3-LOCAL IDENTIFICATIONS OF SOME FINITE SIMPLE GROUPS

by

SARAH ASTILL

A thesis submitted to
The University of Birmingham
for the degree of
MASTER OF PHILOSOPHY (SC, QUAL)

School of Mathematics
The University of Birmingham

Abstract

In this thesis we characterize the groups $\mathrm{PSL}_3(3)$, M_{12}, $G_2(3)$ and $\mathrm{PSp}_4(3)$ by their 3-local structure. We identify each group as a finite faithful completion of a certain type of rank 2-amalgam known as a weak BN-pair.

Acknowledgements

I am grateful for the help, support and encouragement first and foremost from my supervisor Professor Chris Parker. Thanks also go to Dr Rachel Fowler, Dr Murray Clelland, Dr Rebecca Waldecker and James Sprittles. Finally, I gratefully acknowledge the financial support of the EPSRC.

Contents

Introduction

A p-local subgroup (p a prime) of a group is the normalizer of a non-trivial p-subgroup. To identify a group p-locally is to determine the isomorphism type of a group given some information about its p-local structure. Suppose we have a finite group G with a Sylow p-subgroup S such that S has subgroups A and B which are normalized by $N_G(S)$ then the intersection of $N_G(A)$ and $N_G(B)$ contains $N_G(S)$. The Amalgam Method aims to characterize G given the subgroup structure associated to $N_G(A)$ and $N_G(B)$.

A rank two amalgam of finite groups, $\mathcal{A} = (P_1, P_2, C, \phi_1, \phi_2)$, is a collection of three finite groups, P_1, P_2 and C, and two injective homomorphisms, $\phi_1 : C \to P_1$ and $\phi_2 : C \to P_2$. A completion, (G, ψ_1, ψ_2), of the amalgam is a group, G, such that $\psi_1 : P_1 \to G$ and $\psi_2 : P_2 \to G$ are homomorphisms with $G = \langle \psi_1(P_1), \psi_2(P_2) \rangle$ and such that $\phi_1\psi_1 = \phi_2\psi_2$. In [7], Delgado and Stellmacher first defined weak BN-pairs of rank two. They described a situation when a rank two amalgam (P_1, P_2, C) satisfied some local conditions notably that $O_p(P_i)$ ($i = 1, 2$ and p a fixed prime) admitted an action from $O^{p'}(P_i)/O_p(P_i) \cong \mathrm{PSL}_2(p^{n_i}), \mathrm{SL}_2(p^{n_i}), \mathrm{U}_3(p^{n_i}), \mathrm{SU}_3(p^{n_i}), \mathrm{Sz}(2^{n_i})$ or $\mathrm{Dih}(10)$ (and $p = 2$) or $\mathrm{Ree}(3^{n_i}), \mathrm{Ree}(3)'$ (and $p = 3$). They classified the possible types of amalgam and described each one. In [23], Parker and Rowley examined the BN-pairs for which the characteristic prime, p, is odd. They characterized finite faithful completions satisfying some p-local conditions under a $\mathcal{K}$-proper hypothesis. In this thesis we are interested in the weak BN-pairs (P_1, P_2, C) such that, for $i = 1$ or 2, $O_3(P_i)$ admits an action from $\mathrm{SL}_2(3)$ of which there are four types. One of these, the exceptional weak BN-pair of type F_3, has recently been studied by Rachel Fowler to characterize the Thompson sporadic simple group [10]. Her characterization relies on a $\mathcal{K}$-proper hypothesis to recognize a section of the Thompson group which is isomorphic to $G_2(3)$. In this thesis we will describe the remaining three weak BN-pairs which have types $\mathrm{PSL}_3(3)$, $G_2(3)$ and $\mathrm{PSp}_4(3)$. Furthermore, we will characterize the groups $\mathrm{PSL}_3(3)$ and M_{12}; $G_2(3)$; and $\mathrm{PSp}_4(3)$ as finite faithful completions of the respective amalgams. Notably, the characterization of $G_2(3)$ will be used in [11] to strengthen the characterization of the Thompson sporadic simple group thereby removing any reliance on the $\mathcal{K}$-proper hypothesis.

We will examine the amalgams by studying the local group theoretic structure of the groups which constitute the amalgam. Therefore we begin in Chapter 1 with some well known group theoretic results which will be referred to throughout this thesis. In Chapter 2 we discuss some representation theory. In particular, we describe the $\mathrm{SL}_2(3)$-modules which will appear within the group theoretic structure of the groups in the amalgams. In Chapter 3 we will formally define an amalgam and a completion of an amalgam. We will also associate a certain graph, called the coset graph, to a completion of an amalgam. The coset graphs associated to $G_2(3)$ and $\mathrm{PSp}_4(3)$ are Moufang Polygons (these are defined and classified in [29]) and so in Chapter 4 we define such graphs and state the classification theorem of Tits and Weiss. Also in Chapter 4, we present a character theoretic result due to Feit and Thompson ([9]) which describes a finite group containing a self-centralizing element of order three. We also discuss a theorem of the same nature by Smith and Tyrer ([27]). Their theorem describes groups in which the automizer of an abelian Sylow p-subgroup (odd prime p) has order just two. We will use both results several times in the group recognition theorems in later chapters.

In Chapter 5 we begin to prove the main theorems of this thesis. The main hypothesis and theorem in Chapter 5 are as follows.

Hypothesis A. Let G be a finite group with subgroups $A \cong B$ such that $C := A \cap B$ contains a Sylow 3-subgroup of both A and B and such that no non-trivial normal subgroup of C is normal in both A and B. Suppose further that

(i) $G = \langle A, B \rangle$;

(ii) $A/O_3(A) \cong B/O_3(B) \cong \mathrm{GL}_2(3)$;

(iii) $O_3(A)$ and $O_3(B)$ are natural modules with respect to the actions of $A/O_3(A)$ and $B/O_3(B)$ respectively; and

(iv) for $S \in \mathrm{Syl}_3(C)$, $N_G(Z(S)) = N_A(Z(S)) = N_B(Z(S))$.

Theorem A. *If G satisfies Hypothesis A, then $G \cong \mathrm{M}_{12}$ or $\mathrm{PSL}_3(3)$.*

We may refer to the amalgam (A, B, C) as an amalgam of type $\mathrm{PSL}_3(3)$. This amalgam is particularly interesting as it completes to $\mathrm{PSL}_3(3)$ and also to the sporadic simple group M_{12} under the same 3-local assumption, namely condition *(iv)* of the hypothesis.

The main theorem and hypothesis in Chapter 6 are:

Hypothesis B. Let $\mathcal{G}$ be a finite group with non-conjugate subgroups A_1 and A_2 such that $A_{12} := A_1 \cap A_2$ contains a Sylow 3-subgroup of both A_1 and A_2, and such that no non-trivial normal subgroup of A_{12} is normal in both A_1 and A_2. Suppose further that, for $i = 1, 2$,

(i) $|O_3(A_i)| = 3^5$;

(ii) $A_i/O_3(A_i) \cong \mathrm{GL}_2(3)$;

(iii) $O_3(O_3(A_i))/Z(A_i)$ and $Z(O_3(A_i))/O_3(A_i)'$ are natural modules with respect to the action of $A_i/O_3(A_i)$; and

(iv) $N_{\mathcal{G}}(O_3(A_i)') = A_i$.

Theorem B. *Let $\mathcal{G}$ be a group satisfying Hypothesis B. Then $\mathcal{G} \cong G_2(3)$.*

In some sense this is the strongest amalgam theoretic result we prove since we begin with a group containing a completion of the amalgam, as opposed to Theorem A which characterizes just the completion itself.

The methods successfully used in Chapter 6 are extended in Chapter 7 where we describe an amalgam of type $\mathrm{PSp}_4(3)$. The hypothesis we assume is strong and so the theorem is less successful than other characterizations of $\mathrm{PSp}_4(3)$ (see for example [24] and [16]).

Hypothesis C. Let A_1 and A_2 be subgroups of a finite group $G = \langle A_1, A_2 \rangle$ such that $A_{12} := A_1 \cap A_2$ contains a Sylow 3-subgroup of both A_1 and A_2 and such that no non-trivial normal subgroup of A_{12} is normal in both A_1 and A_2. Suppose further that

(*i*) $A_1/O_3(A_1) \cong \mathrm{Sym}(4)$;

(*ii*) $A_2/O_3(A_2) \cong \mathrm{SL}_2(3)$;

(*iii*) $O_3(A_1)$ is elementary abelian of order 3^3 and is a faithful $A_1/O_3(A_1)$-module;

(*iv*) $O_3(A_2)$ is extraspecial of order 3^3 and $O_3(A_2)/Z(O_3(A_2))$, is a natural $A_2/O_3(A_2)$-module;

(*v*) $N_G(O_3(A_1)) = A_1$ and $N_G(Z(O_3(A_2))) = A_2$; and

(*vi*) $O_3(A_1)$ normalizes no non-trivial $3'$-subgroup of G.

Theorem C. *Let G be a group satisfying Hypothesis C. Then $G \cong \mathrm{PSp}_4(3)$.*

Notably condition (*vi*) of the hypothesis makes this theorem less successful than Theorem B. However, it is possible to construct groups which have shape $2^6 : \mathrm{PSp}_4(3)$ and

$5^6 : \mathrm{PSp}_4(3)$ which satisfy the 3-local condition (v). Certainly condition (vi) in the hypothesis rules out such groups however a preferable alternative hypothesis might be to assume $O_{3'}(G) = 1$. At present it is unclear whether this alternative hypothesis would be sufficient. The uncertainty about such groups does however raise an interesting question: for which finite groups G does there exist $1 \neq N \trianglelefteq G$ such that $G/N \cong \mathrm{PSp}_4(3)$? Higman answered a similar question about $\mathrm{SL}_2(2^n)$ in [17] and so Chapter 8 together with much of the representation theory in Chapter 2 is devoted to understanding Higman's result. An open question is whether the methods from Chapter 8 can be extended to $\mathrm{PSp}_4(3)$.

We include also a short appendix which contains some elementary number theoretic proofs concerning orders of fields. The appendix also contains a proof related to the coset graph in Chapter 6.

Before we begin we note that all groups will be finite and all vector spaces will be finite dimensional. We use Atlas [6] notation for groups and group extensions with the exception of the alternating, symmetric and dihedral groups which are labeled $\mathrm{Alt}(n)$, $\mathrm{Sym}(n)$ and $\mathrm{Dih}(n)$ respectively.

Chapter 1

Some Group Theory

1.1 Some General Group Theoretic Results

Lemma 1.1. *Let p be a prime and let A be a p-group acting on a non-trivial p-group V. Then $C_V(A) \neq 1$ and $[V, A] < V$. In particular if V is an FA-module where F is a field of characteristic p then $C_V(A)$ is a non-trivial submodule and $[V, A]$ is a proper submodule of V.*

Proof. If we form the semidirect product $S := V : A$ then S is a p-group with normal subgroup V. Thus, S has non-trivial centre and $Z(S) \cap V \neq 1$. Hence $C_V(A) \neq 1$. Now since S is a finite p-group, S is nilpotent and so for some integer n, $1 = [S, S, n] = [S, S, \ldots, S]$ (n'th term in lower central series). So suppose $[V, A] = V$ then $V = [V, A, A, \ldots, A] = [V, A, n] \leqslant [S, S, n] = 1$ which is a contradiction. $\square$

A group, G, is said to act equivalently on two sets Ω_1 and Ω_2 if there is a bijection $\alpha : \Omega_1 \to \Omega_2$ such that for $\omega \in \Omega_1$, $g \in G$, $\alpha(\omega \cdot g) = \alpha(\omega) \cdot g$.

Lemma 1.2. *Suppose G is a group with subgroups A and B which normalize each other. Suppose further that both are acted on by another group X. Then the action of X on*

AB/A is equivalent to the action of X on $B/(A \cap B)$. In particular X commutes with AB/A if and only if X commutes with $B/(A \cap B)$.

Proof. Let α be the natural isomorphism $\alpha : AB/A \to B/(A \cap B)$ then for $x \in X$ and $Ab \in AB/A$,

$$\alpha(Ab^x) = \alpha(A(b^x)) = (A \cap B)b^x = ((A \cap B)b)^x = \alpha(Ab)^x$$

and so the action is equivalent. □

Lemma 1.3. *Let G be a group and let $a, b, c \in G$. The following identities hold.*

(i) $[a, bc] = [a, c][a, b]^c$.

(ii) $[ab, c] = [a, c]^b[b, c]$.

(iii) If p is a prime and if G is a p-group then $[[a, b], c][[b, c], a][[c, a], b] \in [G, G, G, G]$.

Proof. The first two identities are easy to check the third is Lemma 5.6.1 *(iv)* in [13, p209]. □

Definition 1.4. Let A be a group acting on a group G. The action of A on G is coprime if $|A|$ and $|G|$ are coprime.

Theorem 1.5. *(Coprime Action) Suppose A is a group acting on the group G and suppose the action of A on G is coprime. The following hold.*

(i) $G = [G, A]C_G(A)$ and if G is abelian $G = [G, A] \times C_G(A)$.

(ii) $[G, A] = [G, A, A]$.

(iii) $C_{G/N}(A) = C_G(A)N/N$ for any A-invariant $N \trianglelefteq G$.

(*iv*) *If A is an elementary abelian p-group of order at least p^2 then* $G = \langle C_G(a) | a \in A^{\#} \rangle = \langle C_G(A_1) | [A : A_1] = p \rangle$.

Proof. For (*i*) and (*ii*) see [20, 8.2.7 p187]. For (*iii*) see [20, 8.2.2 p184]. For (*iv*) see [20, 8.3.4 p193]. □

A group G is said to have a normal p-complement if $O_{p'}(G) = O^p(G)$ or equivalently if G has a normal subgroup N such that G is the semidirect product of N with some Sylow p-subgroup.

Theorem 1.6. *(Burnside) Let P be a Sylow p-subgroup of a group G. Suppose $N_G(P) = C_G(P)$. Then G has a normal p-complement.*

Proof. See [20, p169]. □

Lemma 1.7 (Frattini Argument). *Let K be a normal subgroup of a group G and let P be a Sylow p-subgroup of K (for some prime p) then $G = KN_G(P)$.*

Let K be a normal subgroup of a group G and let $R \leqslant G$. Then $G = N_G(R)K$ if and only if $R^G = \{r^g | r \in R, g \in G\} = \{r^k | r \in R, k \in K\} = R^K$.

Proof. The first result is a special case of the second since if P is a Sylow p-subgroup of $K \trianglelefteq G$ then for any $g \in G$, $P^g \leqslant K$ implies $P^g = P^k$ for some $k \in K$ by Sylow's Theorem. So we prove the second result.

Suppose $R^G = R^K$. For any $g \in G$ there exists $k \in K$ such that $R^g = R^k$. Therefore $gk^{-1} \in N_G(R)$ and so $g \in N_G(R)k$. Hence $G = N_G(R)K$. Now suppose $G = N_G(R)K$ and suppose $R^K \subset R^G$. Then there exists $g \in G$ such that $R^g \nsubseteq R^K$. However $g = nk$ where $n \in N_G(R)$ and $k \in K$ and so $R^g = R^{nk} = Rk \subseteq R^K$ which is a contradiction. □

Theorem 1.8. *(Gaschütz) Let p be a prime and V an abelian normal p-subgroup of a group G. Let $V \leqslant P \in \mathrm{Syl}_p(G)$. Then G splits over V if and only if P splits over V.*

Proof. See [1, 10.4 p31]. □

Lemma 1.9. *(Burnside) Let G be a group and let P be a Sylow p-subgroup of G. Suppose A_1 and A_2 are normal subsets of P which are conjugate in G. Then they are already conjugate in $N_G(P)$.*

Proof. See [20, 7.1.5 p167]. □

Definition 1.10. Let G be a group, p be a prime and $S \in \mathrm{Syl}_p(G)$. Let $A(S)$ be the set of abelian subgroups of S of order p^r where p^r is as large as possible. The Thompson subgroup of S is $J(S) = \langle A | A \in A(S) \rangle$.

Lemma 1.11. *Let G be a group, p be a prime and $S \in \mathrm{Syl}_p(G)$. Suppose $J(S) = Z(J(S))$ and suppose $a, b \in J(S)$ are conjugate in G. Then a and b are conjugate in $N_G(J(S))$.*

Proof. Suppose $a^g = b$ for some $g \in G$. Notice first that it follows immediately from the definition of the Thompson subgroup that $J(S)^g = J(S^g)$. Now $J(S), J(S^g) \leqslant C_G(b)$. Let $P, Q \in \mathrm{Syl}_p(C_G(b))$ such that $J(S) \leqslant P$ and $J(S^g) \leqslant Q$. Again, by the definition of the Thompson subgroup, it is clear that $J(S) \leqslant P$ implies $J(S) = J(P)$ and similarly $J(S^g) = J(Q)$. By Sylow's Theorem, there exists $x \in C_G(b)$ such that $Q^x = P$ and so $J(S) = J(P) = J(Q)^x = J(S)^{gx}$. Thus $gx \in N_G(J(S))$ and $a^{gx} = b^x = b$ as required. □

Definition 1.12. The Fitting subgroup of a group G is the group, $F(G)$, generated by all nilpotent normal subgroups in G

Theorem 1.13. *Let G be a group and $F(G)$ the Fitting subgroup. Then the following hold.*

(i) $F(G)$ is the unique maximal nilpotent normal subgroup of G.

(ii) If G is soluble then $C_G(F(G)) \leqslant F(G)$.

Proof. See [13, Thm6.1.2, Thm6.1.3 p218]. □

1.2 Extraspecial Groups

Definition 1.14. Let p be a prime and let E be a p-group. If $E' = Z(E) = \Phi(E)$ is cyclic of order p then E is said to be extraspecial.

Lemma 1.15. *Let E be an extraspecial p-group. Exactly one of the following holds.*

(i) $p = 2$ *and* E *is a central product of* n *copies of* $\mathrm{Dih}(8)$.

(ii) $p = 2$ *and* E *is a central product of* $n-1$ *copies of* $\mathrm{Dih}(8)$ *and one copy of* Q_8.

(iii) $p \neq 2$ *and* E *has exponent* p.

(iv) $p \neq 2$ *and* E *has exponent* p^2.

We denote such groups as $E \cong 2_+^{1+2n}$, 2_-^{1+2n}, p_+^{1+2n} *and* p_-^{1+2n} *respectively.*

Proof. See [8, Thm 20.5]. □

It is well known that $\mathrm{Dih}(8) * \mathrm{Dih}(8) \cong Q_8 * Q_8$ so the description of extraspecial 2-groups given here is not unique.

Theorem 1.16. *Suppose E is an extraspecial p-group of order p^{2n+1}.*

(i) *If* $p = 2$ *and* $E \cong 2_+^{1+2n}$ *then* $\mathrm{Out}(E) \cong \mathrm{O}_{2n}^+(2)$.

(ii) *If* $p = 2$ *and* $E \cong 2_-^{1+2n}$ *then* $\mathrm{Out}(E) \cong \mathrm{O}_{2n}^-(2)$.

(iii) *If* p *is odd and* $E \cong p_+^{1+2n}$ *then* $\mathrm{Out}(E) \cong \mathrm{Sp}_{2n}(p)C_{p-1}$.

(iv) *If* p *is odd and* $E \cong p_-^{1+2n}$ *then* $\mathrm{Out}(E) \cong p_+^{2n-1}\mathrm{Sp}_{2n-2}(p)C_{p-1}$.

Proof. See [15]. □

Corollary 1.17. *Let E be an extraspecial 2-group of order 2^5. If E admits a group of automorphisms of order nine then $E \cong 2_+^{1+4}$.*

Proof. This is clear since 9 does not divide $|O_4^-(2)| = 120$. □

Lemma 1.18. *The extraspecial 2-group 2_+^{1+4} contains exactly two subgroups isomorphic to Q_8 and they commute.*

Proof. Firstly $2_+^{1+4} \cong \mathrm{Dih}(8) * \mathrm{Dih}(8) \cong Q_8 * Q_8$ so there are at least two subgroups isomorphic to Q_8 and we need to prove there cannot be more. We let Q_1 and Q_2 be the two commuting quaternion subgroups and count elements of order four in $Q := \langle Q_1, Q_2 \rangle$. Clearly we see six elements of order four in Q_1 and six more in Q_2. So suppose $q_i \in Q_i$ for $i = 1, 2$ and $q_1 q_2$ is another element of order four. If q_1 has order two then it is central in Q_1 and then $q_1 q_2 \in Q_2$. Therefore q_1, and in the same way q_2, is an element of order four and so both q_1 and q_2 square to the same element in $z \in Z(Q) \cong C_2$. However, this means $(q_1 q_2)^2 = q_1^2 q_2^2 = z^2 = 1$ which is a contradiction. Therefore there are exactly 12 elements of order four in Q. So if $Q_3 \leqslant Q$ is a subgroup isomorphic to Q_8 then Q_3 must contain an element of order four from Q_1 and an element of order four from Q_2. However these two elements commute so Q_3 cannot be isomorphic to Q_8. □

1.3 Fixed-Point-Free Actions

An automorphism of a group G is said to be *fixed-point-free* if it leaves only the identity of G fixed. The following famous theorem was proved by Thompson and says that groups admitting such an action from an automorphism of prime order are nilpotent.

Theorem 1.19. *(Thompson) If G is a group which admits a fixed-point-free automorphism of prime order then G is nilpotent.*

Proof. See [13, Thm 2.1 p337]. □

Lemma 1.20. *Let ϕ be a fixed-point-free automorphism of order two of a group G. Then ϕ inverts every element of G and G is abelian.*

Proof. Define

$$\begin{array}{rcccl} \theta & : & G & \longrightarrow & G \\ & & g & \longmapsto & g^{-1}\phi(g). \end{array}$$

Then θ is injective since $x^{-1}\phi(x) = y^{-1}\phi(y)$ if and only if $yx^{-1} = \phi(y)\phi(x)^{-1} = \phi(yx^{-1})$ if and only if $yx^{-1} = 1$ if and only if $x = y$. Also θ is onto since G is finite. So for each $g \in G$ there is some $h \in G$ such that $g = h^{-1}\phi(h)$ therefore $\phi(g) = \phi(h^{-1})h = g^{-1}$. So ϕ inverts every element of G. Let $x, y \in G$. Then

$$x^{-1}y^{-1} = \phi(x)\phi(y) = \phi(xy) = (xy)^{-1} = y^{-1}x^{-1}$$

and so $xy = yx$ and G is abelian. □

The following lemma and its proof generalizes a well known result which dates back to Burnside the proof of which can be found in [17, Thm 8.1]. We will use the notation $a \equiv b \bmod H$ when $Ha = Hb$ where $a, b \in G \geqslant H$.

Lemma 1.21. *Suppose that p is a prime and Q is a p-group. Furthermore, suppose that $z \in \mathrm{Aut}(Q)$ has order three and $C_Q(z) = \langle t \rangle$ where $t \in Z(Q)$ has prime order. Then Q is nilpotent of class at most three. In particular $[Q, Q, Q] \leqslant \langle t \rangle$ and for any $a, b \in Q$, $[a, b^z] \equiv [a^z, b] \equiv [a, b]^{z^2} \bmod \langle t \rangle$.*

Proof. Let $Q = Q_1 \geqslant Q_2 \geqslant Q_3 \geqslant \dots$ be the lower central series of Q. Then for each i, $\langle t \rangle Q_i / Q_{i+1}$ is a central subgroup of Q/Q_{i+1} which is acted on by z. Moreover, z can only centralize the subgroup $\langle t \rangle Q_{i+1}/Q_{i+1}$.

For any $a \in Q$, $aa^z a^{z^2}$ is a fixed point modulo Q_2 so

$$aa^z a^{z^2} \equiv 1 \bmod \langle t \rangle Q_2.$$

It follows from the commutator relations (Lemma 1.3) and from Q_2/Q_3 being abelian that $[a,b][a^z,b][a^{z^2},b] \equiv [aa^za^{z^2},b] \equiv 1 \bmod Q_3$ and $[a,b][a,b^z][a,b^{z^2}] \equiv [a,bb^zb^{z^2}] \equiv 1 \bmod Q_3$ for any $a,b \in Q$. Therefore

$$[a,b] \equiv [b,a^z][b,a^{z^2}] \equiv [b^z,a][b^{z^2},a] \bmod Q_3.$$

Rearranging gives

$$[a,b^z][b,a^z] \equiv [a^{z^2},b][b^{z^2},a] \bmod Q_3.$$

Therefore $[a,b^z][b,a^z]Q_3$ is a z-invariant element of Q_2/Q_3 and so must be in $\langle t\rangle Q_3/Q_3$. Hence

$$[a,b^z] \equiv [a^z,b] \bmod \langle t\rangle Q_3. \tag{1.1}$$

Now we repeat these arguments modulo Q_4. For $a,b \in Q$ the element $[a,b][a,b]^z[a,b]^{z^2}$ is a fixed point modulo Q_3 and so

$$[a,b][a,b]^z[a,b]^{z^2} \equiv 1 \bmod \langle t\rangle Q_3.$$

Using the commutator relation again and since Q_3/Q_4 is abelian, for $a,b,c \in Q$,

$$[[a,b],c][[a,b]^z,c][[a,b]^{z^2},c] \equiv [[a,b][a,b]^z[a,b]^{z^2},c] \equiv 1 \bmod Q_4.$$

Also,

$$[[a,b],c][[a,b],c^z][[a,b],c^{z^2}] \equiv [[a,b],cc^zc^{z^2}] \equiv 1 \bmod Q_4.$$

Therefore

$$[[a,b],c] \equiv [c,[a,b]^{z^2}][c,[a,b]^z] \equiv [c^z,[a,b]][c^{z^2},[a,b]] \bmod Q_4.$$

Rearranging gives

$$[c,[a,b]^{z^2}][[a,b],c^{z^2}] \equiv [c^z,[a,b]][[a,b]^z,c] \bmod Q_4.$$

The corresponding element modulo Q_4 is z-invariant and therefore must be in $\langle t\rangle Q_4/Q_4$ and so

$$[[a,b]^{z^2},c] \equiv [[a,b],c^{z^2}] \bmod \langle t\rangle Q_4,$$

and in a similar way

$$[[a,b]^{z^2},c] \equiv [[a,b],c^{z^2}] \equiv [[a,b],c]^z \equiv [[a^z,b],c] \equiv [[a,b^z],c] \bmod \langle t\rangle Q_4. \tag{1.2}$$

Now Lemma 1.3 (*iii*) gives

$$[[a,b],c][[b,c],a][[c,a],b] \equiv 1 \bmod Q_4 \tag{1.3}$$

and

$$[[a^z,b],c][[b,c],a^z][[c,a^z],b] \equiv 1 \bmod Q_4. \tag{1.4}$$

Conjugating (1.3) by z and applying (1.2) gives

$$[[a^z,b],c][[b,c],a^{z^2}][[c,a^z],b] \equiv 1 \bmod \langle t\rangle Q_4$$

which together with (1.4) gives

$$[[b,c],a^{z^2}][[c,a^z],b] \equiv [[b,c],a^z][[c,a^z],b] \bmod \langle t\rangle Q_4.$$

Hence $[[b,c],a^{z^2}] \equiv [[b,c],a^z] \bmod \langle t\rangle Q_4$. Finally, using (1.2) we get

$$[[b,c],a]^z \equiv [[b,c],a^{z^2}] \equiv [[b,c],a^z] \equiv [[b,c],a]^{z^2} \bmod \langle t\rangle Q_4$$

is a fixed point mod Q_4 which gives $[[b,c],a] \in \langle t\rangle Q_4$ for any $a,b,c \in Q$, however this implies that $Q_3 \leqslant \langle t\rangle Q_4 \leqslant \langle t\rangle Q_3$. Since $\langle t\rangle$ has prime order, either $\langle t\rangle Q_3 = \langle t\rangle Q_4$ and then $Q_3 = Q_4$ (so Q has nilpotence class two), else, $Q_3 = \langle t\rangle Q_4$. In this second case we get $Q_5 = [Q_4, Q] = [\langle t\rangle Q_3, Q] = [Q_3, Q] = Q_4$ and so $Q_4 = 1$ and $Q_3 = \langle t\rangle$. In either case Equation 1.1 becomes $[a, b^z] \equiv [a^z, b] \bmod \langle t\rangle$ for any a, $b \in Q$ and applying this congruence again replacing a and b with a^{z^2} and b^{z^2} gives $[a, b^z] \equiv [a,b]^{z^2} \bmod \langle t\rangle$. □

Corollary 1.22. *Let Q be a group and let $z \in \mathrm{Aut}(Q)$ have order three and $C_Q(z) = \langle t\rangle$ where $t \in Z(Q)$ has prime order. Then Q is nilpotent of class at most three.*

Proof. By Theorem 1.19, $Q/\langle t\rangle$ is nilpotent and so is a direct product of its Sylow p-subgroups. Since $\langle t\rangle$ is central of prime order, Q is nilpotent and a direct product of its Sylow subgroups. Moreover each Sylow subgroup is nilpotent of class less or equal to three and so Q is nilpotent of class less or equal to three. □

Corollary 1.23. *Suppose Q is a 2-group with $z \in \mathrm{Aut}(Q)$ of order 3 and $C_Q(z) = \langle t\rangle \cong C_2$. If $Q = \langle X, Y\rangle$ with $X \cong Y \cong Q_8$ and $Z(X) = Z(Y) = \langle t\rangle$ then $[x, y^z] \equiv [x^z, y] \bmod \langle t\rangle$ for all $x \in X$ and all $y \in Y$.*

In fact such a group Q has order at most 2^7 and there exist two isomorphism classes of groups of this order admitting such an automorphism. They can be constructed in Magma (see [4]) by deriving possible relations from the congruence $[a, b^z] \equiv [a^z, b] \bmod \langle t\rangle$ for all $a, b \in Q$.

Lemma 1.24. *(Burnside) Suppose that Q is a group and suppose that $z \in \mathrm{Aut}(Q)$ has order three and acts fixed-point-freely on $Q\backslash\{1\}$. Then Q is nilpotent of class at most two.*

Proof. Apply Corollary 1.22 with $t = 1$. □

Lemma 1.25. *Suppose S is a 2-group and A,B are fours groups with $A \neq B$ and $S = \langle A, B\rangle$. If $z \in \mathrm{Aut}(S)$ has order 3, A and B are z-invariant and $C_S(z) = 1$, then either S is elementary abelian of order 2^4 or special of order 2^6 with $|Z(S)| = 2^2$.*

Proof. By Lemma 1.24, S has nilpotence class at most two. If S is abelian then S has order 2^4 so assume not then S has class two. Thus commutators are central giving us that $S' = \langle [a,b] | a \in A, b \in B \rangle$ and for every $a \in A$, $b \in B$,

$$1 = [[a,b],b] = (baba)b(abab)b = (baba)(baba) = [b,a]^2,$$

and so S' is elementary abelian. Since both A and B are z-invariant, we can write $A \backslash \{1\} = \{a_0, a_1, a_2\}$ where $a_1 = a_0^z$ and $a_2 = a_0^{z^2}$ and similarly we label $B \backslash \{1\} = \{b_0, b_1, b_2\}$. Thus, for $i, j \in \mathbb{Z}_3$, $[a_i, b_j][a_{i+1}, b_{j+1}][a_{i+2}, b_{j+2}] \in C_S(z) = 1$. And so

$$\begin{aligned} [a_i, b_j][a_{i+1}, b_{j+1}] &= [a_{i+2}, b_{j+2}] \\ &= [a_i a_{i+1}, b_j b_{j+1}] \\ &= [a_i, b_j][a_i, b_{j+1}][a_{i+1}, b_j][a_{i+1}, b_{j+1}]. \end{aligned}$$

Hence for every $i, j \in \mathbb{Z}_3$,

$$[a_i, b_{j+1}] = [a_{i+1}, b_j],$$

and so $S' = \langle [a_1, b_1], [a_1, b_2], [a_1, b_0] \rangle$. But now $[a_1, b_1][a_1, b_2] = [a_1, b_0]$ and so S' has order at most 2^2. Since S' is z-invariant, $|S'| = 2^2$. Now A and B do not commute and so $A \cap S' \leqslant A \cap Z(S) = 1$ and similarly $B \cap S' = 1$ (the intersections could not have order two because they are z-invariant). Therefore $AS'/S' \cong BS'/S' \cong 2 \times 2$ and so $\frac{\langle A, B \rangle}{S'} = (\frac{A}{S'})(\frac{B}{S'}) \cong 2 \times 2 \times 2 \times 2$ and so S has order 2^6. Now suppose $S' < Z(S)$. Since $S \neq Z(S)$ and $Z(S)$ is z-invariant, $Z(S)$ must have order 2^4. However, $Z(S) \cap A = 1$ so $S = Z(S)A$ but this is a contradiction since $S' = [Z(S)A, Z(S)A] = [Z(S), Z(S)][A, Z(S)][A, A][Z(S), A] = 1$ (see Lemma 1.3). $\square$

1.4 Strongly Embedded Subgroups

Definition 1.26. Let $G \geqslant E$ be groups of even order. We say E is a strongly embedded subgroup of G if $E \cap E^g$ has odd order for every $g \in G \backslash E$.

We immediately see that a strongly embedded subgroup is necessarily self-normalizing.

The following arguments originate from Bender (see [3]) and can, in particular, be found in Aschbacher's *Sporadic Groups* [2, Lemma 7.6]. Let G and E be groups of even order with E a strongly embedded subgroup of G. Let $\mathcal{I}$ be the set of involutions in G and let Ω be the set of conjugates of E in G. We consider the action of $\mathcal{I}$ on Ω.

Lemma 1.27. *Each $i \in \mathcal{I}$ fixes precisely one element of Ω.*

Proof. Let $A \in \Omega$ then A is a conjugate of E and so has even order. Therefore there exists some $u \in \mathcal{I} \cap A$ and so $A^u = A$. Suppose $B^u = B$ for some $B \in \Omega \backslash \{A\}$. Since B is strongly embedded, B is self-normalizing and so $u \in B$. Therefore $u \in B \cap A$. However $A \cap B$ has odd and so $u \in \mathcal{I} \cap A$ can fix no other element of Ω. Also, since u is an involution, u must swap pairs in Ω and so Ω has odd order. Now, since Ω has odd order, any involution acts on Ω and fixes at least one element. So suppose $v \in \mathcal{I}$ and $C^v = C$ for some $C \in \Omega$. As we have seen, C is self normalizing and so $v \in \mathcal{I} \cap C$ and then v fixes precisely one element of Ω. □

Lemma 1.28. *Let $E \neq E^u \in \Omega$. Any involution swapping E and E^u lies in the coset $u(E \cap E^u)$.*

Proof. Let w be such an involution. Then $E^w = E^u$ and so $uw \in E$. Also, $(uw)^{-1} = wu = (uw)^u \in E^u$ and so $uw \in E \cap E^u$. Therefore $w \in u(E \cap E^u)$. □

Lemma 1.29. *Let $E \neq E^u \in \Omega$ and set $K = E \cap E^u$. The number of involutions in $\mathcal{I}$ that swap E and E^u is equal to $|J|$ where $J = \{k \in K | k^u = k^{-1}\}$.*

Proof. Any such involution, v say, which swaps E and E^u lies in the coset $u(E \cap E^u) = uK$. So let $v = uk$ for $k \in K$. Then $1 = v^2 = k^u k$ and so $k^u = k^{-1}$ and then $k \in J$ and $v = uk \in uJ$. Of course any element of uJ is an involution and swaps E and E^u. Therefore uJ is the set of all involutions in uK and so $|J| = |uJ|$ is the number of involutions swapping E and E^u. □

Theorem 1.30. *Let G be a group and E a strongly embedded subgroup of G. If for some involution $t \in E$, $C_G(t) = C_E(t)$ intersects trivially with every distinct conjugate of E, then G contains an abelian subgroup K such that $E = KC_G(t)$ and $K \cap C_G(t) = 1$.*

Proof. Set $n = [G : E]$. Count the triples (v, A, B) such that $v \in \mathcal{I}$ and $A, B \in \Omega$ with $A^v = B$. Let $\mathcal{T}$ be the set of such triples. By Lemma 1.27, each involution fixes a unique element of Ω and permutes $\frac{n-1}{2}$ pairs so $|\mathcal{T}| = |\mathcal{I}|\frac{(n-1)}{2} \geqslant [G : C_G(t)]\frac{(n-1)}{2} = [E : C_E(t)]\frac{n(n-1)}{2}$.

Now we choose an involution $u \in \mathcal{I}$ such that $|\mathcal{I} \cap \langle u \rangle (E \cap E^u)|$ is maximal. Equivalently we have chosen two conjugates of E which are permuted by a maximal number of involutions. As before set $K = E \cap E^u$ and $J = \{k \in K | k^u = k^{-1}\}$.

Now $|\mathcal{T}| = \sum_{A,B \in \Omega} M_{AB}$ where M_{AB} is the number of involutions swapping A and B. So $M_{AB} \leqslant M_{E,E^u} = |J|$. Thus $|\mathcal{T}| \leqslant \binom{n}{2} M_{E,E^u} = \frac{n(n-1)}{2}|J|$. So $[E : C_E(t)] \leqslant |J|$. Now $C_G(t) = C_E(t)$ intersects trivially with every distinct conjugate of E and so $C_G(t) \cap K = 1$. Therefore every element of K lies in a unique coset of $C_G(t)$. There are $[E : C_E(t)]$ cosets of $C_E(t)$ in E and so this number is greater than $|\{C_E(t)k | k \in K\}| = |K|$. Hence $|J| \leqslant |K| \leqslant [E : C_G(t)]$. So we have that

$$|J|\frac{n(n-1)}{2} \leqslant |K|\frac{n(n-1)}{2} \leqslant [E : C_G(t)]\frac{n(n-1)}{2} \leqslant |\mathcal{T}| = |\mathcal{I}|\frac{(n-1)}{2} \leqslant \frac{n(n-1)}{2}|J|.$$

Hence $J = K$ and $|\mathcal{I}| = n[E : C_G(t)] = [G : C_G(t)]$. Furthermore, since u inverts every element of $J = K$, K is an abelian subgroup by Lemma 1.20 and from the group orders we get $E = KC_G(t)$. $\square$

1.5 Automorphisms of Abelian Groups

Let A be an additive abelian group that is isomorphic to a direct product of m cyclic groups of order q where $q = p^n$ for some prime p. Consider the ring of endomorphisms of A, $\mathrm{End}(A)$. This is the set of group homomorphisms from A to itself with ring multiplication given by composition of maps and addition given by $(\theta + \varphi)(a) := \theta(a) + \varphi(a)$ for all homomorphisms θ and φ and all $a \in A$. We will identify this endomorphism ring with a ring of matrices and then determine which matrices define automorphisms of A. A reference for this section is [25]. From now on we will view A as a direct sum of m copies of the integers modulo q. So any $a \in A$ has the form $a = (\overline{a_1}, \overline{a_2}, \ldots, \overline{a_m})$ where each $\overline{a_i}$ represents an equivalence class of integers modulo q and a_i an integer representative of the class. Let π be the natural group homomorphism $\pi : \mathbb{Z}^m \to A$ given by $\pi(a_1, a_2, \ldots, a_m) \mapsto (\overline{a_1}, \overline{a_2}, \ldots, \overline{a_m})$. Consider the map

$$\begin{array}{rcccl} \psi_q & : & M_m(\mathbb{Z}) & \longrightarrow & \mathrm{End}(A) = \mathrm{End}(\mathbb{Z}_q^m) \\ & & M & \mapsto & \psi_q(M), \end{array}$$

where $\psi_q(M) : (\overline{a_1}, \overline{a_2}, \ldots, \overline{a_m}) \mapsto \pi((a_1, a_2, \ldots, a_m)M)$.

Lemma 1.31. *The map ψ_q is a surjective ring homomorphism.*

Proof. We first show each $\psi_q(M)$ is a well defined endomorphism of A. Suppose $(a_1 \ldots, a_m)$ and $(b_1, \ldots, b_m)$ satisfy $\pi(a_1 \ldots, a_m) = \pi(b_1, \ldots, b_m)$. Then $q | a_i - b_i$ for each $1 \leqslant i \leqslant m$.

Thus

$$\begin{aligned}
\psi_q(M)(\overline{a_1}\ldots,\overline{a_m}) - \psi_q(M)(\overline{b_1}\ldots,\overline{b_m}) &= \pi((a_1\ldots,a_m)M) - \pi((b_1,\ldots,b_m)M) \\
&= \pi(\Sigma a_i m_{i1},\ldots,\Sigma a_i m_{im}) - \pi(\Sigma b_i m_{i1},\ldots,\Sigma b_i m_{im}) \\
&= \pi(\Sigma(a_i-b_i)m_{i1},\ldots,\Sigma(a_i-b_i)m_{im}) \\
&= 0_A.
\end{aligned}$$

So $\psi_q(M)$ is well defined and also clearly a group homomorphism of A as π is linear and matrix multiplication is distributive. So ψ_q is a map into $\mathrm{End}(A)$ and it remains to prove ψ_q is a surjective homomorphism. Again it is clear that ψ_q is a ring homomorphism as π is linear and matrix multiplication is distributive and associative. Now any endomorphism of A is determined by where it maps each $w_i := (0,\ldots,\overline{1},\ldots 0)$, the vector whose only non-zero entry is a $\overline{1}$ in the i'th position. So suppose $\theta \in \mathrm{End}(A)$ and $\theta(w_i) = (\overline{a_1},\ldots,\overline{a_m})$. Then consider a matrix $M = (m_{ij})$ where $m_{ij} = a_j$ for each $j \leqslant m$. Do this for each $i \leqslant m$ and it follows that $\theta = \psi_q(M)$. Thus ψ_q is a surjective ring homomorphism. □

Lemma 1.32. *The kernel of ψ_q is the set $K := \{M = (m_{ij}) \in M_n(\mathbb{Z}) |\ q|m_{ij}\ \forall i,j\}$.*

Proof. It is clear that for all $k \in K$ and each $w_i := (0,\ldots,1,\ldots 0)$ defined as before, $\psi_q(k)(w_i) = 0_A$. Since A is generated by the w_i's, $K \subseteq \mathrm{Ker}(\psi_q)$. However if we suppose that some matrix, $M = (M_{ij})$, is in the kernel then $\psi_q(M)(w_i) = 0_A$. Therefore q divides m_{ij} for each j. We do this for each i to see that q divides each entry in M and so $M \in K$.□

Lemma 1.33. *$\theta = \psi_q(M) \in \mathrm{End}(A)$ is an automorphism of A if and only if $\det(M)$ is prime to p.*

Proof. Suppose $M \in M_m(\mathbb{Z})$ has determinant prime to p. Consider the cofactor matrix, N, of M. This is the matrix which satisfies $MN^t = \det(M)I$. Since M has integer entries, so does N. Since $\det(M)$ is prime to p, we can find $s \in \mathbb{Z}$ such that $s\det(M) \equiv 1 \bmod q$. Set $\psi_M^{-1} := \psi(sN)$ and we see that $\psi_M \circ \psi_{sN^t} = \psi_{sMN^t} = \psi_{s\det(M)I} = 1_{\mathrm{End}(A)}$ and so ψ_M is invertible.

Conversely suppose $M \in M_m(\mathbb{Z})$ with ψ_M an invertible endomorphism of A. Suppose ${\psi_M}^{-1} = \psi_N$ for some $N \in M_m(\mathbb{Z})$. Then

$$\psi(MN - I) = \psi(MN) - \psi(I) = \psi_M \psi_N - 1_{\mathrm{End}(A)} = 0_{\mathrm{End}(A)}.$$

Thus $MN - I \in \mathrm{Ker}(\psi)$ and so q divides every entry of $MN - I$ and so the entries of MN are equal to the entries of I modulo p. Thus

$$1 \equiv \det(MN) \equiv \det(M)\det(N) \bmod p.$$

Hence $\det(M)$ is prime to p. □

Lemma 1.34. *Set* $\mathrm{GL}_m(\mathbb{Z}_q)$ *to be the subset of* $M_m(\mathbb{Z}_q)$ *containing matrices with determinant prime to* p*. Then* $\mathrm{GL}_m(\mathbb{Z}_q) \cong \mathrm{Aut}(A)$ *and has order* $p^{(n-1)m^2}|\mathrm{GL}_m(p)|$.

