To Jerzy Browkin
on his 70th birthday

Introduction

The present paper deals with the circle of problems considered by several mathematicians, beginning with F. Klein in 1876 and ending with L. Summerer in 2004. Even before Klein's fundamental paper [15], A. Clebsch and P. Gordan [6] in 1867 and A. Clebsch [5] in 1872 made important contributions to one of the problems in question without formulating it explicitly.

Let K be a field of characteristic $\pi \geq 0$, $T \in \mathrm{GL}_2(K)$ and $f \in K[x,y]$ be a form such that

$$f(T(x,y)) = rf(x,y), \qquad \text{where } r \in K^*.$$

Segre [22] calls T a *weak automorph* of f ("automorfismo in senso lato"), as opposed to a *strict automorph* ("automorfismo in senso stritto"), for which $r = 1$, and considers for $K = \mathbb{Q}$ the quotient group $\mathrm{Aut}(f,K)$ (notation mine, some authors denote similarly the group of strict automorphs) of the group of all weak automorphs of f defined over K divided by the group of trivial weak automorphs, given by $T(x,y) = (\varrho x, \varrho y)$ for $\varrho \in K^*$ (this definition extends immediately to forms defined over any field L containing K; then $r \in L^*$).

Segre determines the forms $f \in \mathbb{Q}[x,y]$ such that $\mathrm{Aut}(f,\mathbb{Q})$ contains a given non-trivial group $\mathcal{G}$ of one of the possible eight types: cyclic of order $2,3,4,6$ and dihedral of order $4,6,8,12$. For every group $\mathcal{G}$ Segre takes a convenient conjugate in the group $\mathrm{PGL}_2(\mathbb{Q})$, which simplifies calculation. Earlier for $\mathbb{C}$ instead of $\mathbb{Q}$ a similar result was obtained by Klein [16, Chapter 2]: here all cyclic and dihedral groups are possible and, in addition, three polyhedral groups. Dickson [9], [10] obtained analogous results for K being a finite field. For a modern treatment of the case $K = \mathbb{C}$, see Huffman [14].

The characterization of forms in question given by Klein and Segre is the following ($K = \mathbb{C}$ or $\mathbb{Q}$, $\overline{K}$ is an algebraic closure of K).

For a given finite subgroup $\mathcal{G}$ of $\mathrm{PGL}_2(K)$ of order $|\mathcal{G}| = \nu$ all forms $f \in K[x,y]$ for which $\mathcal{G} \subset \mathrm{Aut}(f,K)$ and only those are expressible as

$$f(x,y) = \prod_{i=1}^{h} \chi_i(x,y)^{c_i} \psi(p(x,y), q(x,y)),$$

where $p, q \in K[x,y]$, $\chi_i \in \overline{K}[x,y]$ are forms determined by $\mathcal{G}$; p, q are of degree ν, χ_i are of degree ν/m_i, c_i are integers satisfying $0 \leq c_i < m_i$ and if χ_i, χ_j are conjugate over K, then $c_i = c_j$; ψ is a binary form over K. Klein's proof is not rigorous and in Segre's proof given in Subsection 19 of [22] several details are missing. In particular,

no connection is indicated between p, q and χ_i. On the other hand, in Subsections 20 and 24, 29 of [22] Segre explicitly determines p, q and χ_i for every $\mathcal{G}$ up to conjugation.

Having proved in §1 of the present paper several lemmas about $\mathrm{PGL}_2(K)$ we determine in §2 the forms p, q and χ_i for every cyclic subgroup of $\mathrm{PGL}_2(K)$ with a given generator (Theorem 1). Then we prove an analogue of the above result of Klein, Dickson and Segre for an arbitrary field K (Theorems 2 and 3). Consideration of fields K that are not perfect is the only novel feature of this proof. As an application we prove in §3 an upper bound for the order of $\mathrm{Aut}(f, K)$ (Theorems 4 and 5). The bound is sharp for every π and for $\pi = 0$ it is better for $\deg f > 12$ than Olver's bound [19], [1].

In Subsections 22–23 of [22] Segre gives a method to decide whether a given cubic or quadratic binary form f over $\mathbb{Q}$ has a strict non-trivial automorph defined over $\mathbb{Q}$, the only trivial automorph being here the identity. The method involves invariants and covariants of f. In §4 we consider an analogous question for weak automorphs defined over K and give an answer in terms of the Galois group $\mathrm{Gal}(f, K)$ of the polynomial $f(x, 1)$ over K (Theorem 6). For cubic forms and $K = \mathbb{Q}$ a necessary and sufficient condition (if f is irreducible, the discriminant of f has to be a square in $\mathbb{Q}$) has been given in a recent unpublished manuscript of A. Choudhry [4]. For forms of odd degree with non-zero discriminant (in what follows called *non-singular*), existence of a weak non-trivial automorph is equivalent to existence of a strict non-trivial automorph (see [22, p. 40] and [20, Theorem 3.5]), but it is not obvious that Choudhry's condition and Segre's condition ([22, p. 48]) are equivalent. For non-singular cubic forms with $f(1, 0) \neq 0$ the structure of $\mathrm{Gal}(f, K)$ determines the isomorphism class of $\mathrm{Aut}(f, K)$, for quartic forms it does not in general. On the other hand, for K algebraically closed and f a non-singular quartic, the isomorphism class of $\mathrm{Aut}(f, K)$ is determined by invariants of f (§5, Theorem 7). For $K = \mathbb{C}$ this is well known ([1, Example 3.6], cf. also [24, Proposition 3.2]), but at least for $\mathrm{char}\, K = 2, 3$ it seems new.

For forms f of degree 5 a characterization of the isomorphism class of $\mathrm{Aut}(f, \mathbb{C})$ by invariants and covariants of f can be deduced from the work of Clebsch and Gordan [6] and of Clebsch [5] on the so called typical representations of binary forms. For f non-singular of degree 6 a characterization of the isomorphism class of $\mathrm{Aut}(f, \mathbb{C})$ by covariants of f was obtained by Maiasano [17] and one by invariants of f by Bolza [2]. Recently a practical way of finding $\mathrm{Aut}(f, \mathbb{C})$ by means of covariants of f has been proposed by Berchenko and Olver [1]. However, it is not clear from it whether for non-singular forms f of degree greater than 6 the condition $|\mathrm{Aut}(f, K)| > 1$ can be characterized by invariants of f. We shall show (Theorem 8) that the set of forms $f \in \mathbb{C}[x, y]$ with $|\mathrm{Aut}(f, \mathbb{C})| > 1$ is Zariski closed only for $n \leq 5$.

I conclude this introduction by expressing my thanks to A. Choudhry for sending me his unpublished manuscript [4] as well as a copy of [2], to A. Pokrzywa for factoring several multivariate polynomials that appeared in an earlier version of the paper and to A. Sładek who suggested many corrections and a simplification.

1. Lemmas on $\mathrm{PGL}_2(K)$

DEFINITION 1. Let K be a field of characteristic π. If $T_0(x,y) = (\alpha x + \beta y,\ \gamma x + \delta y) \in \mathrm{GL}_2(K)$, the image of T_0 in $\mathrm{PGL}_2(K)$ will be denoted by $T = \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)K^*$, or if $\mathrm{PGL}_2(K)$ is represented as the group of fractional linear transformations, by T^*. The order of T in $\mathrm{PGL}_2(K)$ will be denoted by $o(T)$, the unit element by E. Moreover, ζ_ν is a primitive root of unity of order ν in $\overline{K}$, if it exists.

LEMMA 1. $\mathrm{PGL}_2(K)$ *contains an element of order* $\nu > 1$ *if and only if either* $\nu = \pi$, *or* $\nu \not\equiv 0 \bmod \pi$ *and* $\zeta_\nu + \zeta_\nu^{-1} \in K$. *If this condition is satisfied, then* $\mathrm{PGL}_2(K)$ *contains a dihedral group of order* 2ν *except for* $K = \mathbb{F}_2$, $\nu = 2$.

Proof. Let $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)K^*$ be an element of order $\nu > 1$ in $\mathrm{PGL}_2(K)$. By the Jordan normal form theorem (see [26, §88]) there exist a, b, c, d in $\overline{K}$ such that $ad - bc \neq 0$ and

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}^{-1}\begin{pmatrix}\lambda_1 & \mu\\ 0 & \lambda_2\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix},$$

where $\lambda_1\lambda_2 \neq 0$ and either $\mu = 0$, or $\lambda_1 = \lambda_2 = \lambda$ and $\mu = 1$. In the former case λ_1/λ_2 is a primitive root of unity ζ of order ν, hence $\nu \not\equiv 0 \bmod \pi$ and

$$\lambda_2(1+\zeta) = \lambda_1 + \lambda_2 = \mathrm{Tr}\begin{pmatrix}\lambda_1 & \mu\\ 0 & \lambda_2\end{pmatrix} = \mathrm{Tr}\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} = \alpha + \delta \in K,$$

$$\lambda_2^2\zeta = \lambda_1\lambda_2 = \begin{vmatrix}\lambda_1 & \mu\\ 0 & \lambda_2\end{vmatrix} = \begin{vmatrix}\alpha & \beta\\ \gamma & \delta\end{vmatrix} = \alpha\delta - \beta\gamma \in K.$$

Hence $\zeta + \zeta^{-1} = (\lambda_2(1+\zeta))^2/\lambda_2^2\zeta - 2 \in K$. In the latter case

$$\begin{pmatrix}\lambda_1 & \mu\\ 0 & \lambda_2\end{pmatrix}^\nu = \begin{pmatrix}\lambda^\nu & \nu\lambda^{\nu-1}\\ 0 & \lambda^\nu\end{pmatrix},$$

hence $\nu = \pi$.

If the asserted condition is satisfied, then $\mathrm{PGL}_2(K)$ contains a dihedral group of order 2ν generated by

$$\begin{pmatrix}1+\zeta+\zeta^{-1} & -1\\ 1 & 1\end{pmatrix}K^* \quad\text{and}\quad \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}K^* \qquad \text{if } \nu \not\equiv 0 \bmod \pi,$$

$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}K^* \quad\text{and}\quad \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}K^* \qquad \text{if } \nu = \pi \neq 2,$$

$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}K^* \quad\text{and}\quad \begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}K^* \qquad \text{if } \nu = \pi = 2,\ a \in K \setminus \mathbb{F}_2.$$

REMARK. For $K = \mathbb{Q}$ Lemma 1 has been proved by Segre in Subsection 9 of [22].

LEMMA 2. $\mathrm{PGL}_2(K)$ *contains a subgroup isomorphic to* $\mathfrak{A}_4$ *if and only if either* $\pi \neq 2$ *and* $\mathrm{level}\, K \leq 2$, *or* $\pi = 2$ *and* $\mathbb{F}_4 \subset K$. *If and only if the former condition is satisfied,* $\mathrm{PGL}_2(K)$ *contains a subgroup isomorphic to* $\mathfrak{S}_4$.

$\mathrm{PGL}_2(K)$ *contains a subgroup isomorphic to* $\mathfrak{A}_5$ *if and only if either* $\pi \neq 2$, $\mathrm{level}\, K \leq 2$ *and* $\sqrt{5} \in K$, *or* $\pi = 2$ *and* $\mathbb{F}_4 \subset K$.

REMARK. The *level* of a field K is the minimal number k such that $x_1^2+\dots+x_k^2=-1$ for some $x_i \in K$.

Proof. If $\pi = 3$ the condition on the level is trivially satisfied, so assume $\pi \neq 3$ and let M be a matrix over K such that MK^* is of order 3 in $\mathrm{PGL}_2(K)$. Then M is equivalent over $\overline{K}$ to a matrix $\left(\begin{smallmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{smallmatrix}\right)$, where λ_1/λ_2 is a primitive root of unity ζ of order 3 and $M\frac{1+\zeta^{-1}}{\lambda_2}$ is equivalent over $\overline{K}$ to

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

But (see the proof of Lemma 1) $\lambda_2(1+\zeta) \in K$ and $(1+\zeta^2)/\zeta \in K$, hence, on division, $\lambda_2/(1+\zeta^{-1}) \in K$ and $M\frac{1+\zeta^{-1}}{\lambda_2}$ is defined over K. It follows that

$$M\frac{1+\zeta^{-1}}{\lambda_2} \text{ is equivalent to } \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \text{ over } K.$$

Hence a subgroup of $\mathrm{PGL}_2(K)$ isomorphic to $\mathfrak{A}_4$ is conjugate to a subgroup $\mathcal{G}$ containing $\left(\begin{smallmatrix}0 & -1\\ 1 & 1\end{smallmatrix}\right)K^* = T$. Thus there exists $S \in \mathcal{G}$ such that

$$S^2 = E \quad \text{and} \quad TST = ST^{-1}S.$$

Taking $S = \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)K^*$ we obtain by calculation $\delta = -\alpha$, $(2\alpha+\gamma-\beta)^2+\beta^2+\gamma^2 = 0$ and if $\pi = 2$, then $\beta^2-\beta\gamma+\gamma^2 = 0$. Thus $\operatorname{level} K \leq 2$ and if $\pi = 2$, then β/γ is a primitive root of unity of order 3, hence $\mathbb{F}_4 \subset K$.

In the opposite direction, if $\pi = 2$ and ζ is a primitive root of unity of order 3, then the group

$$\left\langle \begin{pmatrix} 0 & \zeta \\ 1 & 0 \end{pmatrix} K^*, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} K^* \right\rangle$$

is isomorphic to $\mathfrak{A}_4$. If $\pi \neq 2$, then the assumption that $\operatorname{level} K \leq 2$ implies existence of x_1, x_2 in K such that $x_1^2+x_2^2+1 = 0$. Then the group generated by

$$S = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} K^*, \quad T = \begin{pmatrix} x_1 & x_2+1 \\ x_2-1 & -x_1 \end{pmatrix} K^*$$

is isomorphic to $\mathfrak{S}_4$. Indeed, $S^4 = E$, $T^2 = E$ and $(ST)^3 = E$, which gives the required property (see [7, Table 1]). If $\pi = 2$, then $\mathrm{PGL}_2(K)$ does not contain a subgroup isomorphic to $\mathfrak{S}_4$ since, by Lemma 1, it contains no element of order 4.

Assume now that $\mathrm{PGL}_2(K)$ contains a subgroup isomorphic to $\mathfrak{A}_5$. Since $\mathfrak{A}_5$ contains $\mathfrak{A}_4$ and $\mathfrak{C}_5$, it follows from the already proved part of the lemma and from Lemma 1 that either $\pi \neq 2$ and $\operatorname{level} K \leq 2$, or $\pi = 2$ and $\mathbb{F}_4 \subset K$; moreover, either $\zeta+\zeta^{-1} \in K$, where ζ is a primitive root of unity of order 5, or $\pi = 5$. If $\pi = 2$ and $\mathbb{F}_4 \subset K$, then $\mathrm{PGL}_2(K)$ contains an isomorphic image of $\mathrm{PGL}_2(\mathbb{F}_4) \cong \mathfrak{A}_5$; if $\pi \neq 2$, then the condition $\zeta+\zeta^{-1} \in K$ implies $\varrho = (\sqrt{5}-1)/2 \in K$, which also holds for $\pi = 5$. Conversely, if $\sqrt{5} \in K$ and $\operatorname{level} K \leq 2$, we have $x_1^2+x_2^2+1 = 0$ for some x_1, x_2 in K, hence the group $\langle R, S\rangle$, where

$$R = \begin{pmatrix} -1+x_2\varrho & x_1+x_2\varrho-\varrho-1 \\ 2 & 1-x_2\varrho \end{pmatrix} K^*, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} K^*,$$

is isomorphic to $\mathfrak{A}_5$, provided

$$\begin{vmatrix} -1+x_2\varrho & x_1+x_2\varrho-\varrho-1 \\ 2 & 1-x_2\varrho \end{vmatrix} = -x_2^2\varrho^2 - 2x_1 + 2\varrho + 2 \neq 0,$$

and this follows from $\pi \neq 2$ if $x_1 = 0$, while it can be achieved by changing the sign of x_1 if $x_1 \neq 0$. Indeed, we have $R^2 = E$, $S^3 = E$ and $(RS)^5 = E$, which implies $\langle R, S\rangle \cong \mathfrak{A}_5$ (see [7, Table 5]).

REMARK. Lemma 2 in an equivalent formulation is given without proof by Serre [23]. Segre only proves ([22, Subsection 12]) that if K is real, then $\mathrm{PGL}_2(K)$ does not contain a copy of $\mathfrak{A}_4$.

LEMMA 3. *Let $\mathcal{G}$ be a non-trivial subgroup of $\mathrm{PGL}_2(K)$. If for all elements S of $\mathcal{G} \setminus \{E\}$ the equation $S^*\xi = \xi$ has exactly one solution in $\overline{K} \cup \{\infty\}$, then $\pi > 0$ and $\mathcal{G}$ is a π-group. Every such finite group is generated by elements*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} \lambda_i & 1 \\ 0 & \lambda_i \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} K^* \qquad (1 \leq i \leq g)$$

where $ad - bc \neq 0$, the λ_i^{-1} are linearly independent over $\mathbb{F}_\pi$ and either $a, b, c, d, \lambda_i \in K$, or $\pi = 2$, $a = 0$, $b = 1$, $c \in K$, $K(d)$ is a quadratic inseparable extension of K and $\lambda_i + d \in K$. Every infinite π-group contained in $\mathrm{PGL}_2(K)$ contains the above finite groups for all g.

Proof. Let $S_1 = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) K^* \in \mathcal{G} \setminus \{E\}$, hence $\alpha\delta - \beta\gamma \neq 0$. By the Jordan normal form theorem there exists a non-singular matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ over $\overline{K}$ such that

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} \lambda & \mu \\ 0 & \nu \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

where $\lambda\nu \neq 0$ and either $\mu = 0$, or $\lambda = \nu$ and $\mu = 1$. In the former case the equation $S_1^*\xi = \xi$ has two solutions in $\overline{K} \cup \{\infty\}$, namely $-b/a$ and $-d/c$. Since the case $\lambda = \nu$, $\mu = 0$ is excluded by the assumption $S_1 \neq E$, we obtain $\mu = 1$ and

$$4\lambda^2 = (\alpha + \delta)^2 = 4(\alpha\delta - \beta\gamma). \tag{1}$$

The second equality of (1) holds for all elements S of $\mathcal{G}$. Let

$$S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} \varepsilon & \zeta \\ \eta & \vartheta \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} K^* \in \mathcal{G} \setminus \{E\}.$$

Since $S_1^i S \in \mathcal{G}$ and

$$\begin{pmatrix} \lambda & i \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} \varepsilon & \zeta \\ \eta & \vartheta \end{pmatrix} = \begin{pmatrix} \lambda\varepsilon + i\eta & \lambda\zeta + i\vartheta \\ \lambda\eta & \lambda\vartheta \end{pmatrix}$$

we obtain from (1)

$$(\lambda\varepsilon + \lambda\vartheta + i\eta)^2 = 4\lambda^2(\varepsilon\vartheta - \eta\zeta) \quad (i = 0, 1, 2),$$

hence

$$\eta = 0, \qquad \varepsilon = \vartheta, \qquad \zeta \neq 0,$$

hence S is of infinite order in $\mathrm{PGL}_2(K)$ unless $\pi > 0$, in which case $S^\pi = E$ and $\mathcal{G}$ is a π-group. This proves the first part of the lemma.

In order to prove the second part let us again consider S_1. The condition $S_1^\pi = E \neq S_1$ implies in the above notation

$$\lambda^\pi = \nu^\pi, \quad \mu \neq 0,$$

hence $\lambda = \nu =: \lambda_1$ and $\mu = 1$. It follows that we have again equation (1) and for every S in $\mathcal{G}$,

$$S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} \varepsilon & \zeta \\ 0 & \varepsilon \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} K^*.$$

If $\lambda_1 \in K$, then a, b, c, d can be chosen in K and hence $\varepsilon, \zeta \in K$ and

$$S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} 1 & \zeta/\varepsilon \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} K^*.$$

For S running through $\mathcal{G}$, ζ/ε runs through a linear space L over $\mathbb{F}_\pi$ and letting $\lambda_1^{-1}, \ldots$ $\ldots, \lambda_g^{-1}$ be a basis of this space we obtain the assertion of the lemma.

If $\lambda_1 \notin K$, then the polynomial $z^2 - (\alpha + \delta)z + (\alpha\delta - \beta\gamma)$ is irreducible inseparable over K, hence $\pi = 2$, $\gamma \neq 0$ and we can choose $a = 0$, $b = 1$, $c = \gamma$, $d = \lambda_1 - \alpha$. Then the condition $S \in \mathrm{PGL}_2(K)$ gives $\varepsilon + d\zeta \in K$, $d^2\zeta \in K$, hence $\zeta \in K$ and

$$S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} \varepsilon/\zeta & 1 \\ 0 & \varepsilon/\zeta \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} K^*.$$

Taking again a basis $\lambda_1^{-1}, \ldots, \lambda_g^{-1}$ of L we obtain $\lambda_i + d \in K$, which completes the proof for finite groups $\mathcal{G}$. If $\mathcal{G}$ is infinite, so is L and for every g it contains $\lambda_1^{-1}, \ldots, \lambda_g^{-1}$ linearly independent.

LEMMA 4. *Let $\mathcal{G}$ be a non-trivial finite subgroup of $\mathrm{PGL}_2(K)$ and let*

$$O(\mathcal{G}) = \bigcup_{S \in \mathcal{G} \setminus \{E\}} \left\{ \xi \in \overline{K} \cup \{\infty\} : S^*\xi = \xi \right\}.$$

If $\mathcal{G}$ is not a π-group, then the number h of orbits of $O(\mathcal{G})$ under the action of $\mathcal{G}$ is either two or three.

