ENUMERATING ISOCLINISM CLASSES OF SEMI-EXTRASPECIAL GROUPS

MARK L. LEWIS AND JOSHUA MAGLIONE

ABSTRACT. We enumerate the number of isoclinism classes of semi-extraspecial p-groups with derived subgroup of order p^2. To do this, we enumerate $\mathrm{GL}(2, p)$-orbits of sets of irreducible, monic polynomials in $\mathbb{F}_p[x]$. Along the way, we also provide a new construction of an infinite family of semi-extraspecial groups as central quotients of Heisenberg groups over local algebras.

1. INTRODUCTION

All groups in this paper are finite, and p is a prime. A p-group G is said to be *semi-extraspecial* if every subgroup N having index p in $Z(G)$ satisfies the condition that G/N is extra-special. Semi-extraspecial groups are a special case of Camina groups, i.e. groups G where every irreducible character vanishes on $G \backslash G'$ [C, M1, CMS]. In fact, semi-extraspecial groups are exactly the Camina p-groups of class 2 [V2, Theorem 1.2].

These groups are virtually indistinguishable, so in the context of group isomorphism and enumeration, they pose a challenge. Indeed, the (nontrivial) central quotients of Heisenberg groups over fields, considered in [LW], are all semi-extraspecial groups. Those quotients have exponent p, isomorphic character tables, two possible orders of centralizers, and a limited number of possible isomorphism types of automorphism groups—after fixing the order of the group and derived subgroup.

Applying ideas of Brooksbank-Maglione-Wilson [BMW], we the study of semi-extraspecial p-groups G with $|G'| = p^2$ by considering a $\mathrm{PGL}(2, p)$-action on multi-sets of polynomials in $\mathbb{F}_p[x]$. In particular, we enumerate the number of isoclinism classes of such groups up to order p^{12}. A slight extension of Verardi [V2, Corollary 5.11] states that there is a unique isoclinism class of semi-extraspecial groups G with $|G| = p^6$ and $|G'| = p^2$ for each prime p. We show that a similar result holds for the next larger size of semi-extraspecial groups.

Theorem 1.1. *For each prime p, there is a unique isoclinism class of semi-extraspecial groups G with $|G| = p^8$ and $|G'| = p^2$.*

At this point, one might be tempted to conjecture for every prime p and every positive integer n that there is a unique isoclinism class of semi-extraspecial groups G with $|G| = p^{2n+2}$ and $|G'| = p^2$. However, starting with the next size, we will see that the situation becomes more complicated.

Theorem 1.2. *For every prime p, there are $p + 3 - \gcd(2, p)$ isoclinism classes of semi-extraspecial groups G with $|G| = p^{10}$ and $|G'| = p^2$.*

For the next size, the formula gets even more complicated.

Theorem 1.3. *For every prime p, the number of isoclinism classes of semi-extraspecial groups G with $|G| = p^{12}$ and $|G'| = p^2$ is*

$$\frac{1}{30} \left(11p^2 - 5p - 22 + 10 \gcd(3, p-2) + 6 \gcd(5, p) + 12 \gcd(5, p^2 - 1)\right).$$

We could continue in this fashion and find formulas, depending on p, for the number of isoclinism classes of semi-extraspecial groups G with $|G| = p^{2n+2}$ and $|G'| = p^2$ for values of n that are larger than 5. However, these functions appear to get progressively more complicated as n increases, and we believe that these cases illustrate the procedure so that the sufficiently motivated reader can compute the function for larger n if desired.

Along the way to enumerating these isoclinism classes, we find a new way to construct an infinite family of semi-extraspecial groups. To date, all known constructions of semi-extraspecial groups begin with a semifield A or by taking a central product of semi-extraspecial groups. A (finite) semi-field is an algebra with identity where the product $a * b = 0$ if and only if either $a = 0$ or $b = 0$. Since A is finite, this implies that every nonzero element has both a left inverse and a right inverse. However, since A is not necessarily associative or commutative, these left and right inverses need not be equal. It is this invertibility condition that makes the following groups semi-extraspecial.

If A is any algebra, the Heisenberg group over A is the group

$$(1.4) \qquad H(A) = \left\{ \begin{bmatrix} 1 & e & z \\ & 1 & f \\ & & 1 \end{bmatrix} \;\middle|\; e, f, z \in A \right\}.$$

It is not difficult to see that $H(A)$ is semi-extraspecial if and only if A is a semi-field [L1]. Because $H(A)$ is semi-extraspecial when A is a semifield, every central quotient is either abelian or semi-extraspecial. One can twist the semifield group in (1.4) to get a different class of semi-extraspecial groups [L2]. At this time, the only way we know how to construct a semi-extraspecial group is to take a quotient of $H(A)$ for a semifield A, a quotient of the twisted semifield groups in [L2], or to take central products of these groups.

To obtain the new construction in this paper, we start with an algebra A with zero divisors. Because of the zero divisors, $H(A)$ is not semi-extraspecial. We correct this by constructing the quotient by a subspace that complements the minimal ideal in A.

Theorem 1.5. *Let K be a finite field, $a(x) \in K[x]$ be irreducible of degree ≥ 2, and let $c > 1$ be an integer. Suppose $S \leq A$ is a K-subspace, and set $G = H(A)/N(S)$, where*

$$N(S) = \left\{ \begin{bmatrix} 1 & 0 & s \\ & 1 & 0 \\ & & 1 \end{bmatrix} \;\middle|\; s \in S \right\}.$$

Then G is semi-extraspecial if, and only if, $A = S + (a(x)^{c-1})$.

We ask whether all of the groups in Theorem 1.5 are also central quotients of the semifield groups in (1.4). This is true for all of the ones we have been able to determine. The case we have studied most closely are the quotients of the semifield groups of order 3^{12}. We note that although there are many infinite families of

semifields that have been constructed [JJB, K1], there is no evidence that these families contain all of them. Indeed, they do not span the table of semifields of order 81 [D1]. Going back to our initial question, we ask if G is as in Theorem 1.5, then does there exist a semifield A of order p^{cd} such that $G \cong H(A)/Z$ where Z is some proper subgroup of the center of $H(A)$? It is possible that the construction in Theorem 1.5 might yield new semi-extraspecial groups that do not arise as a quotient of a group associated with any semifield.

2. Groups and bilinear maps

Assume that K is a field and U, V, and W are K-vector spaces. A map $\circ : U \times V \rightarrowtail W$ is K-bilinear if for all $u, u' \in U$, $v, v' \in V$, and $k \in K$,

$$(u + ku') \circ v = u \circ v + k(u' \circ v), \qquad u \circ (v + kv') = u \circ v + k(u \circ v').$$

We will use $\rightarrowtail$ to denote a bilinear map (bimap), and in the case where $\dim_K(W) = 1$, we call $\circ$ a bilinear *form*. The *radicals* of $\circ$ are $U^\perp = \{v \in V \mid U \circ v = 0\}$ and $V^\perp = \{u \in U \mid u \circ V = 0\}$. The bimap $\circ$ is *nondegenerate* if $U^\perp$ and $V^\perp$ are trivial, and $\circ$ is *full* if $U \circ V = W$. We say a bimap is *fully nondegenerate* if it is both full and nondegenerate.

