J. Math. Soc. Japan
Vol. 61, No. 4 (2009) pp. 1013–1070
doi: 10.2969/jmsj/06141013

Some primitive linear groups of prime degree

In Memory of Walter Feit

By Ming-chang KANG, Ji-ping ZHANG, Jian-yi SHI, Yung YU and Stephen S. T. YAU

(Received Oct. 3, 2007)
(Revised Aug. 6, 2008)

Abstract. A classical problem in finite group theory dating back to Jordan, Klein, E. H. Moore, Dickson, Blichfeldt etc. is to determine all finite subgroups in $SL(n, \boldsymbol{C})$ up to conjugation for some small values of n. This question is important in group theory as well as in the study of quotient singularities. Some results of Blichfeldt when $n = 3, 4$ were generalized to the case of finite primitive subgroups of $SL(5, \boldsymbol{C})$ and $SL(7, \boldsymbol{C})$ by Brauer and Wales. The purpose of this article is to consider the following case. Let p be any odd prime number and G be a finite primitive subgroup of $SL(p, \boldsymbol{C})$ containing a non-trivial monomial normal subgroup H so that H has a non-scalar diagonal matrix. We will classify all these groups G up to conjugation in $SL(p, \boldsymbol{C})$ by exhibiting the generators of G and representing G as some group extensions. In particular, see the Appendix for a list of these subgroups when $p = 5$ or 7.

1. Introduction.

There is no question that the most renowned problem in the finite group theory is the classification of finite simple groups. Another classification problem dating back to Jordan, Klein, E. H. Moore, Dickson, Blichfeldt etc. is the determination of all finite subgroups in $SL(n, \boldsymbol{C})$ up to conjugation for some small values of n [**Fe1**, Section 6], [**Br1**], [**Br2**, pp.32–33], [**Wa1**], [**Li**], [**Si**], [**Zh2**]. The latter problem was initiated by Camille Jordan (1838–1922) in an attempt to classify differential equations of the Fuchsian class with algebraic solutions. More precisely, a linear homogeneous differential equation of order n, whose coefficients are meromorphic functions on the complex plane, is called an equation of the Fuchsian class if it has only regular singularities [**Po**, p.76], [**Gr**, Chapter 2], a solution of such a differential equation is an algebraic solution if it is locally a branch of some algebraic function [**Gr**, p.48]. Besides solving these equations, Fuchs tried to characterize those equations with algebraic solutions [**Gr**, p.48], [**Po**, Chapters IV and V]. Jordan discovered a group-theoretic answer to this

2000 *Mathematics Subject Classification.* Primary 20C15.
Key Words and Phrases. linear groups of prime degree, monomial groups.

question: An n-th order differential equation of the Fuchsian class has algebraic solutions if and only if its monodromy group is a finite subgroup of $SL(n, \boldsymbol{C})$ [**Jo**], [**Gr**, Chapter 3], [**Po**, pp.45–46]. Hence it fell on the shoulders of group theorists to list all finite subgroups of $SL(n, \boldsymbol{C})$, at least when n is small.

It was solved by Jordan and Klein to classify all finite subgroups in $SL(n, \boldsymbol{C})$ up to conjugation in the case $n = 2$ [**Suz**, p.404] and by Blichfeldt in the case $n = 3, 4$ [**Bl**], [**Fl1**], [**Fl2**], [**Hö**]. Richard Brauer was absolutely fascinated by this problem, as remarked by Feit [**Fe2**, p.13], that "for a long time Brauer had been intrigued by the work of H. F. Blichfeldt [**Bl**]" (see Ron Solomon's comment also [**So**, p.733]). In recent years this program attracts curiosity of people working on symbolic algebraic computation also.

This question is important not only in the study of pure group theory, but also for the understanding of quotient singularities [**MM**], [**KW**], [**YY**]. Let X be a complex smooth manifold and ω_X be its canonical bundle. Supposing that $\Gamma(X, \omega_X^n) \neq 0$, Kodaira defines the n-th pluricanonical map $\phi_n : X \to \boldsymbol{P}(\Gamma(X, \omega_X^n)^*)$. The manifold X is of general type if ϕ_n is a birational map when n is large enough. Since $\phi_n(X)$ is canonically sitting inside the complex projective space, it is this birational model of X that is studied most of the time [**MS**]. The singularities which occur in $\phi_n(X)$ are called canonical singularities. If $\dim X = 1$, the pluricanonical models are always smooth. If $\dim X = 2$, the canonical singularities are isolated quotient singularities $\boldsymbol{C}^2/G$ where G is some finite subgroup of $SL(2, \boldsymbol{C})$. These points are called rational double points and can be represented locally by hypersurfaces in $\boldsymbol{C}^3$ through the explicit A-D-E equations:

$$
\begin{aligned}
&A_k : x^2 + y^2 + z^{k+1} = 0, \ k \geq 1,\\
&D_k : x^2 + y^2 z + z^{k-1} = 0, \ k \geq 4,\\
&E_6 : x^2 + y^3 + z^4 = 0,\\
&E_7 : x^2 + y^3 + yz^3 = 0,\\
&E_8 : x^2 + y^3 + z^5 = 0.
\end{aligned}
$$

The theory of quotient singularities in higher dimensions has received a lot of attention. Let Γ be a finite subgroup of $GL(n, \boldsymbol{C})$ and $Y_\Gamma = \boldsymbol{C}^n/\Gamma$. An element $g \in \Gamma$ is called a pseudo-reflection if $\operatorname{rank}(g - I) = 1$. A classical theorem of Shephard-Todd-Chevalley asserts that Y_Γ is smooth if and only if Γ is generated by pseudo-reflections [**ST**], [**Ch**], [**Co**]. In general, let Γ_0 be the subgroup of Γ generated by pseudo-reflection elements in Γ, and define $\widehat{\Gamma} = \Gamma/\Gamma_0$. Then it is clear that $Y_\Gamma = Y_{\Gamma_0}/\widehat{\Gamma}$; moreover, the group $\widehat{\Gamma}$ is a small subgroup, i.e. it has no pseudo-reflection element.

The dualizing sheaf ω_{Y_Γ} of a quotient singularity Y_Γ is studied by Watanabe: If Γ is a small subgroup of $GL(n, \boldsymbol{C})$, then Y_Γ is Gorenstein if and only if $\Gamma \subset SL(n, \boldsymbol{C})$ [**Wat**]. In this situation, i.e. $\Gamma \subset GL(n, \boldsymbol{C})$ is a small subgroup, Prill shows that the singular locus of Y_Γ is equal to S/Γ where $S = \{x \in \boldsymbol{C}^n : g(x) = x \text{ for some } g \in \Gamma \setminus \{I\}\}$ [**Pr**]. As a corollary, if Γ is a small cyclic group of order N, then Y_Γ has an isolated singularity if and only if all the eigenvalues of a generator of Γ consist of primitive n-th roots of unity. If $n \geq 3$, Schlessinger shows that an isolated singularity of $\boldsymbol{C}^n/\Gamma$ is rigid, and therefore it can never be a hypersurface singularity [**Sc**]. On the other hand, Kac and Watanabe show that a quotient singularity is not isolated if $n \geq 3$ [**KW**]. In short, it is crucial to know what finite subgroups of $SL(n, \boldsymbol{C})$ and $GL(n, \boldsymbol{C})$ look like in the study of quotient singularities. For other applications, see [**Ro**], [**BKR**], [**GM**] and the references therein.

Now let's return to the classification of subgroups in $SL(n, \boldsymbol{C})$ for small values of n. In his approach [**Bl**], Blichfeldt considered the reducible and irreducible finite subgroups in $SL(3, \boldsymbol{C})$ (resp. $SL(4, \boldsymbol{C})$) separately. For the irreducible groups, he considered the primitive groups and imprimitive groups (see Definition 1.1). There are three classes of finite primitive groups: (i) those groups in which all the proper normal subgroups are reducible; (ii) those groups with an irreducible imprimitive normal subgroup; (iii) those groups with an irreducible primitive normal subgroup. We may find finite subgroups in $GL(n, \boldsymbol{C})$ through our knowledge for finite subgroups in $SL(n, \boldsymbol{C})$ by the method of A. M. Cohen in [**Co**, (3.1), p.392]. Since $SL(n, \boldsymbol{C})$ contains no pseudo-reflections, the quotient singularities associated with finite subgroups of $SL(n, \boldsymbol{C})$ are always Gorenstein by Watanabe's Theorem [**Wat**].

Many techniques and results of Blichfeldt may be generalized to linear groups of degree ≥ 5 [**Br1**], [**Wa1**], [**Wa2**], [**Wa3**], [**BZ**]. In fact, it is possible to get concrete information for linear groups of prime degree [**Li**], [**Si**], [**Su**], [**DZ1**], [**DZ2**], [**TZ**], [**Zh1**]. The purpose of this article is to find, by listing a set of generators, all the finite primitive subgroups G in $SL(p, \boldsymbol{C})$ with p an odd prime number such that G contains a monomial normal subgroup H so that H has a non-scalar diagonal matrix. Note that a (qualitative) description of these groups were already known and can be found in [**Si**], [**DZ1**]; we will emphasize that our goal is an explicit exhibition of these groups in terms of generators.

Before stating our main results, we will clarify some notions first. Throughout this paper, p denotes an odd prime number. Two finite subgroups G_1 and G_2 in $SL(p, \boldsymbol{C})$ are called equivalent, if there exists some $g \in SL(p, \boldsymbol{C})$ such that $G_2 = gG_1g^{-1}$. A general program initiated by Jordan, Klein and Blichfeldt is to find a complete list of all the non-equivalent finite subgroups in $SL(n, \boldsymbol{C})$ by exhibiting their generators, when n is a small positive integer.

DEFINITION 1.1. Given $SL(n, \boldsymbol{C})$, take $x_0, x_1, \ldots, x_{n-1}$ to be the standard basis and denote $V = \oplus_{0 \le i \le n-1} \boldsymbol{C} \cdot x_i$ so that we get an isomorphism between $SL(n, \boldsymbol{C})$ and $SL(V)$ via this basis $x_0, \ldots, x_{n-1}$.

A finite subgroup $G \subset SL(n, \boldsymbol{C})$ is called *imprimitive* if G is irreducible and there exists a decomposition $V = V_1 \oplus \cdots \oplus V_r$ of V into a direct sum of proper subspaces $V_i \neq 0$, $1 \le i \le r$ such that the action of any $g \in G$ on V induces a permutation on the set $\{V_i \mid 1 \le i \le r\}$.

A finite subgroup $G \subset SL(n, \boldsymbol{C})$ is called *primitive* if G is irreducible and is not imprimitive.

If we choose a fixed basis for V, we will call an imprimitive subgroup of $GL(n, \boldsymbol{C})$ a monomial group if all the imprimitivity subspaces are one-dimensional. Specifically a monomial group $G \subset SL(n, \boldsymbol{C})$ is irreducible and consists of matrices, where each row (resp. column) has only one non-zero entry (remember that we choose the standard basis $x_0, x_1, \ldots, x_{n-1}$ to be the basis for presenting matrices of $SL(n, \boldsymbol{C})$).

In order to have a better perspective of the question we investigate in this paper, we will review some previously known results.

THEOREM 1.2 (Blichfeldt [**Bl**, p.106], [**YY**, p.18]). *Let G be a finite primitive subgroup in $SL(3, \boldsymbol{C})$ such that G contains a monomial normal subgroup. Then G is equivalent to one of the following three groups,*

(i) *G_1 is a group of order* 108 *generated by*

$$S = \begin{pmatrix} 1 & & \\ & \omega & \\ & & \omega^2 \end{pmatrix}, \quad T = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad V = \frac{1}{\sqrt{-3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$$

where ω is a primitive cubic root of unity;

(ii) *G_2 is a group of order* 216 *generated by G_1 and*

$$W = \frac{1}{\sqrt{-3}} \begin{pmatrix} 1 & 1 & \omega^2 \\ 1 & \omega & 1 \\ \omega & 1 & 1 \end{pmatrix};$$

(iii) *G_3 is a group of order* 648 *generated by G_1 and*

$$U = \begin{pmatrix} \xi & & \\ & \xi & \\ & & \xi\omega \end{pmatrix}$$

where ξ is a primitive 9-th root of unity satisfying $\xi^3 = \omega^2$.

THEOREM 1.3. *Let G be a finite primitive subgroup in $SL(p, \boldsymbol{C})$ containing a non-trivial monomial normal subgroup.*

(1) (Brauer [**Br1**, (9A)]) *If $p = 5$, then G is equivalent to either* (i) *G_0, a uniquely determined group of order $5^4 \cdot 24$ whose Sylow 5-subgroups are not abelian, and which contains a normal subgroup D of order 5^3 and exponent 5, or* (ii) *a certain subgroup of G_0 in* (i) *with D as its Sylow 5-subgroup.*

(2) (Wales [**Wa2**, Theorem 4.1]) *If $p = 7$, then G is equivalent to either* (i) *G_0, a uniquely determined group of order $7^4 \cdot 48$ whose Sylow 7-subgroups are not abelian, and which contains a normal subgroup D of order 7^3 and exponent 7 satisfying $G_0/D \simeq SL(2, \boldsymbol{F}_7)$; or* (ii) *a certain subgroup of G_0 in* (i) *with D as its Sylow 7-subgroup.*

THEOREM 1.4 (Dixon and Zalesski [**DZ1**, Lemma 1.1]). *Let G be a finite primitive subgroup of $SL(p, \boldsymbol{C})$ and Z be its center. Let S be the socle of G/Z. If S is an elementary abelian p-group of order p^2, then G/Z is isomorphic to a subgroup of $SL(p, \boldsymbol{C})$ which is a split extension of S by $SL(2, \boldsymbol{F}_p)$.*

In the above theorem, the extension of S by $SL(2, \boldsymbol{F}_p)$ was explained in [**DZ1**, p.126, the fourth paragraph]; see [**Si**, Theorem 1] also. For applications to problems in geometry, the goal of this article is to provide a more explicit description of the group G beyond the qualitative information (see Theorems 2.5, 2.6, 2.7, Summary and Example 8.14 at the end of Section 8). In particular, see the appendix for a list of generators of these subgroups (there are precisely six non-equivalent such groups if $p = 5$, and precisely eleven such groups if $p = 7$). Our proof will not assume previous knowledge of results in [**Si**], [**DZ1**], [**Su**]. We remark that, in Theorem 1.4 if the socle S is not an elementary abelian p-group of order p^2, then it is a non-abelian simple group and its structure is depicted in [**DZ1**, Theorem 1.2] (see also the remark of Proposition 2.3).

In this article, we will denote by p an odd prime number. $\boldsymbol{F}_p \simeq \boldsymbol{Z}_p$ is the finite field with p elements and $\zeta = e^{2\pi\sqrt{-1}/p}$ is a primitive p-th root of unity. S_n, $GL(n, \boldsymbol{F}_p)$ and $PGL(n, \boldsymbol{F}_p)$ denote the symmetric group on n letters, the general linear group and the projective linear group over $\boldsymbol{F}_p$ respectively. We emphasize that a monomial (or imprimitive) group in $SL(p, \boldsymbol{C})$ is necessarily irreducible.

2. Main results.

In Blichfeldt's proof, the invariant triangles were crucial in determining the group structure [**Bl**, p.105], [**YY**, p.18]. Unfortunately Blichfeldt talked about them in passing without taking the trouble to provide a formal definition. Here is a notion which will play the same role as invariant triangles in our case.

DEFINITION 2.1. Let Γ be a finite monomial subgroup of $GL(n, \boldsymbol{C})$ and $U = \oplus_{0\le i\le n-1} \boldsymbol{C}\cdot x_i$, where $x_0, x_1, \ldots, x_{n-1}$ is the standard basis. A Γ-polygon $\Delta = \{v_0, v_1, \ldots, v_{n-1}\}$ is a set of n vectors in U satisfying (i) $U = \sum_{0\le i\le n-1} \boldsymbol{C}\cdot v_i$, and (ii) for any $g \in \Gamma$, any $0 \le i \le n-1$, $g\cdot v_i \in \boldsymbol{C}v_j$ for some j. Two Γ-polygons $\{v_0, v_1, \ldots, v_{n-1}\}$ and $\{\lambda_0 v_0, \lambda_1 v_1, \ldots, \lambda_{n-1} v_{n-1}\}$, $\lambda_i \in \boldsymbol{C}\setminus\{0\}$, will be regarded as the same Γ-polygon.

From the definition, $\{x_0, x_1, \ldots, x_{n-1}\}$ is a Γ-polygon. We will show that there are only finitely many Γ-polygons (see Lemma 3.1).

DEFINITION 2.2. Let $x_0, x_1, \ldots, x_{p-1}$ be the standard basis. We will define $\sigma, \tau, \lambda_d \in SL(p, \boldsymbol{C})$ by

$$\begin{aligned} \sigma &: x_j \mapsto x_{j+1}, \\ \tau &: x_j \mapsto \zeta^j x_j, \\ \lambda_d &: x_j \mapsto \varepsilon x_{dj} \end{aligned}$$

where $d \not\equiv 0 \pmod p$, $0 \le j \le p-1$, and $\varepsilon \in \boldsymbol{C}\setminus\{0\}$ is adjusted to ensure $\det(\lambda_d) = 1$. In particular, we require $\varepsilon = 1$ or -1.

The following Proposition, although it will not be used anywhere in this paper, shows that our assumptions are equivalent to those of Dixon and Zalesski in Theorem 1.4 [**DZ1**, Lemma 1.1]. Its proof relies on the validity of Lemmas 3.7 and 3.8 to be proved later; we include this Proposition and its proof here for the convenience of the reader.

PROPOSITION 2.3. *Let G be a finite primitive subgroup in $SL(p, \boldsymbol{C})$. Then the followings are equivalent.*

(1) *G contains a monomial normal subgroup H so that H has a non-scalar diagonal matrix.*

(2) *If S is the socle of G/Z with Z being the center of G, then S is an elementary abelian group of order p^2.*

PROOF. (1) $\Rightarrow$ (2) By Lemma 3.7 and Lemma 3.8 D is an extra-special group of order p^3, and $D \triangleleft G$. Hence the socle of G/Z is not a non-abelian simple

group. Apply [**DZ1**].

(2) $\Rightarrow$ (1) From the proof of [**DZ1**, Lemma 1.1], there exists a normal subgroup S_0 in G such that S_0 is an extra-special group of order p^3. Hence S_0 is equivalent to a monomial group containing a non-scalar diagonal matrix. $\square$

REMARK. In a previous version we even tried to prove that any one statement in Proposition 2.3 is equivalent to a weaker condition that G contains a non-trivial monomial normal subgroup H (such a subgroup is not contained in the center of G, because H is irreducible by Definition 1.1), using [**DZ1**, Theorem 1.2] and the classification of finite simple groups. We thank Zalesski for communicating one of us that the list in [**DZ1**, Theorem 1.2] missed some groups (e-mail to J. Zhang, 28 Feb. 2007).

DEFINITION 2.4. Let $x_0, x_1, \ldots, x_{p-1}$ be the standard basis. We will define $p+1$ sets $\Delta_\infty, \Delta_0, \ldots, \Delta_{p-1}$ as follows.

$$\Delta_\infty = \{x_0, x_1, \ldots, x_{p-1}\};$$
$$\Delta_0 = \{u_0, u_1, \ldots, u_{p-1}\}, \text{ where } u_j = \sum_{0\le\ell\le p-1} \zeta^{j\ell} x_\ell \text{ for } 0 \le j \le p-1;$$
$$\Delta_i = \{v_0, v_1, \ldots, v_{p-1}\}, \text{ where } 1 \le i \le p-1 \text{ and}$$
$$v_0 = \sum_{0\le\ell\le p-1} \zeta^{i\binom{\ell}{2}} x_\ell,\ v_j = \sigma^j(v_0) = \sum_{0\le\ell\le p-1} \zeta^{i\binom{\ell}{2}} x_{\ell+j}$$

for $1 \le j \le p-1$.

We will prove that they are all the D-polygons for some monomial group $D \subset SL(p, \boldsymbol{C})$.

The following Theorems 2.5–2.7 are the main tools of finding explicit generators of all the primitive groups $G \subset SL(p, \boldsymbol{C})$ with monomial normal subgroups (containing a non-scalar diagonal matrix). In fact, use Theorems 2.6 and 2.7 first, and reduce the question to finding the conjugacy classes of some subgroups in $SL(2, \boldsymbol{F}_p)$, which will be explained more precisely in Lemma 7.2 and Theorem 7.5. Then we may apply Theorem 2.5 to achieve our goal. A detailed strategy of solving this question will be given in Section 8. A list of these groups will be provided in the Appendix when $p = 5$ or 7.