Proof. Let the orbits in question be $O_1, \ldots, O_h$. For each $\xi \in O_i$ the number $|\{S \in \mathcal{G} : S^*\xi = \xi\}|$ is the same, say ν_i. Clearly $|\mathcal{G}| = \nu_i \mu_i$, where $\mu_i = |O_i|$ and

$$\sum_{i=1}^{h} (\nu_i - 1)\mu_i = \sum_{\xi \in \overline{K} \cup \{\infty\}} \sum_{\substack{S \in \mathcal{G} \setminus \{E\} \\ S^*\xi = \xi}} 1 = \sum_{S \in \mathcal{G} \setminus \{E\}} \sum_{\substack{\xi \in \overline{K} \cup \{\infty\} \\ S^*\xi = \xi}} 1.$$

But for each $S \in \mathcal{G} \setminus \{E\}$ the equation $S^*\xi = \xi$ has in $\overline{K} \cup \{\infty\}$ either one or two solutions and, by Lemma 3, the latter possibility occurs at least once. It follows that

$$2|\mathcal{G}| - 2 \geq \sum_{i=1}^{h} (\nu_i - 1)\, \mu_i > |\mathcal{G}| - 1.$$

Since

$$\sum_{i=1}^{h} (\nu_i - 1)\mu_i = h|\mathcal{G}| - \sum_{i=1}^{h} \mu_i \in \left[\frac{h}{2} |\mathcal{G}|,\, h|\mathcal{G}| - h \right],$$

we obtain $2 \leq h \leq 3$.

REMARK. For $K = \mathbb{C}$ and $K = \mathbb{F}_\pi$, $|\mathcal{G}| \not\equiv 0 \bmod \pi$, Lemma 4 and the above proof are well known (see [27, Vol. II, §68 and §87].

LEMMA 5. *In the notation of the proof of Lemma* 4, *if* $T \in \mathcal{G}$, $\xi \in O_j$ *and* $T^*\xi = \xi$, *then* $o(T) \mid |\mathcal{G}|/|O_j|$.

Proof. The group $\langle T\rangle$ of order $o(T)$ is a subgroup of the stabilizer of ξ in $\mathcal{G}$ of order $|\mathcal{G}|/|O_j|$.

LEMMA 6. *Under the assumptions of Lemma* 4, *let* $K_j = K(O_j \setminus \{\infty\})$. *Then* $[K_j : K] \leq 2$ *for all* $j \leq h$. *We have the following possibilities*:

(2) *for all* $j \leq h$ *either* $[K_j : K]_s = 1$ *or* $[K_j : K]_s = 2$, $\infty \notin O_j$, $\mathrm{Gal}(K_j/K) = \langle\sigma_j\rangle$, *and* $\sigma_j(O_j) = O_j$;

(3) *for a suitable numbering of* O_j, $[K_1 : K]_s = 2, \mathrm{Gal}(K_1/K) = \langle\sigma_1\rangle$, $\infty \notin O_1$, $\sigma_1(O_1) = O_2$ *and either* $h = 2$, *or* $h = 3, [K_3 : K]_s = 1$, *or* $h = 3, [K_3 : K]_s = 2$, $\mathrm{Gal}(K_3/K) = \langle\sigma_3\rangle, \infty \notin O_3, \sigma_3(O_3) = O_3$.

Proof. If $\xi \in O(\mathcal{G}) \setminus \{\infty\}$, then $S^*\xi = \xi$ for an $S \in \mathcal{G}$, hence $[K(\xi) : K] \leq 2$ and if $\xi \in O_j$, then $[K_j : K] \leq 2$. If $[K_j : K] = 2$, then $\infty \notin O_j$ since $S^*(\infty) \in K \cup \{\infty\}$ for all $S \in \mathcal{G}$. If (2) does not hold, then for some j we have $[K_j : K]_s = 2$, $\mathrm{Gal}(K_j/K) = \langle\sigma_j\rangle$ and $\sigma_j(O_j) \neq O_j$. Therefore, there exists $\xi_0 \in O_j$ such that $\sigma_j(\xi_0) \notin O_j$. But $S_0^*\xi_0 = \xi_0$ for some $S_0 \in \mathcal{G} \setminus \{E\}$; then also $S_0^*\sigma_j(\xi_0) = \sigma_j(\xi_0)$, hence $\sigma_j(\xi_0) \in O_k$ for some $k \neq j$ and renumbering the O_i we may assume that $j = 1$, $k = 2$, $\sigma_1(O_1) = O_2$. If $h = 3$ the situation cannot repeat itself with $j = 3$ since there exists no suitable k, thus either $[K_3 : K]_s = 1$, or $[K_3 : K]_s = 2$, $\mathrm{Gal}(K_3/K) = \langle\sigma_3\rangle$ and $\sigma_3(O_3) = O_3$. This gives (3).

LEMMA 7. *For every finite subgroup* $\mathcal{G}$ *of* $\mathrm{PGL}_2(K)$ *of order not divisible by* π *the sequence* $|O_1|, \ldots, |O_h|$ *in the notation of the proof of Lemma* 4 *is a permutation of one of the sequences*: $\langle 1, 1\rangle$ ($\mathcal{G} \cong \mathfrak{C}_\nu$), $\langle |\mathcal{G}|/2, |\mathcal{G}|/2, 2\rangle$ ($\mathcal{G} \cong \mathfrak{D}_\nu$), $\langle 4, 4, 6\rangle$ ($\mathcal{G} \cong \mathfrak{A}_4$), $\langle 6, 8, 12\rangle$ ($\mathcal{G} \cong \mathfrak{S}_4$), $\langle 12, 20, 30\rangle$ ($\mathcal{G} \simeq \mathfrak{A}_5$).

Proof. If $|\mathcal{G}| \not\equiv 0 \bmod \pi$, then by Lemma 3 for every $S \in \mathcal{G} \setminus \{E\}$ the number of solutions of $S^*\xi = \xi$ is 2, hence following the proof of Lemma 4 we obtain

$$2|\mathcal{G}| - 2 = \sum_{i=1}^{h} (\nu_i - 1)\mu_i = h|\mathcal{G}| - \sum_{i=1}^{h} |\mathcal{G}|/\nu_i$$

for $h = 2$ or 3. This equation is well known (see [27, Vol. II, §68]) and gives for decreasing ν_i either $h = 2$, $\nu_1 = \nu_2 = |\mathcal{G}|$, or $h = 3$, $\langle \nu_1, \nu_2, \nu_3\rangle = \langle |\mathcal{G}|/2, 2, 2\rangle$, or $h = 3$, $\langle |\mathcal{G}|; \nu_1, \nu_2, \nu_3\rangle = \langle 12; 3, 3, 2\rangle$, $\langle 24; 4, 3, 2\rangle$, $\langle 60; 5, 3, 2\rangle$. Since $\mu_i = |\mathcal{G}|/\nu_i$ we obtain the lemma.

LEMMA 8. *Let* $\mathcal{G} = \mathrm{PSL}_2(\mathbb{F}_q)$. *In the notation of Lemma* 4 *we have*

$$O(\mathcal{G}) = \mathbb{F}_{q^2} \cup \{\infty\} \tag{4}$$

and, up to a permutation, $O_1 = \mathbb{F}_q \cup \{\infty\}$, $O_2 = \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

Proof. The formulae

$$S \in \mathcal{G} \setminus \{E\}, \quad \xi \in \overline{\mathbb{F}}_q \cup \{\infty\}, \quad S^*\xi = \xi \tag{5}$$

imply $\xi \in \mathbb{F}_{q^2} \cup \{\infty\}$. On the other hand, if $\xi \in \mathbb{F}_q$ or $\xi \in \mathbb{F}_{q^2}$, $\xi^2 + a\xi + b = 0$, $a, b \in \mathbb{F}_q$, or $\xi = \{\infty\}$, then (5) holds for

$$S = \begin{pmatrix} 1+\xi & -\xi^2 \\ 1 & 1-\xi \end{pmatrix}\mathbb{F}_q^* \quad \text{or} \quad \begin{pmatrix} \alpha\varepsilon^{-1} & -b\varepsilon^{-1} \\ \varepsilon^{-1} & \alpha\varepsilon^{-1} + a\varepsilon^{-1} \end{pmatrix}\mathbb{F}_q^* \quad \text{or} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\mathbb{F}_q^*,$$

respectively, where α and ε are chosen in $\mathbb{F}_q$ so that $\alpha^2 + a\alpha + b = \varepsilon^2$; $\varepsilon \neq 0$ since $x^2 + ax + b$ is irreducible over $\mathbb{F}_q$. This proves (4).

Moreover, if $\xi = 0$, $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\mathbb{F}_q^*$ or $\xi \in \mathbb{F}_q^*$, $S = \left(\begin{smallmatrix} \xi & 0 \\ 1 & \xi^{-1} \end{smallmatrix}\right)\mathbb{F}_q^*$ we have

$$S \in \mathcal{G}, \quad S^*\infty = \xi.$$

Finally, if $\xi, \eta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and ξ', η' are conjugates of ξ, η with respect to $\mathbb{F}_q$ we have $(\eta - \eta')/(\xi - \xi') \in \mathbb{F}_q$. There exist δ, ε in $\mathbb{F}_q$ such that

$$\frac{\eta - \eta'}{\xi - \xi'}(\delta + \xi)(\delta + \xi') = \varepsilon^2 \neq 0.$$

Then taking

$$S = \begin{pmatrix} \dfrac{\delta(\eta - \eta') + (\eta\xi - \eta'\xi')}{\varepsilon(\xi - \xi')} & \dfrac{\delta(\eta'\xi - \eta\xi') + \xi\xi'(\eta' - \eta)}{\varepsilon(\xi - \xi')} \\ \varepsilon^{-1} & \delta\varepsilon^{-1} \end{pmatrix}\mathbb{F}_q^*$$

we find $S \in \mathcal{G}$ such that $S^*\xi = \eta$, which completes the proof.

LEMMA 9. *The statement of Lemma* 8 *is also true for* $\mathcal{G} = \mathrm{PGL}_2(\mathbb{F}_q)$.

Proof. If $\mathcal{H}_1 = \mathrm{PGL}_2(\mathbb{F}_q)$, $\mathcal{H}_2 = \mathrm{PSL}_2(\mathbb{F}_q)$ we have, in the notation of Lemma 4,

$$O(\mathcal{H}_2) \subset O(\mathcal{H}_1);$$

but, clearly, $O(\mathcal{H}_1) \subset \mathbb{F}_{q^2} \cup \{\infty\}$, hence by Lemma 8,

$$O(\mathcal{H}_1) = \mathbb{F}_{q^2} \cup \{\infty\}.$$

Since $\mathcal{H}_2 \subset \mathcal{H}_1$ the orbits of $\mathbb{F}_{q^2} \cup \{\infty\}$ under the action of $\mathcal{H}_1$ are unions of orbits under the action of $\mathcal{H}_2$; Lemma 8 shows that they are either $\mathbb{F}_q \cup \{\infty\}$ and $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$, or $\mathbb{F}_{q^2} \cup \{\infty\}$. As the image of $\mathbb{F}_q \cup \{\infty\}$ under the action of $\mathcal{H}_1$ is again $\mathbb{F}_q \cup \{\infty\}$, the former case holds.

DEFINITION 2. If K, L are fields, $K \subset L$ and $\mathcal{G}$ is a subgroup of $\mathrm{PGL}_2(K)$, then $\mathcal{G}L^*/L^*$ is the subgroup of $\mathrm{PGL}_2(L)$ defined as

$$\{ML^* : M \in \mathrm{GL}_2(K),\ MK^* \in \mathcal{G}\}.$$

LEMMA 10. *For* $\pi > 0$ *every finite subgroup of* $\mathrm{PGL}_2(K)$ *is isomorphic to a subgroup of* $\mathrm{PSL}_2(\mathbb{F}_s)$, *where* s *is a power of* π.

Proof. Let $\mathcal{G} = \left\{\left(\begin{smallmatrix} \alpha_i & \beta_i \\ \gamma_i & \delta_i \end{smallmatrix}\right)K^* : 1 \leq i \leq k\right\}$. The isomorphism class of $\mathcal{G}$ is determined by finitely many equalities $F_i(\alpha_1, \ldots, \delta_k) = 0$ and inequalities $G_j(\alpha_1, \ldots, \delta_k) \neq 0$, where F_i and G_j are polynomials over $\mathbb{F}_\pi$. By the theorem on elimination of existential quantifiers in algebraically closed fields, if this system of equalities and inequalities is solvable in K, it is also solvable in the algebraic closure of $\mathbb{F}_\pi$, hence also in a field $\mathbb{F}_q$, where q is a power of π. Thus $\mathcal{G}$ is isomorphic to a subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$. Since for $s = q^2$, $\mathrm{PGL}_2(\mathbb{F}_q)\mathbb{F}_s^*/\mathbb{F}_s^*$ is contained in $\mathrm{PSL}_2(\mathbb{F}_s)$, it follows that s satisfies the assertion of the lemma.

LEMMA 11. *For $\pi > 0$ and a finite subgroup $\mathcal{G}$ of $\mathrm{PGL}_2(K)$ of order divisible exactly by π^g $(g > 0)$ let σ be the number of π-Sylow subgroups in $\mathcal{G}$. We have the following possibilities*:

$$\sigma = 1;$$
$$\sigma = \pi^g + 1, \quad \mathcal{G} \cong \mathrm{PGL}_2(\mathbb{F}_{\pi^g}) \text{ or } \mathrm{PSL}_2(\mathbb{F}_{\pi^g});$$
$$\pi^g = 2, \quad \sigma = 2\varrho + 1\,(\varrho \geq 1), \quad \mathcal{G} \cong \mathfrak{D}_{2\varrho+1};$$
$$\pi^g = 3, \quad \sigma = 10, \quad \mathcal{G} \cong \mathfrak{A}_5.$$

Proof. In view of Lemma 10 this follows from an analogous property of subgroups of $\mathrm{PSL}_2(\mathbb{F}_s)$ (see [12, Chapter XII, Sections 249–253], with m replaced by g and f by ϱ).

LEMMA 12. *Let $\mathcal{H}_1 = \mathrm{PGL}_2(\mathbb{F}_q)$ and $\mathcal{H}_2 = \mathrm{PSL}_2(\mathbb{F}_q)$, where $q = \pi^g$. Every subgroup of $\mathrm{PGL}_2(\overline{K})$ isomorphic to $\mathcal{H}_i$ is conjugate to $\mathcal{H}_i\overline{K}^*/\overline{K}^*$.*

Proof. The existence of a subgroup of $\mathrm{PGL}_2(\overline{K})$ isomorphic to $\mathcal{H}_i$, but not conjugate to $\mathcal{H}_i\overline{K}^*/\overline{K}^*$ is a statement involving finitely many existential and universal quantifiers and equalities and inequalities concerning polynomials with coefficients in $\mathbb{F}_q$. By the theorem on elimination of existential quantifiers in algebraically closed fields, if this statement is true, it is also true in $\overline{\mathbb{F}}_q$. Therefore, there exists a subgroup $\mathcal{G}$ of $\mathrm{PGL}_2(\overline{\mathbb{F}}_q)$ isomorphic to $\mathcal{H}_i$, but not conjugate to $\mathcal{H}_i\overline{\mathbb{F}}_q^*/\overline{\mathbb{F}}_q^*$. For A running through $\mathrm{GL}_2(\overline{\mathbb{F}}_q)$ such that $A\overline{\mathbb{F}}_q^* \in \mathcal{G}$, $A/\sqrt{\det A}$ runs through finitely many matrices, which all lie in $\mathrm{SL}_2(\mathbb{F}_s)$ for some s which is a power of q. If

$$\mathcal{G}_0 = \left\{ \frac{M}{\sqrt{\det M}}\,\mathbb{F}_s^* : M\mathbb{F}_q^* \in \mathcal{G} \right\}, \tag{6}$$

then $\mathcal{G}_0$ is isomorphic to $\mathcal{G}$, hence to $\mathcal{H}_i$. By the known property of $\mathrm{PSL}_2(\mathbb{F}_s)$ (see [12, Chapter XII, italicized statements on pp. 274 and 278 and the normalization of G_Ω on p. 273]), $\mathcal{G}_0$ is conjugate in $\mathrm{PGL}_2(\mathbb{F}_s)$ to $\mathcal{H}_i\mathbb{F}_s^*/\mathbb{F}_s^*$. Hence there exists $A_0 \in \mathrm{GL}_2(\mathbb{F}_s)$ such that

$$\mathcal{G}_0 = A_0\mathcal{H}_iA_0^{-1}.$$

By (6) this gives

$$\mathcal{G}_0 = A_0\mathcal{H}_iA_0^{-1}\overline{\mathbb{F}}_q^*/\overline{\mathbb{F}}_q^*,$$

thus $\mathcal{G}$ is conjugate in $\mathrm{PGL}_2(\overline{\mathbb{F}}_q)$ to $\mathcal{H}_i\overline{\mathbb{F}}_q^*/\overline{\mathbb{F}}_q^*$, a contradiction.

LEMMA 13. *If $\mathbb{F}_q \subset K$, then every subgroup $\mathcal{G}$ of $\mathrm{PGL}_2(K)$ isomorphic to $\mathcal{H}_i$ (notation of Lemma 12) is conjugate to $\mathcal{H}_iK^*/K^*$.*

Proof. By Lemma 12 there exists $A \in \mathrm{GL}_2(\overline{K})$ such that for $i = 1$ or 2,

$$\mathcal{G}\overline{K}^*/\overline{K}^* = A\mathcal{H}_iA^{-1}\overline{K}^*/\overline{K}^*. \tag{7}$$

It follows that for all $M \in \mathrm{SL}_2(\mathbb{F}_q)\mathbb{F}_q^{*2}$ there exists $t \in \overline{K}^*$ such that

$$tAMA^{-1} \in \mathrm{GL}_2(K). \tag{8}$$

Now, if

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

then

$$AMA^{-1} = \frac{1}{ad-bc}\begin{pmatrix} ad\alpha - ac\beta + bd\gamma - bc\delta & -ab\alpha + a^2\beta - b^2\gamma + ab\delta \\ cd\alpha - c^2\beta + d^2\gamma - cd\delta & -bc\alpha + ac\beta - bd\gamma + ad\delta \end{pmatrix}.$$

Applying (8) with

$$M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix},$$

we obtain

$$(9_1)\quad t\frac{ad}{ad-bc} \in K, \qquad (9_2)\quad t\frac{ac}{ad-bc} \in K, \qquad (9_3)\quad t\frac{bc}{ad-bc} \in K;$$

$$(10_1)\quad t\frac{ab}{ad-bc} \in K, \qquad (10_2)\quad t\frac{a^2}{ad-bc} \in K;$$

$$(11_1)\quad t\frac{c^2}{ad-bc} \in K, \qquad (11_2)\quad t\frac{cd}{ad-bc} \in K.$$

Since $ad-bc \neq 0$ we have $a \neq 0$ or $c \neq 0$. If $a \neq 0$, then (9_1) and (10_2) imply $d/a \in K$, (9_2) and (10_2) imply $c/a \in K$, and (10_1) and (10_2) imply $b/a \in K$, hence $a^{-1}A \in \mathrm{GL}_2(K)$. If $c \neq 0$ the same conclusion follows from (9_2), (9_3), (11_2) and (11_1). By (7),

$$\mathcal{G}\overline{K}^*/\overline{K}^* = a^{-1}A\mathcal{H}_iA^{-1}a\overline{K}^*/\overline{K}^*,$$

hence

$$\mathcal{G} = a^{-1}A\mathcal{H}_iA^{-1}a\overline{K}^*/\overline{K}^*,$$

which gives the assertion.

2. Determination of all binary forms with a given group of weak automorphs

Definition 3. If

$$\langle\alpha,\beta,\gamma,\delta\rangle \in K^4, \quad \alpha\delta-\beta\gamma \neq 0, \quad \langle\alpha,\beta,\gamma,\delta\rangle \neq \langle\alpha,0,0,\alpha\rangle \tag{12}$$

and

$$z^2-(\alpha+\delta)z+(\alpha\delta-\beta\gamma) = (z-\lambda_1)(z-\lambda_2), \quad \lambda_1,\lambda_2 \in \overline{K},\ \lambda_1 \neq \lambda_2, \tag{13}$$

we put

$$\chi_i = \gamma x + (\lambda_i-\alpha)y \quad (i=1,2) \quad \text{if } \gamma \neq 0,$$
$$\chi_1 = (\alpha-\delta)x + \beta y, \quad \chi_2 = y \quad \text{otherwise.}$$

Definition 4. If (12) holds and

$$z^2-(\alpha+\delta)z+(\alpha\delta-\beta\gamma) = (z-\lambda)^2, \quad \lambda \in \overline{K}, \tag{14}$$

we put

$$\chi_1 = \gamma x + (\lambda-\alpha)y, \quad \chi_2 = y \quad \text{if } \gamma \neq 0,$$
$$\chi_1 = \beta y, \quad \chi_2 = x \quad \text{otherwise.}$$

Theorem 1. *Let* $\langle\alpha,\beta,\gamma,\delta\rangle$ *satisfy* (12) *and* $T = \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)K^*$ *be of order* ν *in* $\mathrm{PGL}_2(K)$. *A form* $f \in \overline{K}[x,y] \setminus \{0\}$ *satisfies the conditions*

$$f \in K[x,y] \tag{15}$$

and

$$T \in \mathrm{Aut}(f, K) \tag{16}$$

if and only if either (13) *holds and*

$$f = \chi_1^{c_1}\chi_2^{c_2}\psi(\chi_1^{\nu} + \chi_2^{\nu}, \lambda_1\chi_1^{\nu} + \lambda_2\chi_2^{\nu}), \tag{17}$$

where χ_1, χ_2 *are given in Definition* 3, ψ *is a binary form over* K, *while* c_i *are integers satisfying* $0 \le c_i < \nu$ *and* $c_1 = c_2$ *if* χ_1, χ_2 *are conjugate over* K, *or* (14) *holds and*

$$f = \chi_1^{c_1}\psi(\chi_1^{\pi}, \lambda^{\pi-1}\chi_2^{\pi} - \chi_2\chi_1^{\pi-1}), \tag{18}$$

where χ_1, χ_2 *are given in Definition* 4, ψ *is a binary form over* K, *while* c_1 *is a non-negative integer satisfying* $c_1 < \pi = \nu$ *unless either* $\pi = 0$, *in which case* $\psi \in K^*$, c_1 *arbitrary, or* $\pi = 2 = \nu$, $\lambda \notin K$, *in which case* $c_1 = 0$.

Corollary 1. *If a form* $f \in K[x, y]$ *of degree* $n \not\equiv 0 \bmod \pi$ *has a weak automorph of order* ν *in* $\mathrm{PGL}_2(K)$, *then either* $\nu \mid n$ *and* $\zeta_\nu + \zeta_\nu^{-1} \in K$, *or* f *is the product of two forms with such automorphs, one of which, say* g, *is linear or quadratic.*

Corollary 2. *If a form* $f \in K[x, y]$ *of degree* $n \not\equiv 1 \bmod \pi$, $n > 2$, *has a weak automorph of order* ν *in* $\mathrm{PGL}_2(K)$ *and* f *is the product of a linear factor and another factor defined and irreducible over* K, *then* $\nu \mid n - 1$ *and* $\zeta_\nu \in K$.

