TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 347, Number 5, May 1995

LOCAL SUBGROUPS OF THE MONSTER AND ODD CODE LOOPS

THOMAS M. RICHARDSON

ABSTRACT. The main result of this work is an explicit construction of p-local subgroups of the Monster, the largest sporadic simple group. The groups constructed are the normalizers in the Monster of certain subgroups of order 3^2, 5^2, and 7^2 and have shapes

$$3^{2+5+10}\cdot(M_{11}\times GL(2,3)),\quad 5^{2+2+4}\cdot(S_3\times GL(2,5)),\quad \text{and } 7^{2+1+2}\cdot GL(2,7).$$

These groups result from a general construction which proceeds in three steps. We start with a self-orthogonal code C of length n over the field $\mathbb{F}_p$, where p is an odd prime. The first step is to define a code loop L whose structure is based on C. The second step is to define a group N of permutations of functions from $\mathbb{F}_p^2$ to L. The final step is to show that N has a normal subgroup K of order p^2. The result of this construction is the quotient group N/K of shape $p^{2+m+2m}(S\times GL(2,p))$, where $m+1=\dim(C)$ and S is the group of permutations of $\mathrm{Aut}(C)$.

To show that the groups we construct are contained in the Monster, we make use of certain lattices $\Lambda(C)$, defined in terms of the code C. One step in demonstrating this is to show that the centralizer of an element of order p in N/K is contained in the centralizer of an element of order p in the Monster. The lattices are useful in this regard since a quotient of the automorphism group of the lattice is a composition factor of the appropriate centralizer in the Monster.

This work was inspired by a similar construction using code loops based on binary codes that John Conway used to construct a subgroup of the Monster of shape $2^{2+11+22}\cdot(M_{24}\times GL(2,2))$.

1. INTRODUCTION

The main result of this work is an explicit construction of p-local subgroups of the finite simple group known as the Monster of shapes

$$3^{2+5+10}\cdot(M_{11}\times GL(2,3)),\quad 5^{2+2+4}\cdot(S_3\times GL(2,5)),\quad \text{and}\quad 7^{2+1+2}.GL(2,7).$$

The method that we use is quite general and can be summarized as consisting of three steps:

(1) Given a self-orthogonal code C over a field $\mathbb{F}_p$ for p an odd prime, construct a loop L whose multiplication depends on C.

(2) Construct a group N of permutations of functions from $\mathbb{F}_p^2\to L$.

Received by the editors January 24, 1992 and, in revised form, March 25, 1994.
1991 *Mathematics Subject Classification.* Primary 20D08; Secondary 20N05.
Key words and phrases. Monster group, loops.

0002-9947/95 $1.00 + $.25 per page

(3) Show that N has a normal subgroup K of order p^2 and that N/K has properties which imply the uniqueness of the isomorphism type of of N/K. For certain codes over $\mathbb{F}_3$, $\mathbb{F}_5$, and $\mathbb{F}_7$, the groups that result from this construction turn out to be the subgroups of the Monster mentioned above.

A previous construction of this sort was done by Conway [3], who constructed a subgroup of the Monster of shape $2^{2+11+22} \cdot (M_{24} \times GL(2, 2))$. Also, Griess [10] constructed a subgroup $2^{2+3+6} \cdot (GL(3, 2) \times GL(2, 2))$ of $\mathrm{Spin}(8, \mathbb{C}):S_3$ by similar methods. These constructions were the inspiration of our work, which can be seen as a generalization of them. However, the definition of loops based on codes over $\mathbb{F}_p$ for p odd, or odd code loops, is not an obvious generalization of the construction of loops based on binary codes that Conway and Griess used, though the definition of them is quite simple. The definition of the permutations in step (2) is also not an obvious generalization. This part of the construction is more complicated for us, and much of the added complexity can be attributed to the greater complexity of $GL(2, p)$ for $p > 2$.

Some work is required to show that the groups N/K are subgroups of the Monster in the three particular cases mentioned. Our approach is to show that some properties shared by our groups and the corresponding subgroups of the Monster imply that they are isomorphic. The key property concerns the structure of N_∞, the normalizer in N/K of an element of order p. It turns out that N_∞ has a normal subgroup Q which is an extraspecial group. In addition, the quotient N_∞/Q is isomorphic to a monomial group of automorphisms of a lattice Λ over the ring $\mathbb{Z}[\varepsilon]$, where ε is a primitive pth root of unity. The action of N_∞/Q on Q extends to an action of $\mathrm{Aut}_{\mathbb{Z}[\varepsilon]}(\Lambda)$ on Q. Again, this part of the construction is quite general and can be carried out for any self-orthogonal code over $\mathbb{F}_p$ for p an odd prime.

For the 5- and 7-local subgroups, these properties of N_∞ are enough to prove that N_∞ is a subgroup of the Monster. This is not the case for the 3-local subgroup. In that case, there is another group with structure very similar to that of N_∞, and it is not obvious which is a subgroup of the Monster. We construct representations of N_∞ whose basis elements correspond to certain sets of functions from $\mathbb{F}_3^2$ to the loop L, and we use these representations to show that N_∞ is a subgroup of the Monster.

This paper is organized as follows. In §2 we cover some preliminary results. The construction of odd code loops is carried out in §3. The construction of groups of permutations of "luples" is done in §4. In §5, we study the structure of N_∞ and related lattices. We devote §6 to showing that the subgroup N_∞ of the 3-local group is a subgroup of the Monster. Finally, we prove uniqueness theorems for the three groups that turn out to be subgroups of the Monster in §7.

This work comprises much of the author's Ph.D. thesis written at the University of Michigan under the direction of Professor Robert Griess.

2. Preliminary results

Codes. We begin with some terminology about codes. A *code* is a subspace of a vector space over a finite field $\mathbb{F}_q$. If a code C is a subspace of an n-dimensional vector space we say the n is the *length* of C. If a code word $c \in C$ has w nonzero coordinates we say that w is the *weight* of c and denote it by

$wt(c)$. There is a natural bilinear form on $\mathbb{F}_q^n$ given by $(c, d) = \sum_{i=1}^n c_i d_i$. We let $C^\perp = \{\delta \in \mathbb{F}_q^n \mid (\delta, c) = 0 \ \forall c \in C\}$. If $C = C^\perp$ we say that C is *self-orthogonal.* If we say that a code word has *shape* $(a^i, b^j, \dots)$ we mean that it has i coordinates equal to a, j equal to b, and so on. The *support* of a code word $c = (c_1, \dots, c_n)$ is the set of all i such that $c_i \neq 0$. The automorphism group of a code C of length n consists of all $n \times n$ monomial matrices over $\mathbb{F}_q$ which preserve C as a subspace of $\mathbb{F}_q^n$. We say that codes C and C' are *equivalent* if there is an $n \times n$ monomial matrix which sends C to C'.

Before we discuss in detail the three codes that will be of particular interest to us, we describe some notation that we shall use for groups and group extensions.

Notation for groups and group extensions. We say that a group G has shape $A \cdot B$, or $G \cong A \cdot B$, if G has a normal subgroup isomorphic to A and $G/A \cong B$. Inductively, we say that $G \cong A_1 \cdot A_2 \cdot \cdots \cdot A_n$ if G has a normal subgroup isomorphic to A_1 and $G/A_1 \cong A_2 \cdot \cdots \cdot A_n$. We write $G \cong A{:}B$ if the extension is a split extension.

We will use m to denote a cyclic group of order m, and we use p^n to denote an elementary abelian group of order p^n. We shall sometimes use $p^{a_1+\cdots+a_n}$ to denote a group of shape $p^{a_1} \cdot \cdots \cdot p^{a_n}$. In particular, we will write p^{1+n} for an extraspecial group. Recall that a group P of order p^{1+n} is extraspecial if $Z(P) = P' = \Phi(P)$ and $|P'| = p$. We will write $P \cong p_+^{1+n}$ for an extraspecial group which has exponent p.

The ternary Golay code. The ternary Golay code, which we denote $\mathcal{G}$, is a self-orthogonal code of length 12 over $\mathbb{F}_3$ with minimum weight 6. There are a number of constructions for $\mathcal{G}$ in [18] and [4]. We shall occasionally refer to specific elements of $\mathcal{G}$. Our code $\mathcal{G}$ is the image of the code constructed using the "MiniMog" in [4] by a certain diagonal matrix. The code word $(c_1, \dots, c_{12}) \in \mathcal{G}$ is the image by the matrix

$$\operatorname{diag}(-1, -1, -1, 1, 1, 1, 1, 1, 1, -1, -1, -1)$$

of the word

$-c_1$	c_4	c_7	$-c_{10}$
$-c_2$	c_5	c_8	$-c_{11}$
$-c_3$	c_6	c_9	$-c_{12}$

in the code given by the MiniMog. In $\mathcal{G}$ there are 2×132 words of weight 6, 2×220 words of weight 9, and 2×12 words of weight 12. The automorphism group of $\mathcal{G}$ is $2M_{12}$, the double cover of the Mathieu group M_{12}. The stabilizer of the code word (1^{12}) is the Mathieu group M_{11}, acting as a 3-transitive permutation group of degree 12. Under the action of M_{11}, $\mathcal{G}$ contains three orbits of cosets of (1^{12}): 22 cosets $\{(1^6, 0^6), (0^6, -1^6), (-1^6, 1^6)\}$, 220 cosets $\{(1^3, -1^3, 0^6), (0^3, 1^3, -1^6), (-1^3, 0^3, 1^6)\}$, and 1 coset $\{(0^{12}), (1^{12}), (-1^{12})\}$.

Ward [22] proves the existence and uniqueness of a trilinear form for M_{11} on any faithful irreducible degree 5 representation over $\mathbb{F}_3$. More precisely, he proves that there is a unique irreducible symmetric trilinear form $(\ ,\ ,\ )$ on

$\mathbb{F}_3^5$ such that there are vectors $z \in \mathbb{F}_3^5$ with $(z, z, x) = 0$ for all $x \in \mathbb{F}_3^5$. Then he shows that the automorphism group of $(\ ,\ ,\ )$ is M_{11}.

The Golay code provides a nice way to see this form. For $x, y, z \in \mathcal{G}$, we define $(x, y, z) = \sum_{i=1}^{12} x_i y_i z_i$. It is clear that $(\ ,\ ,\ )$ is invariant under the action of the group M_{11} which fixes (1^{12}), since this M_{11} acts as a group of permutations. By the *radical* of a trilinear form we mean the set of all x such that $(x, y, z) = (y, x, z) = (y, z, x) = 0$ for all y, z. Since $\mathcal{G}$ is self-orthogonal, (1^{12}) is in the radical of the form. Then we check that this is the full radical of the form. There are only two nontrivial orbits of cosets of (1^{12}). The vectors

$$x = (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \qquad \text{and}$$
$$y = (0, 1, 2, 0, 0, 0, 0, 2, 1, 0, 2, 1).$$

are representatives of cosets from the two different orbits. Since $(x, y, y) = 2$, we see that the radical is spanned by (1^{12}). We also note that $(x, x, z) = 0$ for all $z \in \mathcal{G}$ since $\mathcal{G}$ is self-orthogonal. Thus we can regard $(\ ,\ ,\ )$ as a form on $\mathcal{G}/(1^{12})$, and by [22] it is the unique such form on $\mathcal{G}/(1^{12})$.

In §6 we will need to know the structure of $\mathbb{F}_3^{12}$ as a module for the group $M_{11} < \mathrm{Aut}(\mathcal{G})$. We write $\bar{\mathcal{G}}$ for $\mathcal{G}/\langle(1^{12})\rangle$, $\mathcal{G}^*$ for $\mathrm{Hom}(\mathcal{G}, \mathbb{F}_3)$, and $\bar{\mathcal{G}}^*$ for $\mathrm{Hom}(\bar{\mathcal{G}}, \mathbb{F}_3)$.

Lemma 2.1. *The 12-dimensional transitive permutation module of M_{11} over $\mathbb{F}_3$ is uniserial with ascending structure $1 \cdot \bar{\mathcal{G}} \cdot \bar{\mathcal{G}}^* \cdot 1$.*

Proof. Let P be the 12-dimensional transitive permutation module. Certainly $\mathcal{G}$ is a submodule of P, and we claim (1^{12}) has no complement in $\mathcal{G}$. Any complement must contain a vector of shape either $(1^6 0^6)$, $(-1^6 0^6)$, or $(1^6 - 1^6)$, M_{11} is transitive on the sets of vectors of these shapes, and the vectors of any one of these shapes span $\mathcal{G}$, proving the claim.

Since $\mathcal{G}$ is self-orthogonal, we identify $\mathbb{F}_3^{12}/\mathcal{G}$ with $\mathcal{G}^*$ by identifying the coset $(\delta_1, \ldots, \delta_{12}) + \mathcal{G}$ with the map δ defined by $\delta(c) = \sum_{i=1}^{12} \delta_i c_i$. Let $P_0 < P$ be the submodule of P consisting of all δ such that $\sum_{i=1}^{12} \delta_i = 0$. Then P_0 is an M_{11}-submodule of P and $P_0/\mathcal{G} \cong \bar{\mathcal{G}}^*$. We show that P_0 is uniserial as an M_{11} module.

If P_0 is not uniserial, then since the factors of P_0 are isomorphic to $\mathbb{F}_3$, $\bar{\mathcal{G}}$ and $\bar{\mathcal{G}}^*$, and $\mathcal{G} = 1.\bar{\mathcal{G}}$ is a nonsplit module extension, there must be a submodule W with factors isomorphic to $\mathbb{F}_3$ and $\bar{\mathcal{G}}^*$. Now W contains a vector w such that $w = \hat{w} + c$ where $\hat{w}$ is a vector of shape $(1, -1, 0^{10})$, and $c \in \mathcal{G}$. Since M_{11} is a 3-transitive permutation group on the standard basis of P, $\hat{w}$ is in an orbit of size 132 under the action of M_{11}, while c is in an orbit of size 1, 22, or 220.

If c is in an orbit of size 1, then $\hat{w} \in W$. Now the 2-transitivity of M_{11} implies that W contains all vectors of shape $(1, -1, 0^{10})$, so $W = P_0$.

If c is in an orbit of size 22, then W contains a vector $\hat{\hat{w}} + c$ where $\hat{\hat{w}}$ has shape $(1, -1, 0^{10})$ and $\hat{\hat{w}} \neq \hat{w}$. This implies that W contains $w' = \hat{w} - \hat{\hat{w}}$, a vector of weight 2, 3, or 4. If w' has weight 2, then $W = P_0$ as in the previous case. If w' has weight 3, then w' has shape $(1^3, 0^9)$. Now 3-transitivity of M_{11} implies that W contains all vectors of shape $(1^3, 0^9)$, so $W = P_0$. If

w' has weight 4, then w' has shape $(1^2, -1^2, 0^8)$. Now 3-transitivity of M_{11} implies that W contains a vector of weight 2 or 3, since it must contain a pair of vectors that look like

$$(1, 1, -1, -1, 0, 0, 0, 0, 0, 0, 0, 0),$$
$$(1, -1, 1, -1, 0, 0, 0, 0, 0, 0, 0, 0)$$

or

$$(1, 1, -1, -1, 0, 0, 0, 0, 0, 0, 0, 0),$$
$$(1, -1, 1, 0, -1, 0, 0, 0, 0, 0, 0, 0).$$

Now from the previous two cases we have $W = P_0$.

If c is in an orbit of size 220, then W contains elements $\hat{w} + c$ and $\hat{w} + \hat{c}$, with $c \not\equiv \hat{c} \pmod{(1^{12})}$. Thus W contains $c - \hat{c}$, which generates an M_{11}-submodule ismorphic to $\mathscr{G}$, so again $W = P_0$.

Thus each possibility for the orbit of c leads to the conclusion that $W = P_0$, so this shows that P_0 cannot have a submodule W with factors isomorphic to $\mathbb{F}_3$ and $\mathscr{G}^*$. Hence P_0 is uniserial with ascending series $1 \cdot \mathscr{G} \cdot \mathscr{G}^*$. Since P is a permutation module, it is self dual as an M_{11}-module, so we see that it is uniserial with ascending series $1 \cdot \mathscr{G} \cdot \mathscr{G}^* \cdot 1$. □

The Pentacode. The pentacode $\mathscr{F}$ is the code of length 6 and minimum weight 4 over $\mathbb{F}_5$ spanned by

$$a = (1, 0, 1, 0, 2, -2),$$
$$b = (1, 0, 2, -2, 1, 0), \quad \text{and} \quad c = (2, -2, 1, 0, 1, 0).$$

It is easily checked that $\mathscr{F}$ is self-orthogonal. Let $u = -a - b - c = (1, 2, 1, 2, 1, 2)$.

Lemma 2.2. $\mathrm{Aut}(\mathscr{F}) \cong 4 \times S_5$, *and the stabilizer of* $\langle u \rangle$ *is a group* $4 \times S_3 \times 2$.

Proof. First we show that $\mathrm{Aut}(\mathscr{F})$ is 3-transitive on the six coordinate spaces of $\mathbb{F}_5^6$. There is an obvious subgroup $S < \mathrm{Aut}(\mathscr{F})$ of permutation matrices isomorphic to the symmetric group S_3. The group S acts transitively on the sets $\{1, 3, 5\}$ and $\{2, 4, 6\}$ and also preserves the blocks $\{1, 2\}$, $\{3, 4\}$, and $\{5, 6\}$. We check that

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

is in $\mathrm{Aut}(\mathscr{F})$. It is easy to see that $aA = (0, 1, 0, 1, 2, 2) = -a + 2b + 2c \in \mathscr{F}$ and also that bA and cA are in $\mathscr{F}$. This shows that $\mathrm{Aut}(\mathscr{F})$ is transitive on the coordinate spaces.

Next we check that

$$B = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

is in $\mathrm{Aut}(\mathscr{F})$. We have

$$\begin{aligned} aB &= (2, 1, 0, 0, -2, -1) = 2c - 2a, \\ bB &= (1, 1, 0, -2, 0, -2) = a + b + 2c, \qquad \text{and} \\ cB &= (1, 2, 2, 0, 0, -1) = -2a - c, \end{aligned}$$

so $B \in \mathrm{Aut}(\mathscr{F})$. This shows that $\mathrm{Aut}(\mathscr{F})$ is 2-transitive on the coordinate spaces since B acts on them as the permutation $(1, 2, 3, 6, 5)$.

Now we show that

$$C = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

is in $\mathrm{Aut}(\mathscr{F})$. We have

$$aC = (0, 1, 0, 1, 2, 2),$$
$$bC = (-2, 1, 0, 2, 1, 0), \quad \text{and} \quad cC = (0, 2, -2, 1, 1, 0),$$

and these words are clearly in $\mathscr{F}$, since $aC = aA$, and bC and cC are each the image by an element of S of a multiple of cB. This shows that $\mathrm{Aut}(\mathscr{F})$ is 3-transitive on the coordinate spaces since B acts on them as the permutation $(1, 2, 3, 4)$.

We claim that $\mathscr{F}$ contains a single orbit of words of weight 5. Since $\mathscr{F}$ is self-orthogonal, it cannot contain any word of weight 1 or 3. By the 2-transitivity of $\mathrm{Aut}(\mathscr{F})$, it is clear that $\mathscr{F}$ cannot contain any word of weight 2, since some word in its orbit would not be orthogonal to $a = (1, 0, 1, 0, 2, -2)$. Now suppose x and y are two words of weight 5 which are not multiples of each other and which are zero on the same coordinate. We may assume that every nonzero entry of x and y is ± 1. Thus either $x + y$ or $x - y$ has weight less than 4, a contradiction. Now transitivity of $\mathrm{Aut}(\mathscr{F})$ implies there is a single orbit of words of weight 5.

Next we show that $\mathrm{Aut}(\mathscr{F})$ is not 4-transitive on the coordinate spaces. Two words of weight 5 in $\mathscr{F}$ are

$$r = (1, 0, -1, -1, -1, -1) \quad \text{and} \quad s = (-1, -1, -1, -1, 1, 0).$$

Suppose that $D \in \mathrm{Aut}(\mathscr{F})$ and D fixes each of the first three coordinate spaces. Then rD is a multiple of r, and by multiplying D by a scalar if necessary we may assume $rD = r$. Thus D must act trivially on the first three coordinate

spaces and as a permutation on the last three coordinate spaces. But if D acts as a nontrivial permutation on the last three coordinate spaces, we find that sD is not orthogonal to s, contradicting the self-orthogonality of $\mathscr{F}$. Thus D is the identity and so $\mathrm{Aut}(\mathscr{F})$ is not 4-transitive.

Next we show that the only diagonal elements of $\mathrm{Aut}(\mathscr{F})$ are scalars. Suppose that D is the matrix $\mathrm{diag}(\alpha_1, \ldots, \alpha_6) \in \mathrm{Aut}(\mathscr{F})$. Then D sends r and s to multiples of themselves. By looking at rD we see that $\alpha_3 = \alpha_4 = \alpha_5 = \alpha_6$ and by looking at sD we see that $\alpha_1 = \alpha_2 = \alpha_3 = \alpha_4$, so D is a scalar.

Also, the image of $\mathrm{Aut}(\mathscr{F})$ in S_6 is 3-transitive and not 4-transitive, so it must isomorphic to S_5. Thus $\mathrm{Aut}(C)$ is a group of shape $4 \cdot S_5$. Now let $\mathrm{Aut}_0(\mathscr{F})$ be the subgroup of $\mathrm{Aut}(\mathscr{F})$ consisting of the matrices whose nonzero entries are ± 1, so $\mathrm{Aut}_0(\mathscr{F})$ is a group of shape $2 \cdot S_5$, and let A_0 be the subgroup of $\mathrm{Aut}_0(\mathscr{F})$ of shape $2 \cdot A_5$. The elements of the group S which interchange a pair of blocks have order 2, and they act as even permutations on the six coordinate spaces. Hence they are contained in A_0, implying that $A_0 \cong 2 \times A_5$. Now A is an element of $\mathrm{Aut}_0(\mathscr{F})$ which has order 4 but acts on the coordinate spaces as an involution. Thus $\mathrm{Aut}_0(\mathscr{F})$ is a nonsplit extension $2 \cdot S_5$. Finally, we have $\mathrm{Aut}(C) \cong 4 \times S_5$, since the matrix A' gotten by multiplying A by an appropriate scalar normalizes $A_0' \cong A_5$ and has order 2.

The stabilizer of the word $u = (1, 2, 1, 2, 1, 2)$ is easily seen to contain A and the subgroup S of block permutations. The block permutations and A obviously commute, so they generate a group of order 24 isomorphic to $4 \times S_3$. Furthermore, the group generated by S_3, A, and the scalars is the maximal subgroup $4 \times S_2 \times S_3$ of $4 \times S_5$, and B does not fix $\langle u \rangle$, proving the last statement. □

Lemma 2.3. *Let* $S_u = \mathrm{stab}_{\mathrm{Aut}(\mathscr{F})}(\langle u \rangle)$, *let* $c_1 = (1, -2, -1, 2, 0, 0)$, *and let* $c_2 = (0, 0, 1, -2, -1, 2)$. *Then* S_u *stabilizes* $\mathscr{F}_0 = \langle c_1, c_2 \rangle < \mathscr{F}$, *a complement of* u *under the action of* S_u.

Proof. In the proof of the previous lemma we saw that S_u is generated by the scalars, S, and A. Obviously the scalars stabilize $\mathscr{F}_0$, and for any $c \in \mathscr{F}_0$ we have $cA = 2c$. Finally, we note that $c_1 + c_2 = (1, -2, 0, 0, -1, 2)$, so S stabilizes $\mathscr{F}_0$. □

The Heptacode. The last code we study in detail is the heptacode $\mathscr{H}$, the code of length 4 and minimum weight 3 over $\mathbb{F}_7$ spanned by

$$u = (-2, 1, 1, 1) \qquad \text{and} \qquad b = (0, 1, 2, -3).$$

It is easy to check that $\mathscr{H}$ is self-orthogonal.

Lemma 2.4. $\mathrm{Aut}(\mathscr{H}) \cong 3 \times 2A_4 \cong 3 \times SL(2, 3)$, *and the stabilizer of* $\langle u \rangle$ *is a group* 6×3.

Proof. The matrices

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

are in $\mathrm{Aut}(\mathscr{K})$, since $uA = u$ and $bA = 2b$, while $uB = (1, 2, 1, -1) = 3u - b$ and $bB = (1, 0, -3, -2) = 3u - 3b$ are in $\mathscr{K}$. We claim that the group generated by A and B is the double cover of A_4. It is clear that $\langle A, B\rangle$ acts on the coordinate spaces as A_4. We compute that

$$B^A = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix},$$

so it is easy to verify that $[B, B^A] = \mathrm{diag}(-1^4)$. Thus $\langle B^A, B\rangle$ is isomorphic to the quaternion group of order 8, so $\langle A, B\rangle$ is isomorphic to $SL(2, 3)$, the double cover of A_4. We claim that $\mathrm{Aut}(\mathscr{K})$ cannot permute the coordinate spaces as S_4. If so, it would contain a matrix

$$C = \begin{pmatrix} x & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & y \\ 0 & 0 & z & 0 \end{pmatrix}$$

for some $x, y, z \in \mathbb{F}_7$. Then $bC = (0, 1, 4z, 2y)$, which implies that $z = 4$ and $y = 2$. This implies that $uC = (-2x, 1, 4, 2)$. But $(-2x, 1, 4, 2)$ is not orthogonal to b, a contradiction.

Now suppose that $D = \mathrm{diag}(\alpha_1, \ldots, \alpha_4)$ is in $\mathrm{Aut}(\mathscr{K})$. Now $\langle b\rangle$ is the only 1-space of $\mathscr{K}$ with the first coordinate 0, so bD is a multiple of b and so $\alpha_2 = \alpha_3 = \alpha_4$. Similarly $\langle u - b\rangle$ is the only 1-space of $\mathscr{K}$ with the second coordinate 0, so $(u - b)D$ is a multiple of $u - b$ and so $\alpha_1 = \alpha_3 = \alpha_4$. Thus the only diagonal elements of $\mathrm{Aut}(\mathscr{K})$ are the scalars, so $\mathrm{Aut}(\mathscr{K}) \cong 3 \times 2A_4 \cong 3 \times SL(2, 3)$.

The stabilizer of $\langle u\rangle$ clearly contains A and the scalars, which together generate a group 6×3. Since the image of A in $\mathrm{Aut}(\mathscr{K})/Z(\mathrm{Aut}(\mathscr{K})) \cong A_4$ is maximal and since B does not stabilize $\langle u\rangle$, the group generated by A and the scalars is $\mathrm{stab}_{\mathrm{Aut}(\mathscr{K})}(\langle u\rangle)$. □

We remark that $\langle A\rangle$ is the set of permutation matrices in $\mathrm{Aut}(\mathscr{K})$, since each permutation matrix lies in the subgroup $A_0 \cong 2A_4$ consisting of the matrices with each entry equal to 0 or ± 1, $A_0 = O_2(A_0) : \langle A\rangle$, and no element of $O_2(A_0) = \langle B^A, B\rangle$ is a permutation. Also, $\langle b\rangle$ is a complement to $\langle u\rangle$ under the action of A.

The complex Leech lattice. Next we consider a lattice constructed from the ternary Golay code, the complex Leech lattice $\Lambda_{\mathbb{C}}$. This lattice is a special case of the lattices of Definition 5.1. The complex Leech lattice is a 12-dimensional lattice over $\mathbb{Z}[\omega]$ where ω is a primitive cube root of 1. Lindsey [16] shows that $\mathrm{Aut}_{\mathbb{Z}[\omega]}(\Lambda_{\mathbb{C}})$ is generated by a monomial group $3^6 : M_{11}$ along with another nonmonomial transformation and that $\mathrm{Aut}_{\mathbb{Z}[\omega]}(\Lambda_{\mathbb{C}})$ is isomorphic to the covering group $6Suz$ of the sporadic Suzuki group. The M_{11} factor of the monomial group acts as a 3-transitive group of permutations, while the factor 3^6 acts as the diagonal matrices $\mathrm{diag}(\omega^{c_i})$ where (c_i) is a Golay code word. Lindsey also shows that there is a $\mathbb{Z}$-valued quadratic form on $\Lambda_{\mathbb{C}}$ that makes

it into a 24-dimensional lattice over $\mathbb{Z}$. The form is preserved by $\mathrm{Aut}_{\mathbb{Z}[\omega]}(\Lambda_{\mathbb{C}})$ and makes $\Lambda_{\mathbb{C}}$ into the Leech lattice.

Let $(,)$ be the hermitian form on $\Lambda_{\mathbb{C}}$ given by $(\lambda, \mu) = \sum_{i=1}^{n} \lambda_i \bar{\mu}_i$. Let $\bar{\omega} = \omega^{-1}$, and let $\Theta = \omega - \bar{\omega}$. Now the image of $6Suz$ in the automorphism group of $\Lambda_{\mathbb{C}}/\Theta\Lambda_{\mathbb{C}}$ is isomorphic to the nonsplit extension $2Suz$. The form $(,)$ on $\Lambda_{\mathbb{C}}$ gives an inherited form $\langle , \rangle$ on $\Lambda_{\mathbb{C}}/\Theta\Lambda_{\mathbb{C}}$ defined by $\langle \bar{\lambda}, \bar{\mu} \rangle = (\lambda, \mu) \pmod{9\mathbb{Z}[\omega]}$, where $\bar{\lambda}$ and $\bar{\mu}$ are the images of λ and μ in $\Lambda_{\mathbb{C}}/\Theta\Lambda_{\mathbb{C}}$. It can be checked that $3\Theta\mathbb{Z}[\omega]$ is the image of $(,)$ (this follows from Lemma 5.4), so the image of $\langle , \rangle$ lies in $3\Theta\mathbb{Z}[\omega]/9\mathbb{Z}[\omega] \cong \mathbb{F}_3$. Now if $\langle \bar{\lambda}, \bar{\mu} \rangle \neq 0$, we have $(\lambda, \mu) \equiv \pm 3\Theta \pmod{9\mathbb{Z}[\omega]}$. Thus we have $(\mu, \lambda) = \overline{(\lambda, \mu)} \equiv -(\lambda, \mu)$, so $\langle , \rangle$ is alternating. We also observe that any nonzero $2Suz$-invariant bilinear form on $\Lambda_{\mathbb{C}}/\Theta\Lambda_{\mathbb{C}}$ is nonsingular, since each of the two orbits of nonzero vectors spans $\Lambda_{\mathbb{C}}/\Theta\Lambda_{\mathbb{C}}$. Thus there is an imbedding of $2Suz$ into the symplectic group $\mathrm{Sp}(12, 3)$.

Extraspecial groups and holomorphs.

Lemma 2.5. *Suppose that P is a group of order p^{2+n} and exponent p, and that $|Z(P)| = p^2$, that $|P'| = p$, and $P' < Z(P)$. Then P is the direct product of a cyclic group of order p and an extraspecial group p_+^{1+n}.*

Proof. Let $x \in Z(P) \setminus P'$, and let f be the natural map from P to P/P'. Since $P' < Z(P)$, the commutator gives a map $g : P/P' \times P/P' \to P'$, and this map is a bilinear form. Since $P' < Z(P)$ and $|Z(P)| = p^2$, the radical of g is spanned by $f(x)$. Thus if $A < f(P)$ is a complement of $f(x)$, the form $g|_A$ is nondegenerate, so $f^{-1}(A)$ is an extraspecial group p_+^{1+n}. Then $P = \langle x \rangle \times f^{-1}(Z) \cong Z_p \times p_+^{1+n}$. □

The following material is discussed in detail in [9, Appendix 1]. Let Q be an extraspecial p-group p_+^{1+2n} with p odd. There are $p-1$ faithful irreducibles for Q, each of degree p^n. The centralizer in $\mathrm{Aut}(Q)$ of $Z(Q)$ is a group $p^{2n} : \mathrm{Sp}(2n, p)$. A *holomorph* of Q is a group G with $Q \triangleleft G$ and $G/Q \cong \mathrm{Sp}(2n, p)$. A *partial holomorph* of Q is a group G_1 with $Q \leq G_1 \leq G$ where G is a holomorph. If G has a faithful representation of degree p^n we say that G is a *standard holomorph*. A partial holomorph is standard if it is contained in a standard holomorph. If not, we say it is *twisted*.

By [9, Proposition 1, §1, Appendix 1], standard holomorphs exist, and if G is a standard holomorph with $\mathrm{Hom}(G, \mathbb{Z}_p) = 0$ then G is unique. If ρ_s is a faithful representation of G of degree p^n we say that ρ_s is a *standard representation* of G. Now suppose that G is a twisted partial holomorph of Q. Then there exists a standard holomorph G_s with $G_s/Q \cong G/Q$. If G is perfect and $\hat{G}$ is a covering group of G, then both G and G_s are quotients of $\hat{G}$. Let A and A_s be the kernels of the maps onto G and G_s, respectively. If there exists $\hat{Q} < \hat{G}$ with $\hat{Q} \cong Q$ and $\hat{Q} \cap A = \hat{Q} \cap A_s = 1$, then every representation of G can be written as $\rho_s \otimes \sigma$ where ρ_s is a standard representation of G_s and σ is a representation of $\hat{G}/\hat{Q}$.

Now we want to study holomorphs G of shape $3_+^{1+12} \cdot 2Suz$, where $\overline{G} = G/Z(G)$ is the split extension $3^{12}{:}2Suz$ and $3^{12} \cong \Lambda_{\mathbb{C}}/\Theta\Lambda_{\mathbb{C}}$ as a $2Suz$ module. By the previous remarks, any such holomorph is a quotient of the covering group of $\overline{G}$, so we determine the Schur multiplier of $\overline{G}$. First we need a lemma.

Lemma 2.6. *Let E be an elementary abelian p-group, with p an odd prime, and let $Z = \mathbb{Z}/p\mathbb{Z}$. Then $H^2(E, Z) = H^2_{ab}(E, Z) \oplus H^2_{sk}(E, Z)$, where elements of $H^2_{ab}(E, Z)$ are represented by symmetric cocycles and elements of $H^2_{sk}(E, Z)$ are represented by cocycles which are bilinear and alternating.*

Proof. Let f be any 2-cocycle. Define the cocycles f' and f'' by $f'(x, y) = \frac{1}{2}f(x, y) + \frac{1}{2}f(y, x)$ and $f''(x, y) = \frac{1}{2}f(x, y) - \frac{1}{2}f(y, x)$. If we let $Z^2_{ab}(E, Z)$ denote the span of all the cocyles f' and let $Z^2_{sk}(E, Z)$ denote the span of all the f'', we have $Z^2(E, Z) = Z^2_{ab}(E, Z) \oplus Z^2_{sk}(E, Z)$. By definition, f is a coboundary if there is a function $g : E \to Z$ such that $f(x, y) = \delta g(x, y) = g(x) + g(y) - g(x + y)$ for all x, y, so every coboundary is symmetric. Thus any cocycle which is cohomologous to a symmetric cocycle is symmetric, so no cocycle in $Z^2_{ab}(E, Z)$ is cohomologous to a cocycle in $Z^2_{sk}(E, Z)$. Hence we see that $H^2(E, Z) = H^2_{ab}(E, Z) \oplus H^2_{sk}(E, Z)$.

All that remains to prove, then, is that elements of $Z^2_{sk}(E, Z)$ are bilinear and alternating. Let $f \in Z^2_{sk}(E, Z)$. We know that $f(x, y) = -f(y, x)$ by definition of Z^2_{sk}, so we only need to show $f(x, y + z) = f(x, y) + f(x, z)$. By definition, a 2-cocycle satisfies

$$f(x, y) + f(x + y, z) = f(y, z) + f(x, y + z)$$

for all x, y, z. Thus we have $f(x, y + z) = f(x, y) + f(x + y, z) - f(y, z)$, and by interchanging y and z we have $f(x, y + z) = f(x, z) + f(x + z, y) - f(z, y)$. Adding these two equations we have $2f(x, y + z) = f(x, y) + f(x, z) + f(x + y, z) + f(x + z, y)$. Now by the definition of 2-cocycle we have $f(y + x, z) - f(y, x + z) = f(x, z) - f(y, x)$, so we may replace $f(x + y, z) + f(x + z, y)$ with $f(x, y) + f(x, z)$ in the previous equation. Hence $2f(x, y + z) = 2f(x, y) + 2f(x, z)$, proving the linearity of f in the second variable. This also shows that f is linear in the first variable, since $f(x, y) = -f(y, x)$. □

Recall that $\overline{G}$ is the split extension $3^{12}:2Suz$, with $O_3(\overline{G})$ isomorphic to $\Lambda_{\mathbb{C}}/\Theta\Lambda_{\mathbb{C}}$ as a $2Suz$-module.

Lemma 2.7. *The Schur multiplier of $\overline{G}$ is an elementary abelian group of order 9.*

Proof. Write $\overline{\Lambda_{\mathbb{C}}}$ for $\Lambda_{\mathbb{C}}/\Theta\Lambda_{\mathbb{C}}$, and let $M(H)$ denote the Schur multiplier of a group H. By Theorem 2.2.5 of [14], $M(\overline{G}) \cong \tilde{M}(\overline{G}) \times M(2Suz)$ where $\tilde{M}(\overline{G})$ is the kernel of the restriction map $M(\overline{G}) \to M(2Suz)$, and there is an exact sequence

$$1 \to H^1(2Suz, \overline{\Lambda_{\mathbb{C}}}) \to \tilde{M}(\overline{G}) \to M(\overline{\Lambda_{\mathbb{C}}})^{2Suz} \to H^2(2Suz, \overline{\Lambda_{\mathbb{C}}}) \to 1.$$

We have $H^1(2Suz, \overline{\Lambda_{\mathbb{C}}}) = H^2(2Suz, \overline{\Lambda_{\mathbb{C}}}) = 1$, since from [16] $Z(2Suz)$ acts fixed point freely. Hence we have $\tilde{M}(\overline{\Lambda_{\mathbb{C}}}) = M(\overline{\Lambda_{\mathbb{C}}})^{2Suz}$. Now by [7] the multiplier of $2Suz$ has order 3, so all that remains is to show that $M(\overline{\Lambda_{\mathbb{C}}})^{2Suz}$ has order 3.

Let $\mathbb{Z}_3^* = \mathrm{Hom}(\mathbb{Z}_3, \mathbb{C}^\times)$. For $f \in Z^2(H, Z)$ or $Z^2(H, \mathbb{C}^\times)$, write $\bar{f}$ for the image of f in $f \in H^2(H, Z)$ or $H^2(H, \mathbb{C}^\times)$, respectively. Define the map $\psi : H^2(\overline{\Lambda_{\mathbb{C}}}, \mathbb{Z}_3) \to \mathrm{Hom}(\mathbb{Z}_3^*, M(\overline{\Lambda_{\mathbb{C}}}))$ by $\psi(\bar{f})(\alpha) = \overline{\alpha \circ f}$. The map ψ

is well defined since if $f = \delta g$, then $\alpha \circ f = \alpha \circ \delta g = \delta(\alpha \circ g) \in B^2(H, \mathbb{C}^\times)$. Theorem 2.1.19 of [14] implies that ψ is surjective, and the kernel of ψ is $H^2_{ab}(\overline{\Lambda_\mathbb{C}}, \mathbb{Z}_3)$. Since $M(\overline{\Lambda_\mathbb{C}})$ has exponent 3, $\mathrm{Hom}(\mathbb{Z}_3^*, M(\overline{\Lambda_\mathbb{C}}))$ is isomorphic to $M(\overline{\Lambda_\mathbb{C}})$. Thus we have

$$M(\overline{\Lambda_\mathbb{C}}) \cong H^2(\overline{\Lambda_\mathbb{C}}, \mathbb{Z}_3)/H^2_{ab}(\overline{\Lambda_\mathbb{C}}, \mathbb{Z}_3) \cong H^2_{sk}(\overline{\Lambda_\mathbb{C}}, \mathbb{Z}_3) \cong Z^2_{sk}(\overline{\Lambda_\mathbb{C}}, \mathbb{Z}_3).$$

Now fix a generator x of $\mathbb{Z}_3^*$. For $m \in M(\overline{\Lambda_\mathbb{C}})$, let $\tilde{m} \in \mathrm{Hom}(\mathbb{Z}_3^*, M(\overline{\Lambda_\mathbb{C}}))$ be defined by $\tilde{m}(x) = m$. Clearly $\tilde{m}$ is fixed by $2Suz$ if and only if m is fixed by $2Suz$. It follows from Lemma 2.6 that there is a unique element m_z in $Z^2_{sk}(\overline{\Lambda_\mathbb{C}}, \mathbb{Z}_3) \cap \psi^{-1}(\tilde{m})$. Since $2Suz$ stabilizes the set $Z^2_{sk}(\overline{\Lambda_\mathbb{C}}, \mathbb{Z}_3)$, the group $2Suz$ fixes $\tilde{m}$ if and only if it fixes m_z. Thus to show that $M(\overline{\Lambda_\mathbb{C}})^{2Suz} \cong \mathbb{Z}_3$, it suffices to show that there is, up to a scalar, a unique $2Suz$-invariant alternating form on $\overline{\Lambda_\mathbb{C}}$.