Proof. The set $\mathrm{GL}_m(\mathbb{Z}_q)$ is a group under matrix multiplication. Consider the map,

$$\Psi \quad : \quad \mathrm{GL}_m(\mathbb{Z}_q) \quad \longrightarrow \quad \mathrm{Aut}(A),$$

where each $(\overline{a_{ij}}) \in \mathrm{GL}_m(\mathbb{Z}_q)$ $\Psi_q((a_{ij}))$. This map is a well defined homomorphism as Ψ_q is and non-zero since for each such $(\overline{a_{ij}})$, the matrix (a_{ij}) is not in $\mathrm{Ker}(\Psi_q)$. It is also injective since if $(\overline{a_{ij}}), (\overline{b_{ij}}) \in \mathrm{GL}_m(\mathbb{Z}_q)$ with $\Psi_q((a_{ij})) = \Psi_q((b_{ij}))$ then $a_{ij} - b_{ij} \in \mathrm{Ker}(\Psi_q)$ and then $q|(a_{ij} - b_{ij})$ for each i, j and so $(\overline{a_{ij}}) = (\overline{b_{ij}})$. Now, for any automorphism of A we can find $M = (m_{ij}) \in M_n(\mathbb{Z})$ such that M has determinant prime to p. Therefore $(\overline{m_{ij}}) \in \mathrm{GL}_m(\mathbb{Z}_q)$ and so Ψ is surjective.

Consider the map $\Theta : \mathrm{GL}_m(\mathbb{Z}_q) \to \mathrm{GL}_m(\mathbb{Z}_p)$ where for each $M \in \mathrm{GL}_m(\mathbb{Z}_q)$ we restrict the matrix entries modulo p. Then $\Theta(M)$ has non-zero determinant modulo p and so is an element of $\mathrm{GL}_m(p)$. Clearly Θ is a surjective group homomorphism. The kernel is the set of matrices $\{(m_{ij})|m_{ii} \equiv 1 \bmod p\ \forall i \text{ and } m_{ij} \equiv 0 \bmod p\ \forall i \neq j\}$. So there are p^{n-1}

choices for each entry and so $p^{(n-1)m^2}$ elements in the kernel. Thus $\mathrm{GL}_m(\mathbb{Z}_q) \cong \mathrm{Aut}(A)$ has order $p^{(n-1)m^2}|\mathrm{GL}_m(p)|$. $\square$

We have seen that if $A = \mathbb{Z}_q^m$ then elements of $\mathrm{Aut}(A)$ can be viewed as m by m matrices with elements in $\mathbb{Z}_q$ which have determinant prime to p. Notice $\mathrm{GL}_m(\mathbb{Z}_q)$ acts on the vector space $V := A/\Omega_{n-1}(A) \cong \mathbb{Z}_p^m$ and so there is an homomorphism $\mathrm{GL}_m(\mathbb{Z}_q) \to \mathrm{GL}_m(\mathbb{Z}_p) = \mathrm{Aut}(\mathbb{Z}_p^m)$. Moreover this homomorphism simply restricts matrix entries modulo p.

Lemma 1.35. *Let p be a prime and set $q = p^n$. Let G be a group acting on an abelian group $A \cong \mathbb{Z}_q^m$. Then there are homomorphisms*

$$\begin{aligned} \alpha &: G \longrightarrow \mathrm{GL}_m(\mathbb{Z}_q), \\ \beta &: G \longrightarrow \mathrm{GL}_m(\mathbb{Z}_p) \end{aligned}$$

for which entries of $\alpha(g)$ are congruent modulo p to entries of $\beta(g)$ for each $g \in G$. Furthermore β is a representation affording the module $A/\Omega_{n-1}(A)$ and if $\beta_1 : G \to \mathrm{GL}_m(\mathbb{Z}_p)$ is an equivalent representation then there is a homomorphism $\alpha_1 : G \to \mathrm{GL}_m(\mathbb{Z}_q)$ for which entries of $\alpha_1(g)$ are congruent modulo p to entries of $\beta_1(g)$ for each $g \in G$.

Proof. Since G acts on A, there is a homomorphism, α, from G to $\mathrm{Aut}(A) \cong \mathrm{GL}_m(\mathbb{Z}_q)$ as described previously. Moreover we have seen that restricting matrix entries modulo p describes the action of G on the quotient group $A/\Omega_{n-1}(A) \cong \mathbb{Z}_p^m$ and so we have the required representation β. So suppose $\beta_1 : G \to \mathrm{GL}_m(\mathbb{Z}_p)$ is an equivalent representation then there is a matrix $M \in \mathrm{GL}_m(\mathbb{Z}_p)$ such that for each $g \in G$, $\beta_1(g) = M^{-1}\beta(g)M$. Since M is a matrix whose elements are integers modulo p and whose determinant is not a multiple of p, we can view M as a matrix in $\mathrm{GL}_m(\mathbb{Z}_q)$ simply by viewing each integer modulo p as the same integer modulo q. Now it makes sense to consider the homomorphism $\alpha_1 : G \to \mathrm{GL}_m(\mathbb{Z}_q)$ where $\alpha_1(g) = M^{-1}\alpha(g)M$ and so entries of α_1 are congruent modulo p to entries of $\beta_1(g)$ as required. $\square$

Chapter 2

Some Representation Theory

In this chapter we discuss endomorphism rings, tensor products, some modular representation theory and natural modules. The results on natural $\mathrm{GL}_2(3)$ and $\mathrm{SL}_2(3)$-modules will be used throughout Chapters 5, 6 and 7. The natural $\mathrm{SL}_2(2^n)$-modules will appear again in Chapter 8 as will much of the work on tensor products and modular character theory.

Theorem 2.1. *(Maschke) Let G be a group and let F be a field whose characteristic does not divide $|G|$. Then every FG-module is completely reducible.*

Proof. See [19, 1.9 p4]. □

Lemma 2.2. *Let p be a prime and let $K = \mathrm{GF}(p^n)$. If H is a group with $H \cong K^\times$ then any irreducible KH-module has dimension one.*

Proof. Suppose V is an irreducible KH-module with representation $\rho : H \to GL(V)$. Let $\langle h \rangle = H$ then h has order $p^n - 1$ and so any eigenvalue for $\rho(h)$ is a $p^n - 1$'th root of unity and so will lie in K. Thus we can find a corresponding eigenvector for $\rho(h)$. The eigenspace spanned by the eigenvector is 1-dimensional and H invariant and therefore a KH-submodule and so V must have dimension one. □

2.1 Endomorphism Rings

Definition 2.3. Let G be a group, F a field and let V and W be FG-modules. Define $\mathrm{Hom}_{FG}(V, W)$ to be the ring of all FG-homomorphisms from V to W. The endomorphism ring of V is the ring $\mathrm{End}_{FG}(V) := \mathrm{Hom}_{FG}(V, V)$.

If V is an FG-module and $E := \mathrm{End}_{FG}(V)$ then V can be viewed as a vector space over E by defining scalar multiplication as $e \cdot v := e(v)$ for $e \in E, v \in V$. Thus V is also an EG-module.

Lemma 2.4. *(Schur) If V is an irreducible FG-module then $\mathrm{End}_{FG}(V)$ is a division ring. If, furthermore, F is a finite field then $\mathrm{End}_{FG}(V)$ is a field.*

Proof. Let $0 \neq \phi \in \mathrm{End}_{FG}(V)$. Set $W = \phi(V)$. Since ϕ is non-zero, $W \neq \{0\}$. Hence for all $v \in V$ and $g \in G$

$$(\phi(v))g = \phi(vg) \in W$$

and so W is an FG-submodule. Since V is irreducible and $W \neq \{0\}$, $V = W$. So ϕ is onto and by the rank-nullity result ϕ is a non-singular linear transform on V and thus invertible. Clearly ϕ^{-1} is a linear transform and $vg = \phi(\phi^{-1}(v))g = \phi(\phi^{-1}(v)g)$ and so $\phi^{-1}(vg) = \phi^{-1}(v)g$ and $\phi^{-1} \in \mathrm{End}_{FG}(V)$. A quick check verifies $\mathrm{End}_{FG}(V)$ is a ring with usual addition and composition of functions and so it is a division ring. Now Wedderburn's Theorem says that a finite division ring is a field. So if F is a finite field then $\mathrm{Hom}_{FG}(V, V)$ is finite and hence a field. □

Lemma 2.5. *If V is a faithful irreducible FG-module where F is a finite field and G an abelian group then $\mathrm{End}_{FG}(V)$ is a field of order $|V|$.*

Proof. By Schur's Lemma, $E := \mathrm{End}_{FG}(V)$ is a field. Since elements of F define endomorphisms of V which commute with the action of G, we see an embedding of F in E.

Also, as G is abelian, G embeds in the multiplicative group of E. We can view E as an FG-module by defining scalar multiplication and an action of G simply by composition of maps. We then define an FG-module homomorphism,

$$\begin{array}{rcl} \Phi : E & \longrightarrow & V \\ \alpha & \longmapsto & \alpha(v), \end{array}$$

where v is some fixed non-zero vector in V. This map is non-zero and so the kernel is an ideal and so must be trivial. It follows that this map is a bijection and so $|E| = |V|$. □

Lemma 2.6. *Let G be a group and $H \leqslant G$. Let F be a finite field of characteristic p and let V be an irreducible FG-module. Suppose $\chi : G \to \mathbb{C}$ is the character afforded by V and finally suppose that p does not divide $|H|$. Then* $\dim(C_V(H)) = \langle \chi_{|_H}, 1_{|_H} \rangle$.

Proof. By Maschke's Theorem, V decomposes into irreducible H-modules, $V = V_1 \oplus \ldots \oplus V_n$, and $\chi_{|_H}$ decomposes into irreducible characters for H, $\chi_{|_H} = \chi_1 + \ldots + \chi_n$. The inner product in H, $\langle \chi_{|_H}, 1_{|_H} \rangle$ gives us the number of times the trivial character appears in the decomposition and similarly the number of 1-dimensional modules on which H acts trivially. Hence $\dim(C_V(H)) = \langle \chi_{|_H}, 1_{|_H} \rangle$. □

2.2 Tensor Products

See, for example, [1] for more explanation and proofs of results. Let G be a group, K a field and F an extension field of K.

Definition 2.7. Let U and V be KG-modules. A K-balanced map $\theta : U \times V \to A$, where A is an abelian group, is a map which satisfies

$$k\theta_T(u, v) = \theta_T(ku, v) = \theta_T(u, kv),$$

$$\theta(u+u',v)=\theta(u,v)+\theta(u',v)$$

and

$$\theta(u,v+v')=\theta(u,v)+\theta(u,v')$$

for $k \in K$, $u, u' \in U$, $v, v' \in V$. An abelian group T is a tensor product of U and V over K if there is a surjective K-balanced map $\theta_T : U \times V \to T$ such that if S is an abelian group and $\theta_S : U \times V \to S$ is a surjective K-balanced map then there is a unique K-linear homomorphism $\alpha : T \to S$ such that $\alpha\theta_T = \theta_S$.

We denote a tensor product of U and V by $U \otimes_K V$ (or $U \otimes V$ if there is no ambiguity for the field). The tensor product exists and is unique up to isomorphism and is a KG-module when we define

$$(u \otimes v) \cdot g := u \cdot g \otimes v \cdot g$$

for $u \in U, v \in V, g \in G$.

Suppose $\{u_i | 1 \leqslant i \leqslant n\}$ is a basis for U over K and $\{v_j | 1 \leqslant j \leqslant m\}$ is a basis for V over K. Then $U \otimes_K V$ is a vector space over K with basis $\{u_i \otimes_K v_j | 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m\}$. Now consider the field extension F/K. Since F is a vector space over K, we can form the tensor product $F \otimes_K V$. This gives a vector space over F when we define $f_1 \cdot (f \otimes v) := (f_1 f \otimes v)$. Notice that $\{1_F \otimes v_i | 1 \leqslant i \leqslant n\}$ is an F-basis for $F \otimes V$ and so the dimension of this space over F is equal to the dimension of V over K.

An irreducible KG-module, V, is called *absolutely irreducible* if the FG-module $F \otimes_K V$ is irreducible for each extension field F of K.

Lemma 2.8. *Let V be an irreducible KG-module. Then V is absolutely irreducible if and only if* $\mathrm{End}_{KG}(V) \cong K$.

Proof. See [1, 25.8]. □

Lemma 2.9. *Let U and V be KG-modules. Then the FG-modules $(U \otimes_K F) \otimes_F (V \otimes_K F)$ and $(U \otimes_K V) \otimes_K F$ are FG-module isomorphic.*

Proof. Consider the map

$$\begin{aligned} \Theta \ : \ (U \otimes_K F) \times (V \otimes_K F) &\longrightarrow (U \otimes_K V) \otimes_K F \\ (u \otimes f, v \otimes e) &\longmapsto (u \otimes v) \otimes fe. \end{aligned}$$

We claim Θ is an F-balanced map. Let $f, f_1, f_2, e \in F$, $u, u_1, u_2 \in U$, $v \in V$ and observe

$$\begin{aligned} \Theta(u_1 + u_2 \otimes f, v \otimes e) &= (u_1 + u_2 \otimes v) \otimes fe \\ &= (u_1 \otimes v) \otimes fe + (u_2 \otimes v) \otimes fe \\ &= \Theta(u_1 \otimes f, v \otimes e) + \Theta(u_2 \otimes f, v \otimes e) \end{aligned}$$

$$\begin{aligned} \Theta(u \otimes f_1 + f_2, v \otimes e) &= (u \otimes v) \otimes f_1 e + f_2 e \\ &= (u \otimes v) \otimes f_1 e + (u \otimes v) \otimes f_2 e \\ &= \Theta(u \otimes f_1, v \otimes e) + \Theta(u \otimes f_2, v \otimes e) \end{aligned}$$

and linearity in the second variable holds in the same way. Also

$$\begin{aligned} f_1\Theta(u \otimes f v \otimes e) = (u \otimes v) \otimes f_1 f e &= \Theta(u \otimes f_1 f, v \otimes e) &= \Theta(u \otimes f, v \otimes f_1 e) \\ &= \Theta(f_1(u \otimes f), v \otimes e) &= \Theta(u \otimes f, f_1(v \otimes e)). \end{aligned}$$

So Θ is an F-balanced map. Also if $g \in G$ then

$$\Theta(u \otimes f, v \otimes e)g = (u \otimes v)g \otimes fe = (ug \otimes vg) \otimes fe = \Theta((u \otimes f)g, (v \otimes e)g) = \Theta((u \otimes f, v \otimes e)g).$$

Now, by the definition of the tensor product, there is an F-linear map $\alpha : (U \otimes_K F) \otimes_F (V \otimes_K F) \to (U \otimes_K V) \otimes_K F$ such that $\alpha\theta_T = \Theta$ where θ_T is the usual tensor product map $\theta_T : (U \otimes_K F) \times (V \otimes_K F) \to (U \otimes_K F) \otimes_F (V \otimes_K F)$. It is easy to check θ_T

commutes with the action of G and so we get that α is FG-linear. Since θ_T is surjective by definition and Θ is also clearly surjective, α is surjective. Finally since the dimension of $(U \otimes_K F) \otimes F(V \otimes_K F)$ over F equals the dimension of $(U \otimes_K V) \otimes_K F$ over F, α is an FG-isomorphism. □

Given a KG-module, V, and corresponding representation, $\rho : G \to \mathrm{GL}(V)$, we can define a representation $\rho^F : G \to \mathrm{GL}(F \otimes_K V)$ where for $g \in G$, $\rho^F : g \mapsto 1 \otimes \rho(g)$ and for $f \otimes v \in F \otimes_K V$, $1 \otimes \rho(g) : f \otimes v \mapsto f \otimes \rho(g)(v)$.

Lemma 2.10. *Let F be an extension field of K and suppose $\theta : G \to \mathrm{GL}_n(K)$ is a representation with corresponding module V. Let ι be the inclusion map $\iota : \mathrm{GL}_n(K) \to \mathrm{GL}_n(F)$. Then the representation $\theta^F : G \to \mathrm{GL}_n(F)$ corresponding to the module $F \otimes_K V$ is equivalent to the representation $\iota\theta$.*

Proof. Fix a K-basis $\{v_1, \ldots, v_n\}$ for V and write each $g \in G$ as a matrix $\theta(g) = (a_{ij})$ where $\theta(g)(v_i) := a_{i1}v_1 + \ldots + a_{in}v_n$ and each a_{ij} is in $K \leqslant F$. The module $F \otimes_K V$ affords the representation $\theta^F : G \to \mathrm{GL}(F \otimes_K V)$ where $g \in G$ maps to the linear transformation $1 \otimes \theta(g) : f \otimes v \mapsto f \otimes \theta(g)(v)$. Choose a basis for $F \otimes_K V$ to be $\{1 \otimes v_1, \ldots, 1 \otimes v_n\}$. Then, with respect to this basis, the matrices representing G via $\theta^F : G \to \mathrm{GL}(F \otimes_K V)$ are exactly the matrices representing G via θ since $\theta^F(g)(1 \otimes v_i) = 1 \otimes \theta(g)(v_i) = 1 \otimes a_{i1}v_1 + \ldots + a_{in}v_n = 1 \otimes a_{i1}v_1 + \ldots + 1 \otimes a_{in}v_n$. □

If V is a vector space over a field F and $\phi_1, \ldots, \phi_n$ are F-linear transformations of V, we say $\phi_1, \ldots, \phi_n$ are simultaneously diagonalizable if there is a basis for V, $\{v_1, \ldots, v_m\}$, such that for each $1 \leqslant i \leqslant n$ and each $1 \leqslant j \leqslant m$, v_j is an eigenvector for ϕ_i.

Lemma 2.11. *Let V be a vector space over a finite field $K = \mathrm{GF}(p)$ and let $\phi_1, \ldots, \phi_n$ be commuting K-linear transformations of V with order prime to p. Furthermore let F be a field extension of K that contains all eigenvalues for $\phi_1, \ldots, \phi_n$. Then the linear transformations of $F \otimes_K V$, $1 \otimes_K \phi_1, 1 \otimes_K \ldots, 1 \otimes_K \phi_n$, can be simultaneously diagonalized.*

Proof. Each ϕ_i has order, r_i say, prime to p and so has eigenvalues which are all r_i'th roots of unity and so there exists some extension field, $F \geqslant K$, which contains every eigenvalue for every ϕ_i. Let $V^F = F \otimes_K V$ and let $\phi_i^F := 1 \otimes_K \phi_i : f \otimes v \mapsto f \otimes \phi_i(v)$ be the corresponding linear transformations. Notice that the linear transformations, $\phi_1^F, \ldots, \phi_n^F$, all commute. Find the eigenspaces for some $\phi := \phi_i^F$. Let $\varepsilon_1, \ldots, \varepsilon_m \in F$ be the eigenvalues for ϕ and $\mathrm{Eig}(\varepsilon_1), \ldots, \mathrm{Eig}(\varepsilon_m)$ the corresponding eigenspaces in V^F. Suppose $1 \leqslant k \leqslant m$ and $v \in \mathrm{Eig}(\varepsilon_k)$, then, $\phi\phi_j^F(v) = \phi_j^F\phi(v) = \phi_j^F(\varepsilon v) = \varepsilon\phi_j^F(v)$. So each ϕ_j^F preserves each eigenspace for ϕ. Now ϕ is diagonalizable with respect to a basis of eigenvectors. We now show we can choose a basis for V^F with respect to which every ϕ_j^F is diagonalizable. If we can find a basis for each eigenspace with respect to which each ϕ_j^F is diagonalizable then we are done. So we proceed by induction on the dimension of the eigenspace. If $\mathrm{Eig}(\varepsilon_k)$ has dimension one then, as it is preserved by each ϕ_j^F, each ϕ_j^F is scalar. So suppose $\mathrm{Eig}(\varepsilon_k)$ has dimension $n+1$ and that each ϕ_j^F is diagonalizable on any eigenspace of lesser dimension. Suppose some ϕ_j^F is not diagonalizable on $\mathrm{Eig}(\varepsilon_k)$. Then the vector space $\mathrm{Eig}(\varepsilon_k)$ decomposes into eigenspaces for ϕ_j^F each of which is preserved by each linear transformation, $\phi_1^F, \ldots, \phi_n^F$ and by induction there is a basis for each for which each $\phi_1^F, \ldots, \phi_n^F$ is diagonalizable. However this gives us a basis for $\mathrm{Eig}(\varepsilon_k)$ on which ϕ_j is diagonalizable contrary to assumption. $\square$

In the following corollary K is a field extension of L and is therefore a vector space over L. We use the notation $\mathrm{GL}(L, K)$ for the group of invertible L-linear transformations of K.

Corollary 2.12. *Let p be a prime and let $L = \mathrm{GF}(p)$ and $K = \mathrm{GF}(p^n)$ for some $n \geqslant 1$. Each $k \in K^\times$ defines a linear transformation of K as a vector space over L and there is an embedding $\phi : K^\times \hookrightarrow \mathrm{GL}_n(L) \hookrightarrow \mathrm{GL}_n(K)$. Furthermore there exists $M \in \mathrm{GL}_n(K)$ such that $\phi(k)^M = \mathrm{diag}(k)$ for all $k \in K^\times$.*

Proof. It is clear that K is an n-dimensional vector space over L and each non-zero, $k \in K$, defines a linear transformation, $\lambda_k : a \mapsto ka$ (for each $a \in K$). Thus there is an embedding $\theta : K^\times \hookrightarrow \mathrm{GL}_n(L) \cong \mathrm{GL}(L, K)$ and since $L \leqslant K$, we see the inclusion map $\iota : \mathrm{GL}_n(L) \to \mathrm{GL}_n(K)$ thus $\phi := \iota\theta : K^\times \hookrightarrow \mathrm{GL}_n(K)$. Now, the linear transformations $\{\lambda_k | k \in K^\times\}$ commute pairwise and are all scalar on K so by Lemma 2.11, the corresponding linear transformations of $K \otimes_L K$ (as an n-dimensional vector space over K), $\{1 \otimes_L \lambda_k | k \in K^\times\}$ are simultaneously diagonalizable. Therefore we can assume there is an image of $K^\times$ in $\mathrm{GL}(K, K \otimes_L K)$, via θ^K say, in which $\theta^K(k)$ is scalar for each $k \in K^\times$. Finally, by Lemma 2.10, the representation ϕ is equivalent to θ^K. Therefore, there exists $M \in GL_n(K) \cong \mathrm{GL}(K, K \otimes_L K)$ such that $\phi(k)^M = \mathrm{diag}(k)$ for each $k \in K^\times$. □

2.3 Natural $\mathbf{GL_2(3)}$-Modules

In later chapters we will consider amalgams. These will be subgroups inside a larger group and the structure of the subgroups will be described via $\mathrm{GL}_2(3)$ and $\mathrm{SL}_2(3)$-modules. In the following section set $G \cong \mathrm{GL}_2(3)$, $G > H \cong \mathrm{SL}_2(3)$ and $F = \mathrm{GF}(3)$.

Lemma 2.13. *The following are true in $G \cong \mathrm{GL}_2(3)$.*

(i) Any subgroup of G isomorphic to 2×2 is conjugate to the subgroup of diagonal matrices.

(ii) $Q_8 \cong O_2(G) \leqslant H$.

(iii) $H \cong \mathrm{SL}_2(3)$ is the unique subgroup of G at index two.

Proof. Let $2 \times 2 \cong T \leqslant G$. Consider the eigenvalues for each $t \in T^\#$. Each $t \in T$ satisfies the polynomial $X^2 = 1$ and so the possible eigenvalues are 1 and -1. If t has only the eigenvalue 1 then t is the identity. If t has only the eigenvalue -1 then t must be the central scalar matrix $\mathrm{diag}(-1, -1)$. If t has eigenvalues 1 and -1 then t is conjugate to the matrix diag$(-1,1)$. If T contains the central involution then we are done since we only need to diagonalize one more element of T. So suppose not then we must have $t \in T$ with eigenvalues 1 and -1. Let u and v be eigenvectors for t such that $t(u) = u$ and $t(v) = -v$. Let $s \in T \backslash \langle t \rangle$ then $s(u) = s(t(u)) = t(s(u))$ so $s(u)$ is in the eigenspace $\langle u \rangle$ similarly $s(v)$ is in the eigenspace $\langle v \rangle$ and it follows that s must be diagonal with respect to the basis $\{u, v\}$ and so we can simultaneously diagonalize T. Therefore (i) holds.

Notice that

$$K := \langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \rangle$$

is a normal subgroup of G isomorphic to Q_8 and that this subgroup is contained in H. Furthermore G cannot have a larger normal 2-subgroup since we can find two distinct Sylow 2-subgroups of order 2^4 by including the element $\begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$ or $\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$ so (ii) holds.

Now, H is a normal subgroup of G at index two so suppose K is another subgroup of G at index two. Then $H \cap K \trianglelefteq G$ has at index four in G and has order 32^2. If $H \cap K$ contains a normal Sylow 3-subgroup, S say, then S char $H \cap K \trianglelefteq G$ implies $S \trianglelefteq G$ which is a contradiction since G does not have a normal Sylow 3-subgroup. In fact G contains four Sylow 3-subgroups namely,

$$\left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle$$

which pairwise intersect trivially. Each is normalized in G by a group of order 32^2 and so by Sylow's Theorem, G has exactly four Sylow 3-subgroups. Also, by Sylow's Theorem, $H \cap K$ contains four Sylow 3-subgroups and so $H \cap K$ contains 104 elements of order three. Therefore $H \cap K$ can contain only three elements of order two and so necessarily has a normal subgroup of order four, F say. However, H contains a Sylow 2-subgroup which is quaternion of order eight and so F must be cyclic of order four and therefore admits no automorphism of order three. This implies that $C_{H\cap K}(F) = N_{H\cap K}(F) = H \cap K$ and so F commutes with each Sylow 3-subgroup but then each Sylow 3-subgroup in $H \cap K$ is normal in $H \cap K$ which is a contradiction. $\square$

Definition 2.14. Let V be a 2-dimensional vector space over GF(3). We identify G with $\mathrm{GL}(V)$ and H with $\mathrm{SL}(V)$ and call V the natural G-module and natural H-module respectively.

Lemma 2.15. *Let V be a natural G-module or a natural H-module. The following hold.*

(*i*) *For $S \in \mathrm{Syl}_3(G)$, $C_V(S)$ is a subspace of V of dimension one.*

(*ii*) *Both G and H act transitively on the subspaces of V of dimension one.*

(*iii*) *Both G and H act transitively on the non-zero vectors in V.*

(*iv*) *The action of G (and H) on V is faithful.*

Proof. (*i*) Let $S \in \mathrm{Syl}_3(G)$ then S is conjugate to the group of strictly lower triangular matrices. It is easy to check that this group of matrices fix precisely the 1-space $\langle(1, 0)\rangle$. Thus $C_V(S)$ has dimension one.

(*ii*) There are four subspaces of V with dimension one. The stabilizer in G of the space $\langle(1, 0)\rangle$ is the subgroup of lower triangular matrices which has index four in G. Similarly the stabilizer in H of $\langle(1, 0)\rangle$ is the subgroup of lower triangular matrices with determinant 1 which has index four in H. Therefore both G and H are transitive on the 1-spaces in V.

(*iii*) We repeat the same arguments to see that the stabilizer in G (and in H) of a non-zero vector in V has index eight. Therefore both G and H are transitive on the eight non-zero vectors in V.

(*iv*) This is just by definition since we identified $\mathrm{GL}_2(3)$ with the group of automorphisms $\mathrm{GL}(V)$. $\square$

The following lemma describes a situation which will occur many times when we are dealing with groups involving natural modules.

Lemma 2.16. *Suppose S is a 3-group with subgroups $P \neq Q \leqslant S$ of index three. Suppose further that t is an involution in $\mathrm{Aut}(S)$ which leaves P and Q invariant. Then t acts on S/P (and S/Q) and either centralizes or inverts S/P. If t centralizes S/P then there exists $x \in Q\backslash P$ such that t centralizes x. If t inverts S/P then there exists $x \in Q\backslash P$ such that t inverts x.*

Proof. It is clear that t acts on S/P such that for any element $Py \in S/P$, $Py^t := P(y^t)$. Pick $y \in Q\backslash P$ then the coset Py is either inverted or centralized by t. Suppose first that Py is centralized by t then t describes a permutation of the set Py. Furthermore elements $py \in Py$ are in Q if and only if $p \in Q \cap P$ and t preserves Q so preserves those elements. Since t is an involution and $Py \cap Q$ is a set of odd order, $|P \cap Q|$, t must fix some element, x say. Thus x is in $Q\backslash P$ and is centralized by t. Now suppose that Py is inverted by t then $[y,t] \notin P$. Also $[y,t]^t = (y^{-1}y^t)^t = (y^{-1})^t y = [y,t]^{-1}$ and so $[y,t]$ is inverted by t. Thus $[y,t] \in Q\backslash P$ and is inverted by t. □

2.4 Sym(4)-Modules

Lemma 2.17. *Suppose that $X \cong \mathrm{Sym}(4)$ and that V is a faithful 3-dimensional $\mathrm{GF}(3)X$-module. Let $\{q_1, q_2, q_3\} = O_2(X)^{\#}$. The following hold.*

(i) There is a set of distinct 1-dimensional subspaces $\mathcal{B} := \{\langle v_1\rangle, \langle v_2\rangle, \langle v_3\rangle\}$ where $\langle v_i\rangle = C_V(q_i)$.

(ii) X has orbits of lengths 3, 4 and 6 on the 1-dimensional subspaces of V with representatives

Type 1A - $\langle v_1\rangle$,

Type 1B - $\langle v_1 + v_2 + v_3 \rangle$ *and*

Type 1C - $\langle v_1 + v_2 \rangle$

respectively.

(iii) *X has orbits of lengths* 3, 4, *and* 6 *on the* 2*-dimensional subspaces of* V *with representatives*

Type 2A - $\langle v_1, v_2 \rangle$,

Type 2B - $\langle v_1 + v_2, v_2 + v_3 \rangle$ *and*

Type 2C - $\langle v_1, v_1 + v_2 + v_3 \rangle$

respectively.

(iv) *If* $x \in X$ *has order three then the subspace* $C_V(x)$ *has dimension one and lies in the orbit of* 1*-spaces with representative* $\langle v_1 + v_2 + v_3 \rangle$.

(v) *For* $i \neq j$, v_i *is negated by* q_j. *For* $\{i, j, k\} = \{1, 2, 3\}$, q_k *negates* $v_i + v_j$.

(vi) $|C_X(v_i)| = 4$, $|C_X(v_i + v_j)| = 2$ *for* $i \neq j$.

(vii) *If* $x \in X \backslash O_2(X)$ *has order two then* x *centralizes a* 1*-space of type* $1C$.

Proof. Set $Q = O_2(X)$ then $Q^{\#} = \{q_1, q_2, q_3\}$. By coprime action of Q on V,

$$V = \langle C_V(q_i) | i = 1, 2, 3 \rangle.$$

Each $C_V(q_i)$ is a non-trivial subspace of V and as X acts transitively on $Q^{\#}$, X acts transitively on the three subspaces $C_V(q_1)$, $C_V(q_2)$ and $C_V(q_3)$. Thus each has the same dimension. Since X acts faithfully on V, each subspace is proper. Suppose each $C_V(q_i)$ has dimension two. Consider $C_V(q_1) \cap C_V(q_2)$. This must be non-trivial. Moreover any vector fixed by q_1 and q_2 must be fixed by Q and so this intersection is X-invariant. However this is a contradiction since X cannot act faithfully on a 1-dimensional subspace. Choose vectors v_i such that $\langle v_i \rangle = C_V(q_i)$ then

$$V = \langle v_1 \rangle \oplus \langle v_2 \rangle \oplus \langle v_3 \rangle.$$

Clearly $\{\langle v_i \rangle \mid 1 \leqslant i \leqslant 3\}$ forms an orbit of length 3 on the 1-dimensional subspaces of V. We also have that the subspaces $\langle v_1 \pm v_2 \pm v_3 \rangle$ form an orbit of length 4 on V and the subspaces $\langle v_i \pm v_j \rangle$, where $i \neq j$ form an orbit of length 6.

Clearly the subspaces $\langle v_i, v_j \rangle$ for $i \neq j$ give an orbit of length 3 on the 2-dimensional subspaces of V. The subspaces $\langle v_i \pm v_j, v_j \pm v_k \rangle$ form an orbit of length 4. Finally the subspaces $\langle v_i, v_i + v_j - v_k \rangle$, for i j and k distinct form an orbit of length 6. We note that for each choice of i we have two choices for k.

We see that any element of order three cycles the set $Q^{\#}$ and so cycles the spaces $\langle v_1 \rangle, \langle v_2 \rangle, \langle v_3 \rangle$. But if $x \in X$ cycles $\langle v_1 \rangle, \langle v_2 \rangle, \langle v_3 \rangle$, it must also cycle the spaces of type $\langle v_1 + v_2 \rangle$ of which there are six. Since spaces of type $\langle v_1 + v_2 + v_3 \rangle$ lie in an orbit of length four, x necessarily fixes at least one of them. However if it fixes them all it acts trivially on V which is impossible.

The space $\langle v_i \rangle$ is preserved by $N_X(q_i)$. So for $j \neq i$, q_j fixes this one space. However we have seen that $C_V(q_i) \cap C_V(q_j)$ is trivial thus q_j negates v_i. Now if we let k be distinct from both i and j then q_k negates v_i and v_j and thus the vector $v_i + v_j$.

We consider the action of X on the set of vectors. We have seen that v_i lies in an orbit with its inverse and with the non-trivial elements of the other 1-spaces of type $1A$. Thus v_i lies in an orbit of length six and so $|C_X(v_i)| = 4$. Also $v_i + v_j$ lies in an orbit with its inverse and the non-trivial elements of the other 1-spaces of type $1C$. Thus the orbit has length 12 and so $|C_X(v_i + v_j)| = 2$. The element of order two in X centralizing $v_i + v_j$ cannot lie in $O_2(X)$ by (iv) and so must be in the other conjugacy class of involutions.

Since all involutions outside of $O_2(X)$ lie in this conjugacy class, each fixes some conjugate of $v_i + v_j$. □

Lemma 2.18. *Suppose that* $X \cong \mathrm{Sym}(4)$ *and that* V *is a faithful* 3*-dimensional* $\mathrm{GF}(3)X$*-module. Then the subspaces of order* 3^2 *have the following forms.*

(*i*) *Type 2A - These contains two* 1*-dimensional subspaces conjugate to* $\langle v_1 + v_2 \rangle$ *and two conjugate to* $\langle v_1 \rangle$*. There are three such subspaces.*

(*ii*) *Type 2B - These contain one* 1*-dimensional subspace conjugate to* $\langle v_1+v_2+v_3 \rangle$ *three* 1*-dimensional subspaces conjugate to* $\langle v_1 + v_2 \rangle$*. There are four such subspaces.*

(*iii*) *Type 2C - These contain two* 1*-dimensional subspaces conjugate to* $\langle v_1 + v_2 + v_3 \rangle$*, one conjugate to* $\langle v_1 + v_2 \rangle$ *and one conjugate to* $\langle v_1 \rangle$*. There are six such subspaces.*

Proof. Let $Y = \langle v_1, v_2 \rangle$. Then Y contains the 1-dimensional subspaces $\langle v_1 \rangle$, $\langle v_2 \rangle$, $\langle v_1+v_2 \rangle$ and $\langle v_1 - v_2 \rangle$. Hence Y is of type 2A.

Now let $W = \langle v_1+v_2, v_2-v_3 \rangle$. Then W contains the 1-dimensional subspaces $\langle v_1+v_2 \rangle$, $\langle v_2 - v_3 \rangle$, $\langle v_1 + v_3 \rangle$ and $\langle v_1 - v_2 - v_3 \rangle$. Hence W is of type 2B.

Finally let $U = \langle v_1, v_1 + v_2 + v_3 \rangle$. Then U contains the 1-dimensional subspaces $\langle v_1 \rangle$, $\langle v_1 + v_2 + v_3 \rangle$, $\langle v_2 + v_3 \rangle$ and $\langle v_1 - v_2 - v_3 \rangle$. Hence U is of type 2C.

The number of each type of subgroup follows from Lemma 2.17 (*iii*). □

There are two isomorphism types of 3-dimensional Sym(4)-modules and we give an example of both. Firstly, let

$$A = \langle (123), (456), (789), (147)(258)(369), (14)(2536) \rangle.$$

Then A has shape $3^3 : \mathrm{Sym}(4)$ and $A \leqslant \mathrm{Alt}(9)$. Secondly, let

$$B = \langle (123), (456), (789), (147)(258)(369), (14)(2536)(78) \rangle,$$

then B also has shape $3^3 : \mathrm{Sym}(4)$. We see that $B \leqslant \mathrm{Sym}(9)$ but $B \nleqslant \mathrm{Alt}(9)$. Notice in both groups that we can apply Lemma 2.17 by setting $v_1 = (123)$, $v_2 = (456)$ and $v_3 = (789)$. Notice also that in B the element (789) is inverted by the element $(14)(2536)(78)$ however one can check that $C_A((789)) = N_A((789))$. Also, by Lemma 2.17 (vi), $|C_A((789))| = |C_B((789))| = 4$ however in A, (789) commutes with an element of order four, $(14)(2536)$, and again one can check that in B, (789) commutes with an elementary abelian group of order four. We will use Lemma 2.17 and Lemma 2.18 in Chapter 7 where it will become clear we have a $\mathrm{Sym}(4)$-module of the second type.

2.5 Some Modular Character Theory

We introduce a small amount of modular character theory which we will require in Chapter 8. Results will be stated without proof. The main reference for this chapter has been Chapter 15 of [19].

Let $\mathbb{A}$ be the ring of algebraic integers and let M be a maximal ideal of $\mathbb{A}$ containing $\mathbb{A}p$ where p is a fixed prime. Set F to be the field $\mathbb{A}/M$ which necessarily has characteristic p and set $* : \mathbb{A} \rightarrow F$ to be the natural ring homomorphism. Notice that we may have some choice over M and hence over F but our choice makes no difference to the following results. Finally, set $U = \{\varepsilon \in \mathbb{A} | \varepsilon^n = 1 \text{ for } n \in \mathbb{Z} \text{ with } (n,p) = 1\}$. The following hold.

(i) $*\big|_U : U \rightarrow F^\times$ is a group isomorphism.

(ii) F is an algebraically closed field.

Let G be a group and let $\rho : G \to \mathrm{GL}_n(F)$ be a representation of G affording the character χ. Let Ω be the set of elements of G with order prime to p. We define the Brauer character of G to be the map $\phi : \Omega \to \mathbb{C}$ as follows. For each $x \in \Omega$, $\rho(x)$ has eigenvalues $\varepsilon_1, \ldots, \varepsilon_n \in F^\times$ as F is algebraically closed. Since $*\big|_U$ is a group isomorphism onto $F^\times$, we can find a unique $u_i \in U$ such that $* : u_i \mapsto \varepsilon_i$. Thus we can define $\phi(x) = \Sigma u_i$. A Brauer character is said to be irreducible if the representation affording it is irreducible. Each Brauer character is clearly constant on conjugacy classes of G in Ω and so is an example of a class function defined on the elements of Ω.

Lemma 2.19. *Suppose U and V are FG-modules affording characters χ_1 and χ_2 respectively. Then $U \otimes_F V$ affords the character $\chi_1\chi_2$ defined by $\chi_1\chi_2(g) = \chi_1(g)\chi_2(g)$ for each $g \in G$.*

Proof. If $u \in U$ is a λ-eigenvector and $v \in V$ is a μ-eigenvector then $u \otimes v \in U \otimes V$ is an eigenvector and the eigenvalue is $\lambda\mu$. Suppose $\rho_1 : G \to \mathrm{GL}(U)$ and $\rho_2 : G \to \mathrm{GL}(V)$ are the corresponding representations. Let $g \in G$ and let $\{\lambda_1, \ldots, \lambda_n\}$ be the eigenvalues for $\rho_1(g)$ and let $\{\mu_1, \ldots, \mu_m\}$ be the eigenvalues for $\rho_2(g)$. Then $\{\lambda_i\mu_j | 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m\}$ are the eigenvalues for $\rho(g)$ where $\rho : G \to \mathrm{GL}(U \otimes V)$. Now, by the definition of the Brauer character,

$$\chi_1(g) = \sum_{i=1}^{n} a_i \quad \text{and} \quad \chi_2(g) = \sum_{j=1}^{m} b_j$$

where $*(a_i) = \lambda_i$ and $*(b_j) = \mu_j$. The Brauer character afforded by U $\otimes V$ is $\chi(g) = \sum_{i=1}^{n}\sum_{j=1}^{m} c_{ij}$ where $*(c_{ij}) = \lambda_i\mu_k = *(a_i) * (b_j) = *(a_i b_j)$ since $*$ is a group homomorphism. Therefore

$$\chi(g) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j = \sum_{i=1}^{n} a_i \sum_{j=1}^{m} b_j = \chi_1(g)\chi_2(g).$$

□

Theorem 2.20. *The irreducible Brauer characters give a basis for the space of $\mathbb{C}$-valued* *class functions defined on Ω. The number of irreducible Brauer characters of G is equal to the number of conjugacy classes of elements of order prime to p.*

Proof. This theorem is Theorem 15.10 in [19]. □

Lemma 2.21. *Let χ be an ordinary character of G and let $\widehat{\chi}$ be the restriction of χ to the elements in Ω. Then $\widehat{\chi}$ is a Brauer character of G.*

Proof. [19, 15.6 p265] □

Theorem 2.22. *Let χ be an ordinary irreducible character of G such that $|G|/\chi(1)$ is prime to p. Then $\widehat{\chi}$ is an irreducible Brauer character of G.*

This theorem is essentially Theorem 15.29 in [19] which proves that the set $\{\chi, \widehat{\chi}\}$ is a block.

Let V be an n-dimensional module for G over some finite field, K, of characteristic p. Then consider the module $F \otimes_K V$. This is an n-dimensional module for G over F when we define $(f \otimes v) \cdot g = f \otimes (v \cdot g)$ for $f \in F$, $v \in V$ and $g \in G$. A basis for $F \otimes_K V$ is $\{1 \otimes_K v_i | 1 \leqslant i \leqslant n\}$ over F where $\{v_i | 1 \leqslant i \leqslant n\}$ is a basis for V over K. By Lemma 2.8, if V is irreducible and $\mathrm{End}_{KG}(V) = K$ then $V \otimes_K F$ is irreducible. So we have some tools for classifying possible modules for G over finite fields.

2.6 Natural $\mathbf{SL_2(2^n)}$-Modules

In all that follows let $X \cong \mathrm{SL}_2(2^n)$ where $n \geq 2$, $T \in \mathrm{Syl}_2(X)$ and set $L := \mathrm{GF}(2)$ and $K := \mathrm{GF}(2^n)$. We will calculate the Brauer character table for X and so we must choose an algebraically closed field, F, of characteristic two in which to calculate.

Lemma 2.23. *The following hold in $X \cong \mathrm{SL}_2(2^n)$.*

(*i*) *There are at most* 2^n *conjugacy classes of elements of odd order.*

(*ii*) *Let* $S, T \in \mathrm{Syl}_2(X)$. *Then* $S \cap T = 1$ *and* S *acts transitively on the set* $\mathrm{Syl}_2(X) \backslash \{S\}$.

(*iii*) *For* $S, T \in \mathrm{Syl}_2(X)$, $N_X(S) \cap N_X(T)$ *has order* $2^n - 1$ *and fixes precisely two elements in* $\mathrm{Syl}_2(X)$.

(*iv*) X *acts sharply* 3*-transitively on* $\mathrm{Syl}_2(X)$.

(*v*) *For* $S, T \in \mathrm{Syl}_2(X)$ *and* $t \in T^{\#}$, $X = \langle S, T \rangle = \langle S, t \rangle$.

Proof. The characteristic polynomial for a non-identity element, A, of X is $x^2 - tr(A)x + 1$. Since conjugate elements have the same characteristic polynomial and values of the trace lie in K, we have 2^n possibilities. So together with the identity we have at most $2^n + 1$ conjugacy classes in X. As one of these classes contains elements of order 2, we have at most 2^n classes of elements of odd order.

Every Sylow 2-subgroup has order 2^n and is normalized by a subgroup of X conjugate to the Borel subgroup of lower triangular matrices. This has order $2^n(2^n - 1)$ and so there are $2^n + 1$ Sylow 2-subgroups in X. We consider the action of X on the set $\Omega := \mathrm{Syl}_2(X)$. Let $S \in \Omega$. It is clear that no non-trivial element of S fixes any other element of Ω else we would have a larger 2-group and since $|\Omega \backslash \{S\}| = 2^n = |S|$, we see S is transitive on $\Omega \backslash \{S\}$. Thus X is 2-transitive on $\mathrm{Syl}_2(X)$. Consider two elements of Ω namely, U, the upper triangular and, L, the lower triangular matrices. These intersect trivially and so any pair of Sylow 2-subgroups intersect trivially. Notice that both are normalized by the subgroup of diagonal matrices, D. In fact $D = N_X(U) \cap N_X(L)$ for the intersection can be no larger with out having even order. Suppose D normalizes a third element of Ω, P say. Find $x \in U$ such that $L^x = P$. Then $D, D^x \leqslant N_X(L^x) \cap N_X(U)$. But then $D = D^x$ and so $x \in N_U(D) = 1$. Thus D fixes exactly 2 elements of Ω and so is transitive on $\Omega \backslash \{U, L\}$. So now we have shown that a 2-point stabilizer is transitive on the remaining $2^n - 1$ points and that the stabilizer of three points is trivial. Hence X is sharply 3-transitive on Ω.

