to invert T. Contradiction as $Z(C_G(j)^\circ) \leq T$ is infinite. □

Corollary 4.54 *If $C_G(i)$ is connected, then $G \cong \mathrm{G}_2(K)$.*

Proof. If $C_G(i)$ is connected, then G contains one conjugacy class of involutions by Lemma 4.53. Since furthermore the centralisers of involutions in $\mathrm{G}_2(K)$ are isomorphic to $\mathrm{SL}_2(K) * \mathrm{SL}_2(K)$, the claim follows by Theorem 4.49. □

Lemma 4.55 $N_G(L_1) = C_G(i)^\circ C_G(C_G(i)^\circ)$.

Proof. As $C_G(i)^\circ C_G(C_G(i)^\circ) \leq N_G(L_1)$, we only need to prove the reverse inclusion. Let $g \in N_G(L_1)$. As $Z(L_1) = \langle i\rangle$, $g \in C_G(i)$ and $g \in N_G(L_2)$ as well by [18, 7.1]. By Lemma 4.45 and Lemma 4.46, $g \in C_G(L_1)L_1 \cap C_G(L_2)L_2$. Thus there exists $l_n \in L_n$ for $n = 1, 2$ such that $gl_n \in C_G(L_n)$. As L_1 and L_2 commute, $gl_1l_2 \in C_G(L_1) \cap C_G(L_2)$ and hence $g \in C_G(C_G(i)^\circ)C_G(i)^\circ$. □

Set $K_s := C_G(C_G(s)^\circ)$ for all involutions $s \in G$.

Lemma 4.56 *Let $s \in I(G)$. Then $K_s \cap C_G(s)^\circ = Z(C_G(s)^\circ)$. Furthermore*

(i) K_i is a finite group,

(ii) $I(K_i) = i$,

(iii) $K_i \cap K_s = 1$ for all $s \in D^*$ such that $i \neq s$.

Proof. As $Z(C_G(i)^\circ) = \langle i\rangle$, $K_i \leq C_G(i)$ and $K_i \cap C_G(i)^\circ = \langle i\rangle$. Hence $K_i^\circ \leq C_G(i)^\circ \cap K_i = \langle i\rangle$ and K_i is a finite group, proving (i).

To show (ii) let $t \in I(K)$ be an involution. Then $O(C_G(t)) = 1$ by Corollary 3.16. Assume that $C_G(t)^\circ > C_G(i)^\circ$. Then $C_G(t)^\circ \cong \mathrm{G}_2$ or $C_G(t)^\circ \cong \mathrm{PSp}_4(K)$ by Fact 3.9 as $pr(C_G(t)^\circ) = pr(G) = 2$. However this would imply that $C_G(j)^\circ, C_G(ij)^\circ \leq C_G(t)^\circ$ by Proposition 4.2 and $G = C_G(t)^\circ$ by Proposition 4.50. Contradiction. Thus $C_G(t)^\circ = C_G(i)^\circ = C_G(it)^\circ$ and $t = i$, as otherwise $\langle i, t\rangle$ is a four-subgroup and $G = C_G(i)^\circ$ by Proposition 4.50.

Let finally $s \in D^*$ such that $s \neq i$. As $C_G(i)^\circ, C_G(s)^\circ \leq C_G(K_i \cap K_s)$ and si is conjugate to s in $C_G(i)^\circ$, [19, 5.14] and Proposition 4.50 imply that $C_G(K_s \cap K_t)^\circ = G$. As G is simple, $K_i \cap K_s = 1$. □

Corollary 4.57 *$C_G(i) = (C_G(i)^\circ * K_i) \rtimes \langle v \rangle$ for any $v \in G$ such that $L_1^v = L_2$. In this case $v^2 \in C_G(i)^\circ K_i$ and we can choose $v \in N_G(T)$ to be a 2-element.*

Proof. Assume that there exists an element $v \in G$ such that $L_1^v = L_2$. As $Z(L_1) = Z(L_2) = \langle i \rangle$, $v \in C_G(i) \backslash C_G(i)^\circ$, $L_2^v = L_1$ by [18, 7.1] and $v^2 \in C_G(i)^\circ K_i$ by Lemma 4.55.

Let $x \in C_G(i)$. There are two possibilities: Either $x \in N_G(L_1) = C_G(i)^\circ * K_i$ by Lemma 4.55 and Lemma 4.56 or $L_1^x = L_2$ and $L_2^x = L_1$ by [18, 7.1]. In the second case $xv \in N_G(L_1) = C_G(i)^\circ K_i$ by Lemma 4.55 again. Thus $x \in (C_G(i)^\circ * K_i) \rtimes \langle v \rangle$ in all cases.

Let finally $d(v) = V \times F$, where V is a connected divisible group and $F = \langle f \rangle$ a finite cylic group by [18, ex. 10, p. 93]. Then $V \leq C_G(i)^\circ$ and $f^2 \in N_G(L_1)$. Thus f has even order. Let $o(f) = 2^k m$ where $k \geq 1$ and $m \in \mathbb{N}$ is odd. Then f^m is a 2-element such that $L_1^{f^m} = L_2$. Furthermore f^m is contained in a Sylow 2-subgroup of $C_G(i)$ and as they are all conjugate to each other, we may assume that $f^m \in N_G(T)$. □

Lemma 4.58 *If all involutions in D are conjugate, then $K_i = \langle i \rangle$.*

Proof. Assume that all involutions in D are conjugate. Then there exists an element $y \in N_G(T)$, such that $i^y = j$ by [18, 10.22]. Let $w \in N_G(T) \cap C_G(i)^\circ$ such that $E := D\langle w \rangle$ is an elementary abelian 2-subgroup of order 8. w inverts T and all other involutions that invert T are contained in $wC_G(T) = wTK_i$ by Corollary 4.57. However, $I(wTK_i) = wT$ by Lemma 4.56 and $w^y \in wT$. K_i acts hence on $C_G(j)^\circ$ centralising $T\langle w \rangle$. Thus $K_i \leq C_G(j)^\circ K_j$ by Corollary 4.57. Let $k \in K_i$ and $x \in C_G(j)^\circ$, $k_1 \in K_j$ such that $k = xk_1$. Then $x = kk_1^{-1} \in C_G(E) \cap C_G(j)^\circ = E$. Thus $K_j \leq EK_i$. Furthermore $K_{ij} = K_j^{w_1} \leq EK_i$, where $w_1 \in L_1 \cap N_G(E)$ is an involution conjugating j and ij. Let now $k := |K_i|$. As all involutions in D are conjugate, $k = |K_l|$ for all $l \in D^*$. Furthermore $|EK_i| = 4k$ as $E \cap K_i = \langle i \rangle$. On the other hand $K_i, K_j, K_{ij} \leq EK_i$ and all three subgroups normalise each other. Hence $k^3 \leq 4k$ by Lemma 4.56 and $k = 2$. Thus $K = \langle i \rangle$, if all involutions in D are conjugate. □

Proposition 4.59 *If all involutions in D are conjugate, then $C_G(i)$ is connected.*

Proof. Suppose that all involutions in D are conjugate. Then $K_i = \langle i \rangle$ by Lemma 4.58. Assume that $C_G(i)$ is not connected. Then there exists a 2-element

$v \in N_G(T)$ such that $C_G(i) = C_G(i)^\circ \rtimes \langle v \rangle$ where $L_1^v = L_2$ by Lemma 4.57. As $v^2 \in C_G(i)^\circ$ is a 2-element, it is contained in a maximal torus of $C_G(i)^\circ$. As maximal tori are divisible, there exists an element $t \in C_G(i)^\circ$, such that $t^2 = v^2$. Assume that $t = t_1 t_2^v$, where $t_1, t_2 \in L_1$. Then

$$(*) \quad 1 = v^2 t^{-2} = v^2 (t_2^{-2v} t_1^{-2}) = v t_2^{-2} v t_1^{-2}.$$

On the other hand $v^2 \in C_G(v)$ and thus $t_1^2 t_2^{2v} = (t_1^2 t_2^{2v})^v = t_2^{2v^2} t_1^{2v}$. This implies that

$$t_2^{-2v^2} t_1^2 = t_1^{2v} t_2^{-2v} \in L_1 \cap L_2 = \langle i \rangle$$

Hence either $t_1^2 = t_2^2$ or $t_1^2 = i t_2^2$. Set $s := t_1^2$. If $t^2 = s s^v$, then $(*)$ implies that vs^{-1} is an involution. If $t^2 = iss^v$, then $(vs^{-1})^2 = i$. By replacing v with a conjugate of vs^{-1}, we may assume that $v \in N_G(T)$, such that $v^2 \in \langle i \rangle$.

As all involutions in D are conjugate and j is conjugate to ij in $C_G(i)$, there exists an element $y \in N_G(T)$, such that $i^{y^2} = j^y = ij$ by [18, 10.22], where $y^3 \in T$. Furthermore $v \in C_G(D)$ and v does not invert T. This implies that $v \in C_G(j) \backslash C_G(j)^\circ$ and $v \in C_G(ij) \backslash C_G(ij)^\circ$. Thus there exist elements $x_1, x_2 \in C_G(D)$ such that $v^y = v x_1$ and $v^{y^2} = v x_2$, where $x_1 \in C_G(j)^\circ$ and $x_2 \in C_G(ij)^\circ$ by Corollary 4.57.

Let $P := C_T(v)^\circ$. Then $P = \{l l^v | l \in T \cap L_1\}$ and $C_T(v) = P\langle i \rangle$. On the other hand x_n either inverts T or centralizes it for some $n = 1, 2$. If x_n would centralize T for $n = 1, 2$, then $P = C_T(v x_n)^\circ = (C_T(v)^{y^n})^\circ = P^{y^n}$. Contradiction as P contains a unique involution from D. Thus x_1 and x_2 invert T.

Let $T[v] := \{t \in T | t^v = t^{-1}\}$. Then $T[v] \leq T$ and $T[v]^\circ = \{l l^{-v} | l \in T \cap L_1\}$. Obviously $T = PT[v]$. As x_n inverts T for $n = 1, 2$, $C_T(x^{y^n}) = C_T(v x_n) = T[v]$. Thus $T[v]^\circ = (C_T(v^y)^\circ)^y = (T[v]^\circ)^y$. Contradiction again, as $T[v]^\circ$ contains a unique involution from D. Hence $C_G(i) = C_G(i)^\circ$ is connected. □

Proposition 4.60 *If $C_G(i)$ is not connected, then $C_G(i) = C_G(i)^\circ \rtimes \langle u \rangle$, where $u \in C_G(D)$ is an involution such that $L_1^u = L_2$.*

Proof. As $C_G(i)$ is not connected, i and j are not conjugate in G by Proposition 4.59 and $C := C_G(j)^\circ \cong \mathrm{PSL}_2(K) \times K^*$ by Corollary 4.52. Let $u \in (N_G(T) \cap C) \backslash T$ be an involution. Then $u \in C_G(D)$ but $u \notin C_G(i)^\circ$, as u does not invert T. Thus $C_G(i) = C_G(i)^\circ K_i \langle u \rangle$ by Lemma 4.57 and we need to show that $K_i = \langle i \rangle$.

As K_i centralizes $Z(C)$, $K_i \leq K_j C$ by Lemma 4.45 and Lemma 4.46. We show that $C_{K_i}(u) = \langle i \rangle$. u acts on K_i. Let $k \in C_{K_i}(u)$. Then k centralizes the elementary abelian subgroup $E_1 := \langle i, j, u \rangle$. As $K_i \leq K_j C$ and $C_C(E_1) =$

$Z(C)\langle u\rangle$, we must have $k \in K_j\langle u\rangle$ by Lemma 4.56. Thus $k^2 \in K_j \cap K_i = 1$ by Lemma 4.56 and $k \in \langle i\rangle$ by Lemma 4.56 again. Especially $C_{K_i}(u) = \langle i\rangle$.

As $|K_i|/|C_{K_i}(u)| = |S|$, where $S = \{[k,u] |\, k \in K_i\} \subseteq K_i$ consists of elements inverted by u by [18, ex. 17, p. 7], $2|S| = |K_i|$. Let $s \in S$. Then $u^s \in C$ and $u^s = s^u us = us^2$. Furthermore s centralizes T and thus $u^s \in N_G(T)\backslash T$ which implies that there exists a $t \in T$ such that $us^2 = u^s = ut$. Hence $s^2 = t \in K_i \cap T = \langle i\rangle$. Assume that $s^2 = i$. Then $u^s = ui$. As $\langle j, u\rangle$ is conjugate to D in C, u and uj belong to different conjugacy classes. However, there are at most two conjugacy classes of involutions in $uC_G(i)^\circ$ by Lemma 3.19, namely u^T and $(ui)^T$. Contradiction. Hence $s^2 = 1$ by Lemma 4.56 and $s \in \langle i\rangle$. Then $|K_i| = 2|S| \leq 4$.

We finally prove that $|S| = 1$. Assume that $|S| = 2$. Then $|K_i| = 4$ and there exists an element $k \in K_i$ of order 4 by Lemma 4.56. As $C_{K_i}(u) = \langle i\rangle$, $k^u = k^3 = k^{-1}$. Especially $u^k = k^u uk = uk^2 = ui$. Contradiction as before and we are done. $\square$

Proposition 4.61 *If $C_G(i)$ is not connected, $C_G(j) \cong (\mathrm{GL}_2(K)/\langle -I\rangle) \rtimes \langle w\rangle$ where $-I = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $w \in C_G(D) \cap C_G(i)^\circ$ is an involution that acts as an inverse-transpose automorphism on $\mathrm{GL}_2(K)$, i.e.*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^w = (ad - bc)^{-1} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

for any $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$.

