LOCAL CONJUGACY IN $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$

SPUR FINAL PAPER, SUMMER 2016

HYUN JONG KIM
MENTOR: ATTICUS CHRISTENSEN
PROJECT SUGGESTED BY ANDREW SUTHERLAND

Abstract. Subgroups H_1 and H_2 of a group G are said to be locally conjugate if there is a bijection $f : H_1 \to H_2$ such that h and $f(h)$ are conjugate in G. We study local conjugacy among subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$, where p is an odd prime, building on Andrew Sutherland's categorizations of subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and local conjugacy among them. We obtain a classification of locally conjugate subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ in the kernel of the natural map $\varphi : \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. We further inspect local conjugacy among subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ using this classification.

Contents

1. Introduction

Sutherland was led to consider subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ which are locally conjugate but not necessarily conjugate as he was developing an algorithm to compute the images of Galois representation given by the Galois action on p-torsion points of elliptic curves. In his paper, Sutherland fully identifies nontrivially locally conjugate subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ (see Theorem 2), where p is an odd prime. Our hope is to understand local conjugacy in $\mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$ where $k \geq 2$ and also in the projective limit $\mathrm{GL}_2(\mathbb{Z}_p)$. In this paper, we work with the case when $k = 2$. We eventually eliminate some pairs of subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ that cannot be nontrivially locally conjugate (see Corollary 3, Remark 8). Sutherland's result with $k = 1$ and our observations with $k = 2$ and $p = 3$ lead us to believe that locally conjugate subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$ come in pairs up to conjugacy and that the subgroups are isomorphic.

2. Notation

Throughout this paper, p is an odd prime. ϵ is taken to be a nonsquare of $\mathbb{Z}/p\mathbb{Z}$.

For a group G and $g \in G$, we take g^G to be the conjugacy class of g in G. Furthermore, for $S \subseteq G$, $S^G = \bigcup_{s \in S} s^G$.

Definition 1. *Given 2×2 matrices M_1 and M_2, we say that they are* ***diagonally swapped*** *or that they are* ***diagonal swaps*** *if M_2 is obtained by switching the diagonal entries of M_1. Moreover, given groups of matrices H_1 and H_2, we say that they are diagonally swapped if the elements of H_2 are diagonal swaps of elements of H_1.*

2.1. Groups.

$\mathrm{GL}_2(R), \mathrm{SL}_2(R)$ and $\mathrm{PGL}_2(R)$ denote the general, special and projective linear groups of 2×2 matrices over a ring R. In particular, we define the following subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$:

Definition 2.

$$Z(p) = \left\{ \begin{pmatrix} w & 0 \\ 0 & w \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z}) \right\}$$

$$C_s(p) = \left\{ \begin{pmatrix} w & 0 \\ 0 & z \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z}) \right\}$$

$$C_{ns}(p) = \left\{ \begin{pmatrix} w & \epsilon y \\ y & w \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z}) \right\}$$

$$B(p) = \left\{ \begin{pmatrix} w & x \\ 0 & z \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z}) \right\},$$

are called the ***center***, ***Cartan-split subgroup***, ***Cartan-nonsplit subgroup*** *and* ***Borel subgroup*** *of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ respectively. For $H \leq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, let $N(H)$ denote the normalizer of H in $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. In particular,*

$$N(C_s(p)) = C_s(p) \cup \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} C_s(p)$$

$$N(C_{ns}(p)) = C_{ns}(p) \cup \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} C_{ns}(p).$$

3. Properties of Locally Conjugate Subgroups

In this section, we define locally conjugate subgroups and discuss some properties of local conjugacy.

Definition 3. *Let G be a group and $H_1, H_2 \leq G$. (G, H_1, H_2) is a **Gassman triple** if there is a bijection $f : H_1 \to H_2$ such that h and $f(h)$ are conjugate in G for all $h \in H_1$. We also say that H_1 and H_2 are **locally conjugate** in G. If H_1 and H_2 are conjugate in G, then they are also locally conjugate in G, in which case we say that they are **trivially locally conjugate**.*

Note that local conjugacy between subgroups H_1 and H_2 of G is determined not only by H_1 and H_2, but also by G. For example, we will see later that the kernel of the natural homomorphism $\varphi : \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ has subgroups that are nontrivially locally conjugate with respect to $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$. However, such subgroups are not locally conjugate with respect to $\ker \varphi$ because $\ker \varphi$ is abelian, in which case locally conjugate subgroups are always equal.

Proposition 1. *Let G be a group and $H_1, H_2 \leq G$. H_1 and H_2 are locally conjugate in G if and only if $|H_1 \cap C| = |H_2 \cap C|$ for all conjugacy classes C of G.*

Proof. Suppose H_1 and H_2 are locally conjugate in G via $f : H_1 \to H_2$. For every conjugacy class C of G, $f\mid_{H_1 \cap C}$ maps into $H_2 \cap C$. Likewise, $f^{-1}\mid_{H_2 \cap C}$ maps into $H_1 \cap C$ and is the inverse of $f\mid_{H_1 \cap C}$. Thus, $|H_1 \cap C| = |H_2 \cap C|$.

Conversely, suppose $|H_1 \cap C| = |H_2 \cap C|$ for every conjugacy class C of G. Choose some bijections $f_C : H_1 \cap C \to H_2 \cap C$ and define $f : H_1 \to H_2$ as $f(h) = f_{h^G}(h)$. f is a well defined bijection because the conjugacy classes of G partition G. Moreover, h and $f(h)$ are in the same conjugacy class for every $h \in H_1$, so H_1 and H_2 are locally conjugate. □

Proposition 2. *Let G be a group, $H_1, H_2 \leq G$ and $N \lhd G$. If H_1 and H_2 are locally conjugate in G, then $H_1 \cap N$ and $H_2 \cap N$ are locally conjugate in G.*

Proof. N is the disjoint union of some conjugacy classes of G. Let C be a conjugacy class of G. If $C \subseteq N$, then $|(H_i \cap N) \cap C| = |H_i \cap C|$ for $i = 1, 2$. Otherwise, $|(H_i \cap N) \cap C| = 0$. $H_1 \cap N$ and $H_2 \cap N$ are therefore locally conjugate in G by Proposition 1 □

Proposition 3. *Let G, G' be finite groups, $H_1, H_2 \leq G$ and $\varphi : G \to G'$ a surjective homomorphism. If H_1 and H_2 are locally conjugate in G, then $\varphi(H_1)$ and $\varphi(H_2)$ are locally conjugate in G'.*

Proof. Let C' be any conjugacy class of G' and let $U = \bigcup_{x \in C'} (\varphi^{-1}(x))^G$. We claim that $\varphi^{-1}(C') = U$. If $d \in \varphi^{-1}(C')$, then $\varphi(d) \in C'$, in which case $\varphi(d) \in (\varphi^{-1}(\varphi(d))^G \subseteq U$. Therefore, $\varphi^{-1}(C') \subseteq U$. Conversely, if $d \in (\varphi^{-1}(x))^G$ for some $x \in C'$, then $d = gyg^{-1}$ for some $g \in G$ and $y \in \varphi^{-1}(x)$. It follows that $\varphi(d) = \varphi(g)\varphi(y)\varphi(g)^{-1} = \varphi(g)x\varphi(g)^{-1}$, and so $d \in \varphi^{-1}(C')$. Hence, $U \subseteq \varphi^{-1}(C')$, as desired. In particular, $\varphi^{-1}(C')$ is the union of conjugacy classes of G.

$\ker \varphi$ is the union of conjugacy classes of G because it is normal in G. Moreover, since H_1 and H_2 are locally conjugate, $|H_1 \cap \ker \varphi| = |H_2 \cap \ker \varphi|$. Similarly, $|H_1 \cap \varphi^{-1}(C')| = |H_2 \cap \varphi^{-1}(C')|$. Note that $\varphi(H_i) \cap C' = \varphi(H_i \cap \varphi^{-1}(C'))$, so $|\varphi(H_i \cap C')| = |H_i \cap \varphi^{-1}(C')| / |H_i \cap \ker \varphi|$ for $i = 1, 2$. Thus, $|\varphi(H_1) \cap C'| = |\varphi(H_2) \cap C'|$. □

Lemma 1. *Let G be a finite group and $H_1, H_2 \leq G$ with H_1 and H_2 locally conjugate in G. If H_1 is cyclic, then so is H_2 and H_1 and H_2 are conjugate.*

Proof. Say that h_1 generates H_1. There is some $h_2 \in H_2$ that is conjugate to h_1. h_1 and h_2 have the same order, which is $|H_1| = |H_2|$, so h_2 generates H_2. □

4. Subgroups of the Kernel of the Homomorphism $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$

For the rest of the paper, φ denotes the natural homomorphism $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ unless stated otherwise. Elements of $\ker\varphi$ are of the form $I + Ap$, where we may identify A as an element of $\mathrm{Mat}_2(\mathbb{Z}/p\mathbb{Z})$. $\ker\varphi \simeq (\mathbb{Z}/p\mathbb{Z})^4$ because $(I+A_1p)(I+A_2p) = I + (A_1 + A_2)p$. Therefore, $\ker\varphi$ is a $\mathbb{Z}/p\mathbb{Z}$ vector space of dimension 4.

By Propositions 2 and 3, $H_1 \cap \ker\varphi$ and $H_2 \cap \ker\varphi$ are locally conjugate in $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ and $\varphi(H_1)$ and $\varphi(H_2)$ are locally conjugate in $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ if H_1 and H_2 are locally conjugate in $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$. Sutherland fully identifies local conjugacy in $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ (see Theorem 2). In this section, we determine local conjugacy between subgroups of $\ker\varphi$ with respect to $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ up to conjugacy. To categorize the subgroups of $\ker\varphi$ up to conjugacy, we conjugate the subgroups to pick some generators to be of desired form. To determine local conjugacy among the subgroups, we apply Lemma 3 below.

Lemma 2. *Fix $I + Ap \in \ker\varphi$ and let $g \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. The conjugation $g(I + Ap)g^{-1}$ depends only on $\varphi(g)$ or equivalently, on g modulo p.*

Proof. For any $B \in \mathrm{Mat}_2(\mathbb{Z}/p\mathbb{Z})$, $(g - Bp)^{-1} = g^{-1} - g^{-1}Bg^{-1}$. Therefore,

$$\begin{aligned}(g + Bp)(I + Ap)(g - Bp)^{-1} &= (g + Bp)(I + Ap)(g^{-1} - g^{-1}Bg^{-1}p)\\ &= I + (-gIg^{-1}Bg^{-1} + gAg^{-1} + BIg^{-1})p\\ &= I + gAg^{-1}p.\end{aligned}$$

□

Remark 1. *The conjugacy classes of $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ in $\ker\varphi$ corresponds to the orbits of $\mathrm{Mat}_2(\mathbb{Z}/p\mathbb{Z})$ under conjugation by elements of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$: the conjugacy class of $I + Ap$ corresponds to the orbit of A.*

4.1. Orbits of $\mathrm{Mat}_2(\mathbb{Z}/p\mathbb{Z})$ under conjugation by elements of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Sutherland gives representatives for all the distinct conjugacy classes of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, see [3, Table 3.1]. We extend his table with Table 4.1 to include representatives of zero determinant.

