Appendix 1
by J. Tate
Algebraic Formulas in Arbitrary Characteristic

§1. GENERALIZED WEIERSTRASS FORM

Let K be a field. An **elliptic curve** over K is a connected algebraic curve A smooth and proper over K, of genus 1. An **abelian variety of dimension 1 over** K is the same thing as an elliptic curve A over K furnished with a K-rational point, O. Given such an A, there exist functions x and y on A defined over K such that x (resp. y) has a double (resp. triple) pole at O and no other poles. Moreover, if $\omega \neq 0$ is a given differential of first kind on A and $\omega = dt + \cdots$ is its expansion in terms of a uniformizing parameter at O, one can arrange (by multiplying x and y by constants) that $x = t^{-2} + \cdots$ and $y = -t^{-3} + \cdots$. Then in the projective imbedding defined by $3(O)$ the equation for A is of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.1}$$

with $a_i \in K$. Homogeneity: y is of weight 3, x of weight 2, and the a_i of weight i, meaning that if we replace ω by $u\omega$, then x is replaced by $u^{-2}x$, y by $u^{-3}y$, etc.

If we are given an equation of the form (1.1), we define associated quantities $b_2, b_4, b_6, b_8, c_4, c_6, \Delta$, and j by the following formulas:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \qquad b_4 = a_1a_3 + 2a_4, \qquad b_6 = a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2 \end{aligned} \tag{1.2}$$

$$c_4 = b_2^2 - 24b_4 \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6 \tag{1.3}$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \tag{1.4}$$

$$j = \frac{c_4^3}{\Delta} \qquad \text{(if } \Delta \text{ is invertible).} \tag{1.5}$$

These quantities are related by the identities

$$(1.6) \qquad 4b_8 = b_2b_6 - b_4^2, \qquad \text{and} \qquad 1728\Delta = c_4^3 - c_6^2.$$

If the characteristic is $\neq 2$ or 3 and we put

$$(1.7) \qquad \eta = y + \frac{a_1x + a_3}{2}, \qquad \text{and} \qquad \xi = x + \frac{b_2}{12},$$

then equation (1.1) becomes

$$(1.8) \qquad \eta^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4} = \xi^3 - \frac{c_4}{48}\xi - \frac{c_6}{864}.$$

The relation to the classical Weierstrass theory is given by

$$(1.9) \qquad \begin{matrix} \xi = \wp(u) & c_4 = 12g_2 & \Delta = g_2^3 - 27g_3^2 \\ 2\eta = \wp'(u) & c_6 = 216g_3 & j = 1728J, \end{matrix}$$

and $\omega = \dfrac{d\ddot{\xi}}{2\eta} = du$ (see below).

Some of the first facts to be proved are summarized by the following theorems:

Theorem 1. *The plane cubic curve* (1.1) *is smooth (and hence defines an abelian variety A of dimension one over K with the point O at infinity as origin) if and only if $\Delta \neq 0$, in which case the differential of first kind ω we started with is given by*

$$(1.10) \qquad \omega = \frac{dx}{2y + a_1x + a_3} = \frac{dx}{F_y} = -\frac{dy}{F_x} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y},$$

where

$$(1.11) \qquad F(X, Y) = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6$$

is the equation of the curve.

Theorem 2. *Let A and A' be two abelian varieties of dimension one over K, given by equations of the form* (1.1), *and let j and j' be their "invariants". Then A and A' are isomorphic over some extension field of K if and only if $j = j'$, in which case they are isomorphic over a separable extension of degree dividing* 24, *and indeed of degree* 2, *if $j \neq 0$ or* 1728.

Theorem 3. *For each $j \in K$, there exists an abelian variety A of dimension one over K with invariant j. Indeed if $j \neq 0$ or* 1728, *such as A is given by the equation*

$$(1.12) \qquad y^2 + xy = x^3 - \frac{36}{j - 1728}x - \frac{1}{j - 1728},$$

for which

$$c_4 = c_6 = \frac{j}{j - 1728} \qquad \text{and} \qquad \Delta = \frac{j^2}{(j - 1728)^3}.$$

Theorem 4. *The group of automorphisms of an abelian variety of dimension one is finite, or order dividing* 24, *and if $j \neq 0$ or* 1728, *it is of order* 2, *generated by $x \mapsto x$ and $y \mapsto -y - a_1x - a_3$* (i.e., *by $P \mapsto -P$*).