Now for any distinct pair of Sylow 2-subgroups, S and T, and any $t \in T^{\#}$, the group $Y := \langle S, t \rangle$ contains Sylow subgroups of order 2^n and also an element from each Sylow 2-subgroup. As they all intersect trivially it contains all Sylow subgroups. However, the subgroup of X generated by all Sylow 2-subgroups must be normal in X but X is simple and so it must be all of X. □

Definition 2.24. Let R be the polynomial ring in two commuting indeterminates, x and y, with coefficients in K. Then R is a KX-module when we set

$$x \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ax + by$$

and

$$y \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = cx + dy.$$

Let $R(1) = \{f \in R | \deg f = 1\} \cup \{0\}$. Then $R(1)$ is a 2-dimensional submodule which we will call the natural module over K.

Lemma 2.25. *Let V be a natural module for X over K. The following hold.*

(i) V is irreducible.

(ii) X is transitive on non-zero vectors of V.

(iii) X is 2-transitive on the 1-subspaces of V.

(iv) Elements of X with odd order act fixed-point-freely on V.

Proof. The stabilizer of a 1-space is clearly the normalizer of a Sylow 2-subgroup, i.e. conjugate to a group of triangular matrices, which again is transitive on all remaining 1-spaces. It is then clear that V is irreducible since there can be no X-invariant subspace. Moreover, the group of triangular matrices is transitive on the non-zero vectors in the

1-space and so X is transitive on non-zero vectors. Finally, the stabilizer of a non-zero vector is a Sylow 2-subgroup and so any non-identity element of X with odd order fixes no non-zero vector in V. □

Lemma 2.26. *There are at least n non-isomorphic, 2-dimensional, irreducible modules for X over K, namely the natural module over K and its n algebraic conjugates.*

Proof. If $\phi : X \to \mathrm{GL}(V)$ is the representation of X affording a natural module, V, over K and $\sigma \in \mathrm{Aut}(K)$ then, after choosing a basis for V and writing X as matrices, we can define another representation $\phi^\sigma : X \to \mathrm{GL}(V)$ simply by applying σ to the matrix entries. The corresponding module we label V^σ and call it a Galois twist of V. It is clear that no choice of basis elements allow the matrices to be written purely by elements of L. See [1, 26.3] for a proof that this means V and V^σ cannot be isomorphic as KX-modules. Since $K = \mathrm{GF}(2^n)$ has n automorphisms, namely $k \mapsto k^{2^i}$ $0 \leq i \leq n-1$, we see n distinct irreducible modules for X over K. □

Let $V_1, \ldots, V_n$ be these 2-dimensional irreducible KX-modules.

Theorem 2.27. *Let V be an irreducible KX-module and let $K' \geqslant K$ be a field extension. Then the $K'X$-module $K' \otimes_K V$ is irreducible.*

Proof. Recall that an irreducible KX-module, V is called absolutely irreducible if $K' \otimes_K V$ is an irreducible $K'X$-module for each extension $K' \geqslant K$. The splitting field for X is the field, S, with the property that every irreducible SX-module is absolutely irreducible. Remark 2.8.8 in [14] says that the splitting field for X is K. Thus every irreducible KX-module is absolutely irreducible. □

Corollary 2.28. *Let V be an irreducible KX-module then $\mathrm{End}_{KX}(V) \cong K$.*

Proof. By Theorem 2.27, V is absolutely irreducible and so by Lemma 2.8, $\mathrm{End}_{KX}(V) \cong K$. □

Let $M_i = F \otimes V_i$ for $1 \leq i \leq n$. Recall these are 2-dimensional modules over the algebraically closed field F and by Theorem 2.27, each M_i is irreducible.

Lemma 2.29. *Let $x \in X$ have odd order and let χ_i be the Brauer character afforded by the FX-module M_i. Then $\chi_i(x) = \varepsilon^{2^{i-1}} + \varepsilon^{-2^{i-1}}$ where ε is some fixed m'th root of unity and m and the order of x both divide $2^n - 1$ or both divide $2^n + 1$.*

Proof. Any element, $x \in X$, of odd order either normalizes a Sylow 2-subgroup and so has order dividing $2^n - 1$ or is fixed-point-free on the Sylow 2-subgroups and so has order dividing 2^n+1. Let ρ_1 be the natural K-representation affording the KX-module V_1. The possible eigenvalues for $\rho_1(x)$ in the algebraically closed extension field F are therefore field elements, α and α^{-1}, satisfying the polynomial $X^{2^n-1} - 1$ or $X^{2^n+1} - 1$. By Lemma 2.10, the Brauer character afforded by the module M_1 for x is $\varepsilon+\varepsilon^{-1}$ where ε is some fixed m'th root of unity in $\mathbb{C}$ and m divides either $2^n - 1$ or $2^n + 1$. The entries of the matrices representing the action of X on each module V_i are altered by a Galois automorphism. So, by Lemma 2.10, the Brauer character afforded by the module M_i for x is $\varepsilon^{2^{i-1}} + \varepsilon^{-2^{i-1}}$.□

Lemma 2.30. *There are 2^n irreducible modules for X over F. They are the 2^n possible tensor products $\bigotimes_{i \in I} M_i$ where $I \subseteq \{1, 2, \ldots, n\}$.*

Proof. We begin by identifying an irreducible character for X in characteristic zero of degree 2^n. Consider the action of X on its Sylow 2-subgroups. Let χ be the corresponding class function and set $\chi_1 = \chi - I$ where I is the trivial character. It follows from Lemma 2.23 that any element of X which normalizes a Sylow 2-subgroup either has order two and fixes precisely one Sylow 2-subgroup or lies outside of it and fixes exactly two of them. Thus the class function χ gives values 1 for elements of order two, 2 for elements whose order divides $2^n - 1$ and 0 for elements whose order divides $2^n + 1$. So χ_1 gives respective values 0, 1, -1. We see that this class function is an irreducible character by taking its inner product. This gives

$$\begin{aligned}\langle \chi_1, \chi_1 \rangle &= \tfrac{2^{2n}}{2^n(2^n-1)(2^n+1)} + \tfrac{0}{2^n} + a\left(\tfrac{1}{2^n-1}\right) + b\left(\tfrac{(-1)^2}{2^n+1}\right) \\ &= \tfrac{1}{2^{2n}-1}\left(2^n + a(2^n+1) + b(2^n-1)\right),\end{aligned}$$

where a is the number of conjugacy classes of elements whose order divides $2^n - 1$ and b is the number of classes of elements whose order divides $2^n + 1$. Thus $a + b = 2^n - 1$ and it follows that $\langle \chi_1, \chi_1 \rangle$ is strictly less than 2 and so must be 1 and so χ_1 is irreducible. Now by Theorem 2.22, the restriction of χ_1 to the elements of x with odd order is an irreducible Brauer character, $\widehat{\chi_1}$. Clearly $\chi(1) = |\mathrm{Syl}_2(X)| = 2^n + 1$ and so $\chi_1(1) = 2^n$. Therefore we have found an irreducible Brauer character for X in characteristic two of degree 2^n.

We now begin to identify all irreducible representations of X over F. Consider the Brauer character for some element, x, of odd order afforded by the module $M_1 \otimes_F \ldots \otimes_F M_n$. By Lemma 2.29 and Lemma 2.19, this will give values

$$\prod_{i=1}^{n} (\varepsilon^{2^{i-1}} + \varepsilon^{-2^{i-1}}) = \frac{\varepsilon^{2^n} - \varepsilon^{-2^n}}{\varepsilon - \varepsilon^{-1}},$$

where ε is some fixed m'th root of unity and m divides $2^n - 1$ or $2^n + 1$. So if x has order dividing $2^n - 1$ then the character value is 1 otherwise it is -1. Now we have a direct agreement between the character induced by the module $M_1 \otimes \ldots \otimes M_n$ and the character $\widehat{\chi_1}$. This means that $M_1 \otimes \ldots \otimes M_n$ is an irreducible module. It follows immediately that every module $M_{r_1} \otimes \ldots \otimes M_{r_k}$ where $1 \leqslant r_1 < r_2 < \ldots < r_k \leqslant n$ is irreducible since any proper submodule of $M_{r_1} \otimes \ldots \otimes M_{r_k}$ would give a proper submodule of $M_1 \otimes \ldots \otimes M_n$. If M is any X-module then the module $M \otimes M$ is not irreducible since it has a proper submodule $\langle m \otimes n - n \otimes m | m, n \in M \rangle$. So suppose $M_{r_1} \otimes \ldots \otimes M_{r_k}$ and $M_{s_1} \otimes \ldots \otimes M_{s_k}$ are isomorphic. Then their tensor product would be reducible but then there is some repeated natural module M_i. Continuing in this way we would see $M_{r_1} \otimes \ldots \otimes M_{r_k} = M_{s_1} \otimes \ldots \otimes M_{s_k}$. Thus we have identified 2^n distinct irreducible modules for X over F. We have already seen that there are at most 2^n conjugacy classes of elements of odd order and so by Theorem 2.20, there are exactly 2^n classes and 2^n irreducible modules. □

Lemma 2.31. *There are exactly 2^n irreducible modules for X over K. They are all possible tensor products (over K) $\bigotimes_{i\in I} V_i$ where $I \subseteq \{1, 2, \ldots, n\}$.*

Proof. For any set $I \subseteq \{1, \ldots, n\}$, $(\bigotimes_{i\in I,K} V_i) \otimes_K F \cong \otimes_{i\in I,F} M_i$ by repeated us of Lemma 2.9. Suppose $(\bigotimes_{i\in I,K} V_i)$ had a proper KX-submodule W. Then $W \otimes_K F$ would be a proper FX-submodule of the irreducible module $\otimes_{i\in I,F} M_i$ and so must be trivial. Thus each $(\bigotimes_{i\in I,K} V_i)$ is an irreducible KX-module. If for $I, J \subseteq \{1, \ldots, n\}$, $\bigotimes_{i\in I,K} V_i$ was KX-isomorphic to $\bigotimes_{j\in J,K} V_j$ then $\bigotimes_{i\in I,F} M_i \cong \bigotimes_{j\in J,F} M_j$ and so by Lemma 2.30, $I = J$. Therefore we have at least 2^n irreducible KX-module. Suppose we could find one more, U say. Then by Lemma 2.27, $U \otimes_K F$ is irreducible and we would have $U \otimes_K F \cong \bigotimes_{i\in I,F} M_i \cong (\bigotimes_{i\in I,K} V_i) \otimes_K F$ and so $U \cong \bigotimes_{i\in I,K} V_i$. Thus there are exactly 2^n irreducible KX-modules. □

The previous lemma is also a famous theorem by Robert Steinberg.

Theorem 2.32. *(Steinberg) There are exactly 2^n irreducible modules for X over K. They are all possible tensor products (over K) $\bigotimes_{i\in I} V_i$ where $I \subseteq \{1, 2, \ldots, n\}$.*

Proof. See [28, 13.1]. □

Lemma 2.33. *(i) The only irreducible modules for X over F which admit an element of order three acting fixed-point-freely are the modules $M_1, \ldots, M_n$.*

(ii) The only irreducible modules for X over K which admit an element of order three acting fixed-point-freely are $V_1, \ldots, V_n$.

Proof. We consider the possible Brauer character values for some element g of order three acting fixed-point-freely. Let χ_i be the character corresponding to M_i. Then $\chi_i(g) = \omega + \omega^2 = -1$ where ω is a primitive cube root of unity. Thus if χ is the character value corresponding to some irreducible FX-module, $M = M_{r_1} \otimes \ldots \otimes M_{r_k}$, then $\chi(g) = 1$ or -1. By Lemma 2.6,

$$C_M(\langle g \rangle) = \langle \chi_{|_{\langle g \rangle}}, 1_{|_{\langle g \rangle}} \rangle = \frac{1}{3}(\chi(1) + \chi(g) + \chi(g^2)).$$

So g acts fixed-point-freely on M if and only if $\chi(1) = \dim(M) = 2$ if and only if $M = M_i$ for some $1 \leqslant i \leqslant n$.

Suppose now that V is some irreducible KX-module admitting g fixed-point-freely. By Theorem 2.27, $F \otimes_K V$ is an irreducible FX-module. Observe that g acts fixed-point-freely on $F \otimes_K V$ since $(f \otimes v) \cdot g = f \otimes v \cdot g = f \otimes v$ if and only if $v \cdot g = v$ for $f \in F$ and $v \in V$. So now $F \otimes_K V$ must have dimension two and so V must be KX-isomorphic to V_i for some $1 \leqslant i \leqslant n$. Finally, by Lemma 2.25, X acts fixed-point-freely on V_1 and similarly on each algebraic conjugate. □

Definition 2.34. A natural module for X over L is an irreducible $2n$-dimensional module, V, such that $\mathrm{End}_{LX}(V) \cong \mathrm{GF}(2^n)$.

Lemma 2.35. *(i) Let V be a natural module for X over L. Then V can be viewed as a 2-dimensional vector space over K and as such is KX-isomorphic to an algebraic conjugate of the natural module over K.*

(ii) Let U be an algebraic conjugate of the natural module for X over K. Then U can be viewed as a $2n$-dimensional vector space over L and as such is LX-isomorphic to a natural module over K.

(iii) The natural module over L is unique up to LX-isomorphism.

Proof. Let V be a natural module over L. Then V admits an action by its endomorphism ring and so is a vector space over K of dimension two. Let U represent the vector space V over K. Suppose U is not irreducible then U contains a KX-invariant proper subspace U_0 say. However this would mean that U_0 was LX-invariant and so also a submodule of V, the vector space over L, which contradicts that V is irreducible by definition. So U is irreducible of dimension two and therefore must be the natural module over L or one of its algebraic conjugates.

Now let U be a natural module for X over K then U is also a vector space over L. Let V represent this restriction module then V is a vector space over L and V is irreducible as an X-module since X is transitive on non-zero vectors of U by Lemma 2.25. We can define an action of K on V and so K is embedded in $E := \mathrm{End}_{LX}(V)$. By Schur's Lemma, E is a field. However, since all elements of E commute with K, it follows that $E = \mathrm{End}_{KX}(V) = \mathrm{End}_{KX}(U) = K$ by Lemma 2.28. So by definition V is a natural LX-module and so the restriction of any of the irreducible 2-dimensional modules over K gives a natural module over L.

Let V be the natural module over K and V^σ a Galois twist of V. Consider the following map

$$\begin{array}{rccc} \Phi : & V & \rightarrow & V^\sigma \\ & (k_1, k_2) & \mapsto & ({k_1}^\sigma, {k_2}^\sigma). \end{array}$$

Then Φ is an LX-module isomorphism since for all $v = (k_1, k_2) \in V$ and every matrix in the corresponding representation of X,

$$\begin{aligned}
\Phi\left((k_1,k_2)\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) &= ((k_1a+k_2c)^\sigma,(k_1b+k_2d)^\sigma) \\
&= (k_1^\sigma,k_2^\sigma)\begin{pmatrix} a^\sigma & b^\sigma \\ c^\sigma & d^\sigma \end{pmatrix} \\
&= \Phi\left((k_1,k_2)\right)\cdot\begin{pmatrix} a & b \\ c & d \end{pmatrix}.
\end{aligned}$$

Also because σ is trivial on L we have $\Phi(lv) = l\Phi(v)$ for all $l \in L$. Thus V and V^σ are isomorphic as LX-modules. In particular it will follow that their restrictions over L are isomorphic as LX-modules. □

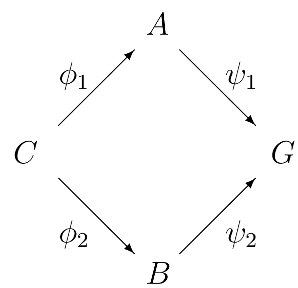
Chapter 3

Amalgams and the Coset Graph

An amalgam of finite groups is an ordered collection of three finite groups and two injective homomorphisms $\mathcal{A} = (A, B, C, \phi_1, \phi_2)$, such that $\phi_1 : C \to A$ and $\phi_2 : C \to B$.

We say that two amalgams $\mathcal{A}_1 = (A_1, B_1, C_1, \phi_1, \phi_2)$ and $\mathcal{A}_2 = (A_2, B_2, C_2, \theta_1, \theta_2)$ are isomorphic if there exist isomorphisms $\alpha : A_1 \to A_2$, $\beta : B_1 \to B_2$ and $\gamma : C_1 \to C_2$ such that $\alpha\phi_1 = \theta_1\gamma$ and $\beta\phi_2 = \theta_2\gamma$. We say that $\mathcal{A}$ is a simple amalgam if, whenever $K \leqslant B$, with $\phi_1(K) \trianglelefteq A_1$ and $\phi_2(K) \trianglelefteq A_2$, then $K = 1$.

A completion of an amalgam, $\mathcal{A} = (A, B, C, \phi_1, \phi_2)$, is a collection triple (G, ψ_1, ψ_2) where G is a group such that $\psi_1 : A \to G$ and $\psi_2 : B \to G$ are homomorphisms with $G = \langle \psi_1(A), \psi_2(B) \rangle$ and such that $\psi_1\phi_1 = \psi_2\phi_2$. That is that the following diagram commutes:



A completion, G, is faithful if ψ_1 and ψ_2 are injective. In this case we often suppress use of monomorphisms and identify A, B and C with their images in G. In fact, when we describe particular amalgams in this thesis we will often assume we have a group G with subgroups A, B and $C := A \cap B$ such that $G = \langle A, B \rangle$. Therefore we are implicitly assuming that (G, I_1, I_2) is a completion of the amalgam (A, B, C, i_1, i_2) where i_1 and i_2 are the inclusion maps $i_1 : C \hookrightarrow A$ and $i_2 : C \hookrightarrow B$ and I_1, I_2 are the inclusion maps $I_1 : A \hookrightarrow G$ and $I_2 : B \hookrightarrow G$.

A completion (F, Ψ_1, Ψ_2) of $\mathcal{A}$ is called *universal* if given any other completion (G, ψ_1, ψ_2) there is a unique homomorphism $\pi : F \to G$ such that $\Psi_i \pi = \psi_i$ for $i = 1, 2$. This implies that any completion of $\mathcal{A}$ is isomorphic to a quotient of the universal completion of $\mathcal{A}$ and that the universal completion is itself unique up to isomorphism. Isomorphic amalgams have the same groups as completions so to recognize possible completions we need to recognize the possible isomorphism classes of the amalgam. A fundamental result which has become known as the *Goldschmidt Lemma* (see [12, 2.7]) gives us a method for calculating the number of isomorphism classes of a given type of amalgam.

Lemma 3.1. *(Goldschmidt Lemma) Let (X, Y, Z) be an amalgam of finite groups and set $X^* = N_{\mathrm{Aut}(X)}(Z)/C_{\mathrm{Aut}(X)}(Z)$, $Y^* = N_{\mathrm{Aut}(Y)}(Z)/C_{\mathrm{Aut}(Y)}(Z)$ then there is a one-to-one correspondence between isomorphism classes of type (X, Y, Z) and (X^*, Y^*)-double cosets in $\mathrm{Aut}(Z)$.*

Let $\mathcal{A} = \mathcal{A}(A_1, A_2, B)$ be a simple amalgam and let G be a faithful completion of $\mathcal{A}$. We identify A_1, A_2 and B with their images in G and regard ϕ_i as the inclusion map of B into A_i. We also suppose that $B = A_1 \cap A_2$. The *coset graph* of the amalgam $\mathcal{A}$ is the graph $\Gamma = \Gamma(G, A_1, A_2, B)$ that has vertex set

$$V(\Gamma) = \{A_i g \mid g \in G, i \in \{1, 2\}\},$$

and edge set

$$E(\Gamma) = \{\{A_i g, A_j h\} \mid A_i g \cap A_j h \neq \emptyset, i \neq j\}.$$

Since G is a simple amalgam, G acts faithfully by right multiplication on Γ and this action preserves the edge set $E(\Gamma)$.

For $\gamma \in V(\Gamma)$, let $G_\gamma = \mathrm{Stab}_G(\gamma)$ and let $\Gamma(\gamma) = \{\delta \in V(\Gamma) \mid \{\gamma, \delta\} \in E(\Gamma)\}$ be the set of vertices adjacent to γ in Γ. For $\{\gamma, \delta\} \in \mathrm{E}(\Gamma)$, let $G_{\gamma\delta} = \mathrm{Stab}_G(\{\gamma, \delta\}) = G_\gamma \cap G_\delta$. The following results are well known and easy to prove.

Lemma 3.2. *Let G be a faithful completion of a simple amalgam of groups (A_1, A_2, B) and let Γ be the coset graph.*

(*i*) *G acts faithfully on Γ.*

(*ii*) *G has two orbits on $V(\Gamma)$ and is transitive on $E(\Gamma)$.*

(*iii*) *For $\gamma \in V(\Gamma)$, G_γ is G-conjugate to either A_1 or A_2.*

(*iv*) *For $\{\gamma, \delta\} \in E(\Gamma)$, $G_{\gamma\delta}$ is G-conjugate to B.*

(*v*) *For $\gamma \in V(\Gamma)$, G_γ acts transitively on $\Gamma(\gamma)$. In particular, $|\Gamma(\gamma)| = [G_\gamma : G_{\gamma\delta}]$ for any $\delta \in \Gamma(\gamma)$.*

(*vi*) *The graph Γ is connected.*

Proof. See [22, Lemma 4.1, Lemmas 4.3 and 4.5]. □

Parts (*ii*) and (*iii*) of Lemma 3.2 imply that the amalgam $\mathcal{A} = \mathcal{A}(A_1, A_2, B)$ is isomorphic to the amalgam $\mathcal{A}' = \mathcal{A}'(G_\gamma, G_\delta, G_{\gamma\delta})$ for $\{\gamma, \delta\} \in E(\Gamma)$.

Definition 3.3. Let $(\alpha_1, \alpha_2, \ldots, \alpha_{n+1})$ and $(\beta_1, \beta_2, \ldots, \beta_{n+1})$ be any two paths of $n+1$ vertices in Γ where α_1 and β_1 lie in the same G-orbit. If there exists $g \in G$ such that $a_i \cdot g = b_i$ for each $1 \leqslant i \leqslant n = 1$ we say that G acts locally n-arc transitively on Γ.

Lemma 3.4. *G acts locally n-arc transitively if and only if the stabilizer of any path of m vertices, $(\alpha_1, \ldots, \alpha_m)$, is transitive on $\Gamma(\alpha_m)\backslash\{\alpha_{m-1}\}$ for each $1 \leqslant m \leqslant n$.*

Proof. Suppose G acts locally n-arc transitively on Γ. Let $1 \leqslant m \leqslant n$ and let $(\alpha_1, \ldots, \alpha_m)$ be a path of m vertices in Γ. Suppose $\beta_1, \beta_2 \in \Gamma(\alpha_m)\backslash\{\alpha_{m-1}\}$ then by n-arc transitivity, there is some $g \in G$ that maps the path $(\alpha_1, \ldots, \alpha_m, \beta_1)$ to the path $(\alpha_1, \ldots, \alpha_m, \beta_2)$ and so $\beta_1 g = \beta_2$.

Now suppose that $(\alpha_1, \alpha_2, \ldots, \alpha_{n+1})$ and $(\beta_1, \beta_2, \ldots, \beta_{n+1})$ are two paths of $n+1$ vertices in Γ with α_1 and β_1 lying in the same G-orbit. By edge-transitivity, there exists $g_1 \in G$ such that $\{\alpha_1, \alpha_2\}g_1 = \{\beta_1, \beta_2\}$. Now $\alpha_3 g_1 \in \Gamma(\beta_2)\backslash\{\beta_1\}$ so, by assumption, there exists $g_2 \in G_{\beta_1,\beta_2}$ such that $\alpha_3 g_1 g_2 = \beta_3$ and then $\{\alpha_1, \alpha_2, \alpha_3\}g_1 g_2 = \{\beta_1, \beta_2, \beta_3\}$. Continuing in this way proves G acts locally n-arc transitively on Γ. □

Chapter 4

Background Results

In this chapter we include several known results which will be used in this thesis. We discuss theorems of Feit and Thompson, Smith and Tyrer, and Hayden which are all character theoretic as well as a result from representation theory by McLaughlin. In contrast, we also discuss a graph theoretic theorem of Tits and Weiss.

The following result of Feit and Thompson (see [9] and [17]) characterizes a finite group containing a self-centralizing element of order three. The proof determines some of the character theory of a minimal counter example.

Theorem 4.1. *(Feit-Thompson) Let G be a finite group containing a subgroup, X, of order three such that $C_G(X) = X$. Then one of the following hold.*

(i) *G contains a nilpotent normal subgroup, N, such that G/N is isomorphic to* $\mathrm{Sym}(3)$ *or C_3.*

(ii) *G contains a nilpotent normal 2-subgroup, N, such that $G/N \cong \mathrm{Alt}(5)$.*

(iii) *G is isomorphic to $\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$.*

When applying Theorem 4.1 we will often need the following.

Lemma 4.2. *(i) Neither* Alt(5) *or* $\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$ *admit an outer automorphism of order three.*

(ii) If G is a group with a central involution, t, such that $G/\langle t \rangle \cong \mathrm{PSL}_2(7)$ then $G \cong$ $\mathrm{SL}_2(7)$.

Proof. It is well known (see [6]) that Alt(5) and $\mathrm{PSL}_2(7)$ both have outer automorphism groups of order two. It is also well known that the Schur multiplier of $\mathrm{PSL}_2(7)$ has order two so if G is a group satisfying $G/N \cong \mathrm{PSL}_2(7)$ where N is a central subgroup of G then N has order two and $G \cong \mathrm{SL}_2(7)$. □

The following result of Smith and Tyrer is of a similar nature to Theorem 4.1. It describes a group containing a p-subgroup (odd prime p) with restricted normalizer. The situation it describes is one which will appear several times in this thesis and so the theorem is one of the most well used here. We will use it when we have a group with an elementary abelian p-subgroup with restricted normalizer to say that the group has either a proper normal subgroup at index a power of p or the group is p-soluble of length one. First we define p-soluble.

Definition 4.3. A group G is p-soluble if every composition factor of G is either a p-group or a p'-group.

Consider the following series

$$1 \trianglelefteq O_{p'}(G) \trianglelefteq O_{p',p}(G) \trianglelefteq O_{p',p,p'}(G) \trianglelefteq \dots$$

where $O_{p',p}(G)$ is the preimage in G of $O_p(G/O_{p'}(G))$ and $O_{p',p,p'}(G)$ is the preimage in G of $O_{p'}(G/O_{p',p}(G))$ and so on. This series defines a minimal factorization of G into p and p' factors (minimal in the sense that the number of factors is as few as possible). We call this the lower p-series for G.

Definition 4.4. A p-soluble group G has length n if there are n factors in the lower p-series for G which are p-groups. In particular, G is p-soluble of length one if $G = O_{p',p,p'}(G)$. Alternatively, G is p-soluble of length one if for any Sylow p-subgroup, S, of G, $O_{p'}(G)S \trianglelefteq G$.

Theorem 4.5. *(Smith-Tyrer) Let G be a finite group and let P be a Sylow p-subgroup of G for an odd prime p. Suppose P is abelian and $[N_G(P) : C_G(P)] = 2$.*

- *(i) If G is perfect then P is cyclic.*
- *(ii) If P is non-cyclic, then $O^p(G) < G$ or G is p-soluble of length one.*

Proof. See [27]. □

This theorem is used many times in Chapters 6 and 7. It is particularly well suited to the problems encountered in Chapter 6 since each time it is used we can rule out one of the possibilities given by the theorem. However the group structures which we encounter in Chapter 7 satisfy both conclusions of the Smith-Tyrer theorem and so the theorem is less useful in those cases. It is easy to construct such groups which are both p-soluble of length one and have a proper p-residue. For example, consider the following subgroup of Sym(10).

$$G := \langle (1, 2, 3), (4, 5, 6), (7, 8, 9, 10), (1, 2)\rangle.$$

Notice first that G has a normal Sylow 3-subgroup for which the centralizer of the Sylow 3-subgroup has index two in G. Notice also that $O_{3'}(G) = \langle (7, 8, 9, 10\rangle$ and then $O_{3',3}(G) = \langle (7, 8, 9, 10), (1, 2, 3), (4, 5, 6)\rangle$ has index two in G and so G is 3-soluble of length one. However, $O^3(G) = \langle (7, 8, 9, 10), (1, 2), (1, 2, 3)\rangle \neq G$ and so G satisfies both conclusions of Theorem 4.5.

Corollary 4.6. *Let G be a group and let S be a Sylow p-subgroup of G (odd prime p). Suppose S is elementary abelian of order at least p^3 and $|N_G(S)/C_G(S)| = 2$. Finally, for some $x \in S$ of order p, suppose $x \in Z(G)$. Then* *(i) G is either p-soluble of length one or $O^p(G) < G$; and*

(ii) if G is not p-soluble of length one then $O^p(G)$ has index at least p^2 in G and does not contain x.

Proof. We apply the theorem of Smith and Tyrer to G to see that either G is p-soluble of length 1 or $O^p(G) < G$. We can apply these arguments again to $\overline{G} := G/\langle x\rangle$ to see that $\overline{G}$ is either p-soluble of length one or $O^p(\overline{G}) < \overline{G}$. So suppose $\overline{G}$ is p-soluble of length one. Let $\overline{N} := O_{p'}(\overline{G})$ and consider its preimage in G, N say. Then $\langle x\rangle$ is a Sylow p-subgroup of N and so N splits over $\langle x\rangle$ and therefore $N = M\langle x\rangle$ say. It follows that M is a normal subgroup of G of order prime to p. Now $MS = NS$ is normal in G since $\overline{NS}$ is normal in $\overline{G}$ because $\overline{G}$ is p-soluble of length one. Thus we have that G is p-soluble of length one.

So we see that $\overline{G}$ being p-soluble of length one forces G to have the same property. We now suppose that G does not have this property then neither does $\overline{G}$ and so both have normal subgroups of index a proper power of p. By Gaschütz's Theorem, there is a complement to $\langle x\rangle$ in G, L say, which is necessarily normal in G. Thus $O^p(G) \leqslant L$ and $\langle x\rangle \notin O^p(G)$. So consider now the preimage in G of $O^p(\overline{G})$. This preimage gives a normal subgroup of index at least p which contains x and so is distinct from L. Thus $O^p(G)$ is contained in the intersection of the preimage of $O^p(G)$ and L and so $G/O^p(G)$ has order at least p^2 and does not contain x. □

The following theorem is of the same nature as the previous theorems and is also proved using characters. It can be found in [16, 3.3 p545].

Theorem 4.7. *(Hayden) Let G be a finite group and let $T \in \mathrm{Syl}_3(G)$ be elementary abelian of order nine. Assume that*

(i) $N_G(T)/C_G(T) \cong 2 \times 2$;

(ii) $C_G(T) = T$; and

(iii) $C_G(t) \leqslant N_G(T)$ *for each* $t \in T^{\#}$.

Then $G = N_G(T)$.

The following theorem of Jack McLaughlin comes from the paper *Some Groups Generated by Transvections* [21] and will be used in the proof of Theorem B. It can be used to describe a situation in which an elementary abelian group is normalized by a group generated by elements which each act trivially on a maximal subgroup.

Theorem 4.8. *(McLaughlin) Let* V *be a vector space over* $\mathrm{GF}(p)$ *for odd prime* p. *Suppose* H *is a subgroup of* $\mathrm{GL}(V)$ *such that* $H = \langle h_1, \ldots, h_r \rangle$ *where* $[V : C_V(h_i)] = p$ *for each* $1 \leqslant i \leqslant r$. *Furthermore, suppose that* H *contains no non-trivial normal* p*-subgroup. Then for some* $n \geqslant 1$,

$$V = V_0 \oplus V_1 \oplus \ldots \oplus V_n,$$

where each V_i *is a* G*-module and*

$$H = H_1 \times \ldots \times H_n$$

where each $H_j \cong \mathrm{SL}(V_j)$ *or* $H_j \cong \mathrm{Sp}(V_j)$. *Finally for* $i \neq j$, H_j *acts trivially on* V_i.

Proof. See [21]. □

We demonstrate an application of this theorem by introducing a scenario which will occur inside the amalgam of type $G_2(3)$.

Lemma 4.9. *Let* M *be a group and let* $V := O_3(M)$ *be elementary abelian and self-centralizing in* G *of order* 3^4. *Let* $\overline{M} = M/V$ *and let* $\overline{R} \in \mathrm{Syl}_3(\overline{M})$ *have order* 3^2 *and let* $\overline{S}, \overline{T}$ *be non-conjugate subgroups of* $\overline{R}$ *of order three and suppose* $[V : C_V(\overline{S})] = [V : C_V(\overline{T})] = 3$. *Then* $\langle \overline{S}^M \rangle \cong \mathrm{SL}_2(3)$, $\langle \overline{T}^M \rangle \cong \mathrm{SL}_2(3)$ *and* $[\langle \overline{S}^M \rangle, \langle \overline{T}^M \rangle] = 1$.

Proof. Let $\overline{H} = \langle \overline{S}^M, \overline{T}^M \rangle \leqslant \overline{M}$. Since V is self-centralizing in M, $\overline{H}$ is isomorphic to a subgroup of the group of automorphisms of V, $\mathrm{Aut}(V) \cong \mathrm{GL}(V)$. Since $V = O_3(M)$, by correspondence, $\overline{M}$ contains no normal 3-subgroup. Thus the intersection of all its Sylow 3-subgroups is trivial. Clearly $\overline{H}$ is a subgroup of $\overline{M}$ containing every Sylow 3-subgroup of $\overline{M}$ and therefore $\overline{H}$ can have no normal 3-subgroup either. Thus we can apply Theorem 4.8 to decompose both V and $\overline{H}$. Therefore there is an integer n such that $V = V_0 \oplus V_1 \oplus \ldots \oplus V_n$ and $H = H_1 \times \ldots \times H_n$. We have several possibilities to consider.

(i) $n = 1$. Then $V = V_0 \oplus V_1$ where V_1 has order 3, 3^2, 3^3 or 3^4 and so $\overline{H} \cong 1$, $\mathrm{SL}_2(3)$, $\mathrm{SL}_3(3)$, $\mathrm{SL}_4(3)$ or $\mathrm{Sp}_4(3)$. However H has Sylow 3-subgroups of order 3^2 and so $n \neq 1$.

(ii) $n = 2$. Then $V = V_0 \oplus V_1 \oplus V_2$ where V_1 has order 3 or 3^2 or 3^3 and V_2 has order 3 or 3^2 and so $\overline{H} \cong \mathrm{SL}_2(3) \times 1$, $\mathrm{SL}_2(3) \times \mathrm{SL}_2(3)$ or $\mathrm{SL}_3(3) \times 1$. The only possibility is $H \cong \mathrm{SL}_2(3) \times \mathrm{SL}_2(3)$ again because of the order of the Sylow 3-subgroup.

(iii) $n = 3$. Then $V = V_0 \oplus V_1 \oplus V_2 \oplus V_3$ where V_1 has order 3 or 3^2 and V_2, V_3 both have order 3. In this case $\overline{H} \cong \mathrm{SL}_2(3) \times 1 \times 1$ or $1 \times 1 \times 1$. Neither of which is possible.

(iv) $n = 4$. Then $V = V_1 \oplus V_2 \oplus V_3 \oplus V_4$ where each has order 3 and so $\overline{H} \cong 1 \times 1 \times 1 \times 1$ which cannot happen.

Therefore V can be decomposed as $V = V_1 \oplus V_2$ where V_i is a 2-dimensional $\overline{H}$-module for $i = 1, 2$ and $\overline{H} = \mathrm{SL}(V_1) \times \mathrm{SL}(V_2)$. We consider the elements, x, of order three in $\mathrm{SL}(V_1) \times \mathrm{SL}(V_2)$. There are three types.

(i) $x = a$ where $a \in \mathrm{SL}(V_1)^{\#}$. These act trivially on V_2 and fix a 1-subspace of V_1 and are all conjugate in $\mathrm{SL}(V_1)$.

(ii) $x = ab$ where $a \in \mathrm{SL}(V_1)^\#$ and $b \in \mathrm{SL}(V_2)^\#$. These act non-trivially on both V_1 and V_2 but fix a 1-subspace in both.

(iii) $x = b$ where $b \in \mathrm{SL}(V_2))^\#$. These act trivially on V_1 and fix a 1-subspace of V_2 and are all conjugate in $\mathrm{SL}(V_2)$.

Recall that $\overline{S}, \overline{T} \leqslant \overline{H}$ fix 3-dimensional subspaces of V and so have type *(i)* or *(iii)*. However $\overline{S}$ and $\overline{T}$ are non-conjugate and so, without loss of generality, we must have $\langle \overline{S}^M \rangle = \mathrm{SL}(V_1)$ and $\langle \overline{T}^M \rangle = \mathrm{SL}(V_2)$ and $\overline{H} = \langle \overline{S}^M \rangle \times \langle \overline{T}^M \rangle$. □

We now introduce a graph called a Moufang polygon. Such a graph is bipartite and contains circuits of length $2n$ for some fixed integer n as well as satisfying the so-called *Moufang condition*. Theorem B and Theorem C in this thesis rely on the classification of Moufang polygons which was completed by Jacques Tits and Richard Weiss in 2002 (see [29]).

Definition 4.10. The diameter of a graph, Δ, is n where n is the largest possible integer for which there exists vertices α and β in Δ with $d(\alpha, \beta) = n$. The girth of Δ is the smallest integer m where Δ contains a circuit of length m.

Definition 4.11. A generalized n-gon is a bipartite graph which has girth n and diameter $2n$. In particular, a generalized hexagon is a generalized 6-gon and a generalized quadrangle is a generalized 4-gon.

Definition 4.12. Let Δ be a generalized n-gon in which each vertex has valency three or more. Let $\Theta = (\alpha_0, \ldots, \alpha_n)$ be a path of length n which is contained in a circuit of length $2n$. We set U_Θ to be the stabilizer in $\mathrm{Aut}(\Delta)$ of the set of vertices $\{\Gamma(\alpha_1), \Gamma(\alpha_2), \ldots, \Gamma(\alpha_{n-1})\}$ and call U_Θ the root group corresponding to Θ. If U_Θ is transitive on $\Gamma(\alpha_n) \backslash \{\alpha_{n-1}\}$. Then Δ is said to satisfy the Moufang condition.

Let Δ be a generalized n-gon then Δ is a bipartite graph so we consider the subgroup of the automorphism group of Δ which preserves the partition. We call this group $\mathrm{Aut}^o(\Delta)$. Now let $\Theta = (\alpha_0, \alpha_1, \ldots, \alpha_n)$ be a path of $n+1$ vertices contained in an n-cycle and consider the root group U_Θ. The subgroup of $\mathrm{Aut}^o(\Delta)$ generated by all root groups is a normal subgroup of $\mathrm{Aut}^o(\Delta)$ which we call $G^\dagger$.

Theorem 4.13. *(Tits/Weiss) Let Δ be a finite generalized quadrangle or hexagon satisfying the Moufang condition. Then Δ is uniquely defined by its order. In particular, if Δ is a Moufang quadrangle with 80 vertices then $G^\dagger \cong U_4(2) \cong \mathrm{PSp}_4(3)$ and if Δ is a Moufang hexagon with 728 vertices then $G^\dagger \cong G_2(3)$.*

Proof. See section 17 and 34 in [29]. In particular pages 378-379. □

Chapter 5

An Amalgam of Type $\mathrm{PSL}_3(3)$

In [23] amalgams of type $\mathrm{PSL}_3(p^a)$ are classified when $a > 1$ and when p is an odd prime. The methods used to identify completions for $a > 1$ do not extend to the smaller cases of type $\mathrm{PSL}_3(p)$. In this chapter we describe an amalgam of type $\mathrm{PSL}_3(3)$. In $\mathrm{PSL}_3(3)$ there are two maximal parabolic subgroups which intersect at the normalizer of a Sylow 3-subgroup. The amalgam consists of these two parabolic subgroups and we will assume we have a completion of this amalgam which satisfies a 3-local condition. Under such conditions the amalgam completes to $\mathrm{PSL}_3(3)$ and also to the sporadic simple group M_{12}. We can describe the amalgam in each group as follows. Consider the action of a group $G_1 \cong \mathrm{PSL}_3(3)$ on a vector space of dimension three over a field of order three. Let $A_1 := \mathrm{Stab}_{G_1}(\langle(1,0,0)\rangle)$ and $B_1 := \mathrm{Stab}_{G_1}(\langle(1,0,0),(0,1,0)\rangle)$. Now consider the action of $G_2 \cong \mathrm{M}_{12}$ on a set of twelve points $\Omega := \{1,2,\ldots,12\}$. Let $A_2 = \mathrm{Stab}_{G_2}(\{1,2,3\})$ and $B_2 = \mathrm{Stab}_{G_2}(\{1,2,3\}\{4,5,6\}\{7,8,9\}\{10,11,12\})$. A result of Goldschmidt can be used to prove that the two amalgams $(A_1, B_1, A_1 \cap B_1)$ and $(A_2, B_2, A_2 \cap B_2)$ are isomorphic.

The two groups, $\mathrm{PSL}_3(3)$ and M_{12}, share an isomorphic amalgam and an isomorphic centralizer of a 3-central element but differ in their centralizer of an involution. We will apply the theorem of Feit and Thompson (Theorem 4.1) to the involution centralizer in an abstract finite completion of the amalgam which satisfies a 3-local condition. This, together with a result of Burnside about fixed-point-free automorphisms of order three (Lemma 1.24), will allow us to restrict the structure of the completion. Furthermore, the Burnside lemma we use will give us a particular group relation. The techniques which will be used in later chapters are not suitable in this amalgam since the subgroups are small. Instead we use a computer algebra package. We will create the subgroups which constitute the amalgam in Magma and then make the universal completion as the amalgamated free product. Factoring the universal completion by a relation forced by Lemma 1.21 and using the coset enumeration package will then confirm the only possible completions are M_{12} and $\mathrm{PSL}_3(3)$.

Hypothesis A. Let G be a finite group with subgroups $A \cong B$ such that $C := A \cap B$ contains a Sylow 3-subgroup of both A and B and such that no non-trivial normal subgroup of C is normal in both A and B. Suppose further that

(i) $G = \langle A, B \rangle$;

(ii) $A/O_3(A) \cong B/O_3(B) \cong \mathrm{GL}_2(3)$;

(iii) $O_3(A)$ and $O_3(B)$ are natural modules with respect to the actions of $A/O_3(A)$ and $B/O_3(B)$ respectively; and

(iv) for $S \in \mathrm{Syl}_3(C)$, $N_G(Z(S)) = N_A(Z(S)) = N_B(Z(S))$.

Our main theorem in this chapter is the following.

Theorem A. *If G satisfies Hypothesis A, then $G \cong \mathrm{M}_{12}$ or $\mathrm{PSL}_3(3)$.*

5.1 Some Structure of the Amalgam $(\mathbf{A}, \mathbf{B}, \mathbf{C})$

We assume Hypothesis A and define some further notation. Set $Q_A := O_3(A)$ and $Q_B := O_3(B)$.

Lemma 5.1. *The following hold.*

(*i*) $S := Q_A Q_B$ *is a normal Sylow* 3*-subgroup of* C *and* $S \cong 3^{1+2}_+$.

(*ii*) $Q_A \cap Q_B = Z(S)$.

(*iii*) $C = N_A(S) = N_B(S) = N_A(Z(S)) = N_B(Z(S)) = N_G(Z(S))$ *has index four in* A *and in* B.

(*iv*) $C_G(Z(S))$ *has index two in* C.

Proof. (*i*) If $Q_A = Q_B$ then A and B would share a normal subgroup which is not possible. Also, Sylow 3-subgroups of A and B have order 3^3 and C contains one of them so C contains Q_A and Q_B which necessarily normalize each other. Thus $S := Q_A Q_B \in \mathrm{Syl}_3(C)$ is normal in C. Now choose some $x \in Q_B \backslash Q_A$ then $1 \neq Q_A x \in A/Q_A \cong \mathrm{GL}_2(3)$. Since Q_A is a natural A/Q_A-module, $Q_A x$ acts non-trivially on Q_A. In particular, S is non-abelian. If $Z(S)$ has index three in S then we could choose any $x \in S \backslash Z(S)$ which would necessarily commute with $\langle x, Z(S) \rangle = S$ and S would be abelian. Therefore $Z(S)$ must have order three. It is then immediate that $Z(S) = S'$. Furthermore $S/Z(S) = (\frac{Q_A}{Z(S)})(\frac{Q_B}{Z(S)})$ is elementary abelian so S is extraspecial. Now since Q_A and Q_B have exponent three, it follows that $S \cong 3^{1+2}_+$.