Table 1. Representatives of Orbits of $\mathrm{Mat}_2(\mathbb{Z}/p\mathbb{Z})$ Under Conjugation by $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$

Representative	det	trace	χ
$\begin{pmatrix} w & 0 \\ 0 & w \end{pmatrix}$ $0 \leq w < p$	w^2	$2w$	0
$\begin{pmatrix} w & 1 \\ 0 & w \end{pmatrix}$ $0 \leq w < p$	w^2	$2w$	0
$\begin{pmatrix} w & 0 \\ 0 & z \end{pmatrix}$ $0 \leq w < z < p$	wz	$w + z$	1
$\begin{pmatrix} w & \epsilon y \\ y & w \end{pmatrix}$ $0 < y \leq p - 1/2$	$w^2 - \epsilon y^2$	$2w$	-1

We show that the representatives in Table 4.1 represent distinct conjugacy classes. Define χ as the quadratic character $\chi(g) = \left(\frac{\operatorname{trace}(g)^2-4\det(g)}{p}\right)$ for $g \in \operatorname{Mat}_2(\mathbb{Z}/p\mathbb{Z})$. It is $1, 0, -1$ when g has exactly $2, 1, 0$ eigenvalues in $\mathbb{Z}/p\mathbb{Z}$ respectively. Since the trace and determinant of a matrix are fixed under conjugation, χ is also fixed under conjugation. Matrices of the first and second types, matrices of the third type and matrices of the fourth type are therefore not conjugate to one another. Furthermore, matrices of the first type are not conjugate to those of the second type because the former are conjugate only to themselves. Comparing the trace and determinant among matrices of the same type shows that distinct matrices in the table are not conjugate.

We also explain why the representatives exhaust all of the orbits. We start with $g \in \operatorname{Mat}_2(\mathbb{Z}/p\mathbb{Z})$. If it diagonalizes over $\mathbb{Z}/p\mathbb{Z}$, then g is conjugate to a matrix of the first or third type. If g diagonalizes over $\mathbb{F}_p$, then g is conjugate over $\mathbb{F}_p$ to a matrix of the form $\begin{pmatrix} w+\sqrt{\epsilon}y & 0 \\ 0 & w-\sqrt{\epsilon}y \end{pmatrix}$, which is conjugate to $\begin{pmatrix} w & \epsilon y \\ y & w \end{pmatrix}$ via $\begin{pmatrix} -\sqrt{\epsilon} & -\epsilon \\ -\sqrt{\epsilon} & \epsilon \end{pmatrix}^{-1}$. One can check that g and $\begin{pmatrix} w & \epsilon y \\ y & w \end{pmatrix}$ are conjugate over $\mathbb{Z}/p\mathbb{Z}$. If g does not diagonalize, then it has a double eigenvalue, in which case it is conjugate to a matrix of the second type.

Remark 2. *The orbit of an element $g \in \operatorname{Mat}_2(\mathbb{Z}/p\mathbb{Z})$ that is not of the form $\begin{pmatrix} w & 0 \\ 0 & w \end{pmatrix}$ is completely determined by the trace and determinant of g.*

4.2. Subgroups in a Subgroup of $\ker\varphi$ Up to Conjugacy by $\operatorname{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$.

Definition 4. *Let $k = I + Ap \in \ker\varphi$. We call A the **p-part** of k and denote A by $p(k)$.*

Define $T = \{k \in \ker\varphi \mid \operatorname{trace}(p(k)) = 0\}$. T is generated by $I + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} p$, $I + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} p$ and $I + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} p$, so T has dimension 3. Moreover, T is normal in $\operatorname{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$. We determine local conjugacy between subgroups of T with respect to $\operatorname{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$.

Definition 5. *Let $Z = \left\{ I + \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} p \mid a \in \mathbb{Z}/p\mathbb{Z} \right\}$ and $H \leq \ker\varphi$. For $t, d \in \mathbb{Z}/p\mathbb{Z}$, denote $\chi(H, t, d)$ as the number of elements $h \in H \setminus Z$ such that $\operatorname{trace}(p(h)) = t$ and $\det(p(h)) = d$.*

Lemma 3. *Let $H_1, H_2 \leq \ker\varphi$. H_1 and H_2 are locally conjugate in $\operatorname{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ if and only if $H_1 \cap Z = H_2 \cap Z$ and $\chi(H_1, t, d) = \chi(H_2, t, d)$ for all $t, d \in \mathbb{Z}/p\mathbb{Z}$.*

Proof. This is because the orbit of an element of $\operatorname{Mat}_2(\mathbb{Z}/p\mathbb{Z})$ which is not of the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ is determined by the element's trace and determinant and matrices of the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ are in their own orbit. □

Lemma 4. *Two locally conjugate subgroups of $\operatorname{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ in $\ker\varphi$ must have equal dimension.*

Proof. Any two locally conjugate subgroups are bijective. □

T has exactly one subgroup of dimension 0 and exactly one subgroup of dimension 3: they are $\langle I\rangle$ and T, respectively. We categorize the subgroups of dimensions 1 and 2 of T below.

Proposition 4. *The subgroups of T of dimension 1 are conjugate in $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ to one of the following:*

(1) $\left\langle I+\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}p\right\rangle$

(2) $\left\langle I+\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}p\right\rangle$

(3) $\left\langle I+\begin{pmatrix}0 & \epsilon\\ 1 & 0\end{pmatrix}p\right\rangle$

No two distinct subgroups among these are locally conjugate.

Proof. A cyclic subgroup is determined, up to conjugacy, by a generator's conjugacy class. We choose a generator so that its p-part is a representative listed in Table 4.1. By Lemma 1, No two of these subgroups are locally conjugate because they are not conjugate. $\square$

Proposition 5. *The subgroups of T of dimension 2 are conjugate in $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ to one of the following:*

(1) $\left\langle I+\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}p, I+\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}p\right\rangle$

(2) $\left\langle I+\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}p, I+\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}p\right\rangle$

(3) $\left\langle I+\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}p, I+\begin{pmatrix}0 & \epsilon\\ 1 & 0\end{pmatrix}p\right\rangle$

Proof. If $H \leq T$ has dimension 2, then we now show that we can replace H with a conjugate so that H has $I+\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}p$. Suppose first that $\det(p(h)) = -a^2$ where $a \neq 0$ for some $h \in H$ that is not I. h is conjugate to $h' = I+\begin{pmatrix}a & 0\\ 0 & -a\end{pmatrix}p$, so we can replace H with a conjugate so that h' is in H. Since a is nonzero, some power of h' is $I+\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}p$.

Now assume that $\det(p(h)) \neq -a^2$ for any nonidentity $h \in H$ and nonzero $a \in \mathbb{Z}/p\mathbb{Z}$. Suppose that $\det(p(h)) = 0$ for some nonidentity $h \in H$. h is conjugate to $u_1 = I+\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}p$, so replace H with a conjugate containing u_1. Choose $u_2 \in H$ so that (u_1, u_2) is a basis of H and $u_2 = I+\begin{pmatrix}a & 0\\ c & -a\end{pmatrix}p$ for some $a, c \in \mathbb{Z}/p\mathbb{Z}$. a must be 0 because $u_2 \neq I$ and $\det(p(u_2)) = -a^2$. Thus, c is nonzero, in which case $H = \left\langle I+\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}p, I+\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}p\right\rangle$. However, $I+\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}p$, whose p-part has determinant -1, is in H, which is a contradiction. Hence, this case does not occur.

We now assume that $\det(p(h)) \neq 0, -a^2$ for every $h \in H$ and nonzero a. $-\det(p(h))/\epsilon$ is then a nonzero square for any nonidentity $h \in H$. h is thus conjugate to $v_1 = I+\begin{pmatrix}0 & \epsilon y\\ y & 0\end{pmatrix}p$, where $y \in \mathbb{Z}/p\mathbb{Z}$ is nonzero. We choose $v_2 \in H$ so that (v_1, v_2) is a basis of H and v_2 is of the form $I + \begin{pmatrix} a & 0 \\ c & -a \end{pmatrix} p$. However, $\det(p(v_2)) = -a^2$, which is a contradiction. Hence, this case does not occur either, and so H must contain $w_1 = I + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} p$ up to conjugation.

Choose $w_2 \in H$ so that (w_1, w_2) is a basis of H and w_2 is of the form $I + \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} p$. If $c = 0$, then $b \neq 0$, in which case H is subgroup 1. Similarly, if $b = 0$, then $c \neq 0$, in which case H is conjugate to subgroup 1 via $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Otherwise, $bc \neq 0$. If bc is a square, then H is conjugate to subgroup 2 via $\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{b/c} \end{pmatrix}$. If bc is a nonsquare, then H is conjugate to subgroup 3 via $\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{b/(c\epsilon)} \end{pmatrix}$. Subgroups of T of dimension 2 are therefore conjugate to one of the three listed.

We now show that the three subgroups are not locally conjugate to one another. Define $Z \subseteq \ker\varphi$ as in Definition 5. Z shares only I with each of subgroups 1, 2 and 3. Elements of subgroups 1, 2 and 3 have p-parts of form $x_1 \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + y_1 \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $x_2 \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + y_2 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $x_3 \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + y_3 \begin{pmatrix} 0 & \epsilon \\ 1 & 0 \end{pmatrix}$, which all have trace 0 and have determinants $-x_1^2, -x_2^2 - y_2^2$ and $-x_3^2 - \epsilon y_3^2$ respectively. Letting x_2 be so that $x_2^2 + 1$ is nonsquare in $\mathbb{Z}/p\mathbb{Z}$ and letting $y_2 = 1$ shows that subgroups 1 and 2 are not locally conjugate by Lemma 3. Letting $x_3 = 0$ and $y_3 = 1$ shows that subgroups 1 and 3 are not locally conjugate as well. Moreover, $-x_2^2 - y_2^2 = 0$ has nonzero solutions exactly when -1 is a square in $\mathbb{Z}/p\mathbb{Z}$, which is exactly when $-x_3^2 - \epsilon y_3^2 = 0$ does not have nonzero solutions. Subgroups 2 and 3 are therefore not locally conjugate. □

4.3. **Subgroups of** $\ker\varphi$ **Up to Conjugacy by** $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$**.**

Subgroups H of $\ker\varphi$ of dimension at least 2 have nontrivial intersection with T since $\dim(\ker\varphi) = 4$ and $\dim(T) = 3$. In particular, if $\dim(H) = 2$, then $\dim(H \cap T) \geq 1$ and if $\dim(H) = 3$, then $\dim(H \cap T) \geq 2$. We categorize the subgroups of $\ker\varphi$ that are not subgroups of T.

Proposition 6. *The subgroups of* $\ker\varphi$ *of dimension* 1 *that are not subgroups of* T *are conjugate in* $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ *to one of the following:*

(1) $\left\langle I + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} p \right\rangle$

(2) $\left\langle I + \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} p \right\rangle$

(3) $\left\langle I + \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} p \right\rangle$, *where* $d \in \mathbb{Z}/p\mathbb{Z}$ *is not* ± 1

(4) $\left\langle I + \begin{pmatrix} 1 & \epsilon c \\ c & 1 \end{pmatrix} p \right\rangle$.