Proof. As $C_G(i)$ is not connected, $C_G(j)^\circ \cong \mathrm{PSL}_2(K) \times K^* \cong \mathrm{GL}_2(K)/\langle -I\rangle$ by Proposition 4.59 and Corollary 4.52. Set $C := C_G(j)^\circ$.

Let $w \in C_G(D) \cap C_G(i)^\circ$ be an involution that inverts T. We show that $C_G(j) = C \rtimes \langle w\rangle$. As w inverts T, $w \notin C$ and $C_G(j) \geq C \rtimes \langle w\rangle$. To prove the other inclusion let $\overline{C} := C/Z(C)$. By Lemma 4.45 $C_G(j) = C_{C_G(j)}(\overline{C})C$. Let $h \in C_{C_G(j)}(\overline{C})$. Then $T^h \leq TZ(C) = T$ and $h \in N_G(T)$. As $h \in C_G(j)$ and i and ij are not conjugate, $h \in C_G(D) = T\langle u, w\rangle$. Thus, as $T\langle u\rangle \leq C$, $C_G(j) = C\langle w\rangle = C_{C_G(j)}(\overline{C})C$.

As w inverts T, $w \notin C_{C_G(j)}(\overline{C})$. Thus there exists $v \in C_G(D)$ such that $wv \in C_{C_G(j)}(\overline{C})$. w inverts T and $v \in C$, hence wv inverts $Z(C)$. Furthermore $[wv, C] \subseteq Z(C)$ and $C = Z(C) * C_C(wv)$ by [18, ex. 10, p. 98] where $Z(C) \cap C_C(wv) = \langle j\rangle$. Set $H := C_C(wv)^\circ$. As $C \cong \mathrm{PSL}_2(K) \times K^*$, $H \cong PSL_2(K)$ and $C = Z(C) \times H$. We may assume that $v \in H$.

Let $x \in C$. Then there exists $z \in Z(C)$ and $h \in H$ such that $x = zh$. Furthermore $x^{wv} = z^{-1}h$, and $x^w = z^{-1}h^v$. Thus $h^w = h^v$ for all $h \in H$. Set $T_1 = H \cap T$. As w inverts T_1, v has to invert T_1 as well. Hence $v \in I(N_G(T_1)\backslash T_1)$

and after maybe conjugating w with an element from T, we may assume that v corresponds to $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. This implies the claim. (Compare Section 3.2.) □

Proof of Theorem 4.44. Let G be as in Theorem 4.44. If $C_G(i)$ is connected, then $G \cong \mathrm{G}_2(K)$ by Corollary 4.54. If on the other hand $C_G(i)$ is not connected, $C_G(i)$ and $C_G(j)$ are isomorphic to centralizers of involutions in $\mathrm{PSp}_4(K)$ by Proposition 4.60 and Proposition 4.61. (Compare Section 3.2. again.) Thus $G \cong \mathrm{PSp}_4(K)$ by Theorem 4.48. □

4.2.2 $\mathrm{PSp}_4(K)$

This section is devoted to the proof of Theorem 4.48. Let G be as in Theorem 4.48. Then $C_G(i) = (L_1 * L_2)\langle u \rangle$ where $L_n \cong \mathrm{SL}_2(K)$ for $n = 1, 2$, u is an involution in G such that $L_1^u = L_2$, and furthermore $L_1 \cap L_2 = Z(L_1) = Z(L_2) = \langle i \rangle$. We may furthermore assume as in the proof of Theorem 3.18 that there exists a Sylow 2-subgroup S of G, such that $i, j \in S^\circ$ and $S \leq C_G(i)$. Let $D := \langle i, j \rangle$ and $T := C_G(D)^\circ$.

We are going to construct a BN-pair of G, where N is $N_G(T)$ and $B := N_G(Q)^\circ$ for a maximal quasiunipotent subgroup Q of G. Let U be a maximal quasiunipotent subgroup of L_1 that is normalized by T and $f := rk(Z(C_G(j)^\circ))$.

Lemma 4.62 *$W := UU^u$ is properly contained in a maximal quasiunipotent subgroup of G which is normalized by T.*

Proof. W is a maximal quasiunipotent subgroup of $C_G(i)$. Assume that W is already a maximal quasiunipotent subgroup of G. Let $V := C_W(u)$. Then $rk(V) \geq f$ by Lemma 4.20 and V is normalized by T. We may assume by Lemma 3.19 that $u \in C_G(j)^\circ$ and that u is conjugate to ij in $C_G(j)^\circ$. Thus V is a maximal quasiunipotent subgroup of $C_G(u)$ and $rk(V) = f$. Consider now $N_G(V)^\circ$ and let D_1 be a four-subgroup of $C_G(u)$ such that $C_G(D_1)^\circ$ normalises V. Then $N_G(V)^\circ = \langle C_{N_G(V)}(l)^\circ |\ l \in D_1^* \rangle$ by [19, 5.14]. Since W normalises V, $N_G(V)^\circ$ cannot be solvable because otherwise $u \in N_G(V)^\circ \leq N_G(W)^\circ = TW \leq C_G(i)^\circ$ by Proposition 2.20 and Proposition 2.16 since W normalises V. Let B be a Borel subgroup of $N_G(V)$ such that $W \leq B$. B contains a maximal normal quasiunipotent subgroup by Proposition 2.16 which must be equal to W by assumption. This implies that $B \leq N_G(W)^\circ \cap N_G(V)^\circ = TW \cap N_G(V)^\circ = Z(C_G(u)^\circ)W$ by Proposition 2.20 again. Especially $pr(B) = 1$. On the other hand there exists a Borel subgroup B_1 of $N_G(V)^\circ$ such that $C_G(D_1)^\circ \leq B_1$. Then $pr(B_1) = 2$. Contradiction as Borel subgroups of K-groups are conjugate by Proposition 1.6. □

Proposition 4.63 *There exists a maximal quasiunipotent subgroup X of $C_G(j)$ which is normalized by T, such that $Q := W\langle X, X^{w_2}\rangle$ is a maximal quasiunipotent subgroup of G, where w_2 is an involution in $(L_2T \cap N_G(T))\backslash T$.*

Proof. Consider $C_G(U)^\circ$. $C_G(U)$ has Prüfer 2-rank 1, since $C_G(T)^\circ = T$. Thus, since $L_2 \leq C_G(U)^\circ$, $C_G(U)^\circ$ is not solvable and $C_G(U)^\circ/\sigma$ is isomorphic to $\mathrm{PSL}(2, K)$ where σ is the solvable radical of $C_G(U)^\circ$ by [2] and Lemma 3.11. Let Q be a maximal quasiunipotent subgroup of G which contains $W = UU^u$. By Lemma 4.62 $W < Q$. By Proposition 2.18 we can choose Q to be normalized by T. Assume that $Q\cap\sigma = U$. Then $Q\sigma/\sigma \cong Q/U > W/U \cong U^u$ is a quasiunipotent subgroup of $C_G(U)^\circ/\sigma$. Contradiction. Hence $Q \cap \sigma > U$. On the other hand $Q \cap \sigma$ is the maximal quasiunipotent subgroup of σ and thus normal in $C_G(U)^\circ$. In particular $(Q \cap \sigma)^{w_2} = Q \cap \sigma$. Furthermore $Q(\sigma) = \langle C_{Q(\sigma)}(l) |\; l \in D^*\rangle$ by [19, 4.6], i.e. $Q \cap \sigma = U\langle C_{Q\cap\sigma}(j)^\circ, C_{Q\cap\sigma}(ij)^\circ\rangle$. As $j^{w_2} = ij$ and $Q \cap \sigma > U$, there is a maximal quasiunipotent subgroup X of $C_G(j)$ such that $Q \cap \sigma = U\langle X, X^{w_2}\rangle$ and X is normalized by T since $Q \cap \sigma$ is. Hence $C_G(U)^\circ$ contains a maximal quasiunipotent subgroup Q of G such that $Q = UU^u\langle X, X^{w_2}\rangle$. □

Let $\overline{x} := xT$ for all $x \in N_G(T)$

Lemma 4.64 *(i) $W := N_G(T)/T$ is a finite group of order 8, which is generated by $\overline{u}$ and $\overline{w}_2$. The other elements of W are $\overline{1}$, $\overline{w_1} = \overline{w}_2^{\overline{u}}$, $\overline{w} = \overline{w}_2^{\overline{u}}\overline{w}_2 = \overline{w}_2\overline{w}_2^{\overline{u}}$, $\overline{uw} = \overline{wu} = \overline{u}^{\overline{w}_2}$, $\overline{uw_2}$ and $\overline{w}_2\overline{u} = \overline{uw_1}$.*

(ii) $uTXu \subseteq TXuX$ and $w_2TU^uw_2 \subseteq TU^uw_2U^u$.

(iii) $C_G(j)^\circ = \langle T, X, u\rangle$ and $C_G(i)^\circ = \langle T, W, w_1, w_2\rangle$.

(iv) $X^{w_2u} = X^{w_2}$ and $U^{w_2} = U$.

Proof. (i) follows directly from the definitions noting that $N_G(T) \leq C_G(i)$.

$C_G(j)^\circ$, being a reductive algebraic group of rank 1, has a BN-pair (B_1, N_1), where $B_1 := TX$ and $N_1 = \langle u, T\rangle$. Hence $uTXu \subseteq TX \cup TXuX = TXuX$ and $C_G(j)^\circ = \langle B_1, N_1\rangle$. L_2T has a BN-pair (B_2, N_2), where $B_2 := TU^u \cap L_2$ and $N_2 = \langle w_2, T\rangle$. This gives us that $w_2TU^uw_2 \subseteq TU^uw_2U^u$ and $L_2T = \langle B_2, N_2\rangle$. This implies (ii) and (iii) as $(L_1T)^u = L_2T$.

Furthermore $C_G(j)^\circ$ contains exactly two quasiunipotent subgroups that are normalized by T and swapped by u and w. In particular $X^{uw} = X$ and $X^{w_2u} = X^{uw_1(w_2w_2)} = X^{w_2}$. Finally, $U \leq L_1$ is normalized by w_2 as $w_2 \in L_2T$, proving (iv). □

Proposition 4.65 *There exists a quasiunipotent subgroup Q of G which is normalized by T such that*

(i) $Q = Y \rtimes X$, where Y is normalized by u and

(ii) $Q = Z \rtimes U^u$, where Z is normalized by w_2.

Furthermore $Q = \langle W, X, X^{w_2}\rangle$.

Proof. We have chosen $\langle X, X^{w_2}\rangle \leq C_G(U)$ by Proposition 4.63. Thus U centralizes X^{w_2} and U^u centralizes $X^{w_2 u} = X^{w_2}$ by Lemma 4.64. Set $Y := WX^{w_2}$. Then Y is a quasiunipotent group that is normalized by u by Fact 2.4. Furthermore $Q := YX$ is a maximal quasiunipotent subgroup of G by Proposition 4.63. Thus Y has infinite index in $N_Q(Y)$ by [18, 6.3], as $Q > Y$. As $N_Q(Y)$ is normalized by T, $N_Q(Y)^\circ = \langle C_{N_Q(Y)}(l)^\circ | \; l \in D^*\rangle$ by [19, 4.6]. Hence $X \leq N_Q(Y)$ and $Q = Y \rtimes X$.

Set $Z := U\langle X, X^{w_2}\rangle$. Then $Z \leq Q$ is normalized by w_2 by Lemma 4.64. Furthermore U^u normalizes Z by the proof of Proposition 4.63 and $Q = Z \rtimes U^u$. □

We are now in the position to construct a BN-pair of our group G.

Theorem 4.66 *G is a split BN-pair of Tits rank 2, where $B := N_G(Q)^\circ$, $N := N_G(T)$ and $\overline{u}, \overline{w}_2$ are the generators of the Weyl group.*

Note that this proves our result, Theorem 4.48, by Theorem 4.1.

Proof. By Corollary 3.17, $G = \langle C_G(k)^\circ | \; k \in D^*\rangle$. Since $\langle N, UU^u\rangle \geq C_G(i)^\circ$, $\langle N, X\rangle \geq C_G(j)^\circ$ and $\langle N, X^{w_2}\rangle \geq C_G(ij)^\circ$ by Lemma 4.64, it follows that $G = \langle B, N\rangle$. As $B = QT$ by Proposition 2.20, $B \cap N = T \lhd N$ and BN1 is valid. Furthermore we have $\langle \overline{u}, \overline{w}_2\rangle = N_G(T)/T$ by Lemma 4.64 proving BN2. Let $S := \{\overline{u}, \overline{w}_2\}$ and $W := N/T$.

