ON RANK-TWO COMPLEX REFLECTION GROUPS

PRAMOD N. ACHAR AND ANNE-MARIE AUBERT

ABSTRACT. We describe a class of groups with the property that the finite ones among them are precisely the complex reflection groups of rank two. This situation is reminiscent of Coxeter groups, among which the finite ones are precisely the real reflection groups. We also study braid relations between complex reflections and indicate connections to an axiomatic study of root systems and to the Shephard-Todd "collineation groups."

1. INTRODUCTION

A *complex reflection group* is a finite group of transformations of a complex vector space generated by *complex reflections* or *pseudo-reflections*, *i.e.,* transformations that fix some hyperplane. Any finite Coxeter group can naturally be thought of as a complex reflection group, simply by complexifying the vector space on which the reflection representation acts, but there are many complex reflection groups that do not arise in this way. Recent work by a number of people has shown that various structures attached to Weyl groups, can be generalized to complex reflection groups, even though there is no analogue of the underlying algebraic group.

Many aspects of the theory of finite Coxeter groups are actually present in the much broader setting of all Coxeter groups. Indeed, it should be remembered that the following characterization of reflection groups is a theorem, not a definition:

Theorem 1.1 (Coxeter)**.** *A group is a real reflection group if and only if it is finite and a Coxeter group. Moreover, for such a group, the Coxeter presentation is uniquely determined.*

Philosophically, we might even say that most features of the theory of real reflection groups (length functions, Bruhat order, deletion and exchange conditions, *etc.*) are *primarily* features of the theory of Coxeter groups, and that the remarkable theorem above allows these features to be applied to real reflection groups.

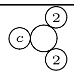
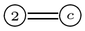
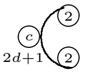
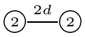
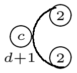
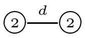
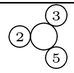
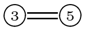
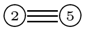
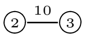
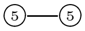
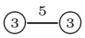
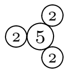
In this paper, we seek a characterization in the spirit of Theorem 1.1 of complex reflection groups of rank two. Of course, these groups have been known since the classification by Shephard and Todd [9] of all complex reflection groups, but a suitable general setting in which to study these groups, in the spirit of Theorem 1.1, is not known.

Given three positive integers a, b, and c, let us define a group

$$J\left(\begin{smallmatrix} a & b & c \\ 1 & 1 & 1 \end{smallmatrix}\right) = \langle s, t, u \mid s^a = t^b = u^c = 1,\ stu = tus = ust \rangle. \tag{1}$$

Next, let a', b', and c' be three pairwise relatively prime positive integers that divide a, b, and c, respectively. We define

$$J\left(\begin{smallmatrix} a & b & c \\ a' & b' & c' \end{smallmatrix}\right) = \begin{array}{c}\text{the smallest normal subgroup of } J\left(\begin{smallmatrix} a & b & c \\ 1 & 1 & 1 \end{smallmatrix}\right) \\ \text{containing } s^{a'},\ t^{b'}, \text{ and } u^{c'}.\end{array} \tag{2}$$

J	BMR	ST	Triples
$J\left(\begin{smallmatrix} 2 & 2 & c \\ & & \end{smallmatrix}\right)$		$G(2c,2,2)$	
$J\left(\begin{smallmatrix} 2 & 2 & c \\ 2 & & \end{smallmatrix}\right)$		$G(c,1,2)$	$(2,c,4)$
$J\left(\begin{smallmatrix} 2 & 2 & cd \\ & & d \end{smallmatrix}\right)$		$G(2cd,2d,2)$	
$J\left(\begin{smallmatrix} 2 & 2 & d \\ & & d \end{smallmatrix}\right)$		$G(2d,2d,2)$	$(2,2,2d)$
$J\left(\begin{smallmatrix} 2 & 2 & cd \\ 2 & & d \end{smallmatrix}\right)$		$G(cd,d,2)$	
$J\left(\begin{smallmatrix} 2 & 2 & d \\ 2 & & d \end{smallmatrix}\right)$		$G(d,d,2)$	$(2,2,d)$
$J\left(\begin{smallmatrix} 2 & 3 & 5 \\ & & \end{smallmatrix}\right)$		G_{19}	
$J\left(\begin{smallmatrix} 2 & 3 & 5 \\ 2 & & \end{smallmatrix}\right)$		G_{18}	$(3,5,4),(3,5,6),(3,5,10)$
$J\left(\begin{smallmatrix} 2 & 3 & 5 \\ & 3 & \end{smallmatrix}\right)$		G_{17}	$(2,5,6),(2,5,10)$
$J\left(\begin{smallmatrix} 2 & 3 & 5 \\ & & 5 \end{smallmatrix}\right)$		G_{21}	$(2,3,10)$
$J\left(\begin{smallmatrix} 2 & 3 & 5 \\ 2 & 3 & \end{smallmatrix}\right)$		G_{16}	$(5,5,3),(5,5,5)$
$J\left(\begin{smallmatrix} 2 & 3 & 5 \\ 2 & & 5 \end{smallmatrix}\right)$		G_{20}	$(3,3,5)$
$J\left(\begin{smallmatrix} 2 & 3 & 5 \\ & 3 & 5 \end{smallmatrix}\right)$		G_{22}	

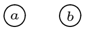
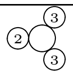
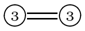
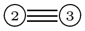
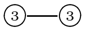
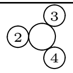
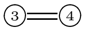
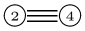
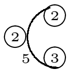
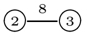
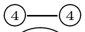
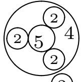
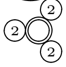
J	BMR	ST	Triples
$J\left(\begin{smallmatrix} 1 & a & b \\ & & \end{smallmatrix}\right)$			$(a,b,2)$
$J\left(\begin{smallmatrix} 2 & 3 & 3 \\ & & \end{smallmatrix}\right)$		G_7	
$J\left(\begin{smallmatrix} 2 & 3 & 3 \\ 2 & & \end{smallmatrix}\right)$		G_5	$(3,3,4)$
$J\left(\begin{smallmatrix} 2 & 3 & 3 \\ & 3 & \end{smallmatrix}\right)$		G_6	$(2,3,6)$
$J\left(\begin{smallmatrix} 2 & 3 & 3 \\ 2 & 3 & \end{smallmatrix}\right)$		G_4	$(3,3,3)$
$J\left(\begin{smallmatrix} 2 & 3 & 4 \\ & & \end{smallmatrix}\right)$		G_{11}	
$J\left(\begin{smallmatrix} 2 & 3 & 4 \\ 2 & & \end{smallmatrix}\right)$		G_{10}	$(3,4,4)$
$J\left(\begin{smallmatrix} 2 & 3 & 4 \\ & 3 & \end{smallmatrix}\right)$		G_9	$(2,4,6)$
$J\left(\begin{smallmatrix} 2 & 3 & 4 \\ & & 2 \end{smallmatrix}\right)$		G_{15}	
$J\left(\begin{smallmatrix} 2 & 3 & 4 \\ & & 4 \end{smallmatrix}\right)$		G_{14}	$(2,3,8)$
$J\left(\begin{smallmatrix} 2 & 3 & 4 \\ 2 & 3 & \end{smallmatrix}\right)$		G_8	$(4,4,3)$
$J\left(\begin{smallmatrix} 2 & 3 & 4 \\ & 3 & 2 \end{smallmatrix}\right)$		G_{13}	
$J\left(\begin{smallmatrix} 2 & 3 & 4 \\ & 3 & 4 \end{smallmatrix}\right)$		G_{12}	

Table 1. The complex reflection groups of rank 2.

(The relative primality assumption is required for the uniqueness part of the theorem below.) These groups will be referred to colloquially throughout the paper as "J-groups." We usually omit 1's from the second row of parameters. The main result of the paper is the following:

Theorem 1.2. *A group is a complex reflection group of rank two if and only if it is a finite J-group. Moreover, for such a group, the parameters a, b, c, a', b', and c' are uniquely determined up to permutation.*

All the rank-two complex reflection groups are listed in Table 1. For each group, we identify the corresponding finite J-group; we give the Broué-Malle-Rouquier (BMR) presentation from [4]; and we give the Shephard-Todd (ST) designation from [9]. In the last column, we list the associated admissible triples (see Section 3).

Of course, this theorem is interesting only if there are important facts about rank-two complex reflection groups whose proofs can be carried out in the setting of J-groups. As a step in this direction, in a forthcoming paper [1], the authors hope to show how to associate a "Hecke-like" algebra to each J-group (and, indeed, to a much larger class of groups as well) that (i) is a free module over a suitable ring of Laurent polynomials, (ii) admits a natural basis indexed by elements of the J-group, and (iii) has a specialization isomorphic to the group algebra of the J-group, in which the aforementioned natural basis becomes the natural basis of the group algebra.

A broad outline of the proof is as follows: after laying some groundwork in Section 2, we introduce and study "admissible triples" in Section 3. These are ordered triples of integers (a,b,l) that are attached to pairs of reflections that generate a finite group. In Section 4, we show that finding the finite J-groups is equivalent to classifying those admissible triples (a, b, l) in which l is even. Finally, in Sections 5 and 6, we actually classify all admissible triples. (Admissible triples have previously been defined and classified by Hughes and Morris [6], but there seems to be a gap in their work: see Remark 3.18.)

The full classification of admissible triples is more information than we need in order to prove Theorem 1.2, but it finds application in Section 7, where we use it to investigate root systems for complex reflection groups, following a definition recently proposed by Nebe [8] (*cf.* Cohen's work [5] on a different notion of root system in rank at least 3).

Finally, recall that the method of the original Shephard-Todd classification gave a natural arrangement of the exceptional groups (*i.e.,* those not in the infinite series $G(r, p, n)$) into families. Remarkably, for rank-two groups, these Shephard-Todd families coincide with the grouping in Table 1 by J-group parameters. We conclude the paper in Section 8 with an explanation for this phenomenon.

It should be stressed that hardly any of the facts about complex reflection groups that are proved in this paper are new. Rather, it is the methods of proof and the perspective of having J-groups in mind that hold interest. Indeed, it is expected that with a more-developed theory of these groups, it should be possible to give a proof of Theorem 1.2 that is independent of the classification of complex reflections groups. That is not achieved in this paper, but an attempt has nevertheless been made to keep references to the classification to a minimum: specifically, we only refer to the presentations given in [4] to make the identifications listed in Table 1, and to establish the uniqueness asserted in Theorem 1.2.

We would like to thank M. Broué and R. Pollack for helpful conversations.

2. Hermitian Spaces over Number Fields

According to, *e.g.,* [2, Propositon 7.1.1], every complex reflection group can actually be realized as a reflection group over some finite abelian extension of $\mathbb{Q}$. That is the context in which we will work. Throughout the paper, K will denote such a field, and V will be a K-vector space (usually 2-dimensional). $\mathbb{Z}_K$ will denote the ring of algebraic integers in K, and μ_K will denote the group of roots of unity of K. We also fix a generator η of μ_K, and we write m for the order of μ_K. Any abelian number field has a unique automorphism $^-\colon K \to K$ that extends to complex conjugation on $\mathbb{C}$ under any imbedding $K \hookrightarrow \mathbb{C}$. The existence of such a map means that we can speak of "Hermitian forms" on K-vector spaces. We adopt the convention that Hermitian forms are conjugate-linear in the first variable and linear in the second.

Definition 2.1. A Hermitian form on a K-vector space V is said to be *definite* if, for every imbedding $K \hookrightarrow \mathbb{C}$, the corresponding induced form on $V_{\mathbb{C}} = V \otimes_K \mathbb{C}$ is definite (*i.e.,* either positive definite or negative definite).

Remark 2.2. In general, even a definite Hermitian form cannot be described as being "positive" or "negative" definite without fixing an imbedding of K into $\mathbb{C}$. For example, take $K = \mathbb{Q}(\sqrt{2})$, and let $(,)$ be the form on K^2 corresponding to the quadratic form $\sqrt{2}x^2 + \sqrt{2}y^2$. It is clear that this form induces a positive definite form on $\mathbb{C}^2$ under one imbedding $K \hookrightarrow \mathbb{C}$, and a negative definite form under the other one.

Also, over $\mathbb{C}$, definiteness of a Hermitian form is equivalent to the condition that $(x,x) \neq 0$ for all nonzero x, but this equivalence does not hold in general over number fields. Again for $K = \mathbb{Q}(\sqrt{2})$, consider the form corresponding to the quadratic form $x^2 + \sqrt{2}y^2$. Under the imbedding which sends $\sqrt{2}$ to a negative real number, this form induces an indefinite form on $\mathbb{C}^2$: indeed, $v = (2^{1/4}, 1) \in \mathbb{C}^2$ is a vector satisfying $(v,v) = 0$. However, there are no vectors in K^2 satisfying that equation.

The following criterion for deciding whether a given form is definite will play a central role in the classification of admissible triples.

Lemma 2.3. *Let $\{x,y\}$ be a basis for a 2-dimensional K-vector space V, endowed with a nondegenerate Hermitian form $(,)$. Assume that (x,x) and (y,y) are both nonzero. Then the form $(,)$ is definite if and only if the inequalities*

$$0 < \frac{(x,y)(y,x)}{(x,x)(y,y)} < 1 \tag{3}$$

hold under every imbedding of K into $\mathbb{C}$.

Proof. With respect to a given imbedding of K into $\mathbb{C}$, the form $(,)$ is positive (resp. negative) definite if and only if the matrix

$$B = \begin{pmatrix} (x,x) & (x,y) \\ (y,x) & (y,y) \end{pmatrix}$$

is positive (resp. negative) definite. Now, B is positive definite if

$$(x,x) > 0 \qquad \text{and} \qquad \det B = (x,x)(y,y) - (x,y)(y,x) > 0. \tag{4}$$

Since (x,y) and (y,x) are complex conjugates of one another, the product $(x,y)(y,x)$ is necessarily a positive real number. Using this observation, it is readily verified that the conditions in (4) imply the inequalities in (3). Similarly, if B is negative definite, then $(x,x) < 0$ and $\det B > 0$, and again one can deduce (3).

Conversely, if (3) holds, then, since $(x,y)(y,x)$ is positive, we see immediately that $(x,x)(y,y) > (x,y)(y,x) > 0$. Therefore, $\det B > 0$, so B must be either positive definite or negative definite. □

We will also require the following elementary result:

Lemma 2.4. *If G is a finite group acting on a K-vector space V, then there is a definite nondegenerate G-invariant Hermitian form on V. If the G-action is irreducible, then in fact every G-invariant Hermitian form on V is a scalar multiple of that one (and therefore either nondegenerate and definite, or zero).*

The proof of this fact (which we omit) employs the usual "unitary trick," and, for the second part, Schur's lemma, but a little extra care is required because the meaning of "definite" over K is subtler than it is over $\mathbb{C}$.

Finally, we require a criterion for deciding whether certain matrix groups over K are finite. Recall that there is a one-to-one correspondence between $n \times n$ Hermitian matrices over K and Hermitian forms on K^n: if B is a Hermitian matrix, we denote the corresponding form by $(,)_B$. We say that a Hermitian matrix B is *definite* if the form $(,)_B$ is (equivalently, if every imbedding $K \hookrightarrow \mathbb{C}$ sends B to a definite complex matrix).

We write $U_n(\mathbb{Z}_K, B)$ for the group of $n \times n$ invertible matrices with entries in $\mathbb{Z}_K$ that preserve B.

Proposition 2.5. *Let B be a nonzero $n \times n$ Hermitian matrix, and let $G \subset U_n(\mathbb{Z}_K, B)$ be a group that acts irreducibly on K^n. G is finite if and only if B is definite.*

Proof. If G is finite, the definiteness of B is a consequence of Lemma 2.4. Conversely, suppose that B is definite.

For any $A \in U_n(\mathbb{Z}_K, B)$, note that the characteristic polynomial of A is a monic polynomial of degree n with coefficients in $\mathbb{Z}_K$. It follows that the eigenvalues of A are algebraic integers of degree at most n over K. Let K_0 be the maximal totally real subfield of K, and let L be the smallest Galois extension of K_0 containing both K and the splitting field of the characteristic polynomial of A. Since the complex conjugation map $^-\colon K \to K$ may be regarded as an element of $\mathrm{Gal}(K/K_0)$, it can be extended to an automorphism $^-\colon L \to L$.

We can therefore regard B as a Hermitian matrix over L, and $(,)_B$ as a Hermitian form on L^n. Now, if λ is an eigenvalue of A, and $x \in L^n$ is a corresponding eigenvector, we have

$$(x, x)_B = (Ax, Ax)_B = (\lambda x, \lambda x)_B = \lambda\bar{\lambda}(x, x)_B.$$

Since B is definite, $(x, x)_B$ is nonzero, so we see that $\lambda\bar{\lambda} = 1$.

Next, since K is a Galois extension of $\mathbb{Q}$, the restriction of any automorphism $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ to K is an automorphism of K. In particular, B^σ is a Hermitian matrix with coefficients in K, A^σ is an element of $U_n(\mathbb{Z}_K, B^\sigma)$, and λ^σ is an eigenvalue of A^σ. By the argument given above, we again have $\lambda^\sigma \overline{\lambda^\sigma} = 1$. In other words, λ is an algebraic integer all of whose conjugates over $\mathbb{Q}$ have complex absolute value 1. It is an elementary fact that any such element is a root of unity.

