Symmetries of Polynomials*

Irina Berchenko
School of Mathematics
University of Minnesota
Minneapolis, MN 55455
berchenk@math.umn.edu

Peter J. Olver
School of Mathematics
University of Minnesota
Minneapolis, MN 55455
olver@math.umn.edu
http://math.umn.edu/∼olver

Abstract

New algorithms for determining discrete and continuous symmetries of polynomials — also known as binary forms in classical invariant theory — are presented. Implementations in MATHEMATICA and MAPLE are discussed and compared. The results are based on a new, comprehensive theory of moving frames that completely characterizes the equivalence and symmetry properties of submanifolds under general Lie group actions.

*This work was partially supported by NSF Grant DMS 98–03154.

1 Introduction.

The purpose of this paper is to explain the detailed implementation of a new algorithm for determining the symmetries of polynomials (binary forms). The method was first described in the second author's new book [24], and the present paper adds details and refinements. We shall demonstrate that the symmetry group of both real and complex binary forms can be completely determined by solving two simultaneous bivariate polynomial equations, which are based on two fundamental covariants of the form. Bounds on the dimension of the symmetry group, as well as the explicit formulae for the symmetries can be readily established.

Despite the evident simplicity of the particular problem under consideration, our results are new, even for ordinary polynomials. Besides a new algorithm for computing discrete and continuous symmetries, the method also provides a new solution to the equivalence problem for binary forms, based on the identification of their "signature curves" which are explicitly parametrized by two absolute rational covariants. For instance, the method gives new, readily verifiable conditions that a given form be equivalent to a sum of two n^{th} powers. An extensive search has convinced us that most of these results do not have a counterpart in any of the classical, or more recent, invariant-theoretic literature. The method can be easily implemented in most computer algebra systems, including MAPLE or MATHEMATICA — although neither is completely adept at handling the required polynomial computations. The standard routines do not produce fully simplified formulae for the symmetries of reasonably elementary polynomials, and necessitate hands-on manipulations of the formulae to give the correct results. The key weakness of both systems is their poor handling of both algebraic numbers and rational algebraic functions. MAPLE code and illustrative examples appear in the appendices.

The results are based on a new adaptation of Cartan's geometric theory of moving frames and differential invariants, [7, 11, 17], recently developed by the second author and M. Fels, [9, 10]. The theory is completely algorithmic; moreover, it is not restricted to classical geometrical situations, but also applies to general Lie group actions (and, even, infinite-dimensional pseudogroups). The moving frame provides a complete system of differential invariants that govern the symmetry and equivalence properties of submanifolds under the group action. Symmetry and equivalence of binary forms can be readily recast as a very particular case of this general theory. Interestingly, Lie himself, in [20, Chapter 23], championed the applications of Lie group methods and differential invariants in classical invariant theory. However, the adaptations of the moving frame method in this context is new.

Space permits only a short summary of the geometric and algebraic prerequisites here. We refer the reader to [24] for additional details on classical invariant theory and [10] for the moving frame method. There exist a remarkable range of new, as well as classical, applications of moving frames — not only to geometry, [12], but also complete classifications of differential invariants and their syzygies, [10], classification of joint invariants and joint differential invariants, [9], applications to the problem of object recognition in computer vision, [5], and the construction of invariant numerical approximations to differential invariants and invariant differential equations, [6].

2 Symmetries of Binary Forms.

In classical invariant theory, a *binary form* refers to a homogeneous polynomial function of two variables:

$$Q(x,y) = \sum_{i=0}^{n} a_i\, x^i y^{n-i}. \tag{2.1}$$

The coefficients $a_0, \dots, a_n$ can be taken to be either real or complex. There is a direct correspondence between homogeneous binary forms (2.1) and inhomogeneous polynomials

$$Q(p) \equiv Q(p,1) = \sum_{i=0}^{n} a_i \, p^i, \tag{2.2}$$

depending on a single scalar variable p, known as the *projective coordinate*. We can identify $p = x/y$ with the ratio of homogeneous coordinates, and thereby recover the homogeneous form (2.1) via the simple rule

$$Q(x,y) = y^n \, Q\left(\frac{x}{y}\right). \tag{2.3}$$

The passage from a binary form to its inhomogeneous version reflects the passage from a homogeneous function on a vector space to a function (depending on one fewer variable) on the associated projective space. We shall find it useful to retain the same symbol Q for both versions (2.1), (2.2) of the given binary form.

The general linear group

$$\mathrm{GL}(2) = \left\{ \, A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \;\Big|\; \alpha\delta - \beta\gamma \neq 0 \, \right\} \tag{2.4}$$

acts on two-dimensional space by invertible linear transformations

$$\overline{x} = \alpha x + \beta y, \qquad \overline{y} = \gamma x + \delta y, \tag{2.5}$$

and thereby induces an irreducible representation on the space of binary forms of a fixed degree. Both real and complex changes of variables are of interest. In the sequel, we shall concentrate on the complex version, but will also indicate how to adapt the results to real binary forms. Two forms $Q(x,y)$ and $\overline{Q}(\overline{x},\overline{y})$ are called *equivalent* if there exists a linear transformation (2.5) mapping one to the other, so that

$$\overline{Q}(\overline{x},\overline{y}) = \overline{Q}(\alpha x + \beta y, \gamma x + \delta y) = Q(x,y). \tag{2.6}$$

Thus, each linear transformation induces a linear transformation $a_i \mapsto \overline{a}_i$ of the coefficients of Q. The explicit formulae are not difficult to write down, but are not particularly useful. In particular, a *symmetry* of a binary form is, by definition, a linear transformation that maps Q to itself, i.e., a self-equivalence. The principal goal of this paper is to describe an explicit computational algorithm for finding the symmetries of binary forms.

The induced action of a linear transformation (2.5) on the projective coordinate $p = x/y$ is by linear fractional transformations

$$\overline{p} = \frac{\alpha p + \beta}{\gamma p + \delta}. \tag{2.7}$$

Note that two matrices which are scalar multiples of each other, $\widetilde{A} = \lambda A$, induce the same linear fractional transformation, and so (2.7) defines an action of the projective group $\mathrm{PSL}(2) = \mathrm{GL}(2)/\{\lambda \, \mathrm{I}\}$. Let $\pi \colon \mathrm{GL}(2) \to \mathrm{PSL}(2)$ denote the standard projection. The induced transformation rule for inhomogeneous polynomials of degree n, which is

$$Q(p) = (\gamma p + \delta)^n \, \overline{Q}(\bar{p}) = (\gamma p + \delta)^n \, \overline{Q}\left(\frac{\alpha p + \beta}{\gamma p + \delta}\right), \tag{2.8}$$

defines a multiplier representation of $\mathrm{GL}(2)$, cf. [23, 24].

Remark: The degree of an inhomogeneous binary form is not necessarily that of its leading term. For example, the quartic form $x^2y^2+y^4$ has inhomogeneous counterpart p^2+1, which is a degenerate quartic polynomial and *not* a quadratic polynomial. Indeed, the inhomogeneous quartic has four roots — two simple roots at $p = \pm i$ and a double root at $p = \infty$, while the quadratic p^2+1 has only two finite roots. Moreover, the two obey quite different transformation rules (2.8). Consequently, the inhomogeneous form of a polynomial does not uniquely characterize it as a binary form — one must also specify its degree.

Definition 2.1 The *symmetry group* of a binary form Q is the subgroup $G \subset \mathrm{GL}(2)$ consisting of all linear transformations that map Q to itself. The *projective symmetry group* of Q is the subgroup $\Gamma = \pi(G) \subset \mathrm{PSL}(2)$ consisting of all linear fractional transformations (2.7) that give rise to symmetries of Q.

Since $Q(\lambda x, \lambda y) = \lambda^n Q(x,y)$, if ω is any n^{th} root of unity, $\omega^n = 1$, then the diagonal matrix $\omega \mathrm{I}$ always belongs to the symmetry group of Q. Moreover, if $A \in \mathrm{GL}(2)$ is any matrix whose associated linear fractional transformation (2.7) belongs to the projective symmetry group of Q, so that $\pi(A) \in \Gamma$, then A maps Q to a scalar multiple of itself, say $\mu\, Q(p)$. Consequently, the scalar multiple $\widehat{A} = \lambda A$, where $\lambda = 1/\sqrt[n]{\mu}$, is a genuine symmetry of the form.

We conclude that, in the complex case, each element of the projective symmetry group corresponds to n distinct matrices in the full symmetry group. In the real case, if the degree of Q is odd, $n = 2m+1$, then there is a unique real n^{th} root of unity, and each projective symmetry corresponds to a unique symmetry, and so $\Gamma \simeq G$; on the other hand, if the degree of Q is even, $n = 2m$, then each projective symmetry corresponds to two matrix symmetries.

Definition 2.2 A binary form is called *nonsingular* if its symmetry group G is finite. The *index* of a nonsingular binary form $Q(p)$ is the cardinality $\#G$ of its symmetry group. The *projective index* of $Q(p)$ is the cardinality $\#\Gamma$ of its projective symmetry group $\Gamma = \pi(G)$.

Thus, for nonsingular binary forms, the indices are simply related by

$$\#G = l \cdot \#\Gamma, \qquad \text{where} \qquad l = \begin{cases} n & \text{for complex forms of degree } n, \\ 2 & \text{for real forms of even degree } n = 2m, \\ 1 & \text{for real forms of odd degree } n = 2m+1. \end{cases} \tag{2.9}$$

In many cases, the full symmetry group $G \simeq \Gamma \times \mathbb{Z}_n$ is just a Cartesian product of the projective symmetry group with the cyclic group generated by the n^{th} roots of unity, although this is not universally true.

Remark: Each symmetry of a polynomial will permute its roots, and preserve cross-ratios between them, cf. [24]. Hence, there are interesting connections between the geometric symmetry group considered here and the Galois group of the polynomial. However, the precise relationship between the two groups remains, at least to us, a bit obscure.

Our algorithm for determining the symmetry group of a binary form will rely on the following important classical covariants. Recall first that a *covariant* of *weight* k of a binary form Q of degree n is a function $C(a_0, \dots, a_n; x, y)$ depending on the coefficients a_i of Q and on the independent variables x, y, which, up to a determinantal factor, is unchanged under linear transformations:

$$C(a_0, \dots, a_n; x, y) = (\alpha\delta - \beta\gamma)^k \, C(\overline{a}_0, \dots, \overline{a}_n; \overline{x}, \overline{y}). \tag{2.10}$$

The form Q itself is trivially a covariant of weight 0. The simplest nontrivial example is the *Hessian*

$$H = Q_{xx} Q_{yy} - Q_{xy}^2, \tag{2.11}$$

which is a covariant of weight 2. (Subscripts denote partial derivatives of Q.) If C, D are two covariants of a binary form Q, then their *Jacobian*

$$J[C, D] = \frac{\partial(C, D)}{\partial(x, y)} = C_x D_y - C_y D_x \tag{2.12}$$

is also a covariant. If C has weight k, and D has weight l, then $J[C, D]$ has weight $k + l + 1$. For our purposes, the most important Jacobians are the following:

$$T = J[Q, H] = Q_x H_y - Q_y H_x, \qquad U = J[Q, T] = Q_x T_y - Q_y T_x, \tag{2.13}$$

of respective weights 3 and 4. Note that if Q is a binary form of degree n, then H has degree $2n - 4$, while T has degree $3n - 6$ and U has degree $4n - 8$.