It will follow that there is, up to scalar, at most one such bilinear form if we can show that $\overline{\Lambda_\mathbb{C}}$ is an absolutely irreducible $2Suz$ module, for let f be a $2Suz$-invariant bilinear form on $\overline{\Lambda_\mathbb{C}}$. Then for $x \in \overline{\Lambda_\mathbb{C}}$, we define $f_x \in \mathrm{Hom}(\overline{\Lambda_\mathbb{C}}, \mathbb{F}_3) = \overline{\Lambda_\mathbb{C}}^*$ by $f_x(y) = f(x, y)$. Now the map defined by $x \mapsto f_x$ is an element of $\mathrm{Hom}_{\mathbb{F}_3 2Suz}(\overline{\Lambda_\mathbb{C}}, \overline{\Lambda_\mathbb{C}}^*)$, and if $\overline{\Lambda_\mathbb{C}}$ is absolutely irreducible, $\mathrm{Hom}_{\mathbb{F}_3 2Suz}(\overline{\Lambda_\mathbb{C}}, \overline{\Lambda_\mathbb{C}}^*)$ has dimension at most 1.

Next we show that $\overline{\Lambda_\mathbb{C}}$ is absolutely irreducible. The group $2Suz$ has a subgroup $Q \cong 2_-^{1+6}$, where x is the generator of $Z(Q)$ and $Q \setminus Q'$ contains an element y which is conjugate to x in $2Suz$. Let B_x^ϵ be the ϵ eigenspace of x on $\overline{\Lambda_\mathbb{C}}$ for $\epsilon = \pm 1$, and let B_y^ϵ be the ϵ eigenspace of y. Then B_x^{-1} and B_y^{-1} both have dimension 8, and B_x^{-1} is an absolutely irreducible Q module. Also, $B_x^{-1} \cap B_y^{-1}$ has dimension 4, and $B_x^1 \cap B_y^1 = \{0\}$.

Suppose that A is a $2Suz$ submodule of $\overline{\Lambda_\mathbb{C}}$. We show that $A = \overline{\Lambda_\mathbb{C}}$ or $A = \{0\}$. Since B^{-1} is an irreducible Q-module, $A \cap B_x^{-1}$ is either trivial or all of B_x^{-1}. If A contains B_x^{-1}, then it also contains B_y^{-1}, and these two subspaces span $\overline{\Lambda_\mathbb{C}}$. Thus A intersects both B_x^{-1} and B_y^{-1} trivially. Hence A has dimension at most 4, and since $|Suz| > |L_4(3)|$, $2Suz$ acts trivially on A. Thus $A < B_x^1 \cap B_y^1$. Since $B_x^1 \cap B_y^1 = \{0\}$, we have $A = \{0\}$.

This shows that if there exists a bilinear form on $\overline{\Lambda_\mathbb{C}}$, then it is unique up to a scalar. The existence follows by taking the alternating form $\langle , \rangle$ that $\overline{\Lambda_\mathbb{C}}$ inherits from $\Lambda_\mathbb{C}$. This shows that $\tilde{M}(\overline{G})$ has order 3, so $M(\overline{G}) \cong \tilde{M}(\overline{G}) \times M(2Suz) \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. □

Now every partial holomorph of shape $3_+^{1+12} \cdot 2Suz$ with quotient isomorphic to $\overline{G} \cong \overline{\Lambda_\mathbb{C}}{:}2Suz$ is a quotient of $\hat{G}$, the covering group of $\overline{G}$. Lemma 2.7 implies that $Z(\hat{G})$ has four subgroups of order 3. The quotients by these subgroups are: a group of shape $3^{12}{:}6Suz$; the standard holomorph G_s; and two twisted holomorphs. The above discussion on representations of holomorphs shows that we can distinguish the twisted holomorphs as follows. Let ρ_s be a standard representation of G_s, let σ be a faithful representation of $6Suz$, and let $\bar{\sigma}$ be the algebraic conjugate of σ. We may regard ρ_s, σ, and $\bar{\sigma}$ as rep-

resentations of $\hat{G}$. Then $\rho_s \otimes \sigma$ is a representation of one twisted holomorph and $\rho_s \otimes \bar{\sigma}$ is a representation of the other.

The following lemma is from [17].

Lemma 2.8. *Let* $\varepsilon = e^{2\pi i/p}$ *and* $n < p$. *The congruence* $\sum_{i=0}^{p-1} a_i \varepsilon^i \equiv 0 \pmod{(\varepsilon - 1)^n}$ *holds if and only if the congruences* $\sum_{i=0}^{p-1} a_i i^k \equiv 0 \pmod{p}$ *hold for* $0 \leq k < n$.

We apply this lemma to the situations that arise in §5. The function l is defined in Definition 3.6.

Lemma 2.9. *Let* p *be an odd prime, let* a *and* b *be elements of* $\mathbb{Z}$, *and let* ε *be a primitive* p*th root of* 1. *Then the following congruences hold in* $\mathbb{Z}[\varepsilon]$:

$$\varepsilon^a - \varepsilon^{-a} \equiv a(\varepsilon - \varepsilon^{-1}) \pmod{(\varepsilon - 1)^3}; \tag{2.1}$$

$$a\varepsilon^b - \varepsilon^{ab} + \varepsilon^{-ab} - a\varepsilon^{-b} \equiv \begin{cases} l(1/3)b^3(a - a^3)(\varepsilon - 1)^3 \pmod{(\varepsilon - 1)^4} & \text{if } p > 3, \\ 0 & \text{if } p = 3; \end{cases} \tag{2.2}$$

$$\varepsilon^a - 1 \equiv a(\varepsilon - 1) + l(1/2)(a^2 - a)(\varepsilon - 1)^2 \pmod{(\varepsilon - 1)^3}; \tag{2.3}$$

$$p \equiv 0 \pmod{(\varepsilon - 1)^{p-1}}. \tag{2.4}$$

Proof. Equation (2.1) is equivalent to showing that

$$\varepsilon^a - a\varepsilon + a\varepsilon^{-1} - \varepsilon^{-a} \equiv 0 \pmod{(\varepsilon - 1)^3}.$$

To apply Lemma 2.8 to this we need to show that

$$a^k - a + a(-1)^k - (-a)^k \equiv 0 \pmod{p}$$

for $k = 0$, 1, and 2. When $k = 0$ we check $1 - a + a - 1 = 0$, when $k = 1$ we check $1(a) - a(1) + a(-1) - 1(-a) = 0$, and when $k = 2$ we check $1(a^2) - a(1^2) + a((-1)^2) - 1(-a)^2 = a^2 - a + a - a^2 = 0$. The equation is now implied by Lemma 2.8.

For (2.2), we note first that to apply Lemma 2.8 in the case $p > 3$, we need to show that

$$\begin{aligned} &ab^k - (ab)^k + (-ab)^k - a(-b)^k \\ &\quad - l(1/3)ab^3(1 - a^2)(3^k - 3(2^k) + 3 - 0^k) \equiv 0 \pmod{p} \end{aligned}$$

for $k = 0$, 1, 2 and 3. Equation (2.1) implies that

$$a\varepsilon^b - \varepsilon^{ab} + \varepsilon^{-ab} - a\varepsilon^{-b} \in (\varepsilon - 1)^3,$$

so by Lemma 2.8 the congruence holds for $k \leq 2$. For $k = 3$ we check that $ab^3 - a^3b^3 - a^3b^3 + ab^3 - l(1/3)ab^3(1 - a^2)(27 - 3(8) + 3(1)) = 2ab^3 - 2(ab)^3 - 6l(1/3)(ab^3 - (ab)^3) \equiv 0 \pmod{p}$. If $p = 3$, then if $a = 0$ we have $a\varepsilon^b - \varepsilon^{ab} + \varepsilon^{-ab} - a\varepsilon^{-b} = -\varepsilon^0 + \varepsilon^0 = 0$, if $a = 1$ we have $a\varepsilon^b - \varepsilon^{ab} + \varepsilon^{-ab} - a\varepsilon^{-b} = \varepsilon^b - \varepsilon^b + \varepsilon^{-b} - \varepsilon^{-b} = 0$, and if $a = -1$ we have $a\varepsilon^b - \varepsilon^{ab} + \varepsilon^{-ab} - a\varepsilon^{-b} = -\varepsilon^b - \varepsilon^{-b} + \varepsilon^b + \varepsilon^{-b} = 0$. Thus in each case, (2.2) is true.

Equation (2.3) is equivalent to

$$2\varepsilon^a - 2 \equiv 2a(\varepsilon - 1) + (a^2 - a)(\varepsilon - 1)^2 \pmod{(\varepsilon - 1)^3}.$$

This equivalence is equivalent to

$$\begin{aligned} &2\varepsilon^a - 2 - 2a(\varepsilon - 1) - (a^2 - a)(\varepsilon - 1)^2 \\ &\quad = 2\varepsilon^a - 2 - 2a(\varepsilon - 1) - (a^2 - a)(\varepsilon^2 - 2\varepsilon + 1) \\ &\quad = 2\varepsilon^a - (a^2 - a)\varepsilon^2 + (2a^2 - 4a)\varepsilon - 2 + 3a - a^2 \\ &\quad \equiv 0 \pmod{(\varepsilon - 1)^3}. \end{aligned}$$

To apply Lemma 2.8, we check that $\sum_{i=0}^{p-1} a_i = 2 - (a^2 - a) + (2a^2 - 4a) - 2 + 3a - a^2 = 0$, that $\sum_{i=0}^{p-1} a_i i = 2a - 2(a^2 - a) + (2a^2 - 4a) = 0$, and that $\sum_{i=0}^{p-1} a_i i = 2a^2 - 4(a^2 - a) + (2a^2 - 4a) = 0$. Now Lemma 2.8 implies that (2.3) holds.

Equation (2.4) is obvious from Lemma 2.8. □

Lemma 2.10. *Let ω be a primitive cube root of 1, and let $\Theta = \omega - \bar{\omega}$. Then*

$$\omega^a - \omega^{-a} + \omega^b - \omega^{-b} - \omega^{a+b} + \omega^{-a-b} \equiv -ab(a+b)3\Theta \pmod{9\mathbb{Z}[\omega]}$$

for $a, b \in \{0, 1, -1\}$.

Proof. If a or b is 0, or $a + b = 0$, both sides of the equation are obviously 0. Thus we may assume $a = b$ and so $\omega^a - \omega^{-a} + \omega^b - \omega^{-b} - \omega^{a+b} + \omega^{-a-b} = 3(\omega^a - \omega^{-a}) = 3a\Theta$. Now $b(a + b) = 2$ and $3\Theta \equiv -6\Theta \pmod{9\mathbb{Z}[\omega]}$, so $a3\Theta \equiv -ab(a+b)\Theta \pmod{9\mathbb{Z}[\omega]}$. □

Blichfeldt showed in [1] that if there is a 4-dimensional representation of $2A_7$, then it is equivalent to a representation whose image is generated by the matrices in the next lemma. He also showed that the image of this group in $PSL(4, \mathbb{C})$ is a maximal finite subgroup of $PSL(4, \mathbb{C})$. Blichfeldt referred to [19] for a proof that these matrices actually generate a group isomorphic to $2A_7$.

Lemma 2.11. *Let $\varepsilon = e^{2\pi i/7}$, let $s = \varepsilon + \varepsilon^2 + \varepsilon^4$, let $n = \varepsilon^3 + \varepsilon^5 + \varepsilon^6$, and let $\Theta = s - n$. Then the matrices*

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \varepsilon & 0 & 0 \\ 0 & 0 & \varepsilon^2 & 0 \\ 0 & 0 & 0 & \varepsilon^4 \end{pmatrix} \quad \text{and} \quad \frac{1}{\Theta}\begin{pmatrix} -s^2 & 1 & 1 & 1 \\ 1 & n & s & s \\ 1 & s & n & s \\ 1 & s & s & n \end{pmatrix}$$

generate a group isomorphic to $2A_7$, the double cover of the alternating group on 7 letters. Also, the image of this group in $PSL(4, \mathbb{C})$ is a maximal finite subgroup of $PSL(4, \mathbb{C})$.

3. Code loops of odd order

In this chapter we define a class of loops whose multiplication operation is given by the structure of a code over $\mathbb{F}_p$, the field with p elements, for p an odd prime. In [11], Griess constructs a class of loops whose multiplication is based on codes over $\mathbb{F}_2$. The definition of our loops is quite simple, whereas

Griess has to do a fair amount of work to establish the existence of code loops over $\mathbb{F}_2$. On the other hand, a calculus developed by Ward in [23] can be used to show a similarity between the two constructions.

Definition 3.1. A *loop* is a set L and a binary operation $\cdot$ satisfying the following properties:

(1) There is an identity element $1_L \in L$ such that $x \cdot 1_L = 1_L \cdot x = x$ for all $x \in L$.
(2) Given $a, b \in L$, there exists a unique $x \in L$ such that $a \cdot x = b$.
(3) Given $a, b \in L$, there exists a unique $y \in L$ such that $y \cdot a = b$.

We occasionally omit the symbol $\cdot$ from our products and write xy for $x \cdot y$. We also use $xy \cdot z$ to mean $(x \cdot y) \cdot z$.

Definition 3.2. Let p be an odd prime, let C be a self-orthogonal code of length n over the field $\mathbb{F}_p$, let S be the set of permutation matrices in $\mathrm{Aut}(C)$, and suppose that $u \in C$ is a vector of weight n which is fixed by S. We define the function $\varphi : C \times C \to \mathbb{F}_p$ by $\varphi(x, y) = \sum_{i=1}^{n} u_i^{-1} x_i y_i^2$, and we define $L(C)$ to be the set $\mathbb{F}_p \times C$ with multiplication $(a, c) \cdot (b, d) = (a + b + \varphi(c, d), c + d)$.

Lemma 3.1. *$L(C)$ is a loop.*

Proof. We need to check that $L(C)$ satisfies conditions (1), (2), and (3) of Definition 3.1. It is clear from this definition that $(0, 0)$ is the identity of $L(C)$, since $\varphi(0, c) = \varphi(c, 0) = 0$ for all $c \in C$, so $L(C)$ satisfies (1). Given (a, c) and $(b, d) \in L(C)$, suppose that $(a, c) \cdot (x, y) = (b, d)$. Then clearly $y = d - c$, and so we must then have $x = b - a - \varphi(c, d - c)$. Hence $(b - a - \varphi(d - c, c), d - c)$ is the unique element $(x, y) \in L(C)$ with $(a, c) \cdot (x, y) = (b, d)$. Similarly, $(b - a - \varphi(d - c, c), d - c)$ is the unique element $(z, w) \in L(C)$ with $(z, w) \cdot (a, c) = (b, d)$, so $L(C)$ satisfies conditions (2) and (3). □

We let π denote the projection map $L(C) \to C$, and for $x \in L(C)$, we use x_i to denote the ith coordinate of $\pi(x)$. We will refer to the loops $L(C)$ as *code loops*, or as *odd code loops* when we wish to distinguish them from the loops defined in [11].

We remark that not every self-orthogonal code contains a vector of weight n fixed by S, the group of permutations in $\mathrm{Aut}(C)$. We can generalize Definition 3.2 by letting $\varphi(x, y) = \sum_{i \in \mathrm{supp}(u)} u_i^{-1} x_i y_i^2$ for some u fixed by S, not necessarily of weight n. Another generalization may be gotten as follows. Suppose $(\ ,\ ,\ )$ is a trilinear form on a vector space V over $\mathbb{F}_p$. Define $\varphi : V \times V \to \mathbb{F}_p$ by $\varphi(x, y) = (x, y, y)$. Now define $L(V)$ to be the set $\mathbb{F}_p \times V$ with multiplication $(a, c)(b, d) \mapsto (a + b + \varphi(c, d), c + d)$. All the loops that we investigate here, however, are given by Definition 3.2.

Now for $x, y \in L(C)$, we define $[x, y]$, the commutator of x and y, by $xy = [x, y](yx)$. Similarly, we define $[x, y, z]$, the associator of x, y, and z, by $xy \cdot z = [x, y, z](x \cdot yz)$. Using the definition of $L(C)$, it is easy to

compute that

$$[x, y] = \left(\sum_{i=1}^{n} u_i^{-1} x_i y_i (y_i - x_i), 0\right) \text{ and} \tag{3.1}$$

$$[x, y, z] = \left(-2\sum_{i=1}^{n} u_i^{-1} x_i y_i z_i, 0\right). \tag{3.2}$$

It is clear from this that commutators are products of associators, and satisfy

$$[x, y]^2 = [x, x, y][x, y, y]^{-1}. \tag{3.3}$$

This motivates the definition of a symmetric trilinear form on C which describes φ, the commutators, and the associators.

Definition 3.3. The symmetric trilinear form $(\ ,\ ,\ )$ on C is given by

$$(a, b, c) = -2\sum_{i=1}^{n} u_i^{-1} a_i b_i c_i. \tag{3.4}$$

It follows from the definitions that $-2\varphi(c, d) = (c, d, d)$. The definitions also show that $[x, y, z] = ((\pi(x), \pi(y), \pi(z)), 0)$.

Definition 3.4. The *center* of a loop L, $Z(L)$, is the set of all elements $z \in L$ such that $[z, x] = 1_L$ and $[z, x, y] = [x, z, y] = [x, y, z] = 1_L$ for all $x, y \in L$.

Define elements $\not{c}$ and $\$ \in L(C)$ by

$$\not{c} = (1, 0) \quad \text{and} \quad \$ = (0, u). \tag{3.5}$$

From (3.1) and (3.2) we see that f is in the center of $L(C)$ if and only if $\pi(f)$ is in the radical of $(\ ,\ ,\ )$. Since C is a self-orthogonal code, we see that u is in the radical of $(\ ,\ ,\ )$, so $\$$ is in the center of $L(C)$. Obviously $\not{c}$ is also in the center of $L(C)$. It is clear that $L(C)'$, the subloop of $L(C)$ generated by all commutators and associators, is contained in $\langle \not{c} \rangle \leq Z(L(C))$.

Automorphisms of $L(C)$.

Lemma 3.2. (i) *For $k \in \mathbb{F}_p^\times$, the map μ_k defined by $(a, c)^{\mu_k} = (ak^3, ck)$ is an automorphism of $L(C)$.* (ii) *For $\delta \in \mathrm{Hom}(C, \mathbb{F}_p)$, the map defined by $(a, c)^\delta = (a + \delta(c), c)$ is an automorphism of $L(C)$.* (iii) *For $\alpha \in S$, the map defined by $(a, c)^\alpha = (a, c^\alpha)$ is an automorphism of $L(C)$.*

Proof. Applying the definition of μ_k we have

$$\begin{aligned}(a, c)^{\mu_k}(b, d)^{\mu_k} &= (ak^3, ck)(bk^3, dk) \\ &= (ak^3 + bk^3 + \varphi(ck, dk), ck + dk),\end{aligned}$$

and since $\varphi(ck, dk) = \varphi(c, d)k^3$, this is equal to

$$((a + b + \varphi(c, d))k^3, (c + d)k) = (a + b + \varphi(c, d), c + d)^{\mu_k} = ((a, c)(b, d))^{\mu_k}.$$

Thus μ_k is an endomorphism. Since $\mu_{k^{-1}}\mu_k$ is the identity map, μ_k is an automorphism. We have $(a, c)^\delta(b, d)^\delta = (a + \delta(c), c)(b + \delta(d), d) = (a +$

$\delta(c) + b + \delta(d) + \varphi(c, d), c + d) = (a + b + \varphi(c, d) + \delta(c + d), c + d) = (a + b + \varphi(c, d), c + d)^{\delta}$. Thus δ gives rise to an automorphism of $L(C)$. Since $\alpha \in S$ means that α acts as a permutation matrix which fixes u, it is easy to see that $\varphi(c^{\alpha}, d^{\alpha}) = \varphi(c, d)$, and this shows that α gives rise to an automorphism of $L(C)$. □

In the future, we shall use δ and α to refer to an element of $\mathrm{Hom}(C, \mathbb{F}_p)$ and $\mathrm{Aut}(C)$, respectively, and the associated loop automorphism. The context will make it clear which we mean.

Definition 3.5. Let R be the subgroup of $\mathrm{Aut}(L(C))$ generated by all $\delta \in \mathrm{Hom}(C, \mathbb{F}_p)$; $R_0 < R$, the subgroup generated by all δ such that $\delta(u) = 0$, $A = \langle R, S \rangle$; and $A_0 = \langle R_0, S \rangle$.

The following functions can be used to exhibit an analogy between code loops over $\mathbb{F}_2$ and code loops over fields of odd prime order.

Definition 3.6. For $k \in \mathbb{F}_p$, let $l(k)$ be the element of $\mathbb{Z}$ satisfying $l(k) \equiv k \pmod{p\mathbb{Z}}$ and $|l(k)| < p/2$.

Lemma 3.3. *If C is a self-orthogonal code over $\mathbb{F}_3$, then $\sum_{i \in \mathrm{supp}(d)}^{n} d_i^{-1} c_i^3 = 0$ for all $d, c \in C$. Thus $\varphi(c, c) = 0$ for all $c \in C$.*

Proof. We have $d_i^{-1} = d_i$ for $d_i \neq 0$ and $c_i^3 = c_i$, so $\sum_{i \in \mathrm{supp}(d)}^{n} d_i^{-1} c_i^3 = \sum_{i=1}^{n} d_i c_i = 0$ since C is self-orthogonal. Also, $\varphi(c, c) = \sum_{i=1}^{n} u_i^{-1} c_i^3$, proving the second statement. □

Definition 3.7. Let C, u be as in Definition 3.2. We define $\Psi : C \to \mathbb{F}_p$ by

$$\Psi(c) = \begin{cases} l(-2/3) \sum_{i=1}^{n} l(u_i^{-1} c_i^3) \pmod{p\mathbb{Z}} & \text{if } p > 3, \\ 1/3 \sum_{i=1}^{n} l(u_i^{-1} c_i^3) \pmod{3\mathbb{Z}} & \text{if } p = 3. \end{cases}$$

Lemma 3.3 shows that when $p = 3$, $\Psi(c)$ lies in $\mathbb{Z}/3\mathbb{Z}$ and not just in $\frac{1}{3}\mathbb{Z}/3\mathbb{Z}$.

Definition 3.8. Let C, u be as in Definition 3.2. The function $\mathscr{Y} : L(C) \to L(C)$ is defined by $(a, c)^{\mathscr{Y}} = (a + \Psi(c), c)$. Also, for $(a, c) = d \in L(C)$, we let $\psi_d = (\Psi(c), 0)$.

We remark that if $p > 3$, then $\psi_d^3 = [d, d, d]$. The binomial theorem implies that

$$\psi_{fg} = \psi_f \psi_g [f, f, g][f, g, g], \tag{3.6}$$

and this equation is used often in what follows. The linearity of $(\ ,\ ,\ )$ implies that for all $x, y, z, w \in L(C)$,

$$\begin{aligned} [xy, z, w] &= [x, z, w][y, z, w], \\ [x, yz, w] &= [x, y, w][x, z, w], \text{ and} \\ [x, y, zw] &= [x, y, z][x, y, w]. \end{aligned} \tag{3.7}$$

The following definition is from [23].

Definition 3.9. Let A and B be abelian groups, and let f be a function from A to B. The *combinatorial polarization* of f, df, is the function from subsets of A to B defined by

$$df(s) = \sum_{t \subset s} (-1)^{|s|-|t|} f(\sum t),$$

where $\sum t = \sum_{a \in t} a$ and $\sum \emptyset = 0$.

For a doubly even binary code C, the codes for which code loops are constructed in [11], define $q : C \to \mathbb{F}_2$ by $q(x) = \frac{1}{4} wt(x)$. In [11], Griess describes commutators and associators in code loops based on C in terms of $dq(x, y)$ and $dq(x, y, z)$. If L is an odd code loop, the function Ψ is an analog of q in that $d\Psi(x, y) = \sum_{i=1}^{n} u_i^{-1} x_i y_i (x_i + y_i)$ and $d\Psi(x, y, z) = -2 \sum_{i=1}^{n} u_i^{-1} x_i y_i z_i$ describe a commutator and an associator in $L(C)$.

Definition 3.10. For $k \in \mathbb{F}_p$, we define a function $e_k : L(C) \to L(C)$ by $(a, c)^{e_k} = (ka, kc)$. For $d \in L(C)$, we denote d^{e_k} by d^k.

Definition 3.11. An element $f \in L$, where L is any loop, is *power associative* if the subloop generated by f is associative. The loop L is power associative if every element of L is power associative.

Lemma 3.4. *An element $f \in L(C)$ is power associative if and only if the associator $[f, f, f] = 1_L$.*

Proof. Obviously $[f, f, f] = 1_L$ if f is power associative. Now if x, y, z are in the subloop generated by f and $f = (a, c)$, we have $x = (x_1, x_2 c)$, $y = (y_1, y_2 c)$, and $z = (z_1, z_2 c)$ for some $x_i, y_i, z_i \in \mathbb{F}_p$. Thus $[x, y, z] = (x_2 y_2 z_2 (c, c, c), 0)$, and if $[f, f, f] = 1_L$, then $(c, c, c) = 0$, so $[x, y, z] = 1_L$. □

Corollary 3.5. *If C and u are as in Definition* 3.2, *and $p = 3$, then $L(C)$ is power associative.*

Proof. Combine Lemmas 3.3 and 3.4. □

The corollary implies that when C is a self-orthogonal code over $\mathbb{F}_3$, each element of $L(C)$ has a well-defined inverse. In fact, it is a simple matter to check that $(a, c)^{-1} = (-a, -c) = (a, c)^{\mu_{-1}}$, so when $p = 3$, L has an automorphism which maps each $x \in L$ to its inverse. We note also that it is true in general that $\mu_{-1} = e_{-1}$.

Lemma 3.6. *An odd code loop L is commutative if and only if it is associative.*

Proof. For any $x, y \in L$, we have $[x, y]^2 = [x, x, y][x, y, y]^{-1}$; so clearly if L is associative, then it is commutative. Now suppose that L is commutative. If there exists a nontrivial associator of the form $[x, y, y]$, then we must have $[x, x, y] = [x, y, y]$. But then $[x, y^{-1}, y^{-1}] = [x, y, y] = [x, x, y^{-1}]^{-1}$, so $[x, y^{-1}]^2 = [x, y, y]^{-2} \neq 1_L$, contradicting the commutativity of L. Thus there does not exist a nontrivial associator $[x, y, y]$. Then by the discussion following Definition 3.3, we find φ is identically 0, in which case L is an elementary abelian group and is associative. □

Corollary 3.7. *If C and u are as in Definition* 3.1, *and $p > 3$, then $L(C)$ is power associative if and only if it is associative.*

Proof. Clearly, if $L(C)$ is associative, then it is power associative. Now if $L(C)$ is power associative and $f, g \in L(C)$, we have

$$\begin{aligned} 1_{L(C)} &= [fg^{-1}, fg^{-1}, fg^{-1}] \\ &= [f, f, f][f, f, g^{-1}]^3[f, g^{-1}, g^{-1}]^3[g^{-1}, g^{-1}, g^{-1}] \\ &= [f, f, g]^{-3}[f, g, g]^3 \\ &= [g, f]^6. \end{aligned}$$

Thus $L(C)$ is commutative, hence associative. □

In general, the product of an element $f \in L(C)$ with itself k times depends on the association. If f is a power associative element of $L(C)$, then the product of f with itself k times does not depend on the association and is equal to f^{e_k}. This fact is our rationale for the abuse of notation $f^k = f^{e_k}$ introduced in Definition 3.10.

Lemma 3.8. *The map e_k commutes with A as a permutation of $L(C)$.*

Proof. Let $f = (a, c) \in L(C)$. For $\delta \in R$, we have $f^{\delta k} = (a + \delta(c), c)^k = (ka + k\delta(c), kc) = (ka + \delta(kc), kc) = (ka, kc)^\delta = f^{k\delta}$. For $\alpha \in S$, we have $f^{\alpha k} = (a, c^\alpha)^k = (ka, kc^\alpha) = (ka, kc)^\alpha = f^{k\alpha}$. Since A is generated by R and S, this shows that A commutes with e_k. □

The Group Generated by Translations. We investigate the group of maps from $L(C) \to L(C)$ generated by the left and right translation maps. From here on, we use L to refer to $L(C)$.

Definition 3.12. We define the following maps from $L \to L$ where L is a odd code loop and $a, b, x \in L$:

$$\rho_a : x \mapsto xa, \qquad \lambda_a : x \mapsto ax,$$
$$\zeta_{a,b} : x \mapsto x[a, b], \qquad \zeta_a : x \mapsto x\psi_a,$$
$$\eta_{a,b} : x \mapsto x[x, a, b]\, \tau_a : x \mapsto x[a, x, x]\, \zeta_{a,b,c} : x \mapsto x[a, b, c].$$

Definition 3.13. We define the following groups:

$$U = \langle \lambda_f, \rho_f \mid f \in L \rangle, \quad X(f) = \langle \lambda_f, \rho_f, \zeta_f \rangle,$$
$$K = \langle \lambda_f \mid f \in L \rangle, \qquad D = \langle \rho_f \mid f \in L \rangle,$$
$$E = \langle \eta_{f,g} \mid f, g \in L \rangle, \qquad F = \langle \tau_f \mid f \in L \rangle.$$

For any $f \in L$, the map $\zeta_{f,f,f}$ is the identity if $p = 3$ and $\zeta_{f,f,f} = \zeta_f^3$ if $p > 3$. Some equations that hold among these maps regardless of p are $\lambda_f = \tau_f^{-1/2}\eta_{f,f}^{1/2}\rho_f$, $[\rho_f, \eta_{f,f}] = \zeta_{f,f,f}$ and $[\rho_f, \tau_f] = \zeta_{f,f,f}\eta_{f,f}^2$. Thus we can express every element of $X(f)$ in terms of τ_f, $\eta_{f,f}$, ζ_f, and ρ_f. It will be convenient to have a standard way to refer to an element of $X(f)$ in terms of these maps.

Definition 3.14. Let $f \in L(C)$ and $\alpha, \beta, \gamma \in \mathbb{F}_p$. The map $R(f; \alpha, \beta, \gamma) \in X(f)$ is defined by

$$x \mapsto xf[f, f, x]^\alpha[f, x, x]^\beta \zeta_f^\gamma.$$

The map $r(f;\alpha,\beta,\gamma)$ is defined by

$$x \mapsto x[f,f,x]^{\alpha}[f,x,x]^{\beta}\zeta_f^{\gamma}.$$

We may also write these maps as $R(f;\alpha,\beta,\gamma) = \eta_{f,f}^{\alpha}\tau_f^{\beta}\zeta_f^{\gamma}\rho_f$ and $r(f;\alpha,\beta,\gamma) = \eta_{f,f}^{\alpha}\tau_f^{\beta}\zeta_f^{\gamma}$.

Lemma 3.9. *For $k \in \mathbb{F}_p$, $k \neq 0$, we have*

$$e_k^{-1}R(f;\alpha,\beta,\gamma)e_k = R(f^k;k^{-2}\alpha + 2^{-1}(1-k^{-2}),k^{-2}\beta,k^{-2}\gamma).$$

Proof. We assume that $f = (b,d)$. We compute that e_k^{-1} sends $x = (a,c) \in L$ to $(k^{-1}a,k^{-1}c)$ and that $R(f;\alpha,\beta,\gamma)$ sends this to

$$\left(\frac{1}{k}a + b + \frac{1}{k}\varphi(c,d) + \frac{1}{k}\alpha(c,d,d) + \frac{1}{k^2}\beta(c,c,d) + \gamma\psi_d, \frac{1}{k}c + d\right).$$

Then we check that e_k sends this to

$$\left(a + kb + \varphi(c,d) + \alpha(c,d,d) + \frac{1}{k}\beta(c,c,d) + k\gamma\psi_d\ ,\ c + kd\right).$$

Since $\varphi(c,d) = -2^{-1}(c,d,d)$, we see that this is equal to

$$\left(a + kb + \varphi(c,kd) + \left(\left(\frac{1}{2} - \frac{1}{2k^2}\right) + \frac{1}{k^2}\alpha\right)(c,kd,kd) + \frac{1}{k^2}\beta(c,c,kd) + \frac{1}{k^2}\gamma\psi_{kd}, c + kd\right).$$

The last expression is the image of the loop element (a,c) under the map $R(f^k;k^{-2}\alpha + 2^{-1}(1-k^{-2}),k^{-2}\beta,k^{-2}\gamma)$. □

Lemma 3.10. *For $k \in \mathbb{F}_p$, $k \neq 0$, we have*

$$e_k^{-1}r(f;\alpha,\beta,\gamma)e_k = r(f;\alpha,k^{-1}\beta,k\gamma).$$

We also have $r(f;\alpha,k^{-1}\beta,k\gamma) = r(f^k;k^{-2}\alpha,k^{-2}\beta,k^{-2}\gamma)$.

Proof. We assume that $f = (b,d)$. We compute that e_k^{-1} sends $x = (a,c) \in L$ to $(k^{-1}a,k^{-1}c)$ and that $r(f;\alpha,\beta,\gamma)$ sends this to

$$\left(\frac{1}{k}a + \frac{1}{k}\alpha(c,d,d) + \frac{1}{k^2}\beta(c,c,d) + \gamma\zeta_d, \frac{1}{k}c\right).$$

Then we check that e_k sends this to

$$\left(a + \alpha(c,d,d) + \frac{1}{k}\beta(c,c,d) + k\gamma\zeta_d, c\right).$$

This is the image of (a,c) under the map $r(f;\alpha,k^{-1}\beta,k\gamma)$. The second statement follows by noticing that $r(f^k;\alpha,\beta,\gamma)$ sends $x \in L$ to

$$x[f^k,f^k,x]^{\alpha}[f^k,x,x]^{\beta}\psi_{f^k}^{\gamma} = x[f,f,x]^{k^2\alpha}[f,x,x]^{k\beta}\psi_f^{k^3\gamma}$$

and this is the action of $r(f; k^2\alpha, k\beta, k^3\gamma)$. Replacing α, β, and γ with $k^{-2}\alpha$, $k^{-2}\beta$, and $k^{-2}\gamma$, this proves the second statement. □

Lemma 3.11. *For $f, g \in L$, we have $f^k g^k = (fg)^k [f, g, g]^{(k-k^3)/2}$.*

Proof. Suppose that $f = (a, c)$ and $g = (b, d)$. We have

$$\begin{aligned}(fg)^k [f, g, g]^{(k-k^3)/2} &= (k(a + b + \varphi(c, d)), k(c + d))[f, g, g]^{(k-k^3)/2} \\ &= (k(a + b + \varphi(c, d)) + 2^{-1}(k - k^3)(c, d, d), k(c + d)).\end{aligned}$$

Since $\varphi(c, d) = -2^{-1}(c, d, d)$, this is equal to

$$\begin{aligned}&(k(a + b + \varphi(c, d)) + (k^3 - k)\varphi(c, d), k(c + d)) \\ &\quad = (k(a + b) + k^3\varphi(c, d), k(c + d)) \\ &\quad = (ka + kb + \varphi(kc, kd), kc + kd) \\ &\quad = (ka, kc)(kb, kd) \\ &\quad = f^k g^k.\end{aligned}$$

Thus $f^k g^k = (fg)^k [f, g, g]^{(k-k^3)/2}$. □

Lemma 3.12. *The following relations hold:*

(i) $R(d; \alpha, \beta, \gamma)R(e; \alpha, \beta, \gamma) = \eta_{d,e}^{-2\alpha+2\beta+1} R(de; \alpha, \beta, \gamma)\zeta_{d,e,e}^{\alpha-\gamma}\zeta_{d,d,e}^{\beta-\gamma}$.

(ii) $[R(d; \alpha, \beta, \gamma), R(e; \sigma, \delta, \tau)] = \eta_{d,e}^{2\delta-2\beta}\zeta_{d,e,e}^{\sigma-\beta}\zeta_{d,d,e}^{\delta-\alpha}\zeta_{d,e}$.

(iii) $[R(d; \alpha, \beta, \gamma), r(e; \sigma, \delta, \tau)] = \eta_{d,e}^{2\delta}\zeta_{d,e,e}^{\sigma}\zeta_{d,d,e}^{\delta}$.

(iv) $r(d; \alpha, \beta, \gamma)R(d; \sigma, \delta, \tau) = R(d; \alpha + \sigma, \beta + \delta, \gamma + \tau)$.

(v) $r(d; \alpha, \beta, \gamma)r(e; \alpha, \beta, \gamma) = r(de; \alpha, \beta, \gamma)\eta_{d,e}^{-2\alpha}\zeta_{d,d,e}^{-\gamma}\zeta_{d,e,e}^{-\gamma}$.

(vi) $R(d; \alpha, \beta, \gamma)^p = 1$.

(vii)

$$\begin{aligned}&R(d^k; \alpha, \beta, \gamma)R(d^l; \sigma, \delta, \tau). \\ &\quad = R(d^{k+l}; (k + l)^{-2}(k^2\alpha + l^2\sigma + 2kl\delta + kl), (k + l)^{-1}(k\beta + l\delta), \\ &\qquad (k + l)^{-3}(k^3\gamma + l^3\tau + 3kl^2(\sigma - 1/2) + 3k^2 l\delta))\end{aligned}$$

(viii)

$$\begin{aligned}&R(d^k; \alpha, \beta, \gamma)R(d^{-k}; \sigma, \delta, \tau) \\ &\quad = r(d; k^2(\alpha + \sigma - 2\delta - 1), k(\beta - \delta), k^3(\gamma - \tau + 3\sigma - 3(\delta + 1/2)))\end{aligned}$$

Proof. (i) The left-hand side $R(d; \alpha, \beta, \gamma)R(e; \alpha, \beta, \gamma)$ maps $x \in L$ to

$$xd \cdot e[d, d, x]^\alpha [d, x, x]^\beta \psi_d^\gamma [e, e, dx]^\alpha [e, dx, dx]^\beta \psi_e^\gamma.$$

This is equal to

$$\begin{aligned}&xd \cdot e[d, d, x]^\alpha [d, x, x]^\beta \psi_d^\gamma [e, e, x]^\alpha [e, e, d]^\alpha \\ &\quad \cdot [e, x, x]^\beta [e, d, d]^\beta [d, e, x]^{2\beta} \psi_e^\gamma.\end{aligned}$$

By definition, $R(de;\alpha,\beta,\gamma)$ maps x to

$$\begin{aligned} &x\cdot de[de,de,x]^{\alpha}[de,x,x]^{\beta}\psi_{de}^{\gamma}\\ &\quad = xd\cdot e[d,d,x]^{\alpha}[e,e,x]^{\alpha}[d,e,x]^{2\alpha-1}[d,x,x]^{\beta}\\ &\qquad\cdot[e,x,x]^{\beta}\psi_d^{\gamma}\psi_e^{\gamma}[d,d,e]^{\gamma}[d,e,e]^{\gamma}. \end{aligned}$$

Thus after rearranging terms, we see that $\eta_{d,e}^{-2\alpha+2\beta+1}R(de;\alpha,\beta,\gamma)\zeta_{d,e,e}^{\alpha-\gamma}\zeta_{d,d,e}^{\beta-\gamma}$, which is the right-hand side of relation (ii), maps x to

$$\begin{aligned} &xd\cdot e[d,d,x]^{\alpha}[d,x,x]^{\beta}\psi_d^{\gamma}[e,e,x]^{\alpha}[e,e,d]^{\gamma+\alpha-\gamma}\\ &\qquad\cdot[e,x,x]^{\beta}[e,d,d]^{\gamma+\beta-\gamma}[d,e,x]^{2\alpha-1-2\alpha+2\beta+1}\psi_e^{\gamma} \end{aligned}$$

and, comparing the exponent of each term, we see this is the same as the image of the left-hand side.

(ii) Similarly to (i), $R(d;\alpha,\beta,\gamma)R(e;\sigma,\delta,\tau)$ maps $x\in L$ to

$$\begin{aligned} &xd\cdot e[d,d,x]^{\alpha}[d,x,x]^{\beta}\psi_d^{\gamma}[e,e,dx]^{\sigma}[e,dx,dx]^{\delta}\psi_e^{\tau}\\ &\quad = xd\cdot e[d,d,x]^{\alpha}[d,x,x]^{\beta}\psi_d^{\gamma}[e,e,x]^{\sigma}[e,x,x]^{\delta}\\ &\qquad\cdot\psi_e^{\tau}[e,e,d]^{\sigma}[e,d,d]^{\delta}[e,d,x]^{2\delta}. \end{aligned}$$

Also, $R(e;\sigma,\delta,\tau)R(d;\alpha,\beta,\gamma)$ maps x to

$$\begin{aligned} &xe\cdot d[e,e,x]^{\sigma}[e,x,x]^{\delta}\psi_e^{\tau}[d,d,ex]^{\alpha}[d,ex,ex]^{\beta}\psi_d^{\gamma}\\ &\quad = xe\cdot d[e,e,x]^{\sigma}[e,x,x]^{\delta}\psi_e^{\tau}[d,d,x]^{\alpha}\\ &\qquad\cdot[d,x,x]^{\beta}\psi_d^{\gamma}[d,d,e]^{\alpha}[d,e,e]^{\beta}[d,e,x]^{2\beta}. \end{aligned}$$

Rearranging terms, this is

$$\begin{aligned} &xe\cdot d[d,d,x]^{\alpha}[d,x,x]^{\beta}\psi_d^{\gamma}[e,e,x]^{\sigma}[e,x,x]^{\delta}\\ &\qquad\cdot\psi_e^{\tau}[d,e,e]^{\beta}[d,d,e]^{\alpha}[d,e,x]^{2\beta}. \end{aligned}$$

If we compare this with the last expression for $R(d;\alpha,\beta,\gamma)R(e;\sigma,\delta,\tau)$, and also observe that $xd\cdot e=[d,e]xe\cdot d$, we see that

$$[R(d;\alpha,\beta,\gamma),R(e;\sigma,\delta,\tau)]=\eta_{d,e}^{2\delta-2\beta}\zeta_{e,e,d}^{\sigma-\beta}\zeta_{d,d,e}^{\delta-\alpha}\zeta_{d,e}.$$

(iii) The left-hand side $R(d;\alpha,\beta,\gamma)r(e;\sigma,\delta,\tau)$ maps $x\in L$ to

$$\begin{aligned} &xd[d,d,x]^{\alpha}[d,x,x]^{\beta}\psi_d^{\gamma}[e,e,dx]^{\sigma}[e,dx,dx]^{\delta}\psi_e^{\tau}\\ &\quad = xd[d,d,x]^{\alpha}[d,x,x]^{\beta}\psi_d^{\gamma}[e,e,x]^{\sigma}[e,x,x]^{\delta}\\ &\qquad\cdot\psi_e^{\tau}[e,e,d]^{\sigma}[e,d,d]^{\delta}[e,d,x]^{2\delta}, \end{aligned}$$

while $r(e;\sigma,\delta,\tau)R(d;\alpha,\beta,\gamma)$ maps $x\in L$ to

$$xd[e,e,x]^{\sigma}[e,x,x]^{\delta}\psi_e^{\tau}[d,d,x]^{\alpha}[d,x,x]^{\beta}\psi_d^{\gamma}.$$

Hence we see that $[R(d;\alpha,\beta,\gamma),r(d;\sigma,\delta,\tau)]=\eta_{d,e}^{2\delta}\zeta_{d,d,e}^{\delta}\zeta_{d,e,e}^{\sigma}$.

