# On Reconstructing Configurations of Points in $\mathbb{P}^2$ from a Joint Distribution of Invariants

Mireille Boutin and Gregor Kemper

April 5, 2004

### Abstract

Consider the diagonal action of the projective group $\mathrm{PGL}_3$ on $n$ copies of $\mathbb{P}^2$. In addition, consider the action of the symmetric group $\Sigma_n$ by permuting the copies. In this paper we find a set of generators for the invariant field of the combined group $\Sigma_n \times \mathrm{PGL}_3$. As the main application, we obtain a reconstruction principle for point configurations in $\mathbb{P}^2$ from their sub-configurations of five points. Finally, we address the question of how such reconstruction principles pass down to subgroups.

## Introduction

Consider the problem of recognizing a flat object from its shadow. This is a common problem in computer vision where one often represents objects by the boundary of their image on a picture. For simplicity, assume that the flat object is represented by a finite set of points $p_1, \ldots, p_n \in \mathbb{R}^3$. Rotations and translations of such a flat object in $\mathbb{R}^3$ (almost always) induce a transformation of the image points $P_1, \ldots, P_n \in \mathbb{R}^2$ which can be written as

$$P_i \mapsto \frac{\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} P_i + \begin{pmatrix} a_{13} \\ a_{23} \end{pmatrix}}{(a_{31}, a_{32})P_i + a_{33}}, \text{ for all } i = 1, \ldots, n, \text{ with } \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \in GL(3) \quad (0.1)$$

(where of course we have to assume that the above denominator does not vanish). In the computer vision community, this group action is called the projective group action $(PGL_3(\mathbb{R}) = GL_3(\mathbb{R})/\mathbb{R}^*)$ and plays an important role in many applications.

In order to be able to recognize a flat object from its shadow, we thus need to be able to determine whether two sets of $n$ points in the plane lie in the same orbit under the simultaneous action of the projective group on each of the points. More precisely, given $P_1, \ldots, P_n \in \mathbb{R}^2$ and $Q_1, \ldots, Q_n \in \mathbb{R}^2$, we need to be able to determine whether there exists a projective transformation $g \in PGL_3(\mathbb{R})$ such that $g(P_i) = Q_i$, for all $i = 1, \ldots, n$. However, in many applications, the point correspondence between the two objects is unknown: a priori, we ignore which point is going to be mapped to which. So, more generally, given any $P_1, \ldots, P_n$ and $Q_1, \ldots, Q_n \in \mathbb{R}^2$, we need to be able to determine whether there exists a permutation $\pi \in \Sigma_n$ and a projective transformation $g \in PGL_3(\mathbb{R})$ such that $g(P_i) = Q_{\pi(i)}$, for all $i = 1, \ldots, n$.

In an earlier publication [2], we considered the analogue problem with the Euclidean group $AO(2)$, which is a subgroup of the projective group. More precisely, we considered those projective transformations whose matrix is given by

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ 0 & 0 & 1 \end{pmatrix}, \text{ with } \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathrm{O}(2),$$

where O denotes the orthogonal group.

The squared distances $d_{i,j} = < P_i - P_j, P_i - P_j >$ are invariants under the Euclidean group action, i.e. they remain unchanged when $P_i$ and $P_j$ are replaced by $g(P_i)$ and $g(P_j)$ respectively, for any $g \in \mathrm{AO}(2)$. Given $P_1, \ldots, P_n \in \mathbb{R}^2$ and $Q_1, \ldots, Q_n \in \mathbb{R}^2$, it is a well known fact that $< P_i - P_j, P_i - P_j > = < Q_i - Q_j, Q_i - Q_j >$ for every $i, j = 1, \ldots, n$ if and only if there exists a Euclidean transformation mapping $P_i$ to $Q_i$, for every $i = 1, \ldots, n$. In order to take care of the labeling ambiguity, we have tried to compare the *distribution* of the pairwise distances of each point configurations, i.e. the number of times each value of the distances occurs. Although there exist $P_1, \ldots, P_n \in \mathbb{R}^2$ and $Q_1, \ldots, Q_n \in \mathbb{R}^2$ which have the same distribution of distances but are not the same up to a relabeling of the point and a Euclidean transformation, such examples are fairly rare. In fact, we have shown that there exists a non-zero polynomial $f$ in $2n$ variables such that if $f(P_1, \ldots, P_n) \neq 0$, then the point configuration $P_1, \ldots, P_n$ is uniquely determined up to a Euclidean transformation and a relabeling. In other words, if $f(P_1, \ldots, P_n) \neq 0$, then for any $Q_1, \ldots, Q_n \in \mathbb{R}^2$ with the same distribution of distances as $P_1, \ldots, P_n$, there exists a relabeling $\pi \in \Sigma_n$ and a Euclidean transformation $g \in \mathrm{AO}(2)$ such that $g(P_i) = Q_{\pi(i)}$, for every $i = 1, \ldots, n$.

In [2], we also considered the group of area preserving affine transformations, which consists of those matrices

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ 0 & 0 & 1 \end{pmatrix} \text{ with } \left| \begin{array}{cc} a_{11} & a_{12} \\ a_{21} & a_{22} \end{array} \right| = \pm 1.$$

In that case, we looked at the distribution of the triangular areas $\Delta_{i_1 i_2 i_3} = \frac{1}{2} |(P_{i_2} - P_{i_1}) \times (P_{i_3} - P_{i_1})|$, for every distinct $i_1, i_2, i_3 \in \{1, \ldots, n\}$. Obviously, areas remain unchanged under any area-preserving affine transformation. In a similar manner as with the Euclidean group, we were able to show that there exists a non-zero polynomial $f$ in $2n$ variables such that if $f(P_1, \ldots, P_n) \neq 0$, then $P_1, \ldots, P_n$ is uniquely determined, up to a relabeling and an area preserving linear transformation, by the distribution of its triangular areas. In other words, there exists a Zariski-open set of point configurations $(P_1, \ldots, P_n) \in (\mathbb{R}^2)^n$ which are completely determined, up to an area-preserving affine transformation and a relabeling, by the distribution of the triangular areas between the $P_i's$.

We are now ready to attack the general case of a projective transformation on $\mathbb{P}^2(\mathbb{R})$. In fact, everything we are about to say holds for the more general case of the projective group $PGL_3(K)$ acting on the two-dimensional projective space $\mathbb{P}^2(K)$ for any infinite field $K$. In this context, the action given in (0.1) corresponds to the action on the subsets of projective points of the form $(x : y : 1)$. In Section 1, we start by obtaining a generating set of invariants for the diagonal (= simultaneous) action of the projective group on $n$ copies of $\mathbb{P}^2(K)$. Some of these invariants turn out to be redundant and we obtain a full set of relationships between them. These relationships will be used over and over in the following. In classical invariant theory, a theorem giving a full generating set of invariants of some group $G$ acting diagonally on $n$ copies of the natural representation is often called the *first fundamental theorem* for that group $G$, and then a theorem giving all relations between the generators is called the *second fundamental theorem*. The generating set we give has already appeared in Olver [5], but the determination of the relations is, to the best of our knowledge, new. In Section 2, we consider the case $n = 5$ and take the action of the symmetric group $\Sigma_5$ into account. We find two invariants $a$ and $b$ which generate the invariant field $K \left( \left( \mathbb{P}^2(K) \right)^5 \right)^{\Sigma_5 \times \mathrm{PGL}_3}$. This is a crucial step toward the case of general $n$, which we attack in Section 3. In that section, we find a generating set of the field of invariants of $\Sigma_n$ and $\mathrm{PGL}_3(K)$. In particular, given $P_1, \ldots, P_n \in \mathbb{P}^2(K)$, we consider the joint distribution of the $a$'s and $b$'s evaluated at every $P_{i_1}, P_{i_2}, P_{i_3}, P_{i_4}, P_{i_5} \in \{P_1, \ldots, P_n\}$, with $i_1, i_2, i_3, i_4, i_5$ distinct. The final result (Corollary 3.5) of Section 3 states that there exists a Zariski open subset $\Omega$ of $\left( \mathbb{P}^2(K) \right)^n$ such that any $(P_1, \ldots, P_n) \in \Omega$ is completely determined, up to a projective transformation and a relabeling of the points, by the joint distribution of the $a$'s and $b$'s.

Note that in this paper and in [2] the general approach to reconstructing objects (modulo group

actions) is to consider the distribution of specified sub-objects (e.g., triangles, pentagons). In the final section of the paper, we formalize and generalize this approach. Then we prove a theorem which under rather mild hypotheses allows to transport this approach from one group to an arbitrary subgroup. Combining this with Corollary 3.5 and with the results from [2], we obtain reconstruction theorems for arbitrary subgroups of $\mathrm{PGL}_3$ and of area preserving transformations.

# 1   The first and second fundamental theorem for $\mathrm{PGL}_3$

The main goal of this section is to prove what in classical invariant theory would be termed the first and second fundamental theorem for $\mathrm{PGL}_3$.

Let $K$ be any infinite field. We write $\mathbb{P}^2 = \mathbb{P}^2(K)$ for the two-dimensional projective space, and $\mathrm{PGL}_3 = \mathrm{PGL}_3(K) = \mathrm{GL}_3(K)/K^*$ for the projective group acting on $\mathbb{P}^2$. Points from $\mathbb{P}^2$ are given by their homogeneous coordinates $(\alpha_1 : \alpha_2 : \alpha_3)$ with $\alpha_i \in K$ not all zero. The first lemma is an elementary fact from projective geometry.

**Lemma 1.1.** *Let $P_1, \ldots, P_4 \in \mathbb{P}^2$ be four projective points such that no three of them are collinear. Then there exists $g \in \mathrm{PGL}_3$ such that*

$$g(P_1) = (1 : 0 : 0), \quad g(P_2) = (0 : 1 : 0), \quad g(P_3) = (0 : 0 : 1), \quad \text{and} \quad g(P_4) = (1 : 1 : 1).$$

*This $g$ is unique.*

*Proof.* For each point $P_i$ take a representative $v_i \in K^3$. Since $v_1$, $v_2$, and $v_3$ are linearly independent, we have

$$v_3 = \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3$$

with $\alpha_i \in K$. Since no three of the $P_i$ are collinear, all $\alpha_i$ are non-zero. Thus we can choose the $v_i$ in such a way that $\alpha_i = 1$ for all $i$. There exists a $\varphi \in \mathrm{GL}_3(K)$ such that

$$\varphi(v_1) = (1, 0, 0), \quad \varphi(v_2) = (0, 1, 0), \quad \text{and} \quad \varphi(v_3) = (0, 0, 1).$$

Now $v_4 = v_1 + v_2 + v_3$ implies $\varphi(v_4) = (1, 1, 1)$. This proves the existence of $g \in \mathrm{PGL}_3$ with the claimed properties.

To prove the uniqueness of $g$ assume we have $\psi \in \mathrm{GL}_3(K)$ with

$$\psi(v_1) = \beta_1 \cdot (1, 0, 0), \quad \psi(v_2) = \beta_2 \cdot (0, 1, 0), \quad \psi(v_3) = \beta_3 \cdot (0, 0, 1), \quad \text{and} \quad \psi(v_4) = \beta_4 \cdot (1, 1, 1),$$

where $\beta_i \in K \setminus \{0\}$ for all $i$. Then $v_1 + v_2 + v_3 = v_4$ implies $(\beta_1, \beta_2, \beta_3) = (\beta_4, \beta_4, \beta_4)$, so all $\beta$'s are equal, and $\psi = \beta_1 \cdot \varphi$. Therefore $\psi$ and $\varphi$ define the same element in $\mathrm{PGL}_3$, which proves uniqueness. $\square$

Following Olver [5], we describe rational invariants of $n$ projective points. So let $n$ be a positive integer and take $3n$ indeterminates $x_{i,j}$ ($i \in \{1, \ldots, n\}$, $j \in \{0, 1, 2\}$). We write $K(\underline{x})$ for the field of rational functions in the $x_{i,j}$, and

$$K(\underline{x})_0 := K\left(\frac{x_{1,1}}{x_{1,0}}, \ldots, \frac{x_{n,1}}{x_{n,0}}, \frac{x_{1,2}}{x_{1,0}}, \ldots, \frac{x_{n,2}}{x_{n,0}}\right),$$

which is the function field on $\left(\mathbb{P}^2(K)\right)^n$. Alternatively, $K(\underline{x})_0$ can be defined as the field of all rational functions $f \in K(\underline{x})$ where for each $i \in \{1, \ldots, n\}$ the numerator and the denominator of $f$

are homogeneous as polynomials in $x_{i,0}$, $x_{i,1}$, $x_{i,2}$, and of the same degree. We have a diagonal action of $\mathrm{PGL}_3$ on $\left(\mathbb{P}^2\right)^n$, which induces an action on the function field $K(\underline{x})_0$ by $g(f) = f \circ g^{-1}$. For indices $i_0, i_1, i_2 \in \{1, \ldots, n\}$ define the "bracket"

$$[i_0, i_1, i_2] := \det\left(x_{i_\nu, \mu}\right)_{\nu, \mu = 0,1,2} \in K(\underline{x}),$$

and for $i, j, k, l, m \in \{1, \ldots, n\}$ pairwise distinct define

$$c_{i,j,k,l,m} := \frac{[i,j,k][i,l,m]}{[i,j,l][i,k,m]} \in K(\underline{x})_0. \tag{1.1}$$

It is easy to see that the $c_{i,j,k,l,m}$ are $\mathrm{PGL}_3$-invariants. We write

$$K(\underline{x})_0^{\mathrm{PGL}_3(K)} = \{f \in K(\underline{x})_0 \mid g(f) = f \text{ for all } g \in \mathrm{PGL}_3(K)\}$$

for the field of all $\mathrm{PGL}_3$-invariants. The first part of the following theorem already appeared in Olver [5] (though his statement is slightly different).

**Theorem 1.2.** *With the above notation we have*

(a) *(First fundamental theorem for $\mathrm{PGL}_3$.) The $c_{i,j,k,l,m}$ generate the field of $\mathrm{PGL}_3$-invariants, i.e.,*

$$K(\underline{x})_0^{\mathrm{PGL}_3(K)} = K\left(c_{i,j,k,l,m} \mid i, j, k, l, m \in \{1, \ldots, n\} \text{ pairwise distinct}\right).$$

(b) *The $c_{i,j,k,l,m}$ separate $\mathrm{PGL}_3$-orbits on a dense open subset of $\left(\mathbb{P}^2\right)^n$. More precisely, let $P_1, \ldots, P_n \in \mathbb{P}^2(K)$ be points such that no three of them are collinear, and let $Q_1, \ldots, Q_n \in \mathbb{P}^2(K)$ be further points such that*

$$c_{i,j,k,l,m}(P_1, \ldots, P_n) = c_{i,j,k,l,m}(Q_1, \ldots, Q_n)$$

*for all $i, j, k, l, m \in \{1, \ldots, n\}$ pairwise distinct (implying that no zero-division occurs when evaluating the $c_{i,j,k,l,m}$ at $Q_1, \ldots, Q_n$), then there exists $g \in \mathrm{PGL}_3(K)$ such that*

$$g(P_i) = Q_i$$

*for all $i \in \{1, \ldots, n\}$.*

*Proof.* Let $d \in K[\underline{x}]$ be the product of all $[i, j, k]$ with $1 \leq i < j < k \leq n$. For $P_1, \ldots, P_n \in \mathbb{P}^2(K)$ with homogeneous coordinates $P_i = (\xi_{i,0} : \xi_{i,1} : \xi_{i,2})$, we have that no three of the $P_i$ are collinear if and only if $d(\underline{\xi}) \neq 0$.

