ON THE JACOBIANS OF PLANE CUBICS

Michael Artin, Fernando Rodriguez-Villegas, and John Tate

§1 Introduction

In 1953 A. Weil [We1] proved that, given a curve of genus 1 by an equation

$$y^2 = f(x) \ ,$$

with f a polynomial of degree 4, one may compute a Weierstrass model for its Jacobian by means of the invariant theory of the quartic f. (He based his discussion on a paper by Hermite but later even traced the theory to Euler [We2].) His main motivation was his attempt to prove that if a curve C is defined over a field K, the Jacobian of C can also be defined over K, and he found that the paper of Hermite contained "most of the formulas needed for treating one fairly typical special case".

In the notes to [We1] in his collected papers, Weil remarks that he has also examined the case of plane cubics from the same point of view, and that this case offers no difficulty if one consults Chapter V of Salmon's classic book [Sa]. On p.203 of that book one finds an identity showing that the covariants Θ, J and H and invariants S and T of a ternary cubic U satisfy, on the curve $U = 0$, the equation

$$J^2 = 4\Theta^3 + 108S\Theta H^4 - 27TH^6 \ , \tag{1.1}$$

a relation which can be used to show that the elliptic curve $y^2 = 4x^3 + 108Sx - 27T$ is the Jacobian of the plane cubic $U = 0$. Here S and T are the classical invariants of degree 4 and 6 of ternary cubic forms discovered by Aronholdt [Ar] in 1849.

These ideas are discussed in detail and the two cases of quartics and cubics presented together, over an arbitrary ground field of characteristic $\neq 2, 3$, in [AKM^{3}P].

In characteristics 2 or 3 the classical invariants S and T don't suffice because one needs the more general equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.2}$$

to describe the Jacobian. In this paper we will refer to an equation of the form (1.2) as a *Weierstrass equation*, and will use the standard notations $b_2, b_4, b_6, b_8, c_4, c_6$, and Δ ([Ta], [Si])

Typeset by $\mathcal{AMS}$-TEX

for the primitive integral polynomials in a_1, a_2, a_3, a_4, a_6 associated to such an equation which are defined by the following identities, in which $y_1 := y + \frac{a_1 x + a_3}{2}$ and $x_1 := x + \frac{b_2}{12}$

$$\tag{1.3} \begin{cases} y_1^2 = x^3 + \dfrac{b_2}{4}x^2 + \dfrac{b_4}{2}x + \dfrac{b_6}{4} = x_1^3 - \dfrac{c_4}{48}x_1 - \dfrac{c_6}{864} \\ b_8 = \dfrac{b_2 b_6 - b_4^2}{4} \ , \quad \Delta = \dfrac{c_4^3 - c_6^2}{1728} \in \mathbb{Z}[b_2, b_4, b_6, b_8] \ . \end{cases}$$

We associate to a ternary cubic

$$\tag{1.4} f = f(x,y,z) = Ax^3 + By^3 + Cz^3 + Px^2y + Qy^2z + Rz^2x + Txy^2 + Uyz^2 + Vzx^2 + Mxyz$$

a *Weierstrass cubic*

$$\tag{1.5} f^* = f^*(x,y,z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3$$

whose coefficients $a_i = a_i(f)$ are homogeneous polynomials in the ten coefficients of f defined as follows.

$$\tag{1.6} \begin{aligned} a_1 &= M, \\ a_2 &= -(PU + QV + RT), \\ a_3 &= 9ABC - (AQU + BRV + CPT) - (TUV + PQR), \\ a_4 &= (ARQ^2 + BPR^2 + CQP^2 + ATU^2 + BUV^2 + CVT^2) \\ &\quad + (PQUV + QRVT + RPTU) - 3(ABRU + BCPV + CAQT), \\ a_6 &= -27A^2B^2C^2 + 9(A^2BCQU + B^2CARV + C^2ABPT) \\ &\quad + 3ABC(TUV + PQR) - (ABQRUV + BCRVPT + CAPQTU) \\ &\quad - (A^2CQ^3 + B^2AR^3 + C^2BP^3 + A^2BU^3 + B^2CV^3 + C^2AT^3) - PQRTUV \\ &\quad + 2(ACQ^2TV + BAR^2UT + CBP^2VU + ACQRT^2 + BARPU^2 + CBPQV^2) \\ &\quad - (AQTVU^2 + BRUTV^2 + CPVUT^2 + APQ^2RU + BQR^2PV + CRP^2QT) \\ &\quad - (AQ^2R^2T + BR^2P^2U + CP^2Q^2V + ART^2U^2 + BPU^2V^2 + CQV^2T^2) \\ &\quad + M(ABU^2V + BCV^2T + CAT^2U + ABR^2Q + BCP^2R + CAQ^2P) \\ &\quad + M(AQRTU + BRPUV + CPQVT - 3ABC(QV + RT + PU)) \\ &\quad - M^2(ABRU + BCPV + CAQT) + M^3ABC \end{aligned}$$

It is easy to check by computer that $(f^*)^* = f^*$, that is, $a_i(f^*) = a_i(f)$. Hence we can define $b_i(f) := b_i(f^*)$, $c_i(f) := c_i(f^*)$ and $\Delta(f) := \Delta(f^*)$ without ambiguity. Another easy check shows then that c_4 and c_6 are related to the classical invariants of ternary cubics [Sa] by

$$\tag{1.7} c_4 = -2^4 3^4 S \ , \qquad \text{and} \qquad c_6 = 2^3 3^6 T^1$$

It follows from (1.3) that over a field of characteristic different from 2 and 3, the cubic $f^* = 0$ is isomorphic to the cubic $y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}$ and therefore, by [AKM^{3}P], that the Jacobian of a smooth plane cubic $f = 0$ is the elliptic curve $f^* = 0$. We show that this is true in all characteristics. But more is true. Our main result, Theorem 1 below, is that the same holds for an arbitrary family X of plane cubics, over an arbitrary base scheme S, if we interpret the Jacobian of X/S as the relative Picard scheme $\mathrm{Pic}^0_{X/S}$ ([BLR], Chs. 8,9). Moreover X/S need not be smooth — its fibers can be arbitrary plane cubic divisors, even triple lines.