(*ii*) Since Q_A and Q_B are not equal and have index three in S, $Q_A \cap Q_B$ has order three and is a normal subgroup of S. It is therefore central in S and so $Q_A \cap Q_B = Z(S)$.

(*iii*) The normalizer of a Sylow 3-subgroup in A is the preimage in $A/Q_A \cong \mathrm{GL}_2(3)$ of the normalizer of a Sylow 3-subgroup which has index four. Therefore the normalizer of a Sylow 3-subgroup in A (and in B) has index four. We have $N_A(S) \leqslant N_A(Z(S)) = N_B(Z(S)) \leqslant B$ and $N_B(S) \leqslant N_B(Z(S)) = N_A(Z(S)) \leqslant A$ and so $C \leqslant N_A(S), N_B(S) \leqslant A \cap B = C$ which means $C = N_A(S) + N_B(S)$ has index four in A and in B.

(iv) We have seen that $C = N_A(S) = N_B(S) \leqslant N_G(Z(S))$. Since $N_G(Z(S)) = N_A(Z(S)) = N_B(Z(S)) \leqslant A \cap B$, $C = N_G(Z(S))$. Choose $t \in A$ such that $\langle tQ_A \rangle = Z(A/Q_A)$. Then t normalizes S and so lies in C. Also t inverts the natural module Q_A and so t inverts $Z(S)$ which is not central in C. Therefore $C_C(Z(S))$ has index two in C. □

Lemma 5.2. *If $t \in A$ is an involution such that $tQ_A \in Z(A/Q_A)$ then $C_A(t) \cong \mathrm{GL}_2(3)$ and there is $x \in C_A(t)$ of order three such that $\langle x \rangle = Z(P)$ for some $P \in \mathrm{Syl}_3(B)$.*

Proof. Let $t \in A$ be an involution such that $tQ_A \in Z(A/Q_A) \cong \mathbb{Z}_2$. Then tQ_A commutes with each Sylow 3-subgroup of A/Q_A and in particular commutes with $Q_AQ_B/Q_A \cong Q_B/(Q_A \cap Q_B)$. By Lemma 2.16, there is some $x \in Q_B \backslash Q_A$ that commutes with t. Notice that A has at most 27 Sylow 2-subgroups of A and since t is in the centre of a Sylow 2-subgroup, at most 27 A-conjugates of t. However, t commutes with an element of order three, $x \in Q_B \backslash Q_A$, and so there can be at most nine A-conjugates of t in A. Moreover t inverts Q_A and so the set $t^{Q_A} = \{t^q | q \in Q_A\}$ has order nine and therefore $\langle t \rangle^{Q_A} = \langle t \rangle^A$. By a Frattini argument (Lemma 1.7), $A = N_A(\langle t \rangle)Q_A = C_A(t)Q_A$ and so by an isomorphism theorem,

$$C_A(t) \cong \frac{C_A(t)}{C_A(t) \cap Q_A} \cong \frac{C_A(t)Q_A}{Q_A} = \frac{A}{Q_A} \cong \mathrm{GL}_2(3).$$

Finally, since $x \in Q_B^\#$ and Q_B is a natural B/Q_B-module, Lemma 2.15 (ii) implies that $\langle x \rangle$ is conjugate to $Z(S)$ in B. Thus there exists $P \in \mathrm{Syl}_3(B)$ such that $\langle x \rangle = Z(P)$. □

Lemma 5.3. *Let $u \in C$ be an involution then $C_S(u)$ has order three. In particular, if u is an involution in G normalizing a Sylow 3-subgroup P of G then $|C_P(u)| = 3$.*

Proof. We can find a complement, $T \cong 2 \times 2$, to S in C by Sylow's Theorem and $TQ_A/Q_A \leqslant A/Q_A \cong \mathrm{GL}_2(3)$ and $TQ_B/Q_B \leqslant B/Q_B \cong \mathrm{GL}_2(3)$. By Lemma 2.13, any subgroup of $\mathrm{GL}_2(3)$ isomorphic to 2×2 contains the central element. So choose $t \in T$ such that $tQ_A \in Z(A/Q_A)$ and choose $s \in T$ such that $sQ_B \in Z(B/Q_B)$. We have seen that t inverts each element of Q_A and centralizes some element $x \in Q_B \backslash Q_A$. Similarly s inverts Q_B and centralizes some element $y \in Q_A \backslash Q_B$. In particular, $t \neq s$ and therefore $T = \langle t, s\rangle$. Now we see that st centralizes the group $Q_A \cap Q_B = Z(S)$ and inverts the groups $\langle x\rangle$ and $\langle y\rangle$. So suppose $C_S(st)$ had order nine. Then $S = C_S(st)\langle x\rangle = C_S(st)\langle y\rangle$ and therefore $x = zy$ for some $z \in C_S(st)$. However this implies $y^{-1}z^{-1} = x^{-1} = x^{st} = z^{st}y^{st} = zy^{-1}$ and so $[y, z] = z^2$. Therefore $z \in S' = Z(S)$ (Lemma 5.1). However this implies that $z^2 = [y, z] = 1$ and so $z = 1$ and $x = y$ which is not possible. Hence each element of $T^\#$ centralizes just an element of order three in S. □

Lemma 5.4. *Let $t \in A$ be as in Lemma 5.2 then $C_G(t)/\langle t\rangle$ contains a self-centralizing element of order three.*

Proof. We have seen that there is an element of order three, $x \in C_A(t)$, such that $\langle x\rangle$ is the centre of some Sylow 3-subgroup in B. By Lemma 5.1 (*iv*), $C_G(x)$ has order $3^3 2$ and is contained in B. More precisely, $C_G(x) = P\langle t\rangle$ for some $P \in \mathrm{Syl}_3(B)$. Now Lemma 5.3 implies that $C_P(t)$ has order three and so $C_G(x) \cap C_G(t) = \langle x, t\rangle$. Therefore $x\langle t\rangle$ is a self-centralizing element of order three in $C_G(t)/\langle t\rangle$. □

5.2 A Presentation for the Amalgam

Lemma 5.5. $A \cong B \cong \mathrm{AGL}_2(3)$

Proof. If V is a 2-dimensional vector space over $\mathrm{GF}(3)$ then $\mathrm{AGL}_2(3)$ is defined to be the set of affine transformations $\phi + w$ where $w \in V$ and $\phi \in \mathrm{GL}(V)$ and for each $v \in V$, $\phi + w : v \mapsto \phi(v) + w$. There are $9|\mathrm{GL}(V)| = 2^4 3^3$ such transformations.

Notice that by Lemma 5.2, we can choose an involution $t \in A$ such that $C_A(t) \cong \mathrm{GL}_2(3)$ and so $D := C_A(t)$ is a complement to Q_A in A. We will define a map, Θ, from A to $\mathrm{AGL}_2(3)$ as follows. Each $a \in A$ can be written uniquely as $a = bc$ where $b \in Q_A$ and $c \in D$. Now, for each $v \in Q_A \cong V$, define $\Theta(bc) : v \mapsto b(v^{c^{-1}})$. We check that Θ is a homomorphism. Let bc and b_1c_1 be in A such that $b, b_1 \in Q_A$ and $c, c_1 \in D$. There exists $b_2 \in Q_A$ such that $b_2 = cb_1c^{-1}$ and so $bcb_1c_1 = bb_2cc_1$. Therefore $\Theta(bcb_1c_1) = \Theta(bb_2cc_1)$ and for $v \in V$,

$$\Theta(bb_2cc_1)(v) = bb_2(v^{c_1^{-1}c^{-1}}) = bb_1^{c^{-1}}(v^{c_1^{-1}c^{-1}}) = b((b_1v^{c_1^{-1}})^{c^{-1}}) = \Theta(bc)(\Theta(b_1c_1)(v)).$$

So Θ is a homomorphism. Suppose $bc \in \mathrm{Ker}(\Theta)$ then for each $v \in Q_A$, $bv^{c^{-1}} = v$ and so $bv^{2c^{-1}} = v^2$. However $bv^{2c^{-1}} = b(v^{c^{-1}})^2 = b(b^{-1}v)^2 = b^{-1}v^2$ and it follows that $b = 1$. Therefore $v^c = v$ for all $v \in Q_A$. However Q_A is a natural A/Q_A-module so only the identity acts trivially (see Lemma 2.15 (iv)). Therefore the kernel of this map is trivial and since $|A| = |\mathrm{AGL}_2(3)|$, the map is an isomorphism. □

There are two faithful representations of $\mathrm{AGL}_2(3)$ in $\mathrm{PSL}_3(3)$ which we shall see.

Consider an amalgam of type (X, Y, Z) where $X \cong Y \cong \mathrm{AGL}_2(3)$ and $Z \cong N_X(S)$ where $S \in \mathrm{Syl}_3(X)$. Both X and Y have an elementary abelian normal 3-subgroup, $O_3(X)$ and $O_3(Y)$ respectively, of order 9. Suppose ϕ_1 and ϕ_2 define embeddings of Z into X and Y respectively. The image of Z in X contains $O_3(X)$ and the image of Z in Y contains $O_3(Y)$. If H is some completion of (X, Y, Z) we can ask if the corresponding images in H share the same 3-radical subgroup. We easily see instances of both possibilities and so can immediately identify at least two isomorphism classes of this amalgam. Firstly suppose $X = Y$. Such an amalgam cannot be isomorphic to the following amalgam of subgroups in $H \cong \mathrm{PSL}_3(3)$. Let H act on the vector space of dimension three over GF(3) and set

$$\begin{aligned} X &= \mathrm{Stab}_H(\langle(1,0,0)\rangle) \\ &= \left\{ \begin{pmatrix} \alpha & \beta & 0 \\ \gamma & \delta & 0 \\ \epsilon & \zeta & \eta \end{pmatrix} \middle| \alpha,\beta,\gamma,\delta,\epsilon,\zeta \in \mathrm{GF}(3), \eta = (\alpha\delta-\beta\gamma)^{-1} \in \mathrm{GF}(3)\backslash\{0\} \right\} \end{aligned}$$

and

$$\begin{aligned} Y &= \mathrm{Stab}_H\{(\langle(1,0,0),(0,1,0)\rangle)\} \\ &= \left\{ \begin{pmatrix} \eta & 0 & 0 \\ \epsilon & \alpha & \beta \\ \zeta & \gamma & \delta \end{pmatrix} \middle| \alpha,\beta,\gamma,\delta,\epsilon,\zeta \in \mathrm{GF}(3), \eta = (\alpha\delta-\beta\gamma)^{-1} \in \mathrm{GF}(3)\backslash\{0\} \right\}. \end{aligned}$$

Let $\mathcal{A}$ represent the isomorphism class of this amalgam (X,Y,Z).

Lemma 5.6. *Let $X \cong \mathrm{AGL}_2(3)$ and $Z = N_X(S)$ where $S \in \mathrm{Syl}_3(X)$. Then the following hold.*

(i) Both Z and X have trivial centres.

(ii) $C_X(Z) = 1$ and $N_X(Z) = Z$.

(iii) $Z/S \cong 2 \times 2$.

(iv) $C_Z(S) = Z(S)$

Proof. The representation of $\mathrm{AGL}_2(3)$ in $\mathrm{PSL}_3(3)$ makes checking most of these results trivial when we identify Z with the group

$$\left\{ \begin{pmatrix} \alpha & 0 & 0 \\ \delta & \beta & 0 \\ \epsilon & \zeta & \gamma \end{pmatrix} \middle| \alpha,\beta,\gamma,\delta,\epsilon,\zeta \in \mathrm{GF}(3), \alpha\beta\gamma = 1 \right\}.$$

To show $N_X(Z) = Z$ we observe that $S \trianglelefteq Z$ so $Z \leqslant N_X(Z) \leqslant N_X(S) = Z$. ◻

Lemma 5.7. *Let $X \cong \mathrm{AGL}_2(3)$ and $Z \cong N_X(S)$ where $S \in \mathrm{Syl}_3(X)$.*

(*i*) $\mathrm{Inn}(Z) \cong Z$ *and* $|\mathrm{Aut}(Z)/\mathrm{Inn}(Z)| = 2$.

(*ii*) $\mathrm{Aut}(X) = \mathrm{Inn}(X) \cong X$.

Proof. (*i*) By Lemma 5.6, Z has trivial centre so we identify $Z \cong \mathrm{Inn}(Z)$ with its image in $\mathrm{Aut}(Z)$. Let $\mathrm{Aut}(Z) \geq R > Z$ be such that R/Z has prime order q. Suppose first that $C_R(S) > C_Z(S) = Z(S)$ then $C_R(S)/C_Z(S)$ has order q. Since Z is soluble and R/Z is cyclic of prime order, R is soluble. The Fitting subgroup of R contains all nilpotent normal subgroups of R so $S \leqslant F(R)$. By Lemma 1.13, $C_R(F(R)) \leqslant F(R)$ so $F(R) \geqslant C_R(S)$. Since $F(R)$ is nilpotent, it is a direct product of its Sylow subgroups so as no element of order two in Z commutes with S, we have $F(R) \cap Z = S$. Therefore it follows that $|F(R)| = 3^3 q$. If $q \neq 3$ then R contains a normal subgroup, N say, of order q and then $[N, Z] \leqslant N \cap Z = 1$ but then N would act trivially on Z, thus $q = 3$. Let T be a Sylow 2-subgroup of Z then T acts on the normal subgroup $C_R(S)$. Moreover, this action is coprime so $C_R(S) = [C_R(S), T]C_{C_R(S)}(T)$. However $[C_R(S), T] \leqslant C_R(S) \cap Z = C_Z(S)$ and so $1 \neq C_{C_R(S)}(T)$. This means that some $x \in R \backslash Z$ is trivial on $\langle T, S\rangle = Z$ which is a contradiction. So suppose instead that $C_R(S) = C_Z(S)$. Then $R/C_R(S)$ embeds into $\mathrm{Aut}(S)$ and in particular R/S embeds into $\mathrm{Out}(S) \cong \mathrm{GL}_2(3)$ (Lemma 1.16). Now $2 \times 2 \cong Z/S \trianglelefteq R/S$ and any subgroup of $\mathrm{GL}_2(3)$ isomorphic to 2×2 is conjugate to the group of diagonal matrices (see Lemma 2.13). So we identify Z/S with the subgroup of diagonal matrices in $\mathrm{GL}_2(3)$ which sits at index two in its normalizer in $\mathrm{GL}_2(3)$. However, this implies that $q = 2$. Therefore the only prime dividing $\mathrm{Aut}(Z)/\mathrm{Inn}(Z)$ is two. So we repeat the same argument since $2 \times 2 \cong Z/S \trianglelefteq \mathrm{Aut}(Z)/S$ and so $|\mathrm{Aut}(Z)/\mathrm{Inn}(Z)| \leqslant 2$. Finally we see that $\mathrm{Aut}(Z)/\mathrm{Inn}(Z)$ has order exactly two with the following outer automorphism.

$$\alpha : \begin{pmatrix} \alpha & 0 & 0 \\ \gamma & \alpha\beta & 0 \\ \delta & \epsilon & \beta \end{pmatrix} \mapsto \begin{pmatrix} \beta & 0 & 0 \\ \epsilon\alpha & \alpha\beta & 0 \\ \gamma\epsilon - \alpha\beta\delta & \gamma\beta & \alpha \end{pmatrix}.$$

(*ii*) The centre of X is trivial so we immediately identify $X \cong \mathrm{Inn}(X)$ with its image inside $\mathrm{Aut}(X)$. Let $Q := O_3(X) \cong 3^2$ and let R be such that $\mathrm{Aut}(X) \geq R > X$ and R/X is cyclic of prime order q. By an isomorphism theorem,

$$\mathrm{Aut}(Q) \cong \mathrm{GL}_2(3) \cong \frac{X}{Q} = \frac{X}{C_X(Q)} = \frac{X}{X \cap C_R(Q)} \cong \frac{XC_R(Q)}{C_R(Q)} \leqslant \frac{R}{C_R(Q)} \hookrightarrow \mathrm{Aut}(Q).$$

So $R/C_R(Q) \cong \mathrm{GL}_2(3)$ and $C_R(Q)/Q$ must have order q. Now $C_R(Q) \trianglelefteq R$ and has order 3^2q. Suppose $q \neq 3$ then R contains a normal subgroup, N say, of order q. But then $[N, X] \leqslant N \cap X = 1$ and N acts trivially on X which is a contradiction. Hence $q = 3$ and $C_R(Q)$ is a group of order 27. Now by a Frattini argument, $R = XN_R(S)$ and by an isomorphism theorem.

$$\frac{N_R(S)}{Z} = \frac{N_R(S)}{N_R(S) \cap X} \cong \frac{R}{X} \cong C_3.$$

In particular, $N_R(S)$ normalizes Z and so $N_R(S) = N_R(Z)$. By part (i), $|\mathrm{Aut}(Z)|_3 = 3^3$ and so $|N_R(Z)/C_R(Z)|_3 \leqslant 3^3$ and it follows that 3 divides $C_R(Z)$ and so $R = X : C_R(Z)$. Now $C_R(Z) \leqslant C_R(t)$ where $t = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and $C_X(t) \cong \mathrm{GL}_2(3)$. Therefore $C_R(Z)$ normalizes $O_2(C_X(t)) \cong Q_8$ and so by coprime action we get

$$O_2(C_X(t)) = C_{O_2(C_X(t))}(C_R(Z))[O_2(C_X(t)), C_R(Z)].$$

However $C_R(Z) \leqslant C_R(Q) \trianglelefteq R$ so $[O_2(C_X(t)), C_R(Z)] \leqslant O_2(C_X(t)) \cap C_R(Q) = 1$. Thus $C_R(Z)$ commutes with $\langle Z, O_2(C_X(t))\rangle = X$ which is a contradiction. □

Lemma 5.8. *There are exactly two isomorphism classes of amalgams of type* (X, Y, Z) *with* $X \cong Y \cong \mathrm{AGL}_2(3)$ *and* $Z \cong N_X(S)$ *where* $S \in \mathrm{Syl}_3(X)$.

Proof. We will use the Goldschmidt Lemma (3.1), Lemma 5.6 and Lemma 5.7. Firstly,

$$X^* = N_{\mathrm{Aut}(X)}(Z)/C_{\mathrm{Aut}(X)}(Z) \cong N_X(Z)/C_X(Z) \cong N_X(Z) \cong Z$$

and similarly $Y^* \cong Z$ giving us exactly two (X^*, Y^*)-double cosets in $\mathrm{Aut}(C)$. Now the

Goldschmidt Lemma implies that there are exactly two isomorphism classes of amalgams of type (X, Y, Z). □

Corollary 5.9. *Suppose* $\mathcal{A}_1 = (X_1, Y_1, Z_1)$ *is an amalgam with* $X_1 \cong Y_1 \cong \mathrm{AGL}_2(3)$ *and* $Z_1 \cong N_X(S)$ *where* $S \in \mathrm{Syl}_3(X_1)$*. If* $O_3(X_1) \neq O_3(Y_1)$ *then* $\mathcal{A}_1$ *is isomorphic to* $\mathcal{A}$*.*

Proof. We have seen there are exactly two isomorphism types of this amalgam and we have seen examples of both. The first can be seen when $X_1 = Y_1$ and the second can be seen in $\mathrm{PSL}_3(3)$ which can, in particular, be characterized by the fact that the 3-radical subgroups in the two groups constituting the amalgam are distinct. □

Lemma 5.10. $(A, B, C = A \cap B)$ *is isomorphic to the amalgam* $\mathcal{A}$*.*

Proof. Lemma 5.5 gives $A \cong B \cong \mathrm{AGL}_2(3)$ and Lemma 5.1 gives that $C = N_A(S)$ for some $S \in \mathrm{Syl}_3(A)$. If $O_3(A) = O_3(B)$ then A and B would share a normal subgroup and so $O_3(A) \neq O_3(B)$ and so the amalgam (A, B, C) is isomorphic to $\mathcal{A}$. □

We can now identify our amalgam (A, B, C) with the amalgam $\mathcal{A}$ of matrices seen in $\mathrm{PSL}_3(3)$. In the following lemma we give a presentation for the universal completion of the amalgam $\mathcal{A}$.

Lemma 5.11. *Let*

$$\begin{aligned}\mathcal{R}_C &= \{a^3 = b^3 = [a,b]^3 = [a,[a,b]] = [b,[a,b]] = t^2 = u^2 = [t,u] = 1,\\ &\qquad a^u = a,\ b^u = b^{-1},\ a^t = a^{-1},\ b^t = b\},\end{aligned}$$

$$\begin{aligned}\mathcal{R}_A &= \mathcal{R}_C \cup \{p^4 = q^4 = 1,\ p^2 = q^2 = t,\ [a,b]^p = a,\ [a,b]^q = [b,a]a,\\ &\qquad p^u = p^{-1},\ p^b = pq,\ q^b = p\},\end{aligned}$$

and

$$\begin{aligned}\mathcal{R}_B &= \mathcal{R}_C \cup \{r^4 = s^4 = 1,\ r^2 = s^2 = u,\ [a,b]^r = b^{-1},\ [a,b]^s = b^{-1}[b,a],\\ &\qquad r^t = r^{-1},\ r^a = rs,\ s^a = r\}.\end{aligned}$$

Then $C \cong \langle a,b,t,u|\mathcal{R}_C\rangle$, $A \cong \langle a,b,p,q,t,u|\mathcal{R}_A\rangle$, $B \cong \langle a,b,r,s,t,u|\mathcal{R}_B\rangle$ *and* $F := \langle a,b,p,q,r,s,t,u|\mathcal{R}_A,\mathcal{R}_B\rangle$ *is the universal completion of* $\mathcal{A}$.

Proof. We make the following identifications of matrices in C to elements in the presentation.

$$a \sim \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ b \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \ t \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \ u \sim \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Therefore $\langle a,b,t,u|\mathcal{R}_C\rangle$ is a group with a quotient group isomorphic to C since the elements of C satisfy the relations. Coset enumeration using MAGMA ([4]) ensures it is isomorphic to C. Similarly if we identify

$$p \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}, \ q \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

then coset enumeration gives $\langle a,b,p,q,t,u|\mathcal{R}_A\rangle \cong \mathrm{AGL}_2(3)$ and again if we identify

$$r \sim \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}, \ s \sim \begin{pmatrix} -1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

then $\langle a,b,r,s,t,u|\mathcal{R}_B\rangle \cong \mathrm{AGL}_2(3)$. By Corollary 5.9, the amalgam

$$(\langle a,b,p,q,t,u|\mathcal{R}_A\rangle, \langle a,b,r,s,t,u|\mathcal{R}_B\rangle, \langle a,b,t,u|\mathcal{R}_C\rangle)$$

is isomorphic to $\mathcal{A}$ and so $F := \langle a,b,p,q,r,s,t,u|\mathcal{R}_A,\mathcal{R}_B\rangle$ is the universal completion of the amalgam (see [26, Thm 1 p3] for justification that F is universal). □

Recall Lemma 5.2 and Lemma 5.4 where we found an involution in A whose centralizer in A was isomorphic to $\mathrm{GL}_2(3)$. Notice that with the identifications we made in Lemma 5.11, the involution t satisfies the properties described in Lemma 5.2. For the remainder of this chapter we identify A and B with the finitely presented groups and in particular we identify $t \in A = \langle a, b, p, q, t, u | \mathcal{R}_A \rangle$ with the involution in Lemmas 5.2 and 5.4. We also identify G with some quotient of F.

Lemma 5.12. *Let G' be any faithful completion of $\mathcal{A}$ then $C_{G'}(t)$ contains two (not necessarily distinct) subgroups isomorphic to Q_8 both of which are normalized but not centralized by the group $\langle b, u \rangle \cong \mathrm{Sym}(3)$.*

Proof. It is clear from the presentation that $P := \langle p, q \rangle$ and $\langle r, s \rangle$ are quaternion groups of order eight. Notice that $u^{pr} = t$ follows from the relations $p^u = p^{-1}$ and $r^t = r^{-1}$. So $R := \langle r, s \rangle^{pr}$ is a quaternion group with central element t. It follows from the relations of $\langle a, b \rangle$ as an extraspecial group of order 27 that $[a, b]^{-1} = [a^{-1}, b]$ and so we notice that $a^{pr} = [a, b]^{p^2 r} = [a, b]^{tr} = [a^{-1}, b]^r = ([a, b]^{-1})^r = b$. Therefore $prb = apr$ and so $\langle r^{prb}, s^{prb} \rangle = \langle rs, r \rangle^{pr}$ is normalized by $\langle b \rangle$. Also $pru = pur = up^{-1}r = utpr$ and so $\langle r^{pru}, s^{pru} \rangle = \langle r^{-1}, sr \rangle^{pr}$ is normalized by $\langle u \rangle$ also. We point out that any faithful completion of the amalgam contains injective images of the groups constituting the amalgam. Therefore the groups $\langle p, q \rangle$, $\langle r, s \rangle$ and $\langle b, u \rangle$ will always have the isomorphism types claimed. $\square$

We continue to set $P = \langle p, q \rangle$ and $R = \langle x, y \rangle$, where $x = r^{pr}$ and $y = s^{pr}$.

Lemma 5.13. *$C_G(t)$ contains a nilpotent normal subgroup, N and $P, R \leqslant N$. In particular P and R generate a 2-group.*

Proof. By Lemma 5.4, we can apply Theorem 4.1 to $C_G(t)/\langle t \rangle$. Suppose $C_G(t)/\langle t \rangle \cong \mathrm{PSL}_2(7)$ then by Lemma 4.2, $C_G(t) \cong \mathrm{SL}_2(7)$ which only contains one element of order two. This is a contradiction since we know that t commutes with another involution $u \in C$. Therefore $C_G(t)/\langle t \rangle$ contains a nilpotent normal subgroup of order prime to 3. Let N be the preimage in $C_G(t)$ of this normal subgroup then $\langle t \rangle \leq N \trianglelefteq C_G(t)$ and $C_G(t)/N \cong \mathrm{Alt}(5)$ or $\mathrm{Sym}(3)$ or C_3. By Lemma 5.12, $C_G(t)$ contains the two groups $P \cong R \cong Q_8$ which are normalized in $C_G(t)$ by $\langle b, u \rangle \cong \mathrm{Sym}(3)$. We consider $P \cap N$.

Notice first that $D := P\langle b, u\rangle \cong \mathrm{GL}_2(3)$ so $O_{3'}(D) = O_2(D) = P \cong Q_8$. Also $N \cap D$ is a normal $3'$ subgroup and so $N \cap D = N \cap P$. Suppose $P \cap N = \langle t\rangle$ then

$$\left|\frac{C_G(t)}{N}\right| \geqslant \left|\frac{DN}{N}\right| = \left|\frac{D}{N \cap D}\right| = \frac{2^4 3}{2} = 2^3 3$$

which is not possible. So suppose $|P \cap N| = 4$. The group of order three, $\langle b\rangle$, in D acts regularly on $P/\langle t\rangle$ and normalizes N and so we have a contradiction since $P = \langle (P \cap N)^{\langle b\rangle}\rangle \leqslant N$. Thus $P \leqslant N$. We can argue in the same way with R since R is normalized but not centralized by $\langle b, u\rangle$. Thus $P, R \leqslant N$. Since N is a nilpotent group and P and R are 2-groups, $\langle P, R\rangle$ is a 2-group. □

We have that G is a faithful completion of the amalgam $\mathcal{A}$ so is a quotient of the universal completion F. Furthermore it contains the 2-group generated by P and R and so $\langle P, R\rangle$ satisfies the congruences described in Corollary 1.23. Therefore, for any $\alpha \in P$ and any $\beta \in R$, $[\alpha^b, \beta][\beta^b, \alpha] \in \langle t\rangle$. We make the following four sets of relations:

(i) $\mathcal{R}_1 = \{[y^b, q][q^b, y] = 1, [pq^b, x][x^b, pq] = 1\}$;

(ii) $\mathcal{R}_2 = \{[y^b, q][q^b, y] = t, [pq^b, x][x^b, pq] = 1\}$;

(iii) $\mathcal{R}_3 = \{[y^b, q][q^b, y] = 1, [pq^b, x][x^b, pq] = t\}$;

(iv) $\mathcal{R}_4 = \{[y^b, q][q^b, y] = t, [pq^b, x][x^b, pq] = t\}$.

Lemma 5.14. *$|G|$ divides 95040 or $|G|$ divides 5616.*

Proof. G is a quotient of one of the following groups

$$F_1 = \langle a, b, p, q, r, s, t, u | \mathcal{R}_A, \mathcal{R}_B, \mathcal{R}_1\rangle,$$

$$F_2 = \langle a, b, p, q, r, s, t, u | \mathcal{R}_A, \mathcal{R}_B, \mathcal{R}_2\rangle,$$

$$F_3 = \langle a, b, p, q, r, s, t, u | \mathcal{R}_A, \mathcal{R}_B, \mathcal{R}_3\rangle,$$

$$F_4 = \langle a, b, p, q, r, s, t, u | \mathcal{R}_A, \mathcal{R}_B, \mathcal{R}_4 \rangle.$$

Coset enumeration, using MAGMA ([4]), gives respective group orders of 95040, 1, 5616, 1. □

A final corollary proves Theorem A

Corollary 5.15. *$G \cong \mathrm{M}_{12}$ or $\mathrm{PSL}_3(3)$.*

Proof. Both M_{12} and $\mathrm{PSL}_3(3)$ satisfy Hypothesis A and so are completions of the amalgam $\mathcal{A}$. Therefore each must be a quotient of one of the four groups presented in the previous lemma. However the orders of the two non-trivial groups give the orders of M_{12} and $\mathrm{PSL}_3(3)$. It follows that $F_1 \cong \mathrm{M}_{12}$ and $F_3 \cong \mathrm{PSL}_3(3)$. □

Chapter 6

An Amalgam of Type $G_2(3)$

In *Local Characteristic p Completions of Weak BN-Pairs* [23] a completion of an amalgam of type $G_2(p^a)$ (odd prime p) is proven to be isomorphic to $G_2(p^a)$ under a $\mathcal{K}$-proper hypothesis and some strong p-local conditions. An amalgam of type $G_2(3)$ is an amalgam of groups comprising two maximal 3-local subgroups in $G_2(3)$ which intersect at the normalizer of a Sylow 3-subgroup. Here we will prove that a group, $\mathcal{G}$, which contains a faithful completion, G, of an amalgam of type $G_2(3)$ and satisfies a 3-local condition must be isomorphic to $G_2(3)$. We will describe the structure of this amalgam as in [23] and analyse the conjugacy classes of elements of order three which we see. This allows us to fully determine the centralizer of an involution. We consider the coset graph given by a completion of the amalgam and this will turn out to be a generalized 6-gon with 728 vertices. Thus we can appeal to the classification of generalized polygons by Tits and Weiss to recognize the uniqueness of this graph and force the completion of the amalgam to be isomorphic to $G_2(3)$. We are left to rule out the possibility of a strict containment $\mathcal{G} > G$. However knowledge of the full centralizer of an involution gives us that G is strongly embedded in $\mathcal{G}$ and a contradiction follows.

Limiting the structure of the centralizers of 3-elements and proving that exactly 5 conjugacy classes exist allows us to limit the structure of many 3-local subgroups. Thus a modular character theoretic result of Stephen Smith and Peter Tyrer proves useful and we use it on three occasions (see Theorem 4.5).

The hypothesis we will assume is:

Hypothesis B. Let $\mathcal{G}$ be a finite group with non-conjugate subgroups A_1, A_2 such that $A_{12} := A_1 \cap A_2$ contains a Sylow 3-subgroup of both A_1 and A_2 and such that no non-trivial normal subgroup of A_{12} is normal in both A_1 and A_2. Suppose further that, for $i = 1, 2$,

(i) $|O_3(A_i)| = 3^5$;

(ii) $A_i/O_3(A_i) \cong \mathrm{GL}_2(3)$;

(iii) $O_3(A_i)/Z(O_3(A_i))$ and $Z(O_3(A_i))/O_3(A_i)'$ are natural modules with respect to the action of $A_i/O_3(A_i)$;

(iv) $N_{\mathcal{G}}(O_3(A_i)') = A_i$.

The main theorem of this chapter is:

Theorem B. *Let $\mathcal{G}$ be a group satisfying Hypothesis B. Then $\mathcal{G} \cong G_2(3)$.*

6.1 The Amalgam

We assume Hypothesis B and define some further notation. Let $G := \langle A_1, A_2 \rangle \leqslant \mathcal{G}$ then G is a faithful completion of the simple amalgam (A_1, A_2, A_{12}). We can thus introduce the coset graph $\Gamma = \Gamma(G, A_1, A_2, A_{12})$ and by naming the vertices $\alpha = A_1$, $\beta = A_2 \in V(\Gamma)$ we get $G_\alpha := A_1 = \mathrm{Stab}_G(A_1)$, $G_\beta := A_2 = \mathrm{Stab}_G(A_2)$ and $G_{\alpha\beta} := A_{12} = \mathrm{Stab}_G(\{A_1, A_2\})$.

Let $\gamma \in \{\alpha, \beta\}$ and set

(i) $Q_\gamma = O_3(G_\gamma)$ - this has order 3^5 and is normal in G_γ;

(ii) $Z_\gamma = Z(Q_\gamma)$ - this is also normal in G_γ and has order 3^3 since Q_γ/Z_γ is a natural module so has order 3^2;

(iii) $Y_\gamma = Q'_\gamma$ - this has order three and is normalized by G_γ;

and choose $S_{\alpha\beta} \in \mathrm{Syl}_3(G_{\alpha\beta})$. We also introduce the following notation for the corresponding intersections $Q_{\alpha\beta} := Q_\alpha \cap Q_\beta$, $Z_{\alpha\beta} := Z_\alpha \cap Z_\beta$.

We now begin to build up an understanding of the structure of the subgroups in the amalgam $(G_\alpha, G_\beta, G_{\alpha\beta})$.

Lemma 6.1. *The following hold.*

(i) $S_{\alpha\beta} = Q_\alpha Q_\beta \trianglelefteq G_{\alpha\beta}$.

(ii) $Z_{\alpha\beta} = Z(S_{\alpha\beta}) = Y_\alpha Y_\beta$ *has order* 3^2.

(iii) *For* $\{\gamma, \delta\} = \{\alpha, \beta\}$, $Z_\gamma \leqslant Q_\delta$.

(iv) $Z_\alpha Z_\beta = Q_{\alpha\beta}$ *is elementary abelian of order* 3^4.

(v) Q_γ *has exponent* 3, *for* $\gamma \in \{\alpha, \beta\}$.

These results are from Lemma 6.5 in [23]. In the following proof we use Lemma 2.15 several times. Lemma 2.15 gives us information on the natural $\mathrm{GL}_2(3)$-module and in particular that elements of order three in G_γ/Q_γ act non-trivially on the natural module and that G_γ/Q_γ is transitive on vectors and 1-subspaces of the natural module ($\gamma \in \{\alpha, \beta\}$).

Proof. (i) We have that $Q_\alpha \neq Q_\beta$ as the amalgam is simple and so $Q_\alpha Q_\beta \in \mathrm{Syl}_3(G_{\alpha\beta})$. Moreover $Q_\alpha \trianglelefteq G_{\alpha\beta}$ and $Q_\beta \trianglelefteq G_{\alpha\beta}$ and so $Q_\alpha Q_\beta$ is normal in $G_{\alpha\beta}$ and therefore is the unique Sylow 3-subgroup of $G_{\alpha\beta}$. Thus $S_{\alpha\beta} = Q_\alpha Q_\beta$.

(ii) Notice first that both Y_α and Y_β are central in $S_{\alpha\beta}$. Also Z_α is central in Q_α and Z_β is central in Q_β and so $Z_{\alpha\beta}$ is central in $Q_\alpha Q_\beta = S_{\alpha\beta}$. Suppose $Z(S_{\alpha\beta}) \nleqslant Q_\alpha$ then $S_{\alpha\beta} = Q_\alpha Z(S_{\alpha\beta})$. However this would mean that $S_{\alpha\beta}/Q_\alpha$ acts trivially on the natural modules Q_α/Z_α and Z_α/Y_α which is not possible by Lemma 2.15 and so $Z(S_{\alpha\beta}) \leqslant Z(Q_\alpha)$ and similarly $Z(S_{\alpha\beta}) \leqslant Z(Q_\beta)$. Hence $Z(S_{\alpha\beta}) = Z_{\alpha\beta}$. Also, since the amalgam is simple, $Z_\alpha \neq Z_\beta$ and $Y_\alpha \neq Y_\beta$. Thus $Y_\alpha Y_\beta \leqslant Z(S_{\alpha\beta}) \lneqq Z_\alpha, Z_\beta$ and so we get the order 3^2.

(iii) Let $\{\gamma, \delta\} = \{\alpha, \beta\}$ and suppose that $Z_\gamma \nleqslant Q_\delta$. Then

$$Z_\gamma > Z_\gamma \cap Q_\delta \geqslant Z_\gamma \cap Z_\delta = Z(S_{\gamma\delta})$$

by (ii). Hence $Z_\gamma \cap Q_\delta = Z(S_{\gamma\delta})$ follows by considering group orders. So,

$$[Z_\gamma, Q_\delta] \leqslant Z_\gamma \cap Q_\delta = Z(S_{\gamma\delta}) \leqslant Z_\delta.$$ □

Therefore, $S_{\gamma\delta}/Q_\delta = Z_\gamma Q_\delta/Q_\delta$ acts trivially on the natural module Q_δ/Z_δ which is not possible by Lemma 2.15. Hence $Z_\gamma \leqslant Q_\delta$.

(iv) We have seen that $Q_\alpha \neq Q_\beta$ and that both subgroups have index three in $S_{\alpha\beta}$. Thus $Q_{\alpha\beta}$ has index 3^2 in $S_{\alpha\beta}$ and so has order 3^4. We have also seen that $Z_\alpha \neq Z_\beta$ and that $Z_\alpha \cap Z_\beta$ has order 3^2. So by an isomorphism theorem, $C_3 \cong Z_\beta/Z_{\alpha\beta} \cong Z_\alpha Z_\beta/Z_\alpha$ and so $Z_\alpha Z_\beta$ has order 3^4. However $Z_\alpha \leqslant Q_\alpha \cap Q_\beta$ and $Z_\beta \leqslant Q_\beta \cap Q_\alpha$ by (iii) and so $Z_\alpha Z_\beta = Q_{\alpha\beta}$. Now let $\{\gamma, \delta\} = \{\alpha, \beta\}$ and consider the cosets in Z_γ/Y_γ. Every element in the cosets $Z_{\gamma\delta}/Y_\gamma$ has order dividing three and G_γ/Q_γ is transitive on the non-identity cosets of Z_γ/Y_γ by Lemma 2.15 so every element in each coset of Z_γ/Y_γ has order dividing three. Hence Z_α and Z_β are elementary abelian. Furthermore $Z_\alpha \leqslant Q_\beta$ and $Z_\beta = Z(Q_\beta)$ by (iii) so $[Z_\alpha, Z_\beta] = 1$. Thus $Z_\alpha Z_\beta$ is elementary abelian.

(v) We have seen that $Z_\alpha Z_\beta = Q_\alpha \cap Q_\beta$ is elementary abelian. Let $\{\gamma, \delta\} = \{\alpha, \beta\}$. The elements of the cosets of $Z_\gamma Z_\delta/Z_\gamma$ have order dividing three. We have that $G_\gamma/Q_\gamma \cong$

$\mathrm{GL}_2(3)$ acts transitively on the non-trivial elements of Q_γ/Z_γ and therefore the elements of every coset of Z_γ in Q_γ have order dividing three. Hence Q_γ has exponent three.

Lemma 6.2. *(i) If $u \in Q_\alpha \backslash Q_\beta$ and $v \in Q_\beta \backslash Q_\alpha$, $[v,u,u] \neq 1 \neq [v,u,v]$.*

(ii) If $z \in S_{\alpha\beta}$ has order three, then $z \in Q_\alpha \cup Q_\beta$.

(iii) $Z_{\alpha\beta} \lneqq S'_{\alpha\beta} \lneqq Q_{\alpha\beta}$ and $S'_{\alpha\beta} \neq Z_\alpha, Z_\beta$.

(iv) The cube of any element of order nine lies in the set $\{ab | a \in Y_\alpha^{\#}, b \in Y_\beta^{\#}\}$.

Proof. (*i*) Let $u \in Q_\alpha \backslash Q_\beta$ and $v \in Q_\beta \backslash Q_\alpha$ We show that $[v,u,u] \neq 1$, the proof for $[v,u,v]$ is similar. Suppose $[v,u] \in Z_\alpha$. Since $u \in Q_\alpha$ and $v \notin Q_\alpha$, we consider the action of $Q_\alpha v \in G_\alpha/{Q_\alpha}^{\#}$ on $Z_\alpha u \in Q_\alpha/{Z_\alpha}^{\#}$. Since $[v,u] \in Z_\alpha$, $Q_\alpha v$ fixes $Z_\alpha u$. By Lemma 2.15, $Q_\alpha v$ centralizes only the subspace $Z_\alpha Z_\beta/Z_\alpha = Q_{\alpha\beta}/Z_\alpha$. Thus $u \in Q_{\alpha\beta}$ which is a contradiction since $u \notin Q_\beta$. Now suppose $[v,u,u] = 1$. Then $C_{Q_{\alpha\beta}}(u) \geqslant \langle Z_\alpha, [v,u]\rangle$ and $|\langle Z_\alpha, [v,u]\rangle| = 3^4$. Therefore u commutes with $Q_{\alpha\beta}$. So consider the action of $Q_\beta u \in G_\beta/{Q_\beta}^{\#}$ on Z_β/Y_β. Then u centralizes $Q_{\alpha\beta} \geqslant Z_\beta$ so $Q_\beta u$ acts trivially on Z_β/Y_β which is not possible and therefore $[v,u,u] \neq 1$.

(*ii*) Let $z \in S_{\alpha\beta} \backslash (Q_\alpha \cup Q_\beta)$. Since $S_{\alpha\beta} = Q_\alpha Q_\beta$, we can write $z = xy$ for $x \in Q_\alpha \backslash Q_\beta$ and $y \in Q_\beta \backslash Q_\alpha$. Both Q_α and Q_β have exponent three so x and y both have order three and hence z has order three or nine (no element of $S_{\alpha\beta}$ can order greater than nine, if $w \in S_{\alpha\beta}$ had order 27 then $S_{\alpha\beta}/Q_\alpha = \langle w\rangle Q_\alpha/Q_\alpha \cong \langle w\rangle/(\langle w\rangle \cap Q_\alpha)$ and then $\langle w\rangle \cap Q_\alpha$ would contain elements of order nine). Suppose z has order three. We will perform a calculation under this assumption for which we must first observe that $S'_{\alpha\beta} \leqslant Q_{\alpha\beta}$ since $Q_{\alpha\beta} = Q_\alpha \cap Q_\beta$ is normal in $S_{\alpha\beta}$ and has index nine. Furthermore $[S'_{\alpha\beta}, Q_\alpha] \leqslant [Q_{\alpha\beta}, Q_\alpha] \leqslant Q'_\alpha = Y_\alpha$ and similarly $[S'_{\alpha\beta}, Q_\beta] \leqslant Y_\beta$. Thus commutators of the form $[y,x,x]$ and $[y,x,y]$ are central in $S_{\alpha\beta}$. Also notice that

$$y[y,x][y,x,y] = [y,x]y \quad (*)$$

and

$$x[y,x][y,x,x] = [y,x]x \quad (**).$$

We do the following calculation.

$$\begin{aligned}
1 &= xyxyxy \\
&= x^2y([y,x]y)xy \\
&= x^2y(y[y,x][y,x,y])xy && \text{by } (*) \\
&= x^2y^2([y,x]x)y[y,x,y] \\
&= x^2y^2(x[y,x][y,x,x])y[y,x,y] && \text{by } (**) \\
&= x^2y^2x([y,x]y)[y,x,x][y,x,y] \\
&= x^2y^2x(y[y,x][y,x,y])[y,x,x][y,x,y] && \text{by } (*) \\
&= [x,y][y,x][y,x,x][y,x,y]^2 \\
&= [y,x,x][y,x,y]^2.
\end{aligned}$$

So $[y,x,x] = [y,x,y]$. However $[y,x,x] \in Y_\alpha$, $[y,x,y] \in Y_\beta$ and $Y_\alpha \cap Y_\beta = 1$. So $[y,x,x] = [y,x,y] = 1$ and this contradicts part (i). Hence z has order 3^2.