(iv) This is obvious.

(v) The map $r(de;\alpha,\beta,\gamma)$ sends $x \in L$ to

$$\begin{aligned} &x[de,de,x]^{\alpha}[de,x,x]^{\beta}\psi_{de}^{\gamma} \\ &\quad = x[d,d,x]^{\alpha}[e,e,x]^{\alpha}[d,e,x]^{2\alpha}[d,x,x]^{\beta} \\ &\qquad \cdot [e,x,x]^{\beta}\psi_d^{\gamma}\psi_e^{\gamma}[d,d,e]^{\gamma}[d,e,e]^{\gamma}, \end{aligned}$$

which follows from (3.6) and (3.7). Rearranging terms, this is

$$x[d,d,x]^{\alpha}[d,x,x]^{\beta}\psi_d^{\gamma}[e,e,x]^{\alpha}[e,x,x]^{\beta}\psi_e^{\gamma}[d,e,x]^{2\alpha}[d,d,e]^{\gamma}[d,e,e]^{\gamma}.$$

This is the same as the image of x under

$$r(d;\alpha,\beta,\gamma)r(e;\alpha,\beta,\gamma)\eta_{d,e}^{2\alpha}\zeta_{d,d,e}^{\gamma}\zeta_{d,e,e}^{\gamma},$$

so we have proven (v).

(vi) First, for $f \in L$ define $f^{[k]}$ by $f^{[1]} = 1$ and $f^{[k]} = f^{[k-1]}f$. Now if $f = (a, c)$, we claim that $f^{[k]} = (ka + ((k^2 - k)/2)\varphi(c, c), kc)$. This is obvious for $k = 1$, and for $k > 1$ we have

$$\begin{aligned} f^{[k]} &= f^{[k-1]}f \\ &= \left((k-1)a + \frac{(k-1)^2 - (k-1)}{2}\varphi(c,c), (k-1)c\right)(a,c) \\ &= \left((k-1)a + \frac{(k-1)^2 - (k-1)}{2}\varphi(c,c) + a + \varphi((k-1)c,c), (k-1)c + c\right) \\ &= \left(ka + \frac{(k-1)^2 - (k-1)}{2}\varphi(c,c) + (k-1)\varphi(c,c), kc\right) \\ &= \left(ka + \frac{k^2 - k}{2}\varphi(c,c), kc\right). \end{aligned}$$

Hence we see that $f^{[p]} = 1_L$. Now applying (i) to $R(d;\alpha,\beta,\gamma)^p$ we have

$$\begin{aligned} &R(d;\alpha,\beta,\gamma)^p \\ &\quad = \eta_{d,d}^{-2\alpha+2\beta+1}R(dd;\alpha,\beta,\gamma)\zeta_{d,d,d}^{\alpha-\gamma}\zeta_{d,d,d}^{\beta-\gamma}R(d;\alpha,\beta,\gamma)^{p-2} \\ &\quad = (\eta_{d,d}\eta_{d,d^2})^{-2\alpha+2\beta+1}R(dd\cdot d;\alpha,\beta,\gamma) \\ &\qquad \cdot (\zeta_{d,d,d}\zeta_{d^2,d,d})^{\alpha-\gamma}(\zeta_{d,d,d}\zeta_{d,d^2,d^2})^{\beta-\gamma}R(d;\alpha,\beta,\gamma)^{p-3} \\ &\quad = \quad \vdots \\ &\quad = \prod_{i=1}^{p-1}\eta_{d,d^i}^{-2\alpha+2\beta+1}R(d^{[p]};\alpha,\beta,\gamma)\prod_{i=1}^{p-1}\zeta_{d^i,d,d}^{\alpha-\gamma}\prod_{i=1}^{p-1}\zeta_{d,d^i,d^i}^{\beta-\gamma}. \end{aligned}$$

Now $d^{[p]} = 1_L$, so we may rewrite this as

$$\eta_{d,d}^{S_1(-2\alpha+2\beta+1)}\zeta_{d,d,d}^{S_1(\alpha-\gamma)}\zeta_{d,d,d}^{S_2(\beta-\gamma)}$$

where $S_1 = \sum_{i=1}^{p-1} i$ and $S_2 = \sum_{i=1}^{p-1} i^2$. Now $S_1 \equiv 0 \pmod p$ for $p \geq 3$, $S_2 \equiv 0 \pmod p$ for $p > 3$, and $\zeta_{d,d,d} = 1_L$ if $p = 3$, so this is 1_L in all cases.

(vii) $R(d^k;\alpha,\beta,\gamma)R(d^l;\sigma,\delta,\tau)$ maps $x \in L$ to

$$\begin{aligned}
&xd^k \cdot d^l[d^k, d^k, x]^\alpha[d^k, x, x]^\beta \psi_{d^k}^\gamma[d^l, d^l, d^k x]^\sigma[d^l, d^k x, d^k x]^\delta \psi_{d^l}^\tau \\
&\quad = x \cdot d^k d^l[d, d, x]^{kl+k^2\alpha}[d, x, x]^{k\beta} \psi_d^{k^3\gamma}[d, d, x]^{l^2\sigma+2kl\delta} \\
&\qquad \cdot [d, x, x]^{l\delta} \psi_d^{l^3\tau+3kl^2\sigma+3k^2l\delta} \\
&\quad = x \cdot d^{k+l}[d, d, x]^{kl+k^2\alpha+l^2\sigma+2kl\delta}[d, x, x]^{k\beta+l\delta} \psi_d^{k^3\gamma+l^3\tau+3kl^2(\sigma-1/2)+3k^2l\delta}
\end{aligned}$$

This last expression is the image of x under the map

$$R(d^{k+l}; (k+l)^{-2}(k^2\alpha + l^2\sigma + 2kl\delta + kl), (k+l)^{-1}(k\beta + l\delta), \\ (k+l)^{-3}(k^3\gamma + l^3\tau + 3kl^2(\sigma - 1/2) + 3k^2l\delta)).$$

(viii) $R(d^k;\alpha,\beta,\gamma)R(d^{-k};\sigma,\delta,\tau)$ maps $x \in L$ to

$$\begin{aligned}
&xd^k \cdot d^{-k}[d^k, d^k, x]^\alpha[d^k, x, x]^\beta \\
&\quad \cdot \psi_{d^k}^\gamma[d^{-k}, d^{-k}, d^k x]^\sigma[d^{-k}, d^k x, d^k x]^\delta \psi_{d^{-k}}^\tau \\
&\qquad = x \cdot d^k d^{-k}[d, d, x]^{k^2\alpha-k^2}[d, x, x]^{k\beta} \\
&\qquad\quad \cdot \psi_d^{k^3\gamma}[d, d, x]^{k^2\sigma-2k^2\delta}[d, x, x]^{-k\delta} \psi_d^{k^3(3\sigma-\tau-3\delta)} \\
&\qquad = x[d, d, x]^{k^2\alpha-k^2}[d, x, x]^{k\beta} \\
&\qquad\quad \cdot \psi_d^{k^3\gamma}[d, d, x]^{k^2\sigma-2k^2\delta}[d, x, x]^{-k\delta} \psi_d^{k^3(3\sigma-\tau-3\delta-3/2)}.
\end{aligned}$$

This last expression is the image of x under the map

$$r(d; k^2(\alpha + \sigma - 2\delta - 1), k(\beta - \delta), k^3(\gamma - \tau + 3\sigma - 3\delta - 3/2)). \quad \square$$

4. Permutations of luples

Given an odd code loop L, we define luples, which are functions from $\mathbb{F}_p^2$ to L. Then we construct a group of permutations of luples. We will call this group N. The construction proceeds in two steps. First, we construct a group N_0, whose members act on the range of a luple as either a translation or an automorphism. Second, we construct a group isomorphic to $GL(2, p)$, whose members act on both the domain and the range of a luple. These two subgroups generate N. Then we identify a normal subgroup K of N of order p^2. In the following sections, we show that for certain codes, the group $\overline{N} = N/K$ is a subgroup of the Monster.

The group N_0.

Definition 4.1. Let V be a 2-dimensional vector space over $\mathbb{F}_p$, let C be a self-orthogonal code over $\mathbb{F}_p$, and let $L(C)$ be the code loop based on C from Definition 3.2. A *luple* is a function from $V \to L(C)$. A *standard luple* is a

luple θ satisfying the properties

$$\pi \circ \theta \in \mathrm{Hom}_{\mathbb{F}_p}(V, C) \quad \text{and} \tag{4.1}$$

$$\theta(kv) = \theta(v)^k. \tag{4.2}$$

We use $\mathscr{L}$ to denote the set of all luples and $\mathscr{S}$ to denote the set of all standard luples.

All of the permutations of luples which we consider preserve the set of standard luples. The restrictions imposed by (4.1) and (4.2), then, will have a strong effect on the definitions of these permutations. The first observation we make is (4.2) implies that for a standard luple θ, we have $\theta(0) = 1_L$. Thus we ignore $\theta(0)$, and it should be assumed that every permutation of luples we consider acts trivially on $\theta(0)$.

Now let $f \in L$, and suppose that σ is a permutation of $\mathscr{L}$ which preserves $\mathscr{S}$. Also assume that for any luple θ, $\theta^\sigma(v) = \theta(v)^\rho$, where $\rho = \rho(v)$ is an element of $X(f)$ which depends on v. Now (4.2) implies that for $k \in \mathbb{F}_p$, $\theta^\sigma(kv) = \theta(kv)^{\rho(kv)} = \theta(v)^{k\rho(kv)}$, and also $\theta^\sigma(kv) = \theta^\sigma(v)^k = (\theta(v)^{\rho(v)})^k$. Thus we have $e_k\rho(kv) = \rho(v)e_k$ or $\rho(kv) = e_k^{-1}\rho(v)e_k$. Hence if we know $\rho(v)$, Lemma 3.9 tells us what $\rho(kv)$ must be in order for σ to preserve $\mathscr{S}$.

From the results of §3 we know that $\rho(v)$ can be written as $r(f; \alpha, \beta, \gamma)$ or as $R(f^k; \alpha, \beta, \gamma)$ with $k \neq 0$. If θ^σ is to satisfy (4.1), then it is the case that if $\rho(v) = R(f^k; \alpha, \beta, \gamma)$ and $\rho(w) = R(f^l; \sigma, \delta, \tau)$, then $\rho(v+w) = R(f^{k+l}; \upsilon, \nu, \omega)$ if $k + l \neq 0$ or $r(f; \upsilon, \nu, \omega)$ if $k + l = 0$, for some values of $\alpha, \beta, \ldots, \omega$.

The observations of the preceding paragraphs motivate our scheme for defining permutations which act like σ. Before giving the definition, we need some notation for the elements of V. Fix a basis $\{x, y\}$ of V, and let θ be a standard luple. For $j \in \mathbb{F}_p$, we use $\theta(\underline{j})$ as an abbreviation for $\theta(x + jy)$ and $\theta(\underline{\infty})$ for $\theta(y)$.

Definition 4.2. For $i, j \in \mathbb{F}_p \cup \{\infty\}$ we define i_f to be the permutation of $\mathscr{L}$ which preserves the set $\mathscr{S}$ and whose action is given by

$$\theta^{i_f}(\underline{j}) = \begin{cases} \theta(\underline{j})^{R(f^{k_{ij}}; \alpha_{ij}, \beta_{ij}, \gamma_{ij})} & \text{if } k_{ij} \neq 0, \\ \theta(\underline{j})^{r(f; \alpha_{ij}, \beta_{ij}, \gamma_{ij})} & \text{if } k_{ij} = 0. \end{cases}$$

The values k_{ij}, α_{ij}, β_{ij}, and γ_{ij} are as follows:

$$k_{ij} = \begin{cases} 0 & \text{if } i = j = \infty, \\ 1 & \text{if } j \neq \infty, \\ 1 & \text{if } i \neq \infty, \\ i + j & \text{otherwise;} \end{cases} \qquad \beta_{ij} = \begin{cases} -1 & \text{if } i = j = \infty, \\ j & \text{if } j \neq \infty, \\ -i & \text{if } i \neq \infty, \\ 1 & \text{if } i + j = 0, \\ (i+j)^{-1} + j & \text{otherwise;} \end{cases}$$

$$\alpha_{ij} = \begin{cases} \beta_{ij} + 1/2 & \text{if } k_{ij} \neq 0, \\ 0 & \text{if } k_{ij} = 0; \end{cases} \qquad \gamma_{ij} = \begin{cases} \beta_{ij} & \text{if } k_{ij} \neq 0, \\ 0 & \text{if } k_{ij} = 0. \end{cases}$$

Since we assert that θ^{i_f} is a standard luple, we check that it satisfies (4.1) and (4.2) if θ does. As described in the discussion which precedes the definition, the requirement that θ^{i_f} satisfy (4.2) if θ satisfies (4.2) implies that it suffices to give $\theta^{i_f}(v)$ for one representative v of each one-space of V, which is what we do in Definition 4.1. If we know $\theta^{i_f}(v)$, then $\theta^{i_f}(kv) = (\theta^{i_f}(v))^k$ by (4.2). The next lemma expresses this more explicitly, and shows that θ^{i_f} must then also satisfy (4.1).

Lemma 4.1. (1) *Suppose that $v \in V$ is one of the vectors denoted by $j \in \mathbb{F}_p \cup \{\infty\}$, so v is either y or $x + jy$. If i_f acts on $\theta(v)$ as $R(f^l; \beta + 1/2, \beta, \beta)$ with $l \neq 0$, then i_f acts on $\theta(kv)$ as $R(f^{kl}; k^{-2}\beta + 1/2, k^{-2}\beta, k^{-2}\beta)$. If i_f acts on $\theta(v)$ as $r(f; 0, \beta, 0)$, then i_f acts on $\theta(kv)$ as $r(f; 0, k^{-1}\beta, 0)$.*

(2) *If a luple θ satisfies* (4.1), *then θ^{i_f} also satisfies* (4.1).

Proof. The preceding discussion showed that the action of i_f on $\theta(kv)$ is $e_k^{-1}R(f^l; \beta + 1/2, \beta, \beta)e_k$. Now by Lemma 3.9, this is

$$R(f^{kl}; k^{-2}(\beta + 1/2) + 2^{-1}(1 - k^{-2}), k^{-2}\beta, k^{-2}\beta),$$

which simplifies to $R(f^{kl}; k^{-2}\beta + 1/2, k^{-2}\beta, k^{-2}\beta)$. In the case that i_f acts on $\theta(v)$ as $r(f; 0, \beta, 0)$, the result is obvious from Lemma 3.10. This proves (i).

To prove (ii), suppose first that $i \neq \infty$. Let $v = \alpha x + \sigma y$ and let $w = \gamma x + \delta y$. Then

$$\begin{aligned}\theta^{i_f}(v + w) &= \theta(v + w)^{R(f^{(\alpha i+\gamma i+\sigma+\delta)}; \beta_{v+w}+1/2, \beta_{v+w}, \beta_{v+w})} \\ &\equiv \theta(v)^{R(f^{(\alpha i+\sigma)}; \beta_v+1/2, \beta_v, \beta_v)}\theta(w)^{R(f^{(\gamma i+\delta)}; \beta_w+1/2, \beta_w, \beta_w)} \\ &\equiv \theta^{i_f}(v)\theta^{i_f}(w) \pmod{L'},\end{aligned}$$

where β_{v+w}, β_v, and β_v are as given in Definition 4.2 or part (i). This shows that (4.1) holds in the case $i \neq \infty$. We also have

$$\begin{aligned}\theta^{\infty_f}(v + w) &= \theta(v + w)^{R(f^{(\alpha+\gamma)}; \beta_{v+w}+1/2, \beta_{v+w}, \beta_{v+w})} \\ &\equiv \theta(v)^{R(f^{(\alpha)}; \beta_v+1/2, \beta_v, \beta_v)}\theta(w)^{R(f^{(\gamma)}; \beta_w+1/2, \beta_w, \beta_w)} \\ &\equiv \theta^{\infty_f}(v)\theta^{\infty_f}(w) \pmod{L'}.\end{aligned}$$

This completes the proof. □

In general, suppose that a group G has a left action on a set A and a group H has a right action on a set B. Let $\mathrm{Maps}(A, B)$ be the set of all functions from A to B. Then $G \times H$ has a right action on $\mathrm{Maps}(A, B)$ according to the rule $f^{(g,h)}(a) = f(ga)^h$. Since a luple is just an element of $\mathrm{Maps}(V, L)$, any permutation of V or L can be viewed to act on luples in this way, by identifying Σ_L with $\mathrm{id}_V \times \Sigma_L$ and Σ_V with $\Sigma_V \times \mathrm{id}_L$, where id_V and id_L are the identity maps on V and L, respectively.

Lemma 4.2. *The set of standard luples is preserved by $\alpha \in A_0$, where $A_0 = R_0{:}S$ is the group of Definition* 3.5.

Proof. Clearly α preserves (4.1), since any loop automorphism does. Now checking that α preserves (4.2) is equivalent to checking that α commutes with e_k, which we proved in Lemma 3.8. □

Lemma 4.3. *The maps i_f and $\delta \in A_0$ satisfy the following relations:*

$$i_f i_g = i_{fg} i_{[f,g,g]}^{1/2}, \tag{4.3}$$

$$[i_f, j_g] = \eta_{f,g}^{2i-2j} i_{[f,f,g]}^{i-j} j_{[f,g,g]}^{i-j} \qquad \text{for } i, j \neq \infty, \tag{4.4}$$

$$[\infty_f, j_g] = \eta_{f,g}^{2} \infty_{[f,f,g]} j_{[f,g,g]}, \tag{4.5}$$

$$i_f \delta = \delta i_{f\delta} \qquad \text{for } \delta \in A_0. \tag{4.6}$$

Remark. Since $[f, g, g] = (-2\varphi(\pi(f), \pi(g)), 0)$, (4.3) implies that if $f = (a, c)$, $g = (b, d)$, and $h = (a+b, c+d)$, then $i_f i_g = i_h$. In particular, for any $n \in \mathbb{N}$ we have $i_f^n = i_{f^n}$, providing further rationalization for the abuse of notation $f^n = f^{e_n}$.

Proof. To prove (4.3), we begin by noticing that i_f acts on $\theta(\underline{j})$ as one of the maps $R(f^{k_{ij}}; \beta_{ij} + 1/2, \beta_{ij}, \beta_{ij})$ or $r(f; 0, \pm 1, 0)$ for each j. Lemma 3.12(v) shows that

$$r(f; 0, \varepsilon, 0) r(g; 0, \varepsilon, 0) = r(fg; 0, \varepsilon, 0), \tag{4.7}$$

where $\varepsilon = \pm 1$. Now let $k = k_{ij}$ and let $\beta = \beta_{ij}$. By Lemma 3.12(i) we have that

$$\begin{aligned} R(f^k; \beta + \tfrac{1}{2}, \beta, \beta) R(g^k; \beta + \tfrac{1}{2}, \beta, \beta) &= R(f^k g^k; \beta + \tfrac{1}{2}, \beta, \beta) \zeta_{f^k, g^k, g^k}^{1/2} \\ &= R(f^k g^k; \beta + \tfrac{1}{2}, \beta, \beta) \zeta_{f,g,g}^{k^3/2}. \end{aligned}$$

By Lemma 4.3 we have $f^k g^k = (fg)^k [f, g, g]^{(k-k^3)/2}$, so the last expression is equal to

$$R((fg)^k; \beta + \tfrac{1}{2}, \beta, \beta) \zeta_{f,g,g}^{k/2}. \tag{4.8}$$

Equations (4.7) and (4.8) give the action of $i_f i_g$ on $\theta(\underline{-i})$ and $\theta(\underline{j})$ for $j \neq -i$, respectively. By comparing these with the definitions of i_{fg} and $i_{[f,g,g]}$ it is clear that $i_f i_g = i_{fg} i_{[f,g,g]}^{1/2}$, as required.

To prove (4.4) we suppose first that $k \neq \infty$, $k \neq -i$ and $k \neq -j$. Then i_f acts on $\theta(\underline{k})$ as

$$R(f^{i+k}; \tfrac{1}{i+k} + k + \tfrac{1}{2}, \tfrac{1}{i+k} + k, \tfrac{1}{i+k} + k),$$

and j_g acts on $\theta(\underline{k})$ as

$$R(g^{j+k}; \tfrac{1}{j+k} + k + \tfrac{1}{2}, \tfrac{1}{j+k} + k, \tfrac{1}{j+k} + k).$$

Thus by Lemma 3.12(ii) we have that $[i_f, j_g]$ acts on $\theta(\underline{k})$ as

$$\eta_{f^{i+k}, g^{j+k}}^{2((j+k)^{-1} - (i+k)^{-1})} \zeta_{f^{i+k}, g^{j+k}, g^{j+k}}^{(j+k)^{-1} - (i+k)^{-1} + 1/2} \zeta_{f^{i+k}, f^{i+k}, g^{j+k}}^{(j+k)^{-1} - (i+k)^{-1} - 1/2} \zeta_{f^{i+k}, g^{j+k}}.$$

Now by (3.3) we have $[a, b] = [a, b, b]^{-1/2}[a, a, b]^{1/2}$, so $\zeta_{f,g} = \zeta_{[f,f,g]}^{1/2} \cdot \zeta_{[f,g,g]}^{-1/2}$, and we may rewrite this expression as

$$\eta_{f^{i+k},g^{j+k}}^{2((j+k)^{-1}-(i+k)^{-1})}\zeta_{f^{i+k},g^{j+k},g^{j+k}}^{(j+k)^{-1}-(i+k)^{-1}}\zeta_{f^{i+k},f^{i+k},g^{j+k}}^{(j+k)^{-1}-(i+k)^{-1}} = \eta_{f,g}^{2(i-j)}\zeta_{f,g,g}^{(i-j)(j+k)}\zeta_{f,f,g}^{(i-j)(i+k)}. \tag{4.9}$$

The last equality follows since (3.7) implies that for any $f, g \in L$ and $a \in \mathbb{F}_p$ we have $\eta_{f^a,g} = \eta_{f,g}^a$. If $k = \infty$, then i_f acts on $\theta(\underline{\infty})$ as $R(f; -i + 1/2, -i, -i)$ and j_g acts on $\theta(\underline{\infty})$ as $R(g; -j + 1/2, -j, -j)$. Now Lemma 3.12(ii) shows that $[i_f, j_g]$ acts on $\theta(\underline{\infty})$ as

$$\eta_{f,g}^{2(-j+i)}\zeta_{f,g,g}^{-j+i+1/2}\zeta_{f,f,g}^{-j+i-1/2}\zeta_{f,g}.$$

Similarly to the previous case, this is equal to

$$\eta_{f,g}^{2(i-j)}\zeta_{f,g,g}^{i-j}\zeta_{f,f,g}^{i-j}. \tag{4.10}$$

If $k = -j$, we have that i_f acts on $\theta(\underline{-j})$ as

$$R(f^{i-j}; (i-j)^{-1} - j + 1/2, (i-j)^{-1} - j, (i-j)^{-1} - j)$$

and j_g acts on $\theta(\underline{-j})$ as $r(g; 0, 1, 0)$. Now by Lemma 3.12(iii) we have that $[i_f, j_g]$ acts on $\theta(\underline{-j})$ as

$$\eta_{f^{i-j},g}^2\zeta_{f^{i-j},f^{i-j},g} = \eta_{f,g}^{2(i-j)}\zeta_{f,f,g}^{(i-j)^2}. \tag{4.11}$$

A similar calculation shows that $[i_f, j_g]$ acts on $\theta(\underline{-i})$ as

$$\eta_{f,g}^{2(i-j)}\zeta_{f,g,g}^{-(i-j)^2}. \tag{4.12}$$

Comparison of (4.9)–(4.12) with the definitions of $i_{[f,f,g]}$ and $j_{[f,g,g]}$ now shows $[i_f, j_g] = \eta_{f,g}^{2(i-j)} i_{[f,f,g]}^{(i-j)} j_{[f,g,g]}^{(i-j)}$.

The proof of (4.5) is similar but easier than the proof of (4.4). Suppose first that $k \neq \infty$ and $k \neq -j$. Then ∞_f acts on $\theta(\underline{k})$ as $R(f; k + 1/2, k, k)$ and j_g acts on $\theta(\underline{k})$ as $R(g^{j+k}; (j+k)^{-1} + k + 1/2, (j+k)^{-1} + k, (j+k)^{-1} + k)$. Thus by Lemma 3.12(ii) we have that $[\infty_f, j_g]$ acts on $\theta(\underline{k})$ as

$$\eta_{f,g^{j+k}}^{2(j+k)^{-1}}\zeta_{f,g^{j+k},g^{j+k}}^{(j+k)^{-1}+1/2}\zeta_{f,f,g^{j+k}}^{(j+k)^{-1}-1/2}\zeta_{f,g^{j+k}}.$$

As before we may rewrite this expression as

$$\eta_{f,g^{j+k}}^{2(j+k)^{-1}}\zeta_{f,g^{j+k},g^{j+k}}^{(j+k)^{-1}}\zeta_{f,f,g^{j+k}}^{(j+k)^{-1}} = \eta_{f,g}^2\zeta_{f,g,g}^{j+k}\zeta_{f,f,g}. \tag{4.13}$$

If $k = -j$, we have that ∞_f acts on $\theta(\underline{k})$ as $R(f; -j + 1/2, -j, -j)$ and j_g acts on $\theta(\underline{\infty})$ as $r(g; 0, 1, 0)$. Now by Lemma 3.12(iii) we have that $[\infty_f, j_g]$ acts on $\theta(\underline{-j})$ as

$$\eta_{f,g}^2\zeta_{f,f,g}. \tag{4.14}$$

If $k = \infty$, we have that ∞_f acts on $\theta(\underline{\infty})$ as $r(f; 0, -1, 0)$ and j_g acts on $\theta(\underline{\infty})$ as $R(g; -j + 1/2, -j, -j)$. Again Lemma 3.12(iii) shows that $[\infty_f, j_g]$

acts on $\theta(\underline{\infty})$ as

$$\eta^2_{f,g}\zeta_{f,g,g}. \tag{4.15}$$

As with the proof of (4.4), comparison of (4.13)–(4.15) with the definitions of $\infty_{[f,f,g]}$ and $j_{[f,g,g]}$ now shows $[\infty_f, j_g] = \eta^2_{f,g}\infty_{[f,f,g]}j_{[f,g,g]}$.

The proof of (4.6) is easy. For $g \in L$ we have

$$g^{R(f^k;\alpha,\beta,\gamma)\delta} = g^{\delta R(f^{k\delta};\alpha,\beta,\gamma)},$$

and by Lemma 3.8 $f^{k\delta} = f^{\delta k}$, so we have $i_f\delta = \delta i_{f^\delta}$. □

Lemma 4.4. *For $f \in L$, we have*

$$\infty_f i_f = \eta_{f,f}(i+1)_f(i+2)_{\psi_f}. \tag{4.16}$$

Proof. For $k \neq -i-1$, $k \neq \infty$, and $k \neq -i$ we have that ∞_f acts on $\theta(\underline{k})$ as $R(f; k+1/2, k, k)$ and i_f acts on $\theta(\underline{k})$ as

$$R(f^{i+k}; (i+k)^{-1}+k+1/2, (i+k)^{-1}+k, (i+k)^{-1}+k).$$

Now using Lemma 3.12(vii) we see that $\infty_f i_f$ acts on $\theta(\underline{k})$ as $R(f^{i+k+1}; A, B, \Gamma)$ where

$$A = \frac{1}{(i+k+1)^2}\left(k+\frac{1}{2}+(i+k)^2\left(\frac{1}{i+k}+k+\frac{1}{2}\right)\right.$$
$$\left.+2(i+k)\left(\frac{1}{i+k}+k+\frac{1}{2}\right)\right),$$
$$B = \frac{1}{i+k+1}\left(k+(i+k)\left(\frac{1}{i+k}+k\right)\right),$$

and

$$\Gamma = \frac{1}{(i+k+1)^3}\left(k+(i+k)^3\left(\frac{1}{i+k}+k\right)\right.$$
$$\left.+3(i+k)^2\left(\frac{1}{i+k}+k\right)+3(i+k)\left(\frac{1}{i+k}+k\right)\right).$$

Simplifying, we get that

$$\begin{aligned}
A &= \frac{1}{(i+k+1)^2}\left(k+\frac{1}{2}+((i+k+1)^2-1)\left(k+\frac{1}{2}+\frac{1}{i+k}\right)\right)\\
&= k+\frac{1}{2}+\frac{1}{i+k}-\frac{1}{(i+k)(i+k+1)^2}\\
&= k+\frac{1}{2}+\frac{1}{i+k+1}+\frac{1}{(i+k)(i+k+1)}-\frac{1}{(i+k)(i+k+1)^2}\\
&= k+\frac{1}{2}+\frac{1}{i+k+1}+\frac{1}{(i+k)(i+k+1)}\left(1-\frac{1}{i+k+1}\right)\\
&= k+\frac{1}{2}+\frac{1}{i+k+1}+\frac{1}{(i+k)(i+k+1)}\left(\frac{i+k}{i+k+1}\right)\\
&= k+\frac{1}{2}+\frac{1}{i+k+1}+\frac{1}{(i+k+1)^2},\\
B &= \frac{1}{i+k+1}\left(k+1+(i+k)k\right)\\
&= \frac{1}{i+k+1}\left(1+(i+k+1)k\right)\\
&= \frac{1}{i+k+1}+k,
\end{aligned}$$

and

$$\begin{aligned}
\Gamma &= \frac{1}{(i+k+1)^3}\left(k+((i+k+1)^3-1)\left(k+\frac{1}{i+k}\right)\right)\\
&= k+\frac{1}{i+k}-\frac{1}{(i+k)(i+k+1)^3}\\
&= k+\frac{1}{i+k+1}+\frac{1}{(i+k)(i+k+1)}-\frac{1}{(i+k)(i+k+1)^3}\\
&= k+\frac{1}{i+k+1}+\frac{1}{(i+k)(i+k+1)}\left(1-\frac{1}{(i+k+1)^2}\right)\\
&= k+\frac{1}{i+k+1}+\frac{1}{(i+k)(i+k+1)}\left(\frac{(i+k)(i+k+2)}{(i+k+1)^2}\right)\\
&= k+\frac{1}{i+k+1}+\frac{i+k+2}{(i+k+1)^3}.
\end{aligned}$$

Thus we have

$$\begin{aligned}
R(f^{i+k+1};A,B,\Gamma) = R\Bigg(&f^{1+k+1};k+\frac{1}{i+k+1}+\frac{1}{2}+\frac{1}{(i+k+1)^2},\\
&k+\frac{1}{i+k+1},k+\frac{1}{i+k+1}+\frac{i+k+2}{(i+k+1)^3}\Bigg).
\end{aligned}$$

Now we have $\eta_{f^{i+k+1}, f^{i+k+1}}^{(i+k+1)^{-2}} = \eta_{f,f}$ and $\zeta_{f^{i+k+1}}^{(i+k+2)(i+k+1)^{-3}} = \zeta_f^{i+k+2}$, so this is the map

(4.17)
$$\eta_{f,f} R\left(f^{i+k+1}; k + \frac{1}{i+k+1} + \frac{1}{2}, k + \frac{1}{i+k+1}, k + \frac{1}{i+k+1}\right) \zeta_f^{i+k+2}.$$

When $k = \infty$, we have that ∞_f acts on $\theta(\underline{\infty})$ as $r(f; 0, -1, 0)$ and i_f acts on $\theta(\underline{\infty})$ as $R(f; -i + 1/2, -i, -i)$. Thus, using Lemma 3.12(iv), we see that $\infty_f i_f$ acts on $\theta(\underline{\infty})$ as

(4.18)
$$R(f; -i + 1/2, -i - 1, -i) = \eta_{f,f}\zeta_f R(f; -i - 1 + 1/2, -i - 1, -i - 1).$$

When $k = -i$, we have that ∞_f acts on $\theta(\underline{-i})$ as $R(f; -i + 1/2, -i, -i)$ and i_f acts on $\theta(\underline{-i})$ as $r(f; 0, 1, 0)$. Now using Lemma 3.12(iii) and 3.12(iv), we see that $\infty_f i_f$ acts on $\theta(\underline{-i})$ as

(4.19)
$$\begin{aligned} &\eta_{f,f}^2 \zeta_{f,f,f} R(f; -i + 1/2, -i + 1, -i) \\ &\quad = \eta_{f,f}\zeta_f^2 R(f; -i + 1 + 1/2, -i + 1, -i + 1). \end{aligned}$$

When $k = -i - 1$, we have that ∞_f acts on $\theta(\underline{k})$ as

$$R(f; -i - 1/2, -i - 1, -i - 1)$$

and i_f acts on $\theta(\underline{k})$ as $R(f^{-1}; -2 - i + 1/2, -2 - i, -2 - i)$. Now Lemma 3.12(viii) shows that $\infty_f i_f$ acts on $\theta(\underline{-i-1})$ as $r(f; A, B, \Gamma)$ where

$$\begin{aligned} A &= -i - \tfrac{1}{2} + (-2 - i + \tfrac{1}{2}) - 2(-2 - i) - 1, \\ B &= -i - 1 - (-2 - i), \end{aligned}$$

and

$$\Gamma = (-i - 1 - (-2 - i) + 3(-2 - i + \tfrac{1}{2}) - 3(-2 - i + \tfrac{1}{2})).$$

Thus we have $A = 1$, $B = 1$, and $\Gamma = 1$, so $\infty_f i_f$ acts on $\theta(\underline{-i-1})$ as

(4.20)
$$r(f; 1, 1, 1) = \eta_{f,f}\zeta_f r(f; 0, 1, 0).$$

Now by comparing (4.17)–(4.20) with the definitions of $(i+1)_f$ and $(i+2)_{\psi_f}$, we see that $\infty_f i_f = \eta_{f,f}(i+1)_f(i+2)_{\psi_f}$. □

Definition 4.3. We define the groups P and N_0 by $P = \langle i_f, \delta \mid i \in \mathbb{F}_p \cup \{\infty\}, f \in L, \delta \in R_0 \rangle$ and $N_0 = \langle P, \alpha, \mid \alpha \in A_0 \rangle$.

Lemma 4.5. *$N_0 \cong (p^2 \times p^2) \cdot p^m \cdot p^{2m} \cdot S$, where $m = \dim(C) - 1$.*

Proof. Throughout the proof we use ζ to denote an arbitrary element of $\langle \infty_{\not\zeta}, 0_{\not\zeta} \rangle$. The first step is to show that every element $x \in P$ can be written in the form $\eta \infty_f 0_g$ for some $\eta \in R_0$ and $f, g \in L$. We assume that $x = \prod_s \xi_s$ where each term ξ_s is equal to i_f for some $i \in \mathbb{F}_p \cup \{\infty\}$ and $f \in L$.

Now we replace each $\xi_s = i_f$ such that $i \neq 0$ or ∞ with $\eta_{f,f}^{-i} \infty_f^i 0_f \zeta$ as follows. According to (4.16), we may write $i_f = \eta_{f,f}^{-1} \infty_f (i-1)_f (i+1)_{\psi_f}^{-1}$. Now

if $i-1=0$, this is the desired form and we are done. If $i-1>0$, then by induction we write $(i-1)_f = \eta_{f,f}^{-i+1}\infty_f^{i-1}0_f\zeta$ and get

$$i_f = \eta_{f,f}^{-1}\infty_f\eta_{f,f}^{-i+1}\infty_f^{i-1}0_f\zeta(i+1)_{\psi_f}^{-1}.$$

Thus we see that we can write $i_f = \eta_{f,f}^{-i}\infty_f^{-i}0_f\zeta$ for some $\zeta \in \langle \infty_{\not\in}, 0_{\not\in}\rangle$.

We use (4.6) to move all the terms $\eta_{f,f}$ to the left. Now we use (4.5) to move each term ∞_f to precede each term 0_g and use (4.6) to move all terms $\eta_{f,g}$ this process introduces to the left. Then we use (4.3) to combine the ∞_f and 0_g into a single term ∞_f and 0_g, respectively, and (4.6) again to move all terms $\eta_{f,g}$ that this process introduces to the left. Clearly we may combine all terms $\eta_{f,g}$ that we have collected at the left into a single term η. Additionally, we may write the product of all the terms $\zeta \in \langle \infty_{\not\in}, 0_{\not\in}\rangle$ as a product of $\infty_{\not\in^i}$ and $0_{\not\in^j}$; and since these lie in the center, we can combine these with ∞_f and 0_g according to (4.3). This shows that each $x \in P$ can be written as $\eta\infty_f 0_g$.

Now there are p^m choices for η and p^{m+2} choices for each of f and g, so $|P| \le p^{3m+4}$. Further, (4.5) and (4.6) imply that $Z(P) = \langle \infty_{\not\in}, 0_{\not\in}, \infty_{\$}, 0_{\$}\rangle$, that $P' = \langle \eta, \infty_{\not\in}, 0_{\not\in} \mid \eta \in R_0\rangle$, and that $[P, P'] = \langle \infty_{\not\in}, 0_{\not\in}\rangle$.

Now we claim that if $\eta\infty_f 0_g$ acts trivially on $\mathscr{S}$, then $f = g = 1_L$ and η is the identity of R_0. Suppose that $\eta\infty_f 0_g$ acts trivially on $\mathscr{S}$. Choose $\theta \in \mathscr{S}$ such that $\theta(\underline{0}) = 1_L$. Then $\theta^{\eta\infty_f 0_g}(\underline{0}) = f$, so we have $f = 1_L$. Similarly we have $g = 1_L$. Now if η is not the identity, there exist $d \in L$ with $d^\eta \ne d$ and $\theta \in \mathscr{S}$ with $\theta(\underline{0}) = d$. But then $\theta^\eta(\underline{0}) \ne d$, so $\theta^\eta \ne \theta$. Thus η is the identity, so we have proved the claim. Hence $|P| = p^{3m+4}$ and so P has the desired structure.

Now it is clear from the definition of N_0 that $N_0 = P{:}S$, and (4.6) shows that S normalizes P, so we are done. □

The group $X = GL(2, p)$. Now we proceed to the second step in constructing the group N, defining a group X of permutations of standard luples which is isomorphic to $GL(2, p)$. We have a number of goals in mind. We intend that X will normalize N_0 and P. Also, X will normalize a subgroup $K < Z(P)$ with $|K| = p^2$ and $K \cap P' = 1$.

Here is how we proceed. For each element $g \in GL(V)$, we want to describe a permutation of luples x_g. We define x_g only for two elements $t, \nu \in GL(V)$ which generate $GL(V)$. Then we show that the group $X = \langle x_t, x_\nu\rangle$ is isomorphic to $GL(2, p)$.

For the remainder of this section fix $k \in \mathbb{F}_p$ such that $-k$ is a generator of $\mathbb{F}_p^\times$. Let $t \in GL(2, p)$ satisfy $t(x) = x + y$ and $t(y) = y$, and let $\nu \in GL(2, p)$ satisfy $\nu(x) = y$ and $\nu(y) = kx$. Then t and ν have matrices $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0 & k\\ 1 & 0\end{smallmatrix}\right)$, respectively, with respect to the basis $\{x = \left(\begin{smallmatrix}0\\ 1\end{smallmatrix}\right), y = \left(\begin{smallmatrix}1\\ 0\end{smallmatrix}\right)\}$.

Lemma 4.6. *The group $GL(V)$ is generated by t and ν.*

Proof. It is a standard fact that $SL(V)$ is generated by the subgroups $\langle\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)\rangle$ and $\langle\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)\rangle$. Now $t = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ and $t^\nu = \left(\begin{smallmatrix}1 & 0\\ k & 1\end{smallmatrix}\right)$, so we see that $\langle t, \nu\rangle$ contains $SL(V)$. It is also clear that $GL(V)/SL(V) \cong \mathbb{F}_p^\times$, and the homomorphism of $GL(V)$ onto $\mathbb{F}_p^\times$ is given by the determinant. Since the determinant of $\left(\begin{smallmatrix}0 & k\\ 1 & 0\end{smallmatrix}\right)$

is a generator of $\mathbb{F}_p^\times$, we see that $\langle t, \nu\rangle$ maps onto $\mathbb{F}_p^\times$, so it must be all of $GL(V)$. □

The permutations x_g, $g \in \mathrm{Aut}(V)$, will act as the composition of the natural action of g acting on $\mathrm{Maps}(V, L)$ as described earlier, and certain maps from L to L acting on the range of a luple, which we call "twisting maps". Before we define the maps x_g, we study the twisting maps.