No two distinct subgroups among these are locally conjugate.

Proof. The proof is similar to that of Proposition 4. □

Proposition 7. *The subgroups of* $\ker\varphi$ *of dimension* 2 *that are not subgroups of* T *are conjugate in* $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ *to one of the following:*

(1) $\left\langle I+\begin{pmatrix}0&1\\0&0\end{pmatrix}p, I+\begin{pmatrix}0&0\\1&1\end{pmatrix}p\right\rangle$

(2) $\left\langle I+\begin{pmatrix}0&1\\0&0\end{pmatrix}p, I+\begin{pmatrix}0&0\\0&1\end{pmatrix}p\right\rangle$

(3) $\left\langle I+\begin{pmatrix}0&1\\0&0\end{pmatrix}p, I+\begin{pmatrix}1&0\\0&d\end{pmatrix}p\right\rangle$, *where* $d\in\mathbb{Z}/p\mathbb{Z}$ *is not* -1

(4) $\left\langle I+\begin{pmatrix}1&0\\0&-1\end{pmatrix}p, I+\begin{pmatrix}0&1\\c&1\end{pmatrix}p\right\rangle$, *where* $c\in\mathbb{Z}/p\mathbb{Z}$

(5) $\left\langle I+\begin{pmatrix}1&0\\0&-1\end{pmatrix}p, I+\begin{pmatrix}0&0\\0&1\end{pmatrix}p\right\rangle$

(6) $\left\langle I+\begin{pmatrix}0&\epsilon\\1&0\end{pmatrix}p, I+\begin{pmatrix}1+a&-\epsilon b\\b&1-a\end{pmatrix}p\right\rangle$, *where* $a,b\in\mathbb{Z}/p\mathbb{Z}$.

Subgroup 2 and the type 3 subgroup where $d=0$ *are nontrivially locally conjugate. Two type 3 subgroups are nontrivially locally conjugate if their* d *values are multiplicative inverses. If* H_1 *and* H_2 *are type 6 subgroups where* $(a,b)=(a_1,b_1)$ *and* (a_2,b_2) *respectively, then* H_1 *and* H_2 *are conjugate if* $a_1^2-\epsilon b_1^2=a_2^2-\epsilon b_2^2$. *All other pairs of distinct subgroups above are not locally conjugate.*

Proof. Suppose $H\leq\ker\varphi$ has dimension 2 and is not a subgroup of T. $H\cap T$ has dimension 1. Replace H with a conjugate so that $H\cap T$ is one of the subgroups of T as listed in Section 4.2.

Suppose $H\cap T=\left\langle I+\begin{pmatrix}0&1\\0&0\end{pmatrix}p\right\rangle$. Choose a second basis element of H to be of the form $I+\begin{pmatrix}a&0\\c&d\end{pmatrix}p$. Note that $a+d\neq 0$ because $H\cap T$ has dimension 1. If $a=0$, then we scale this basis element so that $d=1$. In this case, if $c=0$, then H is subgroup 2. Otherwise, H is conjugate to subgroup 1 via $\begin{pmatrix}c&0\\0&1\end{pmatrix}$. If $a\neq 0$, then we may let $a=1$ by scaling the basis element. Since $a+d\neq 0$, $d\neq -1$. If $c=0$, then H is a type 3 subgroup. Otherwise, H is conjugate to subgroup 2 via $\begin{pmatrix}\frac{c}{d+1}&-\frac{1}{d+1}\\0&1\end{pmatrix}$.

Suppose $H\cap T=\left\langle I+\begin{pmatrix}1&0\\0&-1\end{pmatrix}p\right\rangle$. Choose a second basis element of H to be of the form $I+\begin{pmatrix}0&b\\c&d\end{pmatrix}p$. d must be nonzero, so we can let $d=1$ after scaling the second basis element. If $b=c=0$, then H is subgroup 5. If $b\neq 0$, then H is conjugate to a type 4 subgroup via $\begin{pmatrix}1&0\\0&b\end{pmatrix}$. Otherwise, $b=0$ and $c\neq 0$, but conjugating H via $\begin{pmatrix}0&1\\1&0\end{pmatrix}$ reduces this case to the case where $b\neq 0$.

Suppose $H \cap T = \left\langle I + \begin{pmatrix} 0 & \epsilon \\ 1 & 0 \end{pmatrix} p \right\rangle$. Choose a second basis element of $H \cap T$ to have trace 2. That is, the basis element is of the form $I + \begin{pmatrix} 1+a & b' \\ c' & 1-a \end{pmatrix} p$. Note that

$$\left(I + \begin{pmatrix} 1+a & b' \\ c' & 1-a \end{pmatrix} p\right) \left(I + \begin{pmatrix} 0 & \epsilon \\ 1 & 0 \end{pmatrix} p\right)^{-(b'+\epsilon c')/(2\epsilon)} = I + \begin{pmatrix} 1+a & -b\epsilon \\ b & 1-a \end{pmatrix} p,$$

where $b = c' - (b' + \epsilon c')/(2\epsilon)$. We may therefore replace the second basis element by this product, so H is a type 6 subgroup.

We determine conjugacy and local conjugacy among the subgroups. If H_1 and H_2 are locally conjugate and among the subgroups listed, then their intersections with T must be locally conjugate and thus equal because T is normal in $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$. For any of the listed subgroups H, let A and B be its first and second generators respectively, i.e. $\mathrm{trace}(A) = 0$ and $\mathrm{trace}(B) \neq 0$. The p-parts of the elements H are of the form $xA + yB$ where $x, y \in \mathbb{Z}/p\mathbb{Z}$. Since A has trace 0, the trace of $xA + yB$ depends only on y. Moreover, $\chi(H, rt, r^2 d) = \chi(H, t, d)$ for all $t, d \in \mathbb{Z}/p\mathbb{Z}$. Given that $H_1 \cap T = H_2 \cap T$, local conjugacy between H_1 and H_2 thus depends only on their intersections with Z, as defined in Definition 5, and on $\chi(H_i, 1, d)$ for $d \in \mathbb{Z}/p\mathbb{Z}$. We will refer to the determinant and trace of the p-parts of elements of $\ker \varphi$ simply as the element's determinant and trace in the rest of this proof.

The p-parts of all subgroup 2 elements have zero determinant, so subgroup 2 is not locally conjugate to subgroup 1 or type 3 subgroups where $d \neq 0$. Let H_1 and H_2 be subgroup 2 and the type 3 subgroup where $d = 0$, respectively. H_1 and H_2 are locally conjugate because $I + \begin{pmatrix} 0 & x \\ 0 & y \end{pmatrix} p$ is conjugate to $I + \begin{pmatrix} y & x \\ 0 & 0 \end{pmatrix} p$. Suppose, for contradiction, that H_1 and H_2 are conjugate. Any conjugation from H_1 to H_2 preserves $H_1 \cap T$, meaning that the conjugation sends $I + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} p$ to $I + \begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix} p$ for some nonzero $r \in \mathbb{Z}/p\mathbb{Z}$. Any such conjugation is done via an upper triangular matrix of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, but such a conjugation preserves H_1. Hence, subgroup 2 and the type 3 subgroup where $d = 0$ are nontrivially locally conjugate.

A trace 1 element of subgroup 1 can have any determinant, whereas a trace 1 element of a type 3 subgroup can only have determinant of the same quadratic character as d. Subgroup 1 is therefore not locally conjugate to subgroup 3.

The type 3 subgroup where $d = 0$ is not locally conjugate to other type 3 subgroups because the latter has only elements whose p-parts have zero determinant. Now suppose H_1 and H_2 are type 3 subgroups where $d = d_1, d_2$ respectively and $d_1, d_2 \neq 0$. The trace 1 elements have determinant $d_i/(d_i+1)^2$ where $i = 1, 2$. Thus, H_1 and H_2 are locally conjugate exactly when $d_1/(d_1+1)^2 = d_2/(d_2+1)^2$, which is when $d_1 = d_2$ or $d_1 d_2 = 1$. Just as before, H_1 and H_2 are not locally conjugate if $d_1 \neq d_2$ because any conjugation from H_1 to H_2 would have to be by an upper triangular matrix of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, but such a conjugation preserves H_1.

The determinants of the trace 1 elements of a type 4 subgroup are of the form $-x^2 + x - c$. Those of subgroup 5 are of the form $-x^2 + x$. $-x^2 + x - c = -(x - 1/2)^2 - c + 1/4$ takes the value $-c + 1/4$ exactly once and all other values exactly two or zero times. On the other hand, $-x^2 + x$ takes the value $1/4$ exactly once and all other values exactly two or zero times. Thus, the type 4 subgroup where $c \neq 0$ is not locally conjugate to subgroup 5. Furthermore, the type 4 subgroup where $c = 0$ is not locally conjugate to subgroup 5 because the two subgroups have different intersection with Z.

Say that H_1 and H_2 are two type 6 subgroups with $(a, b) = (a_1, b_1)$ and (a_2, b_2) respectively, where $a_1^2 - \epsilon b_1^2 = a_2^2 - \epsilon b_2^2$. Conjugating a type 6 subgroup via $\begin{pmatrix} -\sqrt{\epsilon} & -\epsilon \\ -\sqrt{\epsilon} & \epsilon \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_{p^2})$ yields the group $\left\langle I + \begin{pmatrix} \sqrt{\epsilon} & 0 \\ 0 & -\sqrt{\epsilon} \end{pmatrix} p, I + \begin{pmatrix} 1 & a + b\sqrt{\epsilon} \\ a - b\sqrt{\epsilon} & 1 \end{pmatrix} p \right\rangle$. Conjugating this group by $\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix}$ further yields $\left\langle I + \begin{pmatrix} \sqrt{\epsilon} & 0 \\ 0 & -\sqrt{\epsilon} \end{pmatrix} p, I + \begin{pmatrix} 1 & (a + b\sqrt{\epsilon})\frac{\alpha}{\delta} \\ (a - b\sqrt{\epsilon})\frac{\delta}{\alpha} & 1 \end{pmatrix} p \right\rangle$. H_1 is thus conjugate to H_2 via $\begin{pmatrix} -\sqrt{\epsilon} & -\epsilon \\ -\sqrt{\epsilon} & \epsilon \end{pmatrix}^{-1} \begin{pmatrix} a_2 + b_2\sqrt{\epsilon} & 0 \\ 0 & a_1 + b_1\sqrt{\epsilon} \end{pmatrix} \begin{pmatrix} -\sqrt{\epsilon} & -\epsilon \\ -\sqrt{\epsilon} & \epsilon \end{pmatrix}$, which is a scalar multiple of $\begin{pmatrix} (a_1 + a_2)^2 - (b_1 + b_2)^2\epsilon & 2(a_2b_1 - a_1b_2) \\ \frac{2(a_2b_1 - a_1b_2)}{\epsilon} & (a_1 + a_2)^2 - (b_1 + b_2)^2\epsilon \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Thus, H_1 and H_2 are conjugate in $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$.