Each homogeneous polynomial covariant $C(a_0, \dots, a_n; x, y)$ has an inhomogeneous counterpart

$$C(a_0, \dots, a_n; p) = C(a_0, \dots, a_n; p, 1),$$

which plays a similar role for the inhomogeneous form (2.2). Again, we use the same letter to denote both the homogeneous and inhomogeneous covariant. The inhomogeneous forms of our particular covariants can be computed directly from (2.2) using the following formulae, cf. [13, 24]. First, the Hessian of a polynomial $Q(p)$ of degree n is given by

$$H[Q] = n(n-1) \left[Q Q'' - \frac{n-1}{n} (Q')^2 \right]. \tag{2.14}$$

Formula (2.14) can be used to provide an immediate proof of the following important result.

Proposition 2.3 *A complex binary form $Q(x, y)$ has vanishing Hessian, $H \equiv 0$, if and only if $Q(x, y) = (cx + dy)^n$ is the n^{th} power of a linear form.*

Proof: It suffices to note that $Q(p) = (cp + d)^n$ is the general solution to the elementary second order homogeneous differential equation $QQ'' = \frac{n-1}{n} (Q')^2$. *Q.E.D.*

In other words, the form has identically vanishing Hessian if and only if it can be mapped to the form y^n via a linear transformation. In projective coordinates, this means that the form is equivalent to the constant form $Q(p) \equiv 1$, which has a single root of multiplicity n at $p = \infty$. The same result holds for real forms of odd degree $n = 2m + 1$. For real forms of even degree $n = 2m$, the sign of $Q(p)$ is invariant, and hence real forms with vanishing Hessian have the form $\pm(cp+d)^n$ and are equivalent to one of the two inequivalent constant forms ± 1, depending on the sign of Q.

If $C(p)$ is a covariant of degree k and $D(p)$ a covariant of degree l, then their Jacobian is

$$J[C, D] = l\, C' D - k\, C D'. \tag{2.15}$$

Applying this to the Jacobian covariants (2.13) results in the following formulae. First

$$T = -n^2(n-1) \left[Q^2 Q''' - 3 \frac{(n-2)}{n} Q Q' Q'' + 2 \frac{(n-1)(n-2)}{n^2} (Q')^3 \right]. \tag{2.16}$$

Second,

$$U = n^3(n-1)\,V - 3\,\frac{(n-2)}{(n-1)}\,H^2, \qquad \text{where}$$
$$V = Q^3Q'''' - 4\,\frac{(n-3)}{n}\,Q^2Q'Q''' + 6\,\frac{(n-2)(n-3)}{n^2}\,QQ'^2Q'' - \tag{2.17}$$
$$- 3\,\frac{(n-1)(n-2)(n-3)}{n^3}\,(Q')^4.$$

Note that V is also a covariant of weight 4 and degree $4n-8$.

Since a covariant is scaled by a power of the determinant under a linear transformation, its (nonzero) values do not carry any invariant significance. (But, in the real category, the *sign* of an even weight covariant *is* invariant.) The exceptions are those of weight 0, known as *absolute covariants*, which are typically formed by taking suitable rational combinations of polynomial covariants. In view of the weights of the Hessian and Jacobian covariants, the following particular combinations

$$J = \frac{T^2}{H^3}, \qquad K = \frac{U}{H^2}, \tag{2.18}$$

are absolute rational covariants. Proposition 2.3 implies that J, K are well-defined rational functions provided Q is not the n^{th} power of a linear form. The remarkable fact is that the symmetry and equivalence properties of a binary form are entirely determined by just these two fundamental rational covariants!

Theorem 2.4 *Let $Q(p) \not\equiv 0$ be a nonzero binary form of degree n. The symmetry group of Q is:*

a) A two-parameter group if and only if $H \equiv 0$ if and only if Q is equivalent to a constant.

b) A one-parameter group if and only if $H \not\equiv 0$ and T^2 is a constant multiple of H^3 if and only if Q is complex-equivalent to a monomial p^k, with $k \neq 0, n$.

c) A finite group in all other cases.

Remark: A real binary form is complex-equivalent to a monomial if and only if it is real-equivalent to either a real monomial $\pm p^k$ or to the form $\pm(p^2+1)^m$, the latter only occurring in the case of even degree $n = 2m$.

Therefore, a binary form is nonsingular if and only if its rational covariant J is *not* constant if and only if the form is not complex-equivalent to a monomial. The next result forms the basis for our algorithm for determining the (finite) symmetry group of a nonsingular binary form.

Theorem 2.5 *Let $Q(p)$ be a nonsingular complex binary form. Then $q = \varphi(p)$ is a complex analytic solution to the* rational symmetry equations

$$J(q) = J(p), \qquad K(q) = K(p), \tag{2.19}$$

if and only if $q = (\alpha p + \beta)/(\gamma p + \delta)$ is a linear fractional transformation belonging to the projective symmetry group of Q.

The fact that *all* the solutions to the symmetry equations (2.19) are necessarily linear fractional transformations is striking! As remarked above, given a projective symmetry, the corresponding symmetry matrix $A \in \mathrm{GL}(2)$ is uniquely determined up to multiplication by an n^{th} root of unity. Since the linear fractional transformation only determines A up to a scalar multiple, one must substitute into the transformation rule (2.8) for the form to unambiguously specify the symmetry matrix.

In the real case, if the degree of Q is odd, $n = 2m + 1$, then the basic symmetry Theorem 2.5 holds as stated. Moreover, each real linear fractional solution to the symmetry equations (2.19) corresponds to a unique matrix symmetry. On the other hand, if the degree of Q is even, $n = 2m$, then the sign of Q is invariant, and a real solution to the symmetry equations (2.19) will induce a real projective symmetry, and thereby two real matrix symmetries of the form if and only if it preserves the sign of Q.

Remark: The original transformation rules (2.6), (2.8) apply to binary forms of weight zero. One can, more generally, consider binary forms of nonzero weight k, with transformation rules

$$Q(x,y) = (\alpha\delta - \beta\gamma)^k \, \overline{Q}(\alpha x + \beta y, \gamma x + \delta y), \quad Q(p) = (\alpha\delta - \beta\gamma)^k \, (\gamma p + \delta)^n \, \overline{Q}\left(\frac{\alpha p + \beta}{\gamma p + \delta}\right). \tag{2.20}$$

If $n + 2k \neq 0$, then the projective symmetry group of a weight k binary form is the same as that of its weight 0 counterpart. However, the full symmetry groups may not have the same cardinality, and so are not necessarily isomorphic. In the exceptional case $n = -2k$, if $A \in \mathrm{GL}(2)$ is any symmetry, so is *any* scalar multiple λA, and so each projective symmetry gives rise to a one-parameter family of symmetries in GL(2). Moreover, in this case the projective symmetry group is *not* necessarily the same as that of the weight zero version of the form.

3 Algorithms and Symmetry Bounds.

In this section we discuss the basic algorithms for determining the explicit formulae for the symmetries of a nonsingular complex binary form. The method relies on Theorem 2.5, and hence requires solving the fundamental symmetry equations (2.19). We shall apply this result to straightforwardly derive bounds on the number of symmetries of a nonsingular binary form.

The rational symmetry equations (2.19) are recast as a pair of polynomial equations for q as a function of p. We must eliminate any common factors in the numerator and denominator of the two rational absolute covariants, and then rewrite the symmetry equations in polynomial form. For instance, formulas (2.14), (2.16), (2.17) imply that if Q has a multiple root, there will be a common factor in H, T and U, which must be canceled when taking the ratios (2.18).

The classical method of finding common factors of polynomials is based on their subresultants, cf. [3, p. 197]. Let

$$P(p) = a_m p^m + a_{m-1} p^{m-1} + \cdots + a_0, \qquad Q(p) = b_n p^n + b_{n-1} p^{n-1} + \cdots + b_0, \tag{3.1}$$

be binary forms of respective degrees m and n. The $(m+n) \times (m+n)$ determinant

$$\mathbf{R}[P,Q] \quad = \quad \det \begin{vmatrix} a_m & a_{m-1} & \cdots & \cdots & a_0 & & & \\ & a_m & a_{m-1} & \cdots & \cdots & a_0 & & \\ & & \ddots & & & & \ddots & \\ & & & a_m & a_{m-1} & \cdots & \cdots & a_0 \\ & & & & b_n & b_{n-1} & \cdots & b_0 \\ & & & b_n & b_{n-1} & \cdots & b_0 & \\ & & \iddots & & & \iddots & & \\ & b_n & b_{n-1} & \cdots & b_0 & & & \\ b_n & b_{n-1} & \cdots & b_0 & & & & \end{vmatrix}, \tag{3.2}$$

in which there are n rows of a's and m rows of b's, and all blank spaces are 0, is their classical *resultant*. The k^{th} *subresultant* $R_k = \mathbf{R}_k[P,Q]$ is the $(m+n-2k) \times (m+n-2k)$ determinant obtained by deleting[1] the first and last k rows as well as the first and last k columns from the resultant determinant (3.2). Just as the vanishing of the resultant detects the existence of a single common root of the two polynomials, the subresultants similarly detect multiple common roots.

Theorem 3.1 *Two polynomials $P(p)$ and $Q(p)$ have a greatest common factor $F(p)$ of degree k if and only if their first k subresultants $R_0, R_1, \dots, R_{k-1}$ vanish, while $R_k \not\equiv 0$. The common factor $F(p)$ is equal to the determinant obtained by replacing the last column of the k^{th} subresultant matrix by the column vector $\big(p^{n-k-1}P(p), \dots, pP(p), P(p), Q(p), pQ(p), \dots, p^{m-k-1}Q(p) \big)^T$.*

Turning to the solution to the symmetry equations (2.19), we write

$$J(p) = \frac{A(p)}{B(p)}, \qquad K(p) = \frac{C(p)}{D(p)}, \tag{3.3}$$

in reduced form, so that A and B have no common factors, nor do C and D. As a result, all solutions to the symmetry equations (2.19) will be obtained by solving the bivariate polynomial equations

$$F(p,q) = A(q)\,B(p) - A(p)\,B(q) = 0, \qquad G(p,q) = C(q)\,D(p) - C(p)\,D(q) = 0. \tag{3.4}$$

Theorem 2.4 implies that every common solution $q = \varphi(p)$ to the equations (3.4) is necessarily a projective symmetry of the binary form.

Bounds on the index or number of symmetries of a binary form can be determined without explicitly solving the bivariate symmetry equations (3.4). The fact that Q is not equivalent to a monomial implies that T^2 is a not a constant multiple of H^3, and hence $F(p,q) \not\equiv 0$ is a nontrivial polynomial. Therefore, the projective index of Q is always bounded by the degree of F in p, which in turn is bounded by $6n-12$ with equality if and only if T and H have no common factors. The second bivariate polynomial is trivial, $G(p,q) \equiv 0$, if and only if the covariant U is a constant multiple of H^2. Forms for which $U = cH^2$ will be distinguished as belonging to the *maximal discrete symmetry class*. Indeed, if T and H have no common factors and all the roots of $F(p,q) = 0$ are simple, then the projective index of such a form takes its maximum possible value, namely $6n-12$. On the other hand, if U is not a constant multiple of H^2, then the projective index is bounded by the degree of $G(p,q) \not\equiv 0$, which is at most $4n-8$. We do not know a convenient geometric interpretation of the maximal discrete symmetry condition $U = cH^2$, nor have we thoroughly investigated the existence and significance of multiple common roots to the symmetry equations (3.4).