(iii) Let $u \in Q_\alpha \backslash Q_\beta$ and $v \in Q_\beta \backslash Q_\alpha$ then $[u,v,u] \neq 1$ and $[u,v,v] \neq 1$. In particular, the derived subgroup, $S'_{\alpha\beta}$ is not central in Q_α or Q_β and so is not contained in Z_α or Z_β but it does contain $Z_{\alpha\beta} = Y_\alpha Y_\beta = Q'_\alpha Q'_\beta$. Thus

$$S'_{\alpha\beta} = [Q_{\alpha\beta}\langle u,v\rangle, Q_{\alpha\beta}\langle u,v\rangle] \leqslant [Q_{\alpha\beta}, Q_{\alpha\beta}][Q_\alpha, Q_\alpha][Q_\beta, Q_\beta]\langle [u,v]\rangle = Y_\alpha Y_\beta \langle [u,v]\rangle$$

has order 3^3. It follows that $S'_{\alpha\beta}$ lies strictly between $Q_{\alpha\beta}$ and $Z_{\alpha\beta}$ but is not equal to Z_α or Z_β.

(iv) Let $z = xy$ be an element of order nine as before (where $x \in Q_\alpha \backslash Q_\beta$ and $y \in Q_\beta \backslash Q_\alpha$) then $(xy)^3 = [y,x,x][y,x,y]^2$. We have seen that $S'_{\alpha\beta} \leqslant Q_{\alpha\beta}$ and so $[y,x,x] \in [S'_{\alpha\beta}, Q_\alpha] \leqslant Q'_\alpha = Y_\alpha$ and $[y,x,y] \in [S'_{\alpha\beta}, Q_\beta] \leqslant Q'_\beta = Y_\beta$. Finally $[y,x,x] \neq 1 \neq [y,x,y]$

and so the result holds. $\square$

6.2 The Coset Graph

Recall that $\Gamma = \Gamma(G, G_\alpha, G_\beta, G_{\alpha\beta})$ is the coset graph of the amalgam where $G = \langle G_\alpha, G_\beta \rangle$.

Lemma 6.3. *The coset graph* Γ *has valency four.*

Proof. We have seen that the valency of the vertex α is given by $[G_\alpha : G_{\alpha\beta}]$ and the valency of β by $[G_\beta : G_{\alpha\beta}]$. We have seen also that $S_{\alpha\beta} \trianglelefteq G_{\alpha\beta} \leqslant N_{G_\alpha}(S_{\alpha\beta}), N_{G_\beta}(S_{\alpha\beta})$. It follows from the structure of $G_\alpha/Q_\alpha \cong G_\beta/Q_\beta \cong \mathrm{GL}_2(3)$ that both G_α and G_β have four Sylow 3-subgroups and so $G_{\alpha\beta}$ has index at least four in both G_α and G_β. By Lemma 6.2, the normalizer of $S_{\alpha\beta}$ preserves $Q_\alpha \cup Q_\beta$ as this is the set of all elements of order three in $S_{\alpha\beta}$ together with the identity. In particular this implies that $S_{\alpha\beta}$ contains no other subgroup isomorphic to $Q_\alpha \cong Q_\beta$. Therefore $N_{G_\alpha}(S_{\alpha\beta})$ normalizes Q_α and so must also normalize Q_β. Thus $N_{G_\alpha}(S_{\alpha\beta}) \leqslant N_G(Q_\beta) = G_\beta$ ($N_G(Q_\alpha) = G_\alpha$ and $N_G(Q_\beta) = G_\beta$ follow from Hypothesis B). Similarly $N_{G_\beta}(S_{\alpha\beta}) \leqslant N_G(Q_\alpha) = G_\alpha$ and so $N_{G_\alpha}(S_{\alpha\beta}) \leqslant G_\beta \cap G_\alpha$ and $N_{G_\beta}(S_{\alpha\beta}) \leqslant G_\alpha \cap G_\beta$. Therefore $G_{\alpha\beta}$ has index exactly four in both G_α and G_β and since G has two orbits on $V(\Gamma)$ with representatives α and β, we see that every vertex in Γ has valency four. $\square$

We extend our earlier notation to all groups G_λ where $\lambda \in V(\Gamma)$.

Lemma 6.4. *Let* (λ, μ, ν) *be a path of three distinct vertices in* Γ*. Then*

(i) $S_{\mu\nu} = Q_\mu Q_\nu$;

(ii) $Q_\mu = Q_{\lambda\mu} Q_{\mu\nu} = S_{\lambda\mu} \cap S_{\mu\nu}$;

(iii) $Q_{\mu\nu} = Z_\mu Z_\nu$;

(iv) $Z_\mu = Q_{\lambda\mu} \cap Q_{\mu\nu} = Z_{\lambda\mu}Z_{\mu\nu}$;

(v) $Z_{\mu\nu} = Y_\mu Y_\nu$; *and*

(vi) $Y_\mu = Z_{\lambda\mu} \cap Z_{\mu\nu}$.

Proof. (i) Since G is edge transitive, this is just Lemma 6.1 (i).

(ii) Suppose $Q_{\lambda\mu} = Q_{\mu\nu}$. Notice that $G_\mu = \langle G_{\lambda\mu}, G_{\mu\nu}\rangle$. Lemma 6.2 implies that $Q_{\alpha\beta}$ is characteristic in $S_{\alpha\beta}$ and thus normal in $G_{\alpha\beta}$. So if $Q_{\lambda\mu} = Q_{\mu\nu}$ then this group is normal in G_μ. However this is a contradiction since $Q_{\mu\nu}/Z_\mu$ is a 1-space of Q_μ/Z_μ and is not preserved by G_μ. Thus $Q_{\lambda\mu} \neq Q_{\mu\nu}$ and both groups commute modulo Z_μ and therefore normalize each other. Hence $Q_\mu = Q_{\lambda\mu}Q_{\mu\nu}$. Also $Q_\mu \leqslant S_{\lambda\mu} \cap S_{\mu\nu} = Q_\lambda Q_\mu \cap Q_\mu Q_\nu$ and $Q_{\lambda\mu} \neq Q_{\mu\nu}$ so we have $Q_\mu = S_{\lambda\mu} \cap S_{\mu\nu}$.

(iii) This is just Lemma 6.1 (iv).

(iv) Since $Q_\mu = Q_{\lambda\mu}Q_{\mu\nu}$, $Q_{\lambda\mu} \cap Q_{\mu\nu}$ has order 3^3. Since $Q_{\lambda\mu}$ and $Q_{\mu\nu}$ are both abelian groups, their intersection commutes with Q_μ. Thus $Z_\mu = Q_{\lambda\mu} \cap Q_{\mu\nu}$. Suppose $Z_{\lambda\mu} = Z_{\mu\nu}$ then $Z(S_{\lambda\mu}) = Z(S_{\mu\nu})$ is normalized by $\langle G_{\lambda\mu}, G_{\mu\nu}\rangle = G_\mu$ which leads to a contradiction as before. Thus $Z_\mu = Z_{\lambda\mu}Z_{\mu\nu}$.

(v) This is just Lemma 6.1 (ii).

(vi) We have seen that $Z_{\lambda\mu} \neq Z_{\mu\nu}$ and so this follows immediately. □

Lemma 6.5. *Let $(\alpha, \beta, \gamma, \delta)$ be a path of vertices in Γ. Then*

$$\mathbb{Z}_3 \cong S_{\alpha\beta}/Q_\alpha \cong Q_\beta/Q_{\alpha\beta} \cong Q_{\beta\gamma}/Z_\beta \cong Z_\gamma/Z_{\beta\gamma} \cong Z_{\gamma\delta}/Y_\gamma \cong Y_\delta.$$

Proof. This follows from repeated use of Lemma 6.4 and an isomorphism theorem. □

Lemma 6.6. *Given any fours group $T \leqslant G_{\alpha\beta}$ such that $G_{\alpha\beta} = S_{\alpha\beta}T$ and we can choose involutions $t_\alpha, t_\beta \in T$ such that $Q_\alpha t_\alpha \in Z(G_\alpha/Q_\alpha)$ and $Q_\beta t_\beta \in Z(G_\beta/Q_\beta)$.*

Proof. Notice that for $\gamma \in \{\alpha, \beta\}$, $G_\gamma/Q_\gamma \cong \mathrm{GL}_2(3)$ and $\mathrm{GL}_2(3)$ has a central involution. Notice also that this central involution normalizes every Sylow 3-subgroup in $\mathrm{GL}_2(3)$. Also, in $\mathrm{GL}_2(3)$ every Sylow 3-subgroup is normalized by an elementary abelian group of order four. Choose such a fours group $T \leqslant G_\gamma$ such that $G_{\alpha\beta} = S_{\alpha\beta}T$. Of course T contains three involutions and so we choose one of these, t_γ, such that $Q_\gamma t_\gamma \leqslant Z(G_\gamma/Q_\gamma)$. This will of course hold in any choice of complement, T, such that $G_{\alpha\beta} = S_{\alpha\beta}T$. □

Of course we can do a similar thing for any pair of adjacent vertices, γ, δ in Γ. Notice however that any choice of t_γ and t_δ relies on having first chosen a fours group.

Lemma 6.7. *Let γ, δ be adjacent vertices in Γ. The following hold.*

(i) t_γ *inverts all non-trivial elements in* $Q_\gamma/Q_{\gamma\delta}$, $Q_{\gamma\delta}/Z_\gamma$, $Z_\gamma/Z_{\gamma\delta}$, $Z_{\gamma\delta}/Y_\gamma$, $S_{\gamma\delta}/Q_\delta$, $Q_{\gamma\delta}/Z_\delta$, $Z_\delta/Z_{\gamma\delta}$, *and* Y_δ.

(ii) t_γ *centralizes* $S_{\gamma\delta}/Q_\gamma$, Y_γ, $Q_\delta/Q_{\gamma\delta}$ *and* $Z_{\gamma\delta}/Y_\delta$.

(iii) Given any choice of complement T' *such that* $G_{\gamma\delta} = S_{\gamma\delta}T'$, t_γ *is the unique element in* T' *centralizing* Y_γ. *Furthermore,* $t_\gamma \neq t_\delta$ *and* $T' = \langle t_\gamma, t_\delta \rangle$.

(iv) $G_\gamma = C_{G_\gamma}(Y_\gamma)\,\langle t_\delta \rangle$.

Proof. We show the results hold for $\{\gamma, \delta\} = \{\alpha, \beta\}$ and then the lemma follows by edge transitivity.

Having chosen $t_\alpha \in T \leqslant G_{\alpha\beta}$ as in Lemma 6.6 we consider the action of $Q_\alpha t_\alpha$ on Q_α. Since Q_α/Z_α and Z_α/Y_α are natural G_α/Q_α-modules, $Q_\alpha t_\alpha$ acts on these spaces as the matrix $\mathrm{Diag}(-1,-1)$ in $\mathrm{GL}_2(3)$. So $Q_\alpha t_\alpha$ inverts non-trivial elements. Now $Y_\alpha \trianglelefteq G_\alpha$ and $C_{G_\alpha}(Y_\alpha)$ has index at most two in G_α. Also G_α/Q_α contains elements of order four which square to $Q_\alpha t_\alpha$. So suppose t_α doesn't commute with Y_α then $\langle t_\alpha \rangle$ is a complement to $C_{G_\alpha}(Y_\alpha)$ in G_α. Then by correspondence $G_\alpha/Q_\alpha = (C_{G_\alpha}(Y_\alpha)/Q_\alpha) : (\langle t_\alpha \rangle Q_\alpha/Q_\alpha)$ however

$\langle t_\alpha \rangle Q_\alpha/Q_\alpha = Z(G_\alpha/Q_\alpha)$ and so we have a direct product $G_\alpha/Q_\alpha = C_{G_\alpha}(Y_\alpha)/Q_\alpha \times \langle t_\alpha \rangle Q_\alpha/Q_\alpha$ which is not possible.

Consider the following natural isomorphisms.

(*i*) $S_{\alpha\beta}/Q_\alpha = Q_\alpha Q_\beta/Q_\alpha \cong Q_\beta/Q_{\alpha\beta}$;

(*ii*) $Q_\alpha/Q_{\alpha\beta} \cong Q_\alpha Q_\beta/Q_\beta = S_{\alpha\beta}/Q_\beta$;

(*iii*) $Q_{\alpha\beta}/Z_\alpha = Z_\alpha Z_\beta/Z_\alpha \cong Z_\beta/Z_{\alpha\beta}$;

(*iv*) $Z_\alpha/Z_{\alpha\beta} \cong Z_\alpha Z_\beta/Z_\beta = Q_{\alpha\beta}/Z_\beta$;

(*v*) $Z_{\alpha\beta}/Y_\alpha = Y_\alpha Y_\beta/Y_\alpha \cong Y_\beta/(Y_\alpha \cap Y_\beta) = Y_\beta$;

(*vi*) $Y_\alpha = Y_\alpha/(Y_\alpha \cap Y_\beta) \cong Y_\alpha Y_\beta/Y_\beta = Z_{\alpha\beta}/Y_\beta$.

By Lemma 1.2 we see equivalent actions of $Q_\alpha t_\alpha$ (and of $Q_\beta t_\beta$) on naturally isomorphic groups. This is to say $Q_\alpha t_\alpha$ inverts $Q_\alpha/Q_{\alpha\beta} \cong S_{\alpha\beta}/Q_\beta$, $Q_{\alpha\beta}/Z_\alpha \cong Z_\beta/Z_{\alpha\beta}$, $Z_\alpha/Z_{\alpha\beta} \cong Q_{\alpha\beta}/Z_\beta$ and $Z_{\alpha\beta}/Y_\alpha \cong Y_\beta$ and centralizes $S_{\alpha\beta}/Q_\alpha \cong Q_\beta/Q_{\alpha\beta}$ and $Y_\alpha \cong Z_{\alpha\beta}/Y_\beta$. So (*i*) and (*ii*) hold.

Recall t_α was chosen to lie inside a fours group $T \leqslant G_{\alpha\beta}$ and such that $Q_\alpha t_\alpha \in Z(G_\alpha/Q_\alpha)$ and t_β was chosen such that $Q_\beta t_\beta \in Z(G_\beta/Q_\beta)$. Notice that t_β must centralize Y_β whereas we know t_α inverts Y_β and so $t_\alpha \neq t_\beta$ and therefore $T = \langle t_\alpha, t_\beta \rangle$. Hence $G_\beta = C_{G_\beta}(Y_\beta)\langle t_\alpha \rangle$ and in the same way t_β must invert Y_α and so $G_\alpha = C_{G_\alpha}(Y_\alpha)\langle t_\beta \rangle$. Thus (*iii*) and (*iv*) hold. $\square$

For the remainder of this chapter we will be interested in the involutions $t_\alpha \in G_\alpha$ and $t_\beta \in G_\beta$ so we will assume that we have made a fixed choice $\langle t_\alpha, t_\beta \rangle = T \leqslant G_{\alpha\beta}$.

Lemma 6.8. *T fixes a circuit in Γ.*

Proof. Consider the action of t_α on the graph Γ. We chose t_α inside $G_{\alpha\beta}$ so it certainly fixes the edge $\{\alpha, \beta\}$ in Γ. We have seen also that each vertex in Γ has valency four. Thus t_α acts on the set $\Gamma(\beta)\backslash\{\alpha\}$ which has size three. By the orbit-stabilizer theorem t_α fixes an element of this set. Let γ be the fixed vertex. We repeat the argument to see t_α fixing some other neighbour of γ, δ say. By assumption G is a finite group and so Γ has a finite number of vertices and so t_α fixes some cycle in Γ, $(\alpha, \beta, \gamma, \delta, \ldots, \alpha)$. Of course t_β also fixes some cycle $(a, \beta, \ldots, \alpha)$ and if ϵ is any vertex fixed by t_α then $\epsilon \cdot t_\beta = \epsilon \cdot t_\alpha t_\beta = \epsilon \cdot t_\beta t_\alpha$ and so t_β preserves the subgraph of Γ fixed by t_α. In particular this means we can choose the circuit $(\alpha, \beta, \gamma, \delta, \ldots, \alpha)$ to be fixed by T. □

Lemma 6.9. *Let $\Theta = (\alpha, \beta, \gamma, \delta, \ldots, \alpha)$ be a path in Γ fixed by T. Then T is a complement to $S_{\lambda\mu}$ in $G_{\lambda\mu}$ for each pair of adjacent vertices $\{\lambda, \mu\}$ in Θ furthermore, for each $\lambda \in \Theta$ if we choose $t_\lambda \in T$ as in Lemma 6.6 then $t_\alpha = t_\nu$ for each vertex ν such that $d(\alpha, \nu)$ is a multiple of three.*

Proof. Since T fixes the path Θ then T is a subgroup of each edge stabilizer $G_{\lambda\mu}$ and is therefore a complement as claimed. We have seen how to choose $t_\alpha \in T$ such that $t_\alpha \in Z(G_\alpha/Q_\alpha)$. We have seen also that $T = \langle t_\alpha, t_\beta \rangle$ and that t_α is the only choice of involution from T which centralizes Y_α. We choose t_δ in T uniquely such that it centralizes Y_δ. By Lemma 6.5, we get the natural isomorphism $S_{\alpha\beta}/Q_\alpha \cong Y_\delta$ and by Lemma 1.2, we see that t_α centralizes Y_δ and so $t_\alpha = t_\delta$. This argument holds for any vertex at distance three from α and so for any vertex at distance a multiple of three. □

We illustrate the way t_α acts in Figure 6.1 which shows how t_α acts equivalently on naturally isomorphic groups. If t_α is acting trivially on a section we label with 1 and if it is inverting a section we label with -1.

Given a path $(\alpha, \alpha+1, \alpha+2, \ldots)$ of vertices in Γ fixed by T we use Lemma 6.9 to see $t_\alpha = t_{\alpha+3n}$ for all $n \in \mathbb{Z}$.

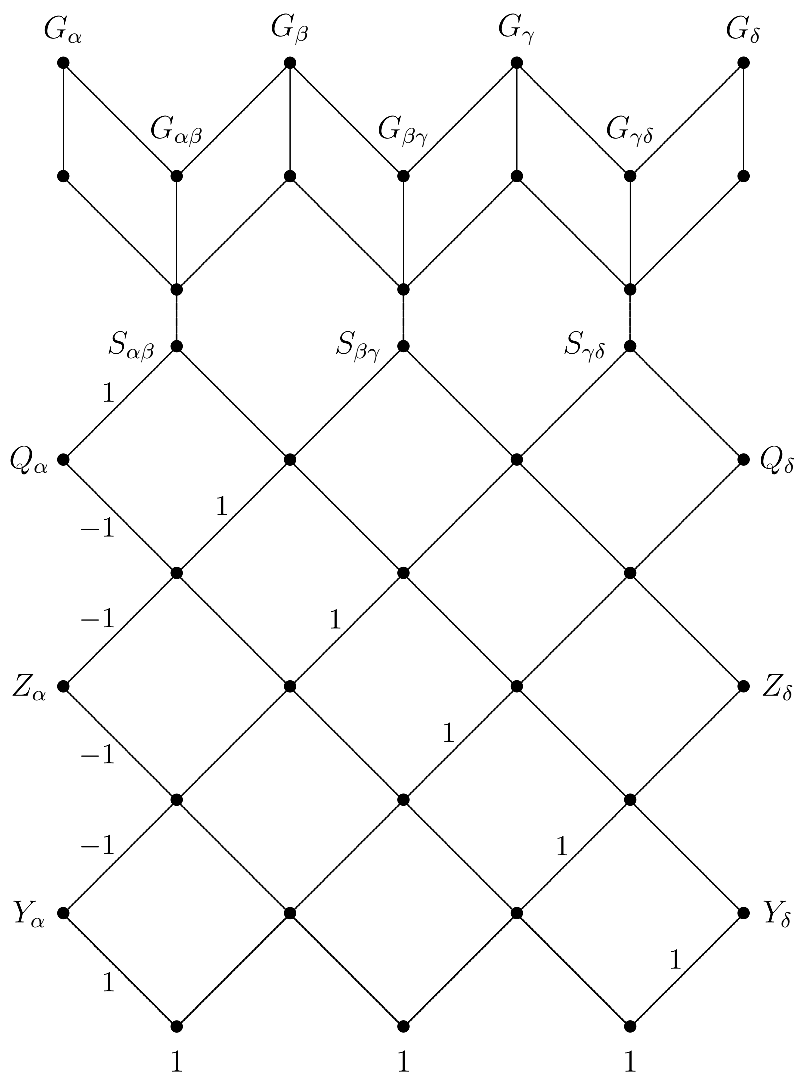


Figure 6.1: Some partial subgroup structure inside G and the action of t_α on sections.

Lemma 6.10. *The elements of $T^{\#}$ are G-conjugate.*

Proof. Let $T \leqslant S \in \mathrm{Syl}_2(G_\beta)$ then $SQ_\beta/Q_\beta \cong S$. So we consider the images of $t_\alpha Q_\beta$ and $t_\beta Q_\beta = t_{\alpha+1}Q_\beta$ in $G_\beta/Q_\beta \cong \mathrm{GL}_2(3)$. Thus we identify

$$t_\beta Q_\beta \sim \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \; t_\alpha Q_\beta \sim \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Consider $x \sim \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then $\langle t_\alpha^x \rangle Q_\beta/Q_\beta = \langle t_\alpha t_\beta \rangle Q_\beta/Q_\beta = \langle t_{\alpha+2} \rangle Q_\beta/Q_\beta$. So by Sylow's Theorem, t_α is conjugate to $t_{\alpha+2}$. By the same arguments t_β is conjugate to $t_{\alpha+3} = t_\alpha$. □

Lemma 6.11. *G is locally 7-arc transitive on Γ.*

Proof. See [7, p73 and p98] or Lemma A.4. □

Lemma 6.12. *For each vertex $\gamma \in \Gamma$ we can choose an involution $t_\gamma \in G_\gamma$ such that $C_{G_\gamma}(t_\gamma)$ has shape $3 : \mathrm{GL}_2(3)$.*

Proof. Define $t_\gamma \in G_\gamma$, as in Lemma 6.6, to be an involution such that $t_\gamma Q_\gamma \in Z(G_\gamma/Q_\gamma)$. Then t_γ is in the centre of a Sylow 2-subgroup of G_γ and also in some complement to $S_{\gamma\delta}$ in $G_{\gamma\delta}$ for each $\delta \in \Gamma(\gamma)$. We have seen that the element t_γ inverts the quotients Q_γ/Z_γ and Z_γ/Y_γ and centralizes $S_{\gamma\delta}/Q_\gamma$ and Y_γ. By Lemma 2.16, $C_{S_{\gamma\delta}}(t_\gamma) = \langle Y_\gamma, b \rangle$ for some $b \in S_{\gamma\delta} \backslash Q_\gamma$ has order 3^2 and is elementary abelian and $C_{Q_\gamma}(t_\gamma) = Y_\gamma$. Thus $C_{G_\gamma}(t_\gamma)$ has order $2^4 3^2$ and by an isomorphism theorem,

$$C_{G_\gamma}(t_\gamma)/Y_\gamma = C_{G_\gamma}(t_\gamma)/(C_{G_\gamma}(t_\gamma) \cap Q_\gamma) \cong C_{G_\gamma}(t_\gamma)Q_\gamma/Q_\gamma \leqslant G_\gamma/Q_\gamma \cong \mathrm{GL}_2(3).$$

So it follows from the order that $C_{G_\gamma}(t_\gamma)/Y_\gamma \cong \mathrm{GL}_2(3)$ and so $C_{G_\gamma}(t_\gamma) \sim 3.\mathrm{GL}_2(3)$. Finally, since the Sylow 3-subgroup is elementary abelian and therefore splits over Y_γ, $C_{G_\gamma}(t_\gamma)$ splits over Y_γ by Theorem 1.8. □

Lemma 6.13. *$O_2(C_{G_\gamma}(t_\gamma)) \cong Q_8$ is transitive on $\Gamma(\gamma)$.*

Proof. By Lemma 6.12, $\mathrm{GL}_2(3) \cong C_{G_\alpha}(t_\alpha)/Y_\alpha$. Since $\mathbb{Z}_3 \cong Y_\alpha \trianglelefteq C_{G_\alpha}(t_\alpha)$, the centralizer of Y_α in $C_{G_\alpha}(t_\alpha)$ has index at most two and since t_β inverts Y_α the index is exactly two. By Lemma 2.13, $\mathrm{GL}_2(3)$ has a unique index two subgroup and so it follows that $C_{C_{G_\alpha}(t_\alpha)}(Y_\alpha)/Y_\alpha \cong \mathrm{SL}_2(3)$. Also by Lemma 2.13, $O_2(C_{G_\alpha}(t_\alpha)/Y_\alpha) \cong Q_8$ is contained in $C_{C_{G_\alpha}(t_\alpha)}(Y_\alpha)/Y_\alpha$. Let L be the preimage in $C_{G_\alpha}(t_\alpha)$ of $O_2(C_{G_\alpha}(t_\alpha)/Y_\alpha)$ then $L \cong 3 \times Q_8$ and so it follows that $C_{G_\alpha}(t_\alpha)$ has a normal subgroup isomorphic to Q_8 and by correspondence it is the largest normal 2-subgroup. Now, this group of order eight acts on $\Gamma(\alpha)$. If any element of order four fixes a vertex in $\Gamma(\alpha)$ then we have an edge stabilizer containing elements of order four which cannot happen. Thus the action is transitive. □

Lemma 6.14. *Let* $(\alpha, \alpha+1, \alpha+2, \alpha+3)$ *be a path of vertices in* Γ *fixed by* t_α. *Let* $X := O_2(C_{G_\alpha}(t_\alpha))$ *and* $Y := O_2(C_{G_{\alpha+3}}(t_{\alpha+3}))$. *Then* $X \neq Y$ *and if* $[X, Y] = 1$ *then* Γ *is a Moufang hexagon with* 728 *vertices. In particular, if* $[X, Y] = 1$ *then* $|G| = 4245696$.

Proof. Suppose $X = Y$. Let $\gamma \in \Gamma(\alpha)$. Since X fixes α and $\alpha + 3$ and is transitive on $\Gamma(\alpha)$, we can find $x \in X$ such that $\gamma \cdot x$ has distance two from $\alpha + 3$. But G preserves distance so α and $\alpha + 3$ lie on a circuit of length six. However this is not possible since G acts 7-arc transitively on Γ.

So suppose $[X, Y] = 1$. Since $X \neq Y$, we can choose $p \in Y \backslash X$ and consider the vertex $\alpha \cdot p \neq \alpha$. This vertex has distance three from $a + 3$ and therefore distance six from α and so we will name it $\alpha + 6 = \alpha \cdot p$. Let $q \in X$ then $(\alpha+6) \cdot q = \alpha \cdot pq = \alpha \cdot qp = \alpha \cdot p = \alpha + 6$. Thus X fixes α and $\alpha+6$ and moves $\alpha+3$ and so arguing as before we see that $\alpha, \alpha+3, \alpha+6$ lie on a circuit of length 12. However $G = \langle G_\alpha, G_\beta \rangle$ acts 7-arc transitively on Γ and so every vertex is contained in a 12-cycle. Now 7-arc transitivity ensures every vertex is in a 12-cycle and so no vertex can be more than six vertices away from any other (so Γ has diameter 6 and girth 12 so is a generalized hexagon). It follows from 7-arc transitivity that the number of vertices at distance $0 - 6$ from α are $1, 4, 12, 36, 108, 324, 243$ and so Γ has 728 vertices. Since $|G_\alpha| = 2^4 3^6 = 11664$ and there are $728/2 = 364$ images of α under

G, we get $|G| = 11664 \times 364 = 4245696$ as required. Finally let $(\alpha_0, \alpha_1, \ldots, \alpha_6)$ be a path of seven vertices in Γ. Since G acts 7-arc transitively on Γ, the stabilizer of the path is transitive on $\Gamma(\alpha_6)\backslash\{\alpha_5\}$ and three divides the order of the path stabilizer. Therefore an element of order three must necessarily fix $\bigcup_{1\leqslant i\leqslant 5}\Gamma(\alpha_i)$ and so Γ satisfies the Moufang condition. □

Theorem 6.15. *Let $\alpha, \alpha+1, \alpha+2, \alpha+3$ be a path in Γ fixed by t_α. If $O_2(C_{G_\alpha}(t_\alpha))$ commutes with $O_2(C_{G_{\alpha+3}}(t_\alpha))$ then $G \cong G_2(3)$.*

Proof. By Theorem 4.13 and Lemma 6.14 the coset graph Γ is a Moufang hexagon with 728 vertices and is uniquely defined. Notice that the stabilizer of a path of length six contains a group of order three conjugate to Y_γ for $\gamma \in \{\alpha, \beta\}$. So the group $\langle Y_\gamma | \gamma \in V(\Gamma)\rangle \leqslant G^\dagger \cap G$ (where $G^\dagger$ is defined in 4.13). To see that $\langle Y_\gamma | \gamma \in V(\Gamma)\rangle = G$ we recall Lemma 6.4 which can be used to show that each Sylow 3-subgroup is contained in $\langle Y_\gamma | \gamma \in V(\Gamma)\rangle$. We have also seen that both G_α and G_β are generated by their Sylow 3-subgroups. Thus $G = \langle G_\alpha, G_\beta\rangle \leqslant \langle Y_\gamma | \gamma \in V(\Gamma)\rangle \leqslant G$. Thus $G \leqslant G^\dagger \cong G_2(3)$. Now it follows from the order of G that $G = G^\dagger \cong G_2(3)$. □

6.3 Controlling the 3-Local Structure

We have our group $\mathcal{G}$ containing a faithful completion of an amalgam $(A_1, A_2, A_{12}) = (G_\alpha, G_\beta, G_{\alpha\beta})$ of type $G_2(3)$. First we will find all conjugacy classes of elements of order three. In particular we will identify an element of order three which acts fixed-point-freely on a section of the centralizer of an involution and apply Lemma 1.25. We will use this to force two subgroups to commute and then invoke Theorem 6.15 to recognize $G_2(3)$ as the completion contained in $\mathcal{G}$. Finally we will show that this containment cannot be proper. First we require further notation.

For $\gamma \in \{\alpha, \beta\}$, set $X_\gamma = [Z_\gamma, t_\gamma]$ and choose elements y_γ such that $\langle y_\gamma \rangle = Y_\gamma$. As in Lemmas 6.6 and 6.7 we fix $T = \langle t_\alpha, t_\beta \rangle$. Set $t_{\alpha\beta} := t_\alpha t_\beta$.

We saw in Lemma 6.2 that the derived subgroup of $S_{\alpha\beta}$ lies strictly between $Q_{\alpha\beta}$ and $Z_{\alpha\beta}$ but is not equal to Z_α or Z_β. Since $Q_{\alpha\beta}$ is elementary abelian, there are four subgroups in $S_{\alpha\beta}$ lying strictly between $Q_{\alpha\beta}$ and $Z_{\alpha\beta}$ three of which are normalized by $G_{\alpha\beta}$, Z_α, Z_β and $S'_{\alpha\beta}$. Thus the fourth is necessarily normalized by $G_{\alpha\beta}$ too. Let A and B be the two subgroups distinct from Z_α and Z_β and we will not need to distinguish which is the derived subgroup of $S_{\alpha\beta}$. We will however choose an element from each. Now by Lemma 6.7, both t_α and t_β invert non-trivial elements in $Q_{\alpha\beta}/Z_{\alpha\beta}$ and both $A/Z_{\alpha\beta}$ and $B/Z_{\alpha\beta}$ are 1-dimensional subspaces so are inverted also. Thus $t_{\alpha\beta}$ centralizes them. In particular this means we can choose $a \in A \backslash Z_{\alpha\beta}$ and $b \in B \backslash Z_{\alpha\beta}$ such that $[a, t_{\alpha\beta}] = [b, t_{\alpha\beta}] = 1$ (see Lemma 2.16).

Lemma 6.16. *Let* $\{\gamma, \delta\} = \{\alpha, \beta\}$*. Then* $L_\gamma := C_{\mathcal{G}}(y_\gamma)$*, has index two in* G_γ*,* $[G_{\gamma\delta} : L_\gamma \cap G_\delta] = 2$*,* $L_\gamma \cap L_\delta = S_{\gamma\delta}$ *and* $L_\gamma/Q_\gamma \cong \mathrm{SL}_2(3)$*.*

Proof. For each vertex δ we choose t_δ as in Lemma 6.6. By Lemma 6.7, $C_{\mathcal{G}}(y_\gamma) = L_\gamma$ has index two in $N_{\mathcal{G}}(Y_\gamma) = G_\gamma$. Suppose $G_{\gamma\delta} \leqslant L_\gamma$ then $S_{\gamma\delta}$ char $G_{\gamma\delta} \trianglelefteq L_\gamma$ and so $S_{\gamma\delta}$ char L_γ. However, L_γ is normal in G_γ and so we have $S_{\gamma\delta} \trianglelefteq G_\gamma$. This contradicts that $Q_\gamma = O_3(G_\gamma)$. Thus $G_{\gamma\delta} \nleqslant L_\gamma$ and so $L_\gamma G_{\gamma\delta} = G_\gamma$. By an isomorphism theorem, $G_{\gamma\delta}/(L_\gamma \cap G_{\gamma\delta}) \cong L_\gamma G_{\gamma\delta}/L_\gamma = G_\gamma/L_\gamma$ and so $L_\gamma \cap G_{\gamma\delta}$ has index two in $G_{\gamma\delta}$. In the same way $L_\delta \cap G_{\gamma\delta}$ has index two in $G_{\gamma\delta}$. By Lemma 6.7, $t_\gamma \notin L_\delta$ but $t_\gamma \in L_\gamma \cap G_{\gamma\delta}$ so $L_\gamma \cap G_{\gamma\delta} \neq L_\delta \cap G_{\gamma\delta}$. However $L_\gamma \cap L_\delta \leqslant G_\gamma \cap G_\delta = G_{\gamma\delta}$ so $L_\gamma \cap L_\delta = L_\gamma \cap L_\delta \cap G_{\gamma\delta}$ has index four in $G_{\gamma\delta}$. Thus $L_\gamma \cap L_\delta = S_{\gamma\delta}$. Finally, L_γ/Q_γ has index 2 in $G_\gamma/Q_\gamma \cong \mathrm{GL}_2(3)$ and by Lemma 2.13 (*iii*), $\mathrm{GL}_2(3)$ has a unique subgroup at index two and therefore $L_\gamma/Q_\gamma \cong \mathrm{SL}_2(3)$. ☐

Lemma 6.17. $X_\gamma = [Z_\gamma, t_\gamma]$ *has order* 3^2*, is a complement to* Y_γ *in* Z_γ *and* $X_\gamma = \{1\} \cup \{y_\delta^g | g \in G_\gamma\}$ *for* $\{\gamma, \delta\} = \{\alpha, \beta\}$*.*

Proof. By coprime action on an abelian group, $Z_\alpha = C_{Z_\alpha}(t_\alpha) \times X_\alpha$. Recall from Lemma 6.7 that t_α centralizes Y_α and inverts Z_α/Y_α and Y_β. So $Y_\alpha \leqslant C_{Z_\alpha}(t_\alpha)$. However if this containment is strict then $C_{Z_\alpha}(t_\alpha)/Y_\alpha$ is a proper subspace of Z_α/Y_α that t_α acts trivially on which is not possible. So $C_{Z_\alpha}(t_\alpha) = Y_\alpha$. Moreover t_α inverts Y_β and so $y_\beta = [y_\beta, t_\beta] \in X_\alpha$. Now Z_α is central in Q_α, and $Q_\alpha\langle t_\alpha\rangle \trianglelefteq G_\alpha$ by correspondence so we see that $[Z_\alpha, t_\alpha] = [Z_\alpha, Q_\alpha\langle t_\alpha\rangle] \trianglelefteq G_\alpha$. Therefore $\{y_\delta^g | g \in G_\gamma\} \subseteq X_\alpha$. Lemma 6.16 implies that $C_{G_\alpha}(Y_\beta) = G_\alpha \cap L_\beta$ has index eight in G_α and so we see eight conjugates of y_β in $X_\alpha = \{1\} \cup \{y_\beta^g | g \in G_\alpha\}$. A similar argument holds for X_β. □

Lemma 6.18. *$Z_{\alpha\beta}$ contains three different $\mathcal{G}$-conjugacy classes of elements of order three and $N_\mathcal{G}(Z_{\alpha\beta}) = N_\mathcal{G}(S_{\alpha\beta}) = G_{\alpha\beta}$.*

Proof. Recall t_α inverts y_β and t_β inverts y_α so $T = \langle t_\alpha, t_\beta\rangle$ is transitive on the set $\Omega := \{y_\alpha y_\beta, y_\alpha^2 y_\beta, y_\alpha y_\beta^2, y_\alpha^2 y_\beta^2\}$. Recall also that by Lemma 6.2 *(iv)*, $S_{\alpha\beta}$ contains elements of order nine and the cube of any such element lies in Ω. Since $Z_{\alpha\beta} = Z(S_{\alpha\beta})$, we can apply Burnside's Lemma 1.9 to see that elements of $Z_{\alpha\beta}$ are conjugate in $\mathcal{G}$ only if they are conjugate in $N_\mathcal{G}(S_{\alpha\beta})$. However any element of $N_\mathcal{G}(S_{\alpha\beta})$ maps elements of order nine to elements of order nine so no element of Ω can be conjugate to y_α or y_β in $\mathcal{G}$. Also we have that y_α and y_β are both $\mathcal{G}$-conjugate to their inverses but not to each other since by Hypothesis B, G_α is not conjugate to G_β. Hence there are three $\mathcal{G}$-conjugacy classes of elements of order three in $Z_{\alpha\beta}$. In particular, any element of $\mathcal{G}$ normalizing $Z_{\alpha\beta}$ normalizes Y_α and Y_β and so lies in $G_{\alpha\beta}$. Thus $N_\mathcal{G}(Z_{\alpha\beta}) = G_{\alpha\beta}$ and since $Z_{\alpha\beta} = Z(S_{\alpha\beta})$, $N_\mathcal{G}(S_{\alpha\beta}) = G_{\alpha\beta}$. □

Recall we chose $a \in A \backslash Z_{\alpha\beta}$ and $b \in A \backslash Z_{\alpha\beta}$ such that $[a, t_{\alpha\beta}] = [b, t_{\alpha\beta}] = 1$.

Lemma 6.19. *$C_{S_{\alpha\beta}}(a) = C_{S_{\alpha\beta}}(b) = Q_{\alpha\beta}$, $|C_{G_{\alpha\beta}}(a)| = |C_{G_{\alpha\beta}}(b)| = 3^4 2$ and $|N_{G_{\alpha\beta}}(\langle a\rangle)| = |N_{G_{\alpha\beta}}(\langle b\rangle)| = 3^4 2^2$.*

Proof. We show the results for a and similar arguments work for b. By Lemma 6.7, t_α inverts the quotient $Q_{\alpha\beta}/Z_{\alpha\beta}$ and so inverts the 1-dimensional subspace $A/Z_{\alpha\beta}$. By Lemma 2.16, we can choose $a' \in A\backslash Z_{\alpha\beta}$ such that t_α inverts a'. Consider $C_{S_{\alpha\beta}}(a') \geqslant Q_{\alpha\beta}$ and suppose this containment is strict. If $Q_\alpha \leqslant C_{S_{\alpha\beta}}(a')$ then $a' \in Z(Q_\alpha) \cap A = Z_{\alpha\beta}$ which would contradict our choice of a'. So $Q_\alpha \nleqslant C_{S_{\alpha\beta}}(a')$ and similarly $Q_\beta \nleqslant C_{S_{\alpha\beta}}(a')$. So choose $x \in C_{S_{\alpha\beta}}(a')\backslash Q_{\alpha\beta}$. By Lemma 6.2, x has order nine. Since t_α inverts a', t_α normalizes $C_{S_{\alpha\beta}}(a')$ so $x^{t_\alpha} \in C_{S_{\alpha\beta}}(a')$. Now $Q_\alpha x \in S_{\alpha\beta}/Q_\alpha$ is centralized by t_α so $x^{t_\alpha}x^{-1} \in Q_\alpha \cap C_{S_{\alpha\beta}}(a') = Q_{\alpha\beta}$. Also, $Q_\beta x \in S_{\alpha\beta}/Q_\beta$ which is inverted by t_α (by Lemma 6.7) so $x^{t_\alpha}x \in Q_\beta \cap C_{S_{\alpha\beta}}(a') = Q_{\alpha\beta}$. Therefore $(x^{t_\alpha}x^{-1})^{-1}x^{t_\alpha}x = x^2 \in Q_{\alpha\beta}$ and it follows that $x \in Q_{\alpha\beta}$ which gives a contradiction. Thus $C_{S_{\alpha\beta}}(a') = Q_{\alpha\beta}$ which has index nine in $S_{\alpha\beta}$. Now we observe nine conjugates of a' in A and since a' is inverted by t_α we see a further nine. Since $A\backslash Z_{\alpha\beta}$ is a set of order 18, each element is a conjugate of a'. Thus $C_{S_{\alpha\beta}}(a) = Q_{\alpha\beta}$. Finally since a is centralized by an involution and a' is inverted by an involution and the two elements are conjugate, it follows that $|C_{G_{\alpha\beta}}(a)| = 3^4 2$ and $|N_{G_{\alpha\beta}}(\langle a \rangle)| = 3^4 2^2$. □

Lemma 6.20. $C_\mathcal{G}(Q_{\alpha\beta}) = Q_{\alpha\beta}$, $N_\mathcal{G}(Q_{\alpha\beta}) = G_{\alpha\beta}$.

Proof. Firstly by Lemmas 6.16 and 6.19,

$$C_\mathcal{G}(Q_{\alpha\beta}) \leqslant C_\mathcal{G}(y_\alpha) \cap C_\mathcal{G}(y_\beta) \cap C_\mathcal{G}(a) = L_\alpha \cap L_\beta \cap C_\mathcal{G}(a) = S_{\alpha\beta} \cap C_\mathcal{G}(a) = Q_{\alpha\beta},$$

and since $Q_{\alpha\beta}$ is abelian, $C_\mathcal{G}(Q_{\alpha\beta}) = Q_{\alpha\beta}$. Now consider $O_3(N_\mathcal{G}(Q_{\alpha\beta}))$. We have $N_\mathcal{G}(Q_{\alpha\beta}) \geqslant G_{\alpha\beta}$ and since $S_{\alpha\beta}$ is a Sylow 3-subgroup of $\mathcal{G}$, $S_{\alpha\beta} \in \mathrm{Syl}_3(N_\mathcal{G}(Q_{\alpha\beta}))$ and so $Q_{\alpha\beta} \leqslant O_3(N_\mathcal{G}(Q_{\alpha\beta})) \leqslant S_{\alpha\beta}$. Suppose $O_3(N_\mathcal{G}(Q_{\alpha\beta})) = Q_\alpha$, then $N_\mathcal{G}(Q_{\alpha\beta}) \leqslant N_\mathcal{G}(Q_\alpha) = G_\alpha$ and so $N_\mathcal{G}(Q_{\alpha\beta}) = N_{G_\alpha}(Q_{\alpha\beta})$. However $Q_{\alpha\beta}/Z_\alpha$ is 1-subspace of the natural G_α/Q_α-module, Q_α/Z_α, and the stabilizer of a 1-space has order 12. But then $N_\mathcal{G}(Q_{\alpha\beta}) = N_{G_\alpha}(Q_{\alpha\beta}) = G_{\alpha\beta}$ as claimed. Similarly if $O_3(N_\mathcal{G}(Q_{\alpha\beta})) = Q_\beta$. So suppose instead that $O_3(N_\mathcal{G}(Q_{\alpha\beta})) = Q_{\alpha\beta}$. In this case we can apply a result which followed from a theorem of McLaughlin, namely Lemma 4.9. We apply it with $M = N_{\mathcal{G}}(Q_{\alpha\beta})$, $V = Q_{\alpha\beta}$, $S = Q_\alpha/Q_{\alpha\beta}$ and $T = Q_\beta/Q_{\alpha\beta}$. This implies that $\langle Q_\alpha^{N_{\mathcal{G}}(Q_{\alpha\beta})}\rangle/Q_{\alpha\beta} \cong \mathrm{SL}_2(3)$ and $\langle Q_\beta^{N_{\mathcal{G}}(Q_{\alpha\beta})}\rangle/Q_{\alpha\beta} \cong \mathrm{SL}_2(3)$ intersect trivially and commute. This means that $\langle Q_\beta^{N_{\mathcal{G}}(Q_{\alpha\beta})}\rangle$ normalizes Q_α and then $\langle Q_\beta^{N_{\mathcal{G}}(Q_{\alpha\beta})}\rangle \leqslant G_\alpha \cap N_{\mathcal{G}}(Q_{\alpha\beta}) = G_{\alpha\beta}$. However, this implies $\langle Q_\beta^{N_{\mathcal{G}}(Q_{\alpha\beta})}\rangle/Q_{\alpha\beta} \leqslant G_{\alpha\beta}/Q_{\alpha\beta} \cong 3^2 : (2 \times 2)$, a contradiction. Therefore we get that $O_3(N_{\mathcal{G}}(Q_{\alpha\beta})) = S_{\alpha\beta}$ and $N_{\mathcal{G}}(Q_{\alpha\beta}) \leqslant N_{\mathcal{G}}(S_{\alpha\beta}) = G_{\alpha\beta}$ by Lemma 6.18. □

Lemma 6.21. $Q_{\alpha\beta} \in \mathrm{Syl}_3(C_{\mathcal{G}}(a)) \cap \mathrm{Syl}_3(C_{\mathcal{G}}(b))$ *and a is not $\mathcal{G}$-conjugate to b.*

Proof. We prove $Q_{\alpha\beta} \in \mathrm{Syl}_3(C)$ where $C := C_{\mathcal{G}}(a)$ and the same proof will work for $C_{\mathcal{G}}(b)$. Suppose $S \in \mathrm{Syl}_3(C)$ such that $Q_{\alpha\beta} < S$ then there exists some $S_0 \leqslant S$ such that $Q_{\alpha\beta} \lhd S_0$. Then $Q_{\alpha\beta} < S_0 \leqslant N_{\mathcal{G}}(Q_{\alpha\beta}) = G_{\alpha\beta}$ and S_0 is a 3-group. Thus $Q_{\alpha\beta} < S_0 \leqslant S_{\alpha\beta} \cap C = Q_{\alpha\beta}$ by Lemma 6.19. So $Q_{\alpha\beta} \in \mathrm{Syl}_3(C)$.

