ALGORITHM FOR DETERMINING THE TYPE OF A SINGULAR FIBER IN AN ELLIPTIC PENCIL.(*)

by J. TATE(**)

CONTENTS

(*) This is a slightly edited version of a letter to Cassels.
(**) Tate's absence from the conference was in protest against the large scale support of basic scientific research by military organizations rather than by agencies whose aims and spirit he thinks are more compatible with those of scientific inquiry.

0.- SUMMARY.

$\mathcal{O}$ is a complete discrete valuation ring with perfect residue field $\mathcal{O}/(\pi)$

(*) $$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \qquad a_i \in \mathcal{O}$$

is an equation for an elliptic curve over the field of fractions of $\mathcal{O}$.

The quantities b_2 , b_4 , b_6 , b_8 , c_4 , c_6 and Δ are as in the "Formulaire" (this volume). Kodaira's symbols are used to denote the type of fiber over the maximal unramified extension of $\mathcal{O}$.

1) Assume $a_i \in \mathcal{O}$. Then $\Delta \not\equiv 0 \Rightarrow$ type I_o , i.e. good reduction.

2) Assume $\pi|\Delta$, and change coordinates so that $\pi|a_3$, a_4 and a_6 . Then $b_2 \not\equiv 0 \Rightarrow$ type I_ν for some $\nu > 0$. Conductor is π , and the multiplicative group is twisted by the root field of the congruence $T^2 + a_1T-a_2 \equiv 0$.

3) Assume also $\pi|b_2$. Then $\pi^2\nmid a_6 \Rightarrow$ type II. Conductor is $\pi^{\mathrm{ord}\,\Delta}$.

4) Assume also $\pi^2|a_6$ (which implies $\pi^2|b_6$ and b_8) . Then $\pi^3\nmid b_8 \Rightarrow$ type III. Conductor is $\pi^{\mathrm{ord}\,\Delta-1}$.

5) Assume also $\pi^3|b_8$ (which implies $\pi^2|b_4$) . Then $\pi^3\nmid b_6 \Rightarrow$ type IV. Conductor is $\pi^{\mathrm{ord}\,\Delta-2}$.

6) Assume also $\pi^3|b_6$. Then it is possible to change coordinates so that also $\pi|a_1$, $\pi^2|a_3$, $\pi|a_2$, $\pi^2|a_4$ and $\pi^3|a_6$. This being done, consider the polynomial $P(T) = T^3 + a_2\pi^{-1}T^2 + a_4\pi^{-2}T + a_6\pi^{-3}$.

Then : (6.1) P(T) has distincts roots $\Rightarrow$ type I_o^* , conductor is $\pi^{\text{ord}\,\Delta-4}$

(6.2) P(T) has one simple root, one double root $\Rightarrow$ type I_ν^* , with some $\nu > 0$

(6.3) P(T) has one triple root $\Rightarrow$ either type II^*, type III^*,or type IV^*, <u>or</u> the original equation was not a "minimal" one.

In case (6.2) the value of ν , and hence the conductor, can be determined from the order of j (which is < 0) except in case $\pi|2$.In case $\pi|2$ there is a simple algorithm, to the routine method of searching for the solutions $x, y \in (\pi)$ of the equation (*) , by successively selving congruences mod π , which (conjecturally) gives ν .

In case (6.3), the same type of algorithm leads in just three steps to a determination of which of the three types, <u>or</u> to a new equation of type (*), with a new $\Delta = \pi^{-12}$ old Δ . (This is also conjectural, but almost certain). Explanation follows later, perhaps-anyway, it must be all in Néron.

The "conductor" is here that given by Ogg's formula : $\pi^{\text{ord}\,\Delta+1-n}$, where n=number of components of fiber.

1.- GENERALISED WEIERSTRASS FORM.

Let E be an elliptic curve defined over a field K with a K-rational point 0 . In the projective embedding defined by 3.0 the curve can be written in the form

(1.1) $$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad a_i \in K$$

put

(1.2) $$\begin{cases} b_2 = a_1^2 + 4a_2 \\ b_4 = a_1\, a_3 + 2a_4 \\ b_6 = a_3^2 + 4a_6 \\ b_8 = a_1^2\, a_6 - a_1\, a_3\, a_4 + 4a_2\, a_6 + a_2\, a_3^2 - a_4^2 \\ c_4 = b_2^2 - 24b_4 \\ c_6 = -b_2^3 + 36b_2\, b_4 - 216b_6 \\ \Delta = -b_2^2\, b_8 - 8b_4^3 - 27b_6^2 + 9b_2\, b_4\, b_6 \neq 0 \\ j = c_4^3\, /\Delta \end{cases}$$