Finally, we note that there are only finitely many roots of unity of degree at most n over K, so the set Λ of all eigenvalues of elements of $U_n(\mathbb{Z}_K, B)$ must be finite. As a result, the image of the trace map $\mathrm{tr} : U_n(\mathbb{Z}_K, B) \to K$ must also be finite. Let T denote this image.

For the remainder of the proof, we fix an imbedding $K \hookrightarrow \mathbb{C}$. With respect to this imbedding, we regard B as a complex Hermitian matrix, and we regard $U_n(\mathbb{Z}_K, B)$ as a subgroup of the Lie group $U_n(\mathbb{C}, B)$ of complex matrices preserving B. Now, the identity matrix is the unique element of $U_n(\mathbb{Z}_K, B)$, and indeed of $U_n(\mathbb{C}, B)$, that has trace n. Consider the open set

$$V = \mathbb{C} \smallsetminus (T \smallsetminus \{n\}).$$

We see that $\mathrm{tr}^{-1}(V)$ is an open subset of $U_n(\mathbb{C}, B)$ that contains no elements of $U_n(\mathbb{Z}_K, B)$ other than the identity matrix. Therefore, $U_n(\mathbb{Z}_K, B)$ is a discrete subgroup of $U_n(\mathbb{C}, B)$. Now, since B is positive definite, $U_n(\mathbb{C}, B)$ is compact, so it follows that $U_n(\mathbb{Z}_K, B)$ is finite, as is its subgroup G. □

3. Admissible Triples and Hughes-Morris Polynomials

In this section, we investigate pairs of reflections in K-vector spaces. To review, recall that just as over $\mathbb{C}$, a *reflection* is any finite-order linear transformation of a vector space that fixes a hyperplane (called its *reflecting hyperplane*). Such a map always has a one-dimensional eigenspace, complementary to its reflecting hyperplane, on which it acts by a root of unity. We call this eigenspace the *root line* of the reflection, and we call any nonzero point on the line a *root.* (This last definition will be replaced by a more specific notion when we come to root systems in Section 7.) Finally, we recall that two reflections s and t are said to satisfy a *braid relation of length l* if

$$\underbrace{sts\cdots}_{l\text{ factors}} = \underbrace{tst\cdots}_{l\text{ factors}}.$$

We also introduce the following new terminology:

Definition 3.1. (1) A reflection of order a is said to be *elementary* if its nontrivial eigenvalue is $\eta^{m/a}$.

(2) A triple of positive integers (a, b, l), where $a \le b$, is called an *admissible triple* if there exist elementary reflections s and t of some K-vector space, of orders a and b respectively, that generate a finite group, and if l is the length of the shortest braid relation they satisfy.

Of course, any reflection has a power that is an elementary reflection of the same order. It is clear that any reflection group may be assumed to be generated by elementary reflections.

In this section, we develop the tools necessary to classify all admissible triples, and at the end of the section, we state the classification theorem. The actual work of classifying them will be done in Sections 5 and 6.

The notion of "admissible triple" that we use here is closely related to that introduced by Hughes and Morris [6]. That paper also provides a classification of admissible triples, but there appears to be a gap in their work: they assert that admissible triples are in bijection with isomorphism classes of complex reflection groups generated by two reflections, but this is not borne out by our Theorem 3.14. The precise nature of the discrepancy is explained in Remark 3.18. Nevertheless, their paper contains some valuable ideas. The main tool of this section, the Hughes-Morris polynomials to be defined below, are taken directly from their work. In addition, the application of admissible triples to Nebe root systems in Section 7 is inspired by their use of admissible triples to study root systems in the sense of Cohen [5].

The easiest example of an admissible triple arises when the two reflections have orthogonal root lines (with respect to some definite Hermitian form invariant under the group generated by the two reflections). In this case, the root line of each reflection lies in the reflecting hyperplane of the other, so it is evident that the two reflections commute. That is, they satisfy a braid relation of length 2. We can construct such commuting reflections of any orders whatsoever, so every triple $(a, b, 2)$ with $2 \le a \le b$ is admissible.

The problem, then, is to understand admissible triples (a, b, l) with $l \ge 3$. Our main tool will be a certain family of polynomials whose roots govern braid relations of reflections. Throughout, V will be a 2-dimensional K-vector space, and s and t will be elementary reflections of V whose root lines neither coincide nor are orthogonal. It follows that neither s nor t preserves the other's eigenspaces. Therefore, the group W generated by s and t acts irreducibly on V.

We do not assume that W is finite, but we do assume that s and t satisfy some braid relation. We also assume that V is endowed with a W-invariant Hermitian form $(,)$, with the additonal property that (α, α) and (β, β) are both nonzero, where α and β are roots for s and t, respectively. By the irreducibility of V as a W-representation, this form is unique up to scalar multiple. (If W happens to be finite, Lemma 2.4 both guarantees the existence of such a form and tells us that it is definite.)

Let a and b be the orders of s and t, respectively, and let $\omega = \eta^{m/a}$ and $\xi = \eta^{m/b}$ be their respective nontrivial eigenvalues. Since s and t both preserve $(,)$, we can give formulas for their action on V as follows:

$$s(x) = x - (1-\omega)(\alpha,\alpha)^{-1}(\alpha,x)\alpha$$
$$t(x) = x - (1-\xi)(\beta,\beta)^{-1}(\beta,x)\beta$$

Let us define $\alpha^\vee = \overline{(1-\omega)(\alpha,\alpha)^{-1}}\alpha$ and $\beta^\vee = \overline{(1-\xi)(\beta,\beta)^{-1}}\beta$, so the preceding formulas become

$$s(x) = x - (\alpha^\vee, x)\alpha, \qquad t(x) = x - (\beta^\vee, x)\beta.$$

Next, we define

$$N = N_{s,t} = (\alpha^\vee,\beta)(\beta^\vee,\alpha).$$

(The notation is evidently reminiscent of that used for roots and coroots when studying Weyl groups; this analogy will be fully developed in Section 7.) Note that since we have assumed that $(\alpha,\beta) \neq 0$, it is necessarily the case that $N \neq 0$.

It turns out that the quantity N, the order of the braid relation of s and t, and the fact that these reflections generate a finite group are all intimately related. To explicate this relationship, we introduce a family of polynomials associated to the pair s, t, called *Hughes-Morris polynomials*, as follows:

$$f_0(x) = 0 \qquad f_{2k}(x) = f_{2k-1}(x) + \xi f_{2k-2}(x) \tag{5}$$
$$f_1(x) = 1 \qquad f_{2k+1}(x) = x f_{2k}(x) + \omega f_{2k-1}(x) \tag{6}$$

In this section, we will show how these polynomials can be used to study the action of st on V, and to pin down the value of $N_{s,t}$. (This is not quite the definition used in Hughes-Morris' paper [6]. If we denote the polynomials of [6] by f_k^{HM}, then the relationship is

$$f_k(x) = (1-\omega)^k(1-\xi)^k f_k^{HM}((1-\omega)^{-1}(1-\xi)^{-1}x).$$

The definition we have given here will be more convenient for the calculations we will carry out.)

Lemma 3.2. *We have the following relations:*

$$(st)^k\alpha = f_{2k+1}(N)\alpha - (\beta^\vee,\alpha)f_{2k}(N)\beta$$
$$t(st)^k\alpha = f_{2k+1}(N)\alpha - (\beta^\vee,\alpha)f_{2k+2}(N)\beta$$

Lemma 3.3. *If $k \geq 4$, then $f_k(x) = (x+\omega+\xi)f_{k-2}(x) - \omega\xi f_{k-4}(x)$.*

The next lemma partly describes the relationship between Hughes-Morris polynomials and braid relations.

Lemma 3.4. *If s and t satisfy a braid relation of length l, then $f_l(N) = 0$.*

Proof. If l is even, then $(st)^{l/2} = t(st)^{l/2-1}s$. From Lemma 3.2, we have

$$(st)^{l/2}\alpha = f_{l+1}(N)\alpha - (\beta^\vee,\alpha)f_l(N)\beta,$$
$$t(st)^{l/2-1}s\alpha = t(st)^{l/2-1}\omega\alpha = \omega f_{l-1}(N)\alpha - \omega(\beta^\vee,\alpha)f_l(N)\beta.$$

This implies that $f_l(N) = \omega f_l(N)$, and therefore that $f_l(N) = 0$. A similar calculation yields the same result if l is odd. □

Conversely, it is also true that if $f_l(N) = 0$, then s and t satisfy a braid relation of length l. Before proving that, however, we need a description of the solutions of $f_k(x) = 0$.

Lemma 3.5. *Suppose that K contains a square root z of $\omega\xi$, and let ζ be a root of unity other than ± 1. We have*

$$\begin{aligned} f_{2k}(z(\zeta+\zeta^{-1}) - \omega - \xi) &= z^{k-1}\frac{\zeta^k - \zeta^{-k}}{\zeta - \zeta^{-1}}, \\ f_{2k+1}(z(\zeta+\zeta^{-1}) - \omega - \xi) &= z^k \frac{(\zeta^{k+1} - \zeta^{-k-1}) - z\omega^{-1}(\zeta^k - \zeta^{-k})}{\zeta - \zeta^{-1}}. \end{aligned}$$

Proof. This is an elementary exercise in proof by induction: it is simply necessary to verify that these formulas satisfy the recurrence relations of (5). We omit the details. □

Corollary 3.6. *Let $k \geq 3$. Suppose that K contains a square root z of $\omega\xi$, as well as all the kth roots of unity. Then K contains the splitting field of $f_k(x)$. If k is even, the solutions of the equation $f_k(x) = 0$ are exactly the elements of*

$$\{z(\zeta + \zeta^{-1}) - \omega - \xi \mid \zeta^k = 1,\ \zeta \neq \pm 1\},$$

each with multiplicity 1. If k is odd and we also assume that $\omega = \xi$, then the solutions of $f_k(x) = 0$ are

$$\{-\omega(\zeta + \zeta^{-1}) - 2\omega \mid \zeta^k = 1,\ \zeta \neq \pm 1\},$$

each with multiplicity 1.

Remark 3.7. At first glance, it seems that if k is even and if we replace z by $-z$, *i.e.,* if we choose the other square root of $\omega\xi$, then we must also replace each ζ by $-\zeta$ in order for the above formula for the solutions of $f_k(x) = 0$ to hold. But $\zeta^k = 1$ if and only if $(-\zeta)^k = 1$, so in fact the set of solutions described above is independent of the choice of z.

Proof of Corollary 3.6. We quickly verify that each element of the form described is indeed a solution of $f_k(x) = 0$, by glancing at the formulas of Lemma 3.5. Now, if k is even, we have found $k/2 - 1$ distinct solutions, and if k is odd, we have found $(k-1)/2$ of them. But it follows from (5) that $f_k(x)$ has degree $k/2 - 1$ if k is even, and degree $(k-1)/2$ if k is odd. Therefore, the above solutions must be all the solutions of $f_k(x) = 0$, and they must each occur with multiplicity 1. □

Proposition 3.8. *The shortest braid relation satisfied by s and t has length l if and only if l is the smallest positive integer such that $f_l(N) = 0$.*

Proof. One direction of this statement is given by Lemma 3.4. For the other direction, we must show that if $f_l(N) = 0$, then in fact s and t satisfy a braid relation of length l.

Let $\{f'_k(x)\}$ be the family of Hughes-Morris polynomials in which we exchange the roles of s and t, and therefore also α and β, as well as ω and ξ. Now, the formulas in Corollary 3.6 are invariant under exchange of ω and ξ, so we see that if k is even, or if $\omega = \xi$, then the set of solutions of $f_l(x) = 0$ coincides with that of $f'_l(x) = 0$.

Now, suppose l is even and $f_l(N) = 0$. By Lemma 3.2, we have

$$(st)^{l/2}\alpha = f_{l+1}(N)\alpha,$$
$$t(st)^{l/2-1}s\alpha = \omega f_{l-1}(N)\alpha.$$

From (5), we know that in fact $f_{l+1}(N) = Nf_l(N) + \omega f_{l-1}(N) = \omega f_{l-1}(N)$, so it follows that $(st)^{l/2}\alpha = (ts)^{l/2}\alpha$. Similar reasoning using the polynomials $\{f'_k(x)\}$, and in particular the fact that $f'_l(N) = 0$, shows that $(ts)^{l/2}\beta = (st)^{l/2}\beta$ as well. Since $(st)^{l/2}$ and $(ts)^{l/2}$ agree on a basis of V, we conclude that $(st)^{l/2} = (ts)^{l/2}$, or

$$\underbrace{sts\cdots}_{l \text{ factors}} = \underbrace{tst\cdots}_{l \text{ factors}}.$$

A similar argument can be carried out if l is odd. □

The following result gives an explicit description of $N_{s,t}$.

Proposition 3.9. *Suppose that K contains the square roots of $\omega\xi$. If l is the order of the braid relation of s and t, then $N_{s,t}$ is of the form*

$$z(\zeta + \zeta^{-1}) - \omega - \xi, \tag{7}$$

where z is a certain square root of $\omega\xi$, and ζ is a primitive lth root of unity. Moreover, if we have either $a = b$ or $l \not\equiv 2 \pmod 4$, then it can be assumed that $z = -\eta^{m(a+b)/2ab}$.

In particular, $N_{s,t}$ is always an algebraic integer.

Proof. For now, let us fix $z = -\eta^{m(a+b)/2ab}$. Note that this gives $z = -\omega$ if $a = b$. From Lemma 3.4, we know that $f_l(N) = 0$, so by Corollary 3.6, N must be of the form $z(\zeta + \zeta^{-1}) - \omega - \xi$ with ζ an lth root of unity. To make a stronger statement about ζ, we consider the various cases separately. Suppose that ζ is a primitive kth root of unity, where $k \mid l$.

If $l \equiv 0 \pmod 4$ and $k < l$, and if in addition k is even, it follows from Corollary 3.6 that $f_k(N) = 0$, in contradiction with Proposition 3.8. If k is odd, the facts that $k \mid l$ and $4 \mid l$ imply that $2k \mid l$. Since $\zeta^{2k} = 1$, we have $f_{2k}(N) = 0$, and since $2k < l$, we again have a contradiction.

If $a = b$ and $k < l$, then again we find that $f_k(N) = 0$ (this time without regard to the parity of k), and again Proposition 3.8 gives a contradiction.

Finally, if $a \neq b$ and $l \equiv 2 \pmod 4$, and if $k < l/2$, then $2k < l$, and once again, we have $f_{2k}(N) = 0$, giving a contradiction. Since $k \mid l$, the only remaining possibilities are $k = l$ or $k = l/2$. If $k = l/2$, note that $-\zeta$ is a primitive lth root of unity. In this one case, we can repair the situation by replacing both z and ζ by their negatives. □

The fact that $N_{s,t}$ is always an integer has strong implications:

Proposition 3.10. *Under a suitable identification $V \simeq K^2$, the W-invariant form on V arises from a Hermitian matrix B, and W is identified with a subgroup of $U_2(\mathbb{Z}_K, B)$.*

Proof. We retain the notation of Section 3. With respect to the basis $\{\alpha, \beta\}$ for V, s and t act by the matrices

$$S = \begin{pmatrix} \omega & -(\alpha^\vee, \beta) \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad T = \begin{pmatrix} \omega & 0 \\ -(\beta^\vee, \alpha) & 1 \end{pmatrix}.$$

Now, if we replace α by a scalar multiple of itself, then we would change both $(\alpha^\vee, \beta)$ and $(\beta^\vee, \alpha)$, but not $N_{s,t}$. Indeed, $(\alpha^\vee, \beta)$ and $(\beta^\vee, \alpha)$ can be made to equal any two elements of K whatsoever whose product is N.

In particular, by choosing a suitable scalar multiple, we may assume that $(\alpha^\vee, \beta)$ is an algebraic integer that divides N. Then $(\beta^\vee, \alpha) = N/(\alpha^\vee, \beta)$ is also an algebraic integer, and the matrices S and T above have entries not just in K, but in $\mathbb{Z}_K$.

The W-invariant form arises from the Hermitian matrix

$$B = \begin{pmatrix} (\alpha, \alpha) & (\alpha, \beta) \\ (\beta, \alpha) & (\alpha, \alpha) \end{pmatrix}.$$

Thus, we have identified W with a subgroup of $U_2(\mathbb{Z}_K, B)$. □

Combining this result with Lemma 2.3 and Proposition 2.5, we obtain the following criterion for admissibility as an immediate corollary:

Proposition 3.11. *Let $\omega = \eta^{m/a}$ and $\xi = \eta^{m/b}$.*

(1) *A triple (a, b, l) is admissible if and only if, for some square root z of $\omega\xi$ and some primitive lth root of unity ζ, we have*

$$0 < \frac{\zeta + \zeta^{-1} - y - y^{-1}}{z + z^{-1} - y - y^{-1}} < 1 \tag{8}$$

under every imbedding of K into $\mathbb{C}$. (Here $y = \omega/z = z/\xi$.)

