The special symplectic structure of binary cubics

Marcus J. Slupinski, Robert J. Stanton

The special symplectic structure of binary cubics

Marcus J. Slupinski * and Robert J. Stanton**

[1] IRMA, Université Louis Pasteur (Strasbourg), 7 rue René Descartes, F-67084 Strasbourg Cedex, France, slupins@math.u-strasbg.fr
[2] Department of Mathematics, Ohio State University, 231 West 18th Avenue, Columbus OH 43210-1174, stanton@math.ohio-state.edu

Abstract

Let k be a field of characteristic not 2 or 3. Let V be the k-space of binary cubic polynomials. The natural symplectic structure on k^2 promotes to a symplectic structure ω on V and from the natural symplectic action of $\mathrm{Sl}(2,k)$ one obtains the symplectic module (V,ω). We give a complete analysis of this symplectic module from the point of view of the associated moment map, its norm square Q (essentially the classical discriminant) and the symplectic gradient of Q. Among the results are a symplectic derivation of the Cardano-Tartaglia formulas for the roots of a cubic, detailed parameters for all $\mathrm{Sl}(2,k)$ and $\mathrm{Gl}(2,k)$-orbits, in particular identifying a group structure on the set of $\mathrm{Sl}(2,k)$-orbits of fixed nonzero discriminant, and a purely symplectic generalization of the classical Eisenstein syzygy for the covariants of a binary cubic. Such fine symplectic analysis is due to the special symplectic nature inherited from the ambient exceptional Lie algebra $\mathfrak{G}_2$.

1 Introduction

Binary cubic polynomials have been studied since the nineteenth century, being the natural setting for a possible extension of the rich theory of binary quadratic forms. An historical summary of progress on this subject can be found in [5], especially concerning results related to integral coefficients. While for a fixed binary cubic interesting questions remain open, e.g. its range in the integers, the number of solutions, etc., it is the structure of the space of all binary cubics that is the topic of this paper.

The space of binary cubics, we will take coefficients in a field, is an example of a prehomogeneous vector space under $\mathrm{Gl}(2,k)$, and from this point of view has been thoroughly investigated. Beginning with the fundamental paper by Shintani [14], recast adelically in [16], an analysis of this pv sufficient to obtain the properties of the

* MJS was supported in part by the Math Research Institute, OSU
** RJS was supported in part by NSF Grants DMS-0301133 and DMS-0701198

Sato-Shintani zeta function was done. Subsequently several descriptions of the orbit structure were obtained, in particular relating them to extensions of the coefficient field. A feature of this space, and some other prehomogeneous spaces, apparently never exploited is the existence of a symplectic structure which is preserved by the natural action of $\mathrm{Sl}(2,k)$.

The purpose of this paper is to expose the rich structure of the space of binary cubics when viewed as a symplectic module using the standard tools of equivariant symplectic geometry, viz. the moment map, its norm square, and its symplectic gradient i.e. the natural Hamiltonian vector field. The advantages are several: somewhat surprisingly, the techniques are universally applicable, with the only hypothesis that the fields not be of characteristic 2 or 3; there are explicit symplectic parameters for each orbit type (including the singular ones not studied previously) that are easily computed for any specific field; the computations are natural; we obtain new results for the space of binary cubics e.g. a group structure on orbits; we obtain ancient results for cubics, namely a symplectic derivation of the Cardano-Tartaglia formula for a root.

This paper arose as a test case to see the extent that we might push a more general project [15] on Heisenberg graded Lie algebras. A symplectic module can be associated to every such graded Lie algebra and in the case of the split Lie algebra $\mathfrak{G}_2$, this symplectic module turns out to be isomorphic to the space of binary cubics with the $\mathrm{Sl}(2,k)$ action mentioned above. Although our approach to binary cubics is inspired by the general situation, in order to give an accessible and elementary presentation, we have made this paper essentially self-contained with only one or two results quoted without proof from [15].

The symplectic technology consists of the following. The moment map, μ, maps the space of binary cubics $\mathrm{S}^3(k^{2^*})$ to the Lie algebra $\mathfrak{sl}(2,k)$ of $\mathrm{Sl}(2,k)$. By means of the Killing form on $\mathfrak{sl}(2,k)$ one obtains a scalar valued function Q on $\mathrm{S}^3(k^{2^*})$, the norm square of μ. Using the symplectic structure one constructs Ψ, the symplectic gradient of Q, as the remaining piece of symplectic machinery. This symplectic module appears to be "special" in several ways, e.g. a consequence of our analysis is that all the $\mathrm{Sl}(2,k)$ orbits in $\mathrm{S}^3(k^{2^*})$ are co-isotropic (see [15] for the general case). Let us recall that over the real numbers it has been shown that there is also a very strong link between special symplectic connections (see [3]) and Heisenberg graded Lie algebras (called 2-graded in [3]).

Here is a more detailed overview of the paper. We will analyze each of the symplectic objects μ, Q, Ψ and determine for each of them their image, their fibre, the $\mathrm{Sl}(2,k)$ orbits in each fibre, and explicit parameters and isotropy for each orbit type. This is all done with symplectic methods, so that furthermore we identify the symplectic geometric meaning of these fibres. For example, we show that the null space, Z, of μ is the set of multiples of cubes of linear forms. As $\mathrm{Sl}(2,k)$ preserves the null space, we obtain a decomposition into a collection of isomorphic Lagrangian orbits which we show are parametrized by k^*/k^{*3}. Binary cubics whose moment lies in the nonzero nilpotent cone of $\mathfrak{sl}(2,k)$ turn out to be those which contain a factor that is the square of a linear form. For these there is only one orbit, whose image under μ we characterize. The pullback by means of μ of the natural symplectic structure on

the image and the restriction of the symplectic form on $\mathrm{S}^3(k^{2^*})$ essentially coincide. The generic case is when the image of the moment map lies in the semisimple orbits of $\mathfrak{sl}(2,k)$. In this case the $\mathrm{Sl}(2,k)$ orbits are different from the $\mathrm{Gl}(2,k)$ orbits, in contrast to the earlier cases. Here each of the values of Q in k^* determine a collection of $\mathrm{Sl}(2,k)$ orbits for which we give symplectic parameters using a 'sum of cubes' theorem. As a consequence we show that the orbits for a fixed nonzero value of Q form a group (over $\mathbb{Z}$ see [1]) which we explicitly identify. Interestingly, a binary cubic is in the orbit corresponding to the identity of this group if and only if it is reducible. The set of binary cubics corresponding to a fixed nonzero value of Q is not stable under $\mathrm{Gl}(2,k)$. However the set of binary cubics for which the value of Q belongs to a fixed nonzero square class of k is stable under $\mathrm{Gl}(2,k)$ and we obtain an explicit parametrisation of all $\mathrm{Gl}(2,k)$ orbits on this set.

If the field of coefficients is specialized to say $\mathbb{C}$ then several of the results herein are known. For example, that the zero set of Q is the tangent variety to Z, or that the generic orbit is the secant variety of Z can be found in the complex algebraic geometric literature. For some other fields other results are in the literature. However, the use of symplectic methods is new to all these cases and gives a unifying approach that seems to make transparent many classic results. For example, a careful analysis of μ and Ψ in the generic case leads to a proof of the Cardano-Tartaglia formula for a root of a cubic. As another application we conclude the paper with a symplectic generalization of the classical Eisenstein syzygy for the covariants (compare to [12],[10]) of a binary cubic. This is interesting because there is an analogue of this form of the Eisenstein syzygy for the symplectic module associated to any Heisenberg graded Lie algebra ([15]). Finally, we remark that the symplectic methodology used in this paper could be used to understand binary cubics over the integers or more general rings.

We are very pleased to acknowledge the support of our respective institutions that made possible extended visits. To the gracious faculty of the Université Louis Pasteur goes a sincere merci beaucoup from RJS. In addition, RJS wants to acknowledge the support of Max Planck Institut, Bonn, for an extended stay during which some of this research was done.

2 Binary cubics as a symplectic space

Let k be a field such that $char(k) \neq 2, 3$. The vector space k^{2^*} has a symplectic structure

$$\Omega(ax + by, a'x + b'y) = ab' - ba'.$$

Functorially one obtains a symplectic structure on the set of binary cubics

$$\mathrm{S}^3(k^{2^*}) = \{ax^3 + 3bx^2y + 3cxy^2 + dy^3 : a, b, c, d \in k\}.$$

Explicitly, if $P = ax^3+3bx^2y+3cxy^2+dy^3$ and $P' = a'x^3+3b'x^2y+3c'xy^2+d'y^3$,

$$\omega(P, P') = ad' - da' - 3bc' + 3cb'. \tag{1}$$

In particular, we have

$$\omega(P,(ex+fy)^3) = P(f,-e). \tag{2}$$

Hence for $ex+fy \neq 0$,

$$(ex+fy) \mid \mathrm{P} \iff \omega(P,(ex+fy)^3) = 0. \tag{3}$$

This indicates that one can use the symplectic form ω to study purely algebraic properties of the space of binary cubics. More generally, the interplay of symplectic methods and the algebra of binary cubics will be the primary theme of this paper.

The group

$$\mathrm{Sl}(2,k) = \{\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} : \alpha\delta - \beta\gamma = 1\}$$

acts on k^{2^*} via the transpose inverse:

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\cdot x = \delta x - \beta y, \quad \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\cdot y = -\gamma x + \alpha y, \tag{4}$$

and this action identifies $\mathrm{Sl}(2,k)$ with the group of transformations of k^{2^*} that preserve the symplectic form Ω, i.e. $\mathrm{Sp}(k^{2^*},\Omega)$. It follows that the functorial action of $\mathrm{Sl}(2,k)$ on $\mathrm{S}^3(k^{2^*})$ preserves the symplectic form ω. There is no kernel of this action thus $\mathrm{Sl}(2,k) \hookrightarrow Sp(\mathrm{S}^3(k^{2^*}),\omega)$.

The Lie algebra $\mathfrak{sl}(2,k)$ acts on k^{2^*} via the negative transpose:

$$\begin{pmatrix}\alpha & \beta\\ \gamma & -\alpha\end{pmatrix}\cdot x = -\alpha x - \beta y, \quad \begin{pmatrix}\alpha & \beta\\ \gamma & -\alpha\end{pmatrix}\cdot y = -\gamma x + \alpha y, \tag{5}$$

which in terms of differential operators acting on polynomial functions on k^2 corresponds to the action

$$\begin{pmatrix}\alpha & \beta\\ \gamma & -\alpha\end{pmatrix}\cdot f = \alpha(-x\partial_x f + y\partial_y f) - \beta y\partial_x f - \gamma x\partial_y f. \tag{6}$$

In particular, this gives the following action of $\mathfrak{sl}(2,k)$ on cubics:

$$\begin{aligned} x^3 &\mapsto -3\alpha x^3 - 3\beta x^2 y\\ x^2 y &\mapsto -\gamma x^3 - \alpha x^2 y - 2\beta x y^2\\ x y^2 &\mapsto -2\gamma x^2 y + \alpha x y^2 - \beta y^3\\ y^3 &\mapsto -3\gamma x y^2 + 3\alpha y^3. \end{aligned}$$

2.1 Symplectic covariants

Among the basic tools of equivariant symplectic geometry are the moment map (μ), its norm square (Q) and the symplectic gradient of Q (Ψ). The symplectic structure on $\mathrm{S}^3(k^{2^*})$ is not generic as it is consistent with one inherited from an ambient

Heisenberg graded Lie algebra, hence the description "special". In [15] in the setting of Heisenberg graded Lie algebras we derive the fundamental properties of the basic symplectic objects as well as give explanations for normalizing constants, and identify characteristic features of these special symplectic structures. For the purposes of this paper the explicit formulae will suffice.

Definition 2.1 *(i) The moment map* $\mu : \mathrm{S}^3(k^{2^*}) \to \mathfrak{sl}(2,k)$ *here is*

$$\mu(ax^3+3bx^2y+3cxy^2+dy^3) = \begin{pmatrix} ad-bc & 2(bd-c^2) \\ 2(b^2-ac) & -(ad-bc) \end{pmatrix}. \tag{7}$$

(ii) The cubic covariant $\Psi : \mathrm{S}^3(k^{2^*}) \to \mathrm{S}^3(k^{2^*})$ *is given by*

$$\begin{aligned} \Psi(P) = \mu(P)\cdot P = (-3a\alpha - 3b\gamma)x^3 + (-3a\beta - 3b\alpha - 6c\gamma)x^2y \\ + (-6b\beta + 3c\alpha - 3d\gamma)xy^2 + (-3c\beta + 3d\alpha)y^3 \end{aligned} \tag{8}$$

where $P = ax^3+3bx^2y+3cxy^2+dy^3$ *and*

$$\begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha \end{pmatrix} = \begin{pmatrix} ad-bc & 2(bd-c^2) \\ 2(b^2-ac) & -(ad-bc) \end{pmatrix}.$$

(iii) The normalised quartic invariant $Q_n : \mathrm{S}^3(k^{2^*}) \to k$ *is*

$$Q_n(P) = -\det\mu(P) = (a^2d^2 - 3b^2c^2 - 6abcd + 4b^3d + 4ac^3). \tag{9}$$

Notice that $Q_n(P)$ is a multiple of the classic discriminant of the polynomial P.

Remark 2.2 *The symmetric role of the coordinates* x *and* y *is implemented by*

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

which satisfies $J\cdot x = y$, $J\cdot y = -x$ *and*

$$J\cdot(ax^3+3bx^2y+3cxy^2+dy^3) = -dx^3+3cx^2y-3bxy^2+ay^3.$$

From (7) *it follows that* $\mu(J\cdot P)$ *is the cofactor matrix of* $\mu(P)$.

Remark 2.3 *The set of symplectic covariants* $\omega, \mu, \Psi, Q, Q_n$ *defined above is not the only choice possible for the purposes of this article. One could just as well use*

$$\omega_\lambda = \lambda\omega, \quad \mu_\lambda = \lambda\mu, \quad \Psi_\lambda = \lambda\Psi, \quad Q_\lambda = \lambda^2 Q$$

where $\lambda \in k^*$.

The moment map is characterised by the identity

$$Tr(\mu(P)\xi) = -\frac{1}{3}\omega(\xi\cdot P, P) \qquad \forall P \in \mathrm{S}^3(k^{2^*}),\ \forall \xi \in \mathfrak{sl}(2,k), \tag{10}$$

which specialized to $\xi = \mu(P)$ gives a characterization of Ψ

$$Q(P) = 8\omega(P, \Psi(P)). \tag{11}$$

From (10) one gets that μ is $\mathrm{Sl}(2,k)$-equivariant:

$$\mu(g \cdot P) = g\mu(P)g^{-1} \qquad \forall P \in \mathrm{S}^3(k^{2^*}),\ \forall g \in \mathrm{Sl}(2,k),$$

and $\mathfrak{sl}(2,k)$-equivariant:

$$d\mu_P(\xi \cdot P) = [\xi, \mu(P)] \qquad \forall P \in \mathrm{S}^3(k^{2^*}),\ \forall \xi \in \mathfrak{sl}(2,k).$$

Here, $d\mu_P(Q) = 2B_\mu(P,Q)$ where $B_\mu : \mathrm{S}^3(k^{2^*}) \times \mathrm{S}^3(k^{2^*}) \to \mathfrak{sl}(2,k)$ is the unique symmetric bilinear map such that $\mu(P) = B_\mu(P,P)$.

From the $\mathrm{Sl}(2,k)$ and $\mathfrak{sl}(2,k)$ equivariance of μ one obtains the $\mathrm{Sl}(2,k)$ and $\mathfrak{sl}(2,k)$ equivariance of Ψ, Q and Q_n. Several useful relations among μ, Ψ and Q are derived in [15]. The following involves a relation between vanishing sets of symplectic covariants.

Proposition 2.4 *Let P be a binary cubic. Then*

$$\mu(P) = 0 \ \Rightarrow\ \Psi(P) = 0 \ \Rightarrow\ Q(P) = 0.$$

Proof. Since $\Psi(P) = \mu(P) \cdot P$, it is obvious that $\mu(P) = 0 \Rightarrow \Psi(P) = 0$. Suppose that $\Psi(P) = 0$. Then by equation (10)

$$Tr(\mu(P)^2) = -\frac{1}{3}\omega(\Psi(P), P) = 0.$$

But $\mu(P)^2 + \det\mu(P)Id = 0$ by the Cayley-Hamilton theorem, so $\det\mu(P) = 0$ and hence $Q(P) = 0$. QED

From the invariant theory point of view a covariant is an $\mathrm{Sl}(2,k)$ invariant in $\mathrm{S}^*(\mathrm{S}^3(\mathrm{k}^{2^*})) \otimes \mathrm{S}^*(\mathrm{k}^{2^*})$. Concerning completeness of the symplectic invariants one has the classic result of Eisenstein [8].

Proposition 2.5 *(i) μ, Ψ, Q and the identity generate the Sl$(2,k)$ invariants in $\mathrm{S}^3(k^{2^*}) \otimes \mathrm{S}^*(k^{2^*})$.*

(ii) The only relation among them viewed as functions on k^2 is

$$\Psi(P)(\cdot)^2 - 9Q_n(P)P(\cdot)^2 = -\frac{9}{2}\Omega_{k^2}(\mu(P)\cdot, \cdot)^3,$$

here Ω is extended by duality to $k^2 \times k^2$.