These quantities are related by

(1.3) $$4b_8 = b_2\, b_6 - b_4^2 \qquad 1728\,\Delta = c_4^3 - c_6^2 .$$

A differential of first kind is given by

(1.4) $$\omega = \frac{dx}{2y + a_1\, x + a_3} = \frac{dx}{F'_y\,(x,y)} = \frac{-dy}{F'_x\,(x,y)} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}$$

where we have put

$$(1.5) \qquad F(X,Y) = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6 \quad .$$

Putting

$$(1.6) \qquad \eta = y + \frac{a_1x + a_3}{2} \qquad\qquad \xi = x + \frac{b_2}{12} \quad ,$$

the equation (1.1) becomes

$$(1.7) \qquad \eta^2 = x^3 + (b_2/4)x^2 + (b_4/2)x + (b_6/4) = \xi^3 - (c_4/48)\xi - (c_6/864) \quad .$$

Then the relation with Weierstrass is given by

$$(1.8) \qquad \begin{cases} \xi = \wp(u) & c_4 = 12g_2 \\ 2\eta = \wp'(u) & c_6 = 216g_3 \end{cases} \qquad \omega = \frac{d\xi}{2\eta} = du \; .$$

2.- CHANGE OF COORDINATES.

Suppose $E' : y'^2 + a'_1\, x'\, y' + \ldots$ is another curve of the same as E, and $f : E' \sim E$ an isomorphism carrying $0'$ into 0. Then there are r, s, t and $u \neq 0$ in K such that

$$(2.1) \qquad \begin{cases} x o f = u^2x' + r \\ y o f = u^3y' + su^2x' + t \end{cases} \qquad \omega o f = u^{-1}\omega' \quad .$$

The coefficients a_i' are related to the a_i and the b_i' to the b_i by the formulas:

$$
(2.2)\qquad
\begin{cases}
u\, a_1' = a_1 + 2s \\
u^2 a_2' = a_2 - sa_1 + 3r - s^2 \\
u^3 a_3' = a_3 + ra_1 + 2t = F_y(r,t) \\
u^4 a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st = -F_x(r,t) - sF_y(r,t) \\
u^6 a_6' = a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1 = -F(r,t) \\
u^8 b_8' = b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4 \\
u^6 b_6' = b_6 + 2rb_4 + r^2 b_2 + 4r^3 \\
u^4 b_4' = b_4 + rb_2 + 6r^2 \\
u^2 b_2' = b_2 + 12r
\end{cases}
$$

From these we check that :

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

<u>Example</u> :"generic E" . The equation

$$
(2.4)\qquad y^2 + xy = x^3 - (36/_{j-1728})x - (1/_{j-1728}) \quad ,
$$

has

$$
c_4 = c_6 = j/_{j-1728} \quad \text{and} \quad \Delta = j^2/_{(j-1728)^3} \quad .
$$

Hence for $j \neq 0, 1728$ it gives a curve with "invariant" j .

Using the formulas above, it is easy to show that j can be arbitrary in K, and that for K algebraically closed, two E's with the same j are isomorphic. It is also easy to compute the group of automorphisms (but not, also, the ring of endomorphisms). See the "Formulaire" (this volume) for the details.

3.- THE "MINIMAL" WEIERSTRASS EQUATIONS OVER A VALUATION RING.

Let v be a discrete valuation of K, with valuation ring R, prime ideal π, and resudue field $k = R/(\pi)$. Let E be an elliptic curve over K, with a K-rational point 0.

Definition 3.1

An equation for E of the form (1.1) is _minimal_ (with respect to v) if $v(a_i) \geq 0$ for all i and if $v(\Delta)$ is minimal, subject to that condition.

Theorem 3.2

A minimal equation for E _exists, and is unique up to a change of coordinates of the form_ (2.1) _with_ $r,s,t \in R$ _and_ u _inversible in_ R.

Existence is obvious. Let $y'^2 + a_1' x' y' + \ldots$ and $y^2 + a_1 xy + \ldots$ be two minimal equations for the same E. Since $\Delta \neq 0$ and $v(\Delta') = v(\Delta)$ we conclude from (2.3) that $v(u) = 0$. Now from the transformation of b_8 and b_6 in (2.2) we see that $3r \in R$ and $4r \in R$, hence $r \in R$. Now the transformation of a_2 shows that $s \in R$, and that of a_6 shows that $t \in R$.

