THEORY OF COMPUTING, Volume 15 (19), 2019, pp. 1–25
www.theoryofcomputing.org

The Threshold for Subgroup Profiles to Agree is Logarithmic

James B. Wilson*

Received December 20, 2016; Revised October 19, 2019; Published December 21, 2019

Abstract: For primes $p > 2$ and $e > 3$ there are at least p^{e-3}/e groups of order p^{2e+2} that have equal multisets of isomorphism types of proper subgroups and proper quotient groups, isomorphic character tables, and power maps. This obstructs recent speculation concerning a path towards efficient isomorphism tests for general finite groups. These groups have a special-purpose deterministic polynomial-time isomorphism test.

ACM Classification: F.2.2

AMS Classification: 68Q17, 20D15, 20F69, 68Q25

Key words and phrases: group isomorphism, profiles, p-groups

1 Introduction

The problem GRAPHISO asks if two graphs of order n are isomorphic. A recent breakthrough by Babai has reduced the complexity of GRAPHISO to $n^{O((\log n)^c)}$ for some $c \geq 1$ [1]. An obstacle to improving this bound is the problem GROUPISO, which asks if two finite groups given by their multiplication tables are isomorphic. As implied by work of Hedrlín-Pultr [16] and shown also by Miller [23], GROUPISO $\leq_P$ GRAPHISO. Amongst the many problems that reduce to GRAPHISO, GROUPISO generates attention. See [12] for a list of many of the key algorithms over the years. As a complexity problem, GROUPISO is interesting in part because its worst-case analysis is largely unchanged from what we obtain by a brute-force algorithm. Specifically, by comparing minimal generating sets one can decide isomorphism against a group G of order n in time $n^{d(G)+O(1)}$ where $d(G)$ denotes the minimum size of a generating set of a group G. By Lagrange's theorem $d(G) \leq \log_2 n$ which gives a bound on the complexity of

*This research was supported in part by NSF grant DMS 1620454.

 DOI: 10.4086/toc.2019.v015a019

GROUPISO of $n^{\log_2 n+O(1)}$. Rosenbaum explored variations of such algorithms that lowered the bound to $n^{0.5\log_2 n+O(1)}$ [27].

A stronger bound on $d(G)$ clarifies the cases of group isomorphism that are most concerning. Using the prime factorization $n = p_1^{e_1}\cdots p_s^{e_s}$, we define the following parameter:

$$\mu(p_1^{e_1}\cdots p_s^{e_s}) = \max\{e_1,\dots,e_s\}. \tag{1.1}$$

Guralnick [15] proved that $d(G) \le \mu(n)+1$. As $n\to\infty$, the number of integers n for which $\mu(n)\le c$ tends to $1/\zeta(c+1)$—the reciprocal of the zeta function (see, e. g., [30]). So for 99% of group orders n, group isomorphism is solved in time polynomial in n; see [11, 10] for an exploration of the complexity of group isomorphism based on the prime factorization of n.

The above suggests that to locate worst-case complexity of group isomorphism we should consider groups of order $n = p^\ell$, p prime, which are known as *p-groups*. Indeed, families of p-groups exist which when given to present-day group isomorphism tests, e. g., those in [12], require $n^{O(\log_p n)}$ operations. In light of these difficulties, and the reductions by Pultr–Hedrlín and Miller, the complexity of p-group isomorphism appears to be a real obstacle to the improvement of graph isomorphism.

Recent speculation by Gowers [14] (see, e. g., Babai [1, p. 693]) posed the possibility of using a portion of the subgroups of a finite group to determine isomorphism types of finite groups. Isomorphism tests have been successfully using such ideas as heuristics for some time; see, e. g., fingerprinting in [12]. Yet, proving efficiency based on these heuristics has been obstructed by 90-year-old examples by Rottlaender and others, that show that subgroup lattices do not characterize groups up to isomorphism [28].

In [14] Gowers introduced a threshold criterion based on the following. We say that a group is *d-generated* if $d(G)\le d$. The *d-subgroup profile* of a group G is the multiset of isomorphism types of d-generated subgroups of G. Define $\kappa(G)$ as the minimum d such that the d-profile of G determines the isomorphism type of G, and finally define

$$\kappa(n) = \max\{\kappa(G) \mid n = |G|\}.$$

Evidently $\kappa(G)\le d(G)$ and so $\kappa(n)\le \mu(n)+1$. Comparing $\kappa(n)$-profiles of groups of order n decides isomorphism in time $n^{2\kappa(n)+O(1)}$. Gowers asked for examples where $\kappa(n)\notin O(1)$. Glauberman and Grabowski [13] gave instances to show $\kappa(p^\ell)\in\Omega(\sqrt{\ell})$. We prove

Theorem 1.2. *For a prime $p>2$, $\kappa(p^\ell)\in\Theta(\ell)$. In particular, isomorphism testing of p-groups by comparing subgroup profiles requires $n^{\Theta(\log_p n)}$ time in the worst case.*

To prove Theorem 1.2 we begin with primes $p>2$ and $e>3$ then set $q=p^e$. Let $\mathbb{F}_q$ be a finite field of order q and define the *Heisenberg group over* $\mathbb{F}_q$ as

$$H = H(\mathbb{F}_q) = \left\{ \begin{bmatrix} 1 & \alpha & \gamma \\ & 1 & \beta \\ & & 1 \end{bmatrix} \,\middle|\, \alpha,\beta,\gamma\in\mathbb{F}_q \right\}. \tag{1.3}$$

Our interest is in the quotients of H, which we collect according to their orders.

$$\mathfrak{H}^g_{p,e} = \{G \mid \exists N \lhd H(\mathbb{F}_{p^e}), |H(\mathbb{F}_{p^e}) : N| = p^{2e+g} \text{ and } G\cong H(\mathbb{F}_{p^e})/N\}. \tag{1.4}$$

We shall see the groups in $\mathfrak{H}^g_{p,e}$ with $-2e \leq g \leq 0$ are all elementary abelian and so they are isomorphic to $\mathbb{Z}_p^{2e+g}$. When $g=1$ the groups are nonabelian but each is what P. Hall called *extraspecial of exponent* p and they are pairwise isomorphic (Theorem 4.9). However for $1 < g \leq e$ we see increasing diversity. Our focus is on $g=2$.

Theorem 1.5. *$\mathfrak{H}^2_{p,e}$ has at least p^{e-3}/e isomorphism classes; yet, the groups in $\mathfrak{H}^2_{p,e}$ have equal multisets of isomorphism types of proper subgroups, and also of proper quotient groups.*

The groups in $\mathfrak{H}^2_{p,e}$ are an extreme illustration of the difficulty to capture group isomorphism by a list of invariants. In Section 6.1 we list numerous other similarities including character tables, conjugacy classes, and at times automorphism groups.

Despite these observations, the following class of groups has an efficient solution to the membership and isomorphism problems.

$$\mathfrak{H}_p = \bigcup_e \bigcup_{1\leq g\leq e} \mathfrak{H}^g_{e,p}. \tag{1.6}$$

For computation a group G can be given by numerous methods, most commonly, by permutations, matrices, or polycyclic presentations; see [29]. The complexity of operations in these models differs, so we adopt the *black-box group* model—as introduced by Babai–Szemerédi, see [29, Chapter 2]. We further assume an oracle for group orders. This means we can access compactly encoded generators for the group G, we can compute all group operations, and we can compute $|G|$, but we model these tasks as requiring only constant time. In prior work with Lewis, the author proved the following.

Theorem 1.7 ([21])**.** *Fix a prime p. For groups given as a black-box with an order oracle, there are deterministic polynomial-time algorithms that*

(a) given a group G, decides if $G \in \mathfrak{H}_p$; and

(b) given groups $G, \bar{G} \in \mathfrak{H}_p$, decides if $G \cong \bar{G}$.

All permutation groups and their quotients have deterministic polynomial-time algorithms for the necessary black-box group oracles and to find a group's order, see [29, Chapter 3]. Since the rows of the multiplication table of a group G are a faithful permutation representation of G, we consider the multiplication table model as the special case of *regular* permutation groups. In the context of matrix groups G we assume p is bounded. In that case work of Luks implies that we can decide in polynomial time if G is a p-group and if so to compute $|G|$ [22]. So in both these models we can replace "black-box polynomial time" with simply "polynomial time." The computational complexity of groups given by polycyclic presentations is nuanced, but in general polynomial-time algorithms for the necessary oracles are not known, see [19, Section 4], [20]. Even so the reports of practical performance with polycyclic groups (e. g., [29, Section 7.2]) suggest they are equally useful input models.

The algorithms of [21] have a complexity of $O(p + e^{2\omega}\log^2 p)$, where $2 \leq \omega < 3$ is the exponent of matrix multiplication, see [31, Chapter 12]. In the special case of groups in $\mathfrak{H}^2_{p,e}$, Brooksbank, Maglione, and the author give an $O(p^3 + e^{\omega}\log^2 p)$-time algorithm [7]. Note that it takes $\Omega(e^2\log^2 p)$ bits to input the groups in $\mathfrak{H}^2_{p,e}$ by any of the standard methods, including matrices, presentations, or permutations. These algorithms have been implemented in the computer algebra system Magma [5] and decide isomorphism for groups as large as $n = 5^{256}$ in about an hour on a general-purpose personal computer [7, Figure 1.1]. The algorithms in [7] further give a complete invariant for the groups in $\mathfrak{H}^2_{p,e}$, which is a homogeneous polynomial of degree e in $\mathbb{F}_p[x,y]$. This implies that the number of isomorphism classes in $\mathfrak{H}^2_{p,e}$ is at most p^e; see [7, Proposition 9.2].

Some of the steps in the proof of Theorem 1.5 can be extracted as special cases of results in [21, 8, 7]. However, there is an increased need to provide an introduction into the methods in those works. We have made this exposition largely self-contained and we rely as much as possible on proofs based in linear algebra as found in [18].

Preliminaries

General claims about groups can be found in [25]. We assume all groups in this note are finite. The *Frattini subgroup* $\Phi(G)$ is the intersection of the maximal subgroups of G. The *exponent* of a group G is the least positive integer m such that for every $g \in G$, $g^m = 1$. The *commutator subgroup* G' is the smallest normal subgroup whose quotient is abelian, equivalently the subgroup generated by the commutators $[x,y] = x^{-1}x^y = x^{-1}y^{-1}xy$. $Z(G)$ denotes the *center* of G. We write $G^p = \langle x^p \mid x \in G\rangle$. As in [7], we borrow terminology from Lie theory and say the *genus* of a group G of nilpotence class 2 and exponent p is

$$p\text{-genus}(G) = \log_p |G| - d(G). \tag{1.8}$$

We will critically involve the following fact found in [25, p. 140].

Theorem 1.9 (Burnside Basis Theorem)**.** *For a p-group G, $\Phi(G) = G'G^p$ and $G/\Phi(G) \cong \mathbb{Z}_p^{d(G)}$.*

We will make frequent use of the fact that $\mathbb{Z}_p^d$ is both an abelian group and a natural $\mathbb{F}_p$-vector space. In this work all rings, algebras, and modules are unital (have a unit element), and subrings use the same unit as the superring. For emphasis we write $A \leq B$ for subsets which also are substructures such as subgroups and subalgebras. Finally we write $\mathrm{GL}_d(\mathbb{F}_q)$ for the group of invertible linear automorphisms on $\mathbb{F}_q^d$, and $\mathrm{SL}_d(\mathbb{F}_q)$ for the subgroup of transformations with determinant 1.