We first treat the case $n \leq 4$. By Lemma 1.1, all $(P_1, \ldots, P_n) \in \left(\mathbb{P}^2\right)^n$ where $d$ takes a non-zero value lie in one single $\mathrm{PGL}_3$-orbit. Hence every invariant $f \in K(\underline{x})_0^{\mathrm{PGL}_3(K)}$ is constant on the set of all these $(P_1, \ldots, P_n)$. By Lemma 1.3 (which is proved after this lemma), $f$ is constant. This proves (a) and (b) of the lemma.

Now assume $n \geq 5$ and consider the subset

$$T := \left\{(P_1, \ldots, P_n) \in \left(\mathbb{P}^2(K)\right)^n \mid P_1 = (1:0:0), P_2 = (0:1:0), P_3 = (0:0:1), P_4 = (1:1:1)\right\}$$

of $\left(\mathbb{P}^2(K)\right)^n$. Lemma 1.1 implies that the set $\mathrm{PGL}_3 \cdot T := \{g(\underline{P}) \mid g \in \mathrm{PGL}_3(K), (\underline{P}) \in T\}$ contains all $(P_1, \ldots, P_n) \in \left(\mathbb{P}^2(K)\right)^n$ such that no three of $P_1$, $P_2$, $P_3$, and $P_4$ are collinear, so in particular $\mathrm{PGL}_3 \cdot T$ contains all $(P_1, \ldots, P_n)$ where $d$ takes a non-zero value. Thus Lemma 1.3 implies:

If two rational functions coincide on $\mathrm{PGL}_3 \cdot T$, they coincide as rational functions. (1.2)

To prove (a), take $0 \neq f \in K(\underline{x})_0^{\mathrm{PGL}_3(K)}$. Being a rational function in the $x_{i,j}$, $f$ can be written as $f = a/b$ with $a, b \in K[x_{i,j} \mid i \in \{1, \ldots, n\}, j \in \{0, 1, 2\}]$ coprime. It is easy to see that for each

$i \in \{1, \ldots, n\}$, $a$ and $b$ are homogeneous as polynomials in $x_{i,0}$, $x_{i,1}$, and $x_{i,2}$. Indeed, for $\alpha \in K$, let $\varphi_{i,\alpha}$ be the $K$-automorphism of $K(\underline{x})$ which sends $x_{i,\nu}$ to $\alpha \cdot x_{i,\nu}$ and $x_{j,\nu}$ to itself for $j \neq i$. Then $f \in K(\underline{x})_0$ implies that $\varphi_{i,\alpha}(a)/\varphi_{i,\alpha}(b) = \varphi_{i,\alpha}(f) = f = a/b$, so

$$b\varphi_{i,\alpha}(a) = \varphi_{i,\alpha}(b)a.$$

By the coprimality of $a$ and $b$ this implies that $b$ divides $\varphi_{i,\alpha}(b)$. Since $\varphi_{i,\alpha}(b)$ and $b$ contain the same monomials, this means that $\varphi_{i,\alpha}(b)$ is a scalar multiple of $b$. Thus $b$ is homogeneous as a polynomial in $x_{i,0}$, $x_{i,1}$, and $x_{i,2}$. The same argument works for $a$. Thus for a vector $(v_1, \ldots, v_n) \in \left(K^3 \setminus \{0\}\right)^n$, whether or not $b(v_1, \ldots, v_n)$ is 0 depends only on the class of $(v_1, \ldots, v_n)$ in $\left(\mathbb{P}^2(K)\right)^n$. So we can write $Z$ for the vanishing set of $b$ *as a subset of* $\left(\mathbb{P}^2(K)\right)^n$. By way of contradiction, assume that $T \subseteq Z$. For $\varphi \in \mathrm{GL}_3(K)$, the $\mathrm{PGL}_3$-invariance of $f$ implies $\varphi(a)/\varphi(b) = a/b$, hence

$$b\varphi(a) = \varphi(b)a.$$

By the coprimality of $a$ and $b$ this implies that $b$ divides $\varphi(b)$, so if $b$ vanishes at a point $(v_1, \ldots, v_n) \in \left(K^3\right)^n$, then $b$ also vanishes at $\left(\varphi^{-1}(v_1), \ldots, \varphi^{-1}(v_n)\right)$ for all $\varphi \in \mathrm{GL}_3(K)$. Therefore the assumption $T \subseteq Z$ implies that $\mathrm{PGL}_3 \cdot T \subseteq Z$. Now (1.2) implies the contradiction $b = 0$.

Having seen that $b$ does not vanish identically on $T$, we may define the restriction of $f$ on $T$ and obtain a rational function on $T$:

$$f|_T = F\left(\frac{x_{5,1}}{x_{5,0}}, \ldots, \frac{x_{n,1}}{x_{n,0}}, \frac{x_{5,2}}{x_{5,0}}, \ldots, \frac{x_{n,2}}{x_{n,0}}\right),$$

with $F$ a rational function in $2(n-4)$ arguments. Remembering the definition of the $c_{i,j,k,l,m}$ and evaluating them on $T$ yields for $i > 4$:

$$c_{3,2,4,i,1}|_T = x_{i,1}/x_{i,0} \quad \text{and} \quad c_{2,3,4,i,1}|_T = x_{i,2}/x_{i,0}. \tag{1.3}$$

Hence

$$f|_T = F\left(c_{3,2,4,5,1}, \ldots, c_{3,2,4,n,1}, c_{2,3,4,5,1}, \ldots, c_{2,3,4,n,1}\right)|_T.$$

So $f$ and $F\left(c_{3,2,4,5,1}, \ldots, c_{3,2,4,n,1}, c_{2,3,4,5,1}, \ldots, c_{2,3,4,n,1}\right)$ are two functions in $K(\underline{x})_0^{\mathrm{PGL}_3(K)}$ which coincide on $T$, hence they also coincide on $\mathrm{PGL}_3 \cdot T$. Now (1.2) implies that these functions coincide as elements of $K(\underline{x})$. This proves (a).

After these preparations, the proof of (b) is easy. First, the hypothesis that none of the denominators vanish when evaluating the $c_{i,j,k,l,m}$ at $(Q_1, \ldots, Q_n)$ implies that, as for the $P_i$, no three of the $Q_i$ are collinear. Thus by Lemma 1.1 there exist $\varphi_1, \varphi_2 \in \mathrm{PGL}_3(K)$ such that

$$(\varphi_1(P_1), \ldots, \varphi_1(P_n)) \in T \quad \text{and} \quad (\varphi_2(Q_1), \ldots, \varphi_2(Q_n)) \in T.$$

The hypothesis in (b) and the invariance of the $c_{i,j,k,l,m}$ imply that

$$c_{i,j,k,l,m}(\varphi_1(P_1), \ldots, \varphi_1(P_n)) = c_{i,j,k,l,m}(\varphi_2(Q_1), \ldots, \varphi_2(Q_n)).$$

Now (1.3) implies that $\varphi_1(P_i) = \varphi_2(Q_i)$ for $i \geq 5$. But for $i \leq 4$ this also holds by the definition of $T$. This completes the proof of (b). $\qquad \square$

The previous proof used the following elementary fact.

**Lemma 1.3.** *Let $f, g \in K(x_1, \ldots, x_m)$ be rational functions in $m$ indeterminates over the infinite field $K$, and let $h \in K[x_1, \ldots, x_m] \setminus \{0\}$ be a non-zero polynomial. If*

$$f(\xi_1, \ldots, \xi_m) = g(\xi_1, \ldots, \xi_m)$$

*for all $\xi_1, \ldots, \xi_m \in K$ such that $h(\xi_1, \ldots, \xi_m) \neq 0$ and the evaluations of $f$ and $g$ at $(\xi_1, \ldots, \xi_m)$ are defined, then $f = g$ (as rational functions).*

*Proof.* After subtracting $g$ from $f$ we may assume that $g = 0$. Next we multiply $h$ by the denominator of $f$, which does not change the hypothesis of the lemma. But now we can also multiply $f$ by its denominator, so we may assume $f \in K[x_1, \ldots, x_m]$. We use induction on $m$. By way of contradiction, assume that $f \neq 0$. Since $K$ is infinite, there exists $\xi_m \in K$ such that $f_1 := f(x_1, \ldots, x_{m-1}, \xi_m) \in K[x_1, \ldots, x_{m-1}]$ is non-zero, and the same for $h_1 := h(x_1, \ldots, x_{m-1}, \xi_m)$. If $m = 1$, this is an immediate contradiction to the hypothesis. If $m > 1$, we obtain a contradiction by induction. $\square$

A major step in our argument is the study of relations between the $c_{i,j,k,l,m}$. Let $P_0$ be a polynomial ring over $K$ with indeterminates $C_{i,j,k,l,m}$ for $i, j, k, l, m \in \{1, \ldots, n\}$ pairwise distinct. Consider the homomorphism

$$\Phi \colon P_0 \to K(\underline{x})_0^{\mathrm{PGL}_3(K)}, \; C_{i,j,k,l,m} \mapsto c_{i,j,k,l,m},$$

and let $I_0 \subseteq P_0$ be the kernel of $\Phi$. Thus $I_0$ is the ideal of relations between the $c_{i,j,k,l,m}$.

**Theorem 1.4** (Second fundamental theorem for $\mathrm{PGL}_3$). *The ideal $I_0$ is generated by the following relations:*

$$\begin{aligned}
& C_{i,j,k,l,m} - C_{i,k,j,m,l}, \\
& C_{i,j,k,l,m} - C_{i,l,m,j,k}, \\
& C_{i,j,k,l,m} - C_{i,m,l,k,j},
\end{aligned} \tag{1.4}$$

$$C_{i,j,k,l,m} \cdot C_{i,j,l,k,m} - 1, \tag{1.5}$$

$$C_{i,j,k,l,m} + C_{i,j,m,l,k} - 1, \tag{1.6}$$

$$C_{i,j,k,l,m} - C_{m,j,k,l,i} \cdot C_{j,i,k,l,m}, \tag{1.7}$$

$$C_{i,j,k,l,m} - C_{i,r,k,l,m} \cdot C_{i,j,k,l,r}, \tag{1.8}$$

*where* (1.4)–(1.7) *are for all* $i, j, k, l, m \in \{1, \ldots, n\}$ *pairwise distinct, and* (1.8) *is for all* $i, j, k, l, m, r \in \{1, \ldots, n\}$ *pairwise distinct.*

*Proof.* We first check that the relations given in (1.4)–(1.8) lie in $I_0$. For (1.4) and (1.5), this is immediately seen from the definition of the $c_{i,j,k,l,m}$. For (1.6), observe that

$$c_{i,j,k,l,m} + c_{i,j,m,l,k} - 1 = \frac{[i,j,k][i,l,m] - [i,j,m][i,l,k] - [i,j,l][i,k,m]}{[i,j,l][i,k,m]}.$$

The numerator is a function of five vectors $v_i, v_j, v_k, v_l, v_m \in K^3$. Fixing $v_i$, we see that the numerator is an alternating bilinear form in the arguments $v_j, v_k, v_l, v_m$. But an alternating bilinear form in four three-dimensional vectors has to be zero, hence the relation (1.6). Next we check (1.7) and (1.8):

$$c_{m,j,k,l,i} \cdot c_{j,i,k,l,m} = \frac{[m,j,k][m,l,i][j,i,k][j,l,m]}{[m,j,l][m,k,i][j,i,l][j,k,m]} = c_{i,j,k,l,m},$$

and

$$c_{i,r,k,l,m} \cdot c_{i,j,k,l,r} = \frac{[i,r,k][i,l,m][i,j,k][i,l,r]}{[i,r,l][i,k,m][i,j,l][i,k,r]} = c_{i,j,k,l,m}.$$

Let $I \subseteq P_0$ be the ideal generated by the relations (1.4)–(1.8), so $I \subseteq I_0$. We need to show the reverse inclusion $I_0 \subseteq I$. To this end, let $R := P_0/I$ be the residue class ring, and for $i, j, k, l, m \in$

$\{1, \ldots, n\}$ distinct, write $\overline{C}_{i,j,k,l,m} := C_{i,j,k,l,m} + I \in R$ for the residue class of $C_{i,j,k,l,m}$. It follows from (1.5) that $\overline{C}_{i,j,k,l,m}$ is invertible in $R$, i.e.

$$\overline{C}_{i,j,k,l,m} \in R^{\times}, \tag{1.9}$$

where $R^{\times}$ denotes the group of units in $R$. Consider the $K$-subalgebra $R_0 \subseteq R$ generated by all $\overline{C}_{2,3,4,i,1}$ and $\overline{C}_{3,2,4,i,1}$ for $i \in \{5, \ldots, n\}$. Moreover, set $S := R_0 \cap R^{\times}$ and

$$R_1 := S^{-1} R_0 \subseteq R.$$

We claim that $R_1 = R$, so we need to prove that for all $i, j, k, l, m \in \{1, \ldots, n\}$ pairwise distinct $\overline{C}_{i,j,k,l,m}$ lies in $R_1$. For this purpose we first remark that if there exists a permutation $\pi$ of the set $\{j, k, l, m\}$ such that $\overline{C}_{i,\pi(j),\pi(k),\pi(l),\pi(m)} \in R_1$, then also $\overline{C}_{i,j,k,l,m} \in R_1$. Before giving the proof, we summarize the claim by stating

$$\exists\, \pi \in \Sigma_{\{j,k,l,m\}} : \ \overline{C}_{i,\pi(j),\pi(k),\pi(l),\pi(m)} \in R_1 \quad \Rightarrow \quad \overline{C}_{i,j,k,l,m} \in R_1, \tag{1.10}$$

where $\Sigma$ denotes the symmetric group. Indeed, if $\pi$ is the permutation given by $j \mapsto k$, $k \mapsto j$, $l \mapsto m$, and $m \mapsto l$, then (1.10) follows directly from (1.4). The same is true if $\pi$ exchanges $j$ with $l$ and $k$ with $m$. Furthermore, if $\pi$ is given by $j \mapsto j$, $k \mapsto m$, $l \mapsto l$, and $m \mapsto k$, then

$$\overline{C}_{i,j,k,l,m} = 1 - \overline{C}_{i,j,m,l,k} = 1 - \overline{C}_{i,\pi(j),\pi(k),\pi(l),\pi(m)}$$

by (1.6), so (1.10) holds for this $\pi$, too. Finally, if $\pi$ is given by $j \mapsto j$, $k \mapsto l$, $l \mapsto k$, and $m \mapsto m$, then

$$\overline{C}_{i,j,k,l,m} = \overline{C}_{i,j,l,k,m}^{-1} = \overline{C}_{i,\pi(j),\pi(k),\pi(l),\pi(m)}^{-1}$$

by (1.5). If $\overline{C}_{i,\pi(j),\pi(k),\pi(l),\pi(m)} \in R_1$, then $\overline{C}_{i,\pi(j),\pi(k),\pi(l),\pi(m)} = f/g$ with $f \in R_0$ and $g \in S$, so

$$f = g \cdot \overline{C}_{i,\pi(j),\pi(k),\pi(l),\pi(m)} \in R^{\times} \cap R_0 = S$$

by (1.9). Thus $\overline{C}_{i,j,k,l,m} = g/f \in R_1$, so (1.10) holds for this $\pi$, too. But the four particular $\pi$'s considered so far generate the symmetric group $\Sigma_{\{j,k,l,m\}}$, so (1.10) follows in general.