Definition 4.4. We define κ to be the permutation of L which sends $(a, c) \mapsto (-ka, c)$ for all $(a, c) \in L$, where k is the generator of $\mathbb{F}_p$ fixed above.

Now fix an element $\partial \in R$ such that $\$^\partial = \$\psi_\$$. For convenience, choose ∂ to be the identity if $\psi_\$ = 1_L$. It will turn out that the twisting maps all lie in $\mathscr{T} = \langle \mathscr{Y}\partial, \kappa\rangle$. Since $\partial \in \mathrm{Aut}(L)$, it is clear that $R(f; \alpha, \beta, \gamma)^\partial = R(f^\partial; \alpha, \beta, \gamma)$. The next two lemmas give similar relations for $\mathscr{Y}$ and κ.

Lemma 4.7. $R(f; \alpha, \beta, \gamma)^{\mathscr{Y}} = R(f; \alpha+1, \beta+1, \gamma+1)$.

Proof. We determine the image of $g \in L$ under the action of $R(f; \alpha, \beta, \gamma)^{\mathscr{Y}}$. We have

$$\begin{aligned} g^{\mathscr{Y}^{-1}R(f;\alpha,\beta,\gamma)\mathscr{Y}} &= (g\psi_g^{-1})^{R(f;\alpha,\beta,\gamma)\mathscr{Y}} \\ &= (gf\psi_g^{-1}[f, f, g]^\alpha[f, g, g]^\beta\psi_f^\gamma)^{\mathscr{Y}} \\ &= gf\psi_g^{-1}[f, f, g]^\alpha[f, g, g]^\beta\psi_f^\gamma\psi_{fg} \\ &= gf[f, f, g]^{\alpha+1}[f, g, g]^{\beta+1}\psi_f^{\gamma+1}, \end{aligned}$$

where the last step follows from (3.6), which says that $\psi_{fg} = \psi_f\psi_g[f, f, g] \cdot [f, g, g]$. The last expression is the image of g under the action of

$$R(f; \alpha+1, \beta+1, \gamma+1). \quad \square$$

Lemma 4.8. $R(f; \alpha, \beta, \gamma)^\kappa = R(f^\kappa; -k\alpha + 2^{-1}(1+k), -k\beta, -k\gamma)$.

Proof. Let $x = (a, c) \in L$, and suppose that $f = (b, d)$. Then

$$\begin{aligned} x^{\kappa^{-1}R(f;\alpha,\beta,\gamma)\kappa} &= (-\tfrac{1}{k}a, c)^{R(f;\alpha,\beta,\gamma)\kappa} \\ &= (-\tfrac{1}{k}a + b - \tfrac{1}{2}(c, d, d) \\ &\qquad + \alpha(c, d, d) + \beta(c, c, d) + \gamma\Psi(d), c + d)^\kappa \\ &= (a - kb + \tfrac{k}{2}(c, d, d) \\ &\qquad - k\alpha(c, d, d) - k\beta(c, c, d) - k\gamma\Psi(d), c + d) \\ &= (a - kb - \tfrac{1}{2}(c, d, d) + (\tfrac{1+k}{2} - k\alpha)(c, d, d) \\ &\qquad - k\beta(c, c, d) - k\gamma\Psi(d), c + d). \end{aligned}$$

This is the image of x under the map $R(f^\kappa; -k\alpha + 2^{-1}(1+k), -k\beta, -k\gamma)$. □

In the definition of the maps i_f, the elements of the various groups $X(f)$ which appear are of the form $R(f; \beta + 1/2, \beta, \beta)$ or $r(f; 0, \pm 1, 0)$. Applying Lemmas 4.7 and 4.8 gives the following corollary, which describes the action of $\mathscr{Y}$ and κ on maps of this form.

Corollary 4.9. *We have*

$$R(f;\beta+1/2,\beta,\beta)^{\mathscr{Y}} = R(f,\beta+1+1/2,\beta+1,\beta+1)$$

and

$$R(f;\beta+1/2,\beta,\beta)^{\kappa} = R(f^{\kappa},-k\beta+\frac{1}{2},-k\beta,-k\beta).$$

Lemma 4.10.

$$r(f;0,1,0)^{\mathscr{Y}} = r(f;0,1,0) \quad \text{and} \quad r(f;0,1,0)^{\kappa} = r(f;0,-k,0).$$

Proof. The first statement is clear since for $x \in L$ we have $x[f,x,x]\psi_x = x\psi_x[f,x,x]$. For the second statement we notice that for $x=(a,c)\in L$ and $f=(b,d)$ we have

$$\begin{aligned} x^{\kappa^{-1}r(f;0,1,0)\kappa} &= (-k^{-1}a,c)^{r(f;0,1,0)\kappa} \\ &= (-k^{-1}a+(c,d,d),c)^{\kappa} \\ &= (a-k(c,d,d),c) \\ &= x^{r(f;0,-k,0)}. \quad \square \end{aligned}$$

Lemma 4.11. *For $f\in L$, the maps $\mathscr{Y}$ and κ satisfy $(f^l)^{\mathscr{Y}} = (f^{\mathscr{Y}^{l^2}})^l$ and $(f^l)^{\kappa} = (f^{\kappa})^l$.*

Proof. We have $(f^l)^{\mathscr{Y}} = f^l\psi_{f^l} = f^l\psi_f^{l^3}$, while $(f^{\mathscr{Y}^{l^2}})^l = (f\psi_f^{l^2})^l = f^l\psi_f^{l^3}$. The second part follows since multiplication in $\mathbb{F}_p$ is commutative. $\square$

Now we are ready to define x_t and x_ν. According to the scheme we outlined above, $\theta^{x_g}(v) = \theta(gv)^{T_v}$ for some $T_v \in \mathscr{T}$ which depends on v. As with the definitions of the maps i_f, if θ^g is to satisfy (4.2) for each standard luple θ, then for $l\in\mathbb{F}_p$ we have $\theta^g(lv) = \theta(lgv)^{T_{lv}} = \theta(gv)^{e_l T_{lv}}$ and also $\theta^g(lv) = \theta^g(v)^l = \theta(gv)^{T_v e_l}$. Thus since every element of $L(C)$ is in the image of some standard luple, we must have $T_{lv} = e_l^{-1}T_v e_l$.

Definition 4.5. The map x_t is the permutation of luples which preserves the set of standard luples and whose action is given by $\theta^{x_t}(\underline{i}) = \theta(\underline{i+1})^{\mathscr{Y}^{-1}\partial^{-1}}$ for $i\in\mathbb{F}_p\cup\{\infty\}$, with the understanding that $\infty+1=\infty$.

Definition 4.6. The map x_ν is the permutation of luples which preserves the set of standard luples and whose action is given by $\theta^{x_\nu}(\underline{i}) = \theta(\nu\underline{i})^{\kappa\mathscr{Y}^{E_i}}$ where $E_i = 0$ if $i=0$ or ∞ and $E_i = i+i^{-1}+k^2i^{-3}$ otherwise.

The definition of x_ν seems to contradict our earlier assertion that all the twisting maps would lie in $\mathscr{T} = \langle \mathscr{Y}\partial, \kappa\rangle$, since it seems to imply that $\mathscr{Y}$ is a twisting map. There is no contradiction, however, since if $p>3$ we have $\psi_{\mathscr{Y}} = 1_L$ and ∂ is the identity, while if $p=3$ we have $E_i = i+i^{-1}+k^2i^{-3} = 0$.

We remark that since elements of $\mathrm{Aut}(V)$ are linear transformations and the twisting maps act trivially on L/L', the luples θ^{x_g} satisfy (4.1) if θ satisfies (4.1).

If v is an element of V denoted by a member of $\mathbb{F}_p\cup\infty$, the requirement that x_t permute $\mathscr{S}$ allows us to determine the action of x_t and x_ν on $\theta(v)$ for those $v\in V$ which are not mentioned explicitly in the definition.

Lemma 4.12. *Suppose that* $l \in \mathbb{F}_p$ *and* $j \in \{\infty\} \cup \mathbb{F}_p$. *Then* $\theta^{x_t}(l\underline{j}) = \theta(tl\underline{j})^{\mathscr{Y}^{-l^2}\partial^{-1}}$ *and* $\theta^{x_\nu}(l\underline{j}) = \theta(\nu l\underline{j})^{\kappa\mathscr{Y}^{l^2}E_j}$.

Proof. The above discussion showed that the twisting map for $\theta(l\underline{j})$ is the conjugate by e_l of the twisting map for $\theta(v)$ if property (4.2) is to be preserved. Thus

$$\theta^{x_t}(l\underline{j}) = (\theta^{x_t}(\underline{j}))^l = (\theta(t\underline{j})^{\mathscr{Y}^{-1}\partial^{-1}})^l = \left((\theta(t(l\underline{j}))^{l^{-1}})^{\mathscr{Y}^{-1}\partial^{-1}}\right)^l.$$

By Lemma 4.11, $e_l^{-1}\mathscr{Y}^{-1}e_l = \mathscr{Y}^{-l^2}$, and by Lemma 3.8, e_l commutes with ∂. Hence we have $\theta^{x_t}(l\underline{j}) = (\theta(t(l\underline{j}))^{\mathscr{Y}^{-l^2}\partial^{-1}}$. A similar calculation gives the corresponding result for x_ν. □

Now we state and prove some relations that show x_t and x_ν normalize P. Corollary 4.9 showed that maps of the form $R(f; \beta + 1/2, \beta, \beta)$ are conjugated to maps of the form $R(f; \widehat{\beta} + 1/2, \widehat{\beta}, \widehat{\beta})$ for some $\widehat{\beta}$. Also, Lemma 4.1 showed that if a map i_f acts on $\theta(v)$ as $R(f; \beta + \frac{1}{2}, \beta, \beta)$ and $k \in \mathbb{F}_p$, then i_f acts on $\theta(kv)$ as $R(f^k; k^{-2}\beta + \frac{1}{2}, k^{-2}\beta, k^{-2}\beta)$. Since all of the maps we consider in the next lemmas are of this form, we adopt the abbreviation $R(f; \beta)$ for $R(f; \beta + \frac{1}{2}, \beta, \beta)$.

Lemma 4.13. *The maps* $\delta \in R_0$, i_f, *and* x_t *satisfy*:

$$\delta^{x_t} = \delta \quad \text{for all } \delta \in R_0, \tag{4.21}$$

$$\infty_f^{x_t} = \infty_{f\partial^{-1}}, \tag{4.22}$$

$$0_f^{x_t} = 1_{f\partial^{-1}}. \tag{4.23}$$

Proof. As remarked earlier, the natural action of t commutes with δ. Also, $\mathscr{Y}$ commutes with δ, since each acts on an element of L by multiplication by some element of $Z(L)$. Obviously ∂ commutes with δ. Thus x_t commutes with δ, proving (4.21).

For $i \in \mathbb{F}_p$, we have that

$$\begin{aligned}\theta^{x_t^{-1}\infty_f x_t}(\underline{i}) &= \theta^{x_t^{-1}\infty_f}(t\underline{i})^{\mathscr{Y}^{-1}\partial^{-1}} \\ &= \theta^{x_t^{-1}}(\underline{i+1})^{R(f;i+1)\mathscr{Y}^{-1}\partial^{-1}} \\ &= \theta(\underline{i})^{\partial\mathscr{Y}R(f;i+1)\mathscr{Y}^{-1}\partial^{-1}}.\end{aligned}$$

By Lemma 4.7, this last expression is $\theta(\underline{i})^{R(f^{\partial^{-1}};i)}$, and this is equal to $\theta^{\infty_{f'}}(\underline{i})$ where $f' = f^{\partial^{-1}}$.

We also have that

$$\begin{aligned}\theta^{x_t^{-1}\infty_f x_t}(\underline{\infty}) &= \theta^{x_t^{-1}\infty_f}(t\underline{\infty})^{\mathscr{Y}^{-1}\partial^{-1}} \\ &= \theta^{x_t^{-1}}(\underline{\infty})^{r(f;0,-1,0)\mathscr{Y}^{-1}\partial^{-1}} \\ &= \theta(\underline{\infty})^{\partial\mathscr{Y}r(f;0,-1,0)\mathscr{Y}^{-1}\partial^{-1}}.\end{aligned}$$

By Corollary 4.9 the last expression is equal to

$$\theta(\underline{\infty})^{r(f^{\vartheta^{-1}};0,-1,0)} = \theta^{\infty_{f'}}(\underline{\infty}).$$

This proves (4.22).

For $i \in \mathbb{F}_p$, $i \neq -1$, we have that

$$\begin{aligned}\theta^{x_t^{-1}0_f x_t}(\underline{i}) &= \theta^{x_t^{-1}0_f}(\underline{i+1})^{\mathscr{Y}^{-1}\partial^{-1}} \\ &= \theta^{x_t^{-1}}(\underline{i+1})^{R(f^{i+1};\, i+1+(i+1)^{-1})\mathscr{Y}^{-1}\partial^{-1}} \\ &= \theta(\underline{i})^{\partial\mathscr{Y}R(f^{i+1};\, i+1+(i+1)^{-1})\mathscr{Y}^{-1}\partial^{-1}}.\end{aligned}$$

Corollary 4.9 implies that

$$\partial\mathscr{Y}R(f^{i+1};\, i+1+(i+1)^{-1})\mathscr{Y}^{-1}\partial^{-1} = R((f^{\vartheta^{-1}})^{i+1};\, i+(i+1)^{-1}),$$

so the last expression is

$$\theta(\underline{i})^{R((f^{\vartheta^{-1}})^{i+1};\, i+(i+1)^{-1})}.$$

This is equal to $\theta^{1_{f'}}(\underline{i})$.

We also have

$$\begin{aligned}\theta^{x_t^{-1}0_f x_t}(\underline{-1}) &= \theta^{x_t^{-1}0_f}(\underline{0})^{\mathscr{Y}^{-1}\partial^{-1}} \\ &= \theta^{x_t^{-1}}(\underline{0})^{r(f;0,1,0)\mathscr{Y}^{-1}\partial^{-1}} \\ &= \theta(\underline{-1})^{\partial\mathscr{Y}r(f;0,1,0)\mathscr{Y}^{-1}\partial^{-1}}.\end{aligned}$$

Lemma 4.10 implies that $\partial\mathscr{Y}r(f;0,1,0)\mathscr{Y}^{-1}\partial^{-1} = r(f^{\partial^{-1}};0,1,0)$, so the last expression is

$$\theta(\underline{-1})^{r(f^{\vartheta^{-1}};0,1,0)}.$$

This is equal to $\theta^{1_{f'}}(\underline{-1})$.

Finally,

$$\begin{aligned}\theta^{x_t^{-1}0_f x_t}(\underline{\infty}) &= \theta^{x_t^{-1}0_f}(\underline{\infty})^{\mathscr{Y}^{-1}\partial^{-1}} \\ &= \theta^{x_t^{-1}}(\underline{\infty})^{R(f;0)\mathscr{Y}^{-1}\partial^{-1}} \\ &= \theta(\underline{\infty})^{\partial\mathscr{Y}R(f;0)\mathscr{Y}^{-1}\partial^{-1}} \\ &= \theta(\underline{\infty})^{R(f^{\vartheta^{-1}};-1)}.\end{aligned}$$

This is equal to $\theta^{1_{f'}}(\underline{\infty})$, thus proving (4.23). □

Lemma 4.14. *The maps δ, i_f, and x_ν satisfy the following relations:*

$$\delta^{x_\nu} = \delta^{-k} \quad \text{for all } \delta \in R_0, \tag{4.24}$$

$$\infty_f^{x_\nu} = 0_{f^\kappa}, \tag{4.25}$$

$$0_f^{x_\nu} = \infty_{f^{k\kappa}}. \tag{4.26}$$

Proof. Again, the natural action of ν commutes with δ, as does $\mathscr{Y}$. Considering κ and δ as maps on L, we have $\kappa^{-1}\delta\kappa = \delta^{-k}$, since for $(a, c) \in L$ we

have $(a, c)^{\kappa^{-1}\delta\kappa} = (-k^{-1}a, c)^{\delta\kappa} = (-k^{-1}a + \delta(c), c)^{\kappa} = (a - k\delta(c), c)$. Thus $\theta^{x_\nu^{-1}\delta x_\nu}(v) = \theta(w)^{\kappa^{-1}\delta\kappa} = \theta(w)^{\delta^{-k}}$. This proves (4.24).

For $i \in \mathbb{F}_p$, $i \neq 0$, we have that $\theta^{x_\nu^{-1}\infty_f x_\nu}(\underline{i}) = \theta^{x_\nu^{-1}\infty_f}(\nu\underline{i})^{\kappa\mathcal{Y}^{E_i}}$, where $E_i = i + i^{-1} + k^2 i^{-3}$ as given in Definition 4.6. Now $\nu\underline{i} = \nu\binom{i}{1} = \binom{k}{i}$, so we have $\nu\underline{i} = \underline{ik/i} = i(x + (k/i)y)$. By the definition of ∞_f and Lemma 4.1, ∞_f acts on $\theta(\nu\underline{i})$ as $R(f^i; i^{-3}k)$, so we have

$$\theta^{x_\nu^{-1}\infty_f}(\nu\underline{i})^{\kappa\mathcal{Y}^{E_i}} = \theta^{x_\nu^{-1}}(\nu\underline{i})^{R(f^i; i^{-3}k)\kappa\mathcal{Y}^{E_i}} = \theta(\underline{i})^{\mathcal{Y}^{-E_i}\kappa^{-1}R(f^i; i^{-3}k)\kappa\mathcal{Y}^{E_i}}.$$

Corollary 4.9 implies that

$$\begin{aligned}\mathcal{Y}^{-E_i}\kappa^{-1}R(f^i; i^{-3}k)\kappa\mathcal{Y}^{E_i} &= \mathcal{Y}^{-E_i}R(f^i; -i^{-3}k^2)\mathcal{Y}^{E_i}\\ &= R(f^i; -i^{-3}k^2 + E_i)\\ &= R(f^i; -i^{-3}k^2 + i + i^{-1} + k^2 i^{-3})\\ &= R(f^{i\kappa}; i + i^{-1}).\end{aligned}$$

This is the action of 0_{f^κ} on $\theta(\underline{i})$.

We also have $\theta^{x_\nu^{-1}\infty_f x_\nu}(\underline{0}) = \theta^{x_\nu^{-1}\infty_f}(\nu\underline{0})^{\kappa}$ and $\nu\underline{0} = \nu\binom{0}{1} = \binom{k}{0}$, so we have $\nu\underline{0} = k\underline{\infty}$. Thus we have

$$\theta^{x_\nu^{-1}\infty_f}(\nu\underline{0})^{\kappa} = \theta^{x_\nu^{-1}}(k\underline{\infty})^{r(f;0,-k^{-1},0)\kappa} = \theta(\underline{0})^{\kappa^{-1}r(f;0,-k^{-1},0)\kappa}.$$

By Lemma 4.10, $\kappa^{-1}r(f; 0, -k^{-1}, 0)\kappa = r(f; 0, 1, 0)$. This is the action of 0_{f^κ} on $\theta(\underline{0})$.

Finally, we have $\theta^{x_\nu^{-1}\infty_f x_\nu}(\underline{\infty}) = \theta^{x_\nu^{-1}\infty_f}(\nu\underline{\infty})^{\kappa}$. Now $\nu\underline{\infty} = \nu\binom{1}{0} = \binom{0}{1}$, so we have

$$\theta^{x_\nu^{-1}\infty_f}(\nu\underline{\infty})^{\kappa} = \theta^{x_\nu^{-1}}(\underline{0})^{R(f;0)\kappa} = \theta(\underline{\infty})^{\kappa^{-1}R(f;0)\kappa} = \theta(\underline{\infty})^{R(f^\kappa;0)}.$$

This is the action of 0_{f^κ} on $\theta(\underline{\infty})$. This proves (4.25).

For $i \in \mathbb{F}_p$, $i \neq 0$, we have that $\theta^{x_\nu^{-1}0_f x_\nu}(\underline{i}) = \theta^{x_\nu^{-1}0_f}(\nu\underline{i})^{\kappa\mathcal{Y}^{E_i}}$, and by our computation during the proof of (4.22) that $\nu\underline{i} = \underline{ik/i}$, we see that this is

$$\theta^{x_\nu^{-1}}(\nu\underline{i})^{R(f^k; i^{-2}(ki^{-1}+ik^{-1}))\kappa\mathcal{Y}^{E_i}} = \theta(\underline{i})^{\mathcal{Y}^{-E_i}\kappa^{-1}R(f^k; ki^{-3}+(ki)^{-1})\kappa\mathcal{Y}^{E_i}}.$$

Now Corollary 4.9 implies that

$$\begin{aligned}\mathcal{Y}^{-E_i}\kappa^{-1}R(f^k; ki^{-3} + (ki)^{-1})\kappa\mathcal{Y}^{E_i} &= \mathcal{Y}^{-E_i}R(f^{k\kappa}; -k^2 i^{-3} - i^{-1})\mathcal{Y}^{E_i}\\ &= R(f^{k\kappa}; -k^2 i^{-3} - i^{-1} + E_i)\\ &= R(f^{k\kappa}; i),\end{aligned}$$

and this is the action of $\infty_{f^{k\kappa}}$ on $\theta(\underline{i})$.

We also have

$$\theta^{x_\nu^{-1}0_f x_\nu}(\underline{0}) = \theta^{x_\nu^{-1}0_f}(\nu\underline{0})^{\kappa} = \theta^{x_\nu^{-1}}(k\underline{\infty})^{R(f^k;0)\kappa} = \theta(\underline{0})^{\kappa^{-1}R(f^k;0)\kappa},$$

and this is equal to $\theta(\underline{0})^{R(f^{k\kappa};0)}$. This is the action of $\infty_{f^{k\kappa}}$ on $\theta(\underline{0})$.

Finally, we check that

$$\begin{aligned}\theta^{x_\nu^{-1}0_f x_\nu}(\underline{\infty}) &= \theta^{x_\nu^{-1}0_f}(\nu\underline{\infty})^\kappa \\ &= \theta^{x_\nu^{-1}0_f}(\underline{0})^\kappa \\ &= \theta^{x_\nu^{-1}}(\underline{0})^{r(f;0,1,0)\kappa} \\ &= \theta(\underline{\infty})^{\kappa^{-1}r(f;0,1,0)\kappa}.\end{aligned}$$

Now Lemma 4.10 implies that $\kappa^{-1}r(f;0,1,0)\kappa = r(f;0,-k,0)$. This is the action of ∞_{f^κ} on $\theta(\underline{\infty})$, thus proving (4.26). □

Now we have defined a set of generators of N.

Definition 4.7. We define the group of permutations of standard luples $N = \langle N_0, x_t, x_\nu\rangle$, where N_0 is the group of Definition 4.3. We also define the subgroup $K = \langle \infty_\$ 0_{\psi_\$}, 0_\$ \infty_{\psi_\$}^{-1}\rangle$.

Theorem 4.15. *$N \cong (p^2 \times p^2)\cdot p^m \cdot p^{2m}\cdot (S \times GL(2,p))$, and K is normal in N.*

Proof. Lemmas 4.5, 4.13, and 4.14 show that N normalizes P. We claim that $[x_g, \alpha] \in P$ for $\alpha \in S$. This then implies that $N_0 \triangleleft N$. First, α and $\mathcal{Y}$ commute, viewed as permutations of L, since $f^{\mathcal{Y}\alpha} = f^\alpha \psi_f$, $f^{\alpha\mathcal{Y}} = f^\alpha \psi_{f^\alpha}$, and $\psi_f = \psi_{f^\alpha}$ when $\alpha \in S$. Then we find that

$$\theta^{x_t^{-1}\alpha x_t}(\underline{i}) = \theta(\underline{i+1})^{\partial\mathcal{Y}\alpha\mathcal{Y}^{-1}\partial^{-1}} = \theta(\underline{i+1})^{\partial\alpha\partial^{-1}} = \theta(\underline{i+1})^{\alpha\partial^\alpha\partial^{-1}}.$$

Now $\partial^\alpha\partial^{-1} \in R_0 < P$, so this proves the claim when $g = t$. Clearly κ commutes with α, so we also have

$$\theta^{x_\nu^{-1}\alpha x_\nu}(\underline{i}) = \theta(\nu\underline{i})^{\mathcal{Y}^{-E_i}\kappa^{-1}\alpha\kappa\mathcal{Y}^{E_i}} = \theta(\nu\underline{i})^\alpha, \tag{4.27}$$

proving the claim when $g = \nu$.

Now that we have shown $N_0 \triangleleft N$, we need only show that $N/N_0 \cong GL(2,p)$. Let $X = \langle x_t, x_\nu\rangle$. Then $N = N_0X$ and $N/N_0 \cong X/X \cap N_0$. There is a map from X to $GL(2,p)$ gotten by considering the action of X on the sets $v(u) = \{\theta \mid \pi\circ\theta(v) = u\}$ where $v \in V$. An element $x_g \in X$ acts on $v(u)$ by its action on the elements of $v(u)$, so we get

$$\begin{aligned}v(u)^{x_g} &= \{\theta^{x_g} \mid \pi\circ\theta(v) = u\} \\ &= \{\theta \mid \pi\circ\theta^{x_{g^{-1}}}(v) = u\} \\ &= \{\theta \mid \pi(\theta(g^{-1}v)^{\kappa^a\mathcal{Y}^b\partial^b}) = u\} \\ &= \{\theta \mid \pi\circ\theta(g^{-1}v) = u\} \\ &= (g^{-1}v)(u).\end{aligned}$$

Next, for $v \in V$ let $\overline{v} = \{v(u) \mid u \in C\}$, so we have $\overline{v}^{x_g} = \overline{g^{-1}v}$. Now we originally let $\mathrm{Aut}(V)$ have a left action on V, but we can get a right action from this by the rule $v^g = g^{-1}v$. If we identify $\overline{v}$ with $v \in V$, then the map $h : X \to \mathrm{Aut}(V)$ defined by $x_g \mapsto g$ is a homomorphism of X onto $\mathrm{Aut}(V) \cong GL(2,p)$, where the action of $\mathrm{Aut}(V)$ on V is on the right.

Now if $x \in X$ is in the kernel of h, for each $j \in \mathbb{F}_p \cup \{\infty\}$ we must have $\theta^x(\underline{j}) = \theta(\underline{j})^{\kappa^a \gamma^b \partial^b}$ for some a, b which depend on j. By using Corollary 4.9, if a and b are not both 0, we can choose β such that $R(f; \beta)^{\kappa^a \gamma^b \partial^b} = R(f^{\partial^b}; \widehat{\beta})$ and $\widehat{\beta} \neq \beta$. Now for any $\beta \in \mathbb{F}_p$ and $j \in \mathbb{F}_p \cup \{\infty\}$, there exists i such that $\beta_{ij} = \beta$, and it follows that $i_f^x \notin P$. This gives a contradiction, since x normalizes P. Hence we have $a = b = 0$, and so x is the identity. Since this is true for any x in the kernel of h, we have $X \cong GL(2, p)$. Now it also follows from this that $X \cap N_0 = 1$, so we have shown that $N \cong (p^2 \times p^2) \cdot p^m \cdot p^{2m} \cdot (S \times GL(2, p))$.

To see that K is normal in N, (4.25) and (4.26) show that x_ν conjugates $\infty_\$ 0_{\psi_\$}^{-1}$ to $0_\$ \infty_{\psi_\$}^{k^2} = 0_\$ \infty_{\psi_\$}$, with the last equality following from the fact that $\psi_\$ = 1_L$ if $p > 3$ and $k^2 = 1$ if $p = 3$. Similarly we get that x_ν conjugates $0_\$ \infty_{\psi_\$}$ to $\infty_{\$^k} 0_{\psi_\$}^{-k} = \infty_{\$^k} 0_{\psi_\$}^{-1}$.

We also compute, using (4.22) and (4.23), that the conjugate of $\infty_\$ 0_{\psi_\$}$ by x_t is $\infty_\$ \infty_{\psi_\$}^{-1} 1_{\psi_\$}$. By (4.16) this is equal to $\infty_\$ 0_{\psi_\$}$. Similarly we get that x_t conjugates $0_\$ \infty_{\psi_\$}^{-1}$ to $1_\$ 1_{\psi_\$}^{-1} \infty_{\psi_\$}^{-1}$. By (4.16) this is equal to $1_\$ 2_{\psi_\$}^{-1}$. Now by (4.16) again we have

$$\infty_\$ 0_{\psi_\$} 0_\$ \infty_{\psi_\$}^{-1} = \infty_\$ 0_\$ 0_{\psi_\$} \infty_{\psi_\$}^{-1} = 1_\$ 2_{\psi_\$} 0_{\psi_\$} \infty_{\psi_\$}^{-1}.$$

Now the terms $i_{\psi_\$}$ simplify as

$$2_{\psi_\$} 0_{\psi_\$} \infty_{\psi_\$}^{-1} = 1_{\psi_\$} 0_{\psi_\$} = \infty_{\psi_\$} 0_{\psi_\$}^2 = (2^{-1})_{\psi_\$}^2.$$

Now in the only possible case where $\psi_\$ \neq 1_L$, we have $p = 3$. Then we have $2^{-1} = 2$, and 2_f has order 3, so

$$(2^{-1})_{\psi_\$}^2 = 2_{\psi_\$}^{-1}.$$

Thus we do have that $(0_\$ \infty_{\psi_\$}^{-1})^{x_t} = 1_\$ 2_{\psi_\$}^{-1}$ is an element of K, so K is normal in N. □

Remark. For any $s \in \mathrm{Aut}(V)$, we define x_s to be $h^{-1}(s)$.

Definition 4.8. Let $\overline{N} = N/K$, and for any subgroup $H \leq N$ let $\overline{H} = HK/K$. Let $Q_\infty = \langle x_t, 0_{\not\in}, \infty_f, \delta, \mid f \in L, \delta \in R_0 \rangle$, and let $N_\infty = N_N(\langle \infty_{\not\in} \rangle)$.

The next lemma describes the action of $x_h \in X$ when h is a diagonal matrix of $GL(2, p)$. Let $\kappa(b) : L \to L$ be the element of $\langle \kappa \rangle$ which acts as $(a, c) \mapsto (ab, c)$. Then from the definition of x_t and x_ν we see that for any $g \in \mathrm{Aut}(V)$, the element of $\langle \kappa \rangle$ which occurs in each twisting map for x_g is $\kappa(\det(g))$, where $\det(g)$ is the determinant of g.

Lemma 4.16. *Let* $x_h \in X = \langle x_t, x_\nu \rangle$ *with* $h = \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$. *Then the action of* x_h *on elements of* Q_∞ *is given by*

$$0_f^{x_h} = 0_{f^{\kappa(ab)}}^{a}, \tag{4.28}$$

$$\delta^{x_h} = \delta^{ab}, \tag{4.29}$$

$$\infty_f^{x_h} = \infty_{f^{\kappa(ab)}}^{b}, \qquad \textit{and} \tag{4.30}$$

$$x_t^{x_h} = x_t^{a^{-1}b}. \tag{4.31}$$

Proof. First, from the comments above we see that each twisting map for x_h is $\kappa(ab)(\partial\mathcal{Y})^c$ for some c. Since $hy = ay$ and $hx = bx$, we compute that for $\theta \in \mathcal{S}$ we have

$$\begin{aligned}\theta^{x_h^{-1}0_f x_h}(y) &= \theta(y)^{(\partial\mathcal{Y})^{-c}\kappa(ab)^{-1}R(f^a;0)\kappa(ab)(\partial\mathcal{Y})^c} \\ &= \theta(y)^{(\partial\mathcal{Y})^{-c}R((f^a)^{\kappa(ab)};0)(\partial\mathcal{Y})^c} \\ &= \theta(y)^{R((f^a)^{\kappa(ab)\partial^c};c)},\end{aligned}$$

the last step following from Corollary 4.9. We also compute

$$\begin{aligned}\theta^{x_h^{-1}0_f x_h}(x) &= \theta(x)^{(\partial\mathcal{Y})^{-c}\kappa(ab)^{-1}r(f;0,b^{-1},0)\kappa(ab)(\partial\mathcal{Y})^c} \\ &= \theta(x)^{r(f;0,a,0)},\end{aligned}$$

the last step following from Lemma 4.10. Since x_h normalizes P, and since elements of the form 0_g for some $g \in L$ are the only elements of P which act on $\theta(x)$ as $r(g;0,a,0)$ and act on $\theta(y)$ as $R(g;c)$, we have $x_h^{-1}0_f x_h = 0_g$ for some $g \in L$, and so $c = 0$. From the discussion following Lemma 4.3 we have $0_{f^a} = 0_f^a$, so we have $0_f^{x_h} = 0_{f^{\kappa(ab)}}^{a}$. This proves (4.29). A similar computation shows that $\infty_f^{x_h} = \infty_{f^{\kappa(ab)}}^{b}$, proving (4.31).

Next, for $\delta \in R_0$ we have

$$\theta^{x_h^{-1}\delta x_h}(x) = \theta(x)^{(\partial\mathcal{Y})^{-c}\kappa(ab)^{-1}\delta\kappa(ab)(\partial\mathcal{Y})^c}.$$

Now for $(c, d) \in L$, we have

$$\begin{aligned}(c,d)^{\kappa(ab)^{-1}\delta\kappa(ab)} &= (c(ab)^{-1}, d)^{\delta\kappa(ab)} \\ &= (c(ab)^{-1} + \delta(d), d)^{\kappa(ab)} \\ &= (c + ab\delta(d), d),\end{aligned}$$

so we have $\kappa(ab)^{-1}\delta\kappa(ab) = \delta^{ab}$. Now for $(c, d) \in L$, we have

$$\begin{aligned}(c,d)^{\mathcal{Y}^{-1}\delta\mathcal{Y}} &= (c - \Psi(d), d)^{\delta\mathcal{Y}} \\ &= (c - \Psi(d) + \delta(d), d)^{\mathcal{Y}} \\ &= (c + \delta(d), d),\end{aligned}$$

so $\mathcal{Y}$ commutes with δ and obviously ∂ commutes with δ. Thus $\delta^{x_h} = \delta^{ab}$, proving (4.30).

Finally, since $t^h = t^{a^{-1}b}$ and the map $x_g \mapsto g$ is an isomorphism from X to $GL(2, p)$, we have $x_t^{x_h} = x_t^{a^{-1}b}$, proving (4.32). □

Theorem 4.17. (1) $Q_\infty \cong p \times p_+^{1+n}$, *and* $\overline{Q_\infty} \cong p_+^{1+n}$.

(2) $N_\infty \cong Q_\infty \cdot ((p-1) \times (p^{m+1}:S):(p-1))$, *and* $\overline{N_\infty} \cong \overline{Q_\infty} \cdot ((p-1) \times (p^m:S):(p-1))$.

Proof. The proof is basically an application of the relations in Lemmas 4.3, 4.4, 4.13, and 4.14. By (4.5), (4.6), (4.21), (4.22), and (4.23) we see that $Q'_\infty = \langle \infty_{\not\phi} \rangle$. We have that $[0_{\not\phi}, x_t] = \infty_{\not\phi}$, and if $f \notin Z(L)$ there exists $\delta \in R_0$ such that $[\infty_f, \delta] = \infty_{\not\phi}$. Also, for $\delta \in R_0$, we can find $f \in L$ such that $[\infty_f, \delta] = \infty_{\not\phi}$. Now $Q_\infty \cap K = \langle \infty_\$ 0_{\psi_\$} \rangle$. Equations (4.5) and (4.6) show that $\infty_\$ 0_{\psi_\$}$ commutes with $0_{\not\phi}$, ∞_f, and $\delta \in R_0$. From (4.22) and (4.23) we have $(\infty_\$ 0_{\psi_\$})^{x_t} = \infty_\$ \infty_{\psi_\$}^{-1} 1_{\psi_\$}$. By (4.16) we have $\infty_{\psi_\$}^{-1} 1_{\psi_\$} = 0_{\psi_\$}$, so $(\infty_\$ 0_{\psi_\$})^{x_t} = \infty_\$ 0_{\psi_\$}$. Thus $Z(Q_\infty) = \langle \infty_{\not\phi}, \infty_\$ 0_{\psi_\$} \rangle$. Now Lemma 2.5 proves that $Q_\infty \cong p \times p_+^{1+n}$. Since $Q_\infty \cap K < Z(Q_\infty) \setminus Q'_\infty$, we have $\overline{Q_\infty} \cong p_+^{1+n}$. This proves (i).

For all $\alpha \in S$, it is clear that α centralizes $\infty_{\not\phi}$. It is also clear that for any $f \in L$, 0_f centralizes $\infty_{\not\phi}$. These maps generate a subgroup of N_∞/Q_∞ isomorphic to $p^{m+1}:S$ where the subgroup of shape p^{m+1} is elementary abelian and isomorphic to C as a module for S. Now let z be the element of $X = \langle x_t, x_\nu \rangle$ of order $p-1$ corresponding to the element of $GL(2, p)$ with matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -k \end{smallmatrix}\right)$, where $-k$ is the generator of the multiplicative group of $\mathbb{F}_p$ as in the definition of x_ν. By (4.31) we see that z normalizes $\langle \infty_{\not\phi} \rangle$. By (4.29) we see that $0_f^z = 0_{f^\kappa}$, so z commutes with 0_f modulo Q_∞. From the proof of Theorem 4.15 we see that the commutator of z and S is contained in Q_∞. Similarly, $Z(X)$ normalizes $\langle \infty_{\not\phi} \rangle$, the subgroup generated by the maps ∞_f, and the subgroup generated by the maps 0_f, for all $f \in L$. Obviously it centralizes x_t and z, so we see that $Q_\infty \lhd N_\infty$ and $N_\infty/Q_\infty = \langle z \rangle \times ((p^{m+1}:S):Z(X)) \cong (p-1) \times ((p^{m+1}:S):(p-1))$. This proves the first part of (ii). To show that $\overline{N_\infty} \cong \overline{Q_\infty} \cdot (p-1 \times (p^m:S):(p-1))$, we note first that $K < N_\infty$, and $K \setminus Q_\infty$ contains $0_\$ \infty_{\psi_\$}^{-1}$. Now $\infty_{\psi_\$}^{-1} \in Q_\infty$, so $\overline{N_\infty} \cong \overline{Q_\infty} = N_\infty/Q_\infty K = N_\infty/\langle Q_\infty, 0_\$ \rangle$. Now $0_\$ \langle Q_\infty \rangle$ is contained in the elementary abelian subgroup of N_∞/Q_∞ which is isomorphic to C as an S module. Thus $N_\infty/\langle Q_\infty, 0_\$ \rangle \cong (p-1) \times p^m:S:(p-1)$, proving the second part of (ii). □

5. Lattices related to the groups $\overline{N}_\infty$

In this section we construct lattices from self-orthogonal codes. These lattices are related to the groups N_∞ in that a large subgroup of N_∞/Q_∞ is isomorphic to a subgroup of the automorphism group of the lattice. For the three codes that are of special interest to us, it turns out that N_∞/Q_∞ is isomorphic to the monomial subgroup of the automorphism group. This construction is a generalization of the construction of the complex Leech lattice in [16] and the lattice

for the Hall-Janko group in [17]. It is also similar to some of the constructions described in Chapters 7 and 8 of [5].

The Lattice Λ.

Definition 5.1. Let p be an odd prime and let $\varepsilon = e^{2\pi i/p}$. Let C be a self-orthogonal code of length n over $\mathbb{F}_p$, and let $u \in C$ be a vector of weight n fixed by S, the group of permutations in $\mathrm{Aut}(C)$. Let l and Ψ be the functions of Definitions 3.6 and 3.7, respectively. The lattice $\Lambda(C)$ is the set of all vectors $v = (v_i)$ in $\mathbb{Z}[\varepsilon]^n$ satisfying the following properties:

(5.1) There exists $m \in \mathbb{Z}$ such that $v_i \equiv ml(u_i) \pmod{(\varepsilon - 1)}$,

(5.2) $$\sum_{i=1}^{n} l(c_i)v_i \equiv 0 \pmod{(\varepsilon - 1)^2} \quad \text{for all } c = (c_i) \in C,$$

(5.3) $$\sum_{i=1}^{n} l(u_i)v_i \equiv -mpl(\Psi(u)) \pmod{(\varepsilon - 1)^3}.$$

We shall usually let the code C be understood and just write Λ for $\Lambda(C)$.

Lemma 5.1. *The lattice Λ contains the following vectors:*

$$\lambda_c = (l(c_i)(\varepsilon - \varepsilon^{-1})) \qquad \text{for } c \in C,$$
$$\lambda_j = (l(u_i) + \delta_{ij}pl(u_j\Psi(u))) \qquad \text{for } 1 \le j \le n,$$
$$\lambda_\delta = \left(l(\delta_i)(\varepsilon - \varepsilon^{-1})(\varepsilon^2 - \varepsilon^{-2})\right) \qquad \text{for } \delta \in \mathbb{F}_p^n,\ \sum \delta_i u_i = 0.$$

Proof. Since $\varepsilon - \varepsilon^{-1} \in (\varepsilon - 1)\mathbb{Z}[\varepsilon]$, λ_c satisfies (5.1) with $m = 0$. For any $d \in C$, we have

$$\sum_{i=1}^{n} l(d_i)l(c_i) \equiv 0 \pmod{(\varepsilon - 1)^2}$$

since C is self-orthogonal and $p \equiv 0 \pmod{(\varepsilon - 1)^{p-1}}$ by (2.4). Thus we see that

$$\sum_{i=1}^{n} l(d_i)l(c_i)(\varepsilon - \varepsilon^{-1}) \equiv 0 \pmod{(\varepsilon - 1)^2} \qquad \text{and}$$
$$\sum_{i=1}^{n} l(u_i)l(c_i)(\varepsilon - \varepsilon^{-1}) \equiv 0 \pmod{(\varepsilon - 1)^3},$$

and thus λ_c satisfies (5.2) and (5.3).