Suppose now that there is $g \in \mathcal{G}$ such that $a^g = b$. Then $Q_{\alpha\beta}, Q_{\alpha\beta}^g \in \mathrm{Syl}_3(C_{\mathcal{G}}(b))$ so there exists some $h \in C_{\mathcal{G}}(b)$ such that $Q_{\alpha\beta}^{gh} = Q_{\alpha\beta}$. But then $gh \in G_{\alpha\beta}$ and $a^{gh} = b$. However $G_{\alpha\beta}$ normalizes A and B and so $a^g h = b \in A \cap B = Z_{\alpha\beta}$ which contradicts our choice of a and b. □

Lemma 6.22. *Let $d \in \{a, b\}$ then $C_{\mathcal{G}}(d) \leqslant G_{\alpha\beta}$. In particular $|C_{\mathcal{G}}(d)| = |C_{G_{\alpha\beta}}(d)| = 3^4 2$ and $|N_{\mathcal{G}}(\langle d\rangle)| = |N_{G_{\alpha\beta}}(\langle d\rangle)| = 3^4 2^2$.*

Proof. We prove $C := C_{\mathcal{G}}(a) \leqslant G_{\alpha\beta}$ and the same proof will work for $C_{\mathcal{G}}(b)$. Let $R := O_{3'}(C)$ and assume $R \neq 1$. We see that R is normalized by $X_\alpha = \{1\} \cup \{{y_\beta}^{G_\alpha}\}$ as a and X_α commute. By coprime action, $R := \langle C_R(y) | y \in Z_\alpha \backslash \{1\}\rangle = \langle C_R(y_\beta^g) | g \in G_\alpha\rangle$ by Lemma 6.17. Consider $C_{\mathcal{G}}(y_\beta)^g \cap R = {L_\beta}^g \cap R$ for any $g \in G_\alpha$. Since L_β is a $\{2,3\}$-group and R has order prime to 3, this is a 2-subgroup of ${L_\beta}^g$. Recall $L_\beta/Q_\beta \cong \mathrm{SL}_2(3)$ and so any 2-subgroup of L_β is isomorphic to a subgroup of Q_8. Now $R \trianglelefteq C$ and $Q_{\alpha\beta} \leqslant C$ so $Q_{\alpha\beta}$ normalizes R. Also $Q_{\alpha\beta} \leqslant Q_\alpha = Q_\alpha^g \leqslant {L_\beta}^g$ so $Q_{\alpha\beta}$ normalizes L_β^g too. Thus $Q_{\alpha\beta}$ normalizes $L_\beta^g \cap R$. But this is isomorphic to a subgroup of Q_8 and so any subgroup normalizing it centralizes the unique involution. However, this contradicts Lemma 6.20 which says $C_{\mathcal{G}}(Q_{\alpha\beta}) = Q_{\alpha\beta}$. Hence $R = 1$.

Now, because of Lemmas 6.19 and 6.20, we can apply a corollary to the theorem of Smith and Tyrer, Corollary 4.6, to C with $Q_{\alpha\beta}$ as its Sylow 3-subgroup. If C were 3-soluble of length one then, since $O_{3'}(C) = 1$, we would have that $Q_{\alpha\beta} \trianglelefteq C \leqslant N_{\mathcal{G}}(Q_{\alpha\beta}) = G_{\alpha\beta}$ and we would be done. So let us assume not. Let $N := O^3(C)$ then C/N has order at least 3^2. Recall that a was chosen to commute with the involution $t_{\alpha\beta}$ and that $t_{\alpha\beta} = t_\alpha t_\beta$ inverts both Y_α and Y_β. Thus $t_{\alpha\beta} \in N$ and so $y_\alpha = [y_\alpha, t_\alpha], y_\beta = [y_\beta, t_\alpha] \in [Q_{\alpha\beta}, t_{\alpha\beta}] \subseteq N$ and so $Z_{\alpha\beta} \in \mathrm{Syl}_3(N)$. By Lemma 6.18, $N_{\mathcal{G}}(Z_{\alpha\beta}) = G_{\alpha\beta}$ so $N_N(Z_{\alpha\beta}) \leqslant G_{\alpha\beta} \cap C$ and so it follows from Lemma 6.19 that $\langle Z_{\alpha\beta}, t_{\alpha\beta}\rangle = N_N(Z_{\alpha\beta})$. Thus we apply Theorem 4.5 to see that N is either 3-soluble of length one or $O^3(N) \neq N$. If N has a normal $3'$-subgroup then so does C. So if N is 3-soluble of length one then $Z_{\alpha\beta} \trianglelefteq N$ and so $N = \langle Z_{\alpha\beta}, t_{\alpha\beta}\rangle$ and then $|C| = 3^4 2$ and we would be done. So suppose $O^3(N) \neq N$. Arguing as before, $t_{\alpha\beta} \in O^3(N)$ and $Z_{\alpha\beta}$ normalizes $O^3(N)$ and so it follows that $Z_{\alpha\beta} = [Z_{\alpha\beta}, t_{\alpha\beta}] \leqslant O^3(N)$ which contradicts that $O^3(N) \neq N$. Hence $C \leqslant G_{\alpha\beta}$ has order $3^4 2$.

The remaining results now follow immediately from Lemma 6.19. □

Lemma 6.23. *There are five conjugacy classes of elements of order 3 in $\mathcal{G}$ and for $\gamma \in \{\alpha, \beta\}$, Z_γ contains only elements from the conjugacy classes with representatives y_α, y_β and $y_\alpha y_\beta$.*

Proof. We have seen at least five conjugacy classes of elements of order three in $\mathcal{G}$ (with representatives y_α, y_β, $y_\alpha y_\beta$, a and b) and that any element of order three in a Sylow 3-subgroup, $S_{\alpha\beta}$, lies in $Q_\alpha \cup Q_\beta$. Thus it remains to prove that each of the 404 elements of order three in $S_{\alpha\beta}$ is in one of the known conjugacy classes.

First we look for conjugates of y_α in $S_{\alpha\beta}$. By Lemma 6.16, $C_{\mathcal{G}}(y_\alpha) \cap G_\beta = L_\alpha \cap G_\beta$ has index 8 in G_β so we see 8 conjugates y_α in Z_β. Of these 8, 6 lie outside Y_α but inside

Q_α. Since Z_β is normal in $G_{\alpha\beta}$ but not in G_α, the normalizer in G_α of Z_β has index 4 in G_α. Thus we see 4 conjugates of each of the 6 we saw already and so we have at least $4 \times 6 + 2 = 26$ conjugates of y_α in $S_{\alpha\beta}$ and similarly at least 26 conjugates of y_β.

In particular, at this point we have counted all elements of order three in Z_α. We counted 16 conjugates of y, 2 conjugates of y_α and 8 of y_β.

Now we count conjugates of $y_\alpha y_\beta =: y$. In Lemma 6.18 we saw four conjugates of y and so it follows that $C_{G_{\alpha\beta}}(y) = S_{\alpha\beta}$. We saw also that $N_{\mathcal{G}}(Z_{\alpha\beta}) = G_{\alpha\beta}$. If y commutes with some 2-element, u, in G_α then u normalizes $Z_{\alpha\beta}$ and so must be in $G_{\alpha\beta}$. However, no such element in $G_{\alpha\beta}$ commutes with y and so no 2-element in G_α (or in G_β by a similar argument) commutes with y. Thus we see 16 conjugates of y in Z_α and 16 in Z_β of which 4 are shared in $Z_{\alpha\beta}$. Of the 16 in Z_α, 12 lie outside $Z_{\alpha\beta}$ and since Z_α is not normal in G_β, each has four conjugates lying inside Q_β giving 64 conjugates in Q_β and similarly 64 in Q_β of which the 28 inside $Z_\alpha \cup Z_\beta$ are shared giving 100 in total.

Finally we count conjugates of a and conjugates of b. We have seen that $C_{\mathcal{G}}(a) = C_{\mathcal{G}}(b)$ has order $3^4 2$ and is contained in $G_{\alpha\beta}$. Therefore we see 72 conjugates in G_α and 72 in G_β of which the 18 in $Q_{\alpha\beta}$ are shared. So we have 126 conjugates of a and 126 of b.

Thus we have counted $26 + 26 + 100 + 126 + 126 = 404$ elements of order three and so can conclude that $\mathcal{G}$ has exactly five such conjugacy classes. $\square$

Notice that all conjugation we observed in this proof occurred within $G_\alpha \cup G_\beta$. So if any two elements of order three in $S_{\alpha\beta}$ are $\mathcal{G}$-conjugate then they are $\langle G_\alpha, G_\beta\rangle$-conjugate. Thus we have the following corollary.

Corollary 6.24. *Let x and y be elements of order three in $G = \langle G_\alpha, G_\beta\rangle$. Suppose x and y are $\mathcal{G}$-conjugate then there exists $g \in G$ such that $x^g = y$.*

Proof. Since x and y are elements of order three in G and G is transitive on its Sylow 3-subgroups, we can assume x and y lie in the same Sylow 3-subgroup of G. So let us assume $x, y \in S_{\alpha\beta}$. As x and y are elements of order three, $x, y \in Q_\alpha \cup Q_\beta$. In Lemma 6.23 we counted all such elements of order three and observed that all conjugacy occurred within $\langle G_\alpha, G_\beta \rangle$ and so we can find $g \in G$ such that $x^g = y$. $\square$

Lemma 6.25. *$N_{\mathcal{G}}(\langle a, b \rangle) \leqslant N_{\mathcal{G}}(\langle a \rangle) \cap N_{\mathcal{G}}(\langle b \rangle) \leqslant G_{\alpha\beta}$ and $Q_{\alpha\beta}$ is the unique Sylow 3-subgroup of $N_{\mathcal{G}}(\langle a, b \rangle)$.*

Proof. By Lemma 6.21, a is not conjugate to b so consider the set $\Omega := \{ab, a^2b^2, a^2b, ab^2\} \subseteq \langle a, b \rangle$. Each element in Ω lies in $Q_{\alpha\beta}$ but not in A or B and so must lie in Z_α or Z_β. However by Lemma 6.23, no element of Ω can be conjugate to either a or b. Thus any element normalizing $\langle a, b \rangle$ must normalize $\langle a \rangle$ and $\langle b \rangle$. By Lemma 6.22, $N_{\mathcal{G}}(\langle a \rangle) \leqslant G_{\alpha\beta}$ and $N_{\mathcal{G}}(\langle b \rangle) \leqslant G_{\alpha\beta}$ and so $N_{\mathcal{G}}(\langle a, b \rangle) \leqslant G_{\alpha\beta}$. By Lemma 6.19 and Lemma 6.22, $Q_{\alpha\beta} \leqslant N_{\mathcal{G}}(\langle a \rangle) \leqslant G_{\alpha\beta}$ and $N_{\mathcal{G}}(\langle a \rangle)$ has order $3^4 2^2$. Therefore $Q_{\alpha\beta}$ is a Sylow 3-subgroup of $N_{\mathcal{G}}(\langle a \rangle) \leqslant G_{\alpha\beta}$ and is necessarily normal. $\square$

6.4 Controlling the Centralizer of an Involution

Lemma 6.26. *Let $S \in \mathrm{Syl}_3(C_{\mathcal{G}}(t_{\alpha\beta}))$. Then S has order 3^2 and $|N_{C_{\mathcal{G}}(t_{\alpha\beta})}(S)/C_{C_{\mathcal{G}}(t_{\alpha\beta})}(S)| \leqslant 2$.*

Proof. Consider $C_{Q_{\alpha\beta}}(t_{\alpha\beta})$. By our choice of a and b, $\langle a, b \rangle \leqslant C_{Q_{\alpha\beta}}(t_{\alpha\beta})$. By Lemma 6.7, $t_{\alpha\beta} = t_\alpha t_\beta$ inverts every element in $Z_{\alpha\beta} = Y_\alpha Y_\beta$. Therefore $C_{Q_{\alpha\beta}}(t_{\alpha\beta})$ has order nine. Suppose $\langle a, b \rangle$ is not a Sylow 3-subgroup of $C_{\mathcal{G}}(t_{\alpha\beta})$ and let $S \in \mathrm{Syl}_3(C_{\mathcal{G}}(t_{\alpha\beta}))$ and suppose $\langle a, b \rangle < S$ then $\langle a, b \rangle \lhd N_S(\langle a, b \rangle) \leqslant Q_{\alpha\beta} \cap C_{\mathcal{G}}(t_{\alpha\beta})$ by Lemma 6.25. However $C_{Q_{\alpha\beta}}(t_{\alpha\beta})$ has order nine so $\langle a, b \rangle$ is a Sylow 3-subgroup. Furthermore if we set $S = \langle a, b \rangle$ then by Lemma 6.25, $N_{C_{\mathcal{G}}(t_{\alpha\beta})}(S) \leqslant N_{C_{\mathcal{G}}(t_{\alpha\beta})}(\langle a \rangle)$ and since $\langle a \rangle$ is a group of order three it is immediate that $|N_{C_{\mathcal{G}}(t_{\alpha\beta})}(\langle a \rangle)/C_{C_{\mathcal{G}}(t_{\alpha\beta})}(\langle a \rangle)| \leqslant 2$ and so $|N_{C_{\mathcal{G}}(t_{\alpha\beta})}(S)/C_{C_{\mathcal{G}}(t_{\alpha\beta})}(S)| \leqslant 2$. $\square$

Recall that t_α, t_β and $t_{\alpha\beta}$ are all conjugate in G by Lemma 6.10. So for any conjugate of t_α, the centralizer in $\mathcal{G}$ contains an element from each of the four conjugacy classes of elements of order three with representatives y_α, y_β, a, and b. From now on set $t := t_\alpha$ and $H := C_\mathcal{G}(t)$. Let $(\alpha, \beta = \alpha+1, \alpha+2, \ldots)$ be a path in Γ fixed by $\langle t_\alpha, t_\beta \rangle$. We have that $t_\alpha = t_{\alpha+3}$ and so $C_{G_\alpha}(t) \cong C_{G_{\alpha+3}}(t)$. Let $P_\alpha = O_2(C_{G_\alpha}(t)) \cong Q_8$ and $P_{\alpha+3} = O_2(C_{G_{\alpha+3}}(t)) \cong Q_8$.

Lemma 6.27. *$V := \langle y_\alpha, y_{\alpha+3} \rangle$ is a Sylow 3-subgroup of H.*

Proof. First observe that since $t = t_\alpha = t_{\alpha+3}$, $Y_\alpha, Y_{\alpha+3} \leqslant H$. We use Lemma 6.4 to see that $Y_\alpha Y_{\alpha+1} = Z_{\alpha,\alpha+1}$ and $Y_{\alpha+1} Y_{\alpha+2} = Z_{\alpha+1,\alpha+2}$ and $Y_{\alpha+2} Y_{\alpha+3} = Z_{\alpha+2,\alpha+3}$. Also we see that $Z_{\alpha,\alpha+1} Z_{\alpha+1,\alpha+2} = Z_{\alpha+1}$ and $Z_{\alpha+1,\alpha+2} Z_{\alpha+2,\alpha+3} = Z_{\alpha+2}$. Finally we see by Lemma 6.4, that $Z_{\alpha+1} Z_{\alpha+2} = Q_{\alpha+1,\alpha+2}$ and so $Y_\alpha Y_{\alpha+1} Y_{\alpha+2} Y_{\alpha+3} = Q_{\alpha+1,\alpha+2}$. In particular $Y_\alpha \neq Y_{\alpha+3}$ since $Q_{\alpha+1,\alpha+2}$ has order 3^4. Also $Y_\alpha Y_{\alpha+3} = \langle y_\alpha, y_{\alpha+3} \rangle = V$ has order 3^2 and by Lemma 6.26 is a Sylow 3-subgroup of H. $\square$

Recall that the involution $t_\beta \in H$ inverts Y_α (by Lemma 6.7) and since $t_\beta = t_{\alpha+4}$ where $\alpha + 4 \in \Gamma(\alpha+3)$, t_β inverts $Y_{\alpha+3}$ also.

Lemma 6.28. *$O_{3'}(H) = \langle P_\alpha, P_{\alpha+3} \rangle$ is a 2-group and $O_{3'}(H)/\langle t \rangle$ admits a fixed-point-free automorphism of order three.*

Proof. By Lemma 6.26, we have $|N_H(V)/C_H(V)| \leqslant 2$ but since t_β inverts V, the index is exactly 2. Since V is abelian, we can apply the theorem of Smith-Tyrer, Theorem 4.5, to H. Clearly $t_\beta \in O^3(H)$ and t_β inverts y_α and $y_{\alpha+3}$ and so $y_\alpha = [y_\alpha, t_\beta], y_{\alpha+3} = [y_{\alpha+3}, t_\beta] \in O^3(H)$. Therefore $O^3(H)$ contains a Sylow 3-subgroup and so $O^3(H) = H$. Thus H must be 3-soluble of length one. Let $R = O_{3'}(H)$. Choose $x \in S$ such that x is a conjugate of a. Then $C_\mathcal{G}(x)$ has order $3^4 2$ and so, as $t \in C_H(x)$, $|C_H(x)| \leqslant 18$. In particular, x acts fixed-point-freely on $\overline{R} := R/\langle t \rangle$. By Corollary 1.22, R is nilpotent. Let p be any prime dividing $|R|$ and let P be a Sylow p-subgroup of R. By coprime action, $P = \langle C_P(v) | v \in V^\# \rangle$. Since the centralizer of every non-trivial element of V is a

$\{2,3\}$-group, P is trivial unless $p = 2$. Thus $R = \langle C_R(v) | v \in V^\# \rangle$ is a 2-group. We have $V = \langle y_\alpha, y_{\alpha+3} \rangle$ so we consider $C_R(v)$ for each $v \in V^\#$. Firstly $C_R(y_\alpha) \leqslant L_\alpha \cap C_{G_\alpha}(t)$ and $L_\alpha \cap C_{G_\alpha}(t)$ has order at most $2^3 3^2$. Also, $C_R(y_\alpha)$ is a 2-group so has order at most eight and so $C_R(y_\alpha) \leqslant P_\alpha$ and similarly $C_R(y_{\alpha+3}) \leqslant P_{\alpha+3}$. The remaining elements in V are conjugates of a and b and so centralize just $\langle t \rangle$ in R. Therefore $R \leqslant \langle P_\alpha, P_{\alpha+3} \rangle$. Finally, since H is 3-soluble of length 1, P_α normalizes RV. Also, V normalizes P_α so by coprime action, $P_\alpha = [P_\alpha, V] C_{P_\alpha}(V) = [P_\alpha, V] \langle t_\alpha \rangle \leqslant RV$ and then $P_\alpha \leqslant R$. Similarly $P_{\alpha+3} \leqslant R$. Thus $R = \langle P_\alpha, P_{\alpha+3} \rangle$ is a 2-group. □

Lemma 6.29. *$P_\alpha P_{\alpha+3} = O_{3'}(H) \cong 2^{1+4}_+$ and $2^{1+4}_+ : 3^2 : 2 \sim C_{\mathcal{G}}(t) \leqslant \langle G_\alpha, G_\beta \rangle$.*

Proof. Applying Lemma 1.25 to $\overline{R} = O_{3'}(H)/\langle t \rangle = \langle P_\alpha, P_{\alpha+3} \rangle / \langle t \rangle$ forces $\overline{R}$ to be special of order 2^6 or elementary abelian of order 2^4. Suppose the former then R has order 2^7 and has a characteristic subgroup, Z say, of order 2^3. Recall $V = \langle y_\alpha, y_{\alpha+3} \rangle$ is a Sylow 3-subgroup of H and so normalizes Z. However it is easy to check that the automorphism group of any group of order eight does not contain a group of order nine. Thus $C_V(Z)$ must be non-trivial and so some element of order three in $V = \langle y_\alpha, y_{\alpha+3} \rangle$ commutes with a group of order eight, Z. The only possibilities are y_α, $y_{\alpha+3}$ and their inverses. Hence $Z \leqslant L_\alpha$ or $Z \leqslant L_{\alpha+3}$ and so $Z = P_\alpha$ or $Z = P_{\alpha+3}$ and then $R = \langle P_\alpha, P_{\alpha+3} \rangle$ has order less than 2^7. So we must have that $\overline{R}$ is elementary abelian. Since R contains quaternion subgroups, R is non-abelian and since $Z(R)$ is normalized by an element of order three, it must have order two or eight. However, the order cannot be eight since no abelian group of order eight has an automorphism of order three. Therefore R is extraspecial and by Corollary 1.17 and Lemma 1.18, R is the central product of P_α and $P_{\alpha+3}$. We have seen already using the theorem of Smith and Tyrer that H is 3-soluble of length 1 and so $R \trianglelefteq RV \trianglelefteq H$. By a Frattini argument $H = RVN_H(V) = R\langle V, t_\beta \rangle$. Thus $H \leqslant \langle G_\alpha, G_\beta \rangle$.

The next result now follows immediately from Theorem 6.15.

Lemma 6.30. *$\mathcal{G}$ contains a subgroup isomorphic to $G_2(3)$.*

We are left with the possibility that $\mathcal{G} > G \cong G_2(3)$ however we know enough about the structure of $\mathcal{G}$ now to rule this out. The following argument relies on the result Lemma 6.23 which implies that $\mathcal{G}$ has five conjugacy classes of elements of order three, moreover if we look only at the elements of order three in G (or any conjugate of G in $\mathcal{G}$) then we see the same conjugacy classes. So if some element of order three, x say, lies in G and in some conjugate G_1 then $C_G(x) \cong C_{G_1}(x)$.

Lemma 6.31. $\mathcal{G} \cong G_2(3)$.

Proof. Suppose $G_2(3) \cong G = \langle G_\alpha, G_\beta \rangle < \mathcal{G}$. By a Frattini argument, $N_{\mathcal{G}}(G) = G_{\alpha\beta}G = G$ so G is self-normalizing. Suppose G^g is a distinct conjugate of G for some $g \in \mathcal{G}$. Suppose further that $|G \cap G^g|$ is even. Since $G_2(3)$ contains just one conjugacy class of involutions (see, for example, [6]), we can, without loss of generality, assume $t \in G \cap G^g$. But then $t = s^g$ for some $s \in G$. Since t and s are involutions in G, they are conjugate in G, say $s^{gh} = t^h = s$ for some $h \in G$. However this implies $gh \in C_{\mathcal{G}}(s) = C_{\mathcal{G}}(t^h) \leqslant G$ and then $g \in G$ which is a contradiction. Thus G is a strongly embedded subgroup of $\mathcal{G}$. Let $x \in C_{\mathcal{G}}(t) \backslash \{1\}$. If x has order two then x is a conjugate of t and so x cannot lie in any other conjugate of G. If x has order three then x is a conjugate of y_α, y_β, a or b. In any case $C_{\mathcal{G}}(x) \leqslant G$. Suppose x lies in some other conjugate of G, $x \in G \cap G^h$ say. Thus $x = y^h$ for some $y \in G$. By Corollary 6.24, there is some $g \in G$ such that $y^{hg} = x^g = y$. Hence $hg \in C_{\mathcal{G}}(y) = C_{\mathcal{G}}(x^g) \leqslant G$ and so $h \in G$. Hence $C_{\mathcal{G}}(t)$ intersects trivially with any conjugate of G. Thus we can apply Lemma 1.30 to get that G contains an abelian subgroup, K say, of order $3^4.7.13$. In particular G contains an abelian subgroup, A say, of order 3^4. Without loss of generality we assume $A \leqslant S_{\alpha\beta}$. If $A \leqslant Q_\alpha$ and $A \leqslant Q_\beta$ then $A = Q_{\alpha\beta}$ and $[Q_{\alpha\beta}, K] = 1$ which contradicts Lemma 6.20. So we may assume that $A \nleqslant Q_\alpha$. Then $|A \cap Q_\alpha| = 3^3$ and so $A \cap X_\alpha > 1$. But then A contains a conjugate of y_β

and so K is contained in some subgroup of G conjugate to G_β which is a contradiction. So G can have no such abelian subgroup and hence $\mathcal{G} = G \cong G_2(3)$. $\square$

Chapter 7

An Amalgam of Type $\mathrm{PSp}_4(3)$

A Sylow 3-subgroup of $\mathrm{PSp}_4(3)$ is isomorphic to a Sylow 3-subgroup of Sym(9) which has order 3^4, centre of order three and for which the Thompson subgroup is elementary abelian subgroup of order 3^3. Given a Sylow 3-subgroup in $\mathrm{PSp}_4(3)$, S say, with Thompson subgroup Q, the amalgam of type $\mathrm{PSp}_4(3)$ comprises of the group A, the normalizer in $\mathrm{PSp}_4(3)$ of Q, together with B, the centralizer in $\mathrm{PSp}_4(3)$ of a 3-central element of order three. Furthermore these two 3-local subgroups intersect at C, the normalizer in $\mathrm{PSp}_4(3)$ of S. Of the three amalgams described in this thesis, this is the only one in which the two groups, A and B, comprising the amalgam are not isomorphic. Also, in the amalgams of type $\mathrm{PSL}_3(3)$ and $G_2(3)$ we observed a natural $\mathrm{GL}_2(3)$ action whereas, in the amalgam of type $\mathrm{PSp}_4(3)$, the elementary abelian subgroup Q is a faithful Sym(4)-module and we see an $\mathrm{SL}_2(3)$ action in B. We do however proceed in the same spirit as Chapter 6 since the task of recognizing $\mathrm{PSp}_4(3)$ as a completion of the amalgam, in some respects, seems to be similar. The centralizer of an involution, which we will determine some of the structure of, admits an action from an elementary abelian subgroup of order nine and the theorem of Smith-Tyrer seems well suited once again. However, things do not run as smoothly as they did in $G_2(3)$. The problem appears to be much harder and consequently we will assume more in our hypothesis. We will assume that Q normalizes no subgroup of the completion of the amalgam with order prime to 3. This is a hypothesis employed in several other characterizations of $\mathrm{PSp}_4(3)$ to be found in the literature (see for example [24] and [16]). Therefore the following theorem is certainly weaker than its predecessors. It is a necessary condition though since groups with the structure $2^6 : \mathrm{PSp}_4(3)$ and $5^6 : \mathrm{PSp}_4(3)$ can be constructed with Magma and furthermore these constructions satisfy the 3-local conditions imposed in Hypothesis C. This does however raise several interesting questions. Firstly, if Q_α normalizes some $3'$-subgroup does this force there to be a normal $3'$-subgroup as in the constructions $2^6 : \mathrm{PSp}_4(3)$ and $5^6 : \mathrm{PSp}_4(3)$? Secondly, given the appropriate 3-local conditions, what do the modules for $\mathrm{PSp}_4(3)$ look like and is it possible that we get a normal $3'$-subgroup which is not elementary abelian? To answer these question further works needs to be done perhaps involving signalizer functors. The second question is reminiscent of a theorem of Graham Higman about a group G for which $G/O_2(G) \cong \mathrm{SL}_2(2^n)$. We will discuss and prove his result in Chapter 8.

The hypothesis and theorem for this chapter are as follows.

Hypothesis C. Let A_1 and A_2 be subgroups of a finite group $G = \langle A_1, A_2 \rangle$ such that $A_{12} := A_1 \cap A_2$ contains a Sylow 3-subgroup of both A_1 and A_2. Suppose further that

(i) no non-trivial normal subgroup of A_{12} is normal in A_1 and A_2;

(ii) $A_1/O_3(A_1) \cong \mathrm{Sym}(4)$;

(iii) $A_2/O_3(A_2) \cong \mathrm{SL}_2(3)$;

(iv) $O_3(A_1)$ is elementary abelian of order 3^3 and is a faithful $A_1/O_3(A_1)$-module;

(v) $O_3(A_2)$ is extraspecial of order 3^3 and $O_3(A_2)/Z(O_3(A_2))$, is a natural $A_2/O_3(A_2)$-module;

(vi) $N_G(O_3(A_1)) = A_1$ and $N_G(Z(O_3(A_2))) = A_2$;

(*vii*) $O_3(A_1)$ normalizes no non-trivial $3'$-subgroup of G.

Theorem C. *Let G be a group satisfying Hypothesis C. Then $G \cong \mathrm{PSp}_4(3)$.*

7.1 The Amalgam

Associate the amalgam (A_1, A_2, A_{12}) to a coset graph, Γ. Let α and β be adjacent vertices in Γ and so set $A_1 = G_\alpha$, $A_2 = G_\beta$.

Let $S_{\alpha\beta} \in \mathrm{Syl}_3(G_{\alpha\beta})$, $Q_{\alpha\beta} = Q_\alpha \cap Q_\beta$, $Z_\beta = Z(Q_\beta)$.

Lemma 7.1. *The following hold in G.*

(*i*) $O_3(G_{\alpha\beta}) = S_{\alpha\beta} = Q_\alpha Q_\beta \in \mathrm{Syl}_3(G_{\alpha\beta})$.

(*ii*) *$Q_{\alpha\beta}$ has order nine and $Q_\beta \cong 3^{1+2}_+$.*

(*iii*) *$Z_\beta = Z(S_{\alpha\beta})$, $Q_\alpha = J(S_{\alpha\beta})$ are characteristic subgroups of $S_{\alpha\beta}$. $C_G(Q_\alpha) = Q_\alpha$.*

(*iv*) $S_{\alpha\beta} \in \mathrm{Syl}_3(G)$.

(*v*) $G_\beta = N_G(Z_\beta) = C_G(Z_\beta)$.

(*vi*) *$N_G(S_{\alpha\beta}) = G_{\alpha\beta}$ and $G_{\alpha\beta}$ has index 4 in both G_α and G_β.*

(*vii*) *If $z \in S_{\alpha\beta}$ has order three then $z \in Q_\alpha \cup Q_\beta$.*

(*viii*) *Q_β is characteristic in $S_{\alpha\beta}$ and $S'_{\alpha\beta} = Q_{\alpha\beta}$.*

Proof. (*i*) We have that G_α and G_β intersect at a group containing a Sylow 3-subgroup of G which has order 3^4. Also $Q_\alpha \trianglelefteq G_\alpha$ and $Q_\beta \trianglelefteq G_\beta$. Thus the product $Q_\alpha Q_\beta$ is normal in $G_{\alpha\beta}$. If $Q_\alpha = Q_\beta$ then the amalgam would not be simple and so $Q_\alpha Q_\beta$ is a Sylow 3-subgroup of $G_{\alpha\beta}$.

(*ii*) Since Q_α and Q_β have index three in $S_{\alpha\beta}$, their intersection $Q_{\alpha\beta}$ has index nine and so has order nine. In particular, the extra special group, Q_β has an elementary abelian subgroup of order nine. Since Q_β/Z_β is a natural G_β/Q_β-module, Lemma 2.15 implies that G_β is transitive on the subgroups of Q_β with order nine. Thus Q_β is extra special of $+$-type.

(*iii*) Suppose $Z(S_{\alpha\beta}) \nleqslant Q_\beta$ then $S_{\alpha\beta} = Z(S_{\alpha\beta})Q_\beta$. But then $S_{\alpha\beta}/Q_\beta \cong Z(S_{\alpha\beta})$ is a Sylow 3-subgroup of G_β/Q_β but acts trivially on the natural module Q_β/Z_β. This is a contradiction (see Lemma 2.15) and so $Z(S_{\alpha\beta}) \leqslant Q_\beta$ and so must be equal to Z_β.

Suppose $S_{\alpha\beta}$ contains another elementary abelian subgroup, A, of order 3^3. Then Q_α and A intersect at a group containing a subgroup of order 3^2 which commutes with $Q_\alpha A = S_{\alpha\beta}$. However this contradicts $Z(S_{\alpha\beta}) = Z_\beta$. Thus Q_α is the Thompson subgroup of $S_{\alpha\beta}$ and in particular is a characteristic subgroup of $S_{\alpha\beta}$.

(*iv*) Since G_α/Q_α acts faithfully on Q_α, no element commutes with all of Q_α. Also, since $C_G(Q_\alpha) \leqslant N_G(Q_\alpha) = G_\alpha$, we see that $C_G(Q_\alpha) = Q_\alpha$.

(*v*) Suppose $S_{\alpha\beta} < S \in \mathrm{Syl}_3(G)$. Then $S_{\alpha\beta} \lhd R$ for some $R \leqslant S$. However, this means $Z_\beta \lhd R \leqslant N_G(Z_\beta) = G_\beta$ which is a contradiction as $S_{\alpha\beta} \in \mathrm{Syl}_3(G_\beta)$. Thus $S_{\alpha\beta} \in \mathrm{Syl}_3(G)$.

(*vi*) Suppose that $C_G(Z_\beta) < G_\beta$ then the index must be 2. However this would give an index 2 subgroup of $G_\beta/Q_\beta \cong \mathrm{SL}_2(3)$ which is not possible.

(*vii*) The normalizer of a Sylow 3-subgroup in both $G_\alpha/Q_\alpha \cong \mathrm{Sym}(4)$ and $G_\beta/Q_\beta \cong \mathrm{SL}_2(3)$ has index 4. Thus by correspondence the same holds in G_α and G_β. Now $S_{\alpha\beta} \trianglelefteq G_{\alpha\beta}$ and so $G_{\alpha\beta}$ has index at least 4 in both G_α and G_β. Since $Z(S_{\alpha\beta}) = Z_\beta$, $N_G(S_{\alpha\beta}) \leqslant N_G(Z_\beta) = G_\beta$. Thus $N_{G_\alpha}(S_{\alpha\beta}) \leqslant G_{\alpha\beta}$ and it follows that $G_{\alpha\beta}$ has exactly index 4 in G_α and so order $3^4 2$. But then $G_{\alpha\beta}$ must have index 4 in G_β also and $N_G(S_{\alpha\beta}) = G_{\alpha\beta}$. □

Lemma 7.2. (*i*) *If $z \in S_{\alpha\beta}$ has order three then $z \in Q_\alpha \cup Q_\beta$.*

(*ii*) *Q_β is characteristic in $S_{\alpha\beta}$ and $S'_{\alpha\beta} = Q_{\alpha\beta}$.*

Proof. (*i*) We have that $S_{\alpha\beta} = Q_\alpha Q_\beta$ so any element in $S_{\alpha\beta} \backslash (Q_\alpha \cup Q_\beta)$ has the form yx where $y \in Q_\beta \backslash Q_\alpha$ and $x \in Q_\alpha \backslash Q_\beta$. Notice that $S'_{\alpha\beta} \leqslant Q_\alpha$ and so $[x, y, x] = 1$ as Q_α is abelian. Suppose $[y, x, y] = 1$, then the element $Q_\alpha y \in G_\alpha / Q_\alpha$ acting on Q_α fixes the 1-space $\langle [y, x] \rangle$. By Lemma 2.17, $Q_\alpha y$ can fix just a 1-space but it already fixes the space Z_β and so we must have $Z_\beta = \langle [y, x] \rangle$.

We also have that $Q_\beta x \in G_\beta / Q_\beta$ acts on Q_β / Z_β and since the action of G_β / Q_β on this module is natural, we see that $Q_\beta x$ fixes precisely the 1-subspace $Q_{\alpha\beta}/Z_\beta$. However, $y \notin Q_{\alpha\beta}$ and $Q_\beta x$ fixes the space $Z_\beta y$ since $[y, x] \in Z_\beta$. This is a contradiction. Thus $[y, x, y] \neq 1$ and $[y, x] \notin Z_\beta$.

Now suppose yx as order three. We use the relations $x[x, y][x, y, x] = [x, y]x$ and $y[x, y][x, y, y] = [x, y]y$ together with $[x, y, x] = 1$ in the following calculations. Also we use that $x \in Q_\alpha$ and so commutes with all commutators. Hence,

$$
\begin{aligned}
1 &= yxyxyx \\
&= y^2x[x, y]xyx \\
&= y^2x^2[x, y][x, y, x]yx \\
&= y^2x^2[x, y]yx \\
&= y^2x^2y[x, y][x, y, y]x \\
&= y^2x^2y[x, y]x[x, y, y] \\
&= y^2x^2yx[x, y][x, y, x][x, y, y] \\
&= y^2x^2yx[x, y][x, y, y] \\
&= [y, x][x, y][x, y, y] \\
&= [x, y, y].
\end{aligned}
$$

Which gives a contradiction. Thus yx has order nine.

(*ii*) If $S_{\alpha\beta}$ contained another extraspecial subgroup of exponent three then we could choose some non-central element of order three inside it that would not be in $Q_\alpha \cup Q_\beta$ and that is not possible. Thus Q_β is a characteristic subgroup. Now $Q_{\alpha\beta} = Q_\alpha \cap Q_\beta$ is a normal subgroup of $S_{\alpha\beta}$ and so $S'_{\alpha\beta} \leqslant Q_{\alpha\beta}$. Suppose the containment was strict then $S_{\alpha\beta}$ would have order three and would be a central subgroup of $S_{\alpha\beta}$ which would mean $S'_{\alpha\beta} = Z_\beta$. However we have seen already that with x and y as before, $[x, y] \nleq Z_\beta$. Thus $Z_\beta \neq S'_{\alpha\beta}$ and so $S'_{\alpha\beta} = Q_{\alpha\beta}$. □

7.2 The Coset Graph

Lemma 7.3. *The coset graph Γ has valency four.*

Proof. We have seen that the valency of the vertex α is given by $[G_\alpha : G_{\alpha\beta}]$ and the valency of β by $[G_\beta : G_{\alpha\beta}]$ both of which are four by Lemma 7.1. Since G has two orbits on $V(\Gamma)$ with representatives α and β, we see that every vertex in Γ has valency four. □

Lemma 7.4. (*i*) *There is an involution $t_\beta \in G_\beta$ such that $G_{\alpha\beta} = S_{\alpha\beta}\langle t_\beta \rangle$ and $Q_\beta t_\beta \in Z(G_\beta/Q_\beta)$.*

(*ii*) *t_β fixes a circuit $\Theta = (\alpha, \beta, \ldots, \alpha)$ in Γ.*

(*iii*) *For each vertex $\gamma \in \Theta$ lying in the same G-orbit as β, $Q_\gamma t_\beta \in Z(G_\gamma/Q_\gamma)$.*

Proof. Notice that the centre of $G_\beta/Q_\beta \cong \mathrm{SL}_2(3)$ has order two and that the central involution normalizes each Sylow 3-subgroup in G_β/Q_β. So choose an element of order two, t_β, as a coset representative such that $Q_\beta\langle t_\beta \rangle/Q_\beta = Z(G_\beta/Q_\beta)$. Since $t_\beta \in G_{\alpha\beta} = N_{G_\beta}(S_{\alpha\beta})$, t_β fixes the edge $\{\alpha, \beta\}$ in Γ and since every vertex has valency four it follows that t_β fixes a circuit in Γ. In particular, this means for any vertex $\gamma \in \Theta$ lying in the same G-orbit as β, $t_\beta \in G_\gamma$ and furthermore t_β normalizes a Sylow 3-subgroup of G_γ and so $Q_\gamma t_\beta \in Z(G_\gamma/Q_\gamma)$ as before. □

Lemma 7.5. *G is locally 5-arc transitive on Γ.*

Proof. See [7, p73 and p98]. □

Lemma 7.6. *$C_{Q_\beta}(t_\beta) = Z_\beta$, $3 \times 3 \cong C_{S_{\alpha\beta}}(t_\beta) \leqslant Q_\alpha$ and $C_{G_\beta}(t_\beta) \cong 3 \times \mathrm{SL}_2(3)$.*

Proof. By the choice of t_β, we have that $Q_\beta t_\beta \in Z(G_\beta/Q_\beta)$ and so t_β is in the centre of a Sylow 2-subgroup of G_β. Also t_β centralizes Z_β and $S_{\alpha\beta}/Q_\beta$. Clearly $C_{Q_\beta}(t_\beta) = Z_\beta$ else we have a non-trivial subgroup of Q_β/Z_β centralized by t_β which contradicts that this group is a natural Q_β/Z_β-module. By Lemma 2.16, we can choose some $x \in Q_\alpha \backslash Q_\beta$ such that t_β commutes with x. Hence $C_{S_{\alpha\beta}}(t_\beta) = \langle x, Z_\beta \rangle \leqslant Q_\alpha$ is elementary abelian of order nine. Consider the set $t_\beta^{G_\beta} = \{t_\beta^g | g \in G_\beta\}$. Since G_β has at most 3^4 Sylow 2-subgroups and t_β is in the centre of one of them, this set has order at most 3^4. However t_β commutes with a group of order nine, $\langle Z_\beta, x \rangle$ so it follows this set has order at most nine and so $\langle t_\beta \rangle^{G_\beta} = \langle t_\beta \rangle^{Q_\beta}$. Now by a Frattini argument (Lemma 1.7), $G_\beta = C_{G_\beta}(t_\beta)Q_\beta$ and by an isomorphism theorem,

$$C_{G_\beta}(t_\beta)/Z_\beta = C_{G_\beta}(t_\beta)/(C_{G_\beta}(t_\beta) \cap Q_\beta) \cong C_{G_\beta}(t_\beta)Q_\beta/Q_\beta = G_\beta/Q_\beta \cong \mathrm{SL}_2(3).$$

The element $\langle x \rangle$ gives a complement to Z_β in $C_{S_{\alpha\beta}}(t_\beta)$ and so by Gaschütz's Theorem (Theorem 1.8), $C_{G_\beta}(t_\beta)$ splits over Z_β and so $C_{G_\beta}(t_\beta) \cong 3 \times \mathrm{SL}_2(3)$. □

At this point we recognize that $C_{G_\beta}(t_\beta)$ has a normal subgroup, X say, isomorphic to $\mathrm{SL}_2(3)$. Therefore $Q_8 \cong O_2(X) = O_2(C_{G_\beta}(t_\beta))$. Also, if γ is a vertex fixed by t_β at distance two from β then $Q_\gamma t_\beta \in Z(G_\gamma/Q_\gamma)$ by Lemma 7.4 and so it follows that $C_{G_\gamma}(t_\beta) \cong 3 \times \mathrm{SL}_2(3)$ and so $Q_8 \cong O_2(C_{G_\gamma}(t_\beta))$ also.

Lemma 7.7. *Let (γ, α, β) be a path of vertices in Γ fixed by t_β. Let $X := O_2(C_{G_\beta}(t_\beta))$ and $Y := O_2(C_{G_\gamma}(t_\beta))$. Then $X \neq Y$ and if $[X, Y] = 1$ then Γ is a Moufang quadrangle with 80 vertices. In particular, if $[X, Y] = 1$ then $|G| = 25920$.*

Proof. Suppose $X = Y$. Each $x \in X$ fixes β and γ. Notice, edge stabilizers have order $3^4 2$ so do not contain elements of order four so if $x \in X$ has order four then x does not fix α. So there are elements in X which fix β and γ but move α. Therefore Γ must contain a four cycle however this is impossible since G acts 5-arc transitively on Γ.