Corollary 3.3

The differential ω associated with a minimal Weierstrass form is unique up to a unit of R .

Remarks :

1) If $a_i \in R$ and $v(\Delta) < 12$, then the equation (1.1) is automatically minimal. The converse is true if $j \in R$ and $p = \text{char } k \neq 2,3$. A complete algorithm for reducing to minimal form in all cases is given below.

2) Let M be a collection of discrete valuations of K . For each $v \in M$, let $y_v^2 + a_{1,v} x_v y_v + \dots$ be a minimal equation for E relative to v , with corresponding differential ω_v and discriminant Δ_v . Then the "divisor" $\mathfrak{D}_E = \sum_{v \in M} v(\Delta_v).v$ should be regarded as the discriminant of E . Let $F(x,y) = y^2 + a_1 xy + \dots$ be an arbitrary Weierstrass equation for E over K , and let ω_F and Δ_F be the corresponding differential and discriminant. Then the class of the divisor $\mathfrak{A}_F = \sum_v v(\omega/\omega_v).v$ is independent of F , and we have $12\mathfrak{A}_F \sim \mathfrak{D}_E$.

3) In case M is the set of valuations associated with a principal ideal domain D with field of fractions K , then it is easy to see that we can find one equation F which is simultaneously minimal for all v , so that $\mathfrak{A}_F = 0$, and $\mathfrak{D} = (\Delta_F)$.

4) If $j \in R$, then Δ divides c_4^3 and c_6^2 : $c_4^3 = \Delta . j$ and $c_6^2 = \Delta .(j-1728)$. From (1.7), we see that if $48\pi^4 | c_4$ and $864\pi^6 | c_6$, then the equation is not minimal. We have $48 = 2^4.3$ and $864 = 2^5.3^3$. Hence, if $j \in R$ and the equation is minimal, we have

$$v(\Delta) < 12 + 12\, v(2) + 6\, v(3) \quad .$$

4.- THE CANONICAL FILTRATION ON THE GROUP OF v-ADIC POINTS.

Let $F(x,y) = y^2 + a_1 xy + \ldots$ be a minimal equation for E relative to a valuation v. Let $F(x,y)$ be the reduction of F (mod π) and let $\tilde{E}$ denote the plane cubic $\tilde{F} = 0$ defined over the residue field k. By Theorem 3.2, $\tilde{E}$ is uniquely determined by E up to a projective transformation of the form (2.1) over k. Let $\tilde{E}_o$ denote the smooth part of $\tilde{E}$. Then $\tilde{E}_o$ is an algebraic group with origin $\tilde{0}$. (If $\tilde{E}$ is non singular, then $\tilde{E}_o = \tilde{E}$ is an elliptic curve ; if $\tilde{E}$ has a node α, then $\tilde{E}_o \approx \mathbb{P}^1$ -(two points) is a multiplicative group ; and if $\tilde{E}$ has a cusp : $\prec$, then $\tilde{E}_o \approx \mathbb{P}^1$ -(one point) is an additive group ; here we have ignored questions of rationality, but if k is perfect, so that the singularity of $\tilde{E}$ is rational over k, then the analysis is the same, except that in case of a node, $\tilde{E}_o$ is a multiplicative group "twisted" by the quadratic extension obtained by adjoining to k the two tangents at the node).

Let $E(K)$ denote the group of points on E rational over K, and let $\rho : E(K) \longrightarrow \tilde{E}(K)$ denote the reduction map (defined naively in terms of the given projective coordinates - by Theorem 3.2 it is independent of the coordinates). Let $E_o(K) = \rho^{-1}(\tilde{E}_o(K))$ be the set of points whose reduction is non singular.

Theorem 4.1

$E_o(K)$ is a subgroup of finite index in $E(K)$, and $\rho_o : E_o(K) \longrightarrow \tilde{E}_o(K)$ is a homomorphism of groups.

A straightforward but tedious proof can be given, using the addition formulae, for everything except the "finite index". That finiteness depends on the minimality of the equation ; and a proof of finiteness is implicit in the algorithm for reducing to minimal form given below.

We denote the kernel of ρ_o by $E_1(K)$, it consist of the points $P = (x,y)$ in $E(K)$ such that $v(x) < 0$ and $v(y) < 0$. Clearly, from (1.1), since $v(a_i) \geq 0$, we have $v(x) < 0 \Leftrightarrow v(y) < 0$, in which case $v(x) = -2m$ and $v(y) = -3m$ for some m . For each $m \geq 1$ we let

$$E_m(K) = \{(x,y) \in E(K) \mid v(x) \leq -2m \text{ and } v(y) \leq -3m\}$$, (understanding of course that $0 \in E_m(K)$ for all m).

