Asian J. Math.
Vol. 12, No. 2, pp. 177–192, June 2008

002

GROUPS WITH ESSENTIAL DIMENSION ONE*

HUAH CHU†, SHOU-JEN HU‡, MING-CHANG KANG†§, AND JIPING ZHANG¶

Abstract. Denote by $\mathrm{ed}_K(G)$ the essential dimension of G over K. If K is an algebraically closed field with $\mathrm{char}\, K = 0$, Buhler and Reichstein determine explicitly all finite groups G with $\mathrm{ed}_K(G) = 1$ [Compositio Math. **106** (1997), Theorem 6.2]. We will prove a generalization of this theorem when K is an arbitrary field.

Key words. Essential dimension, compression of finite group actions, Galois theory, finite subgroups of $SL_2(K)$

AMS subject classifications. 12E05, 12F10, 12F20, 13F30

1. Introduction. Let K be an arbitrary field and G be a finite groups. The essential dimension of G over K, denoted by $\mathrm{ed}_K(G)$, was introduced by Buhler and Reichstein [BR], and was investigated further in [BF; Ka]. A related notion, the covariant dimension, was studied in [KS]. Similar notions may be extended to the case when G is an algebraic group [Re].

It is obvious that $\mathrm{ed}_K(G) = 0$ if and only if $G = \{1\}$ the trivial group. In [BR, Theorem 6.2] the group G with $\mathrm{ed}_K(G) = 1$ was studied.

Theorem 1.1. (Buhler and Reichstein [BR]) *Let K be a field such that* $\mathrm{char}\, K = 0$ *and K contains all roots of unity. If G is a nontrivial finite group, then* $\mathrm{ed}_K(G) = 1$ *if and only if G is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ or D_m where m is an odd integer.*

The purpose of this paper is to generalize the above theorem when K is an arbitrary field. The answer is the following five theorems.

Theorem 1.2. *Let K be an arbitrary field. Suppose that G is a nontrivial finite group with* $\mathrm{ed}_K(G) = 1$.

(1) *If* $\mathrm{char}\, K = 0$, *then G is isomorphic to the cyclic group $\mathbb{Z}/n\mathbb{Z}$ or the dihedral group D_m of order $2m$.*

(2) *If* $\mathrm{char}\, K = p > 0$ *and $p \neq 2$, then G is isomorphic to the cyclic group $\mathbb{Z}/n\mathbb{Z}$, the dihedral group D_m, or the group $G(n, p^r)$.*

(3) *If* $\mathrm{char}\, K = 2$, *then G is isomorphic to the cyclic group $\mathbb{Z}/n\mathbb{Z}$, the dihedral group D_m, the group $G(n, 2^r)$ or the group $SL_2(\mathbb{F}_q)$ where q is some power of 2.*

The group $G(n, p^r)$ or $G(n, 2^r)$ will be defined in Definition 3.4 (and Formula (3.2), Lemma 3.5). When $n = 1$, the group $G(n, p^r)$ is nothing but an elementary abelian group of order p^r. We emphasize that in the definition of $G(n, p^r)$ it is necessary that $p \nmid n$.

Because of Theorem 1.2, it remains to find the necessary and sufficient condition for the groups G of Theorem 1.2 to attain essential dimension one over K.

Theorem 1.3. *Let K be an arbitrary field and $G = \mathbb{Z}/n\mathbb{Z}$ be the cyclic group of order n.*

*Received March 13, 2007; accepted for publication October 25, 2007.

†Department of Mathematics, National Taiwan University, Taipei, Taiwan.
‡Department of Mathematics, Tamkang University, Tamshui, Taiwan.
§kang@math.ntu.edu.tw
¶Department of Mathematics, Peking University, Beijing, 100871, China.

(1) *If* $\operatorname{char} K \nmid n$*, then* $\operatorname{ed}_K(G) = 1$ *if and only if* $\zeta_n + \zeta_n^{-1} \in K$ *when* n *is an odd integer, or* $\zeta_n \in K$ *when* n *is an even integer.*

(2) *If* $\operatorname{char} K = p > 0$ *and* $p \mid n$*, then* $\operatorname{ed}_K(G) = 1$ *if and only if* $n = p$*.*

THEOREM 1.4. *Let* K *be an arbitrary field and* $G = D_n$ *be the dihedral group of order* $2n$*.*

(1) *If* $\operatorname{char} K = 0$*, then* $\operatorname{ed}_K(G) = 1$ *if and only if* n *is an odd integer and* $\zeta_n + \zeta_n^{-1} \in K$*.*

(2) *If* $\operatorname{char} K = p > 0$ *and* $p \neq 2$*, then* $\operatorname{ed}_K(G) = 1$ *if and only if* n *is an odd integer,* $\zeta_n + \zeta_n^{-1} \in K$ *when* $p \nmid n$*, or* $n = p$ *when* $p \mid n$*.*

(3) *If* $\operatorname{char} K = 2$*, then* $\operatorname{ed}_K(G) = 1$ *if and only if* $\zeta_n + \zeta_n^{-1} \in K$ *when* n *is an odd integer, or* $|K| \geq 4$ *with* $n = 2$ *when* n *is an even integer.*

THEOREM 1.5. *Let* K *be an arbitrary field with* $\operatorname{char} K = p > 0$*. If* G *is the group* $G(n, p^r)$*, then* $\operatorname{ed}_K(G) = 1$ *if and only if* n *is an odd integer,* $\zeta_n \in K$ *and* $[K : \mathbb{F}_p] \geq r$*.*

THEOREM 1.6. *Let* K *be an arbitrary field with* $\operatorname{char} K = 2$*. If* G *is the group* $SL_2(\mathbb{F}_q)$ *where* q *is some power of* 2*, then* $\operatorname{ed}_K(G) = 1$ *if and only if* $K \supset \mathbb{F}_q$*.*

As an application of the above theorems, we will prove that, when K is a field with $\operatorname{char} K = 2$, if K doesn't contain $\mathbb{F}_4$, then $\operatorname{ed}_K(A_4) = \operatorname{ed}_K(A_5) = 2$, while $\operatorname{ed}_K(A_4) = \operatorname{ed}_K(A_5) = 1$ if $K \supset \mathbb{F}_4$ (see Proposition 7.4). Similarly, since $\mathbb{Z}/4\mathbb{Z}$ is contained in the symmetric group S_4 and $\operatorname{ed}_K(S_4) = 2$, we find that $\operatorname{ed}_K(\mathbb{Z}/4\mathbb{Z}) = 2$ if $\operatorname{char} K \neq 2$ and $\sqrt{-1} \notin K$; $\operatorname{ed}_K(\mathbb{Z}/4\mathbb{Z}) = 1$ if $\operatorname{char} K \neq 2$ and $\sqrt{-1} \in K$; $\operatorname{ed}_K(\mathbb{Z}/4\mathbb{Z}) = 2$ if $\operatorname{char} K = 2$. (This result was proved in [BF, Theorem 7.6] in the case $\operatorname{char} K \neq 2$ by a different method.) It is not difficult to verify that $\operatorname{ed}_{\mathbb{Q}}(\mathbb{Z}/5\mathbb{Z}) = \operatorname{ed}_{\mathbb{Q}}(\mathbb{Z}/6\mathbb{Z}) = 2$ by the same way; we leave the details to the reader.

We recall some previous results. Besides Buhler and Reichstein's Theorem i.e. Theorem 1.1, it is known that the cyclic group of order n (resp. the dihedral group of order $2n$) over a field K is of essential dimension one provided that n is odd and $\zeta_n + \zeta_n^{-1} \in K$ [Mi; HM; BF]. It is also known that, if G is the group $SL_2(\mathbb{F}_q)$ where q is some power of 2 and $K \supset \mathbb{F}_q$, then $\operatorname{ed}_K(G) = 1$ [Le1]. Ledet studied the case of p-groups over an infinite field in [Le2, Propositions 5 and 7], which can be read out from Theorem 1.5 (for $n = 1$), Theorem 1.3 (for n being a prime power) and Theorem 1.4(3) (for n being an even integer). He proves that, if K is an infinite field, then $\operatorname{ed}_K(G) = 1$ if and only if there exists an embedding $G \to GL_2(K)$ such that the image contains no scalar matrix other than the identity matrix [Le2, Theorem 1].