Theorem 3.2 *Let k denote the projective index of a binary form Q of degree n which is not complex-equivalent to a monomial. Then*

$$k \le \begin{cases} 6n-12 & \text{if } U = cH^2 \text{ for some constant } c, \text{ or} \\ 4n-8 & \text{in all other cases.} \end{cases}$$

The real case clearly admits the same bounds on the projective index, since one must determine the number of common *real* solutions to (3.4), and, in the case of even degree, whether the sign of Q is the same at each solution. Consequently, the index of a binary form of degree n is bounded

[1] The slightly nonstandard arrangements of rows and columns in the resultant determinant (3.2) is critical here. We note that Exercise 2.38 in [24] is not correctly stated due to a misordering of the resultant rows.

by either $(6n-12)l$ or $(4n-8)l$, where $l=n$ in the complex case, $l=2$ in the case of real forms of even degree and $l=1$ for real forms of odd degree.

Since the symmetry groups of equivalent polynomials are related by matrix conjugation in $\mathrm{GL}(2,\mathbf{C})$, a complete list of possible projective symmetry groups is provided by the following theorem, as presented in Blichfeldt, [2, p. 69].

Theorem 3.3 *Up to matrix conjugation there are five different types of finite subgroups of the projective group* PSL(2):

a) The n element abelian group $\mathcal{A}_n$ is generated by the transformation $p \mapsto \omega p$, where ω is a primitive n^{th} root of unity.

b) The $2n$ element dihedral group $\mathcal{D}_n$ *is the group obtained from $\mathcal{A}_n$ by adjoining the transformation $p \mapsto 1/p$.*

c) The 12 element tetrahedral group $\mathcal{T}$ *is the primitive group generated by the transformations*

$$\sigma\colon\ p \longmapsto -p, \qquad\qquad \tau\colon\ p \longmapsto \frac{i(p+1)}{p-1}, \tag{3.5}$$

of respective orders 2 and 3.

d) The 24 element octahedral group $\mathcal{O}$ *is the primitive group generated by the transformation τ in (3.5) along with*

$$\iota\colon\ p \longmapsto ip \tag{3.6}$$

of order 4. Note that $\iota^2 = \sigma$, and so $\mathcal{T} \subset \mathcal{O}$.

e) The 60 element icosahedral group $\mathcal{I}$ *is the primitive group generated by the transformations σ, τ given above, along with the transformation*

$$\rho\colon\ p \longmapsto \frac{2p-(1-\sqrt{5})i-(1+\sqrt{5})}{\left[(1-\sqrt{5})i-(1+\sqrt{5})\right]p-2} \tag{3.7}$$

of order 2. The tetrahedral group is also a subgroup of the icosahedral group: $\mathcal{T} \subset \mathcal{I}$.

Since the maximal number of elements in the projective symmetry group of a form of degree n is bounded by $6n-12$, then the tetrahedral group can appear as a symmetry group only when $n \geq 4$, the octahedral group is a possible symmetry group only if $n \geq 6$ and the icosahedral group is possible only if $n \geq 12$.

We can describe the invariants of the three primitive groups using the following polynomials:

$$\begin{aligned}
K_4 &= x^4 - 2\sqrt{3}\,i\,x^2y^2 + y^4, & \overline{K}_4 &= x^4 + 2\sqrt{3}\,i\,x^2y^2 + y^4,\\
K_6 &= x^5y - xy^5 & K_8 &= x^8 + 14x^4y^4 + y^8 = K_4\overline{K}_4,\\
K_{12} &= x^{12} - 33\left(x^8y^4 + y^8x^4\right) + y^{12}, & & \\
L_{12} &= 22\sqrt{5}K_6^2 + 5K_{12}, & \widetilde{L}_{12} &= -22\sqrt{5}K_6^2 + 5K_{12},\\
L_{20} &= 3K_8K_{12} - 38\sqrt{5}K_6^2K_8, & \widetilde{L}_{20} &= 3K_8K_{12} + 38\sqrt{5}K_6^2K_8,\\
L_{30} &= 6696K_6^5 + 225K_6K_8^3 - 580\sqrt{5}K_6^3K_{12}, & \widetilde{L}_{30} &= 6696K_6^5 + 225K_6K_8^3 + 580\sqrt{5}K_6^3K_{12}.
\end{aligned} \tag{3.8}$$

Huffman, [16, Theorem 4.1], provides the complete characterization of polynomials whose symmetry groups contain one of these primitive groups.

Proposition 3.4 *The symmetry group of a binary form Q contains*:

a) An icosahedral group if and only if it is equivalent to a polynomial of the one of the two forms $\Phi(L_{12}, L_{20}) + L_{30}\Psi(L_{12}, L_{20})$ *or* $\Phi(\widetilde{L}_{12}, \widetilde{L}_{20}) + \widetilde{L}_{30}\Psi(\widetilde{L}_{12}, \widetilde{L}_{20})$.

b) An octahedral group if and only if it is equivalent to a polynomial of the one of the two forms $\Phi(K_6, K_8)$ *or* $K_{12}\Phi(K_6, K_8)$.

c) A tetrahedral group if and only if it is equivalent to a polynomial from the following list:

$$\begin{array}{lll} \Phi(K_6, K_8) + K_{12}\Phi(K_6, K_8), & \Phi(K_4, K_6), & \Phi(\overline{K}_4, K_6), \\ K_4\Phi(K_6, K_8) + K_4^2\,\Phi(K_6, K_8), & K_4\Phi(\overline{K}_4, K_6), & \overline{K}_4\Phi(K_4, K_6), \\ \overline{K}_4\Phi(K_6, K_8) + \overline{K}_4^2\,\Phi(K_6, K_8), & K_4^2\,\Phi(\overline{K}_4, K_6), & \overline{K}_4^2\,\Phi(K_4, K_6). \end{array}$$

Note in particular that only forms of even degree can admit a primitive symmetry group.

MAPLE code was written to explicitly compute the symmetries of binary forms. Details of the programs and some of the difficulties we experienced in the implementation are discussed in the appendices. The program `symm` listed in Appendix A computes the fundamental invariants J and K, determines the dimension of the symmetry group, and, in the case of a finite symmetry group, solves the two equations (2.19) to find explicit form of the projective symmetries. The actual matrix symmetries are then computed by the program `matrices` by substituting the linear fractional transformations in the projective symmetry group into the form in order to determine the appropriate scalar multiple. We now present some typical examples resulting from our computations.

Example 3.5 *Cubic forms.* All binary cubics with discrete symmetries are equivalent to $x^3 + y^3$, or, in inhomogeneous form, to $p^3 + 1$. Therefore, the symmetry group of a nonsingular cubic is isomorphic to the symmetry group of p^3+1. Applying our algorithm, we find a complete solution to the symmetry equations (3.4) is the projective symmetry group Γ given by the six linear fractional transformations taking p to

$$p, \quad \frac{1}{p}, \quad \omega p, \quad \omega^2 p, \quad \frac{\omega}{p}, \quad \frac{\omega^2}{p},$$

where $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ is the primitive cube root of unity. Since the covariants of any cubic form satisfy the syzygy $U = -\frac{3}{2}H^2$, all nondegenerate cubics have maximal discrete symmetry groups of projective index 6, which equals the number of different permutations of the three roots. The full matrix symmetry group G of this cubic has 18 elements, since we can also multiply by a cube root of unity, and is generated by the three matrices

$$\begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}.$$

In this case, $G \simeq \Gamma \times \mathbf{Z}_3$ is a Cartesian product group. In the real case, one requires real solutions to (3.4), and hence Q has (projective) index 6 if its discriminant $\Delta < 0$, but (projective) index 2 if $\Delta > 0$.

The MAPLE code can be used to compute the explicit symmetries of other cubics. For example, the cubic $Q(p) = p^3 + p$ leads to the following six element group of linear fractional transformations

$$p, \quad -p, \quad \frac{ip+1}{3p+i}, \quad \frac{ip-1}{-3p+i}, \quad \frac{-ip+1}{-3p+i}, \quad \frac{-ip+1}{3p+i}.$$

The matrix generators of the symmetry group are

$$\begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \frac{1}{2}\begin{pmatrix} 1 & -i \\ -3i & 1 \end{pmatrix}.$$

The second and third matrices correspond, respectively, to the second and third linear fractional transformations. Note that one must, in accordance with the general procedure, rescale the matrices as required by the condition that Q must be mapped to itself. Difficulties arise when MAPLE gives the solutions of equations (3.4) not as rational functions, but involving roots of polynomials. An example is the cubic $Q(p) = p^3 + p + 1$, which is discussed in Appendix B.

Example 3.6 *Quartic forms.* A polynomial of degree 4 has a finite symmetry group if it is equivalent to either

$$p^4 + \mu\, p^2 + 1, \qquad \text{or} \qquad p^2 + 1,$$

where $\mu \neq \pm 2$. The former has all simple roots; the latter has a double root at ∞.

In the first situation, the symmetry group will depend on the value of μ. For general μ, the projective symmetry group is a dihedral group $\mathcal{D}_2$, generated by $-p$ and $1/p$. When $\mu = 0$ it becomes a dihedral group $\mathcal{D}_4$, generated by ip and $1/p$. The associated matrices are the obvious ones, namely $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ in the first case, and $\begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ in the second.

The cases $\mu = \pm 2i\sqrt{3}$ corresponds to the polynomials K_4 and $\overline{K}_4$ listed in (3.8) above, and so the projective symmetry group is the 12 element octahedral group $\mathcal{O}$. This case has the maximal size discrete symmetry group. The linear fractional transformations are generated by $-p$ and $i\,(p-1)/(p+1)$. These correspond to different matrices in each case:

$$K_4: \quad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \frac{1}{\left(2 - 2i\sqrt{3}\right)^{1/4}} \begin{pmatrix} i & -i \\ 1 & 1 \end{pmatrix}, \qquad \text{when} \quad \mu = 2i\sqrt{3},$$

$$\overline{K}_4: \quad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \frac{1}{\left(2 + 2i\sqrt{3}\right)^{1/4}} \begin{pmatrix} i & -i \\ 1 & 1 \end{pmatrix}, \qquad \text{when} \quad \mu = -2i\sqrt{3}.$$

The transformations and their matrices are given in the form they were computed by MAPLE.

Finally, the projective symmetry group of the quartic form $p^2 + 1$ consists of just two elements: identity and $p \to -p$.

Example 3.7 *Quintic forms.* For polynomials of degree 5, the projective symmetry group is either cyclic, of type $\mathcal{A}_n$, or dihedral, of type $\mathcal{D}_n$. Some representative examples are listed in the following table.

Projective Symmetry Groups of Representative Quintics

i.	$p^5 + 1$	$\mathcal{D}_5$
ii.	$p^5 + p$	$\mathcal{A}_4$
iii.	$p^5 + p^2$	$\mathcal{A}_3$
iv.	$p^5 + p^3$	$\mathcal{A}_2$
v.	$p^5 + p^2 + 1$	$\{e\}$
vi.	$p^5 - 4p - 2$	$\{e\}$

The final quintic is not solvable in terms of radicals. In each case, the symmetry group was computed using our MAPLE code.