The trace 1 elements of a type 6 subgroup have determinants of the form $\frac{1 - a^2 + \epsilon b^2}{4} - \epsilon x^2$. This expression takes the value $\frac{1 - a^2 + \epsilon b^2}{4}$ exactly once, when $x = 0$, and all values exactly two or zero times. Therefore, two type 6 subgroups with distinct $a^2 - \epsilon b^2$ values are not locally conjugate by Lemma 3. □

Proposition 8. *The subgroups of* $\ker \varphi$ *of dimension* 3*, that are not subgroups of* T *are conjugate in* $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ *to one of the following:*

(1) $\left\langle I + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} p, I + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} p, I + \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} p \right\rangle$

(2) $\left\langle I + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} p, I + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} p, I + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} p \right\rangle$

(3) $\left\langle I + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} p, I + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} p, I + \begin{pmatrix} 0 & 0 \\ c & 1 \end{pmatrix} p \right\rangle$*, where* $c \in \mathbb{Z}/p\mathbb{Z}$ *with* $0 \leq c \leq \frac{p-1}{2}$

(4) $\left\langle I + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} p, I + \begin{pmatrix} 0 & \epsilon \\ 1 & 0 \end{pmatrix} p, I + \begin{pmatrix} 0 & 0 \\ c & 1 \end{pmatrix} p \right\rangle$*, where* $c \in \mathbb{Z}/p\mathbb{Z}$ *with* $0 \leq c \leq \frac{p-1}{2}$*.*

No two distinct subgroups among these are locally conjugate.

Proof. Suppose $H \leq \ker \varphi$ has dimension 3 and is not a subgroup of T. $H \cap T$ has dimension 2. Replace H with a conjugate so that $H \cap T$ is one of the subgroups of T as listed in Section 4.2. In any of these cases, a third basis element of H can be chosen to be of the form $I + \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix} p$, where $d \neq 0$. In particular, we may choose d to be 1 by scaling.

Suppose $H \cap T = \left\langle I + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} p, I + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} p \right\rangle$. Note that the upper triangular elements, in particular diagonal ones, normalize $H \cap T$. If $c \neq 0$, then H is conjugate to subgroup 1 via $\begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix}$. If $c = 0$, then H is subgroup 2.

Suppose $H \cap T = \left\langle I + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} p, I + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} p \right\rangle$. If $0 \leq c \leq \frac{p-1}{2}$, then H is a type 3 subgroup. Otherwise, H is conjugate to $\left\langle H \cap T, I + \begin{pmatrix} 0 & 0 \\ -c & 1 \end{pmatrix} p \right\rangle$, which is conjugate to a type 3 subgroup via $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. Similarly, if $H \cap T = \left\langle I + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} p, I + \begin{pmatrix} 0 & \epsilon \\ 1 & 0 \end{pmatrix} p \right\rangle$, then H is either a type 4 subgroup or is conjugate to one via $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

We now show that no two distinct subgroups among the ones listed are locally conjugate. Again, the intersections with T of two locally conjugate subgroups are locally conjugate. Subgroups 1 and 2 are not locally conjugate because subgroup 2 contains Z as defined in Definition 5 whereas subgroup 1 does not. Similarly, a type 3 or 4 subgroup where $c = 0$ is not locally conjugate to another of the same type where $c \neq 0$.

Elements of a subgroup H of type 3 where $c = c_0 \neq 0$ intersect Z only at I. Elements of such a subgroup are of the form

$$h = I + \left(x \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + y \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + z \begin{pmatrix} 0 & 0 \\ c_0 & 1 \end{pmatrix} \right) p.$$

The trace of h is determined by z, so local conjugacy of H is determined by $\chi(H, 1, d)$ for $d \in \mathbb{Z}/p\mathbb{Z}$, i.e. when we fix z to be 1. In this case, $\det(p(h)) = -x^2 + x - y^2 - c_0 y$, so we want to count the number of solutions to $d = -x^2 + x - y^2 - c_0 y$ for each $d \in \mathbb{Z}/p\mathbb{Z}$. This is equal to the number of solutions to $x'^2 + y'^2 = -d + (1 + c_0^2)/4$, where $x', y' \in \mathbb{Z}/p\mathbb{Z}$ are parametrized as $x - 1/2$ and $y + c/2$, respectively.

The number of solutions to $x'^2 + y'^2 = 0$ is 1 if $p \equiv 3 \pmod 4$ and $2p - 1$ if $p \equiv 1 \pmod 4$ because -1 is a nonsquare in the former case and a square in the latter. Now consider the number of solutions to $x'^2 + y'^2 = K$ for nonzero K. x'^2 and y'^2 each take $(p+1)/2$ distinct values including 0 and so x'^2 and $K - y'^2$ each take $(p+1)/2$ distinct values of x' and y'. By the Pigeonhole Principle, $x'^2 + y'^2 = K$ for at least one pair (x', y'). In particular, $(\pm x', \pm y')$ give us at least two distinct solutions to $x'^2 + y'^2 = K$, whether or not x' or $y' = 0$. Furthermore, if $p \equiv 1 \pmod 4$, then the equation $x'^2 + y'^2 = K$ is equivalent to $(x' + iy')(x' - iy') = K$, where $i^2 = -1$. The number of solutions here is therefore $p - 1$.

The number of solutions to $\det(p(h)) = (1 + c_0^2)/4$ is thus 1 if $p \equiv 3 \pmod 4$ and $2p - 1$ if $p \equiv 1 \pmod 4$. Let H' be another type 3 subgroup with $c = c_1 \neq c_0$. Note that $c_0^2 \neq c_1^2$. The number of solutions to $\det(p(h')) = (1 + c_0^2)/4$, where $h' \in H'$, is at least 2 and exactly $p - 1$ if $p \equiv 1 \pmod 4$. H and H' are thus not locally conjugate. Similarly, two distinct type 4 subgroups are not locally conjugate as well. □

5. Locally Conjugate Subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$

5.1. **Subgroups of** $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Remark 3. *The elements of $C_{ns}(p)$ depend of the choice of ϵ, but two choices for $C_{ns}(p)$ are conjugate even with different choices of ϵ.*

Remark 4. *$C_s(p)$ and $C_{ns}(p)$ are isomorphic to $((\mathbb{Z}/p\mathbb{Z})^\times)^2 \simeq (\mathbb{Z}/(p-1)\mathbb{Z})^2$ and $\mathbb{F}_p^\times \simeq \mathbb{Z}/(p^2-1)\mathbb{Z}$ respectively.*

Dickson [1] gives a classification of subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ up to conjugacy in terms of their images in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$.

Theorem 1. *Let $H \leq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ with image $H' \leq \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$. Up to conjugacy, one of the following holds:*

(1) H contains an element of order p.

(a) $H \leq B(p)$
(b) $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \leq H$

(2) H does not contain an element of order p.
(a) H' is cyclic and $H \leq C_s(p)$ or $C_{ns}(p)$.
(b) H' is dihedral and $H \leq N(C_s(p))$ or $N(C_{ns})(p)$ but $H \not\leq C_s(p), C_{ns}(p)$
(c) $H' \simeq A_4, S_4$ or A_5 and $H \not\leq N(C_s(p)), N(C_{ns})(p)$.

Furthermore, Sutherland [3, Section 3, Corollary 3.30] uses Dickson's classification to fully identify nontrivially locally conjugate subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Theorem 2. *Let $H_1, H_2 \leq C_s(p)$ be conjugate but unequal, i.e. they are diagonally swapped (see Lemma 5). $\left\langle H_1, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$ and $\left\langle H_2, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$ are nontrivially locally conjugate. Up to conjugation, these subgroups are the only nontrivially locally conjugate subgroups of* $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Lemma 5. *Let $H_1, H_2 \leq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ be conjugate.*

(1) If $H_1, H_2 \leq C_s(p)$, then $H_1 = H_2$ or H_2 is obtained by swapping the diagonal entries of elements of H_1.

(2) Suppose $H_1, H_2 \leq N(C_s(p))$. Some conjugation from H_1 to H_2 takes diagonal elements to diagonal elements and nondiagonal elements to nondiagonal elements if and only if H_1 and H_2 are conjugate via an element of $N(C_s(p))$.

Proof. (1) Suppose $H_1 \neq H_2$. There is some $\begin{pmatrix} w & 0 \\ 0 & z \end{pmatrix}$ in H_1 but not in H_2. Since H_1 and H_2 are conjugate, $\begin{pmatrix} z & 0 \\ 0 & w \end{pmatrix} \in H_2$. The conjugation must be via a matrix of the form $\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$, which switches the diagonal entries of all elements of H_1.

(2) If H_1 and H_2 are conjugate via an element of $N(C_s(p))$, then the conjugation takes diagonal elements to diagonal elements and nondiagonal elements to nondiagonal elements. Conversely, suppose that there is some conjugation from H_1 to H_2 that takes diagonal elements to diagonal elements and nondiagonal elements to nondiagonal elements. If $H_1, H_2 \leq C_s(p)$, then we are done by the previous part. Otherwise, since some conjugation from H_1 to H_2 takes diagonal elements to diagonal ones, $H_1 \cap C_s(p)$ and $H_2 \cap C_s(p)$ are conjugate. We first conjugate H_1 by an element of $N(C_s(p))$ so that $H_1 \cap C_s(p) = H_2 \cap C_s(p)$. Further note that $H_i = \left\langle H_i \cap C_s(p), \begin{pmatrix} 0 & \beta_i \\ \gamma_i & 0 \end{pmatrix} \right\rangle$ for any $\begin{pmatrix} 0 & \beta_i \\ \gamma_i & 0 \end{pmatrix} \in H_i$. We choose $\begin{pmatrix} 0 & \beta_1 \\ \gamma_1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \beta_2 \\ \gamma_2 & 0 \end{pmatrix}$ to be conjugate. In fact, since $\beta_1\gamma_1 = \beta_2\gamma_2$, the two are conjugate by a diagonal matrix, in which case H_1 and H_2 are conjugate via an element of $N(C_s(p))$ to begin with.

□

Lemma 6. *Let $H \leq B(p)$. H contains an element of order p if and only if $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in H$.*

Proof. $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has order p. By [3, Lemma 3.3], H has $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ p if it has an element of order p. □

Remark 5. *Theorem 2 states that all nontrivially locally conjugate subgroups of* $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ *must be subgroups of* $B(p)$ *with elements of order* p*, so Lemma 5 is valid even if we replaced the term conjugate with locally conjugate in the first sentence.*

5.2. **Stabilizers of Subgroups of** $\ker\varphi$**.** Given a subgroup $H \leq \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ not containing $\ker\varphi$, H can be replaced with a conjugate so that $H \cap \ker\varphi$ is one of the subgroups of $\ker\varphi$ as listed in Sections 4.2 and 4.3. Since $H \cap \ker\varphi$ is normal in H, $\varphi(H)$ must be a subgroup of the stabilizer of $H \cap \ker\varphi$ under conjugation. As we will see in Lemma 7 below, fixing $H \cap \ker\varphi$ in most cases gives some restrictions on $\varphi(H)$.