Proof. We shall give a symplectic proof of the relation (ii) in §3. QED

Remark 2.6 *There are two interesting results related by a simple scaling to the Eisenstein result. Fix $P \in \mathrm{S}^3(k^{2^*})$ with $Q_n(P) \neq 0$. One can associate to P a type of Clifford algebra, $Cliff_P$, and in [9] it is shown that the center of $Cliff_P$ is the coordinate algebra of the genus one curve $X^2 - 27Q_n(P) = Z^3$. The other result arises from the observation that we could work over, say, $\mathbb{Z}$ instead of k. Then in [11] Mordell showed that all integral solutions (X, Y, Z) to $X^2 + kY^2 = Z^3$ with $(X, Z) = 1$ are obtained from some $P \in \mathrm{S}^3(\mathbb{Q}^{2^*})$ with $Q_n(P) = -4k$ and evaluating (ii) at a lattice point in $\mathbb{Q}^2$. We will not use these results in this paper but we will give a symplectic proof at another time.*

Remark 2.7 *The Proposition gives a complete description of binary cubics from the point of view of Sl$(2, k)$ invariant theory. From the symplectic theory point of view, in [15] we give characterizations of Sl$(2, k)$ as the subgroup of $Sp(\mathrm{S}^3(k^{2^*}), \omega)$ that preserves $Q(\cdot)$ and as the subgroup of $Sp(\mathrm{S}^3(k^{2^*}), \omega)$ that commutes with Ψ.*

2.2 The image of the moment map

As $\mu : \mathrm{S}^3(k^{2^*}) \to \mathfrak{sl}(2, k)$ is equivariant, the image of μ is a union of $\mathrm{Sl}(2, k)$ invariant sets. Of course, the invariant functions on $\mathfrak{sl}(2, k)$ are generated by det. The following description of the orbits of $\mathrm{Sl}(2, k)$ acting on level sets of det uses the symplectic structure on k^{2^*}. Lacking any reference for this probably known result we include a proof. Subsequently, Paul Ponomarev brought to our attention the material in [2] p.158-159 from which an alternate albeit non-symplectic proof can be extracted.

Proposition 2.8 *Let $\Delta \in k$ and set*

$$\mathfrak{sl}(2, k)_\Delta = \{X \in \mathfrak{sl}(2, k) \setminus \{0\} : \ \det X = \Delta\},$$
$$k^*_\Delta = \{x \in k^* : \ \exists a, b \in k \text{ such that } x = a^2 + b^2\Delta\}.$$

Then the orbits of Sl$(2, k)$ acting on $\mathfrak{sl}(2, k)_\Delta$ are in bijection with k^*/k^*_Δ under the map $\nu_\Delta : \mathfrak{sl}(2, k)_\Delta \to k^*/k^*_\Delta$ defined by

$$\nu_\Delta(X) = [\Omega(v, X \cdot v)] \tag{12}$$

where v is any element in k^{2^*} which is not an eigenvector of X.

Proof. We make some preliminary remarks before proving the result. First we observe that the definition of $\nu_\Delta(X)$ is independent of choice of v. Indeed, given v which is not an eigenvector of X, then $\{v, X \cdot v\}$ is a basis of k^{2^*}. Given w any other vector which is not an eigenvector then $w = av + bX \cdot v$, and using Cayley-Hamilton we obtain that $[\Omega(v, X \cdot v)] = [\Omega(w, X \cdot w)]$.

Next, note that if $X \in \mathfrak{sl}(2, k)$ there exists $g \in \mathrm{Sl}(2, k)$ and $\beta, \gamma \in k$ such that

$$gXg^{-1} = \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix}.$$

So to prove the result, we need only consider matrices in $\mathfrak{sl}(2,k)_\Delta$ of the form $X = \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix}$ with either β or γ nonzero. Since

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & -\gamma \\ -\beta & 0 \end{pmatrix},$$

we can further suppose that $\gamma \neq 0$. Then x is not an eigenvector of X and $\nu_{\det X}(X) = [\Omega(x, X \cdot x)] = [\Omega(x, \gamma x)] = [\gamma]$.

Suppose $\begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & \beta' \\ \gamma' & 0 \end{pmatrix}$ in $\mathfrak{sl}(2,k)_\Delta$ have the same value of ν_Δ, i.e., $\beta\gamma = -\Delta = \beta'\gamma'$ and $[\gamma] = [\gamma']$.

Then there exist p, q in k such that $\gamma' = (p^2 + q^2 \det X)\gamma$. Take as *Ansatz*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} p & -q\frac{\Delta}{\gamma'} \\ \gamma q & p\frac{\gamma}{\gamma'} \end{pmatrix}.$$

Then

$$\begin{aligned} \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= p^2 \tfrac{\gamma}{\gamma'} + q^2 \Delta \tfrac{\gamma}{\gamma'} \\ &= \tfrac{\gamma}{\gamma'}(p^2 + q^2\Delta) \\ &= 1. \end{aligned}$$

A routine computation shows that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & \beta' \\ \gamma' & 0 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix},$$

and so ν_Δ separates orbits.

To show that given $\alpha \neq 0$, there is an X with $\det X = \Delta$ and $\nu_\Delta(X) = [\alpha]$, take

$$X = \begin{pmatrix} 0 & -\frac{\Delta}{\alpha} \\ \alpha & 0 \end{pmatrix}.$$

Then $\det X = \Delta$ and $\nu_\Delta(X) = [\alpha]$. Finally, $\mathrm{Sl}(2,k)$ invariance of ν_Δ follows from the definition of ν_Δ. QED

Remark 2.9 *We make some elementary observations concerning the Sl$(2,k)$ adjoint orbits. If $-\Delta \in {k^*}^2$, then $k^*_\Delta = k^*$ and there is only one orbit. If $\Delta = 0$ then $k^*_\Delta = {k^*}^2$ and there is one nilpotent orbit for every element of $k^*/{k^*}^2$. If $-\Delta \notin {k^*}^2$ is nonzero, then k^*_Δ is the set of values in k^* taken by the norm function associated to the quadratic extension $k(\sqrt{-\Delta})$ or, equivalently, by the anisotropic quadratic form $x^2 + \Delta y^2$ on k^2. It is well-known that this is a proper subgroup of k^*, at least in characteristic 0, (with thanks to P. Ponomarev for a discussion on characteristic p) and so in characteristic zero there are at least two orbits.*

Remark 2.10 *Since k^*/k^*_Δ is a group, the Proposition puts a natural group structure on the set of orbits of $Sl(2,k)$ acting on trace free matrices of fixed determinant. Alternatively, $\mathfrak{sl}(2,k)$ can be $Sl(2,k)$-equivariantly identified with $S^2(k^{2*})$, the space of binary quadratic forms, by*

$$X \quad \longleftrightarrow \quad q_X(v) = \Omega(v, X \cdot v).$$

By transport of structure, the Proposition then puts a natural group structure on the set of orbits of $Sl(2,k)$ acting on binary quadratic forms of fixed discriminant. One can check that this is Gauss composition. In Theorems 3.34 and 3.46 we will put a natural group structure on orbits of binary cubics with fixed nonzero discriminant.

The image of the moment map can be characterized as follows.

Theorem 2.11 *Let $X \in \mathfrak{sl}(2,k) \setminus \{0\}$. Then*

$$X \in \operatorname{Im}\mu \quad \Longleftrightarrow \quad \nu_{\det X}(X) = [2].$$

Proof. As before, we can suppose without loss of generality that $X = \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix}$ with say β nonzero.
($\Rightarrow$) : If $X = \mu(P)$ and $P = ax^3 + 3bx^2y + 3cxy^2 + dy^3$, we have

$$\begin{aligned} ad - bc &= 0 \\ 2(bd - c^2) &= \beta \\ 2(b^2 - ac) &= \gamma. \end{aligned}$$

Hence $b\beta = d\gamma$ and

$$-\beta = 2(c^2 - d^2\frac{\gamma}{\beta}) = 2(c^2 + (\frac{d}{\beta})^2(-\beta\gamma)) = 2(c^2 + (\frac{d}{\beta})^2 \det X)$$

so that $\nu_{\det X}(X) = [-\beta] = [2]$.
($\Leftarrow$): Since $\nu_{\det X}(X) = [-\beta]$ and by hypothesis $\nu_{\det X}(X) = [2]$, there exist p, q in k such that

$$-\beta = 2(p^2 + q^2 \det X) = 2(p^2 - q^2\beta\gamma).$$

If we set

$$c = p, \quad a = \frac{\gamma}{\beta}p, \quad d = \beta q, \quad b = \gamma q$$

and

$$P = ax^3 + 3bx^2y + 3cxy^2 + dy^3,$$

it is easily checked that

$$\mu(P) = \begin{pmatrix} ad - bc & 2(bd - c^2) \\ 2(b^2 - ac) & -(ad - bc) \end{pmatrix} = \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix} = X.$$

QED

Remark 2.12 *This result is a weak form of the Eisenstein identity. Indeed, if one cubes both sides of* $\nu_{\det X}(X) = [2]$ *and uses Gauss composition, one obtains the Eisenstein identity evaluated at a particular vector.*

Remark 2.13 *Varying the symplectic structure to* $\omega_\lambda, \lambda \in k^*$ *one can sweep out the other orbits with a moment map.*

Corollary 2.14 *Let* P, P' *be nonzero binary cubics such that* $Q_n(P) = Q_n(P')$ *and such that* $\mu(P)$ *and* $\mu(P')$ *are nonzero. Then there exists* $g \in Sl(2,k)$ *such that* $g \cdot \mu(P) = \mu(P')$.

Proof. Since $Q_n(P) = Q_n(P')$, we have $\det \mu(P) = \det \mu(P')$. By the previous theorem,

$$\nu_{\det \mu(P)}(\mu(P)) = \nu_{\det \mu(P')}(\mu(P'))$$

and the result follows from Proposition 2.8. QED

2.3 The image and fibres of Ψ

Proposition 2.15 $P \in \mathrm{S}^3(k^{2^*})$ *with* $Q_n(P) \neq 0$ *is in the image of* Ψ *if and only if* $9Q_n(P)$ *is a cube in* k^*.

Proof. $(\Rightarrow)$: Suppose that $P = \Psi(B)$. The key to the argument is a result from [15] that is special to Heisenberg graded Lie algebras, namely a formula for Ψ^2. From this result one obtains $\Psi^2(B) = -(9Q_n(B))^2 B$. On the other hand we have $\Psi^2(B) = \Psi(P)$. Hence $B = -(9Q_n(B))^{-2}\Psi(P)$. Applying Ψ again and using that Ψ is cubic we obtain $P = \Psi(B) = -\eta^3(9Q_n(P))^2 P$ where $\eta = -(9Q_n(B))^{-2}$. So $(-\eta)^3 = (9Q_n(P))^{-2}$. Now $(-\eta(9Q_n(B))^2)^3 = 1$ so $(9Q_n(B))^6 = (-\eta)^{-3} = (9Q_n(P))^2$. Thus we obtain $9Q_n(P) = (\pm 9Q_n(B))^3$.
$(\Leftarrow)$: Suppose $9Q_n(P) = \lambda^3$. Set $B = -\frac{1}{\lambda^2}\Psi(P)$. Then as above, $\Psi(B) = P$. QED

Corollary 2.16 *For* $P \in \mathrm{S}^3(k^{2^*})$ *with* $9Q_n(P) \in k^{*3}$ *the fiber* $\Psi^{-1}(P)$ *consists of one element.*

Proof. From the previous proof, if $P = \Psi(B)$ then $B = -(9Q_n(B))^{-2}\Psi(P)$. QED

Remark 2.17 *We will see later that a nonzero* $P \in \mathrm{S}^3(k^{2^*})$ *with* $Q_n(P) = 0$ *is in the image of* Ψ *if and only if* $\mu(P) = 0$ *and* $I_T(P) = [6]$ *(cf Proposition 3.19). The fibre of* Ψ *is then given by Proposition 3.23.*

3 Orbits and fibres

3.1 Symplectic covariants and triple roots

One has the natural 'algebraic' condition

Definition 3.1 $T = \{P \in \mathrm{S}^3(k^{2^*}) : P \neq 0$ *and* P *has a triple root*$\}$,

and the natural 'symplectic' condition

Definition 3.2 $Z_\mu = \{P \in \mathrm{S}^3(k^{2^*}) : P \neq 0$ *and* $\mu(P) = 0\}$.

The next proposition shows that the symplectic quantity μ detects the purely algebraic property of whether or not a binary cubic has a triple root.

Proposition 3.3 $T = Z_\mu$.

Proof. Let $P = ax^3 + 3bx^2y + 3cxy^2 + dy^3$. Then $P \in Z_\mu$ iff $\mu(P) = 0$ iff $ad = bc, bd = c^2$ and $b^2 = ac$.

If $bc = 0$, then $cbd = c^3 = 0$ and $b^3 = acb = 0$. Hence $b = c = 0$ and either $a = 0$ or $d = 0$. In the first case $P = dy^3$ and in the second $P = ax^3$.

If $bc \neq 0$, then $a = \frac{b^2}{c}$ and $d = \frac{c^2}{b}$ which means $P = \frac{1}{bc}(bx + cy)^3$. QED

In order to determine the $\mathrm{Sl}(2, k)$ orbit structure in the level set $Z_\mu = \mu^{-1}(0)\backslash\{0\}$ we need to construct an invariant that separates the orbits. We begin with the observation that the factorisation of $P \in T$ is not unique.

Lemma 3.4 *Let* $\lambda, \mu \in k^*$ *and* $\phi, \psi \in k^{2^*}$ *be such that* $\lambda\phi^3 = \mu\psi^3$. *Then* $\frac{\lambda}{\mu}$ *is a cube and* ϕ *and* ψ *are proportional.*

Proof. Unique factorisation. QED

This means the following (algebraic) definition makes sense.

Definition 3.5 *Define* $I_T : T \to k^*/k^{*3}$ *by*

$$I_T(P) = [\lambda]_{k^*/k^{*3}}$$

where $P = \lambda\phi^3, \lambda \in k^*$ *and* $\phi \in k^{2^*}$.

One can formulate the definition using symplectic methods. Given a non-zero $\phi \in k^{2^*}$ there is a $g \in \mathrm{Sl}(2, k)$ with $\Omega(\phi, g \cdot \phi) = 1$. If $P = \lambda\phi^3$ then

$$\omega(P, (g \cdot \phi)^3) = \lambda\omega(\phi^3, (g \cdot \phi)^3) = \lambda\Omega(\phi, g \cdot \phi)^3 = \lambda. \tag{13}$$

Thus $I_T(P) = [\omega(P, (g \cdot \phi)^3)]$.

Proposition 3.6 *(i) Let* $P_1, P_2 \in T$. *Then*

$$Sl(2, k) \cdot P_1 = Sl(2, k) \cdot P_2 \iff I_T(P_1) = I_T(P_2). \tag{14}$$

(ii) The map I_T *induces a bijection of the space of orbits*

$$Z_\mu/Sl(2, k) \longleftrightarrow k^*/k^{*3}. \tag{15}$$

(iii) Let $P \in T$ *and let* $G_P = \{g \in Sl(2, k) : g \cdot P = P\}$ *be the isotropy subgroup of* P. *Then*

$$G_P = \{g \in Sl(2, k) : \exists \mu \in k^* \text{ s.t. } g \cdot \phi = \mu\phi \text{ and } \mu^3 = 1\}$$

where $P = \lambda\phi^3, \lambda \in k^*$ *and* $\phi \in k^{2^*}$.

Proof. (i): Suppose that $P_1 = \lambda\phi^3$ and that there exists $g \in \mathrm{Sl}(2,k)$ such that $g \cdot P_1 = P_2$. Then $P_2 = g \cdot (\lambda\phi^3) = \lambda(g \cdot \phi)^3$ and $I_T(P_2) = [\lambda] = I_T(P_1)$.

Conversely, suppose $P_1 = \lambda_1\phi_1^3$, $P_2 = \lambda_2\phi_2^3$ and $I_T(P_1) = I_T(P_2)$. The action of $\mathrm{Sl}(2,k)$ on nonzero vectors of k^{2^*} is transitive so we can find $g \in \mathrm{Sl}(2,k)$ such that $g \cdot \phi_1 = \phi_2$ and hence such that

$$g \cdot P_1 = \lambda_1\phi_2^3.$$

Since $I_T(P_1) = I_T(P_2)$, there exists $\rho \in k$ such that $\lambda_1 = \rho^3\lambda_2$ and

$$g \cdot P_1 = \lambda_2(\rho\phi_2)^3.$$

Choosing $h \in \mathrm{Sl}(2,k)$ such that $h \cdot (\rho\phi_2) = \phi_2$, we have $(hg) \cdot P_1 = P_2$.
(ii): By (i), the map I_T induces an injection of the space of orbits of $\mathrm{Sl}(2,k)$ acting on T into k^*/k^{*3}. This is in fact a surjection since if $\lambda \in k^*$, $I_T(\lambda x^3) = [\lambda]$.
(iii): This follows from unique factorisation. QED

Remark 3.7 *Extending ϕ to a basis of k^{2^*} we have the isomorphism*

$$G_P \cong \{\begin{pmatrix} \mu & a \\ 0 & \frac{1}{\mu} \end{pmatrix} : \mu \in k^*, \mu^3 = 1 \text{ and } a \in k\}.$$

Consequently all the Sl$(2,k)$ orbits in Z_μ are isomorphic. Hence Z_μ is a smooth variety, and in [15] we show that it is Lagrangian.