We will organize the article as follows. We recall the definition of essential dimensions and prove some basic facts in Section 2. In Section 3 we will define several groups which arise as subgroups of $SL_2(K)$ where K is any algebraically closed field ($\operatorname{char} K$ may be zero or positive). In particular, the definition of $G(n, p^r)$ in Theorem 1.2 and Theorem 1.5 will be given. The proof of Theorem 1.2, Theorem 1.3, Theorem 1.4, Theorem 1.5 and Theorem 1.6 will be given in Section 4, Section 5, Section 6, Section 7 and Section 8 respectively.

Standing notation and terminology. For emphasis, K is an arbitrary field. All the fields in this article are assumed to contain the ground field K. If E is a field extension of K, $\operatorname{trdeg}_K E$ denotes the transcendence degree of E over K. If $F \subset K$ are fields, $[K : F]$ denotes the vector space dimension of K over F. The order of an element σ in a group G is denoted by $\operatorname{ord}(\sigma)$. All the groups G in the sequel are nontrivial finite groups. When we talk about $G \to GL(V)$ is a representation of a finite group G, it is understood that V is a finite-dimensional vector space over K. We will adopt the following notations,

S_n, the symmetric group,
A_n, the alternating group,
$PGL_2(K)$, the group isomorphic to $GL_2(K)/K^\times$,
$\mathbb{Z}/n\mathbb{Z}$, the cyclic group of order n,
D_n, the dihedral group of order $2n$.

We will take the convention that $\operatorname{char} K \nmid n$ means either $\operatorname{char} K = 0$ or $\operatorname{char} K = p > 0$ with $p \nmid n$. ζ_n denotes a primitive n-th root of unity; whenever we write $\zeta_n \in K$, it is assumed tacitly that $\operatorname{char} K \nmid n$. Finally $\mathbb{F}_q$ is the finite field consisting of q elements.

2. Preliminaries. Throughout this paper, K is an arbitrary field. All the fields in this paper are extension fields of K.

Definition 2.1. Let G be a finite group and L be a field containing K. We will call L a G-field (over K) if G acts on L by K-automorphism; L is a faithful G-field if the group homomorphism $G \to \operatorname{Aut}_K(L)$ is injective.

Definition 2.2. Let G be a finite group and K be an arbitrary field. Let $\rho : G \to GL(V)$ be a faithful finite-dimensional representation of G over K, i.e. ρ is an injective group homomorphism and V is a vector space over K with $\dim_K V < \infty$. Define $\operatorname{ed}_K(G) = \min\{\operatorname{trdeg}_K E : E \text{ is a faithful } G\text{-subfield of } K(V)\}$. It is known that $\operatorname{ed}_K(G)$ is independent of the choice of the faithful representation (see [BR, Theorem 3.1]).

Lemma 2.3. *Let K be a field with* $\operatorname{char} K = p > 0$. *Suppose that $\sigma \in PGL_2(K)$ and* $\operatorname{ord}(\sigma)$ *in $PGL_2(K)$ is finite. Then either $p \nmid \operatorname{ord}(\sigma)$ or $\operatorname{ord}(\sigma) = p$.*

Proof. Note that the order of σ in $PGL_2(K)$ is the same as that in $PGL_2(\overline{K})$ where $\overline{K}$ is the algebraic closure of K.

Choose a matrix $T \in GL_2(K)$ such that its image in $PGL_2(K)$ is σ. Find the Jordan canonical form of T in $GL_2(\overline{K})$. It is of the form

$$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

where $a, b \in \overline{K} \backslash \{0\}$. It is not difficult to see that the order of the image of the above matrix in $PGL_2(\overline{K})$ is p for the first case, and the order of the image in $PGL_2(\overline{K})$ is relatively prime to p for the second case. □

Lemma 2.4. ([BF, Lemma 7.2]) *Let K be an arbitrary field and G be a finite group. If* $\operatorname{ed}_K(G) = 1$, *then G can be embedded into $PGL_2(K)$.*

Lemma 2.5. *Let K be an arbitrary field, $\sigma \in PGL_2(K)$ be an element of finite order. If $n = \operatorname{ord}(\sigma)$ and* $\operatorname{char} K \nmid n$, *then $\zeta_n + \zeta_n^{-1} \in K$.*

Remark. The above lemma is a generalization of [BF, Lemma 7.7] where it was required that n is a prime number.

Proof. Choose a matrix $T \in GL_2(K)$ such that its image in $PGL_2(K)$ is σ. Then the Jordan canonical form of T is

$$\begin{pmatrix} \lambda\zeta_n & 0 \\ 0 & \lambda \end{pmatrix}$$

for some λ in the algebraic closure of K.

Note that the rational canonical form of T is

$$\begin{pmatrix} \lambda\zeta_n & 0 \\ 0 & \lambda \end{pmatrix} \text{ or } \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$$

where $\lambda, a, b \in K$ (according to whether the characteristic polynomial is reducible over K or irreducible over K). Then first possibility will imply $\zeta_n \in K$; in particular $\zeta_n + \zeta_n^{-1} \in K$. It remains to consider the second possibility.

Compare the traces and the determinants of these two canonical forms. We find that $b = \lambda\zeta_n + \lambda$ and $-a = \lambda^2\zeta_n$. Thus $\zeta_n + \zeta_n^{-1} + 2 = (\lambda\zeta_n + \lambda)^2(\lambda^2\zeta_n)^{-1} = b^2 \cdot (-a)^{-1} \in K$. □

Lemma 2.6. *Let p be a prime number and K be a field with* $\operatorname{char} K = p > 0$. *For any positive integer r,* $\operatorname{ed}_K((\mathbb{Z}/p\mathbb{Z})^r) = 1$ *if and only if* $[K : \mathbb{F}_p] \geq r$.

Proof. Suppose that $[K : \mathbb{F}_p] \geq r$.

Let $(\mathbb{Z}/p\mathbb{Z})^r = \langle \sigma_i : \sigma_i^p = 1,\ \sigma_i\sigma_j = \sigma_j\sigma_i \text{ for } 1 \leq i \leq r\rangle$. Choose $\alpha_1, \alpha_2, \ldots, \alpha_r \in K$ so that $\alpha_1, \ldots, \alpha_r$ are linearly independent over $\mathbb{F}_p$. Consider the faithful representation $\rho : (\mathbb{Z}/p\mathbb{Z})^r \to GL_2(K)$ defined by

$$\rho(\sigma_i) = \begin{pmatrix} 1 & \alpha_i \\ 0 & 1 \end{pmatrix}$$

for $1 \leq i \leq r$. Thus we have a faithful $(\mathbb{Z}/p\mathbb{Z})^r$-field $K(x, y)$ provided by this representation. Define $t = \frac{x}{y}$. Then $K(t)$ is a faithful $(\mathbb{Z}/p\mathbb{Z})^r$-subfield again.

For the other direction, suppose that $\operatorname{ed}_K((\mathbb{Z}/p\mathbb{Z})^r) = 1$.

If $[K : \mathbb{F}_p] = \infty$, there is nothing to prove. So consider the case that K is a finite field $\mathbb{F}_q$ where $q = p^n$ for some integer n.

Since $\operatorname{ed}_K((\mathbb{Z}/p\mathbb{Z})^r) = 1$, we may embed $(\mathbb{Z}/p\mathbb{Z})^r$ into $PGL_2(K) = PGL_2(\mathbb{F}_q)$ by Lemma 2.4. Let $f : GL_2(\mathbb{F}_q) \to PGL_2(\mathbb{F}_q)$ be the canonical projection. The group $f^{-1}((\mathbb{Z}/p\mathbb{Z})^r)$ is an extension of $(\mathbb{Z}/p\mathbb{Z})^r$ by $\mathbb{F}_q^\times$. Since $\gcd\{|\mathbb{F}_q^\times|, |(\mathbb{Z}/p\mathbb{Z})^r|\} = 1$, we find that the group extension splits by Schur-Zassenhaus's Theorem [Su, p.235]. Hence $(\mathbb{Z}/p\mathbb{Z})^r$ can be embedded into $GL_2(\mathbb{F}_q)$.

Since $|GL_2(\mathbb{F}_q)| = q(q^2 - 1)(q - 1)$, it follows that q is divisible by p^r. □

Theorem 2.7. ([BF, Corollary 4.16]) *If p is a prime number and K is a field such that $\zeta_p \in K$, then* $\operatorname{ed}_K((\mathbb{Z}/p\mathbb{Z})^r) = r$. *In particular, for a field K with* $\operatorname{char} K \neq 2$, $\operatorname{ed}_K((\mathbb{Z}/2\mathbb{Z})^r) = r$.