On the website of one of us (http://www.ma.utexas.edu/users/villegas/cnt), there are PARI-GP routines for the functions $f \mapsto f^*$, $b_i(f)$, $c_i(f)$ and $\Delta(f)$. There are also the analogous functions for the cases in which the curve of genus 1 is described by the affine equations

$$t_0y^2 + (s_0x^2 + s_1x + s_2)y + r_0x^4 + r_1x^3 + r_2x^2 + r_3x + r_4 = 0,$$

or by

$$(t_0x^2 + t_1x + t_2)y^2 + (r_0x^2 + r_1x + r_2)y + s_0x^2 + s_1x + s_2 = 0.$$

There is also, in the cubic case which we are treating in detail in this paper, a formula valid in all characteristics for the degree 9 map from the cubic curve $f = 0$ to its Jacobian $f^* = 0$ which takes a point p on the cubic curve to the class of the divisor $3[p] - H$ of degree 0, where [p] is the divisor of degree 1 determined by p and H is the intersection divisor of the cubic with a line. This is the map which in characteristics not 2 or 3 is given by the covariants and used in [AKM^{3}P] to prove that (1.1) gives the Jacobian of $U = 0$. The formula for it occupies about 1.6 megabytes.

Before stating Theorem 1 we introduce the notion of a Weierstrass group scheme. Let S be a scheme. Suppose a_1, a_2, a_3, a_4, a_6 are sections of $\mathcal{O}_S$. The homogenization of the equation (1.2) defines a closed subscheme $W \subset \mathbb{P}^2_S := \mathrm{Proj}(\mathcal{O}_S[x, y, z])$ which we call a *Weierstrass curve over* S. In [De] there is a detailed study of S-schemes isomorphic locally on S to such a W/S, and a characterization of them by intrinsic properties. Let J be the open subscheme of W where the map $W \to S$ is smooth. As explained in [De, §7], J has a natural structure of commutative group scheme over S. We call J a *Weierstrass group scheme*. The identity section $e : S \to J$ is the constant function $s \mapsto (0, 1, 0) \in \mathbb{P}^2$. The group law can be characterized by the fact that the map which associates to a section $u : S \to J \subset W$ the invertible sheaf $\mathcal{O}_W([u] - [e])$ is an isomorphism of $J(S)$ with the kernel of the homomorphism $e^* : \mathrm{Pic}(W) \to \mathrm{Pic}(S)$, and this is true after an arbitrary base change $S' \to S$. Therefore J represents the functor $\mathrm{Pic}^0_{W/S}$ in the same way that an elliptic curve is isomorphic to its own Jacobian.

An equation (1.2) for J/S determines functions Δ and c_4 on S whose vanishing or nonvanishing determines the nature of the fibers of J. At a geometric point s of S, the fiber J_s is an

[1] This T denotes the classical invariant of degree 6, as it did before (1.5). In the rest of this paper, T will denote the coefficient of xy^2 in f, as in (1.5). The reason for the factors 2^a3^b in (1.7) is that the classical invariant theorists multiplied monomials by the corresponding multinomial coefficients. For instance, they would write the terms Ax^3, Px^2y, $Mxyz$ in (1.4) as Ax^3, $3Px^2y$, $6Mxyz$. Hence, $c_4(A, \ldots , P, \ldots , M) = \pm S(A, \ldots , 3P, \ldots , 6M)$.

elliptic curve if $\Delta(s) \neq 0$, is isomorphic to $\mathbb{G}_m$ if $\Delta(s) = 0$ and $c_4(s) \neq 0$, and is isomorphic to $\mathbb{G}_a$ if $\Delta(s) = c_4(s) = 0$.

Theorem 1. *Let S be a scheme. Suppose the ten coefficients $A, B, \dots, M$ of the ternary cubic f (1.4) are sections of $\mathcal{O}_S$ with no common zero. Let X be the subscheme of $\mathbb{P}^2_S$ defined by the equation $f = 0$. Let W be the subscheme of $\mathbb{P}^2_S$ defined by the Weierstrass cubic $f^* = 0$ (1.5), and let J be the smooth locus of W/S. Then $\mathrm{Pic}^0_{X/S}$ is represented by the Weierstrass group scheme J.*

To prove Theorem 1 we use

Theorem 2. *Let S be a regular irreducible scheme. Suppose G is an algebraic space separated and smooth over S, which is a commutative group over S such that for each $s \in S$ the fiber G_s is connected of dimension 1 and the generic fiber G_η is an elliptic curve. Then*

(i) Each point $s \in S$ has a neighborhood U in S such that G_U is a Weierstrass group scheme over U.

(ii) If $Pic(S) = 0$ and $H^1(S, \mathcal{O}_S) = 0$, G is a Weierstrass group scheme over S.

We prove Theorem 2 in §2. In §3 we apply it to prove Theorem 1. Since the formation of $\mathrm{Pic}^0_{X/S}$ commutes with arbitrary base extension, it suffices to prove Theorem 1 for the generic ternary cubic f. We establish properties of the generic family of ternary cubics X/S which allow us to show for that family that the functor $\mathrm{Pic}^0_{X/S}$ satisfies the hypotheses of Theorem 2 (ii) and is therefore a Weierstrass group scheme. This shows that there must exist five polynomials with integer coefficients in the ten coefficients of f, as in (1.6), such that Theorem 1 is true for the f^* they define. To show that the polynomials (1.6) accomplish this, we show that any five such polynomials which give an f^* whose invariants c_4, c_6, Δ are the same as those of f will do the job. To do this we use

Theorem 3. *Suppose G and G' are two Weierstrass group schemes over a normal irreducible Noetherian base scheme S. Suppose that the generic fibers G_η and G'_η are elliptic curves, and that for s of codimension 1 in S, the fibers G_s and G'_s are semiabelian, that is, are either elliptic curves or forms of $\mathbb{G}_m$.*

(a) If the generic fibers G_η and G'_η are isomorphic, then G and G' are isomorphic.

(b) If the generic fibers G_η and G'_η have the same j-invariant different from 0 and 1728, but are not isomorphic, then there is a separable quadratic field extension L of the function field K of S such that the normalization T of S in L is unramified in codimension 1 on S and such that $G \times_S T$ is isomorphic to $G' \times_S T$.