These theorems, and indeed more precise versions of them than we have bothered to state, can be proved by straightforward computations, once one analyzes the most general allowable coordinate change in (1.1). This is done as follows. Suppose A and A' are abelian varieties of dimension one over K, given by equations $y^2 + a_1xy + \cdots$ and $y'^2 + a_1'x'y' + \cdots$, and suppose $f: A' \xrightarrow{\sim} A$ is an isomorphism defined over K. Then there are elements $u \in K^*$ and $r, s, t \in K$ such that

$$(1.13) \qquad x \circ f = u^2x' + r \qquad y \circ f = u^3y' + su^2x' + t \qquad \omega \circ f = u^{-1}\omega'.$$

The coefficients a_i' are related to the a_i as follows:

$$(1.14) \qquad \begin{aligned} ua_1' &= a_1 + 2s \\ u^2a_2' &= a_2 - sa_1 + 3r - s^2 \\ u^3a_3' &= a_3 + ra_1 + 2t = F_y(r, t) \\ u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st = -F_x(r, t) - sF_y(r, t) \\ u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 = -F(r, t). \end{aligned}$$

For the b_i' we have

$$(1.15) \qquad \begin{aligned} u^2b_2' &= b_2 + 12r \\ u^4b_4' &= b_4 + rb_2 + 6r^2 \\ u^6b_6' &= b_6 + 2rb_4 + r^2b_2 + 4r^3 \\ u^8b_8' &= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4. \end{aligned}$$

For the c_i' and Δ one then finds

$$(1.16) \qquad u^4c_4' = c_4 \qquad u^6c_6' = c_6 \qquad u^{12}\Delta' = \Delta.$$

Hence $j' = j$ is indeed invariant; $j(A)$ depends only on the isomorphism class of A, not on the particular choice of an equation (1.1) defining A'.

§2. CANONICAL FORMS

Let p be the characteristic of our ground field K. The easy case is $\boldsymbol{p \neq 2, 3}$: Then we can always choose coordinates so that A is given by the equation

$$(2.1) \qquad y^2 = x^3 + a_4x + a_6, \qquad \text{with} \qquad \omega = \frac{dx}{2y},$$

and

$$c_4 = -48a_4, \qquad c_6 = -864a_6, \qquad \Delta = -16(4a_4^3 + 27a_6^2). \tag{2.2}$$

Since any curve of the form (1.1) is smooth at the infinite point 0, such a curve is smooth everywhere if and only if the polynomials F, F_x, and F_y have no common zero. In the case of an equation of the form (2.1) with $p \neq 2$, this condition amounts to the non-existence of a common root of the polynomials $G(X) = x^3 + a_4x + a_6$ and $G'(X) = 3x^2 + a_4$, and since $\Delta = 16 \cdot \text{discr. } G(X)$, the condition in this case is just $\Delta \neq 0$, as claimed in Theorem 1.

Let A and A' be given by equations of the form (2.1) with the same invariant $j = j'$. The isomorphisms $f\colon A' \simeq A$ are given simply by

$$x \circ f = u^2x' \qquad y \circ f = u^3y', \tag{2.3}$$

where u is such that $u^4a_4' = a_4$ and $u^6a_6' = a_6$.

Suppose $j \neq 0$, 1728 (i.e. $a_4 \neq 0$, $a_6 \neq 0$). Then A and A' are isomorphic if and only if $a_4a_6'/a_4'a_6$ is a square; the smallest field over which A and A' become isomorphic is the field obtained by adjoining the square root of that quantity to K. The automorphisms of A are given by $u = \pm 1$.

Suppose $j = 1728$ (i.e., $a_6 = 0$). Then A and A' are isomorphic over K if and only if $a_4/a_4' \in (K^*)^4$. The automorphisms of A are given by $u^4 = 1$. A typical curve of this type is given by $y^2 = x^3 - x$.

Suppose $j = 0$ (i.e., $a_4 = 0$). Then $A \cong A'$ over K if and only if $a_6/a_6' \in (K^*)^6$, the automorphisms are given by $u^6 = 1$, and a typical curve is $y^2 = x^3 - 1$.