Lemma 7. *Let* $H \leq \ker\varphi$ *be one of the aforementioned subgroups. The stabilizer of* H *in* $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ *under conjugation is:*

(1) $\langle I\rangle$: $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$

(2) $\left\langle I + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} p \right\rangle$: $B(p)$

(3) $\left\langle I + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} p \right\rangle$: $N(C_s(p))$

(4) $\left\langle I + \begin{pmatrix} 0 & \epsilon \\ 1 & 0 \end{pmatrix} p \right\rangle$: $N(C_{ns}(p))$

(5) $\left\langle I + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} p, I + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} p \right\rangle$: $B(p)$.

(6) $\left\langle I + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} p, I + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} p \right\rangle$: $\left\{ \begin{pmatrix} \alpha & \beta \\ \mp\beta & \pm\alpha \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \right\}$

(7) $\left\langle I + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} p, I + \begin{pmatrix} 0 & \epsilon \\ 1 & 0 \end{pmatrix} p \right\rangle$: $\left\{ \begin{pmatrix} \alpha & \beta \\ \mp\beta/\epsilon & \pm\alpha \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \right\}$

(8) T: $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$

(9) $\left\langle I + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} p \right\rangle$: $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$

(10) $\left\langle I + \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} p \right\rangle$: $\left\langle Z(p), \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$

(11) $\left\langle I + \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} p \right\rangle$*, where* $d \neq \pm 1$: $C_s(p)$

(12) $\left\langle I + \begin{pmatrix} 1 & \epsilon c \\ c & 1 \end{pmatrix} p \right\rangle$*, where* $c \neq 0$: $C_{ns}(p)$

(13) $\left\langle I + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} p, I + \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} p \right\rangle$: $Z(p)$

(14) $\left\langle I + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} p, I + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} p \right\rangle$: $B(p)$

(15) $\left\langle I + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} p, I + \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} p \right\rangle$*, where* $d \neq -1$: $B(p)$

(16) $\left\langle I + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} p, I + \begin{pmatrix} 0 & 1 \\ c & 1 \end{pmatrix} p \right\rangle$*, where* $c \in \mathbb{Z}/p\mathbb{Z}$: $\left\langle Z(p), \begin{pmatrix} 0 & 1 \\ c & 0 \end{pmatrix} \right\rangle$

(17) $\left\langle I + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} p, I + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} p \right\rangle$: $N(C_s(p))$

(18) $\left\langle I+\begin{pmatrix}0&\epsilon\\1&0\end{pmatrix}p, I+\begin{pmatrix}1+a&-\epsilon b\\b&1-a\end{pmatrix}p\right\rangle$, *where* $a,b\in\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$*:* $\left\langle Z(p), \begin{pmatrix}a&-b\epsilon\\b&-a\end{pmatrix}\right\rangle$

(19) $\left\langle I+\begin{pmatrix}1&0\\0&-1\end{pmatrix}p, I+\begin{pmatrix}0&1\\0&0\end{pmatrix}p, I+\begin{pmatrix}0&0\\1&1\end{pmatrix}p\right\rangle$*:* $\left\langle Z(p), \begin{pmatrix}1&1\\0&1\end{pmatrix}\right\rangle$

(20) $\left\langle I+\begin{pmatrix}1&0\\0&-1\end{pmatrix}p, I+\begin{pmatrix}0&1\\0&0\end{pmatrix}p, I+\begin{pmatrix}0&0\\0&1\end{pmatrix}p\right\rangle$*:* $B(p)$

(21) $\left\langle I+\begin{pmatrix}1&0\\0&-1\end{pmatrix}p, I+\begin{pmatrix}0&1\\1&0\end{pmatrix}p, I+\begin{pmatrix}0&0\\0&1\end{pmatrix}p\right\rangle$*:* $\left\{\begin{pmatrix}\alpha&\beta\\\mp\beta&\pm\alpha\end{pmatrix}\in\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})\right\}$

(22) $\left\langle I+\begin{pmatrix}1&0\\0&-1\end{pmatrix}p, I+\begin{pmatrix}0&1\\1&0\end{pmatrix}p, I+\begin{pmatrix}0&0\\c&1\end{pmatrix}p\right\rangle$, *where* $1\le c\le\frac{p-1}{2}$*:*
$\left\{\begin{pmatrix}\alpha&\beta\\-\beta&\alpha\end{pmatrix}\in\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})\right\}$

(23) $\left\langle I+\begin{pmatrix}1&0\\0&-1\end{pmatrix}p, I+\begin{pmatrix}0&1\\\epsilon&0\end{pmatrix}p, I+\begin{pmatrix}0&0\\0&1\end{pmatrix}p\right\rangle$*:* $\left\{\begin{pmatrix}\alpha&\epsilon\gamma\\\mp\gamma&\pm\alpha\end{pmatrix}\right\}$

(24) $\left\langle I+\begin{pmatrix}1&0\\0&-1\end{pmatrix}p, I+\begin{pmatrix}0&1\\\epsilon&0\end{pmatrix}p, I+\begin{pmatrix}0&0\\c&1\end{pmatrix}p\right\rangle$, *where* $1\le c\le\frac{p-1}{2}$*:*
$\left\{\begin{pmatrix}\alpha&\epsilon\gamma\\-\gamma&\alpha\end{pmatrix}\in\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})\right\}$

(25) $\ker\varphi$*:* $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$

If any generator in a stabilizer listed above has zero determinant, then it is not to be included as a generator.

Proof. We will show this only for $H=\left\langle I+\begin{pmatrix}1&0\\0&-1\end{pmatrix}p, I+\begin{pmatrix}0&1\\c&1\end{pmatrix}p\right\rangle$, as the other cases are similar. Given that we know that $N(C_s(p))$ is the stabilizer of $\left\langle I+\begin{pmatrix}1&0\\0&-1\end{pmatrix}p\right\rangle$, any element of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ that preserves H must be in $N(C_s(p))$ because $H\cap T=\left\langle I+\begin{pmatrix}1&0\\0&-1\end{pmatrix}p\right\rangle$ and any conjugation preserves T.

Conjugating H by $\begin{pmatrix}\alpha&0\\0&\delta\end{pmatrix}$ results in the group $H'=\left\langle I+\begin{pmatrix}1&0\\0&-1\end{pmatrix}p, I+\begin{pmatrix}0&\frac{\alpha}{\delta}\\c\frac{\delta}{\alpha}&1\end{pmatrix}p\right\rangle$. $I+\begin{pmatrix}0&1\\c&1\end{pmatrix}p$ and $I+\begin{pmatrix}0&\frac{\alpha}{\delta}\\c\frac{\delta}{\alpha}&1\end{pmatrix}p$ are the unique elements of H and H', respectively, whose p-parts have trace 1 and upper left entry 0. Therefore, $H=H'$ if and only if $\alpha=\delta$, which is when $\begin{pmatrix}\alpha&0\\0&\delta\end{pmatrix}\in Z(p)$.

Conjugating H be $\begin{pmatrix}0&\beta\\\gamma&0\end{pmatrix}$ results in $H'=\left\langle I+\begin{pmatrix}-1&0\\0&1\end{pmatrix}p, I+\begin{pmatrix}1&c\frac{\beta}{\gamma}\\\frac{\gamma}{\beta}&0\end{pmatrix}p\right\rangle$. Note that

$$\left\langle I+\begin{pmatrix}1&0\\0&-1\end{pmatrix}p\right\rangle=\left\langle I+\begin{pmatrix}-1&0\\0&1\end{pmatrix}p\right\rangle$$

and we may replace $I+\begin{pmatrix}1&c\frac{\beta}{\gamma}\\\frac{\gamma}{\beta}&0\end{pmatrix}p$ with $I+\begin{pmatrix}0&c\frac{\beta}{\gamma}\\\frac{\gamma}{\beta}&1\end{pmatrix}p$ as a generator of H'. Similarly as in the last paragraph, $H=H'$ exactly when $\gamma=c\beta$. □

Recall that the only nontrivially locally conjugate subgroups among the ones listed here are subgroup 14 and the type 15 where $d = 0$ and two type 15 subgroups whose d values are multiplicative inverses.

5.3. **Applying the Schur-Zassenhaus Theorem.** We use a special case of the Schur-Zassenhaus theorem as stated in Theorem 3. Recall that a Hall subgroup of a finite group is one whose order is relatively prime to its index.

Theorem 3 (Schur-Zassenhaus)**.** *If K is an abelian normal Hall subgroup of a finite group G, then there is a splitting $\psi : K \to G$, which is unique up to conjugation.*

Proof. See [2, Theorem 7.39, 7.40]. □

Lemma 8. *Suppose $H_1, H_2 \leq \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$. If $H_1 \cap \ker\varphi = H_2 \cap \ker\varphi$, $\varphi(H_1) = \varphi(H_2)$, and p does not divide $|\varphi(H_i)|$, then H_1 and H_2 are conjugate in $\varphi^{-1}(\varphi(H_i))$.*

Proof. For $i = 1, 2$, consider the short exact sequence

$$1 \to \ker\varphi \to \varphi^{-1}(\varphi(H_i)) \to \varphi(H_i) \to 1.$$

Since $\ker\varphi$ is abelian, $|\ker\varphi| = p^4$ and p does not divide $|\varphi(H_i)|$, there is a unique splitting, up to conjugation, $\psi : \varphi(H_i) \to \varphi^{-1}(\varphi(H_i))$ by the Schur-Zassenhaus Theorem. Similarly, there are splittings $\psi_i : \varphi(H_i) \to H_i$ from the short exact sequences

$$1 \to H_i \cap \ker\varphi \to H_i \to \varphi(H_i) \to 1.$$

Since $H_i \leq \varphi^{-1}(\varphi(H_i))$, ψ_i and ψ are conjugate as maps $\varphi(H_i) \to \varphi^{-1}(\varphi(H_i))$. Therefore, ψ_1 and ψ_2 are conjugate in $\varphi^{-1}(\varphi(H_i))$. □

With this lemma, we will now only need to worry about the cases where $H_1 \cap \ker\varphi \neq H_2 \cap \ker\varphi$ or $\varphi(H_1) \neq \varphi(H_2)$.

5.4. **Representations of Elements of** $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$**.** We will discuss some lemmas later that will be useful to determine local conjugacy among subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$. We mention here how we will represent some elements of $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ before stating these lemmas.

There is an injective homomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p^2\mathbb{Z})^\times$ given by $\overline{x} \mapsto x^p$, where $\overline{x} \in \mathbb{Z}/p\mathbb{Z}$ and x is any lift of x in $\mathbb{Z}/p^2\mathbb{Z}$. The map is well defined because $(x + kp)^p = x$ in $\mathbb{Z}/p^2\mathbb{Z}$ by the binomial theorem. We will refer to this map as canonical. Note that elements of the image of the injection have order dividing $p - 1$. We extend the canonical map by choosing $0 \in \mathbb{Z}/p^2\mathbb{Z}$ as the lift of $0 \in \mathbb{Z}/p\mathbb{Z}$.