THEOREM 2.5. *Let $G' \subset SL(p, \boldsymbol{C})$ be a finite primitive subgroup such that G' has a monomial normal subgroup H' containing a non-scalar diagonal matrix. Then G' is equivalent to a group $G \subset SL(p, \boldsymbol{C})$ with the following properties.*

(A) *G contains the subgroup $D = \langle \sigma, \tau \rangle$ as a normal subgroup.*

(B) *$\Delta_\infty, \Delta_0, \ldots, \Delta_{p-1}$ are all the D-polygons.*

(C) *The group G acts on the set $\{\Delta_\infty, \Delta_0, \ldots, \Delta_{p-1}\}$ by $g(\Delta_i) := \{g(w_0), g(w_1), \ldots, g(w_{p-1})\}$ for any $g \in G$, where $i \in \{\infty, 0, 1, \ldots, p-1\}$ and $\Delta_i = \{w_0, w_1, \ldots, w_{p-1}\}$.*

(D) *The group action of G in* (C) *induces a non-trivial group homomorphism $\phi : G \to PGL(2, \boldsymbol{F}_p)$ with $\mathrm{Ker}(\phi) = \langle \sigma, \tau \rangle$ or $\langle \sigma, \tau, \lambda_{p-1} \rangle$ according to whether $\lambda_{p-1} \notin G$ or $\lambda_{p-1} \in G$. Denote $H_0 = \mathrm{Ker}(\phi)$.*

(E) *For any $g \in G$, if $\phi(g)$ is known, then some element ρ may be described explicitly, where $g \in \rho \cdot \mathrm{Ker}(\phi)$. More explicitly, if $g \in G$ satisfies*

(i) *$g : \Delta_\infty \mapsto \Delta_\infty$, $\Delta_0 \mapsto \Delta_0$, then there exist $\rho \in gH_0$ and some integer $k \not\equiv 0 \pmod p$ such that*

$$\rho : x_\ell \mapsto \varepsilon \cdot x_{k\ell}$$

for $0 \le \ell \le p-1$, $\varepsilon \in \boldsymbol{C} \setminus \{0\}$, and $\phi(\rho) \in PGL(2, \boldsymbol{F}_p)$ is the map $x \mapsto k^{-2}x$, where $x = 0, 1, 2, \ldots, p-1, \infty$; or

(ii) *$g : \Delta_\infty \mapsto \Delta_\infty$, $\Delta_0 \mapsto \Delta_i$ for some $1 \le i \le p-1$, then there exist $\rho \in gH_0$ and some integer $k \not\equiv 0 \pmod p$ such that*

$$\rho : x_\ell \mapsto c\,\zeta^{i\binom{k\ell}{2}} x_{k\ell}$$

for $0 \le \ell \le p-1$, $c \in \boldsymbol{C} \setminus \{0\}$, and $\phi(\rho) \in PGL(2, \boldsymbol{F}_p)$ is the map $x \mapsto k^{-2}x + i$, where $x = 0, 1, \ldots, p-1, \infty$; or

(iii) *$g : \Delta_\infty \mapsto \Delta_0 \mapsto \Delta_\infty$, then there exist $\rho \in gH_0$ and some integer $k \not\equiv 0 \pmod p$ such that*

$$\rho : x_\ell \mapsto c \cdot \sum_{0 \le \ell' \le p-1} \zeta^{k\ell\ell'} x_{\ell'}$$

for $0 \le \ell \le p-1$, $c \in \boldsymbol{C} \setminus \{0\}$, and $\phi(\rho) \in PGL(2, \boldsymbol{F}_p)$ is the map $x \mapsto -k^2/x$, where $x = 0, 1, \ldots, p-1, \infty$; or

(iv) *$g : \Delta_\infty \mapsto \Delta_0 \mapsto \Delta_i$ for some $1 \le i \le p-1$, then there exist $\rho \in gH_0$ and some integer $k \not\equiv 0 \pmod p$ such that*

$$\rho : x_\ell \mapsto c\,\zeta^{-i\binom{-i^{-1}k\ell}{2}} \sum_{0 \le \ell' \le p-1} \zeta^{k\ell\ell'} x_{\ell'}$$

for $0 \le \ell \le p-1$, $c \in \boldsymbol{C} \setminus \{0\}$, and $\phi(\rho) \in PGL(2, \boldsymbol{F}_p)$ is the map $x \mapsto i/(1 - k^{-2}ix)$, where $x = 0, 1, \ldots, p-1, \infty$; or

(v) *$g : \Delta_\infty \mapsto \Delta_i \mapsto \Delta_\infty$ for some $1 \le i \le p-1$, then there exist $\rho \in gH_0$ and*

some integer $k \not\equiv 0 \pmod{p}$ *such that*

$$\rho : x_\ell \mapsto c\,\zeta^{-i\binom{\ell}{2}-i\binom{-k\ell}{2}} \sum_{0\le \ell' \le p-1} \zeta^{i\binom{\ell'}{2}} x_{\ell'+k\ell}$$

for $0 \le \ell \le p-1$, $c \in \boldsymbol{C} \setminus \{0\}$ *and* $\phi(\rho) \in PGL(2, \boldsymbol{F}_p)$ *is the map* $x \mapsto (ix - i^2k^2 - i^2)/(x - i)$, *where* $x = 0, 1, \ldots, p-1, \infty$; *or*

(vi) $g : \Delta_\infty \mapsto \Delta_i \mapsto \Delta_0$ *for some* $1 \le i \le p-1$, *then there exist* $\rho \in gH_0$ *and some integer* $k \not\equiv 0 \pmod{p}$ *such that*

$$\rho : x_\ell \mapsto c\,\zeta^{-i\binom{\ell}{2}} \sum_{0\le \ell' \le p-1} \zeta^{i\binom{\ell'}{2}} x_{\ell'+k\ell}$$

for $0 \le \ell \le p-1$, $c \in \boldsymbol{C} \setminus \{0\}$ *and* $\phi(\rho) \in PGL(2, \boldsymbol{F}_p)$ *is the map* $x \mapsto (ix - i^2)/(x + ik^2 - i)$; *or*

(vii) $g : \Delta_\infty \mapsto \Delta_i \mapsto \Delta_j$ *for some* $1 \le i \ne j \le p-1$, *then there exist* $\rho \in gH_0$ *and some integer* $k \not\equiv 0 \pmod{p}$ *such that*

$$\rho : x_\ell \mapsto c\,\zeta^{\frac{1}{2}[\ell^2(\frac{i^2k^2}{i-j}-i-ik^2)+i\ell]} \sum_{0\le \ell' \le p-1} \zeta^{i\binom{\ell'}{2}} x_{\ell'+k\ell}$$

for $0 \le \ell \le p-1$, $c \in \boldsymbol{C} \setminus \{0\}$ *and* $\phi(\rho) \in PGL(2, \boldsymbol{F}_p)$ *is the map* $x \mapsto (ix + \delta j - i^2)/(x + \delta - i)$, *where* $\delta = (i-j)^{-1}i^2k^2$.

REMARKS. In the explicit formula of ρ of Part (E), there are two parameters $c \in \boldsymbol{C} \setminus \{0\}$ and $k \not\equiv 0 \pmod{p}$. It is understood that c is adjusted to ensure that $\rho \in SL(p, \boldsymbol{C})$, and (according to the following Theorem 2.6) k should be chosen to guarantee that the "determinant" of the fractional linear transformation $\phi(\rho) \in PGL(2, \boldsymbol{F}_p)$ is 1.

THEOREM 2.6. *Keep the assumptions and notation in Theorem* 2.5.

(1) *For any* $g \in G$, $\phi(g) \in PSL(2, \boldsymbol{F}_p)$; *thus we may regard* ϕ *as a map from* G *to* $PSL(2, \boldsymbol{F}_p)$.

(2) *For any* $g \in G$, *if* $g \cdot \tau \cdot g^{-1} = \zeta^r \tau^a \sigma^c$, $g \cdot \sigma \cdot g^{-1} = \zeta^s \tau^b \sigma^d$ *for some* $a, b, c, d, r, s \in \boldsymbol{F}_p$, *define*

$$\Phi(g) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \boldsymbol{F}_p).$$

Then $\Phi(g) \in SL(2, \boldsymbol{F}_p)$; *and therefore* $\Phi : G \to SL(2, \boldsymbol{F}_p)$ *is a well-defined group homomorphism with* $\mathrm{Ker}(\Phi) = D$.

(3) *If* $\pi_0 : SL(2, \boldsymbol{F}_p) \to PSL(2, \boldsymbol{F}_p)$ *is the canonical projection, then* $\pi_0\Phi = \phi$.

THEOREM 2.7. *Keep the assumptions and notation in Theorem* 2.5. *Define* $\rho_1, \rho_2, \rho_3 \in SL(p, \boldsymbol{C})$ *by*

$$\begin{aligned}
&\rho_1 : x_\ell \mapsto c_1\, \zeta^{\binom{\ell}{2}} x_\ell,\\
&\rho_2 : x_\ell \mapsto c_2 \cdot \sum_{0 \le \ell' \le p-1} \zeta^{\ell\ell'} x_{\ell'},\\
&\rho_3 : x_\ell \mapsto c_3\, x_{h\ell},
\end{aligned}$$

where h *is a generator of* $\boldsymbol{F}_p^\times$ *and* $c_1, c_2, c_3 \in \boldsymbol{C} \setminus \{0\}$.

(1) *Let* G_0 *be the subgroup of* $SL(p, \boldsymbol{C})$ *generated by* D *and* ρ_1, ρ_2, ρ_3. *Then* G_0 *is a primitive group of order* $p^4(p^2-1)$ *containing a monomial normal subgroup* H *which has a non-scalar diagonal matrix.*

(2) *Let* $G' \subset SL(p, \boldsymbol{C})$ *be any finite primitive subgroup such that* G' *has a monomial normal subgroup* H' *containing a non-scalar diagonal matrix. Then* G' *is equivalent to a subgroup* G *of* G_0 *such that* G *contains* D. *Moreover, if* p^4 *divides the order of* G, *then* $G = G_0$; *if* p^4 *doesn't divide the order of* G, *then* G *is a semi-direct product of* D *and a subgroup of* $SL(2, \boldsymbol{F}_p)$.

One crucial tool in our proof of these theorems is the notion of Γ-polygons for a monomial group $\Gamma \subset SL(n, \boldsymbol{C})$ (see Definition 2.1). Roughly speaking, a Γ-polygon is simply a decomposition of an n-dimensional space into a direct sum of some one-dimensional eigenspaces. In other words, a Γ-polygon corresponds to an index n subgroup D of Γ with a one-dimensional D-eigenspace. Another tool is a formula of Gauss sum $\sum_{0 \le \ell \le p-1} \zeta^{\ell^2}$, which helps to find the explicit formulas of elements in G (see Theorem 4.5 and the proof of Theorem 2.5 in Section 6).

We will explain briefly the ideas of our proof. Let $G \subset SL(p, \boldsymbol{C})$ be a finite primitive subgroup containing a monomial normal group H such that H has a non-scalar diagonal matrix. We consider the projection $\pi : H \to S_p$, where $\pi(h)(i) = j$ if and only if $h(x_i) \in \boldsymbol{C} \cdot x_j$ for $0 \le i \le p-1$. Since H is normal in G and G is primitive, H has at least two H-polygons. Using H-polygons, we may determine explicitly elements in $\mathrm{Ker}(\pi)$ (see Lemma 3.7). With the conjugation action of H on $\mathrm{Ker}(\pi)$ we find that H is solvable (see Lemma 3.8). Hence $\pi(H)$ is a transitive solvable subgroup in S_p; and therefore we know what it looks like. In particular, its Sylow p-subgroup is normal. Thus the preimage of this subgroup

under π, denoted by D, is the unique Sylow p-subgroup of H. It follows that D is a monomial normal subgroup of G; it is the maximal normal p-subgroup studied in [**Br1**].

D is an extra-special group of order p^3. If Z is the center of G, then D/Z is the socle of G/Z in the paper by Dixon and Zalesski [**DZ1**]. With the aid of D and D-polygons, it is possible to find the generators of H. However, we adopt another approach. Because D is monomial normal and contains a non-scalar diagonal matrix, D itself is a "legal" candidate of H. Thus it is unnecessary to find other monomial normal subgroup containing D.

Now consider the conjugation action of G on D/Z. Since D/Z may be regarded as a 2-dimensional vector space over $\boldsymbol{F}_p$, we get a representation of G to $GL(2, \boldsymbol{F}_p)$. Descending to $PGL(2, \boldsymbol{F}_p)$, we get the homomorphism $\phi : G \to PGL(2, \boldsymbol{F}_p)$. This homomorphism induces an action of G on the set of D-polygons. The action of G on these D-polygons is just the same as that described in Theorem 2.5(C). We will proceed to prove Theorem 2.5. For any two points $i, j \in \boldsymbol{P}^1(\boldsymbol{F}_p) = \{0, 1, \ldots, p-1, \infty\}$, if we know the images of $g(\Delta_i)$ and $g(\Delta_j)$, it is possible to obtain an explicit form of some element $\rho \in g \cdot \mathrm{Ker}(\phi)$. In determining the explicit form of ρ, a lot of "tedious" computations are required. It is amid these computations that the formula of Gauss sum comes to the rescue. As a by-product, we find that $\phi(G)$ is a subgroup of $PSL(2, \boldsymbol{F}_p)$; thus we get a homomorphism $\phi : G \to PSL(2, \boldsymbol{F}_p)$. Better than it is that this map $\phi : G \to PSL(2, \boldsymbol{F}_p)$ can be lifted to a map $\Phi : G \to SL(2, \boldsymbol{F}_p)$ so that the associated action of G is equivariant to the aforementioned action of G on D/Z. It is not difficult to find that the kernel of Φ is D.

However we take a slightly different way in the presentation of this paper for this action of G. We study the D-polygons in Section 4. The action of G on these D-polygons is defined as in Theorem 2.5(C) and Lemma 3.3. Thus we get a group homomorphism $\phi : G \to PGL(2, \boldsymbol{F}_p)$ as in Theorem 2.5(D). It will be explained in Section 5 that this action is just the conjugation action of G on D/Z mentioned before. Being armed with this action we will prove Theorem 2.5(E). By Theorem 2.5(E), it can be shown that the image of $\phi : G \to PGL(2, \boldsymbol{F}_p)$ is contained in $PSL(2, \boldsymbol{F}_p)$ and this map can be lifted to $\Phi : G \to SL(2, \boldsymbol{F}_p)$ (see Section 7).

Apparently, the order of the group G is a divisor of $p^4(p^2-1)$, which was anticipated by Brauer and Wales when $p = 5$ or 7 [**Br1**], [**Wa2**]. Moreover, all the subgroups of $SL(2, \boldsymbol{F}_p)$ of the form $\Phi(G)$ can be listed up to conjugation in $SL(2, \boldsymbol{F}_p)$ and the generators of $\Phi(G)$ may be exhibited (see Section 8). Thus we may describe the groups G explicitly by using Theorem 2.5. We will remark that a description of all the subgroups of $SL(2, \boldsymbol{F}_p)$ is usually known as a theorem of Dickson (see Theorem 7.5 or [**Suz**, Theorem, p.404]). What we need is to find all the conjugacy classes of the subgroups and to find a set of generators for a

representative of each conjugacy class, instead of merely a description of these subgroups as abstract groups.

More notation need be introduced (besides those in the last paragraph of Section 1). We will present our results in terms of matrix groups instead of a faithful representation of some group; thus I_n is the $n \times n$ identity matrix and $x_0, x_1, \ldots, x_{p-1}$ is the standard basis. If a is an integer, we denote $\binom{a}{2} = \frac{a(a-1)}{2} \in \boldsymbol{Z}_p$. Note that the simple-minded formula $\binom{a+b}{2} = \binom{a}{2} + \binom{b}{2} + ab$ is quite handy in Section 6. If a is an integer with $a \not\equiv 0 \pmod{p}$, $\left(\frac{a}{p}\right)$ denotes the Legendre symbol.

3. Determining the structure of monomial normal subgroups.

LEMMA 3.1. *Let Γ be a finite monomial group in $GL(n, \boldsymbol{C})$.*

(1) *If $\Delta = \{u_0, u_1, \ldots, u_{n-1}\}$ is a Γ-polygon, then the subgroup $\Gamma_0 := \{g \in \Gamma : g(u_0) \in \boldsymbol{C} \cdot u_0\}$ is of index n in Γ.*

(2) *If Γ_0 is a subgroup Γ of index n and Γ_0 has a "generalized eigenvector", i.e. a non-zero vector v satisfying $g(v) \in \boldsymbol{C} \cdot v$ for any $g \in \Gamma_0$, then the orbit of $\boldsymbol{C} \cdot v$ under Γ forms a Γ-polygon.*

(3) *There is a one-to-one correspondence between the set of Γ-polygons and the set of conjugacy classes of subgroups Γ_0 of Γ satisfying the properties* (i) *$[\Gamma : \Gamma_0] = n$, and* (ii) *Γ_0 has a "generalized eigenvector". In particular, there are only finitely many Γ-polygons.*

PROOF. We will prove (1) only and leave the proof of (2) and (3) to the reader.

For the proof of (1), if $[\Gamma : \Gamma_0] < n$, then the orbit of u_0 under Γ contains less than n elements. Since the subspaces in an orbit of Γ generate a Γ-invariant subspace, this will be a contradiction to the assumption that Γ is irreducible. □

From now on we will consider finite subgroups in $SL(p, \boldsymbol{C})$. Remember that $x_0, x_1, \ldots, x_{p-1}$ denotes the standard basis.

LEMMA 3.2. *If $\widetilde{G}$ is a finite primitive subgroup of $SL(p, \boldsymbol{C})$ such that $\widetilde{G}$ has a monomial normal subgroup $\widetilde{H}$ containing a non-scalar diagonal matrix, then there exists some element $g \in SL(p, \boldsymbol{C})$ satisfying* (i) *$g^{-1}\widetilde{H}g$ is a monomial group,* (ii) *$\sigma \in g^{-1}\widetilde{H}g$ (see Definition 2.2 for σ), and* (iii) *$g^{-1}\widetilde{H}g$ contains a non-scalar diagonal matrix.*

PROOF. Consider the map $\pi' : \widetilde{H} \to S_p$ defined by $\pi'(g)(i) = j$ if and only if $g(x_i) \in \boldsymbol{C} \cdot x_j$ for $0 \le i \le p-1$. Since $\widetilde{H}$ is irreducible, the image $\pi'(\widetilde{H})$ is a transitive subgroup of S_p. We may assume that the p-cycle $(0, 1, \ldots, p-1)$

belongs to $\pi(\widetilde{H})$ if we reindex $x_0, x_1, \ldots, x_{p-1}$ when necessary. Find $\sigma' \in \widetilde{H}$ so that $\pi'(\sigma') = (0, 1, \ldots, p-1)$, i.e. $\sigma'(x_j) \in \boldsymbol{C}x_{j+1}$. Define $x'_0 = x_0$ and $x'_j = \sigma'(x'_{j-1})$ inductively for $1 \le j \le p-1$.

Then $\sigma' : x'_0 \mapsto x'_1 \mapsto x'_2 \mapsto \cdots \mapsto x'_{p-1} \mapsto cx'_0$ for some $c \in \boldsymbol{C} \setminus \{0\}$. Since $\det(\sigma') = 1$, it follows that $c = 1$. Define $g \in SL(p, \boldsymbol{C})$ by $g(x_j) = dx'_j$, for $0 \le j \le p-1$ and $d \in \boldsymbol{C} \setminus \{0\}$ is chosen to ensure that $\det(g) = 1$. It is not difficult to verify that $g^{-1}\widetilde{H}g$ is a monomial group, $\sigma \in g^{-1}\widetilde{H}g$ and $g^{-1}\widetilde{H}g$ contains a non-scalar diagonal matrix. □

CONVENTION. From now on, G and H are the groups defined as: $G = g^{-1}\widetilde{G}g$ and $H = g^{-1}\widetilde{H}g$ in the above lemma. Thus G and H satisfy the properties (i) G is a finite primitive subgroup of $SL(p, \boldsymbol{C})$, (ii) H is a monomial normal subgroup of G, (iii) $\sigma \in H$, and (iv) H contains a non-scalar diagonal matrix. We will define $\pi : H \to S_p$ by $\pi(h)(i) = j$ if and only if $h(x_i) \in \boldsymbol{C}x_j$ for $0 \le i, j \le p-1$. Define $D = \langle \mathrm{Ker}(\pi), \sigma \rangle$. All these notation will remain in force till the end of this paper, unless otherwise specified.

In the rest of this section we will prove that $\mathrm{Ker}(\pi) = \langle \tau, \zeta I_p \rangle$; in particular, τ and ζI_p belong to H.

LEMMA 3.3. *For any $g \in G$ and any H-polygon $\Delta = \{u_0, u_1, \ldots, u_{p-1}\}$, define $g(\Delta) = \{g(u_0), g(u_1), \ldots, g(u_{p-1})\}$.*

(1) *$g(\Delta)$ is an H-polygon. In particular, the group G acts on the set of all H-polygons.*

(2) *There are at least two H-polygons. Thus there are at least two D-polygons also.*

PROOF. (1) For any $h \in H$, we will show that $h(g(u_i)) \in \boldsymbol{C} \cdot g(u_j)$ for some j. Since $g^{-1}hg \in H$, it follows that $h(g(u_i)) = g(g^{-1}hg)(u_i) = g(g^{-1}hg(u_i)) = g(\lambda \cdot u_j)$ for some j and some $\lambda \in \boldsymbol{C} \setminus \{0\}$. Thus $h(g(u_i)) = \lambda \cdot g(u_j)$.

(2) Assume that there is only one H-polygon. Thus $\Delta = \{x_0, x_1, \ldots, x_{p-1}\}$ is the unique H-polygon. From (1), $g(\Delta) = \Delta$ for any $g \in G$. Thus $g(x_i) = \lambda_i x_j$ for some j and some $\lambda_i \in \boldsymbol{C} \setminus \{0\}$, i.e. G is a monomial group, which contradicts with the assumption that G is primitive. □

LEMMA 3.4. *Let $\Delta = \{u_0, u_1, \ldots, u_{p-1}\}$ be a D-polygon. If $\sigma(u_i) \in \boldsymbol{C}u_i$ for some $0 \le i \le p-1$, then $\Delta = \{\sum_{0 \le \ell \le p-1} \zeta^{i\ell} x_\ell : 0 \le i \le p-1\}$.*

PROOF. The cyclic group $\langle \sigma \rangle$ acts on the set $\{\boldsymbol{C}u_i : 0 \le i \le p-1\}$. If it has a fixed point, then the action is trivial because any σ-orbit in the set has length 1 or p. Thus, if $\sigma(u_i) \in \boldsymbol{C}u_i$ for some i, then $\sigma(u_j) \in \boldsymbol{C}u_j$ for any $0 \le j \le p-1$. It

follows that $u_0, u_1, \ldots, u_{p-1}$ are linearly independent eigenvectors of σ. However, all the eigenvectors of σ (up to a scalar) are of the form $\sum_{0\le\ell\le p-1}\zeta^{i\ell}x_\ell$ for some $0 \le i \le p-1$. □

DEFINITION 3.5. Let $\Delta = \{v_0, v_1, \ldots, v_{p-1}\}$ be a D-polygon so that $\sigma(v_i) \notin \boldsymbol{C}v_i$ for any $0 \le i \le p-1$. Since the σ-orbit containing $\boldsymbol{C}v_0$ is of length p, this orbit is just $\{\boldsymbol{C}v_j : 0 \le j \le p-1\}$. Thus, after reindexing $v_0, v_1, \ldots, v_{p-1}$, we may assume that $\sigma \cdot v_j \in \boldsymbol{C}v_{j+1}$. Define a map $\pi_\Delta : D \to S_p$ by $\pi_\Delta(h)(i) = j$ if and only if $h(v_i) \in \boldsymbol{C}v_j$ for $0 \le i \le p-1$. We find that $\pi_\Delta(\sigma) = (0, 1, \ldots, p-1)$.

Recall the definition of $\Delta_\infty, \Delta_0, \Delta_1, \ldots, \Delta_{p-1}$ in Definition 2.4.

LEMMA 3.6. *Let $\Delta = \{v_0, v_1, \ldots, v_{p-1}\}$ be a D-polygon and $\Delta \ne \Delta_\infty$. Assume that $\sigma(v_i) \notin \boldsymbol{C}v_i$ for any $0 \le i \le p-1$.*

(1) *$\pi_\Delta(D)$ is the cyclic group generated by $\pi_\Delta(\sigma)$.*

(2) *If $\rho \in \mathrm{Ker}(\pi)$ is a non-scalar matrix, then $\pi_\Delta(\rho)$ is also a generator of $\pi_\Delta(D)$.*

(3) $\mathrm{Ker}(\pi) = \langle \tau, \zeta I_p \rangle$.

PROOF.

Step 1: Note that $\mathrm{Ker}(\pi)$ is abelian, because it consists of diagonal matrices. Thus $D = \langle \mathrm{Ker}(\pi), \sigma \rangle$ is solvable. It follows that $\pi_\Delta(D)$ is a solvable subgroup of S_p. Thus $\pi_\Delta(D)$ is generated by the permutation s_1 and s_2, where $s_1 : x \mapsto x+1$ and $s_2 : x \mapsto dx$ for $0 \le x \le p-1$ and some $d \not\equiv 0 \pmod p$ by [**Coh**, Proposition 11.6, p.117]. Note that $\pi_\Delta(D)$ is abelian if and only if $d \equiv 1 \pmod p$.

Since $\pi_\Delta(\sigma) = (0, 1, \ldots, p-1)$, we find that $\langle \pi_\Delta(\sigma) \rangle$ is normal in $\pi_\Delta(D)$ and $\Delta = \{v_0, \sigma(v_0), \ldots, \sigma^{p-1}(v_0)\}$. If we write $\sigma^i(v_0) = \sum_{0\le j\le p-1} c_{ij}x_j$, where $c_{ij} \in \boldsymbol{C}$, there exists some i so that $c_{i0} \ne 0$. Multiplying $\sigma^i(v_0)$ by a non-zero scalar, we can assume that $c_{i0} = 1$. By abusing the notation we will denote $\sigma^i(v_0)$ by v_0. Write $v_0 = \sum_{0\le j\le p-1} c_j x_j$ and $v_i = \sigma^i(v_0) = \sum_{0\le j\le p-1} c_j x_{j+i}$, where $c_0 = 1$ and $c_j \in \boldsymbol{C}$. Note that the set $\{v_0, v_1, \ldots, v_{p-1}\}$ is a D-polygon equivalent to (i.e. regarded as the same as) the previous one. Thus we call this "new" D-polygon by Δ also.

Step 2: For any $\rho \in \mathrm{Ker}(\pi)$ which is not a scalar matrix, $\pi_\Delta(\rho)$ is not the identity permutation.