Our main source of bimaps come from finite p-groups, G, of exponent p and class 2, via the Baer correspondence. For such a group we define the biadditive commutator map to be $\circ_G : G/Z(G) \times G/Z(G) \rightarrowtail G'$, where

$$(Z(G)g) \circ (Z(G)h) = [g, h].$$

Then $\circ_G$ is $\mathbb{F}_p$-bilinear and fully nondegenerate. In the case when G is semi-extraspecial, both $G/Z(G)$ and G' are elementary abelian, and we write $\circ_G : V \times V \rightarrowtail W$, where $V = G/Z(G)$ and $W = G'$.

Two bimaps $\circ, \bullet : V \times V \rightarrowtail W$ are *pseudo-isometric* if there exists $(f, g) \in \mathrm{Aut}(V) \times \mathrm{Aut}(W)$ such that for all $u, v \in V$, $(uf) \bullet (vf) = (u \circ v)g$. The bimaps are *isometric* if they are pseudo-isometric with pseudo-isometry $(f, 1)$. In [H1], Hall initiated a study of p-groups up to isoclinism as a weaker form of isomorphism. Two class 2 groups G and H are *isoclinic* if there exists isomorphisms between $f : G/Z(G) \to H/Z(H)$ and $g : G' \to H'$ such that (f, g) is a pseudo isometry from $\circ_G$ to $\circ_H$.

Definition 2.1. A class 2 p-group G is *semi-extraspecial* if $G' = Z(G) = G^p$ and if for all $g \in G \backslash Z(G)$ and $z \in G'$, there exists $h \in G$ such that $[g, h] = z$.

In the context of bimaps, $\circ : V \times V \rightarrowtail W$, this is equivalent to the following. For all $u \in V$ the linear maps $L_u, R_u : V \to W$, where $vL_u = u \circ v$ and $vR_u = v \circ u$, are surjective. As our bimaps are alternating, it is enough to check this for just This implies that $\dim(W) \leq \dim(V)$.

An important algebra associated to a K-bimap $\circ : V \times V \rightarrowtail W$ is its centroid: the largest algebra C for which is C-bilinear. For $\Omega = \mathrm{End}(U) \times \mathrm{End}(V) \times \mathrm{End}(W)$, the centroid is

$$\mathcal{C}(\circ) = \{(X, Y, Z) \in \Omega \mid (uX) \circ v = u \circ (vY) = (u \circ v)Z\}.$$

If $\circ$ is fully nondegenerate, then $\mathcal{C}(\circ)$ is commutative. The centroid plays a critical role in direct decompositions of groups [W1] and in the definition of genus [BMW].

2.1. **Pfaffians of bimaps.** Fix a K-bimap, $\circ : V \times V \rightarrowtail W$. For $\omega \in W^* :=$ $\text{Hom}(W, K)$, define $\circ^\omega : U \times V \rightarrowtail K$ where

$$u \circ^\omega v = (u \circ v)\omega.$$

Fix a basis $\mathcal{X}$ for V and $\mathcal{Z}^*$ for W^*. For each $\omega \in \mathcal{Z}^*$, write $\circ^\omega$ as a matrix M_ω with respect to $\mathcal{X}$, the structure constants of the K-form $\circ^\omega$. The *generalized discriminant* of $\circ : V \times V \rightarrowtail W$, with respect to $\mathcal{X}$ and $\mathcal{Z}^*$, is a polynomial in indeterminants x_ω, for $\omega \in \mathcal{Z}^*$, where

$$\text{disc}(\circ) = \det \left(\sum_{\omega \in \mathcal{Z}^*} M_\omega x_\omega \right).$$

When $\circ$ is *alternating*, i.e. for all $u \in V$, $u \circ u = 0$, define the (*generalized*) *Pfaffian* of $\circ$ to be the homogeneous polynomial $\text{Pf}(\circ)$ such that $\text{Pf}(\circ)^2 = \text{disc}(\circ)$.

The next theorem is due to I.D. Macdonald [M1] who proved the conclusion for Camina groups.

Theorem 2.2 ([M1, Theorem 3.1]). *A Pfaffian of $\circ_G : V \times V \rightarrowtail W$ has no solutions in $\mathbb{P}W$ if, and only if, G is semi-extraspecial.*

3. Decompositions, groups of genus 2, and Pfaffians

A *central decomposition* of a group G is a set $\mathcal{H} = \{H : H \leq G\}$ such that $\langle \mathcal{H} \rangle = G$, for all $H \in \mathcal{H}$, $\langle \mathcal{H} - H \rangle \neq G$, and $[H, \langle \mathcal{H} - H \rangle] = 1$. Note that this definition allows for $Z(H_1) \neq Z(H_2)$ for $H_1, H_2 \in \mathcal{H}$. A group G is *centrally indecomposable* if $\{G\}$ is the only central decomposition of G. A *direct decomposition* of G is a central decomposition $\mathcal{H}$ such that for all $H \in \mathcal{H}$, $H \cap \langle \mathcal{H} - H \rangle = 1$, and G is *directly indecomposable* if $\{G\}$ is the only direct decomposition of G. We say a central (or direct) decomposition $\mathcal{H}$ is *fully-refined* if for all $H \in \mathcal{H}$, H is centrally (or directly) indecomposable.

Lemma 3.1. *If G is semi-extraspecial, then G is directly indecomposable.*

Proof. Suppose $\mathcal{H}$ is a direct decomposition of G with $H, K \in \mathcal{H}$. By definition, $[G, H] \leq H$, but since G is semi-extraspecial, it follows that for all $z \in Z(K)$, there exists $g \in G$ such that $[g, h] = z$. Therefore, $H = K$, so $\mathcal{H} = \{G\}$. $\qquad\square$

The central product of G with H can be defined as a central quotient of $G \times H$ with an isomorphism $\theta : Z(G) \to Z(H)$, c.f. Hall [H1]. We note that different isomorphisms θ may produce non-isomorphic central products of groups. Our definition above allows for the case where $Z(G)$ may properly embed into $Z(H)$. Because of this, we prove that with semi-extraspecial groups, we must have all the centers of each central factor isomorphic. The following proposition is a slight generalization of Beisiegel [B, Lemma 2].

Proposition 3.2. *Suppose $\mathcal{H}$ is a central decomposition of G such that each $H \in \mathcal{H}$ is semi-extraspecial. Then G is semi-extraspecial if, and only if, for each $H \in \mathcal{H}$, $Z(H) = Z(G)$.*

Proof. First, we suppose that for all $H \in \mathcal{H}$, $Z(H) = Z(G)$. If $N < Z(G)$ is a maximal subgroup, then N is a maximal subgroup of each $Z(H)$. Therefore, H/N is extraspecial, and $G/N = \langle H/N : H \in \mathcal{H} \rangle$, where $Z(H/N) = Z(G/N)$. This is a central decomposition of G/N into extraspecial groups; hence, G/N is extraspecial.

Conversely, suppose there exists $H \in \mathcal{H}$ such that $Z(H) \neq Z(G)$. Let $N < Z(G)$ be a maximal subgroup. If $Z(H) > Z(G)$, then N is not a maximal subgroup of $Z(H)$, and in particular, H/N is not extraspecial. Therefore, $\langle HN/N : H \in \mathcal{H} \rangle$ cannot be extraspecial, so G is not semi-extraspecial. On the other hand, suppose there exists $z \in Z(G)$ such that $z \notin Z(H) = H'$. Then for all $h \in H$ and $g \in H$, $[g, h] \neq z$. From the central decomposition property, it follows that for all $h \in H$ and $g \in G$, $[g, h] \neq z$, so that G is not semi-extraspecial. $\qquad \square$

We state a useful theorem of Wilson [W1] characterizing direct decompositions of p-groups of class 2. A commutative ring is *local* if it has a unique maximal ideal.