Since by (2.4) $p \in (\varepsilon - 1)^{p-1}$, we see that λ_j satisfies (5.1) with $m = 1$. To show that λ_j satisfies (5.2) we need to check that

$$\sum_{i=1}^{n} l(c_i)(l(u_i) + \delta_{ij}pl(u_j\Psi(u))) \equiv 0 \pmod{(\varepsilon - 1)^2}.$$

This is clear since C is self-orthogonal and $p \in (\varepsilon - 1)^{p-1}$. To show that it satisfies (5.3) we need to check that

$$\sum_{i=1}^{n} l(u_i)(l(u_i) + \delta_{ij} p l(u_i \Psi(u))) \equiv -p l(\Psi(u)) \pmod{(\varepsilon - 1)^3}.$$

From the definition of Ψ we have $\sum_{i=1}^{n} l(u_i)^2 \equiv 3l(\Psi(u))$. If $\Psi(u) = 0$, then this shows λ_j satisfies (5.3) since $\sum_{i=1}^{n} l(u_i)^2 \equiv 3l(\Psi(u)) \equiv 0 \pmod{(\varepsilon - 1)^3}$. If $\Psi(u) \neq 0$, we have $p = 3$, so $l(u_i)^2 = 1$. Thus $l(u_j)^2 \Psi(u) = \Psi(u)$, so we have $\sum_{i=1}^{n} l(u_i)^2 + 3l(\Psi(u)) \equiv 3l(\Psi(u)) + 3l(\Psi(u)) \equiv -3\Psi(u) \pmod{(\varepsilon - 1)^3}$. Since in this case we have $m = 1$, where m is the constant from (5.1), λ_j satisfies (5.3).

Obviously λ_δ satisfies (5.1) and (5.2), since $(\varepsilon - \varepsilon^{-1})(\varepsilon^2 - \varepsilon^{-2}) \in (\varepsilon - 1)^2$. We have

$$\sum_{i=1}^{n} l(u_i) l(\delta_i)(\varepsilon - \varepsilon^{-1})(\varepsilon^2 - \varepsilon^{-2}) \equiv 0 \pmod{(\varepsilon - 1)^3}$$

since $\delta(u) = 0$ implies $\sum_{i=1}^{n} l(u_i) l(\delta_i) \equiv 0 \pmod{(\varepsilon - 1)^{p-1}}$. Thus λ_δ satisfies (5.3). □

Occasionally we use λ_t to denote the vector $(l(u_i))$. Thus if $\Psi(u) = 0$, we have $\lambda_t = \lambda_j$ for any j.

We let Λ^i be the set of all $v \in \Lambda$ such that i is the smallest integer such that for some j with $1 \leq j \leq n$, v_j is a multiple of $(\varepsilon - 1)^i$ but not a multiple of $(\varepsilon - 1)^{i+1}$. Thus we have $\lambda_\delta \in \Lambda^2$, $\lambda_c \in \Lambda^1$, and $\lambda_j \in \Lambda^0$.

Now we describe some diagonal matrices in $\mathrm{Aut}_{\mathbb{Z}[\varepsilon]}(\Lambda)$.

Definition 5.2. Let A_c be the diagonal matrix $\mathrm{diag}(\varepsilon^{u_i^{-1} c_i})$.

Lemma 5.2. *The matrix A_c is in* $\mathrm{Aut}_{\mathbb{Z}[\varepsilon]}(\Lambda)$.

Proof. If $v \in \Lambda$, then vA_c satisfies (5.1) with the same value of m, since $(vA_c)_i \equiv v_i \pmod{(\varepsilon - 1)}$. To show that vA_c satisfies (5.2) we need to check that $\sum_{i=1}^{n} l(d_i) \varepsilon^{u_i^{-1} c_i} v_i \equiv 0 \pmod{(\varepsilon - 1)^2}$ for $d \in C$. We have

$$\begin{aligned}\sum_{i=1}^{n} l(d_i) \varepsilon^{u_i^{-1} c_i} v_i &= \sum_{i=1}^{n} l(d_i) v_i + \sum_{i=1}^{n} l(d_i)(\varepsilon^{u_i^{-1} c_i} - 1) v_i \\ &\equiv \sum_{i=1}^{n} l(d_i) v_i + \sum_{i=1}^{n} l(d_i) l(u_i^{-1} c_i)(\varepsilon - 1) v_i \pmod{(\varepsilon - 1)^2},\end{aligned}$$

the last step following from (2.3). Now $\sum_{i=1}^{n} l(d_i) v_i \equiv 0 \pmod{(\varepsilon - 1)^2}$ since $v \in \Lambda$, so all that remains to show is that

$$\sum_{i=1}^{n} l(d_i) l(u_i^{-1} c_i)(\varepsilon - 1) v_i \equiv 0 \pmod{(\varepsilon - 1)^2}.$$

We have $(\varepsilon - 1) v_i \equiv (\varepsilon - 1) m l(u_i) \pmod{(\varepsilon - 1)^2}$, so this is congruent to

$$\sum_{i=1}^{n} l(d_i) l(u_i^{-1} c_i)(\varepsilon - 1) m l(u_i) \equiv m(\varepsilon - 1) \sum_{i=1}^{n} l(d_i) l(c_i) \pmod{(\varepsilon - 1)^2}.$$

Since C is self-orthogonal, we have $\sum_{i=1}^{n} l(d_i)l(c_i) \equiv 0 \pmod{(\varepsilon-1)^{p-1}}$, so the last expression is congruent to 0 and vA_c satisfies (5.2).

To show that vA_c satisfies (5.3) we must check that $\sum_{i=1}^{n} l(u_i)\varepsilon^{u_i^{-1}c_i}v_i \equiv -mpl(\Psi(u)) \pmod{(\varepsilon-1)^3}$. Similar to the argument in checking (5.2), we have

$$\begin{aligned}\sum_{i=1}^{n} l(u_i)\varepsilon^{u_i^{-1}c_i}v_i &= \sum_{i=1}^{n} l(u_i)v_i + \sum_{i=1}^{n} l(u_i)(\varepsilon^{u_i^{-1}c_i}-1)v_i \\ &= \sum_{i=1}^{n} l(u_i)v_i + \sum_{i=1}^{n} l(u_i)(\varepsilon^{u_i^{-1}c_i/2})(\varepsilon^{u_i^{-1}c_i/2}-\varepsilon^{-u_i^{-1}c_i/2})v_i \\ &\equiv \sum_{i=1}^{n} l(u_i)v_i + \sum_{i=1}^{n} l(u_i)\varepsilon^{u_i^{-1}c_i/2}l(u_i^{-1}c_i/2)(\varepsilon-\varepsilon^{-1})v_i \\ &\qquad \pmod{(\varepsilon-1)^3},\end{aligned}$$

with the last equivalence following from (2.1). This last expression is equivalent to

$$\sum_{i=1}^{n} l(u_i)v_i + l(1/2)\sum_{i=1}^{n} \varepsilon^{u_i^{-1}c_i/2}l(c_i)(\varepsilon-\varepsilon^{-1})v_i \pmod{(\varepsilon-1)^3}.$$

In the argument that vA_c satisfies (5.2) we showed that $\sum_{i=1}^{n} \varepsilon^{u_i^{-1}c_i/2}l(c_i)v_i \equiv 0 \pmod{(\varepsilon-1)^2}$, so we have

$$l(1/2)\sum_{i=1}^{n} \varepsilon^{u_i^{-1}c_i/2}l(c_i)(\varepsilon-\varepsilon^{-1})v_i \equiv 0 \pmod{(\varepsilon-1)^3}.$$

Since $\sum_{i=1}^{n} l(u_i)v_i \equiv -mp\Psi(u) \pmod{(\varepsilon-1)^3}$ and the value of m in (5.1) is the same for v and vA_c, we see that vA_c satisfies (5.3). □

In addition to the diagonal matrices A_c, we get elements of $\mathrm{Aut}_{\mathbb{Z}[\varepsilon]}(\Lambda)$ from certain elements of $\mathrm{Aut}(C)$. Let $\mathrm{Aut}_1(C)$ be the set of all matrices in $\mathrm{Aut}(C)$ which have each entry equal to ± 1. Suppose that $B \in \mathrm{Aut}_1(C)$ and B stabilizes $\langle u\rangle$. Define $l(B)$, an $n \times n$ matrix over $\mathbb{Z}$, by $l(B)_{ij} = (l(B_{ij}))$. It is clear that if $v \in \Lambda$, then $vl(B)$ also is in Λ, since it satisfies (5.1)–(5.3). Let $S_u = \langle l(B) \mid B \in \mathrm{Aut}_1(C)\rangle$.

It is clear that the scalar matrix $\mathrm{diag}(-1^n) \in \mathrm{Aut}_{\mathbb{Z}[\varepsilon]}(\Lambda)$, and that A_u is the scalar matrix $\mathrm{diag}(\varepsilon^n)$. Use σ_k to denote the $\mathbb{Z}$-automorphism of Λ induced by the ring automorpism of $\mathbb{Z}[\varepsilon]$ defined by $\varepsilon \mapsto \varepsilon^k$.

Definition 5.3. We define $M(\Lambda) = \langle A_c, l(B), \mathrm{diag}(-1^n) \mid c \in C, B \in S\rangle$ and $M^*(\Lambda) = \langle M(\Lambda), \sigma_k \mid k \in \mathbb{F}_p^\times\rangle$. Also let $\overline{M}(\Lambda) = M(\Lambda)/\langle A_u\rangle$ and $\overline{M}^*(\Lambda) = M^*(\Lambda)/\langle A_u\rangle$.

It is easy to see that $M(\Lambda) \cong 2 \times C{:}S$ and $M^*(\Lambda) \cong 2 \times C{:}S{:}(p-1)$.

The homomorphism ϕ.

Definition 5.4. We let $\lambda_b \in \Lambda$ be the element of $\Lambda + (\varepsilon - 1)\Lambda$ represented by any of the vectors

$$(l(u_i^{-1})(\varepsilon - \varepsilon^{-1})(\varepsilon^2 - \varepsilon^{-2})(\varepsilon^4 - \varepsilon^{-4})_{\text{on } i}, 0_{\text{elsewhere}}).$$

Recall that in Chapter 4 we defined the twisting map for x_t to be the map $\mathscr{Y}^{-1}\partial^{-1}$, where ∂ is a fixed element of R such that $\$^{\partial} = \$^{\mathscr{Y}}$. The group R is isomorphic to $\mathrm{Hom}(C, \mathbb{F}_p)$. We identify $\mathbb{F}_p^n/C$ with $\mathrm{Hom}(C, \mathbb{F}_p)$ by letting $\delta = (\delta_i) \in \mathbb{F}_p^n$ correspond to the map $c \mapsto \sum_{i=1}^n \delta_i c_i$. Since C is self-orthogonal, C is in the kernel of this map from $\mathbb{F}_p^n \to \mathrm{Hom}(C, \mathbb{F}_p)$. Now let ∂_j be the element of R whose corresponding coset in $\mathbb{F}_p^n/C$ contains

$$(u_j^{-1}\Psi(u)_{\text{on } j}, 0_{\text{elsewhere}}).$$

Then $\partial\partial_j^{-1} \in R_0$, so we may view it as an element of N. Now we let $x_j = x_t\partial\partial_j^{-1}$ (so $x_j = x_t$ if $\Psi(u) = 0$).

Definition 5.5. We define the map $\phi : Q_\infty \to \Lambda/(\varepsilon - 1)\Lambda$ by

$$\begin{aligned}
\phi(0_{\not\phi}) &= -\lambda_b + \Lambda/(\varepsilon - 1)\Lambda;\\
\phi(\delta) &= l(8)\lambda_\delta + \Lambda/(\varepsilon - 1)\Lambda;\\
\phi(\infty_f) &= \begin{cases} \lambda_{\pi(f)} - \Psi(\pi(f))\lambda_b + \Lambda/(\varepsilon - 1)\Lambda & \text{if } p = 3,\\ -l(128)\lambda_{\pi(f)} + \Lambda/(\varepsilon - 1)\Lambda & \text{if } p \geq 3; \end{cases}\\
\phi(x_j) &= l(256)\lambda_j + \Lambda/(\varepsilon - 1)\Lambda
\end{aligned}$$

and extend by linearity to get the value of ϕ on those elements of Q_∞ not mentioned explicitly.

Since the intersection of any pair of the subgroups

$$\langle 0_{\not\phi}\rangle, \ \langle \delta \mid \delta \in R_0\rangle, \ \langle \infty_f \mid f \in L\rangle, \text{ and } \langle x_j\rangle$$

is the identity and ϕ takes the identity of Q_∞ to $0 \in \Lambda/(\varepsilon - 1)\Lambda$, ϕ is well defined.

Lemma 5.3. *The map ϕ is a group homomorphism.*

Proof. This amounts to checking that $\phi(\delta\epsilon) \equiv \phi(\delta) + \phi(\epsilon)$ for $\delta, \epsilon \in R_0$ and $\phi(\infty_f\infty_g) \equiv \phi(\infty_f) + \phi(\infty_g)$. For the first of these we need to show that $\lambda_\delta + (\varepsilon - 1)\Lambda$ is independent of the representative chosen for δ in $\mathbb{F}_p^n$. Thus we need to show that if $c \in C$, then $v = (\varepsilon - \varepsilon^{-1})(\varepsilon^2 - \varepsilon^{-2})(l(c_i)) \in (\varepsilon - 1)\Lambda$. This is easy to verify since $(\varepsilon - \varepsilon^{-1})(l(c_i)) \in \Lambda$. Then it is clear that for $\delta, \epsilon \in R_0$, we have $\phi(\delta) + \phi(\epsilon) = \lambda_\delta + \lambda_\epsilon \equiv \lambda_{\delta\epsilon} \pmod{(\varepsilon - 1)\Lambda}$, and $\lambda_{\delta\epsilon} = \phi(\delta\epsilon)$.

Next we check that $\phi(\infty_f\infty_g) \equiv \phi(\infty_f) + \phi(\infty_g)$. If $p > 3$ we have $\Psi(c) = 0$ for all $c \in C$, and $p \in (\varepsilon - 1)^4$, so the vector $(p_{\text{on } i}, 0_{\text{elsewhere}})$ is a multiple of $(\varepsilon - 1)\lambda_b$ and so lies in $(\varepsilon - 1)\Lambda$. Thus clearly

$$\big(l(c_i)(\varepsilon - \varepsilon^{-1})\big) + \big(l(d_i)(\varepsilon - \varepsilon^{-1})\big) \equiv \big(l(c_i + d_i)(\varepsilon - \varepsilon^{-1})\big) \pmod{(\varepsilon - 1)\Lambda}.$$

Thus we have

$$\begin{aligned}\phi(\infty_f\infty_g) &= \phi(\infty_{fg}\infty_{[f,f,g]}^{(1/2)})\\ &= -l(1/128)\lambda_{\pi(fg)}\\ &= -l(1/128)\lambda_{\pi(f)} - l(1/128)\lambda_{\pi(g)}\\ &= \phi(\infty_f) + \phi(\infty_g)\end{aligned}$$

as required.

When $p = 3$, we find that

$$\begin{aligned}\phi(\infty_f) + \phi(\infty_g) &= \lambda_{\pi(f)} - \Psi(f)\lambda_b + \lambda_{\pi(g)} - \Psi(g)\lambda_b\\ &= (\varepsilon^{f_i} - \varepsilon^{-f_i}) + (\varepsilon^{g_i} - \varepsilon^{-g_i}) - \big(\Psi(f) + \Psi(g)\big)\lambda_b\\ &= (\varepsilon^{f_i} - \varepsilon^{-f_i} + \varepsilon^{g_i} - \varepsilon^{-g_i} - \varepsilon^{f_i+g_i} + \varepsilon^{-f_i-g_i})\\ &\quad + (\varepsilon^{f_i+g_i} - \varepsilon^{-f_i-g_i}) - \big(\Psi(f) + \Psi(g)\big)\lambda_b.\end{aligned}$$

Now by Lemma 2.10 we have

$$\begin{aligned}&\varepsilon^{f_i} - \varepsilon^{-f_i} + \varepsilon^{g_i} - \varepsilon^{-g_i} - \varepsilon^{f_i+g_i} + \varepsilon^{-f_i-g_i}\\ &\quad\equiv -f_ig_i(f_i+g_i)\big((\varepsilon-\varepsilon^{-1})(\varepsilon^2-\varepsilon^{-2})(\varepsilon^4-\varepsilon^{-4})\big) \pmod{(\varepsilon-1)^4}.\end{aligned}$$

Since $p = 3$, we have $u_i = u_i^{-1}$, so

$$\big((\varepsilon-\varepsilon^{-1})(\varepsilon^2-\varepsilon^{-2})(\varepsilon^4-\varepsilon^{-4})_{\text{on } i},\ 0_{\text{elsewhere}}\big) = u_i\lambda_b = u_i^{-1}\lambda_b,$$

and so we get

$$\begin{aligned}&(\varepsilon^{f_i} - \varepsilon^{-f_i} + \varepsilon^{g_i} - \varepsilon^{-g_i} - \varepsilon^{f_i+g_i} + \varepsilon^{-f_i-g_i}) + (\varepsilon^{f_i+g_i} - \varepsilon^{-f_i-g_i}) - \big(\Psi(f) + \Psi(g)\big)\lambda_b\\ &\quad= (\varepsilon^{f_i+g_i} - \varepsilon^{-f_i-g_i}) - \sum_{i=1}^{n} u_i^{-1}f_ig_i(f_i+g_i)\lambda_b - \big(\Psi(f) + \Psi(g)\big)\lambda_b\\ &\quad= \lambda_{\pi(fg)} - \Psi(fg)\lambda_b,\end{aligned}$$

and this is equal to $\phi(\infty_{fg})$. □

Next we show that ϕ is an isometry from $Q_\infty/Z(Q_\infty)$ to $\Lambda/(\varepsilon-1)\Lambda$. The form on $Q_\infty/Z(Q_\infty)$ is the alternating form given by the commutator map. Now Λ has a natural bilinear form given by $(v, w) = \sum_{i=1}^{n} v_i\overline{w_i}$, where $^-$ denotes complex conjugation.

Lemma 5.4. *The image of the bilinear form* $(\ ,\ )$ *is* $(\varepsilon-1)^3\mathbb{Z}[\varepsilon]$.

Proof. Obviously $(\lambda_b, \lambda_j) \in (\varepsilon-1)^3\mathbb{Z}[\varepsilon] \setminus (\varepsilon-1)^4\mathbb{Z}[\varepsilon]$, so the image of the form contains $(\varepsilon-1)^3\mathbb{Z}[\varepsilon]$. Now we want to show that (λ, μ) lies in $(\varepsilon-1)^3\mathbb{Z}[\varepsilon]$ for $\lambda, \mu \in \Lambda$. Suppose that $\lambda \in \Lambda^0$. Then by (5.1), we may write $\lambda = r\lambda_j + \lambda'$ for some $r \in \mathbb{Z}$ and $\lambda' \in \Lambda^i$ with $i \geq 1$. Then $(\lambda, \mu) = r(\lambda_j, \mu) + (\lambda', \mu)$. Now the definition of λ_j and (5.3) imply that $(\lambda_j, \mu) \in (\varepsilon-1)^3$, since $(\lambda_j, \mu) = \sum_{i=1}^{n} l(u_i)\overline{\mu_i} + pl(u_j\Psi(u))\overline{\mu_j} \equiv -mpl(\Psi(u)) + mpl(u_j^2)l(\Psi(u))$, where $\mu_i \equiv ml(u_i) \pmod{(\varepsilon-1)}$. (Recall that if $\Psi(u) \neq 0$, then $p = 3$, so $l(u_j)^2 = 1$.) Thus we need to show that $(\lambda', \mu) \in (\varepsilon-1)^3\mathbb{Z}[\varepsilon]$. We may write $\lambda' = \lambda_c + \lambda''$ with $\lambda'' \in \Lambda^i$ and $i \geq 2$. If $\mu \in \Lambda^0$, we may write $\mu = m\lambda_j + \mu'$ with $\mu' \in \Lambda^i$ and $i \geq 1$. Now $(\lambda', \mu) = (\lambda_c, m\lambda_j) + (\lambda_c, \mu') +$

$(\lambda'', m\lambda_j) + (\lambda'', \mu')$. Now by (2.4) and (5.3), $(\lambda_c, m\lambda_j)$ and $(\lambda'', m\lambda_j)$ are in $(\varepsilon - 1)^3\mathbb{Z}[\varepsilon]$. Since $\lambda'' \in \Lambda^i$ for $i \geq 2$ and $\mu' \in \Lambda^j$ for $j \geq 1$, it is clear that $(\lambda'', \mu') \in (\varepsilon - 1)^3\mathbb{Z}[\varepsilon]$. By (5.2), (λ_c, μ') lies in $(\varepsilon - 1)^3\mathbb{Z}[\varepsilon]$. This proves the lemma. □

Thus the induced form on $\Lambda/(\varepsilon - 1)\Lambda$ has values in $(\varepsilon - 1)^3\mathbb{Z}[\varepsilon]/(\varepsilon - 1)^4\mathbb{Z}[\varepsilon] \cong \mathbb{F}_p$. This form is alternating since $(w, v) = \overline{(v, w)}$ and

$$\overline{(\varepsilon - 1)}^3 \equiv (\varepsilon^{-1} - 1)^3 \equiv (1 - \varepsilon)^3 \pmod{(\varepsilon - 1)^4\mathbb{Z}[\varepsilon]},$$

and $(1 - \varepsilon)^3 = -(\varepsilon - 1)^3$.

Lemma 5.5. *The map ϕ is an isometry from $Q_\infty/Z(Q_\infty)$ to $\Lambda/(\varepsilon - 1)\Lambda$.*

Proof. We need to show that for $q, r \in Q_\infty$, we have

$$[q, r] = \infty_{\not\epsilon}^{(\phi(q), \phi(r))}$$

where $(\phi(q), \phi(r))$ is viewed as an element of $\mathbb{F}_p$ under some fixed map

$$(\varepsilon - 1)^3\mathbb{Z}[\varepsilon]/(\varepsilon - 1)^4\mathbb{Z}[\varepsilon] \longrightarrow \mathbb{F}_p.$$

Then we have 10 cases to consider: $\phi(q) \in \Lambda^i$ and $\phi(r) \in \Lambda^j$ for $0 \leq i \leq 3$ and $0 \leq j \leq i$.

First we do the cases where the form vanishes.

We have $(\lambda_b, v) \equiv 0$ unless $v \in \Lambda^0$, since obviously the value of the form here lies in $(\varepsilon - 1)^4\mathbb{Z}[\varepsilon]$. We also have $[0_{\not\epsilon}, 0_{\not\epsilon}] = [0_{\not\epsilon}, \delta] = [0_{\not\epsilon}, \infty_f] = 1 = \infty_{\not\epsilon}^0$, using (4.5) and (4.6).

As above we have $(\lambda_\delta, v) \equiv 0$ unless $v \in \Lambda^0$ or Λ^1. We also have that $(\lambda_\delta, \lambda_j) \equiv (\varepsilon - \varepsilon^{-1})(\varepsilon^2 - \varepsilon^{-2}) \sum_{i=1}^n l(\delta_i)l(u_i)$, and $\sum_{i=1}^n l(\delta_i)l(u_i) \in (\varepsilon - 1)^2$, so $(\lambda_\delta, \lambda_j) \equiv 0$. For the corresponding relations in Q_∞ we have $[\delta, \epsilon] = 1$ since δ and ϵ are elements of an abelian group, and $[\delta, x_t] = 1$ by (4.21).

We have

$$(\lambda_f, \lambda_g) \equiv -(\varepsilon - \varepsilon^{-1})^2 \sum_{i=1}^n l(f_i)l(g_i),$$

and $\sum_{i=1}^n l(f_i)l(g_i) \in (\varepsilon - 1)^2$, so $(\lambda_f, \lambda_g) = 0$. We also have that

$$(\lambda_f, \lambda_j) \equiv (\varepsilon - \varepsilon^{-1}) \sum_{i=1}^n l(f_i)l(u_i) + (\varepsilon - \varepsilon^{-1})pl(f_j)l(u_j\Psi(u)).$$

Now $\sum_{i=1}^n l(f_i)l(u_i) \in (\varepsilon - 1)^4$ if $p > 3$, so in that case we have $(\lambda_f, \lambda_j) \equiv 0$. If $p = 3$, then (λ_f, λ_j) may not always be 0, and we determine its value below along with the other nonzero values of the form. For the corresponding relations in Q_∞ we get $[\infty_f, \infty_g] = 1$ from (4.3), and when $p > 3$, $[\infty_f, x_t] = \infty_{\not\epsilon}^{-\partial(f)} = 1$ from (4.23), since ∂ is trivial if $p > 3$.

Finally, we have $(\lambda_j, \lambda_j) \equiv 0$ since the form on $\Lambda/(\varepsilon - 1)\Lambda$ is alternating. Thus the only possible pairs for which the form is nonzero are (λ_b, λ_j), $(\lambda_\delta, \lambda_f)$, and (λ_f, λ_j) when $p = 3$. If $p = 3$, then by (4.23), (4.6), and the

definition of x_j, we see that $[\infty_f, x_j] = \infty_{\not c}^{-f_j u_j \Psi(u)}$. We have

$$\begin{aligned}(\phi(\infty_f), \phi(x_j)) &= (\lambda_{\pi(f)}, \lambda_j) - l(\Psi(f))(\lambda_b, \lambda_j)\\ &= (\varepsilon - \varepsilon^{-1}) \sum_{i=1}^{n} l(f_i) l(u_i) + 3(\varepsilon - \varepsilon^{-1}) l(f_j) l(u_j) l(\Psi(u))\\ &\quad - l(\Psi(f))(\varepsilon - \varepsilon^{-1})(\varepsilon^2 - \varepsilon^{-2})(\varepsilon^4 - \varepsilon^{-4}).\end{aligned}$$

Now $\sum_{i=1}^{n} l(f_i) l(u_i) = \sum_{i=1}^{n} l(f_i)^3 l(u_i^{-1}) = 3l(\Psi(f))$, and $(\varepsilon - \varepsilon^{-1})(\varepsilon^2 - \varepsilon^{-2}) \cdot (\varepsilon^4 - \varepsilon^{-4}) = 3(\varepsilon - \varepsilon^{-1})$, so

$$\begin{aligned}&(\varepsilon - \varepsilon^{-1}) \sum_{i=1}^{n} l(f_i) l(u_i) + 3(\varepsilon - \varepsilon^{-1}) l(f_j) l(u_j) l(\Psi(u))\\ &\quad - l(\Psi(f))(\varepsilon - \varepsilon^{-1})(\varepsilon^2 - \varepsilon^{-2})(\varepsilon^4 - \varepsilon^{-4})\\ &= (\varepsilon - \varepsilon^{-1}) 3l(\Psi(f)) + 3(\varepsilon - \varepsilon^{-1}) l(f_j) l(u_j) l(\Psi(u)) - l(\Psi(f)) 3(\varepsilon - \varepsilon^{-1})\\ &= 3(\varepsilon - \varepsilon^{-1}) l(f_j) l(u_j) l(\Psi(u)).\end{aligned}$$

Thus we have

$$\begin{aligned}[\infty_f, x_j] &= \infty_{\not c}^{-f_j u_j \Psi(u)} \quad \text{and}\\ (\phi(\infty_f), \phi(x_j)) &\equiv (\varepsilon - 1)^3 l(f_j) l(u_j) l(\Psi(u)).\end{aligned} \tag{5.4}$$

For any $p \geq 3$ we have

$$(\lambda_b, \lambda_j) \equiv (\varepsilon - \varepsilon^{-1})(\varepsilon^2 - \varepsilon^{-2})(\varepsilon^4 - \varepsilon^{-4}) \equiv l(64)(\varepsilon - 1)^3, \quad \text{and}$$

$$(\lambda_\delta, \lambda_f) \equiv -(\varepsilon - \varepsilon^{-1})^2 (\varepsilon^2 - \varepsilon^{-2}) \sum_{i=1}^{n} l(\delta_i) l(f_i) \equiv -l(16)(\varepsilon - 1)^3 l(\delta(\pi(f))).$$

We also have $[0_{\not c}, x_j] = \infty_{\not c}$ by (4.23) and $[\delta, \infty_f] = \infty_{\not c}^{-\delta(\pi(f))}$ by (4.6). Thus by applying the definition of ϕ we have

$$\begin{aligned}[0_{\not c}, x_j] &= \infty_{\not c} \quad \text{and}\\ (\phi(0_{\not c}), \phi(x_j)) &= l(2^6) l(2^7) (\varepsilon - 1)^3,\end{aligned} \tag{5.5}$$

and also

$$\begin{aligned}[\delta, \infty_f] &= \infty_{\not c}^{-\delta(\pi(f))} \quad \text{and}\\ (\phi(\delta), \phi(\infty_f)) &= -l(2^4) l(2^9) (\varepsilon - 1)^3 l(\delta(\pi(f))).\end{aligned} \tag{5.6}$$

By looking at (5.4)–(5.6) we see that if we identify $\langle \infty_{\not c} \rangle$ with $\mathbb{F}_p$ by sending $\infty_{\not c}$ to $l(2^{13})(\varepsilon - 1)^3 \pmod{(\varepsilon - 1)^4 \mathbb{Z}[\varepsilon]}$, then ϕ is an isometry. □

The following series of lemmas will be used to compare the action of the matrices A_c on $\Lambda/(\varepsilon - 1)\Lambda$ with the action of the maps 0_f on $Q_\infty / Z(Q_\infty)$.

Lemma 5.6. $\lambda_\delta A_c \equiv \lambda_\delta + (1/8) l(\delta(c)) \lambda_b \pmod{(\varepsilon - 1)\Lambda}$.

Proof. We have

$$\begin{aligned}\lambda_\delta A_c &= (\varepsilon-\varepsilon^{-1})(\varepsilon^2-\varepsilon^{-2})(\varepsilon^{u_i^{-1}c_i}l(\delta_i))\\ &= \lambda_\delta + (\varepsilon-\varepsilon^{-1})(\varepsilon^2-\varepsilon^{-2})((\varepsilon^{u_i^{-1}c_i}-1)l(\delta_i)).\end{aligned}$$

By (2.3) $\varepsilon^{u_i^{-1}c_i}-1 \equiv l(u_i^{-1}c_i)(\varepsilon-1) \pmod{(\varepsilon-1)^2}$, so this is congruent to

$$\lambda_\delta + (\varepsilon-\varepsilon^{-1})(\varepsilon^2-\varepsilon^{-2})(l(u_i^{-1}c_i)(\varepsilon-1)l(\delta_i)).$$

Now

$$(l(u_i^{-1})(\varepsilon-\varepsilon^{-1})(\varepsilon^2-\varepsilon^{-2})(\varepsilon-1)_{\text{on } i},\ 0_{\text{elsewhere}}) \equiv l(1/8)\lambda_b \pmod{(\varepsilon-1)\Lambda}$$

since $\varepsilon-1 \equiv l(1/8)(\varepsilon^4-\varepsilon^{-4}) \pmod{\varepsilon-1}$. Thus

$$\lambda_\delta A_c \equiv \lambda_\delta + l(1/8)\sum_{i=1}^{n} l(\delta_i)l(c_i)\lambda_b \equiv \lambda_\delta + l(1/8)l(\delta(c))\lambda_b,$$

proving the Lemma. □

Lemma 5.7. $\lambda_d A_c = \lambda_d - l(1/8)\lambda_{c\cdot d} - l(1/128)(c, c, d)\lambda_b$.

Proof. We have $\lambda_d A_c = (\varepsilon^{u_i^{-1}c_i}l(d_i)(\varepsilon-\varepsilon^{-1})) = \lambda_d + ((\varepsilon^{u_i^{-1}c_i}-1)l(d_i)(\varepsilon-\varepsilon^{-1}))$. By (2.3) we may replace $\varepsilon^{u_i^{-1}c_i}-1$ with

$$l(u_i^{-1}c_i)(\varepsilon-1) + l(1/64)l(u_i^{-1}c_i(u_i^{-1}c_i-1))(\varepsilon^2-\varepsilon^{-2})(\varepsilon^4-\varepsilon^{-4}).$$

Doing this, we have

$$\begin{aligned}\lambda_d A_c = \lambda_d &+ (l(u_i^{-1}c_i d_i(\varepsilon-1)(\varepsilon-\varepsilon^{-1}))\\ &+ l(1/64)(l(u_i^{-1}c_i d_i)(u_i^{-1}c_i-1)(\varepsilon^2-\varepsilon^{-2})(\varepsilon^4-\varepsilon^{-4})(\varepsilon-\varepsilon^{-1})).\end{aligned}$$

Now $(l(u_i^{-1}c_i d_i)(\varepsilon-1)(\varepsilon-\varepsilon^{-1})) \equiv -l(1/8)\lambda_{c\cdot d}$, and

$$\begin{aligned}&l(1/64)(u_i^{-1}c_i d_i(u_i^{-1}c_i-1)(\varepsilon-\varepsilon^{-1})(\varepsilon^2-\varepsilon^{-2})(\varepsilon^4-\varepsilon^{-4}))\\ &\quad= l(1/64)(u_i^{-1}c_i d_i u_i^{-1}c_i(\varepsilon-\varepsilon^{-1})(\varepsilon^2-\varepsilon^{-2})(\varepsilon^4-\varepsilon^{-4}))\\ &\qquad- l(1/64)(u_i^{-1}c_i d_i(\varepsilon-\varepsilon^{-1})(\varepsilon^2-\varepsilon^{-2})(\varepsilon^4-\varepsilon^{-4}))\\ &\quad\equiv -l(1/128)\left(-2\sum_{i=1}^{n} u_i^{-1}c_i c_i d_i\right)\lambda_b + (\varepsilon^4-\varepsilon^{-4})l(1/128)\lambda_{c\cdot d}\\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (\text{mod } (\varepsilon-1)\Lambda).\end{aligned}$$

Thus we have $\lambda_d A_c \equiv \lambda_d - l(1/8)\lambda_{c\cdot d} - l(1/128)(c, c, d)\lambda_b$, which proves the lemma. □

Lemma 5.8. *If $p > 3$ we have*

$$\lambda_j A_c \equiv \lambda_j + (1/2)\lambda_c - l(1/32)\lambda_{c\cdot c} - l(1/256)l(\Psi(c))\lambda_b;$$

and if $p = 3$ we have

$$\lambda_j A_c \equiv \lambda_j - \lambda_c + \lambda_{c\cdot c} - l(u_j c_j \Psi(u))\lambda_b.$$

Proof. First suppose that $p > 3$, so we have $\Psi(u) = 0$ and $\lambda_j = \lambda_t$. We compute

$$\begin{aligned}
\lambda_t A_c &= (\varepsilon^{u_i^{-1}c_i} l(u_i)) \\
&= \lambda_t + ((\varepsilon^{u_i^{-1}c_i} - 1) l(u_i)) \\
&= \lambda_t + (\varepsilon^{u_i^{-1}c_i/2}(\varepsilon^{u_i^{-1}c_i/2} - \varepsilon^{-u_i^{-1}c_i/2}) l(u_i)) \\
&= \lambda_t + (\varepsilon^{u_i^{-1}c_i/2}(\varepsilon - \varepsilon^{-1}) l(u_i^{-1}c_i/2) l(u_i)) \\
&\quad + (\varepsilon^{u_i^{-1}c_i/2} l(u_i)(\varepsilon^{u_i^{-1}c_i/2} - l(u_i^{-1}c_i/2)\varepsilon + l(u_i^{-1}c_i/2)\varepsilon^{-1} - \varepsilon^{-u_i^{-1}c_i/2})) \\
&= \lambda_t + l(1/2)\lambda_c A_{(1/2)c} \\
&\quad + (\varepsilon^{u_i^{-1}c_i/2} l(u_i)(\varepsilon^{u_i^{-1}c_i/2} - l(u_i^{-1}c_i/2)\varepsilon + l(u_i^{-1}c_i/2)\varepsilon^{-1} - \varepsilon^{-u_i^{-1}c_i/2})).
\end{aligned}$$

Now by (2.2) we have that

$$\begin{aligned}
&\varepsilon^{u_i^{-1}c_i/2} - l(u_i^{-1}c_i/2)\varepsilon + l(u_i^{-1}c_i/2)\varepsilon^{-1} - \varepsilon^{-u_i^{-1}c_i/2} \\
&\quad \equiv -l(1/3) l(u_i^{-1}c_i/2)(1 - (u_i^{-1}c_i/2)^2)(\varepsilon - 1)^3 \pmod{(\varepsilon - 1)^4 \mathbb{Z}[\varepsilon]} \\
&\quad \equiv -l(1/3) l(u_i^{-1}c_i/2)(1 - (u_i^{-1}c_i/2)^2) l(1/64)(\varepsilon - \varepsilon^{-1})(\varepsilon^2 - \varepsilon^{-2})(\varepsilon^4 - \varepsilon^{-4}).
\end{aligned}$$

Thus we find that the vector

$$\begin{aligned}
&(\varepsilon^{u_i^{-1}c_i/2} l(u_i)(\varepsilon^{u_i^{-1}c_i/2} - l(u_i^{-1}c_i/2)\varepsilon + l(u_i^{-1}c_i/2)\varepsilon^{-1} - \varepsilon^{-u_i^{-1}c_i/2})) \\
&\quad \equiv -\sum_{i=1}^{n} l(u_i) l(1/3) l(c_i/2) l(1/64) \lambda_b \\
&\qquad + \sum_{i=1}^{n} l(u_i) l(1/3) l(c_i/2) l(u_i^{-2} c_i^2/4) l(1/64) \lambda_b \\
&\quad \equiv \sum_{i=1}^{n} l(1/8) l(1/64) l(1/3) l(u_i^{-1} c_i^3) \lambda_b \\
&\quad \equiv -l(1/1024) l(\Psi(c)) \lambda_b \pmod{(\varepsilon - 1)\Lambda}.
\end{aligned}$$

Since the previous lemma shows that

$$l(1/2)\lambda_c A_{(1/2)c} = l(1/2)\lambda_c - l(1/32)\lambda c \cdot c - l(1/1024)(c, c, c)\lambda_b,$$

and since $(c, c, c) = 3\Psi(c)$, we get

$$\begin{aligned}
\lambda_t A_c &= \lambda_t + (1/2)\lambda_c A_{(1/2)c} - l(1/1024)\Psi(c)\lambda_b \\
&= \lambda_t + (1/2)\lambda_c - l(1/32)\lambda c \cdot c - l(1/1024)((c, c, c) + \Psi(c))\lambda_b \\
&= \lambda_t + (1/2)\lambda_c - l(1/32)\lambda c \cdot c - l(1/256)(\Psi(c))\lambda_b.
\end{aligned}$$

This proves the result when $p > 3$.

If $p = 3$, then

$$\begin{aligned}\lambda_j A_c &= \lambda_j + (\varepsilon^{u_i^{-1}c_i} - 1)\lambda_j \\ &= \lambda_j + \big((\varepsilon^{u_i^{-1}c_i} - 1)l(u_i)\big) + \big((\varepsilon^{u_j^{-1}c_j} - 1)3l(u_j\Psi(u))_{\text{on } j}, 0_{\text{elsewhere}}\big) \\ &= \lambda_j + \big(\varepsilon^{u_i^{-1}c_i/2}(\varepsilon^{u_i^{-1}c_i/2} - \varepsilon^{-u_i^{-1}c_i/2})l(u_i)\big) \\ &\quad + \big(\varepsilon^{u_j^{-1}c_j/2}(\varepsilon^{u_j^{-1}c_j/2} - \varepsilon^{-u_j^{-1}c_j/2})3l(u_j\Psi(u))_{\text{on } j}, 0_{\text{elsewhere}}\big).\end{aligned}$$

Now from (2.2) we have

$$\varepsilon^{u_i^{-1}c_i/2} - l(u_i^{-1}c_i/2)\varepsilon + l(u_i^{-1}c_i/2)\varepsilon^{-1} - \varepsilon^{-u_i^{-1}c_i/2} = 0,$$

and since $p = 3$ we have $l(1/2) \equiv -1 \pmod 3$, so we may rewrite this expression as

$$\begin{aligned}&= \lambda_j + \big(\varepsilon^{-u_i^{-1}c_i}(l(-u_i^{-1}c_i)\varepsilon - l(-u_i^{-1}c_i)\varepsilon^{-1})l(u_i)\big) \\ &\quad + \big(\varepsilon^{-u_j^{-1}c_j}(\varepsilon^{-u_j^{-1}c_j} - \varepsilon^{u_j^{-1}c_j})3l(u_j\Psi(u))_{\text{on } j}, 0_{\text{elsewhere}}\big) \\ &\equiv \lambda_j + \big(\varepsilon^{-u_i^{-1}c_i}l(-c_i)(\varepsilon - \varepsilon^{-1})\big) \\ &\quad + \big(l(-u_jc_j)(\varepsilon - \varepsilon^{-1})3l(u_j\Psi(u))_{\text{on } j}, 0_{\text{elsewhere}}\big) \\ &\equiv \lambda_j + \lambda_{-c}A_{-c} - l(c_ju_j\Psi(u))\lambda_b.\end{aligned}$$

By Lemma 5.7 we have $\lambda_{-c}A_{-c} = \lambda_{-c} + \lambda_{c\cdot c}$ and it is clear that $\lambda_{-c} = -\lambda_c$, so we have

$$\lambda_j A_c = \lambda_j - \lambda_c + \lambda_{c\cdot c} - l(c_ju_j\Psi(u))\lambda_b$$

when $p = 3$. This finishes the proof. □

Now we need to restate some of the relations for elements of N.