Proof. We first prove (a), then use (a) to prove (b). Let x, y be Weierstrass coordinates on G and x', y' on G'. We can identify the generic fibers G_η and G'_η. Then there are rational functions u, r, s, t on S so that

(1.8) $$x = u^2x' + r \qquad y = u^3y' + su^2x' + t\ .$$

In obvious notation we have then

$$u^4 c_4' = c_4 \qquad u^{12}\Delta' = \Delta. \tag{1.9}$$

By our hypotheses we know that at a point s of codimension 1, not both c_4' and Δ' are zero. Hence, by (1.9), u is in $\mathcal{O}_s$. By symmetry, u^{-1} is in $\mathcal{O}_s$. A standard argument ([De], proof of Prop. 5.3 or [Si], VII, 1.3) shows then that r, s, t are integral over $\mathcal{O}_s$, hence are in $\mathcal{O}_s$. Since s was an arbitrary point of codimension 1 in the normal scheme S, the functions u, u^{-1}, r, s, t are defined everywhere on S and (1.8) defines an isomorphism $G \approx G'$ over all of S. This concludes the proof of (a).

(b) In this case the only automorphisms of G_η are $p \mapsto \pm p$, and there is a separable quadratic extension field L of K and an isomorphism $\phi : G'_L \to G_L$. This follows from [De] Prop. 5.3 (III), and can also be proved by an easy computation using the special Weierstrass forms in [Si], App.A, Prop. 1.1. Let T be the normalisation of S in L. By (a), applied over T, we know ϕ extends to an isomorphism $G' \times_S T \to G \times_S T$. We must show that T/S is unramified at each point s of codimension 1 in S. Let u, r, s, t be elements of L describing ϕ as in (1.8), Let * denote conjugation in L/K. Since G_K is not isomorphic to G'_K, ϕ^* is a different isomorphism from ϕ and is therefore equal to $-\phi$. If a_i are Weierstrass coefficients for G, the automorphism $p \mapsto -p$ on G is given by $(x, y) \mapsto (x, -y - a_1x - a_3)$. Using this a simple computation shows

$$u^* = -u, \qquad r^* = r, \qquad s^* = -s - a_1, \qquad t^* = -t - a_1r - a_3$$

Let s be a point of codimension 1 in S. We claim that the fiber T_s is the spectrum of a separable quadratic extension of $k(s)$. This follows from the first of the three displayed equations if 2 is invertible in $\mathcal{O}_S$, and from one of the other two equations is $k(s)$ is of characteristic 2, because in that case a_1 and a_3 do not both vanish at s since G_s is not the additive group.

An immediate consequence of a theorem of Raynaud ([Ra], Cor.IX, 1.5) together with a result on the uniqueness of Néron models ([BLR], §7.4, Prop.3) is a more general version of Theorem 3 (a). With the same assumptions on the base scheme S, the statement (a) is true for group schemes G and G' whose fibers are smooth and connected, are semi-abelian in codimension 1, and abelian at the generic point. This gives a proof of Theorem 1 in which the only need for Theorem 2 is to know that $\mathrm{Pic}^0_{X/S}$ is represented by a scheme. If Raynaud's theorem is true for algebraic space groups, this argument together with the result of [AKM^{3}P] would give a proof of Theorem 1 independent of our Theorems 2 and 3.

How unique are our polynomials (1.6)? Not at all unique, for we can change cordinates as in (1.8) with $u = \pm 1$, and arbitrary $r, s, t \in \mathbb{Z}[A, \dots, M]$. This would change a_i to a_i' by the well known formulas

$$\pm a_1' = a_1 + 2s, \qquad a_2' = a_2 - sa_1 + 3r - s^2, \qquad \pm a_3 = a_3 + ra_1 + 2t, \quad \text{etc.}$$

and we would also have

$$b_2' = b_2 + 12r, \quad \text{etc.}$$

(cf. [Ta], (7), or [Si], III, table 1.2). In particular, b_2 can be changed arbitrarily modulo 12 and a_1 and a_3 arbitrarily modulo 2. However, c_4, c_6 and Δ are unchanged. To find polynomials like those in (1.6), knowing c_4 and c_6 from (1.7), one can use the expressions for the c's as functions of the b's to guess suitable b's, then the expressions for the b's as functions of the a's to guess suitable a's. One first solves the congruences

$$b_2^2 \equiv c_4 \bmod 24, \qquad b_2^3 \equiv c_6 \bmod 36,$$

which determine b_2 modulo 12. A choice of solution b_2 then determines b_4, b_6 and b_8 uniquely. With these b's, the congruences

$$a_1^2 \equiv b_2 \bmod 4, \qquad a_3^2 \equiv b_6 \bmod 4,$$

determine a_1 and a_3 modulo 2. A choice of solutions a_1 and a_3 then determines a_2, a_4 and a_6.

We found the polynomials (1.6) by using simple and symmetric solutions b_2, a_1 and a_3 to those congruences.

Theorem 4. *Our polynomials* (1.6) *are uniquely determined by the properties:*

(i) $c_4(f^*)$ *and* $c_6(f^*)$ *are the classical invariants of ternary cubics, normalized so that for* $f(x,y,z)=xyz$, $c_4(f) = 1$ *and* $c_6(f) = -1$.
(ii) If $Z \in GL_3$ *is a diagonal matrix or a permutation matrix, then* $a_i(Zf) = (\det Z)^i a_i(f)$, *where* $(Zf)(x, y, z) := f((x, y, z)Z)$. *(In particular,* a_i *is homogeneous of degree i.)*
(iii) $(f^*)^* = f^*$.
(iv) $a_4(f)$ *is independent of the coefficient* M *of* xyz *in* f.

Proof. Left to the reader. Properties (i), (ii) and (iii) determine $a_1(f)$ and $a_2(f)$ uniquely. The reason the inelegant condition (iv) is needed is that there are polynomials $d_3 = mABC + n(TUV + PQR)$ for $m, n \in \mathbb{Z}$ which satisfy the same partial invariance (ii) as a_3 and such that $d_3(f) = 0$ if f is a Weierstrass cubic. Then the five polynomials

$$a_1, \qquad a_2, \qquad a_3 + 2d_3, \qquad a_4 - Md_3, \qquad a_6 - a_3 d_3 - d_3^2$$

satisfy conditions (i),(ii) and (iii), but not (iv) unless $d_3 = 0$.

§2 Proof of Theorem 2

We begin with three general lemmas. Although they are presumably well known, at least for schemes, we include proofs.