Corollary 3. *If a quartic form* $f \in K[x, y]$ *has in* $\mathrm{PGL}_2(K)$ *a weak automorph of order* 3, *then either* $\sqrt{-3} \in K$ *or* f *is a square in* $\overline{K}[x, y]$.

Corollary 4. *If* $T_0 \in \mathrm{GL}_2(K)$ *and* $T = T_0K^*$ *is of finite order in* $\mathrm{PGL}_2(K)$, *then there exists* $c(T_0) \in K$ *such that if* $T \in \mathrm{Aut}(f, K)$, *then*

$$f(T_0)^{o(T)} = c(T_0)^{\deg f} f$$

and if, moreover, $f(\xi, 1) = 0$ *implies* $T^*\xi \ne \xi$, *then* $o(T) \mid \deg f$ *and*

$$f(T_0) = c(T_0)^{\deg f/o(T)} f.$$

Here $f(\infty, 1) = 0$ *means* $f(1, 0) = 0$.

Corollary 5. *Under the assumption of Theorem* 1 *about* T, *a form* $f \in \overline{K}[x, y] \setminus \{0\}$ *satisfies* (16) *if and only if either* (13) *and* (17) *hold, where* χ_1, χ_2 *are given in Definition* 3, ψ *is a binary form over* $\overline{K}$, *while* c_i *are integers satisfying* $0 \le c_i < \nu$, *or* (14) *and* (18) *hold, where* χ_1, χ_2 *are given in Definition* 4, *while* c_1 *is a non-negative integer satisfying* $c_1 < \pi = \nu$ *unless* $\pi = 0$, *in which case* $\psi \in K^*$, c_1 *arbitrary.*

The proof of Theorem 1 is based on three lemmas.

Lemma 14. *The linear forms* χ_1, χ_2 *given in Definition* 3 *are linearly independent and satisfy* $\chi_i(\alpha x + \beta y, \gamma x + \delta y) = \lambda_i\chi_i$ $(i = 1, 2)$, *provided for* $\gamma = 0$ *we have* $\lambda_1 = \alpha$, $\lambda_2 = \delta$. *Moreover, either* $\chi_i \in K[x, y]$ $(i = 1, 2)$, *or* χ_1, χ_2 *are conjugate over* K.

If $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)K^*$ *is of order* $\nu > 2$ *in* $\mathrm{PGL}_2(K)$, *then* $\chi_i \in K[x, y]$ *if and only if* K *contains a primitive root of unity of order* ν.

Proof. The first two assertions are proved by calculation and inspection. To prove the third assertion notice that $\chi_i \in K[x, y]$ if and only if $\lambda_i \in K$. If $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)K^*$ is of order

$\nu > 2$ in $\mathrm{PGL}_2(K)$ we know from the proof of Lemma 1 that λ_1/λ_2 is a primitive root of unity of order ν and that

$$\lambda_2(1+\lambda_1/\lambda_2) = \alpha + \delta \in K,$$

hence $\lambda_i \in K$ $(i = 1, 2)$ is equivalent to existence in K of a primitive root of unity of order ν.

LEMMA 15. *The linear forms χ_1, χ_2 given in Definition 4 are linearly independent and satisfy*

$$\chi_1(\alpha x + \beta y, \gamma x + \delta y) = \lambda\chi_1, \qquad \chi_2(\alpha x + \beta y, \gamma x + \delta y) = \lambda\chi_2 + \chi_1.$$

Moreover $\chi_1 \in K[x, y]$ unless $\pi = 2$ and $\lambda \notin K$.

Proof. By calculation and inspection.

LEMMA 16. *If $G \in K[x] \setminus K$, $\lambda \in \overline{K}^*$ and*

$$G(x + \lambda^{-1}) = rG(x), \qquad r \in K(\lambda)^*, \tag{19}$$

then $\pi \neq 0$ and

$$G(x) = H(\lambda^{\pi-1}x^\pi - x), \qquad \text{where } H \in K(\lambda)[x]. \tag{20}$$

REMARK. For K being a finite field and $\lambda \in K$ the lemma is due to Dickson.

Proof. By comparing the leading coefficients on both sides of (19) we obtain $r = 1$. Now (19) implies that

$$G\left(l\lambda^{-1}\right) = G(0) \qquad \text{for all } l \in \mathbb{Z},$$

hence $\pi \neq 0$. We shall prove (20) by induction on the degree of G, say n. If $n = 0$, then (20) holds with $H = G$. Assume that (20) is true for all G satisfying (19) of degree less than n and that $\deg G = n$. From (19) we obtain

$$\prod_{l=0}^{\pi-1}(x - l\lambda^{-1}) \,\Big|\, G(x) - G(0).$$

But

$$\prod_{l=0}^{\pi-1}(x - l\lambda^{-1}) = \lambda^{1-\pi}(\lambda^{\pi-1}x^\pi - x)$$

and

$$\lambda^{\pi-1}(x + \lambda^{-1})^\pi - (x + \lambda^{-1}) = \lambda^{\pi-1}x^\pi - x.$$

Taking

$$G_1(x) = \frac{G(x) - G(0)}{\lambda^{\pi-1}x^\pi - x}$$

we deduce from (19) that $G_1(x + \lambda^{-1}) = G_1(x)$, hence by the inductive assumption

$$G_1(x) = H_1(\lambda^{\pi-1}x^\pi - x), \qquad H_1 \in K(\lambda)[x],$$

and (20) holds with $H = xH_1(x) + G(0)$.

Proof of Theorem 1. Necessity. First assume (13). Since by Lemma 14, χ_1, χ_2 are linearly independent over $\overline{K}$ we can write

$$f(x, y) = \sum_{i=0}^{n} a_i \chi_1^{n-i}\chi_2^i, \qquad \text{where } a_i \in K(\lambda_1, \lambda_2), \tag{21}$$

and we set

$$I = \{i : a_i \neq 0\}.$$

It follows from (16) and Lemma 14 that

$$f(\alpha x + \beta y, \gamma x + \delta y) = \sum_{i\in I} a_i \lambda_1^{n-i}\lambda_2^i \chi_1^{n-i}\chi_2^i \tag{22}$$
$$= \lambda_1^n \sum_{i\in I} a_i (\lambda_2/\lambda_1)^i \chi_1^{n-i}\chi_2^i = r\sum_{i\in I} a_i \chi_1^{n-i}\chi_2^i.$$

Since T is in $\mathrm{PGL}_2(K)$ of order ν, λ_2/λ_1 is a primitive root of unity of order ν in $\overline{K}$.

If $I = \{j\}$, then we have (17) with $\psi = a_j$. If $|I| > 1$, then the condition (22) implies that there exist integers c_1, c_2 such that $0 \leq c_j < \nu$ and $i \equiv c_2$, $n - i \equiv c_1 \bmod \nu$ for all $i \in I$. Since

$$p = \chi_1^\nu + \chi_2^\nu,\ q = \lambda_1\chi_1^\nu + \lambda_2\chi_2^\nu \quad \text{is equivalent to} \quad \chi_1^\nu = \frac{q - \lambda_2 p}{\lambda_1 - \lambda_2},\ \chi_2^\nu = \frac{\lambda_1 p - q}{\lambda_1 - \lambda_2}, \tag{23}$$

if λ_1, λ_2 are in K we obtain (17) with

$$\psi(p,q) = \sum_{i\in I} a_i (\lambda_1 - \lambda_2)^{(c_1+c_2-n)/\nu} (q - \lambda_2 p)^{(n-i-c_1)/\nu} (\lambda_1 p - q)^{(i-c_2)/\nu}. \tag{24}$$

If $\lambda_1 \notin K$, then χ_1, χ_2 are conjugate over K by Lemma 14, and denoting conjugation by prime, from (14) and (21) we obtain

$$0 = f'(x,y) - f(x,y) = \sum_{i=0}^n a_i' \chi_2^{n-i}\chi_1^i - \sum_{i=0}^n a_i \chi_1^{n-i}\chi_2^i = \sum_{i=0}^n (a_i' - a_{n-i})\,\chi_1^{n-i}\chi_2^i,$$

hence $a_i' = a_{n-i}$ for all $i \leq n$. It follows that i and $n - i$ belong simultaneously to I, thus $c_1 = c_2$. Now, the form $\psi(p,q)$ given by (24) satisfies

$$\begin{aligned}\psi'(p,q) - \psi(p,q) &= \sum_{i\in I} a_i' (\lambda_2 - \lambda_1)^{(2c_1-n)/\nu} (q - \lambda_1 p)^{(n-i-c_1)/\nu} (\lambda_2 p - q)^{(i-c_1)/\nu} \\ &\quad - \sum_{i\in I} a_i (\lambda_1 - \lambda_2)^{(2c_1-n)/\nu} (q - \lambda_2 p)^{(n-i-c_1)/\nu} (\lambda_1 p - q)^{(i-c_1)/\nu} \\ &= \sum_{i\in I} a_{n-i} (\lambda_2 - \lambda_1)^{(2c_1-n)/\nu} (q - \lambda_1 p)^{(n-i-c_1)/\nu} (\lambda_2 p - q)^{(i-c_1)/\nu} \\ &\quad - \sum_{i\in I} a_{n-i} (\lambda_1 - \lambda_2)^{(2c_1-n)/\nu} (q - \lambda_2 p)^{(i-c_1)/\nu} (\lambda_1 p - q)^{(n-i-c_1)/\nu} = 0\end{aligned}$$

and since the extension $K(\lambda_1, \lambda_2)/K$ is separable, we get $\psi \in K[x,y]$ and from (21) and (23) we again obtain (17).

Assume now that (14) holds. Since, by Lemma 15, χ_1, χ_2 are linearly independent over $\overline{K}$, we have

$$f(x,y) = g(\chi_1, \chi_2), \qquad g \in K(\lambda)[x,y].$$

By (16) and Lemma 15,

$$\begin{aligned}(\lambda\chi_1, \lambda\chi_2 + \chi_1) &= g(\chi_1(\alpha x + \beta y, \gamma x + \delta y), \chi_2(\alpha x + \beta y, \gamma x + \delta y)) \\ &= f(\alpha x + \beta y, \gamma x + \delta y) = rf(x,y) = rg(\chi_1, \chi_2),\end{aligned}$$

hence $G(x) = g(1, x)$ satisfies

$$G(x + \lambda^{-1}) = rG(x)$$

and, by Lemma 16, we have either $G \in K$, or $\pi \neq 0$ and

$$G(x) = H(\lambda^{\pi-1}x^\pi - x), \quad H \in K(\lambda)[x].$$

In the former case we have (18) with

$$\begin{aligned}
&\psi(p,q) = 1, && c_1 = n && \text{if } \pi = 0,\\
&\psi(p,q) = p^{\lfloor n/\pi \rfloor}, && c_1 = n - \pi\left\lfloor \frac{n}{\pi} \right\rfloor && \text{if } \pi > 0,\ \lambda \in K,\\
&\psi(p,q) = p^{n/2}, && c_1 = 0 && \text{if } \pi = 2,\ \lambda \notin K.
\end{aligned}$$

In the latter case we have for $n \equiv c_1 \bmod \pi$, $0 \leq c_1 < \pi$,

$$g(\chi_1, \chi_2) = \chi_1^n G\left(\frac{\chi_2}{\chi_1}\right) = \chi_1^n H\left(\lambda^{\pi-1}\left(\frac{\chi_2}{\chi_1}\right)^\pi - \frac{\chi_2}{\chi_1}\right),$$

thus (18) holds with

$$\psi(p,q) = p^{(n-c_1)/\pi} H(q/p).$$

If $\lambda \in K$, then clearly $\psi \in K[p,q]$.

It remains to consider the case $\pi = 2$, $\lambda \notin K$. Let

$$\psi(p,q) = p^m \psi_1(p,q), \quad \text{where } \psi_1(0,1) \neq 0 \tag{25}$$

($m = (n - c_1 - \deg g)/2$), so that

$$(\psi_1(\chi_1^2, \lambda\chi_2^2 - \chi_2\chi_1), \chi_1) = 1. \tag{26}$$

By (18) we have $\chi_1^{2m+c_1} \mid f$, $(\chi_1^2)^{2m+c_1} \mid f^2$, and since χ_1^2 is irreducible over K, also $(\chi_1^2)^{m+\lceil c_1/2 \rceil} \mid f$. By (18), (25) and (26) this gives

$$2m + 2\lceil c_1/2 \rceil = 2m + c_1,$$

hence $c_1 = 0$, $\psi(\chi_1^2, \lambda\chi_2^2 - \chi_2\chi_1) = f \in K[x,y]$ and since

$$\chi_1^2 = \gamma^2 x^2 + \beta\gamma y^2 \in K[x,y], \quad \lambda\chi_2^2 - \chi_1\chi_2 = \gamma xy + \alpha y^2 \in K[x,y] \tag{27}$$

and $\chi_1^2, \lambda\chi_2^2 - \chi_1\chi_2$ are algebraically independent over K, it follows that $\psi \in K[p,q]$.

Sufficiency. If (13) holds and T is of order ν in $\mathrm{PGL}_2(K)$, then we have $\lambda_1^\nu = \lambda_2^\nu$, hence $\chi_i(\alpha x + \beta y, \gamma x + \delta y)^\nu = \lambda_1^\nu \chi_i^\nu$ and, by (17),

$$f(\alpha x + \beta y, \gamma x + \delta y) = \lambda_1^{c_1}\lambda_2^{c_2}\lambda_1^{\nu \deg \psi} f,$$

thus (16) holds. Also, if $\lambda_1, \lambda_2 \in K$, then (15) holds. If λ_1, λ_2 are conjugate over K, then (15) holds again by the condition $c_1 = c_2$, since $\chi_1\chi_2$, $\chi_1^\nu + \chi_2^\nu$ and $\lambda_1\chi_1^\nu + \lambda_2\chi_2^\nu$ are invariant under conjugation.

If (14) holds and $\pi = 0$, then, by (18), $f(\alpha x + \beta y, \gamma x + \delta y) = \lambda^{c_1} f$, thus (16) holds. Also (15) holds, since in this case $\lambda \in K$. If $\pi > 0$, then by (18) and Lemma 15,

$$\begin{aligned}
&f(\alpha x + \beta y, \gamma x + \delta y)\\
&\quad = \lambda^{c_1}\chi_1^{c_1}\psi(\lambda^\pi\chi_1^\pi, \lambda^{\pi-1}(\lambda^\pi\chi_2^\pi + \chi_1^\pi) - (\lambda\chi_2 + \chi_1)\lambda^{\pi-1}\chi_1^{\pi-1}) = \lambda^{c_1 + \deg\psi} f,
\end{aligned}$$

thus (16) holds. Also if $\lambda \in K$, then (15) holds. If $\lambda \notin K$, then $\pi = 2$, $c_1 = 0$ and (15) follows from (27).

Proof of Corollary 1. If $T = \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)K^* \in \mathrm{Aut}(f,K)$ of order $\nu > 1$ in $\mathrm{PGL}_2(K)$ satisfies (13), then, by Lemma 1, $\zeta + \zeta^{-1} \in K$, where $\zeta = \lambda_2/\lambda_1$ is a primitive root of unity of order ν in $\overline{K}$. If $n \equiv 0 \bmod \nu$ the first term of the alternative holds. By Theorem 1 we have $n \equiv c_1 + c_2 \bmod \nu$, thus $n \not\equiv 0 \bmod \nu$ implies $c_i := \max\{c_1, c_2\} > 0$. If $\chi_i \in K[x,y]$ we take $g = \chi_i$, and if χ_1, χ_2 are conjugate over K, we take $g = \chi_1\chi_2$.

If T satisfies (14), then either $\pi = 0$ and $f = \chi_1^{c_1}$, in which case we take $g = \chi_1$, or $\pi > 0$, in which case we have $n \equiv c_1 \bmod \pi$. By assumption, $n \not\equiv 0 \bmod \pi$, thus $c_1 > 0$, $\pi \neq 2$ and we take $g = \chi_1$.

Proof of Corollary 2. Let $T_0(x,y) = (\alpha x + \beta y, \gamma x + \delta y)$, $T = \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)K^* \in \mathrm{Aut}(f,K)$ be of order $\nu > 1$ in $\mathrm{PGL}_2(K)$, and L be a linear factor of f in $K[x]$ such that f/L is irreducible over K. Since $L(T_0) \mid f(T_0) \mid f$ and f/L is of degree $n-1 > 1$ we have $L(T_0)/L \in K^*$, hence (cf. Lemmas 14 and 15)

$$L = a\chi_i, \quad a \in K^*, \quad \text{where } i = 1 \text{ or } 2 \text{ in case (13)}, \ i = 1 \text{ in case (14)}. \tag{28}$$

In case (13) it follows that $\lambda_1, \lambda_2 \in K$, thus a primitive root of unity $\zeta_\nu = \lambda_2/\lambda_1$ is in K. Now (17) implies that either $c_i = 1$ and $c_{3-i} = 0$, in which case $\nu \mid n-1$, or $c_i = c_{3-i} = 0$ and

$$\chi_i \mid \psi(\chi_1^\nu + \chi_2^\nu, \lambda_1\chi_1^\nu + \lambda_2\chi_2^\nu).$$

This gives

$$\chi_i \mid \psi(\chi_{3-i}^\nu, \lambda_{3-i}\chi_{3-i}^\nu) = \chi_{3-i}^{\nu \deg \psi}\psi(1, \lambda_{3-i}),$$

hence $\psi(1, \lambda_{3-i}) = 0$,

$$\psi = (\lambda_{3-i}p - q)\psi_1, \quad \psi_1 \in K[p,q],$$

and

$$f/\chi_i = (\lambda_{3-i} - \lambda_i)\chi_i^{\nu-1}\psi_1(\chi_1^\nu + \chi_2^\nu, \lambda_1\chi_1^\nu + \lambda_2\chi_2^\nu)$$

is reducible for $n > 2$, contrary to assumption.

In case (14) it follows from (28) that $\lambda \in K$ and, by (18), we have $\pi > 0$. If $c_1 = 1$ we have $n \equiv 1 \bmod \pi$, contrary to assumption, while if $c_1 = 0$,

$$\chi_1 \mid \psi(\chi_1^\pi, \lambda^{\pi-1}\chi_2^\pi - \chi_2\chi_1^{\pi-1}).$$

This gives

$$\chi_1 \mid \psi(0, \lambda^{\pi-1}\chi_2^\pi) = (\lambda^{\pi-1}\chi_2^\pi)^{\deg\psi}\psi(0,1),$$

hence $\psi(0,1) = 0$, $\psi = p\psi_1$, $\psi_1 \in K[p,q]$ and

$$f/\chi_1 = \chi_1^{\pi-1}\psi_1(\chi_1^\pi, \lambda^{\pi-1}\chi_2^\pi - \chi_2\chi_1^{\pi-1})$$

is reducible for $n > 2$, contrary to assumption.

Proof of Corollary 3. If $\pi = 3$ the conclusion holds trivially. If $\pi \neq 3$ then by Theorem 1,

$$f = \chi_1^{c_1}\chi_2^{c_2}\psi(\chi_1^3 + \chi_2^3, \lambda_1\chi_1^3 + \lambda_2\chi_2^3),$$

where χ_1, χ_2 are given in Definition 3, c_1, c_2 are non-negative integers and ψ is a binary form over K. If $\sqrt{-3} \notin K$, then $\chi_i \notin K[x,y]$, by Lemma 14; hence, by Theorem 1, $c_1 = c_2$ and the above equation for f gives $4 \equiv 2c_1 \bmod 3$. It follows that $c_1 = c_2 = 2$, $\psi \in K^*$ and f is a square in $\overline{K}[x,y]$.

Proof of Corollary 4. For $T_0 = (\alpha x + \beta y, \gamma x + \delta y)$ we take

$$c(T_0) = \begin{cases} \lambda_1^{o(T)} = \lambda_2^{o(T)} & \text{if (13) holds,} \\ \lambda^{o(T)} & \text{if (14) holds.} \end{cases}$$

If $T_0 K^* \in \mathrm{Aut}(f, K)$ we have, by Theorem 1, for the case (13),

$$f(T_0)^{o(T)} = \lambda_1^{c_1 o(T)} \lambda_2^{c_2 o(T)} c(T_0)^{\deg \psi \cdot o(T)} f = c(T_0)^{c_1 + c_2 + \deg \psi \cdot o(T)} f = c(T_0)^{\deg f} f;$$

and for the case (14),

$$f(T_0)^{o(T)} = \lambda^{c_1 o(T)} c(T_0)^{\deg \psi \cdot o(T)} f = c(T_0)^{c_1 + \deg \psi \cdot o(T)} f = c(T_0)^{\deg f} f.$$

If, moreover, $f(\xi, 1) = 0$ implies $T^* \xi \neq \xi$, then $c_1 = c_2 = 0$ if (13) holds, and $c_1 = 0$ if (14) holds, hence

$$\deg f = \deg \psi \cdot o(T) \quad \text{and} \quad f(T_0) = c(T_0)^{\deg \psi} f = c(T_0)^{\deg f / o(T)} f.$$

Proof of Corollary 5. It suffices to apply Theorem 1 with K replaced by $\overline{K}$ and T replaced by $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \overline{K}^*$.

DEFINITION 5. Let $\mathcal{G}$ be a finite subgroup of $\mathrm{PGL}_2(K)$ which is not a π-group, and let, in the notation of Lemma 6,

$$\chi_{j0} = \prod_{\eta \in O_j \setminus \{\infty\}} (x - \eta y) \prod_{\eta \in O_j \cap \{\infty\}} y, \quad \chi_j = \chi_{j0}^{[K_j : K]_i} \quad (1 \leq j \leq h).$$

Further, if (2) holds, set

$$p = \chi_1^{|\mathcal{G}|/\deg \chi_1}, \quad q = \chi_2^{|\mathcal{G}|/\deg \chi_2};$$

and if (3) holds and $K_1 = K(\vartheta)$, set

$$p = \chi_1^{|\mathcal{G}|/\deg \chi_1} + \chi_2^{|\mathcal{G}|/\deg \chi_2}, \quad q = \vartheta \chi_1^{|\mathcal{G}|/\deg \chi_1} + \sigma_1(\vartheta) \chi_2^{|\mathcal{G}|/\deg \chi_2}.$$

COROLLARY 6. *Either $\chi_j \in K[x, y]$ for all $j \leq h$, or χ_1, χ_2 are conjugate over K and for $h = 3$, $\chi_3 \in K[x, y]$. Moreover $\mathcal{G} \subset \mathrm{Aut}(\chi_j, K)$ for all $j \leq h$.*

Proof. This is an immediate consequence of Lemma 6.