Since $X \neq Y$, we can choose $p \in Y \backslash X$ and consider the vertex $\beta \cdot p \neq \beta$. This vertex has distance two from γ and therefore distance four from β. Let $q \in X$ then $\beta \cdot pq = \beta \cdot qp = \beta \cdot p$. Thus X fixes β and $\beta \cdot p$ and moves γ and so arguing as before we see that $\beta, \gamma, \beta \cdot p$ lie on a circuit of length 8. However, $G = \langle G_\alpha, G_\beta \rangle$ acts 5-arc transitively on Γ and so every vertex is contained in an 8-cycle and no vertex can be more than four vertices away from any other (so Γ has diameter 4 and girth 8). The number of vertices at distance $0-4$ from α are $1, 4, 12, 36, 27$ and so Γ has 80 vertices. Since $|G_\alpha| = 2^3 3^4 = 648$ and there are $80/2 = 40$ images of α under G, we get $|G| = 40 \times 648 = 25920$ as required. Finally let $(\alpha_0, \alpha_1, \alpha_2, \alpha_3, \alpha_4)$ be a path of five vertices in Γ. Since G acts 5-arc transitively on Γ, the stabilizer of the path is transitive on $\Gamma(\alpha_4) \backslash \{\alpha_3\}$ and so we must have three dividing the stabilizer of the path. Therefore an element of order three must necessarily fix $\bigcup_{1 \leqslant i \leqslant 3} \Gamma(\alpha_i)$ and so Γ satisfies the Moufang condition. □

Theorem 7.8. *Let γ, α, β be a path in Γ fixed by t_β. If $O_2(C_{G_\beta}(t_\beta))$ commutes with $O_2(C_{G_\gamma}(t_\beta))$ then $G \cong \mathrm{PSp}_4(3)$.*

Proof. By Theorem 4.13 and Lemma 7.7, the coset graph Γ is a Moufang quadrangle with 80 vertices and is uniquely defined. Notice that the stabilizer of the path of length three, $\gamma, \alpha, \beta, \delta$, contains $Q_{\alpha\beta}$. Thus the group $G^\dagger$ (as defined in 4.13) contains all conjugates of $Q_{\alpha\beta}$. Notice that $Q_{\alpha\beta} Q_{\beta\delta} = Q_\beta$ so $Q_\beta \leqslant G^\dagger$ and similarly $Q_\alpha \leqslant G^\dagger$. It now follows that $G^\dagger$ contains every Sylow 3-subgroup of G and since G_α and G_β are both generated by their Sylow 3-subgroups, $G \leqslant G^\dagger$. Now it follows immediately from the order of G and Theorem 4.13 that $G = G^\dagger \cong \mathrm{PSp}_4(3)$. □

7.3 Controlling the 3 and 2-Local Structure

By Hypothesis C, Q_α is a 3-dimensional faithful Sym(4)-module for G_α/Q_α so we will use Lemmas 2.17 and 2.18 and we will use the terminology introduced by referring to the proper, non-trivial subgroups of Q_α as being of type $1A$, $1B$, $1C$, $2A$, $2B$ or $2C$. Find a, b and c in Q_α as in Lemma 2.17 where $a \sim v_1$, $b \sim v_2$ and $c \sim v_3$ give the subspaces fixed by the non-trivial elements in $O_2(G_\alpha/Q_\alpha)$. Then $Q_\alpha = \langle a, b, c\rangle$. Notice that the only type of 1-space centralized by an element of order three in G_α/Q_α has type $1B$ therefore Z_β has type $1B$. Choose a, b and c in such a way that $Z_\beta = \langle abc\rangle$.

Lemma 7.9. *$Q_{\alpha\beta} = S'_{\alpha\beta}$ has type $2B$.*

Proof. The group G_α has four Sylow 3-subgroups which intersect at $O_3(G_\alpha) = Q_\alpha$. Now, G_α is transitive on its Sylow 3-subgroups and thus on their corresponding derived subgroups which each have order 3^2. However, by Lemma 2.17, there is no orbit of subgroups of order nine in Q_α of length one. Therefore the derived subgroups must be distinct and have type $2B$. □

Lemma 7.10. *$S_{\alpha\beta}$ has four G-conjugacy classes of elements of order three with representatives a, ab, abc, $a^2b^2c^2$. In particular $\{abc, a^2b^2c, a^2bc^2, ab^2c^2\}$ and $\{a^2b^2c^2, abc^2, ab^2c, a^2bc\}$ are in disjoint conjugacy classes.*

Proof. A lemma of Burnside (1.9) says that $abc \in Z_\beta$ is conjugate to its inverse in G only if it is conjugate to it in $N_G(S_{\alpha\beta}) = G_{\alpha\beta} \leqslant C_G(Z_\beta)$. Thus abc and any other 3-central element is not conjugate to its inverse. By Lemma 2.17, elements such as a and ab are conjugate to their inverses and so cannot be conjugate to elements of type abc.

Subgroups of type $2B$ contain one subgroup of type $1B$ and three of type $1C$. Now consider $S'_{\alpha\beta} = Q_{\alpha\beta}$. This group of order 3^2 has type $2B$. Since Q_β/Z_β is a natural G_β/Q_β-module, G_β is transitive on the 1-spaces and so G_β is transitive on subgroups of order 3^2 contained in Q_β. By Lemma 7.2, every element of order three in $S_{\alpha\beta}$ lies in $Q_\alpha \cup Q_\beta$ and so any element of order three in $S_{\alpha\beta}$ lies in a subgroup of type $1A$, $1B$ or $1C$. Finally, since $Q_\alpha = J(S_{\alpha\beta})$, Lemma 1.11 proves that no conjugate of ab can be conjugate to any conjugate of a in G else they would already be conjugate in G_α. Thus there are exactly four conjugacy classes of elements of order three in G.

In particular, notice that by Lemma 2.17 (v), abc is conjugate to a^2b^2c, a^2bc^2 and ab^2c^2. □

Lemma 7.11. *$\langle a, abc\rangle = C_{S_{\alpha\beta}}(t_\beta) \leqslant Q_\alpha$ has order nine and has type $2C$, $C_{G_\alpha}(t_\beta) \sim 3 \times 3 : 2 \times 2$ and $\langle a, abc, t_\beta\rangle = C_{G_{\alpha\beta}}(t_\beta) \sim 3 \times 3 \times 2$.*

Proof. In Lemma 7.6 we saw that $3 \times 3 \cong C_{S_{\alpha\beta}}(t_\beta) \leqslant Q_\alpha$. Choose some element $d \in Q_\alpha$ such that $\langle Z_\beta, d\rangle = C_{S_{\alpha\beta}}(t_\beta)$. Notice that $Q_\alpha t_\beta \in (G_\alpha/Q_\alpha) \setminus O_2(G_\alpha/Q_\alpha)$ (we see this is true since $Q_\alpha t_\beta$ normalizes a Sylow 3-subgroup of G_α/Q_α). Now by Lemma 2.17 (vi), $Q_\alpha t_\beta$ centralizes a subgroup of Q_α of type $1C$ and so we can choose d so that $\langle d\rangle$ has type $1C$. By Lemma 2.18, $\langle Z_\beta, d\rangle$ has type $2B$ or $2C$. It is easily checked that there are four groups of order nine in Q_α containing Z_β of which three have type $2C$ and one has type $2B$. We have seen that the subgroup of type $2B$ is $S'_{\alpha\beta} = Q_{\alpha\beta}$ however $C_{Q_\beta}(t_\beta) = Z_\beta$ by Lemma 7.6 and so $\langle Z_\beta, d\rangle$ must have type $2C$. In particular this means $C_{S_{\alpha\beta}}(t_\beta)$ has a subgroup of type $1A$ and so we may as well assume $\langle a\rangle \leqslant C_{S_{\alpha\beta}}(t_\beta)$ and then $d \in \langle bc\rangle$.

Now we see that

$$\frac{Q_\alpha C_{G_\alpha}(t_\beta)}{Q_\alpha} \leqslant C_{G_\alpha/Q_\alpha}(Q_\alpha t_\beta) \cong 2 \times 2$$

since $Q_\alpha t_\beta$ is an involution in Sym(4) which normalizes a Sylow 3-subgroup and so commutes with just a group of order four. In fact, we have equality in the previous expression since G_α has Sylow 2-subgroups which are dihedral of order eight and so t_β at least commutes with another involution. Now, by an isomorphism theorem,

$$2 \times 2 \cong \frac{Q_\alpha C_{G_\alpha}(t_\beta)}{Q_\alpha} \cong \frac{C_{G_\alpha}(t_\beta)}{C_{Q_\alpha}(t_\beta)}$$

and we have seen already that $C_{Q_\alpha}(t_\beta) \cong 3 \times 3$.

It is immediate that $C_{G_{\alpha\beta}}(t_\beta)$ has order 18 and is abelian. $\square$

We have now that $C_{S_{\alpha\beta}}(t_\beta)$ is a subgroup of type $2C$ and therefore contains subgroups of type $1A$, $1B$ and $1C$. Thus, this group of order nine contains an element from each of the four conjugacy classes of elements of order three in G. We therefore aim to restrict the structure of the normalizer in G of this subgroup and then use the Theorem of Smith and Tyrer once again. First we must restrict the structure of some of the 3-local subgroups in G.

We continue to set $\langle Z_\beta, d\rangle = C_{S_{\alpha\beta}}(t_\beta)$ where $d \in Q_\alpha \backslash Q_\beta$ is chosen so that $\langle d\rangle$ has type $1C$.

Lemma 7.12. $\langle Q_\alpha, t_\beta\rangle = C_{G_\beta}(d) = C_{G_\alpha}(d) = C_{G_{\alpha\beta}}(d) \sim 3^3.2$.

Proof. By Lemma 2.17 (*iv*), $C_{G_\alpha/Q_\alpha}(d)$ has order two. Also, as d is not central in $S_{\alpha\beta}$, it commutes with exactly Q_α here. So $Q_\alpha t_\beta \in C_{G_\alpha}(d)/Q_\alpha \leqslant C_{G_\alpha/Q_\alpha}(d) \sim 2$ which implies that $C_{G_\alpha}(d) = \langle Q_\alpha, t_\beta\rangle$ has order $3^3 2$.

We chose d such that $d \in Q_\alpha \backslash Q_\beta$ and so $Q_\beta\langle d\rangle/Q_\beta$ is a Sylow 3-subgroup of G_β/Q_β. Therefore $C_{G_\beta/Q_\beta}(Q_\beta d) \sim 3 \times 2$. By an isomorphism theorem,

$$C_{G_\beta}(d)Q_\beta/Q_\beta \cong C_{G_\beta}(d)/C_{Q_\beta}(d) = C_{G_\beta}(d)/Q_{\alpha\beta}.$$

Also, it is easily seen that $C_{G_\beta}(d)Q_\beta/Q_\beta \leqslant C_{G_\beta/Q_\beta}(d) = C_{G_\beta/Q_\beta}(Q_\beta d)$. Together this gives us

$$C_{G_\beta}(d)/Q_{\alpha\beta} \cong C_{G_\beta}(d)Q_\beta/Q_\beta \leqslant C_{G_\beta/Q_\beta}(Q_\beta d) \sim 3 \times 2.$$

Hence $C_{G_\beta}(d) \sim 3^3.2$ and so the result follows. □

Lemma 7.13. *$Q_\alpha \in \mathrm{Syl}_3(C_G(d))$ and $C_G(d)$ is either 3-soluble of length one or has a normal subgroup at index nine.*

Proof. Set $C := C_G(d)$ and notice that $Q_\alpha \leqslant C$. Now $N_C(Q_\alpha) = N_G(Q_\alpha) \cap C = G_\alpha \cap C = C_{G_\alpha}(d) \sim 3^3.2$. So suppose Q_α is not a Sylow 3-subgroup of C then $Q_\alpha < P \in \mathrm{Syl}_3(C)$ and then $Q_\alpha \lhd N_P(Q_\alpha)$ which is a contradiction since $|N_C(Q_\alpha)| = 23^3$. By Lemma 7.1 (*iv*), $C_G(Q_\alpha) = Q_\alpha$ and so $|N_C(Q_\alpha)/C_C(Q_\alpha)| = 2$. Therefore C satisfies Corollary 4.6 and so C is either 3-soluble of length one or $O^3(C)$ has index at least nine. Suppose $|C/O^3(C)| = 3^3$ then $O^3(C) = O_{3'}(C)$ and C would be 3-soluble of length one so we are done. □

Now we make full use of our strong assumption in Hypothesis C that Q_α does not normalize any non-trivial $3'$-group in G.

Lemma 7.14. *$C_G(d) \leqslant G_{\alpha\beta}$, $N_G(d) \leqslant G_\alpha$.*

Proof. Again we set $C := C_G(d)$ and we consider the two possibilities given by Lemma 7.13. First we suppose C is 3-soluble of length one. Since Q_α does not normalize any non-trivial subgroup of G of order prime to three, $O_{3'}(C) = 1$. Thus C has a normal Sylow 3-subgroup and so $C = N_C(Q_\alpha) = G_\alpha \cap C = \langle Q_\alpha, t_\beta \rangle \leqslant G_{\alpha\beta}$ and then $C \leqslant G_{\alpha\beta}$ and $N_G(d) \leqslant N_G(Q_\alpha) \leqslant G_\alpha$ as claimed. So suppose C is not 3-soluble of length one then C has a normal subgroup, N say, at index nine. Let x be an element of order three in N and consider $C_N(x)$. By Burnside's normal p-complement Theorem (1.6), $C_N(x)$ has a normal 3-complement, M say. However M is normalized by Q_α and has order prime to 3 and so must be trivial. Therefore x is self-centralizing in N and so we can apply a theorem of Feit and Thompson (4.1) to N. Since $O_{3'}(C) = 1$, $O_{3'}(N) = 1$. Therefore by Theorem 4.1, $N \cong \mathrm{Alt}(5)$ or $N \cong \mathrm{Sym}(3)$ or $N \cong \mathrm{PSL}_3(2)$. Notice N admits an action from Z_β and $C_N(Z_\beta) = N \cap G_\beta \leqslant C \cap G_\beta \sim 3^2 2$. Hence $C_N(Z_\beta) = \langle x, t_\beta \rangle$ can have order just six. Suppose $N \cong \mathrm{Alt}(5)$ or $N \cong \mathrm{PSL}_3(2)$. By Lemma 4.2, N does not admit an outer automorphism of order three. Therefore $\langle x, Z_\beta \rangle \cap C_C(N)$ is non trivial. Clearly neither x nor Z_β commutes with N so choose $z_\beta \in Z_\beta^\#$ such that $xz_\beta \in C_C(N)$. Then $1 = [xz_\beta, t_\beta] = t_\beta^{xz_\beta} t_\beta$ as $t_\beta \in N$. Therefore $t_\beta = t_\beta^{z_\beta^{-1}} = t_\beta^x$ which contradicts that x is self centralizing in N. Thus $N \cong \mathrm{Sym}(3)$ and so $|C| = 6.3^2$ which forces $C \leqslant G_{\alpha\beta}$. Finally, by Lemma 2.17 (v), an element of order two in G_α inverts d. Thus $N_G(\langle d \rangle) \leqslant G_\alpha$. □

Corollary 7.15. *Let $d' \in Q_\alpha$ such that $\langle d' \rangle$ is a subgroup of type* $1C$. *Then* $3^3 : 2 \sim C_G(d') \leqslant G_\alpha$.

Proof. This is now immediate since all such elements in Q_α are conjugate in G_α. □

We now know the centralizers in G of elements of order three from three of the four conjugacy classes. So we will consider $C_G(a)$ and by our choice of a we have $t_\beta \in C_G(a)$.

Lemma 7.16. $C_{G_\alpha}(a) \sim 3^3 : (2 \times 2)$ *and* $Q_\alpha \in \mathrm{Syl}_3(C_G(a))$. *In particular* $N_{C_G(a)}(Q_\alpha) \sim 3^3 : (2 \times 2)$.

Proof. By Lemma 2.17, $C_{G_\alpha/Q_\alpha}(a)$ has order four. Also $Q_\alpha t_\beta \in C_{G_\alpha/Q_\alpha}(a)$. Notice that this forces $C_{G_\alpha/Q_\alpha}(a)$ to be elementary abelian (since $Q_\alpha t_\beta$ normalizes an element of order three in $G_\alpha/Q_\alpha \cong \mathrm{Sym}(4)$ and so no element of order four squares to $Q_\alpha t_\beta$). Now, we clearly have $C_{G_\alpha}(a)/Q_\alpha \leqslant C_{G_\alpha/Q_\alpha}(a)$, however, equality follows since $a \in Q_\alpha$ is abelian. Thus $C_{G_\alpha}(a)/Q_\alpha \cong 2 \times 2$ and so $C_{G_\alpha}(a) \sim 3^3 : (2 \times 2)$.

We have $N_{C_G(a)}(Q_\alpha) = N_G(Q_\alpha) \cap C_G(a) = C_{G_\alpha}(a) \sim 3^3 : (2 \times 2)$. So if Q_α were not a Sylow 3-subgroup of $C_G(a)$ then we would have $Q_\alpha < T$ for some $T \in \mathrm{Syl}_3(C_G(a))$ and then $Q_\alpha \lhd N_T(Q_\alpha) \leqslant N_{C_G(a)}(Q_\alpha) \sim 3^3 : (2 \times 2)$. This is a contradiction and so Q_α is a Sylow 3-subgroup of $C_G(a)$ with normalizer as described. □

We will apply a theorem of Hayden (Theorem 4.7) to the group $\overline{C_G(a)} = C_G(a)/\langle a \rangle$ so we must first work to show the hypothesis of the theorem holds.

Lemma 7.17. *Set* $T := \overline{Q_\alpha} \leqslant \overline{C_G(a)} =: A$ *then* A *and* T *satisfy the following.*

(i) $N_A(T)/C_A(T) \cong 2 \times 2$.

(ii) $C_A(T) = T$.

(iii) $C_A(t) \leqslant N_A(T)$ *for each* $t \in T^\#$.

In particular, $A = N_A(T)$.

Proof. By Lemma 7.16, $T = \overline{Q_\alpha}$ is a Sylow 3-subgroup of $A = \overline{C_G(a)}$ and it is clear that $N_A(T) = N_{C_G(a)}(Q_\alpha)/\langle a \rangle$. We now choose some coset representatives for the elements of T and consider their centralizers in A. We choose $\langle \overline{ab}, \overline{abc} \rangle = T$ and so we must consider the groups (i) $C_A(\overline{ab})$, (ii) $C_A(\overline{abc})$, (iii) $C_A(\overline{a^2b^2c})$ and (iv) $C_A(\overline{c})$. We will show each is contained in $\overline{C_{G_\alpha}(a)}$.

(i) Suppose $\overline{x} \in C_A(\overline{ab})$. Then $[\overline{ab}, \overline{x}] = \overline{1}$ implies $[ab, x] \in \langle a \rangle$ and then $(ab)^x \in \{ab, a^2b, b\}$. Lemma 7.10 implies that ab cannot be conjugate to b in G but is conjugate to a^2b in G_α. So there exists $y \in G_\alpha$ such that $(ab)^y = a^2b$. So suppose $(ab)^x = a^2b$ then $(ab)^{xy^{-1}} = ab$. Therefore $xy^{-1} \in C_G(ab) \leqslant G_\alpha$ by Corollary 7.15 and so $x \in G_\alpha$. If instead $(ab)^x = ab$ then $x \in C_G(ab) \leqslant G_\alpha$ so again $x \in G_\alpha$.

(ii) Suppose $\overline{x} \in C_A(\overline{abc})$. Then $[\overline{abc}, \overline{x}] = \overline{1}$ implies $[abc, x] \in \langle a \rangle$. Therefore $(abc)^x \in \{abc, a^2bc, bc\}$. By Lemma 7.10, the only possibility is $(abc)^x = abc$. Therefore $x \in C_G(abc) = G_\beta$. So $x \in C_G(abc) \cap C_G(a) \leqslant C_G(bc) \leqslant G_\alpha$ by Corollary 7.15.

(iii) Suppose $\overline{x} \in C_A(\overline{a^2b^2c})$. Then $[\overline{a^2bc^2}, \overline{x}] = \overline{1}$ implies $[a^2b^2c, x] \in \langle a \rangle$. Therefore $(a^2b^2c)^x \in \{a^2b^2c, b^2c, ab^2c\}$. Lemma 7.10 implies that $(a^2b^2c)^x = a^2b^2c$ and so $x \in C_G(a) \cap C_G(a^2b^2c) \leqslant C_G(b^2c) \leqslant G_\alpha$ by Corollary 7.15.

(iv) Finally we suppose $\overline{x} \in C_A(\overline{c})$. Then $[\overline{c}, \overline{x}] = \overline{1}$ implies $[c, x] \in \langle a \rangle$. Therefore $c^x \in \{c, ac, a^2c\}$. Once again by Lemma 7.10, we have $c^x = c$ and so $x \in C_G(a) \cap C_G(c) \leqslant C_G(ac) \leqslant G_\alpha$ by Corollary 7.15.

So we have shown that $C_A(t) \leqslant \overline{C_{G_\alpha}(a)} = \overline{N_{C_G(a)}(Q_\alpha)} = N_A(T)$ for each $t \in T^\#$. Our calculations also show that if $\overline{x} \in C_A(T)$ then $x \in C_G(\langle abc, c, a\rangle) = C_G(Q_\alpha) = Q_\alpha$ by Lemma 7.2. Therefore $C_A(T) = T$ and $N_A(T)/C_A(T) \cong 2 \times 2$. Thus we have shown A satisfies the hypothesis of Theorem 4.7 and so $A = N_A(T) = N_{C_G(a)}(Q_\alpha)/\langle a\rangle$. □

Corollary 7.18. $3^3 : (2 \times 2) \sim C_G(e) \leqslant G_\alpha$ *for each* $e \in Q_\alpha$ *such that* $\langle e\rangle$ *has type* $1A$.

Proof. By Lemma 7.17, we have that $C_G(a)/\langle a\rangle = N_{C_G(a)}(Q_\alpha)/\langle a\rangle = (C_G(a) \cap G_\alpha)/\langle a\rangle$ and so $C_G(a) \leqslant G_\alpha$. If $e \in Q_\alpha$ and $\langle e\rangle$ has type $1A$ then e is a conjugate of a by an element of G_α and so the result holds. □

We have now calculated the centralizer in G of every conjugacy class of element of order three so the following result is immediate.

Corollary 7.19. *If* $x \in G$ *has order three then* $C_G(x)$ *is a* $\{2, 3\}$*-group. In particular if* $x \in S_{\alpha\beta}$ *then* $C_G(x) \leqslant G_\alpha$ *or* $C_G(x) \leqslant G_\beta$.

We now work to restrict the structure of the group $H := C_G(t_\beta)$.

Lemma 7.20. $S := C_{S_{\alpha\beta}}(t_\beta)$ *is a Sylow* 3*-subgroup of* H *and* $|N_H(S)/C_H(S)| = 2$.

Proof. By Lemma 7.11, S has type $2C$ and so contains elements of order three from each of the four G-conjugacy classes of elements of order three. In particular the only conjugate of d in S is d^{-1} so for any $x \in N_H(S)\backslash S$, $x \in N_G(\langle d\rangle) \leqslant G_\alpha$. Therefore, by Lemma 7.11, $S \leqslant N_H(S) \leqslant G_\alpha \cap H = C_{G_\alpha}(t_\beta) \sim 3^2 : 2^2$ has a normal 3-subgroup of order nine. So $N_H(S) = C_{G_\alpha}(t_\beta)$ has order $2^2 3^2$. In particular, this means $S \in \mathrm{Syl}_3(H)$ since if not then $S < T \in \mathrm{Syl}_3(H)$ and then $S \lhd N_T(S) \leqslant N_H(S)$ which contradicts that $|N_H(S)|_3 = 3^2$. Now, $C_H(S) \leqslant C_H(Z_\beta) \cap C_H(d) = C_{G_\beta}(d) \sim 3^3.2$ by Lemma 7.12 and so $C_H(S)$ has order at most 23^2. In fact this is the exact order as S commutes with itself and with t_β. Hence $|N_H(T)/C_H(T)| = 2$. □

Recall Lemma 7.4 implies that the involution t_β fixes a circuit in Γ, $(\gamma, \alpha, \beta, \ldots)$ and $Q_\gamma t_\beta \in Z(G_\gamma/Q_\gamma)$. Thus $C_{G_\gamma}(t_\beta) \cong 3 \times \mathrm{SL}_2(3)$. Furthermore $Z_\gamma \leqslant C_{G_\gamma}(t_\beta)$ and $\langle Z_\beta, Z_\gamma\rangle \leqslant Q_\alpha$ is abelian. So $\langle Z_\beta, Z_\gamma\rangle \leqslant C_{S_{\alpha\beta}}(t_\beta) = S$ and therefore $S = \langle Z_\beta, Z_\delta\rangle$.

Lemma 7.21. *$1 \neq O_{3'}(H)$ is nilpotent and contains $A := O_2(C_{G_\beta}(t_\beta))$ and $B := O_2(C_{G_\gamma}(t_\beta))$.*

Proof. By Lemma 7.20, $|N_H(S)/C_H(S)| = 2$ and so we can once again apply the theorem of Smith and Tyrer (Theorem 4.5) to see that either H is 3-soluble of length one or $O^3(H) \neq H$. If H is 3-soluble of length one then $X := O_{3'}(H)S$ is a normal subgroup of H. Then a Frattini argument implies that $H = XN_H(S)$. It is clear that $t_\beta \in O_{3'}(H)$ and so $\langle t_\beta, S\rangle \leqslant X \cap N_H(S)$ and so by an isomorphism theorem, $H/X \cong N_H(S)/(X \cap N_H(S))$ has order at most two. Therefore X is a normal subgroup of H at index at most two. If $H = X$ then H has a normal 3-complement and clearly $A, B \leqslant O_{3'}(H)$. So we may as well assume X has index two in H. Suppose $A \nleqslant X$. Then by an isomorphism theorem, $2 = |H/X| = |AX/X| = |A/(A \cap X)|$ and so $A \cap X$ has order four. However $3 \times \mathrm{SL}_2(3) \cong C_{G_\beta}(t_\beta) \leqslant H$ and so $X \geqslant \langle (A \cap X)^{C_{G_\beta}(t_\beta)}\rangle = A$ which is a contradiction. Therefore $A \leqslant X$ and similarly $B \leqslant X$ and then clearly both quaternion groups are contained in $O_{3'}(H)$.

So we are left to consider the possibility that $Y := O^3(H) \neq H$. By Lemma 7.11 and Lemma 7.14, $C_H(d) \leqslant G_{\alpha\beta} \cap H \cong 3 \times 3 \times 2$. So $C_H(d) = \langle S, t_\beta\rangle$.

Since we know $|N_H(S)/C_H(S)| = 2$, there exists an element of even order $x \in N_H(S)\backslash C_H(S)$. If $x \in C_H(d)$ then x commutes with S. Recall, S has type $2C$ and the only conjugate of d in S is d^{-1} (see Lemma 2.18 and Lemma 7.10). Thus x must invert d as d^{-1} is the only other conjugate of d in S. Since x has even order, $x \in Y$ and therefore $Y \ni dxd^{-1} = dxd^x = d^2x$ and so $d \in Y$. Now $C_Y(d) = \langle S, t_\beta\rangle \cap Y$ has order 6 so if we set $\overline{H} := H/\langle t_\beta\rangle$ then $\overline{d}$ is a self-centralizing element of order three in $\overline{Y}$. Hence we can apply Theorem 4.1 to $\overline{Y}$ and we have three cases to consider.

Firstly, suppose $\overline{Y} \cong \mathrm{PSL}_3(2)$. Then by Lemma 4.2, $S \cap C_G(\overline{Y})$ is non-trivial else we would have an outer automorphism of $\mathrm{PSL}_3(2)$ of order three which is not possible. Thus for some $s \in S^{\#}$, and each $y\langle t_\beta\rangle \in \overline{Y}$, $y\langle t_\beta\rangle^s = y\langle t_\beta\rangle$. Since the coset $y\langle t_\beta\rangle$ has order two and $s \in S$ has order three, s must centralize each element of the coset. In particular we could choose $y\langle t_\beta\rangle$ to have order seven. Then y has order seven and commutes with $s \in S^{\#}$ and this contradicts Corollary 7.19.

Secondly, suppose $\overline{Y}$ has a normal 2-subgroup, $\overline{M}$, such that $Y/M \cong \overline{Y}/\overline{M} \cong \mathrm{Alt}(5)$. Then by Lemma 4.2, $S \cap C_G(Y/M)$ is non-trivial else we would have an outer automorphism of $\mathrm{Alt}(5)$ of order three which is not possible. Thus for some $s \in S^{\#}$, and each $yM \in Y/M$, $yM^s = yM$. Since the coset yM has order a power of 2 and $s \in S$ has order three, s must centralize each element of the coset. In particular we could choose yM to have order five. Then y has order a multiple of five but commutes with $s \in S^{\#}$ and this contradicts Corollary 7.19.

So we are left only with the third case given by Theorem 4.1. Therefore $\overline{Y}$ has a normal $3'$-subgroup $\overline{M}$ such that $Y/M \cong \overline{Y}/\overline{M} \cong \mathrm{Sym}(3)$ or C_3. In particular this means that $M : S$ is a subgroup of H at index at most two and so is normal. It follows that H must be 3-soluble of length one and so by the previous argument we see that H has a normal $3'$-subgroup containing the necessary quaternion subgroups.

It remains only to prove that in each case $O_{3'}(H)$ is nilpotent. First notice that $t_\beta \in O_{3'}(H)$ and $C_H(d) \cap O_{3'}(H) = \langle t_\beta\rangle$ so we can apply Corollary 1.22 to $O_{3'}(H)$ to see that $O_{3'}(H)$ is nilpotent. □

Lemma 7.22. *$X := \langle O_2(C_{G_\beta}(t_\beta)), O_2(C_{G_\gamma}(t_\beta))\rangle$ is an extraspecial 2-group and has shape 2_+^{1+4}. In particular, $[O_2(C_{G_\beta}(t_\beta)), O_2(C_{G_\gamma}(t_\beta))] = 1$.*

Proof. Since $O_{3'}(H)$ is nilpotent, it is a direct product of its Sylow subgroups and so the two 2-groups $A := O_2(C_{G_\beta}(t_\beta))$ and $B := O_2(C_{G_\gamma}(t_\beta))$ generate a 2-group. We apply Lemma 1.25 to $X/\langle t_\beta\rangle = \langle A, B\rangle/\langle t_\beta\rangle$ to get that $X/\langle t_\beta\rangle$ is either elementary abelian of order 2^4 or special of order 2^6 with centre of order four. Suppose the latter then, by correspondence, X has a normal subgroup of order eight, Z say, containing t_β. By coprime action, $Z = \langle C_Z(s) | s \in S^\# \rangle$ so we consider the conjugacy class of each $s \in S^\#$. If $s = d$ (or d^{-1}) then $C_Z(s) = \langle t_\beta \rangle$ since we already saw that d acts fixed-point-freely on $O_{3'}(H)/\langle t_\beta \rangle$. Consider $C_Z(s) \leqslant X \cap G_\beta = A$ for $s \in Z_\beta^\#$. Notice

$$C_Z(s) \leqslant X \cap C_G(s) = X \cap G_\beta \leqslant C_{G_\beta}(t_\beta) \cong 3 \times \mathrm{SL}_2(3)$$

and $C_Z(s)$ will be a normal 2-subgroup of $C_{G_\beta}(t_\beta)$ and so $C_Z(s) \leqslant A$. If $A \leqslant Z$ then $A = Z \trianglelefteq X$ which is a contradiction since $X = \langle A, B \rangle$ has order 2^7. Suppose $|A \cap Z| = 4$ then $A \cap Z$ is normalized by S and consequently centralized by S which is a contradiction since $C_Z(d) = \langle t_\beta \rangle$. Thus $A \cap Z = C_Z(s) = \langle t_\beta \rangle$. Similarly if $s \in Z_\gamma^\#$ then $C_Z(s) = B \cap Z = \langle t_\beta \rangle$. So we must have $Z = \langle C_Z(s) | s \in S^\# \rangle = C_Z(a)$ has order eight. However this is a contradiction since eight does not divide the order of $C_G(a)$ by 7.18. Hence $X/\langle t_\beta \rangle$ must be elementary abelian. Finally, since X contains non-abelian quaternion groups, X is non-abelian and $t_\beta \in Z(X)$ admits an automorphism of order three which centralizes precisely $\langle t_\beta \rangle$ so $Z(X)$ has order two or eight. However, the order cannot be eight since no abelian group of order eight has an automorphism of order three. Thus X is extraspecial of order 2^5. Now Corollary 1.17 together with Lemma 1.18 concludes the result. □

We can now use Theorem 7.8 to prove Theorem C.

Corollary 7.23. $G \cong \mathrm{PSp}_4(3)$.

Chapter 8

Higman's Theorem on Fixed-Point-Free Elements of Order Three

Theorem 8.2 of Higman's notes, *Odd Characterisations of Finite Simple Groups* [17], is a powerful result about an action of $\mathrm{SL}_2(2^n)$ in which an element of order three acts fixed-point-freely on a 2-group. The theorem is as follows.

Theorem 8.1. *Let G be a finite group with a normal 2-subgroup, Q, such that $X := G/Q \cong \mathrm{SL}_2(2^n)$ for some $n \geqslant 2$ and some element of order three in G acts fixed-point-freely on Q. Then Q is elementary abelian and a direct product of natural modules.*

Higman's proof is sketchy and incomplete so we give a complete proof here. We will use new methods of Chermak and Meierfrankenfeld found in [5] to give conditions under which $\mathrm{SL}_2(2^n)$ modules can be decomposed and then finally we use Higman's arguments to prove that the subgroup Q is elementary abelian and thus an $\mathrm{SL}_2(2^n)$ module. In all that follows let $X \cong \mathrm{SL}_2(2^n)$ where $n \geq 2$, $T \in \mathrm{Syl}_2(X)$ and set $L := \mathrm{GF}(2)$ and $K := \mathrm{GF}(2^n)$.

We must recall much of Chapter 2. In particular the definitions of the natural modules over K and that these are the only irreducible modules over K for $\mathrm{SL}_2(2^n)$ which admit an element of order three acting fixed-point-freely. We recall the definition of the natural module over L also. We continue notation from Chapter 2 where we set $V_1, \ldots, V_n$ to be the irreducible 2-dimensional KX-modules. We also fixed an algebraically closed extension field F of K over which we could define Brauer characters and we set $M_i = F \otimes_K V_i$. We proved these were the only 2-dimensional X-modules over an F. Recall also that by Lemma 2.33, these were the only irreducible FX-modules admitting an element of order three in X acting fixed-point-freely.

Lemma 8.2. *Let $V_1, \ldots, V_n$ be the n algebraic conjugates of the natural KX-module. Then* $\mathrm{Hom}_{KX}(V_i \otimes_K V_j, V_k) = 0$ *for all $i, j, k \leqslant n$.*

Proof. Firstly if $i \neq j$ then we have seen in Lemma 2.31 that $V_i \otimes V_j$ is irreducible so the only KH-module homomorphism $V_i \otimes_K V_j \to V_k$ is the zero map. So we consider the case $i = j$. Suppose $\alpha : V_i \otimes_K V_i \to V_k$ is a KX-homomorphism. Since V_k is irreducible, this map is either a zero map or surjective so we will assume α is surjective. Let $U = \mathrm{Ker}(\alpha)$ then U is a 2-dimensional submodule of $V := V_i \otimes_K V_i$. Set $W := \langle m \otimes n + n \otimes m | m, n \in V_i \rangle$ then W is a KX-submodule of V. Let $\{v_1, v_2\}$ be a basis for V_i and write all elements of X as matrices with respect to this basis. Any element of V_i can be written $v = av_1 + bv_2$ for $a, b \in K$. So for $a, b, c, d \in K$, a general element of W has the form

$$(av_1 + bv_2) \otimes (cv_1 + dv_2) + (cv_1 + dv_2) \otimes (av_1 + bv_2) = (ad + bc)v_1 \otimes v_2 + (ad + bc)v_2 \otimes v_1.$$

Thus W has dimension 1 and is spanned by the element $\langle v_1 \otimes v_2 + v_2 \otimes v_1 \rangle$. If $W \nleq U$ then $1 \neq WU/U \lneq V/U \cong V_k$ where the isomorphism is an isomorphism of KX-modules. This is not possible as V_k is irreducible. So $W \leqslant U$. Consider the 3-dimensional KX-module V/W. This contains a 1-dimensional submodule U/W. The only 1-dimensional KX-module is the trivial module (see Lemma 2.31) and so X acts trivially on U/W. A basis for $\overline{V} := V/W$ is $\{\overline{v_1 \otimes v_1}, \overline{v_2 \otimes v_2}, \overline{v_1 \otimes v_2}\}$. Consider the element $x := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ in X (represented with respect to the module V_i and the basis chosen) and let $\overline{v} := a\overline{v_1 \otimes v_1} + b\overline{v_2 \otimes v_2} + c\overline{v_1 \otimes v_2} \in \overline{V}$ for $a, b, c \in K$. Now $v_1 \cdot x = v_2$ and $v_2 \cdot x = v_1 + v_2$ and so

$$\overline{v} \cdot x = b\overline{v_1 \otimes v_1} + (a+b+c)\overline{v_2 \otimes v_2} + c\overline{v_1 \otimes v_2}.$$

So if $\overline{v}$ were contained in $\overline{U}$ then it would be fixed by x and so $a = b = c$. Since $K > L$, there is some $\omega \in K$ such that $\omega \neq 0, 1$. So consider $y := \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \in X$. Then $v_1 \cdot y = \omega v_1$ and $v_2 \cdot y = \omega^{-1} v_2$. So $\overline{w} := \overline{v_1 \otimes v_1} + \overline{v_2 \otimes v_2} + \overline{v_1 \otimes v_2} \in \overline{U}$ must be centralized by y. However

$$\overline{w} \cdot y = \omega^2 \overline{v_1 \otimes v_1} + \omega^{-2} \overline{v_2 \otimes v_2} + \overline{v_1 \otimes v_2} \neq \overline{w}.$$

Thus there can be no such $0 \neq \alpha \in \mathrm{Hom}_{KX}(V_i, V_i, V_k)$. □

Corollary 8.3. *Let U, V, W be non-trivial KX-modules admitting an element of order three acting fixed-point-freely then* $\mathrm{Hom}_{KX}(U \otimes_K V, W) = 0$.

Proof. Suppose we have a surjective map, $\rho : U \otimes V \to W$. Every irreducible KX-submodule of U, V and W is KX-isomorphic to V_i for some $1 \leqslant i \leqslant n$ by Lemma 2.33. Let W_1 be an irreducible submodule of W and consider the preimage in $U \otimes V$ of W_1. There must exist submodules $U_1 \leqslant U$ and $V_1 \leqslant V$ such that $\rho : U_1 \otimes V_1 \to W_1$. Suppose U_1 is not irreducible. For each proper submodule U_2 of U_1, ρ maps $U_2 \otimes V_1$ to a submodule of W_1. Since W_1 is irreducible, this image is either W_1 or $\{0\}$. Since $\rho\big|_{U_1 \otimes V_1}$ is non-zero we must be able to choose an irreducible submodule, U_2 of U_1 such that $\rho : U_2 \otimes V_1 \to W_1$. We repeat these arguments in the case that V_1 is not irreducible to find an irreducible submodule $V_2 \leqslant V_1$ such that ρ must map $U_2 \otimes V_2$ to W_1 where each of U_2, V_2, W_1 is KX-isomorphic to a natural KX-module. However, by Lemma 8.2, this is not possible and so we have a contradiction. □

In the following lemma we will refer to some known number theoretic results which can be found in the appendix.

Lemma 8.4. *(Chermak)[5, 4.1] If V is an LX-module satisfying $[V,T,T]=0$ and such that $C_V(X)=0$ then $[V,X]$ is a direct sum of natural modules for X.*

Proof. Set $B=N_X(T)$ and let $H\cong C_{q-1}$ be a complement to T in B. Choose an element $s\in X$ that normalizes H but is not in B. Now, T is a 2-group and V is a module over a field of characteristic two so $C_V(T)\neq 0$ and is B-invariant. In particular $|H|$ is coprime to $|C_V(T)|$ so $C_V(T)$ is completely reducible as a sum of irreducible LH-modules by Maschke's Theorem. Let U be one of these irreducible modules. Set $E:=\mathrm{End}_{LH}(U)$. By Schur's Lemma, E is a finite field of order 2^m for some m. Moreover, as H is abelian, there is a homomorphic image of H in the multiplicative group $E^\times$. Let $\widetilde{H}$ be this image and let $r=|\widetilde{H}|$. Since U is an irreducible H-module, it is also an irreducible $\widetilde{H}$-module. Now $\widetilde{H}\leqslant E^\times$ and so r divides $|E^\times|=2^m-1$. Also, r divides $|H|=2^n-1$. Let d be the greatest common divisor or 2^n-1 and 2^m-1 and let g be the greatest common divisor of n and m. Then $d=2^g-1$ by Lemma A.2 and r divides 2^g-1. Since g divides m, E contains a subfield, E_0 say, of order 2^g (See Lemma A.3). Also, since r divides 2^g-1 and multiplicative groups of fields are cyclic, it follows that $\widetilde{H}\leqslant E_0^\times$. We can view U as a vector space over E and also as a vector space over E_0. Since E_0 contains $\widetilde{H}$, any 1-dimensional E_0-subspace of U is H-invariant so U has dimension 1 over E_0. It follows that $|U|=|E_0|\leqslant 2^n$.

For any $C\subseteq X$ set $U^C:=\langle u^c|u\in U,c\in C\rangle$ and for $D\leqslant X$ set $[U^C,D]:=\langle [u^c,d]=u^{cd}-u^c|u\in U,c\in C,d\in D\rangle$. Now consider the LX-module $W:=U^X$. By the BN-property of X, we have $X=B\cup BsB$ and so

$$W=U^B+U^{BsB}=U+U^{sB}=U+U^{sHT}=U+U^{sT}$$

because s normalizes H. Now for any $u\in U$ and any $t\in T$, $u^{st}=u^s+[u^s,t]\in U^s+[U^s,T]$

so $U^{sT} \leqslant U^s + [U^s, T]$. Also, $U^s \leqslant U^{sT}$ and $[U^s, T] \leqslant U^{sT}$. Thus $W = U + U^s + [U^s, T]$. Since the action of T is quadratic on V and $U \leqslant C_V(T)$, $U + [U^s, T] \leqslant C_W(T)$. Suppose $[U^s, T] = 0$, then U commutes with $\langle T, T^{s^{-1}} \rangle = X$ (by Lemma 2.23) which contradicts that $C_V(X) = 0$. Hence $W/C_W(T) \cong U^s$ has order $|U|$.

Now, $[U^s, T^s] = 0$, so $U^s \leqslant C_W(T^s)$ and therefore $W = C_W(T) + C_W(T^s)$. Consider $C_W(T) \cap C_W(T^s)$. This space commutes with $\langle T, T^s \rangle = X$ and so must be trivial. Now by an isomorphism theorem,

$$U^s \cong \frac{W}{C_W(T)} = \frac{C_W(T) + C_W(T^s)}{C_W(T)} \cong \frac{C_W(T^s)}{C_W(T) \cap C_W(T^s)} \cong C_W(T^s).$$

Since W is X-invariant, and therefore s-invariant, $C_W(T^s) = C_W(T)^s$ and so $C_W(T)$ has order $|U|$ and therefore $|W| = |C_W(T)||U^s| = |U|^2$ and $W = U \oplus U^s$.

Let $0 \neq v \in U^s$. If $[v, t] = 0$ for any $1 \neq t \in T$ then $v \in C_V(T^s) \cap C_V(t) = C_V(\langle T^s, t \rangle) = C_V(X) = \{0\}$ (by Lemma 2.23). Hence $C_T(v) = 1$ and so the set $\{[v, t] = v \cdot t - v | t \in T\} \subseteq [v, T]$ has order $|T| = 2^n$. Since T acts quadratically on V, $[v, T, T] = 0$ and so $[v, T] \leqslant C_W(T) = U$. Hence $|T| \leqslant |U|$. But we already saw that $|U| \leqslant 2^n$ and therefore $|U| = |T| = 2^n$ and so $|W| = 2^{2n}$. Also, $C_T(v) = 1$ implies that T acts regularly on non-zero vectors in U^s. Similarly T^s acts regularly on non-zero vectors in U. So suppose W_1 is a proper X-invariant submodule of W. If $u \in U^\#$ is in W_1 then all of U is in W_1 and then so is U^s and so $W = W_1$. Similarly if u^s in W_1 then so is all of U^s and again all of U. So suppose $u_1, u_2 \in U^\#$ and $w = u_1 + u_2^s \in W_1$. Then for $t \in T^\#$, $w^t = u_1 + u_2^{st} \in W$ and then $w - w^t = u_2^s - u_2^{st} \in U \cap W_1 = \{0\}$ and so $u_2^s = u_2^{st}$ which contradicts that T acts regularly on U^s. Hence W is an irreducible LX-module.