Theorem 3.3 ([W1, Theorem 8]). *Let G be class 2 and exponent p. Then $\mathcal{C}(\circ_G)$ is a local $\mathbb{F}_p$-algebra if, and only if, G is directly indecomposable.*

Lemma 3.1 together with Theorem 3.3 are key to proving the following proposition. In general for fully nondegenerate bimaps, the centroid is a commutative ring. In the next lemma, we show that because $\mathcal{C}(\circ_G)$ is Artinian with trivial nilradical, $\mathcal{C}(\circ_G)$ must be a simple $\mathbb{F}_p$-algebra.

Proposition 3.4. *If G is semi-extraspecial, then $\mathcal{C}(\circ_G)$ is a field.*

Proof. Suppose $(X, Z) \in \mathcal{C}(\circ_G) \subseteq \mathrm{End}(V) \times \mathrm{End}(W)$ is nilpotent. For all $u \in V$, we claim that the linear map $L_{uX} : V \to W$, where $v \mapsto (uX) \circ v$, is not surjective. In fact, since $(X, Z) \in \mathcal{C}(\circ_G)$, it follows that $\mathrm{im}(L_{uX}) \leq \mathrm{im}(Z)$. As Z is nilpotent, $\mathrm{im}(Z) < W$, so for all $g \in G$, there exists $z \in Z(G)$ such that $z \notin [g, G]$. This would imply that G is not semi-extraspecial. Therefore, the nilradical of $\mathcal{C}(\circ_G)$ is trivial. Since $\mathcal{C}(\circ_G)$ is Artinian (in particular finite), it follows that $\mathcal{C}(\circ_G)$ is semi-simple. By Lemma 3.1 and Theorem 3.3, it follows that $\mathcal{C}(\circ_G)$ is a simple $\mathbb{F}_p$-algebra. Because $\circ_G$ is fully nondegenerate, $\mathcal{C}(\circ_G)$ is commutative, and by the Wedderburn–Artin Theorem, $\mathcal{C}(\circ_G)$ is a field. $\qquad \square$

Remark 3.5. Because $K = \mathcal{C}(\circ_G)$ is a field and $\circ_G$ is K-bilinear, we now assume throughout that $\circ_G : V \times V \rightarrowtail W$ is a bimap over K, so V and W are K-vector spaces. Another fact that we will use later is that $\mathcal{C}(\circ_G)$ is faithfully represented on all three coordinates whenever $\circ_G$ is fully nondegenerate; in particular it is faithfully represented in $\mathrm{End}(W)$. Indeed, if $(X, Z), (Y, Z) \in \mathcal{C}(\circ_G) \subseteq \mathrm{End}(V) \times \mathrm{End}(W)$, then for all $u, v \in V$, $(uX - uY) \circ_G v = 0$. Because $\circ_G$ has trivial radical, $X = Y$.

Definition 3.6. Suppose G is a nilpotent class 2 and isoclinic to a direct product $H_1 \times \cdots \times H_r$ of directly indecomposable groups. The *genus* of G is the maximum rank of $[H_i, H_i]$ as a $\mathcal{C}(\circ_{H_i})$-module.

Lemma 3.1 and Proposition 3.4 enable a simpler definition of genus for our purposes. The genus of a semi-extraspecial group G is the dimension of G' as a $\mathcal{C}(\circ_G)$-vector space. We will say a (semi-extraspecial) group G is *genus d over K* if $\mathcal{C}(\circ_G) \cong K$ and $\dim_K(G') = d$.

3.1. **Groups of genus 2.** We cite two key theorems from [BMW] that we use later. Involved in the classification of groups of genus 2 are Heisenberg groups over local algebras, $A = K[x]/(a(x)^c)$, where $a(x)$ is irreducible in $K[x]$ and $c \geq 1$,

$$H(A) = \left\{ \begin{bmatrix} 1 & e & z \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix} \;\middle|\; e, f, z \in A \right\}.$$

Observe that $H(A)$ is semi-extraspecial if, and only if, $c = 1$. To see this, when $c = 1$, this is a Heisenberg group over a field which is semi-extraspecial, but on the other hand, if $c > 1$, then the ring $K[x]/(a(x)^c)$ has nilpotent elements. These nilpotent elements prevent the group from satisfying the property that for all $g \in G \backslash G'$ and $z \in G'$, there exists $h \in G$ such that $[g, h] = z$. In the case when $c > 1$, quotients of $H(A)$ can still be semi-extraspecial even though the group is not semi-extraspecial. We will characterize these quotients in Section 4.

Theorem 3.7 ([BMW, Theorem 1.2]). *A centrally indecomposable p-group of exponent p and genus 2 over a finite field K is isomorphic to one of the following*

  (i) *a central quotient of the Heisenberg group $H = H(K[x]/(a(x)^c))$ by a subgroup N, such that $1 - N$ is a K-subspace of $1 - H'$;*
 (ii) *the matrix group*

$$H^\flat(K, m) := \left\{ \left. \left[\begin{array}{c|cccc|c} I_2 & e_1 & \cdots & e_m & 0 & z_1 \\ & 0 & e_1 & \cdots & e_m & z_2 \\ \hline & & & & & f_0 \\ & & I_{m+1} & & & \vdots \\ & & & & & f_m \\ \hline & & & & & 1 \end{array} \right] \; \right| \; e_i, f_i, z_i \in K \right\}.$$

A key idea used throughout the paper comes from the following theorem. This converts the problem of enumerating groups to enumerating orbits of (principal ideals of) polynomials under the action of $\Gamma\mathrm{L}(2, K) = \mathrm{GL}(2, K) \rtimes \mathrm{Gal}(K)$. We will describe the details of this action in Section 3.2. For our purposes, the crux is that the isomorphism problem of semi-extraspecial groups of order p^{2n+2} with exponent p and derived subgroup of order p^2 is determined by the $\mathrm{GL}(2, p)$ action on the *multiset* of Pfaffians of a fully refined central decomposition of G. Specifically, if $\mathcal{H}$ is a fully-refined central decomposition of G, then the multiset of Pfaffians of G is $\{\mathrm{Pf}(\circ_H) \mid H \in \mathcal{H}\}$. If every $H \in \mathcal{H}$ is isomorphic to a group from Theorem 3.7(i), then this multiset completely determines the group.

Theorem 3.8 ([BMW, Theorem 3.22]). *Suppose G_1 and G_2 are p-groups of class 2, exponent p, and genus 2 over K. Let $\mathcal{H}_1 = \{H_1, \ldots, H_s\}$ and $\mathcal{H}_2 = \{K_1, \ldots, K_t\}$ be fully-refined central decompositions of G_1 and G_2 respectively. Then $G_1 \cong G_2$ if, and only if, $s = t$ and there exists $M \in \Gamma\mathrm{L}(2, K)$ and σ, a permutation of $\{1, \ldots, t\}$, such that for all i,*

$$\left(\mathrm{Pf}(\circ_{H_i})^M \right) = \left(\mathrm{Pf}(\circ_{K_{i\sigma}}) \right).$$

We want to pause to give two examples that illustrate some of the nuances of Pfaffians. Our first example shows the need to first determine a fully refined central decomposition of the group, before computing its Pfaffian. We note that these examples apply more generally for every prime.