For, write $\rho : x_j \mapsto \lambda_j x_j$, where $\lambda_j \in \boldsymbol{C} \setminus \{0\}$ and assume that $\pi_\Delta(\rho)$ is the identity permutation. Then $\rho(v_i) = a_i v_i$ for some $a_i \in \boldsymbol{C} \setminus \{0\}$, i.e. $\sum_j c_j\lambda_{j+i}x_{j+i} = a_i \sum_j c_j x_{j+i}$. Thus $c_j\lambda_{j+i} = a_i c_j$ for any $0 \le j \le p-1$. Since $c_0 = 1$, we find $a_i = \lambda_i$. It follows that $c_j\lambda_{j+i} = \lambda_i c_j$ for any $0 \le i, j \le p-1$. By assumption $\Delta \ne \Delta_\infty$. Thus there is some index ℓ with $1 \le \ell \le p-1$ satisfying that $c_\ell \ne 0$. Hence $\lambda_{\ell+i} = \lambda_i$ for any $0 \le i \le p-1$. It follows that $\lambda_0 = \lambda_\ell = \lambda_{2\ell} = \cdots = \lambda_{(p-1)\ell}$, i.e. $\lambda_0 = \lambda_1 = \cdots =$

λ_{p-1} and ρ is a scalar matrix.

Step 3: There is some non-scalar matrix $\rho \in \mathrm{Ker}(\pi)$ such that $\pi_\Delta(\rho)$ belongs to $\langle \pi_\Delta(\sigma) \rangle$, and thus it is a generator of $\langle \pi_\Delta(\sigma) \rangle$. Hence $\pi_\Delta(D) = \pi_\Delta(\mathrm{Ker}(\pi))$.

Assume that $\pi_\Delta(\rho) \notin \langle \pi_\Delta(\sigma) \rangle$ for any non-scalar matrix $\rho \in \mathrm{Ker}(\pi)$. Then $\pi_\Delta(\mathrm{Ker}(\pi)) \cap \langle \pi_\Delta(\sigma) \rangle = \{\mathrm{id}\}$. Since $\mathrm{Ker}(\pi) \triangleleft D$, it follows that $\pi_\Delta(\mathrm{Ker}(\pi))$ is normal in $\pi_\Delta(D)$. Because both $\langle \pi_\Delta(\sigma) \rangle$ and $\pi_\Delta(\mathrm{Ker}(\pi))$ are normal subgroups, $\pi_\Delta(D)$ is a direct product of $\langle \pi_\Delta(\sigma) \rangle$ and $\pi_\Delta(\mathrm{Ker}(\pi))$. Thus $\pi_\Delta(D)$ is an abelian group. From the structure of $\pi_\Delta(D)$, we find $s_2 = \mathrm{id}$ and thus $\pi_\Delta(D) \langle \pi_\Delta(\sigma) \rangle$. We are led to the conclusion $\pi_\Delta(\rho) \in \langle \pi_\Delta(\sigma) \rangle$ for any non-scalar matrix ρ in $\mathrm{Ker}(\pi)$. A contradiction to the starting assumption.

Thus there is some non-scalar $\rho \in \mathrm{Ker}(\pi)$ such that $\langle \pi_\Delta(\rho) \rangle = \langle \pi_\Delta(\sigma) \rangle$. It follows that $\pi_\Delta(D) = \pi_\Delta(\mathrm{Ker}(\pi))$.

Step 4: Proof of (1) and (2).

Since $\mathrm{Ker}(\pi)$ is abelian, we find that $\pi_\Delta(D)$ is abelian and $s_2 = \mathrm{id}$. Thus we find that $\pi_\Delta(D) = \langle \pi_\Delta(\sigma) \rangle$, which is equal to $\langle \pi_\Delta(\rho) \rangle$ for some non-scalar $\rho \in \mathrm{Ker}(\pi)$.

Now consider any non-scalar matrix ρ in $\mathrm{Ker}(\pi)$. Since $\pi_\Delta(\rho)$ is not the identity permutation, it is also a generator of the cyclic group generated by $\pi_\Delta(\sigma)$.

Step 5: If $\rho \in \mathrm{Ker}(\pi)$ is any non-scalar matrix and $1 \leq k' \leq p-1$, then $\rho^{k'}$ is not a scalar matrix.

For, if $\rho^{k'}$ is a scalar matrix, then $\pi_\Delta(\rho^{k'}) = \mathrm{id}$. On the other hand, $\pi_\Delta(\rho) = \pi_\Delta(\sigma)^k$ for some $1 \leq k \leq p-1$. Thus $\mathrm{id} = \pi_\Delta(\rho^{k'}) = \pi_\Delta(\rho)^{k'} = \pi_\Delta(\sigma)^{kk'}$. Since $\pi_\Delta(\sigma)$ is a p-cycle, this is impossible.

Step 6: If $\rho' \in \mathrm{Ker}(\pi)$ be any non-scalar matrix, then there is some $1 \leq k' \leq p-1$ such that $\rho'^{k'} = \zeta^b \tau^a$, where $1 \leq a, b \leq p-1$. Moreover, $\langle \tau, \zeta I_p \rangle \subset \mathrm{Ker}(\pi)$.

Let $\rho' \in \mathrm{Ker}(\pi)$ be any non-scalar matrix. Then $\pi_\Delta(\rho') = \pi_\Delta(\sigma)^k$ for some $1 \leq k \leq p-1$. Choose k' such that $kk' \equiv 1 \pmod{p}$ and define $\rho = \rho'^{k'}$. Then $\rho \in \mathrm{Ker}(\pi)$ is not a scalar matrix by Step 5 and $\pi_\Delta(\rho) = \pi_\Delta(\sigma) = (0, 1, \ldots, p-1)$.

Write $\rho : x_j \mapsto t_j x_j$ for $0 \leq j \leq p-1$ and $t_j \in \boldsymbol{C} \setminus \{0\}$. Note that $\rho(v_j) = b_j v_{j+1}$ for any $0 \leq j \leq p-1$, where $b_j \in \boldsymbol{C} \setminus \{0\}$. Substitute it into the formula $v_j = \sum_\ell c_\ell x_{\ell+j}$ with $c_0 = 1$. We get $\sum_\ell c_\ell t_{\ell+j} x_{\ell+j} = b_j \sum_\ell c_\ell x_{\ell+j+1}$. Hence $b_j = c_1 t_{j+1}$ and $c_{\ell+1} t_{\ell+j+1} = c_1 c_\ell t_{j+1}$ for any $0 \leq \ell, j \leq p-1$. In particular $c_j \neq 0$ for all $0 \leq j \leq p-1$.

Taking $\ell = 1$ in the formula $c_{\ell+1} t_{\ell+j+1} = c_1 c_\ell t_{j+1}$, we get

$$\frac{t_{j+1}}{t_j} = \frac{c_1^2}{c_2}$$

for any $0 \leq j \leq p-1$. Denote $t = c_1^2/c_2$. We find that $t^p = \prod_{0 \leq j \leq p-1} (t_{j+1}/t_j) = 1$.

Hence $t = \zeta^a$ for some a, i.e. $t_{j+1} = \zeta^a t_j$ for $0 \le j \le p-1$. Note that $a \not\equiv 0 \pmod p$; otherwise ρ would be a scalar matrix.

Thus we may write $\rho : x_j \mapsto t_0 \zeta^{aj} x_j$ for $0 \le j \le p-1$. Since $\det(\rho) = 1$, we find $t_0 = \zeta^b$ for some integer b.

It is easy to verify that $\sigma\rho\sigma^{-1} = \zeta^{-a}\rho$. Thus $\zeta^{-a} I_p = \sigma\rho\sigma^{-1}\rho^{-1} \in D$. Hence $\zeta I_p \in \mathrm{Ker}(\pi)$. Since $\rho = \zeta^b \tau^a$, we find that $\tau \in \mathrm{Ker}(\pi)$ and $\rho \in \langle \tau, \zeta I_p \rangle$. In particular, the order of ρ is p.

Step 7: $\mathrm{Ker}(\pi) = \langle \tau, \zeta I_p \rangle$.

Because of Step 6, it remains to show that $\mathrm{Ker}(\pi)$ is a p-group. Suppose not. Since $\mathrm{Ker}(\pi)$ is abelian, there exists an element ρ' in $\mathrm{Ker}(\pi)$ and the order of ρ' is k' with $1 \le k' \le p-1$. Obviously ρ' is not a scalar matrix. Now there is some $1 \le k'' \le p-1$ such that $\rho'^{k''}$ is of order p. This is impossible. □

LEMMA 3.7. *$\mathrm{Ker}(\pi) = \langle \tau, \zeta I_p \rangle$. In particular, $\langle \tau, \zeta I_p \rangle$ is a normal subgroup of H.*

PROOF. By Lemma 3.3, there are at least two D-polygons. Let $\Delta = \{u_0, u_1, \ldots, u_{p-1}\}$ be a D-polygon other than Δ_∞.

Case 1: $\sigma(u_i) \notin \boldsymbol{C} u_i$ for any $0 \le i \le p-1$.

Apply Lemma 3.6.

Case 2: $\sigma(u_i) \in \boldsymbol{C} u_i$ for some $0 \le i \le p-1$.

Apply Lemma 3.4 and get $u_i = \sum_{0 \le j \le p-1} \zeta^{ij} x_j$ for $0 \le i \le p-1$. For any non-scalar matrix $\rho \in \mathrm{Ker}(\pi)$, we find that $\rho(u_0) = a u_i$ for some i. Obviously $i \not\equiv 0 \pmod p$.

Write $\rho : x_j \mapsto c_j x_j$ for $c_j \in \boldsymbol{C} \setminus \{0\}$. From the relation $\rho(u_0) = a u_i$, we find $a = c_0$ and $c_j = c_0 \zeta^{ij}$. Thus the non-scalar matrix ρ is just $c_0 \tau^i$. Since $\det(\rho) = 1$ we find $c_0 = \zeta^b$ for some integer b. Consider $\sigma\rho\sigma^{-1}\rho^{-1}$ again. We conclude that $\mathrm{Ker}(\pi) = \langle \tau, \zeta I_p \rangle$ as in the proof of Lemma 3.6(3). □

LEMMA 3.8. *H is a solvable group and D is a normal subgroup of G.*

PROOF. Since $\langle \tau, \zeta I_p \rangle$ is normal in H by Lemma 3.7, we find that $\rho\tau\rho^{-1} = \tau^a \cdot \zeta^b I_p$ for some $a, b \in \boldsymbol{Z}_p$ with $a \not\equiv 0 \pmod p$. Hence the following map Ψ is a homomorphism from H to $\boldsymbol{Z}_p \cdot \boldsymbol{Z}_p^\times$ (the semi-direct product of $\boldsymbol{Z}_p$ with $\boldsymbol{Z}_p^\times$ where $\boldsymbol{Z}_p$ is a normal subgroup),

$$\begin{aligned} \Psi : H &\longrightarrow \boldsymbol{Z}_p \cdot \boldsymbol{Z}_p^\times \\ \rho &\longmapsto (a, b) \end{aligned}$$

if $\rho\tau\rho^{-1} = \tau^a \cdot \zeta^b I_p$.

We claim that $\mathrm{Ker}(\Psi) = \langle \tau, \zeta I_p \rangle$. Suppose that $\rho \in \mathrm{Ker}(\Psi)$. Then $\rho\tau = \tau\rho$. Since τ is a diagonal matrix with distinct eigenvalues, it is not difficult to find that ρ is also a diagonal matrix. Thus $\rho \in \mathrm{Ker}(\pi) = \langle \tau, \zeta I_p \rangle$.

Since the kernel and the image of Ψ are solvable groups, so is H. Now $\pi(H)$ is a transitive solvable subgroup of S_p. Hence $|\pi(H)| = pf$ for some f dividing $p-1$; moreover, the p-cycle $(0, 1, \ldots, p-1)$ generates a normal subgroup of $\pi(H)$. Hence $D = \pi^{-1}(\langle (0, 1, \ldots, p-1) \rangle)$ is a normal Sylow p-subgroup of H. It follows that D is a characteristic subgroup of H. Thus $D \triangleleft G$. □

4. *D*-polygons and Gauss sums.

First we will determine all the D-polygons.

LEMMA 4.1. *The monomial group D has precisely $p+1$ subgroups of index p : $D_\infty = \langle \tau, \zeta I_p \rangle$ and $D_i = \langle \sigma\tau^i, \zeta I_p \rangle$, where $0 \le i \le p-1$. These subgroups provide all the D-polygons $\Delta_\infty, \Delta_0, \Delta_1, \ldots, \Delta_{p-1}$, which are defined in Definition 2.4.*

PROOF. Note that $\sigma\tau\sigma^{-1}\tau^{-1} = \zeta^{-1} I_p$.

It is not difficult to show that all the index p subgroups of D are D_∞ and D_i with $0 \le i \le p-1$. Now we will determine D-polygons via these index p subgroups. We will do this for D_i, where $0 \le i \le p-1$ and leave the case D_∞ to the reader.

Write the coset decomposition of D with respect to D_i, i.e. $D = \bigcup_{0 \le j \le p-1} g_j D_i$ with $g_0 = \mathrm{id}$. Let v be a common eigenvector for all elements in D_i. By Lemma 3.1 the set $\{g_j(v) : 0 \le j \le p-1\}$ is the D-polygon associated to D_i.

Since the subspace $\boldsymbol{C} \cdot v$ is fixed by D_i, all the other subspaces $\boldsymbol{C} \cdot g_j(v)$ are fixed by D_i also (see the proof of Lemma 3.4). Hence these $g_j(v)$ are nothing but the eigenvectors of $\sigma\tau^i$.

The map $\sigma\tau^i$ can be exhibited as $\sigma\tau^i : x_j \mapsto \zeta^{ij} x_{j+1}$. Thus it is routine to verify all elements of Δ_i in Definition 2.4 are eigenvectors of $\sigma\tau^i$. □

Once we know that D is a monomial normal subgroup of G, it would be unnecessary to determine the structure of H. We may simply replace H by D and proceed to the proof of Theorem 2.5.

Recall the definitions of u_i, v_j in Definition 2.4.

LEMMA 4.2. *Let $g \in G$.*

(1) *If $g(\Delta_\infty) = \Delta_\infty$ and $g(x_0) \in \boldsymbol{C} \cdot x_0$, then there exists some $k \not\equiv 0 \pmod p$ such that $g : x_\ell \mapsto c_\ell x_{k\ell}$ for $0 \le \ell \le p-1$ and $c_\ell \in \boldsymbol{C} \setminus \{0\}$.*

(2) *If $g(\Delta_\infty) = \Delta_0$ and $g(x_0) \in \boldsymbol{C} \cdot u_0$, then there exists some $k \not\equiv 0 \pmod p$*

such that $g : x_\ell \mapsto c_\ell u_{k\ell}$ *for* $0 \le \ell \le p-1$ *and* $c_\ell \in \boldsymbol{C} \setminus \{0\}$.

(3) *If* $g(\Delta_\infty) = \Delta_i$ *for some* $1 \le i \le p-1$ *and* $g(x_0) \in \boldsymbol{C} \cdot v_0$, *then there exists some* $k \not\equiv 0 \pmod p$ *such that* $g : x_\ell \mapsto c_\ell v_{k\ell}$ *for* $0 \le \ell \le p-1$ *and* $c_\ell \in \boldsymbol{C} \setminus \{0\}$.

PROOF. We will prove (1) only, because the proof of (2) and (3) are almost the same.

Since $g(\Delta_\infty) = \Delta_\infty$ there is a permutation $\delta \in S_p$ such that $g(x_\ell) = c_\ell x_{\delta(\ell)}$ and $\delta(0) = 0$.

Note that $g^{-1}\sigma g = \zeta^r \sigma^s \tau^t$ for some r, s, t because $D \triangleleft G$. Suppose that $g(x_k) \in \boldsymbol{C} \cdot x_1$, i.e. $\delta(k) = 1$. Consider $g^{-1}\sigma g(x_0) = \zeta^r \sigma^s \tau^t(x_0)$. We find that $k = s$, i.e. $\sigma g = \zeta^r g \sigma^k \tau^t$.

For any $0 \le j \le p-1$, consider $\sigma g(x_j) = \zeta^r g \sigma^k \tau^t(x_j)$. We find that $\sigma(j) = \delta(j+k)$ for any j. By induction we get $\delta(jk) = j$ for any j, i.e. $\delta(j) = k^{-1}j$ for $0 \le j \le p-1$.

In case of (2), we may consider $g^{-1}\tau g$; in case of (3), consider $g^{-1}\sigma g$. □

LEMMA 4.3. *Keep the notation in Theorem* 2.5; *in particular,* $H_0 = \mathrm{Ker}(\phi)$. *Then* $H_0 = \langle \sigma.\tau, \lambda_d \rangle$ *for some integer* d *with* $d^2 \equiv 1 \pmod p$. *More generally, if* $g \in G$ *satisfies* $g(\Delta_\infty) = \Delta_\infty$ *and* $g(\Delta_i) = \Delta_i$ *for some* $0 \le i \le p-1$, *then* $\langle g, H_0 \rangle = \langle g', H_0 \rangle$, *where* g' *is defined by*

$$g' : x_\ell \mapsto \varepsilon \zeta^{i\binom{d'\ell}{2} - i\binom{\ell}{2}} x_{d'\ell}$$

for some $d' \not\equiv 0 \pmod p$, *for any* $0 \le \ell \le p-1$, *and* $\varepsilon = 1$ *or* -1.

PROOF.

Step 1: If $g \in \mathrm{Ker}(\phi)$, then $\langle g, D \rangle = \langle \lambda_d, D \rangle$ for some $d \not\equiv 0 \pmod p$ with $d^2 \equiv 1 \pmod p$.

Since $g(\Delta_\infty) = \Delta_\infty$ and $g(\Delta_0) = \Delta_0$, replace g by $\sigma^r g \tau^s$ for suitable r and s if necessary; we will denote $\sigma^r g \tau^s$ by g (by abusing the notation). We may assume that $g(x_0) \in \boldsymbol{C} \cdot x_0$ and $g(u_0) \in \boldsymbol{C} \cdot u_0$, where $u_0 = \sum_{0 \le \ell \le p-1} x_\ell$.

By Lemma 4.2 there exists an integer $d \not\equiv 0 \pmod p$ such that $g : x_\ell \mapsto c_\ell x_{d\ell}$ for $0 \le \ell \le p-1$. Substitute it into $g(u_0) = a u_0$ for some $a \in \boldsymbol{C} \setminus \{0\}$. It follows that $c_0 = c_1 = \cdots = c_{p-1}$.

Since $g(\Delta_i) = \Delta_i$ for any $1 \le i \le p-1$, we have $g(v_0) = b \cdot v_t$ for some $0 \le t \le p-1$, $b \in \boldsymbol{C} \setminus \{0\}$, where $v_0 = \sum_{0 \le \ell \le p-1} \zeta^{i\binom{\ell}{2}} x_\ell$ and $\Delta_i = \{v_0, v_1, \ldots, v_{p-1}\}$. Substitute $g : x_\ell \mapsto c x_{d\ell}$ into this formula. We get

$$c\sum_{0\le\ell\le p-1}\zeta^{i\binom{\ell}{2}}x_{d\ell}=a\sum_{0\le\ell\le p-1}\zeta^{i\binom{\ell}{2}}x_{\ell+t}$$
$$=a\sum_{0\le\ell\le p-1}\zeta^{i\binom{d\ell-t}{2}}x_{d\ell}.$$

Hence

$$c\cdot\zeta^{i\binom{\ell}{2}}=a\zeta^{i\binom{d\ell-t}{2}}$$

for any $0\le\ell\le p-1$.

Thus, for any $0\le\ell\le p-1$, the value

$$\xi^{i\binom{d\ell-t}{2}-i\binom{\ell}{2}}=\xi^{\frac{i}{2}[(d^2-1)\ell^2-(2dt+d-1)\ell+(t^2-t)]}$$

is a constant. Hence $d^2\equiv 1\ (\mathrm{mod}\, p)$.

Step 2: If i is some integer with $0\le i\le p-1$ and $g\in G$ satisfies $g(\Delta_\infty)=\Delta_\infty$ and $g(\Delta_i)=\Delta_i$, then there is some $g'\in\langle g,D\rangle$ given by

$$g':x_\ell\mapsto\varepsilon\xi^{i\binom{d'\ell}{2}-i\binom{\ell}{2}}x_{d'\ell}$$

for some $d'\not\equiv 0\ (\mathrm{mod}\, p)$, $\varepsilon=\pm1$.

When $i\equiv 0\ (\mathrm{mod}\, p)$, the proof is similar to Step 1 and is left to the reader. It remains to prove the case when $1\le i\le p-1$.

Replacing g by $\sigma^r g\tau^s$ if necessary, we may assume that $g(x_0)\in\boldsymbol{C}\cdot x_0$ and $g(v_0)\in\boldsymbol{C}\cdot v_0$, where $v_0=\sum_{0\le\ell\le p-1}\zeta^{i\binom{\ell}{2}}x_\ell$.

Apply Lemma 4.2. Find an integer $d'\not\equiv 0\ (\mathrm{mod}\, p)$ so that $g':x_\ell\mapsto c_\ell x_{d'\ell}$ for $c_\ell\in\boldsymbol{C}\setminus\{0\}$. Substitute it into $g(v_0)=av_0$ for some $a\in\boldsymbol{C}\setminus\{0\}$. We find that $c_\ell\cdot c_0^{-1}=\zeta^{i\binom{d'\ell}{2}-i\binom{\ell}{2}}$ for any ℓ. Since $\det(g)=1$, it follows that $c_0=\varepsilon\cdot\zeta^t$, where $\varepsilon=\mathrm{sgn}\{x\mapsto d'x:0\le x\le p-1\}$ and t is some integer. □

LEMMA 4.4. *Let a be an integer. Then*

$$\sum_{0\le\ell\le p-1}\zeta^{a\ell}=\begin{cases}0, & \text{if } a\not\equiv 0\ (\mathrm{mod}\, p)\\ p, & \text{if } a\equiv 0\ (\mathrm{mod}\, p).\end{cases}$$

PROOF. This formula is standard and thus its proof is omitted. □

THEOREM 4.5. *Let a be an integer with $a \not\equiv 0 \pmod p$. Then*

$$\sum_{0\le\ell\le p-1} \zeta^{a\ell^2} = \left(\frac{a}{p}\right)\sqrt{\left(\frac{-1}{p}\right)p}\,.$$

PROOF. Omitted. □

LEMMA 4.6. *If a and b are integers with $a \not\equiv 0 \pmod p$, then*

$$\sum_{0\le\ell\le p-1} \zeta^{a\binom{\ell}{2}+b\ell} = \left(\frac{2a}{p}\right)\zeta^{-\frac{a(2a^{-1}b-1)^2}{8}}\sqrt{\left(\frac{-1}{p}\right)p}.$$

PROOF.

$$\begin{aligned}
\sum_{0\le\ell\le p-1} \zeta^{a\binom{\ell}{2}+b\ell} &= \sum_{\ell} \zeta^{\frac{a}{2}(\ell^2-\ell)+b\ell} = \sum_{\ell} \zeta^{\frac{a}{2}[\ell^2-\ell+2a^{-1}b\ell]} \\
&= \sum_{\ell} \zeta^{\frac{a}{2}[\ell^2+(2a^{-1}b-1)\ell]} = \sum_{\ell} \zeta^{\frac{a}{2}[(\ell+\frac{2a^{-1}b-1}{2})^2-\frac{(2a^{-1}b-1)^2}{4}]} \\
&= \sum_{\ell} \zeta^{\frac{a}{2}(\ell+\frac{2a^{-1}b-1}{2})^2-\frac{a(2a^{-1}b-1)^2}{8}} \\
&= \zeta^{-\frac{a(2a^{-1}b-1)^2}{8}} \sum_{\ell} \zeta^{\frac{a}{2}\ell^2}.
\end{aligned}$$

□

5. Proof of Theorem 2.5: the first stage.

We will start to prove Theorem 2.5. The proof of Theorem 2.5(E) will be delayed till Section 6.

(A) has been proved in Lemma 3.8.

(B) is proved in Lemma 4.1.