Now we prove that $\overline{C}_{i,j,k,l,m} \in R_1$ for all $i, j, k, l, m \in \{1, \ldots, n\}$ distinct. If $2 \notin \{i, j, k, l, m\}$, then

$$\overline{C}_{i,j,k,l,m} = \overline{C}_{i,2,k,l,m} \cdot \overline{C}_{i,j,k,l,2}$$

by (1.8). Thus we are done if we can show that all $\overline{C}_{i,j,k,l,m}$ with $2 \in \{i, j, k, l, m\}$ lie in $R_1$. In other words, we may assume that $2 \in \{i, j, k, l, m\}$. By (1.10) we may even assume that $i = 2$ or $k = 2$. Furthermore, if $3 \notin \{i, j, k, l, m\}$, then

$$\overline{C}_{i,j,k,l,m} = \overline{C}_{i,3,k,l,m} \cdot \overline{C}_{i,j,k,l,3}$$

by (1.8), so we may assume that $3 \in \{i, j, k, l, m\}$ (preserving $i = 2$ or $k = 2$). If $i \neq 2$ and $i \neq 3$, we may assume $j = 2$ and $m = 3$ by using (1.10). Then

$$\overline{C}_{i,j,k,l,m} = \overline{C}_{i,2,k,l,3} = \overline{C}_{3,2,k,l,i} \cdot \overline{C}_{2,i,k,l,3}$$

by (1.7). This means that we may assume $i = 2$ or $i = 3$ and, moreover (using (1.10)) that $\{i, k\} = \{2, 3\}$. Now if $1 \notin \{j, k, l, m\}$, then

$$\overline{C}_{i,j,k,l,m} = \overline{C}_{i,1,k,l,m} \cdot \overline{C}_{i,j,k,l,1}$$

by (1.7), so after all we may assume $1 \in \{j, k, l, m\}$. Using (1.10) again, we can achieve $\{i, k, l\} = \{1, 2, 3\}$. If $4 \notin \{j, m\}$ then

$$\overline{C}_{i,j,k,l,m} = \overline{C}_{i,4,k,l,m} \cdot \overline{C}_{i,j,k,l,4}$$

by (1.8), so we may assume $4 \in \{j, k, l, m\}$. Using (1.10) again, we obtain $(i, j, k, l, m) = (2, 3, 4, l, 1)$ or $(i, j, k, l, m) = (3, 2, 4, l, 1)$. Thus $\overline{C}_{i,j,k,l,m}$ lies in $R_1$ as claimed, which completes the proof that $R_1 = R$.

We still need to prove that $I_0 \subseteq I$, so take $f \in I_0$. We have $f + I \in R = R_1$, so there exist polynomials $g, h \in P$ involving only the indeterminates $C_{2,3,4,i,1}$ and $C_{3,2,4,i,1}$ $(i \in \{5, \ldots, n\})$ such that $hf - g \in I$ and $h + I \in R^{\times}$. Since $f \in I_0$ we obtain

$$\Phi(g) = \Phi(h) \cdot \Phi(f) = 0. \tag{1.11}$$

Consider the subset $T_0 \in \left(\mathbb{P}^2(K)\right)^n$ consisting of all those $(P_1, \ldots, P_n) \in \left(\mathbb{P}^2(K)\right)^n$ with $P_1 = (1 : 0 : 0)$, $P_2 = (0 : 1 : 0)$, $P_3 = (0 : 0 : 1)$, and $P_4 = (1 : 1 : 1)$, such that the first coordinate of all $P_i$ with $i \geq 5$ is non-zero (see the proof of Theorem 1.2). Let $\bar{g} \in K\left(x_{5,2}/x_{5,0}, \ldots, x_{n,2}/x_{n,0}, x_{5,1}/x_{5,0}, \ldots, x_{n,1}/x_{n,0}\right)$ be the rational function obtained from $g$ by substituting each $C_{2,3,4,i,1}$ by $x_{i,2}/x_{i,0}$ and each $C_{3,2,4,i,1}$ by $x_{i,1}/x_{i,0}$ (for $i \geq 5$). It follows from (1.3) that $\bar{g}$ and $\Phi(g)$ coincide as functions on $T_0$. Thus by (1.11), $\bar{g}$ vanishes on $T_0$. But a rational function in indeterminates $x_{i,2}/x_{i,0}$ and $x_{i,1}/x_{i,0}$ $(i \geq 5)$ vanishing on $T_0$ must be zero by Lemma 1.3. Since the $x_{i,2}/x_{i,0}$ and $x_{i,1}/x_{i,0}$ are algebraically independent it follows that $g = 0$. Now $hf - g \in I$ implies $hf \in I$. Together with $h + I \in R^{\times}$, this implies $f \in I$. This completes the proof that $I_0 \subseteq I$.                                             $\square$

**Remark.** One can see from the proof of Theorem 1.4 that the invariant field $K(\underline{x})_0^{\mathrm{PGL}_3(K)}$ is in fact generated by the $c_{2,3,4,i,1}$ and $c_{3,2,4,i,1}$ with $i \in \{5, \ldots, n\}$ (other choices are possible), and that these $2(n - 4)$ generators are algebraically independent. So in particular $K(\underline{x})_0^{\mathrm{PGL}_3(K)}$ is purely transcendental over $K$. The "extended" generating system containing all $c_{i,j,k,l,m}$ is nevertheless more suitable for our purposes, since it is permuted by the action of the symmetric group $\Sigma_n$ on the indices of each $c_{i,j,k,l,m}$.

In Sections 2 and 3 we will need the following lemma, which gives some "non-relations".

**Lemma 1.5.** *We keep the notation of Theorem 1.4.*

(a) *The relations given in (1.4) are the only equalities that exist between the $c_{i,j,k,l,m}$. More precisely, if*

$$c_{i',j',k',l',m'} = c_{i,j,k,l,m},$$

*then $i' = i$, and the list $[j', k', l', m']$ is one of $[j, k, l, m]$, $[k, j, m, l]$, $[l, m, j, k]$, or $[m, l, k, j]$.*

(b) *For each $\nu \in \{1, 2, 3\}$, let $i_\nu, j_\nu, k_\nu, l_\nu, m_\nu \in \{1, \ldots, n\}$ be pairwise distinct indices, and suppose that*

$$c_{i_1,j_1,k_1,l_1,m_1} = c_{i_2,j_2,k_2,l_2,m_2} \cdot c_{i_3,j_3,k_3,l_3,m_3}. \tag{1.12}$$

*Then*

$$s := |\{i_1, j_1, k_1, l_1, m_1, i_2, j_2, k_2, l_2, m_2, i_3, j_3, k_3, l_3, m_3\}| \in \{5, 6\},$$

*i.e., only five or six indices occur in the above relation.*

(c) *If $s = 6$ in (b), then $i_1 = i_2 = i_3$.*

(d) *If $i_1 = i_2 = i_3$ does* not *hold in (b), then*

$$\{i_2, i_3\} = \{j_1, m_1\} \quad or \quad \{i_2, i_3\} = \{k_1, l_1\}.$$

*Proof.* To prove (a), assume $c_{i',j',k',l',m'} = c_{i,j,k,l,m}$. Then every bracket $[\nu, \mu, \eta]$ occurring in $c_{i',j',k',l',m'}$ must contain the index $i$, hence $i' = i$. Moreover, $c_{i',j',k',l',m'}$ must have the bracket $[i, j, k]$ or $[i, k, j]$ in its numerator and bracket $[i, j, l]$ or $[i, l, j]$ in its denominator, hence the claim.

Now assume the hypothesis of (b). First observe that if some index $\nu$ occurs in this relation, it must occur at least twice, since otherwise one side of (1.12) would involve the indeterminates $x_{\nu,\mu}$ while the other side would not.

We will study the behavior of both sides of (1.12) when we equate some of the arguments $v_i$. More precisely, for $i, j \in \{1, \ldots, n\}$ distinct and for $f \in K[\underline{x}]$ an irreducible polynomial, set $w_{\{i,j\}} := 1$ if $f$ lies in the ideal generated by $x_{i,0} - x_{j,0}$, $x_{i,1} - x_{j,1}$, and $x_{i,2} - x_{j,2}$, and set $w_{\{i,j\}} := 0$ otherwise. Extend $w_{\{i,j\}}$ to a function $(K(\underline{x}) \setminus \{0\}) \to \mathbb{Z}$ by using the rule $w_{\{i,j\}}(fg) = w_{\{i,j\}}(f) + w_{\{i,j\}}(g)$. Thus for $i, j, k, l, m \in \{1, \ldots, n\}$ pairwise distinct we have:

$$w_{\{j,k\}}(c_{i,j,k,l,m}) = w_{\{l,m\}}(c_{i,j,k,l,m}) = 1,$$
$$w_{\{j,l\}}(c_{i,j,k,l,m}) = w_{\{k,m\}}(c_{i,j,k,l,m}) = -1, \quad \text{and}$$
$$w_{\{\nu,\mu\}}(c_{i,j,k,l,m}) = 0 \quad \text{for} \quad \{\nu,\mu\} \notin \left\{ \{j,k\}, \{l,m\}, \{j,l\}, \{k,m\} \right\}.$$

These equations will be used frequently in the sequel. Equation (1.12) implies

$$w_{\{j_1,k_1\}}(c_{i_2,j_2,k_2,l_2,m_2}) + w_{\{j_1,k_1\}}(c_{i_3,j_3,k_3,l_3,m_3}) = 1,$$

so $\{j_1, k_1\} \in \left\{ \{j_2, k_2\}, \{l_2, m_2\}, \{j_3, k_3\}, \{l_3, m_3\} \right\}$. Possibly exchanging factors on the left hand side of (1.12) (which does not change any of the assertions of part (b), (c), or (d) of the lemma), we may assume that $\{j_1, k_1\} = \{j_2, k_2\}$ or $\{j_1, k_1\} = \{l_2, m_2\}$. Using (1.4), we may now reorder the indices $j_2, k_2, l_2, m_2$ in such a way that

$$j_1 = j_2 \quad \text{and (consequently)} \quad k_1 = k_2.$$

Using the same argument with $w_{\{l_1,m_1\}}$ yields $\{l_1, m_1\} \in \left\{ \{l_2, m_2\}, \{j_3, k_3\}, \{l_3, m_3\} \right\}$.

First consider the case $\{l_1, m_1\} = \{l_2, m_2\}$. Then (1.12) becomes

$$c_{i_1,j_1,k_1,l_1,m_1} = c_{i_2,j_1,k_1,l_1,m_1} \cdot c_{i_3,j_3,k_3,l_3,m_3} \quad \text{or} \quad c_{i_1,j_1,k_1,l_1,m_1} = c_{i_2,j_1,k_1,m_1,l_1} \cdot c_{i_3,j_3,k_3,l_3,m_3}.$$

It follows that $\{j_3, k_3, l_3, m_3\} = \{j_1, k_1, l_1, m_1\}$, since otherwise some $w_{\{\nu,\mu\}}$ would take the value 1 on the right hand side of the above equation but 0 on the left hand side. (For example, if $j_3 \notin \{j_1, k_1, l_1, m_1\}$, this would apply to $w_{\{j_3,k_3\}}$.) But then $i_1 = i_2 = i_3$, since otherwise some $i_\nu$ would occur only once as an index in (1.12), which cannot happen. Thus $s = 5$ and we are done with proving (b)–(d) in this case. (In fact, carrying the arguments further shows that this case cannot occur.)

It remains to consider the cases $\{l_1, m_1\} = \{j_3, k_3\}$ or $\{l_1, m_1\} = \{l_3, m_3\}$. As above we may use (1.4) to reorder the indices $j_3, k_3, l_3, m_3$ in such a way that $l_1 = l_3$ and (consequently) $m_1 = m_3$, so (1.12) becomes

$$c_{i_1,j_1,k_1,l_1,m_1} = c_{i_2,j_1,k_1,l_2,m_2} \cdot c_{i_3,j_3,k_3,l_1,m_1}.$$

Since $w_{\{j_1,l_1\}}(c_{i_1,j_1,k_1,l_1,m_1}) = -1$, we must have $\{j_1, l_1\} \in \left\{ \{j_1, l_2\}, \{k_1, m_2\}, \{j_3, l_1\}, \{k_3, m_1\} \right\}$. The second and the fourth possibilities would violate the distinctness of $i_2, j_1, k_1, l_2, m_2$ or $i_3, j_3, k_3, l_1, m_1$, respectively, so we have $l_1 = l_2$ or $j_1 = j_3$.

Consider the case $l_1 = l_2$. Then

$$c_{i_1,j_1,k_1,l_1,m_1} = c_{i_2,j_1,k_1,l_1,m_2} \cdot c_{i_3,j_3,k_3,l_1,m_1}.$$

Applying the above argument again (using $w_{\{k_1,m_1\}}$) shows $m_1 = m_2$ or $k_1 = k_3$. But if $m_1 = m_2$, then $w_{\{l_1,m_1\}}$ takes different values on the different sides of the above equation, so $k_1 = k_3$. Thus

$$c_{i_1,j_1,k_1,l_1,m_1} = c_{i_2,j_1,k_1,l_1,m_2} \cdot c_{i_3,j_3,k_1,l_1,m_1}.$$

We have $m_1 \neq m_2$ and $j_1 = j_2 \neq m_2$, hence

$$0 = w_{\{l_1,m_2\}}(c_{i_1,j_1,k_1,l_1,m_1}) = 1 + w_{\{l_1,m_2\}}(c_{i_3,j_3,k_1,l_1,m_1}),$$

implying $j_3 = m_2$. We are left with

$$c_{i_1,j_1,k_1,l_1,m_1} = c_{i_2,j_1,k_1,l_1,m_2} \cdot c_{i_3,m_2,k_1,l_1,m_1}. \tag{1.13}$$

The set $T := \{j_1, k_1, l_1, m_1, m_2\}$ has 5 (distinct) elements. Assume $i_1 \notin T$. Then for the prime polynomial $[i_1, j_1, k_1]$ to appear in the numerator of $c_{i_2,j_1,k_1,l_1,m_2} \cdot c_{i_3,m_2,k_1,l_1,m_1}$ we must have $i_2 = i_1$. Furthermore, $i_3 = i_1$, since otherwise $[i_1, l_1, m_1]$ could not appear in that numerator. Now assume $i_2 \notin T$. Then $i_1 = i_2$, since otherwise $[i_2, j_1, k_1]$ would appear only once on the right hand side of (1.13) and not at all on the left hand side. Moreover, $[i_2, k_1, m_2]$ does not appear on the left hand side, so it must be cancelled on the right hand side, so $i_3 = i_2$. Likewise, if $i_3 \notin T$, then $[i_3, m_2, k_1]$ must be cancelled on the right hand side of (1.13), so $i_2 = i_3$, and $[i_3, k_1, m_1]$ must appear on the left hand side, so $i_1 = i_3$. Thus we have seen that if any of the $i_\nu$ lie in $T$, then $i_1 = i_2 = i_3$ and thus $s = 6$. The other possibility is that all $i_\nu$ lie in $T$. But then $s = 5$ and $i_1 = m_2$ (otherwise the indices on the left hand side of (1.13) would not be distinct), $i_2 = m_1$, and $i_3 = j_1$. So we are in one of the cases described by part (d) of the lemma. Thus parts (b)–(d) are proved in the case $l_1 = l_2$.