Theorem 4.2

Let $z = -x/y$. Then z is a uniformising parameter at 0 . The expansions.

$$(4.3) \begin{cases} x = z^{-2} - a_1 z^{-1} - a_2 - a_3 z - (a_4 + a_1 a_3) z^2 - \dots \\ y = -z^{-1} x = -z^{-3} + a_1 z^{-2} + a_2 z^{-1} + a_3 + (a_4 + a_1 a_3) z + \dots \\ \omega = dz(1 + a_1 z + (a_1^2 + a_2) z^2 + (a_1^3 + 2a_1 a_2 + a_3) z^3 + (a_1^4 + 3a_1^2 a_2 + 6a_1 a_3 + \\ \quad + a_2^2 + 2a_4) z^4 + \dots \end{cases}$$

have coefficients in R . So also does the formal group law $\Phi(Z_1, Z_2) = Z_1 + Z_2 + \dots$ defined by the equation $z(P + Q) = \Phi(z(P), z(Q))$. If R is complete, then the map $z \longmapsto (x(z), y(z))$, for $z \in (\pi)$ gives an isomorphism of $(\pi)_\Phi$ (the prime ideal endowed with group structure via Φ) onto $E_1(K)$, under which the subgroups $(\pi^m)_\Phi$ correspond to $E_m(K)$ for all $m \geq 1$.

The proof is straightforward. Let $z = -x/y$, $w = -1/y$, so that $x = z/w$ and $y = -1/w$. Then in terms of w and z the equation for E is

$$(4.4) \qquad w(1 - a_1 z - a_3 w) = z^3 + a_2 z^2 w + a_4 z w^2 + a_6 w^3 \quad .$$

This shows that we have

$$(4.5)\quad \begin{cases} w = z^3 + a_1 z^4 + (a_1^2 + a_2)z^5 + (a_1^3 + 2a_1a_2 + a_3)z^6 + \\ \quad + (a_1^4 + 3a_1^2a_2 + 3a_1a_3 + a_2^2 + a_4)z^7 + \ldots \\ w = z^3 + A_1 z^4 + A_2 z^5 + \ldots \end{cases}$$

where A_ν is a polynomial of weight ν in the a_i with positive integral coefficients. Hence the expansions of $y = -1/w$ and $x = -zy$ in terms of z have coefficients in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$.

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

has coefficients in $\mathbb{Z}[1/2, a_1, \ldots, a_6]$ but also in $\mathbb{Z}[1/3, a_1, \ldots, a_6]$, hence in $\mathbb{Z}[a_1,\ldots, a_6]$. As for the group law, if z_1 and $z_2 \in (\pi)$, then the line joining the points (z_1, w_1), (z_2,w_2) in the (z, w)-plane has slope $\in (\pi)^2$, because

$$\frac{w_2 - w_1}{z_2 - z_1} = \frac{z_2^3 - z_1^3}{z_2 - z_1} + A_1 \frac{z_2^4 - z_1^4}{z_2 - z_1} + \ldots$$ with A_i as above in (4.5).

Call this slope $\lambda = \lambda(z_1, z_2) = z_2^2 + z_1z_2 + z_1^2 + A_1(z_2^3+z_2^2z_1+z_1z_2^2+z_1^3)+\ldots$ Put $\nu = \nu(z_1,z_2) = w_i - \lambda z_i$ $(i = 1,2)$. Substituing $w = \lambda(z_1,z_2)z + \nu(z_1,z_2)$ in (4.4 we find a cubic in z with roots w_1 and w_2. Looking at the sum of the roots, one sees that the third root z_3 is expressed as a power series in z_1,z_2 with coefficients in R. In fact,

$$(4.6)\qquad z_1 + z_2 + z_3 = \frac{a_1\lambda + a_3\lambda^2 - a_2\nu - 2a_4\lambda\nu - 3a_6\lambda^2\nu}{1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3}.$$

Thus we have the "canonical filtration"

$$(4.7)\qquad E(K) \supset E_o(K) \supset E_1(K) \supset E_2(K) \supset \ldots \supset (0) = \bigcap_{m=1}^{\infty} E_m(K)$$

with quotients

$$E(K)/E_o(K) \text{ finite}, \quad E_o/E_1 \hookrightarrow \tilde{E}_o(K), \text{ and } E_m/E_{m+1} \hookrightarrow k^+ \text{ for } m \geq 1.$$

Of course the conclusions $\hookrightarrow$ are bijections $\xrightarrow{\sim}$ if R is complete.