Example 3.9. Let K be a quadratic extension of $\mathbb{F}_5$, and let G be a central product of two copies of $H(K)$ with centers identified. So $|G| = 5^{10}$ and $|G'| = 5^2$. Now let $A = \mathbb{F}_5[x]/\left((x^2 + 2)^2\right)$ and consider the group $H(A)$. The ideal $(x^2 + 2)$ is spanned by $\{x^2 + 2, x^3 + 2x\}$ in A, and let S be the subspace spanned by $\{1, x\}$. Let

$$N = \left\{ \left. \left[\begin{array}{ccc} 1 & 0 & s \\ & 1 & 0 \\ & & 1 \end{array} \right] \; \right| \; s \in S \right\} \lhd H(A).$$

Later we prove in Theorem 4.3 that $H = H(A)/N$ is centrally indecomposable and semi-extraspecial. Importantly, $|H| = 5^{10}$ and $|H'| = 5^2$. Because G is decomposable and H is indecomposable, they are not isomorphic. Note also that G is genus 1 over K and H is genus 2 over $\mathbb{F}_5$.

We will show they have the same Pfaffians. Assume $\{\alpha, 1\}$ is a basis for K, where $\alpha^2 + 2 = 0$. Set

$$B = \left[\begin{array}{cc|cc} \alpha & 1 & & \\ 3 & \alpha & & 0 \\ \hline & 0 & \alpha & 1 \\ & & 3 & \alpha \end{array}\right],$$

so the bimap $\circ_G : \mathbb{F}_5^8 \times \mathbb{F}_5^8 \rightarrowtail \mathbb{F}_5^2$ has structure constants $\left[\begin{smallmatrix} 0 & B \\ -B^T & 0 \end{smallmatrix}\right]$. Replacing the basis of K with indeterminants X and Y, the Pfaffian of G is $(X^2 + 2Y)^2$. On the other hand, set

$$C = \begin{bmatrix} 0 & 0 & 2(3x^2+1) & x^3+2x \\ 0 & 2(3x^2+1) & x^3+2x & 3x^2+1 \\ 2(3x^2+1) & x^3+2x & 3x^2+1 & 0 \\ x^3+2x & 3x^2+1 & 0 & 0 \end{bmatrix}.$$

Assuming the basis for A is $\{1, x, x^2+2, x^3+2x\}$, then the structure constants for the bimap $\circ_H$ is $\left[\begin{smallmatrix} 0 & C \\ -C^T & 0 \end{smallmatrix}\right]$. Set the basis of the codomain of $\circ_H$ to be $\{x^3+2x, 3x^2+1\}$. Replacing that with indeterminants X and Y, the Pfaffian is equal to $(X^2+2Y^2)^2$. Therefore, the Pfaffians of $\circ_G$ and $\circ_H$ are identical even though $G \not\cong H$.

However, if we instead first determine a fully refined central decomposition for G and H and compute the Pfaffians of the indecomposable factors we get different invariants. The multiset of Pfaffians for G is $\{X^2+2Y^2, X^2+2Y^2\}$ (or just $\{X, X\}$ over K), and the multiset of Pfaffians for H is $\{(X^2+2Y^2)^2\}$, which are not equivalent. $\qquad\square$

Theorem 3.8 greatly depends on the fact that the groups are genus 2. When the genus is larger, deciding isomorphism of groups does not reduce to deciding if their Pfaffians are equivalent with respect to Theorem 3.8. In fact, such groups can have the same Pfaffian and not be isomorphic as the next example illustrates.

Example 3.10. We present two bimaps $V \times V \rightarrowtail W$ with the same Pfaffian that are not pseudo-isometric, so the corresponding groups are not isomorphic. Suppose $p = 3$, then $f(x) = x^3 + 2x + 1$ is irreducible in $\mathbb{F}_3[x]$. The matrices

$$M_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 2 & 0 \end{bmatrix} \qquad M_2 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 2 \end{bmatrix} \qquad M_3 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

form the structure constants of the $\mathbb{F}_3$-algebra $\mathbb{F}_3[x]/(f(x))$ with respect to the ordered basis $(1, x, x^2)$. Let A be the 3×3 matrix with 1 in the $(1,2)$-entry, -1 in the $(2,1)$-entry, and 0 elsewhere. Set $V = \mathbb{F}_3^6$ and $W = \mathbb{F}_3^3$. Define two alternating forms with the following structure constants

$$\left(\begin{bmatrix} 0 & M_i \\ -M_i & 0 \end{bmatrix}\right) \qquad \text{and} \qquad \left(\begin{bmatrix} 0 & M_i \\ -M_i & A \end{bmatrix}\right).$$

Both bimaps have the same Pfaffians: $x^3 + x^2y + xy^2 + 2xz^2 + 2y^3 + 2y^2z + z^3$. However, the two bimaps cannot be pseudo-isometric as the former contains at

least two 3-dimensional totally isotropic subspaces in V, and the latter contains exactly one 3-dimensional totally isotropic subspace. In the context of 3-groups, the corresponding groups are not isomorphic as the former contains at least two abelian subgroups of order 3^6 where the latter contains exactly one such abelian subgroup, see [L2] for a proof. $\square$

The multiple threes in Example 3.10 are a red herring. Instead, it illustrates a general phenomenon that happens when the genus is at least 3. When the genus is 2, $\circ_G$ can be written as a pair of alternating forms. Kronecker–Dieudonné [D3] and Scharlau [S1] classify indecomposable pairs of alternating forms. For the (centrally indecomposable) groups coming from Theorem 3.7(i), there exists bases for V and W such that $\circ_G$ is given by the pair of matrices

$$\left\{ \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}, \begin{bmatrix} 0 & C \\ -C^T & 0 \end{bmatrix} \right\},$$

where C is the companion matrix of a power of an irreducible polynomial in $K[x]$. Together with the fact that the Pfaffian of $\circ_G$ is 0 when $\dim_K(V)$ is odd, this proves the following proposition.

Proposition 3.11. *Suppose G is exponent p and genus 2 over K. If G is centrally indecomposable, then the ideal generated by the Pfaffian of $\circ_G : V \times V \rightarrowtail W$ is primary in $K[x, y]$.*

3.2. $\Gamma L(2, K)$ **action on the Pfaffians.** The group $\Gamma L(2, K)$ acts on polynomials $f(x, y)$ by substitution. That is, for $M = \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \sigma \right) \in \mathrm{GL}(2, K) \rtimes \mathrm{Gal}(K)$, set $f^M(x, y) = f^\sigma(ax + by, cx + dy)$, where σ acts on the coefficients. Let f and g be homogeneous polynomials in x, y. Then f is equivalent to g if there exists $k \in K^\times$ and $M \in \Gamma L(2, K)$ such that $f^M = k \cdot g$. In other words, the ideals are equal, $(f^M) = (g)$. Another perspective is to consider univariate polynomials $f \in K[x]$, with $\deg f = n$, and define

$$f^M(x) = (cx + d)^n f^\sigma \left(\frac{ax + b}{cx + d} \right).$$

Because the Pfaffians are homogeneous, we consider both of these actions.