3. Theorems of Klein and Dickson. Most material in this section may be found in [Sp; Su].

Definition 3.1. A binary dihedral group of order $4n$ is defined by the presentation $\langle \sigma, \tau : \sigma^n = \tau^2,\ \tau^{-1}\sigma\tau = \sigma^{-1}\rangle$. If K is an algebraically closed field and $\operatorname{char} K \nmid 2n$, this group can be embedded in $SL_2(K)$ (see [Sp, p.89]) by defining

$$\sigma = \begin{pmatrix} \zeta_{2n} & 0 \\ 0 & \zeta_{2n}^{-1} \end{pmatrix}, \quad \tau = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}.$$

Definition 3.2. A binary tetrahedral (resp. octahedral, icosahedral) group G is a central extension of A_4 (resp. S_4, A_5) by $\mathbb{Z}/2\mathbb{Z}$, i.e. there is an element $\sigma \in G$ so that (i) $\operatorname{ord}(\sigma) = 2$, (ii) σ belongs to the center of G, and (iii) $G/\langle\sigma\rangle$ is isomorphic to A_4 (resp. S_4, A_5).

If K is an algebraically closed field and $\operatorname{char} K \neq 2$, then both the binary tetrahedral group and the binary octahedral group can be embedded in $SL_2(K)$ (see [Sp, p.91–92]). As an abstract group, the binary tetrahedral group is isomorphic to $SL_2(\mathbb{F}_3)$ and the binary octahedral group is isomorphic to the representation group of S_4 in which the transpositions correspond to the elements of order 4 [Su, Theorem 6.17, p.404].

If K is an algebraically closed field and $\operatorname{char} K \nmid 10$, then the binary icosahedral group can be embedded in $SL_2(K)$ (see [Sp, p.93]). As an abstract group, the binary icosahedral group is isomorphic to $SL_2(\mathbb{F}_5)$.

Theorem 3.3. (Klein [Sp, p.89–93; Su, Theorem 6.17, p.404]) *Let K be an algebraically closed field and* $\operatorname{char} K = 0$. *If G is a finite group, then G can be embedded in $SL_2(K)$ if and only if G is isomorphic to a cyclic group, a binary dihedral group, a binary tetrahedral group, a binary octahedral group or a binary icosahedral group.*

Definition 3.4. We will define the group $G(n, p^r)$ with the condition that $p \nmid n$, $s \mid r$ where $s := [\mathbb{F}_p(\zeta_n^2) : \mathbb{F}_p]$. We will adopt the following convention: Whenever we talk about $G(n, p^r)$, it is assumed that the condition $p \nmid n$ and $s \mid r$ with $s := [\mathbb{F}_p(\zeta_n^2) : \mathbb{F}_p]$ is satisfied automatically.

We will define the group $G(n, p^r)$ first as a subgroup of $SL_2(K)$ where K is an algebraically closed field with $\operatorname{char} K = p > 0$. Then another definition of $G(n, p^r)$ as an abstract group will be given in the form of generators and relations (see (3.2)). Finally the group $G(n, p^r)$ will be characterized as a subgroup of $SL_2(K)$ (where K is an algebraically closed field with $\operatorname{char} K = p > 0$), which is a semi-direct product of an elementary abelian p-group with a cyclic group (see Lemma 3.5).

Now suppose that K is an algebraically closed field with $\operatorname{char} K = p > 0$. Regard K as a vector space over $\mathbb{F}_p$. Since $\zeta_n \in K$, K is also a vector space over $\mathbb{F}_p(\zeta_n)$ (and therefore over $\mathbb{F}_p(\zeta_n^2)$). Choose a vector subspace V of K over $\mathbb{F}_p(\zeta_n^2)$ so that $[V : \mathbb{F}_p] = r$. (Note that $r = [V : \mathbb{F}_p(\zeta_n^2)][\mathbb{F}_p(\zeta_n^2) : \mathbb{F}_p]$.) Choose a basis $\alpha_1, \ldots, \alpha_r$ of V over $\mathbb{F}_p$. Define $\sigma_1, \ldots, \sigma_r$, $\tau \in SL_2(K)$ by

$$\sigma_i = \begin{pmatrix} 1 & \alpha_i \\ 0 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} \zeta_n & a \\ 0 & \zeta_n^{-1} \end{pmatrix} \tag{3.1}$$

where a is any element in K if $n \geq 3$, while $a = 0$ if $n = 1$ or 2.

Define $G(n, p^r)$ to be the subgroup of $SL_2(K)$ generated by $\sigma_1, \ldots, \sigma_r$, τ, i.e. $G(n, p^r) = \langle \sigma_1, \ldots, \sigma_r, \ \tau\rangle$. Note that $G(1, p^r)$ is an elementary abelian p-group and $G(2, p^r)$ is a direct product of an elementary abelian p-group with $\mathbb{Z}/2\mathbb{Z}$.

Define $Q = \langle \sigma_1, \ldots, \sigma_r\rangle \subset G(n, p^r)$. It is clear that Q is a normal subgroup of $G(n, p^r)$ and Q is an elementary abelian p-group. A typical element in Q is of the form

$$\sigma = \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix}$$

for some $v \in V$. It is easy to verify that

$$\tau \cdot \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix} \cdot \tau^{-1} = \begin{pmatrix} 1 & \zeta^2 \cdot v \\ 0 & 1 \end{pmatrix}.$$

The next step is to define $G(n,p^r)$ as an abstract group. Choose a basis $\beta_1,\ldots,\beta_t$ of V over $\mathbb{F}_p(\zeta_n^2)$ (thus $r=st$ where $s=[\mathbb{F}_p(\zeta_n^2):\mathbb{F}_p]$). Let $f(X)=X^s-a_sX^{s-1}-a_{s-1}X^{s-2}-\cdots-a_1\in\mathbb{F}_p[T]$ be the minimum polynomial of ζ_n^2 over $\mathbb{F}_p$. (Note that $f(X)$ is an irreducible factor of the cyclotomic polynomial $\Phi_n(X)$ or $\Phi_{n/2}(X)$ over $\mathbb{F}_p$.) Define $\beta_{ij}=\zeta_n^{2(j-1)}\beta_i$ where $1\le j\le s$. Then β_{ij} is a basis of V over $\mathbb{F}_p$. It is not difficult to show that $G(n,p^r)$ is generated by

$$\begin{pmatrix}1&\beta_{ij}\\0&1\end{pmatrix},\quad\begin{pmatrix}\zeta_n&a\\0&\zeta_n^{-1}\end{pmatrix}$$

where $1\le i\le t$, $1\le j\le s$ and $r=st$. Moreover, the group $G(n,p^r)$ may be defined by generators σ_{ij} and τ (with $1\le i\le t$, $1\le j\le s$) and the relations are given by

$$\begin{aligned}&\sigma_{ij}^p=\tau^n=1,\quad \sigma_{ij}\sigma_{kl}=\sigma_{kl}\sigma_{ij},\\ &\tau\sigma_{ij}\tau^{-1}=\sigma_{i,j+1}\quad\text{for }\ 1\le i\le t,\ 1\le j\le s-1,\\ &\tau\sigma_{i,s}\tau^{-1}=\prod_{1\le j\le s}\sigma_{i,j}^{a_j}\quad\text{for }\ 1\le i\le t.\end{aligned}\tag{3.2}$$

Thus, as an abstract group, $G(n,p^r)$ is independent of the choice of a in (3.1).

LEMMA 3.5. *Let K be an algebraically closed field with* $\operatorname{char}K=p>0$. *Let G be a finite subgroup of $SL_2(K)$ and Q be a p-Sylow subgroup of G. Assume that Q is a normal subgroup of G and Q is an elementary abelian group so that G/Q is a cyclic group. Then G is conjugate to $G(n,p^r)$ for some integers n and r.*

Proof. Note that G is a semi-direct product of Q and $\langle\tau\rangle$ ($\simeq G/Q$) because $\gcd\{|Q|,\,|G/Q|\}=1$ and we may apply Schur-Zassenhaus Theorem [Su, Theorem 8.10, p.235]. Let $n=\operatorname{ord}(\tau)$.

Since Q is an elementary abelian group, we may triangulate all elements of Q simultaneously. In other words, up to conjugation in $SL_2(K)$, we may assume elements of Q are of the form

$$\begin{pmatrix}1&v\\0&1\end{pmatrix}$$

for some $v\in K$. Write $Q=\langle\sigma_1,\ldots,\sigma_r\rangle$ ($\simeq(\mathbb{Z}/p\mathbb{Z})^r$) and

$$\sigma_i=\begin{pmatrix}1&\alpha_i\\0&1\end{pmatrix}$$

for $\alpha_i\in K$. Define $V=\bigoplus_{1\le i\le r}\mathbb{F}_p\cdot\alpha_i\subset K$. Then, any $\sigma\in Q$ can be written as

$$\sigma=\begin{pmatrix}1&v\\0&1\end{pmatrix}$$

for some $v\in V$.