(C) The group action of G on the set $\{\Delta_\infty, \Delta_0, \ldots, \Delta_{p-1}\}$ is well-defined because of Lemma 3.3.

It remains to discuss (D).

Now we will consider the action of G on the D-polygons $\Delta_\infty, \Delta_0, \ldots, \Delta_{p-1}$. Note that, for $i = 0, 1, \ldots, p-1, \infty$, each Δ_i is associated to D_i, where $D_\infty = \langle \tau, \zeta I_p\rangle$, $D_i = \langle \sigma\tau^i, \zeta I_p\rangle$ for $0 \le i \le p-1$.

Since $D \triangleleft G$ and that $D_\infty, D_0, \ldots, D_{p-1}$ are all the index p subgroup D, it follows that G permutes $D_\infty, D_0, \ldots, D_{p-1}$.

LEMMA 5.1. *Let $x, y \in \{\infty, 0, 1, \ldots, p-1\}$. For any $g \in G$, $g(\Delta_x) = \Delta_y$ if and only if $g \cdot D_x \cdot g^{-1} = D_y$.*

PROOF. From the proof of Lemma 4.1, elements of Δ_x are precisely the linearly independent eigenvectors of D_x. Hence the result. □

DEFINITION 5.2. For any $g \in G$, if $g \cdot \tau \cdot g^{-1} = \zeta^r \tau^a \sigma^c$, $g \cdot \sigma \cdot g^{-1} = \zeta^s \tau^b \sigma^d$ for some $a, b, c, d, r, s \in \boldsymbol{F}_p$. We will define a map $\Phi : G \to GL(2, \boldsymbol{F}_p)$ by

$$\Phi(g) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \boldsymbol{F}_p).$$

This map is the conjugation action of G on $D/\langle \zeta I_p \rangle \simeq \boldsymbol{F}_p \cdot \tau' \oplus \boldsymbol{F}_p \cdot \sigma' \simeq \boldsymbol{F}_p^2$, where τ' and σ' are the images of τ and σ in $D/\langle \zeta I_p \rangle$ respectively. The coordinates of τ' and σ' are $\binom{1}{0}$ and $\binom{0}{1}$ respectively. The projective line $\boldsymbol{P}^1(\boldsymbol{F}_p)$ consists of $p+1$ points: $\infty = \binom{1}{0}$, $i = \binom{i}{1}$ for $0 \le i \le p-1$. These points correspond to D_∞, D_i for $0 \le i \le p-1$, and they also correspond to Δ_∞, Δ_i for $0 \le i \le p-1$. It is straightforward to see that these correspondences respect the actions of G.

We will show that $\Phi(g) \in SL(2, \boldsymbol{F}_p)$ in Section 7. At present we only know that $\Phi(g) \in GL(2, \boldsymbol{F}_p)$. Let $\pi_0 : GL(2, \boldsymbol{F}_p) \to PGL(2, \boldsymbol{F}_p)$ be the canonical projection. By Lemma 5.1 we find that $\phi(g) = \pi_0 \Phi(g)$. Note that

$$\phi(g) \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PGL(2, \boldsymbol{F}_p)$$

may be regarded as a fractional linear transformation on $\boldsymbol{P}^1(\boldsymbol{F}_p)$ which sends $x \in \boldsymbol{P}^1(\boldsymbol{F}_p) = \{\infty, 0, 1, \ldots, p-1\}$ to $(ax+b)/(cx+d)$.

We record the above discussion as the following lemma.

LEMMA 5.3. *Keep the notation in Theorem 2.5. Let the points $\infty, 0, 1, \ldots, p-1$ on $\boldsymbol{P}^1(\boldsymbol{F}_p)$ correspond to the D-polygons $\Delta_\infty, \Delta_0, \Delta_1, \ldots, \Delta_{p-1}$. If $g \in G$ satisfies $g \cdot \tau \cdot g^{-1} = \zeta^r \tau^a \sigma^c$, $g \cdot \sigma \cdot g^{-1} = \zeta^s \tau^b \sigma^d$ for some $a, b, c, d, r, s \in \boldsymbol{F}_p$, then g permutes $\Delta_\infty, \Delta_0, \Delta_1, \ldots, \Delta_{p-1}$ as the fractional linear transformation $x \mapsto (ax+b)/(cx+d)$, where $x = \infty, 0, 1, \ldots, p-1$. Moreover this action induces a non-trivial group homomorphism $\phi : G \to PGL(2, \boldsymbol{F}_p)$ such that $\mathrm{Ker}(\phi) = \langle \sigma, \tau, \lambda_d \rangle$ for some integer $d^2 \equiv 1 \pmod{p}$.*

PROOF. The assertion about $\mathrm{Ker}(\phi)$ is proved in Lemma 4.3.

If ϕ is trivial, i.e. $G = \mathrm{Ker}(\phi)$, then $G = \langle \sigma, \tau, \lambda_d \rangle$ is a monomial group. This is

a contradiction to the assumption that G is primitive. □

6. Proof of Theorem 2.5: the second stage.

All the notation are the same as in Theorem 2.5.

Let $g \in G$.

Case 1: $g : \Delta_\infty \mapsto \Delta_\infty$, $\Delta_0 \mapsto \Delta_0$.

Apply Lemma 4.3. There exists $\rho \in gH_0$ such that $\rho : x_\ell \mapsto \varepsilon x_{k\ell}$ for some $k \not\equiv 0 \pmod p$ and for any $0 \le \ell \le p-1$.

It remains to find $\phi(\rho)$ explicitly. Note that $\phi(g) = \phi(\rho)$.

Since Δ_∞ and Δ_0 correspond to the groups $D_\infty = \langle \tau, \zeta I_p \rangle$ and $D_0 = \langle \sigma, \zeta I_p \rangle$ respectively, the assumption that $g(\Delta_\infty) = \Delta_\infty$ and $g(\Delta_0) = \Delta_0$ is equivalent to that $g\tau g^{-1} = \zeta^r \tau^a$ and $g\sigma g^{-1} = \zeta^s \sigma^d$ for some integers r, s, a, d. Hence g gives rise to the matrix

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix} \in PGL(2, \boldsymbol{F}_p) \tag{6.1}$$

where $\lambda = ad^{-1} \in \boldsymbol{F}_p^\times$. It remains to evaluate λ in terms of the constant k in the definition of ρ.

Note that (6.1) corresponds to the fractional linear transformation $x \mapsto \lambda x$. Since $1 \mapsto \lambda$, it suffices to find $g(\Delta_1)$.

Clearly $g(\Delta_1) = \Delta_i$ for some $1 \le i \le p-1$.

Write $\Delta_i = \{w_0, w_1, \ldots, w_{p-1}\}$, where $w_0 = \sum_{0 \le \ell \le p-1} \zeta^{i\binom{\ell}{2}} x_\ell$, and $\Delta_1 = \{v_0, \ldots, v_{p-1}\}$, where $v_0 = \sum_{0 \le \ell \le p-1} \zeta^{\binom{\ell}{2}} x_\ell$.

From the assumption $\rho(v_0) = a \cdot w_t$ for some $0 \le t \le p-1$, we find

$$\begin{aligned} \varepsilon \sum_{0 \le \ell \le p-1} \zeta^{\binom{\ell}{2}} x_{k\ell} &= a \sum_{0 \le \ell \le p-1} \zeta^{i\binom{\ell}{2}} x_{\ell+t} \\ &= a \sum_{0 \le \ell \le p-1} \zeta^{i\binom{\ell-t}{2}} x_\ell \\ &= a \sum_{0 \le \ell \le p-1} \zeta^{i\binom{k\ell-t}{2}} x_{k\ell}. \end{aligned}$$

Thus we find that, for any $0 \le \ell \le p-1$,

$$\varepsilon \zeta^{\binom{\ell}{2}} = a \zeta^{i\binom{k\ell-t}{2}}.$$

Hence we get $ik^2 \equiv 1 \pmod{p}$ and $1 = ik(1+2t)$, i.e. $g(\Delta_1) = \Delta_{k^{-2}}$ and $\lambda = k^{-2}$.

Case 2: $g : \Delta_\infty \mapsto \Delta_\infty$, $\Delta_0 \mapsto \Delta_i$ for some $1 \leq i \leq p-1$.

Write $\Delta_0 = \{u_0, \ldots, u_{p-1}\}$, $\Delta_i = \{v_0, \ldots, v_{p-1}\}$, where $u_0 = x_0 + \cdots + x_{p-1}$ and $v_0 = \sum_{0 \leq \ell \leq p-1} \zeta^{i\binom{\ell}{2}} x_\ell$.

As in the proof of Lemma 4.3, consider $\sigma^{-r} g \tau^s$ for suitable r, s. We find $\rho \in gH_0$ such that $\rho(x_0) \in \boldsymbol{C} \cdot x_0$ and $\rho(u_0) \in \boldsymbol{C} \cdot v_0$.

Apply Lemma 4.2. There exists $k \not\equiv 0 \pmod{p}$ such that $\rho : x_\ell \mapsto c_\ell x_{k\ell}$ for $0 \leq \ell \leq p-1$ and $c_\ell \in \boldsymbol{C} \setminus \{0\}$. Substitute it into $\rho(u_0) = av_0$ for $a \in \boldsymbol{C} \setminus \{0\}$. We get

$$\sum_{0 \leq \ell \leq p-1} c_\ell x_{k\ell} = a \sum_{0 \leq \ell \leq p-1} \zeta^{i\binom{\ell}{2}} x_\ell = a \sum_{0 \leq \ell \leq p-1} \zeta^{i\binom{k\ell}{2}} x_{k\ell}.$$

Thus we get

$$\rho : x_\ell \mapsto c \cdot \zeta^{i\binom{k\ell}{2}} x_{k\ell}$$

for some $c \in \boldsymbol{C} \setminus \{0\}$.

It remains to determine $\phi(\rho)$. Note that g determines the element

$$\begin{pmatrix} a & bi \\ 0 & b \end{pmatrix} = \begin{pmatrix} \lambda & i \\ 0 & 1 \end{pmatrix} \in PGL(2, \boldsymbol{F}_p) \tag{6.2}$$

where $\lambda \in \boldsymbol{F}_p^\times$.

Since (6.2) determines the map $x \mapsto \lambda x + i$, we will find $g(\Delta_1)$. Note that either $g(\Delta_1) = \Delta_0$ or $g(\Delta_1) = \Delta_j$ for some $1 \leq j \leq p-1$. It is not difficult to show that, (i) if $g(\Delta_1) = \Delta_0$, then $1 + ik^2 \equiv 0 \pmod{p}$; and (ii) if $g(\Delta_1) = \Delta_j$, then $1 + (i-j)k^2 \equiv 0 \pmod{p}$.

In either case, it will imply that $\lambda = k^{-2}$. The details are left to the reader.

Case 3: $g : \Delta_\infty \mapsto \Delta_0 \mapsto \Delta_\infty$.

Use similar methods in Case 2. Let $\rho = \sigma^{-r} g \tau^s$ so that $\rho(x_0) \in \boldsymbol{C} \cdot u_0$ and $\rho(u_0) \in \boldsymbol{C} \cdot x_0$. Apply Lemma 4.2 to get that $\rho : x_\ell \mapsto c_\ell u_{k\ell}$ for some $k \not\equiv 0 \pmod{p}$ and $c_\ell \in \boldsymbol{C} \setminus \{0\}$. Substitute it into $\rho(u_0) = ax_0$ for some $a \in \boldsymbol{C} \setminus \{0\}$. We get

$$\sum_{0 \leq \ell' \leq p-1} \left(\sum_{0 \leq \ell \leq p-1} c_\ell \zeta^{k\ell\ell'} \right) x_{\ell'} = ax_0.$$

Define a complex $p \times p$ matrix $T = (t_{\ell',\ell})_{0\le\ell',\ell\le p-1}$ by defining $t_{\ell',\ell} = \zeta^{k\ell\ell'}$.

If $0 \le \ell' \ne \ell'' \le p-1$, then $\sum_{0\le\ell\le p-1} t_{\ell',\ell} \cdot \overline{t}_{\ell'',\ell} = \sum_{0\le\ell\le p-1} \zeta^{k(\ell'-\ell'')\ell} = 0$ by Lemma 4.4.

Thus $T \cdot {}^t\overline{T} = p \cdot I_p$, where ${}^t\overline{T}$ is the conjugate transpose of the matrix T. Moreover,

$$T \begin{pmatrix} c_0 \\ c_1 \\ \\ \vdots \\ \\ c_{p-1} \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \\ \\ \vdots \\ \\ 0 \end{pmatrix}.$$

Multiply ${}^t\overline{T}$ on both side of the above identity. We get

$$pc_\ell = a$$

for any $0 \le \ell \le p-1$. Thus $\rho : x_\ell \mapsto c\sum_{0\le\ell'\le p-1} \zeta^{k\ell\ell'} x_{\ell'}$ for some $c \in \boldsymbol{C} \setminus \{0\}$.

Now we will determine $\phi(\rho)$. Since g determines

$$\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix} = \begin{pmatrix} 0 & \lambda \\ 1 & 0 \end{pmatrix} \in PGL(2, \boldsymbol{F}_p),$$

$\phi(\rho)$ is the map $x \mapsto \lambda/x$. We will find $g(\Delta_1)$. Note that $g(\Delta_1) = \Delta_i$ for some $1 \le i \le p-1$.

Thus we have a relation $g(\sum_\ell \zeta^{\binom{\ell}{2}} x_\ell) = a\sum_\ell \zeta^{i\binom{\ell}{2}} x_{\ell+t}$ for some $a \in \boldsymbol{C} \setminus \{0\}$ and some $0 \le t \le p-1$. Hence get

$$c\sum_\ell \zeta^{\binom{\ell}{2}+k\ell\ell'} = a\zeta^{i\binom{\ell'-t}{2}}$$

for any $0 \le \ell' \le p-1$. Apply Lemma 4.6 to evaluate the left-hand side of the above relation (with $a = 1$ and $b = k\ell'$). We find a non-zero constant A such that

$$c \cdot A \cdot \zeta^{-\frac{(2k\ell'-1)^2}{8}} = a\zeta^{i\binom{\ell'-t}{2}} \tag{6.3}$$

for any $0 \le \ell' \le p-1$. In particular, taking $\ell' \equiv 0 \pmod p$, we get

$$c \cdot A \cdot \zeta^{-\frac{1}{8}} = a\zeta^{i\binom{-t}{2}}. \tag{6.4}$$

Dividing (6.3) by (6.4), we find that

$$\zeta^{-\frac{(2k\ell'-1)^2}{8}+\frac{1}{8}} = \zeta^{i\binom{\ell'-t}{2}-i\binom{-t}{2}}$$

for any $0 \le \ell' \le p-1$. It is easy to find that $i = -k^2$. Thus $\lambda = -k^2$.

Case 4: $g : \Delta_\infty \mapsto \Delta_0 \mapsto \Delta_i$ for some $1 \le i \le p-1$.

Define $u_0 = x_0 + \cdots + x_{p-1}$ and $v_0 = \sum_{0\le\ell\le p-1} \zeta^{i\binom{\ell}{2}} x_\ell$.

Find suitable r and s so that $\rho = \tau^r g \tau^s \in gH_0$ and $\rho(x_0) \in \boldsymbol{C}u_0$, $\rho(u_0) \in \boldsymbol{C} \cdot v_0$. By Lemma 4.2, there exists $k \not\equiv 0 \pmod p$ such that $\rho : x_\ell \mapsto c_\ell \sum_{0\le\ell'\le p-1} \zeta^{k\ell\ell'} x_{\ell'}$ for $0 \le \ell \le p-1$ and $c_\ell \in \boldsymbol{C} \setminus \{0\}$. Substitute it into $\rho(u_0) = av_0$ for some $a \in \boldsymbol{C} \setminus \{0\}$. We find that

$$\sum_{0\le\ell\le p-1} c_\ell \zeta^{k\ell\ell'} = a\zeta^{i\binom{\ell'}{2}}$$

for any $0 \le \ell' \le p-1$.

We will use the same method in Case 3 and define a complex $p \times p$ matrix $T = (t_{\ell',\ell})_{0\le\ell',\ell\le p-1}$ by defining $t_{\ell',\ell} = \zeta^{k\ell\ell'}$.

Then $T \cdot {}^t\overline{T} = p \cdot I_p$ and

$$T \cdot \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{p-1} \end{pmatrix} = a \begin{pmatrix} 1 \\ \vdots \\ \zeta^{i\binom{\ell'}{2}} \\ \vdots \end{pmatrix}.$$

It follows that

$$p \cdot \begin{pmatrix} c_0 \\ \vdots \\ c_{p-1} \end{pmatrix} = a \cdot {}^t\overline{T} \begin{pmatrix} 1 \\ \vdots \\ \zeta^{i\binom{\ell'}{2}} \\ \vdots \end{pmatrix}.$$

Hence

$$p \cdot c_\ell = a \sum_{0 \le \ell' \le p-1} \zeta^{-k\ell\ell'} \cdot \zeta^{i\binom{\ell'}{2}} = a \sum_{0 \le \ell' \le p-1} \zeta^{i\binom{\ell'}{2} - k\ell\ell'}$$

for any $0 \le \ell \le p-1$.

Apply Lemma 4.6. We find a non-zero constant A such that

$$c_\ell = A \cdot \zeta^{-\frac{i(2i^{-1}k\ell+1)^2}{8}}$$

for $0 \le \ell \le p-1$. In particular, $c_0 = A \cdot \zeta^{-\frac{i}{8}}$. Hence

$$c_\ell \cdot c_0^{-1} = \zeta^{-i\frac{[(2i^{-1}k\ell+1)^2-1]}{8}} = \zeta^{-i\binom{-i^{-1}k\ell}{2}}$$

as desired.

Now consider $\phi(\rho)$. Since $g \cdot \tau \cdot g^{-1} = \zeta^r \sigma^a$, $g \cdot \sigma \cdot g^{-1} = \zeta^s (\sigma\tau^i)^b$ for some $a, b \not\equiv 0 \pmod p$, we find that $\phi(\rho)$ determines

$$\begin{pmatrix} 0 & ib \\ a & b \end{pmatrix} = \begin{pmatrix} 0 & i \\ \lambda & 1 \end{pmatrix} \in PGL(2, \boldsymbol{F}_p).$$

Hence $\phi(\rho)$ is the map $x \mapsto i/(1+\lambda x)$. We will find the value of λ. Since $-\lambda^{-1} \mapsto \infty$, we will find some $1 \le j \le p-1$ such that $g(\Delta_j) = \Delta_\infty$.

Consider $\rho(\sum_{0 \le \ell \le p-1} \zeta^{j\binom{\ell}{2}} x_\ell) = a x_t$ for some $0 \le t \le p-1$ and $a \in \boldsymbol{C} \setminus \{0\}$. Substitute the map $\rho : x_\ell \mapsto c\zeta^{-i\binom{-i^{-1}k\ell}{2}} \sum_{0 \le \ell' \le p-1} \zeta^{k\ell\ell'} x_{\ell'}$ to get

$$\sum_{0 \le \ell \le p-1} \zeta^{j\binom{\ell}{2} - i\binom{-i^{-1}k\ell}{2} + k\ell\ell' = 0} \tag{6.5}$$

for any $\ell' \not\equiv t \pmod p$.

The left-hand side of (6.5) can be written as

$$\sum_\ell \zeta^{\frac{j}{2}(\ell^2-\ell) - \frac{k}{2}(i^{-1}k\ell^2+\ell) + k\ell\ell'} = \sum_\ell \zeta^{(j - i^{-1}k^2)\binom{\ell}{2} + \frac{2k\ell' - k - i^{-1}k^2}{2}\ell}$$

which is not zero for any $0 \le \ell' \le p-1$ provided that $j - i^{-1}k^2 \not\equiv 0 \pmod p$, because of Lemma 4.6.

Thus $j \equiv i^{-1}k^2 \pmod p$ and $\lambda = -k^{-2}i$.

Case 5: $g : \Delta_\infty \mapsto \Delta_i \mapsto \Delta_\infty$ for some $1 \le i \le p-1$.

Find $\rho = \sigma^{-r}g\tau^t \in gH_0$, where r, t are suitable integers so that $\rho(x_0) \in \boldsymbol{C} \cdot v_0$ and $\rho(v_0) \in \boldsymbol{C} \cdot x_0$, where $\Delta_i = \{v_0, v_1, \dots, v_{p-1}\}$ and $v_0 = \sum_{0 \le \ell \le p-1} \zeta^{i\binom{\ell}{2}} x_\ell$. Apply Lemma 4.2 to get $\rho : x_\ell \mapsto c_\ell v_{k\ell}$ for some $k \not\equiv 0 \pmod p$. Substitute it into $\rho(v_0) = ax_0$ for some $a \in \boldsymbol{C} \setminus \{0\}$. We find that

$$\sum_{0 \le \ell, \ell' \le p-1} c_\ell \zeta^{i\binom{\ell}{2} + i\binom{\ell'}{2}} x_{\ell' + k\ell} = ax_0.$$

The left-hand side of the above identity may be written as

$$\sum_{\ell, \ell'} c_\ell \zeta^{i\binom{\ell}{2} + i\binom{\ell' - k\ell}{2}} x_{\ell'} = \sum_{0 \le \ell' \le p-1} \left(\sum_{0 \le \ell \le p-1} c_\ell \zeta^{i\binom{\ell}{2} + i\binom{\ell' - k\ell}{2}} \right) x_{\ell'}.$$

Define a complex $p \times p$ matrix $T = (t_{\ell', \ell})_{0 \le \ell', \ell \le p-1}$, where $t_{\ell', \ell} = \zeta^{i\binom{\ell}{2} + i\binom{\ell' - k\ell}{2}}$.

If $0 \le \ell' \ne \ell'' \le p-1$, then $\sum_{0 \le \ell \le p-1} t_{\ell', \ell} \cdot \overline{t}_{\ell'', \ell} = \sum_\ell \zeta^{i\binom{\ell' - k\ell}{2} - i\binom{\ell'' - k\ell}{2}} = \sum_\ell \zeta^{i\binom{\ell'}{2} - i\binom{\ell''}{2} + ik\ell(\ell'' - \ell')} = \zeta^{i\binom{\ell'}{2} - i\binom{\ell''}{2}} = \sum_\ell (\zeta^{ik(\ell'' - \ell')})^\ell = 0$ by Lemma 4.4. In summary, $T \cdot {}^t\overline{T} = p \cdot I_p$, where ${}^t\overline{T}$ is the conjugate transpose of the matrix T.

We also find that

$$T \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{p-1} \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Multiply ${}^t\overline{T}$ on both sides of the above identity. We get

$$pc_\ell = a \cdot \zeta^{-i\binom{\ell}{2} - i\binom{-k\ell}{2}}.$$

Thus ρ may be defined as

$$\rho : x_\ell \mapsto c \cdot \zeta^{-i\binom{\ell}{2} - i\binom{-k\ell}{2}} \sum_{0 \le \ell' \le p-1} \zeta^{i\binom{\ell}{2}} x_{\ell' + k\ell}$$

for any $0 \le \ell \le p-1$ and for some $c \in \boldsymbol{C} \setminus \{0\}$.

Now we will determine $\phi(\rho)$.

Since $g\cdot\tau\cdot g^{-1}=\zeta^r(\sigma\tau^i)^a$, $g\cdot\sigma\tau^i\cdot g^{-1}=\zeta^s\cdot\tau^b$ for some $a,b\not\equiv 0 \pmod p$, we get $g\cdot\sigma\cdot g^{-1}=\zeta^{s'}\tau^{b-ai^2}\sigma^{-ai}$. The matrix determined by g is

$$\begin{pmatrix} ai & b-ai^2 \\ a & -ai \end{pmatrix} = \begin{pmatrix} i & \lambda-i^2 \\ 1 & -i \end{pmatrix} \in PGL(2,\boldsymbol{F}_p).$$

Thus $\phi(\rho)$ is the map $x\mapsto(ix+\lambda-i^2)/(x-i)$.