Now consider the remaining case $j_1 = j_3$. We have

$$c_{i_1,j_1,k_1,l_1,m_1} = c_{i_2,j_1,k_1,l_2,m_2} \cdot c_{i_3,j_1,k_3,l_1,m_1}.$$

Considering $w_{\{k_1,m_1\}}$ yields $m_1 = m_2$ or $k_1 = k_3$. The possibility $k_1 = k_3$ is ruled out by considering $w_{\{j_1,k_1\}}$, so $m_1 = m_2$. Thus $l_1 \neq l_2$ (since $l_1 = l_2$ was considered above) and $k_1 = k_2 \neq l_2$ yield

$$0 = w_{\{l_2,m_1\}}(c_{i_1,j_1,k_1,l_1,m_1}) = 1 + w_{\{l_2,m_1\}}(c_{i_3,j_1,k_3,l_1,m_1}),$$

so $k_3 = l_2$, and we obtain

$$c_{i_1,j_1,k_1,l_1,m_1} = c_{i_2,j_1,k_1,l_2,m_1} \cdot c_{i_3,j_1,l_2,l_1,m_1}.$$

In this case we consider the set $T := \{j_1, k_1, l_1, m_1, l_2\}$ of size 5. Using exactly the same arguments as in the previous case, we conclude that either $s = 6$ and $i_1 = i_2 = i_3$, or $s = 5$ and $i_1 = l_2$, $i_2 = l_1$, and $i_3 = k_1$. So parts (b)–(d) of the lemma are proved in this case, too. □

Before we go on, it is useful to introduce some notation which deviates slightly from the notation introduced before Theorem 1.4. By (1.4) and Lemma 1.5(a) there are precisely $n(n-1)(n-2)(n-3)(n-4)/4$ distinct $c_{i,j,k,l,m}$. We take as many indeterminates as follows: For $i, j, k, l, m \in \{1, \ldots, n\}$ pairwise distinct with $j = \min\{j, k, l, m\}$ let $C_{i,j,k,l,m}$ be an indeterminate over $K$. For $i, j, k, l, m$ distinct but *not* meeting the additional constraint that $j = \min\{j, k, l, m\}$, we define $C_{i,j,k,l,m}$ by imposing the equations

$$C_{i,j,k,l,m} = C_{i,k,j,m,l} = C_{i,l,m,j,k} = C_{i,m,l,k,j}, \tag{1.14}$$

which reflect (1.4). Let $P$ be the polynomial ring generated by the $C_{i,j,k,l,m}$, and let $I$ be the kernel of the homomorphism $P \to K(\underline{x})$ of $K$-algebras sending $C_{i,j,k,l,m}$ to $c_{i,j,k,l,m}$. Thus $I$ is the ideal of relations between the $c$'s. The distinction between the polynomial rings $P_0$ (introduced before Theorem 1.4) and $P$ may seem a bit subtle, but introducing $P$ ultimately renders our notation much simpler. $P_0$ will not be used anymore in the sequel.

## 2  The case $n = 5$

In this section we will work out a set of generating invariants for $K(\underline{x})_0^{\Sigma_n \times \mathrm{PGL}_3(K)}$ in the case $n = 5$. Here and in the sequel we write $\Sigma_n$ for the symmetric group in $n$ symbols. Recall that $K$ is an infinite field and $K(\underline{x})_0 = K(x_{i,j}/x_{i,0} \mid i = 1, \ldots, n, j = 1, 2)$ is the function field of $(\mathbb{P}^2(K))^n$. We will also use the $\mathrm{PGL}_3(K)$-invariants $c_{i,j,k,l,m}$ defined in (1.1) and the indeterminates $C_{i,j,k,l,m}$

defined at the end of Section 1. Theorem 1.4 and Lemma 1.5 give information on the ideal $I$ of relations between the $c_{i,j,k,l,m}$. As we consider the case $n = 5$, there are precisely 30 $C_{i,j,k,l,m}$. We denote the group of all permutations of these 30 elements by $\Sigma_{30}$. (Note that this is a slight deviation from the notation $\Sigma_n$ for the symmetric group in $n$ symbols.) Any such permutation acts on the polynomial ring $P$ generated by the $C_{i,j,k,l,m}$. The crucial step in this section is the proof of the following lemma.

**Lemma 2.1.** *Let $\varphi \in \Sigma_{30}$ be a permutation of the $C_{i,j,k,l,m}$ with $\{i, j, k, l, m\} = \{1, 2, 3, 4, 5\}$ and $j = \min\{j, k, l, m\}$. Assume that $\varphi$ maps the ideal $I \subset P$ into itself. Then there exists a permutation $\pi \in \Sigma_5$ of the numbers $1, \dots, 5$ such that for all indices $i, j, k, l, m$ we have*

$$\varphi(C_{i,j,k,l,m}) = C_{\pi(i),\pi(j),\pi(k),\pi(l),\pi(m)}.$$

*Proof.* Take $i, j, k, l, m \in \{1, 2, 3, 4, 5\}$ pairwise distinct with $j = \min\{j, k, l, m\}$ (meaning $j = 1$ if $i \neq 1$ and $j = 2$ otherwise), and suppose

$$\varphi(C_{i,j,k,l,m}) = C_{r,s,t,u,v}$$

with $\{r, s, t, u, v\} = \{1, 2, 3, 4, 5\}$, $s = \min\{s, t, u, v\}$. By (1.6) we have $C_{i,j,k,l,m} + C_{i,j,m,l,k} - 1 \in I$, hence our hypothesis implies $C_{r,s,t,u,v} + \varphi(C_{i,j,m,l,k}) - 1 \in I$. On the other hand, $C_{r,s,t,u,v} + C_{r,s,v,u,t} - 1 \in I$, so $\varphi(C_{i,j,m,l,k}) - C_{r,s,v,u,t} \in I$. By Lemma 1.5(a) it follows that

$$\varphi(C_{i,j,m,l,k}) = C_{r,s,v,u,t}. \tag{2.1}$$

Using (1.5) we see that $C_{i,j,k,l,m}C_{i,j,l,k,m} - 1 \in I$, hence $C_{r,s,t,u,v}\varphi(C_{i,j,l,k,m}) - 1 \in I$. But also $C_{r,s,t,u,v}C_{r,s,u,t,v} - 1 \in I$, and the uniqueness of inverses in any ring (here: $P/I$) leads to

$$\varphi(C_{i,j,l,k,m}) = C_{r,s,u,t,v}. \tag{2.2}$$

Repeated application of (2.1) and (2.2) shows that $\varphi(C_{i,j,*,*,*}) = C_{r,s,+,+,+}$, where the $*$'s are the indices $k, l, m$ appearing in some order, and the $+$'s stand for $t, u, v$ appearing in the corresponding order.

Now define a map $\pi : \{1, \dots, 5\} \to \{1, \dots, 5\}$ as follows: For $i \in \{1, \dots, 5\}$ there are unique $j, k, l, m$ with $\{i, j, k, l, m\} = \{1, \dots, 5\}$ and $j < k < l < m$. Let $\pi(i)$ be the first index of $\varphi(C_{i,j,k,l,m})$. There are precisely 6 (distinct) $C_{r,s,t,u,v}$ with $r = \pi(i)$. By the above observation it follows that all these $C_{r,s,t,u,v}$ are images of suitable $C_{i,j,*,*,*}$ under $\varphi$. Therefore the hypothesis that $\varphi$ permutes the $C$'s implies that $\pi$ is actually a permutation of the set $\{1, \dots, 5\}$. Define $\varphi_\pi$ by

$$\varphi_\pi(C_{i,j,k,l,m}) = C_{\pi(i),\pi(j),\pi(k),\pi(l),\pi(m)}.$$

We wish to show that $\varphi = \varphi_\pi$. We know that for any $i, j, k, l, m \in \{1, \dots, 5\}$ distinct we have $\varphi(C_{i,j,k,l,m}) = C_{\pi(i),s,t,u,v}$ with $s, t, u, v \in \{1, \dots, 5\} \setminus \{\pi(i)\}$. Hence $(\varphi_\pi^{-1} \circ \varphi)(C_{i,j,k,l,m}) = C_{i,\pi^{-1}(s),\pi^{-1}(t),\pi^{-1}(u),\pi^{-1}(v)}$. Using (1.14) we may reorder $\pi^{-1}(s), \pi^{-1}(t), \pi^{-1}(u), \varphi^{-1}(v)$ in such a way that $j$ (which has to be among the $\pi^{-1}(s), \pi^{-1}(t), \pi^{-1}(u), \varphi^{-1}(v)$ since $\{i, j, k, l, m\} = \{1, \dots, 5\} = \{i, \pi^{-1}(s), \pi^{-1}(t), \pi^{-1}(u), \pi^{-1}(v)\}$) appears first. Thus for $\{i, j, k, l, m\} = \{1, \dots, 5\}$ we have

$$\left(\varphi_\pi^{-1} \circ \varphi\right)(C_{i,j,k,l,m}) = C_{i,j,r,s,t} \tag{2.3}$$

with $\{r, s, t\} = \{k, l, m\}$. The permutation $\varphi_\pi$ sends the relation ideal $I \subset P$ to itself. In fact, $\pi$ induces an automorphism $\psi_\pi$ of $K(\underline{x})$ given by $\psi_\pi(x_{i,\nu}) = x_{\pi(i),\nu}$. With $\Phi : P \to K(\underline{x})$ given by $\Phi(C_{i,j,k,l,m}) = c_{i,j,k,l,m}$, we clearly have $\Phi(\varphi_\pi(f)) = \psi_\pi(\Phi(f))$ for $f \in P$, hence $f \in I$ implies $\Phi(\varphi_\pi(f)) = \psi_\pi(0) = 0$, so indeed $\varphi_\pi(f) \in I$. To simplify notation, we may thus replace $\varphi$ by $\varphi_\pi^{-1} \circ \varphi$. Then (2.3) leads to

$$\varphi(C_{i,j,k,l,m}) = C_{i,j,r,s,t} \quad \text{with} \quad \{r, s, t\} = \{k, l, m\}, \tag{2.4}$$

and we have to show that $\varphi = \mathrm{id}$. By (1.7) we have $C_{i,j,k,l,m} - C_{m,j,k,l,i}C_{j,i,k,l,m} \in I$. Since $\varphi(I) \subseteq I$, this implies $C_{i,j,r,s,t} - C_{m,j,*,*,*}C_{j,i,*,*,*} \in I$ with the $*$'s standing for appropriate (as yet unknown) indices. By Lemma 1.5(d) we conclude $\{j,m\} = \{j,t\}$ or $\{j,m\} = \{r,s\}$. The second possibility is ruled out by the distinctness of $i,j,r,s,t$, hence $t = m$.

Furthermore, we have $C_{i,j,k,l,m} + C_{i,j,m,l,k} - 1 \in I$ by (1.6), hence $C_{i,j,r,s,t} + \varphi(C_{i,j,m,l,k}) - 1 \in I$. On the other hand, $C_{i,j,r,s,t} + C_{i,j,t,s,r} - 1 \in I$, implying $\varphi(C_{i,j,m,l,k}) = C_{i,j,t,s,r}$. Using (1.7) again, we obtain $C_{i,j,m,l,k} - C_{k,j,m,l,i}C_{j,i,m,l,k} \in I$, hence $C_{i,j,t,s,r} - C_{k,j,*,*,*}C_{j,i,*,*,*} \in I$. Lemma 1.5(d) tells us that $\{k,j\} = \{j,r\}$ or $\{k,j\} = \{s,t\}$, hence $r = k$. Having seen that $t = m$ and $r = k$, we conclude that also $s = l$, since $\{r,s,t\} = \{k,l,m\}$ by (2.4). Thus (2.4) becomes $\varphi(C_{i,j,k,l,m}) = C_{i,j,k,l,m}$, so indeed $\varphi = \mathrm{id}$. This completes the proof. $\qquad\square$

Now we are ready to prove the main result of this section, which gives a generating set for $K(\underline{x})_0^{\Sigma_n \times \mathrm{PGL}_3(K)}$ in the case $n = 5$.

**Theorem 2.2.** *With the $\mathrm{PGL}_3(K)$-invariants $c_{i,j,k,l,m}$ defined as in (1.1), form*

$$a := \sum_{\pi \in \Sigma_5} c_{\pi(1),\pi(2),\pi(3),\pi(4),\pi(5)}^2 \quad and \quad b := \sum_{\pi \in \Sigma_5} c_{\pi(1),\pi(2),\pi(3),\pi(4),\pi(5)}^4.$$

*If the characteristic of $K$ is not 2, then*

$$K(\underline{x})_0^{\Sigma_5 \times \mathrm{PGL}_3(K)} = K(a,b).$$

*Proof.* Clearly $a$ and $b$ are invariant under $\Sigma_5$ and $\mathrm{PGL}_3(K)$, which shows the inclusion "$\supseteq$". So we need to prove "$\subseteq$". Theorem 1.2(a) and (1.4) tell us that

$$N := K(\underline{x})_0^{\mathrm{PGL}_3(K)} = K\left(c_{i,j,k,l,m} \mid \{i,j,k,l,m\} = \{1,\ldots,5\}, j = \min\{j,k,l,m\}\right).$$

With $T$ an additional indeterminate, form the polynomial

$$F := \prod_{\substack{\{i,j,k,l,m\}=\{1,\ldots,5\}, \\ j=\min\{j,k,l,m\}}} (T - c_{i,j,k,l,m}) \in N[T].$$

A fairly easy computation using the computer algebra system Magma [1] shows that the coefficients of $F$ lie in $L := K(a,b)$. In fact, using the relations given in (1.4)–(1.7), one can express all $c_{i,j,k,l,m}$ with $\{i,j,k,l,m\} = \{1,\ldots,5\}$ and $j = \min\{j,k,l,m\}$ as rational functions in $c_{1,2,3,4,5}$ and $c_{2,1,3,4,5}$. So we get $c_{i,j,k,l,m} = f_{i,j,k,l,m}(c_{1,2,3,4,5}, c_{2,1,3,4,5})$ with $f_{i,j,k,l,m} \in K(X,Y)$, where $X$ and $Y$ are new indeterminates. Details on what the $f_{i,j,k,l,m}$ actually are can be found in Remark 2.3(a). Now all that we need to do is express the 30 elementary symmetric functions of the $f_{i,j,k,l,m}$ in terms of the sum of squares and the sum of fourth powers of the $f_{i,j,k,l,m}$. Our Magma computation, which only involves rational functions in $X$ and $Y$, shows that (thanks to the special form of the $f_{i,j,k,l,m}$) this is indeed possible. It is in this computation that $\mathrm{char}(K) \neq 2$ is required.