To prove BN3 we will show that $vBw \subseteq BvwB \cup BvB$ for all $v, w \in N$ such that $\overline{v} \in W$ and $\overline{w} \in S$. This is obviously equivalent to the original condition. By Lemma 4.64 and Proposition 4.65

$$uBu = uTXYu \subseteq TXuXY \subseteq BuB$$

$$w_2Bu = w_2TXYu = TX^{w_2}w_2uY \subseteq Bw_2uB$$

$$uwBu = uwTXYu = TX(uw)uXY \subseteq B(uw)uB$$

$$uw_2Bu = uw_2TXYu = TX^{w_2}(uw_2)uY \subseteq B(uw_2)uB.$$

Thus

$$w_1Bu = (uw_2)uBu \subseteq uw_2BuB \subseteq Buw_2uB = Bw_1B$$

$$wBu = (wu)uBu \subseteq wuBuB \subseteq BwB$$

$$w_2uBu \subseteq w_2BuB \subseteq Bw_2uB.$$

Now $1Bw \subseteq B1wB$ for all $w \in N$ and there are only seven cases left. By Lemma 4.64 and Proposition 4.65 again

$$uBw_2 = uTU^uZw_2 = TUuw_2Z \subseteq Buw_2B$$

$$w_2Bw_2 = w_2TU^uZw_2 \subseteq TU^uw_2U^uZ \subseteq Bw_2B$$

$$w_1Bw_2 = w_1TU^uZw_2 = TU^uw_1w_2Z \subseteq Bw_1w_2B$$

$$w_2uBw_2 = w_2uTU^uZw_2 = TUw_2uw_2Z \subseteq Bw_2uw_2B$$

Hence

$$wBw_2 = w_1w_2Bw_2 \subseteq w_1Bw_2B \subseteq Bw_1w_2B = BwB$$

$$uwBw_2 = (w_2u)w_2Bw_2 \subseteq w_2uBw_2B \subseteq Bw_2uw_2B = BuwB$$

$$uw_2Bw_2 \subseteq uBw_2B \subseteq Buw_2B$$

and BN3 is valid. By Proposition 4.65 finally $Q = XY = U^uZ$, $Q^u = X^uY \neq Q$ and $Q^{w_2} = U^{uw_2}Z \neq Q$ which proves BN4 and gives us the theorem. □

4.2.3 $\mathrm{G}_2(K)$

In this section we prove Theorem 4.49. Let G be as in Theorem 4.49, $D := \langle i_0, i_1\rangle$ a four-subgroup which is contained in the connected component of a Sylow 2-subgroup of G and set $i_2 = i_0i_1$. Let furthermore $T := C_G(D)^\circ$. Then $C_G(i_0)$ contains four quasiunipotent subgroups which are normalized by T and isomorphic to K^+. Let X and Y be two of them that centralize each other and let v be an involution in $N_{C_G(i_0)}(T)\backslash T$ that normalizes X. Write $\overline{x} := xT$ for all $x \in N_G(T)$.

Lemma 4.67 *Let* $W := N_G(T)/T$. *Then* $|W| = 12$ *and* W *is generated by two involutions* $\overline{w}$ *and* $\overline{v}$, *where* $w \in I(C_G(i_1))$, *such that* $i_0^{wv} = i_1 = i_2^{vw}$ *and* $o(wv) = 6$. *The center of* W *is* $\langle \overline{z} \rangle$ *where* $z := (wv)^3$. *Set* $y := (wv)^4 = (wv)z$ *and* $w_{k+1} := w^{y^k}$, $v_k := v^{y^k}$ *for* $k \in \mathbb{N}$. *Then* $\overline{w}_k = \overline{w_{k+3}}$ *and* $\overline{v}_k = \overline{v_{k+3}}$. *The elements in* W *are hence*

$$\overline{1}, \overline{z} = \overline{(wv)^3}, \overline{wv} = \overline{yz}, \overline{(wv)^2} = \overline{y^{-1}}, \overline{(wv)^4} = \overline{y}, \overline{(wv)^5} = \overline{vw} = \overline{y^{-1}z}$$

and

$$\overline{w}_{k+1} = \overline{w^{(vw)^{2k}}} = \overline{y^k w} \text{ and } \overline{v}_k = \overline{v^{(vw)^{2k}}} = \overline{y^k v}$$

for $k = 0, 1, 2$.

Proof. As G contains one conjugacy class of involutions, all involutions of D are conjugate in $N_G(T)$ by [18, 10.22]. $N_G(D)/C_G(D) \cong S_3$, $N_G(T) = N_G(D)$ and $|C_G(D)/C_G(T)| = 2$, which implies that W is the dihedral group of order 12. $\square$

Lemma 4.68 *Let* w_0, v_0 *as in Lemma 4.67. Then* $w_0 T X w_0 \subseteq T X w_0 X$ *and* $v_0 T Y v_0 \subseteq T Y v_0 Y$. *Furthermore* $C_G(i_0)^\circ = \langle T, X, Y, v_0, w_0 \rangle$.

Proof. $L := \langle X, T, X^{w_0} \rangle$ is a reductive algebraic group of rank 1. L has thus a BN-pair (B_1, N_1), where $B_1 := TX$ and $N_1 = \langle w_0, T \rangle$. Hence $w_0 T X w_0 \subseteq TX \cup TXw_0X = TXw_0X$ and $L := \langle T, X, w_o \rangle$. The same argument for $\langle Y, T, Y_0 \rangle$ yields the remaining part of the lemma. $\square$

Lemma 4.69 *Let* $X_1 := X$, $Y_1 := Y$, $X_2 := X_1^{w_0}$, $Y_2 := Y_1^{v_0}$ *and* $X_n^{(\lambda)} := X_n^{y^\lambda}$ *as well as* $Y_n^{(\lambda)} := Y_n^{y^\lambda}$ *for any* $n = 1, 2$ *and* $\lambda \in \mathbb{Z}$. *Then*

(i) $X_n^{(\lambda)} = X_n^{(\lambda+3)}$ *and* $Y_n^{(\lambda)} = Y_n^{(\lambda+3)}$ *for all* $n = 1, 2$ *and* $\lambda \in \mathbb{Z}$.

(ii) v_λ *centralizes* $X_n^{(\lambda)}$ *and* w_λ *centralizes* $Y_n^{(\lambda)}$ *for* $\lambda = 0, 1, 2$ *and* $n = 1, 2$.

(iii) $(X_1^{(\kappa)})^{w_\lambda} = X_2^{(2\kappa-\lambda)}$ *and* $(X_1^{(\kappa)})^{v_\lambda} = X_1^{(2\kappa-\lambda)}$ *for* $\kappa, \lambda = 0, 1, 2$.

(iv) $(Y_1^{(\kappa)})^{w_\lambda} = Y_1^{(2\kappa-\lambda)}$ *and* $(Y_1^{(\kappa)})^{v_\lambda} = Y_2^{(2\kappa-\lambda)}$ *for* $\kappa, \lambda = 0, 1, 2$.

Proof. Since $\overline{y^3} = \overline{1}$, (i) follows. We have furthermore chosen w_0 such that w_0 centralizes Y_1. Hence v_0 has to centralize X_1 which yields (ii). To prove (iii) note that $\overline{y^\lambda} = \overline{w_\lambda w_0} = \overline{v_\lambda v_0}$ and hence

$$\overline{y^\kappa w_\lambda y^{\lambda-2\kappa} w_0} = \overline{y^{3\kappa-\lambda} w_\lambda w_0} = \overline{y^{-\lambda} y^\lambda} = \overline{1}$$

and

$$\overline{y^{\kappa}v_{\lambda}y^{\lambda-2\kappa}v_0} = \overline{y^{3\kappa-\lambda}v_{\lambda}v_0} = \overline{1}$$

for $\lambda, \kappa \in 0,1,2$. Since however $X_1^{w_0} = X_2$, $X_1^{v_0} = X_1$, $Y_1^{w_0} = Y_1$ and $Y_1^{v_0} = Y_2$ by (ii), (iii) and (iv) follow. □

Lemma 4.70 *Let G be a connected K-group of finite Morley rank such that the solvable radical σ of G is finite. Then G is a central product of quasi-simple algebraic groups over algebraically closed fields.*

Proof. Since any definable action of a definable connected group on a finite set is trivial $\sigma = Z(G)$. Furthermore G/σ is isomorphic to the direct product of simple algebraic groups over algebraically closed fields by [2]. Then $G/\sigma = (G/\sigma)' = G'\sigma/\sigma \cong G'/(G' \cap \sigma)$ and $rk(G) = rk(G')$. As G is connected, $G = G'$ and G is semisimple. Assume that G is quasi-simple. Then G is an algebraic group by [4]. Let now $G/\sigma \cong A_1 \times \cdots \times A_m$ for some $m \in \mathbb{N}$, where A_i are simple algebraic groups over algebraically closed fields for $1 \le i \le m$. Let G_i be the preimages of A_i in G for $1 \le i \le m$. Then $G = G_1^\circ ....G_m^\circ$. Now $[G_i^\circ, G_j^\circ]$ is a connected subgroup of σ and hence trivial for any $1 \le i < j \le m$. Furthermore $[G_i^\circ, G_i^\circ] = G_i^\circ$ for any $1 \le i \le m$ as above. Thus G is a central product of m quasi-simple algebraic groups by the first case. □

Proposition 4.71 *If $char(K) \neq 3$ then there exists an element t of order 3, such that $C_G(t)^\circ \cong \mathrm{SL}_3(K)$. Actually $C_G(t)^\circ \cong \mathrm{SL}_3(K)$ for exactly two elements of order 3 in T.*

Proof. Assume that $char(K)$ is not 3. Since $y^3 \in T$, $y = y't$, where we can choose y' to be a 3-element by [18, ex. 11, p. 93]. Let P be a Sylow 3-subgroup of $N_G(T)$. Since $N_G(T)$ is solvable, P is nilpotent-by-finite by [18, 6.20]. Hence there exists an element $t \in T \cap Z(P)$ by [18, ex. 12, p. 14]. It follows that t is centralized by y. Thus $(t^{w_0}t)^{y^2} = (t^{w_0}t)^{w_2 w_0} = t^{y w_0}t = t^{w_0}t$ and $t^{w_0}t \in C_T(y)$. Hence either $t^{w_0} = t^{-1}$ or $t^{w_0}t \in C_T(y)$ is an element of order 3 that is inverted by w_0. We may assume that t is inverted by w_0. Now $C_G(t)^\circ = \langle C_{C_G(t)}(l)^\circ |\ l \in D^*\rangle$ and $C_{C_G(i_0)}(t) = C_{C_G(i_1)}(t)^{y^2} = C_{C_G(i_2)}(t)^y$. However, $C_{C_G(i_0)}(t)^\circ \cong \mathrm{GL}_2(K)$.

We show that the solvable radical σ of $C_G(t)^\circ$ is finite. σ is normalized by T and hence $\sigma^\circ = \langle C_\sigma(l)^\circ | l \in D\rangle$ by [19, 4.12]. However, $C_\sigma(l)^\circ \le Z(C_{C_G(l)}(t)^\circ)$ for all $l \in D^*$ as $C_\sigma(l)^\circ$ is contained in the solvable radical of $C_{C_G(l)}(t)^\circ$. Thus $\sigma^\circ \le \bigcap_{l \in D^*} Z(C_{C_G(l)}(t)^\circ) \le T$. One the other hand $Z(C_{C_G(i_0)}(t)^\circ) \cong K^*$ and as G does not interpret a bad field, σ is either finite or $i_0 \in Z(C_{C_G(i_0)}(t)^\circ) = Z(C_{C_G(i_1)}(t)^\circ)$. The second case cannot occur since $C_G(D)^\circ = T$ and σ finite.

Thus $C_G(t)^\circ$ is a central product of quasi-simple algebraic groups by Lemma 4.70 and $C_G(t)^\circ \cong \mathrm{SL}_3(K)$. Furthermore $T \leq C_G(t)^\circ$ contains eight elements of order 3 and while y centralizes exactly t and t^{-1}, yw operates transitively on the remaining six. □

Now we can construct a BN-pair as in [16].

Proposition 4.72 *If $char(K) \neq 3$ then there exists a maximal quasiunipotent group Q in G which is normalized by T such that*

(i) $Q = V \rtimes Y_1$ where V is normalized by v_0 and

(ii) $Q = M \rtimes X_2^{(1)}$ where M is normalized by w_1.

Furthermore $Q = \langle X_1, X_2^{(1)}, X_2^{(2)}, Y_1, Y_2^{(1)}, Y_1^{(2)} \rangle$.

Proof. Since $char(K)$ is not 3, there exists an element $t \in T$ of order 3, such that $C_G(t)^\circ \cong \mathrm{SL}_3(K)$. We can hence assume that $C_G(t)^\circ$ contains the maximal quasiunipotent subgroup $U := X_1\langle X_2^{(1)}, X_2^{(2)} \rangle$, where X_1 is central in U. (Compare Section 4.2). Consider $C_G(X_1)$. We proceed as in Lemma 4.63. $U \leq C_G(X_1)$ and $L := \langle T, Y_1, Y_2 \rangle \leq C_G(X_1)$. Thus $C_G(X_1)^\circ$ is not solvable. Furthermore $C_G(X_1)^\circ$ has Prüfer 2-rank 1, since $C_G(T)^\circ = T$. Thus $C_G(X_1)^\circ/\sigma \cong \mathrm{PSL}_2(K)$ by [2] and Lemma 3.11, where σ is the solvable radical of $C_G(X_1)$. On the other hand $L\sigma/\sigma \cong L/(\sigma \cap L) \cong L/Z(L) \cong \mathrm{PSL}_2(K)$. Hence $C_G(X_1)^\circ = L\sigma^\circ$ and $U \leq \sigma$. Set $V := Q(\sigma)$. Then $V^{v_0} = V$.