Say $g_1, g_2, g_3 \in \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ where $\varphi(g_1) = \begin{pmatrix} \overline{w} & 0 \\ 0 & \overline{w} \end{pmatrix}$, $\varphi(g_2) = \begin{pmatrix} \overline{w} & 0 \\ 0 & \overline{z} \end{pmatrix}$, $\varphi(g_3) = \begin{pmatrix} 0 & \overline{x} \\ \overline{y} & 0 \end{pmatrix}$ and $\varphi(g_4) = \begin{pmatrix} 1 & \overline{n} \\ 0 & 1 \end{pmatrix}$ respectively. Throughout this paper, we will represent these matrices in the form

$$g_1 = \begin{pmatrix} w & 0 \\ 0 & w \end{pmatrix} + A_1 p,\ g_2 = \begin{pmatrix} w & 0 \\ 0 & z \end{pmatrix} + A_2 p,\ g_3 = \begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix} + A_3 p,\ g_4 = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} + A_4 p$$

respectively for some $A_1, A_2, A_3, A_4 \in \mathrm{Mat}_2(\mathbb{Z}/p\mathbb{Z})$, where w, x, y, z, n are chosen canonically in $\mathbb{Z}/p^2\mathbb{Z}$. We omit the bars on residues of elements of $\mathbb{Z}/p^2\mathbb{Z}$ in $\mathbb{Z}/p\mathbb{Z}$ later on, i.e. if we have $x \in \mathbb{Z}/p\mathbb{Z}$, then we denote $x \in \mathbb{Z}/p^2\mathbb{Z}$ as the canonical lift.

5.5. **Conjugacy and Local Conjugacy.**

Lemma 9. *Let $H \leq \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$. If $h \in H$ where $\varphi(h) = \begin{pmatrix} w & 0 \\ 0 & w \end{pmatrix}$, then $\begin{pmatrix} w & 0 \\ 0 & w \end{pmatrix} \in H$. In particular, $\begin{pmatrix} w & 0 \\ 0 & w \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} p \in H$ if and only if $I + \begin{pmatrix} a & b \\ c & d \end{pmatrix} p \in H$.*

Proof. We express h as $h = \begin{pmatrix} w & 0 \\ 0 & w \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} p$. Since $\begin{pmatrix} w & 0 \\ 0 & w \end{pmatrix}$ commutes with all matrices, $h^p = \begin{pmatrix} w & 0 \\ 0 & w \end{pmatrix}$ by the binomial theorem.

$\begin{pmatrix} w & 0 \\ 0 & w \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} p \in H$ if and only if $\begin{pmatrix} w & 0 \\ 0 & w \end{pmatrix}^{-1} \left(\begin{pmatrix} w & 0 \\ 0 & w \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} p \right) = I + \begin{pmatrix} a/w & b/w \\ c/w & d/w \end{pmatrix} p \in H$. Scaling tells us that $I + \begin{pmatrix} a/w & b/w \\ c/w & d/w \end{pmatrix} p \in H$ if and only if $I + \begin{pmatrix} a & b \\ c & d \end{pmatrix} p$. □

Corollary 1. *Let $H \leq \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ with $\varphi(H) \leq Z(p)$. H is the direct product $(H \cap \ker \varphi) \times (H \cap \psi(Z(p)))$, where $\psi : Z(p) \to \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ is the canonical injection. In particular, two subgroups $H_1, H_2 \leq \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ are locally conjugate if and only if $H_1 \cap \ker \varphi$ and $H_2 \cap \ker \varphi$ are.*

With the Corollary 1 in mind, we will assume that $\varphi(H) \not\leq Z(p)$ for any $H \leq \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ from here.

Lemma 10. *Let $H \leq \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$. If $h \in H$ where $h = \begin{pmatrix} w & 0 \\ 0 & z \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} p$ where $w \not\equiv z \pmod{p}$, then $\begin{pmatrix} w & 0 \\ 0 & z \end{pmatrix} + \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} p \in H$.*

Proof. By expanding h^p, we compute

$$\begin{aligned} h^p &= \begin{pmatrix} w & 0 \\ 0 & z \end{pmatrix}^p + \left(\sum_{k=0}^{p-1} \begin{pmatrix} w & 0 \\ 0 & z \end{pmatrix}^k \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w & 0 \\ 0 & z \end{pmatrix} \right) p \\ &= I + \sum_{k=0}^{p-1} \begin{pmatrix} aw^{p-1} & bw^k z^{p-1-k} \\ cz^k w^{p-1-k} & dz^{p-1} \end{pmatrix} p. \end{aligned}$$

Since $w \not\equiv z \pmod{p}$, $\sum_{k=0}^{p-1} w^k z^{p-1-k}$ and $\sum_{k=0}^{p-1} z^k w^{p-1-k}$ are geometric series that evaluate to 1. Therefore, $h^p = \begin{pmatrix} w & 0 \\ 0 & z \end{pmatrix} + \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} p$. □

Corollary 2. *Let $H \leq \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$. If $h = \begin{pmatrix} w & 0 \\ 0 & z \end{pmatrix} + Ap \in H$ where $w \not\equiv z \pmod{p}$, then H can be conjugated by an element of $\ker \varphi$ so that $\begin{pmatrix} w & 0 \\ 0 & z \end{pmatrix} \in H$.*

Proof. Letting $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\begin{pmatrix} w & 0 \\ 0 & z \end{pmatrix} + \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} p$ is in H by the previous lemma. $\begin{pmatrix} w & 0 \\ 0 & z \end{pmatrix} + \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} p$ is conjugate to $\begin{pmatrix} w & 0 \\ 0 & z \end{pmatrix}$ via $I + \begin{pmatrix} 0 & \frac{b}{w-z} \\ \frac{c}{z-w} & 0 \end{pmatrix} p$. □

By Corollary 2, if $\varphi(H)$ has some diagonal element, then we can conjugate H, without affecting $H \cap \ker \varphi$, so that H has a diagonal element whose entries are images of the canonical map $(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p^2\mathbb{Z})^\times$ and which is the lift of the diagonal element of $\varphi(H)$.

In Lemmas 11 through 18, we let $H_1, H_2 \leq \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ be locally conjugate where $H_1 \cap \ker \varphi = H_2 \cap \ker \varphi$ is one of the subgroups of $\ker \varphi$ listed in Lemma 7 and $\varphi(H_1), \varphi(H_2) \not\leq Z(p)$.

Lemma 11. *Suppose that the stabilizer of $H_i \cap \ker \varphi$ is $C_s(p)$. H_1 and H_2 are conjugate.*

Proof. Note that $H_i \cap \ker \varphi = \left\langle I + \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} p \right\rangle$ where $d \neq \pm 1$. Since $\varphi(H_i) \leq C_s(p)$, $\varphi(H_1)$ and $\varphi(H_2)$ are equal or they are diagonal swaps. We know that H_1 and H_2 must be conjugate in the former case by Lemma 8, so we assume that they are unequal and hence are diagonal swaps. Choose $h_1 = \begin{pmatrix} w & 0 \\ 0 & z \end{pmatrix} \in H_1$ where $w \not\equiv z \pmod{p}$ so that $h_2 = \begin{pmatrix} z & 0 \\ 0 & w \end{pmatrix} \in H_2$ but $h_1 \notin H_2$. Note that such choices can be made using Corollary 2. Moreover,

$$h_1' = h_1 \left(I + \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} p \right) = h_1 + \begin{pmatrix} w & 0 \\ 0 & dz \end{pmatrix} p \in H_1,$$

A in H_2 conjugate to h_1' must map down to $\varphi(h_2)$, i.e. the conjugate is of the form $h_2 k$ for some $k \in H_2 \cap \ker \varphi$. Such a matrix is of the form

$$h_2' = h_2 \left(I + \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} p \right)^r = h_2 + \begin{pmatrix} rz & 0 \\ 0 & rdw \end{pmatrix} p.$$

The determinants of h_1' and h_2' are $wz + wz(1+d)p$ and $wz + rwz(1+d)p$ respectively, so $r = 1$. The traces are $(w+z) + (w+dz)p$ and $(w+z) + (z+dw)p$ respectively, so $(w-z) \equiv d(w-z) \pmod{p}$ which is a contradiction. Hence, H_1 and H_2 are not nontrivially locally conjugate in either case. □

Lemma 12. *Suppose that the stabilizer of $H_i \cap \ker \varphi$ is $N(C_s(p))$. H_1 and H_2 are conjugate.*

Proof. If there is a conjugation from $\varphi(H_1)$ to $\varphi(H_2)$ taking diagonal matrices to diagonal ones and nondiagonal matrices to nondiagonal ones, then $\varphi(H_1)$ and $\varphi(H_2)$ are conjugate via an element of $N(C_s(p))$ by Lemma 5, in which case we can conjugate H_1 so that $\varphi(H_1) = \varphi(H_2)$ and $H_1 \cap \ker \varphi = H_2 \cap \ker \varphi$.

Otherwise, all conjugations from $\varphi(H_1)$ to $\varphi(H_2)$ take some diagonal element to a nondiagonal one or some nondiagonal element to a diagonal one. In particular, $\varphi(H_1) \neq \varphi(H_2)$. Note that diagonal matrices and nondiagonal matrices of $N(C_s(p))$ that are conjugate are of the form $\begin{pmatrix} w & 0 \\ 0 & -w \end{pmatrix}$ and $\begin{pmatrix} 0 & wr \\ w/r & 0 \end{pmatrix}$. Moreover, $\begin{pmatrix} w & 0 \\ 0 & -w \end{pmatrix}$ is conjugate to $\begin{pmatrix} 0 & wr \\ w/r & 0 \end{pmatrix}$ only via matrices of the form $\begin{pmatrix} a & b \\ a/r & -b/r \end{pmatrix}$, so $\begin{pmatrix} 0 & wr \\ w/r & 0 \end{pmatrix}$ is conjugate to $\begin{pmatrix} w & 0 \\ 0 & -w \end{pmatrix}$ via

$\begin{pmatrix} a & b \\ a/r & -b/r \end{pmatrix}^{-1}$. Conjugating $\begin{pmatrix} w & 0 \\ 0 & z \end{pmatrix}$ where $w \neq \pm z$ by $\begin{pmatrix} a & b \\ a/r & -b/r \end{pmatrix}$ or $\begin{pmatrix} a & b \\ a/r & -b/r \end{pmatrix}^{-1}$ does not yield a matrix in $N(C_s(p))$, so $\varphi(H_1)$ and $\varphi(H_2)$ do not have such matrices.