Lemma 5.9. *The following relations hold in* N_∞:

$$\delta^{0_f} = \delta 0_{\not c}^{-\delta(\pi(f))}. \tag{5.7}$$

$$0_{\not c}^{0_f} = 0_{\not c}. \tag{5.8}$$

$$\infty_g^{0_f} = \infty_g \eta_{f,g}^2 \infty_{[f,g,g]}^{-1} 0_{[f,f,g]}^{-1}. \tag{5.9}$$

$$x_t^{0_f} = x_t 1_{\not c}^{\partial(\pi(f))} 2_{\psi_f} \infty_{[f,f,f]}^{-1} \infty_f^{-1} \eta_{f,f}^{-1}. \tag{5.10}$$

Proof. Equation (5.7) follows directly from (4.6), and (5.8) follows from (4.3).

For (5.9) we want to find $0_f^{-1}\infty_g 0_f$. By (4.3) we know that $i_f^{-1} = i_{f^{-1}}$. Then (4.5) implies that

$$\infty_{g^{-1}} 0_{f^{-1}} \infty_g 0_f = [\infty_{g^{-1}}, 0_{f^{-1}}] = \eta_{f,g}^2 \infty_{[f,g,g]}^{-1} 0_{[f,f,g]}^{-1}.$$

Thus $0_f^{-1}\infty_g 0_f = \infty_g \eta_{f,g}^2 \infty_{[f,g,g]}^{-1} 0_{[f,f,g]}^{-1}$.

For (5.10) we want to find $0_f^{-1} x_t 0_f$. We have $x_t^{-1} 0_f x_t = 1_f 1_{\not c}^{-\partial(\pi(f))}$ by (4.23), so we have $x_t^{-1} 0_f^{-1} x_t = 1_f^{-1} 1_{\not c}^{\partial(\pi(f))}$. Thus, $0_f^{-1} x_t 0_f = x_t 1_f^{-1} 1_{\not c}^{\partial(\pi(f))} 0_f$.

Now by (4.16) we have

$$1_f = \eta_{f,f}^{-1}\infty_f 0_f 2_{\psi_f^{-1}},$$

so

$$1_f^{-1} = 2_{\psi_f} 0_f^{-1}\infty_f^{-1}\eta_{f,f}.$$

Now we get

$$\begin{aligned}
1_f^{-1}0_f &= 2_{\psi_f}0_f^{-1}\infty_f^{-1}\eta_{f,f}0_f \\
&= 2_{\psi_f}0_f^{-1}\infty_f^{-1}0_f\eta_{f,f}0_{[f,f,f]}^{-1} \\
&= 2_{\psi_f}0_{[f,f,f]}\infty_{[f,f,f]}\eta_{f,f}^{-2}\infty_f^{-1}\eta_{f,f}0_{[f,f,f]}^{-1} \\
&= 2_{\psi_f}\infty_{[f,f,f]}^{-1}\infty_f^{-1}\eta_{f,f}^{-2}\eta_{f,f} \\
&= 2_{\psi_f}\infty_{[f,f,f]}^{-1}\infty_f^{-1}\eta_{f,f}^{-1}.
\end{aligned}$$

Thus we have

$$\begin{aligned}
0_f^{-1}x_t 0_f &= x_t 1_f^{-1} 1_{\not\in}^{\partial(\pi(f))}0_f \\
&= x_t 1_{\not\in}^{\partial(\pi(f))}2_{\psi_f}\infty_{[f,f,f]}^{-1}\infty_f^{-1}\eta_{f,f}^{-1},
\end{aligned}$$

which shows that (5.10) is true. □

Lemma 5.10. *The action of* 0_f *on* $Q_\infty/Z(Q_\infty)$ *is related to the action of* $A_{\pi(f)}$ *on* $\Lambda/(\varepsilon-1)\Lambda$ *by*

$$\phi(q^{0_f}) = \phi(q)A_{\pi(f)} \qquad \text{for } q \in A_\infty. \tag{5.11}$$

Proof. The map 0_f acts trivially on $0_{\not\in}$, and A_c acts trivially on $\lambda_b + (\varepsilon-1)\Lambda$, so

$$\phi(0_{\not\in}^{0_f}) = \phi(0_{\not\in})A_{\pi(f)}.$$

By (5.7) we have $\delta^{0_f} = \delta 0_{\not\in}^{-\delta(\pi(f))}$, so

$$\phi(\delta^{0_f}) = l(8)\lambda_\delta + \delta(\pi(f))\lambda_b.$$

Now $\phi(\delta) = l(8)\lambda_\delta$ and by Lemma 5.6 we have

$$l(8)\lambda_\delta A_{\pi(f)} = l(8)\lambda_\delta + \delta(\pi(f))\lambda_b,$$

so $\phi(\delta^{0_f}) = \phi(\delta)A_{\pi(f)}$.

By (5.9) we have $\infty_g^{0_f} = \infty_g\eta_{f,g}^2\infty_{[f,g,g]}^{-1}0_{[f,f,g]}^{-1}$, so

$$\phi(\infty_g^{0_f}) \equiv \begin{cases} -l(128)\lambda_{\pi(g)} + l(16)\lambda_{f,g} + (\pi(f),\pi(f),\pi(g))\lambda_b & \text{if } p>3, \\ \lambda_{\pi(g)} - \Psi(\pi(g))\lambda_b + \lambda_{f,g} + (\pi(f),\pi(f),\pi(g))\lambda_b & \text{if } p=3. \end{cases}$$

Now $\phi(\infty_g) \equiv -l(128)\lambda_{\pi(g)}$ if $p>3$ and $\phi(\infty_g) \equiv \lambda_{\pi(g)} - \Psi(\pi(g))\lambda_b$ if $p=3$. By Lemma 5.7, if $p>3$ we have

$$-128\lambda_{\pi(g)}A_{\pi(f)} \equiv -128\lambda_{\pi(g)} + 16\lambda_{f,g} + (\pi(f),\pi(f),\pi(g))\lambda_b$$

and if $p = 3$ we have

$$(\lambda_{\pi(g)} - \Psi(\pi(g))\lambda_b)A_{\pi(f)} \equiv \lambda_{\pi(g)} + \lambda_{f,g} + (\pi(f), \pi(f), \pi(g))\lambda_b - \Psi(\pi(g))\lambda_b.$$

Thus $\phi(\infty_g^{0_f}) = \phi(\infty_g)A_{\pi(f)}$.

By (5.10) we have $x_j^{0_f} = x_j 1_{\not\infty}^{u_j f_j \Psi(u)} 2_{\psi_f} \infty_{[f,f,f]}^{-1} \infty_f^{-1} \eta_{f,f}^{-1}$, so

$$\phi(x_j^{0_f}) = \begin{cases} l(256)\lambda_j + l(128)\lambda_{\pi(f)} - l(8)\lambda_{f,f} - l(\Psi(\pi(f)))\lambda_b & \text{if } p > 3, \\ \lambda_j - \lambda_{\pi(f)} + \lambda_{f,f} - l(u_j f_j \Psi(u))\lambda_b & \text{if } p = 3. \end{cases}$$

Now $\phi(x_j) = l(256)\lambda_j$, and by Lemma 5.7 we have

$$256\lambda_j A_{\pi(f)} \equiv 256\lambda_j + 128\lambda_{\pi(f)} - 8\lambda_{\pi(f)\cdot\pi(f)} - l(\Psi(\pi(f)))\lambda_b$$

when $p > 3$ and

$$\lambda_j A_{\pi(f)} \equiv \lambda_j - \lambda_{\pi(f)} + \lambda_{\pi(f)\cdot\pi(f)} - l(u_j f_j \Psi(u))\lambda_b$$

when $p = 3$. Thus $\phi(x_j^{0_f}) = \phi(x_j)A_{\pi(f)}$. The elements $0_{\not\infty}$, δ, ∞_f, and x_j generate Q_∞, and we have shown that (5.11) is true for these elements, so it must be true for all elements of Q_∞. □

Lemma 5.11. *Let $x_h \in N$ with $h = \left(\begin{smallmatrix} k & 0 \\ 0 & k \end{smallmatrix}\right)$, and let σ_k be the $\mathbb{Z}$-automorphism of Λ given by the ring automorphism $\varepsilon \mapsto \varepsilon^k$ of $\mathbb{Z}[\varepsilon]$. Then for $q \in Q_\infty$ we have $\phi(q^{x_h}) = \phi(q)\sigma_k$.*

Proof. From Lemma 4.16 we have

$$0_{\not\infty}^{x_h} = 0_{\not\infty}^{k^3}, \quad \delta^{x_h} = \delta^{k^2}, \quad \infty_f^{x_h} = \infty_{f^{\kappa(k^2)}}^{k}, \quad \text{and} \quad x_t^{x_h} = x_t.$$

Now suppose that $\lambda \equiv (\varepsilon - 1)^j(l(w_i))$ for some $w \in \mathbb{F}_p^n$. Then

$$\lambda\sigma_k \equiv (\varepsilon^k - 1)^j(l(w_i)) \equiv k^j(\varepsilon - 1)^j\lambda \pmod{(\varepsilon - 1)\Lambda}.$$

The vectors λ_b, λ_δ, λ_c, and λ_j are all of this form, with $j = 3, 2, 1$, and 0 respectively. Thus we have

$$\lambda_b\sigma_k \equiv k^3\lambda_b, \quad \lambda_\delta\sigma_k \equiv k^2\lambda_\delta, \quad \lambda_c\sigma_k \equiv k\lambda_c, \quad \text{and} \quad \lambda_t\sigma_k \equiv \lambda_t.$$

Now comparing the action of σ_k on $\phi(q)$ with $\phi(q^{x_h})$ we see that $\phi(q^{x_h}) = \phi(q)\sigma_k$. □

Lemma 5.12. *Let $x_h \in N$ with $h = \left(\begin{smallmatrix} 1 & 0 \\ 0 & b \end{smallmatrix}\right)$. Then for $q \in Q_\infty$ we have $\phi(q^{x_h}) \equiv l(b)\phi(q)$.*

Proof. From Lemma 4.16 we have

$$0_{\not\infty}^{x_h} = 0_{\not\infty}^{b}, \quad \delta^{x_h} = \delta^{b}, \quad \infty_f^{x_h} = \infty_{f^{\kappa(b)}}^{b}, \quad \text{and} \quad x_t^{x_h} = x_t^{b}.$$

This proves the lemma. □

Lemma 5.13. *Let $\alpha \in S$. Then for $q \in Q_\infty$ we have $\phi(q^\alpha) \equiv \phi(q)l(\alpha)$.*

Proof. From (4.5) we have $0_{\not\infty}^{\alpha} = 0_{\not\infty}$ and $\infty_f^{\alpha} = \infty_{f^{\alpha(b)}}$. Since α fixes u, we have $\lambda_b l(\alpha) = \lambda_b$. Thus $\phi(0_{\not\infty}^{\alpha}) \equiv \phi(0_{\not\infty})l(\alpha)$. It is clear that $\lambda_\delta l(\alpha) = \lambda_{\delta^\alpha}$,

so $\phi(\delta^\alpha) \equiv l(1/8)\lambda_{\delta^\alpha} \equiv l(1/8)\lambda_\delta l(\alpha)$. It is also clear that $\lambda_c l(\alpha) = \lambda_{c^\alpha}$, so $\phi(\infty_f^\alpha) \equiv -l(1/128)\lambda_{f^\alpha} \equiv -l(1/128)\lambda_f l(\alpha)$ if $p > 3$. If $p = 3$, then $\phi(\infty_f^\alpha) \equiv \lambda_{f^\alpha} - \Psi(\pi(f^\alpha))\lambda_b \equiv \lambda_f l(\alpha) - \Psi(\pi(f))\lambda_b$. Finally, since α fixes u, we have $x_j^\alpha = x_{j^\alpha}$ and $\lambda_j l(\alpha) = \lambda_{j^\alpha}$. This proves the lemma. □

Definition 5.6. Let $M_\infty = \langle Q_\infty, 0_f, S, x_h \mid f \in L, h = \left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right), h = \left(\begin{smallmatrix}k & 0\\ 0 & k\end{smallmatrix}\right)\rangle$.

Theorem 5.14. *$\overline{M_\infty}/\overline{Q_\infty} \cong \overline{M}^*(\Lambda)$, and the map ϕ is an isomorphism of $\overline{M_\infty}/\overline{Q_\infty}$ modules.*

Proof. First, define $F : M_\infty/Q_\infty \to M^*(\Lambda)$ by

$$F(x_h) = \operatorname{diag}(-1^n) \quad \text{for } h = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},$$

$$F(0_f) = A_{\pi(f)},$$

$$F(\alpha) = l(\alpha),$$

$$F(x_h) = \sigma_k \quad \text{for } h = \begin{pmatrix}k & 0\\ 0 & k\end{pmatrix}.$$

Now Lemmas 5.10, 5.11, 5.12, and 5.13 imply that for $q \in Q_\infty$ and $g \in \langle x_h, 0_f, x_h\rangle$ we have

$$\phi(q^g) = \phi(q)F(g). \tag{5.12}$$

This shows that the quotients of M_∞/Q_∞ and $M^*(\Lambda)$ by the kernel of the action on $Q_\infty/Z(Q_\infty)$ and $\Lambda/(\varepsilon - 1)\Lambda$, respectively, are isomorphic. The kernel of the action of M_∞/Q_∞ on $Q_\infty/Z(Q_\infty)$ is $\langle 0_\$\rangle\langle Q_\infty\rangle$, and the kernel of the action of $M^*(\Lambda)$ on $\Lambda/(\varepsilon - 1)\Lambda$ is $\langle \operatorname{diag}(\varepsilon^n)\rangle$. Thus $\overline{M_\infty}/\overline{Q_\infty} \cong \overline{M}^*(\Lambda)$, and it is clear from (5.12) that ϕ is an isomorphism of $\overline{M_\infty}/\overline{Q_\infty}$ modules. □

Let x_{-1} denote the element of X that corresponds to the element of $GL(2, p)$ with matrix $\left(\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right)$. It follows from (4.2) that all twisting maps for x_{-1} are trivial. Thus x_{-1} has the same action on standard luples as the map $e_{-1} : L \to L$, which is a loop automorphism. (See Lemma 3.2 and Definition 3.10.)

Examples. We use $\operatorname{Aut}^*_{\mathbb{Z}[\varepsilon]}(\Lambda)$ to denote the group of semilinear automorphisms of Λ, that is, the group generated by $\operatorname{Aut}_{\mathbb{Z}[\varepsilon]}(\Lambda)$ and the ring automorphisms σ_k.

Definition 5.7. Let $\operatorname{Mon}(\Lambda)$ be the set of monomial matrices in $\operatorname{Aut}_{\mathbb{Z}[\varepsilon]}(\Lambda)$, and let $\operatorname{Mon}^*(\Lambda)$ be the group $\langle \operatorname{Mon}(\Lambda), \sigma_k \mid k \in \mathbb{F}_p^\times\rangle$. Also let $\overline{\operatorname{Mon}}(\Lambda) = \operatorname{Mon}(\Lambda)/\langle A_u\rangle$ and $\overline{\operatorname{Mon}}^*(\Lambda) = \operatorname{Mon}^*(\Lambda)/\langle A_u\rangle$.

When C is the ternary Golay code, the pentacode, or the heptacode, we show that $\overline{N_\infty}/\overline{Q_\infty}$ is isomorphic to $\overline{\operatorname{Mon}}^*(\Lambda)$. Theorem 5.14 shows this is true for the respective subgroups $\overline{M_\infty}/\overline{Q_\infty}$ and $\overline{M}^*(\Lambda)$, and these groups have shape $2 \times \overline{C}:S:(p-1)$. Now in Theorem 4.17 we showed that $\overline{N_\infty}/\overline{Q_\infty} \cong (p-1) \times \overline{C}:S:(p-1)$. Thus we need to show that there exists a subgroup of $\operatorname{Mon}^*(\Lambda)$ of order $p-1$ which commutes with $M^*(\Lambda)$ and that this subgroup along with $M^*(\Lambda)$ generates $\operatorname{Mon}^*(\Lambda)$.

Theorem 5.15. *Let C be the ternary Golay code. Then $\overline{N_\infty}/\overline{Q_\infty}$ is isomorphic to $\overline{\mathrm{Mon}}^*(\Lambda)$.*

Proof. Theorem 5.14 shows that $\overline{N_\infty}/\overline{Q_\infty} \leq \overline{M}^*(\Lambda)$, since in this case $p-1=2$ and $M_\infty = N_\infty$. By [16], $\mathrm{Aut}^*_{\mathbb{Z}[\varepsilon]}(\Lambda)$ is a group of shape $6Suz:2$. The intersection of $M^*(\Lambda)$ with $6Suz:2$ is a group of shape $2\times 3^6 M_{11}$, and by [24] this is a maximal subgroup of $6Suz:2$. Then it follows from [16] that $M^*(\Lambda) = \mathrm{Mon}^*(\Lambda)$, so we have $\overline{N_\infty}/\overline{Q_\infty} \cong \overline{\mathrm{Mon}}^*(\Lambda)$. □

We call the elements of $S_u < \mathrm{Aut}(C)$ which act as a scalar on $\overline{C}$ *disappearing automorphisms.* When C is the pentacode or the heptacode, it turns out that there are elements x_h which have the same matrices in their action on $\Lambda/(\varepsilon-1)\Lambda$ as disappearing automorphisms of C have in their action on $\mathbb{F}_p^n$. Thus the elements x_h can be viewed as "reappearing" automorphisms. Now both the pentacode and the heptacode have disappearing automorphisms, but only the heptacode has disappearing automorphisms which are permutations. All elements of S_u give rise to loop automorphisms, but if α acts nontrivially on $\langle u\rangle$, it may not be the case that the action of α on $Q_\infty/Z(Q_\infty)$ is the same as the action of $l(\alpha)$ on $\Lambda/(\varepsilon-1)\Lambda$. This motivates the definition of the following subgroups, which we eventually show are subgroups of the Monster.

Definition 5.8. Let N_3 be the group N/K which results from the construction of §4 when C is the ternary Golay code, and let N_5 be the group N/K when C is the pentacode. When C is the heptacode, let $\widehat{N_7}$ be the subgroup of N of index 3 gotten by omitting the elements of S from the set of generators, and let $N_7 = \widehat{N_7}/K$.

As it turns out, we could also have taken $\widehat{N_7}$ to be the subgroup of N gotten by omitting the generators x_h for $h \in O_3(GL(2,7))$.

Lemma 5.16. *Let C be the pentacode, and let $\Lambda = \Lambda(C)$. Let $x_h \in N_5$ where $h = \left(\begin{smallmatrix}-1 & 0\\ 0 & 2\end{smallmatrix}\right) \in \mathrm{Aut}(V)$, and let B be the automorphism of Λ with matrix $\left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right) \oplus \left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right) \oplus \left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right)$. Then for $q \in Q_\infty$ we have $\phi(q^{x_h}) = \phi(q)B$.*

Proof. First, we remark that x_h is twisted by the map $\kappa(-2):(a,c)\mapsto(-2a,c)$ since $\det(h) = -2$. Then from Lemma 4.16 we find that

$$0_{\not\infty}^{x_h} = 0_{\not\infty}^2, \quad \delta^{x_h} = \delta^{-2}, \quad \infty_f^{x_h} = \infty_{f^{\kappa(-2)}}^2, \qquad \text{and} \qquad x_t^{x_h} = x_t^{-2}.$$

Now we determine the action of B on the elements of Λ. If we take

$$((\varepsilon-\varepsilon^{-1})(\varepsilon^2-\varepsilon^{-2})(\varepsilon^4-\varepsilon^{-4}),0,0,0,0,0)$$

as a representative of λ_b, then we see that we may take

$$(0,(\varepsilon-\varepsilon^{-1})(\varepsilon^2-\varepsilon^{-2})(\varepsilon^4-\varepsilon^{-4}),0,0,0,0)$$

as a representative for $\lambda_b B$. Now λ_b also has

$$(0,-2(\varepsilon-\varepsilon^{-1})(\varepsilon^2-\varepsilon^{-2})(\varepsilon^4-\varepsilon^{-4}),0,0,0,0)$$

as a representative, so we see that $\lambda_b B \equiv 2\lambda_b$. Now any vector of the form λ_δ is congruent to a vector in the span of

$$\lambda_{1,3} = (\varepsilon - \varepsilon^{-1})(\varepsilon^2 - \varepsilon^{-2})(1, 0, -1, 0, 0, 0) \quad \text{and}$$
$$\lambda_{1,5} = (\varepsilon - \varepsilon^{-1})(\varepsilon^2 - \varepsilon^{-2})(1, 0, 0, 0, -1, 0).$$

We compute that $\lambda_{1,3}B$ has as a representative the vector

$$(\varepsilon - \varepsilon^{-1})(\varepsilon^2 - \varepsilon^{-2})(0, 1, 0, -1, 0, 0);$$

and since $(2, 1, -2, -1, 0, 0) \in C$, we see that $\lambda_{1,3}B$ is also represented by

$$-2\lambda_{1,3} = (\varepsilon - \varepsilon^{-1})(\varepsilon^2 - \varepsilon^{-2})(-2, 0, 2, 0, 0, 0).$$

A similar calculation holds for $\lambda_{1,5}$, so we see that $\lambda_\delta B \equiv -2\lambda_\delta$. Any vector of the form λ_c is congruent to a vector in the span of

$$\lambda_a = ((\varepsilon - \varepsilon^{-1}), -2(\varepsilon - \varepsilon^{-1}), -(\varepsilon - \varepsilon^{-1}), 2(\varepsilon - \varepsilon^{-1}), 0, 0) \quad \text{and}$$
$$\lambda_d = ((\varepsilon - \varepsilon^{-1}), -2(\varepsilon - \varepsilon^{-1}), 0, 0, -(\varepsilon - \varepsilon^{-1}), 2(\varepsilon - \varepsilon^{-1})).$$

We compute that $\lambda_a B$ has as a representative the vector

$$(2(\varepsilon - \varepsilon^{-1}), (\varepsilon - \varepsilon^{-1}), -2(\varepsilon - \varepsilon^{-1}), -(\varepsilon - \varepsilon^{-1}), 0, 0)$$

and this is the vector $2\lambda_a$. A similar calculation holds for λ_d, so we see that $\lambda_c B \equiv 2\lambda_c$. We have $\lambda_t = (1, 2, 1, 2, 1, 2)$, and we see that

$$\lambda_t B = (-2, 1, -2, 1, -2, 1) \equiv -2\lambda_b.$$

Now comparing the action of B on $\phi(q)$ with $\phi(q^{x_h})$ we see that the Lemma is true. □

Theorem 5.17. *When $C = \mathscr{F}$, the group $\overline{N_\infty}/\overline{Q_\infty}$ is isomorphic to $\overline{\mathrm{Mon}}^*(\Lambda)$.*

Proof. By Theorem 5.14 and Lemma 5.16, $\overline{N_\infty}/\overline{Q_\infty}$ is isomorphic to the image in $\overline{\mathrm{Mon}}^*(\Lambda)$ of the subgroup $\langle M^*(\Lambda), B\rangle$ of $\mathrm{Aut}^*_{\mathbb{Z}[\varepsilon]}(\Lambda)$. By [17], $\mathrm{Aut}^*_{\mathbb{Z}[\varepsilon]}(\Lambda)$ is a group of shape $(5 \times 2HJ){:}4$. The intersection of the group $\langle M^*(\Lambda), B\rangle$ with the subgroup $2HJ < \mathrm{Aut}_{\mathbb{Z}[\varepsilon]}(\Lambda)$ is a group of shape $5^2{:}(4 \times S_3)$, and by [6] this is a maximal subgroup of $2HJ$. Since $\langle M^*(\Lambda), B\rangle$ also contains the scalar $\mathrm{diag}(\varepsilon^6)$ and the ring automorphism $\varepsilon \mapsto \varepsilon^2$, $\langle M^*(\Lambda), B\rangle$ is maximal in $\mathrm{Aut}^*_{\mathbb{Z}[\varepsilon]}(\Lambda)$. Now by [17], $\mathrm{Aut}^*_{\mathbb{Z}[\varepsilon]}(\Lambda)$ contains elements which are not monomial, so $\langle M^*(\Lambda), B\rangle = \mathrm{Mon}^*(\Lambda)$. Thus $\overline{N_\infty}/\overline{Q_\infty} \cong \overline{\mathrm{Mon}}^*(\Lambda)$. □

Lemma 5.18. *Let C be the heptacode, and let $\Lambda = \Lambda(C)$. Let $x_h \in N_7$ where $h = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right) \in \mathrm{Aut}(V)$, and let B be the automorphism of Λ with matrix*

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Then for $q \in Q_\infty$ we have $\phi(q^{x_h}) = \phi(q)B$.

Proof. In this case, x_h is twisted by the map $\kappa : (a, c) \mapsto (4a, c)$ since $\det(h) = 4$. Then we find that

$$0_{\not\phi}^{x_h} = 0_{\not\phi}, \quad \delta^{x_h} = \delta^4, \quad \infty_f^{x_h} = \infty_{f\kappa}^2, \qquad \text{and} \quad x_t^{x_h} = x_t.$$

Now we determine the action of B on the elements of Λ. If we take

$$((\varepsilon - \varepsilon^{-1})(\varepsilon^2 - \varepsilon^{-2})(\varepsilon^4 - \varepsilon^{-4}), 0, 0, 0)$$

as a representative of λ_b, it is obvious that $\lambda_b B = \lambda_b$. Any vector of the form λ_δ is in the span of

$$\lambda_{2,3} = (\varepsilon - \varepsilon^{-1})(\varepsilon^2 - \varepsilon^{-2})(0, 1, -1, 0).$$

We compute that $\lambda_{2,3}B$ has as a representative the vector

$$(\varepsilon - \varepsilon^{-1})(\varepsilon^2 - \varepsilon^{-2})(0, -1, 0, 1);$$

and since

$$(0, -1, 0, 1) - (0, 4, -4, 0) = (0, 2, 4, 1) \in C,$$

we see that $\lambda_{2,3}B$ is also represented by

$$4\lambda_{2,3} = (\varepsilon - \varepsilon^{-1})(\varepsilon^2 - \varepsilon^{-2})(0, 4, -4, 0).$$

Thus $\lambda_\delta B \equiv 4\lambda_\delta$. Any vector of the form λ_c is in the span of the vector

$$\lambda_a = (\varepsilon - \varepsilon^{-1})(0, 1, 2, 4).$$

We compute that $\lambda_a B$ has as a representative the vector

$$(\varepsilon - \varepsilon^{-1})(0, 2, 4, 1),$$

and this is the vector $2\lambda_a$. We have $\lambda_t = (5, 1, 1, 1)$, and clearly

$$\lambda_t B = (5, 1, 1, 1) = \lambda_t.$$

Now comparing the action of B on $\phi(q)$ with $\phi(q^{x_h})$ we see that the Lemma is true. □

The next lemma determines $\mathrm{Aut}^*_{\mathbb{Z}[\varepsilon]}(\Lambda)$ when C is the heptacode.

Theorem 5.19. *If C is the heptacode,* $\mathrm{Aut}^*_{\mathbb{Z}[\varepsilon]}(\Lambda) \cong 7 \times 3 \times 2S_7$.

Proof. Let $s = \varepsilon + \varepsilon^2 + \varepsilon^4$, let $n = \varepsilon^3 + \varepsilon^5 + \varepsilon^6$, and let $\Theta = s - n$. We remark that $\Theta \in (\varepsilon - 1)^3$. Lemma 5.2 and the definition of $l(B)$ for $B \in \mathrm{Aut}(\mathscr{H})$ show that the matrices B from Lemma 5.18 and $C = \mathrm{diag}(1, \varepsilon, \varepsilon^2, \varepsilon^4)$ are contained in $\mathrm{Aut}_{\mathbb{Z}[\varepsilon]}(\Lambda)$. Next we check that the matrix

$$A = \frac{1}{\Theta}\begin{pmatrix} -s^2 & 1 & 1 & 1 \\ 1 & n & s & s \\ 1 & s & n & s \\ 1 & s & s & n \end{pmatrix}$$

is in $\mathrm{Aut}_{\mathbb{Z}[\varepsilon]}(\Lambda)$ by checking that Av satisfies (5.1)–(5.3). We will use the substitution $s^2 = s + 2n$ a number of times.

First we check that vA satisfies (5.1). We suppose that

$$v_1 \equiv -2m \pmod{(\varepsilon - 1)} \quad \text{and} \quad v_i \equiv m \pmod{(\varepsilon - 1)}$$

for $i = 2, 3, 4$. We also assume that $\sum_{i=1}^{4} l(u_i)v_i \equiv k\Theta \pmod{(\varepsilon - 1)^4}$. We first see that

$$\begin{aligned}(vA)_1 &= (1/\Theta)(-s^2v_1 + v_2 + v_3 + v_4)\\ &= (1/\Theta)\big((-2v_1 + v_2 + v_3 + v_4) + (2 - s - 2n)v_1\big)\\ &= (1/\Theta)\big((-2v_1 + v_2 + v_3 + v_4) - (3s + 4n)v_1\big)\\ &= (1/\Theta)\big((-2v_1 + v_2 + v_3 + v_4) - (3\Theta + 7n)v_1\big)\\ &\equiv k - m \pmod{(\varepsilon - 1)}.\end{aligned}$$

We also have

$$\begin{aligned}(vA)_2 &= (1/\Theta)(v_1 + nv_2 + sv_3 + sv_4)\\ &= (1/\Theta)\big((v_1 + 3v_2 + 3v_3 + 3v_4) + (n - 3)v_2 + (s - 3)v_2 + (s - 3)v_2\big).\end{aligned}$$

Now $n - 3 = 4n + 3s = 3\Theta + 7n$ and $s - 3 = 4s + 3n = -3\Theta + 7s$, so we can rewrite this expression as

$$\begin{aligned}&(1/\Theta)\big((v_1 + 3v_2 + 3v_3 + 3v_4) + 3\Theta(v_2 - v_3 - v_4) + 7(nv_2 + sv_3 + sv_4)\big)\\ &\quad \equiv 3k - 3m \pmod{(\varepsilon - 1)}.\end{aligned}$$

Similarly, we find that $(vA)_3 \equiv (vA)_4 \equiv 3k - 3m \pmod{(\varepsilon - 1)}$. This shows that vA satisfies (5.1).

To see that vA satisfies (5.3) we need to check that

$$-2(vA)_1 + (vA)_2 + (vA)_3 + (vA)_4 \in (\varepsilon - 1)^3.$$

Now we expand this to get

$$\begin{aligned}&-2(vA)_1 + (vA)_2 + (vA)_3 + (vA)_4\\ &\quad = (1/\Theta)(-2(-s^2v_1 + v_2 + v_3 + v_4) + (v_1 + nv_2 + sv_3 + sv_4)\\ &\qquad\qquad + (v_1 + sv_2 + nv_3 + sv_4) + (v_1 + sv_2 + sv_3 + nv_4))\\ &\quad = (1/\Theta)((2s + 4n + 3)v_1 + (2s + n - 2)v_2\\ &\qquad\qquad + (2s + n - 2)v_3 + (2s + n - 2)v_4)\\ &\quad = (1/\Theta)(-\Theta v_1 + (-3\Theta + 7s)(v_2 + v_3 + v_4)\\ &\quad = -v_1 - 3v_2 - 3v_3 - 3v_4 - \Theta(v_2 + v_3 + v_4).\end{aligned}$$

The last expression is in $(\varepsilon - 1)^3$, as $-v_1 - 3v_2 - 3v_3 - 3v_4$ is in $(\varepsilon - 1)^3$ by (5.3) since $v \in \Lambda$.

Finally, to show that vA satisfies (5.2) we need only check that $(vA)_2 + 2(vA)_3 + 4(vA)_4$ is in $(\varepsilon - 1)^2$. Now we have

$$\begin{aligned}
&(vA)_2 + 2(vA)_3 + 4(vA)_4 \\
&\quad = (1/\Theta)((v_1 + nv_2 + sv_3 + sv_4) \\
&\qquad\qquad + 2(v_1 + sv_2 + nv_3 + sv_4) + 4(v_1 + sv_2 + sv_3 + nv_4)) \\
&\quad = (1/\Theta)(7v_1 + (n + 6s)v_2 + (2n + 5s)v_3 + (4n + 3s)v_4) \\
&\quad \equiv (1/\Theta)(n - s)(v_2 + 2v_3 + 4v_4) \pmod{(\varepsilon - 1)^2} \\
&\quad \equiv -v_2 - 2v_3 - 4v_4 \equiv 0 \pmod{(\varepsilon - 1)^2}
\end{aligned}$$

since $v \in \Lambda$ satisfies (5.2). Thus vA satisfies (5.1)–(5.3) and so is in $\mathrm{Aut}_{\mathbb{Z}[\varepsilon]}(\Lambda)$.

Now by Lemma 2.11, A, B, and C generate a group isomorphic to $2A_7$, and the image of this group in $PSL(4, \mathbb{C})$ is a maximal finite subgroup of $PSL(4, \mathbb{C})$. We just showed that A, B, and C are in $\mathrm{Aut}_{\mathbb{Z}[\varepsilon]}(\Lambda)$, and obviously $\mathrm{Aut}_{\mathbb{Z}[\varepsilon]}(\Lambda)$ contains the scalars, so $\mathrm{Aut}_{\mathbb{Z}[\varepsilon]}(\Lambda) \cong 7 \times 2A_7$. Now the automorphism σ_{-1} normalizes the cyclic group generated by each of these matrices. Furthermore, since $D^{\sigma_{-1}} = D^{-1}$ and no element of $2A_7$ inverts D, we have $\langle 2A_7, \sigma_{-1}\rangle \cong 2S_7$. Now Lemma 5.18 implies that σ_2 has exactly the same action on Λ as B, so $\sigma_4 B$ has order 3, acts trivially on Λ, and commutes with $2S_7$. Thus $\mathrm{Aut}^*_{\mathbb{Z}[\varepsilon]}(\Lambda) \cong 7 \times 3 \times 2S_7$. □

Theorem 5.20. *When $C = \mathscr{H}$, the group $\overline{N_\infty}/\overline{Q_\infty}$ is isomorphic to $\overline{\mathrm{Mon}}^*(\Lambda)$.*

Proof. By Theorem 5.14 and Lemma 5.18, $\overline{M_\infty}/\overline{Q_\infty}$ is isomorphic to the subgroup $\overline{M}^*(\Lambda) = \langle \mathrm{diag}(-1^4), C, \sigma_3\rangle$ of $\overline{\mathrm{Mon}}^*(\Lambda)$. These groups both have shape $2 \times 7 : 6$. Furthermore, from Lemma 5.18 we find that $\sigma_4 B$ commutes with $\overline{M}^*(\Lambda)$, and from Lemma 4.16 the element x_h commutes with $\overline{M_\infty}/\overline{Q_\infty}$ for $h = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$. Since $\sigma_4 B$ and x_h both have order 3, this proves that $\overline{N_\infty}/\overline{Q_\infty} = \langle \overline{M_\infty}, x_h\rangle/\overline{Q_\infty} \cong \langle \mathrm{diag}(-1^4), B, C, \sigma_3\rangle$. Now $\langle \mathrm{diag}(-1^4), B, C\rangle$ is a maximal subgroup of $2A_7$, since it is the normalizer of an element of order 7. Since $\mathrm{Aut}_{\mathbb{Z}[\varepsilon]}(\Lambda)$ contains the element A which is not monomial, we find that $\mathrm{Mon}(\Lambda) = \langle \mathrm{diag}(\varepsilon^4), \mathrm{diag}(-1^4), B, C, \rangle$. Hence $\mathrm{Mon}^*(\Lambda) = \langle \mathrm{diag}(\varepsilon^4), \mathrm{diag}(-1^4), B, C, \sigma_3\rangle$ and so we find that $\overline{N_\infty}/\overline{Q_\infty} \cong \overline{\mathrm{Mon}}^*(\Lambda)$. □

If C is the ternary Golay code or the pentacode, then Theorem 5.14 and Lemma 5.16 show that $\overline{N_\infty}/\overline{Q_\infty}$ acts on $Q_\infty/Z(Q_\infty)$ as $\overline{\mathrm{Mon}}^*(\Lambda)$ acts on $\Lambda/(\varepsilon - 1)\Lambda$, and that ϕ may be viewed as an isomorphism of $\overline{N_\infty}/\overline{Q_\infty}$ modules. This is not true when C is the heptacode. In that case, the element $\sigma_4 B$ acts trivially on $\Lambda/(\varepsilon - 1)\Lambda$, while x_h with $h = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ acts as the scalar $\mathrm{diag}(2^4)$ on $Q_\infty/Z(Q_\infty)$. If we replace Λ by $(\varepsilon - \varepsilon^{-1})(\varepsilon^2 - \varepsilon^{-2})\Lambda$, then $\sigma_4 B$ acts on $\Lambda/(\varepsilon - 1)\Lambda$ as the scalar $\mathrm{diag}(2^4)$, and the corresponding map ϕ is an isomorphism of $\overline{N_\infty}/\overline{Q_\infty}$ modules.

6. Representations of N_∞

The goal of this section is to show that the subgroup $\overline{N}_\infty$ of N_3 is a subgroup of the Monster. The subtlety involved in this is indicated by the fact that it turns out that the subgroup of the Monster of shape $3^{1+12} \cdot 2Suz$ is a

twisted holomorph, and there are two nonisomorphic twisted holomorphs of shape $3^{1+12} \cdot 2Suz$ as described in the discussion following Lemma 2.7. We define some representations of N_∞ by giving their bases in terms of sets of lu-ples. Then we use these representations to determine the trace of an element of N_∞ on the Monster algebra, under the assumptions that the Monster contains a particular twisted holomorph and the character table of the Monster algebra is as printed in [4]. This will show that one of the twisted holomorphs cannot be contained in the Monster and that $\overline{N}_\infty$ is contained in the other twisted holomorph.

The natural module for $6Suz$. Throughout this discussion we assume that N_∞ is the group given by Definition 4.8 when C is the ternary Golay code. We begin our discussion of the representations of N_∞ by defining certain objects permuted by N_∞. Let $\omega = e^{2\pi i/3}$, and let $\bar{\omega} = e^{-2\pi i/3}$. We first want to define objects permuted by N_∞ such that the $\mathbb{Q}[\omega]$-permutation module that they span has the natural 12-dimensional modules for $6Suz$ as submodules. By this we mean that the image of N_∞ acting on each 12-dimensional submodule is the monomial subgroup $2 \times 3^6{:}M_{11}$ of $\mathrm{Aut}_{\mathbb{Z}[\omega]}(\Lambda_{\mathbb{C}}) \cong 6Suz$.

Definition 6.1. For $1 \le i \le n$ and $j \in \{\infty\} \cup \mathbb{F}_p$, we define $v_{i,j}^{\sigma,\tau}$ for $\sigma \in \mathbb{F}_3$ and $\tau = \pm 1$ by

$$v_{i,\infty}^{\sigma,\tau} = \{\theta \in \mathscr{L} \mid \theta(y) = d\phi^\tau,\ \theta(-y) = d^{-1}\phi^\tau,\ d_i = \sigma\}, \qquad \text{and}$$

$$v_{i,j}^{\sigma,\tau} = \{\theta \in \mathscr{L} \mid \theta(x - jy) = d\phi^\tau,\ \theta(-x + jy) = d^{-1}\phi^\tau,\ d_i = \sigma\} \qquad \text{if } j \neq \infty.$$

Here x and y are the bases of V that we fixed in §4.

Now N_∞ fixes the set of all $v_{i,\infty}^{\sigma,\tau}$, so we abbreviate $v_{i,\infty}^{\sigma,\tau}$ as $v_i^{\sigma,\tau}$. We do not make use of $v_{i,j}^{\sigma,\tau}$ with $j \neq \infty$ in this section.

Definition 6.2. Let

$$v_i = v_i^{0,1} + \bar{\omega}v_i^{1,1} + \omega v_i^{-1,1} - v_i^{0,-1} - \bar{\omega}v_i^{1,-1} - \omega v_i^{-1,-1} \qquad \text{and}$$

$$\bar{v}_i = v_i^{0,1} + \omega v_i^{1,1} + \bar{\omega}v_i^{-1,1} - v_i^{0,-1} - \omega v_i^{1,-1} - \bar{\omega}v_i^{-1,-1}.$$

Let Υ_∞ be a vector space over $\mathbb{Q}[\omega]$ with basis $\{v_i \mid 1 \le i \le n\}$, and let $\overline{\Upsilon}_\infty$ be a vector space over $\mathbb{Q}[\omega]$ with basis $\{\bar{v}_i \mid 1 \le i \le n\}$.

Let $C_\infty = C_{N_\infty}(\infty_\phi)$, so $N_\infty = C_\infty{:}\langle x_{-1}\rangle$.