5.- APPLICATION: THE RELATION BETWEEN $L_v(1)$ AND $\int_{E_v} |\omega_v|$ IN CASE k FINITE.

Suppose now R is complete and k is finite with q = Card k . On K we agree to use the additive Haar mesure with respect to which R has mesure 1 . This being agreed, a differential ω on E gives us a mesure $|\omega|$ on E(K) in the usual manner.

Corollary 5.1 (of Theorem 4.2) $\int_{E_1(K)} |\omega| = 1/q$, if ω is a differential of first kind on E coming from a "minimal equation".

Indeed, by (4.2) we have $\int_{E_1(K)} |\omega| = \int_{(\pi)} |dz| = \dfrac{\int_R |dz|}{(R:(\pi))} = 1/q$.

The local factor occuring in the Euler product with a good functional equation should be (Serre tells me) as follows, in which $N_v = \text{Card}\,(\tilde{E}_o(K))$.

(5.2) $L_v(s) = \begin{cases} \dfrac{1}{1-(q+1-N_v)q^{-s}+q^{1-2s}} & \text{, if } \tilde{E} \text{ is non-singular} \\ \dfrac{1}{1-q^{-s}} & \text{, if } \tilde{E} \text{ has a node with two tangents rational over } k \text{ (in which case } N_v = q-1 \text{ and } \tilde{E}_o \text{ is the multiplicative group).} \\ \dfrac{1}{1+q^{-s}} & \text{, if } \tilde{E} \text{ has a node with irrational tangents (in which case } N_v = q+1 \text{, and } \tilde{E}_o \text{ is the twisted multiplicative group).} \\ 1 & \text{, if } \tilde{E} \text{ has a cusp (in which case } N_v = q \text{ and } \tilde{E}_o \text{ is the additive group) .} \end{cases}$

In all cases therefore, $L_v(1) = q/N_v$. Since $N_v = (E_o(K) : E_1(K))$ it follows from corollary 5.1 that we have $\int_{E_o(K)} |\omega| = (L_v(1))^{-1}$, because $|\omega|$ is invariant under translation. Finally then,

Theorem 5.2

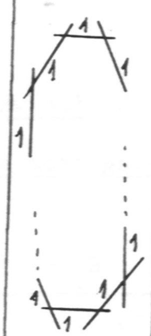
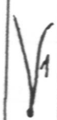
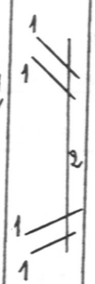
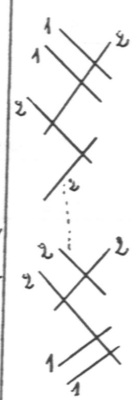
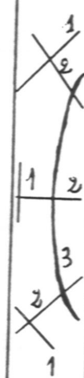
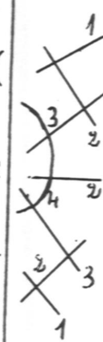
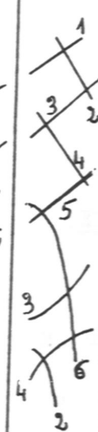
If we use the measure on K for which R gets measure 1 , and use a differential of first kind ω coming from a minimal equation then

$$\int_{E(K)} |\omega| = \frac{(E(K) : E_o(K))}{L_v(1)} \qquad (5.3)$$

In other words, the "fudge factors" of Birch and Swinnerton-Dyer are just the indices $(E(K):E_o(K))$

6. - THE NERON MINIMUM MODEL.

Suppose k algebraically closed. One can find a regular sheme X over R such that $X \times_R K \approx E$ and such that X is "minimal" relative to the map $X \to \operatorname{Spec} R$ (i.e. such that that map cannot be factored $X \to X' \to \operatorname{Spec} R$ in such a way that $X \times_R K \xrightarrow{\sim} X' \times_R K$ is an isomorphism). Such an X is unique up to isomorphism. Its fiber $\tilde{X} = X \times_R k$ is one of the following types :