COROLLARY 7. *We have $p, q \in K[x, y]$ and $(p, q) = 1$.*

Proof. First, p and q are forms over $\overline{K}$. If (3) holds, or (2) holds and $[K_1 : K]_i = [K_2 : K]_i = 1$, this is clear, since $\deg \chi_j = |O_j|$ divides $|\mathcal{G}|$ for all $j \leq h$. If (2) holds and $[K_j : K]_i = 2$, then for each $S \in \mathcal{G} \setminus \{E\}$ and $\xi \in O_j$ with $S^* \xi = \xi$ we have $o(S) \equiv 0 \bmod 2$, hence $2 | O_j | \, | \, | \mathcal{G} |$ by Lemma 5.

Now, if (2) holds we have $\chi_j \in K[x, y]$ $(1 \leq j \leq h)$, hence $p, q \in K[x, y]$. If (3) holds, then $\chi_2 = \sigma_1(\chi_1)$, hence $\sigma_1(p) = p$, $\sigma_1(q) = q$, thus $p, q \in K[x, y]$. Since $(\chi_1, \chi_2) = 1$ we have $(p, q) = 1$.

THEOREM 2. *Let $\mathcal{G}$ be a finite subgroup of $\mathrm{PGL}_2(K)$ which is not a π-group. A form $f \in \overline{K}[x, y] \setminus \{0\}$ satisfies*

$$f \in K[x, y] \tag{29}$$

and

$$\mathcal{G} \subset \mathrm{Aut}(f, K) \tag{30}$$

if and only if

$$f = \prod_{j=1}^{h} \chi_j^{c_j} \psi(p,q), \tag{31}$$

where χ_j *and* p, q *are given in Definition* 5, ψ *is a binary form over* K *and* c_j *are integers satisfying* $0 \le c_j < |\mathcal{G}|/\deg \chi_j$ *and* $c_1 = c_2$ *if* χ_1, χ_2 *are conjugate over* K.

COROLLARY 8. *Under the assumption of Theorem* 2 *about* $\mathcal{G}$, *a form* $f \in \overline{K}[x,y]$ *satisfies* (30) *if and only if* (31) *holds, where* χ_j *are given in Definition* 5,

$$p = \chi_1^{|\mathcal{G}|/\deg \chi_1}, \qquad q = \chi_2^{|\mathcal{G}|/\deg \chi_2},$$

ψ *is a binary form over* $\overline{K}$ *and* c_j *are integers satisfying* $0 \le c_j < |\mathcal{G}|/\deg \chi_j$.

The proof of Theorem 2 is based on five lemmas.

LEMMA 17. *Let* $f \in \overline{K}[x,y] \setminus \{0\}$ *be a form and, for* $\xi \in \overline{K}$, $e_f(\xi)$ *be the multiplicity of* ξ *as a zero of* $f(x,1)$, *and* $e_f(\infty)$ *be the multiplicity of* 0 *as a zero of* $f(1,y)$. *We have*

$$S \in \mathrm{Aut}(f,K) \tag{32}$$

if and only if for all $\xi \in \overline{K} \cup \{\infty\}$,

$$e_f(S^*\xi) = e_f(\xi). \tag{33}$$

Proof. By making a preliminary linear transformation we may assume that

$$f = \prod_{i=1}^{n} (x - \xi_i y) \quad \text{and} \quad S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} K^*,$$

where

$$\alpha\delta - \beta\gamma \neq 0. \tag{34}$$

Necessity. If (32) holds and for some ξ_i we have $\gamma\xi_i + \delta = 0$, then with an $r \in K^*$,

$$(\alpha\xi_i + \beta)^n = f(\alpha\xi_i + \beta, \gamma\xi_i + \delta) = r f(\xi_i, 1) = 0,$$

hence $\alpha\xi_i + \beta = 0$ and $\alpha\delta - \beta\gamma = 0$, contrary to (34). Thus $\gamma\xi_i + \delta \neq 0$ $(i = 1, \dots, n)$ and

$$\begin{aligned} \prod_{i=1}^{n} \left(\alpha x + \beta y - \frac{\alpha\xi_i + \beta}{\gamma\xi_i + \delta} (\gamma x + \delta y) \right) &= \frac{(\alpha\delta - \beta\gamma)^n}{(-1)^n f(-\delta, \gamma)} \prod_{i=1}^{n} (x - \xi_i y) \\ &= \frac{(\beta\gamma - \alpha\delta)^n}{f(-\delta, \gamma)} f(x,y) = \frac{(\beta\gamma - \alpha\delta)^n}{r f(-\delta, \gamma)} f(\alpha x + \beta y, \gamma x + \delta y) \\ &= \frac{(\beta\gamma - \alpha\delta)^n}{r f(-\delta, \gamma)} \prod_{i=1}^{n} (\alpha x + \beta y - \xi_i(\gamma x + \delta y)), \end{aligned}$$

hence (33) holds.

Sufficiency. If (33) holds, there is a permutation σ of $\{1, \dots, n\}$ such that

$$\frac{\alpha\xi_i + \beta}{\gamma\xi_i + \delta} = \xi_{\sigma(i)}.$$

Then by (34) we have $\gamma\xi_i + \delta \neq 0$ for all $i \leq n$ and it follows that

$$\begin{aligned} f(\alpha x + \beta y, \gamma x + \delta y) &= \prod_{i=1}^{n} (\alpha x + \beta y - \xi_{\sigma(i)}(\gamma x + \delta y)) \\ &= \prod \left(\alpha x + \beta y - \frac{\alpha\xi_i + \beta}{\gamma\xi_i - \delta} (\gamma x + \delta y) \right) \\ &= \frac{(\alpha\delta - \beta\gamma)^n}{(-1)^n f(-\delta, \gamma)} \prod_{i=1}^{n} (x - \xi_1 y) = \frac{(\beta\gamma - \alpha\delta)^n}{f(-\delta, \gamma)} f(x, y), \end{aligned}$$

hence (32) holds.

LEMMA 18. *If $e_f(\eta) = 0$ for all $\eta \in O(\mathcal{G})$ and $\mathcal{G} \subset \mathrm{Aut}(f, K)$, then*

$$\deg f \equiv 0 \bmod |\mathcal{G}|.$$

Proof. Let us divide all $\xi \in \overline{K} \cup \{\infty\}$ with $e_f(\xi) > 0$ into classes by assigning ξ_1 and ξ_2 to the same class C if $\xi_1 = S^*\xi_2$ for some $S \in \mathcal{G}$. Since $e_f(\eta) = 0$ for all $\eta \in O(\mathcal{G})$, we have $\xi \neq S^*\xi$ for all ξ with $e_f(\xi) > 0$, hence by Lemma 17, the number of elements in each class is $|\mathcal{G}|$. On the other hand, by Lemma 17, for each C in the set Γ of all classes, there is $e(C) \in \mathbb{N}$ such that $e_f(\xi) = e(C)$ for all $\xi \in C$. We obtain

$$\deg f = \sum_{\xi \in \overline{K} \cup \{\infty\}} e_f(\xi) = \sum_{C \in \Gamma} e(C)|\mathcal{G}| \equiv 0 \bmod |\mathcal{G}|.$$

LEMMA 19. *If $f \in K[x, y] \setminus \{0\}$, $\mathcal{G} \subset \mathrm{Aut}(f, K)$ and $(\chi_j, f) \neq 1$ then $\chi_j \mid f$.*

Proof. Assume that $e_f(\eta) > 0$ for some $\eta \in O_j$. By Lemma 17 we have $e_f(S^*\eta) > 0$ for all $S \in \mathcal{G}$, hence $\chi_{j0} \mid f$. Therefore,

$$\chi_j \mid f^{[K_j : K]_i}. \tag{35}$$

If $[K_j : K]_i = 1$ the assertion is proved. If $[K_j : K]_i = 2$, then $O_j \subset K_j \setminus K$. Therefore, for all $\eta \in O_j$, $(x - \eta y)^2$ is irreducible over K and (35) implies

$$(x - \eta)^2 \mid f,$$

which gives $\chi_j \mid f$, as asserted.

REMARK. For $K = \mathbb{C}$ the lemma is well known (see [27, Vol. II, §70]) and for $\pi \neq 2$ the proof given there needs no modification.

LEMMA 20. *The field $L = \{\varphi \in K(t) : \varphi(S^*) = \varphi \text{ for all } S \in \mathcal{G}\}$ is generated by $p(t, 1)/q(t, 1)$, where p, q are given in Definition 5.*

Proof. By Definition 5, $\mathcal{G} \subset \mathrm{Aut}(\chi_{j0}, K)$, hence, by Corollary 3, for every $S_0 \in \mathrm{GL}_2(K)$ with $S = S_0K^* \in \mathcal{G}$ we have

$$\chi_{j0}(S_0)^{o(S)} = c(S_0)^{\deg \chi_{j0}} \chi_{j0}.$$

If $S^*\xi = \xi$ for some $\xi \in O_j$, we have, by Lemma 5,

$$o(S) \,|\, |\mathcal{G}|/|O_j| = |\mathcal{G}|/\deg \chi_{j0},$$

and so

$$\chi_j(S_0)^{|\mathcal{G}|/\deg \chi_j} = \chi_{j0}(S_0)^{|\mathcal{G}|/\deg \chi_{j0}} = c(S_0)^{|\mathcal{G}|/o(S)} \chi_j^{|\mathcal{G}|/\deg \chi_j}. \tag{36}$$

If $S_0^*\xi \neq \xi$ for all $\xi = O_j$ the same conclusion holds by the second part of Corollary 4. Therefore,

$$p(S_0) = c(S_0)^{|\mathcal{G}|/o(S)}p, \quad q(S_0) = c(S_0)^{|\mathcal{G}|/o(S)}q \tag{37}$$

and

$$\frac{p(S_0^*t,1)}{q(S_0^*t,1)} = \frac{p(t,1)}{q(t,1)}, \quad \text{thus} \quad \frac{p(t,1)}{q(t,1)} \in L.$$

Since $(\chi_1,\chi_2)=1$ we have $p(t,1)/q(t,1) \notin K$ and, by Lüroth's theorem, $L = K(r)$, where $r \in K(t) \setminus K$. Without loss of generality we may assume that $r = p_1/q_1$, where p_1 and q_1 are coprime polynomials of the same degree d. Let

$$p_2 = p_1(x/y)y^d, \quad q_2 = q_1(x/y)y^d.$$

Since $r(S^*t) = r(t)$ for all $S \in \mathcal{G}$ we have, for all $S_0 \in \mathrm{GL}_2(K)$ with $S_0K^* \in \mathcal{G}$,

$$p_2(S_0) = c_1(S_0)p_2, \quad q_2(S_0) = c_1(S_0)q_2,$$

where $c_1(S_0) \in K^*$. It follows that

$$\lambda p_2(S_0) + \mu q_2(S_0) = c_1(S_0)(\lambda p_2 + \mu q_2) \tag{38}$$

for all λ, μ in $\overline{K}$. Now, choose λ_0 and μ_0 in $\overline{K}$ such that

$$\begin{aligned} &\lambda_0 p_2(\eta,1) + \mu_0 q_2(\eta,1) \neq 0 \quad \text{for all } \eta \in O(\mathcal{G}) \setminus \{\infty\}, \\ &\lambda_0 p_2(1,0) + \mu_0 q_2(1,0) \neq 0 \quad \text{if } \infty \in O(\mathcal{G}). \end{aligned} \tag{39}$$

This is possible, since $\langle p_2(\eta,1), q_2(\eta,1)\rangle \neq \langle 0,0\rangle$ and $p(1,0) \neq 0$. By Lemma 18 we have

$$d \equiv 0 \bmod |\mathcal{G}|.$$

On the other hand, since $p(t,1)/q(t,1) \in K(r)$ we have

$$|\mathcal{G}| = \deg p(t,1)/q(t,1) \equiv 0 \bmod d.$$

It follows that $d = \deg p(t,1)/q(t,1)$ and $K(p(t,1)/q(t,1)) = K(r) = L$.

LEMMA 21. *If f_1 is a binary form over K of degree divisible by $|\mathcal{G}|$ and for every $S_0 \in \mathrm{GL}_2(K)$ with $S = S_0K^* \in \mathcal{G}$ we have*

$$f_1(S_0) = c(S_0)^{\deg f_1/o(S)}f_1,$$

then $f_1 = \psi_1(p,q)$, where p, q are given in Definition 5 and ψ_1 is a binary form over K.

Proof. By (37) for every S_0 in question

$$q(S_0)^{\deg f_1/|\mathcal{G}|} = c(S_0)^{\deg f_1/|\mathcal{G}|}q^{\deg f_1/|\mathcal{G}|},$$

hence

$$\frac{f_1(S^*t,1)}{q(S^*t,1)^{\deg f_1/|\mathcal{G}|}} = \frac{f_1(t,1)}{q(t,1)^{\deg f_1/|\mathcal{G}|}},$$

and since this holds for every $S \in \mathcal{G}$,

$$\frac{f_1(t,1)}{q(t,1)^{\deg f_1/|\mathcal{G}|}} \in L.$$

By Lemma 20 we have

$$\frac{f_1(t,1)}{q(t,1)^{\deg f_1/|\mathcal{G}|}} = u\left(\frac{p(t,1)}{q(t,1)}\right).$$

Let $u = v/w$, where v, w are coprime polynomials over K. Putting $v(x,y) = v(x/y)y^{\deg v}$ and $w(x,y) = w(x/y)y^{\deg w}$, we obtain

$$\frac{f_1(t,1)}{q(t,1)^{\deg f_1/|\mathcal{G}|}} = \frac{v(p(t,1),\, q(t,1))q(t,1)^{\deg w}}{w(p(t,1),\, q(t,1))q(t,1)^{\deg v}}.$$

Since $(p(t,1),\, q(t,1)) = 1$ by Corollary 7, we have

$$(w(p(t,1),q(t,1)),\, v(p(t,1),q(t,1))) = 1$$

and

$$(v(p(t,1),q(t,1))w(p(t,1),q(t,1)),q(t,1)) = 1,$$

hence $w \in K^*$ and $\deg f_1/|\mathcal{G}| \geq \deg v$, and

$$f_1(t,1) = w^{-1}v(p(t,1),\, q(t,1))q^{\deg f_1/|\mathcal{G}|-\deg v}.$$

Substituting $t = x/y$ and cancelling the denominators we obtain

$$f_1 = w^{-1}v(p,q)q^{\deg f_1/|\mathcal{G}|-\deg v}.$$

Proof of Theorem 2. Necessity. By Lemma 19 we may write

$$f = \prod_{j=1}^{h} \chi_j^{c_j} f_0, \quad \text{where} \quad f_0 \in \overline{K}[x,y], \ \Big(f_0, \prod_{j=1}^{h} \chi_j\Big) = 1. \tag{40}$$

If $\chi_1 \notin K[x,y]$, then by Corollary 6, χ_1, χ_2 are conjugate and $\chi_1^{c_1} \mid f$ implies $\chi_2^{c_1} \mid f$, hence $c_1 \leq c_2$. Similarly $c_2 \leq c_1$, hence $c_1 = c_2$ as asserted and $f_0 \in K[x,y]$. Now,

$$e_{f_0}(\eta) = 0 \quad \text{for all } \eta \in O(\mathcal{G})$$

and by Lemma 18,

$$\deg f_0 \equiv 0 \bmod |\mathcal{G}|.$$

Moreover, by Corollary 4, for every $S_0 \in \mathrm{GL}_2(K)$ with $S = S_0K^* \in \mathcal{G}$ we have

$$f_0(S_0) = c(S_0)^{\deg f_0/o(S)} f_0.$$

By Lemma 21 with $f_1 = f_0$,

$$f_0 = \psi(p,q),$$

where ψ is a binary form over K, thus (31) follows from (40).

Now, by (36) for each $j \leq k$ and every $S_0 \in \mathrm{GL}_2(K)$ with $S_0K^* \in \mathcal{G}$,

$$\chi_j^{|\mathcal{G}|/\deg \chi_j}(S_0) = c(S_0)^{|\mathcal{G}|/o(S)} \chi_j^{|\mathcal{G}|/\deg \chi_j},$$

hence, applying Lemma 21 with $f_1 = \chi_j^{|\mathcal{G}|/\deg \chi_j}$ if $\chi_j \in K[x,y]$, or with $f_1 = (\chi_1\chi_2)^{n|\mathcal{G}|/\deg \chi_j}$ if χ_1, χ_2 are conjugate, we obtain

$$\chi_j^{|\mathcal{G}|/\deg \chi_j} = \psi_j(p,q) \quad \text{or} \quad (\chi_1\chi_2)^{|\mathcal{G}|/\deg \chi_j} = \psi_1(p,q),$$

respectively, where ψ_j are binary forms over K. This gives the required upper bound for c_j.

Sufficiency. Assuming (31) we obtain (29) by Corollary 6 and the condition $c_1 = c_2$ if χ_1, χ_2 are conjugate over K. On the other hand, for every $S_0 \in \mathrm{GL}_2(K)$ such that $S = S_0 K^* \in \mathcal{G}$ we have, by (31),

$$\psi(p(S_0),\, q(S_0)) = c(S_0)^{|\mathcal{G}|/o(S)}\psi(p,q),$$

thus $\mathcal{G} \subset \mathrm{Aut}(\psi(p,q), K)$ and (30) follows from (31) by Corollary 6.

Proof of Corollary 8. It suffices to apply Theorem 2 with K replaced by $\overline{K}$ and $\mathcal{G}$ replaced by $\mathcal{G}\overline{K}^*/\overline{K}^*$.

Example. We give without proof formulae for χ_1, χ_2, χ_3 for dihedral subgroups of $\mathrm{PGL}_2(K)$. For the dihedral subgroup of order 4 generated by

$$\begin{pmatrix} a & b \\ c & -a \end{pmatrix} K^*, \begin{pmatrix} d & e \\ f & -d \end{pmatrix} K^*, \quad \text{where} \quad a, \ldots, f \in K,\ (a^2+bc)(d^2+ef) \neq 0,\ 2ad+bf+ce = 0$$

(the last condition ensures commutativity) we have

$$\chi_1 = cx^2 - 2axy - by^2, \quad \chi_2 = fx^2 - 2dxy - ey^2,$$

$$\chi_3 = (cd-af)x^2 - 2(ad+bf)xy - (bd-ae)y^2.$$

For the dihedral group of order $2\nu > 4$ generated by

$$\begin{pmatrix} a & b \\ a(\zeta+\zeta^{-1})+b & -a \end{pmatrix} K^* \quad \text{and} \quad \begin{pmatrix} 1+\zeta+\zeta^{-1} & -1 \\ 1 & 1 \end{pmatrix} K^*,$$

where ζ is a primitive root of unity of order $\nu \not\equiv 0 \bmod \pi$, $a, b \in K$, $(a\zeta+b)(a\zeta^{-1}+b) \neq 0$, the polynomials χ_i $(1 \leq i \leq 3)$ are given by the formulae

$$\chi_3 = x^2 - (\zeta+\zeta^{-1})xy + y^2,$$

$$\chi_{(3-\varepsilon)/2} = \frac{B-A}{\zeta^{-1}-\zeta}\left(\zeta^{-1}(x-\zeta y)^\nu + \zeta(x-\zeta^{-1}y)^\nu\right) + \left(\varepsilon\sqrt{AB} - \frac{\zeta B - \zeta^{-1}A}{\zeta^{-1}-\zeta}\right)\left((x-\zeta y)^\nu + (x-\zeta^{-1})^\nu\right) \quad (\varepsilon = \pm 1)$$

if

$$A = (-a\zeta^2 - b\zeta)^\nu \neq B = (-a\zeta^{-2} - b\zeta^{-1})^\nu,$$

and

$$\chi_1 = (\zeta-\zeta^{-1})(x-\zeta y)^\nu + (\zeta^{-1}-\zeta)(x-\zeta^{-1}y)^\nu,$$
$$\chi_2 = (x-\zeta y)^\nu + (x-\zeta^{-1}y)^\nu,$$

otherwise. We shall use the fact, easy to check directly, that for $a = 1$, $b = 0$ the two generators of the group are weak automorphs of χ_i, hence $\mathrm{Aut}(\chi_i, K)$ contains the group for $i = 2$ or 3.

For the dihedral group generated by

$$\begin{pmatrix} -1 & b \\ 0 & 1 \end{pmatrix} K^* \quad \text{and} \quad \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} K^*,$$

where $\pi > 0$, $\lambda \in K^*$, $b \in K$, the polynomials χ_i $(1 \leq i \leq 2)$ are given by the formulae

$$\chi_1 = y, \quad \chi_2 = -2\lambda^{\pi-1}x^\pi + 2xy^{\pi-1} + (\lambda^{\pi-1}b^\pi - b)y^\pi.$$

DEFINITION 6. Let $\mathcal{G}$ be a π-subgroup of $\mathrm{PGL}_2(K)$ generated by elements S_iK^*, where

$$S_i = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} \lambda_i & 1 \\ 0 & \lambda_i \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad (1 \le i \le g), \tag{41}$$

$ad-bc \neq 0$, $\lambda_1^{-1}, \dots, \lambda_g^{-1}$ are linearly independent over $\mathbb{F}_\pi$ and either a, b, c, d, λ_j are in K, or $a = 0$, $b = 1$, $c \in K$, $K(d)$ is a quadratic inseparable extension of K and $d + \lambda_j \in K$. Then we put

$$\chi_1 = cx + dy, \quad \chi_2 = ax + by,$$
$$p = \chi_1^{\pi^g}, \quad q = \chi_2 \prod_{\langle a_1,\dots,a_g\rangle \in \mathbb{F}_\pi^g \setminus \{\mathbf{0}\}} \Big(\chi_1 + \chi_2\Big(\sum_{j=1}^g a_j \lambda_j^{-1}\Big)^{-1}\Big).$$

COROLLARY 9. *We have $p \in K[x,y]$, $q \in K[x,y]$, $(p,q) = 1$ and p, q are algebraically independent.*

Proof. The assertion is clear unless $\pi = 2$, $\lambda_1 \notin K$. In the exceptional case $c \in K$, $\lambda_1^2 \in K$, hence $p \in K[x,y]$. Also for each $j \le g$,

$$d\lambda_j^{-2} + \lambda_j^{-1} \in K,$$

hence for all $\langle a_1, \dots, a_g\rangle \in \mathbb{F}_2^g \setminus \{\mathbf{0}\}$,

$$d\Big(\sum_{j=1}^g a_j \lambda_j^{-1}\Big)^2 + \sum_{j=1}^g a_j \lambda_j^{-1} \in K,$$

which gives $\chi_1 + \chi_2(\sum_{j=1}^g a_j\lambda_j^{-1})^{-1} \in K[x,y]$ and $q \in K[x,y]$. Moreover, $(p,q) = 1$, since $(\chi_1, \chi_2) = 1$, and since p, q are forms, it follows that they are algebraically independent.