We will find $g(\Delta_0)$. Note that $g(\Delta_0)$ may be Δ_0 or Δ_j for some $1\le j\le p-1$.

Case 5.1: Suppose that $g(\Delta_0)=\Delta_0$.

From $\rho(\sum_\ell x_\ell)=a\sum_\ell\zeta^{j\ell}x_\ell$, where $a\in\boldsymbol{C}\setminus\{0\}$, we get

$$c\cdot\sum_{0\le\ell\le p-1}\zeta^{-i\binom{\ell}{2}-i\binom{-k\ell}{2}+i\binom{\ell'-k\ell}{2}}=a\zeta^{j\ell'} \tag{6.6}$$

for any $0\le\ell'\le p-1$.

The left-hand side of (6.6) may be simplified as

$$\begin{aligned} c\cdot\sum_{0\le\ell\le p-1}\zeta^{-i\binom{\ell}{2}+i\binom{\ell'}{2}-ik\ell\ell'} &= c\cdot\zeta^{i\binom{\ell'}{2}}\sum_{0\le\ell\le p-1}\zeta^{-i\binom{\ell}{2}-ik\ell\ell'} \\ &= A\zeta^{i\binom{\ell'}{2}+\frac{i(2k\ell'-1)^2}{8}} \end{aligned}$$

for some non-zero constant A which is independent of ℓ', by Lemma 4.6. Thus

$$A\cdot\zeta^{i\binom{\ell'}{2}+\frac{i(2k\ell'-1)^2}{8}}=a\zeta^{j\ell'}$$

for any $0\le\ell'\le p-1$. In particular, $A\cdot\zeta^{\frac{i}{8}}=a$. Thus we have

$$\zeta^{i\binom{\ell'}{2}+\frac{i(2k\ell'-1)^2}{8}-\frac{i}{8}}=\zeta^{j\ell'}$$

for any $0\le\ell'\le p-1$. It follows that

$$i\binom{\ell'}{2}+\frac{ik\ell'(k\ell'-1)}{2}\equiv j\ell' \pmod p$$

for any $0\le\ell'\le p-1$.

Thus $i+ik^2\equiv 0 \pmod p$, i.e. $k^2\equiv -1 \pmod p$.

Case 5.2: Suppose that $g(\Delta_0)=\Delta_j$ for some $1\le j\le p-1$. It is clear that $j\not\equiv i \pmod p$.

From $\rho(\sum_\ell x_\ell) = a\sum_\ell \zeta^{j\binom{\ell}{2}} x_{\ell+t}$ for some $0 \le t \le p-1$ and $a \in \boldsymbol{C} \setminus \{0\}$, we get

$$c \cdot \sum_{0\le\ell\le p-1} \zeta^{-i\binom{\ell}{2}-i\binom{-k\ell}{2}+i\binom{\ell'-k\ell}{2}} = a\zeta^{j\binom{\ell'-t}{2}} \tag{6.7}$$

for any $0 \le \ell' \le p-1$.

Note that the left-hand side of (6.7) is the same as that of (6.6). Hence we get

$$A \cdot \zeta^{i\binom{\ell'}{2}+\frac{i(2k\ell'-1)^2}{8}} = a\zeta^{j\binom{\ell'-t}{2}}$$

for any $0 \le \ell' \le p-1$. It follows that

$$\zeta^{i\binom{\ell'}{2}+\frac{i(2k\ell'-1)^2}{8}-\frac{i}{8}} = \zeta^{j\binom{\ell'-t}{2}-j\binom{-t}{2}}$$

for any $0 \le \ell' \le p-1$.

Hence we get $i + ik^2 = j$.

Combine the results of Case 5.1 and Case 5.2. We find that $g(\Delta_0) = \Delta_{i+ik^2}$.

On the other hand, the fractional linear transformation we obtain is $x \mapsto (ix + \lambda - i^2)/(x - i)$. Hence $0 \mapsto (\lambda - i^2)/(-i)$. We get $i + ik^2 = (\lambda - i^2)/(-i)$. Thus $\lambda = -i^2k^2$.

Case 6: $g : \Delta_\infty \mapsto \Delta_i \mapsto \Delta_0$ for some $1 \le i \le p-1$.

Find suitable r and s so that $\rho = \sigma^r g \tau^s \in gH_0$ and $\rho(x_0) \in \boldsymbol{C} \cdot v_0$, $\rho(v_0) \in \boldsymbol{C} \cdot u_0$, where $v_0 = \sum_\ell \zeta^{i\binom{\ell}{2}} x_\ell$, $u_0 = \sum_\ell x_\ell$.

By Lemma 4.2, there exists $k \not\equiv 0 \pmod p$ and $\rho : x_\ell \mapsto c_\ell \sum_{0\le\ell'\le p-1} \zeta^{i\binom{\ell'}{2}} x_{\ell'+k\ell}$. Substitute this into $\rho(v_0) = au_0$ for some $a \in \boldsymbol{C} \setminus \{0\}$. We get

$$\sum_{0\le\ell\le p-1} c_\ell \zeta^{i\binom{\ell}{2}+i\binom{\ell'-k\ell}{2}} = a$$

for any $0 \le \ell' \le p-1$.

Define a $p \times p$ complex matrix $T = (t_{\ell',\ell})_{0\le\ell',\ell\le p-1}$, where $t_{\ell',\ell} = \zeta^{i\binom{\ell}{2}+i\binom{\ell'-k\ell}{2}}$.

If $\ell' \ne \ell$, then

$$\sum_{0\le\ell\le p-1} t_{\ell',\ell} \cdot \overline{t}_{\ell'',\ell} = \sum_{0\le\ell\le p-1} \zeta^{\frac{i}{2}(\ell''-\ell)(\ell''+\ell'-1+k\ell)} = 0$$

by Lemma 4.4.

Hence we find that $T \cdot {}^t\overline{T} = p \cdot I_p$ and

$$T\begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{p-1} \end{pmatrix} = a\begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}.$$

Solve these c_ℓ. We get

$$pc_\ell = a\sum_{0\le\ell'\le p-1} \zeta^{-i\binom{\ell}{2}-i\binom{\ell'-k\ell}{2}} \tag{6.8}$$

for $0 \le \ell \le p-1$.

The right-hand side of (6.8) may be simplified as

$$\begin{aligned} a\sum_{\ell'} \zeta^{-i[\binom{\ell}{2}+\binom{\ell'}{2}+\binom{-k\ell}{2}-k\ell\ell']} &= a\zeta^{-i\binom{\ell}{2}-i\binom{-k\ell}{2}}\sum_{\ell'} \zeta^{i\binom{\ell'}{2}+ik\ell\ell'} \\ &= A\zeta^{-i\binom{\ell}{2}}\cdot\zeta^{-i\binom{-k\ell}{2}}\cdot\zeta^{\frac{i(2k\ell+1)^2}{8}}. \end{aligned}$$

for some non-zero constant A which is independent of ℓ, by Lemma 4.6.

We obtain

$$pc_\ell = A\cdot\zeta^{-i\binom{\ell}{2}-i\binom{-k\ell}{2}+\frac{i(2k\ell+1)^2}{8}}$$

and

$$c_\ell\cdot c_0^{-1} = \zeta^{-i\binom{\ell}{2}-i\binom{-k\ell}{2}+\frac{i(2k\ell+1)^2}{8}-\frac{i}{8}} = \zeta^{i\binom{\ell}{2}}.$$

Thus ρ can be chosen as the following map

$$\rho : x_\ell \mapsto c\cdot\zeta^{-i\binom{\ell}{2}}\sum_{0\le\ell'\le p-1}\zeta^{i\binom{\ell'}{2}}x_{\ell'+k\ell}.$$

It remains to determine $\phi(\rho)$. From $g\cdot\tau\cdot g^{-1} = \zeta^r(\sigma\tau^i)^a$ and $g\cdot(\sigma\tau^i)\cdot g^{-1} = \zeta^s\cdot\sigma^b$, where $a, b \not\equiv 0 \pmod p$, we find that $g\sigma g^{-1} = \zeta^{s'}\tau^{-ai^2}\sigma^{b-ai}$. We get the matrix

$$\begin{pmatrix} ai & -ai^2 \\ a & b-ai \end{pmatrix} = \begin{pmatrix} i & -i^2 \\ 1 & \lambda - i \end{pmatrix} \in PGL(2, \boldsymbol{F}_p).$$

Hence $\phi(\rho)$ is the map $x \mapsto (ix - i^2)/(x + \lambda - i)$.

We will find $g(\Delta_0)$. Note that $g(\Delta_0)$ may be Δ_∞ or Δ_0 for some $1 \le j \le p-1$.

Case 6.1: Suppose that $g(\Delta_0) = \Delta_\infty$.

From the relation $g(\sum_\ell x_\ell) = ax_t$ for some $0 \le t \le p-1$ and some $a \in \boldsymbol{C} \setminus \{0\}$, we find that

$$c \cdot \sum_{\ell'} \left(\sum_{\ell} \zeta^{-i\binom{\ell}{2} + i\binom{\ell'-k\ell}{2}} \right) x_{\ell'} = ax_t.$$

Thus

$$\sum_{\ell} \zeta^{-i\binom{\ell}{2} + i\binom{\ell'-k\ell}{2}} = 0 \tag{6.9}$$

for any $\ell' \not\equiv t \pmod p$.

The left-hand side of (6.9) can be written as

$$\begin{aligned} \sum_{\ell} \zeta^{-i\binom{\ell}{2} + i\binom{\ell'}{2} + i\binom{-k\ell}{2} - ik\ell\ell'} &= \zeta^{i\binom{\ell'}{2}} \sum_{\ell} \zeta^{-i\binom{\ell}{2} + i\binom{-k\ell}{2} - ik\ell\ell'} \\ &= \zeta^{i\binom{\ell'}{2}} \sum_{\ell} \zeta^{\frac{i}{2}[(k^2-1)\ell^2 + (k+1-2k\ell')\ell]} \end{aligned}$$

which is never zero by Lemma 4.6, if $k^2 - 1 \not\equiv 0 \pmod p$.

We conclude that $k^2 - 1 \equiv 0 \pmod p$.

Case 6.2: Suppose that $g(\Delta_0) = \Delta_j$, for some $1 \le j \le p-1$.

From the relation $g(\sum_\ell x_\ell) = a \sum_\ell \zeta^{j\binom{\ell}{2}} x_{\ell+t}$ for some $0 \le t \le p-1$ and some $a \in \boldsymbol{C} \setminus \{0\}$, we find that

$$c \cdot \sum_{\ell} \zeta^{-i\binom{\ell}{2} + i\binom{\ell'-k\ell}{2}} = a\zeta^{j\binom{\ell'-t}{2}}$$

for any $0 \le \ell' \le p-1$.

Proceed as in Case 6.1. We get

$$c\cdot\zeta^{i\binom{\ell'}{2}}\sum_{\ell}\zeta^{\frac{i}{2}[(k^2-1)\ell^2+(k+1-2k\ell')\ell]}=a\zeta^{j\binom{\ell'-t}{2}} \tag{6.10}$$

for any $0\le\ell'\le p-1$.

If $k^2-1\equiv 0\ (\mathrm{mod}\,p)$, then the left-hand side of (6.10) becomes zero for those ℓ' such that $k+1-2k\ell'\not\equiv 0\ (\mathrm{mod}\,p)$. This will lead to a contradiction. Thus $k^2-1\neq 0$.

We rewrite the left-hand-side of (6.10) as

$$c\cdot\zeta^{i\binom{\ell'}{2}}\sum_{\ell}\zeta^{i(k^2-1)\binom{\ell}{2}+\frac{i(k^2+k-2k\ell')}{2}\ell}=A\zeta^{i\binom{\ell'}{2}-\frac{i(k-2k\ell'+1)^2}{8(k^2-1)}}$$

by Lemma 4.6, where A is a constant independent of ℓ'.

Hence we get

$$\zeta^{i\binom{\ell'}{2}-\frac{i(k-2k\ell'+1)^2}{8(k^2-1)}+\frac{i(k+1)^2}{8(k^2-1)}}=\zeta^{j\binom{\ell'-t}{2}-j\binom{-t}{2}}$$

for $0\le\ell'\le p-1$.

We find that

$$i\ell'(\ell'-1)-\frac{-ik\ell'(k\ell'-k-1)}{k^2-1}=j\ell'(\ell'-1)-2jt\ell'$$

for $0\le\ell'\le p-1$.

Hence $j=i-\frac{ik^2}{k^2-1}=-i(k^2-1)^{-1}$.

Combine the results of Case 6.1 and Case 6.2, we find that $\lambda=ik^2$.

Case 7: $g:\Delta_\infty\mapsto\Delta_i\mapsto\Delta_j$ for some $1\le i\neq j\le p-1$.

Find suitable r and s so that $\rho=\sigma^r g\tau^s\in gH_0$ and $\rho(x_0)\in\boldsymbol{C}v_0$, $\rho(v_0)\in\boldsymbol{C}w_0$, where $v_0=\sum_\ell\zeta^{i\binom{\ell}{2}}x_\ell$, $w_0=\sum_\ell\zeta^{j\binom{\ell}{2}}x_\ell$.

By Lemma 4.2 there exists $k\not\equiv 0\ (\mathrm{mod}\,p)$ such that

$$\rho:x_\ell\mapsto c_\ell\sum_{0\le\ell'\le p-1}\zeta^{i\binom{\ell'}{2}}x_{\ell'+k\ell}.$$

Substitute it into $\rho(v_0)=aw_0$ for some $a\in\boldsymbol{C}\setminus\{0\}$. We get

$$\sum_{\ell'}\left(\sum_{\ell}c_\ell\zeta^{i\binom{\ell}{2}+i\binom{\ell'-k\ell}{2}}\right)x_{\ell'}=a\sum_{\ell'}\zeta^{j\binom{\ell'}{2}}x_{\ell'}.$$

Use the same technique as in Case 6. We find that

$$c_\ell c_0^{-1} = A\zeta^{\frac{1}{2}[\ell^2(\frac{i^2k^2}{i-j}-i-ik^2)+i\ell]}$$

for any $0 \le \ell \le p-1$. The details are left to the reader.

Now consider $\phi(\rho)$. The matrix determined by g is

$$\begin{pmatrix} ai & bj-ai^2 \\ a & b-ai \end{pmatrix} = \begin{pmatrix} i & \lambda j - i^2 \\ 1 & \lambda - i \end{pmatrix} \in PGL(2, \boldsymbol{F}_p).$$

Hence $\phi(\rho)$ is the map $x \mapsto (ix + \lambda j - i^2)/(x + \lambda - i)$.

We will determine the preimage of Δ_∞. It may happen that $g(\Delta_0) = \Delta_\infty$ or $g(\Delta_t) = \Delta_\infty$ for some $1 \le t \le p-1$.

Case 7.1: Suppose that $g(\Delta_0) = \Delta_\infty$.

From $g(\sum_\ell x_\ell) = ax_{t'}$ for some $0 \le t' \le p-1$ and some $a \in \boldsymbol{C} \setminus \{0\}$, we find that

$$c \cdot \sum_{0 \le \ell' \le p-1} \left(\sum_{0 \le \ell \le p-1} \xi^{\alpha_\ell + i\binom{\ell'-k\ell}{2}} \right) x_{\ell'} = ax_{t'}$$

where $\alpha_\ell = \dfrac{1}{2}[\ell^2(\frac{i^2k^2}{i-j} - i - ik^2) + i\ell]$.

Hence

$$\sum_{0 \le \ell \le p-1} \zeta^{\alpha_\ell + i\binom{\ell'-k\ell}{2}} = 0$$

for any $\ell' \not\equiv t' \pmod p$.

This will imply $j \equiv i - ik^2 \pmod p$. The verification is omitted.

Case 7.2: Suppose that $g(\Delta_t) = \Delta_\infty$ for some $1 \le t \le p-1$.

From $g(\sum_\ell \zeta^{t\binom{\ell}{2}} x_\ell) = ax_{t'}$ for some $0 \le t' \le p-1$ and some $a \in \boldsymbol{C} \setminus \{0\}$, we find that

$$c \cdot \sum_{0 \le \ell' \le p-1} \left(\sum_{0 \le \ell \le p-1} \zeta^{\alpha_\ell + t\binom{\ell}{2} + i\binom{\ell'-k\ell}{2}} \right) x_{\ell'} = ax_{t'}$$

where α_ℓ is same as in the previous case.

It follows that

$$\sum_{0\le\ell\le p-1}\zeta^{\alpha_\ell+t\binom{\ell}{2}+i\binom{\ell'-k\ell}{2}}=0$$

for any $\ell'\not\equiv t'\pmod p$.

Note that

$$\begin{aligned}\sum_{0\le\ell\le p-1}\zeta^{\alpha_\ell+t\binom{\ell}{2}+i\binom{\ell'-k\ell}{2}}&=\sum_{0\le\ell\le p-1}\zeta^{\alpha_\ell+t\binom{\ell}{2}+i[\binom{\ell'}{2}+\binom{-k\ell}{2}-k\ell\ell']}\\&=\zeta^{i\binom{\ell'}{2}}\sum_{0\le\ell\le p-1}\zeta^{\frac12[\ell^2(\frac{i^2k^2}{i-j}-i+t)+\ell(i-t+ik-2ik\ell')]}\end{aligned}$$

is never zero by Lemma 4.6, provided that $\frac{i^2k^2}{i-j}-i+t\not\equiv 0\pmod p$.

We conclude that $\frac{i^2k^2}{i-j}-i+t\equiv 0\pmod p$.

Combine the results of Case 7.1 and Case 7.2. We find $g(\Delta_t)=\Delta_\infty$ with $t=i-\frac{i^2k^2}{i-j}$. Hence $\lambda=(i-j)^{-1}i^2k^2$.

7. Proof of Theorem 2.6 and Theorem 2.7.

PROOF OF THEOREM 2.6 (1).

The "determinants" of the fractional linear transformation in (i) $\sim$ (vii) of (E) in Theorem 2.5 belong to $\boldsymbol{F}_p^{\times 2}$. Thus these elements may be adjusted to become elements in $PSL(2,\boldsymbol{F}_p)$.

Because of Theorem 2.6(1) it is important to know the subgroups in $PSL(2,\boldsymbol{F}_p)$.

THEOREM 7.1 ([**Hu**, 8.27 Hauptsatz, p.213]). *A subgroup of $PSL(2,\boldsymbol{F}_p)$ is isomorphic to one of the following groups,*

(i) *a cyclic group of order m, where m is a divisor of $p,(p-1)/2$ or $(p+1)/2$,*

(ii) *a dihedral group of order $2m$, where m is a divisor of $(p-1)/2$ or $(p+1)/2$,*

(iii) *the alternating group A_4,*

(iv) *the symmetric group S_4 if $p^2\equiv 1\pmod{16}$,*

(v) *the alternating group A_5 if $p=5$ or $p^2\equiv 1\pmod 5$,*

(vi) *a semi-direct product of a cyclic group of order p with a cyclic group of order m, where m is a divisor of $p-1$,*

(vii) *the group $PSL(2,\boldsymbol{F}_p)$ itself.*

PROOF OF THEOREM 2.7.

(1) It is routine to verify that $\rho_1\tau\rho_1^{-1}=\tau$, $\rho_1\sigma\rho_1^{-1}=\sigma\tau$, $\rho_2\tau\rho_2^{-1}=\sigma^{-1}$,

$\rho_2\sigma\rho_2^{-1} = \tau$, $\rho_3\tau\rho_3^{-1} = \tau^{h^{-1}}$, $\rho_3\sigma\rho_3^{-1} = \sigma^h$. In the notation of Theorem 2.6(2), we find that

$$\Phi(\rho_1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \Phi(\rho_2) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \Phi(\rho_3) = \begin{pmatrix} h^{-1} & 0 \\ 0 & h \end{pmatrix}.$$

Thus $\Phi(\rho_i) \in SL(2, \boldsymbol{F}_p)$ for $i = 1, 2, 3$. Clearly $\phi(\rho_i) = \pi_0\Phi(\rho_i)$ by Lemma 5.3.

Since every matrix in $SL(2, \boldsymbol{F}_p)$ can be brought to a diagonal matrix by the row operations and the column operations, it follows that $SL(2, \boldsymbol{F}_p)$ is generated by $\Phi(\rho_1), \Phi(\rho_2), \Phi(\rho_3)$. Thus $\phi(G_0) = PSL(2, \boldsymbol{F}_p)$.

Note that λ_{p-1} belongs to the cyclic subgroup generated by ρ_3. It follows that the order of G_0 is $2p^3 \cdot |PSL(2, \boldsymbol{F}_p)| = p^4(p^2 - 1)$. Obviously G_0 is primitive.

(2) Since $\phi(G) \subset \phi(G_0)$, hence $G \subset G_0$. The proof of the remaining part will be delayed till we finish the proof of Theorem 2.6.

Proof of Theorem 2.6 (2) and (3).

By Theorem 2.7(2), $G \subset G_0$. Hence $\Phi(G) \subset \Phi(G_0)$. In the proof of Theorem 2.6(1) we have found that $\Phi(G_0) = \langle \Phi(\rho_i) : i = 1, 2, 3\rangle \subset SL(2, \boldsymbol{F}_p)$ and $\phi(\rho_i) = \pi_0\Phi(\rho_i)$. Hence the same conclusions are valid for all elements of G. Note that λ_{p-1} is not in the kernel of Φ. Apply Lemma 4.3 to show that $\mathrm{Ker}(\Phi) = D$.

Lemma 7.2. *Keep the assumptions and notation in Theorem* 2.7. *If G_1, G_2 are primitive subgroups of G_0 containing D such that $\Phi(G_1)$ and $\Phi(G_2)$ are conjugate to each other in $SL(2, \boldsymbol{F}_p)$, then G_1 is conjugate to G_2 in G_0. In particular, they are equivalent in $SL(p, \boldsymbol{C})$.*

Proof. Suppose that $\Phi(G_2) = g'\Phi(G_1)g'^{-1}$ for some $g' \in SL(2, \boldsymbol{F}_p)$. Choose a preimage $g \in G_0$ of g'. Then $G_2 = gG_1g^{-1}$. □

Lemma 7.3. *Keep the assumptions and notation in Theorem* 2.5. *If $\phi(G)$ is isomorphic to a cyclic group of order m with m dividing $p(p-1)/2$ or the semi-direct product in* (vi) *of Theorem* 7.1, *then G is not a primitive group.*

Proof. We may assume that $\phi(G)$ is nontrivial. If $\phi(G)$ is a subgroup of a cyclic group of order p or $(p-1)/2$, it is conjugate to a cyclic group with generator of the form $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ for some $a \in \boldsymbol{F}_p \setminus \{0\}$. Apply Part (ii) of (E) in Theorem 2.5. The group G is equivalent to a monomial group.

Now suppose $\phi(G)$ is isomorphic to the semi-direct product in (vi) of Theorem 7.1. Without loss of generality we may assume that the generator of the

cyclic subgroup of order p in $\phi(G)$ is of the form $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. It is routine to verify that $\phi(G)$ is a triangular matrix group in $PSL(2, \boldsymbol{F}_p)$. Apply Part (ii) of (E) in Theorem 2.5 to show that G is a monomial group. □

LEMMA 7.4. *If Γ is a subgroup of $SL(2, \boldsymbol{F}_p)$ and $\pi_0(\Gamma) = PSL(2, \boldsymbol{F}_p)$, where $\pi_0 : SL(2, \boldsymbol{F}_p) \to PSL(2, \boldsymbol{F}_p)$ is the canonical projection, then $\Gamma = SL(2, \boldsymbol{F}_p)$.*

PROOF.

Case 1: $-I_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \Gamma$.

Clearly we have $\Gamma = SL(2, \boldsymbol{F}_p)$.

Case 2: $-I_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \notin \Gamma$.