As the center of Gl$(2,k)$ acts on Z_μ by "cubes" it preserves I_T, and thus the Sl$(2,k)$ orbits in Z_μ are the same as the Gl$(2,k)$ orbits. From the point of view of algebraic groups, the result by Demazure [4] characterizes Sl$(2,k)$ as the subgroup of the automorphisms of $\mathrm{S}^3(k^{2^*})$ that preserves Z_μ.

3.2 Symplectic covariants and double roots

In a similar way next we consider the 'algebraic' condition

Definition 3.8 $D = \{P \in \mathrm{S}^3(k^{2^*}) : P \neq 0$ *and P has a double root*$\}$,

and the 'symplectic' condition

Definition 3.9 $N_\mu = \{P \in \mathrm{S}^3(k^{2^*}) : P \neq 0$ *and $\mu(P)$ is nonzero nilpotent*$\}$.

Again it turns out that the symplectic quantity μ detects the purely algebraic property of whether or not a binary cubic has a double root.

Theorem 3.10 $D = N_\mu$.

Proof. The inclusion $D \subseteq N_\mu$ follows from the

Lemma 3.11 *Let $P \in D$ and write $P = (ex+fy)^2(rx+sy)$ with $ex+fy$ and $rx+sy$ independent. Then*

$$\mu(P) = \frac{2}{9}(es-fr)^2 \begin{pmatrix} -ef & -f^2 \\ e^2 & ef \end{pmatrix}.$$

In particular, $\mathrm{Ker}\,\mu(P)$ *is spanned by the double root $ex+fy$.*

Proof. Straightforward calculation. QED

To prove the inclusion $N_\mu \subseteq D$, suppose $\mu(P)$ is a nonzero nilpotent. Then $\operatorname{Ker}\mu(P)$ is one-dimensional, spanned by, say, $v \in k^{2^*}$. Since $\mathrm{Sl}(2,k)$ acts transitively on nonzero vectors in k^{2^*}, there exists $g \in \mathrm{Sl}(2,k)$ such that $g \cdot v = x$. Then $\mu(g \cdot P) = g\mu(P)g^{-1}$ is nonzero nilpotent with kernel spanned by x. Let $g \cdot P = ax^3 + 3bx^2y + 3cxy^2 + dy^3$. Then by the formulae (6) and (7), the condition $\mu(g \cdot P) \cdot x = 0$ is equivalent to the system

$$\begin{aligned} ad - bc &= 0 \\ bd - c^2 &= 0. \end{aligned}$$

If $(c,d) \neq (0,0)$ this implies there exists $\lambda, \nu \in k$ such that $(a,b) = \lambda(c,d)$ and $(b,c) = \nu(c,d)$. Hence $c = \nu d, b = \nu^2 d, a = \nu^3 d$ and $\mu(g \cdot P) = 0$ which is a contradiction. Thus $c = d = 0$ and $g \cdot P = ax^3 + 3bx^2y = x^2(ax + 3by)$. We have $b \neq 0$ (otherwise $\mu(P) = 0$) so x and $ax + by$ form a basis of k^2. Applying g^{-1} to $g \cdot P = x^2(ax + 3by)$ completes the proof. QED

Again, in order to obtain parameters for the orbit structure of N_μ we need standard representatives. The factorisation of $P \in N_\mu$ given by Theorem 3.10 is not unique. However we can use the symplectic form Ω on k^{2^*} to get a canonical form for P.

Lemma 3.12 *Let $P \in N_\mu$. There exists a unique basis $\{\phi, \xi\}$ of k^{2^*} such that $P = \phi^2\xi$ and $\Omega(\phi, \xi) = 1$.*

Proof. If $P \in N_\mu$ then P has a double root by Theorem 3.10. Fix a factorisation $P = \phi_1^2\xi_1$. By unique factorisation, any other factorisation is of the form $P = \phi^2\xi$ where

$$\phi = \lambda\phi_1, \quad \xi = \frac{1}{\lambda^2}\xi_1$$

for some $\lambda \in k^*$. Then $\Omega(\phi, \xi) = 1$ iff $\lambda = \Omega(\phi_1, \xi_1)$ and this proves the claim. QED

Proposition 3.13 *The group $Sl(2,k)$ acts simply transitively on N_μ. Consequently, $Gl(2,k)$ has one orbit on N_μ.*

Proof. Let $P, Q \in N_\mu$ and write $P = \phi^2\xi$ and $Q = \phi'^2\xi'$ with $\Omega(\phi, \xi) = \Omega(\phi', \xi') = 1$. The element g of $GL(2,k)$ defined by $g \cdot \phi = \phi'$ and $g \cdot \xi = \xi'$ is clearly in $\mathrm{Sl}(2,k)$, satisfies $g \cdot P = Q$ and is the unique element of $\mathrm{Sl}(2,k)$ sending P to Q. QED

Remark 3.14 *In [15] when char $k = 0$ we show that N_μ is the tangent variety to Z_μ.*

Remark 3.15 *From Proposition 3.3, Theorem 3.10 and* (9) *we see that $Q_n(P) = 0$ iff P has a multiple root, which is consistent with the classic discriminant interpretation. Also, the open subset of double roots is isomorphic to Sl$(2, k)$. Consequently the variety $Q_n(P) = 0$ is not smooth, but has singular set which is a union over k^*/k^{*3} of isomorphic Lagrangian Sl$(2, k)$-orbits.*

Image and Fibres of $\mu : N_\mu \to \mathfrak{sl}(2, k)$

The image of the moment map on N_μ is given by Theorem 2.11:

Corollary 3.16 $\mu(N_\mu) = \{X \in \mathfrak{sl}(2, k) \setminus \{0\} : \det X = 0$ *and* $\nu_0(X) = [2]\}$.

Now we give two descriptions of the fibres of $\mu : N_\mu \to \mathfrak{sl}(2, k)$: the first symplectic, the second algebraic. Note that the fibres of the moment map are symplectic objects so it is not a priori clear that they have a purely algebraic description.

Proposition 3.17 *Let $P \in N_\mu$ and let $\phi \in k^{2^*}$ be a square factor of P.*

(a) $\mu^{-1}(\mu(P)) = \{P + a\Psi(P) : a \in k\} \cup \{-P + b\Psi(P) : b \in k\}$.

(b) $\mu^{-1}(\mu(P)) = \{P + a\phi^3 : a \in k\} \cup \{-P + b\phi^3 : b \in k\}$.

(c) The affine lines in (a) and (b) are disjoint.

Proof. Since Sl$(2, k)$ acts transitively on N_μ we can assume without loss of generality that $P = 3x^2y$. Then by (7) and (8),

$$\mu(3x^2y) = \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix}, \quad \Psi(3x^2y) = -6x^3.$$

We want to find all $Q \in \mathrm{S}^3(k^{2^*})$ such that

$$\mu(Q) = \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix}. \tag{16}$$

By Theorem 3.10, a solution of this equation is of the form $Q = (ex+fy)^2(rx+sy)$ with $es - fr \neq 0$. Substituting back in (16) we get

$$\frac{2}{9}(es - fr)^2 \begin{pmatrix} -ef & -f^2 \\ e^2 & ef \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix}$$

from which it follows that the set of solutions of equation (16) is:

$$\{x^2(e^2rx + 3y) : e \in k^*, r \in k\} \cup \{x^2(e^2rx - 3y) : e \in k^*, r \in k\}.$$

Since $P = 3x^2y$ and $\Psi(P) = -6x^3$, this proves (a), (b) and (c). QED

The fibre of μ at $\mu(P)$ is also the orbit through P of the isotropy group of $\mu(P)$.

Corollary 3.18 *Let $P \in N_\mu$ and let $G_{\mu(P)} = \{g \in$ Sl$(2, k) : g\mu(P)g^{-1} = \mu(P)\}$. Then $\mu^{-1}(\mu(P)) = G_{\mu(P)} \cdot P$.*

Proof. Since $\mu(P)$ is nilpotent nonzero, a simple calculation shows that

$$G_{\mu(P)} = \{Id + a\mu(P) : a \in k\} \cup \{-Id + b\mu(P) : b \in k\}$$

and the result follows from Proposition 3.17. QED

It appears that N_μ is a regular contact variety. If one endows the nilpotent variety $\mathcal{N}$ in $\mathfrak{sl}(2,k)$ with the KKS symplectic structure, then $\mu : N_\mu \to \mathcal{N}$ is a prequantization of the image of μ.

Image and Fibres of $\Psi : N_\mu \to Z_\mu$

We begin with some properties of Ψ.

Proposition 3.19 *Let $P = \phi^2\xi$ with $\phi, \xi \in k^{2*}$. Then:*

(i) $\mu(\Psi(P)) = 0$;

(ii) ϕ^3 divides $\Psi(P)$;

(iii) $\Psi(P) = 0$ iff $\mu(P) = 0$;

(iv) $\Psi(P) \neq 0 \Rightarrow I_T(\Psi(P)) = [6]_{k^*/k^{*3}}$.

Proof. Set $\phi = ex + fy$ and $\xi = rx + sy$. Then calculation gives

$$\mu(P) = \frac{2}{9}(es - fr)^2 \begin{pmatrix} -ef & -f^2 \\ e^2 & ef \end{pmatrix},$$

$$\Psi(P) = -\frac{2}{9}(es - fr)^3(ex + fy)^3 \tag{17}$$

and all parts of the proposition follow immediately from these formulae. QED

Corollary 3.20 *The image of Ψ on N_μ is $Z_\mu[6]$.*

Proof. According to Proposition 3.19(iv), if $P \in N_\mu$ then $\Psi(P) \in Z_\mu$ and $I_T(\Psi(P)) = [6]_{k^*/k^{*3}}$. Since Ψ is $\mathrm{Sl}(2,k)$-equivariant and $\mathrm{Sl}(2,k)$ acts transitively on both N_μ and $Z_\mu[6]$, it is clear that Ψ maps N_μ onto $Z_\mu[6]$. QED

To describe the fibres we need a symplectic characterization of the double root of a $P \in Z_\mu$. Recall that $ex + fy \neq 0$ is a root of P iff $\omega(P, (ex + fy)^3) = 0$. Analogous to this result we have

Proposition 3.21 *Let P be a binary cubic and $(ex + fy) \in k^{2*}$ be nonzero.*

$$(ex + fy)^2 \mid P \iff B_\mu(P, (ex + fy)^3) = 0. \tag{18}$$

Proof. We begin with two remarks. First, since $\mathrm{Sl}(2,k)$ acts transitively on nonzero elements of k^{2*} and since B_μ and Ψ are $\mathrm{Sl}(2,k)$-equivariant, we can assume without loss of generality that $ex + fy = x$. Second, the formula for B_μ obtained by polarising (7) is

$$B_\mu(P,P') = \begin{pmatrix} \frac{1}{2}(ad' + da' - bc' - cb') & (bd' + db') - cc' \\ bb' - (ac' + ca') & -\frac{1}{2}(ad' + da' - bc' - cb') \end{pmatrix} \qquad (19)$$

if $P = ax^3 + 3bx^2y + 3cxy^2 + dy^3$ and $P' = a'x^3 + 3b'x^2y + 3c'xy^2 + d'y^3$.
Let $P = ax^3 + 3bx^2y + 3cxy^2 + dy^3$. Then

$$B_\mu(P, x^3) = \begin{pmatrix} \frac{1}{2}d & 0 \\ -c & -\frac{1}{2}d \end{pmatrix}$$

and hence x^2 divides P iff $c = d = 0$ iff $B_\mu(P, x^3) = 0$. QED

Now since Ψ maps D to T we expect a criterion involving Ψ for $ex + fy \neq 0$ to be a double root of P.

Proposition 3.22 *Let P be a binary cubic and $(ex + fy) \in k^{2^*}$ be nonzero.*

(i) If $(ex + fy)^2$ divides P then $\Psi(P)$ is proportional to $(ex + fy)^3$.

(ii) If $\Psi(P)$ is a nonzero multiple of $(ex + fy)^3$ then $(ex + fy)^2$ divides P.

(iii) $\{P \in \mathrm{S}^3(k^{2^*}) : B_\mu(P, (ex+fy)^3) = 0\}$ is a Lagrangian subspace of $\mathrm{S}^3(k^{2^*})$.

Proof. (i): If x^2 divides P then taking $e = 1$ and $f = 0$ in the formulae (17) we get $\Psi(P) = -\frac{2}{9}d^3x^3$.
(ii): If there exists $\lambda \in k^*$ such that $(ex + fy)^3 = \frac{1}{\lambda}\Psi(P)$, we have

$$B_\mu(P, (ex + fy)^3) = \frac{1}{\lambda}B_\mu(P, \mu(P) \cdot P).$$

But $B_\mu(P, \mu(P) \cdot P) + B_\mu(\mu(P) \cdot P, P) = [\mu(P), \mu(P)] = 0$ since B_μ is $\mathfrak{sl}(2, k)$-equivariant. Hence $B_\mu(P, \mu(P) \cdot P) = 0$ and $B_\mu(P, (ex + fy)^3) = 0$ which implies by the previous result that $(ex + fy)^2$ divides P.
(iii): Let $L = \{P \in \mathrm{S}^3(k^{2^*}) : B_\mu(P, (ex + fy)^3) = 0\}$. As we saw in the proof above, the binary cubic $ax^3 + 3bx^2y + 3cxy^2 + dy^3$ is in L iff $c = d = 0$ and hence L is of dimension two. It follows from (1) that $\omega(P, P') = 0$ if $P, P' \in L$ and hence L is Lagrangian. QED

We can now give two descriptions of the fibres of $\Psi : N_\mu \to Z_\mu[6]$, the first symplectic, the second algebraic. Again, as the fibres of Ψ are symplectic objects it is not a priori clear that they have a purely algebraic description.

Proposition 3.23 *Let $P \in N_\mu$ and let $\phi \in k^{2^*}$ be a square factor of P.*

(i) $\Psi^{-1}(\Psi(P)) = \{aP + b\Psi(P) : a \in k^*, b \in k\}$.

(ii) $\Psi^{-1}(\Psi(P)) = \{Q \in N_\mu : \phi^2$ divides $Q\}$.

Explicit factorisation of P when $Q_n(P) = 0$

From what has been done thus far we obtain readily

Proposition 3.24 *Let $P = ax^3 + 3bx^2y + 3cxy^2 + dy^3$ be a nonzero binary cubic over a field k such that $\mathrm{char}(k) \neq 2, 3$.*

(i) If $\mu(P) = 0$ then $Q_n(P) = 0$ and

$$P = \begin{cases} ax^3 \text{ or } dy^3 & \text{if } bc = 0, \\ \frac{1}{bc}(bx + cy)^3 & \text{if } bc \neq 0. \end{cases}$$

(ii) If $\mu(P) \neq 0$ and $Q_n(P) = 0$ then

$$P = \begin{cases} x^2(ax + 3by) \text{ or } (3cx + d)y^2 & \text{if } ad - bc = 0, \\ \big(-(b^2 - ac)x + \frac{1}{2}(ad - bc)y\big)^2(\frac{a}{(b^2-ac)^2}x + \frac{4d}{(ad-bc)^2}y) & \text{if } ad - bc \neq 0. \end{cases}$$

3.3 Symplectic covariants and sums of coprime cubes

We have seen that a P with multiple roots corresponds to $Q_n(P) = 0$. So we begin the study of P with $Q_n(P) \neq 0$, in which case the $\mathrm{Sl}(2, k)$ orbits are not the same as the $\mathrm{Gl}(2, k)$ orbits. The values of the symplectic invariant $Q_n(P)$ will have much to say about the roots of P. We begin with the 'natural' condition

Definition 3.25 $\mathcal{O}_{[1]} = \{P \in \mathrm{S}^3(k^{2^*}) : Q_n(P)$ *is a square in* $k^*\}$.

The relevant 'algebraic' definition turns out to be

Definition 3.26 $S = \{P \in \mathrm{S}^3(k^{2^*}) : \exists T_1, T_2 \in T$ *s.t* $P = T_1 + T_2$ *with* T_1, T_2 *coprime*$\}$.

Specializing to the space of binary cubics a general theorem valid for the symplectic covariants of the $\mathfrak{g}_1$ of any Heisenberg graded Lie algebra $\mathfrak{g}$, we get the

Theorem 3.27 *(i) Let $P \in S$ and let $P = T_1 + T_2$ with $T_1, T_2 \in T$ coprime. Then T_1, T_2 are unique up to permutation.*

(ii) Let $P = T_1 + T_2$ with $T_1, T_2 \in T$. Then

$$Q_n(P) = \omega(T_1, T_2)^2. \tag{20}$$

(iii) Let $P \in \mathcal{O}_{[1]}$ and suppose $Q_n(P) = q^2$ with $q \in k^*$. Then

$$T_1 = \frac{1}{2}(P + \frac{1}{3q}\Psi(P)), \quad T_2 = \frac{1}{2}(P - \frac{1}{3q}\Psi(P))$$

are coprime elements of T such that $P = T_1 + T_2$.