2 A formula for subgroup profiles

We prove a formula that, under some hypotheses, calculates the subgroup profiles in p-groups. This allows us to construct groups that produce the same profile without need to directly compare the groups.

Theorem 2.1. *Let G be a p-group in which $\mathrm{Aut}(G)$ acts transitively on maximal subgroups and such that for a maximal subgroup M of G, $d(G) = 1 + d(M)$. Then for every $J < G$, the size of $\mathfrak{J}(J) = \{K < G \mid K \cong J\}$ is*

$$\sum_{f=1}^{1+d(M)} \frac{p^{1+d(M)}-1}{p^f-1} \left|\left\{K \leq M \;\middle|\; K \cong J \text{ and } |M : K\Phi(M)| = p^{f-1}\right\}\right|.$$

Hence the profile map $J \mapsto |\mathfrak{J}(J)|$ depends only on the isomorphism type of a maximal subgroup of G.

While the hypothesis of Theorem 2.1 is restrictive, in Proposition 5.1 we demonstrate that the automorphism groups of groups $G \in \mathfrak{H}^{g}_{p,e}$ each contain $\mathrm{SL}_2(\mathbb{F}_{p^e})$ acting transitively on the maximal subgroups of G, just as $\mathrm{SL}_2(\mathbb{F}_{p^e})$ acts transitively on $\mathbb{F}_p$-hyperplanes of $\mathbb{F}_p^{2e} \cong G/\Phi(G)$. Having targeted this particular action may help expose the reason we chose Heisenberg groups $H(\mathbb{F}_{p^e})$ at the start. Similar constructions can be fashioned for example from the symplectic group $\mathrm{Sp}_{2m}(\mathbb{F}_{p^{2e}})$ and other linear subgroups.

Lemma 2.2. *Let G be a p-group G with a maximal subgroup M having $d(G) = 1 + d(M)$. Then $\Phi(G) = \Phi(M)$.*

Proof. Using the Burnside Basis Theorem on G and on M we calculate

$$1 = \frac{|G : \Phi(G)| \cdot |\Phi(G)|}{|G : M| \cdot |M : \Phi(M)| \cdot |\Phi(M)|} = \frac{p^{d(G)}|\Phi(G)|}{p^{1+d(M)}|\Phi(M)|} = \frac{|\Phi(G)|}{|\Phi(M)|}.$$

As $\Phi(M) = M'M^p \le G'G^p = \Phi(G)$, we find that $\Phi(M) = \Phi(G)$. □

Proof of Theorem 2.1. Fix $J < G$. We use an $\mathrm{Aut}(G)$-invariant partition

$$\mathcal{J}(J) = \bigcup_{f=1}^{d(G)} \mathcal{J}(J, f), \qquad\qquad \mathcal{J}(J, f) = \left\{ K \in \mathcal{J}(J) \;\middle|\; |G : K\Phi(G)| = p^f \right\}.$$

Let $\mathcal{M}$ be the set of maximal subgroups of G and fix $M \in \mathcal{M}$ with $d(G) = 1 + d(M)$.

Fix f and define a bipartite graph between the two sets $\mathcal{J}(J, f)$ and $\mathcal{M}$, such that $(K, X) \in \mathcal{J}(J, f) \times \mathcal{M}$ is an edge if, and only if, $K \le X$. The action of $\mathrm{Aut}(G)$ on this graph permutes the vertices of $\mathcal{M}$ transitively. In particular, the degree of every vertex $X \in \mathcal{M}$ is the same as the degree of M. Apply Lemma 2.2 to conclude that $\Phi(G) = \Phi(M)$. Thus, for every $K \le M$, $K\Phi(G) = K\Phi(M)$ and so

$$\begin{aligned} \deg M &= \left| \left\{ K \le M \;\middle|\; K \cong J, |G : K\Phi(G)| = p^f \right\} \right| \\ &= \left| \left\{ K \le M \;\middle|\; K \cong J,\ |M : K\Phi(M)| = p^{f-1} \right\} \right|. \end{aligned}$$

Next we compute the degree of $K \in \mathcal{J}(J, f)$, i. e., the size of the set

$$\{X \in \mathcal{M} \mid K \le X\} = \{X \in \mathcal{M} \mid K\Phi(G) \le X\}.$$

Since $G/\Phi(G) \cong \mathbb{Z}_p^{d(G)}$ and $|G : K\Phi(G)| = p^f$ it follows that

$$(G/\Phi(G))/(K\Phi(G)/\Phi(G)) \cong \mathbb{Z}_p^f.$$

In particular the number of maximal subgroups of G containing K equals the number of hyperplanes in an f-dimensional $\mathbb{F}_p$-vector space.

At this point we count the number of edges in our graph in two ways.

$$\frac{p^{d(G)} - 1}{p - 1} \deg M = \sum_{X \in \mathcal{M}} \deg X = \sum_{K \in \mathcal{J}(J,f)} \deg K = |\mathcal{J}(J, f)| \frac{p^f - 1}{p - 1}.$$

Thus $|\mathcal{J}(J, f)| = \deg M \cdot (p^{1+d(M)} - 1)/(p^f - 1)$. The theorem follows. □

3 Making p-groups with matrices

We are interested in quotients of groups of (3×3)-matrices, but it will be easier to discuss properties of a larger class of groups. For that we use a general constructions of p-groups that has roots in studies of Brahana and Baer [6, 2]. Throughout this section $\mathbb{F}=\mathbb{F}_p$ is the field of coefficients.

Fix a set $\{T_1,\dots,T_g\}$ of $(r\times c)$-matrices. Here and throughout empty blocks in matrices are presumed to be 0 and $\top$ denotes the transpose. Define

$$M(u,v,w) := \left[\begin{array}{c|c|ccc} 1 & u & & w & \\ \hline & I_r & T_1v^\top & \cdots & T_gv^\top \\ \hline & & & I_g & \end{array}\right] \quad \text{for } u\in\mathbb{F}^r, v\in\mathbb{F}^c \text{ and } w\in\mathbb{F}^g. \tag{3.1}$$

We abbreviate $u*v=(uT_1v^\top,\dots,uT_gv^\top)$ and witness multiplication of these matrices behaves as follows.

$$\begin{aligned} M(u,v,w)M(u',v',w') &= M(u+u',v+v',w+w'+u*v'), \\ [M(u,v,w),M(u',v',w')] &= M(0,0,u*v'-u'*v), \\ M(u,v,w)^i &= M\left(iu,iv,iw+\binom{i}{2}u*v\right). \end{aligned}$$

From these we fashion the following group of matrices.

$$B(T_1,\dots,T_g)=\{M(u,v,w)\mid u\in\mathbb{F}^r, v\in\mathbb{F}^c, w\in\mathbb{F}^g\}. \tag{3.2}$$

Proposition 3.3. *Assuming $B=B(T_1,\dots,T_g)$ the following hold.*

(i) $B'\leq\{M(0,0,w)\mid w\in\mathbb{F}_p^g\}$ *with equality whenever* $\langle u*v\mid u\in\mathbb{F}^r, v\in\mathbb{F}^c\rangle=\mathbb{F}^g$.

(ii) $Z(B)\geq\{M(0,0,w)\mid w\in\mathbb{F}_p^g\}$ *with equality if* $\bigcap_i \mathrm{Null}(T_i)=0$, *where* $\mathrm{Null}(T_i)=\{u\mid uT_i=0\}$.

(iii) If $p>2$, then $M(u,v,w)^p=1$; hence, $\Phi(B)=B'$ and $\dim\langle T_1,\dots,T_g\rangle$ is the genus of B.

(iv) If $\bigcap_i \mathrm{Null}(T_i^\top)=0$, then $|B|=p^{r+c+g}$.

Notice if $r,s,g\approx n/3$ then there are $p^{n^3/27+\Theta(n^2)}$ distinct tuples $T_*=(T_1,\dots,T_g)$. Yet $d(B(T_*))\in O(n)$ so the number of isomorphism classes is bounded by $p^{O(n^2)}$. As a result these groups comprise $p^{n^3/27+\Theta(n^2)}$ pairwise distinct isomorphism types of groups of order p^n. Sims has shown the total number of groups of order p^n is $p^{2n^3/27+O(n^{2.5})}$ [4, Chapters 4 & 5]. So despite its humble appearance, this family is extremely complex.

As our fields $\mathbb{F}_{p^e}$ are finite, there exists an $\omega\in\mathbb{F}_{p^e}$ such that $\mathbb{F}_{p^e}=\mathbb{F}_p(\omega)$. Hence, $\{1,\omega,\dots,\omega^{e-1}\}$ is a basis for $\mathbb{F}_{p^e}$ as an $\mathbb{F}_p$-vector space. Define $t(\omega)_{ij}^{(k)}\in\mathbb{F}_p$ as the *structure constants* so that

$$\omega^i\cdot\omega^j=\sum_{k=0}^{e-1} t(\omega)_{ij}^{(k)}\omega^k.$$

Also let $T_k \in \mathbb{M}_e(\mathbb{F}_p)$ be such that $[T_{k+1}]_{(i+1)(j+1)} = t(\omega)^{(k)}_{ij}$.

Example 3.4. If $\mathbb{F}_{p^e} = \mathbb{F}_p(\omega)$ then $H(\mathbb{F}_q) \cong B(T_1, \dots, T_e)$.

In the next section we shall prove the following theorem.

Theorem 3.5. *For primes p and e, $G \in \mathfrak{H}^2_{p,e}$ if, and only if, there are invertible $(e \times e)$-matrices (T_1, T_2) such that $G \cong B(T_1, T_2)$ where $T_1^{-1}T_2$ has an irreducible minimal polynomial of degree e.*

3.1 Subgroups by row, column, and matrix elimination

One way to explore the subgroups of the groups $B(T_1, \dots, T_g)$ is to restrict the range of values of u or v in the formula given in (3.2). For instance, suppose we restrict the coordinate $u_i = 0$. The result is that the values in the i-th row of each matrix $T_1, \dots, T_g$ can be ignored within that subgroup. Hence the subgroup we get is isomorphic to the group we obtain by first removing the i-th row of each matrix in $\{T_1, \dots, T_g\}$ and then using the construction of (3.2) to create a group on these smaller matrices. Removing one row produces a maximal subgroup, two rows a subgroup of index p^2, and so on. A similar idea applies to columns. Reversing the process and inserting rows or columns creates subgroup embeddings.

Restricting values of w in (3.2) may result in a subset that is not closed under multiplication. A way to avoid that concern is to eliminate entries w_i only once the corresponding matrix $T_i = 0$.

Example 3.6. To build an embedding of Brahana groups, e. g., $H(\mathbb{F}_3)$ into $H(\mathbb{F}_9)$, we may add matrices to our list of matrices, or add to the rows and columns of the matrices we posses. In this example we let

$$\mathbb{F}_9 = \left\{ \begin{bmatrix} a_0 & a_1 \\ -a_1 & a_0 \end{bmatrix} \;\middle|\; a_0, a_1 \in \mathbb{F}_3 \right\}.$$

We display the concatenations as partitioned matrices.

$$\begin{aligned} H(\mathbb{F}_3) \cong B([1]) &\hookrightarrow B([1],[0]) \\ &\hookrightarrow B([1|0],[0|1]) \\ &\hookrightarrow B\left(\left[\begin{array}{cc} 1 & 0 \\ \hline 0 & 1 \end{array}\right], \left[\begin{array}{cc} 0 & 1 \\ \hline -1 & 0 \end{array}\right] \right) \cong H(\mathbb{F}_9). \end{aligned}$$

Using this process in reverse (removing rows, columns, or matrices) lets us explore many of the subgroups of Brahana groups. We emphasize that this approach is not guaranteed to explore every subgroup.