We conclude that $N$ is the splitting field of $F$ over $L$. Lemma 1.5(a) implies that $F$ is a separable polynomial, hence $N$ is Galois as a field extension of $L$. By Galois theory we are done if we can show that the Galois group of $N$ over $L$ is contained in $\Sigma_5$ (in which case it will be equal to $\Sigma_5$). So take $\varphi \in \mathrm{Gal}(N/L)$. Since $N$ is the splitting field of $F$, $\varphi$ permutes the roots $c_{i,j,k,l,m}$ of $F$, and $\varphi$ is determined by its permutation action on these roots. But since $\varphi$ is a field automorphism, it preserves all relations between the $c_{i,j,k,l,m}$. This means that $\varphi$, viewed as a permutation of the indeterminates $C_{i,j,k,l,m}$, maps the relation ideal $I$ into itself. Now it follows from Lemma 2.1 that indeed $\varphi \in \Sigma_5$. This completes the proof. $\qquad\square$

**Remark 2.3.**  (a) It looks as if we had to evaluate all 30 of the $c_{i,j,k,l,m}$ with $\{i,j,k,l,m\} = \{1,\ldots,5\}$ and $j = \min\{j,k,l,m\}$ in order to obtain the values of the invariants $a$ and $b$ appearing in Theorem 2.2. But in fact they can all be expressed in terms of $c_{1,2,3,4,5}$ and

$c_{2,1,3,4,5}$. Let us explain how. Form the set $\mathcal{M} := \{X, Y, X/Y, (X-1)/(Y-1), X(1-Y)/(X-Y)\}$ with $X$ and $Y$ indeterminates. For each $f \in \mathcal{M}$, also add $1/f$, $1-f$, $1/(1-f)$, $(f-1)/f$, and $f/(f-1)$ into $\mathcal{M}$, so that $\mathcal{M}$ contains a total of 30 rational functions in $X$ and $Y$. Then all $c_{i,j,k,l,m}$ are obtained by substituting $X = c_{1,2,3,4,5}$ and $Y = c_{2,1,3,4,5}$ in the rational functions $f$ from $\mathcal{M}$. This can be seen from the relations (1.4)–(1.7). In particular, if we form

$$A := \sum_{f \in \mathcal{M}} f^2 \quad \text{and} \quad B := \sum_{f \in \mathcal{M}} f^4, \tag{2.5}$$

we obtain

$$a = 4 \cdot A(c_{1,2,3,4,5}, c_{2,1,3,4,5}) \quad \text{and} \quad b = 4 \cdot B(c_{1,2,3,4,5}, c_{2,1,3,4,5}).$$

(b) If follows from (1.3) that $c_{3,2,4,5,1}$ and $c_{2,3,4,5,1}$ are algebraically independent over $K$. Thus the transcendence degree of $N := K(\underline{x})_0^{\mathrm{PGL}_3(K)} = K\left(c_{i,j,k,l,m} \mid \{i,j,k,l,m\} = \{1,\ldots,5\}\right)$ over $K$ is at least 2. But $L := K(\underline{x})_0^{\Sigma_5 \times \mathrm{PGL}_3(K)} = N^{\Sigma_5}$ has the same transcendence degree, since $N$ is algebraic over $L$. From Theorem 2.2, the transcendence degree of $L$ is at most 2. It follows that the transcendence degree of both fields is precisely 2, and the generating invariants $a_{1,2,3,4,5}$ and $b_{1,2,3,4,5}$ are algebraically independent. In particular, two is the smallest number of generating invariants for $L$ that we could have expected.

(c) We can also deal with the case $\mathrm{char}(K) = 2$. In fact, this just requires a slight change of the invariants $a$ and $b$. Instead of taking the sum of the squares and of fourth powers of the $c_{i,j,k,l,m}$, we need to take the second and fourth elementary symmetric functions in the $c_{i,j,k,l,m}$ with $\{i,j,k,l,m\} = \{1,\ldots,5\}$ and $j = \min\{j,k,l,m\}$. In the context of part (a) of this remark, we need to replace $A$ and $B$ by the second and fourth elementary symmetric function in the $f$'s from $\mathcal{M}$. A Magma computation as mentioned in the proof of Theorem 2.2 then shows that *all* elementary symmetric functions in the $f$'s from $\mathcal{M}$ can be expressed as rational functions in $A$ and $B$.

(d) Meer et al. [4, page 141] determined a set of five $\mathrm{PGL}_3$-invariants of five points $(P_1, \ldots, P_5)$ which are also invariant under the action of the symmetric group $\Sigma_4$ acting by permutations of the last four points $P_2, P_3, P_4, P_5$. These five invariants are permuted by the action of the complete permutation group $\Sigma_5$. The authors propose to take the values of these five invariants, ordered in increasing sequence, as invariants of $\Sigma_5 \times \mathrm{PGL}_3$.

# 3 The case of general $n$

In this section we attack the problem of finding generating invariants of $K(\underline{x})_0^{\Sigma_n \times \mathrm{PGL}_3(K)}$ for a general positive integer $n$. Recall our notation. $K$ is an infinite field, $K(\underline{x}) = K\left(x_{i,j} \mid 1 \le i \le n, 0 \le j \le 2\right)$ is a rational function field in $3n$ indeterminates over a field $K$, and for $i,j,k,l,m \in \{1,\ldots,n\}$ pairwise distinct we have a rational function $c_{i,j,k,l,m}$ as given in (1.1). $P$ is a polynomial ring over $K$ in $n(n-1)(n-2)(n-3)(n-4)/4$ indeterminates $C_{i,j,k,l,m}$ labeled by $i,j,k,l,m \in \{1,\ldots,n\}$ pairwise distinct with $j = \min\{j,k,l,m\}$. Using (1.14), which mirrors the equalities (1.4) existing between the $c_{i,j,k,l,m}$, we define $C_{i,j,k,l,m}$ for *any* pairwise distinct $i,j,k,l,m \in \{1,\ldots,n\}$. The ideal $I \subset P$ is the kernel of the map $P \to K(\underline{x})$ sending each $C_{i,j,k,l,m}$ to $c_{i,j,k,l,m}$; thus $I$ is the ideal of relations of the $c_{i,j,k,l,m}$. The following lemma is tailored for proving the main result, Theorem 3.3, of the section.

**Lemma 3.1.** *Let $\psi$ be a permutation of the set*

$$\mathcal{M} := \{S \subseteq \{1,\ldots,n\} \mid |S| = 5\},$$

*and for each $S \in \mathcal{M}$ let $\pi_S \colon S \to \psi(S)$ be a bijection. Define a homomorphism $\varphi \colon P \to P$ of $K$-algebras by*

$$\varphi(C_{i,j,k,l,m}) := C_{\pi_S(i),\pi_S(j),\pi_S(k),\pi_S(l),\pi_S(m)} \quad where \quad S = \{i,j,k,l,m\}.$$

*(Note that $\varphi$ is well-defined since the equalities (1.14) are preserved.) If $\varphi(I) \subseteq I$, then there exists a permutation $\pi \in \Sigma_n$ such that*

$$\varphi(C_{i,j,k,l,m}) = C_{\pi(i),\pi(j),\pi(k),\pi(l),\pi(m)}$$

*for all $i$, $j$, $k$, $l$, $m$.*

*Proof.* There is nothing to show for $n \leq 5$, so we may assume $n \geq 6$.

Let $T = \{i,j,k,l,m,r\} \subseteq \{1,\ldots,n\}$ be a set if six (distinct) elements. By (1.8) we have $C_{i,j,k,l,m} - C_{i,r,k,l,m} \cdot C_{i,j,k,l,r} \in I$, hence by hypothesis also

$$\varphi(C_{i,j,k,l,m}) - \varphi(C_{i,r,k,l,m}) \cdot \varphi(C_{i,j,k,l,r}) \in I. \tag{3.1}$$

With $S := \{i,j,k,l,m\} \in \mathcal{M}$ we have $\varphi(C_{i,j,k,l,m}) = C_{\pi_S(i),\pi_S(j),\pi_S(k),\pi_S(l),\pi_S(m)}$, and correspondingly for the other $C$'s occurring in (3.1). Thus the union of all indices occurring in (3.1) is

$$\widetilde{T} := \psi(\{i,j,k,l,m\}) \cup \psi(\{i,r,k,l,m\}) \cup \psi(\{i,j,k,l,r\}).$$

By Lemma 1.5(b), $\widetilde{T}$ has at most six elements. On the other hand, the injectivity of $\psi$ implies that even the union of the $\psi$-images of just two different sets in $\mathcal{M}$ has at least six elements. Therefore

$$\widetilde{T} = \psi(\{i,j,k,l,m\}) \cup \psi(\{i,r,k,l,m\}) = \psi(\{i,j,k,l,m\}) \cup \psi(\{i,j,k,l,r\}) \tag{3.2}$$

and $\widetilde{T}$ has precisely six elements. It follows that there exists $r' \in \widetilde{T}$ such that $\psi(\{i,j,k,l,m\}) = \widetilde{T} \setminus \{r'\}$. Likewise, $\psi(\{i,r,k,l,m\}) = \widetilde{T} \setminus \{j'\}$ and $\psi(\{i,j,k,l,r\}) = \widetilde{T} \setminus \{m'\}$ with $j', m' \in \widetilde{T}$. Now we use the same argument with the roles of $i$ and $j$ interchanged. This yields

$$\psi(\{j,i,k,l,m\}) \cup \psi(\{j,k,l,m,r\}) = \psi(\{j,i,k,l,m\}) \cup \psi(\{j,i,k,l,r\})$$

The second expression for $\widetilde{T}$ in (3.2) is equal to the right hand side of above equation. Hence $\widetilde{T} = \psi(\{j,i,k,l,m\}) \cup \psi(\{j,k,l,m,r\}) \supseteq \psi(\{j,k,l,m,r\})$, so there exists $i' \in \widetilde{T}$ with $\psi(\{j,k,l,m,r\}) = \widetilde{T} \setminus \{i'\}$. In the same way, interchanging $j$ and $k$ yields $\psi(\{i,k,j,l,m\}) \cup \psi(\{i,j,l,m,r\}) = \widetilde{T}$, so $\psi(\{i,j,l,m,r\}) = \widetilde{T} \setminus \{k'\}$. Finally, interchanging $j$ and $l$ yields $\psi(\{i,l,k,j,m\}) \cup \psi(\{i,k,j,m,r\}) = \widetilde{T}$, so $\psi(\{i,j,k,m,r\}) = \widetilde{T} \setminus \{l'\}$. In summary, there exists a function $\eta_T \colon T \to \widetilde{T} \subseteq \{1,\ldots,n\}$ (which maps $i$ to $i'$ etc.) such that $\psi(T \setminus \{\nu\}) = \widetilde{T} \setminus \{\eta_T(\nu)\}$ for all $\nu \in T$. By hypothesis, $\psi$ is injective, so the same holds for $\eta_T$, hence $\eta_T(T) = \widetilde{T}$. It follows that for any $S \in \mathcal{M}$ with $S \subset T$ we have

$$\psi(S) = \eta_T(S), \tag{3.3}$$

where the right hand side indicates element-wise application of $\eta_T$.

It follows from (3.3) that if two sets $S, S' \in \mathcal{M}$ have four elements in common, then also $\psi(S)$ and $\psi(S')$ have four elements in common. In fact, $T := S \cup S'$ has six elements, hence $\psi(S) = \eta_T(S)$ and $\psi(S') = \eta_T(S')$. These are two subsets of size 5 inside the set $\eta_T(T)$ which has six elements, hence indeed $\psi(S)$ and $\psi(S')$ share four elements. Now take two subsets $T, T' \subseteq \{1,\ldots,n\}$ with $|T| = |T'| = 6$ such that $S := T \cap T'$ has 5 elements. We will show that $\eta_T$ and $\eta_{T'}$ coincide on $S$. Write

$$T = S \cup \{j\} \quad \text{and} \quad T' = S \cup \{k\}$$

with $j, k \in \{1,\ldots,n\}$. For $l \in S$ set $S_l := T' \setminus \{l\}$, so $S_l \in \mathcal{M}$. Then $|S_l \cap (T \setminus \{l\})| = 4$ and $|S_l \cap S| = 4$, so, as noted above, $\psi(S_l)$ shares 4 elements with $\psi(T \setminus \{l\}) = \eta_T(T) \setminus \{\eta_T(l)\}$ and

with $\psi(S) = \eta_T(S) = \eta_T(T) \setminus \{\eta_T(j)\}$. But $\psi(S_l)$ cannot be a subset of $\eta_T(T)$ since this would imply

$$\psi(S_l) = \eta_T\left(\eta_T^{-1}\left(\psi(S_l)\right)\right) = \psi\left(\eta_T^{-1}\left(\psi(S_l)\right)\right),$$

contradicting the injectiveness of $\psi$, since $S_l \not\subseteq T$. It follows that $\psi(S_l) = \eta_T\left(T \setminus \{j, l\}\right) \cup \{r_l\}$ with $r_l \in \{1, \dots, n\} \setminus \eta_T(T)$. We can write this slightly simpler as $\psi(S_l) = \eta_T\left(S \setminus \{l\}\right) \cup \{r_l\}$. On the other hand, we have $S_l \subset T'$, so

$$\psi(S_l) = \eta_{T'}(S_l) = \eta_{T'}\left(S \setminus \{l\}\right) \cup \{\eta_{T'}(k)\}.$$

Intersecting the resulting equality $\eta_T\left(S \setminus \{l\}\right) \cup \{r_l\} = \eta_{T'}\left(S \setminus \{l\}\right) \cup \{\eta_{T'}(k)\}$ over all $l \in S$ yields $\bigcap_{l \in S}\{r_l\} = \{\eta_{T'}(k)\}$. Thus $r_l = \eta_{T'}(k)$ independently of $l$, and $\eta_T\left(S \setminus \{l\}\right) = \eta_{T'}\left(S \setminus \{l\}\right)$ for all $l \in S$. This shows that $\eta_T(l) = \eta_{T'}(l)$ for all $l \in S$, as claimed.

We proceed by taking any two subsets $T, T' \subseteq \{1, \dots, n\}$ with $|T| = |T'| = 6$. We can move from $T$ to $T'$ by successively exchanging elements. Using the above result, we see that $\eta_T$ and $\eta_{T'}$ coincide on $T \cap T'$. Thus we can define $\pi\colon \{1, \dots, n\} \to \{1, \dots, n\}$ such that for every subset $T \subseteq \{1, \dots, n\}$ with $|T| = 6$ the restriction $\pi|_T$ coincides with $\eta_T$. Thus (3.3) yields

$$\psi(S) = \pi(S)$$

for all $S \in \mathcal{M}$, where again the right hand side indicates element-wise application of $\pi$. In particular, $\pi$ is injective, since otherwise $|\pi(S)| < 5$ for some $S \in \mathcal{M}$. Hence $\pi \in \Sigma_n$.