Proof. For k algebraically closed an argument that P is a sum of cubes can be found in [6, 17-18]. The fact that $Q_n(P) = \omega(T_1, T_2)^2$ as well as (i) and (iii) are proved for general k and for Heisenberg graded Lie algebras in [15]. QED

Corollary 3.28 $S = \mathcal{O}_{[1]}$.

Remark 3.29 *There is a natural bi-Lagrangian foliation of $\mathcal{O}_{[1]}$ obtained by means of the decomposition $P = T_1 + T_2$. Modulo some technicalities, if one fixes T_2 and varies over T such that $\omega(T, T_2) = \omega(T_1, T_2)$ mod k^{*2}, then does the same with T_1, one obtains a pair of foliations that are transverse and Lagrangian, for details see [15].*

Recall that elements of T are, up to a scalar factor, cubes of linear forms. Hence a binary cubic P is in S iff there exist a basis $\{\phi_1, \phi_2\}$ of k^{2^*} and $\lambda_1, \lambda_2 \in k^*$ such that

$$P = \lambda_1 \phi_1^3 + \lambda_2 \phi_2^3. \tag{21}$$

The λ_i and ϕ_i in this equation are not unique but the direct sum decomposition

$$k^{2^*} =< \phi_1 > \oplus < \phi_2 >$$

is canonically associated to P as is described in the next result.

Corollary 3.30 *(i) $P \in \mathcal{O}_{[1]}$ iff $\mu(P) \neq 0$ is diagonalisable over k, hence $\mu(P)$ is contained in a semisimple orbit.*

(ii) Let $P \in \mathcal{O}_{[1]}$ and let $\{\phi_1, \phi_2\}$ be a basis of k^{2^*}. The following are equivalent:

(a) There exist $\lambda_1, \lambda_2 \in k^*$ such that $P = \lambda_1 \phi_1^3 + \lambda_2 \phi_2^3$.

(b) $\{\phi_1, \phi_2\}$ is a basis of eigenvectors of $\mu(P)$.

(iii) Let $P \in \mathcal{O}_{[1]}$ and suppose $P = \lambda_1 \phi_1^3 + \lambda_2 \phi_2^3$ where $\lambda_1, \lambda_2 \in k^*$ and $\{\phi_1, \phi_2\}$ is a basis of k^{2^*}. Then if q is the square root $\lambda_1 \lambda_2 \Omega(\phi_1, \phi_2)^3$ of $Q_n(P)$,

$$\begin{aligned} \mu(P) \cdot \phi_1 &= -q\phi_1, \\ \mu(P) \cdot \phi_2 &= q\phi_2. \end{aligned}$$

Proof. (i): By Cayley-Hamilton and equation (9),

$$0 = \mu(P)^2 + \det\mu(P) Id = \mu(P)^2 - Q_n(P) Id.$$

Hence $\mu(P)$ is diagonalisable over k iff $Q_n(P)$ is a square in k.
(ii): Since there exists $g \in \mathrm{Sl}(2, k)$ with $< g \cdot \phi_1 >=< x >$ and $< g \cdot \phi_2 >=< y >$, we can assume without loss of generality that $\phi_1 = x$ and $\phi_2 = y$. Setting $P = ax^3 + 3bx^2y + 3cxy^2 + dy^3$, we have: $\{x^3, y^3\}$ is a basis of eigenvectors of $\mu(P)$ iff $\mu(P)$ is diagonal iff (by equation (7))

$$bd - c^2 = b^2 - ac = 0.$$

This equation implies $b(ad - bc) = 0$ and hence, since $Q_n(P) \neq 0$, that $b = 0$ and $c^2 = bd = 0$. It follows that $\{x^3, y^3\}$ is a basis of eigenvectors of $\mu(P)$ iff $b = c = 0$ iff $P = ax^3 + dy^3$.
(iii): As above, we can suppose without loss of generality that $P = ax^3 + dy^3$ and then

$$\mu(P) = \begin{pmatrix} ad & 0 \\ 0 & -ad \end{pmatrix}$$

which implies $\mu(P)\cdot x = -adx$ and $\mu(P)\cdot y = ady$. This proves (iii) since $\Omega(x,y) = 1$. QED

Corollary 3.31 *(Fibres of μ on $\mathcal{O}_{[1]}$). Let $X \in \mathfrak{sl}(2,k)$ be diagonalisable over k, let $\pm q$ be its eigenvalues and let ϕ_+ and ϕ_- be corresponding eigenvectors in k^{2*}. Then*

$$\mu^{-1}(X) = \{a\phi_-^3 + \frac{q}{a\Omega(\phi_-,\phi_+)^3}\,\phi_+^3 :\ a \in k^*\}.$$

Proof. This follows from Corollary 3.30(ii) and (iii). QED

Orbit parameters for $\mathcal{O}_{[1]}$

For generic k there will be many $\mathrm{Sl}(2,k)$ orbits on $\mathcal{O}_{[1]}$. So the first task is to obtain parameters for the orbits. For this the symplectic result Theorem 3.27 leads to a new and effective method. Let $P \in \mathcal{O}_{[1]}$. Then as we have seen, there exist a unique *unordered* pair of elements T_1, T_2 in T such that

$$\begin{aligned} P &= T_1 + T_2, \\ Q_n(P) &= \omega(T_1,T_2)^2. \end{aligned} \tag{22}$$

Hence the map $I_{\mathcal{O}_{[1]}} : \mathcal{O}_{[1]} \to k^* \times_{Z_2} k^*/k^{*3}$

$$I_{\mathcal{O}_{[1]}}(P) = [\omega(T_1,T_2), I_T(T_1)I_T(T_2)^{-1}] \tag{23}$$

is well-defined where $k^* \times_{Z_2} k^*/k^{*3}$ denotes the quotient of $k^* \times k^*/k^{*3}$ by the Z_2-action

$$-1\cdot(\lambda,\alpha) = (-\lambda,\alpha^{-1}).$$

Remark 3.32 *The invariant $I_{\mathcal{O}_{[1]}}(\cdot)$ is symplectic not algebraic since its definition requires the symplectic form. We have not found this invariant for binary cubics in the literature.*

Theorem 3.33 *Let $I_{\mathcal{O}_{[1]}} : \mathcal{O}_{[1]} \to k^* \times_{Z_2} k^*/k^{*3}$ be defined by* (23) *above.*
(i) Let $P, P' \in \mathcal{O}_{[1]}$. Then

$$Sl(2,k)\cdot P' = Sl(2,k)\cdot P \iff I_{\mathcal{O}_{[1]}}(P') = I_{\mathcal{O}_{[1]}}(P).$$

(ii) The map $I_{\mathcal{O}_{[1]}}$ induces a bijection

$$\mathcal{O}_{[1]}/Sl(2,k) \longleftrightarrow k^* \times_{Z_2} k^*/k^{*3}.$$

(iii) Let $P \in \mathcal{O}_{[1]}$ and suppose $P = \lambda_1\phi_1^3 + \lambda_2\phi_2^3$ where $\lambda_1, \lambda_2 \in k^*$ and $\{\phi_1,\phi_2\}$ is a basis of k^{2*}. Let $G_P = \{g \in Sl(2,k) :\ g\cdot P = P\}$. Then

$$G_P = \{g \in Sl(2,k) :\ \exists \mu \in k^* \text{ s.t. } g\cdot\phi_1 = \mu\phi_1, g\cdot\phi_2 = \frac{1}{\mu}\phi_2 \text{ and } \mu^3 = 1\}.$$

Proof. (i): Since ω and I_T are $\mathrm{Sl}(2,k)$-invariant, it is clear from (23) that the map $I_{\mathcal{O}_{[1]}} : \mathcal{O}_{[1]} \to k^* \times_{Z_2} k^*/k^{*3}$ factors through the action of $\mathrm{Sl}(2,k)$. To show that the induced map on orbit space is injective, suppose that P and P' are binary cubics such that $I_{\mathcal{O}_{[1]}}(P') = I_{\mathcal{O}_{[1]}}(P)$. First choose $g, g' \in \mathrm{Sl}(2,k)$ such that

$$\begin{aligned} g \cdot P &= ax^3 + by^3, \\ g' \cdot P' &= a'x^3 + b'y^3. \end{aligned} \tag{24}$$

From equations (1) and (9) we have

$$\omega(x^3, y^3) = 1, \quad Q_n(P) = a^2b^2, \quad Q_n(P') = a'^2b'^2.$$

Hence $I_{\mathcal{O}_{[1]}}(P') = I_{\mathcal{O}_{[1]}}(P)$ implies

$$[ab\,, [a\,][b]^{-1}\,] = [a'b'\,, [a'][b']^{-1}\,]$$

in $k^* \times_{Z_2} k^*/k^{*3}$. There are two possibilities:

- $ab = a'b', \quad [a\,][b]^{-1} = [a'][b']^{-1}$;
- $ab = -a'b', \quad [a\,][b]^{-1} = [b'][a']^{-1}$.

In the first case, we have

$$[ab][a\,][b]^{-1} = [a'b'][a'][b']^{-1},$$

hence $[a^2] = [a'^2]$ and so $[a] = [a']$ as the group k^*/k^{*3} is of exponent 3. Thus there exists $r \in k^*$ such that $a' = r^3a$ and $b' = \frac{1}{r^3}b$. If we define $h \in GL(2,k)$ by

$$h \cdot x = rx, \quad h \cdot y = \frac{1}{r}y,$$

it is clear that $h \in \mathrm{Sl}(2,k)$ and $h \cdot (g \cdot P) = g' \cdot P'$. Hence P and P' are in the same $\mathrm{Sl}(2,k)$-orbit.

In the second case, we have $[a^2] = [b'^2]$, $[a] = [b']$ and there exists $r \in k^*$ such that $b' = r^3a$ and $a' = -\frac{1}{r^3}b$. If we define $h \in GL(2,k)$ by

$$h \cdot x = ry, \quad h \cdot y = -\frac{1}{r}x,$$

it is clear that $h \in \mathrm{Sl}(2,k)$ and $h \cdot (g \cdot P) = g' \cdot P'$. Hence P and P' are in the same $\mathrm{Sl}(2,k)$-orbit and we have proved that $I_{\mathcal{O}_{[1]}} : \mathcal{O}_{[1]} \to k^* \times_{Z_2} k^*/k^{*3}$ separates $\mathrm{Sl}(2,k)$-orbits.

To prove (ii) it remains to prove that $I_{\mathcal{O}_{[1]}} : \mathcal{O}_{[1]} \to k^* \times_{Z_2} k^*/k^{*3}$ is surjective. Let $[q, [\alpha]] \in k^* \times_{Z_2} k^*/k^{*3}$ and consider the binary cubic

$$P = \frac{1}{q\alpha}x^3 + q^2\alpha y^3.$$

Then

$$I_{\mathcal{O}_{[1]}}(P) = [q,\, [\frac{1}{q\alpha}]\,[q^2\alpha\,]^{-1}] = [q, [\frac{1}{q^3\alpha^2}]] = [q, [\alpha]].$$

and so $I_{\mathcal{O}_{[1]}} : \mathcal{O}_{[1]} \to k^* \times_{Z_2} k^*/{k^*}^3$ is surjective. This completes the proof of (ii).

To prove (iii), recall that the representation $P = \lambda_1\phi_1^3 + \lambda_2\phi_2^3$ is unique up to permutation. Then $g \cdot P = P$ leads to two cases:

- $g \cdot (\lambda_1\phi_1^3) = \lambda_1\phi_1^3$ and $g \cdot (\lambda_2\phi_2^3) = \lambda_2\phi_2^3$;
- $g \cdot (\lambda_1\phi_1^3) = \lambda_2\phi_2^3$ and $g \cdot (\lambda_2\phi_2^3) = \lambda_1\phi_1^3$.

In the first case, $g \cdot \phi_i = j_i\phi_i$ where $j_i^3 = 1$ and since $g \in \mathrm{Sl}(2,k)$, we must have $j_1j_2 = 1$. In the second case, there exist $r, s \in k^*$ such that $g \cdot \phi_1 = r\phi_2$, $g \cdot \phi_2 = s\phi_1$, $\lambda_1 r^3 = \lambda_2$, $\lambda_2 s^3 = \lambda_1$ and $rs = -1$. Hence $(rs)^3 = 1$ and $rs = -1$ which is impossible and this case does not occur. QED

Properties of orbit space

We will use the parametrisation

$$I_{\mathcal{O}_{[1]}} : \mathcal{O}_{[1]}/\mathrm{Sl}(2,k) \longleftrightarrow k^* \times_{Z_2} k^*/{k^*}^3.$$

to study orbit space. The parameter space has two natural maps

$$sq : k^* \times_{Z_2} k^*/{k^*}^3 \to {k^*}^2, \quad sq([q,\alpha]) = q^2, \tag{25}$$

and

$$t : k^* \times_{Z_2} k^*/{k^*}^3 \to (k^*/{k^*}^3)/Z_2, \quad t([q,\alpha]) = [\alpha] \tag{26}$$

corresponding to projection onto the orbit spaces of the two factors. We then have the following diagram:

$$\begin{array}{ccc} & k^* \times_{Z_2} k^*/{k^*}^3 & \\ {\scriptstyle e}\nearrow\ \swarrow{\scriptstyle sq} & & \searrow{\scriptstyle t} \\ {k^*}^2 & & (k^*/{k^*}^3)/Z_2. \end{array} \tag{27}$$

The map

$$sq : k^* \times_{Z_2} k^*/{k^*}^3 \to {k^*}^2 \tag{28}$$

is the fibration associated to the principal Z_2-fibration

$$k^* \to {k^*}^2$$

and the action of Z_2 on $k^*/{k^*}^3$ by inversion. Since Z_2 acts by automorphisms, the fibre $sq^{-1}(q^2)$ over any point $q^2 \in {k^*}^2$ has a natural group structure

$$[q,\alpha] \times [q,\beta] = [q,\alpha\beta] \tag{29}$$

independent of the choice of square root q of q^2. Taking the identity at each point, we get a canonical section $e : {k^*}^2 \to k^* \times_{Z_2} k^*/{k^*}^3$ of (28) given by

$$e(q^2) = [q, 1] \tag{30}$$

but, although each fibre is a group isomorphic to k^*/k^{*3}, the fibration (28) is not in general isomorphic to the product

$$k^{*2} \times k^*/k^{*3} \to k^{*2}.$$

To translate the above features of orbit space into more concrete statements about binary cubics over k, note that the map sq is essentially the quartic Q_n since for all $P \in \mathcal{O}_{[1]}$,

$$sq(I_{\mathcal{O}_{[1]}}(P)) = Q_n(P).$$

Theorem 3.34 *Let $M \in k^{*2}$, let*

$$\mathcal{O}_M = \{P \in S^3(k^{2^*}) : Q_n(P) = M\}$$

and let $\mathcal{O}_M/Sl(2,k)$ be the space of $Sl(2,k)$-orbits in $\mathcal{O}_M$.

(i) The map $I_{\mathcal{O}_{[1]}} : \mathcal{O}_{[1]} \to k^* \times_{Z_2} k^*/k^{*3}$ induces a bijection

$$\mathcal{O}_M/Sl(2,k) \longleftrightarrow sq^{-1}(M)$$

and, by pullback of (29)*, a group structure on $\mathcal{O}_M/Sl(2,k)$.*

(ii) As groups, $\mathcal{O}_M/Sl(2,k) \cong k^*/k^{*3}$.

(iii) Let $q \in k^*$ be a square root of M. The identity element of $\mathcal{O}_M/Sl(2,k)$ is characterised by:

$$Sl(2,k) \cdot P = 1 \Leftrightarrow P \text{ is reducible over } k \Leftrightarrow I_{\mathcal{O}_{[1]}}(P) = [q, 1].$$

Proof. Parts (i) and (ii) follow from the discussion above. Part (iii) follows from Theorem 3.36(i) and equation (30). QED

Remark 3.35 *From the Corollary it follows that if the classical discriminant is a nonzero square there is a unique $Sl(2,k)$ orbit consisting of reducible polynomials. We remove the 'square' restriction in Corollary 3.47. In particular, over an algebraically closed field there is only one orbit of fixed nonzero discriminant.*

To finish this section we briefly discuss the map $t : k^* \times_{Z_2} k^*/k^{*3} \to (k^*/k^{*3})/Z_2$ in diagram (27) given by

$$t([q, \alpha]) = [\alpha].$$

This a fibration with fibre k^* outside the identity coset $[1]$ but

$$t^{-1}([1]) = e(k^{*2})$$

is a 'singular fibre'. There is a k^*-action:

$$\lambda \cdot [q, \alpha] = [\lambda q, \alpha] \tag{31}$$

which maps fibres of sq to fibres of sq:

$$sq([q', \alpha']) = sq([q, \alpha]) \Rightarrow sq(\lambda \cdot [q', \alpha']) = sq(\lambda \cdot [q, \alpha]),$$

and whose orbits are exactly the fibres of t:

$$t([q', \alpha']) = t([q, \alpha]) \Leftrightarrow \exists \lambda \in k^* \text{ s.t. } [q', \alpha'] = \lambda \cdot [q, \alpha].$$

Isotropy for this action is given by: $Isot_{k^*}([q, \alpha]) = \begin{cases} 1 & \text{if } \alpha \neq 1 \\ \{\pm 1\} & \text{if } \alpha = 1. \end{cases}$

It would be interesting to interpret these features of orbit space in terms of the original binary cubics. Conversely, one can also identify actions on the orbits in terms of their orbit parameters. For example, the commutant of $\mathrm{Sl}(2, k)$ in $\mathrm{Gl}(\mathrm{S}^3(k^{2^*}))$ acts on orbit space. This gives the action

$$\lambda \cdot' [q, \alpha] = [\lambda^2 q, \alpha]$$

of k^* on $k^* \times_{Z_2} k^*/k^{*3}$ which is the square of the action (31). Another example is obtained from $\Psi : \mathrm{S}^3(k^{2^*}) \to \mathrm{S}^3(k^{2^*})$ which, since it commutes with the action of $\mathrm{Sl}(2, k)$, induces a map from $k^* \times_{Z_2} k^*/k^{*3}$ to itself. This is easily seen to be given by

$$[q, \alpha] \mapsto [-q^3, [q]\alpha], \tag{32}$$

where $[q]$ denotes the class of q in k^*/k^{*3}.