Since Γ is an index two subgroup in $SL(2, \boldsymbol{F}_p)$, it is a normal subgroup. Thus $SL(2, \boldsymbol{F}_p)$ is a direct product of Γ and $-I_2$.

On the other hand, Γ has an element of order two; call it ρ. Note that ρ and $-I_2$ are conjugate in $GL(2, \boldsymbol{F}_p)$. Since $-I_2$ is in the center of $GL(2, \boldsymbol{F}_p)$, it follows that $\rho = -I_2$. A contradiction. □

PROOF OF THEOREM 2.7 (2) (continued).

Suppose p^4 is a divisor of $|G|$. Then p divides the order of $\phi(G)$. By Theorem 7.1 and Lemma 7.3 we find that $\phi(G) = PSL(2, \boldsymbol{F}_p)$. By Theorem 2.6 $\pi_0(\Phi(G)) = PSL(2, \boldsymbol{F}_p)$. Thus $\Phi(G) = SL(2, \boldsymbol{F}_p)$ by Lemma 7.4. It follows that $G = G_0$.

If p^4 doesn't divide $|G|$, then the order of $\Phi(G) \cong G/D$ is relatively prime to that of D. Hence this group extension splits by Schur-Zassenhaus Theorem [**Suz**, Theorem 8.10, p.235]. □

By Theorem 2.7(2) it remains to find subgroups in $SL(2, \boldsymbol{F}_p)$ whose orders are relatively prime to p. It is a special case of Dickson's Theorem [**Suz**, Theorem 6.17, p.404], [**Hu**, p.213]. We record it as the following theorem.

THEOREM 7.5. *Let p be an odd prime number, $q = p^f$ for some positive integer f, and Γ be a subgroup of $SL(2, \boldsymbol{F}_q)$ such that the order of Γ is relatively prime to p. Then Γ is isomorphic to one of the following groups,*

(i) *a cyclic group of order m, where m is a divisor of $q-1$ or $q+1$,*

(ii) *a group of order $4m$ generated by x, y with relation $x^m = y^2$ and $y^{-1}xy = x^{-1}$, where $m \geq 2$ and is a divisor of $(q-1)/2$ or $(q+1)/2$,*

(iii) *the group $SL(2, \boldsymbol{F}_3)$ if $p \neq 3$,*

(iv) *the group $\widehat{S_4}$ if $q^2 \equiv 1 \pmod{16}$, where $\widehat{S_4}$ is the representation group of the symmetric group of degree 4 in which the transpositions correspond to the*

elements of order 4;

(v) *the group* $SL(2, \boldsymbol{F}_5)$ *if* $q^2 \equiv 1 \pmod 5$.

The group in (ii) *will be called a binary dihedral group of order* $4m$.

8. Subgroups of $SL(2, \boldsymbol{F}_q)$.

In this section we will find explicit generators of all the subgroups (up to conjugation in $SL(2, \boldsymbol{F}_q)$) in Theorem 7.5. We emphasize that q is an odd prime power.

First we give an isomorphism of $SU(2, \boldsymbol{F}_{q^2})$ onto $SL(2, \boldsymbol{F}_q)$.

DEFINITION 8.1. For any $a \in \boldsymbol{F}_{q^2}$, write $\bar{a} = a^q$, the conjugate of a. We define $SU(2, \boldsymbol{F}_{q^2})$ by

$$SU(2, \boldsymbol{F}_{q^2}) = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \in SL(2, \boldsymbol{F}_{q^2}) : a, b \in \boldsymbol{F}_{q^2} \right\}.$$

LEMMA 8.2. *Let* $\alpha \in \boldsymbol{F}_{q^2} \setminus \boldsymbol{F}_q$ *be any element such that* $\alpha\bar{\alpha} = -1$. *Define a group homomorphism* Ψ *by*

$$\begin{aligned} \Psi : \quad & SU(2, \boldsymbol{F}_{q^2}) \longrightarrow SL(2, \boldsymbol{F}_q) \\ & \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \mapsto \begin{pmatrix} 1 & \alpha \\ -\alpha & 1 \end{pmatrix} \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ -\alpha & 1 \end{pmatrix}^{-1}. \end{aligned}$$

Then Ψ *is an isomorphism.*

REMARKS. The existence of α is ensured by the fact that the norm map from $\boldsymbol{F}_{q^2}^{\times}$ to $\boldsymbol{F}_q^{\times}$ is surjective and the preimage of -1 is not contained in $\boldsymbol{F}_q$.

PROOF. The map Ψ is well-defined because it is routine to verify that each entry of $\Psi(A)$, where $A \in SU(2, \boldsymbol{F}_{q^2})$ is invariant under the conjugation map on $\boldsymbol{F}_{q^2}$. Since $SL(2, \boldsymbol{F}_q)$ and $SU(2, \boldsymbol{F}_{q^2})$ have the same order and Ψ is injective, thus Ψ is an isomorphism. See [**Hu**, 8.8 Hilfssatz, p.194] for a somewhat different proof. □

Recall several facts about $SL(2, \boldsymbol{F}_q)$.

LEMMA 8.3 ([**Suz**, (6.23), p.410]).

(1) *There exist an element* A_1 *of order* $q-1$ *and an element* A_2 *of order* $q+1$ *in* $SL(2, \boldsymbol{F}_q)$;

(2) *Any cyclic subgroup of* $SL(2, \boldsymbol{F}_q)$ *with order relatively prime to* q *is conjugate to a subgroup of* $\langle A_1\rangle$ *or* $\langle A_2\rangle$;

(3) *If* $q \neq 3$ (*resp.* $q = 3$ *and* $i = 2$), *the normalizer of* A_i *in* $SL(2, \boldsymbol{F}_q)$ *is a binary dihedral group of order* $2(q + (-1)^i)$ *defined in Theorem* 7.5(ii). *In particular, all binary dihedral groups of order* $2(q + 1)$ (*resp. of order* $2(q - 1)$ *with* $q > 3$) *are conjugate in* $SL(2, \boldsymbol{F}_q)$.

LEMMA 8.4 ([**Suz**, (6.19), p.407]). *Let* x *be a non-scalar matrix of* $SL(2, \boldsymbol{F}_q)$.
(1) x^2 *is a scalar matrix if and only if the trace of* x *is* 0.
(2) x^3 *is the identity matrix if and only if the trace of* x *is* -1.

LEMMA 8.5. *Let* $m \geq 2$ *be an integer, and* $\Gamma = \langle x, y : x^m = y^2, y^{-1}xy = x^{-1}\rangle$ *be a binary dihedral group of order* $4m$. *Let* $n \geq 2$ *be a divisor of* m.

(1) *If* Γ' *is a non-abelian subgroup of* Γ *with order* $4n$, *then it is isomorphic to a binary dihedral group of order* $4n$.

(2) *There are at most two conjugacy classes for binary dihedral groups of order* $4n$ *contained in* Γ. *There are precisely two such conjugacy classes if and only if* m/n *is even.*

PROOF. Let Γ' be a non-abelian subgroup with order $4n$ contained in Γ.

Since Γ' is not contained in $\langle x\rangle$, Γ' contains an element u outside $\langle x\rangle$. Hence $u = x^k y$ for some k. Note that the order of u is 4. Clearly $\Gamma = \langle x, u\rangle$ with $u^{-1}xu = x^{-1}$.

Let v be an element in $\Gamma' \setminus \langle u\rangle$ of maximal order. Note that the order of v must be even. Furthermore we may assume that $v = x^i$ with $i = m/n$. For, if $v = x^i u$ then $x^i \in \Gamma'$ and we may replace $x^i u$ by x^i. It is not difficult to show that $\Gamma' = \langle v, u\rangle$ and is a binary dihedral group of order $4n$.

For any integers j and t, note that $x^j\Gamma' x^{-j} = \langle v, x^{2j}u\rangle = \langle v, v^t x^{2j}u\rangle = \langle v, x^{ti+2j}u\rangle$. In particular, if $i = m/n$ is odd, then Γ' is conjugate to $\langle v, y\rangle$. Similarly, if m/n is even, then Γ' is conjugate either to $\langle v, y\rangle$ or $\langle v, xy\rangle$; it is not difficult to see that $\langle v, y\rangle$ is not conjugate to $\langle v, xy\rangle$ in Γ. □

DEFINITION 8.6. We will define several elements in $\boldsymbol{F}_{q^2}$, which will be used in the remaining part of this section. Let ξ be a fixed generator of $\boldsymbol{F}_{q^2}^{\times}$. Define $\alpha = \xi^{(q-1)/2}, \eta = \xi^{q+1}$ and $\sigma = \xi^{(q^2-1)/4}$. Note that α satisfies the assumption in Lemma 8.2 and σ is a square root of -1. We will choose $\epsilon \in \boldsymbol{F}_{q^2} \setminus \boldsymbol{F}_q$ such that $\epsilon\,\bar{\epsilon} = 1/2$, which is possible because the norm map from $\boldsymbol{F}_{q^2}^{\times}$ to $\boldsymbol{F}_q^{\times}$ is surjective.

DEFINITION 8.7. We will define some matrices in $SL(2, \boldsymbol{F}_q)$ by

$$\tilde{z} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \tilde{x} = \begin{pmatrix} \eta^{-1} & 0 \\ 0 & \eta \end{pmatrix}, \tilde{y} = \begin{pmatrix} 1 & \alpha^{-1} - \alpha \\ \alpha^{-1} - \alpha & \alpha^{-2} + \alpha^2 - 1 \end{pmatrix}.$$

Note that $\tilde{y}$ is equal to

$$\begin{pmatrix} 1 & \alpha \\ -\alpha & 1 \end{pmatrix} \begin{pmatrix} \alpha^2 & 0 \\ 0 & \alpha^{-2} \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ -\alpha & 1 \end{pmatrix}^{-1},$$

which is the pull-back of some matrix of $SU(2, \boldsymbol{F}_{q^2})$ by Lemma 8.2.

Now we will describe conjugacy classes of subgroups in Theorem 7.5.

PROPOSITION 8.8. *The case of cyclic groups.*

Any abelian subgroups of $SL(2, \boldsymbol{F}_q)$ of order relatively prime to q are cyclic groups. Moreover, a cyclic subgroup of $SL(2, \boldsymbol{F}_q)$ of order m dividing $q-1$ (resp. $q+1$) is conjugate to the subgroup $\langle \tilde{x}^k \rangle$, where $q-1 = mk$ (resp. $\langle \tilde{y}^k \rangle$, where $q+1 = mk$).

PROOF. Apply Theorem 7.5 and Lemma 8.3. □

THEOREM 8.9. *The case of binary dihedral groups.*

(1) *The groups $\langle \tilde{x}, \tilde{z} \rangle$ and $\langle \tilde{y}, \tilde{z} \rangle$ are binary dihedral groups of order $2(q-1)$ (if $q \neq 3$) and $2(q+1)$ respectively. Every binary dihedral group of $SL(2, \boldsymbol{F}_q)$ with order $2(q-1)$ (if $q \neq 3$) or $2(q+1)$ is conjugate to $\langle \tilde{x}, \tilde{z} \rangle$ or $\langle \tilde{y}, \tilde{z} \rangle$.*

(2) *Assume that $q \neq 3$. Let $n \geq 4$ be an even divisor of $q-1$ and write $q-1 = nk$. If k is odd, every binary dihedral group in $SL(2, \boldsymbol{F}_q)$ with order $2n$ is conjugate to $\langle \tilde{x}^k, \tilde{z} \rangle$. If k is even, $\langle \tilde{x}^k, \tilde{z} \rangle$ and $\langle \tilde{x}^k, \tilde{x}\tilde{z} \rangle$ are two non-conjugate binary dihedral groups of order $2n$; every binary dihedral group of order $2n$ is conjugate to one of them.*

(3) *Let $n \geq 4$ be an even divisor of $q+1$ and write $q+1 = nk$. If k is odd, every binary dihedral group in $SL(2, \boldsymbol{F}_q)$ with order $2n$ is conjugate to $\langle \tilde{y}^k, \tilde{z} \rangle$. If k is even, $\langle \tilde{y}^k, \tilde{z} \rangle$ and $\langle \tilde{y}^k, \tilde{y}\tilde{z} \rangle$ are two non-conjugate binary dihedral groups of order $2n$; every binary dihedral group of order $2n$ is conjugate to one of them.*

PROOF. (1) follows from Lemma 8.3. (2) and (3) follow from Lemma 8.5 because every binary dihedral group of order $2m$ can be enlarged to a binary dihedral group of order $2(q-1)$ or $2(q+1)$ by Lemma 8.3. □

DEFINITION 8.10. For $i = 0, 1$, we will define elements a_i, b_i, u_i, w_i, s_i,

$t_i \in \boldsymbol{F}_q$.

If $q \equiv 1 \pmod 4$, define

$$a_i = \frac{\eta^i}{4} - \eta^{-i}, \quad b_i = -\sigma\left(\frac{\eta^i}{4} + \eta^{-i}\right)$$

where $i = 0, 1$.

If $q \equiv 3 \pmod 4$, define

$$a_i = \frac{-2\alpha\sigma(\epsilon^2\alpha^{2i} + \epsilon^{2q}\alpha^{-2i}) + (1-\alpha^2)(\epsilon^2\alpha^{2i} - \epsilon^{2q}\alpha^{-2i})}{1+\alpha^2},$$
$$b_i = \frac{2\alpha(\epsilon^2\alpha^{2i} - \epsilon^{2q}\alpha^{-2i}) + \sigma(1-\alpha^2)(\epsilon^2\alpha^{2i} + \epsilon^{2q}\alpha^{-2i})}{1+\alpha^2}$$

where $i = 0, 1$.

After a_i, b_i have been defined, we define u_i, w_i, s_i, t_i by

$$u_i = \frac{b_i - a_i - 1}{2}, \quad w_i = \frac{b_i + a_i - 1}{2},$$
$$s_i(a_i - b_i) = t_i(a_i + b_i)$$

where $s_i^2 + t_i^2 = -1$.

THEOREM 8.11. *The case of $SL(2, \boldsymbol{F}_3)$ if $p \neq 3$, and $\widehat{S_4}$ if $q^2 \equiv 1 \pmod{16}$. We define matrices $E_i, L_i \in SL(2, \boldsymbol{F}_q)$ by*

$$E_i = \begin{pmatrix} u_i & w_i \\ w_i + 1 & -1 - u_i \end{pmatrix}, \; L_i = \begin{pmatrix} s_i & t_i \\ t_i & -s_i \end{pmatrix}$$

where $i = 0, 1$.

(1) *Assume that $q \neq 3$.*

The subgroups $\langle \tilde{z}, E_0 \rangle$ and $\langle \tilde{z}, E_1 \rangle$ are not conjugate in $SL(2, \boldsymbol{F}_p)$ if and only if $q^2 \equiv 1 \pmod{16}$; both of these two groups are isomorphic to $SL(2, \boldsymbol{F}_3)$. Any subgroup of $SL(2, \boldsymbol{F}_p)$, which is isomorphic to $SL(2, \boldsymbol{F}_3)$, is conjugate to $\langle \tilde{z}, E_0 \rangle$ or $\langle \tilde{z}, E_1 \rangle$.

(2) *Assume $q^2 \equiv 1 \pmod{16}$.*

The subgroups $\langle \tilde{z}, E_0, L_0 \rangle$ and $\langle \tilde{z}, E_1, L_1 \rangle$ are not conjugate in $SL(2, \boldsymbol{F}_p)$; both of them are isomorphic to $\widehat{S_4}$. Any subgroup of $SL(2, \boldsymbol{F}_p)$, which is isomorphic to

$\widehat{S_4}$, *is conjugate to* $\langle \tilde{z}, E_0, L_0 \rangle$ *or* $\langle \tilde{z}, E_1, L_1 \rangle$.

PROOF. For brevity we will write $\Sigma = SL(2, \boldsymbol{F}_q)$ and denote a quaternion group of order 8 by Q_8.

Step 1: We will determine conjugacy classes of subgroups in Σ, which are isomorphic to Q_8.

Note that any subgroup in Σ, which is isomorphic to Q_8, is conjugate to $\langle \tilde{z}, M \rangle$, where $\tilde{z}$ is defined in Definition 8.7, M is a matrix of order 4 such that $\tilde{z}^2 = M^2, M^{-1}\tilde{z}M = \tilde{z}^{-1}$. By Lemma 8.4 M has the form

$$M = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$$

where $a^2 + bc = -1$.

Apply the relation $M^{-1}\tilde{z}M = \tilde{z}^{-1}$. We find that $b = c$.

Step 2: For the group $\langle \tilde{z}, M \rangle$ constructed in Step 1, we will find a matrix E such that the order of E is 3 and $\langle \tilde{z}, M, E \rangle$ is isomorphic to $SL(2, \boldsymbol{F}_3)$. In particular, $\langle \tilde{z}, M \rangle$ is a normal subgroup of $\langle \tilde{z}, M, E \rangle$.

Choose any elements $a, b \in \boldsymbol{F}_q$ satisfying $a^2 + b^2 = -1$. Define $u = (b - a - 1)/2, w = (b + a - 1)/2$. Then $u(1 + u) + w(w + 1) = -1$. (We will explain later the reason why we choose u, w in this way.) Define E by

$$E = \begin{pmatrix} u & w \\ w + 1 & -1 - u \end{pmatrix}. \tag{8.1}$$

Then $E \in SL(2, \boldsymbol{F}_q)$ is a matrix of order 3 by Lemma 8.4.

Define

$$y = E^{-1}\tilde{z}E = \begin{pmatrix} 1 + u + w & w - u \\ w - u & -1 - u - w \end{pmatrix}.$$

Substituting the relations $u = (b - a - 1)/2, w = (b + a - 1)/2$ into entries of the above matrix, we get

$$\begin{pmatrix} 1 + u + w & w - u \\ w - u & -1 - u - w \end{pmatrix} = \begin{pmatrix} b & a \\ a & -b \end{pmatrix}.$$

Moreover, it is routine to verify that $E^{-1}yE = \tilde{z}y$. In fact, starting from a matrix E defined by (8.1) (u, w : undetermined coefficients) and defining y by

requiring $y = E^{-1}\tilde{z}E$ and $E^{-1}yE = \tilde{z}y$, we are led to the equation $u(1+u) + w(w+1) = -1$. To solve this equation, we may choose $u = (b-a-1)/2, w = (b+a-1)/2$.

We conclude that $\langle \tilde{z}, y\rangle$ is isomorphic to Q_8 (by Step 1) and $\langle \tilde{z}, E\rangle$ is isomorphic to $SL(2, \boldsymbol{F}_3)$.

Step 3: If $q^2 \equiv 1 \pmod{16}$, then 2 is a square in $\boldsymbol{F}_q$.

Write $q = p^f$ for some positive integer f. If f is an even integer, since $\boldsymbol{F}_{p^2}$ is the unique quadratic extension of the prime field, the equation $X^2 - 2$ is reducible in $\boldsymbol{F}_{p^2}[X]$. Now assume that f is an odd integer. It follows that $q \equiv p \pmod 8$. Since $q^2 \equiv 1 \pmod{16}$, it is necessary that $p \equiv 1$ or $-1 \pmod 8$. Thus 2 is a square in $\boldsymbol{F}_p$ by the quadratic reciprocity law.

Step 4: If $q^2 \equiv 1 \pmod{16}$, we will find a matrix L such that $L^2 = -I_2$ and $\langle \tilde{z}, E, L\rangle \cong \widehat{S_4}$. In particular $\langle \tilde{z}, y\rangle$ is normal in $\langle \tilde{z}, E, L\rangle$.

By Lemma 8.4 and Step 1, choose L to be

$$L = \begin{pmatrix} s & t \\ t & -s \end{pmatrix}$$

where s, t are any elements in $\boldsymbol{F}_q$ satisfying $s^2 + t^2 = -1$. We require furthermore that $s(a-b) = t(a+b)$; be careful that, if $a = b$, choose $s^2 = -1, t = 0$; if $a = -b$, choose $s = 0, t^2 = -1$. (This is possible: If $a = b$ or $-b$, plugging in the relation $a^2 + b^2 = -1$, we get $2a^2 = -1$. Since 2 is a square in $\boldsymbol{F}_q$ by Step 3, so is -1.)

It is easy to verify that $L^{-1}EL = E^{-1}, L^{-1}\tilde{z}L = \tilde{z}^{-1}, L^{-1}yL = y\tilde{z}$. Thus $\langle \tilde{z}, E, L\rangle \cong \widehat{S_4}$.

Step 5: For a finite group Γ, denote by $O_2(\Gamma)$ the maximal normal 2-subgroup of Γ. Consider two subgroups $T_j (j = 0, 1)$ in Σ which are isomorphic to $SL(2, 3)$ (resp. $\widehat{S_4}$). We will prove that T_0 and T_1 are conjugate in Σ if and only if $O_2(T_0)$ and $O_2(T_1)$ are conjugate in Σ. Thus the conjugation problem in Σ for subgroups isomorphic to $SL(2, 3)$ (resp. $\widehat{S_4}$) is equivalent to that for subgroups isomorphic to Q_8 because the maximal normal 2-subgroup of $SL(2, 3)$ (resp. $\widehat{S_4}$) is isomorphic to Q_8.

It suffices to show that, if $O_2(T_0)$ and $O_2(T_1)$ are conjugate in Σ, then T_0 and T_1 are conjugate in Σ.

Consider the normalizer of $O_2(T_i)$ in Σ for $i = 0, 1$. Since $O_2(T_i)$ is isomorphic to Q_8 and the normalizer contains T_i and is a subgroup of Σ, we find that, by Theorem 7.5, this subgroup is either isomorphic to $\widehat{S_4}$ if $q^2 \equiv 1 \pmod{16}$, or isomorphic to $SL(2, 3)$ otherwise. It follows that either T_i equals to the normalizer of $O_2(T_i)$ in Σ or T_i is an index 2 subgroup of the normalizer of $O_2(T_i)$ in Σ. The

latter possibility occurs only when $q^2 \equiv 1 \pmod{16}$. However, the group $\widehat{S_4}$ has only one subgroup of index 2. Thus, if $O_2(T_i)$ are conjugate in Σ for $i = 0, 1$, then the normalizer of $O_2(T_i)$ in Σ are conjugate and therefore T_i are conjugate.

Step 6: We will solve the conjugation problem for subgroups isomorphic to Q_8. In fact, we will exhibit two such subgroups which are possibly non-conjugate and prove that (i) Σ has at most two conjugacy classes of subgroups isomorphic to Q_8, and (ii) Σ has precisely two conjugacy classes of such subgroups if and only if $q^2 \equiv 1 \pmod{16}$.

Case 1: $q \equiv 1 \pmod{4}$.

Recall the definitions of $\xi, \eta, \cdots$ in Definition 8.6 and $\tilde{z}, \tilde{x}, \cdots$ in Definition 8.7. Note that $\tilde{z}, \tilde{x} \in \Sigma$. Define a matrix $y \in \Sigma$ by

$$y = \begin{pmatrix} \sigma & 0 \\ 0 & \sigma^{-1} \end{pmatrix}.$$

A subgroup of Σ, which is isomorphic to Q_8, is conjugate to $\langle y, \tilde{z}\tilde{x}^i \rangle$ for some i. The conjugation by $\tilde{x}$ repeatedly will reduce these subgroups to at most two conjugacy classes : $\langle y, \tilde{z} \rangle$ and $\langle y, \tilde{z}\tilde{x} \rangle$. Note that both $\langle y, \tilde{z} \rangle$ and $\langle y, \tilde{z}\tilde{x} \rangle$ are binary dihedral groups. By Theorem 8.9(2), these two subgroups are not conjugate in Σ if and only if $q - 1 \equiv 0 \pmod{8}$, i.e. $q^2 \equiv 1 \pmod{16}$.

Case 2: $q \equiv 3 \pmod{4}$.