Now suppose $p = 3$. In this case (and more generally if $p \neq 2$) we can always write A in the form

$$y^2 = x^3 + a_2x^2 + a_4x + a_6 = G(x), \qquad \text{say,} \tag{2.4}$$

$$\omega = -\frac{dx}{y}.$$

Using the fact that $p = 3$, we find

$$\begin{aligned} b_2 &= a_2, \qquad & b_4 &= -a_4, \qquad & b_6 &= a_6, \qquad & b_8 &= -a_4^2 + a_2a_6 \\ c_4 &= a_2^2, & c_6 &= -a_2^3, & \Delta &= a_2^2a_4^2 - a_2^3a_6 - a_4^3. \end{aligned} \tag{2.5}$$

Here again Δ is the discriminant of $G(X)$, up to an invertible factor, so $\Delta \neq 0$ is the condition for smoothness.

Suppose A and A' of form (2.4) with $j = j'$.

Suppose $j \neq 0$ (i.e., $a_2 \neq 0$). Then we can make the term in x disappear, getting the reduced form

$$y^2 = x^3 + a_2x^2 + a_6, \qquad \Delta = -a_2^3a_6, \qquad j = -a_2^3/a_6. \tag{2.6}$$

An isomorphism $f\colon A' \simeq A$ is given by

$$x \circ f = u^2x', \qquad y \circ f = u^3y' \tag{2.7}$$

where $u^2a_2' = a_2$. Hence $A' \simeq A$ if and only if $a_2/a_2' \in (K^*)^2$, and the automorphisms of A correspond to $u = \pm 1$.

Suppose $j = 0$ (i.e., $a_2 = 0$). Reduced form:

$$y^2 = x^3 + a_4x + a_6, \qquad \Delta = -a_4^3, \qquad \omega = \frac{dy}{a_4}. \tag{2.8}$$

Isomorphisms:

$$x \circ f = u^2x' + r, \qquad y \circ f = u^3y' \tag{2.9}$$

with

$$u^4a_4' = a_4, \qquad u^6a_6' = a_6 + ra_4 + r^3.$$

Hence A and A' are isomorphic if and only if $(a_4/a_4') \in (K^*)^4$ and $(a_4/a_4')^{\frac{3}{2}}a_6' - a_6$ is of the form $r^2 + ra_4$. This is always so over a separable extension of degree dividing 12. The automorphisms of A are given by the pairs (u, r) such that:

$$\begin{aligned} &\text{either} \quad r^3 + a_4r = 0 \qquad &&\text{and} \qquad u = \pm 1, \\ &\text{or} \quad r^3 + a_4r + 2a_6 = 0 &&\text{and} \qquad u = \pm i, \end{aligned} \tag{2.10}$$

where $i^2 = -1$. Over the separable closure of K, they form a group of order 12, the twisted product of C_4 (cyclic group of order 4) and C_3 with C_3 the normal subgroup acted on by elements of C_4 in the unique non-trivial way—conjugation of C_3 by a generator of C_4 is the map carrying elements of C_3 into their inverses.

A typical curve of this type is $y^2 = x^3 - x$, the automorphisms being given by $u^4 = 1$, $r^3 - r = 0$ (i.e., $r \in \mathbf{F}_3$) in this case.

Last case, $p = 2$. Here we have $ua_1' = a_1$ (see 1.14) and $c_4 = b_2^2 = a_1^4$ (see (1.2) and (1.3)). Hence we have $j = 0 \Leftrightarrow a_1 = 0$, and separate cases accordingly.

Suppose $a_1 \neq 0$ (i.e., $j \neq 0$). Then choosing suitably r, s, and t, we can achieve $a_1 = 1$, $a_3 = 0$, $a_4 = 0$. Hence A is given by an equation of the form

$$y^2 + xy = x^3 + a_2x^2 + a_6, \qquad \text{with} \quad \omega = \frac{dx}{x}, \tag{2.11}$$

and

$$b_2 = 1, \quad b_4 = b_6 = 0, \quad b_8 = a_6, \quad c_4 = 1, \quad \Delta = a_6, \quad j = \frac{1}{a_6}.$$

$F_x = y + x^2$, and $F_y = x$ have their only common zero at $x = y = 0$, and this is on the curve if and only if $a_6 = \Delta = 0$. Hence $\Delta \neq 0$ is condition for smoothness.

Isomorphisms:

$$x \circ f = x', \qquad y \circ f = y' + sx'$$

with

$$a_2' = a_2 + s^2 - s, \qquad a_6' = a_6. \tag{2.12}$$

Two curves A and A' with the same j are isomorphic if and only if $a_2' - a_2$ is of the form $s^2 - s$, which is true over a separable extension of K of degree $\leqq 2$. The group of automorphisms of A has two elements, corresponding to $s = 0, 1$. A typical curve is $y^2 + xy = x^3 + (1/j)$.