(2) *Suppose that either $a = b$ or $l \not\equiv 2 \pmod 4$, and let $z = -\eta^{m(a+b)/2ab}$. Then (a, b, l) is admissible if and only if, for some primitive lth root of unity ζ, the inequalities (8) hold under every imbedding $K \hookrightarrow \mathbb{C}$.*

In practice, for explicit calculations, it is more convenient to have the preceding proposition expressed in terms of conjugates of complex numbers rather than in terms of field imbeddings into $\mathbb{C}$. We therefore restate it for use in Sections 5 and 6 as follows:

Corollary 3.12. (1) *A triple (a, b, l) is admissible if and only if there is a square root z of $e^{\pi i(a+b)/ab}$ and a primitive lth root of unity ζ such that either*

$$(z+z^{-1})^\sigma < (\zeta+\zeta^{-1})^\sigma < (y+y^{-1})^\sigma \quad \text{or} \quad (y+y^{-1})^\sigma < (\zeta+\zeta^{-1})^\sigma < (z+z^{-1})^\sigma \tag{9}$$

for every automorphism $\sigma \in \operatorname{Gal}(\mathbb{Q}(z, y, \zeta)/\mathbb{Q})$. (Here $y = e^{2\pi i/a}/z = z/e^{2\pi i/b}$.

(2) *Suppose that either $a = b$ or $l \not\equiv 2 \pmod 4$, and let $z = -e^{\pi i(a+b)/ab}$. Then (a, b, l) is admissible if and only if, for some primitive lth root of unity ζ, the inequalities (9) hold for every $\sigma \in \operatorname{Gal}(\mathbb{Q}(z, y, \zeta)/\mathbb{Q})$.*

The preceding criteria impose no restrictions whatsoever on which primitive lth root of unity ζ may be, but it turns out that in many cases we can make a particularly simple choice:

Definition 3.13. An admissible triple is said to be *preferred* if, in the situation of Proposition 3.11, the inequalities (8) are satisfied with $\zeta = \eta^{m/l}$, or, equivalently, if the inequalities (9) of Corollary 3.12 are satisfied with $\zeta = e^{2\pi i/l}$.

As we will see below, preferred triples play a special role in the classification.

Theorem 3.14. *The admissible triples fall into three infinite families*

$$\begin{array}{ccc} (a,b,2) & (2,2,l) & (2,b,4) \\ a,b \geq 2 & l \geq 3 & b \geq 3 \end{array}$$

and the following seventeen exceptional cases:

$$\begin{array}{llllll} (3,3,3) & (3,3,4) & (3,3,5) & (2,3,6) & (2,3,8) & (2,3,10) \\ (4,4,3) & (3,4,4) & (5,5,5)^* & (2,4,6) & (3,4,8)^* & (2,5,10)^* \\ (5,5,3) & (3,5,4) & & (2,5,6) & & (3,5,10)^* \\ & & & (3,5,6)^* & & \end{array}$$

Those triples marked with an asterisk are not preferred.

Proof. Direct calculations (which we omit) of the inequalities in Corollary 3.12 can be used to demonstrate the admissibility of each of these triples. Theorem 5.8, to be established in Section 5, asserts that there are no other admissible triples of the form (a, a, l), while Theorem 6.17, which we prove in Section 6, states that there are no other admissible triples of the form (a, b, l) with $a \neq b$. □

Finally, we briefly discuss the relationship between admissible triples and the classification of complex reflection groups. Let $\{s, t\}$ and $\{u, v\}$ be two pairs of elementary K-reflections. If both pairs give rise to the same admissible triple, then the group generated by s and t must be isomorphic to that generated by u and v, since Proposition 3.10 gives explicit realizations of both as matrix groups. But if they give rise to distinct triples, do they necessarily generate distinct groups?

Proposition 3.15. *Let s and t be a pair of elementary reflections generating a finite group. For each generator η^i of μ_K, let (a_i, b_i, l_i) be the admissible triple associated to s^i and t^i, regarded as elementary reflections with respect to η^i. The set of admissible triples $\{(a_i, b_i, l_i) \mid i \text{ relatively prime to } m\}$ contains a unique preferred triple.*

If u and v are another pair of elementary reflections, then they generate a group isomorphic to that generated by s and t if and only if the unique preferred triple among the admissible triples associated to the various u^i and v^i coincides with the unique preferred triple associated to the s^i and t^i. In other words, isomorphism classes of complex reflection groups generated by two reflections are in one-to-one correspondence with preferred admissible triples.

This proposition is somewhat mysterious: no conceptual reason for the special role of preferred admissible triples is known, but if such a reason exists, it is likely related to the following observation (here ζ_n denotes a primitive nth root of unity):

Proposition 3.16. *Let (a, b, l) be an admissible triple. It is preferred if and only if the minimal polynomial for $\zeta_l + \zeta_l^{-1}$ over $\mathbb{Q}$ remains irreducible over $\mathbb{Q}(\zeta_a, \zeta_b)$.*

We omit the proofs of both of these propositions, as the only ones known to the authors are easy and not at all elucidating: for Proposition 3.15, one simply compares Theorem 3.14 with the classification of complex reflection groups, and does a handful of computations for the five nonpreferred triples (for instance, see Example 3.17 below), while Proposition 3.16 is a simple matter of examining the appropriate minimal polynomial in each case.

Example 3.17. Consider the nonpreferred admissible triple $(5, 5, 5)$. For simplicity, let us assume that we are working in a field K with η of order 10 (the smallest possible order in a field containing fifth roots of unity), so $\omega = \xi = \eta^2$. Also, let $\zeta = \eta^4$, $z = -\eta^2 = \eta^7$, and $y = -1$. It is easy to check the inequalities (8) directly, so there exist reflections s and t of some K-vector space, with roots α and β, that generate a finite group, and such that

$$N_{s,t} = (1-\eta^2)^2 \frac{(\alpha,\beta)(\beta,\alpha)}{(\alpha,\alpha)(\beta,\beta)} = -\eta^2(\eta^4+\eta^{-4}) - \eta^2 - \eta^2.$$

Now, let $\eta' = \eta^3$: this is another generator of μ_K. With respect to η', s and t are not elementary reflections, so to study the group they generate, we must first replace them by $s' = s^3$ and $t' = t^3$. Then,

$$\begin{aligned} N_{s',t'} &= (1-{\eta'}^2)^2 \frac{(\alpha,\beta)(\beta,\alpha)}{(\alpha,\alpha)(\beta,\beta)} = \frac{(1-{\eta'}^2)^2}{(1-\eta^2)^2} N_{s,t} \\ &= -\left(\frac{1-\eta^6}{1-\eta^2}\right)^2 \eta^2(\eta^4+\eta^{-4}+2) \\ &= -(1+\eta^2+\eta^4)^2\eta^2(\eta^4+\eta^{-4}+2) \\ &= -(7+7\eta^2+7\eta^4+8\eta^6+7\eta^8) = -\eta^6 = -{\eta'}^2. \end{aligned}$$

What admissible triple do s' and t' give rise to? To find out, we must write $N_{s',t'}$ in the form of (7), with respect to $\omega' = \xi' = {\eta'}^2$ and $z = -{\eta'}^2$. Setting

$$N_{s',t'} = -{\eta'}^2 = -{\eta'}^2(\zeta' + \zeta'^{-1}) - {\eta'}^2 - {\eta'}^2,$$

we find that $\zeta' + \zeta'^{-1} = -1$. The only roots of unity with this property are the primitive cube roots. So s' and t' satisfy a braid relation of length 3, and give rise to the admissible triple $(5,5,3)$.

In particular, we see that the triples $(5,5,5)$ and $(5,5,3)$ arise from the same complex reflection group. In fact, they are the only triples arising from that group, and of them, only $(5,5,3)$ is preferred.

Remark 3.18. Hughes and Morris originally defined admissible triples somewhat differently [6]. Their definition was purely in terms of the roots of the Hughes-Morris polynomials. Specifically, (a,b,l) was said to be admissible if

$$0 < \frac{r}{(1-\omega)(1-\xi)} < 1 \qquad \text{for every root } r \text{ of } f_l(x). \tag{10}$$

They obtain a classification of admissible triples by studying the roots of these polynomials directly. A comparison with Theorem 3.14 above reveals that a triple is admissible in the sense of Hughes-Morris if and only if it is preferred and admissible in the sense of this paper.

In [6, Theorem 3.16], Hughes and Morris prove a statement that is equivalent to our Lemma 3.4. They then observe that $0 < (1-\omega)^{-1}(1-\xi)^{-1}N < 1$, so the inequalities in (10) hold for a certain root of $f_l(x)$. Immediately following that, they erroneously infer that those inequalities must hold for every root of $f_l(x)$, so that reflections generating a finite group necessarily give rise to a triple that is admissible in their sense.

This is not true. The point is that the triples which we have called "admissible but not preferred" do indeed arise from pairs of elementary reflections—Proposition 3.10 tells us how to construct them—but it turns out that in each such case, a different choice of generating reflections results in a preferred admissible triple.

4. Representing J-groups by Reflections

In this section, we return to considering the J-groups introduced in Section 1. We will construct an action of any J-group on some 2-dimensional vector space over a suitable abelian number field. We will also construct a nondegenerate Hermitian form on this vector space that is invariant under the action of the group.

Lemma 4.1. (1) *The element stu is in the center of $J\left(\begin{smallmatrix} a & b & c \end{smallmatrix}\right)$.*

(2) *The generators of $J\left(\begin{smallmatrix} a & b & c \end{smallmatrix}\right)$ satisfy the following relations:*

$$(st)^c = (ts)^c, \qquad (tu)^a = (ut)^a, \qquad (us)^b = (su)^b.$$

(3) *We have $J\left(\begin{smallmatrix} a & b & c \end{smallmatrix}\right)/J\left(\begin{smallmatrix} a & b & c \\ a' & b' & \end{smallmatrix}\right) \simeq \mathbb{Z}/a'\mathbb{Z} \times \mathbb{Z}/b'\mathbb{Z}$.*

(4) *$J\left(\begin{smallmatrix} 1 & b & c \\ & b' & c' \end{smallmatrix}\right) \simeq \mathbb{Z}/(b/b')\mathbb{Z} \times \mathbb{Z}/(c/c')\mathbb{Z}$.*

Proof. (1) It is easy to see that stu commutes with s:

$$(stu)s = s(tus) = s(stu).$$

Similar calculations show that stu commutes with t and u as well.

(2) Let $z = stu$. We have $st = zu^{-1}$, so $(st)^c = z^c$. Next, since $usts = zs = sz$, we see that $ts = (s^{-1}u^{-1}s)z$, so $(ts)^c = z^c$ as well. The other relations follow by symmetry.

(3) Starting from the presentation (1), we obtain a presentation of the quotient $J\left(\begin{smallmatrix} a & b & c \end{smallmatrix}\right)/J\left(\begin{smallmatrix} a & b & c \\ a' & b' & \end{smallmatrix}\right)$ by adding the relations $s^{a'} = t^{b'} = u = 1$. Eliminating u from the presentation, we find that

$$J\left(\begin{smallmatrix} a & b & c \end{smallmatrix}\right)/J\left(\begin{smallmatrix} a & b & c \\ a' & b' & \end{smallmatrix}\right) = \langle s, t \mid s^{a'} = t^{b'} = 1,\ st = ts \rangle.$$

This is evidently a presentation for $\mathbb{Z}/a'\mathbb{Z} \times \mathbb{Z}/b'\mathbb{Z}$.

(4) This is clear from the presentation (1). □

Let K be a finite abelian extension of $\mathbb{Q}$ that contains the roots of unity of orders $2a$, $2b$, and $2c$, and let $\mathbb{Z}_K$ be the ring of algebraic integers in K. As usual, we fix a generator η of μ_K, whose order is denoted m. Let

$$\theta = \eta^{m/2a}, \qquad \phi = \eta^{m/2b}, \qquad \psi = \eta^{m/2c}.$$

Now, let us fix two algebraic integers $q, r \in \mathbb{Z}_K$ such that

$$qr = \theta\phi(\psi + \psi^{-1}) - \theta^2 - \phi^2. \tag{11}$$

Finally, we define the following matrices over $\mathbb{Z}_K$:

$$S = \begin{pmatrix} \theta^2 & q \\ & 1 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & \\ r & \phi^2 \end{pmatrix},$$

$$U = \theta\phi\psi T^{-1}S^{-1} = \begin{pmatrix} \theta^{-1}\phi\psi & -\theta^{-1}\phi\psi q \\ -\theta^{-1}\phi^{-1}\psi r & \theta^{-1}\phi^{-1}\psi qr + \theta\phi^{-1}\psi \end{pmatrix}.$$

Proposition 4.2. *There is homomorphism $\rho : J\left(\begin{smallmatrix} a & b & c \end{smallmatrix}\right) \to GL_2(K)$ defined by $s \mapsto S$, $t \mapsto T$, and $u \mapsto U$.*

Proof. We must show that S, T, and U satisfy the relations (1). It is readily checked that

$$STU = TUS = UST = \theta\phi\psi.$$

Next, since the eigenvalues of S are θ^2 and 1, it clearly has order a; similarly, T has order b. As for U, by using the relation (11), we find that its trace is $\psi^2 + 1$

and its determinant is ψ^2, so its eigenvalues are ψ^2 and 1. Thus, U has order c, as desired. □

Now, consider the Hermitian matrix

$$B = \begin{pmatrix} 1 & -\frac{q}{1-\theta^2} \\ -\frac{\bar{q}}{1-\theta^{-2}} & \frac{\bar{q}(1-\phi^2)}{r(1-\theta^{-2})} \end{pmatrix}.$$

Proposition 4.3. *The Hermitian form on K^2 defined by B is nondegenerate and ρ-invariant.*

Proof. It is trivial to verify that $S^*BS = T^*BT = B$, where * denotes the (Hermitian) adjoint of a matrix. Since

$$U^* = \theta^{-1}\phi^{-1}\psi^{-1}(S^{-1})^*(T^{-1})^*,$$

it follows that $U^*BU = B$ as well. Since the image of ρ is generated by S, T, and U, the form B is ρ-invariant.

Next, we prove nondegeneracy. Let $\alpha = (1,0)$ and $\beta = (0,1)$, and consider the quantity

$$\begin{aligned} P = \frac{\langle\alpha,\beta\rangle\langle\beta,\alpha\rangle}{\langle\alpha,\alpha\rangle\langle\beta,\beta\rangle} &= \frac{q\bar{q}r(1-\theta^{-2})}{(1-\theta^2)(1-\theta^{-2})\bar{q}(1-\phi^2)} \\ = \frac{qr}{(1-\theta^2)(1-\phi^2)} &= \frac{\theta\phi(\psi+\psi^{-1})-\theta^2-\phi^2}{1+\theta^2\phi^2-\theta^2-\phi^2}. \end{aligned}$$

Since $\det B = \langle\alpha,\alpha\rangle\langle\beta,\beta\rangle - \langle\alpha,\beta\rangle\langle\beta,\alpha\rangle$, we see that $\det B = 0$ if and only if $P = 1$. We must therefore show that P cannot be 1.

Now, from the above calculation, we have that $P = 1$ if and only if

$$\psi + \psi^{-1} = \theta\phi + \theta^{-1}\phi^{-1}.$$

Since ψ and $\theta\phi$ are both roots of unity, this equality implies that either $\theta\phi = \psi$ or $\theta\phi = \psi^{-1}$. Let us consider the latter possibility first: in this case we have

$$\theta\phi\psi = \eta^{m(1/2a+1/2b+1/2c)} = 1,$$

from which it follows that

$$\frac{1}{2a} + \frac{1}{2b} + \frac{1}{2c} \in \mathbb{Z}.$$

But on the other hand, since we have assumed that $a,b,c \geq 2$, we know that $1/2a + 1/2b + 1/2c \leq 3/4$, so it cannot be that $\theta\phi = \psi^{-1}$.

Finally, if $\theta\phi = \psi$, then the same reasoning as above shows that

$$\frac{1}{2a} + \frac{1}{2b} - \frac{1}{2c} \in \mathbb{Z}.$$

But now, the assumption that $a \leq b \leq c$ implies that $1/2a \leq 1/2a + 1/2b - 1/2c \leq 1/2a + 1/2b \leq 1/2$, where the last inequality comes, as before, from the fact that $a, b \geq 2$. So the equation $\theta\phi = \psi$ cannot hold either.