Lemma 2.1. *Suppose* $f : X \to Y$ *is a continuous map of topological spaces. The following are equivalent:*

(a) *The map* f *is open.*
(b) *Taking inverse images commutes with closure, that is,* $\overline{f^{-1}(T)} = f^{-1}(\overline{T})$, *for each subset* $T \subset Y$.

This is an easy exercise. There is a proof in [Ku], §XIV .

Lemma 2.2. *Let $f : X \to Y$ be a flat, finite type map of Noetherian algebraic spaces. Suppose Y irreducible, with generic point η. Let X_η denote the fibre of X over η.*

(a) If X_η is irreducible, with generic point ξ, then X is irreducible, and ξ is the generic point of X.

(b) If Y and X_η are reduced, then X is reduced.

Proof. (a) A flat finite type map of noetherian schemes is open (This follows from [Ha], Ch.III, Ex.9.1, because flatness and openness are local properties for the etale topology.) Lemma 2.1 with $T = \{\eta\}$ shows that X is the closure of X_η, and hence of $\{\xi\}$.

(b) Suppose Y and X_η are reduced. Let $x \in X$, put $y = f(x)$, and let X_y denote the fibre of X over y. Then $\mathcal{O}_{X_y,x} \approx \mathcal{O}_{X,x} \otimes_{\mathcal{O}_{Y,y}} k(\eta)$. Consider the restriction maps

$$\mathcal{O}_{X,x} \to \mathcal{O}_{X_y,x} \to k(\xi).$$

The first map is injective by flatness because, since Y is reduced, the map $\mathcal{O}_{Y,y} \to k(\eta)$ is injective. The second map is injective because X_y is reduced. Thus $\mathcal{O}_{X,x} \to k(\xi)$ is injective. Since this is true for for every $x \in X$, X is reduced as claimed.

Lemma 2.3. *Let $f : X \to Y$ be a flat, finite type map of Noetherian algebraic spaces. Suppose Y reduced and irreducible, with generic point η. Suppose also that the fibres X_y over points $y \in Y$ of codimension at most 1 are reduced and irreducible. Let D be a reduced irreducible subspace of X of codimension 1 such that $\eta \notin f(D)$. Let Δ denote the closure of $f(D)$ with its induced reduced structure. Then Δ is a closed irreducible algebraic space of codimension 1 in Y and $D = X \times_Y \Delta$.*

Proof. Let x be the generic point of D and $y = f(x)$. Since $\eta \notin f(D)$, $\dim_y(Y) \geq 1$, and $\dim_x(X) = 1$. On the other hand $\dim_x(X) = \dim_x(X_y) + \dim_y(Y)$. (See [Ha], Ch.III, Prop. 9.5. The dimensions are local for the etale topology.) Hence $\dim_x(X_y) = 0$ and $\dim_y(Y) = 1$, i.e., y has codimension 1 in X. By hypothesis, X_y is reduced and irreducible, x is its generic point, and $D = \overline{\{x\}} = \overline{X}_y$. By Lemma 2.1, $D = f^{-1}(\overline{\{y\}})$. Hence $f(D) \subset \overline{\{y\}}$ and $\Delta = \overline{\{y\}}$ is irreducible. Lemma 2.2, applied to the map $X \times_Y \Delta \to \Delta$, shows that $X \times_Y \Delta$ is reduced and irreducible, hence is equal to D.

We now begin the proof of Theorem 2. The group G, an algebraic space over S, is as in the hypotheses of that theorem. By Lemma 2.2, G is reduced and irreducible, and G is regular because S is regular and G/S smooth. Hence every Weil divisor on G is a Cartier divisor. We will just write divisor from now on. We call a divisor vertical if its support does not meet the generic fiber G_η.

Lemma 2.4. *A vertical divisor D on G is a pull-back from the base scheme S and is principal if $Pic(S) = 0$*

Proof. To prove this we can suppose D is irreducible. By Lemma 2.3 D is a pull-back from the base scheme S, hence is principal if $\mathrm{Pic}(S) = 0$.

A section $a : S \to G$ is a closed immersion because G/S is separated. Its image is a divisor, which we denote by $[a]$. We will use the following lemma to construct rational functions on G.

Lemma 2.5. *Let $a_1, a_2, \dots, a_r$ be sections and $n_1, n_2, \dots, n_r$ integers such that $\Sigma_i n_i a_i = 0$ and $\Sigma_i n_i = 0$. Then the divisor $\Sigma n_i [a_i]$ is principal if $Pic(S) = 0$.*

Proof. This is true on the generic fiber G_η. Hence there is a function f whose divisor has the form $\Sigma n_i [a_i] + Z$, with Z vertical. Lemma 2.4 completes the proof.

Let $e : S \to G$ be the identity section and $\pi : G \to S$ the structure morphism. Define sheaves V_n on S for $n \geq 1$ by $V_1 = \mathcal{O}_S$ and $V_n = \pi_* \mathcal{O}_G(n[e])$ for $n \geq 2$. The V_n are quasicoherent, by [Kn], II, Prop.4.6. We will see in the course of our proof that V_n is a locally free $\mathcal{O}_S$-module of rank n.

Definition 2.6. A *basic section of V_n at s* is a section z of V_n in a neighborhood of s such that the restriction of z to the fiber X_s has a pole of order n at the identity $e(s)$. A *basic section of V_n over S* is a global section of V_n which is basic at every point of S, or equivalently, whose divisor on X has the form $D - n[e]$, where D is an effective divisor whose support does not meet $[e]$.