Write

$$\tau=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in SL_2(K).$$

Since $\tau\sigma\tau^{-1}\in Q$ for any $\sigma\in Q$, it follows that $c=0$. Thus both a and d are primitive n-th root of unity. Hence, without loss of generality, we may write

$$\tau=\begin{pmatrix}\zeta_n&b\\0&\zeta_n^{-1}\end{pmatrix}.$$

Plugging in the relation $\tau\sigma\tau^{-1} \in Q$ for any $\sigma \in Q$, we get

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

for any $v \in V$. We find that $\zeta_n^2 \cdot V \subset V$, i.e. V admits a structure of vector space over $\mathbb{F}_p(\zeta_n^2)$. Hence G is equal to the group $G(n, p^r)$ defined in (3.1). □

Theorem 3.6. (Dickson [Su, Theorem 6.17, p.404]) *Let K be an algebraically closed field with* $\operatorname{char} K = p > 0$. *If G is a finite group, then G can be embedded in $SL_2(K)$ if and only if G is isomorphic to one of the following groups*

Case I. When $p \nmid |G|$

(i) *A cyclic group.*
(ii) *A binary dihedral group of order $4n$.*
(iii) *The binary tetrahedral group, i.e. $SL_2(\mathbb{F}_3)$.*
(iv) *The binary octahedral group, i.e. the representation group of S_4 in which the transpositions correspond to elements of order 4.*
(v) *The binary icosahedral group, i.e. $SL_2(\mathbb{F}_5)$.*

Case II. When $p \mid |G|$

(vi) *The group $G(n, p^r)$ with $p \nmid n$ and $s \mid r$ where $s = [\mathbb{F}_p(\zeta_n^2) : \mathbb{F}_p]$.*
(vii) *$p = 2$ and $G = D_n$ with n being an odd integer.*
(viii) *$p = 3$ and $G = SL_2(\mathbb{F}_5)$.*
(ix) *q is a power of p and $G = SL_2(\mathbb{F}_q)$.*
(x) *p is odd, q is a power of p and*

$$G = \left\langle SL_2(\mathbb{F}_q),\ \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix} \right\rangle$$

where $\varepsilon \in K$ satisfies that $\mathbb{F}_q(\varepsilon) = \mathbb{F}_{q^2}$ and $\mathbb{F}_q^\times = \langle \varepsilon^2 \rangle$.

Remark. In the statement of the above theorem, once we say the group in (iii) is a finite subgroup of $SL_2(K)$, it is assumed tacitly that $p = \operatorname{char} K \neq 2$ or 3. Note that, in (x), it is impossible that $p = 2$; otherwise, the condition $\mathbb{F}_q(\varepsilon) = \mathbb{F}_{q^2}$ and $\mathbb{F}_q^\times = \langle \varepsilon^2 \rangle$ would lead to a contradiction.

4. Proof of Theorem 1.2. We will prove Theorem 1.2 in this section by using Theorem 3.3 and Theorem 3.6.

Let K be an arbitrary field, $\overline{K}$ its algebraic closure.

Suppose that $\operatorname{ed}_K(G) = 1$. Then G may be embedded in $PGL_2(K)$ by Lemma 2.4. Since $PGL_2(K) \subset PGL_2(\overline{K}) = PSL_2(\overline{K})$. We may regard G as a subgroup of $PSL_2(\overline{K})$.

Let $\pi : SL_2(\overline{K}) \to PSL_2(\overline{K})$ be the natural projection and $G' = \pi^{-1}(G)$. Then G' is a finite subgroup of $SL_2(\overline{K})$ and $G = \pi(G')$. The possible candidates for G' are prescribed in Theorem 3.3 and Theorem 3.6.

Case 1. $\operatorname{char} K = 0$.

Apply Theorem 3.3.

If G' is a cyclic group, then G is a cyclic group also.

If G' is a binary dihedral group of order $4m$, then G is a dihedral group of order $2m$.

If G' is a binary tetrahedral (resp. octahedral, icosahedral) group, then G is isomorphic to A_4 (resp. S_4, A_5). Since $A_4 \subset S_4$ and $A_4 \subset A_5$, it follows that

$\mathrm{ed}_K(A_4) \leq \mathrm{ed}_K(S_4)$, $\mathrm{ed}_K(A_4) \leq \mathrm{ed}_K(A_5)$. Because $\mathrm{ed}_K(A_4) \geq \mathrm{ed}_K((\mathbb{Z}/2\mathbb{Z})^2) = 2$ by Theorem 2.7. It follows that $\mathrm{ed}_K(G) \geq 2$.

Case 2. $\mathrm{char}\, K = p > 0$ and $p \neq 2$.

Apply Theorem 3.6.

When $p \nmid |G|$, apply similar arguments as in Case 1.

Suppose $p \mid |G|$.

Note that the order of G' is even.

Suppose that $G' = G(n, p^r)$. Then n is even. Thus $G = \pi(G')$ is of the form $G(n/2, p^r)$ by (3.1) and Lemma 3.5.

If $p = 3$ and $G' = SL_2(\mathbb{F}_5)$, then G is isomorphic to A_5. But $\mathrm{ed}_K(A_5) \geq \mathrm{ed}_K(A_4) \geq 2$.

If p is an odd prime number and $G' = SL_2(\mathbb{F}_q)$ or a group containing $SL_2(\mathbb{F}_q)$, then G contains $PSL_2(\mathbb{F}_q)$. By [Su, Exercise 5(c), p.417], $PSL_2(\mathbb{F}_q)$ contains $(\mathbb{Z}/2\mathbb{Z})^2$. But $\mathrm{ed}_K((\mathbb{Z}/2\mathbb{Z})^2) = 2$ by Theorem 2.7. Thus $\mathrm{ed}_K(G) \geq \mathrm{ed}_K(PSL_2(\mathbb{F}_q)) \geq 2$.

Case 3. $\mathrm{char}\, K = 2$.

Apply Theorem 3.6 again.

Note that $G' \simeq G$ and thus G may be regarded as a finite subgroup of $SL_2(\overline{K})$.

The possible candidates for G are cyclic groups and groups in Case II of Theorem 3.6. The groups in Case II of Theorem 3.6 are (vi) $G(n, 2^r)$ with n being an odd integer, (vii) D_n with n being an odd integer, and (ix) $SL_2(\mathbb{F}_q)$ where q is a power of 2. All these groups belong to the list of Theorem 1.2. □

5. Proof of Theorem 1.3. We will prove Theorem 1.3 in this section.

LEMMA 5.1. *Let K be any arbitrary field with* $\mathrm{char}\, K \nmid n$. *If n is an even integer and* $\mathrm{ed}_K(\mathbb{Z}/n\mathbb{Z}) = 1$, *then* $\zeta_n \in K$.

Proof. Step 1. By Lemma 2.4 we may embed $G := \mathbb{Z}/n\mathbb{Z}$ into $PGL_2(K)$. Thus $PGL_2(K)$ has an element of order n. By Lemma 2.5, $\zeta_n + \zeta_n^{-1} \in K$.

Write $\eta = \zeta_n + \zeta_n^{-1} \in K$. Define a matrix T by

$$T = \begin{pmatrix} 0 & -1 \\ 1 & \eta \end{pmatrix} \in GL_2(K).$$

Note that the Jordan canonical form of T in the algebraic closure of K is

$$\begin{pmatrix} \zeta_n & 0 \\ 0 & \zeta_n^{-1} \end{pmatrix}.$$

Thus the order of T in $GL_2(K)$ is n, while the order of the image of T in $PGL_2(K)$ is $n/2$ because n is even.

Define a faithful representation of $G = \langle \sigma \rangle$ to $GL_2(K)$ by sending σ to T. Let $K(x, y)$ be the G-field associated with this representation so that $\sigma \cdot x = \eta x + y$, $\sigma \cdot y = -x$ where x and y are algebraically independent over K. (In fact, the action of σ on x, y is given by the transpose inverse of the matrix T.)

Step 2. Since $\mathrm{ed}_K(G) = 1$, there is a faithful G-subfield E of $K(x, y)$ with $\mathrm{trdeg}_K E = 1$. By Lüroth's Theorem E may be written as $E = K(u)$ for some $u \in K(x, y) \backslash K$.