By Lemma 2.5, $\mathrm{End}_{LH}(U)$ is a field of order $|U|$ and so $\mathrm{End}_{LH}(U) \cong K$. Notice that any element of $\mathrm{End}_{LX}(W)$ preserves $C_W(T) = U$ and so any LX-endomorphism of W restricts to give an endomorphism of U. Also, any LH-endomorphism of U, α say, extends to an endomorphism of $W = U \oplus U^s$, $\overline{\alpha} : u_1 + u_2^s \mapsto \alpha(u_1) + \alpha(u_2)^s$. Thus $\mathrm{End}_{LX}(W) \cong K$. Also, W has dimension $2n$ over L and is irreducible and therefore is a natural module over L.

Now $[V, X] \leqslant [V, T] + [V, T^s] \leqslant C_V(T) + C_V(T^s)$ and $C_V(T)$ is completely reducible as a product of irreducible H-modules say $C_V(T) = U_1 \oplus \ldots \oplus U_r$. Thus

$$C_V(T) + C_V(T^s) = (U_1 \oplus U_1^s) \oplus \ldots \oplus (U_r \oplus U_r^s)$$

gives a direct sum of natural modules for X and so $[V, X]$ is a submodule of this decomposed module and so also decomposes. □

Lemma 8.5. *The only irreducible module for X over L which admits an element of order three acting fixed-point-freely is the natural module.*

Proof. Suppose V is an irreducible LX-module admitting an element of order three acting fixed-point-freely. Set $E := \mathrm{End}_{LX}(V)$. Then V is an irreducible EX-module and satisfies $E = \mathrm{End}_{EX}(V)$. Recall that F is the algebraically closed field of characteristic two over which we defined Brauer characters. By Lemma 2.8, the FX-module $F \otimes_E V$ is irreducible and also admits an element of order three acting fixed-point-freely. By Lemma 2.33, $F \otimes_E V$ has dimension two over F and so V has dimension two over E. Now, $[V, T]$ is a proper E-subspace of V and so has dimension one and therefore $[V, T, T]$ is trivial. So by Lemma 8.4, $[V, X]$ (as an LX-module) is a direct sum of natural LX-modules. However, some $x \in X$ acts fixed-point-freely on V and so $[V, X] \geqslant [V, x] = [V, x] \oplus C_V(x) = V$ by coprime action. Thus, V is a direct sum of natural LX-modules. Finally, since V is irreducible, V must be a natural LX-module. □

Lemma 8.6. *Let K/L be a field extension and let B be a group. Let U_1 and U_2 be KB-modules such that $\mathrm{End}_{LB}(U_i) \cong K$ for $i = 1, 2$. Suppose that there exists an LB-module* *isomorphism* $\alpha : U_1 \to U_2$*. Then there exists* $\beta \in \mathrm{Gal}(K/L)$ *such that for every* $u \in U_1$ *and every* $k \in K$*,* $\alpha(ku) = \beta(k)\alpha(u)$*.*

Proof. Let $\lambda_i : K \to \mathrm{End}_{LB}(U_i)$ be the ring isomorphism where $\lambda_i(k)$ is the LB-homomorphism induced by multiplication by k. Clearly $\lambda_i(k+j) = \lambda_i(k) + \lambda_i(j)$ and $\lambda_i(kj) = \lambda_i(k)\lambda_i(j)$ for $j, k \in K$. For each $k \in K$, $\alpha\lambda_1(k)\alpha^{-1}$ is an LB-endomorphism of U_2 and so applying λ_2^{-1} to it gives an element of K, $\lambda_2^{-1}(\alpha\lambda_{1k}\alpha^{-1})$. Consider the map $\beta : K \to K$ given by $\beta(k) = \lambda_2^{-1}(\alpha\lambda_1(k)\alpha^{-1})$. We check this is a ring homomorphism. Let $k, j \in K$ then

$$\begin{aligned}
\beta(k+j) &= \lambda_2^{-1}(\alpha\lambda_1(k+j)\alpha^{-1}) \\
&= \lambda_2^{-1}(\alpha(\lambda_1(k) + \lambda_1(j))\alpha^{-1}) \\
&= \lambda_2^{-1}((\alpha\lambda_1(k)\alpha^{-1}) + (\lambda_1(j)\alpha^{-1})) \\
&= \lambda_2^{-1}(\alpha\lambda_1(k)\alpha^{-1}) + \lambda_2^{-1}(\alpha\lambda_1(j)\alpha^{-1}) \\
&= \beta(k) + \beta(j).
\end{aligned}$$

Also,

$$\begin{aligned}
\beta(kj) &= \lambda_2^{-1}(\alpha\lambda_1(kj)\alpha^{-1}) \\
&= \lambda_2^{-1}(\alpha\lambda_1(k)\lambda_1(j)\alpha^{-1}) \\
&= \lambda_2^{-1}(\alpha\lambda_1(k)\alpha^{-1})\lambda_2^{-1}(\alpha\lambda_1(j)\alpha^{-1}) \\
&= \beta(k)\beta(j).
\end{aligned}$$

So β is a non-zero field homomorphism and thus an isomorphism. For $l \in L$, $\alpha\lambda_1(l)\alpha^{-1}$ is just multiplication of U_2 by l as α and α^{-1} are L-linear maps. So $\alpha\lambda_1(l)\alpha^{-1} = \lambda_2(l)$ and therefore $\beta(l) = \lambda_2^{-1}(\lambda_2(l)) = l$. Thus β is an automorphism of K fixing L. Now for each $u \in U_1$ we can find $v \in U_2$ such that $u = \alpha^{-1}(v)$. Thus $\alpha(ku) = \alpha(k\alpha^{-1}(v)) = (\alpha\lambda_1(k)\alpha^{-1})(v) = k_1\alpha(u)$ where $k_1 \in K$ satisfies $\lambda_2(k_1) = \alpha\lambda_1(k)\alpha^{-1}$ and therefore $k_1 = \lambda_2^{-1}(\alpha\lambda_1(k)\alpha^{-1}) = \beta(k)$ as required. □

Lemma 8.7. *Let* $T \in \mathrm{Syl}_2(X)$ *and let* $C_{p-1} \cong H \leq N_X(T)$ *be a complement to* T *in* $N_X(T)$*. Then* T *is a* KH*-module. Let* V, W *be natural* KX*-modules and* σ *a Frobenius* *map such that V^σ and W are isomorphic as KX-modules. Let $V_1 = C_V(T)$ and $W_1 = C_W(T)$.*

(i) If $\alpha : T \to \mathrm{Hom}_K(V_1, W_1)$ is an LH-module isomorphism then there exists $\beta \in \mathrm{Gal}(K/L)$ such that for $0 \neq k \in K$, $\beta(k^2) = k^{-1}\sigma(k)$.

(ii) If $\alpha : T \to \mathrm{Hom}_K(V_1, W/W_1)$ is an LH-module isomorphism then there exists $\beta \in \mathrm{Gal}(K/L)$ such that for $0 \neq k \in K$, $\beta(k^2) = k^{-1}\sigma(k^{-1})$.

(iii) If $\alpha : T \to \mathrm{Hom}_K(V/V_1, W_1)$ is an LH-module isomorphism then there exists $\beta \in \mathrm{Gal}(K/L)$ such that for $0 \neq k \in K$, $\beta(k^2) = k\sigma(k)$.

(iv) If $\alpha : T \to \mathrm{Hom}_K(V/V_1, W/W_1)$ is an LH-module isomorphism then there exists $\beta \in \mathrm{Gal}(K/L)$ such that for $0 \neq k \in K$, $\beta(k^2) = k\sigma(k^{-1})$.

Proof. Identify X with the 2-dimensional representation affording the module V. Choose T to be the upper triangular matrices and H to be the diagonal elements. Fix the parameterizations $K^\times \to H$ of H by $k \mapsto h_k$ and $K \to T$ of T by $l \mapsto t_l$ where

$$h_k = \begin{pmatrix} k^{-1} & 0 \\ 0 & k \end{pmatrix}, \quad t_l = \begin{pmatrix} 1 & l \\ 0 & 1 \end{pmatrix}.$$

So T is a KH-module when we define $kt_l := t_{kl}$ and $t_l \cdot h_k := h_k^{-1} t_l h_k = t_{k^2 l}$ for every $k \in K, h_k \in H, t_l \in T$. In particular $t_l \cdot h_k = k^2 \cdot t_l$. By Lemma 2.5, we see $\mathrm{End}_{LH}(T) \cong K$.

Now given our choice of representation we can identify both V and $W^{\sigma^{-1}}$ with the vector space $\{(a,b) | a, b \in K\}$. For $(a,b) \sim v \in V$ and $h_k \in H$ we have

$$v \cdot h_k \sim \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} k^{-1} & 0 \\ 0 & k \end{pmatrix} = \begin{pmatrix} k^{-1}a & kb \end{pmatrix}$$

and for $(a,b) \sim w \in W = V^\sigma$

$$w \cdot h_k \sim \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} \sigma(k^{-1}) & 0 \\ 0 & \sigma(k) \end{pmatrix} = \begin{pmatrix} \sigma(k^{-1})a & \sigma(k)b \end{pmatrix}.$$

Thus we identify V_1 and $W_1^{\sigma^{-1}}$ with $\{(0,b)|b \in K\}$ and V/V_1 and $(W/W_1)^{\sigma^{-1}}$ with $\{(a,0)+\langle(0,1)\rangle|a \in K\}$. So for each $h_k \in H$,

(i) $v \cdot h_k = kv$ for all $v \in V_1$,

(ii) $w \cdot h_k = \sigma(k)w$ for all $w \in W_1$,

(iii) $v \cdot h_k = k^{-1}v$ for all $v \in V/V_1$,

(iv) $w \cdot h_k = \sigma(k^{-1})w$ for all $w \in W/W_1$.

Consider the K-vector space $M_{AB} := \mathrm{Hom}_K(A,B)$ where $A = V_1$ or V/V_1 and $B = W_1$ or W/W_1. Since A and B are 1-dimensional K-modules and elements of M_{AB} commute with K, each $\phi \in M_{AB}$ is determined by where it maps one non-zero element of A. Therefore, M has order $|B| = 2^n$. Also, M_{AB} is a KH-module when we define $(f \cdot h_k)(a) := f(a \cdot h_k^{-1}) \cdot h_k$ for $f \in M_{AB}$, $k \in K$, $h_k \in H$ and $a \in A$. Now K embeds into $\mathrm{End}_{LX}(M_{AB})$ and M_{AB} is a vector space over $\mathrm{End}_{LX}(M_{AB})$. However, $|M_{AB}| = |K|$ so M_{AB} has dimension one over K and therefore we must have that $K \cong \mathrm{End}_{LX}(M_{AB})$.

We are given the LH-module isomorphism α and so we can apply Lemma 8.6 with $U_1 = T$, $U_2 = M_{AB}$, to see that there exists $\beta \in \mathrm{Gal}(K/L)$ such that $\beta(k^2) \cdot \alpha(t) = \alpha(k^2 \cdot t)$ for every $t \in T$ and every $k \in K$. Now $\alpha(k^2 \cdot t) = \alpha(t \cdot h_k) = \alpha(t) \cdot h_k$ as α is an LH-module homomorphism. The action we defined of H on M_{AB} means for any $a \in A$, $(\alpha(t) \cdot h_k)(a) = \alpha(t)(a \cdot h_k^{-1}) \cdot h_k$. We have four possibilities:

(i) If $A = V_1$, $B = W_1$ then $\alpha(t)(a \cdot h_k^{-1}) \cdot h_k = \sigma(k)\alpha(t)(k^{-1}a) = k^{-1}\sigma(k)\alpha(t)$. Thus $\beta(k^2) = k^{-1}\sigma(k)$.

(ii) If $A = V_1$, $B = W/W_1$ then $\alpha(t)(a \cdot h_k^{-1}) \cdot h_k = \sigma(k^{-1})\alpha(t)(k^{-1}a) = k^{-1}\sigma(k^{-1})\alpha(t)$. Thus $\beta(k^2) = k^{-1}\sigma(k^{-1})$.

(iii) If $A = V/V_1$, $B = W_1$ then $\alpha(t)(a \cdot h_k^{-1}) \cdot h_k = \sigma(k)\alpha(t)(ka) = k\sigma(k)\alpha(t)$. Thus $\beta(k^2) = k\sigma(k)$.

(iv) If $A = V/V_1$, $B = W/W_1$ then $\alpha(t)(a \cdot h_k^{-1}) \cdot h_k = \sigma(k^{-1})\alpha(t)(ka) = k\sigma(k^{-1})\alpha(t)$. Thus $\beta(k^2) = k\sigma(k^{-1})$. □

Lemma 8.8. *(Meierfrankenfeld)[5, 4.2] Let V be an LX-module with a submodule W such that V/W and W are natural modules over L. Then V is completely reducible.*

Proof. By Lemma 2.25, any non-identity element of X with odd order, g say, acts fixed-point-freely on W and on V/W. Therefore g acts fixed-point-freely on V and so $C_V(X) \leqslant C_V(g) = 0$ and by coprime action, $V = [V, g] \oplus C_V(g) = [V, g] \leqslant [V, X] \leqslant V$. Thus if T acts quadratically on V then V is completely reducible by Lemma 8.4 and we are done, so assume not. Set $\widetilde{V} = V \otimes_L K$ so $\widetilde{V}$ is a module over K with $\dim_K(\widetilde{V}) = \dim_L(V)$. Every irreducible KX-submodule of $\widetilde{V}$ is a natural module over K or a Galois conjugate by Lemma 2.33. Assume for a contradiction that there is an indecomposable KX-invariant section V_0 of $\widetilde{V}$ of dimension four. Again we can assume that T does not act quadratically on V_0.

Let W_0 be a 2-dimensional submodule of V_0 and let $\sigma \in \mathrm{Aut}(K)$ such that $(V_0/W_0)^\sigma$ and W_0 are isomorphic as KX-modules. Find $0 \leqslant s < n$ such that σ raises elements of k to the power 2^s. Set $U = C_{W_0}(T)$ then U is a 1-dimensional subspace of W_0 as is $C_{W_0}(t)$ for each $t \in T^\#$ so $U = C_{W_0}(t)$ also. Let R be the preimage in V_0 of $C_{V_0/W_0}(T)$ then R has dimension three and $[R, T] \leqslant W_0$. For each $t \in T$, $[R, t, t] = 0$ and so $[R, t] \leqslant C_{W_0}(t) = U$. Thus $[R, T] = U$.

Since W_0 is 2-dimensional, by Lemma 1.1, we get $[W_0, T, T] = 0$ and since $U = C_{W_0}(T)$ is 1-dimensional, we get $U = [W_0, T]$. Similarly $R/W_0 = [V_0/W_0, T]$ and so $R = W_0 + [V_0, T]$. Since H is transitive on the non-trivial elements of T, H is transitive on the spaces $[V_0, t]$ for $t \in T^\#$ as $[v, t^h] = v\cdot(t^h) - v = (v\cdot h^{-1})\cdot t\cdot h - (v\cdot h^{-1})\cdot h \in [V_0, t]\cdot h$. Now if $[V_0,t,T]=0$ for all $t\in T$ then $[V_0,T,T]=0$. So for some $t\in T^\#$ (and thus all $t\in T^\#$) we have $[V_0,t,T]\neq 0$. The space $[V_0,t]$ is invariant under T so using that $[V_0,t]\leqslant R$ and $[R,T]=U$ we have $0\neq[V_0,t,T]\leqslant[V_0,t]\cap[R,T]=[V_0,t]\cap U$. Thus $U\leqslant[V_0,t]$ for each $t\in T$. If $[V_0,t]$ has dimension one then $[V_0,t]=U$ but then $[V_0,t,T]=0$ and so this containment is strict. Since $[V_0,t,t]=0$, $[V_0,t]\neq[V_0,T]$ else $[V_0,T,t]=0$ for every $t\in T$ and again we would have $[V_0,T,T]=0$. So we have $U\lneqq[V_0,t]\lneqq[V_0,T]=R$. Also, $U\leqslant C_{V_0}(T)\leqslant C_{V_0}(t)$ and $[V_0,t]\leqslant C_{V_0}(t)\lneqq R$. It follows from the dimensions that $C_{V_0}(t)=[V_0,t]$ and when we observe that $[V_0,t]\neq C_{V_0}(T)$ (else $[V_0,t,T]=0$) we get

$$U=C_{V_0}(T)\lneqq[V_0,t]=C_{V_0}(t)\lneqq[V_0,T]=R.$$

Now R/U is a 2-dimensional KH-module so by Maschke's Theorem it is completely reducible. By Lemma 2.2, all irreducible submodules are 1-dimensional. Therefore, we can find some 2-dimensional H-invariant submodule $D\leqslant R$ with $D\cap W_0=U$ and $D+W_0=R$ and since $C_{V_0}(T)=U$, $[D,T]\neq 0$. We see immediately that $[D,T]=U$ since $[D,T]\leqslant[R,Y]=U$. Consider the map,

$$\begin{array}{rcl}\alpha\ :\ T & \longrightarrow & \mathrm{Hom}_K(D/U,U)\\ t & \longmapsto & \lambda_t,\end{array}$$

where $\lambda_t: d+U\mapsto[d,t]$. This map is well defined as $[U,T]=0$. Also, since α is non-zero and both T and $\mathrm{Hom}_K(D/U,U)$ are 1-dimensional, α is an isomorphism. By Lemma 8.7, we see T is a KH-module with H-action $t\cdot h=h^{-1}th$ and $\mathrm{Hom}_K(D/U,U)$ is a KH-module with H-action described by $(f\cdot h)(x)=f(x\cdot h^{-1})\cdot h$ for $f\in\mathrm{Hom}_K(D/U,U)$,

$h \in H$ and $x \in D/U$. Thus, for $t \in T$, $h \in H$, and $d + U \in D/U$ we get

$$\begin{aligned}
(\lambda_t \cdot h)(d+U) &= \lambda_t(d + U \cdot h^{-1}) \cdot h \\
&= \lambda_t(d \cdot h^{-1} + U) \cdot h \\
&= [d \cdot h^{-1}, t] \cdot h \\
&= (d \cdot h^{-1} \cdot t - d \cdot h^{-1}) \cdot h \\
&= d \cdot h^{-1} \cdot t \cdot h - d \cdot h^{-1} \cdot h \\
&= [d, t \cdot h] \\
&= \lambda_{t \cdot h}(d+U).
\end{aligned}$$

Therefore $\alpha(t \cdot h) = \lambda_{t \cdot h} = \lambda_t \cdot h = \alpha(t) \cdot h$ and so α is an LH-module isomorphism.

We have $D/U = D/W_0 \cap D \cong W_0 + D/W_0 = R/W_0$ as KH-modules so we can apply Lemma 8.7 (i) to show there exists some $\beta \in \mathrm{Gal}(K/L) = \mathrm{Aut}(K)$ such that for each non-zero $k \in K$, $\beta(k^2) = k^{-1}\sigma(k)$. We find $0 \leqslant b < n$ such that $\beta(k) = k^{2^b}$. Thus $(k^2)^{2^b} = k^{-1}k^2$ and therefore $2^{b+1} \equiv 2^s - 1 \bmod 2^n - 1$. Since $b, s < n$, $2^{b+1} - 2^s + 1 = 2^n - 1$ and then it follows that $s = 1$ and $b = n - 1$.

Consider the map,

$$\begin{aligned}
\gamma \ : \ T &\longrightarrow \mathrm{Hom}_K(V_0/R, R/D) \\
t &\longmapsto \mu_t,
\end{aligned}$$

where $\mu_t : v + R \mapsto [v, t] + D$. We proceed as before. Firstly μ_t is well defined as $[R, T] = U \leqslant D$. Also, γ is non-zero as $R = [V_0, T]$ and both T and $\mathrm{Hom}_K(V_0/R, R/D)$ are 1-dimensional so γ is an isomorphism. As before T and $\mathrm{Hom}_K(V_0/R, R/D)$ are KH-

modules. Thus for $t \in T$, $h \in H$, and $v + R \in V_0/R$ we get

$$\begin{aligned}(\lambda_t \cdot h)(v+R) &= \lambda_t(v + R \cdot h^{-1}) \cdot h \\ &= \lambda_t(v \cdot h^{-1} + R) \cdot h \\ &= [v \cdot h^{-1}, t] + D \cdot h \\ &= (v \cdot h^{-1} \cdot t - v \cdot h^{-1} + D) \cdot h \\ &= v \cdot h^{-1} \cdot t \cdot h - v \cdot h^{-1} \cdot h + D \\ &= [v, t \cdot h] + D \\ &= \lambda_{t \cdot h}(v + R).\end{aligned}$$

Thus $\gamma(t \cdot h) = \lambda_{t\cdot h} = \lambda_t \cdot h = \gamma(t) \cdot h$ and so γ is an LH-module isomorphism.

Now $R/D = D + W_0/D \cong W_0/(W_0 \cap D) = W_0/U$ as KH-modules so we can apply Lemma 8.7 (iv) to show there exists some $\delta \in \mathrm{Gal}(K/L)$ such that for each non-zero $k \in K$, $\delta(k^2) = k\sigma(k^{-1})$. So, as before, we have some $0 \leqslant d < n$ such that $\delta(k) = k^{2^d}$ and then $2^{d+1} \equiv -2^s + 1 \bmod 2^n - 1$. Therefore $2^n - 1$ divides $2^{d+1} + 2^s - 1 = 2^{d+1} + 1$ as $s = 1$. It follows that $2^n - 1 = 2^{d+1} + 1$ and then $d = 0$ and $n = 2$. So suppose $X \cong \mathrm{SL}_2(4)$. Then T is normalized by an element of order three. Moreover, the element of order three, x say, acts fixed-point-freely on T and fixed-point-freely on V_0. Let vt be some element of the split semidirect product V_0T that is fixed by x. Then $(vt)^x = vt$ and so $v^{-1}v^x = tt^{-x} \in V_0 \cap T = 1$. Thus $v^x = v$ and $t^x = t$ and so $C_{V_0T}(x) = C_{V_0}(x)C_T(x)$. This means x acts fixed-point-freely on the split semidirect product V_0T. Thus by a lemma of Burnside, 1.24, V_0T has nilpotence class at most two. This gives a contradiction since now $1 = [V_0T, V_0T, V_0T] \geqslant [V_0, T, T]$ and so T acts quadratically on V_0. □

Corollary 8.9. *Let V be an LX-module such that an element of order three in X acts fixed-point-freely on V. Then V is completely reducible as a product of natural modules for L.*

Proof. By Lemma 8.5, the only irreducible submodules of V are natural modules over L.

Suppose V is not completely reducible then there must be some submodule of dimension $4n$ which cannot be reduced and satisfies Lemma 8.8 which is a contradiction. $\square$

Lemma 8.10. *Let G be a finite group with a normal 2-subgroup, Q, such that $X := G/Q \cong \mathrm{SL}_2(2^n)$ for some $n \geqslant 2$ and some element of order three in G acts fixed-point-freely on Q. Suppose G is minimal subject to Q being non-elementary abelian then Q is abelian.*

Proof. Suppose Q is non-abelian then by minimality, $\Phi(Q) = Q' = Z(Q) = \Omega_1(Q)$. Set $\overline{Q} = Q/\Phi(Q)$ then $\overline{Q}$ and Q' are LX-modules (where vector addition is group multiplication and the action of X is by conjugation) admitting an element of order three acting fixed-point-freely. Construct the KX-modules $A := \overline{Q} \otimes_L K$ and $B := Q' \otimes_L K$ then these also admit a fixed-point-free element of order three.

We define a surjective map,

$$\begin{array}{rrcl} \phi & : \quad A \times A & \rightarrow & B \\ & (\overline{p} \otimes_L k_1, \overline{q} \otimes_L k_2) & \mapsto & [p,q] \otimes_L k_1 k_2, \end{array}$$

We need to check that ϕ is K-balanced (see Definition 2.7). Let $\overline{p}, \overline{q}, \overline{r} \in \overline{Q}$, $k, k_1, k_2 \in K$. Then

$$\begin{aligned} \phi((\overline{pq} \otimes k_1, \overline{r} \otimes k_2)) &= [pq, r] \otimes k_1 k_2 \\ &= [p,r][q,r] \otimes k_1 k_2 \\ &= [p,r] \otimes k_1 k_2 + [q,r] \otimes k_1 k_2 \\ &= \phi((\overline{p} \otimes k_1, \overline{r} \otimes k_2)) + \phi((\overline{q} \otimes k_1, \overline{r} \otimes k_2)) \end{aligned}$$

and

$$\begin{aligned}\phi((\overline{p}\otimes k+k_1,\overline{q}\otimes k_2)) &= [p,q]\otimes(k+k_1)k_2\\ &= [p,q]\otimes kk_2+k_1k_2\\ &= [p,q]\otimes kk_2+[p,q]\otimes k_1k_2\\ &= \phi((\overline{p}\otimes k,\overline{q}\otimes k_2))+\phi((\overline{p}\otimes k_1,\overline{q}\otimes k_2))\end{aligned}$$

and finally

$$\begin{aligned}k\phi((\overline{p}\otimes k_1,\overline{q}\otimes k_2)) &= k[p,q]\otimes k_1k_2\\ &= [p,q]\otimes kk_1k_2\\ &= \phi((\overline{p}\otimes kk_1,\overline{q}\otimes k_2))\\ &= \phi((\overline{p}\otimes k_1,\overline{q}\otimes kk_2)).\end{aligned}$$

The map is bilinear in the second coordinate in exactly the same way and so ϕ is K-balanced. By the definition of $A\otimes_K A$, there must be a K-homomorphism $\alpha : A\otimes_K A\to B$ such that $\alpha\theta_T=\phi$ where $\theta_T : A\times A\to A\otimes_K A$ is the map $\theta_T : (\overline{p},\overline{q})\mapsto\overline{p}\otimes_K\overline{q}$. We aim to show the action of X on these modules commutes with α. So let $x\in X$, $k\in K$ and $p,q\in Q$. Then

$$\phi((\overline{p}\otimes k_1,\overline{q}\otimes k_2))\cdot x=[p^x,q^x]\otimes k_1k_2=\phi(\overline{p}^x\otimes k_1,\overline{q}^x\otimes k_2)=\phi((\overline{p}\otimes k_1,\overline{q}\otimes k_2)\cdot x)$$

and

$$\theta_T((\overline{p}\otimes k_1,\overline{q}\otimes k_2))\cdot x=(\overline{p}\otimes k_1)\otimes_K(\overline{q}\otimes k_2)\cdot x=(\overline{p}^x\otimes k_1)\otimes_K(\overline{q}^x\otimes k_2)=\theta_T((\overline{p}\otimes k_1,\overline{q}\otimes k_2)\cdot x).$$

So ϕ and θ_T commute with the action of X and since $\alpha\theta_T=\phi$, α commutes with the action of X also. So α is a KX-homomorphism. However, by Corollary 8.3, such a map must be the zero map and so Q must be abelian. $\square$

Theorem 8.11. *Let G be a finite group with a normal 2-subgroup, Q, such that $X := G/Q\cong \mathrm{SL}_2(2^n)$ for some $n\geqslant 2$ and some element of order three in G acts fixed-point-freely on Q. Then Q is elementary abelian and a direct product of natural modules.*

Proof. If Q were elementary abelian and hence an LX-module then by Corollary 8.9, we would be done. Thus all rests on proving Q is elementary abelian.

Let G be a minimal counter example to the theorem. Then Q is not elementary abelian but Q is abelian by Lemma 8.10 and so contains elements of order four. By minimality, $Q/\Omega_1(Q)$ is elementary abelian and therefore Q has exponent four. Let W be the characteristic subgroup of Q generated by all elements of order four. Then $W/\Omega_1(W)$ is an LX-module and so is decomposable into a direct product of natural modules. Let W_1 be the preimage in W of some irreducible submodule of $W/\Omega_1(W)$. Then the irreducible submodule has dimension $2n$ and so W_1 is a direct product of $2n$ cyclic groups of order four. Since X acts on W_1, there is a homomorphism $\Phi : X \to \mathrm{Aut}(W_1) \cong \mathrm{Aut}(\mathbb{Z}_4 \times \ldots \times \mathbb{Z}_4)$. In Section 1.5 we investigated such groups and saw that each element of X can be viewed as a $2n \times 2n$ matrix with entries in $\mathbb{Z}_4$ and with odd determinant. We also saw how each of these matrices acts on the natural module $W_1/\Omega_1(W_1)$ and that the corresponding representation simply restricts matrix entries modulo 2. By Lemma 1.35, we have the map

$$\alpha \quad : \quad X \quad \longrightarrow \quad \mathrm{GL}_{2n}(\mathbb{Z}_4)$$

and the representation affording the natural LX-module

$$\beta \quad : \quad X \quad \longrightarrow \quad \mathrm{GL}_{2n}(2)$$

where for each $x \in X$, the entries in $\alpha(x)$ are congruent modulo 2 to the entries in $\beta(x)$.

We saw in Lemma 2.35 that given any algebraic conjugate of the natural KX-module, we can view it as a module over L and as such it is the natural LX-module. We represent elements of X as 2×2 matrices with entries in K. We then obtain a natural LX-representation as follows. The field K is a vector space of dimension n over L and each $a \in K$ defines an L-linear transformation, namely, for each $a \in K$, $\lambda_a : k \mapsto ak$ for each

$k \in K$. So if we fix a basis for K over L we can make the n-dimensional matrix with entries in L representing λ_a. We will call this matrix $[a]$ for each $a \in K$. Notice that the map $K^\times \to \mathrm{GL}_n(2)$ is a homomorphism and in particular this means for $a, b \in K^\times$ $[a][b] = [b][a]$. Now consider the map

$$\beta_1 \ : \ X \ \longrightarrow \ \mathrm{GL}_{2n}(2)$$

such that $\beta_1 : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} [a] & [b] \\ [c] & [d] \end{pmatrix}$. Then β_1 is a natural LX-representation of X. The natural LX-representation is unique up to equivalence. Lemma 1.35 implies that there is a homomorphism $\alpha_1 : X \to \mathrm{GL}_{2n}(\mathbb{Z}_4)$ such that for each $x \in X$ entries of $\alpha_1(x)$ are congruent modulo 2 to entries of $\beta_1(x)$. Consider the images of the matrices $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ for each $a \in K$. It follows that such a matrix is represented via α_1 as

$$\begin{pmatrix} I + 2A_1 & [a] + 2A_2 \\ 0 + 2A_3 & I + 2A_4 \end{pmatrix}$$

where A_1, A_2, A_3, A_4 are $n \times n$ matrices with $0, 1$ entries. This matrix has order two and so we can simplify to get

$$\begin{pmatrix} I + 2A_1 & [a] + 2A_2 \\ 0 & -I + 2[a]^{-1}A_1[a] \end{pmatrix}.$$

We can now choose non-zero elements $a, b, c \in K$ such that $a + b + c = 0$ thus we follow the same process for a, b and c and we see

$$\begin{pmatrix} I + 2A_1 & [a] + 2A_2 \\ 0 & -I + 2[a]^{-1}A_1[a] \end{pmatrix} \begin{pmatrix} I + 2B_1 & [b] + 2B_2 \\ 0 & -I + 2[b]^{-1}B_1[b] \end{pmatrix} \begin{pmatrix} I + 2C_1 & [c] + 2C_2 \\ 0 & -I + 2[c]^{-1}C_1[c] \end{pmatrix}$$

is equal to the identity matrix. This gives that $A_1 + B_1 + C_1$ is the zero matrix and $[a]^{-1}A_1[a] + [b]^{-1}B_1[b] + [c]^{-1}C_1[c]$ is the identity matrix. Now consider Corollary 2.12. We can view $[a]$, $[b]$ and $[c]$ as matrices over K and so there exists $M \in \mathrm{GL}_n(K)$ such that $[a]^M = \mathrm{diag}(a)$, $[b]^M = \mathrm{diag}(b)$ and $[c]^M = \mathrm{diag}(c)$. Since A_1, B_1 and C_1 are in $M_n(2)$, it makes sense to conjugate each by M and so we have the following.

$$I = I^M = ([a]^{-1})^M A_1^M [a]^M + ([b]^{-1})^M B_1^M [b]^M + ([c]^{-1})^M C_1^M [c]^M = A_1^M + B_1^M + C_1^M = 0^M$$

which is a contradiction. Therefore, there is no minimal counter example and so Q is elementary abelian and a direct product of natural modules over L. $\square$

Appendix

Lemma A. 1. *Let p be a prime and let a and b be natural numbers. Then $p^a - 1$ divides $p^b - 1$ if and only if a divides b.*

Proof. If a divides b then we can write $p^b - 1 = (p^a - 1)(p^{b-a} + p^{b-2a} + \ldots + p^a + 1)$ and so $p^a - 1$ divides $p^b - 1$. So assume that $p^a - 1$ divides $p^b - 1$. Choose an integer k so that $ka \leq b < (k+1)a$. Then $p^a - 1$ divides $p^{ka} - 1$ and so $p^a - 1$ divides $p^b - 1 - (p^{ka} - 1) = p^{ka}(p^{b-ka} - 1)$. Since $p^a - 1$ is coprime to p, $p^a - 1$ divides $p^{b-ka} - 1$. But $p^{b-ka} - 1 < p^a - 1$ by the choice of k. So $p^{b-ka} - 1 = 0$ and this means that $b = ka$ as required. □

Lemma A. 2. *Let p be a prime and let m and n be natural numbers with greatest common divisor g. Then $p^g - 1$ is the greatest common divisor of $p^n - 1$ and $p^m - 1$ for any prime p.*

Proof. Since g divides m and n, $p^g - 1$ is a common divisor of both $p^n - 1$ and $p^m - 1$. Let us assume $m > n$ and m is not a multiple of n or else the result holds trivially. We will use the Euclidean algorithm with $p^n - 1$ and $p^m - 1$ to find their greatest common divisor. Find the integer k such that $0 < m - kn < n$. Notice that $p^m - 1 = (p^n - 1)p^{m-n} + (p^{m-n} - 1)$ and also $p^{m-n} - 1 = (p^n - 1)p^{m-2n} + (p^{m-2n} - 1)$. So substituting the second into the first gives

$$p^m - 1 = (p^n - 1)(p^{m-n} + p^{m-2n}) + (p^{m-2n} - 1)$$

and we continue in this way k times to get

$$p^m - 1 = (p^n - 1)(p^{m-n} + p^{m-2n} + \ldots + p^{m-kn}) + (p^{m-kn} - 1).$$

This gives the first step in the Euclidean algorithm and so we have $\mathrm{GCD}(p^m - 1, p^n - 1) = \mathrm{GCD}(p^n - 1, p^{m-kn} - 1)$. We continue in this way until the process terminates and we have that the greatest common divisor of $p^m - 1$ and $p^n - 1$ has the form $p^l - 1$ for some positive integer l. But now we have that l divides both n and m and so l divides g and furthermore $p^l - 1$ divides $p^g - 1$. Thus $p^g - 1$ is the greatest common divisor of $p^m - 1$ and $p^n - 1$. □

Lemma A. 3. *Let p be a prime and let F be a field of order p^n for some natural number n. Then any subfield of F has order p^m where m divides n. Furthermore if m divides n then there is a subfield of F of order 2^m.*

Proof. Suppose K is a subfield of F then K is a field of characteristic p so has order p^m for some $m \leqslant n$. Also $K^\times$ is a subgroup of $F^\times$. So $p^m - 1$ divides $p^n - 1$. However this can only occur when m divides n.

So suppose now that some natural number m divides n. The group $F^\times$ is cyclic of order $p^n - 1$. Since $p^m - 1$ divides $p^n - 1$, there is a unique subgroup H say of $F^\times$ of order $p^m - 1$. We claim $K := \{H, 0_F\}$ is a subfield of F of order p^m. We need to check K is closed under addition. So let $a, b \in K$. If either a or b is zero it is clear that $a + b \in K$ so we will assume $a, b \in H$ then both a and b have order dividing $p^m - 1$ so $a^{p^m} = a$ and $b^{p^m} = b$. Notice that for any natural number r,

$$(a+b)^r = a^{p^m} + ra^{r-1}b + \frac{r(r-1)}{2}a^{r-2}b^2 + \ldots rab^{r-1} + b^r.$$

So if $r = p^m$ then $(a+b)^{p^m} = a^{p^m} + b^{p^m} = a + b$. Thus either $(a+b)^{p^m-1} = 1$ or $a + b = 0$. If $(a+b)^{p^m-1} = 1$ then $a + b$ lies in the unique subgroup, H, of $F^\times$ of order $p^m - 1$. In either case $a + b \in K$ so K is closed under addition. Now we show K contains additive inverses. We have seen that K is closed under addition so fix some non-zero $k \in K$. Then define a map $\tau : K \to K$ such that for $l \in K$, $\tau : l \mapsto l + k$. This map is clearly injective and since K is a finite set, it must be surjective. In particular this means that there exists some $l \in K$ such that $l + k = 0$ and so K has additive inverses. All other axioms follow trivially so K is a subfield of F. $\square$

Lemma A. 4. *Let G be a faithful completion of an amalgam of type $G_2(3)$ and Γ the coset graph. Then G is locally 7-arc transitive on Γ.*

Proof. Let $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7)$ be a path of seven vertices. By Lemma 3.4, it is necessary to prove that the stabilizer of the path $(\alpha_1, \alpha_2, \ldots, \alpha_i)$ is transitive on $\Gamma(\alpha_i)\backslash\{\alpha_{i-1}\}$ for each $i \leqslant 7$. By the Orbit-Stabilizer Theorem, it is enough to show $|G_{\alpha_1,\alpha_2,\ldots,\alpha_i} : G_{\alpha_1,\alpha_2,\ldots,\alpha_{i+1}}| = 3$ for each $i \leqslant 7$. We apply Lemma 6.4 and Lemma 6.1 several times. Firstly $i = 1$ is just edge transitivity which is always true in a coset graph. When $i = 2$, $G_{\alpha_1\alpha_2} \cap G_{\alpha_2\alpha_3}$ has Sylow 3-subgroup $S_{\alpha_1\alpha_2} \cap S_{\alpha_2\alpha_3} = Q_{\alpha_2}$ and so 3 divides $|G_{\alpha_1,\alpha_2} : G_{\alpha_1,\alpha_2,\alpha_3}|$. When $i = 3$, $G_{\alpha_1,\alpha_2,\alpha_3} \cap G_{\alpha_2,\alpha_3,\alpha_4}$ has Sylow 3-subgroup, $Q_{\alpha_2} \cap Q_{\alpha_3} = Q_{\alpha_2\alpha_3}$, with order 3^4 and so 3 divides $|G_{\alpha_1,\alpha_2,\alpha_3} : G_{\alpha_1,\alpha_2,\alpha_3,\alpha_4}|$. When $i = 4$, $G_{\alpha_1,\alpha_2,\alpha_3,\alpha_4} \cap G_{\alpha_2,\alpha_3,\alpha_4,\alpha_5}$ has Sylow 3-subgroup, $Q_{\alpha_2\alpha_3} \cap Q_{\alpha_3\alpha_4} = Z_{\alpha_3}$, with order 3^3 and so 3 divides $|G_{\alpha_1,\alpha_2,\alpha_3,\alpha_4} : G_{\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5}|$. When $i = 5$, $G_{\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5} \cap G_{\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6}$ has Sylow 3-subgroup, $Z_{\alpha_3} \cap Z_{\alpha_4} = Z_{\alpha_3\alpha_4}$, with order 3^2 and so 3 divides $|G_{\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5} : G_{\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6}|$. When $i = 6$ $G_{\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6} \cap G_{\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6,\alpha_7}$ has Sylow 3-subgroup, $Z_{\alpha_3\alpha_4} \cap Z_{\alpha_4\alpha_5} = Y_{\alpha_4}$, with order 3 and so 3 divides $|G_{\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6} : G_{\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6,\alpha_7}|$. When $i = 7$ $G_{\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6,\alpha_7} \cap G_{\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6,\alpha_7,\alpha_8}$ has Sylow 3-subgroup, $Y_{\alpha_4} \cap Y_{\alpha_5} = 1$, and so 3 divides $|G_{\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6,\alpha_7} : G_{\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6,\alpha_7,\alpha_8}|$. Hence G acts locally 7-arc transitive on Γ. $\square$

Bibliography

[1] M. Aschbacher. *Finite group theory*, volume 10 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 2000.

[2] Michael Aschbacher. *Sporadic groups*, volume 104 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1994.

[3] Helmut Bender. Transitive Gruppen gerader Ordnung, in denen jede Involution genau einen Punkt festläßt. *J. Algebra*, 17:527–554, 1971.

[4] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[5] Andrew Chermak. A class of p-local finite groups of local characteristic p. *Unpublished*, 2007.

[6] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups*. Clarendon Press, Oxford, 1985.

[7] A. Delgado, D. Goldschmidt, and B. Stellmacher. *Groups and graphs: new results and methods*, volume 6 of *DMV Seminar*. Birkhäuser Verlag, Basel, 1985. With a preface by the authors and Bernd Fischer.

[8] Klaus Doerk and Trevor Hawkes. *Finite soluble groups*, volume 4 of *de Gruyter Expositions in Mathematics*. Walter de Gruyter & Co., Berlin, 1992.

[9] Walter Feit and John G. Thompson. Finite groups which contain a self-centralizing subgroup of order 3. *Nagoya Math. J.*, 21:185–197, 1962.

[10] Rachel Fowler. *A 3-local characterization of the Thompson sporadic simple group*. PhD thesis, 2006.

[11] Rachel Fowler and Christopher Parker. A 3-local characterization of the Thompson sporadic simple group. In preparation.

[12] David M. Goldschmidt. Automorphisms of trivalent graphs. *Ann. of Math. (2)*, 111(2):377–406, 1980.

[13] Daniel Gorenstein. *Finite groups*. Chelsea Publishing Co., New York, second edition, 1980.

[14] Daniel Gorenstein, Richard Lyons, and Ronald Solomon. *The classification of the finite simple groups. Number 3.*, volume 40.3 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1998.

[15] Robert L. Griess, Jr. Automorphisms of extra special groups and nonvanishing degree 2 cohomology. *Pacific J. Math.*, 48:403–422, 1973.

[16] John L. Hayden. A characterization of the finite simple group $\mathrm{PSp}_4(3)$. *Canad. J. Math.*, 25:539–553, 1973.

[17] Graham Higman. *Odd Characterisations of Finite Simple Groups, Lecture Notes of University of Michigan*. Ann Arbor. 1968.

[18] Christopher Hillar and Darren Rhea. Automorphisms of finite abelian groups. *Unpublished*.

[19] I. Martin Isaacs. *Character theory of finite groups.* Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1976. Pure and Applied Mathematics, No. 69.

[20] Hans Kurzweil and Bernd Stellmacher. *The theory of finite groups.* Universitext. Springer-Verlag, New York, 2004. An introduction, Translated from the 1998 German original.

[21] Jack McLaughlin. Some groups generated by transvections. *Arch. Math. (Basel)*, 18:364–368, 1967.

[22] Christopher Parker and Peter Rowley. *Symplectic amalgams.* Springer Monographs in Mathematics. Springer-Verlag London Ltd., London, 2002.

[23] Christopher Parker and Peter Rowley. Local characteristic p completions of weak BN-pairs. *Proc. London Math. Soc. (3)*, 93(2):325–394, 2006.

[24] A. R. Prince. A characterization of the simple groups PSp(4, 3) and PSp(6, 2). *J. Algebra*, 45(2):306–320, 1977.

[25] Arthur Ranum. The group of classes of congruent matrices with application to the group of isomorphisms of any abelian group. *Trans. Amer. Math. Soc.*, 8(1):71–91, 1907.

[26] Jean-Pierre Serre. *Trees.* Springer-Verlag, Berlin, 1980. Translated from the French by John Stillwell.

[27] Stephen D. Smith and A. P. Tyrer. On finite groups with a certain Sylow normalizer. I, II. *J. Algebra*, 26:343–365; ibid. 26 (1973), 366–367, 1973.

[28] Robert Steinberg. *Endomorphisms of linear algebraic groups.* Memoirs of the American Mathematical Society, No. 80. American Mathematical Society, Providence, R.I., 1968.

[29] Jacques Tits and Richard M. Weiss. *Moufang polygons.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002.