We conclude that P cannot be 1, and that B is nondegenerate. □

Proposition 4.4. *The group $\rho(J)$ is finite if and only if $(a, b, 2c)$ is a preferred admissible triple.*

Proof. By Proposition 2.5, $\rho(J)$ is finite if and only if the Hermitian matrix B defined above is definite. Let α, β, and P be as in the proof of Proposition 4.3. According to Lemma 2.3, B is definite if and only if $0 < P < 1$ under every imbedding $K \hookrightarrow \mathbb{C}$. From the expression

$$P = \frac{\psi + \psi^{-1} - \theta\phi^{-1} - \theta^{-1}\phi}{\theta\phi + \theta^{-1}\phi^{-1} - \theta\phi^{-1} - \theta^{-1}\phi},$$

we see that the condition $0 < P < 1$ is equivalent to the inequalities (8), with the following identifications:

$$\omega = \theta^2, \qquad \xi = \phi^2, \qquad z = \theta\phi, \qquad y = \theta\phi^{-1}, \qquad \zeta = \psi.$$

Since we have explicitly specified $\zeta = \psi = \eta^{m/2c}$, we deduce from Proposition 3.11 and Definition 3.13 that $0 < P < 1$ holds for every imbedding $K \hookrightarrow \mathbb{C}$ if and only if $(a, b, 2c)$ is a preferred admissible triple. □

Theorem 4.5. *The group $J\left(\begin{smallmatrix} a & b & c \\ a' & b' & c' \end{smallmatrix}\right)$ is finite if and only if the triple (a, b, c) has the form $(2, 2, c)$ or is one of $(2, 3, 3)$, $(2, 3, 4)$, or $(2, 3, 5)$. These groups are all distinct rank-two complex reflection groups, and all rank-two complex reflection groups arise in this way.*

Proof. From Proposition 4.4 and the list of admissible triples in Theorem 3.14, we see immediately that any J-group not listed above is infinite. On the other hand, for each of $J\left(\begin{smallmatrix} 2 & 2 & c \end{smallmatrix}\right)$, $J\left(\begin{smallmatrix} 2 & 3 & 3 \end{smallmatrix}\right)$, $J\left(\begin{smallmatrix} 2 & 3 & 4 \end{smallmatrix}\right)$, and $J\left(\begin{smallmatrix} 2 & 3 & 5 \end{smallmatrix}\right)$, the presentation given in (1) coincides with the presentation given in [4] for some complex reflection group, as listed in Table 1. Thus, these groups are all complex reflection groups.

Once we have identified a given $J\left(\begin{smallmatrix} a & b & c \end{smallmatrix}\right)$ as a complex reflection group, it is evident that its subgroups $J\left(\begin{smallmatrix} a & b & c \\ a' & b' & c' \end{smallmatrix}\right)$ are complex reflection groups as well. Straightforward calculations with the presentations given in [4], as done in [7], allow one to identify each of these groups with a particular group in the Shephard-Todd notation: the results are recorded in Table 1. Finally, we see from the table that the various finite J-groups are all distinct. □

5. Classification: Generators of Equal Order

This section is devoted to the classification of admissible triples (a, b, l) with $a = b$: the main result is Theorem 5.8, which asserts that there are no admissible triples of the form (a, a, l) other than those named in Theorem 3.14. This case is a good deal simpler than the case in which $a \neq b$, since, in the notation of Corollary 3.12, we always have $y = -1$. As a preliminary development, we will study pairs of roots of unity rather than triples.

Definition 5.1. An (unordered) pair of distinct positive integers $\{a, b\}$ is called *reversible* if, for any primitive ath root of unity ζ_a and primitive bth root of unity ζ_b in $\mathbb{C}$, there exist imbeddings $\iota_1 : \mathbb{Q}(\zeta_a, \zeta_b) \hookrightarrow \mathbb{C}$ and $\iota_2 : \mathbb{Q}(\zeta_a, \zeta_b) \hookrightarrow \mathbb{C}$ such that

$$\iota_1({\zeta_a} + {\zeta_a}^{-1}) < \iota_1({\zeta_b} + {\zeta_b}^{-1}) \qquad \text{and} \qquad \iota_2({\zeta_a} + {\zeta_a}^{-1}) > \iota_2({\zeta_b} + {\zeta_b}^{-1}).$$

Otherwise, $\{a, b\}$ is called *nonreversible.*

Remark 5.2. It is clear that any pair of the form $\{1, b\}$ $(b > 1)$ or $\{2, b\}$ $(b > 2)$ is nonreversible.

Proposition 5.3. *The only nonreversible pairs $\{a, b\}$, up to exchanging a and b, are the following:*

$$\{1, b\}, \quad \{2, b\}, \quad \{3, 4\}, \quad \{3, 6\}, \quad \{3, 10\}, \quad \{4, 6\}, \quad \{5, 6\}, \quad \{5, 10\}.$$

We need a few lemmas before undertaking the proof of this proposition.

Lemma 5.4. *Let ζ be a primitive nth root of unity, and let p be a prime. The polynomial $x^p - \zeta$ is irreducible over $\mathbb{Q}(\zeta)$ if $p \mid n$. If $p \nmid n$, then let m be such that $pm \equiv 1 \pmod{n}$. Then $x^p - \zeta$ factors as*

$$(x - \zeta^m)(x^{p-1} + \zeta^m x^{p-2} + \cdots + \zeta^{(p-2)m} x + \zeta^{(p-1)m}),$$

and the second factor is irreducible.

Proof. Since $[\mathbb{Q}(\zeta_{pn}) : \mathbb{Q}] = \phi(pn)$ and $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, we know that $[\mathbb{Q}(\zeta_{pn}) : \mathbb{Q}(\zeta_n)] = \phi(pn)/\phi(n)$. (Here ϕ denotes Euler's totient function.) From the well-known formula for ϕ, it is clear that

$$\phi(pn)/\phi(n) = \begin{cases} p & \text{if } p \mid n, \\ p - 1 & \text{if } p \nmid n. \end{cases}$$

Now, if $p \mid n$, we see that $\mathbb{Q}(\zeta_n)[x]/(x^p - \zeta) = \mathbb{Q}(\zeta_{pn})$. Since the degree of $x^p - \zeta$ coincides with $[\mathbb{Q}(\zeta_{pn}) : \mathbb{Q}(\zeta_n)]$, it is in fact the minimal polynomial for each of its roots, and in particular, it is irreducible over $\mathbb{Q}(\zeta_n)$. A parallel argument shows that if $p \nmid n$ and $pm \equiv 1 \pmod{n}$, then

$$x^{p-1} + \zeta^m x^{p-2} + \cdots + \zeta^{(p-2)m} x + \zeta^{(p-1)m}$$

is irreducible. □

The most important consequence of the preceding lemma is that it will let us conjugate certain roots of unity while holding others fixed.

Corollary 5.5. *Let ζ be a primitive nth root of unity, and let p be a prime. Let ξ be a primitive pth root of unity, and let ω be a pth root of ζ such that $\mathbb{Q}(\zeta, \omega)$ contains all pth roots of ζ. There exist automorphisms of $\mathbb{Q}(\zeta, \omega)$ which fix $\mathbb{Q}(\zeta)$ and carry ω to each of*

$$\omega\xi,\ \omega\xi^2,\ \ldots,\ \omega\xi^{p-1}$$

if $p \mid n$, or to $(p - 2)$ of the above values if $p \nmid n$.

Corollary 5.6. *Let ζ be a primitive nth root of unity, and let ω be a primitive pnth root of unity, where p is a prime. Assume that with respect to some imbedding $\iota : \mathbb{Q}(\zeta) \to \mathbb{C}$, we have $\zeta = e^{2\pi i t}$, with $t \in [0, \pi]$. If $1 - 2t \geq 2/p$ (resp. $2t \geq 2/p$), then ι can be extended to an imbedding $\iota : \mathbb{Q}(\zeta, \omega) \to \mathbb{C}$ such that*

$$\omega + \omega^{-1} < \zeta + \zeta^{-1} \qquad (\textit{resp. } \zeta + \zeta^{-1} < \omega + \omega^{-1}).$$

More precisely, there are at least $\lfloor (1 - 2t)p - 1 \rfloor$ (resp. $\lfloor 2tp - 1 \rfloor$) possible images of ω for which the above inequality is satisfied.

If we also have that $p \mid n$, then the same result holds under the weaker assumption that $1 - 2t \geq 1/p$ (resp. $2t \geq 1/p$), and in general, there are at least $\lfloor (1 - 2t)p \rfloor$ (resp. $\lfloor 2tp \rfloor$) possible images of ω.

Lemma 5.7. *Among all primitive nth roots of unity ζ in $\mathbb{C}$, the minimum possible value of $\zeta + \zeta^{-1}$ is achieved when $\zeta = e^{2\pi i c/n}$, where c is chosen according to the table below. In addition, there are very few (nonprimitive) nth roots of unity $\zeta' = e^{2\pi i d/n}$ for which $\zeta' + \zeta'^{-1}$ attains a smaller value. These are described in the last column.*

$n \bmod 4$	c	d [*order of* $e^{2\pi i d/n}$]
0	$\frac{n-2}{2}$	$\frac{n}{2}\,[2]$
$1, 3$	$\frac{n-1}{2}$	*none*
2	$\frac{n-4}{2}$	$\frac{n\pm 2}{2}\,[\frac{n}{2}],\ \frac{n}{2}\,[2]$

Proof of Proposition 5.3. We divide the proof into two major portions: in the first, we seek nonreversible pairs $\{a, b\}$ in which one of a or b divides the other, and in the second, pairs in which neither a nor b divides the other. We begin with the former, and we assume without loss of generality that b divides a.

Case 1: $b \mid a$. A large family of clearly nonreversible pairs in this category are those of the form $\{a, 1\}$. We henceforth assume that $b > 1$ (and thus $a > 2$ as well). There is some k such that $\zeta_a^k = \zeta_b$, where k is not relatively prime to a. (Note that we are not supposing that $a = kb$.) It is easy to find an imbedding in which ${\zeta_a + \zeta_a}^{-1} > {\zeta_b + \zeta_b}^{-1}$: we simply take $\zeta_a = e^{2\pi i/a}$.

We now seek an imbedding in which $\zeta_a + {\zeta_a}^{-1} < \zeta_b + {\zeta_b}^{-1}$. Choose ζ_a as described in Lemma 5.7 to minimize the value of $\zeta_a + {\zeta_a}^{-1}$. If it is now true that $\zeta_a + {\zeta_a}^{-1} < \zeta_b + {\zeta_b}^{-1}$, then we are done. Otherwise, according to that same lemma, there are very few possibilities for ζ_b (since ζ_b is also an ath root of unity). Indeed, there are none if a is odd; *i.e.,* $\{a, b\}$ is reversible whenever a is odd and b divides it. We now consider what can happen when a is even.

If $a \equiv 0 \pmod 4$, and yet $\zeta_a + {\zeta_a}^{-1} > \zeta_b + {\zeta_b}^{-1}$, then the only possible value of b according to Lemma 5.7 is 2. Thus, in this case, $\{a, 2\}$ is nonreversible, but $\{a, b\}$ is reversible if b is any divisor of a larger than 2.

The case $a \equiv 2 \pmod 4$ is the most difficult. Again, $\{a, 2\}$ is nonreversible, and $\{a, b\}$ is reversible if $b \neq 2, a/2$. We need to consider the case $b = a/2$ more carefully. Recall that $\zeta_b = \zeta_a^k$, for some $k \in \{1, 2, \ldots, a-1\}$. Since we are really only interested in conjugates of $\zeta_b + {\zeta_b}^{-1}$, we may replace ζ_b by its inverse if necessary and make the stronger assumption that $k \in \{1, 2, \ldots, a/2\}$. If $\zeta_a + {\zeta_a}^{-1} > \zeta_b + {\zeta_b}^{-1}$, then ζ_b must be either $e^{2\pi i(a-2)/2a}$ or $e^{2\pi i(a+2)/2a}$. Treating these cases simultaneously, we deduce:

$$\begin{aligned} \frac{a-4}{2} \cdot k &\equiv \frac{a \pm 2}{2} && \pmod a \\ 4k &\equiv \pm 2 && \pmod a \\ 2(2k \mp 1) &\equiv 0 && \pmod a. \end{aligned}$$

That is, $2(2k \mp 1)$ is a multiple of a, so the assumption that $1 \leq k \leq a/2$ implies, in fact, that $2(2k \mp 1) = a$. Now, recall that k and a are not relatively prime. Any common factor of a and k must also divide $a - 4k = \mp 2$, so k is even. This fact eliminates one of the two possibilities expressed by $2(2k \mp 1) = a$: if $a \equiv 2 \pmod 8$, we conclude that $k = (a-2)/4$ (and $2(2k+1) = a$), whereas if $a \equiv 6 \pmod 8$, we have $k = (a+2)/4$ (and $2(2k-1) = a$). Before considering these cases further, let us fix an imbedding in which $\zeta_a = e^{2\pi i(a-8)/2a}$. (One must verify that this is indeed a primitive ath root of unity, *i.e.,* that $(a-8)/2$ is indeed invertible modulo

a. To this end, the following table gives explicit inverses.)

$a \bmod 16$	2	6	10	14
$((a-8)/2)^{-1} \bmod a$	$-(3a+2)/8$	$-(a+2)/8$	$(a-2)/8$	$(3a-2)/8$

If $a \equiv 2 \pmod 8$, then we have

$$\frac{a-8}{2} \cdot \frac{a-2}{4} \equiv \frac{a^2-10a+16}{8} \equiv a\frac{a-10}{8} + 2 \equiv 2 \pmod a,$$

and therefore $\zeta_b = (e^{2\pi i(a-8)/2})^{(a-2)/4} = e^{2\pi i \cdot 2/a}$. Provided that $a \geq 18$, it is clear that $2 < (a-8)/2 < a/2$, and therefore

$$e^{\frac{2\pi i(a-8)}{2a}} + e^{-\frac{2\pi i(a-8)}{2a}} < e^{\frac{2\pi i \cdot 2}{a}} + e^{-\frac{2\pi i \cdot 2}{a}},$$

so $\{a, b\}$ is reversible. However, if $a = 10$, we have $k = 2$ and $b = 5$. (We need not consider the case $a = 2$, as that was dealt with at the beginning of the proof.) Direct calculation of all possible conjugates of ζ_{10} and ζ_{10}^2 shows that $\{10, 5\}$ is indeed nonreversible.

If $a \equiv 6 \pmod 8$, a similar calculation to the above shows that $\zeta_b = e^{2\pi i \cdot (-2)/a}$. This time, the inequalities show that $\{a, b\}$ is reversible if $a \geq 14$. If $a = 6$, however, we find that $k = 2$ and $b = 3$. The pair $\{6, 3\}$ is clearly not reversible.

Case 2: $a \nmid b$ and $b \nmid a$. In this case, there exists a prime p and a number $i > 0$ such that $p^i \mid b$, but $p^{i+1} \nmid b$ and $p^i \nmid a$. Similarly, there is a prime $q \neq p$ and a number $j > 0$ such that $q^j \mid a$, $q^{j+1} \nmid a$, and $q^j \nmid b$. We assume without loss of generality that $p > q$. In particular, this means that $p > 2$.

Our strategy will be to use Corollary 5.6 repeatedly to identify reversible pairs. In particular, we try to find numbers $t_1, t_2 \in [0, 1/2]$ such that $e^{2\pi i t_1}$ and $e^{2\pi i t_2}$ are both primitive bth roots of unity, $1 - 2t_1 \geq 2/3$, and $2t_2 \geq 2/3$. Since $p > 2$, we know that $2/3 \geq 2/p$, so if we find such t_1 and t_2 for a given b, two applications of Corollary 5.6 demonstrate that $\{a, b\}$ is a reversible pair for any a that is neither a divisor nor a multiple of b.

The choice of t_1 is easy: we take $t_1 = 1/b$. Then $1 - 2t_1 \geq 2/3$ as long as $b \geq 6$. The table below shows the value we choose for t_2, depending on the residue class of b modulo 8. In order to verify that $e^{2\pi i t_2}$ is indeed a primitive bth root of unity, we need to check that t_2 is of the form c/b, where c is invertible modulo b. The third column of the table gives an explicit inverse for c.

(12)

	$t_2 = c/b$	$c^{-1} \bmod b$	$2t_2 \geq 2/3$
$b \equiv 0 \pmod 4$	$(b-2)/2b$	$-(b+2)/2$	$b \geq 8$
$b \equiv 2 \pmod 8$	$(b-4)/2b$	$-(b+2)/4$	$b \geq 18$
$b \equiv 6 \pmod 8$	$(b-4)/2b$	$-(3b+2)/4$	$b \geq 14$
$b \equiv 1 \pmod 2$	$(b-1)/2b$	-2	$b \geq 3$

The values of b not accounted for by the above table are:

$$\begin{array}{rl} 1 - 2t_1 < 2/3: & b = 2, 3, 4, 5 \\ 2t_2 < 2/3: & b = 2, 4, 6, 10. \end{array}$$

We will now consider each of these values of b individually to determine the nonreversible pairs.

It has already been remarked that $\{a, 2\}$ is nonreversible for any a.

If $b = 3$, then $1 - 2t_1 = 1/3 > 2/7$, so it follows that $\{a, 3\}$ is reversible provided that $p \geq 7$. Now, $p = 3$ is not permitted, since a is assumed not to be a multiple of

b. Suppose $p = 5$, so that a is a multiple of 5. Using table (12), we can express ζ_a as some $e^{2\pi i s}$ with $2s \geq 2/3$ as long as $a \geq 15$. In these cases, it is easy to see that $e^{2\pi i s} + e^{-2\pi i s} < \zeta_3 + {\zeta_3}^{-1}$. Thus, $\{a, 3\}$ if a is a multiple of 5 that is at least 15. It remains to consider $a = 5$ and $a = 10$. By explicit consideration of the conjugates of $e^{2\pi i/5}$ and $e^{2\pi i/10}$, one finds that $\{5, 3\}$ is reversible, but $\{10, 3\}$ is not.