Define $\varphi_\pi\colon P \to P$ by $\varphi_\pi(C_{i,j,k,l,m}) := C_{\pi(i),\pi(j),\pi(k),\pi(l),\pi(m)}$. We claim that $\varphi = \varphi_\pi$, which is equivalent to $\varphi_{\pi^{-1}} \circ \varphi = \mathrm{id}$. It is clear from the definition of $I$ that $\varphi_\pi$ maps $I$ onto itself, hence $\left(\varphi_{\pi^{-1}} \circ \varphi\right)(I) \subseteq I$. For $i, j, k, l, m \in \{1, \dots, n\}$ distinct we have

$$\left(\varphi_{\pi^{-1}} \circ \varphi\right)(C_{i,j,k,l,m}) = C_{\pi^{-1}(\pi_S(i)),\pi^{-1}(\pi_S(j)),\pi^{-1}(\pi_S(k)),\pi^{-1}(\pi_S(l)),\pi^{-1}(\pi_S(m))},$$

where $S := \{i, j, k, l, m\} \in \mathcal{M}$ and $\pi_S$ is given by the hypothesis of the lemma. Observe that $\left(\pi^{-1} \circ \pi_S\right)(S) = \pi^{-1}(\psi(S)) = \pi^{-1}(\pi(S)) = S$, so $\pi^{-1} \circ \pi_S$ is a bijection $S \to S$. Thus, in order to complete the proof, we may substitute $\varphi$ by $\varphi_{\pi^{-1}} \circ \varphi$, and then we have the hypothesis that every $\pi_S$ is a bijection $S \to S$. Our goal is to show that all $\pi_S$ are equal to the identity.

Assume that there exists an $S \in \mathcal{M}$ and an $i \in S$ such that $\pi(i) \neq i$. Set $j := \pi_S(i) \in S$ and write $S = \{i, j, k, l, m\}$. Moreover, choose any $r \in \{1, \dots, n\} \setminus S$. By (1.8) we have $C_{i,j,k,l,m} - C_{i,r,k,l,m} \cdot C_{i,j,k,l,r} \in I$. With $S' := \{i, r, k, l, m\}$ and $S'' := \{i, j, k, l, r\}$ it follows that

$$C_{\pi_S(i),\pi_S(j),\pi_S(k),\pi_S(l),\pi_S(m)} - C_{\pi_{S'}(i),\pi_{S'}(r),\pi_{S'}(k),\pi_{S'}(l),\pi_{S'}(m)} \cdot C_{\pi_{S''}(i),\pi_{S''}(j),\pi_{S''}(k),\pi_{S''}(l),\pi_{S''}(r)} \in I.$$

By Lemma 1.5(c), this implies $\pi_S(i) = \pi_{S'}(i)$, but $\pi_S(i) = j \notin S' = \pi_{S'}(S')$. This contradiction shows that indeed all $\pi_S$ are the identity, completing the proof. $\qquad\square$

To prove the main result of this section, we still need an elementary lemma from field theory.

**Lemma 3.2.** *Let $N = K(a_1, \dots, a_m, b_1, \dots, b_m)$ be a field extension of $K$ generated by pairwise distinct elements $a_1, \dots, a_m, b_1, \dots, b_m$. Let $G \subseteq \mathrm{Aut}_K(N)$ be the group of all those $K$-automorphisms $\sigma$ of $N$ for which there exists $\pi \in \Sigma_m$ with $\sigma(a_i) = a_{\pi(i)}$ and $\sigma(b_i) = b_{\pi(i)}$ for all $i$. Take indeterminates $X, T_1, T_2$, and consider the polynomial*

$$F := \prod_{i=1}^m \left(X - T_1 a_i - T_2 b_i\right) \in N[X, T_1, T_2].$$

*Let $L \subseteq N$ be the subextension generated by all coefficients of $F$. Then*

$$N^G = L.$$

*Proof.* By the definition of $G$, any $\sigma \in G$ permutes the factors of $F$, hence $L \subseteq N^G$. We use Galois theory to prove the reverse inclusion. It follows from the construction of $L$ that $\prod_{i=1}^{m}(X - a_i)$ and $\prod_{i=1}^{m}(X - b_i)$ lie in $L[X]$. Therefore $N$ is the spitting field over $L$ of the polynomial $\prod_{i=1}^{m}((X - a_i)(X - b_i))$. Hence $N/L$ is Galois, so $L = N^{\mathrm{Gal}(N/L)}$. If we can prove that $\mathrm{Gal}(N/L) \subseteq G$, then $N^G \subseteq N^{\mathrm{Gal}(N/L)} = L$, and we are done. So take any $\sigma \in \mathrm{Gal}(N/L)$. Writing $\sigma(F)$ for the coefficient-wise application of $\sigma$ to $F$, we obtain

$$\prod_{i=1}^{m}(X - T_1 a_i - T_2 b_i) = F = \sigma(F) = \prod_{i=1}^{m}(X - T_1 \sigma(a_i) - T_2 \sigma(b_i)).$$

Since the zeros of a polynomial are uniquely determined up to permutations, there exists $\pi \in \Sigma_m$ such that $T_1 \sigma(a_i) + T_2 \sigma(b_i) = T_1 a_{\pi(i)} + T_2 b_{\pi(i)}$ for all $i$. It follows that indeed $\sigma \in G$.  $\square$

We can now give a generating set for the invariant field $K(\underline{x})_0^{\Sigma_n \times \mathrm{PGL}_3(K)}$. We may assume $n \geq 5$, since for $n \leq 4$ all invariants are constant (this is contained in Theorem 1.2(a)). Let $S \subseteq \{1, \ldots, n\}$ be a subset of five elements. Set

$$a_S := \sum_{\substack{i,j,k,l,m \text{ with} \\ \{1,j,k,l,m\}=S}} c_{i,j,k,l,m}^2 \quad \text{and} \quad b_S := \sum_{\substack{i,j,k,l,m \text{ with} \\ \{1,j,k,l,m\}=S}} c_{i,j,k,l,m}^4$$

with the $c_{i,j,k,l,m}$ defined in (1.1). These are clearly functions in $K(\underline{x})$ which are invariant under the action of $\mathrm{PGL}_3(K)$ and under all those permutations from $\Sigma_n$ which map $S$ to itself.

**Theorem 3.3.** *With the above notation, take additional indeterminates $X$, $T_1$, and $T_2$, assume the characteristic of $K$ is not 2, and form the polynomial*

$$F := \prod_{\substack{S \subseteq \{1,\ldots,n\}, \\ |S|=5}} (X - T_1 a_S - T_2 b_S) \in K(\underline{x})[X, T_1, T_2].$$

*Then the coefficients of $F$ (considered as a polynomial in $X$, $T_1$, $T_2$) form a generating set for the invariant field $K(\underline{x})_0^{\Sigma_n \times \mathrm{PGL}_3(K)}$.*

*Proof.* We may assume $n \geq 5$, since for $n \leq 4$ all invariants of $\mathrm{PGL}_3(K)$ are constant, and the polynomial $F$ is the empty product, so we are claiming $K(\underline{x})_0^{\Sigma_n \times \mathrm{PGL}_3(K)} = K$ in this case, which is true.

Write $L$ for the field extension of $K$ generated by the coefficients of $F$, and set

$$\mathcal{M} := \{S \subseteq \{1, \ldots, n\} \mid |S| = 5\}.$$

Since the coefficients of $F$ are rational functions in the $c_{i,j,k,l,m}$, it follows that all elements from $L$ are $\mathrm{PGL}_3(K)$-invariant. Moreover, any $\pi \in \Sigma_n$ affords a permutation of $\mathcal{M}$, hence the product $F$, and therefore its coefficients, are fixed by $\pi$. It follows that $L \subseteq K(\underline{x})_0^{\Sigma_n \times \mathrm{PGL}_3(K)}$.

To prove the reverse inclusion, set

$$\mathcal{C} := \{c_{i,j,k,l,m} \mid i, j, k, l, m \in \{1, \ldots, n\} \text{ pairwise distinct}\},$$

and for $S \in \mathcal{M}$ set

$$\mathcal{C}_S := \{c_{i,j,k,l,m} \in \mathcal{C} \mid \{i, j, k, l, m\} = S\},$$

so $\mathcal{C}$ is the disjoint union of all the $\mathcal{C}_S$. For $S \in \mathcal{M}$, the polynomial

$$f_S := \prod_{c_{i,j,k,l,m} \in \mathcal{C}_S} (X - c_{i,j,k,l,m})$$

has coefficients which are invariant under all permutations of the set $S$. With $S_0 := \{1, 2, 3, 4, 5\}$, Theorem 2.2 may be restated as

$$K(\mathcal{C}_{S_0})^{\Sigma_5} = K(x_{\nu,\mu} \mid \nu \in \{1, \ldots, 5\}, \mu = 0, 1, 2)^{\Sigma_5 \times \mathrm{PGL}_3(K)} = K(a_{S_0}, b_{S_0}) \qquad (3.4)$$

(where Theorem 1.2 was used for the first equality), so we obtain $f_{S_0} \in K(a_{S_0}, b_{S_0})[X]$. Thus we can write $f_{S_0} = R(a_{S_0}, b_{S_0}, X)$, where $R$ is a rational function of three arguments (with the third argument not appearing in the denominator of $R$). But exactly the same will be true if we replace the indices $1, 2, 3, 4, 5$ by indices $i, j, k, l, m$ with $\{i, j, k, l, m\} = S$. So we obtain

$$f_S = R(a_S, b_S, X) \qquad (3.5)$$

for all $S \in \mathcal{M}$ with $R \in K(Y, Z, X)$ a rational function not depending on $S$. This equation will be used later in the proof. Here we conclude that

$$f := \prod_{c_{i,j,k,l,m} \in \mathcal{C}} (X - c_{i,j,k,l,m}) = \prod_{S \in \mathcal{M}} f_S \in K(a_S, b_S \mid S \in \mathcal{M})[X].$$

Let $\sigma$ be a $K$-automorphism of $K(a_S, b_S \mid S \in \mathcal{M})$ which is given by a permutation $\psi$ of the set $\mathcal{M}$. Then by (3.5), $\sigma$ permutes the factors $f_S$ of $f$ and therefore fixes $f$. Thus the coefficients of $f$ lie in the fixed field of all automorphisms $\sigma$ of this type. Moreover, the $a_S$ and $b_S$ are pairwise distinct, since $a_S$ and $b_S$ are distinct, and for different sets $S$ they involve different sets of variables $x_{\nu,\mu}$. Hence we can use Lemma 3.2, which tells us that the coefficients of $f$ lie in $L$. It follows that the field $K(\mathcal{C})$ generated by the roots of $f$ is the splitting field of $f$ over $L$. Since the $c_{i,j,k,l,m} \in \mathcal{C}$ are pairwise distinct (as we defined $\mathcal{C}$ as a *set*), $f$ is separable, and therefore $K(\mathcal{C})$ is Galois as a field extension of $L$. Assume that we can show that $\mathrm{Gal}(K(\mathcal{C})/L)$ is contained in $\Sigma_n$ (i.e., every $\sigma$ in the Galois group is given by a permutation from $\Sigma_n$ acting on the $c_{i,j,k,l,m} \in \mathcal{C}$ by permuting the indices), then we have

$$K(\underline{x})_0^{\Sigma_n \times \mathrm{PGL}_3(K)} = K(\mathcal{C})^{\Sigma_n} \subseteq K(\mathcal{C})^{\mathrm{Gal}(K(\mathcal{C})/L)} = L$$

(where Theorem 1.2(a) was used for the first equation), and we are done. Thus all we need to show is

$$\mathrm{Gal}(K(\mathcal{C})/L) \subseteq \Sigma_n. \qquad (3.6)$$

So take $\sigma \in \mathrm{Gal}(K(\mathcal{C})/L)$. Since $K(\mathcal{C})$ is the splitting field of $f$ over $L$, $\sigma$ permutes the set $\mathcal{C}$. Moreover, we have

$$\prod_{S \in \mathcal{M}} (X - T_1 a_S - T_2 b_S) = F = \sigma(F) = \prod_{S \in \mathcal{M}} (X - T_1 \sigma(a_S) - T_2 \sigma(b_S)).$$

Since the roots of a polynomial are unique up to permutation, there exists a permutation $\psi$ of $\mathcal{M}$ such that

$$\sigma(a_S) = a_{\psi(S)} \quad \text{and} \quad \sigma(b_S) = b_{\psi(S)} \qquad (3.7)$$

for all $S \in \mathcal{M}$. Together with (3.5), this implies $\sigma(f_S) = f_{\psi(S)}$. Using the definition of $f_S$, this means that

$$\prod_{c_{i,j,k,l,m} \in \mathcal{C}_S} (X - \sigma(c_{i,j,k,l,m})) = \prod_{c_{i,j,k,l,m} \in \mathcal{C}_{\psi(S)}} (X - c_{i,j,k,l,m}),$$

so $\sigma(\mathcal{C}_S) = \mathcal{C}_{\psi(S)}$.

Fix an $S \in \mathcal{M}$ and pick a bijection $\pi_0 \colon \psi(S) \to S$. Define a $K$-automorphism

$$\varphi_{\pi_0} \colon K(x_{\nu,\mu} \mid \nu \in \psi(S), \mu = 0, 1, 2) \to K(x_{\nu,\mu} \mid \nu \in S, \mu = 0, 1, 2)$$

by setting $\varphi_{\pi_0}(x_{\nu,\mu}) := x_{\pi_0(\nu),\mu}$. Then for $\{i, j, k, l, m\} = \psi(S)$ we have $\varphi_{\pi_0}(c_{i,j,k,l,m}) = c_{\pi_0(i),\pi_0(j),\pi_0(k),\pi_0(l),\pi_0(m)}$, so $\varphi_{\pi_0}(a_{\psi(S)}) = a_S$ and $\varphi_{\pi_0}(b_{\psi(S)}) = b_S$. Together with (3.7) this implies $(\varphi_{\pi_0} \circ \sigma)(a_S) = a_S$ and $(\varphi_{\pi_0} \circ \sigma)(b_S) = b_S$. From $\sigma(\mathcal{C}_S) = \mathcal{C}_{\psi(S)}$ we see that $\varphi_{\pi_0} \circ \sigma$ maps

$K(\mathcal{C}_S)$ to itself. Therefore $\varphi_{\pi_0} \circ \sigma$ restricted to $K(\mathcal{C}_S)$ is a $K$-automorphism which fixes $a_S$ and $b_S$. But we have $K(\mathcal{C}_S)^{\Sigma_S} = K(a_S, b_S)$, where $\Sigma_S$ is the group of all permutations of $S$ (this is (3.4) restated with the indices $1, 2, 3, 4, 5$ replaced by $i, j, k, l, m$ with $\{i, j, k, l, m\} = S$). By Galois theory, this implies that $\varphi_{\pi_0} \circ \sigma$ restricted to $K(\mathcal{C}_S)$ lies in $\Sigma_S$, i.e., there exists $\pi \in \Sigma_S$ such that $(\varphi_{\pi_0} \circ \sigma)(c_{i,j,k,l,m}) = c_{\pi(i),\pi(j),\pi(k),\pi(l),\pi(m)}$ for all $i, j, k, l, m$ with $\{i, j, k, l, m\} = S$. Set $\pi_S := \pi_0^{-1} \circ \pi \colon S \to \psi(S)$. Then $\pi_S$ is a bijection and we have $\sigma(c_{i,j,k,l,m}) = c_{\pi_S(i),\pi_S(j),\pi_S(k),\pi_S(l),\pi_S(m)}$ for all $i, j, k, l, m$ with $\{i, j, k, l, m\} = S$. This can be done with all $S \in \mathcal{M}$.