Assume that $U = V$. Then Y_1U is a quasiunipotent group by Fact 2.4. Especially Y_1U is nilpotent and $W := Y_1X_1 < Y_1U$ has infinite index in $N := N_{Y_1U}(W)^\circ$ by [18, 6.3]. N is a quasiunipotent group that is normalized by T and hence $N = \langle C_N(l)^\circ |\, l \in D^* \rangle$ by [19, 4.6]. Furthermore $C_N(i_0) = W$ and $C_N(i_k)$ is either trivial or equals $X_2^{(k)}$ for $k = 1, 2$ as T normalises N and acts transitively on $X_2 \backslash \{1\}$. We may assume that $X_2^{(1)} \leq N$.

Set $P := WX_1^{(2)} \rtimes T$. Then $P \leq N_G(W)$. Let $w \in W\backslash\{1\}$ such that $C_G(w) \cap T = \langle i_0 \rangle$. As T acts transitively on $W\backslash\{1\}$, for any element $x \in P$, there exists an element $t_x \in T$ such that $w^x = w^{t_x}$. Thus $P \subseteq C_P(w)T$. As i_1 and i_2 invert W, $C_P(w)$ is a solvable group normalized by D. Thus $C_P(w)^\circ = \langle C_{C_P(w)}(l)^\circ |\, l \in D^* \rangle$ by [18, 4.6]. Furthermore $(C_P(w) \cap C_G(i_0))^\circ = W$, $(C_P(w) \cap C_G(i_1))^\circ \leq X_1^2$ and $(C_P(w) \cap C_G(i_2))^\circ = 1$. Thus $Q := C_P(w)^\circ \leq WX_1^{(2)}$ is a quasiunipotent subgroup of P containing W. Since there is a definable surjective map from $C_P(w) \times T$ onto $N_P(W)$

$$rk\big(WX_1^{(2)}\big) + rk(T) = rk\big(N_P(W)\big) \leq rk\big(C_P(w)\big) + rk(T) = rk(Q) + rk(T).$$

Thus $Q = WX_1^{(2)}$ and $N_P(W) = C_P(w)^\circ \rtimes T$. Especially $Q \leq C_P(w^t)$ for all $t \in T$ and hence $Q \leq C_G(W)$ as T acts transitively on W. Thus $X_2^{(1)} \leq C_G(W)$ and $X_2^{(1)}$ centralizes Y_1. This implies that $Y_1^{(1)} = Y_1^{w_2} \leq C_G(X_2^{(1)})^{w_2} = C_G(X_1)$. As $C_G(X_1)^\circ = L\sigma$ this implies that $Y_1^{(1)} \leq V$. Contradiction.

Hence $U < V$ and either $\langle Y_2^{(1)}, (Y_2^{(1)})^{v_0}\rangle \leq V$ or $\langle Y_1^{(1)}, (Y_1^{(1)})^{v_0}\rangle \leq V$. We may assume that $V = \langle Y_2^{(1)}, Y_1^{(2)}, U\rangle$. Set $Q := Y_1V$. Q is obviously a maximal quasiunipotent subgroup of G and V is normalized by v_0 by construction. Set $Y := \langle Y_1, Y_2^{(1)}, Y_1^{(2)}\rangle$. Then Y is invariant under w_1 and $M := Q \cap Q^{w_1} = \langle Y, X_1X_2^{(2)}\rangle$. Furthermore M is normalized by $X_2^{(1)}$, since $N_Q(M)^\circ = Q$ by [18, 6.3] as in the previous paragraph. □

Theorem 4.73 *If $char(K) \neq 3$, G is a split BN-pair of Tits rank 2, where $B := N_G(Q)^\circ$, $N := N_G(T)$ and $\overline{w}_2, \overline{v}_0$ are the generators of the Weyl group.*

Note that this proves our result, Theorem 4.49, by Fact 4.1.

Proof. $G = \langle C_G(k) |\ k \in D^*\rangle$ by Corollary 3.17 and $\langle N, X_1Y_1\rangle \geq C_G(i_0)$ by Lemma 4.9. Thus $G = \langle B, N\rangle$ as i_1, i_2 are conjugate to i_0 in N. BN1 now follows since by Proposition 2.20 $B = QT$ and thus $B \cap N = T \lhd N$. Furthermore $\langle \overline{v}_0, \overline{w}_1\rangle = N_G(T)/T$ by Lemma 4.64 proving BN2. Let $S := \{\overline{v}_0, \overline{w}_1\}$ and $W := N/T$.

To prove BN3 we will show that $vBw \subseteq BvwB \cup BvB$ for all $v, w \in N$ such that $\overline{v} \in W$ and $\overline{w} \in S$ as in Theorem 4.66. By Lemma 4.7 and Proposition 4.72

$$1Bv_0 \subseteq B1v_0B$$

$$v_0Bv_0 = v_0TY_1Vv_0 \subseteq TY_1v_0Y_1V \subseteq Bv_0B$$

$$v_2Bv_0 = v_2TY_1Vv_0 = TY_2^{(1)}v_2v_0V \subseteq Bv_2v_0B$$

$$w_0Bv_0 = w_0TY_1Vv_0 = TY_1w_0v_0V \subseteq Bw_0v_0B$$

$$w_1Bv_0 = w_1TY_1Vv_0 = TY_1^{(2)}w_1v_0V \subseteq Bw_1v_0B$$

$$y^2Bv_0 = y^2TY_1Vv_0 = TY_1^{(2)}y^2v_0V \subseteq By^2v_0B$$

$$v_0w_1Bv_0 = v_0w_1TY_1Vv_0 = TY_2^{(1)}v_0w_1v_0 \subseteq Bv_0w_1v_0B$$

and thus

$$zBv_0 = (zv_0)v_0Bv_0 \subseteq w_0Bv_0B \subseteq Bw_0v_0B = BzB$$

$$w_1v_0Bv_0 \subseteq w_1Bv_0B \subseteq Bw_1v_0B$$

$$w_2Bv_0 = (w_2v_0)v_0Bv_0 \subseteq v_0w_1Bv_0B \subseteq Bv_0w_1v_0B = Bw_2B.$$

Finally

$$yBv_0 = yTY_1Vv_0 = TY_1^{(1)}yv_0V = TY_1^{(1)}v_1V = Tv_1Y_1^{(2)}V \subseteq Byv_0B$$

which gives us

$$v_1Bv_0 = (v_1v_0)v_0Bv_0 \subseteq yBv_0B \subseteq Byv_0B = Bv_1B.$$

On the other hand

$$1Bw_1 \subseteq B1w_1B$$

$$w_1Bw_1 = w_1TX_2^{(1)}Mw_1 \subseteq TX_2^{(1)}w_1X_2^{(1)}M \subseteq Bw_1B$$

$$v_1Bw_1 = v_1TX_2^{(1)}Mw_1 = TX_2^{(1)}v_1w_1M \subseteq Bv_1w_1B$$

$$w_2Bw_1 = w_2TX_2^{(1)}Mw_1 = TX_1w_2w_1M \subseteq Bw_2w_1B$$

$$v_0Bw_1 = v_0TX_2^{(1)}Mw_1 = TX_2^{(2)}v_0w_1M \subseteq Bv_0w_1B$$

$$yBw_1 = yTX_2^{(1)}Mw_1 = TX_2^{(2)}yw_1M \subseteq Byw_1B$$

$$w_1v_0Bw_1 = w_1v_0TX_2^{(1)}Mw_1 = TX_1w_1v_0w_1 \subseteq Bw_1v_0w_1B$$

and thus

$$zBw_1 = (zw_1)w_1Bw_1 \subseteq v_1Bw_1B \subseteq Bv_1w_1B = BzB$$

$$v_0w_1Bw_1 \subseteq v_0Bw_1B \subseteq Bv_0w_1B$$

$$w_2Bw_1 = (w_2w_1)w_1Bw_1 \subseteq yBw_1B \subseteq Byw_1B = Bw_2B.$$

Finally

$$y^2Bw_1 = y^2TX_2^{(1)}Mw_1 = TX_2y^2w_1M = TX_2w_0M = Tw_0X_1M \subseteq By^2w_1B$$

which gives us

$$v_2Bw_1 = (v_2w_1)w_1Bw_1 \subseteq w_1v_0Bw_1B \subseteq Bw_1v_0w_1B = Bv_2B.$$

and BN3 is valid. By Proposition 4.72 again $Q^{v_0} = VY_2 \neq VY_1 = Q$ and $Q^{w_2} = MX_1^{(1)} \neq MX_1^{(2)} = Q$ which proves BN4 and gives us the theorem. $\square$

Part II

Black Box Groups

Chapter 5

Reflexive Tori

We are interested in the 2-local structure of finite groups of Lie type over fields of odd characteristic. In this case, many elementary abelian 2-subgroups are contained in maximal tori and normalizers of maximal tori are 2-local subgroups. In this chapter we investigate the possible orders of strongly real elements in maximal tori.

5.1 Basic Properties

As described in Section 1.4, a very good way to study finite groups of Lie type is to deduce their properties from the corresponding properties of algebraic groups by means of the Frobenius map. We are hence going to study strongly real elements of algebraic groups first.

Let G be a connected semisimple algebraic group over some algebraically closed field of odd characteristic. We call a torus of G *reflexive*, if it is inverted by an involution of G. Let $i \in G$ be an involution. If T is a maximal torus of G, denote by $T[i]$ the subgroup of all elements in T which are inverted by i. The Zariski connected component $T[i]^\circ$ is a reflexive torus by [42, 16.2]. Consider the set of tori which are inverted by a conjugate of i and let $\mathcal{Y}_i$ be the set of the maximal ones.

We are going to show that a reflexive torus S contained in a maximal torus T can be assumed to be inverted by an involution in $N_G(T)$. Call an automorphism of an algebraic group H *semisimple automorphism* if it can be achieved by conjugation by a semisimple element of some algebraic group containing H.

Fact 5.1 ([53]) *Every semisimple automorphism of an algebraic group G fixes a Borel subgroup and a maximal torus thereof.*

Corollary 5.2 *Let G be a connected algebraic group, T a maximal torus of G and $S \leq T$ a reflexive torus inverted by i for some $i \in I(G)$. Then $N_G(S) \subseteq N_G(T)C_G(S)$ and there exists $x \in C_G(S)$ such that $i^x \in N_G(T)$.*

Proof. As $C_G(S)$ is connected by [42, 22.3], all maximal tori of $C_G(S)$ are conjugate [42, 21.3]. Let $x \in N_G(S)$. Then $T^x \leq C_G(S)$ and as T is a maximal torus of $C_G(S)$, $T^x = T^z$ for some $z \in C_G(S)$. Thus $N_G(S) \leq N_G(T)C_G(S)$.

Finally, conjugation by i is a semisimple automorphism of $C_G(S)$ and i normalises a maximal torus of $C_G(S)$ by Fact 5.1. Hence there exists $x \in C_G(S)$ such that $i^x \in N_G(T)$. □

Lemma 5.3 *G has finitely many conjugacy classes $Y_1, \ldots Y_s$ on $\mathcal{Y}_i$. Let F be a Frobenius map. Y_m contains a torus S_m fixed by F for all $1 \leq m \leq s$. Let $A_m := N_G(S_m)$. Then G^F has $|H^1(F, A_m)| = |H^1(F, N_G(S_m)/C_G(S_m))|$ conjugacy classes on Y_m^F. If G is a Chevalley group, then $|H^1(F, A_m)|$ is the number of conjugacy classes in $N_G(S_m)/C_G(S_m)$.*

Proof. Let T be a maximal torus in G. As maximal tori are conjugate, every $S \in \mathcal{Y}_i$ is conjugate to a subtorus of T. Assume that $S \in \mathcal{Y}_i$, $S \leq T$ is inverted by i^g. Then S is inverted by $i^x \in N_G(T)$ for some $x \in C_G(S)$ by Corollary 5.2 and $S = T[i^x]^\circ$. As the Weyl-group $N_G(T)/T$ of G is finite, G has finitely many conjugacy classes on $\mathcal{Y}_i$. The result follows now by Fact 1.12 as in the case of maximal tori. □

Let $W_m := N_G(S_m)/C_G(S_m)$ the Weyl-group of a maximal reflexive torus S_m fixed by F. As for maximal tori, we say that $(S_m^{g^{-1}})^F$ is a *reflexive torus of* G^F *twisted by* $w := g^{-1}F(g)C_G(S_m) \in W_m$. To determine W_m, we will need some trivial facts about Coxeter and Weyl groups.

A *Coxeter system* is a pair (W, S), where W has generators $s \in S$ and relations $(ss')^{m(s,s')}$ where $m(s,s) = 1$ and $m(s,s') = m(s',s) \geq 2$ for $s \neq s'$. W is also called *Coxeter group*. Elements of W are called *reflections*, if they are conjugate in W to an element of S. The *length* $l(w)$ of an element $w \in W$ is the minimum length of an expression of the form $w = s_1 \cdots s_r$ where $s_i \in S$. If $l(w) = r$ and $w = s_1 \cdots s_r$ where $s_i \in S$, then $s_1 \cdots s_r$ is called a *reduced expression* for w.