If $b = 4$, then $1 - 2t_1 = 2t_2 = 1/2 > 2/5$, so $\{a, 4\}$ is reversible as long as $p \geq 5$. We consider the case $p = 3$, so that a is a multiple of 3. Proceeding as above, we find that if $a \geq 9$, table (12) gives a way to choose $\zeta_a = e^{2\pi i s}$ so that $e^{2\pi i s} + e^{-2\pi i s} < \zeta_4 + {\zeta_4}^{-1}$. It also clear that for all $a \geq 9$, we can choose $\zeta_a = e^{2\pi i/a}$, in which case $\zeta_a + {\zeta_a}^{-1} > \zeta_4 + {\zeta_4}^{-1}$. On the other hand, if $a = 3$ or 6, the there is only one possible value for $\zeta_a + {\zeta_a}^{-1}$. The pairs $\{3, 4\}$ and $\{6, 4\}$ are not reversible.

If $b = 5$, then $q = 5$, so $p \geq 7$. Although $1 - 2t_1 \not\geq 2/3$, we do have $1 - 2t_1 = 3/5 > 2/7$, so all pairs $\{a, 5\}$ are reversible.

If $b = 6$, then $2t_2 = 1/3 > 2/7$, so $\{a, 6\}$ is reversible if either $p = 3$ and $i > 1$, or $p \geq 7$. It remains to consider the case where $p = 3$ with $i = 1$, and the case $p = 5$. But in fact, $p = 3$ with $i = 1$ cannot occur, since $3 \mid 6$. Finally, if $p = 5$, we proceed as we did in studying the case $b = 3$. Table (12) shows that $\{a, b\}$ is reversible if a is a multiple of 5 and $a \geq 15$. Explicit calculation then shows that $\{5, 6\}$ is not reversible, but $\{10, 6\}$ is.

The last case to consider is that of $b = 10$. Here, we have $2t_2 = 3/5 > 2/5$, so we have that $\{a, 10\}$ is reversible if $p \geq 5$. Now, suppose that $p = 3$, so a is a multiple of 3. Since $1 - 2t_1 > 2/3$, it suffices to find a ζ_a such that $\zeta_a + {\zeta_a}^{-1} > e^{3\pi i/5} + e^{-3\pi i/5}$ to prove that $\{a, 10\}$ is reversible. This is possible if $a \geq 6$, simply by taking $\zeta_a = e^{2\pi i/a}$. As for $a = 3$, we have already noted that $\{3, 10\}$ is not reversible. □

Theorem 5.8. *Suppose that (a, a, l) is an admissible triple. Then, either it is of the form $(2, 2, l)$, or it is one of $(3, 3, 3)$, $(4, 4, 3)$, $(5, 5, 3)$, $(3, 3, 4)$, $(3, 3, 5)$, or $(5, 5, 5)$.*

Proof. In the notation of Section 3, we have $z = -\omega$ and $y = -1$. Choose an imbedding $K \hookrightarrow \mathbb{C}$ such that $\omega = e^{2\pi i/a}$. Let us consider the inequality (9), which becomes

$$-2 < \zeta + \zeta^{-1} < -e^{2\pi i/a} - e^{-2\pi i/a}.$$

We further break down the argument according to the residue class of a modulo 4. If $a \equiv 0 \pmod 4$, then $-e^{2\pi i/a}$ is also a primitive ath root of unity. Since ζ is a primitive lth root of unity, the above inequalities can be preserved by all automorphisms of K only if $\{l, a\}$ is a nonreversible pair. In view of the fact that $l \geq 3$ and $a \equiv 0 \pmod 4$, Proposition 5.3 tells us that the only possibilities are $\{3, 4\}$ and $\{4, 6\}$, but if $l = 6$ and $a = 4$, then the above inequalities are not satisfied to begin with. This leaves $(4, 4, 3)$ as the only possibility.

If $a \equiv 2 \pmod 4$, then $-e^{2\pi i/a}$ is a primitive $(a/2)$th root of unity. According to Proposition 5.3, the only nonreversible pairs $\{l, a/2\}$ with $l \geq 3$ and $a/2$ odd are $\{l, 1\}$, $\{4, 3\}$, $\{6, 3\}$, $\{10, 3\}$, $\{6, 5\}$, and $\{10, 5\}$. However, for each of the pairs other than $\{l, 1\}$, explicit calculation shows that the above inequalities are violated. The only admissible triples with $a \equiv 2 \pmod 4$ are therefore of the form $(2, 2, l)$.

Finally, if a is odd, then $-e^{2\pi i/a}$ is a primitive $(2a)$th root of unity. We examine Proposition 5.3 once again for the nonreversible pairs $\{l, 2a\}$ with $l \geq 3$, $2a \equiv 2 \pmod 4$, and $2a \geq 6$ (since $a \geq 3$). We find that the possibilities are $\{3, 6\}$, $\{3, 10\}$,

$\{4,6\}$, $\{5,6\}$, and $\{5,10\}$. These correspond to the admissible triples $(3,3,3)$, $(5,5,3)$, $(3,3,4)$, $(3,3,5)$, and $(5,5,5)$. □

6. Classification: Generators of Unequal Order

In this section, we conclude the classification of admissible triples by showing that the only admissible triples (a,b,l) with $a \neq b$ are those named in Theorem 3.14. An important tool in this part of the classification is the following technique for obtaining new admissible triples out of old ones by examining certain subgroups of the given complex reflection group.

Definition 6.1. Let (a,b,l) be an admissible triple arising from elementary reflection s and t (of orders a and b, respectively) of some K-vector space. Let $a' \geq 2$ be a divisor of a, and $b' \geq 2$ a divisor of b. Then the transformations $s' = s^{a/a'}$ and $t' = t^{b/b'}$ are again elementary reflections (of orders a' and b', respectively) generating a finite group. These reflections give rise to a new admissible triple, either (a',b',l') or (b',a',l'). An admissible triple obtained in this way is said to be *subordinate* to (a,b,l).

Remark 6.2. There is no way in general to compute l' from the triple (a,b,l), but there is one bit of information we can obtain: if $a \neq b$ (so that l is even), then l' is also even. This follows from the observation that α and β are not in the same W-orbit (since $a \neq b$) and therefore not in the same W'-orbit.

Typically, the concept of subordinate triples is used to rule out certain triples, as follows: if we have proved that there are no admissible triples of the form $(a',b',\cdot)$ or $(b',a',\cdot)$, where $a' \mid a$ and $b' \mid b$, then it follows that there are no admissible triples of the form $(a,b,\cdot)$ either.

Throughout this section, we will use the following notation: with respect to an appropriate imbedding, $\omega = e^{2\pi i/a}$ and $\xi = e^{2\pi i/b}$. Recall that according to Proposition 3.9, we can in most cases take

$$z = -\eta^{m(a+b)/2ab} = \eta^{m(ab+a+b)/2ab} \quad \text{and} \quad y = -\eta^{m(b-a)/2ab} = \eta^{m(ab+b-a)/2ab}. \tag{13}$$

Although we will ultimately see that z and y can be defined in this way always, we must for the time being allow the negatives of these formulas when $l \equiv 2 \pmod 4$. We intend to determine the possible lth roots of unity ζ such that (9) holds. Those inequalities remain unchanged if we replace ζ by ζ^{-1}, so, whenever z and y are given by (13) (resp. the negatives of those formulas), we assume that ζ also lies in the lower (resp. upper) half plane. In particular, we can write ζ in the form $-e^{2\pi is}$ (resp. $e^{2\pi is}$) such that $s \in [0,1/2]$ and

$$(b-a)/2ab < s < (b+a)/2ab. \tag{14}$$

These inequalities hold regardless of whether z and y are given by the formulas (13) or by their negatives. Moreover, since ζ is a primitive lth root of unity, with l even, it follows that $e^{2\pi is}$ is an lth root of unity, although possibly not primitive in the case that $\zeta = -e^{2\pi is}$. So s can always be written as a fraction of the form k/l.

Corollary 6.3. *If (a,b,l) is an admissible triple with l even, then the greatest common divisor of a and b can be at most* 3.

Proof. Let c be the greatest common divisor of a and b, and assume that $c \geq 2$. Then there is an admissible triple of the form (c, c, l') that is subordinate to (a, b, l). By Remark 6.2, we know that l' must also be even. Thus, (c, c, l') must either equal $(3, 3, 4)$ or be of the form $(2, 2, l')$. □

Lemma 6.4. *Let (a, b, l) be an admissible triple, and let c and d denote the orders of z and y, respectively, as roots of unity. Then l is strictly less than the larger of c or d. If $l \equiv 0 \pmod 4$, then l is also strictly less than the larger of the orders of $-z$ and $-y$.*

Proof. If this were not the case, we could violate (9) by conjugating ζ to $e^{2\pi i/l}$, resulting in both $z + z^{-1} < \zeta + \zeta^{-1}$ and $y + y^{-1} < \zeta + \zeta^{-1}$. □

Lemma 6.5. *Let (a, b, l) be an admissible triple with l even. Suppose that there is a prime p such that for some $i > 0$, p^i divides the orders of z and y, but p^{i+1} does not, and in addition, $p^i \nmid l$. Then, if $p \geq 5$, we have $l < 4 + 12/(p - 3)$. If $i > 1$ and $p \geq 3$, we obtain the stronger bound $l < 4 + 4/(p - 1)$.*

Proof. Let n be the least common multiple of l and the orders of z and y, and let ω be a primitive nth root of unity. Since p^i is the largest power of p dividing the orders of z, y, and ω, it is easy to see that z and y can be written as powers of ω with exponents relatively prime to p. It follows that the automorphisms taking ω to each of the values in Corollary 5.5 also take z and y to distinct values. Of course, these automorphisms fix ζ, since $p^i \nmid l$.

By Corollary 5.6, each of z and y has at least $\lfloor (1-2/l)p-1 \rfloor$ conjugates satisfying $z + z^{-1} < \zeta + \zeta^{-1}$ and $y + y^{-1} < \zeta + \zeta^{-1}$ respectively. Conversely, they each have at most $\lceil 2p/l \rceil$ conjugates satisfying the opposite inequality.

Now, let s be as in (14). We claim that

$$\lfloor (1 - 2s)p - 1 \rfloor \leq \lceil 2sp \rceil. \tag{15}$$

If this inequality did not hold, it would mean that z had more conjugates satisfying $z + z^{-1} < \zeta + \zeta^{-1}$ than y had satisfying $y + y^{-1} > \zeta + \zeta^{-1}$, so among all those conjugates for which $z + z^{-1} < \zeta + \zeta^{-1}$, at least one must have had a corresponding value of y for which $y + y^{-1} < \zeta + \zeta^{-1}$ as well. By Corollary 3.12, this contradicts the admissibility of (a, b, l).

From (15), we calculate:

$$\begin{aligned} \lfloor (1 - 2s)p - 1 \rfloor = p - 1 - \lceil 2sp \rceil &\leq \lceil 2sp \rceil \\ (p - 1)/2 &\leq \lceil 2sp \rceil \end{aligned}$$

If $p = 2$, this inequality just says $1/2 \leq \lceil 2sp \rceil$, but this conveys no information, since we know that $\lceil 2sp \rceil$ is a positive integer in any case. If p is odd, however, we get

$$(p - 1)/2 - 1 < 2sp \tag{16}$$

and therefore, if $p \geq 5$, we conclude that

$$s^{-1} < 4p/(p - 3) = 4 + 12/(p - 3).$$

Now, in case $i > 1$, Corollary 5.6 tells us that we can replace (15) by the stronger inequality

$$\lfloor (1 - 2s)p \rfloor \leq \lceil 2sp \rceil.$$

Calculating as above, we find that in place of (16), we have $(p-1)/2 < 2sp$, from which it follows (this time for any odd p) that $s^{-1} < 4 + 4/(p-1)$. Finally, let us choose an imbedding $K \hookrightarrow \mathbb{C}$ such that $\zeta = e^{2\pi i/l}$, so $s^{-1} = l$. The lemma follows. □

The preceding lemma will be one of our most powerful tools for showing that certain triples are not admissible. However, it relies on rather loose estimates in (15). The following result is stronger but much more cumbersome to apply, so we will only use it when the preceding lemma does not suffice.

Corollary 6.6. *Let (a, b, l) be an admissible triple, and let k be such that $\zeta = -e^{2\pi ik/l}$ if (13) holds, or such that $\zeta = e^{2\pi ik/l}$ otherwise. Suppose that there is a prime p such that for some $i > 0$, p^i divides the orders of z and y, but p^{i+1} does not, and in addition, $p^i \nmid l$. Then, both of the following hold:*

$$\lfloor p(1 - k/l - (b+a)/2ab)\rfloor \le \lceil p(k/l + (b-a)/2ab)\rceil, \tag{17}$$

$$\lceil p(1 - k/l - (b+a)/2ab)\rceil \ge \lfloor p(k/l + (b-a)/2ab)\rfloor. \tag{18}$$

If $i > 1$, then we have the following stronger result:

$$\lceil p(1 - k/l - (b+a)/2ab)\rceil = \lceil p(k/l + (b-a)/2ab)\rceil. \tag{19}$$

Proof. Corollary 5.5 tells us that z has $p-1$ or p conjugates of the form

$$e^{2\pi i\left(\frac{b+a}{2ab} + \frac{n}{p}\right)} \tag{20}$$

under automorphisms of K that fix $\mathbb{Q}(\zeta)$. Let us assume that $0 \le n \le p-1$. It is easy to verify that the conjugate z' of z corresponding to n satisfies $z' + z'^{-1} > \zeta + \zeta^{-1}$ if and only if

$$0 \le n < \lceil 1 - k/l - (b+a)/2ab\rceil.$$

Thus, z has at most $\lceil 1 - k/l - (b+a)/2ab\rceil$ (and at least $\lfloor 1 - k/l - (b+a)/2ab\rfloor$) conjugates z' satisfying $z' + z'^{-1} > \zeta + \zeta^{-1}$. A similar calculation for y shows that it has at least $\lfloor p(k/l + (b-a)/2ab)\rfloor$ conjugates y' satisfying $y' + y'^{-1} < \zeta + \zeta^{-1}$, and at most $\lceil p(k/l + (b-a)/2ab)\rceil$. The two inequalities in the statement are then obtained by the same reasoning that gave (15): neither z nor y is permitted to have more conjugates satisfying the appropriate inequality than the other.

If we have the added assumption that $i > 1$, then all elements of the form (20) are conjugates of z (and similarly for y). It follows that z (resp. y) has exactly $\lceil 1 - k/l - (b+a)/2ab\rceil$ (resp. $\lceil p(k/l + (b-a)/2ab)\rceil$) conjugates satisfying the appropriate inequality. The equality in the statement of the corollary follows. □

Lemma 6.7. *Let (a, b, l) be an admissible triple, and suppose that there is a prime number r and some $k > 0$ such that $r^k \mid l$ but r^k does not divide the orders of z or y. Then $r < 2ab/(ab - a - b)$. If $k > 1$, this inequality can be strengthened to $r < ab/(ab - a - b)$.*

Proof. Assume first that (13) holds, so that we have $z^{-1} = -e^{-2\pi i\cdot(a+b)/2ab} = e^{2\pi i\cdot(ab-a-b)/2ab}$. As an immediate consequence of Corollary 5.6, if we have $2(ab - a - b)/2ab \ge 2/r$, then ζ can be replaced by a conjugate ζ' over $\mathbb{Q}(z, y)$ such that $\zeta' + \zeta'^{-1} < z + z^{-1} < y + y^{-1}$. So it must be that $1 - 2(a+b)/2ab < 2/r$, *i.e.*, $r < 2ab/(ab - a - b)$. The stronger inequality for the case $k > 1$ is obtained analagously from the stronger inequality in Corollary 5.6.

If instead the negatives of the formulas in (13) hold, then $z = e^{2\pi i\cdot(a+b)/2ab}$. We again apply Corollary 5.6 to deduce that $1 - 2(a+b)/2ab < 2/r$, whence $r < 2ab/(ab-a-b)$, and we do likewise for the case $k > 1$. □

Finally, there are a handful of triples that are inadmissible but cannot be shown to be such by any of the preceding tools. We must resort to calculating explicit conjugates using Corollary 5.5

Lemma 6.8. *The triples* $(2,6,10)$*,* $(3,4,16)$*, and* $(3,10,20)$ *are inadmissible.*

Proof. Let us write either $\zeta = -e^{2\pi is}$ or $\zeta = e^{2\pi is}$, according to whether (13) or its negatives hold. By inspection, one finds that for each of the above triples, there are at most two possible values of s satisfying (14). These are shown in the table below. For each triple, we note the order of the group of roots of unity in $K = \mathbb{Q}(z, y, \zeta)$, and we describe a certain automorphism $\sigma : K \to K$ by giving its action on μ_K.

Triple	$\frac{a+b}{2ab}$	$\frac{b-a}{2ab}$	s	$\lvert\mu_K\rvert$	$\sigma\rvert_{\mu_K}$
$(2,6,10)$	$1/3$	$1/6$	$2/10$	30	$x \mapsto x^7$
$(3,4,16)$	$7/24$	$1/24$	$1/16, 3/16$	48	$x \mapsto x^{25}$
$(3,10,20)$	$13/60$	$7/60$	$3/20$	60	$x \mapsto x^7$

It is straightforward to check that in each case, the inequalities (9) are not satisfied for the given automorphism σ. □

Proposition 6.9. *If* (a,b,l) *is an admissible triple with* $a < b$*,* $l \neq 2a$*, and* $l \leq 10$*, then it must be one of* $(3,4,4)$*,* $(3,5,4)$*,* $(2,3,6)$*,* $(2,4,6)$*,* $(2,5,6)$*,* $(2,3,8)$*,* $(3,4,8)$*,* $(2,3,10)$*,* $(2,5,10)$*, or* $(3,5,10)$*.*

Proof. We consider each value of $l \in \{4,6,8,10\}$ separately. First, suppose $l = 4$, so $\zeta + \zeta^{-1} = 0$. We do not consider $a = 2$. If $a = 3$, and if $b \geq 6$, then it is readily verified from (13) that $z + z^{-1}$ and $y + y^{-1}$ are both negative, so (9) cannot hold if $l = 4$. The same reasoning applies whenever $b > a \geq 4$. The only remaining possibilities are $(3,4,4)$ and $(3,5,4)$.