Reducibility and factorisation

Theorem 3.36 *Let $P \in S$ and let $\{\phi_1, \phi_2\}$ be a basis of k^{2^*} such that $P = \lambda_1 \phi_1^3 + \lambda_2 \phi_2^3$ with $\lambda_1, \lambda_2 \in k^*$. Let $q \in k^*$ be a square root of $Q_n(P)$. The following are equivalent:*

(a) P is reducible over k.

(b) $\frac{\lambda_1}{\lambda_2}$ is a cube in k^*.

(c) $q\lambda_1$ is a cube in k^*.

(d) $q\lambda_2$ is a cube in k^*.

(e) There is a basis $\{\phi_1', \phi_2'\}$ of k^{2^*} such that $P = \frac{1}{q}(\phi'^3_1 + \phi'^3_2)$.

Proof. $(a) \Rightarrow (b)$: Suppose P is reducible over k. Then for all $g \in \mathrm{Sl}(2, k)$,

$$g \cdot P = \lambda_1 (g \cdot \phi_1)^3 + \lambda_2 (g \cdot \phi_2)^3$$

is also reducible over k. Since ϕ_1, ϕ_2 form a basis of k^{2^*}, we can choose g such that $g \cdot \phi_1 = x$ and $g \cdot \phi_2 = \rho y$ for some $\rho \in k^*$ so that

$$\lambda_1 x^3 + \lambda_2 \rho^3 y^3$$

is reducible over k. Hence there exist $a, b, c, d, e \in k$ such that

$$\lambda_1 x^3 + \lambda_2 \rho^3 y^3 = (ax + by)(cx^2 + dxy + ey^2)$$

which gives the system

$$\lambda_1 = ac,\ 0 = ad + bc,$$
$$\lambda_2 \rho^3 = be,\ 0 = ae + bd.$$

Since λ_1 and λ_2 are nonzero, it follows that a, b, c, d, e are nonzero and, since $c = -\frac{ad}{b}$ and $e = -\frac{bd}{a}$ we get $\frac{\lambda_1}{\lambda_2} = (\rho \frac{a}{b})^3$.
$(b) \Rightarrow (a)$: Suppose $\frac{\lambda_1}{\lambda_2} = r^3$ with $r \in k^*$. Then

$$P = \lambda_2(r^3\phi_1^3 + \phi_2^3) = \lambda_2(r\phi_1 + \phi_2)(r^2\phi_1^2 + r\phi_1\phi_2 + \phi_2^2) \tag{33}$$

and P is reducible over k.
$(b) \Leftrightarrow (c) \Leftrightarrow (d)$: Set $\nu_1 = q\lambda_1$ and $\nu_2 = q\lambda_2$. By Proposition **??**, there exists $s \in k^*$ such that $\nu_1\nu_2 = s^3$. Hence if any one of the three numbers $\nu_1, \nu_2, \frac{\nu_1}{\nu_2} = \frac{\lambda_1}{\lambda_2}$ is a cube so are the other two since formally

$$\nu_1 = \left(\frac{\nu_1}{\sqrt[3]{\frac{\nu_1}{\nu_2}}\sqrt[3]{\nu_1\nu_2}} \right)^3, \quad \nu_2 = \left(\sqrt[3]{\frac{\nu_1}{\nu_2}} \frac{\nu_2}{\sqrt[3]{\nu_1\nu_2}} \right)^3, \quad \nu_2 = \left(\frac{\sqrt[3]{\nu_1\nu_2}}{\sqrt[3]{\nu_1}} \right)^3.$$

$(a) \Rightarrow (e)$: If P is reducible we have just proved that there exists $r \in k^*$ and $s \in k^*$such that $\lambda_1 = \frac{1}{q}r^3$ and $\lambda_2 = \frac{1}{q}s^3$. Set $\phi_1' = r\phi_1$ and $\phi_2' = s\phi_2$. Then

$$P = \lambda_1\phi_1^3 + \lambda_2\phi_2^3 = \frac{1}{q}\left({\phi_1'}^3 + {\phi_2'}^3 \right)$$

which proves (e).
$(e) \Rightarrow (a)$: Evident since ${\phi'}_1 + {\phi'}_2$ divides ${\phi'}_1^3 + {\phi'}_2^3$. QED

Corollary 3.37 *Let $P \in S$ be reducible and let $\{\phi_1', \phi_2'\}$ be a basis of k^{2^*} such that $P = \frac{1}{q}({\phi'}_1^3 + {\phi'}_2^3)$.*

(a) If -3 is not a square in k, then

$$P = \frac{1}{q}(\phi_1' + \phi_2')({\phi_1'}^2 - \phi_1'\phi_2' + {\phi_2'}^2)$$

and ${\phi_1'}^2 - \phi_1'\phi_2' + {\phi_2'}^2$ is irreducible over k.

(b) If -3 is a square in k, then

$$P = \frac{1}{q}(\phi_1' + \phi_2')(j\phi_1' + j^{-1}\phi_2')(j^2\phi_1' + j^{-2}\phi_2') \tag{34}$$

where $j = \frac{1}{2}(-1 + \sqrt{-3})$. The factors of P are pairwise independent.

To a certain extent, we can normalise bases of k^{2^*} satisfying Theorem 3.27(e).

Corollary 3.38 *Let $P \in S$.*

(a) P is reducible iff there is a basis $\{\phi'_1, \phi'_2\}$ of k^{2^*} such that $P = \frac{1}{q}({\phi'}_1^3 + {\phi'}_2^3)$ and $\Omega({\phi'}_1, {\phi'}_2) = q$.

(b If $\{\phi'_1, \phi'_2\}$ and $\{\phi''_1, \phi''_2\}$ are two bases of k^{2^*} satisfying (a), there exists a cube root of unity $j \in k^*$ such that $\phi''_1 = j\phi'_1$ and $\phi''_2 = j^{-1}\phi'_2$.

Proof. Choose a basis $\{\phi_1, \phi_2\}$ of k^{2^*} and $\lambda_1, \lambda_2 \in k^*$ such that $P = \lambda_1\phi_1^3 + \lambda_2\phi_2^3$ and let $q = \lambda_1\lambda_2\Omega(\phi_1, \phi_2)^3$. If P is reducible, by Theorem 3.27, there exists $r \in k^*$ such that $\lambda_1 = \frac{1}{q}r^3$. Set $s = \frac{q}{r\Omega(\phi_1,\phi_2)}$, $\phi'_1 = r\phi_1$ and $\phi'_2 = s\phi_2$. Then $\Omega({\phi'}_1, {\phi'}_2) = q$ and

$$s^3 = \left(\frac{q}{r\Omega(\phi_1,\phi_2)}\right)^3 = \frac{1}{r^3}\left(\frac{q}{\Omega(\phi_1,\phi_2)}\right)^3 = \frac{1}{q\lambda_1}\left(q\lambda_1\right)\left(q\lambda_2\right) = q\lambda_2.$$

Hence

$$P = \lambda_1\phi_1^3 + \lambda_2\phi_2^3 = \frac{1}{q}\left({\phi'_1}^3 + {\phi'_2}^3\right).$$

In the classical literature on cubics this is called the Viète Substitution.

Conversely, if there is a basis $\{\phi'_1, \phi'_2\}$ of k^{2^*} such that $P = \frac{1}{q}({\phi'}_1^3 + {\phi'}_2^3)$, then $\phi'_1 + \phi'_2$ divides P and P is reducible.

To prove (b), note first that by Theorem 3.27(a), we have either ${\phi''_1}^3 = {\phi'_1}^3$ and ${\phi''_2}^3 = {\phi'}_2^3$ or ${\phi''_1}^3 = {\phi'_2}^3$ and ${\phi''_2}^3 = {\phi'}_1^3$.

In the first case, by unique factorisation, there exist cube roots of unity j_1, j_2 such that $\phi''_1 = j_1\phi'_1$, $\phi''_2 = j_2\phi'_2$ and $j_1j_2 = 1$. This is exactly what we want to prove.

In the second case, there exist cube roots of unity j_1, j_2 such that $\phi''_1 = j_1\phi'_2$, $\phi''_2 = j_2\phi'_1$ and $j_1j_2 = -1$. This is impossible since $(j_1j_2)^3 = 1$. QED

Explicit formulae for $I_{\mathcal{O}_{[1]}}$ and Cardano-Tartaglia formulae

Proposition 3.39 *Let $P = ax^3 + 3bx^2y + 3cxy^2 + dy^3$ be an element of $\mathcal{O}_{[1]}$, let $q \in k^*$ be a square root of $Q_n(P)$ and define α, β, γ and δ in k by*

$$\mu(P) = \begin{pmatrix} (ad-bc) & 2(bd-c^2) \\ 2(b^2-ac) & -(ad-bc) \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

Then $P = \lambda_1\phi_1^3 + \lambda_2\phi_2^3$ and $I_{\mathcal{O}_{[1]}}(P) = [\, q\,, [\lambda_1][\lambda_2]^{-1}\,]$ where:

(i) If $\beta = \gamma = 0$,

$$\begin{array}{l} \lambda_1 = a,\ \phi_1 = x, \\ \lambda_2 = d,\ \phi_2 = y, \end{array} \quad ad = q.$$

(ii) If $\gamma \neq 0$,

$$\begin{array}{ll} \lambda_1 = \frac{1}{2q}(\alpha+q)a + \frac{\gamma}{2q}b, & \phi_1 = x - (\frac{\alpha-q}{\gamma})y, \\ \lambda_2 = -\frac{1}{2q}(\alpha-q)a - \frac{\gamma}{2q}b, & \phi_2 = x - (\frac{\alpha+q}{\gamma})y, \end{array} \quad \Omega(\phi_1, \phi_2) = -\frac{2q}{\gamma}.$$

(iii) If $\beta \neq 0$,

$$\begin{array}{l} \lambda_1 = \frac{\beta}{2q}c - \frac{1}{2q}(\alpha - q)d, \quad \phi_1 = (\frac{\alpha+q}{\beta})x + y, \\ \lambda_2 = -\frac{\beta}{2q}c + \frac{1}{2q}(\alpha + q)d, \; \phi_2 = (\frac{\alpha-q}{\beta})x + y, \end{array} \quad \Omega(\phi_1, \phi_2) = \frac{2q}{\beta}.$$

If $P \in \mathcal{O}_{[1]}$ is reducible we can use these formulae together with Theorem 3.36 and Corollary 3.37 to get an explicit formula for a linear factor of P in terms of the coefficients of P, a square root q of $Q_n(P)$ and a cube root r of $q\lambda_1$. Recall that the existence of a cube root of $q\lambda_1$ in k is a necessary and sufficient condition for P to be reducible over k.

Proposition 3.40 *Let* $P = ax^3 + 3bx^2y + 3cxy^2 + dy^3 \in \mathcal{O}_{[1]}$ *be reducible, let* $q \in k^*$ *be a square root of* $Q_n(P)$ *and suppose* $ad \neq 0$.

(i) If $\beta = \gamma = 0$, *let* r *be a cube root of* qa *and let* $s = \frac{q}{r}$. *Then*

$$rx + sy$$

divides P.
(ii) If $\gamma \neq 0$, *let* r *be a cube root of* $(\alpha + q)a + \gamma b$ *and let* $s = -\frac{\gamma}{r}$. *Then*

$$x + \left(\frac{r - s + b}{a}\right) y$$

divides P.
(iii) If $\beta \neq 0$, *let* r *be a cube root of* $\beta c - (\alpha - q)d$ *and let* $s = \frac{\beta}{r}$. *Then*

$$\left(\frac{s - r + c}{d}\right) x + y$$

divides P.

Proof. Since P is reducible, there exists a basis ϕ'_1, ϕ'_2 of k^{2^*} such that $P = \frac{1}{q}(\phi'^3_1 + \phi'^3_2)$ (cf Theorem 3.36) and then $\phi'_1 + \phi'_2$ divides P. As shown in the proof of Corollary 3.38(a), we can take $\phi'_1 = r\phi_1$ and $\phi'_2 = s\phi_2$ where r is a cube root of $q\lambda_1$, $s = \frac{q}{r\Omega(\phi_1,\phi_2)}$ and $\phi_1, \phi_2, \lambda_1$ are given by Proposition 3.39. The explicit formulae in the three cases are:

(a) $\beta = \gamma = 0$: $\quad r$ is a cube root of qa, $rs = q$ and $\phi'_1 = rx$, $\phi'_2 = sy$;

(b) $\gamma \neq 0$: $\quad r$ is a cube root of $\frac{(\alpha+q)a+\gamma b}{2}$, $s = -\frac{\gamma}{2r}$ and

$$\phi'_1 = rx + \frac{1}{2s}(\alpha - q)y, \quad \phi'_2 = sx + \frac{1}{2r}(\alpha + q)y;$$

(c) $\beta \neq 0$: $\quad r$ is a cube root of $\frac{\beta c-(\alpha-q)d}{2}$, $s = \frac{\beta}{2r}$ and

$$\phi'_1 = \frac{1}{2s}(\alpha + q)x + ry, \quad \phi'_2 = \frac{1}{2r}(\alpha - q)x + sy.$$

Calculating ${\phi'}_1 + {\phi'}_2$ in the first case obviously gives (i). In the second case we have

$$\begin{aligned} {\phi'}_1 + {\phi'}_2 &= (r+s)x + \left(\frac{1}{2s}(\alpha - q) + \frac{1}{2r}(\alpha + q)\right) y \\ &= (r+s)x + \left(\frac{1}{2sa}(-2s^3 - \gamma b) + \frac{1}{2ra}(2r^3 - \gamma b)\right) y \end{aligned} \qquad (35)$$

since $r^3 = q\lambda_1 = \frac{(\alpha+q)a+\gamma b}{2}$ and $s^3 = q\lambda_2 = \frac{-(\alpha-q)a-\gamma b}{2}$. Simplifying the coefficient of y we get

$$\frac{1}{2sa}(-2s^3-\gamma b)+\frac{1}{2ra}(2r^3-\gamma b) = \frac{1}{a}\left(r^2 - s^2 - \frac{b\gamma}{2}(\frac{1}{r} + \frac{1}{s})\right) = (r+s)\frac{r-s+b}{a}$$

since $2rs = -\gamma$, and this implies (ii). Similarly, (iii) follows from (c). QED

As an application of the above results, consider the homogeneous Cardano-Tartaglia polynomial

$$P = x^3 + pxy^2 + qy^3$$

over a field k of characteristic not 2 or 3. Assume $p \neq 0$ and $q \neq 0$ so that factorising P is a nontrivial problem. Then

$$\mu(P) = \begin{pmatrix} q & -2\frac{p^2}{9} \\ -2\frac{p}{3} & -q \end{pmatrix}, \quad Q_n(P) = (q^2 + 4\frac{p^3}{27}).$$

To be able to apply our approach we assume $Q_n(P)$ has a square root in k^* which we denote $\sqrt{q^2 + 4\frac{p^3}{27}}$. Then by Theorem 3.36 and Proposition 3.39(ii), P is reducible iff

$$\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \quad \text{or} \quad -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

has a cube root in k.

If this is the case, then Proposition 3.40 (ii) implies that $x + (r-s)y$ divides P where r is a cube root of $\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ and s is the cube root $\frac{p}{3r}$ of $-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$. Hence, with the obvious notation,

$$\frac{p}{3\left(\sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\right)} - \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

is a root of the inhomogeneous cubic $x^3 + px^2 + q$ and this is the classical Cardano-Tartaglia formula. If $k = \mathbb{R}$, this can be written

$$s - r = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} - \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

since cube roots are unique.

3.4 Symplectic covariants and sums of coprime cubes in quadratic extensions

In this article we have until now considered only binary cubics P such that $Q_n(P)$ is a square in k. In this section we will study binary cubics P such that $Q_n(P)$ is a square in a fixed quadratic extension of k.