The classical examples of a Coexter groups are Weyl groups of root systems. In this case the definitions of reflections coincide.

Lemma 5.4 *Let w be an involution in a Coxeter group W. Then w is a product of commuting reflections.*

Proof. By induction on the length of w. Assume that the claim is true for $l(w) = n$ and let $s_1 \dots s_n s_{n+1}$ be a reduced expression for w. Since $w^2 = 1$, $l(ws_1) = n = l(s_1 w)$. Consider now $w_1 = s_1 w s_1$. If $l(w_1) = n - 1$, then w_1 is a product of commuting reflections by induction hypothesis. This implies that $w = w_1^{s_1}$ is the product of commuting reflections as well. If on the other hand $l(w_1) = n + 1 = l(w)$, then $w = s_1 w s_1$ by [43, 7.2] and s_1 commutes with $w_2 = s_2 \dots s_{n+1}$. This implies that w_2 is an involution and the claim follows by induction hypothesis. $\square$.

Lemma 5.5 *Let W be the Weyl-group of a root system Φ over the vector-space V and $w \in W$ an involution. Then $V = E_1 \oplus E_{-1}$, where E_k is the eigenspace of w for the eigenvalue k, $k = \pm 1$. Furthermore E_{-1} is spanned by $\Phi \cap E_{-1}$.*

Proof. Let $A_{rs} := \frac{2(r,s)}{(r,r)}$ for all $r, s \in \Phi$. As w is an involution, there exists a minimal $n \in \mathbb{N}$ and pairwise commuting reflections w_{r_i} for $r \in \Phi$ $(1 \leq i \leq n)$ such that $w = w_{r_1} \dots w_{r_n}$ by Lemma 5.4. Since $w_{r_i} w_{r_j} w_{r_i} = w_{w_{r_i}(r_j)} = w_{r_j - A_{r_i r_j} r_i}$, the r_i are pairwise orthogonal for $1 \leq i \leq n$. This implies that

$$w(v) = v - \sum_{i=1}^{n} A_{r_i v} r_i$$

for all $v \in V$. Hence $w(v) = -v$ if and only if $v \in \langle r_1, \dots, r_n \rangle$. Let E_1 be the eigenspace of w for the eigenvalue 1, E_{-1} the eigenspace of w for the eigenvalue -1. Then $V = E_1 \oplus E_{-1}$ and E_{-1} is spanned by $\Phi \cap E_{-1}$. $\square$

We are assuming from now on, that G is a Chevalley group over an algebraically closed field K of odd characteristic. Most of the theory can be developed in a more general context, but for the present purpose this setting is sufficient.

Proposition 5.6 *Let G be a Chevalley group over an algebraically closed field K, $i \in G$ an involution and $S \in \mathcal{Y}_i$ a reflexive torus. Then, if $T \geq S$ is a maximal torus of G, S is inverted by $j \in N_G(T)$. Let Φ be a root system for G, W the Weyl-group of Φ. Then $N_G(S)/C_G(S) \cong N_W(W_J)/C_W(J)$ where J is a fundamental system of the set of roots inverted by the involution $v \in W$ corresponding to j.*

Proof. Let Δ a fundamental subsystem of Φ, and h and n be the homomorphisms corresponding to T as defined in Section 1.3. As $C_G(T) = T$, S in nontrivial and $S = T[j]^\circ$ for some involution j conjugate to i. By Lemma 5.2 we may assume that $j \in N_G(T)$.

$v := n(j)$ is an involution of the Weyl group W of Φ. Let $\chi, \chi' \in \mathcal{X}$ such that $\chi'(r) = \chi(v(r))$ for all $r \in \Delta$. Then $h(\chi) \in T[j]$ if and only if

$$\chi(r)\chi'(-r) = \chi(r)\chi(v(-r)) = \chi(r + v(-r)) = 1$$

for all $r \in \Delta$. As v is an involution of the Weyl group of Φ, V is the orthogonal sum of the eigenspaces E_1 and E_{-1} as in Lemma 5.5. Let $r \in \Delta$ and $r = r_1 + r_2$ where $r_1 \in E_1$ and $r_2 \in E_{-1}$. Then $v(-r) = -r_1 + r_2$ and $r + v(-r) = 2r_2$. Thus $h(\chi) \in T[i]$ if and only if $\chi(r_2) = \pm 1$ for all $r_2 \in E_{-1}$ such that $(E_1 + r_2) \cap \Delta \neq \emptyset$. This implies that S is generated by $h(\chi_{r,\lambda})$ where $r \in \Psi := \Phi \cap E_{-1}$ and $\lambda \in K^*$.

Ψ is the set of roots inverted by v. Furthermore Ψ is a root system of E_{-1} of its own right as E_{-1} is spanned by Ψ by Lemma 5.4 and $v(w_r(s)) = -s + \frac{2(r,s)}{(r,r)} r = -w_r(s)$ for all $r, s \in \Psi$. Hence we can choose our fundamental system Δ such that $J := \Delta \cap \Psi$ is a fundamental system for Ψ. Especially $\Psi = \Phi_J$ has the Weyl-group $W_J := \langle w_r | r \in J \rangle$ by [25, 2.5].

As $N_G(S) \subseteq N_G(T)C_G(S)$, $N_G(S) = (N_G(T) \cap N_G(S))C_G(S)$ and

$$N_G(S)/C_G(S) \cong \big(N_G(T) \cap N_G(S)\big)/\big((N_G(T) \cap C_G(S)\big).$$

Consider $N := n\big(N_G(T) \cap N_G(S)\big) \leq W$. We claim that $N = N_W(W_J)$ Let $x \in N_G(S) \cap N_G(T)$. xjx^{-1} inverts S. As above S is generated by $h(\chi_{r,\lambda})$ where $r \in \Psi'$, $\lambda \in K^*$ and Ψ' are the roots inverted by $h(xjx^{-1})$. This forces Ψ' to equal Ψ. Set $n := n(x)$ and let $r \in J$. Then $nvn^{-1}(r) = -r$ and $v(n^{-1}(r)) = -n^{-1}(r)$. Thus $n^{-1}(r) \in \Psi$. On the other hand $w_r^n = w_{n^{-1}(r)}$ by [25, 2.4] and $n \in N_W(W_J)$.

Set $C := n\big(N_G(T) \cap C_G(S)\big)$. We show that $C = C_W(J)$. Let $x \in N_G(T) \cap C_G(S)$. As $x \in C_G(S)$, $\chi_{r,\lambda}(s) = \chi_{r,\lambda}(n(x)^{-1}(s))$ for all $r \in \Psi$, $\lambda \in K^*$, $s \in \Delta$ and $\chi_{r,\lambda}\big(s - n(x)^{-1}(s)\big) = 1$. By definition of $\chi_{r,\lambda}$, this implies that $\big(r, s - n(x)^{-1}(s)\big) = 0$ for all $r \in \Psi$, $s \in \Delta$. However E_{-1} is spanned by Ψ and $s - n(x)^{-1}(s) \in E_1$ for all $s \in \Delta$. Furthermore $v \in W_J$ by [25, 2.5.1], $n(x) \in N_W(W_J)$ and $n(x)vn(x)^{-1} \in W_J$. Thus $v\big(s - n(x)^{-1}(s)\big) = -s + n(x)^{-1}(s) = -(s - n(x)^{-1}(s))$ for all $s \in J$. Then $s - n(x)^{-1}(s) \in E_{-1} \cap E_1 = 0$ for all $s \in J$ and $n(x)(s) = s$ for all $s \in J$. This yields the claim and proves the proposition. □

Let $Y_1, \cdots Y_m$ be the conjugacy classes of G on $\mathcal{Y}_i$. Let F be a Frobenius map and T a maximal torus fixed by G. We may take T to be the diagonal of G. Let furthermore $S_k \leq T$ be a reflexive torus in Y_k for $1 \leq k \leq m$.

Proposition 5.7 *Let $S \in \mathcal{Y}_i$. Assume that $S^F \in Y_k$ is a reflexive torus twisted by $w \in W_k := N_G(S_k)/C_G(S_k)$ for some $1 \leq k \leq m$. Then the order of S^F is $|\chi_w(q)|$ where χ_w is the characteristic polynomial of w in W_k and q the number of elements of the base field of G^F.*

Proof. By Corollary 5.2 we may assume that $w = xC_G(S_k)$, where $x \in N_G(T)$. Then $S \leq T_{w_0}$, where $w_0 := xT \in N_G(T)/T$. To determine the order of S^F, note that the dual of S, $X(S)$ is contained in the dual of T_w and that hence F acts on $X(S)$ as qw, where q is he number of elements of the base field of G^F. The order of S^F is therefore $|det(qw-1)|$ computed in $X(S)$. This, however, is nothing but $|\chi_w(q)|$ where χ_w is the characteristic polynomial of w in W_k as in [52]. □

5.2 Examples of reflexive tori

We are going to investigate reflexive tori in Chevalley groups of type B_n and C_n for $n \geq 2$ over a finite field K. As the unlabeled Dynkin diagrams of type B_n and C_n are equal, the corresponding root systems $\Phi := \Phi_{B_n}$ and Φ_{C_n} are isomorphic and hence $W := W(\Phi_{B_n}) \cong W(\Phi_{C_n})$ for all $n \geq 2$. Let $\Delta = \{\alpha_1, ...\alpha_n\}$ be a set of simple roots of Φ. We can represent Δ by $\alpha_k = e_k - e_{k+1}$ for $2 \leq k \leq n$ and $\alpha_1 = 2e_1$ if Φ is of type C_n and $\alpha_1 = e_1$ if Φ is of type B_n where $\{e_1, ...e_n\}$ is an orthonormal basis of V. W is isomorphic to $\mathbb{Z}_2^n \rtimes S_n$ and each element determines a product of disjoint cycles $(j_1 \cdots j_m)$ or $(j_1 \cdots j_m - j_1 \cdots - j_m)$ where $j_i \in \{1, \cdots, n, -1, \cdots - n\}$. The first kind of cycle is said to be *positive of length* m, the second kind *negative of length* m. The *signed cycle-type* of w is the set of lengths of the disjoint cycle together with their signs. The action of W on Δ is as follows. The normal subgroup S_n acts as permutation group on the set of basis vectors of V, $\pi \in S_n$ sending e_i to $e_{\pi(i)}$ for all $1 \leq i \leq n$. The complement $\mathbb{Z}_2^n$ acts by $e_i \longrightarrow \rho_i(z)e_i$ for $1 \leq i \leq n$ where $z \in \mathbb{Z}_2^n$ and ρ_i is the i-th projection map.

Fact 5.8 ([25]) *Two elements of* W *are conjugate if and only if they have the same cycle type. The characteristic polynomial* χ_w *of an element* $w \in W$ *is the product of the following polynomials:* (i) $(q^m - 1)$ *for every positive cycle of length* m *and* (ii) $q^m + 1$ *for every negative cycle of length* m.

Let G be a Chevalley group over the Lie algebra $\mathcal{L}(K)$, where $\mathcal{L}$ is of type B_n or C_n and K is any field of odd characteristic. Then $G \cong \mathrm{PSp}_{2n}(K)$ or $G \cong P\Omega_{2n+1}(K)$ by Fact 1.8. If K is finite, then $K = GF(q)$, where q is an arbitrary power of $char(K)$. For the following compare [56, 11.52,11.53] and [37, 4.3].

Let K be finite or algebraically closed. Then $\mathrm{PSp}_{2n}(K)$ has $[\frac{n}{2}] + 1$ conjugacy classes of involutions. Let $s \in Sp(2n, K)$ represent an element of order 2 in $\mathrm{PSp}_{2n}(K)$. Then either $s^2 = -I$ or $s^2 = I$. All involutions which are represented by an element t such that $s^2 = -I$ form one conjugacy class of involutions of type

t_n. Furthermore for every even number $2 \leq m \leq n$ there is one conjugacy class of involutions of type $t_{m/2}$. If s is an involution of type $t_{m/2}$, then the eigenvalues of s on the underlying natural module are -1 with multiplicity m and 1 with multiplicity $2n - m$.

$\Omega_{2n+1}(K)$ has n conjugacy classes of involutions. There is one conjugacy class of involutions of type $t_{m/2}$ for each even number $2 \leq m \leq 2n$. An involution s is of type t_m if the eigenvalues of s on the underlying natural module are -1 with multiplicity m and 1 with multiplicity $2n + 1 - m$.

Lemma 5.9 *Let $G = PSp_{2n}(K)$ for an algebraically closed field K of odd characteristic and $n \geq 2$. Let T be a maximal torus in G and $i \in N_G(T)$ be an involution.*

(i) If i is of type t_m, where $1 \leq m \leq [\frac{n}{2}]$, then iT can be written as the product of l positive 2-cycles for $0 \leq l \leq m$.

(ii) If i is of type t_n, then iT can be written as the product of l_1 positive 2-cycles and l_2 negative 1-cycles for $l_1, l_2 \in \mathbb{N}$ such that $0 \leq 2(l_1) + l_2 \leq n$.

(iii) $T \in \mathcal{Y}_i$ if and only if i is of type t_n.

Especially iT contains involutions from $[\frac{n}{2}] - 1 - k$ different conjugacy classes, if iT corresponds to the product of $k + 1$ positive 2-cycles for $0 \leq k < [\frac{n}{2}]$.