In light of Theorem 2.1 we build a family of groups each having a maximal subgroup of a fixed isomorphism type. As in [18, p. 70], for a polynomial $a(t) = a_0t^0 + \dots + a_{e-1}t^{e-1} + t^e \in \mathbb{F}_p[t]$, the *companion matrix* will be

$$C(a(t)) = \begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ a_0 & \cdots & & a_{e-1} \end{bmatrix}.$$

Lemma 3.7. *For a polynomial $a(t)$ of degree e, the group $G = B(I_e, C(a(t)))$ has a maximal subgroup M whose isomorphism type depends only on p, e, and $d(G) = 1 + d(M)$.*

Proof. We delete the last row of I_e and $C(a(t))$ to obtain

$$M = B\left(\overbrace{\begin{bmatrix} 1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{bmatrix}}^{e}, \overbrace{\begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \end{bmatrix}}^{e}\right) \hookrightarrow$$

$$B\left(\left[\begin{array}{cccc} 1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0 \\ \hline 0 & \cdots & & 1 \end{array}\right], \left[\begin{array}{cccc} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ \hline a_0 & \cdots & & a_{e-1} \end{array}\right]\right) = G.$$

Evidently $p^{d(M)} = |M : \Phi(M)| = p^{2e-1} = p^{d(G)-1}$. □

3.2 Quotient groups by linear combinations

Next we will want some quotient groups of $B(T_1, \dots, T_g)$. One can see in (3.2) that for each subset $\{i_1, \dots, i_s\} \subseteq \{1, \dots, g\}$, there is a natural surjection $B(T_1, \dots, T_g) \to B(T_{i_1}, \dots, T_{i_s})$ and that is indeed a group homomorphism. This is an analogue to the way we created subgroups in the previous section.

Along with reducing the number of matrices we can take linear combinations. Given scalars $(a_1, \dots, a_g)$ there is an epimorphism from $B(T_1, \dots, T_g)$ to $B(a_1T_1 + \cdots + a_gT_g)$. More generally given a $(g' \times g)$-matrix A, there is an epimorphism

$$B(T_1, \dots, T_g) \mapsto B\left(\sum_{j=1}^{g} A_{1j}T_j, \dots, \sum_{j=1}^{g} A_{g'j}T_j\right).$$

3.3 Notable isomorphisms

There are also direct ways to create groups isomorphic to $B(T_1, \dots, T_g)$. For example, for invertible matrices $X \in \mathbb{M}_r(\mathbb{F}_p)$ and $Y \in \mathbb{M}_c(\mathbb{F}_p)$,

$$B(T_1, \dots, T_g) \cong B(XT_1Y^\top, \dots, XT_gY^\top).$$

We may also permute the order of the matrices. In particular we can always insist the first matrix have largest rank and that it be expressed in the form

$$\begin{bmatrix} I_a & 0 \\ 0 & 0 \end{bmatrix}$$

through Gaussian elimination. Thus the groups $B(T_1)$ can be classified up to isomorphism by the rank of T_1.

More generally, for each $i, j \in \{1,\dots,g\}$, and $s \in \mathbb{F}_p^\times$,

$$B(T_1,\dots,T_g) \cong B(T_1,\dots,T_i + sT_j,\dots,T_g) \cong B(T_1,\dots,sT_i,\dots,T_g).$$

Thus, if $\{T_1',\dots,T_g'\}$ is another basis for $\langle T_1,\dots,T_g\rangle$, then $B(T_1,\dots,T_g) \cong B(T_1',\dots,T_g')$. There can be further isomorphisms between these groups, but these will suffice for our present discussion.

Using these observations we can make even more complex embeddings.

Lemma 3.8. *For every $a(t), b(t) \in \mathbb{F}_p[t]$ with $\deg b(t) =: f < e := \deg a(t)$, there is an embedding $B(I_f, C(b(t)))$ into $B(I_e, C(a(t)))$.*

We emphasize that $b(t)$ has no relation to $a(t)$ other than having lower degree. So there is no algebraic reason to guess the possible embedding of $B(I_f, C(b(t)))$ into $B(I_e, C(a(t)))$. Manipulating matrices demonstrates how this is done.

Proof. Fix $b_0,\dots,b_{e-2} \in \mathbb{F}_p$.

$$\begin{bmatrix} 1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ b_0 & \dots & b_{e-2} & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{bmatrix}, \tag{3.9}$$

$$\begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ b_0 & \dots & b_{e-2} & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ b_0 & \dots & b_{e-2} & 1 \end{bmatrix}. \tag{3.10}$$

Thus, setting $b(t) = b_0 t^0 + \cdots + b_{e-2}t^{e-2} + t^{e-1}$, we obtain the following embedding. For the isomorphism we are using the identity $B(T_1Y^\top, T_2Y^\top) \cong B(T_1, T_2)$ following the calculation of (3.9) and (3.10).

$$\begin{aligned} B(I_{e-1}, C(b(t))) &\hookrightarrow B\left(\left[\begin{array}{cccc|c} 1 & 0 & & & 0 \\ & \ddots & \ddots & & \vdots \\ & & & 1 & 0 \end{array}\right], \left[\begin{array}{cccc|c} 0 & 1 & & & 0 \\ & \ddots & \ddots & & \vdots \\ b_0 & \dots & b_{e-2} & & 1 \end{array}\right] \right) \\ &\cong B\left(\begin{bmatrix} 1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \end{bmatrix} \right) \\ &\hookrightarrow B(I_e, C(a(t))). \end{aligned}$$

□

Remark 3.1. In light of Theorem 3.5, Lemma 3.8 shows that the groups in $\mathfrak{H}^2_{p,e}$ each have $p^{\Omega(e)}$ isomorphism types of proper subgroups.

Proposition 3.11. *Given $(e \times e)$-matrices $(T_1,\dots,T_g)$ where T_1 is invertible, there are polynomials $a_1(t)|\cdots|a_m(t)$ of polynomials in $\mathbb{F}_p[t]$, and matrices $\tilde{T}_3,\dots,\tilde{T}_g$ such that*

$$B(T_1,\dots,T_g) = B(I_e, C(a_1(t)) \oplus \cdots \oplus C(a_m(t)), \tilde{T}_3,\dots,\tilde{T}_g).$$

Proof. Use the Frobenius Normal Form [18, p. 93] to find a divisor chain $a_1(t)|\cdots|a_m(t)$ and an invertible matrix X such that

$$X^{-1}(T_1^{-1}T_2)X = C(a_1(t)) \oplus \cdots \oplus C(a_m(t)).$$

Hence,

$$\begin{aligned} B(T_1, T_2, \ldots, T_g) &\cong B(I_e, T_1^{-1}T_2, \ldots, T_1^{-1}T_g) \\ &\cong B(I_e, C(a_1(t)) \oplus \cdots \oplus C(a_m(t)), \ldots, X^{-1}T_1^{-1}T_gX). \end{aligned}$$

So for $3 \le i \le g$, set $\tilde{T}_i = X^{-1}T_1^{-1}T_2X$. $\square$

4 Isomorphisms between quotients of Heisenberg groups

We have so far created many groups and demonstrated ways to construct varied subgroups and quotients. Our effort now shifts back to Heisenberg groups and in particular we will tackle the question of isomorphisms and automorphisms within $\mathfrak{H}^2_{p,e}$. Our main results in this section are proofs of Theorem 3.5 and the following result.

Theorem 4.1. *Every isomorphism between nonabelian quotients of H of genus $g > 1$ lifts to an automorphism of H.*

This is a special case of [21, Theorem 4.4]. We give a self-contained and largely matrix-based proof.

4.1 The role of commutation

A first principle in the theory of nilpotent groups is to treat groups like algebras by invoking commutation $[x,y] = x^{-1}x^y = x^{-1}y^{-1}xy$ as a skew-commutative multiplication. This very nearly distributes over the usual product, in the following way.

$$[xy,z] = [x,z]^y[y,z], \qquad [x,yz] = [x,z][x,y]^z. \tag{4.2}$$

With $q = p^e$ and $H = H(\mathbb{F}_q)$, commutation takes the following form.

$$\left[\begin{bmatrix} 1 & \alpha & \gamma \\ & 1 & \beta \\ & & 1 \end{bmatrix}, \begin{bmatrix} 1 & \alpha' & \gamma' \\ & 1 & \beta' \\ & & 1 \end{bmatrix}\right] = \begin{bmatrix} 1 & 0 & \alpha\beta' - \alpha'\beta \\ & 1 & 0 \\ & & 1 \end{bmatrix}. \tag{4.3}$$

This shows the following two groups are abelian.

$$H' = [H,H] = \left\{ \begin{bmatrix} 1 & 0 & \gamma \\ & 1 & 0 \\ & & 1 \end{bmatrix} \middle| \gamma \in \mathbb{F}_q \right\}, \qquad H/H' \cong \{(\alpha,\beta) \mid \alpha,\beta \in \mathbb{F}_q^m\}.$$

Evidently there are isomorphisms

$$\iota : H/H' \to \langle \mathbb{F}_q^2, +\rangle \text{ and } \hat{\iota} : H' \to \langle \mathbb{F}_q, +\rangle. \tag{4.4}$$

None of these isomorphisms is natural in the category of groups. In particular neither H/H' nor H' is an obvious $\mathbb{F}_q$-vector space as scalar multiplication is not part of the operations of a group.

Normal subgroups are characterized as follows.

Lemma 4.5. *For $h \in H - H'$, $[h,H] = H'$; thus, if N is normal in H then either $H' \leq N$ or $N \leq H'$.*

4.2 Quotients of H

To inspect the quotients of H we use a method to "linearize" a nilpotent group which is in some sense the reversal of the constructions we gave in Section 3. Early versions of this approach were described by Brahana and Baer [2, 6].

Since elements in $H' = [H,H]$ commute with the whole group, the identities (4.2) imply that commutation factors through $H/H' \times H/H' \to H'$ and thereby affords a biadditive map $[,]_+ : \langle \mathbb{F}_q^2, +\rangle \times \langle \mathbb{F}_q^2, +\rangle \to \langle \mathbb{F}_q, +\rangle$,

$$[(\alpha,\beta),(\alpha',\beta')]_+ = \alpha\beta' - \alpha'\beta = (\alpha,\beta)\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}(\alpha',\beta')^\top. \tag{4.6}$$

To distinguish between the various roles of $[,]$ we let $[,]$ denote group commutation and $[,]_+$ the biadditive mapping that commutation produces.

Remark 4.1. The expression in (4.6) is misleading. While $\alpha\beta'$ and $\alpha'\beta$ are defined in $\mathbb{F}_q$, our codomain is technically the elementary abelian group $\langle \mathbb{F}_q, +\rangle$ and the specific identification depends on the perhaps arbitrary choice of maps $(\iota,\hat{\iota})$ of (4.4). Within isomorphism testing such small intuitive leaps can hide challenging computations and on a theoretical level it remains to be justified that the maps $(\iota,\hat{\iota})$—which are not $\mathbb{F}_q$-linear, nevertheless preserve the geometric properties of an $\mathbb{F}_q$-bilinear form. A more precise formulation of (4.6) capable of addressing these concerns is given below in (4.8).