Now, if $l > 4$, let us write $s = k/l$, where s is as in (14). For each value of l under consideration, there are very few values of k with $0 \leq k \leq l/2$ such that one of $\pm e^{2\pi ik/l}$ is a primitive lth root of unity.

Now, (14) implies $lb - la < 2kab < lb + la$. Since $lb + la < 2lb$, we deduce that $2kab < 2lb$. We also obtain $-la < (2ka - l)b < la$, so (since $l \neq 2a$) we have

$$a < l/k \qquad \text{and} \qquad b < la/|2ka - l|. \tag{21}$$

These inequalities are the starting point for the case-by-case considerations below. In most cases, z and y have the same order, which will be denoted c.

For $l = 6$, we must consider $k = 1$ and $k = 2$. If $k = 1$, we must consider $a = 2, 4, 5$. If $a = 2$, we see from (21) that $b < 6$, and each of $(2,3,6)$, $(2,4,6)$, and $(2,5,6)$ is admissible. If $a = 4$, then $b < 12$. For each of the seven possible values of b, we find that $4 \mid c$, and we get a contradiction by applying Corollary 6.6 with $p = 2$. If $a = 5$, then $b < 15/2$. Each of $b = 6$ and $b = 7$ is ruled out, again using Corollary 6.6, with $p = 5$. Finally, if $k = 2$, then from (21), we have $a < 3$, *i.e.,* $a = 2$, and thence $b < 6$. All the possible triples that this encompasses are, in fact, admissible.

For $l = 8$, we may have either $k = 1$ or $k = 3$. If $k = 1$, we must consider $a = 2, 3, 5, 6, 7$. For $a = 2$, we have $b < 4$, giving the admissible triple $(2,3,8)$. If $a = 3$, then $b < 12$, but among these, $b = 7, 8, 9, 11$ are eliminated by Lemma 6.5

(with $p^i = 7, 16, 9, 11$ respectively). Furthermore, $b = 6$ and $b = 10$ are eliminated by Lemma 6.7 with $r^k = 8$, while $b = 5$ is eliminated by Corollary 6.6: taking $p^i = 5$ leads to a violation of (17). This leaves only $b = 4$, and $(3, 4, 8)$ is admissible. Next, if $a = 5$, then $b < 20$. Each of the cases $b = 7, 9, 11, 13, 14, 17, 18, 19$ is eliminated by Lemma 6.5 applied with $p^i = 7, 9, 11, 13, 7, 17, 9, 19$ respectively. Furthermore, the cases $b = 6, 10, 15$ are eliminated by Lemma 6.7 with $r^k = 8$. For $b = 8, 12, 16$, we must apply Corollary 6.6 with $p = 5$: each of these leads to a violation of (17). If $a = 6$, then $b < 12$. We rule out $b = 7, 9, 11$ by Lemma 6.5 with $p^i = 7, 9, 11$, and $b = 10$ by Lemma 6.7 with $r^k = 8$. For $b = 8$, we use Corollary 6.6 with $p = 3$, and obtain a contradiction of (17). Finally, if $a = 7$, then $b < 28/3$. For $b = 8, 9$, we have $7 \mid c$, so Lemma 6.5 disallows $l = 8$.

For $l = 8$ and $k = 3$, we see that (21) implies $a = 2$, and $b = 3$. The triple $(2, 3, 8)$ is admissible.

For $l = 10$ and $k = 1$, we must consider $a = 2, 3, 4, 6, 7, 8, 9$. For $a = 2$, we get $b < 10/3$, giving the admissible triple $(2, 3, 10)$. If $a = 3$, we have $b < 15/2$. Each of the cases $b = 4, 6, 7$ is eliminated by Lemma 6.7 with $r^k = 5$. This leaves the admissible triple $(3, 5, 10)$. If $a = 4$, we have $b < 20$. Again, every b that is not divisible by 5 is ruled out by Lemma 6.7 with $r^k = 5$, while $b = 5, 10, 15$ are forbidden by Lemma 6.5 with $p^i = 8$. If $a = 6$, then $b < 30$. Once more, Lemma 6.7, applied with $r^k = 5$, eliminates all b not divisible by 5, while for $b = 15, 20, 25$ we get a contradiction by applying Lemma 6.5 with $p^i = 4, 8, 4$ respectively. This leaves just $b = 10$, which is ruled out by applying Corollary 6.6 with $p = 3$, since (17) does not hold. Next, if $a = 7$, then $b < 35/2$, and in every case, $7 \mid c$, so Lemma 6.5 forbids $l = 10$. If $a = 8$, then $b < 40/3$, but each of $b = 9, 11, 12, 13$ is ruled out by Lemma 6.7 (with $r^k = 5$), while $b = 10$ is ruled out because it does not even satisfy (14). Finally, if $a = 9$, then $b < 45/4$, so $b = 10$ or 11, but again, (14) is not satisfied.

If $l = 10$ and $k = 3$, we need only look at $a = 2$ and $a = 3$, for which we have the bounds $b < 10$ and $b < 15/4$. In the latter case, there are no permitted values for b. In the former case, the possibilities $b = 4, 5, 7, 8, 9$ are disallowed by Lemma 6.5 with $p^i = 8, 5, 7, 16, 9$ respectively. This leaves only $b = 3$ and $b = 6$. The latter is ruled out by Lemma 6.8, while the former gives the admissible triple $(2, 3, 10)$. □

Proposition 6.10. *Let (a, b, l) be an admissible triple. Suppose that b is a prime power, that b is relatively prime to a, and that $b \nmid l$. Then (a, b, l) is one of $(2, b, 4)$, $(3, 5, 4)$, $(2, 5, 6)$, $(3, 5, 6)$, $(2, 3, 8)$, or $(2, 3, 10)$.*

Proof. By (13), the orders of z and y are either both ab or both $2ab$. In any case, z and y have the same order. Suppose that $b = q^j$, where q is a prime. Now, each triple named in the statement of the proposition is either one that was already identified as admissible in Proposition 6.9, or one satisfying $2a = l \leq 10$. The following argument is broken into cases according the values of q and j, and in each case, we first show that $l \leq 10$, and second, we show that for each permitted l, the only admissible triples of the form $(l/2, q^j, l)$ are those named above.

If $q \geq 11$, or if $q \geq 3$ and $j > 1$, then Lemma 6.5 implies that $l = 4$. Every triple $(2, b, 4)$ is admissible. We next consider each of $q = 3, 5, 7$ with $j = 1$. If $q = 7$, then $l < 7$ by Lemma 6.5. The triple $(2, 7, 4)$ is admissible, but $(3, 7, 6)$ is inadmissible by Corollary 6.6 applied with $p = 7$, since (17) is violated. Next, if $q = 5$, then $l < 10$ by Lemma 6.5. $(2, 5, 4)$ and $(3, 5, 6)$ are admissible, but $(4, 5, 8)$ is not, as is seen by applying Corollary 6.6 with $p = 5$ (again, (17) is violated). If $q = 3$, then

a must be 2, so $l < 2ab = 12$ by Lemma 6.4. Since $a = 2$, the only triple requiring special consideration is $(2, 3, 4)$, which is admissible.

If $q = 2$, we apply Corollary 5.5 directly, rather than using Lemma 6.5. Note that $p \neq 2$, so $a > 2$. First suppose that $j \geq 3$, so that $b \geq 8$. It is readily seen from (13) that $z + z^{-1}$ and $y + y^{-1}$ are both negative (or both positive, if the negatives of (13) hold). In either case, conjugating them simultaneously according to Corollary 5.5, we replace both z and y by their negatives. After this conjugation, $z + z^{-1}$ and $y + y^{-1}$ both have the sign opposite to that of $\zeta + \zeta^{-1}$, so (9) is clearly violated. So there are no admissible triples with $q = 2$ and $j \geq 3$.

Next, if $q = 2$, $j = 2$, so that $b = 4$, then we must consider $a = 2, 3$. For $a = 2$, after computing the orders of z and y from (13), we get $l < 8$ by Lemma 6.4, and of course, $(2, 4, 4)$ is admissible. For $a = 3$, that lemma gives $l < 24$. We have assumed that $b \nmid l$, but $l = 14, 18, 22$ are forbidden according to Lemma 6.7 applied with $r^k = 7, 9, 11$ respectively. So $l \leq 10$ in this case. We need to check $(3, 4, 6)$: it is inadmissible by Corollary 6.6 with $p^i = 8$, since (19) does not hold. The only remaining case, that of $q = 2$, $j = 1$, cannot occur, since $b > a \geq 2$. □

Lemma 6.11. *Suppose that* $(2, 2^j, l)$ *is an admissible triple, where* $j > 1$*. Then, it is either of the form* $(2, 2^j, 4)$*, or it is* $(2, 4, 6)$*.*

Proof. Every triple $(2, 2^j, 4)$ is admissible, so we assume henceforth that $l > 4$. From (13), z and y both have order 2^{j+1}, so $l < 2^{j+1}$ by Lemma 6.4. If $2^j \nmid l$, then $l < 8$ by Lemma 6.5, so we examine Proposition 6.9 and find that the only triple of this form is $(2, 4, 6)$. On the other hand, if $2^j \mid l$, it follows that $l = 2^j$. Therefore, we can write $\zeta = e^{2\pi ik/2^j}$ where k is odd. From (14), we deduce that

$$(b - a)/2ab = (2^{j-1} - 1)/2^{j+1} < k/2^j < (2^{j-1} + 1)/2^{j+1} = (b + a)/2ab.$$

These inequalities imply that $2k = 2^{j-1}$, but this contradicts the fact that k is odd unless $j = 2$. This gives $l = 4$, but we had assumed $l > 4$, so we have a contradiction. □

Lemma 6.12. *The only admissible triples of the form* $(3, 2^j, l)$ *where* $2^j \mid l$ *are* $(3, 4, 4)$ *and* $(3, 4, 8)$*.*

Proof. For any admissible triple $(3, 2^j, l)$ with $j \geq 3$, there is a subordinate triple $(3, 8, l')$. By Proposition 6.10, there are no admissible triples of this form with $8 \nmid l'$, so $8 \mid l'$. Both z and y have order 48, so if $16 \nmid l'$, then Lemma 6.5 would imply that $l' < 8$, a contradiction. Therefore, $16 \mid l'$. By Lemma 6.4, $l < 48$, so we must consider $l = 16$ and $l = 32$. But these are forbidden by Lemma 6.7 applied with $r^k = 16$ and $r^k = 32$ respectively. Thus, there are no admissible triples $(3, 8, l')$, and hence no admissible triples $(3, 2^j, l)$ with $j \geq 3$ and $2^j \mid l$.

If $j = 2$, then l, assumed to be a multiple of 4, satisfies $l < 24$ by Lemma 6.4. By Lemma 6.7, if $8 \nmid l$, then $l < 8$. The only possibility satisfying this condition is $l = 4$, and indeed, $(3, 4, 4)$ is admissible. On the other hand, if $8 \mid l$, the choices are $l = 8$ and $l = 16$. The latter case is ruled out by Lemma 6.8, while the former gives the admissible triple $(3, 4, 8)$. □

Lemma 6.13. *There are no admissible triples of the form* $(3, 3^j, l)$ *with* $j > 1$*.*

Proof. Any such triple would have a subordinate triple of the form $(3, 9, l')$, so it suffices to prove that there are no admissible triples of this latter form. If $(3, 9, l')$ were an admissible triple, then z and y would either both have order 9, or both have order 18, depending on whether (13) or its negatives held. In either case, $l' < 18$ by Lemma 6.4. Moreover, 9 divides the orders of both z and y, so if $9 \nmid l'$, then Lemma 6.5 gives that $l' < 6$, and therefore $l' = 4$, but $(3, 9, 4)$ is inadmissible by Proposition 6.9. On the other hand, $9 \mid l'$ is also impossible, since no even numbers smaller than 18 satisfy that. Thus, there is no admissible triple of the form $(3, 9, l')$. □

Lemma 6.14. *Let (a, b, l) be an admissible triple with $a \in \{2, 3, 4\}$, and with b odd and relatively prime to a. If $b \mid l$, then (a, b, l) is one of $(2, 4, 4)$, $(2, 3, 6)$, $(2, 5, 10)$, or $(3, 5, 10)$.*

Proof. We first give an outline argument for showing that most triples of the form described above are inadmissible. Later, we will consider each of the cases $a = 2, 3, 4$ individually, filling in various details in the outline argument. This outline depends on the fact that $l \mid 6ab$, a fact that will later be established separately for each value of a.

Since a and b are relatively prime, we know that z and y must both have order either ab or $2ab$. Since $l \mid 6ab$, ζ can be expressed as $e^{2\pi i k/6ab}$. Now, from (14), we obtain

$$3b - 3a < k < 3b + 3a. \tag{22}$$

Now, consider an automorphism σ of K such that $\sigma(\zeta) = e^{2\pi i/l} = e^{2\pi i m/6ab}$. In order to respect (9), we must have either $\sigma(z + z^{-1}) > \sigma(\zeta + \zeta^{-1})$ or $\sigma(y + y^{-1}) > \sigma(\zeta + \zeta^{-1})$. Assume the former holds. This means that $\sigma(z) = e^{2\pi i d/6ab}$ with $1 \le |d| \le m$ (d may be positive or negative). Let us choose some small integers r and s such that

$$rd = sm, \qquad \text{so} \qquad \sigma(z)^r = \sigma(\zeta)^s.$$

If, instead, we have $\sigma(y + y^{-1}) > \sigma(\zeta + \zeta^{-1})$, then a relation of the form $\sigma(y)^r = \sigma(\zeta)^s$ is obtained. Applying σ^{-1}, we obtain either $z^r = \zeta^s$ or $y^r = \zeta^s$. Now, if we in fact have $z^r = \zeta^s$, then we obtain

$$r(3b + 3a) \equiv sk \pmod{6ab}.$$

That is, there is an integer n such that $sk = r(3b + 3a) + 6abn$. Combining this fact with (22), we deduce that

$$s(b - a) < r(b + a) + 2abn < s(b + a),$$

or

$$(s - r)/2a - r/2b - s/2b < n < (s - r)/2a - r/2b + s/2b. \tag{23}$$

If we had instead had $y^r = \zeta^s$, an analogous derivation would yield

$$(s - r)/2a + r/2b - s/2b < n < (s - r)/2a + r/2b + s/2b. \tag{24}$$

We will find that for each a and for most values of b, there are no integers satisfying (23) or (24), as appropriate. It follows that for that particular a and b, no triple (a, b, l) with $b \mid l$ is admissible. We now begin the case-by-case considerations.

For $a = 2$, z and y have order $2ab = 4b$. Since $l < 4b$ and l is even, we have $l = 2b$ and $m = 6$. In the notation of the outline argument, we have $d = \pm 3$, so we obtain $r = \pm 2$ and $s = 1$. If $r = 2$, no integers satisfy (23), while (24) is satisfied by no integers if $b \ge 7$. Similarly, if $r = -2$, (23) has no solutions if $b \ge 7$, but (24) has no solutions at all. Thus, the only triples of the desired form must have $b = 3$ or $b = 5$, and indeed, $(2, 3, 6)$ and $(2, 5, 10)$ are both admissible.

For $a = 3$, z and y have order $ab = 3b$. Since l is even, it must equal $2b$. It follows that $m = 9$ and $d = \pm 6$. This means that $r = \pm 2$ and $s = 2$. If $r = 2$, no integers satisfy either (23) or (24). If $r = -2$, no integers satisfy (23) if $b \geq 7$, and none satisfy (24) at all. From $b = 5$ we obtain the admissible triple $(3, 5, 10)$. (We do not consider $b = 3$, as b is assumed to be relatively prime to a.)

Finally, for $a = 4$, z and y have order $2ab = 8b$. Thus, l may be $2b$, $4b$, or $6b$. This means that $d = 3$, and m may be 12, 6, or 4. In these cases, the pair (r, s) may be one of $(\pm 4, 1)$, $(\pm 2, 1)$, or $(\pm 4, 3)$ respectively. A laborious but straightforward serious of calculations shows that no integers satisfy either (23) or (24) in any of these cases. □

Lemma 6.15. *There are no admissible triples* (a, b, l) *for which* (a, b) *is one of* $(3, 6)$*,* $(3, 10)$*,* $(3, 15)$*,* $(4, 6)$*, or* $(5, 6)$*.*

Proof. Suppose (a, b, l) is an admissible triple, with (a, b) one of the pairs named above. For none of these pairs is there a triple (a, b, l) with $l < 12$, according to Proposition 6.9, so $l \geq 12$. We now treat each of the four pairs individually.