Lemma 2.7. *Suppose S is strictly Henselian and $n \geq 2$. Then V_n has a basic section.*

Proof. The closed fiber of G has an infinity of rational points because it is smooth over a separably closed field. Each of these points can be lifted to a section of G/S. Hence there are sections $a, b : S \to G$ such that $a(s) \neq e(s)$ and $b(s) \neq e(s), -a(s)$. Since S is local, neither $[a]$ nor $[b]$ nor $[a + b]$ meets $[e]$. Since S is regular, $\mathrm{Pic}(S) = 0$ and by Lemma 2.5, there exist functions x, y on G with divisors

$$\mathrm{div}(x) = [a] + [-a] - 2[e] , \qquad \mathrm{div}(y) = [a] + [b] + [-a - b] - 3[e] .$$

Thus x is a basic section of V_2 and y of V_3. With x and y we define a sequence of functions $(z_n)_{n\geq 2}$ such that z_n is a basic section of V_n by putting

$$z_{2i} = x^i \quad z_{2i+1} = x^{i-1} y, \text{ for } i \geq 1.$$

Lemma 2.8. *Let $s \in S$. A basic section of V_n at s exists for each $n \geq 2$.*

Proof. Let S' be a strict Henselization of S at s and s' the closed point of S'. Denote pullback to S' by a prime. Since direct image commutes with flat base extension, we have $V'_n := \pi'_* \mathcal{O}'(ne') = V_n \otimes_S \mathcal{O}_{S'}$.We know that there is a basic section z'_n of V'_n, a section whose restriction to the closed fibre has a pole of order n at $e(s')$. Writing $z'_n = \sum z_i \otimes h_i$ with the z_i sections of V_n at s and the h_i sections of $O_{S'}$ one sees that the restriction to the fibre of at least one z_i also has a pole of order n at $e(s)$, so is a basic section of V_n at s.

Lemma 2.9. *Let $s \in S$. If z is a basic section of V_n at s, then it is basic over some Zariski neighborhood of s.*

Proof. Replacing S by an open neighborhood of s reduces us to the case that z is a global section. Its divisor has the form $D - n[e]$, where D is effective and does not meet $[e]$ at $e(s)$. Then $C := \pi(D \cap [e])$ is a closed subset of S which does not contain s. Its complement is the required neghborhood over which z_n is basic.

Lemma 2.10. *(a) For each $n \geq 2$, each point $s \in S$ has a Zariski neighborhood over which V_n has a basic section.*

(b) Suppose z_i is a basic section of V_i over S for $i = 2, 3, ..., n$. Then V_n is a free $\mathcal{O}_S$-module of rank n with basis $1, z_2, ..., z_n$.

(c) For all n, V_n is locally free of rank n.

Proof. (a) This follows from immediately from the last two lemmas.

(b) Let $z_1 = 1$. To show that the map $\mathcal{O}_S^n \to V_n$ defined by $z_1, z_2, \ldots, z_n$ is bijective it is enough to show the map on stalks $\mathcal{O}_s^n \to (V_n)_s$ is bijective for each $s \in S$. Since formation of direct image commutes with localization, it suffices to treat the case in which S is the spectrum of the regular local ring $\mathcal{O}_s$, and since V_n is quasicoherent, it suffices to show that the $\mathcal{O}_s$-module $(V_n)_s$ is free with basis $z_1, z_2, \ldots, z_n$. The restrictions of the functions z_i to the fiber G_s are linearly independent over $k(s)$ because they have poles of different orders at $e(s)$. At the generic point η the dimension of $V_n(\eta)$ is n, by Riemann-Roch on the elliptic curve G_η. Hence $z_1, z_2, \ldots, z_n$ span $V_n(\eta)$. Let $z \in (V_n)_s$. There are elements $c, c_1, \ldots, c_n \in \mathcal{O}_s$ such that $c \neq 0$ and

$$cz = c_1 z_1 + c_2 z_2 + \cdots + c_n z_n \ ,$$

and since $\mathcal{O}_s$ is a unique factorization domain, we can assume c and the c_i's have no common prime divisor. Then c is invertible in R for if not it would be divisible by a prime p, contradicting the fact that the restrictions of the z_i to the fiber $G_{(p)}$ are independent. Thus $z_1, \ldots, z_n$ span the stalk $(V_n)_s$.

(c) By(a), the hypothesis of (b) is fulfilled if we replace S by a suitable neighborhood U of s.

By Lemma 2.10 (a), the following proposition will complete the proof of Theorem 2.

Proposition 2.11. *Suppose V_2 and V_3 have basic sections over S. Then G/S is a Weierstrass group scheme.*

Proof. For the rest of this section, we suppose that V_2 and V_3 have basic sections over S, which we denote by x and y, respectively. By Lemma 2.10 (b), V_6 is a free $\mathcal{O}_S$-module with basis $1, x, y, x^2, xy, x^3$. Since y^2 is a section of V_6, there are sections a_i of $\mathcal{O}_S$ such that

$$y^2 + a_1 xy + a_3 y = a_0 x^3 + a_1 x^2 + a_4 x + a_6 \ .$$

Since y^2 has a pole of order 6 at e on every fiber, a_0 has no zero on S, so is invertible. Since $a_0 x$, $a_0 y$ satisfy a Weierstrass equation with $a_0 = 1$, we can and do assume $a_0 = 1$ from now on.

The three sections $x, y, 1$ of $\mathcal{O}(3[e])$ have no common zeros, so they define a map $\phi : G \to \mathbb{P}^2_S$, whose image is in the cubic W defined by the homogenization of the above equation. Let $W^0 \subset W$ be the corresponding Weierstrass group scheme.

Lemma 2.12. *The map ϕ factors through W^0. The induced map $\phi : G \to W^0$ is a homomorphism of S-group functors.*

Proof. By construction, ϕ factors through W. Let $H = \phi^{-1}(W^0)$, an open subset of G. Consider the diagram

$$\begin{array}{ccc} H \times H & \xrightarrow{\phi\times\phi} & W^0 \times W^0 \\ {\scriptstyle u}\downarrow & & {\scriptstyle v}\downarrow \\ G & \xrightarrow{\phi} & W \supset W^0 \end{array}$$

where u and v are induced by the group operations in G and W^0. We have two maps $H \times H \to W$, namely $\phi \circ u$ and $v \circ (\phi \times \phi)$. Since by hypothesis the generic fiber G_η is an elliptic curve and, by construction, W_η is a Weierstrass model for it, we have $W^0_\eta = W_\eta$, $H_\eta = G_\eta$ and $\phi : G_\eta \to W^0_\eta$ is a group isomorphism. Therefore our two maps agree generically. Since G/S is separated, the locus on which they agree is closed in $H \times H$. Hence it is all of $H \times H$ and our diagram commutes, u factors through $\phi^{-1}(W^0) = H$, and H is closed under the group law in G. Similarly H is closed under the involution $a \mapsto -a$, so is an open subalgebraic space group of G, and $\phi : H \to W^0$ is a homomorphism of group functors. We claim that $H = G$. Since H is open in G, it suffices to check that the fibers H_s and G_s are equal for each $s \in S$. This is true because G_s is a smooth connected group of dimension 1, and therefore contains no proper subgroup of positive dimension.