Remark: The symmetry bounds of Theorem 3.2 imply that the projective index of a nonsingular quintic is at most 18. None of our quintic examples achieve this maximal number of projective symmetries, and it is unclear to us whether there are any quintics in the maximal discrete symmetry class, or, alternatively, what the optimal symmetry bound is in this case.

Example 3.8 *Higher degree forms.* At the sixth degree, we first encounter a polynomial with an octahedral projective symmetry group: the sextic $Q(p) = p^5 + p$ which corresponds to the form $Q(x,y) = x^5y + xy^5$, cf. (3.8). The inhomogeneous form looks like the the second quintic polynomial listed in the preceding table, but we are now considering it as a sextic with an additional root at ∞, and so the symmetry group is quite different. Initially MAPLE produces symmetries which involve square roots and so do not initially look like linear fractional transformations. However, after some simplifications under the radical we obtain the group of linear fractional transformations generated by

$$i\,p, \qquad \frac{\sqrt{2}(1+i)p - 2}{\sqrt{2}(1-i) + 2p},$$

with corresponding matrices

$$\begin{pmatrix} i^{5/6} & 0 \\ 0 & i^{-1/6} \end{pmatrix}, \qquad \begin{pmatrix} \frac{1}{2}(1+i) & -\frac{1}{2}\sqrt{2} \\ \frac{1}{2}\sqrt{2} & \frac{1}{2}(1-i) \end{pmatrix}.$$

The next time we meet this group is the octavic (degree 8) form $Q(p) = p^8 + 14p^4 + 1$. The octahedral generators are now

$$p \longmapsto i\,p, \qquad p \longmapsto i\,\left(\frac{p+1}{p-1}\right),$$

which correspond to the matrix symmetries

$$\begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}, \qquad \frac{\sqrt{2}}{2}\begin{pmatrix} i & i \\ 1 & -1 \end{pmatrix}.$$

This concludes our presentation of examples. The last part of the paper outlines the underlying moving frame theory that justifies these results.

4 Moving Frames and Differential Invariants.

The fundamental symmetry Theorem 2.5 is not particular to polynomial functions. Indeed, the binary form $Q(p)$ can be replaced by an arbitrary analytic function without changing the statements and conclusions — with one caveat: a non-polynomial function can admit an infinite discrete symmetry group. For example, any periodic function, e.g., $Q(p) = \sin p$, admits an infinite discrete group of translational symmetries.

Moreover, these results are not even particular to the projective action (2.8) of the general linear group, but are special cases of a general theory of symmetry and equivalence of planar curves under Lie transformation groups. The latter, in turn, is the simplest instance of the theory of equivalence of submanifolds under group actions that forms the focus of Cartan's powerful theory of moving frames, [7, 11, 17], and, more particularly, the new foundations and computational tools developed by the second author and M. Fels, [9, 10]. However, to keep the exposition self-contained and reasonably brief, we shall not attempt to describe the moving frame theory in complete generality this short paper.

Let G be an r-dimensional connected[2] Lie group acting analytically on $M = \mathbf{R}^2$, or, in the complex case $M = \mathbf{C}^2$. We shall also assume that G acts *effectively* (also known as faithfully), which means that the only group element which fixes *every* point of M is the identity. Non-effective actions can always be made effective by replacing G by the quotient group G/G_0, where $G_0 = \{g \in G \,|\, g \cdot z = z \text{ for all } z \in M\}$ is the *global isotropy subgroup*, cf. [23].

Since G acts on M, it will transform analytic curves to analytic curves. Given two curves $C, \overline{C} \subset M$, the basic *equivalence problem* is determine whether the curves are *congruent* under a group transformation, mapping one to the other: $\overline{C} = g \cdot C$. In particular, a *symmetry* of a curve is a self-congruence, $C = g \cdot C$, i.e., a group transformation that leaves the curve unchanged.

A simple example from geometry is when G is the *special Euclidean group* $\mathrm{SE}(2)$, consisting of all proper rigid motions of the plane. The general Euclidean motion maps a point $(p, q) \in \mathbf{R}^2$ to the point

$$\overline{p} = p \cos\theta - q \sin\theta + a, \qquad \overline{q} = p \sin\theta + q \cos\theta + b, \tag{4.1}$$

where θ, a, b serve to parametrize the group. Two curves are Euclidean-equivalent if and only if one can be mapped to the other by a rigid motion. The Euclidean symmetry group of a curve consists of all Euclidean transformations that map the curve to itself. For example, a square admits four (proper) Euclidean symmetries, while a circle has an infinite one-parameter symmetry group consisting of all rotations around its center.

In the study of binary forms of degree n, the planar action of $\mathrm{GL}(2)$ given by

$$\overline{p} = \frac{\alpha p + \beta}{\gamma p + \delta}, \qquad \overline{q} = (\gamma p + \delta)^{-n} q, \tag{4.2}$$

is fundamental. This action is not effective except when $n = 2m+1$ is odd and we are dealing with the real plane; otherwise, we should replace $\mathrm{GL}(2)$ by the quotient group $\mathrm{GL}(2)_n = \mathrm{GL}(2)/Z_n$ where $Z_n = \{\omega \,\mathrm{I} \,|\, \omega^n = 1\}$ is the subgroup consisting of all scalar multiples of the identity by an n^{th} root of unity. If we identify a binary form with the plane curve given by its graph, $C = \{q = Q(p)\}$, then it is easy to see that two binary forms are equivalent, as per (2.8), if and only if their graphs are equivalent curves under the action (4.2). In particular, the *symmetry group* of the graph is the subgroup $\Gamma \subset \mathrm{GL}(2)_n$ preserving the curve, and can be identified with the *projective symmetry group* of the form itself. The passage from $\mathrm{GL}(2)$ to the effectively acting quotient $\mathrm{GL}(2)_n$ is indicative of the difference between the projective symmetry group Γ and the full matrix symmetry group $G \subset \mathrm{GL}(2)$ discussed earlier.

In the moving frame approach, the equivalence problem for curves (or more general submanifolds) under a Lie group action is solved by evaluating the fundamental differential invariants. In general, since G transforms curves to curves, it acts on their derivatives in the evident manner. By definition, a *differential invariant* for a curve[3] $q = Q(p)$ is a function $I(p, Q(p), Q'(p), \dots, Q^{(n)}(p))$ depending on the curve and its derivatives which is unchanged under the induced action of the group G.

For example, consider the planar action of the Euclidean group (4.1). A curve $q = Q(p)$ is transformed into the curve $\overline{q} = \overline{Q}(\overline{p})$ which is defined implicitly by the formulae

$$\overline{p} = p \cos\theta - Q(p) \sin\theta + a, \qquad \overline{Q}(\overline{p}) = p \sin\theta + Q(p) \cos\theta + b. \tag{4.3}$$

[2]Disconnected Lie groups are also handled by the same moving frame methods, although one must exercise a little more care in the statement of results. Thus, in the case of real binary forms, one should replace $\mathrm{GL}(2, \mathbf{R})$ by its connected component $\mathrm{GL}(2, \mathbf{R})^+$ consisting of matrices of positive determinant. However, the preceding results were placed in a form that is applicable to all of $\mathrm{GL}(2, \mathbf{R})$, not just the orientation preserving component.

[3]For simplicity, we assume that the curve can be identified with the graph of a function. Extensions to more general parametrized curves are feasible, but the moving frame implementation must take into account the infinite-dimensional reparametrization "pseudogroup", as discussed in detail in [9].

Implicit differentiation shows that the first two derivatives of the curve are transformed via

$$\overline{Q}'(\overline{p}) = \frac{\sin\theta + Q(p)\cos\theta}{\cos\theta - Q(p)\sin\theta}, \qquad \overline{Q}''(\overline{p}) = \frac{Q''(p)}{(\cos\theta - Q(p)\sin\theta)^3}. \tag{4.4}$$

The particular combination

$$\kappa = \frac{Q''(p)}{(1+Q'(p)^2)^{3/2}} \tag{4.5}$$

can be seen to be invariant under such transformations. Thus κ is a second order differential invariant, and defines the classical Euclidean curvature of the curve $q = Q(p)$.

Higher order differential invariants can be obtained by invariant differentiation. Under the transformation (4.3),

$$d\overline{p} = (\cos\theta - Q'(p)\sin\theta)\, dp. \tag{4.6}$$

Therefore, the classical Euclidean arc length

$$ds = \sqrt{1+Q'(p)^2}\, dp \tag{4.7}$$

is an invariant one-form, and the associated derivation

$$\frac{d}{ds} = \frac{1}{\sqrt{1+Q'(p)^2}}\,\frac{d}{dp} \tag{4.8}$$

will map differential invariants to (higher order) differential invariants. For example,

$$\frac{d\kappa}{ds} = \frac{1}{\sqrt{1+Q'(p)^2}}\,\frac{d\kappa}{dp} = \frac{(1+Q'(p)^2)Q'''(p) - 3Q'(p)Q''(p)^2}{(1+Q'(p)^2)^3} \tag{4.9}$$

is the fundamental third order differential invariant. In fact, *every* Euclidean differential invariant can be written (at least locally) as a function $I = H(\kappa, \kappa_s, \kappa_{ss}, \ldots)$ of the curvature invariant and its successive derivatives with respect to arc length.

The remarkable fact is that this well-known structure for Euclidean differential invariants is not particular to the Euclidean group, but holds for most groups acting on the plane. The precise technical requirement is as follows:

Definition 4.1 A planar transformation group G is said to be *transitive* of order k if, given any two curves $C, \overline{C}$ and points $z \in C$, $\overline{z} \in \overline{C}$, there exists a group transformation $g \in G$ such that $\overline{C}$ and C have k^{th} order contact at the common point $\overline{z} = g \cdot z$. The group is *almost transitive* of order k if the same holds for almost all such curves. More precisely, there is a dense open subset $W \subset \mathbf{R}^{k+2}$ (or $\mathbf{C}^{k+2}$) and one requires that the contact condition holds provided both $(p, Q(p), \ldots, Q^{(k)}(p))$ and $(\overline{p}, \overline{Q}(\overline{p}), \ldots, \overline{Q}^{(k)}(\overline{p}))$ lie in W.

Definition 4.2 An r-dimensional connected planar Lie transformation group G is called *ordinary* if it acts effectively and is almost transitive of order $r-2$.

Dimensional considerations imply that $r-2$ is the maximal order at which one might expect (almost) transitivity. Almost all (order 0) transitive, effective planar Lie group actions, including the Euclidean and projective actions introduced above, are ordinary. Indeed, Lie's classification of planar Lie transformation groups, [21, 23], shows that the only transitive group actions which fail to be ordinary are the elementary three-parameter similarity group[4] $(p,q) \mapsto (\lambda p + c, \lambda q + d)$ and some minor variants thereof. The "non-ordinary" groups can also be analyzed but the results are slightly different; details can be found in [23].

[4]The fact that p and q scale in exactly the same way is crucial — all of the other similarity groups $(p,q) \mapsto (\lambda p + c, \lambda^\alpha q + d)$, $\alpha \neq 1$, are ordinary.