Write $u = g/f$ where $f, g \in K[x, y]$. We will find a generator $w \in K(u)$, i.e. $K(u) = K(w)$, satisfying that $w = g_1/f_1$ where $f_1, g_1 \in K[x, y]$ and $\deg f_1 \neq \deg g_1$

(note that $\deg f_1$ and $\deg g_1$ denote the total degree of f_1 and g_1 with respect to x and y).

Start from $u = g/f$. If $\deg f \neq \deg g$, we are done.

Thus we may assume that $\deg f = \deg g$ in Step 3.

Step 3. Note that $\sigma \in \mathrm{Aut}_K(K(u)) \simeq PGL_2(K)$. Hence $\sigma \cdot u = (au+b)/(cu+d)$ for some $a, b, c, d \in K$ with $ad - bc \neq 0$.

Substitute $u = g/f$ into the relation $\sigma \cdot u = (au+b)/(cu+d)$. We get

$$(\sigma \cdot g)[cg + df] = (\sigma \cdot f)[ag + bf]. \tag{5.1}$$

Write $f = f_N + f_{N-1} + \cdots$, $g = g_N + g_{N-1} + \cdots$ where $N = \deg f = \deg g$ and f_i, g_i are homogeneous polynomials in x, y of degree i. From (5.1) we get

(5.2)
$$(\sigma \cdot g_N + \sigma \cdot g_{N-1} + \cdots)[(cg_N + df_N) + \cdots] = (\sigma \cdot f_N + \sigma \cdot f_{N-1} + \cdots)[(ag_N + bf_N) + \cdots]$$

since σ is a linear map on $Kx + Ky$.

We claim that $(cg_N + df_N)(ag_N + bf_N) \neq 0$.

Otherwise, assume that $cg_N + df_N = 0$. Compare the degrees of both sides of (5.2). We find that $ag_N + bf_N = 0$. Since $g_N \cdot f_N \neq 0$, it follows that $ad - bc = 0$. A contradiction.

Since $(\sigma \cdot g_N)(\sigma \cdot f_N) \cdot (cg_N + df_N) \cdot (ag_N + bf_N) \neq 0$, the degrees of both sides of (5.2) are $2N$. Compare the leading terms of (5.2). We get

$$(\sigma \cdot g_N)[cg_N + df_N] = (\sigma \cdot f_N)[ag_N + bf_N]. \tag{5.3}$$

Write $\lambda = g_N/f_N$ and re-write (5.3) as $\sigma \cdot \lambda = (a\lambda + b)/(c\lambda + d)$. Note that the order of

$$S := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PGL_2(K)$$

is n because $\sigma \cdot u = (au+b)/(cu+d)$ and σ is faithful on $K(u)$.

We claim that $\lambda \in K \backslash \{0\}$.

Otherwise λ is transcendental over K and σ is faithful on $K(\lambda)$ because the order of S in $PGL_2(K)$ is n.

On the other hand write $f_N = \sum_{0 \le i \le N} a_i x^{N-i} y^i$, $g_N = \sum_{0 \le i \le N} b_i x^{N-i} y^i$, $t = y/x$. Then $\lambda = g_N/f_N = (\sum b_i t^i)/(\sum a_i t^i) \in K(t)$.

Note that $\sigma \cdot t = \sigma \cdot y / \sigma \cdot x = -x/(\eta x + y) = -1/(t + \eta)$. The order of the fractional linear transformation $t \mapsto -1/(t+\eta)$ is $n/2$ because it is the image of T in $PGL_2(K)$. Hence σ is not faithful on $K(t)$. It follows that σ is not faithful on $K(\lambda)$ because $K(\lambda) \subset K(t)$. A contradiction.

We conclude that $g_N/f_N = \lambda \in K \backslash \{0\}$. Hence $u = g/f = (g_N + g_{N-1} + \cdots)/(f_N + f_{N-1} + \cdots) = \lambda + [(h_{N-1} + h_{N-2} + \cdots)/(f_N + f_{N-1} + \cdots)]$, i.e. $u - \lambda = h/f$ with $f, h \in K[x, y]$ and $\deg f > \deg h$. Clearly $K(u) = K(u - \lambda)$, i.e. the goal of Step 2 is achieved.

Step 4. In summary we find a faithful G-subfield $K(u)$ where $u = g/f$ and $\deg f \neq \deg g$. Without loss of generality we may assume that $\deg f < \deg g$.

Since $\sigma \in \mathrm{Aut}(K(u))$, $\sigma \cdot u = (au+b)/(cu+d)$ where $a, b, c, d \in K$ and $ad - bc \neq 0$. We will show that $c = 0$.

Write $g = g_N + g_{N-1} + \cdots$, $f = f_{N-1} + \cdots$ where $N = \deg g$ and f_i, g_i are homogeneous polynomials in x, y. Substitute it into $\sigma \cdot u = (au + b)/(cu + d)$ with $u = g/f$. We get

$$(5.4)\quad (\sigma \cdot g)[cg_N + (cg_{N-1} + df_{N-1}) + \cdots] = (\sigma \cdot f)[ag_N + (ag_{N-1} + bf_{N-1}) + \cdots].$$

If $c \neq 0$, the degree of the left-hand-side of (5.4) is $2N$ while that of the right-hand-side of (5.4) is $\leq 2N - 1$. We conclude that $c = 0$.

Thus we may write $\sigma \cdot u = \alpha \cdot u + \beta$ with $\alpha, \beta \in K$ and $\alpha \neq 0$. It is easy to verify that $\sigma^i \cdot u = \alpha^i u + \beta(1 + \alpha + \cdots + \alpha^{i-1})$ for any $i \geq 1$. Since the order of σ on $K(u)$ is n, we find that α is a primitive n-th root of unity, i.e. $\zeta_n \in K$. $\square$

Proof of Theorem 1.3. Let $G = \mathbb{Z}/n\mathbb{Z} = \langle \sigma \rangle$.

Suppose that $\mathrm{ed}_K(G) = 1$. If $\operatorname{char} K \nmid n$, then $\zeta_n + \zeta_n^{-1} \in K$ by Lemma 2.4 and Lemma 2.5. Thus it is necessary that $\zeta_n + \zeta_n^{-1} \in K$ in the particular case when n is odd. When n is even, apply Lemma 5.1. If $\operatorname{char} K = p > 0$ and $p \mid n$, we may apply Lemma 2.4 and Lemma 2.3 to conclude that $n = p$.

It remains to show that these necessary conditions are sufficient also.

When $\operatorname{char} K \nmid n$ and n is odd, since $\eta := \zeta_n + \zeta_n^{-1} \in K$, we may define a faithful representation of G to $GL_2(K)$ as in the proof of Step 1 of Lemma 5.1. Let $K(x, y)$ be the same as in the proof of Lemma 5.1. Define $t = y/x$. Then $\sigma \cdot t = -1/t + \eta$. The order of this fractional linear transformation is n because n is an odd integer. Thus $K(t)$ is a faithful G-subfield of $K(x, y)$. Hence $\mathrm{ed}_K(G) = 1$.

When $\operatorname{char} K \nmid n$ and n is even, since $\zeta_n \in K$, we have a faithful one-dimensional representation of G. Thus $\mathrm{ed}_K(G) = 1$.

When $\operatorname{char} K = p > 0$ and $p \mid n$, since $n = p$, it is easy to see that

$$\sigma \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

is a faithful representation for any $a \in K \backslash \{0\}$. Consider the G action on $K(x, y)$ given by $\sigma \cdot x = x - ay$, $\sigma \cdot y = y$ with $\operatorname{trdeg}_K K(x, y) = 2$. Define $t = x/y$. We find $\sigma \cdot t = t - a$. Thus $K(t)$ is a faithful G-subfield. It follows that $\mathrm{ed}_K(G) = 1$. $\square$

6. Proof of Theorem 1.4. Case 1. Assume that $\operatorname{char} K = 0$.

If $\mathrm{ed}_K(D_n) = 1$, by Lemma 2.4 we may embed D_n into $PGL_2(K)$. Thus $PGL_2(K)$ contains an element σ of order n. Apply Lemma 2.5 to get the necessary condition that $\zeta_n + \zeta_n^{-1} \in K$.

We will show that n is odd. Suppose to the contrary that n is even. Then $(\mathbb{Z}/2\mathbb{Z})^2 \subset D_n$. Since $\mathrm{ed}_K((\mathbb{Z}/2\mathbb{Z})^2) = 2$ by Theorem 2.7, we find that $\mathrm{ed}_K(D_n) \geq 2$, which is a contradiction.