Without loss of generality, say that $\varphi(H_1)$ has some matrix of the form $\begin{pmatrix} w & 0 \\ 0 & -w \end{pmatrix}$. $\varphi(H_1)$ is generated by $\varphi(H_1) \cap Z(p)$, $\begin{pmatrix} w & 0 \\ 0 & -w \end{pmatrix}$ and, if $\varphi(H_1)$ has such an element, $\begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}$. Suppose $\varphi(H_1)$ is generated by all three. If $\varphi(H_1)$ is conjugate to $\varphi(H_2)$ via $\begin{pmatrix} a & b \\ a/r & -b/r \end{pmatrix}$, then a^2x must be $\pm b^2y$ to ensure that $\begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}$ is conjugated into $N(C_s(p))$. If $a^2x = -b^2y$, then we replace $\begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}$ with $\begin{pmatrix} w & 0 \\ 0 & -w \end{pmatrix}\begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix} = \begin{pmatrix} 0 & -wx \\ wy & 0 \end{pmatrix}$ so that $a^2x = b^2y$. In this case, $\begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}$ is conjugate to $\begin{pmatrix} ax/b & 0 \\ 0 & -ax/b \end{pmatrix}$. If $\begin{pmatrix} ax/b & 0 \\ 0 & -ax/b \end{pmatrix} = \begin{pmatrix} \pm w & 0 \\ 0 & \mp w \end{pmatrix}$, then $\begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix} = \begin{pmatrix} 0 & \pm bw/a \\ \pm bw/a & 0 \end{pmatrix}$, in which case $\varphi(H_2)$ is generated by $\varphi(H_1) \cap Z(p)$, $\begin{pmatrix} \pm w & 0 \\ 0 & \mp w \end{pmatrix}$ and $\begin{pmatrix} 0 & wr \\ w/r & 0 \end{pmatrix}$. However, $\varphi(H_1)$ is then conjugate to $\varphi(H_2)$ via $\begin{pmatrix} \pm br & 0 \\ 0 & a \end{pmatrix}$, a contradiction. We now assume that no choice of x and y can be made so that $\begin{pmatrix} ax/b & 0 \\ 0 & -ax/b \end{pmatrix} = \begin{pmatrix} \pm w & 0 \\ 0 & \mp w \end{pmatrix}$. In particular, the element of $\varphi(H_2)$ that is conjugate to $\begin{pmatrix} w & 0 \\ 0 & -w \end{pmatrix}$ must of the form $\begin{pmatrix} 0 & wr \\ w/r & 0 \end{pmatrix}$. The case where $\varphi(H_1)$ is conjugate to $\varphi(H_2)$ via $\begin{pmatrix} -b/r & -b \\ -a/r & a \end{pmatrix}$ is similar.

In the case that $\varphi(H_1)$ is generated by only the first two, and so $\varphi(H_1)$ is conjugate to $\varphi(H_2)$ via $\begin{pmatrix} a & b \\ a/r & -b/r \end{pmatrix}$, $\varphi(H_2)$ is generated by $\varphi(H_1) \cap Z(p)$ and $\begin{pmatrix} 0 & wr \\ w/r & 0 \end{pmatrix}$. Therefore, $\begin{pmatrix} w & 0 \\ 0 & -w \end{pmatrix}$ is in $\varphi(H_1)$ and not $\varphi(H_2)$ in either case, so the element of $\varphi(H_2)$ that is conjugate to $\begin{pmatrix} w & 0 \\ 0 & -w \end{pmatrix}$ is $\begin{pmatrix} 0 & wr \\ w/r & 0 \end{pmatrix}$. Conjugating $\varphi(H_2)$ via $\begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix}$ preserves the first two generators of $\varphi(H_2)$ and takes $\begin{pmatrix} 0 & wr \\ w/r & 0 \end{pmatrix}$ to $\begin{pmatrix} 0 & w \\ w & 0 \end{pmatrix}$, so we can conjugate H_2, without affecting $H_2 \cap \ker\varphi$, so that $\varphi(H_2)$ is this new group.

We replace H_1 with a conjugate if necessary so that $\begin{pmatrix} w & 0 \\ 0 & -w \end{pmatrix} \in H_1$. The conjugation preserves $H_1 \cap \ker\varphi$ by Corollary 2. Note that, for both of its possibilities, $H_i \cap \ker\varphi$ only has elements whose p-parts are diagonal. The elements of H_1 whose images are $\begin{pmatrix} w & 0 \\ 0 & -w \end{pmatrix}$ are exactly those of the form

$$h_1 = \begin{pmatrix} w & 0 \\ 0 & -w \end{pmatrix}\left(I + \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} p\right) = \begin{pmatrix} w & 0 \\ 0 & -w \end{pmatrix} + \begin{pmatrix} aw & 0 \\ 0 & -dw \end{pmatrix} p$$

where $I + \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} p \in H_i \cap \ker \varphi$. h_1 has trace $(a-d)wp$.

On the other hand, take some $h_2 \in H_2$ to be conjugate to h_1. h_2 has the form $h_2 = \begin{pmatrix} 0 & w \\ w & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} p \in H_2$. Its square is $\begin{pmatrix} w^2 & 0 \\ 0 & w^2 \end{pmatrix} + \begin{pmatrix} (b+c)w & (a+d)w \\ (a+d)w & (b+c)w \end{pmatrix}$. Therefore, $I + \begin{pmatrix} (b+c)w & (a+d)w \\ (a+d)w & (b+c)w \end{pmatrix} \in H_2$ by Lemma 9, so $a+d=0$. Thus, h_2 has zero trace. However, in both cases of $H_i \cap \ker \varphi$, we can choose a and d in the previous paragraph so that h_1 does not have zero trace, which is a contradiction. Hence, this case does not happen. □

Lemma 13. *Suppose that the stabilizer of $H_i \cap \ker \varphi$ is $C_{ns}(p)$. H_1 and H_2 are conjugate.*

Proof. Since $C_{ns}(p)$ is cyclic and $\varphi(H_1)$ and $\varphi(H_2)$ are locally conjugate in $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, $\varphi(H_1) = \varphi(H_2)$. Hence, H_1 and H_2 are conjugate. □

Lemma 14. *Suppose that the stabilizer of $H_i \cap \ker \varphi$ is $N(C_{ns}(p))$. H_1 and H_2 are conjugate.*

Proof. Note that $H_i \cap \ker \varphi = \left\langle I + \begin{pmatrix} 0 & \epsilon \\ 1 & 0 \end{pmatrix} p \right\rangle$. The proof is similar to that of Lemma 12 once we work in $\mathbb{Z}_p[\sqrt{\epsilon}]/p^2$ and conjugate H_1 and H_2 by $\begin{pmatrix} -\sqrt{\epsilon} & -\epsilon \\ -\sqrt{\epsilon} & \epsilon \end{pmatrix}$, which turns $\begin{pmatrix} w & \epsilon y \\ y & w \end{pmatrix}, \begin{pmatrix} w & \epsilon y \\ -y & -w \end{pmatrix} \in N(C_{ns}(p))$ into $\begin{pmatrix} w+\sqrt{\epsilon}y & 0 \\ 0 & w-\sqrt{\epsilon}y \end{pmatrix}$ and $\begin{pmatrix} 0 & w-\sqrt{\epsilon}y \\ w+\sqrt{\epsilon}y & 0 \end{pmatrix}$ respectively and turns $H_i \cap \ker \varphi$ into $\left\langle I + \begin{pmatrix} \sqrt{\epsilon} & 0 \\ 0 & -\sqrt{\epsilon} \end{pmatrix} p \right\rangle$. □

Lemma 15. *Suppose that the stabilizer of $H_i \cap \ker \varphi$ is $\left\langle Z(p), \begin{pmatrix} 0 & 1 \\ c & 0 \end{pmatrix} \right\rangle$ for some fixed $c \in \mathbb{Z}/p\mathbb{Z}$. H_1 and H_2 are conjugate.*

Proof. Recall that we are assuming that $\varphi(H_i) \not\leq Z(p)$. By extension, we must assume $c \neq 0$. Note that $\varphi(H_i) = \left\langle \varphi(H_i) \cap Z(p), \begin{pmatrix} 0 & \beta_i \\ \beta_i c & 0 \end{pmatrix} \right\rangle$ given that $\begin{pmatrix} 0 & \beta_i \\ \beta_i c & 0 \end{pmatrix} \in \varphi(H_i)$. We choose β_1 and β_2 so that $\begin{pmatrix} 0 & \beta_1 \\ \beta_1 c & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & \beta_2 \\ \beta_2 c & 0 \end{pmatrix}$ are conjugate. By the determinants of these matrices, $\beta_1 = \pm \beta_2$. If $\beta_1 = \beta_2$, then H_1 and H_2 are conjugate, so we assume $\beta_1 = -\beta_2$.

We choose $h_1 \in H_1$ and $h_2 \in H_2$ so that $\varphi(h_1) = \begin{pmatrix} 0 & \beta_1 \\ \beta_1 c & 0 \end{pmatrix}$ and h_2 is conjugate to h_1. It follows that $\varphi(h_2) = \begin{pmatrix} 0 & \beta_2 \\ \beta_2 c & 0 \end{pmatrix}$. Express $h_i = \begin{pmatrix} 0 & \beta_i \\ \beta_i c & 0 \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} p \in H_i$ so that

$$h_i^2 = \begin{pmatrix} \beta_i^2 c & 0 \\ 0 & \beta_i^2 c \end{pmatrix} + \begin{pmatrix} b'\beta_i c + c'\beta_i & (a'+d')\beta_i \\ (a'+d')\beta_i c & b'\beta_i c + c'\beta_i \end{pmatrix} p$$

Therefore, $I + \begin{pmatrix} b'\beta_i c + c'\beta_i & (a'+d')\beta_i \\ (a'+d')\beta_i c & b'\beta_i c + c'\beta_i \end{pmatrix} p \in H_i$ by Lemma 9. Expressing this element of H_i as a linear combination of the basis elements of $H_i \cap \ker \varphi$ tells us that $2(b'c + c') = a' + d'$. Note that the trace and determinant of h_i are $(a'+d')p$ and $-\beta_i^2 c - (b'c + c')\beta_i p$ respectively. Thus, letting $T_i = a' + d'$, the trace and determinant are $T_i p$ and $-\beta_i^2 c - \frac{T_i}{2}\beta_i p$

respectively. Since h_1 and h_2 are conjugate, $T_1 = T_2 = 0$. However, we may replace h_i with $h_i\left(I + \begin{pmatrix}0 & 1\\ c & 1\end{pmatrix}p\right) \in H_i$ so that h_i has nonzero trace, which is a contradiction. Hence, H_1 and H_2 are not locally conjugate in this case. □

Lemma 16. *Suppose that the stabilizer of* $H_i \cap \ker\varphi$ *is* $\left\langle I + \begin{pmatrix}0 & \epsilon\\ 1 & 0\end{pmatrix}p, I + \begin{pmatrix}1+a & -\epsilon b\\ b & 1-a\end{pmatrix}p\right\rangle$ *for some fixed* $a, b \in \mathbb{Z}/p\mathbb{Z}$. H_1 *and* H_2 *are conjugate.*

Proof. The proof is similar to that of the previous lemma, but we need to differentiate the cases $a = 0$ and $a \neq 0$. □

Lemma 17. *For* $g = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} + \begin{pmatrix}a & b\\ c & d\end{pmatrix}p$,

$$g^n = \begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix} + \begin{pmatrix}an + c\frac{n(n-1)}{2} & (a(n-1)+b)n + (d-a+c(n-1))\frac{n(n-1)}{2} - c\sum_{k=0}^{n-1}k^2\\ cn & dn + c\frac{n(n-1)}{2}\end{pmatrix}p$$

Proof. We compute

$$\begin{aligned} g^n &= \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^n + \sum_{k=0}^{n-1}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^k\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^{n-1-k}p\\ &= \begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix} + \sum_{k=0}^{n-1}\begin{pmatrix}a+ck & (a(n-1)+b) + (-a+c(n-1)+d)k - ck^2\\ c & c(n-1)+d-ck\end{pmatrix}\\ &= \begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix} + \begin{pmatrix}an + c\frac{n(n-1)}{2} & (a(n-1)+b)n + (d-a+c(n-1))\frac{n(n-1)}{2} - c\sum_{k=0}^{n-1}k^2\\ cn & dn + c\frac{n(n-1)}{2}\end{pmatrix}p \end{aligned}$$

□

Remark 6. *We leave* $\sum_{k=0}^{n-1}k^2$ *as is even though it is usually expressible as* $\frac{(n-1)n(2n-3)}{6}$ *because this fraction is ambiguous when* $p = 3$.