Let $\hat{k}$ be a quadratic extension of k. Recall that since $\mathrm{char}(k) \neq 2$, the extension $\hat{k}/k$ is Galois and the Galois group $\mathrm{Gal}(\hat{k}/k)$ is isomorphic to Z_2. The Galois group $\mathrm{Gal}(\hat{k}/k)$ acts naturally on any space over $\hat{k}$ obtained by base extension of a space over k and its fixed point set is the original space over k. We always denote the action of the generator of $\mathrm{Gal}(\hat{k}/k)$ by $x \mapsto \bar{x}$ and we denote by $\hat{\Omega}$ and $\hat{\omega}$ respectively the symplectic forms on $\hat{k}^{2*}$ and $S^3(\hat{k}^{2*})$ obtained by base extension of Ω and ω. The quartic on $S^3(\hat{k}^{2*})$ obtained by base extension of Q_n will be denoted $\widehat{Q_n}$ and we set

$$\widehat{\mathcal{O}}_{[1]} = \{P \in S^3(\hat{k}^{2*}) : \widehat{Q_n}(P) \in \hat{k}^{*2}\}.$$

Finally, let $\mathrm{Im}\,\hat{k} = \{\lambda \in \hat{k} : \bar{\lambda} = -\lambda\}$ and let $\widehat{T} \subseteq S^3(\hat{k}^{2*})$ be the set of nonzero binary cubics over $\hat{k}$ which have a triple root over $\hat{k}$.

Remark 3.41 *Note that $(\mathrm{Im}\,\hat{k}^*)^2 \subseteq k^*$ is the inverse image under $k^* \to k^{*2}$ of a single nontrivial square class in k^*/k^{*2}. Conversely, a nontrivial square class in k^*/k^{*2} determines up to isomorphism a quadratic extension of k with this property.*

This notation out of the way, we make a symplectic definition

$$\mathcal{O}(\hat{k}) = \{P \in S^3(k^{2*}) : \hat{k} \text{ is a splitting field of } x^2 - Q_n(P)\}$$

and an algebraic definition

$$S(\hat{k}) = \{P \in S^3(k^{2*}) : \exists T \in \widehat{T} \text{ s.t. } P = T + \bar{T} \text{ with } T, \bar{T} \text{ coprime}\}.$$

Proposition 3.42 $\mathcal{O}(\hat{k}) = S(\hat{k})$.

Proof. Let $P \in \mathcal{O}(\hat{k})$. Then $Q_n(P)$ has two square roots in $\hat{k}$ but no square roots in k since $\hat{k}$ is a splitting field of $x^2 - Q_n(P)$. By Theorem 3.27, there exists $T_1, T_2 \in \widehat{T}$ such that $P = T_1 + T_2$ and the square roots of $Q_n(P)$ are $\pm\hat{\omega}(T_1, T_2)$. Since $\bar{P} = P$ and since T_1 and T_2 are unique up to permutation, we have either $\bar{T}_1 = T_1$ and $\bar{T}_2 = T_2$ or $\bar{T}_1 = T_2$ and $\bar{T}_2 = T_1$. In the first case,

$$\overline{\hat{\omega}(T_1, T_2)} = \hat{\omega}(\bar{T}_1, \bar{T}_2) = \hat{\omega}(T_1, T_2),$$

so $\hat{\omega}(T_1, T_2) \in k$ and $Q_n(P)$ has a square root in k which is a contradiction. Hence $P = T_1 + \bar{T}_1$. To prove that T_1 and $\bar{T}_1$ are coprime, write $T_1 = \lambda\alpha^3$ where $\lambda \in \hat{k}$ and $\alpha \in \hat{k}^{2*}$. Then, by unique factorisation, T_1 and $\bar{T}_1$ are not coprime iff α and $\overline{\alpha}$ are proportional. But then $\hat{\omega}(T_1, \bar{T}_1) = 0$ and $Q_n(P) = 0$ has a square root in k. Hence T_1 and $\bar{T}_1$ are coprime and $P \in S(\hat{k})$.

To prove inclusion in the opposite direction, suppose $P \in S(\hat{k})$ and let $P = T + \bar{T}$ with $T, \bar{T}$ coprime and $T \in \widehat{T}$. Note that $P \neq 0$ since otherwise T and $\bar{T}$ would not be coprime. By Theorem 3.27, we have $Q_n(P) = (\hat{\omega}(T, \bar{T}))^2$ and $Q_n(P)$ has two square roots $\hat{\omega}(T, \bar{T})$ in $\hat{k}$. Let $T = \lambda\alpha^3$ where $\lambda \in \hat{k}^*$ and $\alpha \in \hat{k}^{2*}$. As we saw above, T and $\bar{T}$ are coprime implies α and $\overline{\alpha}$ are not proportional, and this is equivalent to $\hat{\Omega}(\alpha, \overline{\alpha}) \neq 0$ since $\dim \hat{k}^{2*} = 2$. From

$$\hat{\omega}(T, \bar{T}) = \lambda\bar{\lambda}(\hat{\Omega}(\alpha, \overline{\alpha}))^3$$

it follows that $\hat{\omega}(T, \bar{T}) \neq 0$. On the other hand,

$$\overline{\hat{\omega}(T, \bar{T})} = \hat{\omega}(\bar{T}, T) = -\hat{\omega}(T, \bar{T})$$

and $\hat{\omega}(T, \bar{T})$ is pure imaginary. Hence the square roots $\pm\hat{\omega}(T, \bar{T})$ of $Q_n(P)$are not in k and $\hat{k}$ is a splitting field of $x^2 - Q_n(P)$. QED

Proposition 3.43 *(Fibres of μ on $\mathcal{O}(\hat{k})$). Let $X \in \mathfrak{sl}(2, k)$ be such that $-\det X \in (\operatorname{Im} \hat{k}^*)^2$ and $\nu_{\det X}(X) = [2]$. Let $q, \bar{q} \in \operatorname{Im} \hat{k}^*$ be its eigenvalues and let ϕ and $\bar{\phi}$ be corresponding eigenvectors in $\hat{k}^{2*}$.*

(i) There exists $a \in \hat{k}^*$ such that $a\bar{a}\,\Omega(\bar{\phi}, \phi)^3 = q$.

(ii)

$$\mu^{-1}(X) = \{ua\phi^3 + \bar{u}\bar{a}\,\bar{\phi}^3 : u \in \hat{k}^* \text{ and } u\bar{u} = 1\}.$$

Proof. Recall that $\nu_{\det X}(X) = [2]$ is a necessary and sufficient condition for X to be in the image of μ (cf Theorem 2.11). Since $\phi + \bar{\phi}$ is not an eigenvector of X, we have

$$[2] = [\Omega(\phi + \bar{\phi}, X \cdot \phi + X \cdot \bar{\phi})] = [-2q\Omega(\phi, \bar{\phi})].$$

Hence there exists $\alpha \in \hat{k}^*$ such that $\alpha\bar{\alpha} = q\Omega(\bar{\phi}, \phi)$ and then $a = \frac{q^2}{\alpha^3}$ is a solution of (i).

By Corollary 3.31, the fibre of the $\hat{k}$-moment map $\hat{\mu} : S^3(\hat{k}^{2*}) \to \mathrm{sl}(2, \hat{k})$ is

$$\hat{\mu}^{-1}(X) = \{c\bar{\phi}^3 + \frac{q}{c\Omega(\bar{\phi}, \phi)^3}\,\phi^3 : c \in \hat{k}^*\}$$

and hence

$$\mu^{-1}(X) = \{c\bar{\phi}^3 + \frac{q}{c\Omega(\bar{\phi}, \phi)^3}\,\phi^3 : c \in \hat{k}^*,\ \bar{c} = \frac{q}{c\Omega(\bar{\phi}, \phi)^3}\}.$$

This together with (i) implies (ii). QED

Orbit parameters for $\mathcal{O}(\hat{k})$

It is clear that $\mathcal{O}(\hat{k})$ is stable under the action of $\mathrm{Sl}(2, k)$ and in this section we will give a parametrisation of the space of orbits.

Let $P \in \mathcal{O}(\hat{k})$. Then, since $Q_n(P) \in \hat{k}^{*2}$, the $\mathrm{Sl}(2,\hat{k})$ orbit of P regarded as a binary cubic over $\hat{k}$ is entirely determined by $I_{\widehat{\mathcal{O}}_{[1]}}(P)$ where

$$I_{\widehat{\mathcal{O}}_{[1]}} : \widehat{\mathcal{O}}_{[1]} \to \hat{k}^* \times_{Z_2} \hat{k}^* / \hat{k}^{*3}$$

is the $\mathrm{Sl}(2,\hat{k})$-invariant function defined in Theorem 3.33. Recall that to calculate $I_{\widehat{\mathcal{O}}_{[1]}}(P)$, we choose $\lambda \in \hat{k}^*$ and $\alpha \in \hat{k}^{2*}$ such that

$$P = \lambda\alpha^3 + \bar{\lambda}\bar{\alpha}^3$$

and then by definition,

$$I_{\widehat{\mathcal{O}}_{[1]}}(P) = [\hat{\omega}(\lambda\alpha^3, \overline{\lambda}\overline{\alpha}), [\lambda\bar{\lambda}^{-1}]]. \tag{36}$$

The square roots $\pm\hat{\omega}(\lambda\alpha^3, \overline{\lambda}\overline{\alpha}^3)$ of $Q_n(P)$ are pure imaginary since

$$\overline{\hat{\omega}(\lambda\alpha^3, \overline{\lambda_1}\overline{\alpha}^3)} = \hat{\omega}(\overline{\lambda}\overline{\alpha}^3, \lambda\alpha^3) = -\hat{\omega}(\lambda\alpha^3, \overline{\lambda_1}\overline{\alpha}^3),$$

and the class $[\lambda\bar{\lambda}^{-1}]$ of $\lambda\bar{\lambda}^{-1}$ in the group $\hat{k}^*/\hat{k}^{*3}$ satisfies

$$[\lambda\bar{\lambda}^{-1}]\,\overline{[\lambda\bar{\lambda}^{-1}]} = 1.$$

It follows that

$$I_{\widehat{\mathcal{O}}_{[1]}}(P) \in \mathrm{Im}\,\hat{k}^* \times_{Z_2} U(\hat{k}^*/\hat{k}^{*3})$$

where

$$U(\hat{k}^*/\hat{k}^{*3}) = \{\alpha \in \hat{k}^*/\hat{k}^{*3} \text{ s.t. } \alpha\bar{\alpha} = 1\}.$$

is the 'unitary' group of $\hat{k}^*/\hat{k}^{*3}$. Note that the Z_2 action on $\mathrm{Im}\,\hat{k}^* \times U(\hat{k}^*/\hat{k}^{*3})$ is precisely the natural action of $\mathrm{Gal}(\hat{k}/k)$.

Theorem 3.44 *Let $I_{\widehat{\mathcal{O}}_{[1]}} : \mathcal{O}(\hat{k}) \to \mathrm{Im}\,\hat{k}^* \times_{Z_2} U(\hat{k}^*/\hat{k}^{*3})$ be defined by* (36) *above.*

(i) Let $P, P' \in \mathcal{O}(\hat{k})$. Then

$$Sl(2,k)\cdot P' = Sl(2,k)\cdot P \iff I_{\widehat{\mathcal{O}}_{[1]}}(P') = I_{\widehat{\mathcal{O}}_{[1]}}(P).$$

(ii) The map $I_{\widehat{\mathcal{O}}_{[1]}}$ induces a bijection

$$\mathcal{O}(\hat{k})/Sl(2,k) \longleftrightarrow \mathrm{Im}\,\hat{k}^* \times_{Z_2} U(\hat{k}^*/\hat{k}^{*3}).$$

(iii) The isotropy group of $P \in \mathcal{O}(\hat{k})$ is isomorphic to

$$\{\begin{pmatrix}\lambda & 0\\ 0 & \bar{\lambda}\end{pmatrix} \in Sl(2,\hat{k}) :\ \lambda^3 = 1,\ \lambda\bar{\lambda} = 1\}.$$

Proof. (i): The function $I_{\widehat{\mathcal{O}}_{[1]}} : \mathcal{O}(\hat{k}) \to \operatorname{Im} \hat{k}^* \times_{Z_2} U(\hat{k}^* / \hat{k}^{*3})$ is $\mathrm{Sl}(2,k)$-invariant since it is by definition the restriction of an $\mathrm{Sl}(2,\hat{k})$-invariant function on a larger space.

To prove $I_{\widehat{\mathcal{O}}_{[1]}}$ separates orbits, suppose $I_{\widehat{\mathcal{O}}_{[1]}}(P') = I_{\widehat{\mathcal{O}}_{[1]}}(P)$. Writing $P = \lambda\alpha^3 + \bar{\lambda}\overline{\alpha}^3$ and $P' = \lambda'\alpha'^3 + \bar{\lambda}'\overline{\alpha'}^3$, there exists $\sigma \in Z_2$ such that

$$(\,\hat{\omega}(\lambda'\alpha'^3,\, \bar{\lambda}'\overline{\alpha'}^3),\, [\lambda'\bar{\lambda}'^{-1}]\,) = \sigma \cdot (\,\hat{\omega}(\lambda\alpha^3,\, \bar{\lambda}\overline{\alpha}^3),\, [\lambda\bar{\lambda}^{-1}]\,) \tag{37}$$

and, permuting cube terms if necessary, we can suppose without loss of generality that σ is the identity. Then, equation (37) implies

$$\hat{\omega}(\lambda'\alpha'^3,\, \bar{\lambda}'\overline{\alpha'}^3) = \hat{\omega}(\lambda\alpha^3,\, \bar{\lambda}\overline{\alpha}^3), \quad [\lambda'\bar{\lambda}'^{-1}] = [\lambda\bar{\lambda}^{-1}] \tag{38}$$

or equivalently,

$$\lambda'\bar{\lambda}'\hat{\omega}(\alpha'^3,\, \overline{\alpha'}^3) = \lambda\bar{\lambda}\hat{\omega}(\alpha^3,\, \overline{\alpha}^3), \quad [\lambda'\bar{\lambda}'^{-1}] = [\lambda\bar{\lambda}^{-1}]$$

which by (2) is equivalent to

$$\lambda'\bar{\lambda}'\,\widehat{\Omega}(\alpha',\, \overline{\alpha'})^3 = \lambda\bar{\lambda}\,\widehat{\Omega}(\alpha,\, \overline{\alpha})^3, \quad [\lambda'\bar{\lambda}'^{-1}] = [\lambda\bar{\lambda}^{-1}]. \tag{39}$$

Taking classes in $\hat{k}^* / \hat{k}^{*3}$ we get

$$[\lambda'\bar{\lambda}'] = [\lambda\bar{\lambda}], \quad [\lambda'\bar{\lambda}'^{-1}] = [\lambda\bar{\lambda}^{-1}]$$

and multiplying the two equations gives

$$[\lambda'^2] = [\lambda^2].$$

From this it follows that $[\lambda'] = [\lambda]$ since the cube of any element in $\hat{k}^* / \hat{k}^{*3}$ is the identity.

Let now $\xi \in \hat{k}^*$ be such that

$$\lambda' = \xi^3\lambda.$$

Substituting in the first equation of (39) we get

$$\widehat{\Omega}(\xi\alpha',\, \overline{\xi\alpha'})^3 = \widehat{\Omega}(\alpha,\, \overline{\alpha})^3$$

which means

$$\widehat{\Omega}(\xi\alpha',\, \overline{\xi\alpha'}) = j\,\widehat{\Omega}(\alpha,\, \overline{\alpha})$$

for some $j \in \hat{k}$ such that $j^3 = 1$. The conjugate of this equation is

$$-\widehat{\Omega}(\xi\alpha',\, \overline{\xi\alpha'}) = -\bar{j}\,\widehat{\Omega}(\alpha,\, \overline{\alpha})$$

and hence $\bar{j} = j$.

Define $g \in \mathrm{Gl}(2,\hat{k})$ by

$$g \cdot \alpha = j\xi\alpha', \quad g \cdot \overline{\alpha} = j\bar{\xi}\,\overline{\alpha'}.$$

Then g commutes with conjugation by definition, and preserves $\widehat{\Omega}$ since

$$\widehat{\Omega}(g \cdot \alpha, g \cdot \overline{\alpha}) = j^2\widehat{\Omega}(\xi\alpha', \overline{\xi\alpha'}) = j^3\widehat{\Omega}(\alpha, \overline{\alpha}) = \widehat{\Omega}(\alpha, \overline{\alpha}).$$

Hence $g \in \mathrm{Sl}(2,k)$. Furthermore,

$$g \cdot P = \lambda(g \cdot \alpha)^3 + \bar{\lambda}(\overline{g \cdot \alpha})^3 = \lambda(j\xi\alpha')^3 + \bar{\lambda}(j\bar{\xi}\,\overline{\alpha'})^3 = \lambda'\alpha'^3 + \bar{\lambda'}\overline{\alpha'}^3 = P'$$

which shows that P and P' are in the same $\mathrm{Sl}(2,k)$-orbit. This proves (i).

To prove (ii), we only have to show that $I_{\widehat{\mathcal{O}}_{[1]}}$ is surjective since by (i), the function $I_{\widehat{\mathcal{O}}_{[1]}}$ induces an injection $\mathcal{O}(\hat{k})/\mathrm{Sl}(2,k) \hookrightarrow \mathrm{Im}\,\hat{k}^* \times_{Z_2} U(\hat{k}^*/\,\hat{k}^{*3})$.