Theorem 4.3 *Let G be an ordinary r-dimensional planar transformation group. There is a unique (up to functions thereof) differential invariant, $\kappa(p, Q(p), \dots, Q^{(r-1)}(p))$ of lowest order, which we call the G-*invariant curvature*, and a unique (up to constant multiple) G-invariant one-form of lowest order, $ds = S(p, Q(p), \dots, Q^{(k)}(p))\, dx$, for some $k \leq r-2$, which we call the G-*invariant arc length *element. Every differential invariant can be locally expressed as a function $I = H(\kappa, \kappa_s, \kappa_{ss}, \dots)$ of the curvature and its successive derivatives with respect to arc length.*

Let us now consider the action (4.2) relevant to the equivalence problem for binary forms. Given two functions related by (2.8), their derivatives transform according to the general rule

$$\overline{Q}^{(m)}(\overline{p}) = \frac{1}{(\alpha\delta - \beta\gamma)^m (\gamma p + \delta)^{n-m}} \sum_{j=0}^{m} (-1)^{m-j} \binom{m}{j} \frac{(n-j)!}{(n-m)!}\, \gamma^{m-j} (\gamma p + \delta)^j Q^{(j)}(p). \tag{4.10}$$

The verification that the absolute rational covariants, as given in terms of derivatives of the function $Q(p)$ according to (2.11), (2.13), are differential invariants is straightforward, albeit tedious. We can identify $J = \kappa$ with the curvature invariant for the action. The invariant "arc length element" and associated invariant derivation are

$$ds = \frac{T}{QH}\, dp, \qquad \text{and} \qquad \frac{d}{ds} = \frac{QH}{T}\, \frac{d}{dp}. \tag{4.11}$$

In particular,

$$\frac{dJ}{ds} = \frac{2U}{nH^2} - \frac{3T^2}{nH^3} = \frac{2}{n} \left[K - \tfrac{3}{2} J^2 \right]. \tag{4.12}$$

Remark: The "arc length form" (4.11) is not, actually, the lowest order one guaranteed in Theorem 4.3, which is $(\sqrt{H}/Q)\, dp$. We have chosen to eliminate the sign ambiguity by multiplying by the differential invariant $\sqrt{J}$. The resulting one-form and the "curvature" invariant J are, in fact, invariant under the full general linear group GL(2).

Remark: The direct derivation of differential invariants and invariant one-forms is systematically effected by the powerful normalization approach that makes the moving frame theory truly algorithmic. Unfortunately, lack of space precludes a discussion of this method, and its computational implementation, in this short paper. The interested reader can find details in [10, 24].

5 Signature Curves.

The moving frame solution to the general equivalence problem for curves under a planar transformation group relies on the functional relationships between their differential invariants, cf. [7, 17, 10]. Assuming G is an ordinary planar transformation group, we require only the two lowest order differential invariants — the group-invariant curvature κ and its derivative κ_s with respect to the group-invariant arc length element. This idea can be formalized as follows.

Definition 5.1 Let G be an ordinary transformation group. An analytic plane curve $\mathcal{C} \subset \mathbf{R}^2$ is *nondegenerate* if the differential invariants κ, κ_s are defined and analytic on $\mathcal{C}$. The G–invariant *signature set* associated with a regular planar curve is $\mathcal{S} = \{(\kappa(z), \kappa_s(z)) \,|\, z \in \mathcal{C}\} \subset \mathbf{R}^2$. The curve $\mathcal{C}$ is *nonsingular* if its signature set $\mathcal{S}$ is a regular curve, called the *signature curve.*

We shall allow signature curves to self-intersect, and so nonsingularity is entirely guaranteed by the local condition $(\kappa_s, \kappa_{ss}) \neq (0,0)$. In particular, the signature set is not allowed to degenerate to a point — although this important special case will be discussed shortly. The importance of the signature curve lies in the fact that it characterizes the original curve up to a group transformation. The main equivalence theorem follows; the proof relies on the standard existence and uniqueness theorem for ordinary differential equations.

Theorem 5.2 *Let G be an ordinary planar transformation group. Two nonsingular analytic curves $\mathcal{C}$ and $\overline{\mathcal{C}}$ are G-congruent, so $\overline{\mathcal{C}} = g \cdot \mathcal{C}$ for some $g \in G$, if and only if their signature curves are identical*: $\overline{\mathcal{S}} = \mathcal{S}$.

Example 5.3 For an ellipse

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1, \qquad \text{or} \qquad y = \pm\sqrt{b^2 - r^2 x^2}\,, \qquad r = \frac{b}{a}\,, \tag{5.1}$$

when traversed counterclockwise, the Euclidean curvature invariants are given by

$$\kappa = \frac{ab}{(a^2 + (r^2-1)x^2)^{3/2}}\,, \qquad \frac{d\kappa}{ds} = \frac{3(r^2-1)xy}{r(a^2 + (r^2-1)x^2)^3}\,. \tag{5.2}$$

These serve to parametrize the ellipse's Euclidean signature curve

$$\left(\frac{d\kappa}{ds}\right)^2 = 9\kappa^{8/3}\left(\kappa^{2/3} - \frac{a^{2/3}}{b^{4/3}}\right)\left(\kappa^{2/3} - \frac{b^{2/3}}{a^{4/3}}\right). \tag{5.3}$$

Note that for a circular ellipse, of radius $|a| = |b|$, the signature curve $\mathcal{S} = \{\, (1/a, 0) \,\}$ degenerates to a single point.

If the curve $\mathcal{C}$ is nonsingular, the inverse image of a point on the signature curve $\mathcal{S}$ will consist of a discrete number of points in the original curve $\mathcal{C}$. Let us define the *index* of the curve to be the minimal such number. Under our nondegeneracy assumption, it can be proved that, generically, the inverse image of any point in $\mathcal{S}$ has cardinality equal to the curve's index; indeed, the only exceptions are points of self-intersection of the signature curve. The following result is an immediate consequence of our basic equivalence Theorem 5.2.

Theorem 5.4 *A nonsingular curve admits a discrete symmetry group, whose cardinality equals the index of the curve.*

Example 5.5 In view of Example 5.3, any noncircular ellipse forms a nonsingular curve under the Euclidean group. As we move once around the ellipse, its signature curve $\mathcal{S}$, as given in (5.3), is traced twice, and hence the ellipse has index 2. This mirrors the fact that the ellipse admits a single proper Euclidean symmetry — rotation through 180°. There are, of course, reflectional symmetries, which change the sign $\kappa_s \mapsto -\kappa_s$ and hence induce reflectional symmetries (about the κ axis) of the signature curve.

Of particular importance are singular curves whose G–invariant curvature is constant; this happens when the signature set degenerates to a single point. Such curves are distinguished as the (nondegenerate) curves of maximal symmetry.

Theorem 5.6 *Let G be an ordinary transformation group, and let $\mathcal{C} \subset X$ be a nondegenerate analytic curve. Then the following conditions are equivalent*:

i) $\mathcal{C}$ *has constant* G*–invariant curvature* κ.

ii) *The signature curve* $\mathcal{S}$ *degenerates to a point.*

iii) $\mathcal{C}$ *is the orbit of a one-parameter subgroup of* G.

iv) $\mathcal{C}$ *admits a one-parameter symmetry group.*

In Euclidean geometry, the curves having constant Euclidean curvature are the circles and straight lines. Each is the orbit of a particular one-parameter subgroup of SE(2), which also forms the symmetry group of the curve. Circles of the same radius have the same curvature, and clearly only these are equivalent under a Euclidean transformation.

Let us now apply the preceding constructions to binary forms. We assume that Q is nondegenerate, meaning that its Hessian H does not vanish identically, and so Q is *not* the n^{th} power of a linear form. For such curves, the solution to the equivalence problem is effected by analyzing the associated signature curve, which is parametrized by the absolute rational covariants (2.18). In view of the identity (4.12), we find it more convenient to adopt the rational covariant K in place of the differentiated invariant dJ/ds.

Definition 5.7 The *signature set* $\mathcal{S} = \mathcal{S}_Q$ of a nondegenerate complex-valued binary form $Q(p)$ is parametrized by the two fundamental absolute rational covariants,

$$\mathcal{S}_Q = \left\{ (J(p), K(p)) = \left(\frac{T(p)^2}{H(p)^3}\,,\, \frac{U(p)}{H(p)^2} \right) \;\Big|\; H(p) \neq 0 \right\}. \tag{5.4}$$

The binary form is *nonsingular* at a point p provided $H(p) \neq 0$ and $(J'(p), K'(p)) \neq 0$, and so $\mathcal{S}_Q$ is (at least locally) a nondegenerate curve.

A direct application of our general equivalence Theorem 5.2 produces the following Fundamental Equivalence Theorem for binary forms.

Theorem 5.8 *Two nondegenerate binary forms* $Q(p)$ *and* $\overline{Q}(\overline{p})$ *are equivalent if and only if their signature curves are identical*: $\mathcal{S}_Q = \mathcal{S}_{\overline{Q}}$.

Remark: Theorem 5.8 was first proved in [22] via an alternative method based on the solution to an equivalence problem arising in the calculus of variations. The direct approach provided by the method of moving frames relies on the results in [10] and is discussed in detail in [24]. Surprisingly, there is *no* classical counterpart to this result, although Clebsch, [8] and Hilbert, [14, §10], do discuss the equivalence of binary forms in some depth.

Remark: In the polynomial case considered here, the determination of when two rationally parametrized signature curves are identical can be solved by Gröbner basis methods, as described by Buchberger, [4]. This leads to an effective algorithm for solving the equivalence problem for binary forms; however, a full implementation of the equivalence algorithm has not yet been tried.

If Q and $\overline{Q}$ are nonsingular and have identical signature curves, then one can explicitly determine all the transformations mapping Q to $\overline{Q}$ by solving the two rational equations

$$J(p) = \overline{J}(\overline{p}), \qquad K(p) = \overline{K}(\overline{p}). \tag{5.5}$$

The second of these two equations merely serves to delineate the appropriate branch of the signature curve. At a generic point p — meaning at points where the common signature curve does not cross itself — each solution $\overline{p} = \varphi(p)$ to (5.5) will define an equivalence between the two binary forms; in

particular, the theory guarantees φ is necessarily a linear fractional transformation! Moreover, the proof of Theorem 2.4 does not require that $Q(p)$ be a polynomial, and so provides a solution to the equivalence problem for general curves under the action (4.2) of GL(2). In particular, a symmetry of a binary form is merely a self-equivalence, and hence (5.5) reduces to our basic symmetry equation (2.19), thereby proving Theorem 2.5. The maximally symmetric curves (forms) are those for which the curvature invariant J is constant, and so Theorem 5.6 immediately implies our symmetry Theorem 2.4.

Thus, to determine whether a binary form (or more general function) is equivalent to a given form, one only needs to understand the structure of its signature curve. As a sample application, we consider the case $Q(p) = p^n + 1$, which is the inhomogeneous version of the form $x^n + y^n$. The signature curve of this particular form is found by direct computation of its covariants; we find

$$K = -\frac{n-3}{n-2}\, J + \frac{2n(n-2)}{(n-1)^2}\,.$$

Theorem 5.8 then gives a new necessary and sufficient condition for a binary form to be equivalent to a sum of two n^{th} powers; see [22] for details, and [13, 18, 25, 26] for further results on expressing a binary form as a sum of powers.