Lemma 18. *Suppose that the stabilizer of* $H_i \cap \ker\varphi$ *is* $\left\langle Z(p), \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right\rangle$. H_1 *and* H_2 *are conjugate.*

Proof. Recall $H_i \cap \ker\varphi = \left\langle I + \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}p\right\rangle$ or $\left\langle I + \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}p, I + \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}p, I + \begin{pmatrix}0 & 0\\ 1 & 1\end{pmatrix}p\right\rangle$. In the former case, say that $h_i = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} + \begin{pmatrix}a & b\\ c & d\end{pmatrix}p \in H_i$. By Lemma 17,

$$h_i^p = \begin{pmatrix}1 & \left(1 - c\sum_{k=0}^{n-1}k^2\right)p\\ 0 & 1\end{pmatrix},$$

which is $\begin{pmatrix}1 & p\\ 0 & 1\end{pmatrix}$ if $p \neq 3$ or $c \neq 2$. However, $\begin{pmatrix}1 & p\\ 0 & 1\end{pmatrix} \notin H_i \cap \ker\varphi$ by assumption, so $p = 3$ and $c = 2$. We have computationally checked that H_1 and H_2 are conjugate in this case.

In the latter case, note that conjugacy and local conjugacy between H_1 and H_2 does not depend on $\varphi(H_1) \cap Z(p)$ and $\varphi(H_2) \cap Z(p)$, just as long as they are equal. We assume that $\varphi(H_i) \cap Z(p) = \langle I\rangle$. We take $h_1 = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} + \begin{pmatrix}a & b\\ c & d\end{pmatrix}p$. We can replace h_1 by

$h_1\left(I+\begin{pmatrix}0&0\\1&1\end{pmatrix}p\right)^k$ for some k so that h_1 has trace 1. We replace H_1 by its conjugate via $I+\begin{pmatrix}0&0\\a&0\end{pmatrix}p$ so that $h_1=\begin{pmatrix}1&1\\0&1\end{pmatrix}+\begin{pmatrix}0&b\\c&0\end{pmatrix}p$. This conjugation preserves $H_1\cap\ker\varphi$. Moreover, multiplying h_1 by some power of $I+\begin{pmatrix}0&1\\0&0\end{pmatrix}p$ yields $\begin{pmatrix}1&1\\0&1\end{pmatrix}+\begin{pmatrix}0&0\\c&0\end{pmatrix}p$, so H_1 has this matrix. Similarly, we can conjugate H_2 if necessary so that $h_2=\begin{pmatrix}1&1\\0&1\end{pmatrix}+\begin{pmatrix}0&0\\c'&0\end{pmatrix}p\in H_2$.

We use Lemma 3 to determine when H_1 and H_2 are locally conjugate. Multiplying elements of H_i by $e_1=I+\begin{pmatrix}1&0\\0&-1\end{pmatrix}p$ and by $e_2=I+\begin{pmatrix}0&1\\0&0\end{pmatrix}p$ do not affect the trace and determinant. We will thus only consider the traces and determinants of elements of $H_i'=\langle h_i,e_3\rangle$ where $e_3=I+\begin{pmatrix}0&0\\1&1\end{pmatrix}p$.

Elements of H_1' mapping down to $\begin{pmatrix}1&n\\0&1\end{pmatrix}$ have the form

$$\left(\begin{pmatrix}1&1\\0&1\end{pmatrix}+\begin{pmatrix}0&0\\c&0\end{pmatrix}p\right)^n e_3^x=\begin{pmatrix}1&n\\0&1\end{pmatrix}+\begin{pmatrix}c\frac{n(n-1)}{2}+nx&*\\cn+x&c\frac{n(n-1)}{2}+x\end{pmatrix}p$$

for some $x\in\mathbb{Z}/p\mathbb{Z}$, and this has trace $2+(cn^2-cn+nx+x)p$ and determinant $1+(-cn+x)p$. Therefore, the trace-determinant pairs of elements are in correspondence with the pairs $(cn^2-cn+nx+x,-cn+x)$, or equivalently, $(cn^2+nx,-cn+x)$. Similarly, the trace-determinant pairs of elements of H_2' are in correspondence with the pairs $(c'n^2+nx,-c'n+x)$.

Suppose $c\neq0$ but $c'=0$. $-c'n+x=0$ exactly when $x=0$ and so $c'n^2+nx=0$ in this case. On the other hand, $-cn+x=0$ when $x=cn$ and so $cn^2+nx=2cn^2$, which is not always zero. Hence, c and c' must be both zero or nonzero.

If $c,c'\neq0$, then consider the case $-cn+x=1$. Here, $x=1+cn$ and so $cn^2+nx=2cn^2+n=2c(n+1/(4c))^2-1/(8c)$. cn^2+nx takes the value $-1/(8c)$ exactly once and it takes all other values exactly two or zero times. On the other hand, when $-c'n+x=1$, $c'n^2+nx$ takes the value $-1/(8c')$ exactly once but takes all other values exactly two or zero times. Since we need the distribution of pairs $(cn^2+nx,cn+x)$ and $(c'n^2+nx,-c'n+x)$ to be the same for H_1 and H_2 to be locally conjugate, c and c' must equal, i.e. $H_1=H_2$. □

We expect the following to be true based on our observations with $p=3$. However, we have yet to fully identity a proof of this conjecture at the time of this paper. We hope that a proof, if it exists, of this conjecture will work similarly to the proofs of Lemmas 11 through 14 because the stabilizers listed are conjugate to $C_s(p),C_{ns}(p),N(C_s(p))$ or $N(C_{ns}(p))$ depending on p modulo 4.

Conjecture 1. *Suppose that the stabilizer of $H_i\cap\ker\varphi$ is $\left\{\begin{pmatrix}\alpha&\beta\\-\beta&\alpha\end{pmatrix}\in\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})\right\}$, $\left\{\begin{pmatrix}\alpha&\beta\\\mp\beta&\pm\alpha\end{pmatrix}\in\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})\right\}$, $\left\{\begin{pmatrix}\alpha&\epsilon\gamma\\-\gamma&\alpha\end{pmatrix}\in\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})\right\}$ or $\left\{\begin{pmatrix}\alpha&\epsilon\gamma\\\mp\gamma&\pm\alpha\end{pmatrix}\in\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})\right\}$. H_1 and H_2 are conjugate.*

Lemma 19. *Suppose that the stabilizer of $H_i\cap\ker\varphi$ is $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. If $\varphi(H_i)$ does not contain an element of order p, then H_1 and H_2 are conjugate.*

Proof. In this case, $\varphi(H_1)$ and $\varphi(H_2)$ are conjugate as they are locally conjugate. We replace H_1 with a conjugate so that $\varphi(H_1) = \varphi(H_2)$. By Lemma 8, $H_1 = H_2$. □

Lemma 20. *Suppose that $H_i \cap \ker\varphi = \langle I \rangle$ or $\left\langle I + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} p \right\rangle$. H_1 and H_2 are conjugate if $p \neq 3$.*

Proof. Suppose H_1 and H_2 are nontrivially locally conjugate. By Lemma 19, $\varphi(H_i)$ needs to contain an element of order p. Up to conjugation, $\varphi(H_i) \leq B(p)$ or $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \leq \varphi(H_i)$ by Theorem 1. In either case, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \varphi(H_i)$; the former implication is due to Lemma 6. Given that $p \neq 3$, $I + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} p \in H_1$, which is a contradiction. Hence, H_1 and H_2 are conjugate. □

Remark 7. $\left\langle \begin{pmatrix} 8 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 4 \\ 6 & 4 \end{pmatrix} \right\rangle$ *and* $\left\langle \begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix}, \begin{pmatrix} 4 & 4 \\ 6 & 4 \end{pmatrix} \right\rangle$ *are nontrivially locally conjugate and* $\left\langle \begin{pmatrix} 4 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 4 & 4 \\ 6 & 4 \end{pmatrix} \right\rangle$ *and* $\left\langle \begin{pmatrix} 5 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 4 & 4 \\ 6 & 4 \end{pmatrix} \right\rangle$ *are nontrivially locally conjugate when $p = 3$. We have found, through computation, that they are the only pairs up to conjugation that intersect with $\ker\varphi$ at $\langle I \rangle$ and $\left\langle I + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} p \right\rangle$ respectively. We refer to these cases as the special cases of $p = 3$.*

We are left with the following:

Corollary 3. *Barring the special cases of $p = 3$ and the cases of Conjecture 1, let $H_1, H_2 \leq \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ be nontrivially locally conjugate, where $H_1 \cap \ker\varphi$ and $H_2 \cap \ker\varphi$ are some subgroups of $\ker\varphi$ listed in Lemma 7. H_1 and H_2 contain $I + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} p \in H_i$.*

Proof. Lemmas 11 through 18 show that the stabilizer of $H_i \cap \ker\varphi$ is $B(p)$ or $\mathrm{GL}_2(\mathbb{Z})$. In the former case, $H_i \cap \ker\varphi$ must contain $I + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} p$. In the latter, H_i must contain an element mapping down to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ by Lemma 19 and Lemma 6 and since we have ruled out the special cases of $p = 3$, $I + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} p \in H_i$ by Lemma 17. □

Remark 8. *With H_1 and H_2 as in Corollary 3, The stabilizer of $H_i \cap \ker\varphi$ must be $B(p)$ or $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. In the latter case, $\varphi(H_i) \leq B(p)$ or $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \leq \varphi(H_i)$.*

We finish with another conjecture based on data from the case $p = 3$:

Conjecture 2. *Let $H_1, H_2 \leq \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ be nontrivially locally conjugate. Up to conjugation, H_1 and H_2 are diagonal swaps and are thus isomorphic.*

Acknowledgement

I would like to thank my mentor Atticus Christensen for his invaluable insight on approaching the main problem, his daily help on the complicated details towards solving it, and his guidance in constructing this paper. I would also like to thank Professors David Jerison and Ankur Moitra for their encouragement and experienced advice on working with mathematics. I give my final thanks to Dr. Slava Gerovitch and MIT Mathematics for making the Summer Program in Undergraduate Research possible.

References

[1] L.E. Dickson. *Linear Groups with an Exposition of Galois Field Theory*. Cosimo classics science. Lightning Source Incorporated, 2007.

[2] J.J. Rotman. *An introduction to the theory of groups*. Springer, 4 edition, 1994.

[3] Andrew V. Sutherland. Computing images of Galois representations attached to elliptic curves. *Forum Math. Sigma*, 4:e4, 79, 2016.