The $\Gamma L(2, K)$-orbits have been studied by Vaughan-Lee [VL] and Vishnevet-skiĭ [V1] when $K = \mathbb{F}_p$. We let $N(q, n)$ denote the number of $\Gamma L(2, \mathbb{F}_q)$-orbits of monic irreducible polynomials of degree n. One can determine the number of iso-clinism classes of the centrally indecomposable groups of genus 2 (over $\mathbb{F}_p$) using [VL] and Theorem 5.2. Vaughan-Lee's Theorem enumerates the $\mathrm{GL}(2, p)$-orbits of all irreducible monic polynomials in $\mathbb{F}_p[x]$. Since we do not require the full generality, we record Vaughan-Lee's Theorem for $n \leq 5$.

Theorem 3.12 ([VL]). *If p is prime, then*

$$N(p, 2) = 1, \qquad N(p, 4) = \frac{1}{2} \left(p + 2 - \gcd(2, p) \right),$$

$$N(p, 3) = 1, \qquad N(p, 5) = \frac{1}{5} \left(p^2 - 2 + \gcd(5, p) + 2 \gcd(5, p^2 - 1) \right).$$

4. Semi-extraspecial groups of genus 2

We describe the centrally indecomposable, semi-extraspecial groups of genus 2 based on the classification in Theorem 3.7. The following lemmas quickly determine which groups of genus 2 are not semi-extraspecial.

Lemma 4.1. *For all $m \geq 1$, the group $G = H^\flat(K, m)$ is not semi-extraspecial.*

Proof. As $[G : G'] = p^{2m+1}$, the Pfaffian of $\circ_G$ is 0, so invoke Theorem 2.2. $\square$

In what follows, we characterize the quotients of $H(K[x]/(a(x)^c))$ that are semi-extraspecial groups. Set $A = K[x]/(a(x)^c)$. Theorem 3.7(i) is only concerned with central subgroups N such that $1 - N$ is a K-subspace of $1 - H(A)'$. Therefore, for a K-subspace $S \leq A$, we set

$$N(S) = \left\{ \begin{bmatrix} 1 & 0 & s \\ & 1 & 0 \\ & & 1 \end{bmatrix} \,\middle|\, s \in S \right\}.$$

Proposition 4.2. *Let $a(x) \in K[x]$ be an irreducible polynomial, $c > 1$ be an integer, and S a proper K-subspace of $A = K[x]/(a(x)^c)$. Then $H(A)/N(S)$ is semi-extraspecial if, and only if, $A = S + (a(x)^{c-1})$ and $\deg(a(x)) \geq 2$.*

Proof. Let $I = (a(x)^{c-1})$. First, we suppose that $A = S + I$. Since A is a local algebra, the group of units $A^\times$ is $A \setminus (a(x))$. It follows that every nonzero element of A can be written as ua^e, for $u \in A^\times$ and $0 \leq e \leq c - 1$. Since S is a proper subspace of A, it follows that $\emptyset \neq A \setminus S \subseteq I$.

To show that $H(A)/N(S)$ is semi-extraspecial, it is enough to show that for every $0 \neq f \in A$, and $h + S \in A/S$, there exists $g \in A$ such that $fg = h$. Let $f = ua^e$, for some $u \in A^\times$ and $0 \leq e \leq c - 1$. Without loss of generality, $h + S \in A/S$ can be written as $va^{c-1} + S$, for some $v \in A^\times$. With $g = u^{-1}va^{c-e-1}$, we have that $fg = h$, and so $H(A)/N(S)$ is semi-extraspecial.

On the other hand, suppose $S + I \neq A$. Let $h(x) \in A \setminus (S + I)$. Therefore, for all $f(x) \in I$ and for all $g(x) \in A$, $fg \in I$. In particular, $fg + S \neq h + S$, so $H(A)/N(S)$ cannot be semi-extraspecial. $\square$

We summarize the above results in the following theorem to classify all indecomposable, semi-extraspecial groups of genus 2 with exponent p.

Theorem 4.3. *Suppose G is class 2, exponent p, and genus 2 over K. Then G is centrally indecomposable and semi-extraspecial if, and only if, there exists an irreducible polynomial $a(x) \in K[x]$ of degree ≥ 2, a positive integer c, and a subspace $S \leq A := K[x]/(a(x)^c)$ with 2-dimensional complement $\langle f, g \rangle$, such that*

(i) $A = S + (a(x)^{c-1})$,
(ii) A is an irreducible $K[f^{-1}g]$-module, and
(iii) $G \cong H(A)/N(S)$.

Proof. If G is indecomposable and semi-extraspecial, then by Theorem 3.7 G is contained in one of two (disjoint) families of genus 2 groups. By Lemma 4.1 property (iii) holds, and by Proposition 4.2, property (i) holds. Therefore, there exists $f, g \in A^\times$ that span a complement to S in A. As G is indecomposable, by the proof of [BMW, Theorem 3.18], A is an irreducible $K[f^{-1}g]$-module.

If, on the other hand, G satisfies properties (i)–(iii) above, then by Proposition 4.2, G is semi-extraspecial. As $\langle f, g \rangle \oplus S = A$, $\circ_G$ can be written as a pair of alternating matrices with respect to f and g, as in Section 2.1, of the form

$$\left\{ \begin{bmatrix} 0 & M_f \\ -M_f^T & 0 \end{bmatrix}, \begin{bmatrix} 0 & M_g \\ -M_g^T & 0 \end{bmatrix} \right\}.$$

Since G is semi-extraspecial, M_f is invertible, so the block-diagonal matrix $M_f^{-1} \oplus I_{cd}$ induces an isometry of $\circ_G$ to an alternating bimap with I_{cd} and $M_f^{-1}M_g$ in the top-right corners. Because A is an irreducible $K[f^{-1}g]$-module, it follows that the rational canonical form of $M_f^{-1}M_g$ is the companion matrix of a primary polynomial. Thus, G is indecomposable. $\qquad \square$

5. Enumerating isoclinism classes

We use Theorems 3.8 and 4.3 to count the isoclinism classes of semi-extraspecial groups whose derived subgroup has order p^2. Therefore, these groups can have genus 1 or 2 over $\mathbb{F}_p$. The genus 1 case essentially follows from the classification of generalized Heisenberg groups in [LW, Theorem 3.1].

In the next lemma, we use a consequence of Witt's Theorem [A, Chapter 3]: two alternating bilinear K-forms are isometric if, and only if, their radicals have the same dimension.

Lemma 5.1. *Assume $n \geq 2$ and q is a p-power. There are*

$$H(q, n+1) = \begin{cases} 1 & n \text{ even}, \\ 0 & \text{otherwise}, \end{cases}$$

semi-extraspecial groups of order q^{n+1} with exponent p and derived subgroup of order q, where $\mathcal{C}(\circ_G) \cong \mathbb{F}_q$.