Now Lemma 4.5 shows that for $N < H'$, $(H/N)' = H'/N$. So the commutation of the quotient H/N will accordingly afford a new biadditive map

$$[,]_+^{H/N} : \langle \mathbb{F}_q^2, +\rangle \times \langle \mathbb{F}_q^2, +\rangle \to \langle \mathbb{F}_q, +\rangle \xrightarrow{\pi} \mathbb{Z}_p^g$$

where π is given as the homomorphism $\langle \mathbb{F}_q, +\rangle \cong H' \to H'/N \cong \mathbb{Z}_p^g$. The genus of H/N is the value g.

Let us look closely at the case of genus $g = 1$. Fix $\pi : \langle \mathbb{F}_q, +\rangle \to \mathbb{Z}_p$. Choose a basis $\{\alpha_1, \dots, \alpha_e\}$ for $\langle \mathbb{F}_q, +\rangle$ as an $\mathbb{F}_p$-vector space and such that $\pi(\alpha_i) = 1$ if $i = 1$ and 0 otherwise. Define

$$T_{ij} = \pi([(\alpha_i, 0),(0,\alpha_j)]) = \pi(\alpha_i\alpha_j).$$

Observe

$$T_{ij} = \pi(\alpha_i\alpha_j) = \pi(\alpha_j\alpha_i) = T_{ji}. \tag{4.7}$$

So $T = T^\top$. Regarded as a map of $\mathbb{F}_p$-vector spaces we see

$$[(\alpha,\beta),(\alpha',\beta')]_+^{H/N} = \begin{bmatrix}\alpha & \beta\end{bmatrix}\begin{bmatrix}0 & T\\ -T & 0\end{bmatrix}\begin{bmatrix}\alpha'\\ \beta'\end{bmatrix}.$$

As we vary H/N amongst groups of arbitrary genus $1 \le g \le e$ we describe $[,]_+ = [,]_+^{H/N}$ by a list of linearly independent invertible symmetric matrices $T_1,\dots,T_g \in \mathbb{M}_e(\mathbb{F}_p)$ such that

$$[(\alpha,\beta),(\alpha',\beta')]_+ = \left(\begin{bmatrix}\alpha & \beta\end{bmatrix}\begin{bmatrix}0 & T_1\\ -T_1 & 0\end{bmatrix}\begin{bmatrix}\alpha'\\ \beta'\end{bmatrix},\dots,\begin{bmatrix}\alpha & \beta\end{bmatrix}\begin{bmatrix}0 & T_g\\ -T_g & 0\end{bmatrix}\begin{bmatrix}\alpha'\\ \beta'\end{bmatrix}\right). \tag{4.8}$$

This demonstrates the following correspondence.

Theorem 4.9 (Brahana correspondence)**.** *A group H/N whose commutation is described by linearly independent invertible symmetric matrices $(T_1,\dots,T_g)$ where $H/N \cong B(T_1,\dots,T_g)$. In particular all quotients H/N of genus 1 are isomorphic.*

Proof. The $(T_1,\dots,T_g)$ are described above. Recall $M(u,v,w)$ from (3.1). The required isomorphism $B(T_1,\dots,T_g) \to H/N$ is as follows.

$$M(u,v,w) \mapsto \begin{bmatrix}1 & \iota^{-1}(u) & \hat{\iota}^{-1}(w)\\ & 1 & \iota^{-1}(v)\\ & & 1\end{bmatrix} \mod N.$$

If $g = 1$ then $H/N \cong B(T_1) \cong B(I_e)$. □

Corollary 4.10. *The groups in $\mathfrak{H}^2_{p,e}$ have equal multisets of isomorphism types of proper quotient groups.*

Proof. Fix $N \le H'$ with $|H:N| = p^{2e+2}$. As $p^{2e+2} = |H:H'|\cdot|H':N| = p^{2e}|H':N|$ we find that $|H':N| = p^2$, and so H/N has genus 2. As in Lemma 4.5, if $N < K \le H$ and K/N is normal in H/N, then $K < H'$ or $H' \le K$. If $H' \le K$ then $(H/N)/(K/N) \cong H/K \cong \mathbb{Z}_p^f$ where $p^f = |H:K|$. This does not depend on the choice of N. The number of choices for K is the number of subgroups in $\mathbb{Z}_p^{2e}$ of index f, which again does not depend on N. Otherwise $N < K < H'$ and so $|H':K| = p$. Thus $(H/N)/(K/N) \cong H/K$ has genus 1. So by Theorem 4.9 its isomorphism type is fixed and independent of N. Finally, $H'/N \cong \mathbb{Z}_p^2$ so there are exactly $p+1$ choices of K with $N < K < H'$. This is independent of N. □

4.3 Distributive products

Throughout this section $\mathbb{F} = \mathbb{F}_p$ and $q = p^e$. To prove Theorem 4.1 we need a brief detour to discuss distributive products. Take a subset $S \subseteq \mathbb{M}_r(\mathbb{F}) \times \mathbb{M}_c(\mathbb{F})$. Note that we do not require that S be a subring or have any algebraic structure, though often S is a generating set for some interesting algebraic structure; see Remark 4.2. Recall $\top$ denotes transpose. Define

$$\mathbb{F}^r \otimes_S \mathbb{F}^c := \{X \in \mathbb{M}_{r\times c}(\mathbb{F}) \mid \forall (L,R) \in S, L^\top X = XR\}. \tag{4.11}$$

We further develop $\mathbb{F}^r \otimes_S \mathbb{F}^c$ into a distributive product. First $\mathbb{M}_{r\times c}(\mathbb{F}) = (\mathbb{F}^r \otimes_S \mathbb{F}^c) \oplus K(S)$ where

$$K(S) := \langle L^\top X - XR \mid X \in \mathbb{M}_{r\times c}(\mathbb{F}), (L,R) \in S \rangle. \tag{4.12}$$

The map π_S from $\mathbb{M}_{r\times s}(\mathbb{F})$ onto $\mathbb{F}^r \otimes_S \mathbb{F}^c$ with kernel $K(S)$ lets us define a distributive *tensor* product

$$\otimes = \otimes_S : \mathbb{F}^r \times \mathbb{F}^c \to \mathbb{F}^r \otimes_S \mathbb{F}^c, \qquad\qquad u \otimes v = \pi_S(u^\top v).$$

Notice for $(L,R) \in S$, $\pi_S(L^\top X) = \pi_S(XR)$ and so we find

$$(uL) \otimes v = \pi_S(L^\top (u^\top v)) = \pi_S((u^\top v)R) = u \otimes (vR).$$

Example 4.13. Let $C \in \mathbb{M}_e(\mathbb{F})$ such that $K = \{\sum_i a_i C^i \mid a_i \in \mathbb{F}\} \leq \mathbb{M}_e(\mathbb{F}_p)$ is a field of order p^e, e. g., take C to be the companion matrix of an irreducible polynomial of degree e. Then consider the following set of operators in $\mathbb{M}_{2e}(\mathbb{F}) \times \mathbb{M}_{2e}(\mathbb{F})$.

$$S = \left\{ \left(\begin{bmatrix} I_e & 0 \\ 0 & C \end{bmatrix}, \begin{bmatrix} C^\top & 0 \\ 0 & I_e \end{bmatrix} \right), \left(\begin{bmatrix} 0 & I_e \\ I_e & 0 \end{bmatrix}, \begin{bmatrix} 0 & -I_e \\ -I_e & 0 \end{bmatrix} \right) \right\}.$$

By solving the system of linear equations of (4.11) we find

$$\mathbb{F}^{2e} \otimes_S \mathbb{F}^{2e} = \left\{ \begin{bmatrix} 0 & \alpha \\ -\alpha^\top & 0 \end{bmatrix} \;\middle|\; \alpha \in K \right\} = \mathrm{Span}_K \left\langle \begin{bmatrix} 0 & I_e \\ -I_e & 0 \end{bmatrix} \right\rangle.$$

In particular $\mathbb{F}_p^{2e} \cong K^2$ and $\mathbb{F}_p^{2e} \otimes \mathbb{F}_p^{2e} \cong K$, and $\otimes_S : K^2 \times K^2 \to K$ is the same as the mapping in (4.6).

Turning now to a general distributive product $\circ : \mathbb{F}^r \times \mathbb{F}^c \to \mathbb{F}^g$, we can ask if $\circ$ is related to $\otimes_S$. We do so by comparing codomains, specifically we define

$$\otimes_S \to \circ :\equiv (\exists \tau : \mathbb{F}^r \otimes_S \mathbb{F}^c \to \mathbb{F}^g)(u \circ v = \tau(u \otimes_S v)). \tag{4.14}$$

We say $\circ$ *factors through* $\otimes_S$; see [8, (2.4)].

4.4 Adjoint algebras of distributive products

Section 4.3 imagined we possessed a set S of operators from which we craft a product. However our circumstance is reversed. We have distributive products $[,]_+$ arising from groups $G \in \mathfrak{H}^g_{p,e}$, and these products have no associated operators. Even so, we have seen hints, e. g., (4.8), that when we identify G with a quotient of $H(\mathbb{F}_q)$, then the operators $\mathbb{F}_q$ seem applicable to the analysis of $[,]_+$. We cannot expect to recover something arbitrary like $\mathbb{F}_q$ from $[,]_+$, rather we must set our sights on some form of *universal operators* for $[,]_+$, as those will persist independent of representation. We turn to a device introduced in [32] known as the *adjoint algebra* of a product.

Definition 4.15. Fix a distributive product $\circ : \mathbb{F}^r \times \mathbb{F}^c \to \mathbb{F}^g$. An *adjoint pair* $(L,R) \in \mathbb{M}_r(\mathbb{F}) \times \mathbb{M}_s(\mathbb{F})$ satisfies the following for each $u \in \mathbb{F}^r$ and each $v \in \mathbb{F}^c$

$$(uL) \circ v = u \circ (vR).$$

The *adjoint algebra* $\mathrm{Adj}(\circ)$ is the set of all adjoint pairs of $\circ$.

As the name suggests, $\mathrm{Adj}(\circ)$ is an algebra, i. e., an $\mathbb{F}$-vector space with an $\mathbb{F}$-bilinear associative unital multiplication. However, the multiplication is not coordinatewise but requires a twist as follows

$$(L_1, R_1)(L_2, R_2) = (L_1 L_2, R_2 R_1). \tag{4.16}$$

The composition in the second component is also referred to as *op*-multiplication. This makes $\mathrm{Adj}(\circ)$ a subring of what is commonly denoted $\mathbb{M}_{2e}(\mathbb{F}) \times \mathbb{M}_{2e}(\mathbb{F})^{\mathrm{op}}$. Indeed $\mathrm{Adj}(\circ)$ is a unital subalgebra—all our rings, modules and algebras to follow are unital. Given structure constants for $\circ$, such as those given in (4.8) for the products $[,]_+$, then we can compute a basis for $\mathrm{Adj}(\circ)$.

As intended, $\mathrm{Adj}(\circ)$ is a universal set of operators in the following sense. Recall (4.14).