Koraira symbol	I_o	$I_\nu (\nu > 0)$	II	III	IV	I_o^*	$I_\nu^* (\nu > 0)$	IV*	III*	II*
Néron symbol	A	B_ν	C_1	C_2	C_3	C_4	$C_{5,\nu}$	C_6	C_7	C_8
Picture (the numbers indicate multiplicities)										
n = number of irred. components	1	ν	1	2	3	5	$5+\nu$	7	8	9
type of group $E(K)/E_o(K) \approx \tilde{X}_o(k)/\tilde{E}_o(k)$	(1)	(ν)	(1)	(2)	(3)	(2×2)	(4) ν odd ---- (2×2) ν even	(3)	(2)	(1)
$\tilde{E}_o(k) \approx E_o(K)/E_1(K)$	$\tilde{E}(k)$	k^*	k^+	k^+	k^+	k^+	k^+	k^+	k^+	k^+
BELOW THIS LINE THINGS ARE VALID ONLY FOR CHAR(k) $\neq$ 2,3										
$v(\Delta_v)$	0	ν	2	3	4	6	$6+\nu$	8	9	10
$v(\Delta_v)+1-n = f$ =exp. of π in conductor	0	1	2	2	2	2	2	2	2	2
behavior of j	$v(j) \geq 0$	$v(j) = -\nu$	$\tilde{j}=0$	$\tilde{j}=1728$	$\tilde{j}=0$	$v(j) \geq 0$	$v(j) = -\nu$	$\tilde{j}=0$	$\tilde{j}=1728$	$\tilde{j}=0$

Here $\tilde{X}_0$ denotes the non-singular part of the fiber. This is a (non connected in general) algebraic group over k, whose connected component is $\tilde{E}_o$. We have $E(K)/E_1(K) \approx \tilde{X}_o(k)$, the isomorphism induced by the reduction map, and assuming now R complete. Note that if $p = \text{char } k \neq 2,3$, then we have : minimality $\Leftrightarrow$ either $v(\Delta) < 12$, or $v(\Delta)+v(j) < 12$. Also if $p \neq 2,3$, and $f = 2$, then $E_o(K)$ is uniquely divisible by 2 and 3, while $E(K)/E_o(K)$ is killed by 12, hence $E(K)/E_o(K)$ is isomorphic to the group of points in $E(K)$ which are killed by 12 in this case.

7.- ALGORITHM FOR ANALYSING SINGULAR FIBERS (first five cases).

We assume now that our valuation ring R is complete, with perfect residue field k. In connection with various conjectures, it is well to be able to compute effectively various invariants of an elliptic curve E over K, to wit

The conductor $f_E = \pi^f$, where $f = v(\Delta) + 1 - n$, n being the number of components of $\widetilde{X}$ over $\bar{k}$.

The group $E(K)/E_o(K)$, whose order we denote by c

The group $\widetilde{E}_o(K)$.

To compute these it is necessary to analyse the singular fiber $\widetilde{X}$ à la Néron, at least when $p = \text{char } k = 2$ or 3 (if $p \neq 2$ or 3, everything can be read off the table 6., if one notes the remarks at the end of 6., however the algorithm below applies in all cases). When we refer to the "type" we mean the type of the singular fiber $\widetilde{X}$ over the algebraic closure $\bar{k}$ of k, which is designated by one of the 10 Kodaira symbols.

To begin with, we simply assume an equation of the form (1.1) with coefficients $\boxed{a_i \in R}$; we do not assume it minimal. If it is not minimal, our algorithm will lead us to a minimalization of it. As we go along we make more and more assumptions. These are cumulative, and are $\boxed{\text{boxed}}$ for clarity. We include only brief remarks on proofs.

1) $\pi \nmid \Delta \Rightarrow$ type I_o, $f = 0$, $c = 1$, $\widetilde{E}$ elliptic.

2) Assume $\boxed{\pi \mid \Delta}$. Then we can change of coordinates so that $\boxed{\pi \mid a_3, a_4 \text{ and } a_6}$. Do so. Then $\pi \nmid b_2 \Rightarrow$ type I_ν, with $\nu = v(\Delta)$.

Let k' be the splitting field over k of the congruence $T^2+a_1T - a_2= 0$.

2a) $k' = k$: $f = 1$, $c = v(\Delta)$, $\tilde{E}_o(k) \approx k^*$

2b) $k' \neq k$: $f = 1$, $c = 1$ if $v(\Delta)$ is odd and 2 if $v(\Delta)$ is even,
$\tilde{E}_o(k)$ is $\approx$ the group of elements of k' whose norm to k is 1.

Proof : This case (2) is the one in which E can be described by θ-functions, possibly twisted by an unramified extension. Every thing clear from that point of view.