Imitate the proof of the above case and construct the subgroups $\langle y, \tilde{z} \rangle$ and $\langle y, \tilde{z}\bar{x} \rangle$ in $SU(2, \boldsymbol{F}_{q^2})$, where

$$\bar{x} = \begin{pmatrix} \alpha^2 & 0 \\ 0 & \alpha^{2q} \end{pmatrix}.$$

Note that the conjugation by $\bar{x}$ is still an inner automorphism of $SU(2, \boldsymbol{F}_{q^2})$. Thus there are at most two conjugacy classes in $SU(2, \boldsymbol{F}_{q^2})$: $\langle y, \tilde{z} \rangle$ and $\langle y, \tilde{z}\bar{x} \rangle$. Pull back these information from $SU(2, \boldsymbol{F}_{q^2})$ to Σ by Lemma 8.2. Apply Theorem 8.9 (3). We find that these two subgroups are not conjugate in Σ if and only if $q + 1 \equiv 0 \pmod{8}$, i.e. $q^2 \equiv 1 \pmod{16}$.

Step 7: We will construct explicitly the conjugacy classes of subgroups isomorphic to $SL(2, 3)$ or $\widehat{S_4}$. Because of Step 5, we will construct conjugacy classes of subgroups isomorphic to Q_8 with the form in Step 1.

First we solve the question for the case $q \equiv 1 \pmod{4}$. The remaining case will be solved in Step 8.

Define

$$S = \begin{pmatrix} 1 & -\sigma/2 \\ -\sigma & 1/2 \end{pmatrix}.$$

Then

$$S^{-1}\tilde{z}S = \begin{pmatrix} \sigma & 0 \\ 0 & \sigma^{-1} \end{pmatrix}.$$

Now define $y_0 = S\tilde{z}S^{-1}$ and $y_1 = S\tilde{x}\tilde{z}S^{-1}$. Then

$$y_i = \begin{pmatrix} -\sigma(\eta^i/4 + \eta^{-i}) & \eta^i/4 - \eta^{-i} \\ \eta^i/4 - \eta^{-i} & \sigma(\eta^i/4 + \eta^{-i}) \end{pmatrix}.$$

Clearly $\langle \tilde{z}, y_i \rangle \cong Q_8$. Corresponding to y_i we can construct E_i and L_i as in Step 2 and Step 4 so that $\langle \tilde{z}, E_i \rangle \cong SL(2,3), \langle \tilde{z}, E_i, L_i \rangle \cong \widehat{S_4}$.

Step 8: The case $q \equiv 3 \pmod 4$.

We will construct similar groups in $SU(2, \boldsymbol{F}_{q^2})$ and pull back the information by Lemma 8.2. Explicitly define

$$T = \begin{pmatrix} \epsilon & -\bar{\epsilon}\sigma \\ -\sigma\epsilon & \bar{\epsilon} \end{pmatrix} \in SU(2, \boldsymbol{F}_{q^2})$$

where ϵ is defined in Definition 8.6.

It is straightforward to check that

$$T^{-1}\tilde{z}T = \begin{pmatrix} \sigma & 0 \\ 0 & \sigma^{-1} \end{pmatrix}.$$

Define

$$y_i' = \begin{pmatrix} 0 & \alpha^{2i} \\ -\alpha^{-2i} & 0 \end{pmatrix}.$$

We find that $\langle T^{-1}\tilde{z}T, y_i' \rangle \cong Q_8$.

Define

$$y_i = \begin{pmatrix} 1 & \alpha \\ -\alpha & 1 \end{pmatrix} T y_i' T^{-1} \begin{pmatrix} 1 & \alpha \\ -\alpha & 1 \end{pmatrix}^{-1}.$$

It is easy to find that

$$y_i = \begin{pmatrix} b_i & a_i \\ a_i & -b_i \end{pmatrix}$$

where, for $i = 0, 1$,

$$b_i = \frac{2\alpha(\epsilon^2\alpha^{2i} - \epsilon^{2q}\alpha^{-2i}) + \sigma(1-\alpha^2)(\epsilon^2\alpha^{2i} + \epsilon^{2q}\alpha^{-2i})}{1+\alpha^2},$$
$$a_i = \frac{-2\alpha\sigma(\epsilon^2\alpha^{2i} + \epsilon^{2q}\alpha^{-2i}) + (1-\alpha^2)(\epsilon^2\alpha^{2i} - \epsilon^{2q}\alpha^{-2i})}{1+\alpha^2}.$$

These subgroups $\langle \tilde{z}, y_i \rangle$ are isomorphic to Q_8. Once they are constructed, we may find the corresponding E_i and L_i as in Step 7. □

DEFINITION 8.12. Assume that $q^2 \equiv 1 \pmod 5$. Recall the definition of η, α in Definition 8.6.

If $q \equiv 1 \pmod 5$, define $u = (\eta^{2(q-1)/5} - 1)^{-1}$.

If $q \equiv -1 \pmod 5$, define $\beta = \alpha^{2(q+1)/5}$, $u = (\beta^2 - 1)^{-1}$, and $w' \in \boldsymbol{F}_{q^2}$ satisfies $w'\bar{w}' = 1 - u\bar{u}$; such an element w' does exist because the norm map from $\boldsymbol{F}_{q^2}^{\times}$ to $\boldsymbol{F}_q^{\times}$ is surjective.

THEOREM 8.13. *The case of* $SL(2, \boldsymbol{F}_5)$.

(1) *Assume that* $q \equiv 1 \pmod 5$.

Define matrices $B, E_1, E_2 \in SL(2, \boldsymbol{F}_q)$ *by*

$$B = \begin{pmatrix} \eta^{(q-1)/5} & 0 \\ 0 & \eta^{-(q-1)/5} \end{pmatrix}, \quad E_i = \begin{pmatrix} u & \eta^{-i} \\ -\eta^i(1+u+u^2) & -1-u \end{pmatrix}$$

where $i = 0, 1$.

Then $\langle B, E_0 \rangle$ *and* $\langle B, E_1 \rangle$ *are not conjugate in* $SL(2, \boldsymbol{F}_q)$; *both of them are isomorphic to* $SL(2, \boldsymbol{F}_5)$. *Moreover, any subgroup of* $SL(2, \boldsymbol{F}_q)$, *which is isomorphic to* $SL(2, \boldsymbol{F}_5)$, *is conjugate to* $\langle B, E_0 \rangle$ *or* $\langle B, E_1 \rangle$.

(2) *Assume that* $q \equiv -1 \pmod 5$.

Define matrices $B, E_1, E_2 \in SL(2, \boldsymbol{F}_q)$ *by*

$$B = \frac{1}{\beta(1+\alpha^2)} \begin{pmatrix} \beta^2+\alpha^2 & \alpha(1-\beta^2) \\ \alpha(1-\beta^2) & 1+\alpha^2\beta^2 \end{pmatrix}, \quad E_i = \frac{1}{1+\alpha^2} \begin{pmatrix} \bar{\alpha} & \bar{\beta} \\ \bar{\gamma} & \bar{\delta} \end{pmatrix}$$

where

$$\begin{aligned} \bar{\alpha} &= u - \alpha^2(u+1) + \alpha(\alpha^{2i}w' - \alpha^{-2i}w'^q), \\ \bar{\beta} &= -\alpha(1+2u) + \alpha^{2i}w' + \alpha^{2-2i}w'^q, \\ \bar{\gamma} &= -\alpha(1+2u) - \alpha^{2i+2}w' - \alpha^{-2i}w'^q, \\ \bar{\delta} &= -1 - u + \alpha^2 u - \alpha(\alpha^{2i}w' - \alpha^{-2i}w'^q). \end{aligned}$$

Then $\langle B, E_0\rangle$ and $\langle B, E_1\rangle$ are not conjugate in $SL(2, \boldsymbol{F}_q)$; both of them are isomorphic to $SL(2, \boldsymbol{F}_5)$. Moreover, any subgroup of $SL(2, \boldsymbol{F}_q)$, which is isomorphic to $SL(2, \boldsymbol{F}_5)$, is conjugate to $\langle B, E_0\rangle$ or $\langle B, E_1\rangle$.

PROOF. Denote $\Sigma = SL(2, \boldsymbol{F}_q)$.

Step 1: Recall a standard result about $SL(2, \boldsymbol{F}_5)$ (see [**Suz**, Example 4, p.176]): If K is a group defined by $K = \langle x, y : x^5 = y^3 = 1$, where $(xy)^2$ is a central element of order $2\rangle$, then there is a surjection from K onto $SL(2, \boldsymbol{F}_5)$.

In particular, if we can find elements $x, y \in \Sigma$ such that $x^5 = y^3 = 1$ and $(xy)^2 = -I_2$, by Theorem 7.1 and Theorem 7.5, the subgroup $\langle x, y\rangle$ is isomorphic to $SL(2, \boldsymbol{F}_5)$ or Σ. Since $\Sigma/\langle -I_2\rangle$ is a simple group (remember $q^2 \equiv 1 \pmod 5$), $\langle x, y\rangle$ is isomorphic to $SL(2, \boldsymbol{F}_5)$.

We will consider the case $q \equiv 1 \pmod 5$ first and discuss the case $q \equiv -1 \pmod 5$ later.

Define $a = \eta^{(q-1)/5}$ and

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

We will find matrix $X \in \Sigma$ such that $X \neq I_2$ and

$$(BX)^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad X^3 = 1. \tag{8.2}$$

Step 2: By Lemma 8.4 any matrix of order 3 is of the form

$$\begin{pmatrix} u & w \\ v & -1-u \end{pmatrix}$$

where $u, w, v \in \boldsymbol{F}_q$ with $u(1+u)+wv=-1$.

Define $u=(a^2-1)^{-1}, w \in \boldsymbol{F}_q \setminus \{0\}, v=-w^{-1}(1+u+u^2)$ and

$$E=\begin{pmatrix} u & w \\ v & -1-u \end{pmatrix}.$$

Then E is a solution of Equation (8.2), i.e. $(BE)^2=-I_2$ and $E^3=I_2$. In fact, it is obtained as follows.

For any matrix $X \in \Sigma$ with the form

$$X=\begin{pmatrix} u & w \\ v & -1-u \end{pmatrix},$$

consider BX. Note that

$$(BX)^2=\begin{pmatrix} a^2u^2+vw & a^2uw-w(1+u) \\ uv-a^{-2}v(1+u) & vw+a^{-2}(1+u)^2 \end{pmatrix}.$$

Hence $(BX)^2=-I_2$ if and only if $a^2u^2+vw=-1, w(a^2u-(1+u))=v(u-a^{-2}(1+u))=0$ and $a^{-2}(1+u)^2+vw=-1$.

We claim that $vw \neq 0$. Otherwise, $u(1+u)=-1$ and $a^2=-u^{-2}$. It follows that u is of order 3 in $\boldsymbol{F}_q$ and $a^6=u^{-6}=1$, which is contradictory to the fact that the order of a is 5.

Hence $a^2u-(1+u)=0, u=(a^2-1)^{-1}$ and $v=-w^{-1}(1+u+u^2)$, which is the reason why we define the matrix E. Moreover, from the above discussion, Equation (8.2) has exactly $q-1$ solutions in Σ with w an arbitrary element in $\boldsymbol{F}_q \setminus \{0\}$. Any subgroup of Σ, which is isomorphic to $SL(2, \boldsymbol{F}_5)$, is conjugate to $\langle B, E\rangle$ for some $w \in \boldsymbol{F}_q \setminus \{0\}$.

Step 3: We will consider the question of conjugacy classes.

For any $b \in \boldsymbol{F}_q \setminus \{0\}$, note that

$$\begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix}\begin{pmatrix} u & w \\ v & -1-u \end{pmatrix}\begin{pmatrix} b^{-1} & 0 \\ 0 & b \end{pmatrix}=\begin{pmatrix} u & b^2w \\ b^{-2}v & -1-u \end{pmatrix}.$$

Thus any subgroup of Σ, which is isomorphic to $SL(2, \boldsymbol{F}_5)$, is conjugate to $\langle B, E_0\rangle$ or $\langle B, E_1\rangle$, where E_i is defined by

$$E_i = \begin{pmatrix} u & \eta^{-i} \\ -\eta^i(1+u+u^2) & -1-u \end{pmatrix}$$

where $u = (\eta^{2(q-1)/5} - 1)^{-1}$.

Step 4: We claim that $\langle B, E_0\rangle$ is not conjugate to $\langle B, E_1\rangle$ in Σ.

If not, find $x \in \Sigma$ such that $\langle B, E_1\rangle^x = \langle B, E_0\rangle$, where $\langle B, E_1\rangle^x$ denotes $x^{-1} \cdot \langle B, E_1\rangle \cdot x$.

There is an element $t \in \langle B, E_0\rangle$ such that $\langle B\rangle^x = \langle B\rangle^t$. Hence $xt^{-1} \in N_\Sigma(\langle B\rangle) = \langle \tilde{x}, \tilde{z}\rangle$, where $N_\Sigma(\langle B\rangle)$ denotes the normalizer of $\langle B\rangle$ in Σ.

Since $N_\Sigma(\langle B\rangle) \cap \langle B, E_0\rangle = N_{\langle B, E_0\rangle}(\langle B\rangle)$ is of order 20, there is an element s in $\langle B, E_0\rangle$ of order 4 such that $s^{-1}\tilde{x}s = \tilde{x}^{-1}$ and $\langle \tilde{x}, \tilde{z}\rangle = \langle \tilde{x}, s\rangle$, where s is of the form

$$s = \begin{pmatrix} 0 & \eta^\ell \\ -\eta^{-\ell} & 0 \end{pmatrix}.$$

We conclude that there are exactly $(q-1)/10$ subgroups of $\langle B, E_0\rangle$, which are conjugate to $\langle \tilde{x}, \tilde{z}\rangle$; moreover, there are exactly five solutions X to Equation (8.2) in each of $\langle B, E_0\rangle^{\tilde{x}^n}$, where n is any integer. For example, the five solutions in $\langle B, E_0\rangle$ are $B^{-j}E_0B^j$, with $j = 0, 1, 2, 3, 4$.

Since $xt^{-1} = \tilde{x}^{n'}s^{i'}$, and $\langle B, E_0\rangle = \langle B, E_1\rangle^x = \langle B, E_1\rangle^{\tilde{x}^{n'}s^{i'}t}$. Thus $\langle B, E_0\rangle = \langle B, E_1\rangle^{\tilde{x}^{n'}}$ contains at least ten solutions of Equation (8.2), which is a contradiction.

Step 5: Now we consider the case $q \equiv -1 \pmod 5$.

We may apply similar arguments in $SU(2, q^2)$. Thus we will simply exhibit the two non-conjugating classes in $SL(2, \boldsymbol{F}_q)$.

As before, we work in $SU(2, q^2)$ first. Define $\beta = \alpha^{2(q+1)/5}, u = (\beta^2 - 1)^{-1}$. Note that $\beta^{q+1} = 1$ and $u + u^q = (\beta^2 - 1)^{-1} + (\beta^{-2} - 1)^{-1} = -1$. Define

$$B' = \begin{pmatrix} \beta & 0 \\ 0 & \beta^q \end{pmatrix}.$$

All the solutions $X \in SU(2, q^2)$ (where $X \neq I_2$) to the following equation

$$(B'X)^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad X^3 = 1$$

has the form

$$X = \begin{pmatrix} u & w \\ w^q & u^q \end{pmatrix}$$

with $uu^q + ww^q = 1$.

There are exactly $q+1$ of them. Choose any w' satisfying $w'w'^q = 1 - uu^q$ and define

$$E_i' = \begin{pmatrix} u & w'\alpha^{2i} \\ -(w'\alpha^{2i})^q & u^q \end{pmatrix}$$

where $i = 0, 1$. Thus both $\langle B', E_0' \rangle$ and $\langle B', E_1' \rangle$ are isomorphic to $SL(2,5)$.

Now we define

$$B = \begin{pmatrix} 1 & \alpha \\ -\alpha & 1 \end{pmatrix} \begin{pmatrix} \beta & 0 \\ 0 & \beta^q \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ -\alpha & 1 \end{pmatrix}^{-1}$$

and

$$E_i = \begin{pmatrix} 1 & \alpha \\ -\alpha & 1 \end{pmatrix} \begin{pmatrix} u & \alpha^{2i}w' \\ -(\alpha^{2i}w')^q & u^q \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ -\alpha & 1 \end{pmatrix}^{-1}.$$

It is routine to verify that

$$B = \frac{1}{\beta(1+\alpha^2)} \begin{pmatrix} \beta^2 + \alpha^2 & \alpha(1-\beta^2) \\ \alpha(1-\beta^2) & 1 + \alpha^2\beta^2 \end{pmatrix}, \quad E_i = \frac{1}{1+\alpha^2} \begin{pmatrix} \bar{\alpha} & \bar{\beta} \\ \bar{\gamma} & \bar{\delta} \end{pmatrix}$$

where

$$\bar{\alpha} = u - \alpha^2(u+1) + \alpha(\alpha^{2i}w' - \alpha^{-2i}w'^q),$$
$$\bar{\beta} = -\alpha(1+2u) + \alpha^{2i}w' + \alpha^{2-2i}w'^q,$$
$$\bar{\gamma} = -\alpha(1+2u) - \alpha^{2i+2}w' - \alpha^{-2i}w'^q,$$
$$\bar{\delta} = -1 - u + \alpha^2 u - \alpha(\alpha^{2i}w' - \alpha^{-2i}w'^q). \qquad \square$$

Summary.

Because of Lemma 7.2 and Lemma 7.3, we find that any finite primitive subgroup in $SL(p, \boldsymbol{C})$ containing a non-trivial monomial normal subgroup H so that H has a non-scalar diagonal matrix is equivalent to a group G such that $\Phi(G)$ is conjugate to $SL(2, \boldsymbol{F}_p)$, or a cyclic subgroup of order m, where $m \geq 3$ and m is a divisor of $q+1$, or a group of type (ii)–(v) in Theorem 7.5. The generators of these subgroups of $SL(2, \boldsymbol{F}_p)$ (up to conjugation) may be found in Proposition 8.8, Theorem 8.9, Theorem 8.11 and Theorem 8.13. Once these subgroups are obtained, we may apply Theorem 2.5.

In the Appendix the reader will find a list of generators of these subgroups when $p = 5$ or 7. The following example provides a brief account of our method in the case $p \leq 7$.

EXAMPLE 8.14. Subgroups in $SL(3, \boldsymbol{C})$. The conjugacy classes for $\Phi(G)$ are: a cyclic group of order 4, a binary dihedral group of order 8, or the group $SL(2, \boldsymbol{F}_3)$ itself. Thus we recover Theorem 1.2, i.e. Blichfeldt's Theorem.

Subgroups in $SL(5, \boldsymbol{C})$. The conjugacy classes for $\Phi(G)$ are: cyclic groups of order 3 or 6, binary dihedral groups of order 8 or 12, or a group isomorphic to $SL(2, \boldsymbol{F}_3)$, or the group $SL(2, \boldsymbol{F}_5)$ itself. Thus we obtain in total six non-equivalent primitive subgroups of this type. This provides an explicit description of Brauer's Theorem, i.e. Theorem 1.3(1).

Subgroups in $SL(7, \boldsymbol{C})$. The conjugacy classes for $\Phi(G)$ are: cyclic groups of order 4 or 8, binary dihedral groups of order 8 (two non-conjugating subgroups), 12 or 16, or two non-conjugate subgroups isomorphic to $SL(2, \boldsymbol{F}_3)$, or two non-conjugate subgroups isomorphic to $\widehat{S_4}$, or the group $SL(2, \boldsymbol{F}_7)$ itself. Thus we obtain in total eleven non-equivalent primitive subgroups of this type. This provides an explicit description of Wales's Theorem, i.e. Theorem 1.3(2).

Appendix.

For the convenience of the reader, in this appendix we will provide a complete list of non-conjugate finite subgroups of $SL(p, \boldsymbol{C})$ containing a non-trivial monomial normal subgroup together when $p = 5$ or 7 (see Theorem A.3 and Theorem A.6).

LEMMA A.1. *Let $p = 5$ or 7, and $\zeta = e^{2\pi\sqrt{-1}/p}$. Define the Vandermonde matrix $T = (a_{ij})_{0\le i,j\le p-1} \in GL(p, \boldsymbol{C})$ by defining $a_{ij} = \zeta^{ij}$. If $p = 5$, then $\det(T) = -(\sqrt{5})^5$. If $p = 7$, then $\det(T) = (\sqrt{7})^7 \cdot \sqrt{-1}$.*

PROOF. Omitted. □

DEFINITION A.2. We will define matrices in $SL(5, \boldsymbol{C})$, which will be used in Theorem A.3. Let $\zeta = e^{2\pi\sqrt{-1}/5}$. Define

$$\sigma = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \zeta & 0 & 0 & 0 \\ 0 & 0 & \zeta^2 & 0 & 0 \\ 0 & 0 & 0 & \zeta^3 & 0 \\ 0 & 0 & 0 & 0 & \zeta^4 \end{pmatrix},$$

$$\rho_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & \zeta & 0 & 0 \\ 0 & 0 & 0 & \zeta^3 & 0 \\ 0 & 0 & 0 & 0 & \zeta \end{pmatrix}, \quad \rho_2 = -\frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 & \zeta^3 & \zeta^4 \\ 1 & \zeta^2 & \zeta^4 & \zeta & \zeta^3 \\ 1 & \zeta^3 & \zeta & \zeta^4 & \zeta^2 \\ 1 & \zeta^4 & \zeta^3 & \zeta^2 & \zeta \end{pmatrix},$$

$$\rho_3 = -\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}, \quad \rho_4 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & \zeta^2 & \zeta^4 & \zeta & \zeta^3 \\ 1 & 1 & 1 & 1 & 1 \\ \zeta^2 & 1 & \zeta^3 & \zeta & \zeta^4 \\ \zeta & \zeta^2 & \zeta^3 & \zeta^4 & 1 \\ \zeta^2 & \zeta & 1 & \zeta^4 & \zeta^3 \end{pmatrix},$$

$$\rho_5 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & \zeta^3 & \zeta^4 & \zeta^3 \\ 1 & \zeta^2 & \zeta^2 & 1 & \zeta \\ \zeta^4 & \zeta^3 & 1 & 1 & \zeta^3 \\ \zeta^2 & \zeta^3 & \zeta^2 & \zeta^4 & \zeta^4 \\ \zeta^4 & \zeta^2 & \zeta^3 & \zeta^2 & \zeta^4 \end{pmatrix}.$$

THEOREM A.3. *Let $D = \langle \sigma, \tau \rangle \subset SL(5, \boldsymbol{C})$ where σ, τ, ρ_i are defined in Definition* A.2. *If $G \subset SL(5, \boldsymbol{C})$ is a finite primitive group containing a non-trivial monomial normal subgroup, then G is conjugate to exactly one group in the following list,*

$$\begin{aligned} G_1 &= \langle D, \rho_4^2 \rangle, \\ G_2 &= \langle D, \rho_4 \rangle, \\ G_3 &= \langle D, \rho_2, \rho_3 \rangle, \\ G_4 &= \langle D, \rho_2, \rho_4 \rangle, \\ G_5 &= \langle D, \rho_2, \rho_5 \rangle, \\ G_6 &= \langle D, \rho_1, \rho_2, \rho_3 \rangle. \end{aligned}$$

PROOF.

Step 1: By Proposition 2.3 we may assume that G contains a non-scalar diagonal matrix.

Step 2: Apply Theorem 2.5 and Theorem 2.6. We may assume that there is a group homomorphism $\Phi : G \to SL(2, \boldsymbol{F}_5)$ such that $\mathrm{Ker}(\Phi) = D$. It remains to find $\Phi(G)$. Note that the conjugacy class of G in $SL(p, \boldsymbol{C})$ depends only on the conjugacy class of $\Phi(G)$ in $SL(2, \boldsymbol{F}_5)$ by Lemma 7.2.

Step 3: By Theorem 2.7, if $5^4 \big| |G|$, then G is conjugate to $G_0 = \langle D, \rho_1, \rho_2, \rho_3 \rangle$ which is G_6 in our list. Thus we may assume that $5^4 \not| |G|$ from now on.