In summary, we have a permutation $\psi$ of $\mathcal{M}$, and for each $S \in \mathcal{M}$ we have a bijection $\pi_S \colon S \to \varphi(S)$ such that

$$\sigma(c_{i,j,k,l,m}) = c_{\pi_S(i),\pi_S(j),\pi_S(k),\pi_S(l),\pi_S(m)} \quad \text{where} \quad S = \{i, j, k, l, m\}.$$

Being a field-automorphism, $\sigma$ preserves all algebraic relations that exist between the $c_{i,j,k,l,m}$. Thus we are exactly in the situation of Lemma 3.1, which tells us that $\sigma$ lies in $\Sigma_n$. Thus (3.6) is shown and the proof is complete. $\qquad\square$

**Remark.**    (a) Everything that was said in Remark 2.3(a) about the computation of the invariants $a$ and $b$ applies to the computation of the $a_S$ and $b_S$ used in Theorem 3.3, too. In particular, for each subset $S \subseteq \{1, \ldots, n\}$ with five elements, one only needs to evaluate two of the $c_{i,j,k,l,m}$ in order to calculate $a_S$ and $b_S$.

(b) As in the case of Theorem 2.2, we can also deal with the case $\mathrm{char}(K) = 2$ (see Remark 2.3(c)).

We will now turn to looking at separating properties of our invariants. We need the following lemma.

**Lemma 3.4.** *Let $K$ be any field and let $g_1, \ldots, g_m \in K(x_1, \ldots, x_n)$ be rational functions in $n$ indeterminates over $K$. Moreover, assume that $G$ is a finite group acting by $K$-automorphisms on the subfield $K(g_1, \ldots, g_m)$ generated by the $g_i$. Let $f_1, \ldots, f_r$ be generators of the invariant field, i.e., assume $K(g_1, \ldots, g_m)^G = K(f_1, \ldots, f_r)$. Then there exists a non-zero polynomial $h \in K[x_1, \ldots, x_n] \setminus \{0\}$ such that for all $\xi_1, \ldots, \xi_n \in K$ with $h(\xi_1, \ldots, \xi_n) \neq 0$ the following holds: If $\eta_1, \ldots, \eta_n \in K$ are such that $f_i(\eta_1, \ldots, \eta_n) = f_i(\xi_1, \ldots, \xi_n)$ for all $i \in \{1, \ldots, r\}$ (which is meant to imply that no zero-division occurs on either side of the equation), then there exists $\sigma \in G$ such that*

$$g_i(\eta_1, \ldots, \eta_n) = (\sigma(g_i))(\xi_1, \ldots, \xi_n) \quad \text{for} \quad i \in \{1, \ldots, m\}.$$

*Moreover, $h$ can be chosen as the numerator of a polynomial in $f_1, \ldots, f_n$ (viewed as a rational function in $K(x_1, \ldots, x_n)$).*

*Proof.* Parts of this proof are drawn from the proof of Theorem 3.9.13 in Derksen and Kemper [3]. Take additional indeterminates $X$ and $T$, and form the polynomial

$$F := \prod_{\sigma \in G} \left( X - \sum_{i=1}^{m} \sigma(g_i) \cdot T^{i-1} \right) \in K(x_1, \ldots, x_n)[X, T].$$

$F$ is invariant under the action of $G$, thus all coefficients of $F$ lie in $K(g_1, \ldots, g_m)^G = K(f_1, \ldots, f_r)$. Let $c$ be a coefficient of $F$. Then we can write $c = F_c(f_1, \ldots, f_r)/H_c(f_1, \ldots, f_r)$ with $F_c, H_c \in K[T_1, \ldots, T_r]$ polynomials and $H_c(f_1, \ldots, f_r) \neq 0$. Set $H \in K[T_1, \ldots, T_r]$ to be the lcm of all $H_c$ with $c$ a coefficient of $F$. Thus $H(f_1, \ldots, f_r) \neq 0$. Let $h \in K[x_1, \ldots, x_n]$ be the numerator of $H(f_1, \ldots, f_r)$ (as a rational function in $K(x_1, \ldots, x_n)$). Now assume we have $\xi_1, \ldots, \xi_n, \eta_1, \ldots, \eta_n \in K$ such that $h(\xi_1, \ldots, \xi_n) \neq 0$ and

$$f_i(\xi_1, \ldots, \xi_n) = f_i(\eta_1, \ldots, \eta_n) \quad \text{for} \quad i \in \{1, \ldots, r\}. \tag{3.8}$$

It follows that $(H(f_1, \ldots, f_r))(\xi_1, \ldots, \xi_n)$ is non-zero, and by (3.8) the same is true for $(H(f_1, \ldots, f_r))(\eta_1, \ldots, \eta_n)$. Thus every coefficient $c$ of $F$ can be evaluated at $(\xi_1, \ldots, \xi_n)$ and at

$(\eta_1, \ldots, \eta_n)$, and we have $c(\xi_1, \ldots, \xi_n) = c(\eta_1, \ldots, \eta_n)$. For $\sigma \in G$, write $a_\sigma := \sum_{i=1}^{m} \sigma(g_i) \cdot T^{i-1} \in K(x_1, \ldots, x_n)[T]$. It follows from the definition of $F$ that for every $\sigma \in G$ we have $F(a_\sigma) = 0$, where $X$ is taken as the main variable of $F$. Since $F$ is monic, it follows that an irreducible polynomial from $K[x_1, \ldots, x_n, T]$ which divides the denominator of $a_\sigma$ must also divide the denominator of at least one coefficient from $F$. Thus the fact that no zero-division occurs when substituting $(x_1, \ldots, x_n) = (\xi_1, \ldots, \xi_n)$ or $(x_1, \ldots, x_n) = (\eta_1, \ldots, \eta_n)$ into the coefficients of $F$ implies that also all $a_\sigma$ and hence all $\sigma(g_i)$ can be evaluated at $(\xi_1, \ldots, \xi_n)$ and at $(\eta_1, \ldots, \eta_n)$. Using $c(\xi_1, \ldots, \xi_n) = c(\eta_1, \ldots, \eta_n)$ for all coefficients $c$ of $F$, we conclude that

$$\prod_{\sigma \in G} \left( X - \sum_{i=1}^{m} (\sigma(g_i)) (\xi_1, \ldots, \xi_n) \cdot T^{i-1} \right) = \prod_{\sigma \in G} \left( X - \sum_{i=1}^{m} (\sigma(g_i)) (\eta_1, \ldots, \eta_n) \cdot T^{i-1} \right).$$

The right hand side, regarded as a polynomial in $X$, has the zero $\sum_{i=1}^{m} g_i(\eta_1, \ldots, \eta_n) \cdot T^{i-1}$. This must also be a zero of the left hand side, hence there exists a $\sigma \in G$ such that

$$\sum_{i=1}^{m} g_i(\eta_1, \ldots, \eta_n) \cdot T^{i-1} = \sum_{i=1}^{m} (\sigma(g_i)) (\xi_1, \ldots, \xi_n) \cdot T^{i-1}.$$

Comparing coefficients in $T$ now yields $g_i(\eta_1, \ldots, \eta_n) = (\sigma(g_i)) (\xi_1, \ldots, \xi_n)$ for $i \in \{1, \ldots, m\}$, as desired. $\qquad\square$

If we have $n$ points $P_1, \ldots, P_n \in \mathbb{P}^2(K)$ in projective 2-space such that no three of the $P_i$ are collinear, we can evaluate the invariants $a_S$ and $b_S$ at $(P_1, \ldots, P_n)$ for every subset $S \subseteq \{1, \ldots, n\}$ with $|S| = 5$. Thus for each $S$ we obtain a vector $(a_S(\underline{P}), b_S(\underline{P})) \in K^2$. We will consider the *distribution* of these vectors for all subsets $S$. This distribution is adequately represented by the polynomial

$$F_{P_1, \ldots, P_n} := \prod_{\substack{S \subseteq \{1, \ldots, n\}, \\ |S|=5}} \left( X - T_1 a_S(P_1, \ldots, P_n) - T_2 b_S(P_1, \ldots, P_n) \right) \in K[X, T_1, T_2]$$

with $X, T_1, T_2$ indeterminates. It is our goal to use these distributions for two point configurations $(P_1, \ldots, P_n)$ and $(Q_1, \ldots, Q_n) \in \left( \mathbb{P}^2(K) \right)^n$ to determine if $(P_1, \ldots, P_n)$ can be transformed into $(Q_1, \ldots, Q_n)$ by a projective transformation and a relabeling the points. We call a point configuration $(P_1, \ldots, P_n) \in \left( \mathbb{P}^2(K) \right)^n$ **reconstructible from the joint distribution of $a$'s and $b$'s** if for any other $(Q_1, \ldots, Q_n) \in \left( \mathbb{P}^2(K) \right)^n$ with

$$F_{P_1, \ldots, P_n} = F_{Q_1, \ldots, Q_n}$$

there exist a permutation $\pi \in \Sigma_n$ and a transformation $g \in \mathrm{PGL}_3(K)$ such that

$$Q_i = g \left( P_{\pi(i)} \right)$$

for all $i \in \{1, \ldots, n\}$. In order to be able to apply Theorem 3.3, we assume that the characteristic of $K$ is not 2.

**Corollary 3.5.** *With the above notation there exists a non-zero polynomial $f \in K[\underline{x}] = K[x_{i,j} \mid i = 1, \ldots, n, j = 0, 1, 2]$ which for each $i$ is homogeneous as a polynomial in $x_{i,0}, x_{i,1}, x_{i,2}$, such that every point configuration $(P_1, \ldots, P_n) \in \left( \mathbb{P}^2(K) \right)^n$ with $f(P_1, \ldots, P_n) \neq 0$ is reconstructible from the joint distribution of $a$'s and $b$'s.*

*Proof.* Let $G := \Sigma_n$ be the symmetric group acting on the set

$$\mathcal{C} := \{c_{i,j,k,l,m} \mid i, j, k, l, m \in \{1, \ldots, n\} \text{ pairwise distinct}\}$$

by permuting the indices of the $c$'s. Thus $G$ acts by $K$-automorphisms on the field $K(\mathcal{C})$ generated by the $c_{i,j,k,l,m}$. By Theorem 1.2(a) we have that $K(\mathcal{C}) = K(\underline{x})_0^{\mathrm{PGL}_3(K)}$. Write $f_1, \ldots, f_r \in K(\mathcal{C})$ for the coefficients of the polynomial $F$ defined in Theorem 3.3. Then Theorem 3.3 says that

$$K(\mathcal{C})^G = K(\underline{x})_0^{\Sigma_5 \times \mathrm{PGL}_3(K)} = K(f_1, \ldots, f_r).$$

Thus we are exactly in the situation of Lemma 3.4, which gives us a polynomial $h \in K[\underline{x}]$ with the properties stated in the lemma. Since $h$ is the numerator of a polynomial involving the $f_i$ (and therefore the $c_{i,j,k,l,m}$, which lie in $K(\underline{x})_0$), $f$ is homogeneous as a polynomial in $x_{i,0}$, $x_{i,1}$, $x_{i,2}$ for each $i$ (see the proof of Theorem 1.2). Let $f$ be the product of $h$ and all determinants $[i,j,k]$ (defined before (1.1)) with $1 \le i < j < k \le n$. Now take $(P_1, \ldots, P_n) \in \left(\mathbb{P}^2(K)\right)^n$ and assume $f(P_1, \ldots, P_n) \ne 0$. Moreover, take $(Q_1, \ldots, Q_n) \in \left(\mathbb{P}^2(K)\right)^n$ with $F_{P_1,\ldots,P_n} = F_{Q_1,\ldots,Q_n}$. This means that all coefficients of $F$ take the same value when evaluated at $(P_1, \ldots, P_n)$ or at $(Q_1, \ldots, Q_n)$, so $f_i(P_1, \ldots, P_n) = f_i(Q_1, \ldots, Q_n)$ for $i = 1, \ldots, r$. By Lemma 3.4 there exists a $\pi \in G$ such that

$$c_{i,j,k,l,m}(Q_1, \ldots, Q_n) = \left(\pi(c_{i,j,k,l,m})\right)(Q_1, \ldots, P_n) = c_{i,j,k,l,m}(P_{\pi(1)}, \ldots, P_{\pi(n)})$$

for all $i, j, k, l, m \in \{1, \ldots, n\}$ pairwise distinct. Since $f(P_1, \ldots, P_n) \ne 0$ guarantees that no three of the $P_i$ are collinear, it follows from Theorem 1.2(b) that there exists a $g \in \mathrm{PGL}_3(K)$ such that $Q_i = g\left(P_{\pi(i)}\right)$ for all $i = 1, \ldots, n$. So $(P_1, \ldots, P_n)$ is reconstructible from the joint distribution of $a$'s and $b$'s.    $\square$

# 4  Other groups

In this paper and in [2], we only considered some very specific (though important) groups, namely projective, Euclidean and volume-preserving groups. In this section we will look at more general groups. The goal is to use reconstruction theorems such as Corollary 3.5 for deriving reconstructibility statements which classify a point configuration modulo any subgroup of the original group. We will be more precise after proving the following lemma.