From now on, E has a cusp and $\tilde{E}_o = k^+$.

3) Assume $\boxed{\pi \mid b_2}$. Then $\pi^2 \nmid a_6 \Rightarrow$ type II, and $f = v(\Delta)$, $c = 1$,
$\tilde{E}_o(k) = k^+$.

Proof : Consider the 2-dimensional local ring $A = R[x,y]_m$ where $m = (\pi,x,y)$. It is regular because $a_6 \in (x,y) \Rightarrow m = (x,y)$. Hence Weierstrass model = Néron model.

4) Assume $\boxed{\pi^2 \mid a_6}$ (which implies $\pi^2 | b_6$ and b_8) . Then $\pi^3 \nmid b_8 \Rightarrow$ type III, and $f = v(\Delta)-1$, $c = 2$, $\tilde{E}_o(k) = k^+$.

Proof : Let $a_i = \pi^m a_{i,m}$ $x = \pi^m x_m$, $y = \pi^m y_m$, etc... Our equation can be written

(7.1) $$y_1^2 + a_{1,0}\, x_1 y_1 + a_{3,1} y_1 = \pi x_1^3 + a_{2,0} x_1^2 + a_{4,1} x_1 + a_{6,2} .$$

The singular point on the fiber (whose local ring was A) blows up into the conic

(*) $$Y^2 + a_{1,0}XY + a_{3,1}Y = a_{2,0}X^2 + a_{4,1}X + a_{6,2} ,$$

$\Rightarrow (y - \alpha x + \beta)^2 = 0$

whose discriminant is $b_8\pi^{-2} = b_{8,2}$.

5) Assume $\boxed{\pi^3 | b_8}$ (which implies $\pi^2 | b_4$) . Then $\pi^3 \nmid b_6 \Rightarrow$ type IV, and $f = v(\Delta) - 2$, $c = 3$ if $T^2 + a_{3,1}T - a_{6,2} \equiv 0$ has roots in k and 1 if it has not roots in k , $\widetilde{E}_o(k) = k^+$.

<u>Proof</u> : The conic (*) becomes $T^2 + a_{3,1}T - a_{6,2} \equiv 0$, where $T = Y - \alpha X$ is defined by $(Y - \alpha X)^2 = Y^2 + a_1XY - a_2X^2$. The discriminant of $T^2 + a_{3,1}T - a_{6,2}$ is $\pi^{-2} b_6 = b_{6,2}$, so that if $\pi^3 \nmid b_6$, then our conic degenerate into two <u>distinct</u> lines. Dividing (7.1) by X_1^3 , we get an equation of the form $F(u,v) = \pi$, where F is a cubic with coefficients in R which, mod π , factors into three distincts linear factors, $F \equiv L_1L_2L_3 \pmod{\pi}$, such that the congruences $L_i \equiv 0$ have a point in common. The local ring of that point is easily seen to be regular (the maximal ideal is generated by any two of the three factors L_i). Thus (7.1) gives a regular scheme over R with fiber * consisting of the three lines $L_i \equiv 0$, $i = 1,2,3$ meeting in a point. Concerning the value of c , we see that c is equal to the number of these lines which are rational over k . One of them is, and the others are given by $T^2 + a_{3,1}T - a_{6,2} \equiv 0$.

8.- <u>ALGORITHM CONTINUED (the last five cases)</u>.

Assume now that $\boxed{\pi^3 | b_6}$. Then we can change coordinates so that $\boxed{\pi | a_1 \text{ and } a_2 ,\ \pi^2 | a_3 \text{ and } a_4 ,\ \text{and } \pi^3 | a_6}$. This being done, consider the polynomial

(8.1) $$P(T) = T^3 + a_{2,1}T^2 + a_{4,2}T + a_{6,3} ,$$

where the notation is a explained in the proof of step 4) . Our equation now becomes

(8.2) $$\pi y_2^2 + \pi a_{1,1}x_1y_2 + \pi a_{3,2}y_2 = P(x_1) ,$$

and our algorithm has three branches, according to the multiplicities of the roots of the congruence $P(T) \equiv 0$.

<u>First Branch</u> : 6) If $P(T) \equiv 0$ has three distinct roots, then we have type I_o^* , and $f = v(\Delta) - 4$ and $c = 1 +$ (number of roots of $P(T) = 0$ in k).