Proof. Let G be a group satisfying the assumptions and $K = \mathcal{C}(\circ_G)$. As $\circ_G : V \times V \rightarrowtail W$ is K-bilinear and $\dim_K(W) = 1$, it follows that $\circ_G$ is an alternating K-form. By Lemma 3.1, G is directly indecomposable, so $\circ_G$ has trivial radical. This leads to a contradiction if $\dim_K(V)$ is odd, so no such groups exist. On the other hand, if $\dim_K(V) = 2n$, then

$$G \cong \left\{ \begin{bmatrix} 1 & u & w \\ & I_n & v^T \\ & & 1 \end{bmatrix} \;\middle|\; \begin{array}{c} u, v \in K^n, \\ w \in K \end{array} \right\} \leq \mathrm{GL}(n+2, K). \qquad \square$$

To prove the next theorem, we require a way to build nilpotent groups from bimaps. Suppose $\circ : U \times V \rightarrowtail W$ is a K-bimap. Then the Heisenberg group with respect to $\circ$ is the group

$$H(\circ) = \left\{ \begin{bmatrix} 1 & u & w \\ & 1 & v \\ & & 1 \end{bmatrix} \;\middle|\; u \in U, v \in V, w \in W \right\},$$

where the product is given by matrix multiplication using $\circ$. Assuming $\circ$ is fully nondegenerate, the center of $H(\circ)$ equals the derived subgroup and $Z(H(\circ)) \cong W$. Moreover, the commutator bimap of $H(\circ)$ has "doubled" $[,] : (U \oplus V) \times (U \oplus V) \rightarrowtail W$ where

$$\big((u_1, v_1), (u_2, v_2) \big) \mapsto u_1 \circ v_2 - u_2 \circ v_1.$$

As matrices, if $\circ$ has structure constants given by the sequence $(M_i)_{i=1}^d$, then $[,]$ has structure constants of the form $\begin{bmatrix} 0 & M_i \\ -M_i^T & 0 \end{bmatrix}$.

Recall from Section 3.2 that $N(q, n)$ is the number of $\Gamma\mathrm{L}(2, \mathbb{F}_q)$-orbits of monic irreducible polynomials of degree n. As $\mathrm{GL}(2, \mathbb{F}_q)$ is transitive on the nonzero vectors in $\mathbb{F}_q^2$, it follows that $N(q, 1) = 1$.

Theorem 5.2. *Suppose $n \geq 2$ and q is a p-power. There are $I(q, 2n+2) = -1 + \sum_{d|n} N(q,d)$ pairwise non-isomorphic, centrally indecomposable, semi-extraspecial groups of order q^{2n+2} with exponent p and genus 2 over $\mathbb{F}_q$.*

Proof. First apply Theorem 3.8 to establish that two indecomposable genus 2 groups with exponent p are isomorphic if, and only if, their Pfaffians are in the same $\Gamma L(2, q)$-orbit. By Proposition 3.11, their Pfaffians are primary. Let $a(x)^c = x^{cd} + a_{cd-1}x^{cd-1} + \cdots + a_0$, and assume $a(x)$ is an irreducible polynomial in $\mathbb{F}_q[x]$ and $c \geq 1$. Let C be the companion matrix of $a(x)^c$:

$$C = \begin{bmatrix} \begin{array}{c|ccc} 0 & & & \\ \vdots & & I_{cd-1} & \\ 0 & & & \\ \hline -a_0 & -a_1 & \cdots & -a_{cd-1} \end{array} \end{bmatrix}.$$

The group with commutator bimap whose structure constants are

$$\left(\begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}, \begin{bmatrix} 0 & -C \\ C^T & 0 \end{bmatrix} \right)$$

has a Pfaffian equal to $X^{cd} + a_{cd-1}X^{cd-1}Y + \cdots + a_0Y^{cd}$. Note that this is the determinant of $IX - CY$. Therefore, for every irreducible polynomial $a(x)$ of degree d and $c \geq 1$, there exists an indecomposable p-group of order q^{2cd+2} of genus 2 and exponent p where $\mathrm{Pf}(\circ_G) = a(x)^c$. By Theorem 3.8, there are $N(q,d)$ isoclinism classes of this type. By Theorem 2.2, semi-extraspecial groups have no linear factors, so we require $d \geq 2$. Thus, to get the number of isoclinism classes of indecomposable semi-extraspecial groups of order q^{2n+2} that are genus 2 over $\mathbb{F}_q$, we sum over all the divisors d of n, excluding $d = 1$. □

Theorem 5.3. *For every prime p, there is exactly one isoclinism class of semi-extraspecial groups G with the property that $|G| = p^8$ and $|G'| = p^2$.*

Proof. First, we show that G must be indecomposable. If $\{H_1, H_2\}$ is a central decomposition of G, then $|H_i| \in \{p^4, p^5, p^6\}$ because $[G : G'] = p^6$. From Proposition 3.2, $Z(H_i) = Z(G) \cong \mathbb{Z}_p^2$. There are no genus 2 groups of order p^4 and by Lemma 4.1, the genus 2 group of order p^5 is not semi-extraspecial. Therefore, G is indecomposable. By Theorems 3.12 and 5.2, there is $I(p, 8) = N(p, 3) = 1$ isoclinism class. □

Remark 5.4. An interesting consequence of Theorem 5.3 is that every semi-extraspecial group with exponent p and of order p^9 with $|G'| = p^3$, has exactly two non-trivial central nonabelian quotients, determined solely by the order of the factor group. In particular, heuristics to construct characteristic subgroups via graph colorings, like in [BOW], or from algebras associated to $\circ_G$, like in [M2, W2], produce no new information. These groups may pose a formidable challenge to isomorphism testing.

Are there other semi-extraspecial groups, with derived subgroup of order p^3, that have the property in Remark 5.4? That is, if $N, M \leq Z(G)$ and $|N| = |M|$, then G/N and G/M are isoclinic. If there are no other such groups, then what is the lower bound on the number of possible isoclinism classes of the form G/N, for a fixed order $|N|$? On the other end of the spectrum, what is the upper bound?

5.1. **Proof of Theorem 1.2.** Enumerating semi-extraspecial groups of larger order is not as simple as in Theorem 5.3 and will require understanding how $\mathrm{GL}(2,p)$ acts on (principal) ideals of *reducible* polynomials. We now focus on univariate polynomials in $\mathbb{F}_p[x]$, so we dehomogenize $\mathrm{Pf}(\circ_G)$ by setting $y = 1$. If $f \in \mathbb{F}_p[x]$, we let S_f denote the subgroup, $\mathrm{Stab}_{\mathrm{GL}(2,p)}((f))$, stabilizing the ideal (f).

The next lemma is a well-known statement coming from the (maximal) subgroup structure of $\mathrm{PSL}(2,p)$. We refer the reader to Dickson [D2], see also Huppert [H2] and, for historical remarks, King [K2, Theorem 2.1].

Lemma 5.5. *If f is an irreducible quadratic in $\mathbb{F}_p[x]$, then $S_f \cong \Gamma\mathrm{L}(1,p^2)$. The subgroups isomorphic to $\Gamma\mathrm{L}(1,p^2)$ in $\mathrm{GL}(2,p)$ are in bijection to monic irreducible quadratics in $\mathbb{F}_p[x]$.*

Proof. By orbit counting, $|S_f| = 2(p^2 - 1)$. For $\alpha \in \mathbb{F}_{p^2}$ and $M = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$, if $f(x) = (x - \alpha)(x - \alpha^p)$, then

$$f^M(x) = (a - \alpha c)(a - \alpha^p c)\left(x - \frac{\alpha d - b}{a - \alpha c}\right)\left(x - \frac{\alpha^p d - b}{a - \alpha^p c}\right).$$

This is the inverse action on the roots of f, so the lemma follows. $\square$

Note that the kernel of the action of $\mathrm{GL}(2,p)$ on polynomials is its center, so we work with $\mathrm{PGL}(2,p)$ instead. In order to enumerate the isoclinism classes of semi-extraspecial groups order p^{10} with derived subgroup of order p^2, we need to understand an action of dihedral groups in $\mathrm{PGL}(2,p)$. Assuming p is an odd prime, let Δ be the set of maximal dihedral subgroups of $\mathrm{PGL}(2,p)$ of order $2(p+1)$. That is, Δ contains all the images of the subgroups isomorphic to $\Gamma\mathrm{L}(1,p^2)$ in $\mathrm{GL}(2,p)$. Using the bijection given by Lemma 5.5, a dihedral group acts on Δ in the following way. If $D \in \Delta$ and f is an irreducible quadratic associated to $D_f \in \Delta$, then for $\delta \in D$, $D_f^\delta = D_{f^\delta}$. Therefore, for $D \in \Delta$, the D-orbit of D is trivial.