Lemma 2.13. *The map $\phi : G \to W^0$ is a surjective monomorphism.*

Proof. To prove that the homomorphism ϕ is a monomorphism, it suffices to prove its kernel K, a closed subgroup of G, is zero. The divisors of the sections x and y of V_3 are of the form $(x) = -2[e] + D$ and $(y) = -3[e] + D'$, with D and D' effective and not meeting $[e]$. The fact that $1/x$ vanishes on K shows that K is supported on $[e]$. The function x/y vanishes on K, and the divisor of x/y in the complement of the support of $D + D'$ is $[e]$. Therefore the kernel is $[e]$, as claimed.

Lemma 2.14. *The map $\phi : G \to W^0$ is flat.*

Proof. Let $g \in G$ map to $w \in W^0$. We must show that the map of local rings $A = \mathcal{O}_w \to \mathcal{O}_g = B$ is flat. Since the completion of a local ring is faithfully flat over the ring, it suffices to show that $\widehat{A} \to \widehat{B}$ is flat. Let $\mathfrak{m}$ be the maximal ideal of the local ring $\mathcal{O}_s$, where s is the image of g in S. Let $\overline{A} = \widehat{A}/\mathfrak{m}\widehat{A}$ and $\overline{B} = \widehat{B}/\mathfrak{m}\widehat{B}$. These are the completions of the local rings of the fibres of W^0 and G respectively. Because ϕ is an isomorphism on fibres, by Lemma 2.13, $\overline{A} \to \overline{B}$ is an isomorphism. It follows that the map $\widehat{A} \to \widehat{B}$ is surjective, and since $\widehat{A}, \widehat{B}$ are regular local rings of the same dimension, it is bijective.

Since a flat monomorphism is an open immersion ([Kn], II, 6.15), this shows $\phi : G \approx W^0$, finishing the proof of Proposition 2.11 above and Theorem 2.

§3 The generic plane cubic

Throughout this section the following notation is in force. We let S denote the complement of the zero section in affine 10-space $\mathbb{A}^{10}_{\mathbb{Z}}$ over $\mathbb{Z}$, and let f be the generic ternary cubic whose coefficients are the ten coordinate functions on $\mathbb{A}^{10}$. We denote the generic family of plane cubics $f = 0$ by $X \subset \mathbb{P}^2_S$. Let J be the Weierstrass group scheme defined by $f^* = 0$ and let $P := \mathrm{Pic}^0_{X/S}$. Our aim is to show $J \approx P$, that is, to prove Theorem 1 for X/S.

Knowing Theorem 1 for X/S proves it in general because the formation of Pic^0 commutes with base change, and an arbitrary X'/S' as in Theorem 1 is the base change of our generic X/S by the morphism $S' \to S$ taking the variable coefficients of the generic f to the corresponding coefficients of the special cubic f' defining X'.

Proposition 3.1. Properties of X/S.

(i) *The map $\pi : X \to S$ is projective, flat, of relative dimension* 1*.*

(ii) *The map $\pi : X \to S$ is cohomologically flat in dimension* 0*, that is, $\pi_*\mathcal{O}_X = \mathcal{O}_S$, and the same holds after arbitrary base change $S' \to S$.*

(iii) *In codimension one on S, the geometric fibers of X are irreducible plane cubics with at most a node as singularity.*

Proof. (i) That X/S is projective of relative dimension 1 is obvious, It is flat because X is a relative complete intersection, being defined by one equation.

(ii) That $\pi_*\mathcal{O}_X = \mathcal{O}_S$ follows from the exact sequence

$$0 \longrightarrow \mathcal{O}_{\mathbb{P}^2_S}(-3) \xrightarrow{\ f\ } \mathcal{O}_{\mathbb{P}^2_S} \longrightarrow \mathcal{O}_X \longrightarrow 0$$

because $\pi_*\mathcal{O}_{\mathbb{P}^2_S} = O_S$ and $R^q\pi_*\mathcal{O}_{\mathbb{P}^2_S}(-3) = 0$ for $q = 0, 1$. The same holds after an arbitrary base extension $S' \to S$, since we used no special property of S in this argument.

To prove (iii) we note first that the projective spaces of linear forms and quadratic forms in three variables are 2 and 5 respectively. Hence the space of reducible cubics is of codimension 2 in the 9 dimensional space of all ternary cubic curves and the fibers of X of codimension 1 are therefore irreducible. If a cubic has two singular points, it contains the line joining them. Therefore the fibers of X of codimension 1 have at most one singularity.

To show that their only possible singularity is a node we use the following lemma which is surely classical, at least in characteristic 0. We include a proof here for the convenience of the reader. Let $\Delta = \Delta(f)$ and $c_4 = c_4(f)$, functions on S.

Lemma 3.2. *The fiber X_s at a geometric point s of S is smooth if and only if $\Delta(s) \neq 0$. If $\Delta(s) = 0$, then $c_4(s) \neq 0$ if and only if all singularities of X_s are normal crossings.*

Proof. Let $f_s = 0$ be the equation for $X_s \subset \mathbb{P}^2_s$. If f_s is a Weierstrass cubic the lemma is well known ([Si], III, 1.4). If f' is obtained from f_s by a linear change of coordinates with determinant

d then $\Delta(f') = d^{12}\Delta(f_s)$, so we will be done if there is a choice of coordinates in $\mathbb{P}^2_s$ for which X_s is a Weierstrass cubic. It is easy to see that the condition for this is that X be irreducible and have a rational smooth point of inflection. If X_s is smooth this condition is satisfied, even in characteristic 3, because the group of divisor classes of degree 0 is divisible by 3, hence each class of degree 3 is 3 times a class of degree 1. Therefore the linear system of intersections of X_s with lines in $\mathbb{P}^2_s$ contains a divisor which is three times a point, and such a point is a flex.