Lemma 6.1. *Υ_∞ and $\overline{\Upsilon}_\infty$ are C_∞-submodules of the $\mathbb{Q}[\omega]$ span of $\{v_i^{\sigma,\tau}\}$, and x_{-1} interchanges Υ_∞ and $\overline{\Upsilon}_\infty$.*

Proof. First we show that Q_∞ acts trivially on Υ_∞ and $\overline{\Upsilon}_\infty$. The group Q_∞ is generated by the maps ∞_f for $f \in L$, δ for $\delta \in R_0$, x_j for $1 \le j \le n$, and 0_ϕ. The following equations are elementary computations:

$$(v_i^{\sigma,\tau})^{\infty_f} = v_i^{\sigma,\tau}, \tag{6.1}$$

$$(v_i^{\sigma,\tau})^{0_f} = v_i^{\sigma+f_i,\tau}, \tag{6.2}$$

$$(v_i^{\sigma,\tau})^{\delta} = v_i^{\sigma,\tau} \qquad \text{for } \delta \in R_0, \tag{6.3}$$

$$(v_i^{\sigma,\tau})^{x_j} = v_i^{\sigma,\tau}. \tag{6.4}$$

Thus it is clear that the generators of Q_∞ act trivially on Υ_∞, and similarly they act trivially on $\overline{\Upsilon}_\infty$. We may also compute the equations:

$$(\upsilon_i^{\sigma,\tau})^\alpha = \upsilon_{i\alpha}^{\sigma,\tau} \qquad \text{for } \alpha \in S, \tag{6.5}$$

$$(\upsilon_i^{\sigma,\tau})^{x_{-1}} = \upsilon_i^{-\sigma,\tau}, \tag{6.6}$$

$$(\upsilon_i^{\sigma,\tau})^{x_h} = \upsilon_i^{\sigma,-\tau} \qquad \text{where } h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{6.7}$$

Equation (6.5) is obvious. To show (6.6) we calculate

$$\begin{aligned}(\upsilon_i^{\sigma,\tau})^{x_{-1}} &= \{\theta^{x_{-1}} \in \mathscr{L} \mid \theta(y) = d\phi^\tau,\ \theta(-y) = d^{-1}\phi^\tau,\ d_i = \sigma\} \\ &= \{\theta \in \mathscr{L} \mid \theta(y) = d^{-1}\phi^\tau,\ \theta(-y) = d\phi^\tau,\ d_i = \sigma\} \\ &= \{\theta \in \mathscr{L} \mid \theta(y) = d\phi^\tau,\ \theta(y) = d^{-1}\phi^{-\tau},\ d_i = -\sigma\}.\end{aligned}$$

The proof of (6.7) is similar, recalling that x_h is twisted by $\kappa(-1)$.

Now from (6.2) we have

$$\begin{aligned}(\upsilon_i)^{0_f} &= (\upsilon_i^{0,1} + \bar{\omega}\upsilon_i^{1,1} + \omega\upsilon_i^{-1,1} - \upsilon_i^{0,-1} - \bar{\omega}\upsilon_i^{1,-1} - \omega\upsilon_i^{-1,-1})^{0_f} \\ &= \upsilon_i^{f_i,1} + \bar{\omega}\upsilon_i^{1+f_i,1} + \omega\upsilon_i^{-1+f_i,1} - \upsilon_i^{f_i,-1} - \bar{\omega}\upsilon_i^{1+f_i,-1} - \omega\upsilon_i^{-1+f_i,-1} \\ &= \omega^{f_i}\upsilon_i.\end{aligned}$$

This shows that 0_f acts on Υ_∞ as the diagonal matrix $\operatorname{diag}(\omega^{f_i})$. Similarly we get that 0_f acts on $\overline{\Upsilon}_\infty$ as the diagonal matrix $\operatorname{diag}(\bar{\omega}^{f_i})$. Clearly (6.5) implies that $(\upsilon_i)^\alpha = \upsilon_{i\alpha}$ and $(\overline{\upsilon}_i)^\alpha = \overline{\upsilon}_{i\alpha}$. We also have

$$\begin{aligned}(\upsilon_i)^{x_h} &= (\upsilon_i^{0,1} + \bar{\omega}\upsilon_i^{1,1} + \omega\upsilon_i^{-1,1} - \upsilon_i^{0,-1} - \bar{\omega}\upsilon_i^{1,-1} - \omega\upsilon_i^{-1,-1})^{x_h} \\ &= \upsilon_i^{0,-1} + \bar{\omega}\upsilon_i^{1,-1} + \omega\upsilon_i^{-1,-1} - \upsilon_i^{0,1} - \bar{\omega}\upsilon_i^{1,1} - \omega\upsilon_i^{-1,1} \\ &= -\upsilon_i,\end{aligned}$$

and similarly $(\overline{\upsilon}_i)^{x_h} = -\overline{\upsilon}_i$. This shows that Υ_∞ and $\overline{\Upsilon}_\infty$ are N_∞-modules. We also get

$$\begin{aligned}(\upsilon_i)^{x_{-1}} &= (\upsilon_i^{0,1} + \bar{\omega}\upsilon_i^{1,1} + \omega\upsilon_i^{-1,1} - \upsilon_i^{0,-1} - \bar{\omega}\upsilon_i^{1,-1} - \omega\upsilon_i^{-1,-1})^{x_{-1}} \\ &= \upsilon_i^{0,1} + \bar{\omega}\upsilon_i^{-1,1} + \omega\upsilon_i^{1,1} - \upsilon_i^{0,-1} - \bar{\omega}\upsilon_i^{-1,-1} - \omega\upsilon_i^{1,-1} \\ &= \overline{\upsilon}_i,\end{aligned}$$

so x_{-1} interchanges Υ_∞ and $\overline{\Upsilon}_\infty$, and in fact it acts as complex conjugation. □

We have actually proven more; summarizing the last three calculations we have

$$(\upsilon_i)^{0_f} = \omega^{f_i}\upsilon_i, \tag{6.8}$$

$$(\upsilon_i)^{x_h} = -\upsilon_i, \tag{6.9}$$

$$(\upsilon_i)^{x_{-1}} = \overline{\upsilon}_i. \tag{6.10}$$

We remark that the action of 0_f, x_h, and x_α on Υ_∞ can be used to show that the image of C_∞/Q_∞ acting on Υ_∞ is the monomial subgroup of $\operatorname{Aut}_{\mathbb{Z}[\varepsilon]}(\Lambda)$.

The faithful components for Q_∞. We want to define objects permuted by N_∞ such that the $\mathbb{Q}[\omega]$-permutation module that they span has the faithful irreducible modules for $\overline{Q}_\infty$ as submodules. In the following paragraphs we use $+$, $-$, and 0 as superscripts to denote the elements 1, -1, and 0 of $\mathbb{F}_3$.

Definition 6.3. We define $\underline{f}_\infty^\sigma$ for $f \in L$, $\sigma \in \mathbb{F}_3$ by

$$\underline{f}_\infty^\sigma = \{\{\theta_0, \theta_1, \theta_2\} \mid \theta_i \in \mathscr{S}, \text{ and } \theta_i(x + \sigma y) = f(\$\not{\epsilon}^{-\sigma})^i\}$$

This one-line definition manages to obscure most of the ideas behind it, so we elaborate. More concretely, we have

$$\underline{f}_\infty^+ = \{\{\theta_0, \theta_1, \theta_2\} \mid \theta_i \in \mathscr{S},$$
$$\theta_0(x + y) = f,\ \theta_1(x + y) = f\$\not{\epsilon}^{-1},\ \text{and}\ \theta_2(x + y) = f\$^{-1}\not{\epsilon}\}$$

and similarly for $\underline{f}_\infty^-$ and $\underline{f}_\infty^0$. We may observe that $(\underline{f\$})_\infty^\sigma = (\underline{f\not{\epsilon}^\sigma})_\infty^\sigma$, so we have actually defined 3^7 distinct objects.

Definition 6.4. Let

$$f_\infty^\sigma = \underline{f}_\infty^\sigma + \bar{\omega}\underline{f\not{\epsilon}^\sigma}_\infty + \omega\underline{f\not{\epsilon}^{-1^\sigma}}_\infty \qquad \text{and}$$
$$\overline{f}_\infty^\sigma = \underline{f}_\infty^\sigma + \omega\underline{f\not{\epsilon}^\sigma}_\infty + \bar{\omega}\underline{f\not{\epsilon}^{-1^\sigma}}_\infty.$$

Let F_∞ be the vector space over $\mathbb{Q}[\omega]$ with basis $\{f_\infty^\sigma \mid f \in L, \sigma \in \mathbb{F}_3\}$, and let $\overline{F}_\infty$ be the vector space over $\mathbb{Q}[\omega]$ with basis $\{\overline{f}_\infty^\sigma \mid f \in L, \sigma \in \mathbb{F}_3\}$.

Lemma 6.2. *F_∞ and $\overline{F}_\infty$ are faithful Q_∞-modules. Also, x_{-1} interchanges F_∞ and $\overline{F}_\infty$.*

Proof. The idea of this proof is essentially the same as the proof of Lemma 6.1. First we see that

$$\begin{aligned}(f_\infty^\sigma)^{\infty\not{\epsilon}} &= (\underline{f}_\infty^\sigma + \bar{\omega}\underline{f\not{\epsilon}^\sigma}_\infty + \omega\underline{f\not{\epsilon}^{-1^\sigma}}_\infty)^{\infty\not{\epsilon}} \\ &= \underline{f\not{\epsilon}^\sigma}_\infty + \bar{\omega}\underline{f\not{\epsilon}^{-1^\sigma}}_\infty + \omega\underline{f}_\infty^\sigma \\ &= \omega f_\infty^\sigma,\end{aligned}$$

and similarly we see that $(\overline{f}_\infty^\sigma)^{\infty\not{\epsilon}} = \bar{\omega}\overline{f}_\infty^\sigma$, so if F_∞ and $\overline{F}_\infty$ are Q_∞-modules, they are faithful. Also, we see from the definition that F_∞ and $\overline{F}_\infty$ have dimension at most 3^6, which is the dimension of each faithful irreducible $\overline{Q}_\infty$-module; so if F_∞ and $\overline{F}_\infty$ are Q_∞-modules, they are also irreducible. Now Q_∞ is generated by the maps ${}^{\infty}{}_f$, ${}^{0}{}_{\not{\epsilon}}$, $\delta \in R_0$, and x_j. We show that they preserve the span of the f_∞^σ. First, we determine the action of these maps on

the $\underline{f^{\sigma}_{\infty}}$, which we claim is given by

$$(\underline{f^{\sigma}_{\infty}})^{0_{\not\in}} = (\underline{f\not\in^{\sigma}})^{\sigma}_{\infty}, \tag{6.11}$$

$$(\underline{f^{\sigma}_{\infty}})^{\delta} = (\underline{f\not\in^{\delta(\pi(f))}})^{\sigma}_{\infty}, \tag{6.12}$$

$$(\underline{f^{\sigma}_{\infty}})^{\infty_g} = (\underline{f^{R(g;\sigma)}})^{\sigma}_{\infty}, \quad \text{and} \tag{6.13}$$

$$(\underline{f^{\sigma}_{\infty}})^{x_j} = (\underline{f\psi_f^{-1}\not\in^{-f_j}})^{\sigma-1}_{\infty}. \tag{6.14}$$

To prove (6.11) we compute

$$\begin{aligned}
(\underline{f^{\sigma}_{\infty}})^{0_g} &= \{\{\theta_0^{0_g}, \theta_1^{0_g}, \theta_2^{0_g}\} \mid \theta_i \in \mathscr{S}, \text{ and } \theta_i(x+\sigma y) = f(\$\not\in^{-\sigma})^i\} \\
&= \{\{\theta_0, \theta_1, \theta_2\} \mid \theta_i \in \mathscr{S}, \text{ and } \theta_i^{0_g^{-1}}(x+\sigma y) = f(\$\not\in^{-\sigma})^i\} \\
&= \{\{\theta_0, \theta_1, \theta_2\} \mid \theta_i \in \mathscr{S}, \text{ and } \theta_i(x+\sigma y) = (f(\$\not\in^{-\sigma})^i)^{R(g^{\sigma};-\sigma)}\} \\
&= (\underline{f^{R(g^{\sigma};-\sigma)}})^{\sigma}_{\infty}.
\end{aligned}$$

Thus when $g = \not\in$ we have $(\underline{f^{\sigma}_{\infty}})^{0_{\not\in}} = (\underline{f\not\in^{\sigma}})^{\sigma}_{\infty}$. To prove (6.12) we compute

$$\begin{aligned}
(\underline{f^{\sigma}_{\infty}})^{\delta} &= \{\{\theta_0^{\delta}, \theta_1^{\delta}, \theta_2^{\delta}\} \mid \theta_i \in \mathscr{S}, \text{ and } \theta_i(x+\sigma y) = f(\$\not\in^{-\sigma})^i\} \\
&= \{\{\theta_0, \theta_1, \theta_2\} \mid \theta_i \in \mathscr{S}, \text{ and } \theta_i^{\delta^{-1}}(x+\sigma y) = f(\$\not\in^{-\sigma})^i\} \\
&= \{\{\theta_0, \theta_1, \theta_2\} \mid \theta_i \in \mathscr{S}, \text{ and } \theta_i(x+\sigma y) = f^{\delta}(\$\not\in^{-\sigma})^i\} \\
&= (\underline{f\not\in^{\delta(\pi(f))}})^{\sigma}_{\infty}.
\end{aligned}$$

To prove (6.13) we compute

$$\begin{aligned}
(\underline{f^{\sigma}_{\infty}})^{\infty_g} &= \{\{\theta_0^{\infty_g}, \theta_1^{\infty_g}, \theta_2^{\infty_g}\} \mid \theta_i \in \mathscr{S}, \text{ and } \theta_i(x+\sigma y) = f(\$\not\in^{-\sigma})^i\} \\
&= \{\{\theta_0, \theta_1, \theta_2\} \mid \theta_i \in \mathscr{S}, \text{ and } \theta_i^{\infty_g^{-1}}(x+\sigma y) = f(\$\not\in^{-\sigma})^i\} \\
&= \{\{\theta_0, \theta_1, \theta_2\} \mid \theta_i \in \mathscr{S}, \text{ and } \theta_i(x+\sigma y) = (f(\$\not\in^{-\sigma})^i)^{R(g;\sigma)}\} \\
&= (\underline{f^{R(g;\sigma)}})^{\sigma}_{\infty}.
\end{aligned}$$

To prove (6.14) we compute

$$\begin{aligned}
(\underline{f^{\sigma}_{\infty}})^{x_j} &= \{\{\theta_0^{x_j}, \theta_1^{x_j}, \theta_2^{x_j}\} \mid \theta_i \in \mathscr{S}, \text{ and } \theta_i(x+\sigma y) = f(\$\not\in^{-\sigma})^i\} \\
&= \{\{\theta_0, \theta_1, \theta_2\} \mid \theta_i \in \mathscr{S}, \text{ and } \theta_i^{x_j^{-1}}(x+\sigma y) = f(\$\not\in^{-\sigma})^i\} \\
&= \{\{\theta_0, \theta_1, \theta_2\} \mid \theta_i \in \mathscr{S}, \text{ and } \theta_i(x+(\sigma-1)y)^{\mathscr{Y}\partial_j} = f(\$\not\in^{-\sigma})^i\} \\
&= \{\{\theta_0, \theta_1, \theta_2\} \mid \theta_i \in \mathscr{S}, \text{ and } \theta_i(x+(\sigma-1)y) = (f(\$\not\in^{-\sigma})^i)^{\partial_j^{-1}\mathscr{Y}^{-1}}\} \\
&= \{\{\theta_0, \theta_1, \theta_2\} \mid \theta_i \in \mathscr{S}, \text{ and } \theta_i(x+(\sigma-1)y) = f^{\partial_j^{-1}\mathscr{Y}^{-1}}(\$\not\in^{-\sigma+1})^i\} \\
&= \{\{\theta_0, \theta_1, \theta_2\} \mid \theta_i \in \mathscr{S}, \text{ and} \\
&\qquad \theta_i(x+(\sigma-1)y) = f\psi_f^{-1}\not\in^{-f_j}(\$\not\in^{-\sigma+1})^i)\} \\
&= (\underline{f\psi_f^{-1}\not\in^{-f_j}})^{\sigma-1}_{\infty}.
\end{aligned}$$

Applying these equations to the f_∞^σ we get

$$(f_\infty^\sigma)^{0_\phi} = \omega^\sigma f_\infty^\sigma, \tag{6.15}$$

$$(f_\infty^\sigma)^\delta = \omega^{\delta(\pi(f))} f_\infty^\sigma, \tag{6.16}$$

$$(f_\infty^\sigma)^{\infty_g} = (f^{R(g;\sigma)})_\infty^\sigma, \quad \text{and} \tag{6.17}$$

$$(f_\infty^\sigma)^{x_j} = \omega^{-\Psi(\pi(f))-f_j} f_\infty^{\sigma-1}. \tag{6.18}$$

There are similar relations for the $\overline{f}_\infty^\sigma$, so we see that F_∞ and $\overline{F}_\infty$ are Q_∞-modules.

Since $(\underline{f_{-\infty}^\sigma})^{x_{-1}} = \underline{f^{-1}\sigma_\infty}$, we get that

$$\begin{aligned}(f_\infty^\sigma)^{x_{-1}} &= (\underline{f_{-\infty}^\sigma} + \bar{\omega}\underline{f\phi_{-\infty}^\sigma} + \omega\underline{f\phi^{-1\sigma}}_{-\infty})^{x_{-1}} \\ &= \underline{f^{-1\sigma}}_\infty + \bar{\omega}\underline{f^{-1}\phi^{-1\sigma}}_\infty + \omega\underline{f^{-1}\phi^\sigma}_\infty \\ &= \overline{f^{-1}}_\infty^\sigma.\end{aligned}$$

This shows that x_{-1} interchanges F_∞ and $\overline{F}_\infty$. □

Lemma 6.3. *F_∞ and $\overline{F}_\infty$ are C_∞-modules.*

Proof. We have already shown that they are Q_∞-modules, so we only need to check that they are fixed by the maps 0_g, $\alpha \in S$, and x_h where $h = \left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$. Computations similar to those for Lemma 6.2 show that

$$(\underline{f_{-\infty}^\sigma})^\alpha = (\underline{f^\alpha})_\infty^\sigma \qquad \text{for } \alpha \in S, \tag{6.19}$$

$$(\underline{f_{-\infty}^\sigma})^{0_g} = (\underline{f^{R(g^\sigma;-\sigma)}})_\infty^\sigma, \qquad \text{and} \tag{6.20}$$

$$(\underline{f_{-\infty}^\sigma})^{x_h} = (\underline{(f^{-1})^{\kappa(-1)}})_\infty^{-\sigma}. \tag{6.21}$$

The proof of (6.19) is obvious, and we proved (6.20) in the course of proving (6.11). To prove (6.21) we compute

$$\begin{aligned}(\underline{f_{-\infty}^\sigma})^{x_h} &= \{\{\theta_0^{x_h}, \theta_1^{x_h}, \theta_2^{x_h}\} \mid \theta_i \in \mathscr{S}, \text{ and } \theta_i(x+\sigma y) = f(\$\phi^{-\sigma})^i\} \\ &= \{\{\theta_0, \theta_1, \theta_2\} \mid \theta_i \in \mathscr{S}, \text{ and } \theta_i^{x_h}(x+\sigma y) = f(\$\phi^{-\sigma})^i\} \\ &= \{\{\theta_0, \theta_1, \theta_2\} \mid \theta_i \in \mathscr{S}, \text{ and } \theta_i(-x+\sigma y)^{\kappa(-1)} = f(\$\phi^{-\sigma})^i\} \\ &= \{\{\theta_0, \theta_1, \theta_2\} \mid \theta_i \in \mathscr{S}, \text{ and } \theta_i(-x+\sigma y) = f^{\kappa(-1)}(\$\phi^\sigma)^i\} \\ &= \{\{\theta_0, \theta_1, \theta_2\} \mid \theta_i \in \mathscr{S}, \text{ and } \theta_i(x-\sigma y) = (f^{-1})^{\kappa(-1)}(\$\phi^\sigma)^{-i}\} \\ &= (\underline{(f^{-1})^{\kappa(-1)}})_\infty^{-\sigma}.\end{aligned}$$

Applying these relations to the f_∞^σ we have

$$(f_\infty^\sigma)^\alpha = (f^\alpha)_\infty^\sigma, \tag{6.22}$$

$$(f_\infty^\sigma)^{0_g} = (f^{R(g^\sigma;-\sigma)})_\infty^\sigma, \qquad \text{and} \tag{6.23}$$

$$\begin{aligned}(f_\infty^\sigma)^{x_h} &= (\underline{f_{-\infty}^\sigma + \bar{\omega} f \phi^\sigma_\infty + \omega f \phi^{-1^\sigma}_{\infty}})^{x_h} \\ &= (\underline{(f^{-1})^{\kappa(-1)}})_\infty^{-\sigma} + \bar{\omega}(\underline{(f^{-1})^{\kappa(-1)}\phi})_\infty^{-\sigma} + \omega(\underline{(f^{-1})^{\kappa(-1)}\phi^{-1}})_\infty^{-\sigma} \\ &= ((f^{-1})^{\kappa(-1)})_\infty^{-\sigma}.\end{aligned} \tag{6.24}$$

Thus F_∞ is a C_∞-module, and similar relations for the $\overline{f}_\infty^\sigma$ show that $\overline{F}_\infty$ is an N_∞-module. □

We could also define irreducible modules F_j and $\overline{F}_j$ for Q_j, $j \in \mathbb{F}_p$, in a similar way. In fact, we could just take F_j to be the $\mathbb{Q}[\omega]$ vector space whose basis is the image of the basis for F_∞ under an element of N which takes ∞_ϕ to j_ϕ. A precise definition along the lines of Definitions 6.3 and 6.4 would require more complicated notation than those definitions, and we leave it to the reader's imagination.

The representation V_∞. There are 65,520 cosets of $\Lambda_C/\Theta\Lambda_C$ which contain a vector of minimum length. Thus there are $3 \times 65,520$ elements of $\overline{Q}_\infty$ which map onto a coset which contains a vector of minimum length, and these elements are permuted by $\overline{N}_\infty$. Use $\mathscr{M}$ to denote the set of all such elements of $\overline{Q}_\infty$.

Definition 6.5. Let $\underline{V}$ be the $\mathbb{Q}[\omega]$-permutation module for $\overline{N}_\infty$ acting by conjugation on the elements $r \in \mathscr{M}$. We use $\underline{X}_r$ to denote the basis vector of $\underline{V}$ corresponding to r.

If $s = r\infty_\phi$, we use $\underline{X}_{r\phi}$ to denote $\underline{X}_s$, and similarly we use $\underline{X}_{r\phi^{-1}}$ to denote $\underline{X}_s$ if $s = r\infty_{\phi^{-1}}$.

Our goal is to find an N_∞-invariant submodule of $\underline{V}$ whose restriction to Q_∞ affords each linear character of Q_∞ corresponding to an element $r \in \mathscr{M}$ with multiplicity 1.

Definition 6.6. For $r \in \mathscr{M}$, let

$$X_r = \underline{X}_r + \bar{\omega}\underline{X}_{r\phi} + \omega\underline{X}_{r\phi^{-1}} + \underline{X}_{r^{-1}} + \omega\underline{X}_{r^{-1}\phi} + \bar{\omega}\underline{X}_{r^{-1}\phi^{-1}}.$$

We let V_∞ be the span of all the X_r.

Lemma 6.4. *V_∞ is an N_∞-submodule of $\underline{V}$.*

Proof. For $g \in N_\infty$, we have $(\underline{X}_r)^g = \underline{X}_{rg}$, by definition. If g centralizes ∞_ϕ, we then have

$$(\underline{X}_{r\phi})^g = \underline{X}_{(r\phi)g} = \underline{X}_{rg\phi}$$

and similarly $(\underline{X}_{r\phi^{-1}})^g = \underline{X}_{rg\phi^{-1}}$. Thus we have

$$\begin{aligned}(X_r)^g &= (\underline{X}_r + \bar{\omega}\underline{X}_{r\phi} + \omega\underline{X}_{r\phi^{-1}} + \underline{X}_{r^{-1}} + \omega\underline{X}_{r^{-1}\phi} + \bar{\omega}\underline{X}_{r^{-1}\phi^{-1}})^g \\ &= \underline{X}_{rg} + \bar{\omega}\underline{X}_{rg\phi} + \omega\underline{X}_{rg\phi^{-1}} + \underline{X}_{(rg)^{-1}} + \omega\underline{X}_{(rg)^{-1}\phi} + \bar{\omega}\underline{X}_{(rg)^{-1}\phi^{-1}} \\ &= X_{rg}.\end{aligned}$$

If g inverts ∞_ϕ, we have

$$(\underline{X}_{r\phi})^g = \underline{X}_{(r\phi)g} = \underline{X}_{rg\phi^{-1}}.$$

Then we have

$$\begin{aligned}(X_r)^g &= (\underline{X}_r + \bar{\omega}\underline{X}_{r\phi} + \omega\underline{X}_{r\phi^{-1}} + \underline{X}_{r^{-1}} + \omega\underline{X}_{r^{-1}\phi} + \bar{\omega}\underline{X}_{r^{-1}\phi^{-1}})^g \\ &= \underline{X}_{rg} + \bar{\omega}\underline{X}_{rg\phi^{-1}} + \omega\underline{X}_{rg\phi} + \underline{X}_{(rg)^{-1}} + \omega\underline{X}_{(rg)^{-1}\phi^{-1}} + \bar{\omega}\underline{X}_{(rg)^{-1}\phi} \\ &= X_{(rg)^{-1}}.\end{aligned}$$

So we see that N_∞ stabilizes the set $\{X_r\}$ and so V_∞ is an N_∞-module. □

The elements of Q_∞ correspond to linear characters of Q_∞ as follows. For each $q \in Q_\infty$, there exists a linear character of Q_∞ which we call ξ_q, with $\xi_q(r) = \omega^i$ if $[q, r] = \phi^i$. We note that if $q = q'z$ with $q, q' \in Q_\infty$ and $z \in Z(Q_\infty)$ we have $\xi_q = \xi_{q'}$.

Lemma 6.5. *$V_\infty|_{Q_\infty}$ affords the linear characters of Q_∞ which correspond to a coset of $\Lambda_{\mathbb{C}}/\Theta\Lambda_{\mathbb{C}}$ containing a vector of minimum length.*

Proof. Let $r \in Q_\infty$ where r maps onto a coset of $\Lambda_{\mathbb{C}}/\Theta\Lambda_{\mathbb{C}}$ containing a vector of minimal length. Then for $q \in Q_\infty$ we have $X_r^q = X_{rq} = X_{r[r,q]}$. Now $X_{r\phi} = \omega X_r$, so we have $X_r^q = \omega^i X_r$ where $[r, q] = \phi^i$. Thus X_r affords the character ξ_r of Q_∞. □

N_∞ is a subgroup of the Monster. It turns out that the modules Υ_∞, V_∞, and F_∞ are the building blocks for all the representations we need to show that $\overline{N}_\infty$ is a subgroup of the Monster when C is the ternary Golay code. Here is the plan for doing so. We know that $\overline{N}_\infty$ is a subgroup of a group $G_\infty \cong 3^{1+12} \cdot 2Suz:2$, and the Monster also has a subgroup G_0 of this shape. Let B be the 196,884 dimensional module for the Monster. We determine the degrees of the irreducibles of $B|_{G_0}$. We will see that there are two groups of shape $3^{1+12} \cdot 2Suz:2$ with irreducibles of these degrees, and only one is isomorphic to a subgroup of the Monster. Then we use the representations Υ_∞, V_∞, and F_∞ to show that G_∞ is contained in the Monster.

In the remainder of this section we assume that the character tables for Suz and its central extensions in [4] are correct. We also assume that the character of the Monster of degree 196,883 given in [4] is correct. We use χ_M to denote the character afforded by a module M, and we let $\mathbb{M}$ be the Monster simple group.

Lemma 6.6. *Let $G_0 = C_{\mathbb{M}}(z)$ where z is an element of class $3B$ in the Monster. The degrees of the irreducibles of $B|_{G_0}$ are* 144, 65520, 12×3^6, 12×3^6, 78×3^6, *and* 78×3^6.

Proof. Let $Q_0 = O_3(G_0) \cong 3^{1+12}$. Write $B|_{G_0} = U \oplus V \oplus W \oplus \overline{W}$, where $U|_{Q_0}$ is trivial, $V|_{Q_0}$ affords linear characters of Q_0, $W|_{Q_0}$ is faithful, and

TABLE 6.1. The action of $Z(N_0)$ on Υ_∞ and F_∞

	Action on			
Group element	Υ_∞	F_∞^+	F_∞^-	F_∞^0
$\infty_{\not\in}$	1	ω	ω	ω
$\infty_{\$}$	1	$\bar{\omega}$	ω	1
$0_{\not\in}$	1	ω	$\bar{\omega}$	1
$0_{\$}$	ω	1	1	1

$\overline{W}$ is the algebraic conjugate of W. Also set $u = \dim(U)$, $v = \dim(V)$, and $w = \dim(W)$. Obviously we have $u + v + 2w = 196{,}884$. By considering the values of χ_U, χ_V, and χ_W on an element of $Z(Q_0)$ we get $u + v - w = 54$, so we have $w = 90 \times 3^6$.

Now there are two orbits of nontrivial linear characters of Q_0 under the action of $2Suz$, one of length 65,520 and the other of length $3^{12} - 65{,}521$. By dimension considerations, we must have $v = 0$ or $v = 65{,}520$. If $v = 0$, then for $q \in Q_0 \setminus Z(Q_0)$, we have $\chi_B(q) = 65{,}664$, which is a contradiction since there is no such element of order 3 in the Monster. Thus $v = 65,520$ and $u = 144$.

Now let $z \in G_0$ with $z^2 = 1$ and $zQ_0 \in Z(G_0/Q_0)$. Then if R is a faithful irreducible Q_0 module we have $\chi_R(z) = 1$. Now we have $\chi_U(z) = 144$, since the components of U are ordinary representations of Suz or $2Suz$ and $2Suz$ has no faithful representations of degree at most 144. Also, $\chi_V(z) = 0$, so we have $\chi_W(z) = 66$, since $\chi_B(z) = 276$. Thus $W = X \otimes R$, where X is a $6Suz$-module of dimension 90 and $\chi_X(z) = 66$. Examination of the degrees of the ordinary and projective representations of Suz implies then that X is the sum of a 12-dimensional irreducible and a 78-dimensional irreducible. □

Now the irreducibles of dimension 12 and 78 are faithful modules for $6Suz$ and $3Suz$, respectively, so G_0 is not a standard holomorph. Let $U_\infty = \Upsilon_\infty \otimes \overline{\Upsilon_\infty}$. We have shown that U_∞ and V_∞ are isomorphic to the 144- and 65,520-dimensional submodules of $B|_{G_0}$.

Lemma 6.7. *The subgroup $K \triangleleft N$ acts trivially on the N_∞-module $\Upsilon_\infty \otimes F_\infty$.*

Proof. We determine the action of $\infty_{\not\in}$, $0_{\not\in}$, $\infty_{\$}$, and $0_{\$}$ on Υ_∞ and F_∞. By (6.1)–(6.4) the maps $\infty_{\not\in}$, $0_{\not\in}$, and $\infty_{\$}$ all act trivially on Υ_∞, and by (6.8) the map $0_{\$}$ acts as the scalar matrix ω.

Next we determine the action of the elements on F_∞. By (6.17) we see that $\infty_{\not\in}$ acts as the scalar ω on F_∞, and the map $\infty_{\$}$ sends the basis vector f_∞^σ to $(f\$\psi_{\$}^\sigma)^\sigma = \omega^{-\sigma}(f)_\infty^\sigma$. By (6.15) we have $(f_\infty^\sigma)^{0_{\not\in}} = \omega^\sigma f_\infty^\sigma$. By (6.20) we have $(f_\infty^\sigma)^{0_{\$}} = (f\$^\sigma \psi_{\$}^{-\sigma})_\infty^\sigma = f_\infty^\sigma$. Thus we see that the action of these maps on Υ_∞ and F_∞ is as given in Table 6.1. This implies that $\infty_{\$}0_{\not\in}$ and $0_{\$}\infty_{\not\in}^{-1}$ act trivially on $\Upsilon_\infty \otimes F_\infty$. Since, by Definition 4.7,

$$K = \langle \infty_{\$}0_{\not\in},\ 0_{\$}\infty_{\not\in}^{-1} \rangle,$$

we see that this implies that K acts trivially on $\Upsilon_\infty \otimes F_\infty$. □

Lemma 6.1 implies that the image of the action of C_∞ on Υ_∞ is the monomial subgroup of $\mathrm{Aut}_{\mathbb{Z}[\omega]}(\Lambda)$. Also, the Q_∞-module F_∞ is a faithful module for the standard holomorph $G_s \cong 3^{1+12} : 2Suz$. Now G_s and $\mathrm{Aut}_{\mathbb{Z}[\omega]}(\Lambda) \cong 6Suz$ have a common quotient group $2Suz$, and their pullback $\hat{G}$ is the covering group of G_s by Lemma 2.7. From the discussion following Lemma 2.7, $\hat{G}$ has two quotients which are twisted holomorphs of shape $3^{1+12} \cdot 2Suz$ and $\Upsilon_\infty \otimes F_\infty$ is a faithful module for one of them while $\Upsilon_\infty \otimes \overline{F}_\infty$ is a faithful module for the other. Lemma 6.7 showed that $\Upsilon_\infty \otimes F_\infty$ is a faithful module for G_∞. Let G_1 be the twisted holomorph of shape $3^{1+12} \cdot 2Suz$ for which $\Upsilon_\infty \otimes \overline{F}_\infty$ is a faithful module. Also, let N_1 be the image of N_∞ acting on $\Upsilon_\infty \otimes \overline{F}_\infty$.

By Lemma 6.6, either G_∞ or G_1 is a subgroup of the Monster, since the irreducibles of dimensions 12 and 78 are faithful $6Suz$- and $3Suz$-modules, respectively. Thus to show that N_∞ is a subgroup of the Monster it suffices to show that N_1 is not a subgroup of the Monster. We do this by studying the characters of a particular element $t \in N_\infty$ on the modules defined above.

Let $t \in N_\infty$ be the element $0_d\rho$, where $\pi(d) = (-1, -1, -1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$ and ρ is the element of M_{11} which acts on $\{1, \dots, 12\}$ as $(4, 7)(5, 9)(6, 8)(11, 12)$. Obviously $d^\rho = d$, so t has order 6.

Lemma 6.8. *The characters of t on the modules Υ_∞ and F_∞ are given by*

$$\chi_{\Upsilon_\infty}(t) = -2 - 2\Theta \qquad \text{and} \qquad \chi_{F_\infty}(t) = 3\Theta.$$

Proof. Using (6.5) and (6.8) we have $v_i^t = v_i^{0_d\rho} = \omega^{d_i} v_{i^\rho}$, so

$$\chi_{\Upsilon_\infty}(t) = 3\bar{\omega} + \omega = -2 - 2\Theta.$$

Computing $\chi_{F_\infty}(t)$ is a bit more detailed. To do this we need to determine all basis vectors f_∞^σ of F_∞ with $(f_\infty^\sigma)^t = (f\not{e}^i)_\infty^\sigma$ for some i. Now if $\sigma \neq 0$, (6.19) and (6.20) imply that

$$(f_\infty^\sigma)^t = (f_\infty^\sigma)^{0_d\rho} = ((f^{R(d^\sigma; -\sigma)})_\infty^\sigma)^\rho = ((f^\rho)^{R(d^\sigma; -\sigma)})_\infty^\sigma,$$

so if f_∞^σ is an eigenvector for t and $\sigma = \pm 1$, we must have

$$\pi(f)^\rho \pm \pi(d) \equiv \pi(f) \pmod{(1^{12})}.$$

This is impossible, for if $\pi(f) = (f_1, \dots, f_{12})$, we have

$$\pi(f)^\rho \pm \pi(d) = (f_1 \mp 1, f_2 \mp 1, f_3 \mp 1, f_7, f_9, f_8, f_4, f_6, f_5, f_{10} \pm 1, f_{12} \pm 1, f_{11} \pm 1).$$

If this is congruent to $\pi(f)$ modulo (1^{12}), then the vector

$$(\mp 1, \mp 1, \mp 1, f_7 - f_4, f_9 - f_5, f_8 - f_6, f_4 - f_7, f_6 - f_8, f_5 - f_9, \pm 1, f_{12} - f_{11} \pm 1, f_{11} - f_{12} \pm 1)$$

is in $\langle (1^{12}) \rangle$; and comparing the first and tenth coordinates of this vector shows that is absurd. Thus if $(f_\infty^\sigma)^t = (f\not{e}^i)_\infty^\sigma$, we must have $\sigma = 0$.

To determine all $f \in L$ such that $(f_\infty^0)^t = (f\phi^i)_\infty^0$ for some i, we need to find those f such that $\pi(f)$ is fixed by ρ. Further, the relations on the f_∞^0 imply that we only need to find the action on one element $c \in \mathcal{G}$ from each coset of $\langle(1^{12})\rangle$, so it suffices to determine the fixed elements of shapes $(1^6, 0^6)$ and $(1^3, -1^3, 0^6)$. We list these vectors in Table 6.2, giving one representative from each orbit of vectors under the action of $\zeta = (1, 2, 3)(4, 5, 6)(7, 9, 8)$, an element of $S \cong M_{11}$ which centralizes t.

To see that the list is complete, it suffices to see that the $+1$ eigenspace of ρ on $\overline{\mathcal{G}}$ has dimension 3, since there are 27 vectors in our list. Now the trace of ρ on $\mathbb{F}_3^{12}$ is obviously 4. Lemma 2.1 shows that $\mathbb{F}_3^{12} \cong 1 \cdot \overline{\mathcal{G}} \cdot \overline{\mathcal{G}}^* \cdot 1$ as an M_{11}-module. Also, the trace of ρ on $\overline{\mathcal{G}}^*$ is the same as its trace on $\overline{\mathcal{G}}$, so we see that this must be 1. Thus the $+1$ eigenspace has dimension 0 or 3, and since we have exhibited nontrivial $+1$ eigenvectors it has dimension 3, so the list of Table 6.2 is complete.

TABLE 6.2. Elements of $\overline{\mathcal{G}}$ fixed by ρ

Representative of ζ-orbit* c	No. of Words in Orbit	$(\pi(d), c, c)$
(0,0,0,0,0,0,0,0,0,0,0,0)	1	0
(1,2,0,2,1,0,2,0,1,0,0,0)	3	1
(2,1,0,1,2,0,1,0,2,0,0,0)	3	1
(1,1,0,0,0,1,0,1,0,0,1,1)	3	0
(0,0,1,1,1,0,1,0,1,1,0,0)	3	0
(1,0,0,2,0,0,2,0,0,2,1,1)	3	2
(2,0,0,1,0,0,1,0,0,1,2,2)	3	2
(1,1,1,0,0,0,0,0,0,2,2,2)	1	0
(2,2,2,0,0,0,0,0,0,1,1,1)	1	0
(1,1,2,0,0,2,0,2,0,1,0,0)	3	1
(2,2,1,0,0,1,0,1,0,2,0,0)	3	1

* $\zeta = (1, 2, 3)(4, 5, 6)(7, 9, 8) \in S = \mathrm{stab}_{\mathrm{Aut}(\mathcal{G})}(u) \cong M_{11}$; ζ centralizes t.

Now if $f^\rho = f$, then

$$(f_\infty^0)^t = (f_\infty^0)^{0_d} = (f_\infty^0)^{r(d;0,1,0)} = (f[d, f, f])_\infty^0 = \omega^{(\pi(d),\pi(f),\pi(f))} f_\infty^0$$

Thus to compute $\chi_{F_\infty}(t)$ we need to know the values $(\pi(d), c, c)$ for each code word c fixed by ρ. These values are also listed in Table 6.2. Thus we have

$$\begin{aligned}\chi_{F_\infty}(t) &= \sum_{c^\rho = c} \omega^{(\pi(d),c,c)} \\ &= 9 + 12\omega + 6\bar{\omega} \\ &= 3\omega - 3\bar{\omega} = 3\Theta.\end{aligned}$$

This proves the lemma. □

Lemma 6.9. *G_1 is not a subgroup of the Monster.*

Proof. If G_1 is a subgroup of the Monster, then we have

$$B|_{N_1} \cong U_\infty \oplus V_\infty \oplus (\Upsilon_\infty \otimes \overline{F}_\infty) \oplus (\overline{\Upsilon}_\infty \otimes F_\infty) \oplus (S^2(\overline{\Upsilon}_\infty) \otimes \overline{F}_\infty) \oplus (S^2(\Upsilon_\infty) \otimes F_\infty).$$

Now by Lemma 6.5 we have

$$\begin{aligned} \chi_{U_\infty}(t) &= 4 - \Theta^2 = 7, \\ \chi_{\Upsilon_\infty \otimes \overline{F}_\infty}(t) &= -3\Theta(-2 - \Theta) = 6\Theta - 9, \quad \text{and} \\ \chi_{S^2(\overline{\Upsilon}_\infty)\otimes \overline{F}_\infty}(t) &= -3\Theta(1/2)((-2+\Theta)^2 + 3) \\ &= -3\Theta(1/2)(4 - 4\Theta) \\ &= -3\Theta(2 - 2\Theta) \\ &= -18 - 6\Theta. \end{aligned}$$

Now let $z \in G_1$ with $z^2 = 1$, $zQ_1 \in Z(G_1/Q_1)$, and $[z, t] = 1$. We see that the image of t in G_1 lies in $C_{G_1}(z) \cong 6Suz$. Then the character table in [4] implies that t is an element of one of the conjugacy classes 6BC of Suz, so we may compute that

$$\chi_{V_\infty}(t) = 18.$$

Thus we have

$$\chi_B(t) = 7 + 18 - 18 - 36 = -29.$$

Now by the character table of the Monster in [4], there is no element of order 6 in the Monster with trace -29 on B. Thus G_1 cannot be a subgroup of the Monster. □

Theorem 6.10. *$\overline{N}_\infty$ is a subgroup of the Monster.*

Proof. Lemma 6.6 implies that one of the twisted holomorphs G_∞ or G_1 is a subgroup of the Monster. Lemma 6.9 says that the group G_1 is not a subgroup of the Monster, so it must be the case that G_∞ is a subgroup of the Monster. □

7. Uniqueness theorems

The purpose of this section is to show that N_3, N_5, and N_7 are subgroups of the Monster. We do this by proving uniqueness theorems for groups satisfying certain properties, which are easily verified for the groups N_3, N_5, and N_7 and the corresponding subgroups of the Monster. The uniqueness proofs all make use of the following lemma.