Theorem 4.17 (Adjoint-tensor Galois correspondence [8, Theorem 2.11])**.** *Fix a distributive product $\circ : \mathbb{F}^r \times \mathbb{F}^c \to \mathbb{F}_p^g$ and $S \subseteq \mathbb{M}_r(\mathbb{F}) \times \mathbb{M}_s(\mathbb{F})$. Then*

$$S \subseteq \mathrm{Adj}(\circ) \Longleftrightarrow \otimes_S \to \circ.$$

In particular we obtain two closure operations: $S \subseteq \mathrm{Adj}(\otimes_S)$ and $\otimes_{\mathrm{Adj}(\circ)} \to \circ$. Furthermore

$$\mathrm{Adj}(\circ) = \mathrm{Adj}(\otimes_{\mathrm{Adj}(\circ)}), \qquad \otimes_S = \otimes_{\mathrm{Adj}(\otimes_S)}.$$

Notice if A is subalgebra of $\mathbb{M}_r(\mathbb{F}) \times \mathbb{M}_s(\mathbb{F})^{\mathrm{op}}$ generated as an algebra by a set S, then

$$\mathbb{F}^r \otimes_{\mathrm{Adj}(\otimes_S)} \mathbb{F}^c \subseteq \mathbb{F}^r \otimes_A \mathbb{F}^c \subseteq \mathbb{F}^r \otimes_S \mathbb{F}^c = \mathbb{F}^r \otimes_{\mathrm{Adj}(\otimes_S)} \mathbb{F}^c.$$

That is, $\mathbb{F}^r \otimes_S \mathbb{F}^c = \mathbb{F}^r \otimes_A \mathbb{F}^c = \mathbb{F}^r \otimes_{\mathrm{Adj}(\otimes_S)} \mathbb{F}^c$. In this way one sees there is no advantage to assuming at the start that we have an algebra over which we tensor.

Remark 4.2. Historically Whitney introduced tensor products as requiring rings, and that assumption has been carried into the literature, for example [17, Section IV.5]. We have demonstrated that the ring assumption has no actual role in defining tensor products and it is often a barrier to calculations. Indeed, even if we intend to tensor over a ring A, it is often the case that A is a proper subring of $\mathrm{Adj}(\otimes_A)$. So to insist on a fixed ring A is arbitrary. It would be enough to regard the image of A as a set and appeal to $\mathrm{Adj}(\otimes_A)$ for any necessary ring theory. The main point is $\mathbb{F}^r \otimes_S \mathbb{F}^c = \mathbb{F}^r \otimes_{\mathrm{Adj}(\otimes_S)} \mathbb{F}^c$ and the left-hand side is a more flexible construction.

There are two optional assumptions we have made for simplicity but which may be removed. The first is to use matrices instead of constructing $U \otimes_S V$ as a quotient of some infinite abelian group. Secondly, it would be enough to consider functions $S \to \mathbb{M}_r(\mathbb{F}) \times \mathbb{M}_c(\mathbb{F})$ instead of subsets.

One helpful observation is the ability to identify extension of scalars without prior assumptions.

Lemma 4.18. *Let $K \leq \mathbb{M}_e(\mathbb{F})$ be a subalgebra. If $\circ : K^r \times K^c \to K^g$ is biadditive and furthermore satisfies*

$$(\forall \alpha \in K) \qquad (\alpha u) \circ v = \alpha(u \circ v) = u \circ (\alpha v),$$

$u \circ K^c = 0$ only if $u = 0$, and $K^r \circ v = 0$ only if $v = 0$; then for every $(L, R) \in \mathrm{Adj}(\circ)$,

$$(\alpha u)L = \alpha(uL), \qquad (\alpha v)R = \alpha(vR).$$

Proof. The proof is a so-called "three pile shuffle" of the operators:

$$((\alpha u)L)\circ v = (\alpha u)\circ(uR) = \alpha(u\circ(vR)) = \alpha((uL)\circ v) = (\alpha(uL))\circ v.$$

As this is for each v and $((\alpha u)L - \alpha(uL))\circ K^c = 0$, we get that $(\alpha u)L = \alpha(uL)$. Do likewise with R. □

Example 4.19. Let $\mathbb{F}_{p^e} = \mathbb{F}_p(\omega)$ and $C = C(\omega)$ be the matrix of left multiplication matrix of by ω on $\langle \mathbb{F}_{p^e}, +\rangle \cong \mathbb{F}_p^e$. For $H = H(\mathbb{F}_{p^e})$, $[,]_+^H$ as defined in (4.3) with $N = 1$, and $\mathbb{F}_{p^e} \cong K = \{\sum_i a_i C^i \mid a_i \in \mathbb{F}\} \leq \mathbb{M}_e(\mathbb{F})$, we calculate that

$$\mathrm{Adj}([,]_+^H) = \left\{ \left(\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}, \begin{bmatrix} \delta & -\beta \\ -\gamma & \alpha \end{bmatrix} \right) \;\middle|\; \alpha,\beta,\gamma,\delta \in K \right\} \cong \mathbb{M}_2(\mathbb{F}_q).$$

Furthermore, $\langle \mathbb{F}_{p^e}, +\rangle \cong \langle \mathbb{F}_{p^e}^2, +\rangle \otimes_{\mathrm{Adj}([,]_+^H)} \langle \mathbb{F}_{p^e}^2, +\rangle$.

Proof. Consider the matrices $(T_1,\ldots,T_e)$ of (4.3). Notice from their definition that for each $\alpha \in K$

$$\alpha T_i = [(\alpha,0),(0,1)]_+ = [(0,1),(\alpha,0)]_+^{-1} = T_i\alpha. \tag{4.20}$$

In particular $CT_i = T_iC$ for each i. Hence, S from Example 4.13 is contained in $\mathrm{Adj}([,]_+^H)$. So, by the Adjoint-Tensor Galois Correspondence (Theorem 4.17),

$$\otimes_S \to \otimes_{\mathrm{Adj}([,]_+^H)}.$$

That means there is a $\tau : K \cong \mathbb{F}_p^{2e} \otimes_S \mathbb{F}_p^{2e} \to \langle \mathbb{F}_q, +\rangle = H'$ which is surjective because of Proposition 3.3(i). By dimensions this is an ($\mathbb{F}_p$-linear) isomorphism. In particular $\mathrm{Adj}([,]_+^H) = \mathrm{Adj}(\otimes_S)$. From Example 4.13, $\otimes_S : K^2 \times K^2 \to K$ satisfies the hypothesis of Lemma 4.18 so $\mathrm{Adj}(\otimes_S) \subseteq \mathbb{M}_2(K)\times\mathbb{M}_2(K)$. Furthermore, letting

$$J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},$$

and $(L,R) \in \mathrm{Adj}(\otimes_S)$, $L^\top J = JR$ so $R = J^{-1}L^\top J$. Therefore, $\mathrm{Adj}(\otimes_S) = \{(L, J^{-1}L^\top J) \mid L \in \mathbb{M}_2(K)\}$. □

4.5 Adjoint algebras of Heisenberg group commutation

Now we refocus on the goal of Theorem 4.1.

Lemma 4.21. *Fix a unital $\mathbb{F}_p$-subalgebra $K \leq \mathbb{M}_e(\mathbb{F}_p)$ where K is a field of order p^e. If $A \leq \mathbb{M}_e(\mathbb{F}_p)$ is a unital $\mathbb{F}_p$-subalgebra containing K, and e prime, then $A = K$ or $\mathbb{M}_e(\mathbb{F}_p)$.*

Proof. Let $V = \mathbb{F}_p^e$ be the natural (left) module for $\mathbb{M}_e(\mathbb{F}_p)$. So V is also an A-module and an F-vector space. Note that V is 1-dimensional as a K-vector space. As $K \leq A$, it follows that for every $0 \neq v \in V$, $V = Kv = Av$. So V is a simple A-module; hence, A is faithfully represented on a simple module V, that is A is primitive. By the Wedderburn-Artin theorem, A is therefore isomorphic to $\mathbb{M}_f(\Delta)$ for a finite division ring Δ [17, p. 421]. By the Dickson-Wedderburn theorem $\Delta \cong \mathbb{F}_{p^s}$ for some s [17, p. 462]. Lastly, $e = \dim_{\mathbb{F}_p} V = s\dim_{\mathbb{F}_{p^s}} V = fs$. As e is prime either $f = 1$ and $A = K$, or else $f = e$ and $s = 1$ which makes $A = \mathbb{M}_e(\mathbb{F}_p)$. □

Lemma 4.22. *If H/N has genus $g>1$ then* $\mathrm{Adj}([,]^H_+) = \mathrm{Adj}([,]^{H/N}_+) \cong \mathbb{M}_2(\mathbb{F}_q)$.

Proof. We start by observing some necessary adjoints. By the adjoint-tensor Galois correspondence, $\mathrm{Adj}([,]^H_+) \leq \mathrm{Adj}([,]^{H/N}_+)$. Now we claim this is an equality (as subalgebras of $\mathbb{M}_{2e}(\mathbb{F}_p)\times\mathbb{M}_{2e}(\mathbb{F}_p)^{\mathrm{op}}$).

We know that the commutation in H/N is given by a set $\{T_1,\dots,T_g\}$ of linearly independent invertible symmetric matrices (4.7). So the linear equations to solve to describe $\mathrm{Adj}([,]^{H/N}_+)$ are the following. For each $1\leq i\leq g$,

$$\begin{bmatrix} L_{11} & L_{12}\\ L_{21} & L_{22}\end{bmatrix}^{\top}\begin{bmatrix} 0 & T_i\\ -T_i & 0\end{bmatrix} = \begin{bmatrix} 0 & T_i\\ -T_i & 0\end{bmatrix}\begin{bmatrix} R_{11} & R_{12}\\ R_{21} & R_{22}\end{bmatrix}.$$

For $i=1$ we get

$$\begin{bmatrix} R_{11} & R_{12}\\ R_{21} & R_{22}\end{bmatrix} = \begin{bmatrix} 0 & T_1\\ -T_1 & 0\end{bmatrix}^{-1}\begin{bmatrix} L_{11} & L_{12}\\ L_{21} & L_{22}\end{bmatrix}^{\top}\begin{bmatrix} 0 & T_1\\ -T_1 & 0\end{bmatrix}.$$

Now $i=2\leq g$ adds the further constraints $L_{ij}(T_1^{-1}T_2) = (T_1^{-1}T_2)L_{ij}$. (Here we take advantage of the assumption that the T_i are symmetric but this condition can be relaxed at the expense of a more complex formula at this stage.)