<u>Second Branch</u> : 7) If $P(T) = 0$ has one simple and one double root, then Type I_ν^* , $\nu > 0$, and $f = v(\Delta) - 4 - \nu$, $c = 2$ or 4 , where ν and c are obtained by the following procedure :

<u>Subprocedure Branch 7)</u> . Translate x , so that $T \equiv 0$ is a double root of $P(T) \equiv 0$. Then $\pi^3 | a_4, \pi^4 | a_6, \pi^2 \nmid a_2$ and (8.2) becomes

$$(7.1) \quad y_2^2 + \pi a_{1,1} x_2 y_2 + a_{3,2} y_2 = \pi^2 x_2^3 + \pi a_{2,1} x_2^2 + \pi a_{4,3} x_2 + a_{6,4}$$

If $Y^2 + a_{3,2} Y - a_{6,4} \equiv 0$ has distinct roots, then

$\nu = 1$, and $c = 4$ if roots in k,2 if not.

If $Y^2 + a_{3,2} Y - a_{6,4} \equiv 0$ has a double root we can translate y so that the root is $Y \equiv 0$. Then

$\pi^3 \mid a_3, \pi^5 | a_6$, and our equation becomes

$$(7.2) \quad \pi y_3^2 + \pi a_{1,1} x_2 y_3 + \pi a_{3,3} y_3 = \pi x_2^3 + a_{2,1} x_2^2 + a_{4,3} x_2 + a_{6,5}$$

If $a_{2,1} X^2 + a_{4,3} X + a_{6,5} \equiv 0$ has distinct roots then

$\nu = 2$, and $c = 4$ if roots in k , 2 otherwise.

If $a_{2,1}X^2 + a_{4,3}X + a_{6,5} \equiv 0$ has a double root, then we can translate x so that the root is $X \equiv 0$, so that $\pi^1|a_4$ and $\pi^6|a_6$. Equation is now

$$(7.3) \quad y_3^2 + \pi a_{1,1}x_3y_3 + a_{3,3}y_3 + a_{3,3}y_3 = \pi^3x_3^3 + \pi^2a_{2,1}x_3^2 + \pi^2a_{4,4}x_3 + a_{6,6}$$

If $Y^2 + a_{3,3}Y - a_{6,6} = 0$ has distinct roots, then

$\nu = 3$, and $c = 4$ if roots in k, 2 otherwise.

If otherwise.... etc. Keep going until the quadratic congruence which appears has distinct root. The process terminates, because the coefficients a_3, a_4 and a_6 are being made more and more highly divisible by π. Hence also b_4, b_6 and b_8, hence also Δ. But Δ is fixed under all change of coordinates (translations involved). A crude estimate gives $\nu = \text{ord}\,\Delta - 3$ if I'm not mistaken.

Branch 3 begins : 8) Suppose now $P(T) = 0$ has a triple root. We may assume the root is $T = 0$, so $\boxed{\pi^2|a_2, \pi^3|a_4, \text{ and } \pi^4|a_6}$. The equation is

$$(8.1) \quad y_2^2+\pi a_{1,1}x_2y_2+a_{3,3}y_2 = \pi^2x_2^3+\pi^2a_{2,2}x_2^2+\pi a_{4,3}x_2+a_{6,4} .$$

If $Y^2 + a_{3,2}Y - a_{6,4} \equiv 0$ has distinct roots, then type IV^* and $f = v(\Delta)-6$, $c = 3$ if roots are in k, 1 otherwise.

Branch 3 continues : 9) Suppose $Y^2 + a_{3,2}Y - a_{6,4} \equiv 0$ has a double root. Then we can assume it is $Y \equiv 0$, so $\boxed{\pi^3|a_3, \pi^3|a_6}$. The equation is now

$\pi^5|a_6$

$$9.1 \quad \pi y_3^2 + \pi a_{1,1}x_2y_3 + \pi a_{3,3}y_3 = \pi x_2^3 + \pi a_{2,2}x_2^2 + a_{4,3}x_2 + a_{6,5} .$$

If $a_{4,3} \not\equiv 0$, i.e. if $\pi^1 \nmid a_1$, then type III^* and $f = v(\Delta)-7$ and $c = 2$.

<u>Branch 3 continues</u> : 10) Assume $\boxed{\pi^4 | a_4}$. Then $\pi^6 \nmid a_6$ the type is II* and $f = v(\Delta) - 8 \quad c = 1$.

If $\pi^6 | a_6$, original equation was not minimal. Start over with

$$y_3^2 + a_{1,1}x_2y_3 + a_{3,3}y_3 = x_2^3 + a_{2,2}x_2^2 + a_{4,4}x_2 + a_{6,6} \qquad !$$