Since $|D| = 5^3$, it follows that $5 \not| |\Phi(G)|$. Now we may use Theorem 7.5 and Lemma 7.3 to determine the structure of $\Phi(G)$.

Step 4: It is not difficult to see that $\Phi(G)$ is conjugate to one of the subgroups of $SL(2, \boldsymbol{F}_5)$ described in Example 8.14.

Step 5: If $\Phi(G)$ is a cyclic group of order 3 or 6, apply Proposition 8.8. We may assume that $\Phi(G) = \langle \widetilde{y}^2 \rangle$ or $\langle \widetilde{y} \rangle$ (in the notation of Proposition 8.8).

Recall the construction of $\widetilde{y}$ in Definition 8.6 and Definition 8.7. We choose $\alpha \in \boldsymbol{F}_{25}$ such that $\boldsymbol{F}_{25} = \boldsymbol{F}_5(\alpha)$, $\alpha^2 + 3\alpha + 4 = 0$. Note that $\alpha = \xi^2$ for some $\xi \in \boldsymbol{F}_{25}$ with $\boldsymbol{F}_{25}^{\times} = \langle \xi \rangle$. It follows that $\sigma = \eta = 2 \in \boldsymbol{F}_5$. Thus we find that

$$\widetilde{x} = \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}, \qquad \widetilde{y} = \begin{pmatrix} 1 & 3 \\ 3 & 0 \end{pmatrix}.$$

Since $\widetilde{y}$ corresponds to the fractional linear transformation $x \mapsto (x+3)/(3x)$, it follows that $g : \Delta_\infty \mapsto \Delta_2 \mapsto \Delta_0$ where $\Phi(g) = \widetilde{y}$. Apply Theorem 2.5(E) (vi) to find an explicit form of g by taking $k = 1 \pmod 5$. Thus g is the matrix ρ_4. (Note that the matrix $\sqrt{5}\rho_4$ can be transformed to the Vandermonde matrix in Lemma

A.1 by successive elementary row and column operations. Thus we may find its determinant.)

Hence we get the groups G_1 and G_2 in the list.

Step 6: If $\Phi(G)$ is a binary dihedral group of order 8 or 12, apply Theorem 8.9. Thus $\Phi(G)$ is conjugate to $\langle \widetilde{x}, \widetilde{z} \rangle$ or $\langle \widetilde{y}, \widetilde{z} \rangle$.

Note that the matrix $\widetilde{x} \in SL(2, \boldsymbol{F}_5)$ is given in Step 5 while $\widetilde{z}$ is given in Definition 8.7. Let $g_1, g_2 \in G$ such that $\Phi(g_1) = \widetilde{z}$, $\Phi(g_2) = \widetilde{x}$.

Since $\widetilde{z}$ corresponds to the fractional linear transformation $x \mapsto -1/x$, we find that $g_1 : \Delta_\infty \mapsto \Delta_0 \mapsto \Delta_\infty$. Hence we may apply Theorem 2.5(E) (iii) by taking $k = 1 \pmod 5$. Thus, up to an element in D, we may assume that g_1 is ρ_2. Similarly $g_2 : \Delta_\infty \mapsto \Delta_\infty$, $\Delta_0 \mapsto \Delta_0$, $\Delta_1 \mapsto \Delta_4$. Thus we apply Theorem 2.5(E) (i) by taking $k = 2 \pmod 5$. We get $g_2 = \rho_3$.

Step 7: If $\Phi(G)$ is isomorphic to $SL(2, \boldsymbol{F}_3)$, apply Theorem 8.11. Since $5^2 \neq 1 \pmod{16}$, the group $\langle \widetilde{z}, E_0 \rangle$ and $\langle \widetilde{z}, E_1 \rangle$ in Theorem 8.11 are conjugate. Hence it suffices to find $\langle \widetilde{z}, E_0 \rangle$.

By Definition 8.10, since $\eta = 2 \in \boldsymbol{F}_5$ (by Step 5), we find $a_0 = 3$, $b_0 = 0$. Hence $u_0 = 3$, $w_0 = 1$. By Theorem 8.11, we get

$$E_0 = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix} \in SL(2, \boldsymbol{F}_5).$$

Let $g \in G$ satisfying $\Phi(g) = E_0$. Then $g : \Delta_\infty \mapsto \Delta_4 \mapsto \Delta_2$. Apply Theorem 2.5(E) (vii) with $i = 4$, $j = 2$ and $k = 2 \pmod 5$. Thus we may choose $g = \rho_5$. □

DEFINITION A.4. We will consider the case $p = 7$.

We will determine the parameters $\alpha, \eta, \sigma, \ldots$ in Definition 8.6 and Definition 8.10 first.

Choose $\alpha \in \boldsymbol{F}_{49}$ satisfying $\alpha^2 + \alpha - 1 = 0$. Define $\xi = 2 + 3\alpha \in \boldsymbol{F}_{49}$. It is routine to verify that $\boldsymbol{F}_{49}^\times = \langle \xi \rangle$ and $\alpha = \xi^3$.

Define $\eta = \xi^8 = 3 \in \boldsymbol{F}_7$. $\sigma = \xi^{12} = 2 - 3\alpha \in \boldsymbol{F}_{49}$. Choose $\varepsilon = 4 + \alpha$ so that $\varepsilon\overline{\varepsilon} = 1/2$. By Definition 8.10, we find that $a_0 = 4$, $b_0 = 5$, $a_1 = 3$, $b_1 = 5$. Hence $u_0 = 0$, $w_0 = 4$, $u_1 = 4$, $w_1 = 0$. Thus we may choose $s_0 = 3$, $t_0 = 2$, $s_1 = 2$, $t_1 = 3$.

DEFINITION A.5. We will define matrices in $SL(7, \boldsymbol{C})$ which will be used in Theorem A.6. Let $\zeta = e^{2\pi\sqrt{-1}/7}$ and $c = (\sqrt{7}e^{\pi\sqrt{-1}/14})^{-1}$.

Define

$$\sigma=\begin{pmatrix}0&0&0&0&0&0&1\\1&0&0&0&0&0&0\\0&1&0&0&0&0&0\\0&0&1&0&0&0&0\\0&0&0&1&0&0&0\\0&0&0&0&1&0&0\\0&0&0&0&0&1&0\end{pmatrix},\quad \tau=\begin{pmatrix}1&0&0&0&0&0&0\\0&\zeta&0&0&0&0&0\\0&0&\zeta^2&0&0&0&0\\0&0&0&\zeta^3&0&0&0\\0&0&0&0&\zeta^4&0&0\\0&0&0&0&0&\zeta^5&0\\0&0&0&0&0&0&\zeta^6\end{pmatrix},$$

$$\rho_1=\begin{pmatrix}1&0&0&0&0&0&0\\0&1&0&0&0&0&0\\0&0&\zeta&0&0&0&0\\0&0&0&\zeta^3&0&0&0\\0&0&0&0&\zeta^6&0&0\\0&0&0&0&0&\zeta^3&0\\0&0&0&0&0&0&\zeta\end{pmatrix},\quad \rho_2=c\begin{pmatrix}1&1&1&1&1&1&1\\1&\zeta&\zeta^2&\zeta^3&\zeta^4&\zeta^5&\zeta^6\\1&\zeta^2&\zeta^4&\zeta^6&\zeta&\zeta^3&\zeta^5\\1&\zeta^3&\zeta^6&\zeta^2&\zeta^5&\zeta&\zeta^4\\1&\zeta^4&\zeta&\zeta^5&\zeta^2&\zeta^6&\zeta^3\\1&\zeta^5&\zeta^3&\zeta&\zeta^6&\zeta^4&\zeta^2\\1&\zeta^6&\zeta^5&\zeta^4&\zeta^3&\zeta^2&\zeta\end{pmatrix},$$

$$\rho_3=-\begin{pmatrix}1&0&0&0&0&0&0\\0&0&0&0&0&1&0\\0&0&0&1&0&0&0\\0&1&0&0&0&0&0\\0&0&0&0&0&0&1\\0&0&0&0&1&0&0\\0&0&1&0&0&0&0\end{pmatrix},\quad \rho_4=-c\begin{pmatrix}1&\zeta^2&\zeta^6&\zeta^5&\zeta^6&\zeta^2&1\\1&\zeta&\zeta^4&\zeta^2&\zeta^2&\zeta^4&\zeta\\\zeta&\zeta&\zeta^3&1&\zeta^6&1&\zeta^3\\\zeta^3&\zeta^2&\zeta^3&\zeta^6&\zeta^4&\zeta^4&\zeta^6\\\zeta^6&\zeta^4&\zeta^4&\zeta^6&\zeta^3&\zeta^2&\zeta^3\\\zeta^3&1&\zeta^6&1&\zeta^3&\zeta&\zeta\\\zeta&\zeta^4&\zeta^2&\zeta^2&\zeta^4&\zeta&1\end{pmatrix},$$

$$\rho_5=-c\begin{pmatrix}1&\zeta^4&\zeta^5&\zeta^3&\zeta^5&\zeta^4&1\\1&1&\zeta^4&\zeta^5&\zeta^3&\zeta^5&\zeta^4\\1&\zeta^3&\zeta^3&1&\zeta&\zeta^6&\zeta\\1&\zeta^6&\zeta^2&\zeta^2&\zeta^6&1&\zeta^5\\1&\zeta^2&\zeta&\zeta^4&\zeta^4&\zeta&\zeta^2\\1&\zeta^5&1&\zeta^6&\zeta^2&\zeta^2&\zeta^6\\1&\zeta&\zeta^6&\zeta&1&\zeta^3&\zeta^3\end{pmatrix},\ \rho_6=-c\begin{pmatrix}1&1&\zeta^2&\zeta^6&\zeta^5&\zeta^6&\zeta^2\\1&\zeta^6&1&\zeta^3&\zeta&\zeta&\zeta^3\\\zeta^4&\zeta^2&\zeta^2&\zeta^4&\zeta&1&\zeta\\\zeta^5&\zeta^2&\zeta&\zeta^2&\zeta^5&\zeta^3&\zeta^3\\\zeta^3&\zeta^6&\zeta^4&\zeta^4&\zeta^6&\zeta^3&\zeta^2\\\zeta^5&1&\zeta^4&\zeta^3&\zeta^4&1&\zeta^5\\\zeta^4&\zeta^5&\zeta&\zeta^6&\zeta^6&\zeta&\zeta^5\end{pmatrix},$$

$$\rho_7 = c\begin{pmatrix} 1 & 1 & \zeta^2 & \zeta^6 & \zeta^5 & \zeta^6 & \zeta^2 \\ 1 & \zeta^4 & \zeta^3 & \zeta^4 & 1 & \zeta^5 & \zeta^5 \\ \zeta^5 & \zeta^6 & \zeta^2 & 1 & 1 & \zeta^2 & \zeta^6 \\ \zeta & \zeta^6 & \zeta^6 & \zeta & \zeta^5 & \zeta^4 & \zeta^5 \\ \zeta^2 & \zeta^4 & \zeta & 1 & \zeta & \zeta^4 & \zeta^2 \\ \zeta & 1 & \zeta & \zeta^4 & \zeta^2 & \zeta^2 & \zeta^4 \\ \zeta^5 & \zeta & \zeta^6 & \zeta^6 & \zeta & \zeta^5 & \zeta^4 \end{pmatrix}, \quad \rho_8 = -c\begin{pmatrix} 1 & 1 & \zeta^4 & \zeta^5 & \zeta^3 & \zeta^5 & \zeta^4 \\ 1 & \zeta^5 & 1 & \zeta^6 & \zeta^2 & \zeta^2 & \zeta^6 \\ \zeta^3 & \zeta^6 & \zeta^6 & \zeta^3 & \zeta^4 & \zeta^2 & \zeta^4 \\ \zeta^2 & \zeta^3 & \zeta & \zeta^3 & \zeta^2 & \zeta^5 & \zeta^5 \\ \zeta^4 & \zeta^3 & \zeta^6 & \zeta^6 & \zeta^3 & \zeta^4 & \zeta^2 \\ \zeta^2 & \zeta^6 & 1 & \zeta^5 & 1 & \zeta^6 & \zeta^2 \\ \zeta^3 & \zeta^5 & \zeta^4 & 1 & 1 & \zeta^4 & \zeta^5 \end{pmatrix}.$$

THEOREM A.6. *Let $D = \langle \sigma, \tau \rangle \subset SL(7, \boldsymbol{C})$ where σ, τ, ρ_i are defined in Definition* A.5. *If $G \subset SL(7, \boldsymbol{C})$ is a finite primitive group containing a non-trivial monomial normal subgroup, then G is conjugate to exactly one group in the following list,*

$$\begin{aligned} G_1 &= \langle D, \rho_4^2 \rangle, \\ G_2 &= \langle D, \rho_4 \rangle, \\ G_3 &= \langle D, \rho_2, \rho_4^2 \rangle, \\ G_4 &= \langle D, \rho_4\rho_2, \rho_4^2 \rangle, \\ G_5 &= \langle D, \rho_2, \rho_3 \rangle, \\ G_6 &= \langle D, \rho_2, \rho_4 \rangle, \\ G_7 &= \langle D, \rho_2, \rho_5 \rangle, \\ G_8 &= \langle D, \rho_2, \rho_6 \rangle, \\ G_9 &= \langle D, \rho_2, \rho_5, \rho_7 \rangle, \\ G_{10} &= \langle D, \rho_2, \rho_6, \rho_8 \rangle, \\ G_{11} &= \langle D, \rho_1, \rho_2, \rho_3 \rangle. \end{aligned}$$

PROOF. The proof is quite similar to that of Theorem A.3. Thus we will outline the main steps only.

Step 1: Let $\Phi : G \to SL(2, \boldsymbol{F}_7)$ be the group homomorphism in Theorem 2.6. If $7^4 \big| G$, then G is conjugate to $G_0 = \langle D, \rho_1, \rho_2, \rho_3 \rangle$ by Theorem 2.7, which is G_{11} in our list. Otherwise, $\Phi(G)$ is conjugate to one of the subgroups of $SL(2, \boldsymbol{F}_7)$ described in Example 8.14.

Step 2: If $\Phi(G)$ is a cyclic group of order 4 or 8, apply Proposition 8.8. We find that $\Phi(G) = \langle \widetilde{y}^2 \rangle$ or $\langle \widetilde{y} \rangle$. Using the parameters described in Definition A.4, we find that

$$\widetilde{x} = \begin{pmatrix} 5 & 0 \\ 0 & 3 \end{pmatrix}, \quad \widetilde{y} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \quad \widetilde{z} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad E_0 = \begin{pmatrix} 0 & 4 \\ 5 & -1 \end{pmatrix},$$
$$E_1 = \begin{pmatrix} 4 & 0 \\ 1 & 2 \end{pmatrix}, \quad L_0 = \begin{pmatrix} 3 & 2 \\ 2 & -3 \end{pmatrix}, \quad L_1 = \begin{pmatrix} 2 & 3 \\ 3 & -2 \end{pmatrix}.$$

If $g \in G$ satisfies that $\Phi(g) = \widetilde{y}$, then $G : \Delta_\infty \mapsto \Delta_1 \mapsto \Delta_3$. Apply Theorem 2.5(E) (vii) with $i = 1$, $j = 3$, $k = 1$ and $\delta = 3$. We may assume that $g = \rho_4$ without loss of generality. Hence we get G_1 and G_2.

Step 3: If $\Phi(G)$ is a binary dihedral group of order 8 (there are two such groups), 12 or 16, apply Theorem 8.9 and recall the matrices $\widetilde{x}, \widetilde{y}, \widetilde{z}$ in Step 2. If g is a preimage of $\widetilde{x}$, then $g : \Delta_\infty \mapsto \Delta_\infty$, $\Delta_0 \mapsto \Delta_0$, $\Delta_1 \mapsto \Delta_4$; apply Theorem 2.5(E) (i) with $k = 3 \pmod 7$. We find $g = \rho_3$. For $\widetilde{z}$, apply Theorem 2.5(E) (iii) with $k = 1 \pmod 7$; we get $g = \rho_2$. Thus we obtain G_3, G_4, G_5, G_6.

Step 4: If $\Phi(G)$ is isomorphic to $SL(2, \boldsymbol{F}_3)$, apply Theorem 8.11. Let $g_i \in G$ correspond to E_i for $i = 0, 1$. Since $g_0 : \Delta_\infty \mapsto \Delta_0 \mapsto \Delta_3$, we apply Theorem 2.5(E) (iv) with $i = 3$ and $k = 3 \pmod 7$. Thus we may take $g_0 = \rho_5$. Similarly $g_1 : \Delta_\infty \mapsto \Delta_4 \mapsto \Delta_5$; thus we apply Theorem 2.5(E) (vii) with $i = 4$, $j = 5$, $k = 2$, $\delta = -1 \pmod 7$. We find $g_1 = \rho_6$. Thus we get G_7 and G_8.

Step 5: If $\Phi(G)$ is isomorphic to $\widehat{S_4}$, apply Theorem 8.11. Let g_i correspond to L_i for $i = 0, 1$. Since $g_0 : \Delta_\infty \leftrightarrow \Delta_5$, we apply Theorem 2.5(E) (v) with $k = 2 \pmod 7$. We get $g_0 = \rho_7$. Similarly $g_1 : \Delta_\infty \leftrightarrow \Delta_3$. Apply Theorem 2.5(E) (v) with $k = 3 \pmod 7$. We get $g_1 = \rho_8$. □

References

[BKR] T. Bridgeland, A. King and M. Reid, The McKay correspondence as an equivalence of derived categories, J. Amer. Math. Soc., **14** (2001), 535–554.

[Bl] H. F. Blichfeldt, Finite collineation groups, Univ. of Chicago Press, Chicago, 1917.

[Br1] R. Brauer, Über endliche lineare Gruppen von Primzahlgrad, Math. Ann., **169** (1967), 73–96.

[Br2] R. Brauer, Blocks of characters and structure of finite groups, Bull. Amer. Math. Soc., **1** (1979), 21–38.

[BZ] H. I. Blau and J. P. Zhang, Linear groups of small degree over fields of finite characteristic, J. Algebra, **159** (1993), 358–386.

[Ch] C. Chevalley, Invariants of finite groups generated by reflections, Amer. J. Math., **77** (1955), 778–782.

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

[Coh] P. M. Cohn, Algebra, **2**, second edition, John Wiley and Sons, New York, 1989.

[Da] H. Davenport, Multiplicative number theory, second edition, Springer GTM, **74**, Springer-Verlag, Berlin, 1980.

[DZ1] J. D. Dixon and A. Zalesski, Finite primitive linear groups of prime degree, J. London Math. Soc., **57** (1998), 126–134.

[DZ2] J. D. Dixon and A. Zalesski, Finite imprimitive linear groups of prime degree, J. Algebra, **276** (2004), 340–370.

[Fe1] W. Feit, The current situation in the theory of finite simple groups, Actes du Congrès International des Mathématiciens, Proceedings of ICM, Nice, 1970, Tome 1, Gauthier-Villars, Paris, 1971, pp. 55–93.

[Fe2] W. Feit, Richard D. Brauer, Bull. Amer. Math. Soc. (N.S.), **1** (1979), 1–20.

[Fl1] D. L. Flannery, The finite irreducible linear 2-groups of degree 4, Mem. Amer. Math. Soc., **129** (1997), no. 613.

[Fl2] D. L. Flannery, The finite irreducible monomial linear groups of degree 4, J. Algebra, **218** (1999), 436–469.

[GM] A. Grassi and D. R. Morrison, Group representations and the Euler characteristics of elliptically fibered Calabi-Yau threefolds, J. Algebraic Geom., **12** (2003), 321–356.

[Gr] J. J. Gray, Linear differential equations and group theory from Riemann to Poincare, Second Edition, Birkhäuser Boston, Inc., Boston, 2000.

[Hö] B. Höfling, Finite irreducible imprimitive nonmonomial complex linear groups of degree 4, J. Algebra, **236** (2001), 419–470.

[Hu] B. Huppert, Endliche Gruppen I, Springer-Verlag, Berlin, 1967.

[Is] I. M. Isaacs, Character theory of finite groups, Academic Press, New York, 1976.

[Jo] C. Jordan, Mémoire sur les equations differentielles lineaires a integrale algebrique, J. de Math. Pures et Appl., **84** (1878), 89–215; in Oeuvres II, 13–140.

[KW] V. Kac and K. Watanabe, Finite linear groups whose ring of invariants is a complete intersection, Bull. Amer. Math. Soc. (N.S.), **6** (1982), 221–223.

[Li] J. Lindsey, Finite linear groups of prime degree, Math. Ann., **189** (1970), 47–59.

[MM] S. Mori, D. R. Morrison and I. Morrison, On four-dimensional terminal quotient singularities, Math. Comp., **51** (1988), 769–786.

[MS] D. R. Morrison and G. Stevens, Terminal quotient singularities in dimensions three and four, Proc. Amer. Math. Soc., **90** (1984), 15–20.

[Po] E. G. C. Poole, Introduction to the theory of linear differential equations, Oxford University Press, Oxford, 1936; reprinted by Dover Publ., New York, 1960.

[Pr] D. Prill, Local classification of quotients of complex manifolds by discontinuous groups, Duke Math. J., **34** (1967), 375–386.

[Ro] S. S. Roan, Minimal resolutions of Gorenstein orbifolds in dimension 3, Topology, **35** (1996), 489–508.

[Sc] M. Schlessinger, Rigidity of quotient singularities, Invent. Math., **14** (1971), 17–26.

[Si] D. A. Sibley, Certain finite linear groups of prime degree, J. Algebra, **32** (1974), 286–316.

[So] R. Solomon, W. Feit (1930–2004): The Classification Years and History, Notices Amer. Math. Soc., **52** (2005), 732–734.

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

[Su] D.A. Suprunenko, Minimal irreducible soluble linear groups of prime degree, Trans. Moscow Math. Soc., **29** (1973), 215–226 (English translation).

[Suz] M. Suzuki, Group theory I, Springer-Verlag, Berlin, 1982.

[TZ] P. H. Tiep and A. Zalesski, Minimal characters of finite classical groups, Comm. Algebra, **24** (1996), 2093–2167.

[Wa1] D. B. Wales, Finite linear groups of prime degree, Canadian J. Math., **21** (1969), 1025–1041.

[Wa2] D. B. Wales, Finite linear groups of degree seven I, Canadian J. Math., **21** (1969), 1042–1056.

[Wa3] D. B. Wales, Finite linear groups of degree seven II, Pacific J. Math., **34** (1970), 207–235.

[Wat] K. Watanabe, Certain invariant subrings are Gorenstein I, Osaka J. Math., **11** (1974), 1–8; II, ibid. 379–388.

[YY] S. S. T. Yau and Y. Yu, Gorenstein quotient singularity in dimension three, Mem. Amer. Math. Soc., **105** (1993), no. 505.

[Zh1] J. P. Zhang, Finite linear groups of prime degree, Chinese Ann. Math. Ser. A, **11** (1990), 572–575.

[Zh2] J. P. Zhang, Complex linear groups of degree at most $p-1$, Classical groups and related topics (Beijing 1987), Contemp. Math., **82** Amer. Math. Soc., Providence, RI, 1989, pp. 243–254.

Ming-chang KANG
National Taiwan University
Taipei, Taiwan
E-mail: kang@math.ntu.edu.tw

Ji-ping ZHANG
Peking University
Beijing, China
E-mail: jzhang@math.pku.edu.cn

Jian-yi SHI
East China Normal University
Shanghai, China
E-mail: jyshi@math.ecnu.edu.cn

Yung YU
Cheng Kung University
Tainan, Taiwan
E-mail: yungyu@mail.ncku.edu.tw

Stephen S.T. YAU
University of Illinois at Chicago
Chicago 60607-7045, U.S.A.
E-mail: yau@uic.edu