Proposition 5.9 *A binary form $Q(x,y)$ of degree $n \geq 3$ is complex-equivalent to a sum of two n^{th} powers, that is, to $x^n + y^n$, if and only if its covariants H, T, U are related by the equation*

$$HU - \frac{n-3}{n-2}\, T^2 + \frac{2n(n-2)}{(n-1)^2}\, H^3 = 0. \tag{5.6}$$

In the real case, the signs of the Hessian and, possibly, of the form itself come into play, [22, 24]. However, when $T \neq 0$, the sign of H equals the sign of the invariant $J = T^2/H^3$ and hence can be directly determined from the signature curve. Theorem 5.8 holds as stated for real forms of odd degree; however, if the degree is even, then there are, in fact, two distinct signature curves,

$$\mathcal{S}_Q^+ = \{(J(p), K(p)) \mid \ Q(p) > 0\}\,, \qquad \mathcal{S}_Q^- = \{(J(p), K(p)) \mid \ Q(p) < 0\}\,, \tag{5.7}$$

indexed by the sign of the form. (If Q is of one sign, then one of these will be empty.) In this case, both signature curves must agree, so $\mathcal{S}_Q^+ = \mathcal{S}_{\overline{Q}}^+$ and $\mathcal{S}_Q^- = \mathcal{S}_{\overline{Q}}^-$, in order that the two forms be real-equivalent.

Example 5.10 Let us apply these results to binary cubics. The second rational covariant (2.18) is a constant, $K = -\frac{3}{2}$ for any nondegenerate cubic, and so the signature curve is a horizontal line in $\mathbf{C}^2$. The classification of complex cubics then follows immediately.

a) The degenerate case when the Hessian vanishes identically, $H \equiv 0$, in which case the form is the cube of a linear form.

b) The maximally symmetric case when the signature curve degenerates to a point, and so T^2 is a constant multiple of H^3, in which case the cubic has a double root.

c) The nonsingular case when the signature curve is a horizontal line and the cubic has three simple roots.

In the case of real cubics, the sign of the discriminant Δ is invariant, and there are two nondegenerate cases. The rational covariant $K = -\frac{3}{2}$ is still constant, and so it appears that both cases have the same straight line as their real signature curve — even though they are inequivalent. The

resolution of this apparent paradox is that the signature curve is not, in fact, the entire horizontal line! Consider the well-known syzygy

$$T^2 + H^3 = 2^4 3^6 \, \Delta \, Q^2, \tag{5.8}$$

among the fundamental cubic covariants, cf. [24, eq. (2.47)]. If $\Delta < 0$, the cubic has three real roots and $H(p) < 0$ is negative definite. Since $J = T^2/H^3$, (5.8) implies that $-1 \leq J(p) \leq 0$, and hence the signature curve in this case is the horizontal line segment

$$\mathcal{S}_Q = \left\{ \left(a, \tfrac{3}{2}\right) \;\middle|\; -1 \leq a \leq 0 \right\}.$$

On the other hand, if $\Delta > 0$, then (5.8) implies $T^2 + H^3 \geq 0$. In this case, $H(p)$ is indefinite; when $H > 0$, then $J \geq 0$, while when $H < 0$, then $J < -1$. Therefore, the signature curve for a cubic with complex roots consists of two pieces:

$$\mathcal{S}_Q = \left\{ \left(a, \tfrac{3}{2}\right) \;\middle|\; a \geq 0 \right\} \cup \left\{ \left(a, \tfrac{3}{2}\right) \;\middle|\; a < -1 \right\}.$$

We see that the two real signature curves cover *different* portions of the same horizontal line, and so the two cubics cannot be real-equivalent.

6 Extensions.

The moving frame methods developed in [10] are not restricted to planar curves, but apply equally well to curves and higher dimensional submanifolds of general manifolds under very general Lie group actions. Each submanifold gives rise to a signature submanifold, which is parametrized by the fundamental differential invariants, and uniquely characterizes the given submanifold up to group transformations. For example, for a nondegenerate surface in three-dimensional space, the Euclidean signature set is a surface in a six-dimensional space parametrized by the mean curvature, the Gaussian curvature, and their derivatives with respect to the Euclidean-invariant Frenet frame on the surface, cf. [12]. The maximally symmetric submanifolds have all constant differential invariants, and so their signature set degenerates to a single point. They are realized as the orbits of certain subgroups of G of the appropriate dimension. See [10, 17], for precise statements and a variety of geometric examples.

In particular, one can regard the equivalence and symmetry problems for multivariate polynomials as problems for hypersurfaces in $\mathbf{R}^m$ or $\mathbf{C}^m$. The full moving frame machinery can be used to effect a solution, but this work is in progress. Applications to the direct determination of symmetries of elliptic curves $y^2 = x^3 + ax + b$, cf. [19], would be an immediate and interesting consequence of this implementation of the general method.

Acknowledgments: A part of the research discussed in this paper was conducted during the second author's visit to the Mathematical Sciences Research Institute at Berkeley in the fall of 1998. We would like to thank the organizers of the symbolic computation program, particularly Michael Singer and Berndt Sturmfels, for their kind invitation and hospitality.

Appendices

A Implementation.

MAPLE and MATHEMATICA code was written to explicitly compute the symmetries of complex-va=lued binary forms. For brevity we just present the more well-developed MAPLE implementation. Both systems worked well when applied to very simple forms, but experienced similar difficulties simplifying complicated rational algebraic formulae into the basic linear fractional form. the code consists of two main programs — `symm` and `matrices` — and two auxiliary functions — `simple` and `l_f`.

The program `symm` is the main function. The input consists of a complex-valued polynomial $f(p)$ considered as the projective form of homogeneous binary polynomial $F(x, y)$, and the degree $n = deg(F)$. The program computes the invariants J and K in reduced form, determines the dimension of the symmetry group, and, in the case of a finite symmetry group, applies the MAPLE command `solve` to solve the two polynomial symmetry equations (3.4) to find explicit form of symmetries. The output of `symm` consists of the projective index of the form and the explicit formulae for its discrete projective symmetries. The program also notifies the user if the symmetry group is not discrete, or is in the maximal discrete symmetry class.

```
> with(linalg):
> symm:=proc(form,n)
global tr,error;
local Q,Qp,Qpp,Qppp,Qpppp,H,T,V,U,J,K,j,k, Eq1,Eq2,i,eqtr,
ans;
 tr:='tr':
 Q:=form(p);
 Qp:=diff(Q,p);
 Qpp:=diff(Qp,p);
 Qppp:=diff(Qpp,p);
 Qpppp:=diff(Qppp,p);
 H:=n*(n-1)*(Q*Qpp-(n-1)/n*Qp^2);
 if H=0 then
  ans:=`Hessian is zero:  two-dimensional symmetry group`
 else
  T:=-n^2*(n-1)*(Q^2*Qppp-3*(n-2)/n*Q*Qp*Qpp
  +2*(n-1)*(n-2)/n^2*Qp^3);
  V:=Q^3*Qpppp-4*(n-3)/n*Q^2*Qp*Qppp+6*(n-2)*(n-3)/n^2
  *Q*Qp^2*Qpp-3*(n-1)*(n-2)*(n-3)/n^3*Qp^4;
  U:=n^3*(n-1)*V-3*(n-2)/(n-1)*H^2;
  J:=simple(T^2/H^3); K:=simple(U/H^2);
  j:=subs(p=P,J);k:=subs(p=P,K);
  Eq1:=simplify(numer(J)*denom(j)-numer(j)*denom(J));
  Eq2:=simplify(numer(K)*denom(k)-numer(k)*denom(K));
  if Eq1=0 then
   ans:=`Form has a one-dimensional symmetry group`;
  else
   if Eq2=0 then
```

```
      print (‘ Form has the maximal possible discrete
      symmetry group‘);
      eqtr:= [solve(Eq1,P)];
      tr:=map(radsimp,map(allvalues,eqtr));
    else
      eqtr:=[solve({Eq1,Eq2},P)];
      tr:= [];
      for i from 1 to nops(eqtr) do
        tr:=map(radsimp,[op(tr),allvalues(rhs(eqtr[i][1]))]);
      od
    fi;
    print(‘The number of elements in the symmetry group‘
    =nops(tr));
    ans:=map(l_f,tr);
    if error=1 then
      print(‘ERROR: Some of the transformations are not
      linear-fractional‘)
    else
      if error=2 then
        print(‘WARNING: Some of the transformations are not
        written in the form polynomial over polynomial‘)
      fi;
    fi;
  fi;
 fi;
 ans
end:
```

The program `matrices` determines the matrix symmetry corresponding to a given (list of) projective symmetries. As discussed in the text, this only requires determining an overall scalar multiple, which can be found by substituting the projective symmetry into the form. The output consists of each projective symmetry, the scalar factor μ, and the resulting matrix symmetry.

```
> matrices:=proc(form,n,L::list)
local Q,ks,ksi,i,Sf,M;
 ksi:='ksi';
 for i from 1 to nops(L) do
  Sf:=simplify(denom(L[i])^n*form(L[i]));
  ks:=quo(Sf,form(p),p);
  ksi:=simplify(ks^(1/n),radical,symbolic);
  M[i]:=matrix(2,2,[coeff(numer(L[i]),p)/ksi,
  coeff(numer(L[i]),p,0)/ksi,coeff(denom(L[i]),p)/ksi,
  coeff(denom(L[i]),p,0)/ksi]);
  print(L[i], mu=ksi, map(simplify,M[i]))
 od;
end:
```

The auxiliary function `simple` helps to simplify rational expressions by manipulating the numerator and denominator separately. The simplified rational expression is returned.

```
> simple:=proc(x)
local nu,de,num,den;
```

```
  nu:=numer(x);
  de:=denom(x);
  num:=(simplify((nu,radical,symbolic)));
  den:=(simplify((de,radical,symbolic)));
  simplify(num/den);
end:
```

The auxiliary function `l_f` uses polynomial division to reduce rational expressions to linear fractional form (when possible).

```
> l_f:=proc(x)
local A,B,C,S,de,nu,r,R;
global error;error:='error';
  nu:=numer(x);
  de:=denom(x);
  if type(nu,polynom(anything,p))
  and type(de,polynom(anything,p)) then
    if degree(nu,p)+1=degree(de,p) then
      A:=quo(de,nu,p,'B');
      S:=1/A; R:=0
    else
      A:=quo(nu,de,p,'B');
      if B=0 then
        S:=A; R:=0;
      else
        C:=quo(de,B,p,'r'); R:=simple(r);
        S:=simplify(A+1/C)
      fi;
    fi;
    if R=0 then
      collect(S,p)
    else
      error:=1; x
    fi;
  else
    error:=2; x
  fi;
end:
```

B Cubic Forms.

We now present the results of applying the function `symm` and `matrices` to cubic forms. We begin with simple cases, ending with a cubic whose formulae required extensive manipulation.