Lemma 7.1. *Suppose that K and K_1 are groups which satisfy the following properties:*

(i) *There exist subgroups $H \triangleleft K$ and $H_1 \triangleleft K_1$ and an isomorphism $\gamma_H : H \to H_1$.*

(ii) *There exist subgroups $B < K$ and $B_1 < K_1$ with $H \cap B = 1_K$ and $H_1 \cap B_1 = 1_{H_1}$. Let $T = H{:}B$ and let $T_1 = H_1{:}B_1$. There is an isomorphism $\gamma_T : T \to T_1$ with $\gamma_T|_H = \gamma_H$ and $\gamma_T(B) = B_1$.*

(iii) *There exist elements* $n \in K$ *and* $n_1 \in K_1$ *with* $K = \langle H, B, n\rangle$ *and* $K_1 = \langle H_1, B_1, n_1\rangle$.

(iv) *Let* $G = \langle B, n\rangle$ *and let* $G_1 = \langle B_1, n_1\rangle$. *There is an isomorphism* $\gamma_G : G \to G_1$ *with* $\gamma_G|_B = \gamma_T|_B$ *and* $\gamma_G(n) = n_1$. *Also,* $\langle B, n\rangle \cap H = 1$ *and* $\langle B_1, n_1\rangle \cap H = 1$.

(v) *There is an isomorphism* $\gamma_1 : \langle H, n\rangle \to \langle H_1, n_1\rangle$ *with* $\gamma_1|_H = \gamma_H$ *and* $\gamma_1(n) = n_1$.

Then there is an isomorphism $\gamma : K \to K_1$ *with* $\gamma|_T = \gamma_T$ *and* $\gamma(n) = n_1$.

Proof. By assumptions (iii) and (iv) we have $K = HG$ and $K_1 = H_1G_1$. For $k = hg \in K$, define $\gamma(k)$ by $\gamma(hg) = \gamma_H(h)\gamma_G(g)$. Assumption (iv) implies that γ is well defined. Now let $t \in T$, so by assumption (ii) we may write $t = hb$ with $h \in H$, $b \in B$. Then $\gamma(t) = \gamma_H(h)\gamma_G(b) = \gamma_T(h)\gamma_T(b)$ by assumptions (ii) and (iv). This shows that $\gamma|_T = \gamma_T$. Since $n \in G$, we have $\gamma(n) = \gamma_G(n) = n_1$. Thus it only remains to show that γ is an isomomorphism.

Let k, k' be elements of K, and suppose $k = hg$ and $k' = h'g'$ for $h, h' \in H$ and $g, g' \in G$. Now

$$\gamma(hgh'g') = \gamma(hh'^{g^{-1}}gg') = \gamma_H(hh'^{g^{-1}})\gamma_G(gg') = \gamma_H(h)\gamma_H(h'^{g^{-1}})\gamma_G(g)\gamma_G(g'),$$

while

$$\gamma(hg)\gamma(h'g') = \gamma_H(h)\gamma_G(g)\gamma_H(h')\gamma_G(g') = \gamma_H(h)\gamma_H(h')^{\gamma_G(g^{-1})}\gamma_G(g)\gamma_G(g').$$

Thus we see that $\gamma(hgh'g') = \gamma(hg)\gamma(h'g')$ if $\gamma_H(h'^{g^{-1}}) = \gamma_H(h')^{\gamma_G(g^{-1})}$. Now if $g \in B$, then by property (ii) we find $\gamma_H(h'^{g^{-1}}) = \gamma_T(h'^{g^{-1}}) = \gamma_T(h')^{\gamma_T(g^{-1})} = \gamma_H(h')^{\gamma_G(g^{-1})}$. If $g = n$, then by property (v) we find $\gamma_H(h'^{g^{-1}}) = \gamma_1(h'^{g^{-1}}) = \gamma_1(h')^{\gamma_1(g^{-1})} = \gamma_H(h')^{\gamma_G(g^{-1})}$. We claim that this implies $\gamma_H(h'^{g^{-1}}) = \gamma_H(h')^{\gamma_G(g^{-1})}$ for all $g \in \langle B, n\rangle = G$. To prove this claim, it suffices to show that if $g = g_1g_2$ with $g_i \in G$, and $\gamma_H(h'^{g_i^{-1}}) = \gamma_H(h')^{\gamma_G(g_i^{-1})}$ for $i = 1, 2$, then $\gamma_H(h'^{g^{-1}}) = \gamma_H(h')^{\gamma_G(g^{-1})}$. Now $h'^{g_i^{-1}} \in H$ since $H \triangleleft N$, so $\gamma_H(h'^{g^{-1}}) = \gamma_H(h'^{g_2^{-1}g_1^{-1}}) = \gamma_H(h'^{g_2^{-1}})^{\gamma_G(g_1^{-1})} = \gamma_H(h')^{\gamma_G(g_2^{-1})\gamma_G(g_1^{-1})} = \gamma_H(h')^{\gamma_G(g^{-1})}$. This shows the claim and so γ is a homomorphism. Since $N = H{:}G$, $N_1 = H_1{:}G_1$, and γ_G and γ_H are isomorphisms onto G_1 and H_1, it follows that γ is an isomorphism. □

The uniqueness of N_5. Let $\Lambda = \Lambda(\mathscr{F})$. Let N be a group with the following properties:

(1) N has a normal subgroup $V = \langle x, v\rangle$, and V is elementary abelian of order 5^2.

(2) $C = C_N(x)$ has a normal subgroup $Q \cong 5_+^{1+6}$, an extraspecial group of order 5^7 and exponent 5.

(3) $C/Q \cong 5^2{:}(4 \times S_3)$ is isomorphic to the monomial subgroup $\overline{\mathrm{Mon}}(\Lambda) < 2HJ < \mathrm{Aut}_{\mathbb{Z}[\varepsilon]}(\Lambda)$. There is a subgroup $D < N_N(\langle x\rangle)$ of index 2, with $D \cong Q{:}M$ and $M \cong \overline{\mathrm{Mon}}(\Lambda){:}\langle\sigma_{-1}\rangle$.

(4) There is a homomorphism of M-modules $\phi : Q/Q' \to \Lambda/(\varepsilon - 1)\Lambda$, with $\phi(v) \equiv \lambda_b$. Also ϕ is an isometry, where the form on Q/Q' is given by the commutator map and the form on $\Lambda/(\varepsilon - 1)\Lambda$ is as described in Lemma 5.5.

(5) There is an element $t \in Q$ with $\phi(t) \equiv (1, 2, 1, 2, 1, 2)$ and an element $n \in N$ such that $N = \langle C, n\rangle$, $\langle t, n\rangle \cong SL(2, 5)$ and n has matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$

in its action on V. Also, there is an element $s \in M$ of order 4 such that $\langle t, n, s\rangle \cong GL(2, 5)$.

Theorem 7.2. *There is at most one isomorphism class of groups satisfying properties* (1)–(5).

Proof. We let N and N_1 be two groups satisfying (1)–(5). Our strategy is to show that N and N_1 satisfy the hypotheses of the groups K and K_1 of Lemma 7.1 and deduce that $N \cong N_1$.

For each subgroup $G < N$ with properties as given in (1)–(5), let G_1 be the subgroup of N_1 with the same properties. Similarly for each element $g \in N$ with properties as given in (1)–(5), let g_1 be the element of N_1 with the same properties. By (2) we have $Q \cong Q_1$. By (3) and (4) we have $C \cong C_1$ and $D \cong D_1$.

We let $G = \langle t, s, n\rangle$ and $G_1 = \langle t_1, s_1, n_1\rangle$, so that $G \cong G_1 \cong GL(2, 5)$. Now let $E = C_N(V)$ and let $E_1 = C_{N_1}(V_1)$, and since $E < C$ and $E_1 < C_1$, we get $E \cong E_1$.

To apply Lemma 7.1, we let N, N_1, E, E_1, $\langle s, t\rangle$, $\langle s_1, t_1\rangle$, n, and n_1 play the roles of K, K_1, H, H_1, B, B_1, n, and n_1, respectively, in Lemma 7.1. Our groups satisfy property (i), since $E \lhd N$, $E_1 \lhd N_1$, and $E \cong E_1$. They satisfy (ii), since $\langle E, s, t\rangle = C$, $\langle E_1, s_1, t_1\rangle = C_1$, and $C \cong C_1$. Property (5) implies that N and N_1 satisfy (iii). We check that they satisfy (iv). First, we have $G = \langle s, t, n\rangle \cong GL(2, 5) \cong \langle s_1, t_1, n_1\rangle = G_1$. Property (5) also implies that G and G_1 act faithfully on V, so we get $G \cap E = 1$ and $G_1 \cap E_1 = 1$. Finally, $\gamma_G|_{\langle s,t\rangle} = \gamma_T|_{\langle s,t\rangle}$ by considering the action of elements of $\langle s, t\rangle$ and $\langle s_1, t_1\rangle$ on V. Thus all that remains to check is property (v).

Now let γ_E be the isomorphism from E to E_1. The groups N and N_1 act by conjugation on E and E_1, respectively. We also get an action of N_1 on E by the rule $e^g = \gamma_E^{-1}(\gamma_E(e)^g)$ for $e \in E$, $g \in G_1$. Now with this action of G_1 on E, we get $N_1 \cong E{:}G_1$.

Define $\gamma_1 : E{:}\langle n\rangle \to E{:}\langle n_1\rangle$ by $\gamma_1(en^k) = en_1^k$ for $e \in E$ and $k \in \mathbb{N}$. Since both n and n_1 have order 4, γ_1 is an isomorphism if n and n_1 induce the same automorphism of E.

Since $O_5(E)$ is characteristic in E and $E \lhd N$, it is contained in $O_5(N)$. Since $O_5(N/E) = O_5(GL(2, 5)) = 1$, we have $O_5(N) = O_5(E)$ and, similarly, $O_5(N_1) = O_5(E_1)$. We claim that $E \cong 5^{2+2+4}{:}S_3$. Let $P = O_5(E)$. Assumption (4) implies that $V = Z(E)$ and that P' has order 5^4. Then (2) and (4) imply that P' is elementary abelian of order 5^4 and (2) and (3) imply that P/P' is elementary abelian of order 5^4. Now (3) implies that $E = P \cdot S$ where $S \cong S_3$, and this proves the claim.

We want to show that G and G_1 are contained in $C_N(S)$ and $C_{N_1}(S)$, respectively. By Sylow theory, there is a single conjugacy class of subgroups isomorphic to S in E, so the Frattini argument shows that $N = E.C_N(S)$. Hence we have $G < C_N(S)$, and similarly $G_1 < C_{N_1}(S)$.

Now P/P' is a 4-dimensional module for $S \times G$ and $S \times G_1$, $Z(G)$ and $Z(G_1)$ act faithfully on P/P', and S_3 acts faithfully on P/P'. Thus $P/P' \cong \rho \otimes \sigma$, where ρ is the faithful irreducible module of S_3 and σ is the natural module for $GL(2, 5)$. Now $\Lambda^2(\rho \otimes \sigma)$ is easily shown to have irreducible constituents of dimension 3, 2, and 1. Thus since $P'/Z(P)$ is a 2-dimensional

module for $S_3 \times GL(2, 5)$, it must be isomorphic to the 2-dimensional irreducible submodule of $\Lambda^2(\rho \otimes \sigma)$. Thus we have $P'/Z(P) \cong \rho \otimes \delta$, where the character afforded by δ is the determinant of matrices in the natural representation of $GL(2, 5)$.

Let $f : N \to \mathrm{Aut}(E)$ and $g : N_1 \to \mathrm{Aut}(E)$ be the homomorphisms gotten by letting elements of N and N_1, respectively, act on E. By our choice of n and n_1, we see that $f(n)$ and $g(n_1)$ induce the same action on P/P', $P'/Z(P)$, and $Z(P)$. Thus we define $\vartheta : P \to P'/Z(P)$ by

$$p^{\vartheta} = p^{-1}p^{g(n_1)f(n^{-1})}Z(P). \tag{7.1}$$

First we show that ϑ is constant on cosets of P'. For $q \in P'$ we have

$$\begin{aligned}(pq)^{\vartheta} &= q^{-1}p^{-1}p^{g(n_1)f(n^{-1})}q^{g(n_1)f(n^{-1})}Z(P)\\ &= q^{-1}p^{-1}p^{g(n_1)f(n^{-1})}qZ(P)\\ &= p^{-1}p^{g(n_1)f(n^{-1})}Z(P) \;=\; p^{\vartheta}.\end{aligned}$$

Now by multiplying each side of (7.1) by p we get

$$pp^{\vartheta} = p^{g(n_1)f(n^{-1})}Z(P). \tag{7.2}$$

Since $f(n)$ acts trivially on $P'/Z(P)$, applying $f(n)$ to each side of this equation gives

$$p^{f(n)}p^{\vartheta} = p^{g(n_1)}Z(P). \tag{7.3}$$

Now this implies that

(7.4)
$$p^{g(n_1)^2} = (p^{f(n)}p^{\vartheta})^{g(n_1)} = (p^{f(n)}p^{\vartheta})^{f(n)}(p^{f(n)}p^{\vartheta})^{\vartheta} = p^{f(n^2)}p^{\vartheta f(n)}(p^{f(n)}p^{\vartheta})^{\vartheta}.$$

Since ϑ is constant on cosets of P', $(p^{f(n)}p^{\vartheta})^{\vartheta} = p^{f(n)\vartheta}$. As above, $f(n)$ acts trivially on $P'/Z(P)$, so $p^{\vartheta f(n)} = p^{\vartheta}$. Now $n^2 \in D$ and $n_1^2 \in D_1$, so $f(n^2) = g(n_1^2)$. Thus we may rewrite (7.4) to get $p^{g(n_1)^2} = p^{g(n_1^2)}p^{\vartheta}p^{f(n)\vartheta}$, which implies that

$$(p^{f(n)})^{\vartheta} = (p^{\vartheta})^{-1}. \tag{7.5}$$

Next we claim that $(p^{\vartheta})^{-1} = (p^{-1})^{\vartheta}$. From the definition of ϑ we find $(p^{\vartheta})^{-1} = (p^{g(n_1)f(n^{-1})})^{-1}pZ(P)$. Now $f(n)$ and $g(n_1)$ have the same action on P/P', so let $q \in P'$ satisfy $p^{g(n_1)f(n^{-1})} = pq$. Then

$$(p^{\vartheta})^{-1} = (pq)^{-1}pZ(P) = [(pq)^{-1}, p]p(pq)^{-1}Z(P) = [q^{-1}, p]p(pq)^{-1}Z(P).$$

Now the commutator $[q^{-1}, p]$ lies in $[P', P] = Z(P)$, and by the definition of ϑ we have

$$p(pq)^{-1}Z(P) = p(p^{g(n_1)f(n^{-1})})^{-1}Z(P) = p(p^{-1})^{g(n_1)f(n^{-1})}Z(P) = (p^{-1})^{\vartheta},$$

so this proves our claim that

$$(p^{\vartheta})^{-1} = (p^{-1})^{\vartheta}. \tag{7.6}$$

Now $p^{f(n^2)} = p^{-1}$, so by using (7.5) twice we get

$$(7.7)\quad (p^{-1})^{\vartheta} = (p^{f(n^2)})^{\vartheta} = (p^{f(n)f(n)})^{\vartheta} = (p^{f(n)\vartheta})^{-1} = ((p^{\vartheta})^{-1})^{-1} = p^{\vartheta}.$$

Now comparing (7.6) and (7.7) shows that

$$(7.8)\qquad p^{\vartheta} = (p^{-1})^{\vartheta} = (p^{\vartheta})^{-1}.$$

This implies that $p^{\vartheta} = 1$, which implies that $f(n)$ and $g(n_1)$ have the same action on $P/Z(P)$.

All that remains is to show that the map $\tau : P \to Z(P)$ defined by $p^{\tau} = p^{g(n_1)f(n^{-1})}$ is trivial. Since G and G_1 both commute with S, this map defines an S-module homomorphism from $P/Z(P)$ to $Z(P)$. But $Z(P)$ is a trivial S-module, while the only irreducible S-module which occurs as a factor of $P/Z(P)$ is the faithful irreducible S-module. Thus τ is trivial. This shows that $f(n) = g(n_1)$, so γ_1 is an isomorphism, and thus by Lemma 7.1 we have $N \cong N_1$. □

Theorem 7.3. *The group N_5 satisfies* (1)–(5).

Proof. Let $V = \langle \infty_{\not c}, 0_{\not c} \rangle K/K$ and let $x = \infty_{\not c}$, so $C = C_{N_5}(\infty_{\not c})$. Theorem 4.15 implies that $V \triangleleft N_5$, so N_5 satisfies (1). Theorem 4.17 shows that $\overline{Q_\infty} \triangleleft C$, so N_5 satisfies (2).

Theorem 5.17 shows that $C/\overline{Q_\infty} \cong \overline{\mathrm{Mon}}(\Lambda)$. Now let $M = \langle x_h, 0_f, S, x_{-1} \mid h = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 2 \end{smallmatrix}\right), f = (0, c), c \in \mathscr{F}_0 \rangle K/K$. Equation (4.3) implies that if $f = (0, c)$ and $g = (0, c)$, then $0_f 0_g = 0_h$ where $h = (0, c + d)$. Thus $\langle 0_f \mid f = (0, c), c \in \mathscr{F}_0 \rangle$ is elementary abelian of order 5^2. Lemmas 2.3 and 3.2 show that S normalizes $\langle 0_f \mid f = (0, c), c \in \mathscr{F}_0 \rangle$. Now Lemma 4.16 implies that $0_f^{x_h} = 0_{f^{\kappa(-2)}}^{-1} = 0_f^{-1}$, since $f^{\kappa(-2)} = (0, c)^{\kappa(-2)} = (0, c) = f$. We also have $0_f^{x_{-1}} = 0_{f^{-1}}$. Thus x_h and x_{-1} normalize $\langle 0_f \mid f = (0, c), c \in \mathscr{F}_0 \rangle$. Clearly x_h and x_{-1} commute. Finally, it is clear that x_h and x_{-1} commute with S, since S commutes with both the natural action on $\mathrm{Aut}(V)$ and with the maps κ and $\mathscr{Y}$. Lemma 5.11 shows that x_{-1} has the same action on $Q_\infty/Z(Q_\infty)$ as σ_{-1} has on $\Lambda/(\varepsilon - 1)\Lambda$. This shows that M is a complement to $\overline{Q_\infty}$ isomorphic to $\overline{\mathrm{Mon}}(\Lambda):\langle \sigma_{-1} \rangle$, so N_5 satisfies (3).

Let ϕ be the map of Definition 5.5. Then $\phi(0_{\not c}^{-1}) = \lambda_b$, and Lemma 5.5 shows that ϕ is an isometry. Also, Theorem 5.14 and Lemma 5.16 show that ϕ is an isomorphism of M-modules. Thus N_5 satisfies (4).

Now let t be the image of x_t in N_5, let n be the image of x_h in N_5 for $h = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, and let s be the image of x_h in N_5 for $h = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$. Definition 5.5 shows that $\phi(x_t^3) = \lambda_t$. It follows from the proof of Theorem 4.15 that $\langle C, n \rangle = N_5$, that $\langle t, n \rangle = SL(2, 5)$, and that $\langle t, n, s \rangle = GL(2, 5)$. These facts show that N_5 satisfies (5). □

The uniqueness of N_3. Let N be a group satisfying the following assumptions:

(6) N has a normal elementary abelian subgroup $V = \langle x, z \rangle$ of order 9. We let $C = C_N(x)$.

(7) $O_3(C)$ has a subgroup $Q \cong 3_+^{1+12}$ with $x \in Z(Q)$, and $Q \triangleleft C$.

(8) There is an isomorphism of C/Q modules $\phi : Q/Z(Q) \to \Lambda_{\mathbb{C}}/\Theta\Lambda_{\mathbb{C}}$. Also, for $q, r \in Q$, we have $[q, r] = x^{(\phi(q), \phi(r))}$.

(9) $\phi(z\langle x\rangle) = \lambda + \Theta\Lambda_{\mathbb{C}}$, $\lambda = (3\Theta, 0^{11})$.

(10) $C/Q \cong 2 \times 3^5 : M_{11}$.

(11) C is a subgroup of the Monster.

(12) There is an element $t \in Q$ with $\phi(t) \equiv (4, 1^{11})$ and an element $n \in N$ such that $N = \langle C, n\rangle$, $\langle t, n\rangle \cong SL(2, 3)$, and n has matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ in its action on V. There is an element $s \in C \setminus Q$ of order 2 such that $\langle t, n, s\rangle \cong GL(2, 3)$. We also assume that $C_C(n) \cong 3^5 : M_{11}$.

Theorem 7.4. *Let N be a group satisfying the properties* (6)–(12). *Then N is unique up to isomorphism.*

Proof. Let N and N_1 be two groups satisfying (6)–(12). Our strategy is to show that N and N_1 satisfy the hypotheses of the groups K and K_1 of Lemma 7.1 and to deduce that $N \cong N_1$.

For each subgroup $G < N$ with properties as given in (6)–(12), let G_1 be the subgroup of N_1 with the same properties. Similarly for each element $g \in N$ with properties as given in (6)–(12), let g_1 be the element of N_1 with the same properties. By (7) we have $Q \cong Q_1$. By (8), (10), and (11) we have $C \cong C_1$.

We let $G = \langle t, s, n\rangle$ and $G_1 = \langle t_1, s_1, n_1\rangle$, so that $G \cong G_1 \cong GL(2, 3)$. Now let $E = C_N(V)$ and $E_1 = C_{N_1}(V_1)$, and since $E < C$ and $E_1 < C_1$, we get $E \cong E_1$.

To apply Lemma 7.1, we let N, N_1, E, E_1, $\langle s, t\rangle$, $\langle s_1, t_1\rangle$, n, and n_1 play the roles of K, K_1, H, H_1, B, B_1, n, and n_1, respectively, in Lemma 7.1. Our groups satisfy property (i), since $E \lhd N$, $E_1 \lhd N_1$, and $E \cong E_1$. They satisfy (ii), since $\langle E, s, t\rangle = C$, $\langle E_1, s_1, t_1\rangle = C_1$, and $C \cong C_1$. Property (12) implies that N and N_1 satisfy (iii). We check that they satisfy (iv). First, we have $G = \langle s, t, n\rangle \cong GL(2, 3) \cong \langle s_1, t_1, n_1\rangle = G_1$. Property (12) also implies that G and G_1 act faithfully on V, so we get $G \cap E = 1$ and $G_1 \cap E_1 = 1$. Finally, $\gamma_G|_{\langle s,t\rangle} = \gamma_T|_{\langle s,t\rangle}$ by considering the action of elements of $\langle s, t\rangle$ and $\langle s_1, t_1\rangle$ on V. Thus all that remains to check is property (v).

Now let γ_E be the isomorphism from E to E_1. The groups N and N_1 act by conjugation on E and E_1, respectively. We also get an action of N_1 on E by the rule $e^g = \gamma_E^{-1}(\gamma_E(e)^g)$ for $e \in E$, $g \in G_1$. Now with this action of G_1 on E, we get $N_1 \cong E{:}G_1$.

Define $\gamma_1 : E{:}\langle n\rangle \to E{:}\langle n_1\rangle$ by $\gamma_1(en^k) = en_1^k$ for $e \in E$ and $k \in \mathbb{N}$. Since both n and n_1 have order 4, γ_1 is an isomorphism if n and n_1 induce the same automorphism of E.

Since $O_3(E)$ is characteristic in E and $E \lhd N$, it is contained in $O_3(N)$. Since $O_3(N/E) = O_3(GL(2, 3)) = 1$, we have $O_3(N) = O_3(E)$, and similarly $O_3(N_1) = O_3(E_1)$. We claim that $E \cong 3^{2+5+10} : M_{11}$. Let $P = O_3(E)$. Assumptions (8) and (10) imply that $V = Z(E)$, and that P' has order 3^7. Then (7) and (8) imply that P' is elementary abelian of order 3^7 and that P/P' is elementary abelian of order 3^{10}. Now (10) implies that $E = P.S$ where $S \cong M_{11}$, and this proves the claim.

Now P/P' is a 10-dimensional module for $M_{11} \times G$ and $M_{11} \times G_1$, $Z(G)$ and $Z(G_1)$ act faithfully on P/P', and M_{11} acts faithfully on P/P'. It is

clear from (8) and (10) that $P/P' \cong \bar{\mathcal{G}} \otimes \sigma$, where σ is the natural module for $GL(2, 3)$, and that $P'/Z(P) \cong \bar{\mathcal{G}}^* \otimes \delta$, where the character afforded by δ is the determinant of matrices in the natural representation of $GL(2, 3)$.

Let $f : N \to \mathrm{Aut}(E)$ and $g : N_1 \to \mathrm{Aut}(E)$ be the homomorphisms gotten by letting elements of N and N_1, respectively, act on E. By our choice of n and n_1, we see that $f(n)$ and $g(n_1)$ induce the same action on P/P', $P'/Z(P)$, and $Z(P)$. The same argument as we used in the proof of Theorem 7.2 shows that $f(n)$ and $g(n_1)$ induce the same action on $P/Z(P)$. Now we want to show that the map $\tau : P \to Z(P)$ defined by $p^\tau = p^{g(n_1)f(n^{-1})}$ is trivial. By assumption (12), n and n_1 are contained in $C_N(S)$ and $C_{N_1}(S)$, respectively. Thus τ defines an S-module homomorphism from $P/Z(P)$ to $Z(P)$. But $Z(P)$ is a trivial S-module, while the only irreducible S-modules which occur as factors of $P/Z(P)$ are $\bar{\mathcal{G}}$ and $\bar{\mathcal{G}}^*$. Thus τ is trivial. This shows that $f(n) = g(n_1)$, so γ_1 is an isomorphism. This establishes property (v), so by Lemma 7.1 we have $N \cong N_1$. □

Theorem 7.5. *The group N_3 satisfies* (6)–(12).

Proof. Let $V = \langle \infty_{\mathcal{C}}, 0_{\mathcal{C}} \rangle K$ and let $x = \infty_{\mathcal{C}}$, so $C = C_{N_3}(\infty_{\mathcal{C}})$. Then Theorem 4.15 shows that $V \triangleleft N_3$, so N_3 satisfies (6). Theorem 4.17 shows that $\overline{Q_\infty} \triangleleft C$, so N_3 satisfies (7). Theorem 5.14 and Lemma 5.5 show that N_3 satisfies (8). Definition 5.4 shows that $\phi(0_{\mathcal{C}}^{-1}) = \lambda_b$, so N_3 satisfies (9). Theorem 4.17 shows that $C/\overline{Q_\infty} \cong 2 \times 3^5{:}M_{11}$, so N_3 satisfies (10). To show that N_3 satisfies (11) we use Theorem 6.10. Let t be the image of x_j in N_3 for some j, let n be the image of x_h in N_3 for $h = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, and let s be the image of x_h in N_3 for $h = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Definition 5.5 shows that $\phi(x_j) = \lambda_j = (4, 1^{11})$. It follows from the proof of Theorem 4.15 that $\langle C, n \rangle = N_3$, that $\langle t, n \rangle = SL(2, 3)$, and that $\langle t, n, s \rangle = GL(2, 3)$. These facts show that N_3 satisfies (12). □

The uniqueness of N_7. The proof of uniqueness of N_7 is much the same as the proof of uniqueness of N_5. The major difference comes in showing that τ is trivial. In this case there is no nontrivial group S of automorphisms of $L(\mathscr{H})$ for which τ is an S-invariant map. In this case, we let $O_3(G)$ play the role that S played in showing that τ was trivial in the proof of Theorem 7.2. This is interesting in light of the remarks in §5 about "reappearing" automorphisms and the definition of N_7.

Let $\Lambda = \Lambda(\mathscr{H})$. Let N be a group with the following properties:

(13) N has a normal subgroup $V = \langle x, v \rangle$, and V is elementary abelian of order 7^2.

(14) $C = C_N(x)$ has a normal subgroup $Q \cong 7_+^{1+4}$, an extraspecial group of order 7^5 and exponent 7.

(15) $C/Q \cong 2 \times 7{:}3$ is isomorphic to the monomial subgroup $\overline{\mathrm{Mon}}(\Lambda) < 2A_7 < \mathrm{Aut}_{\mathbb{Z}[\varepsilon]}(\Lambda)$. There is a subgroup $D < N_N(\langle x \rangle)$ of index 2, with $D \cong Q{:}M$ and $M \cong \overline{\mathrm{Mon}}(\Lambda) : \langle \sigma_{-1} \rangle$.

(16) There is a homomorphism of M-modules $\phi : Q/Q' \to \Lambda/(\varepsilon - 1)\Lambda$, with $\phi(v) \equiv \lambda_b$. Also ϕ is an isometry, where the form on Q/Q' is given by the

commutator map and the form on $\Lambda/(\varepsilon - 1)\Lambda$ is as described in Lemma 5.5.

(17) There is an element $t \in Q$ with $\phi(t) \equiv (-2, 1, 1, 1)$ and an element $n \in N$ such that $N = \langle C, n\rangle$, $\langle t, n\rangle \cong SL(2, 7)$, and n has matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ in its action on V. Also, there is an element $s \in M$ of order 6 such that $\langle t, n, s\rangle \cong GL(2, 7)$.

Theorem 7.6. *There is at most one isomorphism class of groups satisfying properties* (13)–(17).

Proof. We let N and N_1 be two groups satisfying (13)–(17). As with the proof of Theorem 7.2, our strategy is to show that N and N_1 satisfy the hypotheses of the groups K and K_1 of Lemma 7.1 and deduce that $N \cong N_1$.

For each subgroup $G < N$ with properties as given in (13)–(17), let G_1 be the subgroup of N_1 with the same properties. Similarly for each element $g \in N$ with properties as given in (13)–(17), let g_1 be the element of N_1 with the same properties. By (14) we have $Q \cong Q_1$. By (15) and (16) we have $C \cong C_1$ and $D \cong D_1$.

We let $G = \langle t, s, n\rangle$ and $G_1 = \langle t_1, s_1, n_1\rangle$, so that $G \cong G_1 \cong GL(2, 7)$. Now let $E = C_N(V)$ and $E_1 = C_{N_1}(V_1)$, and since $E < D$ and $E_1 < D_1$, we get $E \cong E_1$.

To apply Lemma 7.1, we let N, N_1, E, E_1, $\langle s, t\rangle$, $\langle s_1, t_1\rangle$, n, and n_1 play the roles of K, K_1, H, H_1, B, B_1, n, and n_1, respectively, in Lemma 7.1. As in Theorem 7.2, our groups N and N_1 satisfy properties (i)–(iv) and all that we need to check is property (v).

Also as in the proof of Theorem 7.2, we identify E and E_1 and get $N_1 \cong E{:}G_1$. Then define $\gamma_1 : E{:}\langle n\rangle \to E{:}\langle n_1\rangle$ by $\gamma_1(en^k) = en_1^k$ for $e \in E$ and $k \in \mathbb{N}$. Since both n and n_1 have order 4, γ_1 is an isomorphism if n and n_1 induce the same automorphism of E.

We define $\gamma_1 : E{:}\langle n\rangle \to E{:}\langle n_1\rangle$ by $\gamma_1(en^k) = en_1^k$ for $p \in E$ and $k \in \mathbb{N}$. Since both n and n_1 have order 4, γ_1 is an isomorphism if n and n_1 induce the same automorphism of P.

Since $O_7(E)$ is characteristic in E and $E \triangleleft N$, it is contained in $O_7(N)$. Since $O_7(N/E) < O_7(GL(2, 7)) = 1$, we have $O_7(N) = O_7(E)$, and similarly $O_7(N_1) = O_7(E_1)$. We claim that $E \cong 7^{2+1+2}{:}3$. Let $P = O_7(E)$. Assumption (16) implies that $V = Z(E)$, and that P' has order 7^3. Then (14) and (16) imply that P' is elementary abelian of order 7^3, and (14) and (15) imply that P/P' is elementary abelian of order 7^2. Now (15) implies that $E = P \cdot S$ where S is cyclic of order 3, and this proves the claim.

Now P/P' is a 2-dimensional module for G and G_1, and $\langle\alpha\rangle = Z(G) = Z(G_1)$ acts faithfully and as a scalar on P/P'. Thus $P/P' \cong \sigma$, the natural module for $GL(2, 7)$. Now $\Lambda^2(\sigma)$ is easily shown to have irreducible constituents of dimension 3 and 1. Since $P'/Z(P)$ is a 1-dimensional module for $GL(2, 7)$, it must be isomorphic to the 1-dimensional irreducible submodule of $\Lambda^2(\sigma)$. Thus we have $P'/Z(P) \cong \delta$, where δ is the determinant of matrices in the natural representation of $GL(2, 7)$.

The argument to show that G and G_1 have exactly the same action on $P/Z(P)$ now proceeds exactly as in Theorem 7.2, so we omit it.

Now define homomorphisms $f : N \to \mathrm{Aut}(E)$ and $g : N_1 \to \mathrm{Aut}(E)$. We know that N and N_1 have the same action on $P/Z(P)$, so we will be done if we

can show that the map $\tau : P/Z(P) \to Z(P)$ defined by $(pZ(P))^\tau = p^{g(n_1)f(n^{-1})}$ is trivial. Let z_0 be the element of C which corresponds to an element of $GL(2, 7)$ with matrix $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ in its action on P/P'. Then z_0 is in the center of both G and G_1. Thus we have that τ is a $\langle z_0 \rangle$-invariant map from P to $Z(P)$. Now P/P' is isomorphic to the natural module for $GL(2, 7)$, and $P'/Z(P)$ is a 1-dimensional module which affords the linear character given by the determinant of matrices of elements acting on the natural module. Thus, since $Z(P) = [P, P']$, we have that $Z(P) < P/P' \otimes P'/Z(P)$ as a $GL(2, 7)$ module. But that means that z_0 acts trivially on $Z(P)$, while it acts nontrivially on P/P' and $P'/Z(P)$. Thus $\mathrm{Hom}_{\mathbb{F}_7\langle z_0 \rangle}(P/Z(P), Z(P)) = 0$, so τ is trivial. Thus n and n_1 induce the same automorphism of P, so γ_1 is an isomorphism, and thus Lemma 7.1 implies that $N \cong N_1$. □

Theorem 7.7. *The group N_7 satisfies* (13)–(17).

Proof. Let $V = \langle \infty_{\not\phi}, 0_{\not\phi} \rangle K/K$ and $x = \infty_{\not\phi}$, so $C = C_{N_7}(\infty_{\not\phi})$ and $D = \langle C, x_{-1} \rangle$. Theorem 4.15 implies that $V \triangleleft N_7$, so N_7 satisfies (13). Theorem 4.17 shows that $\overline{Q_\infty} \triangleleft C$, so N_7 satisfies (14).

Theorem 5.20 shows that $C/\overline{Q_\infty} \cong \overline{\mathrm{Mon}}(\Lambda)$. Let $M = \langle x_h, 0_f, x_{-1} \mid h = \left(\begin{smallmatrix} 2 & 0 \\ 0 & -2 \end{smallmatrix}\right), f = (0, b) \rangle K/K$, where b is the code word $(0, 1, 2, 4) \in \mathscr{H}$. Clearly $C = \langle \overline{Q_\infty}, M \rangle$. Lemma 4.16 implies that $0_f^{x_h} = 0^2_{f^\kappa(-4)} = 0_f^2$ and $0_f^{x_{-1}} = 0_{f^{-1}}$. Thus x_h and x_{-1} normalize $\langle 0_f \mid f = (0, b) \rangle$, and x_h^3 centralizes $\langle 0_f \mid f = (0, b) \rangle$. It is also clear that x_{-1} commutes with x_h. Lemma 5.11 shows that x_{-1} has the same action on $Q_\infty/Z(Q_\infty)$ as σ_{-1} has on $\Lambda/(\varepsilon - 1)\Lambda$. This shows that M is a complement to $\overline{Q_\infty}$ isomorphic to $\overline{\mathrm{Mon}}(\Lambda) : \langle \sigma_{-1} \rangle$, so N_7 satisfies (15).

Let ϕ be the map of Definition 5.5. Then $\phi(0_{\not\phi}^{-1}) = \lambda_b$, and Lemma 5.5 shows that ϕ is an isometry. Since $M < \overline{M_\infty}$, Theorem 5.14 shows that ϕ is an isomorphism of M-modules. Thus N_7 satisfies (16).

Now let t be the image of x_t in N_7, let n be the image of x_h in N_7 for $h = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, and let s be the image of x_h in N_7 for $h = \left(\begin{smallmatrix} 2 & 0 \\ 0 & -2 \end{smallmatrix}\right)$. Definition 5.5 shows that $\phi(x_t^3) = \lambda_t$. It follows from the proof of Theorem 4.15 that $\langle C, n \rangle = N_7$, that $\langle t, n \rangle = SL(2, 7)$, and that $\langle t, n, s \rangle = GL(2, 7)$. These facts show that N_7 satisfies (17). □

Subject Index

REFERENCES

1. H. F. Blichfeldt, *Finite collineation groups*, Univ. of Chicago Press, Chicago, IL, 1917.
2. R. H. Bruck, *A survey of binary systems*, Springer-Verlag, New York, Heidelberg, and Berlin, 1958.
3. J. H. Conway, *A simple construction for the Fischer–Griess Monster group*, Invent. Math. **79** (1985), 513–540.
4. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *ATLAS of finite groups*, Claredon Press, Oxford, 1985.
5. J. H. Conway and J. A. Sloane, *Sphere packings, lattices, and groups*, Springer-Verlag, New York, Heidelberg, and Berlin, 1988.
6. L. Finkelstein and A. Rudvalis, *Maximal subgroups of the Hall-Janko-Wales group*, J. Algebra **24** (1973), 486–493.
7. R. L. Griess, *Schur multipliers of some sporadic simple groups*, J. Algebra **32** (1974), 445–466.
8. ———, *The friendly giant*, Invent. Math. **62** (1982), 1–102.
9. ———, *The Monster and its non-associative algebra*, Proceedings of a Conference on Finite Groups (Montreal, 1985), pp. 121–157.
10. ———, *Code loops and a large finite group containing triality for* D_4, Atti Convegno Internazionale Teoria dei Gruppi e Geometria Combinatoria, Firenze, 1986, pp. 79–98.
11. ———, *Code loops*, J. Algebra **100** (1986), 224–234.
12. ———, *A Moufang loop, the exceptional Jordan algebra, and a cubic form in* 27 *variables*, J. Algebra **131** (1990), 281–293.
13. P. M. Johnson, *Loops of nilpotence class two*, preprint.
14. G. Karpilovsky, *The Schur multiplier*, Oxford Univ. Press, Oxford, 1986.
15. M. Kitazume, *Code loops and even codes over* $\mathbb{F}_4$, J. Algebra **118** (1988), 140–149.
16. J. H. Lindsey, *A correlation between* $PSU_4(3)$, *the Suzuki group, and the Conway group*, Trans. Amer. Math. Soc. **157** (1971), 189–204.
17. ———, *A new lattice for the Hall–Janko group*, Proc. Amer. Math. Soc. **103** (1988), 703–709.
18. J. van Lint, *An introduction to coding theory*, Springer-Verlag, New York, Heidelberg, and Berlin, 1982.
19. H. Maschke, Math. Ann. **51** (1899), 253–298.
20. J. G. Thompson, *Uniqueness of the Fischer–Griess Monster*, Bull. London Math. Soc. **11** (1979), 340–346.
21. J. Tits, *Quaternions over* $\mathbb{Q}(\sqrt{5})$, *Leech's lattice and the sporadic group of Hall–Janko*, J. Algebra **63** (1980), 56–75.
22. H. N. Ward, *A form for* M_{11}, J. Algebra **37** (1975), 340–351.
23. ———, *Combinatorial polarization*, Discrete Math. **26** (1979), 185–197.
24. R. A. Wilson, *Maximal subgroups of the Suzuki group*, J. Algebra **84** (1983),151–188.

DEPARTMENT OF MATHEMATICS AND STATISTICS, WESTERN MICHIGAN UNIVERSITY, KALAMAZOO, MICHIGAN 49008

E-mail address: thomas.m.richardson@wmich.edu