Proof. iT is an involution in W and can thus be written as the product of commuting reflections by Lemma 5.4. The only reflections in W are positive 2-cycles and negative 1-cycles. Assume that iT corresponds to a negative 1-cycle. As $det(i) = 1$, i is conjugate to an element in i_0T where

$$i_0 := \begin{pmatrix} \mathrm{J}_k & & & \\ & 0 & -1 & \\ & 1 & 0 & \\ & & & \mathrm{J}_{n-(k+1)} \end{pmatrix}$$

and J_k is a $2k \times 2k$ matrix of the form $diag(j, -j, \cdots j, -j)$ for all $0 \leq k \leq n$ where $j \in K$ is an element of order 4. Especially i is of type t_n. If on the other hand iT corresponds to a positive 2-cycle, then i is conjugate to an element in j_oT, where

$$j_0 := \begin{pmatrix} 0 & \mathrm{I}_2 & \\ \mathrm{I}_2 & 0 & \\ & & \mathrm{I}_{n-4} \end{pmatrix}.$$

Thus i is of type t_m for $1 \leq m \leq [\frac{n}{2}]$. This implies the claim. □

Corollary 5.10 *Let $G = PSp_{2n}(K)$ for an algebraically closed field K of odd characteristic, $n \geq 2$ and $i \in G$ an involution. Then G acts transitively on $\mathcal{Y}_i$.*

Proof. Let T be a maximal torus. It is sufficient to show that G acts transitively on the reflexive subtori $S \leq T$, where $S \in \mathcal{Y}_i$. Furthermore we may assume that $i \in N_G(T)$ by Lemma 5.2. If i is of type t_n, then $T \in \mathcal{Y}_i$ by Lemma 5.9 and we are done. Assume that i is of type t_m for $1 \leq m < n$. Then $T[j]^\circ \in \mathcal{Y}_i$ for an involution $j \in N_G(T)$ of type t_m if and only if i^g corresponds to the product of m positive 2-cycles by maximality of elements of $\mathcal{Y}_i$ and Lemma 5.9. However, all positive 2-cycles in the Weyl-group of G are conjugate by Fact 5.8. This yields the claim. □

Lemma 5.11 *Let $G = P\Omega_{2n+1}(K)$ for an algebraically closed field K of odd characteristic and $n \geq 2$. Let T be a maximal torus in G and $i \in N_G(T)$ be an involution.*

(i) If i is of type t_m, where $1 \leq m \leq [\frac{n}{2}]$, then iT an be written as the product of l_1 negative 1-cycles and l_2 positive 2-cycles, where $0 \leq [\frac{l_1+1}{2}] + l_2 \leq m$.

(i) If i is of type t_m, where $[\frac{n}{2}] + 1 \leq m \leq n$, then iT can be written as the product of l_1 negative 1-cycles and l_2 positive 2-cycles, where $0 \leq [\frac{l_1}{2}] + l_2 \leq n - m$.

(iii) If n is even, then $T \in \mathcal{Y}_i$ if and only if i is of type $t_{n/2}$.

Especially iT contains involutions from $n - 1 - 2k$ different conjugacy classes, if iT corresponds to the product of $k + 1$ positive 2-cycles for $0 \leq k < [\frac{n}{2}]$.

Proof. iT is an involution in W and can thus be written as the product of commuting reflections by Lemma 5.4. The only reflections in W are positive 2-cycles and negative 1-cycles. Assume that iT corresponds to a positive 2-cycle. Then i is conjugate to an element in i_0T, where

$$i_0 := \begin{pmatrix} \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} & & & & \mathbf{0} \\ & \mathrm{I}_{n-2} & & & \\ & & \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} & & \\ & & & \mathrm{I}_{n-2} & \\ \mathbf{0} & & & & 1 \end{pmatrix}$$

Especially i is of type t_k for some $1 \leq k \leq n-1$. If iT corresponds to a negative 1-cycle, then is conjugate to an element in j_oT, where

$$j_0 := \begin{pmatrix} 0 & & 1 & & \\ & \mathrm{I}_{n-1} & & 0 & \\ 1 & & 0 & & \\ & 0 & & \mathrm{I}_{n-1} & \\ & & & & -1 \end{pmatrix}$$

Hence i is of type t_k for some $1 \leq k \leq n$. If furthermore n is even and i is of type $t_{n/2}$, then i is conjugate to an involution k in $N_G(T)$ that corresponds to n negative 1-cycles. k inverts T and thus $T \in \mathcal{Y}_i$. □

Corollary 5.12 *Let $G = P\Omega(2n, K)$ for an algebraically closed field K of odd characteristic, $n \geq 2$ and $i \in G$. Then G acts transitively on $\mathcal{Y}_i$.*

Proof. Let T be a maximal torus. It is sufficient to show that G acts transitively on the reflexive subtori $S \leq T$, where $S \in \mathcal{Y}_i$. If i is of type t_n, then iT correspond to a single negative 1-cycle and there is nothing to prove. Let i be of type t_m for $1 \leq m \leq [\frac{n}{2}]$. Then $T[j]^\circ \in \mathcal{Y}_i$ for some $j \in N_G(T)$ if and only if j corresponds to the product of $2l_1$ negative 1-cycles and l_2 positive 2-cycles for $l_1 + l_2 = m$ by maximality of elements of $\mathcal{Y}_i$ and Lemma 5.9. Furthermore $T[j_0]^\circ \geq T[j_1]^\circ$ if $j_0, j_1 \in N_G(T)$ such that j_0 corresponds to $(1\ \ -1)(2\ \ -2)$ and j_1 to $(1\ 2)$. Hence $l_2 = 0$ by maximality of elements of $\mathcal{Y}_i$. This implies the claim for $m \leq [\frac{n}{2}]$ as elements of the Weyl-group with the same cycle-type are conjugate by Fact 5.8.

Let i be of type t_m for $[\frac{n}{2}] + 1 \leq m < n$. Then $T[j]^\circ \in \mathcal{Y}_i$ for some $j \in N_G(T)$ if and only if j corresponds to the product of $2(n-m)+1$ negative 1-cycles by maximality of elements of $\mathcal{Y}_i$ and Lemma 5.9 as in the previous paragraph. This implies that all reflexive subtori $S \in \mathcal{Y}_i$ are conjugate and that $S[j]^\circ \in \mathcal{Y}_i$ if and only if j corresponds to the product of $2(n-m)+1$ negative 1-cycles. □

It is not known, however, if a semisimple algebraic group acts in general transitively on $\mathcal{Y}_i$ for any involution i.

Proposition 5.13 *Let G be a Chevalley group of type C_n over an algebraically closed field of of odd characteristic. Let $i \in G$ be an involution of type t_m and F a standard Frobenius map. If q is the number of elements of the base field of G^F, then the order of S^F for any $S \in \mathcal{Y}_i$ is $|\chi(q)|$, where χ is the characteristic polynomial of an element of $W(\Phi_{C_m})$.*

Proof. Let T be a maximal torus of G. G acts transitively on $\mathcal{Y}_i$ by Corollary 5.10. We may assume that $S = T[i]^\circ \in \mathcal{Y}_i$ for some $i \in N_G(T)$ by Lemma 5.2. If i is of type t_n, then $S = T$ and the claim follows by Fact 1.14. If i is of type t_m for $1 \leq m \leq [\frac{n}{2}]$, then we may assume that iT corresponds to $(1\ 2)(3\ 4)\dots(2m-1\ 2m)$ by Lemma 5.9 and Corollary 5.10. Thus $N_G(S)/C_G(S) \cong N_W(W_J)/C_W(J)$ where J is a fundamental system of the set of roots inverted by the involution $v \in W$ corresponding to i by Proposition 5.6. $J = \{\alpha_1, \alpha_3, \cdots, \alpha_m\}$ consists of m components of type A_1 and hence $N_W(W_J) \cong W_J \rtimes W(\Phi_{C_m})$ where $W_J \cong \mathbb{Z}_2^m$ by [40]. Furthermore $C_W(J)$ consists of the reflections corresponding to the long roots of the component C_m by [40] again. Thus

$$N_W(W_J)/C_W(J) \cong W_J \rtimes S_m \cong \mathbb{Z}_2^m \rtimes S_m,$$

the Weyl-group of C_m. By Proposition 5.7 the order of S is thus a characteristic polynomial of an element $w \in W(\Phi_{C_m})$, evaluated at q. □

Proposition 5.14 *Let G be a Chevalley group of type B_n over an algebraically closed field of of characteristic p. Let $i \in G$ be an involution of type $t_{n/2}$ and F a standard Frobenius map. If q is the number of elements of the base field of G^F, then the order of S^F for any $S \in \mathcal{Y}_i$ is $|\chi(q)|$, where χ is the characteristic polyomial of an element of*

- *$W(\Phi_{B_{2m}})$ if $1 \leq m \leq [\frac{n}{2}]$ and of*
- *$W(\Phi_{B_k})$, where $k := 2(n-m)+1$ for $[\frac{n}{2}]+1 \leq m \leq n$.*

Proof. Let T be a maximal torus of G. G acts transitively on $\mathcal{Y}_i$ by Corollary 5.12. We may assume that $S = T[i]^\circ \in \mathcal{Y}_i$ for some $i \in N_G(T)$ by Lemma 5.2. If i is of type t_m for $1 \leq m \leq [\frac{n}{2}]$ then we may assume that iT corresponds to $(1\ -1)\cdots(2m\ -2m)$ by Corollary 5.12. Thus $N_G(S)/C_G(S) \cong N_W(W_J)/C_W(J)$ where J is a fundamental system of the set of roots inverted by the involution $v \in W$ corresponding to i by Proposition 5.6. $J = \{\alpha_1, \alpha_2, \cdots, \alpha_{2m}\}$ consists of one component of type B_{2m} and hence $N_W(W_J) \cong W_J \rtimes W(\Phi_{B_{2m}})$ where $W_J \cong W(\Phi_{B_{2m}})$ by [40]. Furthermore $C_W(J)$ consists of all reflections corresponding to the roots of the component B_{2m} by [40] again. Thus

$$N_W(W_J)/C_W(J) \cong W_J \cong W(\Phi_{B_{2m}}),$$

the Weyl-group of B_{2m}. By Proposition 5.7 the order of S is thus a characteristic polynomial of an element $w \in W(\Phi_{B_{2m}})$,evaluated at q.

If i is of type t_m for $[\frac{n}{2}]+1 \leq m$ then to we may assume that iT corresponds to we may assume that iT corresponds to $(1\ -1)\cdots(k\ -k)$ by Corollary 5.12, where $k = 2(n-m)+1$. The above paragraph implies that the order of S is thus a characteristic polynomial of an element $w \in W(\Phi_{B_k})$, evaluated at q. $\square$

Since the characteristic polynomials of elements in the Weyl-group of Chevalley groups are given in [25], we have thus a complete description of the possible orders of strongly real elements in $\mathrm{PSp}_{2n}(q)$ and $\Omega_{2n+1}(q)$ for q odd and $n \geq 2$.

Chapter 6

Distinguishing B_n and C_n

The aim of this section is to propose a fast Monte-Carlo algorithm to distinguish $\mathrm{PSp}_{2n}(q)$ from $\Omega_{2n+1}(q)$ where n and q are given. Namely we prove the following theorem

Theorem 6.1 *There is a Monte-Carlo algorithm which, when given a black box group G isomorphic to a simple classical group of type B_n or C_n defined over some field of given size q, can decide if G is of type C_n in time $O(\mu n^3 \log q + \xi n)$. The algorithm is one-sided if n is odd.*

In the classical setting it is assumed the black box operations can be performed at unit cost. We will modify these assumptions slightly, in accordance with [46], and set μ to be an upper bound on the time for each multiplication or inversion within the group G. If thus ξ is an upper bound on the time requirement per element for the construction of independent, (nearly) uniformly distributed random elements of G, then ξ can be expressed as a polynomial function of N and μ by Fact 1.16.

In the following we assume for the sake of argument that the Black Box gives us independent uniformly distributed elements of G. For a discussion of this assumption see [11].

As $\mathrm{PSp}_4(q) \cong P\Omega_5(q)$ for all q and $\mathrm{PSp}_{2n}(2^m) \cong P\Omega_{2n+1}(2^m)$ for all $n, m \in \mathbb{N}$, it is enough to give an algorithm for $n \geq 3$ and q odd.

The structure of the algorithm is very straightforward:

(1) Seek an element z of *good order*. (This would guarantee that z is contained in some specified maximal torus of even order.) If it cannot be found after examination of at least $20n$ randomly selected elements of G then return

no. Otherwise go to step (2). The algorithm errs with probability less than 0.01. This step takes $O(\mu n^3 \log q + \xi n)$ time.

(2) Compute the involution x in the cyclic group generated by z in $O(\mu n \log q)$ time.

(3) Compute $y := x^g x^h$ for random elements $g, h \in G$. If $o(y)$ divides $q(q+1)$ or $q(q-1)$ then go to (4). Otherwise return *yes*. The algorithm errs with probability 0 if n is odd and with probability $\frac{2}{2+n}$ if n is even. This step takes $O(\xi + \mu \log q)$ time.

(4) Repeat step (3) $60n$ times. If y always divides $q(q+1)$ or $q(q-1)$ then return *no*. The error probability is $\leq 1/2$ in this case.