Suppose X_s is not smooth. Given a singularity, we can choose coordinates in $\mathbb{P}^2_s$ so it is at $(0,0,1)$. Then, at s, with notation as in (1.4), $C = R = U = 0$, and even without a computer, it is easy to check from (1.6) that the equation of W_s is

$$f^*(x,y,z) = y^2z + Mxyz - x^3 + QVx^2z \ ,$$

and

$$b_2 = M^2 - 4QV, \quad b_4 = b_6 = b_8 = 0 \ , \quad c_4 = (M^2 - 4QV)^2, \quad \Delta = 0 \ .$$

This completes the proof of Lemma 3.2 because c_4 is the discriminant of the quadratic form $y^2 + Mxy + QVx^2$.

To finish the proof of (iii) we must show that all points of the locus $\Delta = c_4 = 0$ on S are of codimension at least 2, or in other words, that Δ and c_4 have no common factor in the polynomial ring $\mathbb{Z}[A, \dots, M]$ generated by the 10 coefficients of f. It suffices to show they have no common factor modulo 2. This is true because

$$c_4 \equiv M^4 \mod 2, \qquad \Delta \equiv (ABC + AQU + BRV + CPT + PQR + TUV)^4 \mod (2, M).$$

Proposition 3.3. Properties of $\mathrm{Pic}^0_{X/S}$**.**

(i) $\mathrm{Pic}_{X/S} = R^1\pi_*\mathbb{G}_m$, *computed in the fppf topology, i.e.,* $\mathrm{Pic}_{X/S}$ *is the fppf sheaf associated to the presheaf* $S' \mapsto \mathrm{Pic}(X \times_S S')$.

(ii) $P := \mathrm{Pic}^0_{X/S}$ *is the subfunctor of* $\mathrm{Pic}_{X/S}$ *which consists of the elements whose restrictions to all fibers belong to the identity component. An equivalent definition if the relative dimension of X/S is 1 is that* $\mathrm{Pic}^0_{X/S}$ *consists of the elements of* $\mathrm{Pic}_{X/S}$ *which are represented by invertible sheaves whose restriction to every reduced irreducible component of every geometric fiber of X/S is of degree 0.*

(iii) *If X'/S' has a section $a : S' \to X'$, then*

$$\mathrm{Pic}_{X/S}(S') \approx \mathrm{Pic}\, X' / \mathrm{Pic}\, S' \approx \ker(a^* : \mathrm{Pic}\, X' \to \mathrm{Pic}\, S').$$

(iv) *The fiber of* $\mathrm{Pic}_{X/S}$ *at a geometric point s is the Picard scheme of the fiber X_s. For s of codimension 1 in S, P_s is either an elliptic curve or $\mathbb{G}_m$.*

(v) $\mathrm{Pic}_{X/S}$ *is represented by an algebraic space locally of finite type over S.*

(vi) $\mathrm{Pic}_{X/S}$ *is smooth over S and P is an open subgroup of* $\mathrm{Pic}_{X/S}$.

(vii) *P is separated over S.*

Proofs. (i) Definition, cf. [BLR], Ch.8.

(ii) Definition, cf. [BLR], p.233 and 9.2, Cor.13.

(iii) In view of Proposition 3.1 (ii) the spectral sequence $H^p(S', R^q\pi'_*\mathbb{G}_m) \Rightarrow H^{p+q}(X', \mathbb{G}_m)$ yields an exact sequence

$$0 \to \operatorname{Pic} S' \xrightarrow{\pi^*} \operatorname{Pic} X' \to \operatorname{Pic}_{X/S}(S') \to H^2(S', \mathbb{G}_m) \xrightarrow{\pi^*} H^2(X', \mathbb{G}_m)$$

and $a^*\pi^* =$ identity. (See [BLR], 8.1, Prop.4).

(iv) By a theorem of Murre and Oort, cf. [BLR], 8.2, Th.3, the fiber of $\operatorname{Pic}_{X/S}$ at a point $s \in S$ is the Picard scheme of the fiber X_s. In codimension 1, X_s is an irreducible plane cubic, either smooth or nodal, and as is well known, P_s is either an elliptic curve or G_m, accordingly.

(v) This is proved in [A, Thm.7.3]; see also [BLR], 8.3.

(vi) This is true because X/S is proper, flat, locally of finite presentation of relative dimension 1, cf. [BLR], 8.4, Prop.2.

(vii) We check the valuative criterion. Let T be a scheme over S which is the spectrum of a discrete valuation ring with local parameter t, generic point ξ, and denote $X \times_S T$ by X_T. We must show $P(T) \to P(\xi)$ is injective. Since P is an fppf sheaf, it suffices to do this after an fppf base change. This will enable us to assume that X_T/T has a section. Let K be a finite extension field of $k(\xi)$ over which X_ξ has a rational point. It is enough to check the valuative criterion with T's which are of essentially finite type over S, so we assume this. Replace T by the localization, at a closed point, of its normalization in K, an fppf base change. Now X_T/T has a section since it is projective and has a section at the generic point. Hence elements of $P(T)$ are represented by invertible sheaves on X_T and what has to be proved is that if L is an invertible sheaf on X_T representing an element of $\operatorname{Pic}^0_{X_T/T}$ such that $L \mid X_\xi \approx \mathcal{O}_{X_\xi}$, then $L \approx \mathcal{O}_X$.

Consider the exact sequence

$$0 \longrightarrow L \xrightarrow{t} L \longrightarrow L_0 \longrightarrow 0\,,$$

where L_0 is the restriction of L to the closed fiber X_0. Since $H^0(X_\xi, L_\xi) \approx k(\xi)$ is of dimension 1, $H^0(X, L)$ is of rank 1. Therefore there exists a section $u \in H^0(X, L)$ whose restriction to the special fiber X_0 is not 0. If we can show that u does not vanish on X_0, then, since its zero locus is closed in X, u does not vanish on X_T, hence generates L. Therefore the following lemma, with $D = X_0$ and $L = L_0$, completes the proof of (vii).

Lemma 3.4. *Let k be a field, D an effective divisor in $\mathbb{P}^2_k$, and $L = L_D$ an invertible sheaf on D whose restriction to each reduced irreducible component of D is of degree ≤ 0. If u is a non-zero section of L, then degree $D = 0$ and u has no zeros on D.*

Proof. We use induction on the degree d of D. If the restriction of u to each reduced irreducible component of D is not zero, then we are done, since the lemma is obvious in case D is reduced and irreducible. Suppose $u \neq 0$, but u vanishes on some reduced irreducible component A of degree a. Let $B = D - A$ and $b = d - a = \deg(B)$. Tensoring the exact sequence

$$0 \to \mathcal{O}_B(-a) \to \mathcal{O}_D \to \mathcal{O}_A \to 0$$

with L gives

$$0 \to L_B(-a) \to L_D \to L_A \to 0$$

and since u is zero in L_A, it is the image of a non-zero section v of $L_B(-a)$. The degree of $L_B(-a)$ is $\deg L_B - ab \leq -ab$. By induction we conclude $a = 0$ or $b = 0$, a contradiction because $D \neq A \neq 0$.