Now consider the subalgebra $C(T_1^{-1}T_2) = \{L\in\mathbb{M}_e(\mathbb{F}_p) \mid LT_1^{-1}T_2 = T_1^{-1}T_2L\}$. Then

$$\begin{aligned}\mathrm{Adj}([,]^{H/N}_+) &\leq \left\{\left(\begin{bmatrix} L_{11} & L_{12}\\ L_{21} & L_{22}\end{bmatrix}, \begin{bmatrix} 0 & T_1\\ -T_1 & 0\end{bmatrix}^{-1}\begin{bmatrix} L_{11} & L_{12}\\ L_{21} & L_{22}\end{bmatrix}^{\top}\begin{bmatrix} 0 & T_1\\ -T_1 & 0\end{bmatrix}\right) \,\middle|\, L_{ij}\in C(T_1^{-1}T_2)\right\}\\ &\cong \mathbb{M}_2(C(T_1^{-1}T_2).\end{aligned}$$

By restricting to the first components of $\mathrm{Adj}([,]^H_+) \leq \mathrm{Adj}([,]^{H/N}_+)$, and invoking Example 4.19, we obtain $\mathbb{M}_2(K)\leq\mathbb{M}_2(C(T_1^{-1}T_2))$ and by first restricting to the upper right block we have $K\leq C(T_1^{-1}T_2)\leq\mathbb{M}_e(\mathbb{F}_p)$. If $C(T_1^{-1}T_2)=\mathbb{M}_e(\mathbb{F}_p)$ then $T_1^{-1}T_2$ commutes with every matrix and thus $T_1^{-1}T_2$ is a scalar matrix. However, T_2 and T_1 are linearly independent. So $T_1^{-1}T_2$ cannot be scalar. As a result $C(T_1^{-1}T_2)\neq\mathbb{M}_e(\mathbb{F}_p)$. By Lemma 4.21, $C(T_1^{-1}T_2)=K$. That is,

$$\mathrm{Adj}([,]^{H/N}_+) \leq \left\{\left(\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}, \begin{bmatrix}\delta & -\beta\\ -\gamma & \alpha\end{bmatrix}\right) \,\middle|\, \alpha,\beta,\gamma,\delta\in\mathbb{F}_q\right\} = \mathrm{Adj}([,]^H_+).$$

So indeed $\mathrm{Adj}([,]^H_+) = \mathrm{Adj}([,]^{H/N}_+)$. □

Proof Theorem 3.5. Fix $G\in\mathfrak{H}^2_{p,e}$. By Theorem 4.9 we know there are linearly independent symmetric invertible matrices (T_1,T_2) such that $G\cong B(T_1,T_2)\cong B(I_e,T_1^{-1}T_2)$. Let $a(t)$ be the minimal polynomial of this new $T_1^{-1}T_2$. As T_1 is independent of T_2, we know that $T_1^{-1}T_2$ cannot be a scalar matrix and so $a(t)$ has degree at least 2. We need to show $\deg a(t) = e$.

Now let $C(T_1^{-1}T_2) = \{L\in\mathbb{M}_e(\mathbb{F}_p) \mid LT_1^{-1}T_2 = T_1^{-1}T_2L\}$. Following the calculation of the adjoint ring above we know that

$$\mathrm{Adj}([,]^{H/N}_+) \cong \mathbb{M}_2(C(T_1^{-1}T_2)).$$

Thus, if $B(T_1,T_2)$ is a quotient of H then $C(T_1^{-1}T_2)\cong\mathbb{F}_q$. Since $\mathbb{F}_p[t]/(a(t))\cong\mathbb{F}_p[T_1^{-1}T_2]\leq C(T_1^{-1}T_2)$ it follows that $\mathbb{F}_p[T_1^{-1}T_2]$ is a subfield of $\mathbb{F}_q$. As $a(t)$ has degree greater than 1 and $\mathbb{F}_q$ has no intermediate fields, it follows that $\mathbb{F}_p[T_1^{-1}T_2]=\mathbb{F}_q$. Thus $a(t)$ is an irreducible polynomial of degree e.

Conversely if T_2 is conjugate to $C(a(t))$ then

$$\mathrm{Adj}\left([,]_+^{H/N}\right)\cong\mathbb{M}_2(\mathbb{F}_q)\cong\mathrm{Adj}([,]_+^H).$$

By the Adjoint-Tensor Galois correspondence, the commutation in $B(I_e,T_1^{-1}T_2)$ factors through the tensor product over $\mathrm{Adj}([,]_+^H)$. By Example 4.19 that tensor is also the commutation of H. So $B(T_1,T_2)$ is a quotient of H. □

Remark 4.3. At this point we can sketch the concepts behind the algorithms in Theorem 1.7(a), which we recall serve to recognize when a group G, given as a black-box group, is a quotient of a Heisenberg group. A key step is to construct the ring $\mathrm{Adj}([,]_+^G)$ and recognize if it isomorphic to $\mathbb{M}_2(\mathbb{F}_{p^e})$ for some e. If so then the commutation in G naturally factors through the tensor over $\mathbb{M}_2(\mathbb{F}_{p^e})$ which we saw in Example 4.19 gives us the commutation of $H(\mathbb{F}_{p^e})$. See [7, 21] for details.

4.6 Automorphisms of Heisenberg groups

Now we need to consider the automorphisms of H, assuming $p>2$. Each automorphism is described by three constituents:

1. a homomorphism $\tau:\langle\mathbb{F}_q^2,+\rangle\to\langle\mathbb{F}_q,+\rangle$,
2. an invertible matrix $\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}$ over $\mathbb{F}_q$, and
3. a field automorphism $\alpha\mapsto\bar{\alpha}$ of $\mathbb{F}_q$.

The corresponding automorphism is as follows.

$$\begin{bmatrix}1 & \alpha' & \gamma'\\ & 1 & \beta'\\ & & 1\end{bmatrix}\mapsto\begin{bmatrix}1 & \overline{\alpha'\alpha+\beta'\gamma} & \overline{(\alpha\delta-\beta\gamma)\gamma'+\tau(\alpha',\beta')}\\ & 1 & \overline{\alpha'\beta+\beta'\delta}\\ & & 1\end{bmatrix}. \tag{4.23}$$

Theorem 4.24. *Every automorphism of H has the form of* (4.23).

Our proof will follow the one give in [21, Proposition 2.9 & Theorem 4.1]. The automorphisms arising from (1), with parts (2) and (3) the identity, form the subgroup of so-called *central automorphisms*. We include them for completeness but remark that they do not influence our proofs to follow.

Remark 4.4. Statements in the literature about the automorphism groups of the of Heisenberg groups based on symplectic geometry can be misunderstood. Most claims concern $\mathbb{F}_p$, $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$, and in the latter cases considers only smooth automorphisms. As we cautioned in Remark 4.1, in the case of $\mathbb{F}_q$, $[,]_+:\langle\mathbb{F}_q^2,+\rangle\times\langle\mathbb{F}_q^2,+\rangle\to\langle\mathbb{F}_q,+\rangle$ is $\mathbb{F}_q$-bilinear but $[,]:H/H'\times H/H'\to H'$ is only biadditive. So only the cases of $\mathbb{Z}$ and $\mathbb{F}_p$ are immediate by standard geometric methods. One must recover the missing ring structure of the coefficients before appealing to geometric reasoning.

We saw in Example 4.19 that the commutation of Heisenberg groups is actually a special type of distributive product, a tensor product. This means instead of acting on a biadditive map we can act on a ring $\mathrm{Adj}([,]_+) \cong \mathbb{M}_2(\mathbb{F}_q)$.

Theorem 4.25 (Skolem-Noether [18, p. 237])**.** *The ring automorphisms of $\mathbb{M}_2(\mathbb{F}_q)$ are $Y \mapsto X^{-1}\bar{Y}X$ where X is an invertible 2×2 matrix and $\alpha \to \bar{\alpha}$ is a field automorphism of $\mathbb{F}_q$ applied to each entry of X.*

Proof. First the automorphism ϕ will send $\alpha I_2 \mapsto \bar{\alpha} I_2$ which gives us the field automorphism σ. Replacing ϕ with $\phi(Y^{\sigma^{-1}})$ we now have an $\mathbb{F}_q$-linear automorphism. That function maps the minimal right ideal

$$\left\{ \begin{bmatrix} \alpha & \beta \\ 0 & 0 \end{bmatrix} : \alpha, \beta \in \mathbb{F}_q \right\}$$

to another minimal right ideal, either

$$\left\{ \begin{bmatrix} 0 & 0 \\ \gamma & \delta \end{bmatrix} : \gamma, \delta \in \mathbb{F}_q \right\} \qquad \text{or} \qquad \left\{ \begin{bmatrix} \gamma & \delta \\ \nu\gamma & \nu\delta \end{bmatrix} : \gamma, \delta \in \mathbb{F}_q \right\},$$

for some $\nu \in \mathbb{F}_q$. Each of these is a 2-dimensional vector space over $\mathbb{F}_q$ so that transformation can be given by an invertible square matrix X. □

Lemma 4.26. *There is an epimorphism $\mathrm{Aut}(H) \to \mathrm{Aut}(\mathbb{M}_2(\mathbb{F}_q))$. The kernel consists of the central automorphisms of H.*

Proof. Let $\phi : H \to H$ be an automorphism. Since $\phi([h,k]) = [\phi(h), \phi(k)]$, ϕ factors through $\mathbb{F}_p^{2e} \cong H/H' \to H/H' \cong \mathbb{F}_p^{2e}$. So we let X be the matrix representing that transformation. Also we let $\hat{X}$ be the matrix describing the restriction of ϕ to $\mathbb{F}_p^e \cong H' \to H' \cong \mathbb{F}_p^e$. Notice $(X, \hat{X})$ satisfy

$$[(\alpha,\beta)X, (\alpha',\beta')X]_+ = [(\alpha,\beta),(\alpha',\beta')]_+\hat{X}.$$

Now take $(L,R) \in \mathrm{Adj}([,]_+)$. It follows that

$$\begin{aligned} [(\alpha,\beta)X^{-1}LX, (\alpha',\beta')]_+ &= [(\alpha,\beta)X^{-1}L, (\alpha',\beta')X^{-1}]_+\hat{X} \\ &= [(\alpha,\beta),(\alpha',\beta')X^{-1}RX]_+. \end{aligned}$$

In this way $\mathrm{Aut}(H)$ acts on $\mathrm{Adj}([,]_+) \cong \mathbb{M}_2(\mathbb{F}_q)$. We saw that commutation in $\mathrm{Aut}(H)$ is the same as the tensor product with $\mathrm{Adj}([,]_+)$ (Example 4.19). So every automorphism of $\mathrm{Adj}([,]_+)$ determines an automorphism of H. If $(X, \hat{X})$ is the identity pair then ϕ is a central automorphism by definition. □

Proof of Theorem 4.1. In the Brahana correspondence (Theorem 4.9) we saw that every nonabelian quotient H/N is determined up to isomorphism by the matrices $(T_1, \dots, T_g)$ which also define $[,]_+^{H/N}$. Fix an isomorphism $\phi : H/N_1 \to H/N_2$. Since $(H/N_i)/(H/N_i)' \cong H/H' \cong \langle \mathbb{F}_q^2, +\rangle$, we see ϕ determines a matrix

$$X = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \mathbb{M}_{2e}(\mathbb{F}_p).$$

Using the isomorphism $\tau : \langle \mathbb{F}_q, + \rangle \to \langle \mathbb{F}_q^2, + \rangle \otimes_{\mathbb{M}_2(\mathbb{F}_q)} \langle \mathbb{F}_q^2, + \rangle$ described in Example 4.19, we define $\Gamma : H \to H$ as follows. If $c \in \langle \mathbb{F}_q, + \rangle$ and $c\tau = \sum_i (a_i, b_i) \otimes (x_i, y_i)$, then define

$$\begin{bmatrix} 1 & a & c \\ & 1 & b \\ & & 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 & aA + bC & \sum_i (a_i, b_i)X \otimes (x_i, y_i)X \\ & 1 & aB + bD \\ & & 1 \end{bmatrix}.$$

From our proof of Lemma 4.26 we notice Γ is an automorphism of H if, and only if, $X^{-1}\mathrm{Adj}([,]_+)X = \mathrm{Adj}([,]_+)$. Since ϕ is an isomorphism $H/N_1 \to H/N_2$ we know that

$$X^{-1}\mathrm{Adj}\left([,]_+^{H/N_1}\right)X = \mathrm{Adj}\left([,]_+^{H/N_2}\right).$$

By Lemma 4.22 we know $\mathrm{Adj}([,]_+) = \mathrm{Adj}\left([,]_+^{H/N_i}\right)$. So $\Gamma \in \mathrm{Aut}(H)$ and $\Gamma(N_1) = N_2$ and induces ϕ. $\square$

Corollary 4.27. *The set $\mathfrak{H}_{p,e}^{2e+2}$ has at least p^{e-3}/e isomorphism types.*

Proof. The number of subgroups $N < H'$ of index p^2 is the number of subspaces of codimension 2 in an $\mathbb{F}_p$-vector space $H' \cong \mathbb{F}_p^e$. That number is

$$\frac{(p^e - 1)(p^e - p)}{(p^2 - 1)(p - 1)}.$$

Meanwhile the action by $\mathrm{Aut}(H)$ on H' has order $e(p^e - 1)$; see (4.23). So the number of orbits is at least p^{e-3}/e. By Theorem 4.1 these orbits are in bijection with isomorphism types so the result follows. $\square$

Remark 4.5. The proof of Theorem 4.1 and the analysis in Corollary 4.27 mimics how we efficiently test isomorphism of quotients of Heisenberg groups as announced in Theorem 1.7(b). We transform the question into one of asking if two $\mathbb{F}_p$-subspaces of $\mathbb{F}_{p^e}$ are in the same orbit under $\mathbb{F}_{p^e}^\times \rtimes \mathrm{Gal}(\mathbb{F}_{p^e})$. As discovered by Rónyai (see [21, Lemma 4.8]), the orbits under $\mathbb{F}_{p^e}^\times$ can be decided by solving a system of linear equations. The remaining action by $\mathrm{Gal}(\mathbb{F}_{p^e})$ has small orbits.