Lemma 5.6. *Let p be an odd prime. For a fixed $D \in \Delta$, the number of D-orbits on $\Delta - D$ is $(p-1)/2$.*

Proof. We count these orbits by counting the fixed points for every $\delta \in D$. First note that if $1 \neq \delta \in D$ is not an involution, then $N_{\mathrm{PGL}(2,p)}(\langle\delta\rangle) = D$. Thus, such a δ cannot fix another dihedral group in Δ, so we focus only on the involutions of D.

Each dihedral group in Δ intersects $\mathrm{PSL}(2,p)$ uniquely in a dihedral group of order $p + 1$. Let $\overline{D} = D \cap \mathrm{PSL}(2,p)$. Up to conjugacy, there are two types of involutions in D: those contained in $\mathrm{PSL}(2,p)$ and those outside [S2, pp. 226–227]. Suppose $p \equiv 1 \bmod 4$, so $\overline{D}$ has exactly $(p+1)/2$ involutions. Since $|\Delta| = (p^2-p)/2$, there are $(p^2 - p)(p+1)/4$ involutions coming up this way. However, $\mathrm{PSL}(2,p)$ has exactly $p(p+1)/2$ involutions [D4, Chapter 38], so each involution in $\mathrm{PSL}(2,p)$ lies in $(p-1)/2$ dihedral subgroups of order $p + 1$. Therefore, the involutions of $\overline{D}$ stabilize $(p-3)/2$ dihedral groups in $\Delta - D$.

There are $(p+3)/2$ involutions in D outside of $\mathrm{PSL}(2,p)$, and as many as $(p^2 - p)(p+3)/4$ involutions outside of $\mathrm{PSL}(2,p)$. One of these involutions, δ, lies in $Z(D)$, so its centralizer is D. As there are $(p^2 - p)/2$ involutions of $\mathrm{PGL}(2,p)$ outside of $\mathrm{PSL}(2,p)$ [D4], it follows that δ fixes $(p+3)/2 - 1$ other dihedral groups in $\Delta - D$. Therefore, the number of orbits in this case is equal to

$$\frac{\left(\frac{1}{2}(p^2 - p) - 1\right) + \left(\frac{1}{2}(p+1)\frac{1}{2}(p-3)\right) + \left(\frac{1}{2}(p+3)\frac{1}{2}(p+1)\right)}{2(p+1)} = \frac{p-1}{2}.$$

The case when $p \equiv 3 \bmod 4$ is similar to the above case. There is one more involution in $\mathrm{PSL}(2, p)$ than above, namely $\overline{D}$ contains a central involution. The number of fixed points for these involutions follows a similar argument as above. The argument for the involutions outside of $\mathrm{PSL}(2, p)$ is slightly different. Of the $(p+1)/2$ involutions of D outside of $\mathrm{PSL}(2, p)$, each one is contained in the center of some dihedral group of order $2(p-1)$, so its centralizer is that dihedral group. Hence, there are $(p^2 - p)/2$ such involutions, which are all of the involutions of $\mathrm{PGL}(2, p)$ outside $\mathrm{PSL}(2, p)$. Therefore, each involution of this type is contained in $(p-1)/2$ groups in Δ, and thus, fixes $(p-3)/2$ groups in $\Delta - D$. $\qquad\square$

Now we are in a position to prove Theorem 1.2.

Proof of Theorem 1.2. If G is indecomposable, then apply Theorems 3.12 and 5.2, so there are

$$I(p, 2 \cdot 4 + 2) = N(p, 4) + N(p, 2) = \frac{1}{2} \left(p + 4 - \gcd(2, p) \right)$$

such isoclinism classes. Now suppose G is centrally decomposable with fully refined central decomposition $\mathcal{H}$. From the proof of Theorem 5.3, for each $H \in \mathcal{H}$, $|H| \geq p^6$. Because $|G| = p^{10}$, it follows that $\mathcal{H} = \{H_1, H_2\}$, where $|H_i| = p^6$. We have two options for the centroid of $\circ_G$ from Proposition 3.4: $\mathcal{C}(\circ_G)$ is isomorphic to either $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$. If $\mathcal{C}(\circ_G)$ is the quadratic extension, then by Lemma 5.1, there is exactly $H(p^2, 5) = 1$ group with this property.

We suppose the centroid is the prime field. In this case, the Pfaffian of $\circ_G$ in $\mathbb{F}_p[x, y]$ is the product of two homogeneous quadratics f and g. Without loss of generality, we assume that both f and g are monic. If $f = g$, then $\circ_G$ is $\mathbb{F}_p[x]/(f)$-bilinear, so the centroid would be a (non-trivial) field extension, which has already been accounted for. Therefore, $f \neq g$. This means that, for $p = 2$, there are no groups of this type because there is a unique irreducible monic quadratic. Thus, we now assume $p > 2$. By Theorem 3.8, the number of isoclinism classes of these groups is the number of $\mathrm{PGL}(2, p)$-orbits on the ideals generated by a product of monic irreducible quadratics. As $\mathrm{PGL}(2, p)$ is transitive on monic irreducible quadratics, the number of orbits is equal to the number of orbits of one of the stabilizers, say, $\mathrm{Stab}_{\mathrm{PGL}(2,p)}((f))$. By Lemmas 5.5 and 5.6, there are exactly $(p-1)/2$ orbits. Thus, the statement of the theorem holds. $\qquad\square$

5.2. **Proof of Theorem 1.3.** Because all the monic irreducible cubics lie in one $\mathrm{PGL}(2, p)$-orbit, c.f. Theorem 3.12, it follows, again by orbit counting, that their stabilizers have order 3 in $\mathrm{PGL}(2, p)$.

Lemma 5.7. *In $\mathrm{PGL}(2, p)$, if $p \equiv 2 \bmod 3$, then there is a bijection between the Sylow 3-subgroups and the dihedral subgroups of order $2(p+1)$ given by inclusion.*

Proof. Let D denote a dihedral subgroup of $G = \mathrm{PGL}(2, p)$ of order $2(p+1)$. As $p \equiv 2 \bmod 3$, D contains a Sylow 3-subgroup, P. If $x \in D$ has order $p+1$, then $P \leq \langle x \rangle$. Because $N_G(\langle x \rangle) = D$, it follows that $N_G(P) = D$. $\qquad\square$

Proof of Theorem 1.3. In the indecomposable case, we apply Theorem 5.2, and in the case where G is genus 2 over the quadratic extension, we apply Lemma 5.1. By Theorem 3.12, the number of isoclinism classes is

$$I(p, 2 \cdot 5 + 2) + H(p^2, 6) = N(p, 5) + 0 = \frac{1}{5} \left(p^2 - 2 + \gcd(5, p) + 2\gcd(5, p^2 - 1) \right).$$

Now, all we have left to do is to count the number isoclinism classes in the decomposable case where the centroid is the prime field. By Proposition 3.2 and Theorem 4.3, a fully refined central decomposition of G is $\{H_1, H_2\}$, where $|H_1| = p^6$ and $|H_2| = p^8$. Thus, the multiset of Pfaffians contains exactly one quadratic and cubic. Hence, the stabilizer, in $\mathrm{GL}(2, p)$, of the multiset is the intersection of stabilizers of a quadratic and a cubic.