$(3, 6)$: z has order 4 and y has order 12, so $l < 12$ by Lemma 6.4. This is a contradiction.

$(3, 10)$: z and y both have order 60, so $l < 60$. Now, 4 and 5 both divide the orders of z and y, but if either $4 \nmid l$ or $5 \nmid l$, then Lemma 6.5 would imply that $l < 8$ or $l < 10$ respectively, so in fact $20 \mid l$. Now, $l \neq 40$ because by Lemma 6.7, we know that $8 \nmid l$. Finally, the triple $(3, 4, 20)$ is inadmissible by Lemma 6.8.

$(3, 15)$: z and y have orders 10 and 30, respectively, if (13) holds, and orders 5 and 15, if the negatives of those formulas hold. In any case, we have $l < 30$ and $5 \mid l$ (applying Lemma 6.5 as above). Since l is even, this means $l = 20$, but Lemma 6.7 implies that $4 \nmid l$.

$(4, 6)$: z and y both have order 24. Since 8 divides the orders of z and y, we argue as above with Lemma 6.5 to conclude that $8 \mid l$. Since $12 \leq l < 24$, this means $l = 16$, yet $16 \nmid l$ by Lemma 6.7.

$(5, 6)$: z and y both have order 60. Just as in the case of $(a, b) = (3, 10)$, we find that $20 \mid l$, and that $l \neq 40$ by Lemma 6.7. To rule out $l = 20$, we use Corollary 6.6 with $p = 3$, as (17) is violated. □

Proposition 6.16. *Let* (a, b, l) *be an admissible triple, in which* a *and* b *are distinct prime powers, say* $a = p^i$ *and* $b = q^j$*. Then* (a, b, l) *is either of the form* $(2, q^j, 4)$*, or it is one of* $(3, 4, 4)$*,* $(3, 5, 4)$*,* $(2, 3, 6)$*,* $(2, 4, 6)$*,* $(2, 5, 6)$*,* $(3, 5, 6)$*,* $(2, 3, 8)$*,* $(3, 4, 8)$*,* $(2, 3, 10)$*,* $(2, 5, 10)$*, or* $(3, 5, 10)$*.*

Proof. We first treat the case in which $p = q$. By Corollary 6.3, we must have $p = 2$ or $p = 3$ and $i = 1$. All triples of the form $(2, 2^j, l)$ or $(3, 3^j, l)$ were identified in Lemmas 6.11 and 6.13, respectively.

Henceforth, we suppose $p \neq q$. By Lemma 6.4, we know that $l < 2ab$. Those triples in which $b \nmid l$ were identified in Proposition 6.10, so we now assume that $b \mid l$. We consider the cases $a \nmid l$ and $ab = l$. If $a \nmid l$, then if $p \geq 5$, or if $p = 3$ and $i > 1$, then Lemma 6.5 says that $l < 10$, but according to Proposition 6.9, there are no admissible triples with $l < 10$ and $a \geq 5$. Thus, we have either $a = 3$, or $a = 2^i$. If $a = 3$, then triples with $q = 2$ were identified in Lemma 6.12, while those with q odd were identified in Lemma 6.14. Finally, if $a = 2^i$, then b must be odd. If $i > 1$, then (a, b, l) would have a subordinate triple of the form $(4, b, l')$, but according to

Lemma 6.14, no such admissible triples exist. We conclude that $i = 1$, and note that all triples with $a = 2$ and b odd were identified in Lemma 6.14.

On the other hand, now suppose that $ab = l$. Since l is even, exactly one of p or q must be 2. If $q = 2$, then necessarily $j > 1$, since $q^j > a > 2$. If $a > 3$, then we can find a subordinate triple of the form $(4, a, l')$, contradicting Lemma 6.14, so $a = 3$. All triples of the form $(3, 2^j, l)$ were identified in Lemma 6.12. On the other hand, if $p = 2$, then again $i > 1$ would let us produce a subordinate triple $(4, b, l')$ that is forbidden by Lemma 6.14, so $i = 1$ and $a = 2$. All triples of the form $(2, b, l)$ were identified in Lemma 6.14. □

Theorem 6.17. *Let (a, b, l) be an admissible triple with $a \neq b$. Then, either it is of the form $(2, b, 4)$, or it is one of $(3, 4, 4)$, $(3, 5, 4)$, $(2, 3, 6)$, $(2, 4, 6)$, $(2, 5, 6)$, $(3, 5, 6)$, $(2, 3, 8)$, $(3, 4, 8)$, $(2, 3, 10)$, $(2, 5, 10)$, or $(3, 5, 10)$.*

Proof. Given an admissible triple (a, b, l), if p^i is any prime power dividing a and q^j is any prime power dividing b, then there is a subordinate triple either of the form (p^i, q^j, l) or (q^j, p^i, l). Assume for now that $a > 2$. We can therefore choose p^i and q^j such that neither of them is equal to 2. Examining Proposition 6.16, we find that each of p^i and q^j must be one of 3, 4, or 5. That is, these are the only possible prime powers dividing a and b, so a and b must both be divisors of $3 \cdot 4 \cdot 5 = 60$.

The factors of 60 larger than 2 are $\{3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$. Among the 45 possible pairs (a, b) with $a < b$ that might be formed out of these numbers, an immense number can be ruled out for the following reasons:

- The greatest common divisor of a and b must be 1, 2, or 3, by Corollary 6.3. This eliminates the 24 pairs $(4, 12)$, $(4, 20)$, $(4, 60)$, $(5, 10)$, $(5, 15)$, $(5, 20)$, $(5, 30)$, $(5, 60)$, $(6, 12)$, $(6, 30)$, $(6, 60)$, $(10, 15)$, $(10, 20)$, $(10, 30)$, $(10, 60)$, $(12, 20)$, $(12, 30)$, $(12, 60)$, $(15, 20)$, $(15, 30)$, $(15, 60)$, $(20, 30)$, $(20, 60)$, and $(30, 60)$.
- There cannot be a subordinate triple of the form $(4, 5, l')$, by Lemma 6.14. This eliminates the 7 pairs $(4, 5)$, $(4, 10)$, $(4, 15)$, $(4, 30)$, $(5, 12)$, $(10, 12)$, and $(12, 15)$.
- There cannot be a subordinate triple of the form $(3, 6, l)$, $(3, 10, l)$, $(3, 15, l)$, $(4, 6, l)$, or $(5, 6, l)$, by Lemma 6.15. This eliminates the 12 pairs $(3, 6)$, $(3, 10)$, $(3, 12)$, $(3, 15)$, $(3, 20)$, $(3, 30)$, $(3, 60)$, $(4, 6)$, $(5, 6)$, and $(6, 15)$.

Indeed, the only possibilities remaining are $(3, 4)$ and $(3, 5)$. All admissible triples for which (a, b) is one of these pairs were identified in Proposition 6.16.

Lastly, we consider the case $a = 2$. All admissible triples $(2, b, l)$ with $b \in \{3, 4, 5\}$ were identified in Proposition 6.16. We now simply need to show that if $b \geq 6$, then $l = 4$. For now, we must consider both (13) and its negatives, although afterwards, since we will have proved that $l \equiv 0 \pmod 4$, we will be able to choose z and y such that (13) holds.

For future reference, we record the orders of z and y in the following table.

	orders			
	$z = -e^{2\pi i(2+b)/4b}$	$y = -e^{2\pi i(b-2)/4b}$	$z = e^{2\pi i(2+b)/4b}$	$y = e^{2\pi i(b-2)/4b}$
$b \equiv 1 \pmod 2$	$4b$	$4b$	$4b$	$4b$
$b \equiv 0 \pmod 4$	$2b$	$2b$	$2b$	$2b$
$b \equiv 2 \pmod 8$	b	$\frac{1}{2}b$	$\frac{1}{2}b$	b
$b \equiv 6 \pmod 8$	$\frac{1}{2}b$	b	b	$\frac{1}{2}b$

Note, in particular, that the orders of z and y always divide $4b$. Also, observe that by Proposition 6.9, there are no triples $(2, b, l)$ with $b \geq 6$ and $6 \leq l \leq 10$. We must therefore show that $l \geq 12$ is also forbidden.

We first show that if $r^k \mid l$ but $r^k \nmid b$, where r is a prime number, then $r = 2$. If r is odd, it follows from the above table that r^k does not divide the orders of z or y, so by Lemma 6.7, $r < 4b/(2b-2-b) = 4b/(b-2)$. If $b \geq 10$, then this inequality implies $r = 3$, but for $b = 6$, both $r = 3$ and $r = 5$ are permitted. Write $\zeta = e^{2\pi i t}$ with $(b-2)/4b < t < (b+2)/4b$. Now, according to Corollary 5.5, if $r = 3$, then ζ is conjugate to at least one of $e^{2\pi i(t+1/3)}$ and $e^{2\pi i(t-1/3)}$. Using the fact that $b \geq 6$, it is easily verified that

$$e^{2\pi i(t+1/3)} + e^{-2\pi i(t+1/3)} < e^{2\pi i(b+2)/4b} + e^{-2\pi i(b+2)/4b} < e^{2\pi i(b-2)/4b} + e^{-2\pi i(b-2)/4b} < e^{2\pi i(t-1/3)} + e^{-2\pi i(t-1/3)},$$

so at least one conjugate of ζ yields a violation of 9. Similarly, if $r = 5$, ζ is conjugate to one of $e^{2\pi i(t\pm 2/5)}$, and the same reasoning applies. Therefore, $r = 2$.

Hence, l can be expressed as $2^m d$, where $d \mid b$. We may suppose that d is in fact the greatest common factor of l and b; *i.e.,* b/d is odd. Assume for now that $b/d > 1$, and let q be the largest prime divisor of b/d. If $q \geq 5$, then Lemma 6.5 implies that $l < 10$, so we are finished. If $q = 3$, and if $3^2 \mid b$, that same lemma again implies $l = 4$. If $q = 3$ and $3^2 \nmid b$, then we have that $b = 3d$. Since $l < 4b = 12d$, we see that $l \in \{d, 2d, 4d, 8d\}$. In particular, l is not divisible by b. In all cases, we have that $l \mid 8b$, so t can be written as a fraction $j/8b$. Recalling that $(b-2)/4b < t < (b+2)/4b$, we have $2b - 3 \leq j \leq 2b + 3$. If $j = 2b$, then clearly ζ is of order 4. It is readily verified that in each of the remaining cases $j = 2b \pm 1$, $j = 2b \pm 2$, or $j = 2b \pm 3$, one always has that the order of ζ is always divisible by b, contradicting the fact that $b \nmid l$. Thus, the assumption that $b/d > 1$ always leads to a contradiction.

Finally, we consider the case $b/d = 1$, so that $l = 2^m b$. By Lemma 6.4, and the above table showing orders of z and y, we see that $b \not\equiv 2 \pmod 4$. Indeed, further examination of that table shows that if b is odd, then $l = 2b$, while if $b \equiv 0 \pmod 4$, we have $l = b$. From Lemma 6.14, we know that there are no admissible triples $(2, b, 2b)$ with b odd and $b \geq 6$. On the other hand, if $b \equiv 0 \pmod 4$, then $t \in ((b-2)/4b), (b+2)/4b)$ should be a multiple of $1/b$, but the only multiple of $1/b$ in that interval is $1/4$. We thus conclude that there are no admissible triples $(2, b, l)$ with $b \geq 6$ and $l \neq 4$. □

With this result, we have also completed the proof of Theorem 3.14.

7. Application: Nebe root systems

The first definition of *root system* for complex reflection groups was given by Cohen [5]. In that paper, Cohen gave a new, self-contained classification of the complex reflection groups. (The Shephard-Todd classification relied on disparate earlier results going back to the late nineteenth century on "collineation groups generated by homologies.") He used root systems as a tool for studying the exceptional groups in dimension greater than 2.

However, Cohen's root systems seem not to lend themselves to axiomatic study as objects in their own right, primarily because there is no analogue of the requirement for ordinary root systems that the inner product of any coroot with any root be an integer. (Thus, even Weyl groups can have infinitely many inequivalent root systems in Cohen's definition.) Recently, Nebe [8]has proposed an intriguing new definition that seems much closer in spirit to the traditional definition of root systems for Weyl groups (following, say, Bourbaki [3]). The following definition is a slightly modified version of that appearing in [8]; the precise difference is explained below.

Definition 7.1. Let V be a finite-dimensional vector space over a finite abelian extension K of $\mathbb{Q}$. Let $\mathbb{Z}_K$ be the ring of integers of K, and let $\mathbb{Z}_K^*$ be its group of units. Also, let μ_K be the group of roots of unity in K, and let m be its order. Given a set $\Phi \subset V$, a function $e : \Phi \to \mathbb{N}$, and a generator η of μ_K, we call the triple (Φ, e, η) a *Nebe K-root system* if

(1) Φ consists of a finite number of $\mathbb{Z}_K^*$-orbits, spans V, and does not contain 0. The function e is constant on $\mathbb{Z}_K^*$-orbits in Φ, and $e(\alpha) \geq 2$ for all $\alpha \in \Phi$.
(2) Given a root $\alpha \in \Phi$, there exists an $\alpha^\vee \in V^*$ such that $\langle \alpha^\vee, \alpha \rangle = 1 - \eta^{m/e(\alpha)}$. In addition, the reflection s_α defined by $s_\alpha(x) = x - \langle \alpha^\vee, x \rangle \alpha$ satisfies $s_\alpha(\Phi) = \Phi$.
(3) For any $\alpha, \beta \in \Phi$, we have $\langle \alpha^\vee, \beta \rangle \in \mathbb{Z}_K$.
(4) For any $\alpha \in \Phi$, we have $K\alpha \cap \Phi = \mathbb{Z}_K^* \alpha$.

The subgroup of $GL(V)$ generated by the s_α is denoted $W(\Phi, e)$. The *rank* of the root system (Φ, e, η) is defined to be $\dim V$.

Two root systems (Φ, e, η) and (Φ', e', η'), in V and V' respectively, are said to be *isomorphic* if there is a linear isomorphism $T : V \xrightarrow{\sim} V'$ such that $T(\Phi) = \Phi'$, and for each $\alpha \in \Phi$, we have $e'(T\alpha) = e(\alpha)$ and $s_{T\alpha} = T s_\alpha T^{-1}$.

In Nebe's original definition [8], in lieu of a choice of generator η of μ_K, one implicitly chooses an imbedding $K \hookrightarrow \mathbb{C}$, and in the second axiom, the quantity $\eta^{m/e(\alpha)}$ is replaced by $e^{2\pi i/e(\alpha)}$. Note that two root systems (Φ, e, η) and (Φ', e', η') can be isomorphic even if $\eta \neq \eta'$; however, the condition $s_{T\alpha} = T s_\alpha T^{-1}$ is equivalent to requiring that $\eta^{m/e(\alpha)} = \eta'^{m/e(\alpha)}$.

Given a root system in a K-vector space V, we can, by Lemma 2.4, endow V with a $W(\Phi, e)$-invariant definite Hermitian form, and hence a conjugate-linear isomorphism $V^* \simeq V$. It is easy to verify that this isomorphism maps each coroot $\alpha^\vee$ to $\overline{(1 - \eta^{m/e(\alpha)})}(\alpha, \alpha)^{-1}\alpha$ (see [8]; the argument is exactly the same as Bourbaki's proof of the corresponding fact for ordinary root systems [3]). In view of this, the calculations of Section 3 can be interpreted as taking place in the context of a root system.

Now, the first step in Bourbaki's development of root systems is a thorough study of the possible relationships between just two roots. He finds that the "Cartan integer" $\langle \alpha^\vee, \beta \rangle \langle \beta^\vee, \alpha \rangle$ must be one of just four possible values—0, 1, 2, or 3—corresponding to the four rank-two root systems, of types $A_1 \times A_1$, A_2, B_2, and G_2, respectively. The results of this section are motivated by this approach.

Lemma 7.2. *Let W be a complex reflection group generated by two elementary reflections s and t, giving rise to an admissible triple (a, b, l). If s and t are conjugate in W, then $a = b$, and $N_{s,t} \in \mathbb{Z}_K^*$.*

Proof. Since a and b are the orders of s and t, respectively, it is obvious that they must be equal if s and t are conjugate. Let $\omega = \eta^{m/a}$. To prove that $N_{s,t}$ is invertible, we must rely on the fact that preferred admissible triples actually correspond to presentations for their corresponding groups, as given in [4] or Table 1.

Specifically, we note that if l were even, then we could define a homomorphism $f : W \to \mu_K$ by $f(s) = \eta^{m/a}$ and $f(t) = 1$. But this shows that s and t cannot be conjugate to one another if l is even.