Let $(q,s) \in \mathrm{Im}\,\hat{k}^* \times U(\hat{k}^*/\,\hat{k}^{*3})$. First, pick $\lambda \in \hat{k}^*$ such that

$$[\lambda] = \bar{s}. \tag{40}$$

Since $[\lambda\bar{\lambda}] = s\bar{s} = 1$, we know $\lambda\bar{\lambda}$ is a cube in $\hat{k}^*$ but in fact, since $\hat{k}^*/k$ is a quadratic extension and $\lambda\bar{\lambda} \in k$, this implies that there exists $r \in k^*$ such that

$$\lambda\bar{\lambda} = r^3. \tag{41}$$

Now let

$$\alpha = -\frac{q}{2r}\hat{x} + \hat{y}$$

(where $\hat{x}, \hat{y} \in \hat{k}^{2*}$ are the base extensions of $x, y \in k^{2^*}$) and let

$$P = \frac{\lambda}{q}\alpha^3 - \frac{\bar{\lambda}}{q}\overline{\alpha}^3. \tag{42}$$

This is a binary cubic of the form $T + \bar{T}$ where $T \in \hat{T}$. We are now going to show that $P \in \mathcal{O}(\hat{k})$ and that $I_{\widehat{\mathcal{O}}_{[1]}}(P) = [q,s]$.

Note first that

$$\widehat{\Omega}(\alpha, \bar{\alpha}) = \widehat{\Omega}(-\frac{q}{2r}\hat{x} + \hat{y}, -\overline{(\frac{q}{2r})}\hat{x} + \hat{y} = -\frac{q}{2r} + \overline{(\frac{q}{2r})} = -\frac{q}{r},$$

so $\widehat{\Omega}(\alpha, \bar{\alpha}) \neq 0$ which means α and $\overline{\alpha}$ are not proportional. Hence α^3 and $\overline{\alpha}^3$ are coprime and $P \in \mathcal{O}(\hat{k})$.

Next, we have

$$\hat{\omega}(\alpha^3, \bar{\alpha}^3) = \widehat{\Omega}(\alpha, \bar{\alpha})^3 = -\frac{q^3}{r^3} \tag{43}$$

and

$$\hat{\omega}(\frac{\lambda}{q}\alpha^3, -\frac{\bar{\lambda}}{q}\overline{\alpha}^3) = -(\frac{1}{q})^2\lambda\bar{\lambda}\hat{\omega}(\alpha^3, \bar{\alpha}^3) = q \tag{44}$$

using equations (41) and (43). Finally, it follows from (40) that

$$\left[\frac{\lambda}{q}(\frac{\overline{\lambda}}{q})^{-1}\right] = \left[\lambda\bar{\lambda}^{-1}\right] = \bar{s}s^{-1} = s^{-1}s^{-1} = s^{-2} = s. \tag{45}$$

Hence, putting together equations (36), (42), (44) and (45), we get

$$I_{\widehat{\mathcal{O}}_{[1]}}(P) = [q, s]$$

and this proves that $I_{\widehat{\mathcal{O}}_{[1]}} : \mathcal{O}(\hat{k}) \to \operatorname{Im}\hat{k}^* \times_{Z_2} U(\hat{k}^*/\hat{k}^{*3})$ is surjective.

Part (iii) follows from Theorem 3.33 (iii).

QED

Corollary 3.45 *Let $P, P' \in \mathcal{O}(\hat{k})$. Then*

$$Sl(2,k)\cdot P' = Sl(2,k)\cdot P \iff Sl(2,\hat{k})\cdot P' = Sl(2,\hat{k})\cdot P.$$

Proof. Both properties are equivalent to $I_{\widehat{\mathcal{O}}_{[1]}}(P) = I_{\widehat{\mathcal{O}}_{[1]}}(P')$ by the above theorem and Theorem 3.33. QED

Properties of orbit space

The parameter space

$$\operatorname{Im}\hat{k}^* \times_{Z_2} U(\hat{k}^*/\hat{k}^{*3})$$

for $\mathrm{Sl}(2,k)$ orbits in $\mathcal{O}(\hat{k})$ is very analogous to the parameter space

$$\hat{k}^* \times_{Z_2} k^*/k^{*3}$$

for $\mathrm{Sl}(2,k)$ orbits in $\mathcal{O}_{[1]}$ that we gave in Theorem 3.33. Its main features can best be summarized in the diagram

$$\begin{array}{ccc} & \operatorname{Im}\hat{k}^* \times_{Z_2} U(\hat{k}^*/\hat{k}^{*3}) & \\ {\scriptstyle\hat{e}}\nearrow \quad \swarrow{\scriptstyle\widehat{sq}} & & \searrow{\scriptstyle\hat{t}} \\ (\operatorname{Im}\hat{k}^*)^2 & & U(\hat{k}^*/\hat{k}^{*3})/Z_2. \end{array} \tag{46}$$

The map

$$\widehat{sq} : \operatorname{Im}\hat{k}^* \times_{Z_2} U(\hat{k}^*/\hat{k}^{*3}) \to (\operatorname{Im}\hat{k}^*)^2 \tag{47}$$

given by

$$\widehat{sq}([q,\alpha]) = q^2$$

is the fibration associated to the principal Z_2-fibration

$$\operatorname{Im}\hat{k}^* \to (\operatorname{Im}\hat{k}^*)^2$$

and the action of Z_2 on $U(\hat{k}^*/\hat{k}^{*3})$ by conjugation. Since Z_2 acts by automorphisms, the fibre $\widehat{sq}^{-1}(q^2)$ over any point $q^2 \in (\operatorname{Im}\hat{k}^*)^2$ has a natural group structure

$$[q, u_1] \times [q, u_2] = [q, u_1 u_2] \tag{48}$$

independent of the choice of square root q of q^2. Taking the identity at each point, we get a canonical section $\hat{e} : (\operatorname{Im} \hat{k}^*)^2 \to \operatorname{Im} \hat{k}^* \times_{Z_2} U(\hat{k}^* / \hat{k}^{*3})$ of (47) given by

$$\hat{e}(q^2) = [q, 1] \tag{49}$$

but, although each fibre is a group isomorphic to $U(\hat{k}^* / \hat{k}^{*3})$, the fibration (47) is not in general isomorphic to the product

$$(\operatorname{Im} \hat{k}^*)^2 \times U(\hat{k}^* / \hat{k}^{*3}) \to (\operatorname{Im} \hat{k}^*)^2.$$

To translate the above features of orbit space into more concrete statements about binary cubics over k, note that the map $\widehat{sq}$ is essentially the quartic Q_n since for all $P \in \mathcal{O}(\hat{k})$,

$$\widehat{sq}(I_{\widehat{\mathcal{O}}_{[1]}}(P)) = Q_n(P).$$

Theorem 3.46 *Let $M \in (\operatorname{Im} \hat{k}^*)^2$, let*

$$\mathcal{O}_M = \{P \in S^3(k^{2^*}) : \, Q_n(P) = M\}$$

and let $\mathcal{O}_M / Sl(2, k)$ be the space of $Sl(2, k)$-orbits in $\mathcal{O}_M$.

(i) The map $I_{\widehat{\mathcal{O}}_{[1]}} : \mathcal{O}(\hat{k}) \to \operatorname{Im} \hat{k}^* \times_{Z_2} U(\hat{k}^* / \hat{k}^{*3})$ induces a bijection

$$\mathcal{O}_M / Sl(2, k) \longleftrightarrow \widehat{sq}^{-1}(M)$$

and, by pullback of (48)*, a group structure on $\mathcal{O}_M / Sl(2, k)$.*

(ii) As groups, $\mathcal{O}_M / Sl(2, k) \cong U(\hat{k}^* / \hat{k}^{*3})$.

(iii) The identity element of $\mathcal{O}_M / Sl(2, k)$ is characterised by:

$$Sl(2, k) \cdot P = 1 \Leftrightarrow P \text{ is reducible over } k.$$

Proof. Parts (i) and (ii) follow from the discussion above. To prove (iii), first note that P is reducible over k iff P is reducible over $\hat{k}$ since P is cubic and $\hat{k}/k$ is a quadratic extension. By Theorem 3.34(iii), P is reducible over $\hat{k}$ iff $I_{\widehat{\mathcal{O}}_{[1]}}(P) = [q, 1]$ where $q \in \hat{k}$ is a square root of M, and by equation (49), this is the identity element of $\mathcal{O}_M / \mathrm{Sl}(2, k)$. QED

Corollary 3.47 *Let $P, P' \in S^3(k^{2^*})$ be reducible binary cubics such that $Q_n(P) = Q_n(P')$ is nonzero. Then there exists $g \in Sl(2, k)$ such that $P' = g \cdot P$.*

Proof. Suppose $Q_n(P) = Q_n(P') = M$. If $M \in k^{*2}$, the result follows from Theorem 3.34(iii). If $M \in k^*$ is not a square, one can find a quadratic extension $\hat{k}$ of k such that $M \in (\operatorname{Im}\hat{k}^*)^2$. The result then follows from Theorem 3.46 (iii). QED

To finish this section we briefly discuss the map $\hat{t} : \operatorname{Im}\hat{k}^* \times_{Z_2} U(\hat{k}^*/\hat{k}^{*3}) \to U(\hat{k}^*/\hat{k}^{*3})/Z_2$ in diagram (46) given by

$$\hat{t}([q,\alpha]) = [\alpha].$$

This a fibration with fibre $\operatorname{Im}\hat{k}^*$ outside the identity coset $[1]$ but

$$\hat{t}^{-1}([1]) = \hat{e}(k^{*2})$$

is a 'singular fibre'. There is a k^*-action:

$$\lambda \cdot [q,\alpha] = [\lambda q, \alpha] \tag{50}$$

which maps fibres of $\widehat{sq}$ to fibres of $\widehat{sq}$:

$$\widehat{sq}([q',\alpha']) = \widehat{sq}([q,\alpha]) \Rightarrow \widehat{sq}(\lambda \cdot [q',\alpha']) = \widehat{sq}(\lambda \cdot [q,\alpha]),$$

and whose orbits are exactly the fibres of $\hat{t}$:

$$\hat{t}([q',\alpha']) = t([q,\alpha]) \Leftrightarrow \exists \lambda \in k^* \text{ s.t. } [q',\alpha'] = \lambda \cdot [q,\alpha].$$

Isotropy for this action is given by: $Isot_{k^*}([q,\alpha]) = \begin{cases} 1 & \text{if } \alpha \neq 1 \\ \{\pm 1\} & \text{if } \alpha = 1. \end{cases}$

It would be interesting to interpret these features of the orbit space in terms of the original binary cubics.

4 Parameter spaces for $\mathbf{Gl}(2,k)$-orbits

We have seen that the $\mathrm{Sl}(2,k)$-orbits in

$$\mathcal{O}_{[1]} = \{P \in S^3(k^{2^*}) : Q_n(P) \in k^{*2}\}$$

are parametrised by

$$k^* \times_{Z_2} k^*/k^{*3}$$

and that if $\hat{k}$ is a quadratic extension of k, the $\mathrm{Sl}(2,k)$-orbits in

$$\mathcal{O}(\hat{k}) = \{P \in S^3(k^{2^*}) : Q_n(P) \in (\operatorname{Im}\hat{k}^*)^2\}$$

are parametrised by

$$\operatorname{Im}\hat{k}^* \times_{Z_2} U(\hat{k}^*/\hat{k}^{*3}).$$

The group $GL(2,k)$ also acts on binary cubics and since

$$Q_n(g \cdot P) = (\det g)^{-6} Q_n(P) \quad \forall g \in \mathrm{Gl}(2,k), \forall P \in S^3(k^{2*}),$$

the spaces $\mathcal{O}_{[1]}$ and $\mathcal{O}(\hat{k})$ are stable under $\mathrm{Gl}(2,k)$.

In general, if $\mathrm{Gl}(2,k)$ acts on a space X there is a map

$$X/\mathrm{Sl}(2,k) \to X/\mathrm{Gl}(2,k)$$

from the set of $\mathrm{Sl}(2,k)$-orbits onto the set of $\mathrm{G}(2,k)$-orbits. The fibres of this map are the orbits of the k^*-action on $X/\mathrm{Sl}(2,k)$ given by

$$\lambda * [x] = [\Lambda \cdot x] \tag{51}$$

where Λ is any element of $\mathrm{Gl}(2,k)$ such that $\det \Lambda = \lambda$. Thus to get parameter spaces for $\mathcal{O}_{[1]}/\mathrm{Gl}(2,k)$ and $\mathcal{O}(\hat{k})/\mathrm{Gl}(2,k)$ we need just to calculate the k^*-actions on $k^* \times_{Z_2} k^*/k^{*3}$ and $\mathrm{Im}\,\hat{k}^* \times_{Z_2} U(\hat{k}^*/\hat{k}^{*3})$ corresponding to (51).

Lemma 4.1 *(i) Let k^* act on $k^* \times_{Z_2} k^*/k^{*3}$ by*

$$\lambda \cdot [\xi, \alpha] = [\lambda\xi, \alpha]$$

and let $I_{\mathcal{O}_{[1]}} : \mathcal{O}_{[1]} \to k^* \times_{Z_2} k^*/k^{*3}$ be defined by (23)*. Then*

$$I_{\mathcal{O}_{[1]}}(g \cdot P) = (\det g)^{-3} \cdot I_{\mathcal{O}_{[1]}}(P) \qquad \forall P \in \mathcal{O}_{[1]},\ \forall g \in Gl(2,k).$$

(ii) Let k^* act on $\mathrm{Im}\,\hat{k}^* \times_{Z_2} U(\hat{k}^*/\hat{k}^{*3})$ by

$$\lambda \cdot [\xi, \alpha] = [\lambda\xi, \alpha]$$

and let $I_{\widehat{\mathcal{O}}_{[1]}} : \mathcal{O}(\hat{k}) \to \mathrm{Im}\,\hat{k}^* \times_{Z_2} U(\hat{k}^*/\hat{k}^{*3})$ be defined by (36)*. Then*

$$I_{\widehat{\mathcal{O}}_{[1]}}(g \cdot P) = (\det g)^{-3} \cdot I_{\mathcal{O}_{[1]}}(P) \qquad \forall P \in \mathcal{O}(\hat{k}),\ \forall g \in Gl(2,k).$$

Proof. To prove (i), since for any $P \in \mathcal{O}_{[1]}$ there exists $h \in \mathrm{Gl}(2,k)$ and $a, b \in k^*$ such that

$$h \cdot P = ax^3 + by^3,$$

it is sufficient to prove that

$$I_{\mathcal{O}_{[1]}}(g \cdot (ax^3 + by^3)) = (\det g)^{-3} \cdot I_{\mathcal{O}_{[1]}}(ax^3 + by^3) \qquad \forall a, b \in k^*,\ \forall g \in \mathrm{Gl}(2,k).$$

Consider

$$g' = \begin{pmatrix} \det g & 0 \\ 0 & 1 \end{pmatrix}.$$

Then $\det g' = \det g$, $g' \cdot x = \frac{1}{\det g} x$ and $g' \cdot y = y$. Hence $g' g^{-1} \in \mathrm{Sl}(2,k)$,

$$I_{\mathcal{O}_{[1]}}(g \cdot (ax^3 + by^3)) = I_{\mathcal{O}_{[1]}}(g' \cdot (ax^3 + by^3))$$

and

$$I_{\mathcal{O}_{[1]}}(g' \cdot (ax^3 + by^3)) = I_{\mathcal{O}_{[1]}}(\frac{a}{(\det g)^3}x^3 + by^3)) = [\frac{ab}{(\det g)^3}, [ab^{-1}]].$$

The result follows since $I_{\mathcal{O}_{[1]}}(ax^3 + by^3) = [ab, [ab^{-1}]]$.

Part (ii) follows from (i) applied to $\hat{k}$. QED

Corollary 4.2 *(i) If $P \in \mathcal{O}_{[1]}$ and $\lambda \in k^*$ then*

$$I_{\mathcal{O}_{[1]}}(\lambda * [P]) = \frac{1}{\lambda^3} \cdot I_{\mathcal{O}_{[1]}}([P]).$$

(ii) If $P \in \mathcal{O}(\hat{k})$ and $\lambda \in k^*$ then

$$I_{\widehat{\mathcal{O}}_{[1]}}(\lambda * [P]) = \frac{1}{\lambda^3} \cdot I_{\widehat{\mathcal{O}}_{[1]}}([P]).$$

Proof. Immediate from the lemma. QED

From this we get the k^*-actions on the parameter spaces $k^* \times_{Z_2} k^*/k^{*3}$ and $\operatorname{Im}\hat{k}^* \times_{Z_2} U(\hat{k}^*/\hat{k}^{*3})$ corresponding to (51) : $\lambda \in k^*$ acts by multiplication by λ^{-3} on the first factor.