THEOREM 3. *Let $\mathcal{G}, \chi_1, p, q$ be as in Definition 6. A form $f \in \overline{K}[x,y] \setminus \{0\}$ satisfies (29) and (30) if and only if*

$$f = \chi_1^{c_1} \psi(p,q), \tag{42}$$

where ψ is a binary form over K, c_1 is an integer, $0 \le c_1 < |\mathcal{G}|$ and if $\chi_1 \notin K[x,y]$ then c_1 is even.

COROLLARY 10. *Under the assumption of Theorem 3 about $\mathcal{G}, \chi_1, p, q$ a form $f \in \overline{K}[x,y]$ satisfies (30) if and only if (42) holds, where ψ is a binary form over $\overline{K}$ and c_1, c_2 are integers with $0 \le c_1 < |\mathcal{G}|$.*

COROLLARY 11. *If a binary form f has at least two coprime linear factors over K and $\mathcal{G}$ is a π-group contained in $\mathrm{Aut}(f, K)$, then $|\mathcal{G}| \le \deg f$.*

The proof of Theorem 3 is based on the following lemma.

LEMMA 22. *If $\pi > 0$, $G \in K[x]$, $\lambda_i \in K(\lambda_1)^*$ $(1 \le i \le g)$, $\lambda_1^{-1}, \dots, \lambda_g^{-1}$ are linearly independent over $\mathbb{F}_\pi$ and*

$$G(x + \lambda_i^{-1}) = r_i G(x), \quad r_i \in K^* \ (1 \le i \le g), \tag{43}$$

then

$$G(x) = H(P(x)), \quad H \in K(\lambda_1)[x], \tag{44}$$

where

$$P(x) = \prod_{\langle a_1,\dots,a_g\rangle \in \mathbb{F}_\pi^g} \Big(x + \sum_{j=1}^{g} a_j \lambda_j^{-1}\Big).$$

REMARK. For K being a finite field of characteristic π and $\lambda_i \in K$ the lemma is due to Dickson.

Proof. On comparing the leading coefficients on both sides of (43) we obtain $r_i = 1$ $(1 \le i \le g)$. We shall prove (44) by induction on the degree of G, say n. If $n = 0$ then (44) holds with $H = G$. Assume that (44) is true for all G satisfying (43) of degree less than n, and that $\deg G = n$. From (43) we obtain, for all $\langle a_1, \dots, a_g\rangle \in \mathbb{F}_\pi^g$,

$$G\Big(-\sum_{j=1}^{g} a_j \lambda_j^{-1}\Big) = G(0),$$

hence by the linear independence of $\lambda_1^{-1}, \dots, \lambda_g^{-1}$ over $\mathbb{F}_\pi$,

$$P(x) \,|\, G(x) - G(0).$$

Taking

$$G_1(x) = \frac{G(x) - G(0)}{P(x)}$$

we deduce from (43) that $G_1(x + \lambda_i^{-1}) = G_1(x)$ $(1 \le i \le g)$, hence by the inductive assumption

$$G_1(x) = H_1\big(P(x)\big), \quad H_1 \in K(\lambda_1)[x],$$

and (44) holds with $H(x) = xH_1(x) + G(0)$.

Proof of Theorem 3. Necessity. Since $ad - bc \neq 0$ and χ_1, χ_2 are linearly independent over K, we have

$$f(x, y) = g(\chi_1, \chi_2), \quad g \in K(\lambda_1)[x, y].$$

By (41),

(45) $$\chi_1(S_i) = \lambda_i \chi_1, \quad \chi_2(S_i) = \lambda_i \chi_2 + \chi_1,$$

hence, by (30), for some $r_i \in K$,

$$g(\lambda_i\chi_1, \lambda_i\chi_2 + \chi_1) = g(\chi_1(S_i), \chi_2(S_i)) = f(S_i) = r_i f = r_i g(\chi_1, \chi_2),$$

thus $G(x) = g(1, x)$ satisfies

$$G(x + \lambda_i^{-1}) = r_i G(x).$$

By Lemma 22 we have

$$G(x) = H\big(P(x)\big), \quad H \in K(\lambda_1)[x].$$

Hence

$$g(\chi_1, \chi_2) = \chi_1^n G\Big(\frac{\chi_2}{\chi_1}\Big) = \chi_1^n H\Big(\frac{\chi_2}{\chi_1}\Big)$$

and for $n \equiv c_1 \bmod \pi^g$ with $0 \le c_1 < \pi^g$, (42) holds with

$$\psi(p, q) = p^{(n-c_1)/\pi^g} H\Big(\frac{q}{p} \prod_{\langle a_1,\dots,a_g\rangle \in \mathbb{F}_\pi^g \setminus \{\mathbf{0}\}} \sum_{j=1}^{g} a_j \lambda_j^{-1}\Big).$$

If $\lambda_1 \in K$ we have $\psi \in K[p, q]$.

It remains to consider the case $\pi = 2$, $K(\lambda_1)$ a quadratic inseparable extension of K. In this case $\chi_1 \notin K[x,y]$ and χ_1^2 is irreducible over K. Let $\psi(p,q) = p^m\psi_1$, where $\psi_1 \in K[p,q]$ and $\psi_1(0,1) \neq 0$. Since, by Corollary 9, $(p,q) = 1$ we have $(\psi_1(p,q), \chi_1) = 1$ and it follows from (42) that

$$\chi_1^{2^g m + c_1} \mid f, \quad \chi_1^{2^g m + c_1 + 1} \nmid f.$$

Further

$$\chi_1^{2^{g+1} m + 2c_1} \mid f^2$$

and since χ_1^2 is irreducible,

$$\chi_1^{2^g m + 2\lceil c_1/2 \rceil} \mid f, \quad 2^g m + 2\lceil c_1/2 \rceil = 2^g m + c_1,$$

$c_1 \equiv 0 \bmod 2$, and $\chi_1^{c_1} \in K[x,y]$. It now follows from (42) that

$$\psi(p,q) \in K[x,y].$$

By Corollary 9, $p, q \in K[x,y]$ and p, q are algebraically independent. Hence $\psi \in K[p,q]$.

Sufficiency. Since χ_1 or χ_1^2 in the exceptional case and p, q are defined over K, (29) is clear. On the other hand, by (45),

$$\begin{aligned}
p(S_i) &= \lambda_i^{\pi^g} p,\\
q(S_i) &= (\lambda_i\chi_2 + \chi_1) \prod_{\langle a_1,\dots,a_g\rangle \in \mathbb{F}_\pi^g \setminus \{\mathbf{0}\}} \Big(\lambda_i\chi_1 + (\lambda_i\chi_2 + \chi_1)\Big(\sum_{j=1}^g a_j\lambda_j^{-1}\Big)^{-1}\Big)\\
&= (\lambda_i\chi_2 + \chi_1)\lambda_i^{\pi^g - 1}\\
&\quad \times \prod_{\langle a_1,\dots,a_g\rangle \in \mathbb{F}_\pi^g \setminus \{\mathbf{0}\}} \Big(\sum_{j=1}^g a_j\lambda_j^{-1}\Big)^{-1} \prod_{\langle a_1,\dots,a_g\rangle \in \mathbb{F}_\pi^g \setminus \{\mathbf{0}\}} \Big(\chi_1 \sum_{j=1}^g a_j\lambda_j^{-1} + \chi_2 + \chi_1\lambda_i^{-1}\Big)\\
&= \lambda_i^{\pi^g} \prod_{\langle a_1,\dots,a_g\rangle \in \mathbb{F}_\pi^g \setminus \{\mathbf{0}\}} \Big(\sum_{j=1}^g a_j\lambda_j^{-1}\Big)^{-1} \prod_{\langle a_1,\dots,a_g\rangle \in \mathbb{F}_\pi^g} \Big(\chi_1 \sum_{j=1}^g a_j\lambda_j^{-1} + \chi_2\Big)\\
&= \lambda_i^{\pi^g} q,
\end{aligned}$$

hence

$$f(S_i) = \chi_1(S_i)^{c_1}\psi(p(S_i), q(S_i)) = \lambda_i^{c_1 + \pi^g \deg\psi}\chi_1^{c_1}\psi(p,q) = \lambda_i^{c_1 + \pi^g \deg\psi} f$$

and (30) holds.

Proof of Corollary 10. It suffices to apply Theorem 3 with K replaced by $\overline{K}$ and $\mathcal{G}$ replaced by $\mathcal{G}\overline{K}^*/\overline{K}^*$.

Proof of Corollary 11. Since $\mathrm{Aut}(f,K) \subset \mathrm{Aut}(f,\overline{K})$ we may assume that $K = \overline{K}$. By Lemma 3 every π-group contained in $\mathrm{PGL}_2(K)$ must contain a π-group considered in Theorem 3. Since f has at least two coprime linear factors, the case $\psi \in K$ in (42) is excluded. Hence

$$|\mathcal{G}| \leq \deg\psi(p,q) \leq n.$$

3. Upper bounds for $|\mathrm{Aut}(f,K)|$

We shall prove

THEOREM 4. *If a form $f \in \overline{K}[x,y] \setminus \{0\}$ of degree n has at least three coprime linear factors over $\overline{K}$, then $\mathrm{Aut}(f,K)$ is finite. Moreover, if*

$$f = cf_0(\alpha x+\beta y, \gamma x+\delta y)^k, \quad \text{where } c\in\overline{K}^*,\ \alpha,\beta,\gamma,\delta\in K,\ \alpha\delta-\beta\gamma\neq 0, \tag{46}$$

$f_0 = x^q y - xy^q$, $\mathbb{F}_q \subset K$, $k\in\mathbb{N}$, *then* $\mathrm{Aut}(f,K)\cong \mathrm{PGL}_2(\mathbb{F}_q)$; *otherwise either*

$$\pi = 2, \quad n = 2\varrho+1, \quad \mathrm{Aut}(f,K)\cong \mathfrak{D}_{2\varrho+1}, \tag{47}$$

or

$$\pi = 3, \quad n = 10, \quad \mathrm{Aut}(f,K)\cong \mathfrak{A}_5, \tag{48}$$

or

$$|\mathrm{Aut}(f,K)| = lm, \tag{49}$$

where $l\not\equiv 0 \bmod \pi$, $\zeta_l+\zeta_l^{-1}\in K$, $l<n$, $m\le n$.

REMARK. It is not clear whether there exist f and K satisfying (48).

COROLLARY 12. *Assume that $f\in K[x,y]$ and all factors of $f(x,1)$ irreducible over K are separable. Then $\mathrm{Aut}(f,K)$ is finite if and only if either K is finite, or f has at least three coprime linear factors over $\overline{K}$.*

DEFINITION 7. For $\pi = 0$ or $\pi > n$ we put

$$\begin{aligned}
&U_n(K) = \left\{\nu\in\mathbb{N} : \nu\le n \text{ and } \zeta_\nu+\zeta_\nu^{-1}\in K\right\},\\
&V_n(K) = \left\{\nu\in\mathbb{N} : \nu\le n \text{ and } \zeta_\nu\in K\right\},\\
&a_1(n,K) = \sup U_n(K), \quad a_2(n,K) = \sup\{\nu\in U_n(K) : \nu\equiv n \bmod 2\},\\
&b(n,K) = \sup V_n(K),\\
&\mathcal{M} = \{6,10,15,21,22\}\cup\{25,\ldots\}\setminus\{29,32,44\},
\end{aligned}$$

where the dots represent consecutive integers greater than 25.

COROLLARY 13. *We have $a_2(n,K)\le a_1(n,K)\le n$ for every n and $a_2(n,K) = a_1(n,K) = n$ for $n\le 4$, $a_1(n,K)\ge 6$ for $n\ge 6$, $a_2(n,K)\ge 6$ for even $n\ge 6$, $2\le b(n,K)\le a_1(n,K)$ for $n\ge 2$.*

DEFINITION 8. Let $A(n,K)$ and $B(n,K)$ for $n\ge 3$ be the maximum of $|\mathrm{Aut}(f,K)|$ over all forms f of degree n in $\overline{K}[x,y]$ or $K[x,y]$ respectively with at least three coprime linear factors over $\overline{K}$ and which are not perfect powers in $\overline{K}[x,y]$.

THEOREM 5. *We have*

$$A(n,K) = B(n,K) = \pi^{3g}-\pi^g \quad \text{if } n = \pi^g+1,\ \mathbb{F}_{\pi^g}\subset K,$$

and

$$A(n,K)\le n(n-1) \quad \text{otherwise.}$$

Moreover, if $\pi = 0$ *or* $\pi > n$ *then*

$$A(n,K) = \begin{cases} 12 \quad \textit{if } \operatorname{level} K \le 2,\ n = 4, \\ \max\{a_1(n,K), 2a_2(n,K), 24\} \textit{ if } \operatorname{level} K \le 2 \textit{ and either} \\ \qquad n = 6, 8, 14 \textit{ or } n = 12,\ \sqrt{5} \notin K \textit{ or} \\ \qquad n = 2m,\ m \ge 9 \textit{ and } \sqrt{5} \notin K \textit{ if } m \in \mathcal{M}, \\ \max\{a_1(n,K), 2a_2(n,K), 60\} \textit{ if } \operatorname{level} K \le 2, \sqrt{5} \in K \\ \qquad \textit{and } n/2 \in \mathcal{M}, \\ \max\{a_1(n,K), 2a_2(n,K)\} \textit{ otherwise}; \end{cases}$$

$$B(n,K) = \begin{cases} 12 \quad \textit{if } n = 4,\ \sqrt{-3} \in K, \\ \max\{b(n-1,K), 2a_2(n,K), 24\} \textit{ if level } K \le 2 \textit{ and either} \\ \qquad n = 6, 8, 14 \textit{ or } n = 12,\ \sqrt{5} \notin K \textit{ or} \\ \qquad n = 2m,\ m \ge 9 \textit{ and } \sqrt{5} \notin K \textit{ if } m \in \mathcal{M}, \\ \max\{b(n-1,K), 2a_2(n,K), 60\} \textit{ if level } K \le 2, \sqrt{5} \in K \\ \qquad \textit{and } n/2 \in \mathcal{M}, \\ \max\{b(n-1,K), 2a_2(n,K)\} \textit{ otherwise.} \end{cases}$$

COROLLARY 14. *We have* $A(n,\mathbb{C}) = 2n$ *unless* $n = 4, 6, 8, 12, 20$, *when* $A(n,\mathbb{C}) = 12, 24, 24, 60, 60$, *respectively.*

REMARK 1. P. Olver [19] and then I. Berchenko and P. Olver [1] gave a bound for $|\mathrm{Aut}(f,\mathbb{C})|$ assumed finite, which asserts that

$$A(n,\mathbb{C}) \le 6n - 12$$

and apart from an exceptional case

$$A(n,\mathbb{C}) \le 4n - 8.$$

The bound given in Corollary 14 is better for all $n > 4$, $n \ne 6, 8, 12$. This bound for $n > 30$ has been anticipated by Summerer in an unpublished paper [25], dealing only with non-singular forms.

REMARK 2. Let $A_0(n,\pi) = \max A(n,K)$, where K runs through all fields of characteristic π. By an analysis of subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$ listed in [12, Chapter 12] one can guess explicit values for $A_0(n,\pi)$ also for $0 < \pi \le n$. Namely, if $n > 20$ and $\pi^g \le n < \pi^{g+1}$, then conjecturally $A_0(\pi^g + 1, \pi) = \pi^{3g} - \pi^g$, otherwise $A_0(n,\pi) = \pi^{2g} - \pi^g$ unless $g = 1$, $(\pi^2 - \pi)/2 < n$, $n \not\equiv \bmod \pi$ or $n = \pi^2 - \pi$ or $g = 3$, $n = \pi^4 - \pi^2$, when $A_0(n,\pi) = 2n$ or $\pi^3 - \pi$ or $\pi^6 - \pi^2$, respectively. For $n \le 20$ there are apparently three exceptions to this rule: $A_0(8,5) = 24$, $A_0(12,7) = A_0(20,7) = 60$.

For the proof of Theorem 4 we need the following

DEFINITION 9. For $\xi \in \overline{K} \cup \{\infty\}$, we set

$$\mathrm{Aut}(f,K,\xi) = \{S \in \mathrm{Aut}(f,K) : S^*\xi = \xi\},$$

$$\mathrm{Aut}_\pi(f,K,\xi) = \begin{cases} \{S \in \mathrm{Aut}(f,K,\xi) : S^{*\pi} = E\} & \text{if } \pi > 0, \\ \{E\} & \text{otherwise.} \end{cases}$$

LEMMA 23. *Let $f \in \overline{K}[x,y]\setminus\{0\}$ be a form of degree n, let $Z = \{\xi \in \overline{K}\cup\{\infty\} : e_f(\xi) > 0\}$ and suppose $|Z| \geq 3$. For every $\xi \in Z$ the set $\mathrm{Aut}_\pi(f,K,\xi)$ is a finite normal subgroup of $\mathrm{Aut}(f,K,\xi)$ and the quotient group is cyclic of order $l < n$ with $l \not\equiv 0 \bmod \pi$ such that $\zeta_l \in K(\xi)$, where $K(\infty) = K$.*

Proof. Assume first $\xi = \infty$. Then $S^*\xi = \xi$ is equivalent to $S = \left(\begin{smallmatrix}\alpha & \beta\\ 0 & 1\end{smallmatrix}\right)K^*$, where $\alpha \in K^*$, $\beta \in K$. Let

$$\mathcal{H} = \left\{\alpha \in K^* : \text{there exists } \beta \in K \text{ such that } \begin{pmatrix}\alpha & \beta\\ 0 & 1\end{pmatrix} K^* \in \mathrm{Aut}(f,K)\right\}.$$

Then $\mathcal{H}$ is a subgroup of the multiplicative group K^* and if $\alpha\in\mathcal{H}$ and $S = \left(\begin{smallmatrix}\alpha & \beta\\ 0 & 1\end{smallmatrix}\right)K^* \in \mathrm{Aut}(f,K)$, then the order of α in K^* is finite. Indeed, otherwise, taking ξ_1, ξ_2 in $Z\setminus\{\infty\}$, $\xi_1 \neq \xi_2$, we should obtain, by Lemma 17,

$$S^{*i}\xi_j \in Z \quad \text{for all } i \in \mathbb{N} \text{ and } j = 1,2,$$

hence for some $i'_j < i''_j = i'_j + i_j$,

$$S^{*i'_j}\xi_j = S^{*i''_j}\xi_j \quad (j = 1,2);$$

$$\alpha^{i_j}\xi_j + \beta(\alpha^{i_j} - 1)/(\alpha - 1) = S^{*i_j}\xi_j = \xi_j;$$

$$(\alpha - 1)\xi_j + \beta = 0 \quad (j = 1,2), \quad \xi_1 = \xi_2, \quad \text{a contradiction.}$$

The above calculation also shows that if $\alpha \in \mathcal{H}\setminus\{1\}$ and $S = \left(\begin{smallmatrix}\alpha & \beta\\ 0 & 1\end{smallmatrix}\right)K^* \in \mathrm{Aut}(f,K)$, then the order of α in K^* is equal to the order ν of S in $\mathrm{PGL}_2(K)$ and is not divisible by π. Since $|Z| \geq 3$, in Theorem 1 applied to f, $\overline{K}$ and S the case $\psi \in \overline{K}$ is excluded and we have $\nu \leq n$ with equality possible only if

$$f = a((\alpha - 1)x + \beta y)^n + by^n, \quad a, b \text{ in } \overline{K}.$$

It now follows from $e_f(\infty) > 0$ that $f(1,0) = 0$, hence $a = 0$, $f = by^n$, $|Z| = 1$, a contradiction. Hence $\nu < n$. Since there are only finitely many $\alpha \in K^*$ with $\alpha^\nu = 1$ for some $\nu < n$, $\mathcal{H}$ is finite and cyclic by the well known lemma (see [3, Algebraic Supplement, §3]). Its order l equal to the order of a generator satisfies

$$|\mathcal{H}| = l < n, \quad l \not\equiv 0 \bmod \pi, \quad \zeta_l \in K. \tag{50}$$

Let

$$\mathcal{G} = \left\{\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix} K^* \in \mathrm{Aut}(f,K)\right\}.$$

Then $\mathcal{G}$ is a normal subgroup of $\mathrm{Aut}(f,K,\infty)$, which in turn is a subgroup of $\mathrm{Aut}(f,K)$. If $\pi = 0$, then $\mathcal{G} = \{E\}$, for otherwise taking $\xi_1 \in Z \setminus \{\infty\}$ and $\beta \in K^*$ such that $S = \left(\begin{smallmatrix}1 & \beta\\ 0 & 1\end{smallmatrix}\right)K^* \in \mathcal{G}$ we should obtain, by Lemma 17, $\xi_1 + i\beta = S^{*i}\xi_1 \in Z$, a contradiction, since $\xi_1 + i\beta$ $(i = 0,\dots,n)$ are distinct. If $\pi > 0$ then

$$\mathcal{G} = \mathrm{Aut}_\pi(f,K,\infty)$$

is a π-group and, by Corollary 11,

$$|\mathcal{G}| = \pi^g \leq n.$$

The quotient group $\mathrm{Aut}(f,K,\infty)/\mathcal{G}$ is isomorphic to $\mathcal{H}$, hence the assertion follows from (50).