1. Cubics with one triple root:

```
>  f:=p->p^3;
```

$$f := p \to p^3$$

```
>  symm(f,3);
```

Hessian is zero : two − dimensional symmetry group

2. Cubics with one double root and one single root:

```
> f:=p->p;
```

$$f := p \to p$$

```
> symm(f,3);
```

Form has a one − dimensional symmetry group

3. Cubics with three simple roots:

```
> f:=p->p^3+1;
```

$$f := p \to p^3 + 1$$

```
> S:=symm(f,3);
```

Form has the maximal possible discrete symmetry group

The number of elements in the symmetry group $= 6$

$$S := \left[p,\ \frac{1}{p},\ \frac{-\frac{1}{2}+\frac{1}{2}I\sqrt{3}}{p},\ \frac{-\frac{1}{2}-\frac{1}{2}I\sqrt{3}}{p},\ (-\frac{1}{2}+\frac{1}{2}I\sqrt{3})\,p,\ (-\frac{1}{2}-\frac{1}{2}I\sqrt{3})\,p \right]$$

```
> matrices(f,3,[S[2],S[4]]);
```

$$\frac{1}{p}, \quad \mu = 1, \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\frac{-\frac{1}{2}-\frac{1}{2}I\sqrt{3}}{p}, \quad \mu = 2, \quad \begin{bmatrix} 0 & -\frac{1}{2}-\frac{1}{2}I\sqrt{3} \\ 1 & 0 \end{bmatrix}$$

4. A more complicated cubic example.

All cubics with a discrete symmetry group are complex equivalent to x^3+y^3 and have projective index 6. However, when we apply the same code to a cubic not in canonical form. The initial MAPLE result is not in the correct linear fractional form. We must simplify the rational algebraic expressions "by hand" to put them in the form of a projective linear fractional transformation.

```
> f:=p->p^3+p+1;
```

$$f := p \to p^3 + p + 1$$

```
> S:=symm(f,3);
```

Form has the maximal possible discrete symmetry group

The number of elements in the symmetry group $= 6$

WARNING : *Some of the transformations are not written in the form polynomial \ over polynomial*

$$S := [p,\ \frac{(-9+I\sqrt{31})\,p+2}{9+I\sqrt{31}+6\,p},\ -\frac{(9+I\sqrt{31})\,p-2}{9-I\sqrt{31}+6\,p},\ \frac{1}{18}((54\,p^4+9\,2^{(2/3)}\,3^{(1/3)}\,\%1^{(1/3)}\,p^3$$
$$+324\,p^3+3\,2^{(1/3)}\,3^{(2/3)}\,\%1^{(2/3)}\,p^2+450\,p^2-108\,p+9\,2^{(1/3)}\,3^{(2/3)}\,\%1^{(2/3)}\,p$$
$$+9\,2^{(2/3)}\,3^{(1/3)}\,\%1^{(1/3)}\,p-2^{(1/3)}\,3^{(2/3)}\,\%1^{(2/3)}+6+9\,2^{(2/3)}\,3^{(1/3)}\,\%1^{(1/3)})3^{(2/3)}$$
$$2^{(1/3)})\Big/(\%1^{(1/3)}\,(27\,p^3-9\,p^2-1)),-\frac{1}{36}((54\,I\sqrt{3}\,p^4+54\,p^4+324\,p^3$$
$$+324\,I\sqrt{3}\,p^3-18\,2^{(2/3)}\,3^{(1/3)}\,\%1^{(1/3)}\,p^3+450\,p^2+450\,I\sqrt{3}\,p^2$$

$$
\begin{aligned}
&- 9\,I\,3^{(1/6)}\,2^{(1/3)}\,\%1^{(2/3)}\,p^2 + 3\,2^{(1/3)}\,3^{(2/3)}\,\%1^{(2/3)}\,p^2 - 27\,I\,3^{(1/6)}\,2^{(1/3)}\,\%1^{(2/3)}\,p \\
&- 108\,p - 18\,2^{(2/3)}\,3^{(1/3)}\,\%1^{(1/3)}\,p + 9\,2^{(1/3)}\,3^{(2/3)}\,\%1^{(2/3)}\,p - 108\,I\,\sqrt{3}\,p \\
&+ 3\,I\,3^{(1/6)}\,2^{(1/3)}\,\%1^{(2/3)} + 6\,I\,\sqrt{3} - 18\,2^{(2/3)}\,3^{(1/3)}\,\%1^{(1/3)} - 2^{(1/3)}\,3^{(2/3)}\,\%1^{(2/3)} + 6 \\
&)3^{(2/3)}\,2^{(1/3)})\Big/(\%1^{(1/3)}\,(27\,p^3 - 9\,p^2 - 1)),\frac{1}{36}((54\,I\,\sqrt{3}\,p^4 - 54\,p^4 - 324\,p^3 \\
&+ 324\,I\,\sqrt{3}\,p^3 + 18\,2^{(2/3)}\,3^{(1/3)}\,\%1^{(1/3)}\,p^3 - 450\,p^2 + 450\,I\,\sqrt{3}\,p^2 \\
&- 9\,I\,3^{(1/6)}\,2^{(1/3)}\,\%1^{(2/3)}\,p^2 - 3\,2^{(1/3)}\,3^{(2/3)}\,\%1^{(2/3)}\,p^2 - 27\,I\,3^{(1/6)}\,2^{(1/3)}\,\%1^{(2/3)}\,p \\
&+ 108\,p + 18\,2^{(2/3)}\,3^{(1/3)}\,\%1^{(1/3)}\,p - 9\,2^{(1/3)}\,3^{(2/3)}\,\%1^{(2/3)}\,p - 108\,I\,\sqrt{3}\,p \\
&+ 3\,I\,3^{(1/6)}\,2^{(1/3)}\,\%1^{(2/3)} + 6\,I\,\sqrt{3} + 18\,2^{(2/3)}\,3^{(1/3)}\,\%1^{(1/3)} + 2^{(1/3)}\,3^{(2/3)}\,\%1^{(2/3)} - 6 \\
&)3^{(2/3)}\,2^{(1/3)})\Big/(\%1^{(1/3)}\,(27\,p^3 - 9\,p^2 - 1))] \\
&\%1 := 9 + 18\,p - 81\,p^2 + 261\,p^3 + 27\,\sqrt{31}\,\sqrt{3}\,p^3 - 9\,\sqrt{31}\,\sqrt{3}\,p^2 - \sqrt{31}\,\sqrt{3}
\end{aligned}
$$

The first three components of `S` are in the proper linear fractional form. The problem with the other expressions is that MAPLE does not automatically factor polynomials under a radical. One approach to simplification is to first do the required factorization:

```
> n1:=factor(9+18*p-81*p^2+261*p^3+27*sqrt(31)*sqrt(3)*p^3
-9*sqrt(31)*sqrt(3)*p^2-sqrt(31)*sqrt(3));
```

$$n1 := -\frac{1}{24}\,(29 + 3\,\sqrt{31}\,\sqrt{3})\,(-6\,p - 9 + \sqrt{31}\,\sqrt{3})^3$$

Substituting `n1` into the fourth rational algebraic expression in `S` above, we can now force MAPLE to take the cube root and obtain the actual linear fractional formula for this symmetry:

```
> simp1:=radsimp(1/18*((54*p^4+9*2^(2/3)*3^(1/3)*(n1)^(1/3)*p^3+324*p^3
+3*2^(1/3)*3^(2/3)*(n1)^(2/3)*p^2+450*p^2+9*2^(1/3)*3^(2/3)*(n1)^(2/3)
*p+9*2^(2/3)*3^(1/3)*(n1)^(1/3)*p-108*p-2^(1/3)*3^(2/3)*(n1)^(2/3)+6
+9*2^(2/3)*3^(1/3)*(n1)^(1/3))*3^(2/3)*2^(1/3))/((n1)^(1/3)
*(27*p^3-9*p^2-1)));
> simp2:=l_f(simp1);
> simp3:=collect(expand(numer(simp2))/expand(denom(simp2)),p);
```

$$
\begin{aligned}
simp3 := &((-226\,2^{(1/3)} - 20\,\%2 - 20\,2^{(2/3)}\,\%1^{(2/3)} - 22\,\%3 - 208\,\%1^{(1/3)})\,p - 8\,\%3 \\
&- 58\,2^{(2/3)}\,\%1^{(2/3)} - 566\,\%1^{(1/3)} - 58\,\%2 - 116\,2^{(1/3)})\Big/(\\
&(-6\,2^{(2/3)}\,\%1^{(2/3)} - 174\,\%1^{(1/3)} - 1686\,2^{(1/3)} - 174\,\%3 - 6\,\%2)\,p \\
&+ 20\,2^{(2/3)}\,\%1^{(2/3)} + 208\,\%1^{(1/3)} + 226\,2^{(1/3)} + 22\,\%3 + 20\,\%2) \\
&\%1 := 29 + 3\,\sqrt{31}\,\sqrt{3} \\
&\%2 := \%1^{(1/3)}\,\sqrt{31}\,\sqrt{3} \\
&\%3 := 2^{(1/3)}\,\sqrt{31}\,\sqrt{3}
\end{aligned}
$$

The linear fractional formulae for the other symmetries are derived in a similar fashion.

C The Octahedral Symmetry Group.

As we remarked in the text, the sextic polynomial $Q(p) = p^5 + p$ has an octahedral symmetry group. Here we illustrate how the symmetries are computed using our MAPLE program.

```
> f:=p->p^5+p;
```

$$f := p \to p^5 + p$$

```
> symm(f,6);
```

Form has the maximal possible discrete symmetry group
The number of elements in the symmetry group $= 24$

WARNING : *Some of the transformations are not written in the form polynomial over polynomial*

$$\left[\frac{1}{p},\ p,\ -p,\ -\frac{1}{p},\ \frac{I}{p},\ -\frac{I}{p},\ I\,p,\ -I\,p,\ \frac{-2\,p^3+2\,I\,p+\%3}{p^4+1},\ \frac{-2\,p^3+2\,I\,p-\%3}{p^4+1},\right.$$
$$\frac{-2\,p^3-2\,I\,p+\%4}{p^4+1},\ \frac{-2\,p^3-2\,I\,p-\%4}{p^4+1},\ \frac{2\,p^3+2\,I\,p+\%4}{p^4+1},\ \frac{2\,p^3+2\,I\,p-\%4}{p^4+1},$$
$$\frac{2\,p^3-2\,I\,p+\%3}{p^4+1},\ \frac{2\,p^3-2\,I\,p-\%3}{p^4+1},\ \frac{-2\,p+2\,I\,p^3+\%1}{p^4+1},\ \frac{-2\,p+2\,I\,p^3-\%1}{p^4+1},$$
$$\frac{-2\,p-2\,I\,p^3+\%2}{p^4+1},\ \frac{-2\,p-2\,I\,p^3-\%2}{p^4+1},\ \frac{2\,p+2\,I\,p^3+\%2}{p^4+1},\ \frac{2\,p+2\,I\,p^3-\%2}{p^4+1},$$
$$\left.\frac{2\,p-2\,I\,p^3+\%1}{p^4+1},\ \frac{2\,p-2\,I\,p^3-\%1}{p^4+1}\right]$$
$$\%1 := \sqrt{-4\,p^6+4\,p^2+I\,p^8-6\,I\,p^4+I}$$
$$\%2 := \sqrt{-4\,p^6+4\,p^2-I\,p^8+6\,I\,p^4-I}$$
$$\%3 := \sqrt{4\,p^6-4\,p^2+I\,p^8-6\,I\,p^4+I}$$
$$\%4 := \sqrt{4\,p^6-4\,p^2-I\,p^8+6\,I\,p^4-I}$$