Now we consider the reverse direction. Assume that n is odd and $\eta := \zeta_n + \zeta_n^{-1} \in K$. Define matrices T and S in $GL_2(K)$ as follows,

$$T = \begin{pmatrix} 0 & -1 \\ 1 & \eta \end{pmatrix}, \quad S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Let σ and τ be generators of D_n with relations $\sigma^n = \tau^2 = (\tau\sigma)^2 = 1$. Define a faithful representation of D_n into $GL_2(K)$ by sending σ to T, and τ to S. Then we have a faithful D_n-field $K(x, y)$ associated with this representation. Define $t = \frac{y}{x}$. Then $K(t)$ is a faithful D_n-subfield because n is odd. Thus $\mathrm{ed}_K(D_n) = 1$.

Case 2. Assume that $\operatorname{char} K = p > 0$ and $p \neq 2$.

Subcase 2.1. Suppose $p \nmid n$.

The proof is the same as Case 1 because we may apply Lemma 2.5.

Subcase 2.2. Suppose $p \mid n$.

If $\mathrm{ed}_K(D_n) = 1$, then $PGL_2(K)$ contains an element σ of order n. Apply Lemma 2.3. We find that $n = p$.

Conversely, let $D_p = \langle \sigma, \tau : \sigma^p = \tau^2 = 1,\ \tau\sigma\tau^{-1} = 1\rangle$. Consider the faithful representation $\rho : D_p \to GL_2(K)$ defined by

$$\rho(\sigma) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \rho(\tau) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

It is not difficult to show that $\mathrm{ed}_K(D_p) = 1$.

Case 3. Assume that $\mathrm{char}\, K = 2$.

Subcase 3.1. Suppose that n is odd.

The situation is the same as in Case 1 or Subcase 2.1.

Subcase 3.2. Suppose that n is even.

The situation is very similar to Subcase 2.2. If $\mathrm{ed}_K(D_n) = 1$, then $n = 2$. Thus D_n is isomorphic to Klein's four group. Apply Lemma 2.6. We find that $|K| \geq 4$.

Conversely, if $n = 2$ and $|K| \geq 4$, choose $\alpha \in K\backslash\{0, 1\}$. Let $D_2 = \langle \sigma, \tau : \sigma^2 = \tau^2 = 1,\ \sigma\tau = \tau\sigma\rangle$. Define a faithful representation $\rho : D_2 \to GL_2(K)$ defined by

$$\rho(\sigma) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \rho(\tau) = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}.$$

It is easy to show that $\mathrm{ed}_K(D_2) = 1$.

7. Proof of Theorem 1.5. In this section K is a field with $\mathrm{char}\, K = p > 0$ and $G = G(n, p^r)$ where $p \nmid n$ and $s \mid r$ with $s := [\mathbb{F}_p(\zeta_n^2) : \mathbb{F}_p]$.

LEMMA 7.1. *Let K be a field with* $\mathrm{char}\, K = p > 0$ *and $p \neq 2$. Let $G = G(n, p^r)$. If $\mathrm{ed}_K(G) = 1$, then $\zeta_n \in K$ and $[K : \mathbb{F}_p] \geq r$.*

Proof. Step 1. By Lemma 2.4 we may embed G into $PGL_2(K)$. Since $PGL_2(K) \simeq \mathrm{Aut}_K(K(u))$ where u is transcendental over K, we may assume that G acts faithfully on $K(u)$ by K-automorphisms.

Let Q be the p-Sylow subgroup of G. Then Q is a normal subgroup of G and $Q \simeq (\mathbb{Z}/p\mathbb{Z})^r$ (see Formula (3.2)). Choose any $\sigma \in Q$, $\sigma \neq 1$. Then $\sigma \cdot u = (au+b)/(cu+d)$ where $a, b, c, d \in K$ and $ad - bc \neq 0$. We will find $w \in K(u)$ so that $K(u) = K(w)$ and $\sigma \cdot w = w + 1$.

In fact, taking the rational canonical form of the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$$

amounts to finding another generator w with $K(w) = K(u)$ and σ acting on w according to this rational form. In other words, without loss of generality, we may assume that the above matrix is of its rational canonical form, i. e. it is of the form

$$T = \begin{pmatrix} 0 & -a \\ 1 & b \end{pmatrix} \in GL_2(K).$$

Thus σ acts on $K(u)$ by $\sigma \cdot u = -a/(u + b)$ where $a, b \in K$ and $a \neq 0$. Since $\mathrm{ord}(\sigma) = p$, the Jordan canonical form of T is

$$\begin{pmatrix} c & 1 \\ 0 & c \end{pmatrix}$$

for some $c \in \overline{K}\backslash\{0\}$. It follows that

$$(7.1) \qquad 2c = b, \quad c^2 = a.$$

Thus we find that $4a = b^2$.

Define $w = b/(2u+b)$. Since $\sigma \cdot u = -a/(u+b)$, it follows that $\sigma \cdot w = w + 1$.

Step 2. Once we know $\sigma \cdot w = w + 1$, we can show that $\lambda \cdot w = \alpha_\lambda w + \beta_\lambda$ for any $\lambda \in Q$ where $\alpha_\lambda, \beta_\lambda \in K$ and $\alpha_\lambda \neq 0$.

For, $\lambda\sigma = \sigma\lambda$ and $\lambda \cdot w = (\alpha w + \beta)/(\gamma w + \delta)$ for some $\alpha, \beta, \gamma, \delta \in K$ with $\alpha\delta - \beta\gamma \neq 0$. From the relation $\lambda\sigma(w) = \sigma\lambda(w)$, we get

$$\left(\frac{(\alpha w + \beta)}{(\gamma w + \delta)}\right) + 1 = \frac{[\alpha(w+1) + \beta]}{[\gamma(w+1) + \delta]}.$$

It follows that $\gamma = 0$.

In other words, for any $\lambda \in Q$, there exist $\alpha_\lambda, \beta_\lambda \in K$, $\alpha_\lambda \neq 0$ so that $\lambda \cdot w = \alpha_\lambda w + \beta_\lambda$.

Since $\lambda^p = 1$ for any $\lambda \in Q$, we find that $\alpha_\lambda = 1$.

In conclusion, for any $\lambda \in Q$, there is some $\beta_\lambda \in K$ so that $\lambda \cdot w = w + \beta_\lambda$. Moreover, it is easy to see the set $V = \{\beta_\lambda \in K : \lambda \in Q\}$ is a vector space over $\mathbb{F}_p$ with $[V : \mathbb{F}_p] = r$. Thus $[K : \mathbb{F}_p] \geq r$.

Step 3. Let $\tau \in G$ be an element of order n so that $G = \langle Q, \tau \rangle$ (see Formula (3.2)). Suppose $\tau \cdot w = (Aw+B)/(Cw+D)$ for some $A, B, C, D \in K$ with $AD - BC \neq 0$. For any $\lambda \in Q$, since $\tau\lambda\tau^{-1} = \lambda' \in Q$, we get $\tau\lambda = \lambda'\tau$. Using the formulae $\lambda \cdot w = w + \beta_\lambda$, $\lambda' \cdot w = w + \beta_{\lambda'}$, we get

$$[(A + \beta_\lambda C)w + (B + \beta_\lambda D)][Cw + (\beta_{\lambda'} C + D)] = [Cw + D][Aw + (\beta_{\lambda'} A + B)].$$

It follows that $C = 0$. Thus we may write $\tau \cdot w = a\tau + b$ for some $a, b \in K$ and $a \neq 0$. From $\operatorname{ord}(\tau) = n$ and $\tau^i \cdot w = a^i\tau + b(1 + a + a^2 + \cdots + a^{i-1})$ for $i \geq 1$, we find that a is a primitive n-th root of unity i.e. $\zeta_n \in K$. $\square$

LEMMA 7.2. *Let K be a field with* $\operatorname{char} K = 2$ *and* $G = G(n, 2^r)$. *If* $\operatorname{ed}_K(G) = 1$, *then* $\zeta_n \in K$ *and* $[K : \mathbb{F}_p] \geq r$.

Proof. We use the same notation and the arguments as in Step 1 of the proof of Lemma 7.1. But Formula (7.1) becomes

$$(7.2) \qquad 0 = 2c = b, \quad c^2 = a$$

Thus $\sigma \cdot u = a/u$ for some $a \in K\backslash\{0\}$. Note that it may happen that $a \in K^2$ or $a \notin K^2$, because c lies in the algebraic closure of K.