The number of necessary repetions in (4) is a very crude estimate, which was sufficient for our theoretical purposes. In practice, one does get a strongly real element which does not divide $q(q+1)$ or $q(q-1)$ at the very first step, if G is of type C_n and $q > 3$.

I have written a short GAP-programme, which uses this algorithm. Tests have shown that it is very fast and reliable.

6.1 Preliminaries

We fix the following notations. Let K be an algebraically closed field of odd characteristic p and let H be either $\mathrm{PSp}_{2n}(K)$ or $\Omega_{2n+1}(K)$. Thus H is an adjoint Chevalley group of type C_n or B_n over the field K. Let F be a standard Frobenius map such that number of elements of the base field is q. Set $G := [H^F, H^F]$. Then $H^F/[H^F, H^F] \cong \mathbb{Z}_2$ and G is a Chevalley group of type C_n or B_n over $GF(q)$. Let $e \in \mathbb{N}$ such that $q = p^e$.

Let T be the diagonal in H. Denote by Φ the set of all roots of H, by Δ a fundamental root system and by W the Weyl-group of H. Let furthermore T_w be a maximal torus of H^F which is twisted by $w \in W$. The order of T_w is the product of numbers of the form $q^k \pm 1$ for $k \leq n$ by Fact 1.14 and Section 5.2. As $|H^F/G| = 2$, a maximal torus T_0 of G has order $|T_w|/2$ for some $w \in W$.

The algorithm works with involutions in the most frequent tori. These are the tori twisted by an element of cycle-type $-n$ or n by Fact 1.14. We have to distinguish the following cases:

(i) $q^n \cong -1 \mod n$, i.e. n odd and $q \cong -1 \mod 4$.

(*ii*) $q^n \cong 1 \mod n$, i.e. n even or $q \cong 1 \mod 4$

In the first case the maximal tori of order $\frac{q^n+1}{2}$ contain an involution, in the second case the maximal tori of order $\frac{q^n-1}{2}$ contain an involution. Note that if n is even, the tori of order $\frac{q^n-1}{2}$ form at least two conjugacy classes of involutions. One arising from twisting with elements of cycle-type n and one from twisting with an elements of cycle-type $(\frac{n}{2}, -\frac{n}{2})$. We call tori in these conjugacy classes *maximal non-split tori of even order*. However if $n \cong 0 \mod 4$, there is even another conjugacy class of tori of order $\frac{q^n-1}{2}$, namely the ones twisted by elements of cycle-type $(\frac{n}{2}, \frac{n}{4}, -\frac{n}{4})$. To distinguish these tori from the maximal non-split tori of even order, we introduce the concept of *2-height*. Let G be a group and $g \in G$ such that $o(g) = 2^k m$ where m is odd. Then k is called the *2-height of g*. We can show, that the 2-height of elements of even order in a torus of order $\frac{q^n-1}{2}$ is maximal if and only if the torus is a maximal non-split torus of even order.

Lemma 6.2 *Let $w = w_1 w_2 \in W$, where w_1 and w_2 operate on disjoint sets and set $H_m := C_T(w_m)$ and $C_m := C_G(H_m)'$ for $m = 1, 2$. Then $(C_1C_2)^F$ contains a torus T_w twisted by w. Furthermore T_w can be chosen to be T_1T_2S where T_m is a torus in C_m^F twisted by w_m for $m = 1, 2$ and $S = T \cap H_1 \cap H_2$.*

Proof. C_1 and C_2 are connected semisimple groups which are generated by the root-subgroups $\{X_\alpha | \ \alpha \in S_1\}$ and $\{X_\beta | \ \beta \in S_2\}$ respectively where $S_m := \{\pi \in \Pi : \exists \rho \in \Pi : \ \pi = \rho - w_m^{-1}(\rho)\}$ by [52, II,4.1]. It is easy to see, that $\alpha + \beta \notin \Pi$ for all $\alpha \in S_1$ and $\beta \in S_2$. Hence C_1 and C_2 commute by [26, 4.1]. Since furthermore $S_1 \cap S_2 = \emptyset$, $C_1 \cap C_2$ is finite. As C_m^F contains a torus T_m twisted by w_m the claim follows. □

Corollary 6.3 *Let $m \in \mathbb{N}$ be even. The 2-height of elements of H^F in tori twisted by an element of cycle type m is greater than the 2-height of elements in tori twisted by elements of cycle type $(\frac{m}{2}, -\frac{m}{2})$.*

Proof. Set $l := \frac{m}{2}$ and let w be an element of cycle type $(l, -l)$. Then $T_w = T_1T_2$ by Lemma 6.2, where T_1 is a cyclic group of order $q^l - 1$ and T_2 is a cyclic group of order $q^l + 1$. Since the order of T_w is $q^m - 1$, T_w contains an elementary abelian subgroup of order 4 and the maximal 2-height is smaller than the 2-height of of a torus twisted by an element of cycle type m. □

Notice that if n is even the maximal 2-height in two non-conjugate maximal non-split tori of even order is the same, since G has index 2 in H^F.

In the following we are looking for elements of maximal 2-height in a maximal non-split torus of even order. To find elements in a maximal non-split torus the notion of *primitive prime divisor elements* of G plays a crucial role as in [48] and [46]. Let p be a prime and $m \geq 2$. A prime dividing $p^m - 1$ but not $p^i - 1$ for $1 \leq i < m$ is called a *primitive prime divisor of* $p^m - 1$. In our case primitive prime divisors always exist by [58]. Furthermore an integer j is called a *ppd*(p, m) if $j | p^m - 1$ and j is divisible by a primitive prime divisor of $p^m - 1$. An element of G of order *ppd*(p, en) is called *primitive prime divisor element.*

Let P be a maximal non-split torus of even order and let $|P| = 2^k m$ where $k, m \in \mathbb{N}$ and m is odd. We say that an element $g \in P$ is of *maximal 2-height*, if the 2-height of g is k. Since P is cyclic, elements of maximal 2-height exists. Furthermore $\frac{1}{2}$ of the elements of P have maximal 2-height as the cyclic group generated by a 2-element x of maximal 2-height contains 2^{k-1} elements of maximal 2-height, namely x^s for $s \in \mathbb{N}$ and s odd.

We call g *good* if it satisfies the following conditions:

- g has maximal 2-height.
- g has *ppd*$(p, 2en)$ order in case (i) and *ppd*(p, en) order in case (ii).
- $o(g) \nmid q^{n/2} + 1$ if n is even and $q \cong 1 \mod 4$.

An element of good order lies in a maximal non-split tori of even order by Corollary 6.3.

Proposition 6.4 *The share of good elements of maximal non-split tori of even order in G is at least $\frac{|G|}{4n}$. If n is even the share of good elements which lay in a torus twisted by an element of cycle-type $(\frac{n}{2}, -\frac{n}{2})$ in the set of good elements is $\frac{2}{2+n}$.*

Proof. Since good elements are regular the result can be proven as the corresponding estimate in [48].

The number of good elements in G is the number of good elements in a maximal non-split torus of even order times the number of maximal non-split tori of even order. We first compute the number of good elements in H^F. By Fact 1.14 there are $\frac{|H^F|}{|C_W(w)|}$ maximal non-split tori if n is odd where $w \in W$ is of cycle-type n or $-n$. If n is even we get $\frac{|H^F|}{|C_W(w_1)|} + \frac{|H^F|}{|C_W(w_2)|}$ maximal non-split tori where $w_1 \in W$ has cycle-type n and $w_2 \in W$ has cycle-type $(\frac{n}{2}, -\frac{n}{2})$. Since $|H^F| = 2|G|$ and $|C_W(w)| = \frac{|W|}{|w^W|} = \frac{2^n n!}{|w^W|}$ for any $w \in W$ we get that $\frac{|H^F|}{|C_W(w)|} = \frac{|G||w^W|}{2^{n-1}n!}$. Furthermore $|w^W|$ is the number of elements in W with the same cycle-type as w and hence $|w^W| = 2^{n-1}(n-1)!$ if w has cycle-type n or $-n$.

If $w \in W$ has cycle-type $(\frac{n}{2}, -\frac{n}{2})$ then $|w^W| = 2^n \frac{(n-1)!}{n}$. Thus if n is odd we have $\frac{|G|}{n}$ maximal non-split tori of even order, if n is even $\frac{|G|}{n} + \frac{2|G|}{n^2}$. If n is even the share of good elements which lay in a torus twisted by an element of cycle-type $(\frac{n}{2}, -\frac{n}{2})$ in the set of good elements is thus $\frac{2}{n^2}/(\frac{1}{n} + \frac{2}{n^2}) = \frac{2}{2+n}$.

Let S be a maximal non-split tours of even order. Let us consider case (ii) first. S is a cyclic group, generated by t. Let $\Phi(n,e)$ the product of all the primitive prime divisors of $q^n - 1$, counting multiplicities. Let S_0 be the set of good elements in S. Then $S_0 = S \backslash \langle t^{\Phi(n,e)} \rangle \cup \langle t^2 \rangle \cup \langle t^r \rangle$, where $r = \frac{q^{n/2}-1}{2}$ if n is even and $q \cong 1 \mod n$ and $r = q^n - 1$ otherwise. Thus if $n = 1 \mod 2$, then $t^r = 1$, if $n = 0 \mod 4$, then r is even and $t^r \in \langle t^2 \rangle$. In all other case, $r \geq 2n$. Since furthermore $\Phi(n,e) \geq n + 1$,

$$(*) \quad |S_0| \geq |S| - (\frac{1}{n+1} - \frac{1}{2} - \frac{1}{2n})|S| = \frac{n-2}{2(n+1)}|S|.$$

If $n \leq 5$ the last term of the sum in $(*)$ can be omitted and $|S_0| \geq |S| \frac{n-1}{2(n+1)} \geq \frac{|S|}{4}$. If $n \geq 6$ then $\frac{n-2}{n+1} \geq \frac{1}{2}$ and $|S_0| \geq \frac{|S|}{4}$ again. The share of good elements is thus at least $\frac{|G|}{4n}$ in this case.

In the second case S is cyclic as well, generated by x. Since every primitive prime divisor of $q^{2n} - 1$ divides $q^n + 1$, again $S_0 = S \backslash \langle x^{\Phi_{2n}(q)} \rangle \cup \langle x^2 \rangle$ and hence the share of good elements in S is at least $\frac{2n-1}{2(2n+1)} \geq \frac{1}{4}$. Hence more than $\frac{|G|}{4n}$ elements of G have good order. $\square$

6.2 Proof of the theorem

The algorithm spends most of its timing testing if elements are good. The following lemma corresponds to [46, 2.7.].

Lemma 6.5 *Let $m_1 := \prod_{i=2}^{2n-1} q^i - 1$ and $m_2 := \prod_{i=2}^{n-1} q^i - 1$. An element $g \in G$ is good*

- *in case (i), if $o(g) | q^{2n} - 1$ but $o(g) \nmid m_1$ and $o(g) \nmid \frac{q^n+1}{4}$,*
- *in case (ii) for n odd, if $o(g) | q^n - 1$ but $o(g) \nmid m_2$ and $o(g) \nmid \frac{q^n-1}{4}$,*
- *in case (ii) for n even, if $o(g) | q^n - 1$ but $o(g) \nmid m_2$ and $o(g) \nmid \frac{q^n-1}{4}$ and $o(g) \nmid q^{n/2} + 1$.*

If an element is good can thus be tested using $O(n^2 \log q)$ multiplications.

Proof. An element is good if it satisfies the conditions in the lemma by definition of good. Furthermore, we can decide if $o(g)$ divides k for any $k \in \mathbb{N}$ by computing g^k and comparing g^k with 1. This requires $O(\log k)$ multiplications if we use the squaring method. $\square$

Hence if $0 < \epsilon < 1$, we can find a good element x in time $O(\mu n^3 \log q + \xi n)$ with probability $1 - \epsilon$ by Proposition 6.4. Especially, a sample of 20n random elements of G contains a good element with probability $(1-(1-\frac{1}{4n})^{20n}) > 1-e^{-5}$.

Since x is an element of maximal 2-height, $i := x^{\frac{q^n+1}{4}}$ is an involution in case (i) and $i := x^{\frac{q^n-1}{4}}$ is an involution in case (ii). Hence i can be computed in time $O(\mu n \log q)$ time.

Proposition 6.6 *Let i be a involution in a maximal non-split torus $T_w \cap G$ of even order.*

(i) If w is of cycle type $-n$ or n, then i is of type t_n.

(ii) If w is of cycle type $(\frac{n}{2}, -\frac{n}{2})$, then i is of type $t_{\frac{n}{2}}$.

Proof. The easiest way to prove the claim is to look which centralizers of involutions of type t_k can contain maximal non-split tori of even order. Conjugacy classes of maximal tori and their orders are given by the tables in [37, 4.5] together with Fact 1.14 and [52]. Thus a maximal non-split torus of order $\frac{q+1}{2}$ can be only contained in centralizers of involutions of type t_n for both groups. A maximal non-split torus of order $\frac{q-1}{2}$ can arise in different ways. It can be contained in centralizers of involutions of type t_n or $t_{\frac{n}{2}}$ if n is even. Assume that n is even and that i is of type $t_{\frac{n}{2}}$. Then a torus in $C_G(i)$ of order $\frac{q-1}{2}$ arises as central product of a torus of order $q^{n/2} - 1$ and $q^{n/2} + 1$. That means that it is a torus twisted by an element of cycle type $(\frac{n}{2}, -\frac{n}{2})$. (Compare Lemma 6.2). This gives us the claim. $\square$

The crucial point of our algorithm is that we can choose elements of good order uniformly in both groups and that we can thus generate involutions of type t_n. However involutions of type t_n behave very differently in the two groups. In Section 5.2. we have seen, that involutions of type t_n invert maximal tori if G is of type C_n and while involutions of type t_n only invert one-dimensional tori if G is of type B_n. We can make this more precise.