5 Proof of Theorem 1.5

In Corollary 4.27 we used the fact that the representation of $\mathrm{Aut}(H)$ on H' induces the group $\mathbb{F}_{p^e}^\times \rtimes \mathrm{Gal}(\mathbb{F}_{p^e})$. Now we use the fact that the kernel of that representation induces the group $\mathrm{SL}(2, \mathbb{F}_{p^e})$ on H/H'.

Proposition 5.1. *For every $N \leq H'$, $\mathrm{Aut}(H/N)$ acts transitively on the maximal subgroups of H/N.*

We need a few observations, compare [25, p. 135 & 140].

Lemma 5.2. *In a group G, for a normal subgroup N contained in $\Phi(G)$ (including $N = 1$), $\Phi(G/N) = \Phi(G)/N$ and the maximal subgroups of G are in bijection with those in G/N and with those in $G/\Phi(G)$.*

Lemma 5.3. *For a p-group G, there is a bijection between the maximal subgroups of G and the projective points in* $(\mathbb{F}_p^{d(G)})^\top$*—the dual space of* $\mathbb{F}_p^{d(G)}$*. In particular* $\mathrm{Aut}(G)$ *acts transitively on its maximal subgroups if, and only if, the induced action of* $\mathrm{Aut}(G)$ *on* $(\mathbb{F}_p^{d(G)})^\top$ *is transitive on projective points.*

Proof. By the Burnside basis theorem there is an isomorphism $\tau : G/\Phi(G) \to \mathbb{F}_p^{d(G)}$. Since each maximal subgroup M of G contains $\Phi(G)$, $M/\Phi(G)$ is maximal in $G/\Phi(G)$ and so $W = \tau(M/\Phi(G))$ is a hyperplane. In particular W is identified with $\{\phi \in (\mathbb{F}_p^{d(G)})^\top \mid W\phi = 0\}$ as a projective point in $W^\top$. □

Lemma 5.4. *The natural action of* $\mathrm{SL}_2(\mathbb{F}_{p^e})$ *on the dual space* $(\mathbb{F}_{p^e}^2)^\top$ *(i. e., the action on column-vectors) is transitive on non-zero vectors, and therefore also on projective points.*

Proof. We show $(1,0)$ can reach both (α,β) and $(0,\alpha)$, provided $\alpha \neq 0$, using determinant 1 matrix.

$$\begin{bmatrix}\alpha & 0\\ \beta & \alpha^{-1}\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}\alpha\\ \beta\end{bmatrix} \qquad\qquad \begin{bmatrix}0 & -\alpha^{-1}\\ \alpha & 0\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\ \alpha\end{bmatrix}.$$ □

Proof of Proposition 5.1. Fix $N \lhd H$ such that $|H : N| = p^{2e+2}$. Because $N \leq \Phi(H)$, by Lemma 5.2, the maximal subgroups of H are in bijection of those of H/N. Following Proposition 3.3 we know $H' = \Phi(H)$ and $(H/N)/\Phi(H/N) \cong H/\Phi(H) \cong \mathbb{F}_p^{2e}$.

Notice from Theorem 4.24 that there is a subgroup

$$C_{\mathrm{Aut}(H)}(H') = \{\phi \in \mathrm{Aut}(H) \mid (H')\phi = 1_{H'}\}.$$

As $N < H'$, there is a homomorphism

$$\rho : C_{\mathrm{Aut}(H)}(H') \to \mathrm{Aut}(H/N).$$

Furthermore, ρ faithfully embeds the automorphisms of H induced by matrices

$$\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}$$

with determinant 1, as described in Theorem 4.24. In particular there is a representation of

$$\mathrm{SL}_2(\mathbb{F}_{p^e}) \to \mathrm{Aut}(H/N)$$

with the natural action on $\mathbb{F}_{p^e}^2 \cong (H/N)/\Phi(H/N)$. By Lemma 5.4, this action is transitive on projective points. By Lemma 5.3 it follows that $\mathrm{Aut}(H/N)$ acts transitively on the maximal subgroups of H/N. □

Proof of Theorem 1.5. Corollaries 4.27 & 4.10 establish that the set $\mathfrak{H}_{p,e}^{2e+2}$ has at least p^{e-3}/e isomorphism types and that these groups all have the same multiset of isomorphism types of proper quotient groups. Finally, Proposition 5.1 and Lemma 3.7 allow us to invoke Theorem 2.1 to conclude the proof. □

6 Closing remarks

6.1 Further comparisons of the groups H/N

The groups in $\mathfrak{H}^2_{p,e}$ are an extreme illustration of the difficulty to capture isomorphism by a list of invariants. Along with equivalent profiles we summarize the following further similarities.

Each $G \in \mathfrak{H}^2_{p,e}$ has $G' = Z(G) = \Phi(G) \cong \mathbb{Z}_p^2$. Also the groups have isomorphic lattices of normal subgroups. They have exponent p and the same multiset of conjugacy class sizes (Lemma 4.5).

Next we remark that for any fixed $g \leq e$, the groups in $\mathfrak{H}^g_{p,e}$ have isomorphic character tables [21, Section 6.2]. (See [25, p. 232] for definitions and basic implications of character tables.) In fact a stronger property holds. Observe that character table columns are indexed by conjugacy classes of a group. Because $(g^{-1}xg)^m = g^{-1}x^m g$ we can speak of the m-th power map as as function on conjugacy classes of G. An often strong isomorphism invariant of groups is to consider character table isomorphisms that also preserve all powers on the conjugacy classes. For instance, the examples of Rottlaender have isomorphic character tables as well but they are distinguished when in addition we add the power-map constraint. For a p-group it suffices to consider the p-th powers. Brauer asked if non-isomorphic groups could have an isomorphism of character tables that also preserves the powers of conjugacy classes of the group. Dade [9] provided examples using groups of order p^7, class 3 and exponent p. Our examples are of class 2, and they also answer Brauer's question providing an infinite family with character tables as large as possible amongst groups of exponent p. See Nenciu [24] for examples with composite exponent.

The groups in $\mathfrak{H}^g_{p,e}$ are directly and centrally indecomposable and with the same algebraic type of indecomposability (an invariant introduced in [32, Theorem 4.41] and [33, Theorem 8], that links indecomposability to isomorphism types of local commutative rings and local Jordan algebras). These features are explored in [21, Section 5].

Finally we argue that automorphisms often agree, though we cannot guarantee that they always agree. By Theorem 4.1 we have that for $G \in \mathfrak{H}^2_{p,e}$,

$$\mathrm{Aut}(G) \hookrightarrow \Gamma\mathrm{L}_2(\mathbb{F}_{p^e}) \ltimes \mathbb{M}_{2e\times 2}(\mathbb{F}_p), \qquad \Gamma\mathrm{L}_2(\mathbb{F}_{p^e}) = \mathrm{Gal}(\mathbb{F}_{p^e}/\mathbb{F}_p) \ltimes \mathrm{GL}_2(\mathbb{F}_{p^e}).$$

Then in our proof of Proposition 5.1 we observed

$$C_{\mathrm{Aut}(G)}(G') := \mathrm{SL}_2(\mathbb{F}_{p^e}) \ltimes \mathbb{M}_{2e\times 2}(\mathbb{F}_p) \hookrightarrow \mathrm{Aut}(G).$$

This means the number of choices for $\mathrm{Aut}(G)$ can be bounded by counting the subgroups of

$$\Gamma\mathrm{L}_2(\mathbb{F}_{p^e})/\mathrm{SL}_2(\mathrm{F}_{p^e}) \cong \mathbb{Z}_e \ltimes \mathbb{Z}_{(p^e-1)/2}.$$

Furthermore, $C_{\mathrm{Aut}(G)}(G')$ is the kernel of the induced representation $\mathrm{Aut}(G) \to \mathrm{GL}_2(\mathbb{F}_p)$ given by the action on $G' \cong \mathbb{Z}_p^2$. In particular, $\mathrm{Aut}(G)/C_{\mathrm{Aut}(G)}(G')$ embeds into both the subgroups of $\mathbb{Z}_e \ltimes \mathbb{Z}_{(p^e-1)/2}$ and $\mathrm{GL}_2(\mathbb{F}_{p^e})$. This limits the order of $\mathrm{Aut}(G)/C_{\mathrm{Aut}(G)}(G')$ to divisors of

$$\ell = \gcd\left(p(p-1)(p+1), e(p^e-1)/2\right) \in O(p^3).$$

Whenever $e \nmid \ell$, then it follows that the ℓ-subgroups of $\mathbb{Z}_e \ltimes \mathbb{Z}_{(p^e-1)/2}$ lie in $\mathbb{Z}_{(p^e-1)/2}$ and are thus unique. So the total number of choices for $\mathrm{Aut}(G)$ as subgroups of $\Gamma\mathrm{L}_2(\mathbb{F}_{p^e})$ is at most the number of subgroups of a cyclic group of order ℓ, which is $O(\log \ell) \subseteq O(\log p)$. By Theorem 1.5 we know $\mathfrak{H}_{p,e}^{2e+2}$ have at least p^{e-3}/e distinct isomorphism types and only $O(\log p)$ choices for automorphisms. So equivalent automorphism groups, as subgroups of $\mathrm{Aut}(H)$, are common.

For example when $p=3$ and $e=7$ then $\ell=1$. So for each $G \in \mathfrak{H}_{3,7}^{2\cdot 7+2}$,

$$\mathrm{Aut}(G) = \mathrm{SL}_2(\mathbb{F}_{3^7}) \ltimes \mathbb{M}_{2e\times 2}(\mathbb{F}_p)$$

as a subgroup of $\mathrm{Aut}(H(\mathbb{F}_{3^7}))$. Meanwhile there are at least 19 isomorphism types in $\mathfrak{H}_{3,7}^{2\cdot 7+2}$.