**Lemma 4.1.** *Let $n$ and $m$ be integers with $0 < m < n$. Then the natural action of the symmetric group $\Sigma_n$ on the set*

$$\mathfrak{X} := \{M \subseteq \{1, \ldots, n\} \mid |M| = m\}$$

*is faithful.*

*Proof.* Suppose that for a $\pi \in \Sigma_n$ we have $\pi(M) = M$ for all $M \in \mathfrak{X}$. Take any $i \in \{1, \ldots, n\}$. Then

$$\pi\left(\{i\}\right) = \pi\left(\bigcap_{\substack{M \in \mathfrak{X}, \\ i \in M}} M\right) = \bigcap_{\substack{M \in \mathfrak{X}, \\ i \in M}} \pi(M) = \bigcap_{\substack{M \in \mathfrak{X}, \\ i \in M}} M = \{i\},$$

where the second equality follows from the injectiveness of $\pi$. Hence $\pi(i) = i$.    $\square$

Let $X$ be any set (e.g., a projective or linear space) and let $G$ be a group acting on $X$. For $M \subseteq X$ and $g \in G$ we write

$$g(M) := \{g(x) \mid x \in M\} \quad \text{and} \quad G(M) := \{g(M) \mid g \in G\}.$$

Thus $G(M)$ is a subset of the power set $\mathfrak{P}(X)$ of $X$. We may think of $X$ as a set of points and of $M$ (if finite) as a point configuration, where the labeling of the points in $M$ is already disregarded since we are considering $M$ as a set. Then $G(M)$ is the class of all point-configurations which are "congruent" to $M$, where the concept of "congruence" is given by the $G$-action. Fix a positive integer $m$. For $C \subseteq X$ a finite subset let $\mu_{m,G}(C)$ be the multiset formed of all $G(M)$ with $M \subseteq C$

and $|M| = m$. Formally, $\mu_{m,G}(C)$ may be defined as the function $\mathfrak{P}(\mathfrak{P}(X)) \to \mathbb{Z}$ assigning to each subset $\mathfrak{X} \subseteq \mathfrak{P}(X)$ the number $|\{M \subseteq C \mid |M| = m, \ G(M) = \mathfrak{X}\}|$. So $\mu_{m,G}(C)$ may be viewed as the distribution of all $m$-subsets of $C$ up to the $G$-action. Clearly for any $g \in G$ we have $\mu_{m,G}(g(C)) = \mu_{m,G}(C)$. We call $C$ **reconstructible from $m$-subsets modulo** $G$ if for every finite subset $D \subseteq X$ with $\mu_{m,G}(D) = \mu_{m,G}(C)$ there exists $g \in G$ with $D = g(C)$.

In this language, Corollary 3.5 implies that "almost" all finite subsets of $\mathbb{P}^2(K)$ are reconstructible from 5-subsets modulo $\mathrm{PGL}_3(K)$. Likewise, Theorem 1.6 from Boutin and Kemper [2] says that almost all finite subsets of $K^m$ (of size $\geq m+2$) are reconstructible from 2-subsets modulo the Euclidean group $\mathrm{AO}_m$.

**Theorem 4.2.** *With the above notation assume that*

*(i) $C$ is reconstructible from $m$-subsets modulo $G$,*

*(ii) for $M, N \subseteq C$ with $|M| = |N| = m$, we have that $G(M) = G(N)$ implies $M = N$, and*

*(iii) there exists a subset $\hat{M} \subseteq C$ with $|\hat{M}| = m + 1$ such that*

$$\left\{ g \in G \mid g(x) = x \text{ for all } x \in \hat{M} \right\} = \{\mathrm{id}\}.$$

*Then for every subgroup $H \leq G$, $C$ is reconstructible from $(m + 1)$-subsets modulo $H$.*

*Proof.* Let $D \subseteq X$ be a finite set with

$$\mu_{m+1,H}(D) = \mu_{m+1,H}(C). \tag{4.1}$$

We wish to show that there exists $h \in H$ with $D = h(C)$. Since $|\mu_{m+1,H}(C)| = \binom{|C|}{m+1}$ and $|C| \geq m+1$ by the assumption (iii), (4.1) certainly implies $|D| = |C|$. Take any subset $M \subseteq C$ with $|M| = m$. The assumption (iii) implies that $|C| > m$, so there exists $x \in C \setminus M$. Set $M' := M \cup \{x\}$. By (4.1) there exists $N' \subseteq D$ with $|N'| = m + 1$ such that $H(M') = H(N')$. So there exists $g \in H$ with $M' = g(N')$. Thus we have $M \subset g(N')$, so there exists a subset $N \subset N'$ with $|N| = m$ and $M = g(N)$. This implies $G(M) = G(N)$. Since $M$ was taken to be an arbitrary $m$-subset of $C$, it follows that $\mu_{m,G}(C) \subseteq \mu_{m,G}(D)$ (observe that by (ii) the multiset $\mu_{m,G}(C)$ has no multiplicities). Since $|C| = |D|$, the cardinalities of $\mu_{m,G}(C)$ and $\mu_{m,G}(D)$ also coincide, and we conclude $\mu_{m,G}(C) = \mu_{m,G}(D)$. Note that this implies that the assumption (ii) also holds for $C$ replaced by $D$. But the main consequence of $\mu_{m,G}(C) = \mu_{m,G}(D)$ is that by (i) there exists $g \in G$ such that

$$g(C) = D. \tag{4.2}$$

Now we consider the subset $\hat{M} \subseteq C$ given by (iii). By (4.1) we have a subset $\hat{N} \subseteq D$ with $|\hat{N}| = m+1$ and $H(\hat{M}) = H(\hat{N})$. So there exists $h \in H$ with $h(\hat{M}) = \hat{N}$. Take any $M \subset \hat{M}$ with $|M| = m$. Then

$$N := h(M) \subset h(\hat{M}) = \hat{N} \subseteq D.$$

$N = h(M)$ implies $G(N) = G(M)$. For $\widetilde{N} := g(M)$ (with $g$ from (4.2)) we also have $G(\widetilde{N}) = G(M)$, so $G(\widetilde{N}) = G(N)$. By (4.2), $\widetilde{N} \subseteq D$, and since (ii) also holds with $C$ replaced by $D$, we conclude that $\widetilde{N} = N$, e.i., $g(M) = h(M)$. This holds for any $m$-subset $M \subset \hat{M}$. Thus

$$g(\hat{M}) = g \Big( \bigcup_{\substack{M \subset \hat{M}, \\ |M|=m}} M \Big) = \bigcup_{\substack{M \subset \hat{M}, \\ |M|=m}} g(M) = \bigcup_{\substack{M \subset \hat{M}, \\ |M|=m}} h(M) = h \Big( \bigcup_{\substack{M \subset \hat{M}, \\ |M|=m}} M \Big) = h(\hat{M}).$$

It follows that $h^{-1} \circ g$ restricts to a permutation $\pi$ of $\hat{M}$. Since $g(M) = h(M)$ for all $m$-subsets $M \subset \hat{M}$, $\pi(M) = M$ for all these $M$. It follows by Lemma 4.1 that $\pi = \mathrm{id}$. Thus $g|_{\hat{M}} = h|_{\hat{M}}$ (the restrictions to $\hat{M}$ coincide). Now (iii) yields $g = h$, so (4.2) implies $h(C) = D$, which completes the proof. $\qquad\square$

**Corollary 4.3** (consequence of Theorem 4.2 and Corollary 3.5)**.** *Let $K$ be an infinite field and $n \geq 6$ an integer. Then there exists a non-zero polynomial $f \in K[\underline{x}] = K[x_{i,j} \mid i = 1, \ldots, n, j = 0, 1, 2]$ which for each $i$ is homogeneous as a polynomial in $x_{i,0}, x_{i,1}, x_{i,2}$, such that for every point configuration $(P_1, \ldots, P_n) \in \left(\mathbb{P}^2(K)\right)^n$ with $f(P_1, \ldots, P_n) \neq 0$ the set $\{P_1, \ldots, P_n\}$ is reconstructible from 6-subsets modulo $G$ for every subgroup $G \leq \mathrm{PGL}_3(K)$.*

*Proof.* By Corollary 3.5 there exists a non-zero polynomial $\widetilde{f}$ such that all $(P_1, \ldots, P_n)$ with $\widetilde{f}(P_1, \ldots, P_n) \neq 0$ is reconstructible from the joint distribution of $a$'s and $b$'s. In particular, this means that for such $(P_1, \ldots, P_n)$ the set $\{P_1, \ldots, P_n\}$ is reconstructible from 5-subsets modulo $\mathrm{PGL}_3$. This provides the hypothesis (i) of Theorem 4.2. The hypothesis (ii) can also be turned into an open condition on $(P_1, \ldots, P_n)$. Indeed, it is enough to impose that for distinct 5-subsets $M$ and $N$ of $\{P_1, \ldots, P_n\}$, the pairs $(a(M), b(M))$ and $(a(N), b(N))$ (with $a$ and $b$ the $(\Sigma_5 \times \mathrm{PGL}_3)$-invariants defined in Theorem 2.2) are also distinct. To make sure that (iii) also holds, it suffices by the uniqueness statement in Lemma 1.1 that there exist four points in $\{P_1, \ldots, P_n\}$ such that no three of them are collinear, which is also an open condition. Finally, one should impose the condition that the $P_i$ are pairwise distinct to ensure that the set of the $P_i$ really has size $n$.     $\square$

In the following corollary, $K$ is any field and $V$ is an $m$-dimensional vector space over $K$. We write $V^n$ for the direct sum of $n$ copies of $V$, and $K[V^n]$ for the ring of polynomials on $V^n$. $\mathrm{ASL}^{\pm}(V)$ is the group generated by all linear transformations of $V$ with determinant $\pm 1$ and all translations of $V$.

**Corollary 4.4** (consequence of Theorem 4.2 and Theorem 3.7 from Boutin and Kemper [2])**.** *Assume $n \geq m + 2$. Then there exists a non-zero polynomial $f \in K[V^n]$ such that for $(P_1, \ldots, P_n) \in V^n$ with $f(P_1, \ldots, P_n) \neq 0$, the set $\{P_1, \ldots, P_n\}$ is reconstructible from $(m + 2)$-subsets modulo $G$ for every subgroup $G \leq \mathrm{ASL}^{\pm}(V)$.*

*Proof.* Theorem 3.7 from Boutin and Kemper [2] says that there exists $\widetilde{f} \in K[V^n] \setminus \{0\}$ such that all $(P_1, \ldots, P_n) \in V^n$ with $\widetilde{f}(P_1, \ldots, f_n) \neq 0$ are reconstructible (up to the actions of $\mathrm{ASL}^{\pm}(V)$ and the symmetric group $\Sigma_n$) from the distribution of volumes of parallelepiped spanned by $(m + 1)$-subsets. In particular, for these $(P_1, \ldots, P_n)$, the set $\{P_1, \ldots, P_n\}$ is reconstructible from $(m + 1)$-subsets modulo $\mathrm{ASL}^{\pm}(V)$. Moreover, imposing that for distinct $(m + 1)$-subsets of $\{P_1, \ldots, P_n\}$ the volumes of the parallelepiped spanned by these subsets also differ is an open condition. Finally, the assumption (iii) in Theorem 4.2 is satisfied if $\{P_1, \ldots, P_n\}$ contains $m + 1$ points which span a parallelepiped of non-zero volume.     $\square$

**Remark 4.5.** Suppose that in the situation of Corollary 4.4 we have (rational) invariants $f_1, \ldots, f_r \in K(V^{m+2})^{\Sigma_{m+2} \times G}$ (where $K(V^{m+2})$ is the rational function field on $V^{m+2}$ and $G$ is the subgroup of $\mathrm{ASL}^{\pm}(V)$ which is considered) such that for a non-empty Zariski-open subset $S \subseteq V^{m+2}$ the invariants $f_i$ can be evaluated on $S$, and for $(P_1, \ldots, P_{m+2}) \in S$ and $(Q_1, \ldots, Q_{m+2}) \in V^{m+2}$ we have that $f_i(P_1, \ldots, P_{m+2}) = f_i(Q_1, \ldots, Q_{m+2})$ for all $i$ implies that $Q_i = g(P_{\pi(i)})$ with $g \in G$ and $\pi \in \Sigma_{m+2}$. Then it follows from Corollary 4.4 that for $n \geq m + 2$ there exists $f \in K[V^n] \setminus \{0\}$ such that all $(P_1, \ldots, P_n) \in V^n$ with $f(P_1, \ldots, P_n) \neq 0$ are reconstructible (modulo the actions of $G$ and $\Sigma_n$) from the joint distribution of $f_1, \ldots, f_r$ (i.e., the distribution of the values $(f_1(M), \ldots, f_r(M)) \in K^r$, where $M$ ranges through all $(m + 2)$-subsets of $\{P_1, \ldots, P_n\}$).

The analogous remark applies in the situation of Corollary 4.3.

*Example 4.6.* This example shows that in Corollary 4.4 the number $m + 2$ cannot be reduced to a lower number. Consider the case $m = 1$ (i.e., $V = K$, and let $G \cong K$ be the group of all translations. Consider a point-configuration $C := \{P_1, \ldots, P_n\} \subseteq K$ and its negative $-C := \{-P_1, \ldots, -P_n\}$. For a 2-subset $\{P_i, P_j\} \subseteq C$ the group element $g := -P_i - P_j$ yields

$$g(\{P_i, P_j\}) = \{-P_j, -P_i\} \subseteq -C.$$

Hence $\mu_{2,G}(C) = \mu_{2,G}(-C)$. But clearly $C$ and $-C$ are only congruent modulo $G$ if $C$ has a special symmetry property. Thus there exists no non-empty Zariski-open subset $S \subseteq K^n$ such that all $n$-subsets of $K$ formed from tuples from $S$ are reconstructible from 2-subsets modulo $G$. This example shows that also in Theorem 4.2 the number $m + 1$ cannot be decreased.

However, by Corollary 4.4, for every $n \geq 3$ there exists an $f \in K[x_1, \ldots, x_n] \setminus \{0\}$ such that for $(P_1, \ldots, P_n) \in K^n$ with $f(P_1, \ldots, P_n) \neq 0$, the set $\{P_1, \ldots, P_n\}$ is reconstructible from 3-subsets modulo $G$. We can also give invariants in $K[x_1, x_2, x_3]^{\Sigma_3 \times G}$ as in Remark 4.5, which can be found easily by using the invariant theory package in Magma [1]. They are

$$f_1 = x^2 + y^2 + z^2 - xy - xz - yz, \quad f_2 = (2x - y - z)(2y - x - z)(2z - x - y),$$

so almost all $n$-point configurations are determined up to $\Sigma_n \times G$ by the distribution of the vectors $(f_1(x_i, x_j, x_k), f_2(x_i, x_j, x_k))$ for $\{i, j, k\} \subseteq \{1, \ldots, n\}$. ◁

# References

[1] Wieb Bosma, John J. Cannon, Catherine Playoust, *The Magma Algebra System I: The User Language*, J. Symb. Comput. **24** (1997), 235–265.

[2] Mireille Boutin, Gregor Kemper, *On Reconstructing n-Point Configurations from the Distribution of Distances or Areas*, Adv. Applied Math. (2004), to appear.

[3] Harm Derksen, Gregor Kemper, *Computational Invariant Theory*, Encyclopaedia of Mathematical Sciences **130**, Springer-Verlag, Berlin, Heidelberg, New York 2002.

[4] Peter Meer, Reiner Lenz, Sudhir Ramakrishna, *Efficient Invariant Representations*, International Journal of Computer Vision **26** (1998), 137–152.

[5] P. J. Olver, *Moving frames and joint differential invariants*, Regul. Chaotic Dyn. **4(4)** (1999), 3–18.

Mireille Boutin
Department of Mathematics
Purdue University
150 N. University St.
West Lafayette, IN 47907
USA
boutin@math.purdue.edu

Gregor Kemper
Technische Universität München
Zentrum Mathematik - M11
Boltzmannstr. 3
85 748 Garching
Germany
kemper@ma.tum.de