Case 1. $a \in K^2$.

Write $a = c^2$ with $c \in K\backslash\{0\}$. Define $w = c/(u+c)$. Then $\sigma \cdot w = w + 1$.

Once we get $\sigma \cdot w = w + 1$, Step 2 and Step 3 of the proof of Lemma 7.1 work also. Hence $\zeta_n \in K$.

Since $(\mathbb{Z}/2\mathbb{Z})^r \simeq Q \subset G$, it follows that $\operatorname{ed}_K((\mathbb{Z}/2\mathbb{Z})^r) = 1$. By Lemma 2.6 we find $[K : \mathbb{F}_2] \geq r$.

Case 2. $a \notin K^2$.

Define $F = K(\sqrt{a})$. Then $\zeta_n \in F$ by Case 1. It follows that $\zeta_n = \alpha + \beta\sqrt{a}$ for some $\alpha, \beta \in K$. Thus $\zeta_n^2 = \alpha^2 + a\beta^2 \in K$. Since n is odd by the definition of $G(n, 2^r)$, we find that ζ_n^2 is also a primitive n-th root of unity. Thus $\zeta_n \in K$.

The fact $[K : \mathbb{F}_2] \geq r$ may be proved as in Case 1. $\square$

LEMMA 7.3. *Let K be a field with* $\operatorname{char} K = p > 0$ *and $p \neq 2$. Let $G = G(n, p^r)$. If n is an even integer, then* $\operatorname{ed}_K(G) \geq 2$.

Proof. Suppose not. Assume that $\operatorname{ed}_K(G) = 1$ and n is even. We will find a contradiction.

Step 1. By Lemma 7.1 we find that $\zeta_n \in K$ and $[K : \mathbb{F}_p] \geq r$. We will find a faithful two-dimensional representation of G.

Let $Q = \langle \sigma_1, \sigma_2, \ldots, \sigma_r \rangle \simeq (\mathbb{Z}/p\mathbb{Z})^r$ be the p-Sylow subgroup of G, and $G = \langle Q, \tau \rangle$ where $\operatorname{ord}(\tau) = n$.

The field K may be regarded as a vector space over $\mathbb{F}_p(\zeta_n)$. Thus it is also a vector space over $\mathbb{F}_p(\zeta_n^2)$. Write $s = [\mathbb{F}_p(\zeta_n^2) : \mathbb{F}_p]$ and $r = st$. Since $[K : \mathbb{F}_p] \geq r$, it follows that $[K : \mathbb{F}_p(\zeta_n^2)] \geq t$. Find a set of linearly independent vectors $\alpha_1, \alpha_2, \ldots, \alpha_t$ over $\mathbb{F}_p(\zeta_n^2)$. Define $V = \bigoplus_{1 \leq i \leq t} \mathbb{F}_p(\zeta_n^2) \cdot \alpha_i \subset K$. Choose a basis $\beta_1, \ldots, \beta_r$ of V over $\mathbb{F}_p$. Define a representation $\rho : G \to GL_2(V)$ by

$$\rho : \sigma_i \mapsto \begin{pmatrix} 1 & -\beta_i \\ 0 & 1 \end{pmatrix}, \quad \tau \mapsto \begin{pmatrix} \zeta_n^{-1} & 0 \\ 0 & \zeta_n \end{pmatrix}.$$

Then ρ is a faithful representation. Let $K(x, y)$ be the G-field associated with this representation so that $\sigma_i \cdot x = x + \beta_i y$, $\sigma_i \cdot y = y$, $\tau \cdot x = \zeta_n x$, $\tau \cdot y = \zeta_n^{-1} y$.

Since $\operatorname{ed}_K(G) = 1$, there is some element $u \in K(x, y) \backslash K$ so that $K(u)$ is a faithful G-subfield.

Step 2. For any $\lambda \in G$, $\lambda(u) = (a_\lambda u + b_\lambda)/(c_\lambda u + d_\lambda)$ where $a_\lambda, b_\lambda, c_\lambda, d_\lambda \in K$ and $a_\lambda d_\lambda - b_\lambda c_\lambda \neq 0$. Write $u = g/f$ where $f, g \in K[x, y]$. We will find $w \in K(u)$ so that $K(u) = K(w)$, $\deg g_1 \neq \deg f_1$ where $w = g_1/f_1$ with $f_1, g_1 \in K[x, y]$. The proof is the same as Step 3 of the proof of Lemma 5.1 by considering the action of τ on $K(u)$. The details are omitted.

In conclusion, without loss of generality, we may write $u = g/f$ where $f, g \in K[x, y]$ and $\deg f < \deg g$.

Step 3. Since $\lambda(u) = (a_\lambda u + b_\lambda)/(c_\lambda u + d_\lambda)$ for $a_\lambda, b_\lambda, c_\lambda, d_\lambda \in K$ with $a_\lambda d_\lambda - b_\lambda c_\lambda \neq 0$ for any $\lambda \in G$, we apply the same arguments in Step 4 of the proof of Lemma 5.1 to conclude that $c_\lambda = 0$ for any $\lambda \in G$.

In short, for any $\sigma \in Q$, $\sigma \cdot u = u + b_\sigma$ for some $b_\sigma \in K$ while $\tau \cdot u = \zeta_n u + b$ for some $b \in K$.

Step 4. Let $Q = \langle \sigma_{ij} : 1 \leq i \leq t,\ 1 \leq j \leq s \rangle$ where $r = st$ and σ_{ij} are the elements defined in Formula (3.2). Recall that $f(X) = X^s - a_s X^{s-1} - \cdots - a_2 X - a_1 \in \mathbb{F}_p[X]$ is the minimum polynomial of ζ_n^2 over $\mathbb{F}_p$.

Write $\sigma_{ij} \cdot u = u + b_{ij}$ and $\tau \cdot u = \zeta_n u + b$. We find that $\tau \sigma_{ij} \tau^{-1} \cdot u = u + \zeta_n^{-1} b_{ij}$.

By Formula (3.2), $\tau \sigma_{ij} \tau^{-1} = \sigma_{i,j+1}$ if $1 \leq j \leq s - 1$, and $\tau \sigma_{is} \tau^{-1} = \prod_j \sigma_{ij}^{a_j}$. Write $\beta = b_{11} \neq 0$. We find that $\zeta_n^{-s} \beta = \sum_{1 \leq j \leq s} a_j \zeta^{-(j-1)} \beta$. We get that $\zeta_n^{-s} - a_s \zeta^{-(s-1)} - a_{s-1} \zeta^{-(s-2)} - \cdots - a_2 \zeta^{-1} - a_1 = 0$, i.e. $f(\zeta_n^{-1}) = 0$. But $f(X)$ is a factor of $\Phi_{n/2}(X)$ (where $\Phi_{n/2}(X)$ is the $n/2$-th cyclotomic polynomial) because $f(X)$ is the minimum polynomial of ζ_n^2. On the other hand ζ_n^{-1} is a primitive n-th root of unity. We find that $f(X)$ divides $\gcd\{\Phi_n(X), \Phi_{n/2}(X)\}$, which is impossible. $\square$

Proof of Theorem 1.5. Let K be a field with $\operatorname{char} K = p > 0$ and $G = G(n, p^r)$.

Suppose that $\operatorname{ed}_K(G) = 1$.

If $p = 2$, then n is odd by Definition 3.4.

If $p \neq 2$ and n is even, then it is impossible that $\operatorname{ed}_K(G) = 1$ by Lemma 7.3. Hence n is odd also.

The facts that $\zeta_n \in K$ and $[K : \mathbb{F}_p] \geq r$ follow from Lemma 7.1 and Lemma 7.2.

Conversely, assume that n is odd, $\zeta_n \in K$ and $[K : \mathbb{F}_p] \geq r$. We will show that $\mathrm{ed}_K(G) = 1$.

We will use the same notation and the same arguments in Step 1 of the proof of Lemma 7.3. In short, $K(x, y)$ is a faithful G-field with $\sigma_i \cdot x = x + \beta_i y$, $\sigma_i \cdot y = y$, $\tau \cdot x = \zeta_n x$, $\tau \cdot y = \zeta_n^{-1} y$ where $1 \leq i \leq r$ and $G = \langle \sigma_1, \ldots, \sigma_r,\ \tau\rangle$.