6.2 Complete invariants

Pivoting to methods that do give information, Barnes and Wall [3] show that the subgroup lattice of a nilpotent group of class 2 and exponent p determines the isomorphism type of the group (which corrects an errant remark of the author). Yet, the groups in $\mathfrak{H}_{p,e}^{g}$ have maximum sized lattices with $|G|^{\Theta(\log|G|)}$ subgroups, chains of length $\log_p|G|$ and antichains of length $|G|^{\Theta(\log_p|G|)}$. Presently we have no tools to compare such large lattices.

Since standard isomorphism invariants are proving unhelpful we suggest one non-standard but effective tool. The idea of a polynomial invariant was suggested to the author by Rónyai [26]. The following version was defined in [7].

For groups $G \cong B(T_1,T_2)$ in $\mathfrak{H}_{p,e}^{2}$, we define the *generalized Pfaffian* as

$$\mathrm{Pf}(T_1,T_2) = \det(x_1T_1 + x_2T_2) \in \mathbb{F}_p[x_1,x_2]. \tag{6.1}$$

As $B(T_1,T_2) \cong B(I_2,C(a(t)))$, the generalized Pfaffian can in fact be computed efficiently as the homogenization of $a(t)$. The lex-least representative of the orbit of the generalized Pfaffian under the action by $\mathrm{GL}_2(\mathbb{F}_p)$ is a defining invariant as proved in [7]. (Note that that work deals with a far more general problem.)

Sketch of Proof of Theorem 1.7. The recognition of the class $\mathfrak{H}_p$ begins by using a suite of now standard algorithms to determine if a group G is a p-group of nilpotence class 2 and exponent p. That work depends on many algorithms, notably by Sims and Luks; see [29].

The next stage constructs the commutator map $[,]_+^G$ for G and solves a system of linear equations to compute the adjoint algebra $\mathrm{Adj}([,]_+^G)$. Using results of Rónyai, Ivanyos, Brooksbank-Luks, and the author we constructively recognize $\mathrm{Adj}([,]_+^G)$ together with its op-composition structure; see [21, 8]. Following Theorem 3.5 (and more general versions) this leads to a constructive recognition of the quotients of Heisenberg groups. The solution of the system of linear equations to compute $\mathrm{Adj}([,]_+^G)$ dominates the calculation and takes $O(e^{2\omega}\log^2 p)$ bit operations.

Having recognized quotients of Heisenberg groups we turn to their isomorphism problem. The first method of [21] builds on Remark 4.5 which shows how to set up a relatively small search problem with in the Galois group of $\mathbb{F}_{p^e}$. In each step of the search we solve a system of linear equations to decide if there is an isomorphism. This leads to an $O(e^{2\omega}\log^2 p)$-time isomorphism test.

For the faster variation we must solve the system of linear equations without a quadratic blow-up. For adjoints this is done in work of Brooksbank and the author. We avoid the later linear algebra problem that arises in the search question by using (6.1). We compute the lex-least representative under the action of $\mathrm{GL}_2(\mathbb{F}_p)$. This leads to a complexity of $O(p^3 + e^{\omega}\log p)$. See [7] for details and references. $\square$

Acknowledgment

Thanks to Laci Babai & Gene Luks who asked me about profiles and offered useful comments on this article, to Bill Kantor for extensive feedback on this article, and to the referees for catching blunders and improving the exposition.

References

[1] LÁSZLÓ BABAI: Graph isomorphism in quasipolynomial time [extended abstract]. In *Proc. 48th STOC*, pp. 684–697. ACM Press, 2016. [doi:10.1145/2897518.2897542, arXiv:1512.03547] 1, 2

[2] REINHOLD BAER: Groups with abelian central quotient group. *Trans. Amer. Math. Soc.*, 44(3):357–386, 1938. [doi:10.2307/1989886] 6, 11

[3] DONALD W. BARNES AND GORDON E. WALL: On normaliser preserving lattice isomorphisms between nilpotent groups. *J. Austral. Math. Soc.*, 4(4):454–469, 1964. [doi:10.1017/S1446788700025295] 22

[4] SIMON R. BLACKBURN, PETER M. NEUMANN, AND GEETHA VENKATARAMAN: *Enumeration of finite groups*. Volume 173 of *Cambridge Tracts in Math.* Cambridge Univ. Press, 2007. [doi:10.1017/CBO9780511542756] 6

[5] WIEB BOSMA, JOHN CANNON, AND CATHERINE PLAYOUST: The Magma algebra system I: The user language. *J. Symbolic Comput.*, 24(3–4):235–265, 1997. [doi:10.1006/jsco.1996.0125] 4

[6] H. R. BRAHANA: Metabelian groups and trilinear forms. *Duke Math. J.*, 1(2):185–197, 1935. [doi:10.1215/S0012-7094-35-00117-X] 6, 11

[7] PETER A. BROOKSBANK, JOSHUA MAGLIONE, AND JAMES B. WILSON: A fast isomorphism test for groups whose Lie algebra has genus 2. *J. Algebra*, 473:545–590, 2017. [doi:10.1016/j.jalgebra.2016.12.007] 3, 4, 17, 22

[8] PETER A. BROOKSBANK AND JAMES B. WILSON: Groups acting on tensor products. *J. Pure Appl. Algebra*, 218(3):405–416, 2014. [doi:10.1016/j.jpaa.2013.06.011, arXiv:1210.0827] 4, 13, 14, 22

[9] EVERETT C. DADE: Answer to a question of R. Brauer. *J. Algebra*, 1(1):1–4, 1964. [doi:10.1016/0021-8693(64)90002-X] 21

[10] HEIKO DIETRICH AND JAMES B. WILSON: Polynomial-time isomorphism testing of groups of most finite orders, 2018. [arXiv:1806.08872] 2

[11] HEIKO DIETRICH AND JAMES B. WILSON: Isomorphism testing of groups of cube-free order. *J. Algebra*, 545:174–197, 2020. [doi:10.1016/j.jalgebra.2019.02.008, arXiv:1810.03467] 2

[12] BETTINA EICK, CHARLES R. LEEDHAM-GREEN, AND EAMONN A. O'BRIEN: Constructing automorphism groups of p-groups. *Communications in Algebra*, 30(5):2271–2295, 2002. [doi:10.1081/AGB-120003468] 1, 2

[13] GEORGE GLAUBERMAN AND ŁUKASZ GRABOWSKI: Groups with identical k-profiles. *Theory of Computing*, 11(15):395–401, 2015. [doi:10.4086/toc.2015.v011a015] 2

[14] W. TIMOTHY GOWERS: Comment on Dick Lipton's blog entry: The Group Isomorphism Problem: A possible polymath problem? Blog entry started November 7, 2011. Comment cited: November 12, 2011. https://rjlipton.wordpress.com/2011/11/07/the-group-isomorphism-problem-a-possible-polymath-problem. 2

[15] ROBERT M. GURALNICK: On the number of generators of a finite group. *Archiv der Mathematik*, 53(6):521–523, 1989. [doi:10.1007/BF01199809] 2

[16] ZDENĚK HEDRLÍN AND ALEŠ PULTR: On full embeddings of categories of algebras. *Illinois J. Math.*, 10(3):392–406, 1966. [doi:10.1215/ijm/1256054991] 1

[17] THOMAS W. HUNGERFORD: *Algebra*. Springer, 1980. [doi:10.1007/978-1-4612-6101-8] 14, 15

[18] NATHAN JACOBSON: *Lectures in Abstract Algebra II. Linear Algebra*. Springer, 1953. [doi:10.1007/978-1-4684-7053-6] 4, 7, 10, 18

[19] CHARLES R. LEEDHAM-GREEN AND LEONARD H. SOICHER: Collection from the left and other strategies. *J. Symb. Comput.*, 9(5–6):665–675, 1990. [doi:10.1016/S0747-7171(08)80081-8] 3

[20] CHARLES R. LEEDHAM-GREEN AND LEONARD H. SOICHER: Symbolic collection using Deep Thought. *LMS J. Comput. Math.*, 1:9–24, 1998. [doi:10.1112/S1461157000000127] 3

[21] MARK L. LEWIS AND JAMES B. WILSON: Isomorphism in expanding families of indistinguishable groups. *Groups Complexity Cryptology*, 4(1):73–110, 2012. [doi:10.1515/gcc-2012-0008, arXiv:1010.5466] 3, 4, 10, 17, 19, 21, 22

[22] EUGENE M. LUKS: Computing in solvable matrix groups. In *Proc. 33rd FOCS*, pp. 111–120. IEEE Comp. Soc., 1992. [doi:10.1109/SFCS.1992.267813] 3

[23] GARY L. MILLER: Graph isomorphism, general remarks. *J. Comput. System Sci.*, 18(2):128–142, 1979. Preliminary version in STOC'77. [doi:10.1016/0022-0000(79)90043-6] 1

[24] ADRIANA NENCIU: Brauer t-tuples. *J. Algebra*, 322(2):410–428, 2009. [doi:10.1016/j.jalgebra.2009.04.019] 21

[25] DEREK J. S. ROBINSON: *A Course in the Theory of Groups*. Springer, 1996. [doi:10.1007/978-1-4419-8594-1] 4, 19, 21

[26] LAJOS RÓNYAI: Private communication, 2011. 22

[27] DAVID J. ROSENBAUM: Breaking the $n^{\log n}$ barrier for solvable-group isomorphism. In *Proc. 24th Ann. ACM-SIAM Symp. on Discrete Algorithms (SODA'13)*, pp. 1054–1073. ACM Press, 2013. [doi:10.1137/1.9781611973105.76, arXiv:1205.0642] 2

[28] ADA ROTTLAENDER: Nachweis der Existenz nicht-isomorpher Gruppen von gleicher Situation der Untergruppen. *Mathematische Zeitschrift*, 28(1):641–653, 1928. [doi:10.1007/BF01181188] 2

[29] ÁKOS SERESS: *Permutation Group Algorithms*. Cambridge Univ. Press, 2003. [doi:10.1017/CBO9780511546549] 3, 22

[30] HAROLD M. STARK: On the asymptotic density of the k-free integers. *Proc. Amer. Math. Soc.*, 17(5):1211–1214, 1966. Available on JSTOR. 2

[31] JOACHIM VON ZUR GATHEN AND JÜRGEN GERHARD: *Modern Computer Algebra*. Cambridge Univ. Press, 1999. [doi:10.1017/CBO9781139856065] 3

[32] JAMES B. WILSON: Decomposing p-groups via Jordan algebras. *J. Algebra*, 322(8):2642–2679, 2009. [doi:10.1016/j.jalgebra.2009.07.029, arXiv:0711.0201] 13, 21

[33] JAMES B. WILSON: Existence, algorithms, and asymptotics of direct product decompositions, I. *Groups Complexity Cryptology*, 4(1):33–72, 2012. [doi:10.1515/gcc-2012-0007] 21

AUTHOR

James B. Wilson
Associate professor
Department of Mathematics
Colorado State University
Fort Collins, Colorado, USA
James.Wilson@ColoState.Edu
https://wwww.math.colostate.edu/~jwilson/

ABOUT THE AUTHOR

JAMES B. WILSON graduated with his Ph. D. in Mathematics from the University of Oregon in 2008 where he studied with Bill Kantor (advisor), Gene Luks, and Charley Wright. Before this he spent nearly four years with the Intel Architecture Labs and still enjoys questions from industry. As a sophomore he asked an innocent question about group isomorphism to Professor F. Rudy Beyl, who kindly delayed a response and instead gave him a copy of a lovely paper by Ada Rottlaender to find the answer himself. This sparked the author's now decades-long obsession with isomorphism in algebra and its complexity.