Hence, by the discussion above, the maps $I_{\mathcal{O}_{[1]}} : \mathcal{O}_{[1]} \to k^* \times_{Z_2} k^*/k^{*3}$ and $I_{\widehat{\mathcal{O}}_{[1]}} : \mathcal{O}(\hat{k}) \to \operatorname{Im}\hat{k}^* \times_{Z_2} U(\hat{k}^*/\hat{k}^{*3})$ induce bijections

$$\begin{aligned} \mathcal{O}_{[1]}/\mathrm{Gl}(2,k) &\longleftrightarrow (k^* \times_{Z_2} k^*/k^{*3})/k^{*3} &&= k^*/k^{*3} \times (k^*/k^{*3})/Z_2, \\ \mathcal{O}(\hat{k})/\mathrm{Gl}(2,k) &\longleftrightarrow (\operatorname{Im}\hat{k}^* \times_{Z_2} U(\hat{k}^*/\hat{k}^{*3}))/k^{*3} &&= (\operatorname{Im}\hat{k}^*)/k^{*3} \times U(\hat{k}^*/\hat{k}^{*3})/Z_2. \end{aligned}$$

To summarize, we have proved the

Theorem 4.3 *(a) Define $\pi : k^* \times_{Z_2} k^*/k^{*3} \to k^*/k^{*3} \times (k^*/k^{*3})/Z_2$ by $\pi([\xi,\alpha]) = ([\xi],[\alpha])$ and $J_{\mathcal{O}_{[1]}} : \mathcal{O}_{[1]} \to k^*/k^{*3} \times (k^*/k^{*3})/Z_2$ by $J_{\mathcal{O}_{[1]}} = \pi \circ I_{\mathcal{O}_{[1]}}$.*

(i) Let $P, P' \in \mathcal{O}_{[1]}$ Then

$$Gl(2,k) \cdot P = Gl(2,k) \cdot P' \quad \Leftrightarrow \quad J_{\mathcal{O}_{[1]}}(P) = J_{\mathcal{O}_{[1]}}(P').$$

(ii) The map $J_{\mathcal{O}_{[1]}}$ induces a bijection

$$\mathcal{O}_{[1]}/Gl(2,k) \longleftrightarrow k^*/k^{*3} \times (k^*/k^{*3})/Z_2.$$

(b) Define $\hat{\pi} : \operatorname{Im}\hat{k}^* \times_{Z_2} U(\hat{k}^*/\hat{k}^{*3}) \to (\operatorname{Im}\hat{k}^*)/k^{*3} \times U(\hat{k}^*/\hat{k}^{*3})/Z_2$ by $\hat{\pi}([\xi,\alpha]) = ([\xi],[\alpha])$ and $J_{\widehat{\mathcal{O}}_{[1]}} : \mathcal{O}(\hat{k}) \to k^*/k^{*3} \times (k^*/k^{*3})/Z_2$ by $J_{\widehat{\mathcal{O}}_{[1]}} = \hat{\pi} \circ I_{\widehat{\mathcal{O}}_{[1]}}$.

(i) Let $P, P' \in \mathcal{O}(\hat{k})$. Then

$$Gl(2,k) \cdot P = Gl(2,k) \cdot P' \quad \Leftrightarrow \quad J_{\widehat{\mathcal{O}}_{[1]}}(P) = J_{\widehat{\mathcal{O}}_{[1]}}(P').$$

(ii) The map $J_{\widehat{\mathcal{O}}_{[1]}}$ induces a bijection

$$\mathcal{O}(\hat{k})/Gl(2,k) \longleftrightarrow (\operatorname{Im}\hat{k}^*)/k^{*3} \times U(\hat{k}^*/\hat{k}^{*3})/Z_2.$$

Orbits spaces when k is a finite field of characteristic not 2 or 3

Let k be a finite field with q elements, not of characteristic 2 or 3. The following facts are well-known:

- $k^*/k^{*2} \cong Z_2$ so up to isomorphsm, there is only one quadratic extension of k and k^{*2} has $\frac{1}{2}(q-1)$ elements;
- if $q = 1 \bmod 3$, $k^*/k^{*3} \cong \mathbb{Z}/3\mathbb{Z}$;
- if $q = 2 \bmod 3$, $k^* = k^{*3}$;
- if $q = 1 \bmod 3$ and $\hat{k}/k$ is a quadratic extension, $U(\hat{k}^*/\hat{k}^{*3}) \cong 1$;
- if $q = 2 \bmod 3$ and $\hat{k}/k$ is a quadratic extension, $U(\hat{k}^*/\hat{k}^{*3}) \cong \mathbb{Z}/3\mathbb{Z}$.

These facts together with Theorem (3.33) and Theorem 4.3 immediately give the

Proposition 4.4 *Let k be a finite field with q elements, not of characteristic 2 or 3 and let $\hat{k}$ be a quadratic extension. Set*

$$\mathcal{O}_{[1]} = \{P \in S^3(k^{2^*}) : Q_n(P) \in k^{*2}\},$$
$$\mathcal{O}(\hat{k}) = \{P \in S^3(k^{2^*}) : Q_n(P) \in (\operatorname{Im} \hat{k}^*)^2\}.$$

(a) If $q = 1$ mod 3, $\mathcal{O}_{[1]}$ is the union of $\frac{3}{2}(q-1)$ Sl$(2,k)$-orbits and $\mathcal{O}(\hat{k})$ is the union of $\frac{1}{2}(q-1)$ Sl$(2,k)$-orbits.

(b) If $q = 1$ mod 3, $\mathcal{O}_{[1]}$ is the union of 6 Gl$(2,k)$-orbits and $\mathcal{O}(\hat{k})$ is the union of 3 Gl$(2,k)$-orbits.

(c) If $q = 2$ mod 3, $\mathcal{O}_{[1]}$ is the union of $\frac{1}{2}(q-1)$ Sl$(2,k)$-orbits and $\mathcal{O}(\hat{k})$ is the union of $\frac{3}{2}(q-1)$ Sl$(2,k)$-orbits.

(d) If $q = 2$ mod 3, $\mathcal{O}_{[1]}$ is a Gl$(2,k)$-orbit and $\mathcal{O}(\hat{k})$ is the union of 2 Gl$(2,k)$-orbits.

Proof. As examples, let us count the number of Sl$(2,k)$-orbits in $\mathcal{O}_{[1]}$ when $q = 1$ mod 3 and the number of Gl$(2,k)$-orbits in $\mathcal{O}(\hat{k})$ when $q = 2$ mod 3.

In the first case, by Theorem (3.33), the parameter space is $k^* \times_{Z_2} k^*/k^{*3}$ which, being a fibre bundle over k^{*2} with fibre k^*/k^{*3}, has $\frac{1}{2}(q-1)\times 3 = \frac{3}{2}(q-1)$ elements.

In the second case, by Theorem 4.3 , the parameter space is $(\operatorname{Im} \hat{k}^*)/k^{*3} \times U(\hat{k}^*/\hat{k}^{*3})/Z_2$ and this has $1 \times 2 = 2$ elements since Z_2 acts on $U(\hat{k}^*/\hat{k}^{*3})$ by inversion. QED

According to [10] (Proposition 5.6) at least part of the following corollary can be found in Dickson [7].

Corollary 4.5 *Let k be a finite field with q elements, not of characteristic 2 or 3. The number of Sl$(2,k)$-orbits of binary cubics with nonzero discriminant is $2(q-1)$. The number of Gl$(2,k)$-orbits of binary cubics with nonzero discriminant is 9 if $q = 1$ mod 3 and 3 if $q = 2$ mod 3.*

Proof. A binary cubic of nonzero discriminant is either in $\mathcal{O}_{[1]}$ or in $\mathcal{O}(\hat{k})$ since up to isomorphism, k has only one quadratic extension. Hence, the total number of

$\mathrm{Sl}(2,k)$-orbits with nonzero discriminant is the number of $\mathrm{Sl}(2,k)$-orbits in $\mathcal{O}_{[1]}$ plus the number of $\mathrm{Sl}(2,k)$-orbits in $\mathcal{O}(\hat{k})$. The same is true for $\mathrm{Gl}(2,k)$-orbits and the result follows from Proposition 4.4. QED

5 A symplectic Eisenstein identity

The following identity is a symplectic generalisation of the classical Eisenstein identity which, as we will see, is obtained from it in the special case when Q is the cube of a linear form. There is an analogous identity for the symplectic module associated to any Heisenberg graded Lie algebra ([15]).

Theorem 5.1 *Let $P, Q \in S^3(k^{2*})$. Then*

$$\omega(\Psi(P),Q)^2 - 9Q_n(P)\,\omega(P,Q)^2 = \\ -\frac{9}{2}\,\omega(\mu(P)^{\otimes 3}\cdot Q, Q) - \frac{9}{2}\,Q_n(P)\,\omega(\mu(P)\cdot Q, Q) \qquad (52)$$

where $\mu(P)^{\otimes 3}$ denotes the unique endomorphism of $S^3(k^{2*})$ satisfying $\mu(P)^{\otimes 3}\cdot(\alpha^3) = (\mu(P)\cdot\alpha)^3$ for all $\alpha \in k^{2*}$.

Proof. If $\mu(P) = 0$, then $\Psi(P) = 0$, $Q_n(P) = 0$ and all terms in the identity are zero.

If $\mu(P)$ is nilpotent nonzero, then $Q_n(P) = 0$ and and there exists $g \in \mathrm{Sl}(2,k)$ such that $g\cdot P = x^2y$. Since the identity (52) is $\mathrm{Sl}(2,k)$-invariant, we can suppose without loss of generality that $P = x^2y$. Then, by calculation,

$$\Psi(P) = -\frac{2}{9}x^3, \quad \mu(P) = \frac{2}{9}\begin{pmatrix}0&0\\1&0\end{pmatrix}$$

and so $\mu(P)\cdot x = 0$ and $\mu(P)\cdot y = -\frac{2}{9}x$. Let

$$Q = px^3 + 3rx^2y + 3sxy^2 + ty^3.$$

The LHS of (52) is

$$\omega(-\frac{2}{9}x^3, Q)^2 = (\frac{2}{9})^2t^2.$$

and the RHS of (52) is

$$-\frac{9}{2}\omega(\mu(P)^{\otimes 3}\cdot Q, Q) = -\frac{9}{2}\omega(-(\frac{2}{9})^3tx^3, Q) = (\frac{2}{9})^2t^2.$$

Thus (52) holds if $\mu(P)$ is nilpotent nonzero.

To complete the proof of the proposition it remains to prove (52) if $Q_n(P) \neq 0$. As the identity is independent of the field we may suppose that $Q_n(P)$ is a square in k^* and hence that $P \in \mathcal{O}_{[1]}$. Since the identity (52) is $\mathrm{Sl}(2,k)$-invariant, we can further suppose without loss of generality that

$$P = ax^3 + dy^3.$$

Then

$$Q_n(P) = a^2d^2, \quad \Psi(P) = 3ad(-ax^3 + dy^3), \quad \mu(P) = \begin{pmatrix} ad & 0 \\ 0 & -ad \end{pmatrix}$$

and so $\mu(P) \cdot x = -adx$ and $\mu(P) \cdot y = ady$. Let

$$Q = px^3 + 3rx^2y + 3sxy^2 + ty^3.$$

The LHS of (52) is

$$\begin{aligned} \omega(\Psi(P)^2, Q) - 9Q_n(P)\omega(P, Q)^2 & \\ &= 9a^2d^2\big(\omega(-ax^3 + dy^3, Q)^2 - \omega(ax^3 + dy^3, Q)^2\big) \\ &= -36a^3d^3\omega(x^3, Q)\omega(y^3, Q) \\ &= 36a^3d^3pt. \end{aligned} \tag{53}$$

On the other hand, the first term of the RHS of (52) is

$$\begin{aligned} -\frac{9}{2}\omega(\mu(P)^{\otimes 3} \cdot Q, Q) &= -\frac{9}{2}a^3d^3\omega(-px^3 + 3rx^2y - 3sxy^2 + ty^3, Q) \\ &= -\frac{9}{2}a^3d^3(-2pt - 6rs) \\ &= 9a^3d^3(pt + 3rs) \end{aligned} \tag{54}$$

and the second term of the RHS of (52) is

$$\begin{aligned} -\frac{9}{2}Q_n(P)\omega(\mu(P) \cdot Q, Q) &= -\frac{9}{2}a^3d^3\omega(-3px^3 - 3rx^2y + 3sxy^2 + 3ty^3, Q) \\ &= -\frac{9}{2}a^3d^3(-6pt + 6rs) \\ &= 27a^3d^3(pt - rs). \end{aligned} \tag{55}$$

The result follows from equations (53), (54) and (55). QED

To obtain the classical Eisenstein identity from this result, recall that one can use the symplectic form Ω on k^{2*} to define a $\mathrm{Sl}(2, k)$-equivariant isomorphism $\tilde{}: k^2 \to k^{2*}$: if $v \in k^2$, we let $\tilde{v} \in k^{2*}$ be the unique linear form such that

$$\phi(v) = \Omega(\phi, \tilde{v}) \quad \forall \phi \in k^{2*}.$$

It then follows that

$$P(v) = \omega(P, \tilde{v}^3) \quad \forall P \in S^3(k^{2*}),\ \forall v \in k^2, \tag{56}$$

so that the operation of evaluating a binary cubic at a point of k^2 can be expressed in terms of the symplectic form ω on $S^3(k^{2*})$. One can also pullback Ω to get an $\mathrm{Sl}(2, k)$-invariant symplectic form Ω_{k^2} on k^2:

$$\Omega_{k^2}(v, w) = \Omega(\tilde{v}, \tilde{w}) \quad \forall v, w \in k^2.$$

Corollary 5.2 *(Classical Eisenstein identity) Let $P \in S^3(k^{2*})$ and let $v \in k^2$.*

$$\Psi(P)(v)^2 - 9Q_n(P)\,P(v)^2 = -\frac{9}{2}\,\Omega_{k^2}(\mu(P)\cdot v, v)^3.$$

Proof. Setting $Q = \tilde{v}^3$ in (52) and using (56), we get

$$\Psi(P)(v)^2 - 9Q_n(P)\,P(v)^2 = \\ -\frac{9}{2}\,\omega(\mu(P)^{\otimes 3}\cdot \tilde{v}^3, \tilde{v}^3) - \frac{9}{2}\,Q_n(P)\,\omega(\mu(P)\cdot \tilde{v}^3, \tilde{v}^3). \qquad (57)$$

The result follows from this since

$$\omega(\mu(P)\cdot \tilde{v}^3, \tilde{v}^3) = 3\omega((\mu(P)\cdot \tilde{v})\tilde{v}^2, \tilde{v}^3) = 0$$

($(\mu(P)\cdot \tilde{v})\tilde{v}^2$ has at least a double root at v) and

$$\omega(\mu(P)^{\otimes 3}\cdot \tilde{v}^3, \tilde{v}^3) = \Omega(\mu(P)\cdot \tilde{v}, \tilde{v})^3 = \Omega_{k^2}(\mu(P)\cdot v, v)^3.$$

QED

References

1. M. BHARGAVA, Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations, *Ann. of Math. (2)* **159** (2004), no. 1, 217–250.
2. N. BOURBAKI, **Élements de mathématique**, Fascicule XXIV, Livre II, Algèbre Chapitre 9, Hermann, Paris, 1959.
3. M. CAHEN AND L. SCHWACHHÖFER, Special symplectic connections and Poisson geometry. *Lett. Math. Phys.* **69** (2004), 115–137.
4. M. DEMAZURE, Automorphismes et déformations des variétés de Borel. *Invent. Math.* **39** (1977), no. 2, 179–186.
5. L. E. DICKSON, **History of the Theory of Numbers**, vol. III. Chelsea, 1952.
6. L. E. DICKSON, **Algebraic Invariants**, Mathematical Monographs, No. 14, John Wiley and Sons, New York, 1914.
7. L. E. DICKSON, **On Invariants and The Theory of Numbers**, The Madison Colloquim, Dover Publications, New York, 1966.
8. G. EISENSTEIN, Untersuchungen über die cubischen Formen mit zwei Variabeln, *J. Crelle* **27** (1844), 89–104 = Mathematische Werke, Band I, Chelsea Publ. Co., 1975, 10–25.
9. D. HAILE, On the Clifford algebra of a binary cubic form, *Amer. J. Math.* **106** (1984), 1269–1280.
10. J. W. HOFFMAN AND J.MORALES, Arithmetic of binary cubic forms, *Enseign. Math. (2)*, **46** (2000), no. 1-2, 61–94.
11. L. J. MORDELL, The diophantine equation $y^2 - k = x^3$, *Proc. Lond. Math. Soc. (2)*, **13**, (1913), 60-80.
12. L. J. MORDELL, **Diophantine equations**, Pure and Applied Mathematics, Vol. 30 Academic Press, London-New York, 1969.

13. J. NAKAGAWA, On the relations among the class numbers of binary cubic forms, *Invent. Math.* **134** (1998), no. 1, 101–138.
14. T. SHINTANI, On Dirichlet series whose coefficients are class numbers of integral binary cubic forms, *J. Math. Soc. Japan* **24**, (1972), 132-188.
15. M. J. SLUPINSKI AND R. J. STANTON, Symplectic geometry of Heisenberg graded Lie algebras, nearing completion.
16. D. J. WRIGHT, The adelic zeta function associated with the space of binary cubic forms, I: global theory, *Math. Ann.* **270** (1985), 503–534.