Assume now $\xi \neq \infty$ and put $f_1 = f(\xi x + y, x)$. We have $f_1(1,0) = f(\xi,1) = 0$, hence $e_{f_1}(\infty) > 0$ and, by the already proved case of the lemma, $\mathrm{Aut}_\pi(f_1, K(\xi), \infty)$ is a finite normal subgroup of $\mathrm{Aut}(f_1, K(\xi), \infty)$ and the quotient group is cyclic of order $l < n$ with $l \not\equiv 0 \bmod \pi$ such that $\zeta_l \in K(\xi)$.

Now

$$\mathrm{Aut}(f,K,\xi) \subset \begin{pmatrix} \xi & 1 \\ 1 & 0 \end{pmatrix} \mathrm{Aut}(f_1, K(\xi), \infty) \begin{pmatrix} \xi & 1 \\ 1 & 0 \end{pmatrix}^{-1},$$

$$\mathrm{Aut}_\pi(f,K,\xi) \subset \begin{pmatrix} \xi & 1 \\ 1 & 0 \end{pmatrix} \mathrm{Aut}_\pi(f_1, K(\xi), \infty) \begin{pmatrix} \xi & 1 \\ 1 & 0 \end{pmatrix}^{-1},$$

and the assertion of the lemma follows from simple facts from group theory.

LEMMA 24. *For $\xi \in Z$ (notation of Lemma 23), let m be the length of the orbit of ξ under the action of $\mathrm{Aut}(f,K)$. If $|\mathrm{Aut}(f,K,\xi)| \equiv 0 \bmod \pi$, then $m \equiv 1 \bmod \pi$, also either $\xi \in K$ or*

$$\pi = 2, \quad \mathrm{Aut}(f,K,\xi) = \mathrm{Aut}_\pi(f,K,\xi). \tag{51}$$

Proof. By Lemma 17, $\mathrm{Aut}(f,K)$, hence also $\mathrm{Aut}_\pi(f,K,\xi)$, acts on Z. Let $O(\xi)$ be the orbit of ξ under the action of $\mathrm{Aut}(f,K)$. Since for $\eta \in Z$ and $S \in \mathrm{Aut}_\pi(f,K,\xi) \setminus \{E\}$, $S^*\eta = \eta$ implies $\eta = \xi$, $\mathrm{Aut}_\pi(f,K,\xi)$ acts on $O(\xi) \setminus \{\xi\}$ and all orbits are of length $|\mathrm{Aut}_\pi(f,K,\xi)|$. Hence $m = |O(\xi)| \equiv 1 \bmod \pi$. By Lemma 3, $\mathrm{Aut}_\pi(f,K,\xi)$ has an element

$$S_0 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} K^*,$$

where $ad - bc \neq 0$, $\lambda \neq 0$ and either $a,b,c,d,\lambda \in K$, or $\pi = 2$, $c \in K^*$, and $K(d)$ is a quadratic inseparable extension of K. The condition $S_0^*\xi = \xi$ gives $\xi = -d/c$. In the former case it follows that $\xi \in K$, in the latter case $K(\xi)$ is a quadratic inseparable extension of K and for $S = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) K^* \in \mathrm{Aut}(f,K,\xi)$ the equation $S^*\xi = \xi$ gives $\alpha = \delta$, $S^\pi = e$, hence (51) holds.

Proof of Theorem 4. Suppose $|\mathrm{Aut}(f,K)|$ is divisible exactly by $\pi^g = q$, and for $\xi \in Z$, let $m(\xi)$ be the length of the orbit of ξ under the action of $\mathrm{Aut}(f,K)$. For all $\xi \in Z$ we have

$$|\mathrm{Aut}(f,K)| = |\mathrm{Aut}(f,K,\xi)| m(\xi) \tag{52}$$

and, by Lemma 17,

$$m(\xi) \leq |Z| \leq n. \tag{53}$$

If $|\mathrm{Aut}(f,K,\xi)| \not\equiv 0 \bmod \pi$ for at least one $\xi \in Z$ then, by Lemma 23, $\mathrm{Aut}(f,K,\xi)$ is cyclic of order $l < n$ with $l \not\equiv 0 \bmod \pi$. By Lemma 1 we have $\zeta_l + \zeta_l^{-1} \in K$. Moreover, by (52),

$$|\mathrm{Aut}(f,K)| = l m(\xi),$$

which together with (53) gives (49).

If $|\mathrm{Aut}(f,K,\xi)| \equiv 0 \bmod \pi$ for all $\xi \in Z$, then, by Lemma 24, $m(\xi) \not\equiv 0 \bmod \pi$, hence by (52),

$$|\mathrm{Aut}(f,K,\xi)| \equiv 0 \bmod q$$

and $\mathrm{Aut}_\pi(f,K,\xi)$ is a π-Sylow subgroup of $\mathrm{Aut}(f,K)$. Since all π-Sylow subgroups are conjugate and the only conjugates of $\mathrm{Aut}_\pi(f,K,\xi)$ in $\mathrm{Aut}(f,K)$ are, by Lemma 17, the groups $\mathrm{Aut}_\pi(f,K,\eta)$, where $e_f(\eta)=e_f(\xi)$, it follows that for all $\xi\in Z$, $m(\xi)=|Z|$, $e_f(\xi)$ has the same value, say k, and the number σ of π-Sylow subgroups is $|Z|\geq 3$. It follows, by Lemma 11, that either

$$\pi=2,\quad |Z|=2\varrho+1,\quad \mathrm{Aut}(f,K)\cong\mathfrak{D}_{2\varrho+1}, \tag{54}$$

or

$$\pi=3,\quad |Z|=10,\quad \mathrm{Aut}(f,K)\cong\mathfrak{A}_5, \tag{55}$$

or

$$|Z|=q+1,\quad \mathrm{Aut}(f,K)\cong\mathcal{H}_i, \tag{56}$$

where $\mathcal{H}_1=\mathrm{PGL}_2(\mathbb{F}_q)$ and $\mathcal{H}_2=\mathrm{PSL}_2(\mathbb{F}_q)$.

For $k=1$ the case (54) gives (47), while (55) gives (48). For $k>1$, (54) and (55) give (49) with $l=2\varrho+1$, $m=2$ or $l=10$, $m=6$, respectively. The case (56) for $q=2$ gives (47) with $\varrho=1$. For $q>2$, (56) gives

$$|\mathrm{Aut}(f,K,\xi)|=q^2-q\quad\text{or}\quad (q^2-q)/(\pi+1,2).$$

In the notation of Lemma 23, $l=q-1$ or $(q-1)/(\pi+1,2)$, hence $q>1$ and, by Lemma 24, $\xi\in K$. The condition $\zeta_l\in K(\xi)$ of Lemma 23 now gives $\mathbb{F}_q\subset K$.

By Lemma 13, $\mathrm{Aut}(f,K)$ is conjugate in $\mathrm{PGL}_2(K)$ to $\mathcal{H}_iK^*/K^*$, hence there exist $\alpha,\beta,\gamma,\delta$ in K such that $\alpha\delta-\beta\gamma\neq 0$ and

$$\mathrm{Aut}(f,K)=\begin{pmatrix}\alpha&\beta\\ \gamma&\delta\end{pmatrix}^{-1}\mathcal{H}_i\begin{pmatrix}\alpha&\beta\\ \gamma&\delta\end{pmatrix}K^*/K^*. \tag{57}$$

Since $e_f(\xi)=k$ for all $\xi\in Z$, we have

$$f=f_1^k,\quad\text{where}\quad f_1\in\overline{K}[x,y],\ \deg f_1=|Z|. \tag{58}$$

Put

$$f_2=f_1(\delta x-\beta y,-\gamma x+\alpha y),\quad a_0=(\alpha\delta-\beta\gamma)^{-n}.$$

It follows from (58) that

$$f=a_0f_2(\alpha x+\beta y,\gamma x+\delta y)^k,\quad \deg f_2=q+1, \tag{59}$$

and

$$\mathrm{Aut}(f,K)=\begin{pmatrix}\alpha&\beta\\ \gamma&\delta\end{pmatrix}^{-1}\mathrm{Aut}(f_2,K)\begin{pmatrix}\alpha&\beta\\ \gamma&\delta\end{pmatrix}. \tag{60}$$

Hence, by (57),

$$\mathrm{Aut}(f_2,K)=\mathcal{H}_iK^*/K^*. \tag{61}$$

By Corollary 8, applied with $\mathcal{G}=\mathrm{Aut}(f_2,K)\overline{K}^*/\overline{K}^*$, by Definition 5 and Lemmas 8 and 9 we obtain

$$f_2=\chi_1^{c_1}\chi_2^{c_2}\psi(p,q),$$

where

$$\chi_1 = y\prod_{\xi\in\mathbb{F}_q}(x-\xi y), \quad \chi_2 = \prod_{\xi\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q}(x-\xi y), \quad p=\chi_1^{|\mathcal{H}_i|/(q+1)}, \quad q=\chi_2^{|\mathcal{H}_i|/(q^2-q)}$$

and ψ is a form over $\overline{K}$. The condition $\deg f_2 = q+1$ implies $c_1=1$, $c_2=0$, $\psi\in\overline{K}$, $f_2 = (x^qy-xy^q)\psi$, hence (46) follows from (59). Since $\mathrm{Aut}(x^qy-xy^q,K)\supset \mathrm{PGL}_2(\mathbb{F}_q)K^*/K^*$ we have $i=1$ in (61) and $\mathrm{Aut}(f,K)\cong\mathrm{PGL}_2(\mathbb{F}_q)$ by (60). This has been deduced from the assumption that $|\mathrm{Aut}(f,K,\xi)|\equiv 0 \bmod \pi$ for all ξ, while in the opposite case one of the formulae (47)–(49) holds. Since f_2 does not satisfy (47)–(49), we have, indeed, $\mathrm{Aut}(f,K)\cong\mathrm{Aut}(f_2,K)\cong\mathrm{PGL}_2(\mathbb{F}_q)$.

Proof of Corollary 12. By Theorem 4 the condition given in the corollary is sufficient. In order to prove that it is necessary assume that K is infinite and f has at most two coprime linear factors over $\overline{K}$. We distinguish three cases: the zeros of $f(x,1)$ are in K; the zeros of $f(x,1)$ are conjugate quadratic irrationalities over K and $\pi\neq 2$; and the zeros of $f(x,1)$ are conjugate quadratic irrationalities over K and $\pi=2$.

In the first case f is equivalent over K to a form $f_1=ax^my^n$, where $a\in K, m, n$ are non-negative integers and f has infinitely many pairwise inequivalent weak automorphs $\left(\begin{smallmatrix}\alpha & 0\\ 0 & 1\end{smallmatrix}\right)K^*$, $\alpha\in K^*$.

In the second case f is equivalent over K to a form $f_2=a(x^2-cy^2)^m$, where $a,c\in K^*$, $m\in\mathbb{N}$ and f_1 has infinitely many pairwise inequivalent weak automorphs $\left(\begin{smallmatrix}\alpha & c\gamma\\ \gamma & \alpha\end{smallmatrix}\right)K^*$, where $\langle\alpha,\gamma\rangle$ runs through infinitely many solutions in K of the equation $\alpha^2-c\gamma^2=1$, and from each pair $\langle\alpha,\gamma\rangle$, $\langle-\alpha,-\gamma\rangle$ we use only one solution.

In the third case f is equivalent over K to a form $f_3=a(x^2+bxy+cy^2)^m$, where $a,b,c\in K^*$ and $m\in\mathbb{N}$. Now we distinguish two subcases.

If c/b^2 is algebraic over $\mathbb{F}_2$ then $(c/b^2)^{2k-1}=1$ for a certain $k\in\mathbb{N}$, hence $c=d^2$, where $d=b(c/b^2)^k\in K^*$. It follows that f_3 has infinitely many pairwise inequivalent weak automorphs $\left(\begin{smallmatrix}d\alpha & bd\alpha+d^2\\ 1 & d\alpha\end{smallmatrix}\right)K^*$, where α runs over K^*. On the other hand, f_3 has a weak automorph $\left(\begin{smallmatrix}c & bc\\ b & b^2+c\end{smallmatrix}\right)K^*$.

If c/b^2 is transcendental over $\mathbb{F}_2$, then this automorph is of infinite order in $\mathrm{PGL}_2(K)$. Indeed, otherwise we should have (see proof of Lemma 1) for a certain $\lambda\in\overline{K}$ and a root of unity ζ, $\lambda(1+\zeta)=b^2$, $\lambda^2\zeta=c^2$, hence $\zeta+\zeta^{-1}=b^4/c^2$, a contradiction.

Proof of Corollary 13. We have $\zeta_\nu\in K$ for $\nu\le 2$, and $\zeta_\nu+\zeta_\nu^{-1}\in K$ for $\nu\le 4$ or $\nu=6$.

For the proof of Theorem 5 we need six lemmas.

LEMMA 25. *Assume $n\ge 3$ and either $\pi=0$ or $\pi>n$. If f of degree n has at least three coprime linear factors over $\overline{K}$ and $\mathrm{Aut}(f,K)$ is cyclic, then*

$$|\mathrm{Aut}(f,K)|\le\begin{cases} a_1(n,K) & \text{if } f\in\overline{K}[x,y],\\ \max\{a_2(n,K),b(n-1,K)\} & \text{if } f\in K[x,y].\end{cases}$$

There exist forms $f_1\in\overline{K}[x,y]$, $f_2,f_3\in K[x,y]$ of degree n, each with at least three

coprime linear factors over $\overline{K}$ *and not a perfect power in* $\overline{K}[x,y]$, *such that*

$$\big|\mathrm{Aut}(f_1,K)\big| \geq a_1(n,K),$$
$$\big|\mathrm{Aut}(f_2,K)\big| \geq a_2(n,K),$$
$$\big|\mathrm{Aut}(f_3,K)\big| \geq b(n-1,K).$$

Proof. If $\mathcal{G} = \mathrm{Aut}(f,K)$ is cyclic, then by Theorem 1 and Corollary 5,

$$f = \chi_1^{c_1}\chi_2^{c_2}\psi(p,q), \tag{62}$$

where

$$\deg\chi_i = 1, \quad \deg p = \deg q = |\mathcal{G}|,$$

and ψ is a form over $\overline{K}$ or over K if $f \in \overline{K}[x,y]$ or $f \in K[x,y]$, respectively. By the assumption on linear factors of f, we have $\deg\psi \geq 1$, hence

$$n = \deg f = c_1 + c_2 + |\mathcal{G}|\deg\psi \geq |\mathcal{G}|. \tag{63}$$

On the other hand, by Lemma 1,

$$\eta_{|\mathcal{G}|} := \zeta_{|\mathcal{G}|} + \zeta_{|\mathcal{G}|}^{-1} \in K, \tag{64}$$

hence by Definition 7,

$$|\mathcal{G}| \leq a_1(n,K). \tag{65}$$

To estimate $|\mathcal{G}|$ for $f \in K[x,y]$ a division into cases is necessary.

If $c_1 + c_2 \equiv 0 \bmod 2$, then

$$n \equiv |\mathcal{G}|\deg\psi \bmod 2.$$

For n odd this implies $n \equiv |\mathcal{G}| \bmod 2$, hence

$$|\mathcal{G}| \leq a_2(n,K). \tag{66}$$

For n even either $\deg\psi \equiv 1 \bmod 2$, and then again (66) holds, or $\deg\psi \equiv 0 \bmod 2$, in which case by (63) and (64),

$$|\mathcal{G}| \leq a_1(n/2,K).$$

But

$$n \equiv 0 \bmod 2 \quad \text{implies} \quad a_1(n/2,K) \leq a_2(n,K), \tag{67}$$

since if $a_1(n/2,K) \equiv 1 \bmod 2$, we have

$$2a_1(n/2,K) \leq n \quad \text{and} \quad \eta_{2a_1(n/2,K)} \in K.$$

If $c_1 + c_2 \equiv 1 \bmod 2$, then $c_1 \neq c_2$, hence $\chi_1 \in K[x,y]$ by Theorem 1, and $\zeta_{|\mathcal{G}|} \in K$ by Lemma 14. Now (63) implies $|\mathcal{G}| \leq n-1$, hence by Definition 7,

$$|\mathcal{G}| \leq b(n-1,K),$$

which together with (65) and (66) proves the first part of the lemma.

To prove the second part we put

$$f_1 = \chi_1^{n-a_1(n,K)}(p+q), \qquad f_2 = (\chi_1\chi_2)^{(n-a_2(n,K))/2}(p+q), \qquad f_3 = \chi_1^{n-b(n-1,K)}(p+q),$$

where χ_1, χ_2 and p, q are given in Definition 5 for $\mathcal{G}$ cyclic of order $a_1(n,K)$, $a_2(n,K)$, $b(n-1,K)$, respectively. Now $p+q$ is prime to $\chi_1\chi_2$, is not a perfect power in $\overline{K}[x,y]$ and has $|\mathcal{G}|$ coprime linear factors over $\overline{K}$. Hence the f_i are not perfect powers and since

for $n \geq 3$, by Corollary 13, $a_1(n,K) \geq 3$, $a_2(n,K) \geq 3$, $b(n-1,K) \geq 2$, each f_i has at least three coprime linear factors over $\overline{K}$.

LEMMA 26. *Assume $n \geq 3$ and either $\pi = 0$ or $\pi > n$. If f of degree n has at least three coprime linear factors over $\overline{K}$ and $\mathrm{Aut}(f,K)$ is dihedral, then*

$$|\mathrm{Aut}(f,K)| \leq 2a_2(n,K).$$

There exists a form $f_0 \in K[x,y]$ of degree n, with at least three coprime linear factors over $\overline{K}$ and not a perfect power in $\overline{K}[x,y]$, such that

$$|\mathrm{Aut}(f_0,K)| \geq 2a_2(n,K).$$

Proof. If $\mathcal{G} = \mathrm{Aut}(f,K)$ is dihedral, then by Lemma 7, Theorem 2 and Corollary 8,

$$f = \chi_1^{c_1}\chi_2^{c_2}\chi_3^{c_3}\psi(p,q), \tag{68}$$

where

$$\deg \chi_1 = \deg \chi_2 = |\mathcal{G}|/2, \quad \deg p = \deg q = |\mathcal{G}|$$

and ψ is a binary form over $\overline{K}$ or K if $f \in \overline{K}[x,y]$ or $f \in K[x,y]$, respectively. On the other hand, by Lemma 1,

$$\eta_{|\mathcal{G}|/2} \in K. \tag{69}$$

It follows from (68) that

$$n = c_1|\mathcal{G}|/2 + c_2|\mathcal{G}|/2 + 2c_3 + |\mathcal{G}|\deg\psi. \tag{70}$$

For n odd it follows that $|\mathcal{G}|/2 \equiv 1 \bmod 2$ and $c_1 + c_2 \equiv 1 \bmod 2$, hence

$$|\mathcal{G}|/2 \leq n, \quad |\mathcal{G}|/2 \equiv n \bmod 2,$$

thus by Definition 7 and (69),

$$|\mathcal{G}| \leq 2a_2(n,K). \tag{71}$$

For n even, if $c_1 + c_2 \equiv 1 \bmod 2$, the same inequality holds; if $c_1 + c_2 \equiv 0 \bmod 2$, then, by (70) and the assumption on linear factors of f, either $c_1 + c_2 \geq 2$ or $\psi \notin K$, hence

$$|\mathcal{G}|/2 \leq n/2, \quad |\mathcal{G}|/2 \leq 2a_1(n/2,K),$$

and by (67) we again obtain (71).

In order to prove the second part of the lemma we put

$$f_0 = \chi_2\chi_3^{(n-a_2(n,K))/2},$$

where χ_2, χ_3 are given in the Example (p. 25) for $\mathcal{G}$ dihedral of order $2a_2(n,K)$ with $a = 1$, $b = 0$. Since $\deg\chi_2 = a_2(n,K)$ and $\deg\chi_3 = 2$ we have $\deg f_0 = n$, and since $\chi_2, \chi_3 \in K[x,y]$ we have $f_0 \in K[x,y]$.

Now, χ_2 is prime to χ_3, is not a perfect power in $\overline{K}[x,y]$ and has $a_2(n,K) \geq 3$ coprime linear factors over $\overline{K}$. Hence f_0 is not a perfect power in $\overline{K}[x,y]$ and has at least three coprime linear factors over $\overline{K}$.

LEMMA 27. *Let $n \geq 3$ and either $\pi = 0$ or $\pi > n$ and let $f \in \overline{K}[x,y]$ be a form of degree n and not a perfect power. If $\mathrm{Aut}(f,K)$ contains a subgroup isomorphic to $\mathcal{G}_i$, where $\mathcal{G}_1 = \mathfrak{A}_4$, $\mathcal{G}_2 = \mathfrak{S}_4$, $\mathcal{G}_3 = \mathfrak{A}_5$, then*

$$n = c_1\frac{|\mathcal{G}_i|}{i+2} + c_2\frac{|\mathcal{G}_i|}{3} + c_3\frac{|\mathcal{G}_i|}{2} + c_4|\mathcal{G}_i|, \tag{72}$$

where c_i are non-negative integers and

$$\text{either } (c_1, c_2, c_3) = 1 \text{ or } c_4 \neq 0. \tag{73}$$

Moreover,

$$\operatorname{level} K \leq 2 \quad \text{and} \quad \text{if} \quad i = 3, \text{ then } \sqrt{5} \in K. \tag{74}$$

If (72)–(74) *are satisfied with $c_4 = 0$, then there exists a form $f \in \overline{K}[x, y]$ of degree n, with at least three coprime linear factors over $\overline{K}$ and not a perfect power in $\overline{K}[x, y]$, such that* $\operatorname{Aut}(f, K)$ *contains $\mathcal{G}_i$. Moreover, for $i > 1$ such a form f exists in $K[x, y]$.*

Proof. If $\operatorname{Aut}(f, K)$ contains a subgroup isomorphic to $\mathcal{G}_i$, then $\mathrm{PGL}_2(K)$ contains such a subgroup, hence (74) holds by Lemma 2. Further, by Corollary 8, we have

$$f = \prod_{i=1}^{k} \chi_i^{c_i} \psi(p, q), \tag{75}$$

where χ_i and p, q are given in Definition 5 and ψ is a binary form over $\overline{K}$. By Lemma 7 we have $h = 3$,

$$\deg \chi_1 = \frac{|\mathcal{G}_i|}{i+2}, \quad \deg \chi_2 = \frac{|\mathcal{G}_i|}{3}, \quad \deg \chi_3 = \frac{|\mathcal{G}_i|}{2}, \tag{76}$$

while, by Definition 5,

$$\deg p = \deg q = |\mathcal{G}_i|.$$

Now (72) follows from (75) with $c_4 = \deg \psi$, and (73) follows from (75) and the condition that f is not a perfect power in $\overline{K}[x, y]$.