Define $t = x/y$. Then $\sigma_i \cdot t = t + \beta_i$, $\tau \cdot t = \zeta_n^2 t$. Since n is odd, G acts faithfully on $K(t)$. Hence $\mathrm{ed}_K(G) = 1$. □

Proposition 7.4. *Let K be a field with* $\mathrm{char}\, K = 2$.
(1) *If $K \supset \mathbb{F}_4$, then* $\mathrm{ed}_K(A_4) = \mathrm{ed}_K(A_5) = 1$.
(2) *If K doesn't contain $\mathbb{F}_4$, then* $\mathrm{ed}_K(A_4) = \mathrm{ed}_K(A_5) = 2$.

Remark. Note that $\mathrm{ed}_K(A_3) = 1$, because $\mathrm{ed}_K(S_3) = 1$.

Proof. (1) Note that $A_5 \simeq SL_2(\mathbb{F}_4)$. If $K \supset \mathbb{F}_4$, then we have a faithful A_5-field $K(x, y)$ provided by the representation $A_5 \to SL_2(\mathbb{F}_4) \subset GL_2(K)$. Define $t = \frac{y}{x}$. Because A_5 is a simple group, it acts faithfully on $K(t)$. Hence $\mathrm{ed}_K(A_5) = 1$.

(2) First note that A_4 is isomorphic to $G(3, 2^2)$. By Theorem 1.5, $\mathrm{ed}_K(G(3, 2^2)) = 1$ if and only if $\zeta_3 \in K$, i.e. $K \supset \mathbb{F}_4$. In other words, if K doesn't contain $\mathbb{F}_4$, then $\mathrm{ed}_K(A_4) \geq 2$. On the other hand, we have $\mathrm{ed}_K(A_5) \leq \mathrm{ed}_K(S_5) \leq 2$. It follows that $2 \leq \mathrm{ed}_K(A_4) \leq \mathrm{ed}_K(A_5) \leq 2$. □

8. Proof of Theorem 1.6. In this section K is a field with $\mathrm{char}\, K = 2$ and q is a power of 2. Recall that ζ_{q+1} is a primitive $(q + 1)$-th root of unity in the algebraic closure of $\mathbb{F}_2$.

Lemma 8.1. *If $q = 2^r$ for some positive integer r, then $\mathbb{F}_2(\zeta_{q+1}) = \mathbb{F}_{q^2}$ and $\mathbb{F}_2(\zeta_{q+1} + \zeta_{q+1}^{-1}) = \mathbb{F}_q$.*

Proof. Note that $\mathbb{F}_{q^2} = \mathbb{F}_2(\zeta_{q^2-1})$. Thus $\zeta_{q+1} \in \mathbb{F}_2(\zeta_{q^2-1}) = \mathbb{F}_{q^2}$. Hence $\mathbb{F}_2(\zeta_{q+1}) \subset \mathbb{F}_{q^2}$. To show that $\mathbb{F}_2(\zeta_{q+1}) = \mathbb{F}_{q^2}$, it suffices to show that ζ_{q+1} doesn't belong to any proper subfield of $\mathbb{F}_{q^2}$.

Since $[\mathbb{F}_{q^2} : \mathbb{F}_2] = 2r$, any proper subfield of $\mathbb{F}_{q^2}$ is of the form $\mathbb{F}_{2^m}$ where m is a divisor of $2r$ and $m \neq 2r$.

Suppose that $2r = tm$ where $t \geq 2$ and $\zeta_{q+1} \in \mathbb{F}_{2^m}$. Then $q + 1$ divides $2^m - 1$. But $q + 1 = 2^r + 1$. Since $m = 2r/t \leq r$, $2^r + 1$ cannot be a divisor $2^m - 1$. Hence $\zeta_{q+1} \notin \mathbb{F}_{2^m}$ and $\mathbb{F}_2(\zeta_{q+1}) = \mathbb{F}_{q^2}$.

Write $\eta = \zeta_{q+1} + \zeta_{q+1}^{-1}$. Then $[\mathbb{F}_2(\zeta_{q+1}) : \mathbb{F}_2(\eta)] \leq 2$ because ζ_{q+1} satisfies the equation $X^2 - \eta X + 1 = 0$. On the other hand, note that $\zeta_{q+1}^{-1} = \zeta_{q+1}^q$. Hence $\eta = \zeta_{q+1} + \zeta_{q+1}^{-1} = \zeta_{q+1} + \zeta_{q+1}^q = \zeta_{q+1} + \sigma(\zeta_{q+1}) \in \mathbb{F}_q$ where σ is the Frobenius automorphism of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Thus $\eta \in \mathbb{F}_q$. Hence $\mathbb{F}_2(\eta) = \mathbb{F}_q$. □

Proof of Theorem 1.6. Let K be a field with $\mathrm{char}\, K = 2$ and $G = SL_2(\mathbb{F}_q)$ where $q = 2^r$ for some positive integer r.

If $r = 1$, then $G = SL_2(\mathbb{F}_2) \simeq S_3$. It is known that $\mathrm{ed}_K(S_3) = 1$. Hence from now on we will assume that $r \geq 2$, and therefore G is a simple group [Su, Theorem 9.9, p.78].

Suppose that $K \supset \mathbb{F}_q$. Then we have the trivial representation of G into $GL_2(K)$ by considering the inclusion map $SL_2(\mathbb{F}_q) \subset GL_2(K)$. Let $K(x, y)$ be the associated G-field with $\mathrm{trdeg}_K\, K(x, y) = 2$ and $\sigma \cdot x = ax + by$, $\sigma \cdot y = cx + dy$ if $\sigma \in G$ is of the form

$$\sigma = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in SL_2(\mathbb{F}_q).$$

Define $t = x/y$. If σ acts on x, y as above, then $\sigma \cdot t = (at+b)/(ct+d) \in K(t)$. Since G is a simple group, G acts faithfully on $K(t)$. Thus $\mathrm{ed}_K(G) = 1$.

Conversely, assume that $\mathrm{ed}_K(G) = 1$.

We claim that G contains an element of order $q+1$. By Lemma 8.1 $\mathbb{F}_2(\zeta_{q+1} + \zeta_{q+1}^{-1}) = \mathbb{F}_q$, i.e. $\eta := \zeta_{q+1} + \zeta_{q+1}^{-1} \in \mathbb{F}_q$. Thus the following matrix T belongs to $SL_2(\mathbb{F}_q)$ where T is defined by

$$T = \begin{pmatrix} 0 & -1 \\ 1 & \eta \end{pmatrix}.$$

The Jordan canonical form of T is

$$\begin{pmatrix} \zeta_{q+1} & 0 \\ 0 & \zeta_{q+1}^{-1} \end{pmatrix}.$$

Thus the order the T is $q+1$.

Since $\mathrm{ed}_K(G) = 1$, G can be embedded in $PGL_2(K)$ by Lemma 2.4. Thus $PGL_2(K)$ contains an element of order $q+1$. By Lemma 2.5, we find $\zeta_{q+1}+\zeta_{q+1}^{-1} \in K$. By Lemma 8.1, $\mathbb{F}_q = \mathbb{F}_2(\zeta_{q+1} + \zeta_{q+1}^{-1})$. Hence $\mathbb{F}_q \subset K$. □

REFERENCES

[BF] G. Berhuy and G. Favi, *Essential dimension: a functorial point of view after A. Merkurjev*, Documenta Math., 8 (2003), pp. 279–330.

[BR] J. Buhler and Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math., 106 (1997), pp. 159–179.

[HM] K. Hashimoto and K. Miyake, *Inverse Galois problem for dihedral groups*, in "Galois theory and modular forms" edited by K. Hashimoto, K. Miyake and H. Nakamura, Kluwer Academic Publ., Dordrecht, 2004.

[Ka] M. Kang, *A central extension theorem for essential dimensions*, Proc. Amer. Math. Soc., 136 (2008), pp. 809–813.

[KS] H. Kraft and G. W. Schwarz, *Compression of finite group actions and covariant dimension*, J. Algebra, 313 (2007), pp. 268–291.

[Le1] A. Ledet, *$PSL(2,2^n)$-extensions over $\mathbb{F}_{2^n}$*, Canadian Math. Bull., 49 (2006), pp. 113–116.

[Le2] A. Ledet, *Finite groups of essential dimension one*, J. Algebra, 311 (2007), pp. 31–37.

[Mi] K. Miyake, *Linear fractional transformations and cyclic polynomials*, Adv. Stud. Contemp. Math. (Pusan), 1 (1999), pp. 137–142.

[Re] Z. Reichstein, *On the notion of essential dimension for algebraic groups*, Transformation Groups, 5 (2000), pp. 265–304.

[Sp] T. A. Springer, *Invariant theory*, LNM vol. 585, Springer-Verlag, Berlin, 1977.

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