Thus, l is odd. According to Proposition 3.9, we have

$$N_{s,t} = -\omega(\zeta + \zeta^{-1}) - \omega - \omega = -\omega(2 + \zeta + \zeta^{-1}) = -\omega(1 + \zeta)(1 + \zeta^{-1}),$$

where ζ is a primitive lth root of unity. It is an elementary fact that when l is odd, $1 + \zeta$ (and hence its conjugate $1 + \zeta^{-1}$) is invertible in $\mathbb{Z}_K$. Thus, $N_{s,t} \in \mathbb{Z}_K^*$. □

Theorem 7.3. *Let W be a complex reflection group generated by two reflections s and t giving rise to an admissible triple (a, b, l). Assume, in addition, that every reflection in W that fixes the reflecting hyperplane of s is in fact a power of s, and likewise for t. The isomorphism classes of Nebe root systems for W are in one-to-one correspondence with $\mathbb{Z}_K^*$-orbits of divisors of $N_{s,t}$. In any such root system, if α is any root for s, and β is any root for t, we have $\langle \alpha^\vee, \beta\rangle\langle \beta^\vee, \alpha\rangle = N_{s,t}$.*

The assumption about the generating reflections of W is minor: if we have a generator that does not satisfy this assumption, we can clearly always replace it by one that does. Also, note that in view of this theorem, one can determine all possible values of $\langle \alpha^\vee, \beta\rangle\langle \beta^\vee, \alpha\rangle$ by referring to Theorem 3.14 and Proposition 3.9.

Proof. Choose a divisor $q \in \mathbb{Z}_K$ of $N_{s,t}$. As we saw in the proof of Proposition 3.10, we may choose roots α and β for s and t such that

$$\langle \alpha^\vee, \beta\rangle = q, \qquad \langle \beta^\vee, \alpha\rangle = N_{s,t}/q.$$

Let us define $\Phi = \mathbb{Z}_K^*(W \cdot \alpha) \cup \mathbb{Z}_K^*(W \cdot \beta)$ and $e : \Phi \to \mathbb{N}$ by

$$e(\gamma) = \begin{cases} a & \text{if } \gamma \in \mathbb{Z}_K^*(W \cdot \alpha), \\ b & \text{if } \gamma \in \mathbb{Z}_K^*(W \cdot \beta) \end{cases}$$

We must verify that (Φ, e, η) is indeed a root system, and we must also check that its isomorphism class is determined by the $\mathbb{Z}_K^*$-orbit of q.

To begin with, let us check that $e : \Phi \to \mathbb{N}$ is indeed well-defined. If $\mathbb{Z}_K^*(W \cdot \alpha)$ meets $\mathbb{Z}_K^*(W \cdot \beta)$, or, more generally, if $K^\times(W \cdot \alpha)$ meets $K^\times(W \cdot \beta)$, then in particular, there exists some $z \in K^\times$ and $w \in W$ such that $w\beta = z\alpha$. This means that wtw^{-1} is a reflection (of order b) along the same root line as s, so by the assumption on the generators of W, wtw^{-1} is a power of s, and b divides a. On the other hand, $w^{-1}sw$ is a power of t, so we see that if $K^\times(W \cdot \alpha)$ meets $K^\times(W \cdot \beta)$, then $a = b$. (Indeed, since wtw^{-1} and s are both elementary reflections of the same order along the root line, they are equal: s and t are conjugate.) Thus e is unambiguously defined in every case.

Next, we define coroots by the conjugate-linear isomorphism $V \simeq V^*$ mentioned above: for each $\gamma \in \Phi$, we define $\gamma^\vee \in V^*$ to be the point identified with $\overline{(1 - \eta^{m/e(\gamma)})}(\gamma, \gamma)^{-1}\gamma \in V$.

Recall from the proof of Proposition 3.10 that s and t, and therefore all $w \in W$, act by matrices with $\mathbb{Z}_K$-coefficients with respect to the basis consisting of α and β. It follows that $\Phi \subset \mathbb{Z}_K\alpha + \mathbb{Z}_K\beta$. Since $\langle \alpha^\vee, \alpha\rangle$ and $\langle \alpha^\vee, \beta\rangle$ are both in $\mathbb{Z}_K$, it follows that $\alpha^\vee, \delta\rangle \in \mathbb{Z}_K$ for all $\delta \in \Phi$. Likewise, $\langle \beta^\vee, \delta\rangle \in \mathbb{Z}_K$ for all $\delta \in \Phi$ as well.

Now, we check the axioms. Axiom (1) is obvious. For axioms (2) and (3), assume that we are considering a root $\gamma \in \mathbb{Z}_K^*(W \cdot \alpha)$, say $\gamma = zw\alpha$ ($z \in \mathbb{Z}_K^*$, $w \in W$).

(The proof is the same if $\gamma \in \mathbb{Z}_K^*(W \cdot \beta)$ instead.) Therefore, $e(\gamma) = a$, and, since W preserves the Hermitian form on V, we have

$$(\gamma, \gamma) = (zw\alpha, zw\alpha) = \bar{z}z(\alpha, \alpha).$$

We have

$$\begin{aligned} s_\gamma(x) &= x - \langle \gamma^\vee, x \rangle \gamma = x - \frac{(1 - \eta^{m/a})(\gamma, x)}{(\gamma, \gamma)} \gamma \\ &= x - \frac{(1 - \eta^{m/a})\bar{z}(w\alpha, x)}{\bar{z}z(\alpha, \alpha)} zw\alpha \\ &= w \left(x - \frac{(1 - \eta^{m/a})(\alpha, w^{-1}x)}{(\alpha, \alpha)} \alpha \right) = ws(w^{-1}x). \end{aligned}$$

Since $s_\gamma = wsw^{-1}$, it is obvious that $s_\gamma(\Phi) = \Phi$.

Next, for any $\delta \in \Phi$, we have

$$\langle \gamma^\vee, \delta \rangle = \frac{(1 - \eta^{m/a})\bar{z}}{\bar{z}z(\alpha, \alpha)} (w\alpha, \delta) = z^{-1} \langle \alpha^\vee, w^{-1}\delta \rangle.$$

As we remarked above, $\langle \alpha^\vee, w^{-1}\delta \rangle \in \mathbb{Z}_K$, and since $z \in \mathbb{Z}_K^*$, we conclude that $\langle \gamma^\vee, \delta \rangle \in \mathbb{Z}_K$ as well.

Finally, we must verify axiom (4). Since W preserves the Hermitian form on V, it is clear that $K\gamma \cap W \cdot \gamma \subset \mu_K \gamma \subset \mathbb{Z}_K^* \gamma$. Then, since

$$K\gamma \cap \mathbb{Z}_K^*(W \cdot \alpha) = K\gamma \cap \mathbb{Z}_K^*(W \cdot \gamma) = \mathbb{Z}_K^*(K\gamma \cap W \cdot \gamma)$$

we conclude that $K\gamma \cap \mathbb{Z}_K^*(W \cdot \alpha) = \mathbb{Z}_K^* \gamma$. It remains to consider $K\gamma \cap \mathbb{Z}_K^*(W \cdot \beta)$. In the case that $K^\times(W \cdot \alpha)$ and $K^\times(W \cdot \beta)$ do not meet, we clearly have $K\gamma \cap \mathbb{Z}_K^*(W \cdot \beta) = \varnothing$, so $K\gamma \cap \Phi = \mathbb{Z}_K^* \gamma$, as desired. On the other hand, suppose $K^\times(W \cdot \alpha)$ and $K^\times(W \cdot \beta)$ do intersect (and so, as discussed above, s and t are conjugate, and $a = b$). Suppose, in particular, that there is some root $\delta \in K\gamma \cap \mathbb{Z}_K^*(W \cdot \beta)$, where $\delta = c\gamma$ for some $c \in K^\times$. We must show that $c \in \mathbb{Z}_K^*$. If $\delta = z_1 w_1 \beta$ (where $z_1 \in \mathbb{Z}_K^*$, $w_1 \in W$), then the root $\delta_1 = z^{-1}w^{-1}\delta = z^{-1}z_1 w^{-1} w_1 \beta$ satisfies $\delta_1 = c\alpha$. Now,

$$\langle \delta_1^\vee, \beta \rangle = \frac{(1 - \eta^{m/a})(c\alpha, \beta)}{(c\alpha, c\alpha)} = c^{-1} \langle \alpha^\vee, \beta \rangle,$$

and similarly, $\langle \beta^\vee, \delta_1 \rangle = c \langle \beta^\vee, \alpha \rangle$. We know from Lemma 7.2 that $N_{s,t}$, and hence both $\langle \alpha^\vee, \beta \rangle$ and $\langle \beta^\vee, \alpha \rangle$, are in $\mathbb{Z}_K^*$. Therefore, the quantities

$$c = \frac{\langle \beta^\vee, \delta_1 \rangle}{\langle \beta^\vee, \alpha \rangle} \qquad \text{and} \qquad c^{-1} = \frac{\langle \delta_1^\vee, \beta \rangle}{\langle \alpha^\vee, \beta \rangle}$$

are both in $\mathbb{Z}_K$, so $c \in \mathbb{Z}_K^*$, as desired. □

8. Collineation groups and Shephard-Todd Families

When Shephard and Todd first classified complex reflection groups in 1954 [9], they treated the exceptional groups (*i.e.,* those groups not in the infinite series $G(r, p, n)$, also called primitive groups) by referring to known classifications of certain finite subgroups of $PGL(V)$, called "collineation groups generated by homologies." (Here, a "homology" is simply the image in $PGL(V)$ of a reflection of V.) For each such group, they worked out the list of possible preimages in $GL(V)$ that are generated by reflections. Their methods thus naturally give a grouping of the exceptional complex reflection groups into families: two groups are in the same family if they have the same image in $PGL(V)$.

A cursory glance at the tables in [9] shows that these families coincide with the grouping in Table 1 by the J-group parameters a, b, c. In fact, this phenomenon has a uniform explanation that applies equally well to the rank-two complex reflection groups in the infinite series.

Specifically, let us define a group

$$P(a\,b\,c) = J\left(\begin{smallmatrix} a & b & c \end{smallmatrix}\right)/\langle stu\rangle.$$

According to [4], the center of each finite group $J\left(\begin{smallmatrix} a & b & c \end{smallmatrix}\right)$ is precisely the subgroup generated by stu, so the image of $J\left(\begin{smallmatrix} a & b & c \end{smallmatrix}\right)$ in $PGL(V)$ is precisely the quotient by that subgroup.

Proposition 8.1. *For any a', b', and c', the natural map $J\left(\begin{smallmatrix} a & b & c \\ a' & b' & c' \end{smallmatrix}\right) \to P(a\,b\,c)$ is surjective.*

Proof. Let $J = J\left(\begin{smallmatrix} a & b & c \end{smallmatrix}\right)$, $J' = J\left(\begin{smallmatrix} a & b & c \\ a' & b' & c' \end{smallmatrix}\right)$, and $P = P(a\,b\,c)$. Also, let D be the quotient of J obtained by making $s^{a'}$, $t^{b'}$, and $u^{c'}$ central: in other words, D is obtained by adding the following relations:

$$s^{a'}t = ts^{a'}, \quad s^{a'}u = us^{a'}, \quad t^{b'}s = st^{b'}, \quad t^{b'}u = ut^{b'}, \quad u^{c'}s = su^{c'}, \quad u^{c'}t = tu^{c'}.$$

Let D' and C be the quotients of J' and P, respectively, obtained by adding these same relations. Let $\pi : J \to D$, $j : J \to P$, and $k : D \to C$ be the quotient maps.

$$\begin{tikzcd}
J' \subset J \arrow[r, "j"] \arrow[d, "\pi"'] & P \arrow[d] \\
D' \subset D \arrow[r, "k"] & C
\end{tikzcd}$$

We remark that the kernel π is precisely the normal closure of the subgroup generated by the six elements $s^{a'}t(ts^{a'})^{-1}, s^{a'}u(us^{a'})^{-1}, \ldots, u^{c'}t(tu^{c'})^{-1}$. In other words, this kernel is generated by all conjugates

$$w \cdot s^{a'}t(ts^{a'})^{-1} \cdot w^{-1}, \qquad w \in J,$$

and the corresponding elements for the other five new relations. Now, each such conjugate can be expressed as a product of commutators:

$$\begin{aligned} w \cdot s^{a'}t(ts^{a'})^{-1} \cdot w^{-1} &= ws^{a'}ts^{-a'}t^{-1}w^{-1} \\ &= ws^{a'}w^{-1}s^{-a'}s^{a'}wts^{-a'}t^{-1}w^{-1} = ws^{a'}w^{-1}s^{-a'} \cdot s^{a'}(wt)s^{-a'}(wt)^{-1}. \end{aligned}$$

Now, it is clear that any commutator of $s^{a'}$ (or $t^{b'}$ or $u^{c'}$) with an arbitrary element of J is in the kernel of π. From the above calculation, we deduce that this kernel is in fact generated by such commutators.

Our goal is to prove that $j|_{J'}$ is surjective. We begin by observing that $J' = \pi^{-1}(D')$: since J' is defined as a normal closure, it is generated by the set

$$\{ws^{a'}w^{-1} \mid w \in J\} \cup \{wt^{b'}w^{-1} \mid w \in J\} \cup \{wu^{c'}w^{-1} \mid w \in J\}.$$

Now, D' need not be defined as a normal closure: since $s^{a'}$, $t^{b'}$, and $u^{c'}$ are in the center of D, the subgroup they generate is already normal. The preimage of D' in J, therefore, is generated by $s^{a'}$, $t^{b'}$, $u^{c'}$, and the kernel of π. That kernel, in turn, is generated by commutators of those three elements with arbitrary elements of J. Thus, $\pi^{-1}(D')$ is generated by

$$\{s^{a'}, t^{b'}, u^{c'}\} \cup \{ws^{a'}w^{-1}s^{-a'} \mid w \in J\} \cup \\ \{wt^{b'}w^{-1}t^{-b'} \mid w \in J\} \cup \{wu^{c'}w^{-1}u^{-c'} \mid w \in J\}$$

It is now clear that $\pi^{-1}(D') = J'$.

Next, we claim that if $k|_{D'}$ is surjective, then so is $j|_{J'}$. If $k|_{D'}$ is surjective, then every element of D differs from some element of D' by an element of $\ker k$. Since this kernel is precisely the subgroup of D generated by stu, the surjectivity of $k|_{D'}$ would mean that every element of D can be written in the form

$$(s^{a'})^m (t^{b'})^n (u^{c'})^p (stu)^q. \tag{25}$$

In turn, this means that every element of J can be written as

$$(s^{a'})^m (t^{b'})^n (u^{c})^p (stu)^q x,$$

for some $x \in \ker \pi$. Now, since $\ker \pi \subset J'$, and since stu is in the center of J, it follows that every element of J can be written as $y(stu)^q$, with $y \in J'$, and thence that the map $j|_{J'}$ is surjective.

Thus, it suffices to prove that $k|_{D'}$ is surjective. Specifically, we must show that in D, each of s, t, and u can be written in the form (25). Now, an examination of Table 1 shows that in any finite J-group, at least one of the parameters a', b', or c' is 1. Suppose, without loss of generality, that $a' = 1$. The fact that s can be written in the form (25) is then self-evident. Next, using the fact that stu and s are both central in D, it is easy to prove that

$$(stu)^q = s^q t^q u^q$$

for any q. Since b' and c' are relatively prime, we can find integers d and e such that

$$b'd + c'e = 1.$$

Using the centrality of s and $u^{c'}$, we calculate:

$$(s^1)^{-c'e}(t^{b'})^d(u^{c'})^{-e}(stu)^{c'e} = (s^1)^{-c'e}(t^{b'})^d(u^{c'})^{-e}s^{c'e}t^{c'e}(u^{c'})^e = t^{b'd+c'e} = t.$$

A similar calculation shows that $(s^1)^{-b'd}(t^{b'})^{-d}(u^{c'})^e(stu)^{b'd} = u$. Thus, $k|_{D'}$ is surjective, and the proposition is proved. □

Corollary 8.2. *Two finite J-groups $J\left(\begin{smallmatrix} a & b & c \\ a' & b' & c' \end{smallmatrix}\right)$ and $J\left(\begin{smallmatrix} d & e & f \\ d' & e' & f' \end{smallmatrix}\right)$ are in the same Shephard-Todd family if and only if the parameters (a, b, c) are equal (up to permutation) to the parameters (d, e, f).*

References

[1] P. Achar and A.-M. Aubert, *Sur une classe d'algèbres de type de Hecke*, in preparation.

[2] D. J. Benson, *Polynomial Invariants of Finite Groups.* London Mathematical Society Lecture Notes Series, 190. Cambridge University Press, Cambridge, 1993.

[3] N. Bourbaki, *Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV: Groupes de Coxeter et systèmes de Tits. Chapitre V: Groupes engendrés par des réflexions. Chapitre VI: Systèmes de racines*, Actualités Scientifiques et Industrielles, No. 1337, Hermann, Paris, 1968.

[4] M. Broué, G. Malle, and R. Rouquier, *Complex reflection groups, braid groups, Hecke algebras*, J. Reine Angew. Math. **500** (1998), 127–190.

[5] A. M. Cohen, *Finite complex reflection groups*, Ann. Sci. École Norm. Sup. (4) **9** (1976), 379–436.

[6] M. Hughes et A. Morris, *Root systems for two dimensional complex reflection groups*, Sém. Lothar. Combin. **45** (2000/01), Art. B45e, 18 pp.

[7] G. Malle, *Degrés relatifs des algèbres cyclotomiques associées aux groupes de réflexions complexes de dimension deux*, Finite reductive groups (Luminy, 1994), Progr. Math., vol. 141, Birkäuser Boston, 1997, pp. 311–332.

[8] G. Nebe, *The root lattices of the complex reflection groups*, J. Group Theory **2** (1999), 15–38.

[9] G. C. Shephard and J. A. Todd, *Finite unitary reflection groups*, Canad. J. Math **6** (1954), 274–304.