In the opposite direction, if (72)–(74) hold with $c_4 = 0$, we take

$$f = \prod_{i=1}^{3} \chi_i^{c_i}.$$

By Definition 5, χ_i are coprime and separable, hence the number of coprime linear factors of f over $\overline{K}$ is at least

$$|\mathcal{G}_i| \left(\frac{\operatorname{sgn} c_1}{i+2} + \frac{\operatorname{sgn} c_2}{3} + \frac{\operatorname{sgn} c_3}{2} \right) \geq \frac{|\mathcal{G}_i|}{i+2} \geq 4.$$

Also f is not a perfect power in $\overline{K}[x, y]$, since $(c_1, c_2, c_3) = 1$ by (73). For $i > 1$, χ_i are of distinct degrees, hence no two of them are conjugate over K and, by Corollary 6, they are in $K[x, y]$. Thus $f \in K[x, y]$.

LEMMA 28. *Assume $\pi = 0$ or $\pi > 3$. A quartic form $f \in K[x, y]$ with at least three coprime linear factors over $\overline{K}$, which is not a perfect power in $\overline{K}[x, y]$ and for which* $\operatorname{Aut}(f, K)$ *contains a subgroup isomorphic to $\mathfrak{A}_4$, exists if and only if $\sqrt{-3} \in K$.*

Proof. If $\operatorname{Aut}(f, K)$ contains a subgroup isomorphic to $\mathfrak{A}_4$, then it has an element of order 3. By Corollary 3 it follows that either $\sqrt{-3} \in K$, or f is square in $K[x, y]$, the possibility excluded by the condition on f.

For the opposite direction, we take $f = x^4 - xy^3$. This form has two non-trivial weak automorphs defined over K,

$$S = \begin{pmatrix} -1 & 1 \\ 2 & 1 \end{pmatrix} K^*, \quad T = \begin{pmatrix} \zeta_3 & 0 \\ 0 & 1 \end{pmatrix} K^*.$$

They satisfy the equations $S^2 = E$, $T^3 = E$, $TST = ST^{-1}S$, hence $\langle S, T \rangle \cong \mathfrak{A}_4$.

LEMMA 29. *If* $\operatorname{level} K \le 2$, $\sqrt{5} \in K$ *and either* $\pi = 0$ *or* $\pi > 5$, *then there exists a form* $f \in K[x,y]$ *of degree* 60, *with at least three coprime linear factors over* $\overline{K}$ *and not a perfect power in* $\overline{K}[x,y]$, *such that* $\operatorname{Aut}(f,K)$ *contains a subgroup isomorphic to* $\mathfrak{A}_5$.

Proof. By Lemma 2, $\mathrm{PGL}_2(K)$ contains a subgroup isomorphic to $\mathfrak{A}_5$. Let χ_1, χ_2, χ_3 be the polynomials defined in Definition 5 for this group $\mathcal{G}$, such that $\chi_i \in K[x,y]$ and

$$\deg \chi_1 = 12, \quad \deg \chi_2 = 20, \quad \deg \chi_3 = 30$$

(see the proof of Lemma 27). We assert that for a certain $\varepsilon = \pm 1$,

$$f_\varepsilon = \chi_1^5 + \varepsilon \chi_2^\varepsilon$$

has the required properties.

If r_ε is the number of distinct zeros of $f_\varepsilon(x,1)$, then by the *abc*-theorem for polynomials (see [18])

$$r_\varepsilon > 60 - \deg \chi_1(x,1) - \deg \chi_2(x,1) \ge 28,$$

thus f_ε has at least 29 coprime linear factors over $\overline{K}$. If f_ε is a perfect power in $\overline{K}[x,y]$, then

$$f_\varepsilon = g_\varepsilon^2, \quad g_\varepsilon \in \overline{K}[x,y].$$

Moreover, $\operatorname{Aut}(g_\varepsilon, K) = \operatorname{Aut}(f_\varepsilon, K)$, hence $\operatorname{Aut}(g_\varepsilon, K)$ contains $\mathcal{G}$ and, by Corollary 8,

$$g_\varepsilon = \prod_{i=1}^{3} \chi_i^{d_{\varepsilon i}} \psi_\varepsilon, \quad \psi_\varepsilon \in \overline{K}.$$

Since $(f_\varepsilon, \chi_1\chi_2) = 1$ and $\deg f_\varepsilon = 2 \deg \chi_3$ we conclude that

$$d_{\varepsilon 1} = d_{\varepsilon 2} = 0, \quad d_{\varepsilon 3} = 1$$

and

$$f_\varepsilon = \psi_\varepsilon^2 \chi_3^2.$$

If this holds for $\varepsilon = 1$ and $\varepsilon = -1$, then

$$2\chi_1^5 = f_1 + f_{-1} = (\psi_1^2 + \psi_{-1}^2)\chi_3^2,$$

which contradicts $(\chi_1, \chi_3) = 1$.

LEMMA 30. *The equation*

$$m = 3c_1 + 4c_2 + 6c_3 \tag{77}$$

is solvable in coprime non-negative integers for every $m \ge 9$, *and the equation*

$$m = 6c_1 + 10c_2 + 15c_3 \tag{78}$$

is solvable in such integers if and only if $m \in \mathcal{M} \setminus \{30\}$.

Proof. Solvability of (77) for $m < 12$ can be checked case by case. By a classical theorem due to Curran Sharp [8] every integer greater than $ab - a - b$ is a linear combination of a, b with non-negative coefficients. For $m \ge 12$ we have $m - 6 \ge 6$ and hence $m - 6 = 3c_1 + 4c_2$, where c_1, c_2 are non-negative integers. It suffices to take $c_3 = 1$.

Solvability of (78) for odd $m < 31$ and for even $m < 76$ can be checked case by case. For odd $m \ge 31$, $(m-15)/2 \ge 8$ is an integer and, by Curran Sharp's theorem, $(m-15)/2 = 3c_1 + 5c_2$, where c_1, c_2 are non-negative integers. It suffices to take $c_3 = 1$.

For even $m \geq 76$, $(m-30)/2 \geq 23$ is an integer, hence by Curran Sharp's theorem $(m-30)/2 = 3d_1 + 5d_2$, where d_1, d_2 are non-negative integers. Moreover, since $23 > 3 \cdot 4 + 5 \cdot 2$, we have either $d_1 \geq 5$ or $d_2 \geq 3$. If at least one d_i is odd we take $c_1 = d_1$, $c_2 = d_2$, $c_3 = 2$, otherwise we take $c_3 = 2$ and either $c_1 = d_1 - 5$, $c_2 = d_2 + 3$ or $c_1 = d_1 + 5$, $c_2 = d_2 - 3$.

Proof of Theorem 5. The assumption that f is not a perfect power in $\overline{K}[x,y]$ implies in the case (46) that $k = 1$, $n = q+1$. This gives $A(\pi^g+1, K) = B(\pi^g+1, K) = \pi^{3g} - \pi^g$ if $\mathbb{F}_{\pi^g} \subset K$. On the other hand, (47)–(49) imply

$$|\mathrm{Aut}(f, K)| \leq n(n-1),$$

hence $A(n,K) \leq n(n-1)$ if either $n \neq \pi^g + 1$ or $\mathbb{F}_{\pi^g} \not\subset K$. This bound is attained for every $\pi > 0$ and $n = \pi^g$. Indeed, for $q = \pi^g$,

$$\mathrm{Aut}(x^q - xy^{q-1}, \mathbb{F}_q) \supset \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} K^* : \alpha \in \mathbb{F}_q^*,\ \beta \in \mathbb{F}_q \right\}.$$

Assume now that $\pi = 0$ or $\pi > n$. By Theorem 4,

$$|\mathrm{Aut}(f, K)| \not\equiv 0 \bmod \pi$$

and, by Lemma 7, $\mathcal{G} = \mathrm{Aut}(f, K)$ is either cyclic, dihedral or polyhedral. The first two cases are considered in Lemmas 25 and 26. If $\mathcal{G}$ is a polyhedral group, then (72) holds by Lemma 27, and since all terms on the right-hand side are even, n is even.

For n odd it follows that $\mathrm{Aut}(f, K)$ is either cyclic or dihedral, and by Lemmas 25, 26,

$$A(n,K) \leq \max\{a_1(n,K), 2a_2(n,K)\},$$
$$B(n,K) \leq \max\{b(n-1,K), 2a_2(n,K)\}.$$

The inequalities in the opposite direction follow from the second part of Lemmas 25 and 26. This gives the theorem for n odd.

For n even a further study of polyhedral groups is necessary. For $n = 4$ the equation (72) gives $i = 1$, $|\mathcal{G}_i| = 12$, $c_3 = c_4 = 0$. Since $12 > 8 = \max\{a_1(4,K), 2a_2(4,K)\}$ we obtain from Lemmas 25–27,

$$A(4,K) = \begin{cases} 12 & \text{if level}\, K \leq 2, \\ \max\{a_1(4,K), 2a_2(4,K)\} & \text{otherwise,} \end{cases}$$

and from Lemmas 25, 26 and 28,

$$B(4,K) = \begin{cases} 12 & \text{if } \sqrt{-3} \in K, \\ \max\{b(3,K), 2a_2(4,K)\} & \text{otherwise.} \end{cases}$$

For even $n > 4$ we have $2a_2(n,K) \geq 12$, hence the equation (72) is of interest only for $i > 1$, and if $n < |\mathcal{G}|$, then $(c_1, c_2, c_3) = 1$ by (72), (73).

For $n = 6, 8, 14$ and $i > 1$, (72) gives $i = 2$ and $\langle c_1, c_2, c_3 \rangle = \langle 1,0,0 \rangle$ or $\langle 0,1,0 \rangle$ or $\langle 1,1,0 \rangle$, respectively. It follows by Lemmas 25–27 that for $n = 6, 8, 14$,

$$A(n,K) = \begin{cases} \max\{a_1(n,K), 2a_2(n,K), 24\} & \text{if level}\, K \leq 2, \\ \max\{a_1(n,K), 2a_2(n,K)\} & \text{otherwise;} \end{cases}$$

$$B(n,K)=\begin{cases}\max\{b(n-1,K),2a_2(n,K),24\} & \text{if level}\, K\le 2,\\ \max\{b(n-1,K),2a_2(n,K)\} & \text{otherwise.}\end{cases}$$

For $n=10,16$ the equation (72) has no solution with $i>1$ and $(c_1,c_2,c_3)=1$, hence, by Lemmas 25–27,

$$A(n,K)=\max\{a_1(n,K),2a_2(n,K)\},$$

$$B(n,K)=\max\{b(n-1,K),2a_2(n,K)\}.$$

For $n=12$, $i>1$ and $(c_1,c_2,c_3)=1$, (72) gives $i=2$, $\langle c_1,c_2,c_3\rangle=\langle 0,0,1\rangle$ or $i=3$, $\langle c_1,c_2,c_3\rangle=\langle 1,0,0\rangle$. Hence, by Lemmas 25–27,

$$A(12,K)=\begin{cases}\max\{a_1(n,K),2a_2(n,K),24\} & \text{if level}\, K\le 2,\ \sqrt{5}\notin K,\\ 60 & \text{if level}\, K\le 2,\ \sqrt{5}\in K,\\ \max\{a_1(n,K),2a_2(n,K)\} & \text{otherwise;}\end{cases}$$

$$B(12,K)=\begin{cases}\max\{b(n-1,K),2a_2(n,K),24\} & \text{if level}\, K\le 2,\ \sqrt{5}\notin K,\\ 60 & \text{if level}\, K\le 2,\ \sqrt{5}\in K,\\ \max\{b(n-1,K),2a_2(n,K)\} & \text{otherwise.}\end{cases}$$

By Lemma 30 for $n=2m$, $m\ge 9$, (72) always has a solution with $i=2$, $c_4=0$, $(c_1,c_2,c_3)=1$, and has a solution with $i=3$, $c_4=0$, $(c_1,c_2,c_3)=1$ if and only if $m\in\mathcal{M}\setminus\{30\}$. Since $\mathcal{M}$ contains all integers greater than 29 except 32 and 44, by Lemmas 25–27, the formulae for $A(n,K)$ and $B(n,K)$ hold for all even n, except possibly for $n=2m$, $m=30,32,44$. For $m=30$ the formulae follow from Lemmas 25, 26 and 29, for $m=32$ or 44 the only solution of (72) does not satisfy (73), hence the formulae follow from Lemmas 25–27.

Proof of Corollary 14. For $K=\mathbb{C}$ we have $a_1(n,K)=n=a_2(n,K)$.

4. Criteria for a form to have a non-trivial automorph over a given arbitrary field

THEOREM 6. *Let $f\in K[x,y]$ be a form of degree $n>2$ without multiple factors over $\overline{K}$. If $\mathrm{Aut}(f,K)$ is non-trivial and $f(x,1)$ of degree m is irreducible over K, then the Galois group of $f(x,1)$ over K is either imprimitive or cyclic of prime order m. For $n\le 4$ the converse holds unless $n=4$ and $m=3$.*

COROLLARY 15. *Assume that K contains no primitive cubic root of unity and $f\in K[x,y]$ is a form of degree $2,3$ or 4 without multiple factors over $\overline{K}$. The group $\mathrm{Aut}(f,K)$ is non-trivial if and only if the Galois group of $f(x,1)$ over K is either transitive imprimitive or abelian with the lengths of orbits not $\langle 3,1\rangle$.*

COROLLARY 16. *Let $f\in K[x,y]$ be a cubic form with $f(1,0)\ne 0$ and without multiple factors over $\overline{K}$ and $\mathcal{G}$ be the Galois group of $f(x,1)$ over K. Then $\mathrm{Aut}(f,K)\cong\mathfrak{D}_3$ if $\mathcal{G}\cong\mathfrak{C}_1$, $\mathrm{Aut}(f,K)\cong\mathfrak{C}_2$ if $\mathcal{G}\cong\mathfrak{C}_2$, $\mathrm{Aut}(f,K)\cong\mathfrak{C}_3$ if $\mathcal{G}\cong\mathfrak{C}_3$, and $\mathrm{Aut}(f,K)\cong\mathfrak{C}_1$ if $\mathcal{G}\cong\mathfrak{D}_3$.*

REMARK. For quartic forms f the structure of the Galois group $\mathcal{G}(f)$ of $f(x,1)$ over $\mathbb{Q}$ does not determine in general the structure of $\mathrm{Aut}(f,\mathbb{Q})$, for instance for $f_1 = x^4+x^3y+x^2y^2+xy^3+y^4$, $f_2 = x^4+4x^3y-6x^2y^2-4xy^3+y^4$, $\mathcal{G}(f_i) \cong \mathfrak{C}_4$, while $\mathrm{Aut}(f_1,\mathbb{Q}) \cong \mathfrak{C}_2$ (proof by means of Lemma 17), and $\mathrm{Aut}(f_2,\mathbb{Q})$ contains $\mathfrak{C}_4$ generated by $\left(\begin{smallmatrix} 1 & 1 \\ -1 & 1 \end{smallmatrix}\right)\mathbb{Q}^*$.

The proof of Theorem 6 is based on the following

LEMMA 31. *Given a pair $\langle g,h\rangle$ of coprime binary forms over K each of degree at most 2 and not both in $K[x^\pi,y^\pi]$, there exists a non-trivial common weak automorph T of g and h. Moreover, if*

$$g = \sum_{i=0}^{2} a_i x^{2-i}y^i, \quad h = \sum_{i=0}^{2} b_i x^{2-i}y^i$$

we can take

$$T = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} K^*, \quad \text{where} \quad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} -a_0b_2+a_2b_0 & -a_1b_2+a_2b_1 \\ a_0b_1-a_1b_0 & a_0b_2-a_2b_0 \end{pmatrix}.$$

Proof. If g,h are both of degree 2 and T is as above we have

$$\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = -R(g,h) \neq 0,$$

where $R(g,h)$ is the resultant of g and h (see [21, p. 219]). Also $\langle \alpha,\beta,\gamma,\delta\rangle = \langle \alpha,0,0,\alpha\rangle$ implies $\pi = 2$, $a_i = b_i = 0$, $g \in K[x^\pi,y^\pi]$, $h \in K[x^\pi,y^\pi]$, contrary to assumption. Moreover

$$g(\alpha x+\beta y,\, \gamma x+\delta y) = R(g,h)g(x,y),$$
$$h(\alpha x+\beta y,\, \gamma x+\delta y) = R(g,h)h(x,y),$$

thus T is a common weak automorph of g and h. The case where one of the forms g,h is linear is reduced to the former by replacing this form by its square.

Proof of Theorem 6. Necessity. By the assumption f is not divisible by y^2, hence $f(x,1)$ is of degree $m \geq n-1 \geq 2$. If $m = 2$ the assertion is trivial, thus assume $m \geq 3$. Let $Z = \{\xi \in \overline{K} \cup \{\infty\} : e_f(\xi) > 0\}$. By Lemma 17, if $T \in \mathrm{Aut}(f,K)$, we have $T^*(Z) = Z$ and since $T^*\infty \in K \cup \{\infty\}$, f has no zeros in K and $T^*(Z \setminus \{\infty\}) = Z \setminus \{\infty\}$. If T is non-trivial, the orbits of $Z \setminus \{\infty\}$ under the action of T^*, say $O_1,\ldots,O_l$, are of lengths greater than 1, since the equation $T^*\xi = \xi$ gives $[K(\xi):K] \leq 2 < m$. They are blocks of imprimitivity of the Galois group $\mathcal{G}$ in question, provided $l > 1$. Indeed, if $\tau \in \mathcal{G}$ and $\xi \in O_i$, $\tau(\xi) \in O_j$, then $\tau(T^*\xi) = T^*\tau(\xi) \in O_j$. If $l = 1$, but m is composite, $m = m_1m_2$, $m_i > 1$, we replace T by T^{m_1} and l by m_1. It remains to consider the case $l = 1$, m a prime. Then $T^* \in \mathcal{G}$. Indeed, since $f(x,1)$ is irreducible, $\mathcal{G}$ is transitive, thus if $f(\xi,1) = 0$ there exists $\tau_0 \in \mathcal{G}$ such that $\tau_0(\xi) = T^*\xi$. It follows that $\tau_0(T^{*i}\xi) = T^{*i}\tau_0(\xi) = T^{*i+1}(\xi)$, hence $\tau_0 = T^*$. Also for every $\tau \in \mathcal{G}$ we have $\tau(\xi) = T^{*j}\xi$ for some j, thus $\tau(T^{*i}\xi) = T^{*i}\tau(\xi) = T^{*i+j}\xi = T^{*j}(T^{*i}\xi)$ for each i, so $\tau = T^{*j}$, hence $\mathcal{G}$ is cyclic, generated by T^*.

Sufficiency for $n \leq 4$. In view of Lemma 31 and the condition $\langle n,m\rangle \neq \langle 4,3\rangle$ it suffices to consider $f(x,1)$ of degree n and monic. Let $n = 3$ and $f(x,1) = x^3+ax^2+bx+c$. Since $\mathcal{G}$ is cyclic there exist d,e,g in K such that $f(\xi,1) = 0$ implies $f(d\xi^2+e\xi+g,1) = 0$

where $\langle d,e,g\rangle \neq \langle 0,0,g\rangle, \langle 0,1,0\rangle$. The system of three linear equations for $\alpha,\beta,\gamma,\delta$,

$$\begin{aligned}(e-ad)\gamma + d\delta &= 0,\\ -\alpha + (g-bd)\gamma + e\delta &= 0,\\ -\beta - cd\gamma + g\delta &= 0,\end{aligned}$$

has a non-zero solution $\langle \alpha,\beta,\gamma,\delta\rangle \in K^4$. This solution satisfies for all zeros ξ of $f(x,1)$ the equation

$$(d\xi^2 + e\xi + g)(\gamma\xi + \delta) = \alpha\xi + \beta.$$

Note that $\gamma\xi+\delta = 0$ would give $\alpha=\beta=\gamma=\delta=0$ since $\xi \notin K$, a contradiction. Hence $\gamma\xi+\delta \neq 0$ and

$$d\xi^2 + e\xi + g = \frac{\alpha\xi+\beta}{\gamma\xi+\delta}.$$

It follows that for some $r \in K$,

$$f\left(\frac{\alpha x+\beta}{\gamma x+\delta}, 1\right)(\gamma x+\delta)^3 = rf(x,1)$$

and

$$f(\alpha x+\beta y,\ \gamma x+\delta y) = rf(x,y).$$

Observe that $\alpha\delta-\beta\gamma = 0$ or $\langle\alpha,\beta,\gamma,\delta\rangle = \langle\alpha,0,0,\alpha\rangle$ would give $d\xi^2+e\xi+g \in K$ or $d\xi^2+e\xi+g=\xi$, contrary to $[K(\xi):K]=3$.

Now, let $n=4$. Since $m=4$, $\mathcal{G}$ is imprimitive. It follows that f is reducible over a separable quadratic extension of K, say $K(\eta)$. Thus we have

$$f = b\Big(\sum_{i=0}^{2} a_i x^{2-i}y^i\Big)\Big(\sum_{i=0}^{2} a_i' x^{2-i}y^i\Big),$$

where $a_i, a_i' \in K(\eta)$ and a_i, a_i' are conjugate over K, while $b \in K$. Applying Lemma 31 with $b_i = a_i'$ we find that the factors of f have a common non-trivial automorph with the matrix

$$M = \begin{pmatrix} -a_0a_2' + a_2a_0' & -a_1a_2' + a_2a_1 \\ a_0a_1' - a_1a_0' & a_0a_2' - a_2a_0' \end{pmatrix},$$

hence also with the matrix $M/(\eta-\eta')$. However, the last matrix is invariant with respect to conjugation, so its elements are in K.

Proof of Corollary 15. This follows at once from Theorem 6 and Corollary 2.

REMARK. The assumption $\zeta \notin K$, where ζ is a primitive cubic root of unity, cannot be omitted in Corollary 15, as the following example shows: $K=\mathbb{Q}(\zeta)$, $T = \left(\begin{smallmatrix}\zeta & 0\\ 0 & 1\end{smallmatrix}\right)K^*$, $f = x(x^3+2y^3)$.