Suppose $a_1 = 0$ (i.e., $j = 0$). Choosing r suitably we can arrange that $a_2 = 0$, so A is given by

$$y^2 + a_3y = x^3 + a_4x + a_6, \qquad \text{with} \quad \omega = \frac{dx}{a_3}, \tag{2.13}$$

and

$$b_2 = b_4 = 0, \qquad b_6 = a_3^2, \qquad b_8 = a_4^2, \qquad \Delta = a_3^4, \qquad j = 0.$$

Since $F_x = x^2 + a_4$ and $F_y = a_3$, the curve is smooth if and only if $a_3 \neq 0$, i.e., $\Delta \neq 0$. Two curves A and A' with the same j are isomorphic if and only if the following equations are soluble in u, s, and t:

$$\begin{aligned} u^3a_3' &= a_3 \\ u^4a_4' &= a_4 + sa_3 + s^4 \\ u^6a_6' &= a_6 + s^2a_4 + ta_3 + s^6 + t^2. \end{aligned} \tag{2.14}$$

This is always so over a separable extension of K of degree $\leqq 24$. A typical curve of this type is

$$y^2 - y = x^3. \tag{2.15}$$

Its group of automorphisms (over the separable closure of K) is of order 24, the elements corresponding to triples (u, s, t) such that

$$u^3 = 1, \quad s^4 + s = 0, \quad \text{and} \quad t^2 + t + s^3 + s^2 = 0.$$

It is isomorphic to the twisted direct product of a cyclic group of order 3 with a quaternion group. The quaternion group is the normal subgroup, and is acted on by the group of order 3 in the obvious way.

§3. EXPANSIONS NEAR O; THE FORMAL GROUP.

Let A be defined by a Weierstrass equation (1.1). Let

$$z = -\frac{x}{y}, \quad w = -\frac{1}{y}, \qquad \text{so} \qquad x = \frac{z}{w}, \quad y = -\frac{1}{w}. \tag{3.1}$$

The equation for A in the affine (z, w)-plane is

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3. \tag{3.2}$$

The point O is given by $(z, w) = (0, 0)$, and z is a local parameter at O. From (3.2) we get the formal expansion

$$\begin{aligned} w = {} & z^3 + a_1z^4 + (a_1^2 + a_2)z^5 + (a_1^3 + 2a_1a_2 + a_3)z^6 + \\ & (a_1^4 + 3a_1^2a_2 + 3a_1a_3 + a_2^2 + a_4)z^7 + \ldots \\ = {} & z^3(1 + A_1z + A_2z^2 + \ldots), \end{aligned} \tag{3.3}$$

where A_n is a polynomial of weight n in the a_i with positive integral coefficients. From (3.3) and (3.1) we get

$$\begin{aligned} x &= z^{-2} - a_1z^{-1} - a_2 - a_3z - (a_4 + a_1a_3)z^2 + \cdots, \\ y &= -z^{-1}x = -z^{-3} + a_1z^{-2} + \cdots, \end{aligned} \tag{3.4}$$

as the formal expansion of x and y. Clearly, the coefficients of these expansions have coefficients in $\mathbf{Z}[a_1, a_2, a_3, a_4, a_6]$. The same is true for the expansion of the invariant differential ω:

$$\omega = H(z)dz \tag{3.5}$$

where $H(z)$ is given by

$$\begin{aligned} H(z) = 1 + a_1z + (a_1^2 + a_2)z^2 & + (a_1^3 + 2a_1a_2 + 2a_3)z^3 \\ & + (a_1^4 + 3a_1^2a_2 + 6a_1a_3 + a_2^2 + 2a_4)z^4 + \ldots \end{aligned}$$

because

$$\begin{aligned} \frac{\omega}{dz} = \frac{dx/dz}{2y + a_1x + a_3} &= \frac{-2z^{-3} + \ldots}{-2z^{-3} + \ldots} \\ = \frac{dy/dz}{3x^2 + 2a_2x + a_4 - a_1y} &= \frac{-3z^{-4} + \ldots}{-3z^{-4} + \ldots} \end{aligned}$$

has coefficients in $\mathbf{Z}[\frac{1}{2}, a_1, \ldots, a_6]$, but also in $\mathbf{Z}[\frac{1}{3}, a_1, \ldots, a_6]$.