Again, MAPLE has failed to simplify the expressions $\%1, \%2, \%3, \%4$, and we need to make it take the square root. In the case of symmetries numbers $9, 11, 13, 15, 17, 19, 21, 23$ this is done as follows. The others are handled in a similar fashion, and, for brevity, we omit the formulae here.

```
> for j in [9,11,13,15,17,19,21,23] do
sq:=sqrt(factor(op(op(numer(tr[j]))[3])[1],I),symbolic):
s[j]:=l_f((op(numer(tr[j]))[1]+op(numer(tr[j]))[2]+sq)/denom(tr[j]));
print(s.j=s[j]);
od:
```

$$s9 = -\frac{(\sqrt{2}+I\,\sqrt{2})\,p-2}{-\sqrt{2}+I\,\sqrt{2}-2\,p}$$
$$s11 = -\frac{(-\sqrt{2}+I\,\sqrt{2})\,p+2}{I\,\sqrt{2}+\sqrt{2}+2\,p}$$
$$s13 = \frac{(-\sqrt{2}+I\,\sqrt{2})\,p-2}{I\,\sqrt{2}+\sqrt{2}-2\,p}$$
$$s15 = \frac{(\sqrt{2}+I\,\sqrt{2})\,p+2}{-\sqrt{2}+I\,\sqrt{2}+2\,p}$$
$$s17 = -\frac{(-\sqrt{2}+I\,\sqrt{2})\,p-2}{-\sqrt{2}+I\,\sqrt{2}-2\,I\,p}$$
$$s19 = -\frac{I\,((\sqrt{2}+I\,\sqrt{2})\,p+2)}{-\sqrt{2}+I\,\sqrt{2}+2\,p}$$

$$s21 = \frac{(\sqrt{2} + I\sqrt{2})\,p - 2}{\sqrt{2} + I\sqrt{2} + 2\,I\,p}$$
$$s23 = \frac{(-\sqrt{2} + I\sqrt{2})\,p + 2}{-\sqrt{2} + I\sqrt{2} + 2\,I\,p}$$

As we remarked in the text, the octahedral symmetry group has two generators. The matrix form of these generators is computed as follows:

```
> matrices(f,6,[tr[7],s[9]]);
```

$$I\,p, \qquad \mu = (-1)^{(1/12)}, \qquad \begin{bmatrix} (-1)^{(5/12)} & 0 \\ 0 & -(-1)^{(11/12)} \end{bmatrix}$$

$$-\frac{(\sqrt{2} + I\sqrt{2})\,p - 2}{-\sqrt{2} + I\sqrt{2} - 2\,p}, \qquad \mu = 2\sqrt{2}, \qquad \begin{bmatrix} -\frac{1}{2} - \frac{1}{2}I & \frac{1}{2}\sqrt{2} \\ -\frac{1}{2}\sqrt{2} & -\frac{1}{2} + \frac{1}{2}I \end{bmatrix}$$

We end with two further examples. We already know that the following octavic polynomial also has an octahedral symmetry group. In this case, `symm` produces the projective symmetries directly:

```
> f:=p->p^8+14*p^4+1;
```

$$f := p \to p^8 + 14\,p^4 + 1$$

```
> S:=symm(f,8);
```

The number of elements in the symmetry group $= 24$

$$S := [-\frac{1}{p}, -\frac{p-1}{p+1}, -\frac{p+1}{p-1}, p, -p, \frac{p+1}{p-1}, \frac{p-1}{p+1}, \frac{1}{p}, \frac{I\,(p-1)}{p+1}, -\frac{I\,(p-1)}{p+1}, \frac{I\,(p+1)}{p-1},$$
$$-\frac{I\,(p+1)}{p-1}, \frac{I}{p}, -\frac{I}{p}, I\,p, -I\,p, \frac{-1+I\,p}{-I+p}, -\frac{1+I\,p}{I+p}, \frac{1+I\,p}{I+p}, -\frac{-1+I\,p}{-I+p}, \frac{-1+I\,p}{1+I\,p},$$
$$\frac{1+I\,p}{-1+I\,p}, -\frac{1+I\,p}{-1+I\,p}, -\frac{-1+I\,p}{1+I\,p}]$$

```
> matrices(f,8,[S[11],S[15]]);
```

$$\frac{I\,(p+1)}{p-1}, \qquad \mu = \sqrt{2}, \qquad \begin{bmatrix} \frac{1}{2}I\sqrt{2} & \frac{1}{2}I\sqrt{2} \\ \frac{1}{2}\sqrt{2} & -\frac{1}{2}\sqrt{2} \end{bmatrix}$$

$$I\,p, \qquad \mu = 1, \qquad \begin{bmatrix} I & 0 \\ 0 & 1 \end{bmatrix}$$

Finally, for illustrative purposes, we present a higher order example given by a binary form of degree 12.

```
> f:=p->p^12-33*p^8-33*p^4+1;
```

$$f := p \to p^{12} - 33\,p^8 - 33\,p^4 + 1$$

```
> S:=symm(f,12);
```

The number of elements in the symmetry group $= 24$

$$S := [p,\ -p,\ -\frac{1}{p},\ \frac{1}{p},\ -\frac{p-1}{p+1},\ -\frac{p+1}{p-1},\ \frac{p+1}{p-1},\ \frac{p-1}{p+1},\ \frac{I}{p},\ -\frac{I}{p},\ I\,p,\ -I\,p,\ \frac{-1+I\,p}{-I+p},\ -\frac{1+I\,p}{I+p},$$
$$\frac{1+I\,p}{I+p},\ -\frac{-1+I\,p}{-I+p},\ \frac{I\,(p-1)}{p+1},\ -\frac{I\,(p-1)}{p+1},\ \frac{I\,(p+1)}{p-1},\ -\frac{I\,(p+1)}{p-1},\ \frac{-1+I\,p}{1+I\,p},\ \frac{1+I\,p}{-1+I\,p},$$
$$-\frac{1+I\,p}{-1+I\,p},\ -\frac{-1+I\,p}{1+I\,p}]$$

```
> matrices(f,12,[S[11],S[19]]);
```

$$I\,p, \qquad \mu = 1, \qquad \begin{bmatrix} I & 0 \\ 0 & 1 \end{bmatrix}$$

$$\frac{I\,(p+1)}{p-1}, \qquad \mu = (-1)^{(1/12)}\sqrt{2}, \qquad \begin{bmatrix} \frac{1}{2}\,(-1)^{(5/12)}\,\sqrt{2} & \frac{1}{2}\,(-1)^{(5/12)}\,\sqrt{2} \\ -\frac{1}{2}\,(-1)^{(11/12)}\,\sqrt{2} & \frac{1}{2}\,(-1)^{(11/12)}\,\sqrt{2} \end{bmatrix}$$

References

[1] Ackerman, M., and Hermann, R., *Hilbert's Invariant Theory Papers*, Lie Groups: History, Frontiers and Applications, vol. 8, Math Sci Press, Brookline, Mass., 1978.

[2] Blichfeldt, H.F., *Finite Collineation Groups*, University of Chicago Press, Chicago, 1917.

[3] Bôcher, M., *Introduction to Higher Algebra*, Macmillan Co., New York, 1907.

[4] Buchberger, B., Applications of Gröbner bases in non-linear computational geometry, *in*: *Mathematical Aspects of Scientific Software*, J.R. Rice, ed., IMA Volumes in Mathematics and its Applications, vol. 14, Springer–Verlag, New York, 1988, pp. 59–87.

[5] Calabi, E., Olver, P.J., Shakiban, C., Tannenbaum, A., and Haker, S., Differential and numerically invariant signature curves applied to object recognition, *Int. J. Computer Vision* **26** (1998), 107–135.

[6] Calabi, E., Olver, P.J., and Tannenbaum, A., Affine geometry, curve flows, and invariant numerical approximations, *Adv. in Math.* **124** (1996), 154–196.

[7] Cartan, É., *La Méthode du Repère Mobile, la Théorie des Groupes Continus, et les Espaces Généralisés*, Exposés de Géométrie No. 5, Hermann, Paris, 1935.

[8] Clebsch, A., *Theorie der Binären Algebraischen Formen*, B.G. Teubner, Leipzig, 1872.

[9] Fels, M., and Olver, P.J., Moving coframes. I. A practical algorithm, *Acta Appl. Math.* **51** (1998), 161–213.

[10] Fels, M., and Olver, P.J., Moving coframes. II. Regularization and theoretical foundations, *Acta Appl. Math.*, to appear.

[11] Griffiths, P.A., On Cartan's method of Lie groups and moving frames as applied to uniqueness and existence questions in differential geometry, *Duke Math. J.* **41** (1974), 775–814.

[12] Guggenheimer, H.W., *Differential Geometry*, McGraw–Hill, New York, 1963.

[13] Gundelfinger, S., Zur Theorie der binären Formen, *J. Reine Angew. Math.* **100** (1886), 413–424.

[14] Hilbert, D., Über die vollen Invariantensystem, *Math. Ann.* **42** (1893), 313–373; also *Gesammelte Abhandlungen*, vol. 2, Springer–Verlag, Berlin, 1933, pp. 287–344; see [1, pp. 225–301] for an English translation.

[15] Hilbert, D., *Theory of Algebraic Invariants*, Cambridge Univ. Press, New York, 1993.

[16] Huffman, W.C., Polynomial invariants of finite linear groups of degree two, *Can. J. Math.* **32** (1980), 317–330.

[17] Jensen, G.R., *Higher order contact of submanifolds of homogeneous spaces*, Lecture Notes in Math., No. 610, Springer–Verlag, New York, 1977.

[18] Kung, J.P.S., Canonical forms for binary forms of even degree, *in*: *Invariant Theory*, S.S. Koh, ed., Lecture Notes in Math, vol. 1278, Springer–Verlag, New York, 1987, pp. 52–61.

[19] Lang, S., *Elliptic Curves: Diophantine Analysis*, Springer–Verlag, New York, 1978.

[20] Lie, S., and Scheffers, G., *Vorlesungen über Continuierliche Gruppen mit Geometrischen und Anderen Anwendungen*, B.G. Teubner, Leipzig, 1893.

[21] Lie, S., Gruppenregister, *in*: *Gesammelte Abhandlungen*, vol. 5, B.G. Teubner, Leipzig, 1924, pp. 767–773.

[22] Olver, P.J., Classical invariant theory and the equivalence problem for particle Lagrangians. I. Binary forms, *Adv. in Math.* **80** (1990), 39–77.

[23] Olver, P.J., *Equivalence, Invariants, and Symmetry*, Cambridge University Press, Cambridge, 1995.

[24] Olver, P.J., *Classical Invariant Theory*, Cambridge University Press, Cambridge, 1999.

[25] Reichstein, B., On symmetric operators of higher degree and their application, *Linear Algebra Appl.*. **75** (1986), 155–172.

[26] Reznick, B.A., *Sums of Even Powers of Real Linear Forms*, Memoirs Amer. Math. Soc., vol. 96, no. 463, Providence, R.I., 1992.

[27] Weyl, H., *Classical Groups*, Princeton Univ. Press, Princeton, N.J., 1946.