By Lemma 5.5 the quadratic stabilizer is isomorphic to $\Gamma\mathrm{L}(1, p^2)$. Since $N(p, 3) = 1$, the stabilizer of a cubic has order $3(p - 1)$ as there are $(p^3 - p)/3$ monic irreducible cubics in $\mathbb{F}_p[x]$. In $\mathrm{PGL}(2, p)$, this is the intersection of the dihedral group of order $2p + 2$ with a cyclic group of order 3. Therefore, when $p \equiv 0, 1 \mod 3$, these intersections are always trivial in $\mathrm{PGL}(2, p)$, and the number of orbits in this case is

$$\frac{\frac{1}{2}(p^2 - p)\frac{1}{3}(p^3 - p)}{(p^3 - p)} = \frac{1}{6}(p^2 - p).$$

When $p \equiv 2 \mod 3$, Lemma 5.7 implies that the Sylow 3-subgroups are cyclic and so contain a unique subgroup of order 3. As there are $(p^3 - p)/3$ irreducible cubics and $(p^2 - p)/2$ subgroups of order 3 in $\mathrm{PGL}(2, p)$, it follows that $2(p + 1)/3$ cubics have identical stabilizers in $\mathrm{PGL}(2, p)$. Hence, for a fixed irreducible quadratic there are $2(p+1)/3$ irreducible cubics such that their stabilizer has order 3; for the remaining $(p^3 - 3p - 2)/3$ cubics, their stabilizer is trivial. Therefore, the number of orbits is given by

$$\frac{\frac{1}{2}(p^2 - p)\left(2(p + 1) + \frac{1}{3}(p^3 - 3p - 2)\right)}{(p^3 - p)} = \frac{1}{6}(p^2 - p + 4). \qquad \square$$

Acknowledgements

References

[A] E. Artin, *Geometric algebra*, Interscience Publishers, Inc., New York-London, 1957. MR0082463

[B] Bert Beisiegel, *Semi-extraspezielle p-Gruppen*, Math. Z. **156** (1977), no. 3, 247–254 (German). MR0473004

[BMW] Peter A. Brooksbank, Joshua Maglione, and James B. Wilson, *A fast isomorphism test for groups whose Lie algebra has genus 2*, J. Algebra **473** (2017), 545–590. MR3591162

[BOW] Peter A. Brooksbank, E.A. O'Brien, and James B. Wilson, *A fast isomorphism test for groups whose Lie algebra has genus 2*, preprint. arXiv:1708.08873.

[C] A. R. Camina, *Some conditions which almost characterize Frobenius groups*, Israel J. Math. **31** (1978), no. 2, 153–160. MR516251

[CMS] David Chillag, Avinoam Mann, and Carlo M. Scoppola, *Generalized Frobenius groups. II*, Israel J. Math. **62** (1988), no. 3, 269–282. MR955132

[D1] Ulrich Dempwolff, *Semifield planes of order 81*, J. Geom. **89** (2008), no. 1-2, 1–16. MR2457018

[D2] Leonard Eugene Dickson, *Linear groups: With an exposition of the Galois field theory*, with an introduction by W. Magnus, Dover Publications, Inc., New York, 1958. MR0104735

[D3] Jean Dieudonné, *Sur la réduction canonique des couples de matrices*, Bull. Soc. Math. France **74** (1946), 130–146 (French). MR0022826

[D4] Larry Dornhoff, *Group representation theory. Part A: Ordinary representation theory*, Marcel Dekker, Inc., New York, 1971. Pure and Applied Mathematics, 7. MR0347959

[H1] P. Hall, *The classification of prime-power groups*, J. Reine Angew. Math. **182** (1940), 130–141. MR0003389

[H2] B. Huppert, *Endliche Gruppen. I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin-New York, 1967 (German). MR0224703

[JJB] Norman L. Johnson, Vikram Jha, and Mauro Biliotti, *Handbook of finite translation planes*, Pure and Applied Mathematics (Boca Raton), vol. 289, Chapman & Hall/CRC, Boca Raton, FL, 2007. MR2290291

[K1] William M. Kantor, *Finite semifields*, Finite geometries, groups, and computation, Walter de Gruyter, Berlin, 2006, pp. 103–114. MR2258004

[K2] Oliver H. King, *The subgroup structure of finite classical groups in terms of geometric configurations*, Surveys in combinatorics 2005, London Math. Soc. Lecture Note Ser., vol. 327, Cambridge Univ. Press, Cambridge, 2005, pp. 29–56. MR2187733

[L1] Mark L. Lewis, *Semi-extraspecial groups*, submitted. arXiv:1709.03857.

[L2] _____, *Semi-extraspecial groups with an abelian subgroup of maximal possible order*, submitted. arXiv:1710.10299.

[LW] Mark L. Lewis and James B. Wilson, *Isomorphism in expanding families of indistinguishable groups*, Groups Complex. Cryptol. **4** (2012), no. 1, 73–110. MR2921156

[M1] I. D. Macdonald, *Some p-groups of Frobenius and extra-special type*, Israel J. Math. **40** (1981), no. 3-4, 350–364 (1982). MR654591

[M2] Joshua Maglione, *Efficient characteristic refinements for finite groups*. part 2, J. Symbolic Comput. **80** (2017), no. part 2, 511–520. MR3574524

[S1] Rudolf Scharlau, *Paare alternierender Formen*, Math. Z. **147** (1976), no. 1, 13–19. MR0419484

[S2] Robert Steinberg, *The representations of* $\mathrm{GL}(3,q), \mathrm{GL}(4,q), \mathrm{PGL}(3,q),$ *and* $\mathrm{PGL}(4,q)$, Canadian J. Math. **3** (1951), 225–235. MR0041851

[VL] Michael Vaughan-Lee, *Orbits of irreducible binary forms over GF(p)*, preprint. arXiv:1705.07418.

[V1] A. L. Vishnevetskiĭ, *The number of classes of projectively equivalent binary forms over a finite field*, Dokl. Akad. Nauk Ukrain. SSR Ser. A **4** (1982), 9–12, 86 (Russian, with English summary). MR659930

[V2] Libero Verardi, *Semi-extraspecial groups of exponent p*, Ann. Mat. Pura Appl. (4) **148** (1987), 131–171 (Italian, with English summary). MR932762

[W1] James B. Wilson, *Existence, algorithms, and asymptotics of direct product decompositions, I*, Groups Complex. Cryptol. **4** (2012), no. 1, 33–72. MR2921155

[W2] _____, *More characteristic subgroups, Lie rings, and isomorphism tests for p-groups*, J. Group Theory **16** (2013), no. 6, 875–897. MR3198722

KENT STATE UNIVERSITY, DEPARTMENT OF MATHEMATICAL SCIENCES, MSB 233, KENT, OH 44242

Email address: lewis@math.kent.edu

KENT STATE UNIVERSITY, DEPARTMENT OF MATHEMATICAL SCIENCES, MSB 233, KENT, OH 44242

Email address: jmaglion@math.kent.edu