Lemma 3.5. *Our base scheme S satisfies* $\mathrm{Pic}(S) = 0$ *and* $H^1(S, \mathcal{O}_S) = 0$.

Proof. The open immersion $S \subset \mathbb{A}^{10}_{\mathbb{Z}}$ gives a bijection on divisors so $\mathrm{Pic}(S) = 0$. Let $\mathbb{P} = S/\mathbb{G}_m$, the 9 dimensional projective space on the variables. The map $\pi : S \to \mathbb{P}$ is affine, so $H^q(S, \mathcal{O}_S) = H^q(\mathbb{P}, \pi_*\mathcal{O}_S)$. The action of $\mathbb{G}_m$ grades $\pi_*\mathcal{O}_S$, and $\pi_*\mathcal{O}_S = \bigoplus_{n\in\mathbb{Z}} \mathcal{O}_{\mathbb{P}}(n)$. Hence $H^q(\mathbb{P}, \pi_*\mathcal{O}_S) = 0$ for $0 < q < 9$.

By Proposition 3.3, and Lemma 3.5, P satisfies the hypotheses of Theorem 2 (ii) in the introduction and is therefore a Weierstrass group scheme.

Lemma 3.6. *Let G be a Weierstrass group scheme over S given by a Weierstrass cubic g with the same invariants c_4, c_6, as f. Then G is isomorphic to P.*

Proof. Since $k(\eta)$ is of characteristic 0, and $1728\Delta = c_4^3 - c_6^2$, g has the same Δ as f. By Proposition 3.1(iii), Δ and c_4 do not vanish simultaneously in codimension 1. Therefore G and P satisfy the hypotheses of Theorem 3 (a), and to finish the proof we have only to show that the generic fibers of G_η and P_η are isomorphic. Here are two ways to do that.

(a) As explained in the introduction, it follows from [AKM^{3}P] that P_η, the Jacobian of the curve over $k(\eta)$ defined by $f = 0$, is the curve

$$y^2 = x^3 - \frac{c_4(f)}{48}x - \frac{c_6(f)}{864}.$$

By (1.3), $G\eta$ is isomorphic to the same curve since by hypothesis $c_i(g) = c_i(f)$ for $i = 4, 6$. Hence $G_\eta \approx P_\eta$.

(b) We use Theorem 3 (b). Let K be an algebraically closed field of characteristic 0 and h a ternary cubic form with coefficients in K whose zero locus is smooth. Let S, T and c_4, c_6 be its invariants as in (1.7). Over $\mathbb{C}$, hence over K, it is classical that the modular invariant $j = j(h)$ defined by

$$j = \frac{64S^3}{64S^3 + T^2} = \frac{1728c_4^3}{c_4^3 - c_6^2} = \frac{c_4^3}{\Delta}$$

depends only on the isomorphism class over K of the curve $h = 0$.

Since X_η and its Jacobian P_η are smooth and isomorphic over the algebraic closure of $k(\eta)$, $j(P_\eta) = j(X_\eta) = j(G_\eta)$. If G_η and P_η were not isomorphic then by Theorem 3 (b) there would exist a quadratic extension L of the field $k(\eta)$ unramified in codimension 1 on S. But $k(\eta)$ is a rational function field over $\mathbb{Q}$, so has no such extension. Hence $G_\eta \approx P_\eta$.

This proves theorem 1, because f^* and f have the same invariants, and Lemma 3.6 with $g = f^*$ shows that J is isomorphic to P.

References

[A] Artin, M., *Algebraization of formal moduli I*, Global Analysis, Papers in Honor of K. Kodaira, Univ. Tokyo Press, Princeton Univ. Press, 1969,, pp. 21–61.

[AKM^{3}P] An, S.Y., Kim, S.Y., Marshall, D.C., Marshall, S.H., McCallum, W.G., Perlis, A.R., *Jacobians of genus one curves*, J. Number Theory **90** (2001,), 304–315.

[Ar] Aronhold, S., *Zur Theorie der homogenen Functionen dritten Grades von drei Variabeln*, J. reine und angew. Math. **34** (1850), 140–159.

[BLR] Bosch, S., Lütkebohmert, W., Raynaud, M., *Neron Models*, Springer Verlag, 1990.

[De] Deligne, P., *Courbes Elliptiques: Formulaire*, Modular Functions of One Variable IV, Lect. Notes in Math.**476**, Springer Verlag, 1975, pp. 54–73.

[Ha] Hartshorne, R., *Algebraic Geometry*, Springer Verlag, 1977.

[Kn] Knutson, D., *Algebraic Spaces*, Lect. Notes in Math.**203**, Springer Verlag, 1971.

[Ku] Kuratowski, K., *Topology*, Vol.1, Academic Press, 1966.

[Ra] Raynaud, M., *Faisceaux Amples sur les schémas en groups et les espaces homogènes*, Lect. Notes in Math.**119**, Springer Verlag, 1970.

[Sa] Salmon, G., *Higher plane curves*, 3rd Ed., 1879, reprinted by Chelsea, NY.

[Si] Silverman, J., *The Arithmetic of Elliptic Curves*, Grad. Texts in Math.**106** Springer Verlag, 1985.

[Ta] Tate, J., *The Arithmetic of Elliptic Curves*, Inv. Math. **21** (1974), 179–206.

[We1] Weil, A., *Remarques sur une memoire d'Hermite*, Arch. Math. **5** (1954), 197–202.

[We2] Weil, A., *Euler and the Jacobians of Elliptic Curves*, Arithmetic Geometry (Artin, M. and Tate, J., eds.), vol. I, Birkhäuser, 1983, pp. 353–359.

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307

E-mail address: artin@math.mit.edu

Department of Mathematics, The University of Texas at Austin, 1 University Station, Austin TX 78712-0257

E-mail address: villegas@math.utexas.edu, tate@math.utexas.edu