Lemma 6.7 *Let $G := \Omega_{2n+1}(q)$ and $i \in G$ an involution of type t_n. Then $o(i^g i^h) | q(q+1)$ or $o(i^g i^h) | q(q-1)$ for all $g, h \in G$.*

Proof. Since i is of type t_n the dimension of V_- is $2n$. Thus dim $W_g \geq 2n-1$ for all $g \in G$ where $W_g := \{v \in V : ii^g(v) = v\}$. Therefore $i^g i^h$ acts as an element of $Gl(2, V)$ for all $g, h \in G$ and the claim follows □

Lemma 6.8 *Let $G := \mathrm{PSp}_{2n}(q)$ and $i \in G$ an involution of type t_n. Then $i^g i^h$ is good with probability $p > \frac{1}{30n}$ for random $g, h \in G$.*

Proof. Consider the map $\varphi : i^G \times i^G \longrightarrow G$. We are interested in the fibers of this map. Let $x \in G$ be a good element. Then x is contained in $\varphi(i^G \times i^G)$ by Lemma 5.9. Furthermore $|\varphi^{-1}(x)| = |I(C_G^*(x))| = |T|$, where T is the maximal non-split torus in which x is contained. Let us first assume $q^n \cong -1$ mod n. At least $\frac{|G|}{4n}$ elements of G are good by Proposition 6.4. Let X be the collection of all good elements, then $|\varphi(X)^{-1}| = |G|\frac{q^n+1}{4n}$. On the other hand $|i^G \times i^G| = |G|^2|C_G(i)|^{-2}$ and the share of pairs of involutions which are sent to a good element is $\frac{|C_G(i)|^2(q^n+1)}{|G|4n}$. Since we are in the first case, the centralizer of i is a twisted group of Lie type extended by a torus of order $q+1$ and an involution. Thus

$$|C_G(i)| = (q+1)q^{\frac{n(n-1)}{2}}(q^2-1)(q^3+1)\ldots(q^n+1)$$

by [26]. Hence

$$\frac{|C_G(i)|^2(q^n+1)}{|G|} = \frac{q^n+1}{q^n}\frac{(q+1)(q^2-1)\ldots(q^n+1)}{(q-1)(q^2+1)\ldots(q^n-1)}$$

If we set $x(n,q) := \prod_{i=1}^n \frac{q^i-(-1)^i}{q^i+(-1)^i}$ then $x(n,q) = e^{\sum_{i=0}^{n-1}(-1)^i f_i(q)}$ where $f_i(q) := ln(q^{i+1}+1) - ln(q^{i+1}-1)$. Since $f_i(q)$ is a strictly decreasing sequence for all $q \in \mathbb{N}, q > 1$, the sum is convergent and $\lim_{n\to\infty} x(n,q)$ exists. Since however by elementary analysis, $f_i(q) > 2\frac{1}{q^{i+1}}$, $x(n,q) > e^{2\sum_{i=0}^{n-1}(-1)^i\frac{1}{q^{i+1}}}$. The right side converges to $e^{2\frac{1}{1+q}}$ and is always greater than 1. Hence the share of pairs of involutions which are sent to good elements is greater than $\frac{1}{4n}$. If $q^n \cong 1 \mod n$, similar arguments apply. Here the share of pairs of involutions which are sent good elements is greater than $\frac{1}{4n}e^{-2}$. As $e(2) * 4 < 30$, this implies the claim. □

Hence an involution i is contained in a maximal non-split torus is of type t_n with probability 1 if n is odd, and probability at least $\frac{2}{2+n}$ if n is even. If, however, i is of type t_n, the type of the group can be recognized by the orders of strongly real elements by Lemma 6.7 and Lemma 6.8. This proves Theorem 6.1.

Bibliography

[1] T. Altınel, Groups of finite Morley rank with weekly embedded subgroup, to appear in J. Algebra.

[2] T. Altınel, Groups of finite Morley rank with strongly embedded subgroups, *J. Algebra* **180** (1996), 778-807.

[3] T. Altınel / A. Borovik / G. Cherlin, Groups of mixed type, *J. Algebra* **192** (1997), 524-571.

[4] T. Altınel / G. Cherlin, On central extensions of algebraic groups, to appear in J. Symb. Logic.

[5] T. Altınel / G. Cherlin / L.-J. Corredor / A. Nesin, A Hall theorem for ω-stable groups, to appear in J. London Math. Soc.

[6] C. Altseimer, "Bender-Gruppen von endlichem Morley Rang", Diplomarbeit an der Eberhard-Karls-Universität Tübingen, 1995.

[7] C. Altseimer / A. Berkman, Quasi- and pseudounipotent groups of finite Morley rank, preprint of the Manchester Centre for Pure Mathematics 1998/5.

[8] C. Altseimer, A Characterization of PSp(4,K), to appear in Comm. Algebra.

[9] L. Babai / E. Szemerédi, On the complexity of matrix group problems, *in* "Proc. 25th IEEE Sympos. Foundations Comp. Sci.", 1984, 229-240.

[10] L. Babai, Local expansion of vertex-transitive graphs and random generation in finite groups, *in* "Proc. ACM Symp. on Theory of Computing", 1991, 164-174.

[11] L. Babai, Randomization in group algorithms: conceptual questions, *in* "Groups and Computations II"(L. Finkelstein / W. Kantor, eds.), DIMACS: Series in Discrete Mathematics and Theoretical Computer Science 28, 1997, 1-17.

[12] L. Babai / P.P. Palfy, Recognizing finite simple groups by order statistics, in preparation.

[13] R. Beals, Towards polynomial time algorithms for matrix groups, *in* "Groups and Computations II"(L. Finkelstein / W. Kantor, eds.), DIMACS: Series in Discrete Mathematics and Theoretical Computer Science 28, 1997, 31-54.

[14] H. Bender, Transitive Gruppen gerader Ordnung, in denen jede Involution genau einen Punkt festläßt, *J. Algebra* **17** (1971), 175-204.

[15] A. Berkman, "Tame Groups of Finite Morley Rank", UMIST, Ph. D. Thesis, 1998.

[16] A. Borovik, 3-local Characterization of $G_2(2^n)$, preprint of the Akademy NAUK CCCP, Institut Mathematiki, Nowosibirsk, 1980, (in Russian).

[17] A. Borovik, On signalizer functors for groups of finite Morley rank, *in* "Soviet-French Colloquium on Model Theory", Karaganda, 1990, 11, (in Russian).

[18] A. Borovik / A. Nesin, "Groups of Finite Morley Rank", Oxford University Press, London, 1994.

[19] A. Borovik, Simply locally finite groups of finite Morley Rank and odd type, *in* "Proceedings of NATO ASI on Finite and Locally Finite Groups", Istanbul, 1994, 248-284.

[20] A. Borovik, Tame groups of odd and even type, to appear in "Algebraic Groups and their Representations"(R.W. Carter / J. Saxl, eds.), NATO ASI Series, Kluwer Academic Publisher, Dordrecht.

[21] R. Brauer, On finite Desarguesian planes I, *Math. Zeitschrift* **90** (1965), 117-123.

[22] R. Brauer, On finite Desarguesian planes II, *Math. Zeitschrift* **91** (1966), 124-151.

[23] R. Brauer, On finite Desarguesian planes III, *Math. Zeitschrift* **117** (1970), 76-82.

[24] D. Bressoud, "Factorization and Primality Testing", Springer, New York / Berlin / Heidelberg, 1989.

[25] R.W. Carter, Conjugacy Classes in the Weyl Group, *in* "Seminar on Algebraic Groups and Related Finite Groups"(A. Borel / R. Carter / C.W. Curtis / N. Iwahori/ T.A. Springer / R. Steinberg, eds.), Lecture Notes in Mathematics 131, Springer, 1970, G1-G22.

[26] R.W. Carter, "Simple Groups of Lie Type", John Wiley & Sons, London/New York/Sydney/Toronto, 1972.

[27] R.W. Carter. "Finite Groups of Lie type: conjugacy classes and complex characters", Wiley, Chichester, 1985.

[28] F. Celler / C. Leedham-Green, A non-constructive recognition algorithm for the special linear and other classical groups, *in* "Groups and Computations II"(L. Finkelstein / W. Kantor, eds.), DIMACS: Series in Discrete Mathematics and Theoretical Computer Science 28, 1997, 61-67.

[29] F. Celler / C. Leedham-Green / S. Murray / A. Niemeyer / E. O'Brien, Generating Random Elements of a finite group, *Comm. Algebra* **23** (1995), 4931-4948.

[30] F. Celler, "Konstruktive Erkennungsalgorithmen klassischer Gruppen in GAP", Aachener Beiträge zur Mathematik 20, Verlag der Augustinus Buchhandlung, Aachen, 1997.

[31] Z. Chatzidakis / L. van den Dries / A. Macintyre, Definable sets over finite fields, *J. reine angew. Math.* **427** (1992), 107-135.

[32] G. Cherlin, Groups of small Morley rank, *Annals of Math. Logic* **17** (1979), 1-28.

[33] M.J. DeBonis / A. Nesin, On BN-Pairs of Tits Rank 2 and of Finite Morley Rank, submitted.

[34] L. Fuchs, "Abelian Groups", 3rd ed., Pergamon Press, Oxford, 1967.

[35] D. Gorenstein, "Finite Groups", 2nd ed., Chelsea, New York, 1980.

[36] D. Gorenstein, "Finite Simple Groups: An Introduction to their Classification", Plenum Press, New York, 1982.

[37] D. Gorenstein / R. Lyons / R. Solomon, "The classification of the finite simple groups 3", Mathematical surveys and Monographs 40, AMS, Providence, 1998.

[38] P. Hall, Some sufficient conditions for a group to be nilpotent, *Illinois J. Math.* **2** (1958), 787-801.

[39] I.M. Isaacs / W.M. Kantor / N. Spaltenstein, On the probability that a group element is p-singular, *J. Algebra* **176** (1995), 139-181.

[40] R. Howlett, Normalizers of Parabolic Subgroups of Reflection Groups, *J. London Math. Soc. (2)* **21** (1980), 62-80.

[41] J. Humphreys, "Introduction to Lie Algebras and Representation Theory", Springer, New York, 1972.

[42] J. Humphreys, "Linear Algebraic Groups", Springer, New York , 1975.

[43] J. Humphreys, "Reflections Groups and Coxeter Groups", Cambridge University Press, 1994.

[44] B. Huppert, "Endliche Gruppen I", Grundlehren der math. Wissenschaften 134, Springer, Berlin, 1979.

[45] N. Iwahori, Centralizers of Involutions in finite Chevalley Groups, *in* "Seminar on Algebraic Groups and Related Finite Groups" (A. Borel / R. Carter / C.W. Curtis / N. Iwahori/ T.A. Springer / R. Steinberg, eds.), Lecture Notes in Mathematics 131,Springer, 1970, F1-F29.

[46] W. Kantor / A. Seress, Black box classical groups, submitted.

[47] W. Kantor / A. Seress, in preparation.

[48] P. Neuman / C. Praeger, A recognition algorithm for special linear groups, *Proc. London Math. Soc. (3)* **65** (1992), 555-603.

[49] A. Niemeyer / C. Praeger, A Recognition Algorithm for Classical Groups over Finite Fields, *Proc. London Math. Soc. (3)* **77** (1998), 117-169.

[50] B. Poizat, "Groupes Stables", Nur al-Mantiq wal Ma'rifah, Lyon, 1987.

[51] M. Schönert et al., "GAP – Groups, Algorithms, and Programming", 3rd. ed., Lehrstuhl D für Mathematik, RWTH Aachen, 1997.

[52] T.A. Springer / R. Steinberg, Conjugacy Classes, *in* "Seminar on Algebraic Groups and Related Finite Groups" (A. Borel / R. Carter / C.W. Curtis / N. Iwahori/ T.A. Springer / R. Steinberg, eds.), Lecture Notes in Mathematics 131, Springer, 1970, E1-E100.

[53] R. Steinberg, "Endomorphisms of Linear Algebraic Groups", Memoirs of the AMS, 80, Providence, Rhode Island, 1968.

[54] M. Suzuki, "Group theory I", Grundlehren der math. Wissenschaften 247, Springer, New York, 1982.

[55] M. Suzuki, "Group theory II", Grundlehren der math. Wissenschaften 248, Springer, New York, 1986.

[56] D.E. Taylor, "The Geometry of the Classical Groups", Heldermann, Berlin, 1992.

[57] W.J. Wong, The characterization of the finite projective symplectic groups $PSp_4(q)$, *Trans. of the Amer. Math. Soc.* **139** (1969), 1-35.

[58] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. für Math. u. Phys.* **3** (1892), 265-284.

Index