Proof of Corollary 16. By Corollary 1, $\mathrm{Aut}(f,K)$ can contain a cyclic group $\mathfrak{C}_\nu$ for $\nu = 2$ or 3 only. The lengths of the orbits of an arbitrary set under the action of $\mathfrak{D}_2$ are even, hence, by Lemma 17, $\mathrm{Aut}(f,K)$ cannot contain a copy of $\mathfrak{D}_2$. On the other hand, $|\mathrm{Aut}(f,K)| \leq 6$ by Theorem 5. This limits the possible types of $\mathrm{Aut}(f,K)$ to $\mathfrak{D}_3, \mathfrak{C}_3, \mathfrak{C}_2$ and $\mathfrak{C}_1$. If $\mathcal{G} \cong \mathfrak{C}_1$, then f is equivalent over K to $axy(x+y)$ and $\mathrm{Aut}(f,K)$ contains the automorphs $\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)K^*$ and $\left(\begin{smallmatrix}0 & -1\\ 1 & 1\end{smallmatrix}\right)K^*$ of orders 2 and 3, respectively, thus

$\mathrm{Aut}(f,K) \cong \mathfrak{D}_3$. If $\mathcal{G} \cong \mathfrak{C}_2$, then, by Corollary 2, $\mathrm{Aut}(f,K)$ does not contain $\mathfrak{C}_3$ and, by Lemma 31, $\mathrm{Aut}(f,K)$ contains a $\mathfrak{C}_2$, thus $\mathrm{Aut}(f,K) \cong \mathfrak{C}_2$. If $\mathcal{G} \cong \mathfrak{C}_3$, then, by Theorem 6, $\mathrm{Aut}(f,K)$ is non-trivial, while, by Corollary 1, it does not contain $\mathfrak{C}_2$, hence $\mathrm{Aut}(f,K) \cong \mathfrak{C}_3$. Finally, if $\mathcal{G} \cong \mathfrak{D}_3$, then $\mathrm{Aut}(f,K) \cong \mathfrak{C}_1$ by Theorem 6.

5. The case of an algebraically closed field

In this section K is an algebraically closed field of characteristic π, Π is the corresponding prime field and f is a non-singular binary form over K of degree n.

If $n = 3$, then $\mathrm{Aut}(f,K) \cong \mathfrak{D}_3$ by Corollary 16. We shall now consider $n = 4$.

DEFINITION 10. For a form $f(x,y) = \sum_{i=0}^{4} a_i x^{4-i} y^i$ put

$$A(f) = a_2^2 - 3a_1a_3 + 12a_0a_4,$$
$$B(f) = 27a_1^2a_4 + 27a_0a_3^2 + 2a_2^3 - 72a_0a_2a_4 - 9a_1a_2a_3.$$

REMARK. $A(f)$, $B(f)$ are invariants of f and satisfy

$$27D(f) = 4A(f)^3 - B(f)^2,$$

where $D(f)$ is the discriminant of f (see [27, Bd I, §70]).

THEOREM 7. *For a non-singular quartic binary form f over K we have*

$$\mathrm{Aut}(f,K) \cong \begin{cases} \mathfrak{S}_4 & \text{if } A(f) = B(f) = 0, \\ \mathfrak{A}_4 & \text{if } A(f) = 0,\ B(f) \neq 0, \\ \mathfrak{D}_4 & \text{if } A(f) \neq 0,\ B(f) = 0, \\ \mathfrak{D}_2 & \text{if } A(f)B(f) \neq 0. \end{cases}$$

The proof is based on three lemmas.

LEMMA 32. *For a non-singular quartic binary form f over K, $\mathrm{Aut}(f,K)$ contains $\mathfrak{C}_3$ if and only if $A(f) = 0$.*

Proof. Necessity. If $\pi \neq 3$ and the cyclic group in question is generated by $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) K^*$ we have, by Theorem 1,

$$f = \chi_i(a\chi_i^3 + b\chi_{3-i}^3) = a\chi_i^4 + b\chi_i\chi_{3-i}^3,$$

where $i \in \{1,2\}$, χ_1, χ_2 are given in Definition 3 and a, b are in K. Denoting by R_1 the resultant of χ_1, χ_2 and by f_1 the form $ax^4 + bxy^3$ we obtain, by the above Remark,

$$A(f) = R_1^2 A(f_1) = 0.$$

If $\pi = 3$ we have, again by Theorem 1,

$$f = \chi_1(a\chi_1^3 + b(\lambda^2\chi_2^3 - \chi_2\chi_1^2)) = a\chi_1^4 - b\chi_1^3\chi_2 + b\lambda^2\chi_1\chi_2^3,$$

where λ, χ_1, χ_2 are as in Definition 4 and a, b are in K. Denoting by R_2 the resultant of χ_1, χ_2 and by f_2 the form $ax^4 - bx^3y + b\lambda^2xy^3$ we obtain, by the Remark,

$$A(f) = R_2^2 A(f_2) = 0.$$

Sufficiency. The form f is clearly equivalent, by a linear transformation over K, to a form

$$f_3 = xy(x^2 + axy - y^2).$$

The condition $A(f) = 0$ gives $a^2 + 3 = A(f_3) = 0$. If $\pi \neq 3$ we choose a primitive cubic root of unity ϱ and conclude that $a = \pm(\varrho^2 - \varrho)$. Then the transformation $T_2(x, y) = (\varrho^2 x \pm \varrho y, y)$ of order 3 in $\mathrm{PGL}_2(K)$ satisfies $f_3(T_2) = f_3$, hence $\mathrm{Aut}(f, K)$ conjugate to $\mathrm{Aut}(f_3, K)$ contains $\mathfrak{C}_3$.

If $\pi = 3$ the condition $A(f_3) = 0$ gives $a = 0$. Then the transformation $T_2(x, y) = (x+y, y)$ of order 3 in $\mathrm{PGL}_2(K)$ satisfies $f_3(T_2) = f_3$, hence again $\mathrm{Aut}(f, K)$ contains $\mathfrak{C}_3$.

LEMMA 33. *For a non-singular quartic binary form f over K, $\mathrm{Aut}(f, K)$ contains $\mathfrak{C}_4$ if and only if $B(f) = 0$.*

Proof. Necessity. If $\pi = 2$, then by Lemma 1 no element of $\mathrm{PGL}_2(K)$ is of order 4, hence the assumption implies $\pi \neq 2$. If $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) K^*$ is an element of order 4 in $\mathrm{Aut}(f, K)$, then by Theorem 1,

$$f = a\chi_1^4 + b\chi_2^4,$$

where χ_1, χ_2 are given in Definition 3. Denoting by R_3 the resultant of χ_1, χ_2 and by f_4 the form $ax^4 + by^4$ we have, by the Remark,

$$B(f) = R_3^3 B(f_4) = 0.$$

Sufficiency. Since $D(f) \neq 0$ the assumption $B(f) = 0$ implies $\pi \neq 2$ by the Remark. Then (see [11, §13]) f is equivalent, by a linear transformation over K, to a form

$$f_5 = x^4 + mx^2y^2 + y^4, \qquad m \in K.$$

The condition $B(f) = 0$ gives

$$2m^3 - 72m = B(f_5) = 0,$$

hence $m = 0, \pm 6$. But the forms $x^4 \pm 6x^2y^2 + y^4$ are equivalent to $f_6 = x^4 + y^4$, since

$$x^4 + 6x^2y^2 + y^4 = \tfrac{1}{2}(x + y)^4 + \tfrac{1}{2}(x - y)^4,$$
$$x^4 - 6x^2y^2 + y^4 = \tfrac{1}{2}(x + \zeta y)^4 + \tfrac{1}{2}(x - \zeta y)^4,$$

where ζ is a primitive quartic root of unity. On the other hand, the transformation $T_3 = (\zeta x, y)$ of order 4 in $\mathrm{PGL}_2(K)$ satisfies $f_6(T_3) = T_3$, hence $\mathrm{Aut}(f, K)$ conjugate to $\mathrm{Aut}(f_6, K)$ contains $\mathfrak{C}_4$.

LEMMA 34. *For a non-singular quartic binary form f over K, $\mathrm{Aut}(f, K)$ contains $\mathfrak{D}_2$, but no $\mathfrak{D}_2 \times \mathfrak{C}_2$.*

Proof. If $\pi \neq 2$ then by the already quoted result f is equivalent by a linear transformation over K to a form

$$f_5 = x^4 + mx^2y^2 + y^4, \qquad m \in K.$$

The transformations $T_4(x, y) = (y, x)$ and $T_5(x, y) = (-x, y)$ satisfy $T_4^2 = E = T_5^2$, $T_4T_5 = T_5T_4$, $f_5(T_4) = f_5 = f_5(T_5)$, hence $\mathrm{Aut}(f, K)$ conjugate to $\mathrm{Aut}(f_5, K)$ contains $\mathfrak{D}_2$. On the other hand, it contains no $\mathfrak{D}_2 \times \mathfrak{C}_2$, since this group is not on the list given in the proof of Lemma 7.

If $\pi = 2$ then f is equivalent, by a linear transformation over K, to a form

$$f_7 = xy(x+\xi y)(x+\xi^{-1}y), \quad \xi \in K \setminus \{0,1\}.$$

The transformations $T_6(x,y) = (x+\xi y, \xi x + y)$, $T_7(x,y) = (\xi x + y, x + \xi y)$ satisfy $T_6^2 = e = T_7^2$, $T_6T_7 = T_7T_6$, $f_7(T_6) = (\xi+1)^4 f_7 = f_7(T_7)$, hence $\mathrm{Aut}(f,K)$ conjugate to $\mathrm{Aut}(f_7,K)$ contains $\mathfrak{D}_2$. On the other hand, it contains no $\mathfrak{D}_2 \times \mathfrak{C}_2$ by Corollary 11.

Proof of Theorem 7. If $A(f) = B(f) = 0$, then since $D(f) \neq 0$ we have $\pi = 3$ by the Remark. The form f is equivalent, by a linear transformation over K, to a form

$$f_3 = xy(x^2 + axy - y^2)$$

and the condition $A(f) = 0$ implies $a = 0$. Hence $\mathrm{Aut}(f,K) \cong \mathrm{Aut}(f_3,K) \cong \mathrm{PGL}_2(\mathbb{F}_3) \cong \mathfrak{S}_4$ by Theorem 4.

If $A(f)$, $B(f)$ are not both 0, then (46) is not satisfied, hence by Theorem 4 and Lemma 34,

$$|\mathrm{Aut}(f,K)| \text{ divides } 8 \text{ or } 12. \tag{79}$$

If $A(f) = 0$ and $B(f) \neq 0$, then by Lemmas 32–34, $\mathrm{Aut}(f,K)$ contains $\mathfrak{C}_3$ and $\mathfrak{D}_2$, but no $\mathfrak{C}_4$ and no $\mathfrak{D}_2 \times \mathfrak{C}_2$. Hence its 2-Sylow subgroup is $\mathfrak{D}_2$. On the other hand, $\mathrm{Aut}(f,K)$ contains no $\mathfrak{C}_6$ by Theorem 1. Hence, $\mathrm{Aut}(f,K) \cong \mathfrak{A}_4$ by (79).

If $A(f) \neq 0$ and $B(f) = 0$, then by Lemmas 32–34, $\mathrm{Aut}(f,K)$ contains $\mathfrak{C}_4$ and $\mathfrak{D}_2$, but no $\mathfrak{C}_3$ and no $\mathfrak{D}_2 \times \mathfrak{C}_2$. Therefore, by (79), $|\mathrm{Aut}(f,K)| = 8$ and $\mathrm{Aut}(f,K) \cong \mathfrak{D}_4$.

If $A(f)B(f) \neq 0$, then by Lemmas 32–34, $\mathrm{Aut}(f,K)$ contains $\mathfrak{D}_2$, but no $\mathfrak{C}_3$, no $\mathfrak{C}_4$ and no $\mathfrak{D}_2 \times \mathfrak{C}_2$. Therefore, by (79), $|\mathrm{Aut}(f,K)| = 4$ and $\mathrm{Aut}(f,K) \cong \mathfrak{D}_2$.

Now, we proceed to the case $n \geq 5$.

DEFINITION 11. $\mathfrak{F}_n(K)$ is the set of all binary forms f of degree n defined over K such that $\mathrm{Aut}(f,K)$ is non-trivial.

THEOREM 8. *$\mathfrak{F}_n(\mathbb{C})$ is Zariski closed for $n \leq 5$ only.*

LEMMA 35. *$\mathfrak{F}_5(\mathbb{C})$ is Zariski closed.*

Proof. $f \in \mathfrak{F}_5(\mathbb{C})$ if and only if $R = 0$, where R is the Hermite invariant of f of degree 18. Indeed, if $f \in \mathfrak{F}_5(\mathbb{C})$, then, by Theorem 1, f is equivalent over $\mathbb{C}$ to one of the forms

$$x^{5-i}y^i \ (0 \leq i \leq 2), \quad xy(x^3+y^3), \quad x^5+y^5, \tag{80}$$

or

$$x(Ax^4 + Bx^2y^2 + Cy^4). \tag{81}$$

In each case we check in the tables of Faà di Bruno [13, Anhang, Tabelle III, Die irreduciebeln Invarianten IV5] that $R = 0$. To prove the converse, let α be the covariant of f of degree 1 and order 5. If $\alpha = 0$, then according to Clebsch [5, §93], f is either equivalent over $\mathbb{C}$ to one of the forms (80), or has a factor of multiplicity at least three, in which case it has a non-trivial automorph by Lemma 31. If $\alpha \neq 0$, but $R = 0$, then again according to Clebsch [5, §94], f is equivalent over $\mathbb{C}$ to a form (81). It now suffices to apply Theorem 1 in the opposite direction.

LEMMA 36. *For $k \geq 2$ and $n \geq k+3$ we have*

$$f_0(x,y) = x^k \prod_{i=1}^{n-k} (x - iy) \notin \mathfrak{F}_n(\mathbb{C}).$$

Proof. Assuming $f_0(\alpha x + \beta y, \gamma x + \delta y) = f_0(x,y)$ we obtain

$$(\alpha x + \beta y)^k \mid f_0(x,y),$$

hence $k \geq 2$ implies $\beta = 0$ and we have

$$\alpha^k \prod_{i=1}^{n-k} \big((\alpha - i\gamma)x - i\delta y\big) = \prod_{i=1}^{n-k} (x - iy),$$

thus the sequence $\langle (\alpha - i\gamma)/i\delta \rangle_{1 \leq i \leq n-k}$ is a permutation of $\langle 1/i \rangle_{1 \leq i \leq n-k}$. Clearly, $\alpha/\delta, \gamma/\delta \in \mathbb{Q}$ and comparing the maxima and minima in both sequences we obtain

$$\text{for } \alpha/\delta > 0, \quad \frac{\alpha}{\delta} - \frac{\gamma}{\delta} = 1, \quad \frac{\alpha}{\delta(n-k)} - \frac{\gamma}{\delta} = \frac{1}{n-k},$$

$$\text{for } \alpha/\delta < 0, \quad \frac{\alpha}{\delta} - \frac{\gamma}{\delta} = \frac{1}{n-k}, \quad \frac{\alpha}{\delta(n-k)} - \frac{\gamma}{\delta} = 1.$$

In the former case it follows that $\alpha/\delta = 1$, $\gamma/\delta = 0$, thus the automorph is trivial; in the latter case

$$\frac{\alpha}{\delta} = -1, \quad \frac{\gamma}{\delta} = -1 - \frac{1}{n-k},$$

thus comparing the second greatest terms in both sequences we get

$$-\frac{1}{n-k-1} + 1 + \frac{1}{n-k} = \frac{1}{2},$$

which gives $n - k = 2$, contrary to assumption.

LEMMA 37. *For an integer $n \geq 5$ and a real number $t \in (0,1)$ we have $f_t(x,y) \in \mathfrak{F}_n(\mathbb{C})$, where*

$$f_t(x,y) = \begin{cases} \displaystyle\prod_{i=1}^{n/2} (x - iy)\left(x - \frac{2(i-1)t}{i + it - 2t}\, y\right) & \text{if } n \equiv 0 \bmod 2, \\ \displaystyle\prod_{i=1}^{(n-1)/2} (x - iy)\left(x - \frac{it}{i + it - t}\, y\right) & \text{if } n \equiv 1 \bmod 2. \end{cases}$$

Proof. For $t \in (0,1)$ let

$$g(x,y) = \prod_{i=1}^{\lfloor n/2 \rfloor} (x - iy),$$

$$h_t(x,y) = \begin{cases} \displaystyle\prod_{i=1}^{n/2} \left(x - \frac{2(i-1)t}{i + it - 2t}\, y\right) & \text{if } n \equiv 0 \bmod 2, \\ \displaystyle x \prod_{i=1}^{(n-1)/2} \left(x - \frac{it}{i + it - t}\, y\right) & \text{if } n \equiv 1 \bmod 2, \end{cases}$$

$$T(x,y) = \begin{cases} (2tx - 2ty,\ (t+1)x - 2ty) & \text{if } n \equiv 0 \bmod 2, \\ (tx,\ (t+1)x - ty) & \text{if } n \equiv 1 \bmod 2. \end{cases}$$

For $n \equiv 0 \bmod 2$ we have

$$g(T(x,y)) = g(2t, t+1)h_t(x,y), \qquad h_t(T(x,y)) = h_t(2t, t+1)g(x,y),$$

hence

$$f_t(T(x,y)) = f_t(2t, t+1)f_t(x,y)$$

and T is a non-trivial weak automorph of f_t.

Similarly, for $n \equiv 1 \bmod 2$,

$$g(T(x,y)) = g(t, t+1)h_t(x,y), \qquad h_t(T(x,y)) = h_t(t, t+1)g(x,y),$$

hence

$$f_t(T(x,y)) = f_t(t, t+1)f_t(x,y)$$

and T is again a non-trivial weak automorph of f_t.

Proof of Theorem 8. For $n \le 4$, $\mathfrak{F}_n(\mathbb{C})$ consists of all binary forms over $\mathbb{C}$ by Lemma 31; the case $n = 5$ is covered by Lemma 35. Suppose that, for $n \ge 6$, $\mathfrak{F}_n(\mathbb{C})$ is given by the alternative of systems of equations $F_{ij}(a_0, \dots, a_n) = 0$ $(j \in J_i)$. Using Lemma 37 and denoting the coefficients of $f_t(x,y)$ by $a_0(t), \dots, a_n(t)$ we obtain for at least one i_0 and t arbitrarily close to 0,

$$F_{i_0 j}(a_0(t), \dots, a_n(t)) = 0 \qquad (j \in J_{i_0}).$$

Taking the limit as t tends to 0 we obtain

$$F_{i_0 j}(a_0, \dots, a_n) = 0 \qquad (j \in J_{i_0}),$$

where $\sum_{i=0}^{n} a_i x^{n-i} y^i = f_0(x,y)$. Thus by our assumption $f_0 \in \mathfrak{F}_n(\mathbb{C})$, contrary to Lemma 36.

References

[1] I. Berchenko and P. J. Olver, *Symmetries of polynomials*, J. Symbolic Comput. 29 (2000), 485–514.

[2] O. Bolza, *On binary sextics with linear transformations into themselves*, Amer. J. Math. 10 (1887), 47–70.

[3] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, 1966.

[4] A. Choudhry, *A study of certain properties of forms with applications to Diophantine equations*, unpublished manuscript, 2003.

[5] A. Clebsch, *Theorie der binären algebraischen Formen*, Leipzig, 1872.

[6] A. Clebsch e P. Gordan, *Sulla reppresentazione tipica delle forme binarie*, Ann. Mat. Pura Appl. (2) 1 (1867), 23–79.

[7] H. S. M. Coxeter and W. O. J. Moser, *Generators and Relations for Discrete Groups*, 3nd ed., Springer, 1972.

[8] W. J. Curran Sharp, *Solution to Problem 7382 (Mathematics)*, Educational Times 41 (1884).

[9] L. E. Dickson, *An invariantive investigation of irreducible binary modular forms*, Trans. Amer. Math. Soc. 12 (1911), 1–18.

[10] —, *Binary modular groups and their invariants*, Amer. J. Math. 33 (1911), 175–192 or *The Collected Papers*, Vol. 1, Chelsea, 1975, 289–395.

[11] —, *Modern Algebraic Theories*, B. H. Sanborn, 1926.

[12] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, reprint, Dover, 1958.
[13] F. Faà di Bruno, *Einleitung in die Theorie der binären Formen*, Leipzig, 1891.
[14] W. C. Huffman, *Polynomial invariants of finite linear groups of degree two*, Canad. J. Math. 32 (1980), 317–330.
[15] F. Klein, *Ueber binäre Formen mit linearen Transformationen in sich selbst*, Math. Ann. 9 (1875–1876), 183–208 or *Gesammelte Mathematische Abhandlungen*, Bd. II, Springer, 1922, 275–301.
[16] —, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen von fünften Grade*, Leipzig, 1894.
[17] G. Maiasano, *La sestica binaria*, Atti R. Accad. Lincei Mem. (3) 19 (1884), 9–60.
[18] R. C. Mason, *Equations over function fields*, in: Number Theory (Noordvijkerhout, 1983), Lecture Notes in Math. 1068, Springer, 1984, 149–157.
[19] P. J. Olver, *Classical Invariant Theory*, Cambridge Univ. Press, 1999.
[20] M. O'Ryan, *On the similarity group of forms of higher degree*, J. Algebra 168 (1999), 968–980.
[21] O. Perron, *Algebra*, Band I, de Gruyter, 1927.
[22] B. Segre, *Equivalenza ed automorfismi delle forme binarie in un dato anello o campo numerico*, Univ. Nac. Tucuman Revista 4 (1946), 7–67.
[23] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), 259–331 or *Oeuvres* (Collected Papers), Vol. 3, Springer, 1986, 1–73.
[24] L. Summerer, *Decomposable forms and automorphisms*, J. Number Theory 99 (2003), 232–254.
[25] —, *Automorphisms of binary forms*, preprint, 2004.
[26] B. L. van der Waerden, *Algebra*, *Zweiter Teil*, 5th ed., Springer, 1967.
[27] H. Weber, *Lehrbuch der Algebra*, reprint, Chelsea, 1961.