Finally, if $P_3 = P_1 + P_2$ and $P_i = (z_i, w_i)$, then we can express $z_3 = F(z_1, z_2)$ as a formal power series in z_1 and z_2, with coefficients in $\mathbf{Z}[a_1, \ldots, a_6]$. The expansion begins

$$\begin{aligned} F(z_1, z_2) = z_1 + z_2 - a_1z_1z_2 & - a_2(z_1^2z_2 + z_1z_2^2) \\ & - 2a_3(z_1^3z_2 + z_1z_2^3) + (a_1a_2 - 3a_3)z_1^2z_2^2 + \ldots. \end{aligned} \tag{3.6}$$

This is the "formal group on one parameter" associated with A.

For each integer $n \geqq 1$ we have, formally,

$$z(nP) = \psi_n(z(P)), \tag{3.7}$$

where the series ψ_n are defined inductively by

$$\psi_1(z) = z, \qquad \psi_{n+1}(z) = F(z, \psi_n(z)). \tag{3.8}$$

For example, we have

$$(3.9)\quad \psi_2(z) = 2z - a_1z^2 - 2a_2z^3 + (a_1a_2 - 7a_3)z^4 + \cdots$$

and

$$(3.10)\quad \psi_3(z) = 3z - 3a_1z^2 + (a_1 - 8a_2)z^3 + 3(4a_1a_2 - 13a_3)z^4 + \cdots.$$

In characteristic $p > 0$, the series ψ_p is of the form

$$\psi_p(z) = c_1z^{p^h} + c_2z^{2p^h} + c_3z^{3p^h} + \dots$$

with $c_1 \neq 0$, where h is an integer equal to 1 or 2, because the isogeny

$$p\delta : A \to A$$

is of degree p^2, and is not separable. This means that $z \circ p\delta$ lies in the inseparable subfield of degree p or p^2 of the function field of A, whence our assertion follows.

EXERCISE

Let $p = \operatorname{char}(K)$ be arbitrary, let $j \in K$ with $j \neq 0$ or 1728, and let A_j denote the abelian variety of dimension 1 over K given by the equation (1.12), i.e.,

$$y^2 + xy = x^3 - \frac{36}{j - 1728}x - \frac{1}{j - 1728}.$$

Show that for each separable quadratic extension L of K there exists an abelian variety $A_{j,L}$ of dimension one over K such that $A_{j,L}$ is isomorphic to A_j over L, but not over K, and $A_{j,L}$ is uniquely determined up to isomorphism by j and L. Show also that (denoting by $A(K)$ the group of points on A rational over K) we have

$$A_{j,L}(K) = \{P \in A_j(L) | \sigma P = -P\},$$

where σ is the non-trivial automorphism of L/K, (and where

$$-P = (x, -y - a_1x - a_3) \quad \text{if} \quad P = (x, y)).$$

Appendix 2
The Trace of Frobenius and the Differential of First Kind

§1. THE TRACE OF FROBENIUS

Theorem 1. *Let A be an elliptic curve defined over the prime field $\mathbf{F}_p$ of characteristic p, let t be a local parameter at the origin in the function field $\mathbf{F}_p(A)$. Let ω be a differential of first kind in $\mathbf{F}_p(A)$, with expansion*

$$\omega = \sum_{\nu=1}^{\infty} c_\nu t^\nu \frac{dt}{t}$$

normalized such that $c_1 = 1$. Let $\pi = \pi_p$ be the Frobenius endomorphism of A. Then

$$\omega \circ \pi' = c_p\omega, \quad \text{and} \quad t\circ(p\delta) \equiv c_pt^p \,(\operatorname{mod} t^{2p}).$$

Proof. We lift an equation for the elliptic curve to the integers. Thus it is useful to write $\bar{A}$ for the curve in characteristic p, and A for its lifting. We do this in a naive way, by lifting the coefficients in a Weierstrass equation if $p \neq 2, 3$, or in a normalized equation otherwise. We let $\bar{t}$ be the parameter at the origin $\bar{O}$, and let t be a parameter at the origin O of A, reducing to $\bar{t}$. Then

$$\bar{\omega} = \sum_{\nu=1}^{\infty} \bar{c}_\nu \bar{t}^\nu \frac{d\bar{t}}{\bar{t}},$$

and the differential form ω on A has the expansion

$$\omega = \sum_{\nu=1}^{\infty} c_\nu t^\nu \frac{dt}{t} = h(t)dt$$

with $c_1 \equiv 1 \,(\operatorname{mod} p)$.