J. Math. Soc. Japan
Vol. 20, Nos. 1-2, 1968

On the algebraic theory of elliptic modular functions[1)]

Dedicated to S. Iyanaga on his 60th birthday

By Jun-ichi IGUSA

(Received Jan. 23, 1967)

Let k denote an algebraically closed field over a prime field $\boldsymbol{F}$ $(=\boldsymbol{Q}$ or $\boldsymbol{Z}/p\boldsymbol{Z})$ and j a variable over k. Choose an elliptic curve A_j defined over $\boldsymbol{F}(j)$ with j as its absolute invariant. Two such elliptic curves are isomorphic, but the isomorphism is not necessarily defined over $\boldsymbol{F}(j)$. In order to avoid this difficulty, we introduce the Kummer morphism "Ku" defined over $\boldsymbol{F}(j)$. Then, for every positive integer n, the field $\boldsymbol{F}(j, Ku({}_nA_j))$ is *intrinsic* in the sense that it is a uniquely determined finite normal extension of $\boldsymbol{F}(j)$ depending only on p and n. In the case when n is not divisible by p, the extension is separable and, taking k instead of $\boldsymbol{F}$ as ground field, it is called the *elliptic modular function field* of level n in characteristic p. If we take $\boldsymbol{C}$ as k, we get back to the classical case. One of the basic theorems in the algebraic theory of elliptic modular functions describes the Galois group and the ramification of $\boldsymbol{F}(j, Ku({}_nA_j))$ relative to $\boldsymbol{F}(j)$ (5). The purpose of this paper is to give a similar description also in the case when $n=p^e$ for $p\neq 0$. It turns out that $\boldsymbol{F}(j, Ku({}_nA_j))$ is a regular extension of $\boldsymbol{F}$ (cf. 8) and a normal extension of degree $\frac{1}{2}\cdot p^{2e-1}(p-1)$ of $\boldsymbol{F}(j)$. Furthermore, the separable part has the same Galois group as $\boldsymbol{Q}(\cos(2\pi/n))$ relative to $\boldsymbol{Q}$. The ramification (of the separable part) takes place at supersingular invariants (cf. 2) and also at $j=0, 12^3$ so that the genus g of $\boldsymbol{F}(j, Ku({}_nA_j))$ is given by

$$2g-2=(1/24)(p-1)(p^{2e-1}-12p^{e-1}+1)-h\,,$$

in which h is the number of supersingular invariants. The formula has to be adjusted by $-3/8$ and $-1/3$ respectively for $p=2$ and 3. Also, in the special case when $p=2$, $e=1$, we have to take $g=0$. It seems possible to better understand this genus formula by the Kroneckerian geometry, i.e., by the geometry of a scheme over $\boldsymbol{Z}$ constructed from $\boldsymbol{Q}(j, Ku({}_nA_j))$.

1. Jacobi quartics. We shall assume that the characteristic p is different from 2. Consider a plane curve defined inhomogeneously by the following

1) This work was partially supported by the National Science Foundation.

equation

$$Y^2 = X^4 - 2\rho \cdot X^2 + 1 .$$

This curve is absolutely irreducible if and only if $\rho^2 \neq 1$ (and $\rho \neq \infty$). Moreover, in this case, the point at infinity is the only singularity and the curve is of genus 1. Therefore, we can introduce a normal law of composition over $\boldsymbol{F}(\rho)$ taking the point (0, 1), say, as its neutral element. We call the curve with this normal law of composition the *Jacobi quartic* of *modulus* ρ and we shall denote it by J_ρ. We note that the law of composition transported to a non-singular model A, say, of J_ρ converts A into an elliptic curve (= complete group variety of dimension 1). Moreover, under the morphism $A \rightarrow J_\rho$, two points of order 2 on A are mapped to the singular point of J_ρ. If u is a point of A, we shall denote the x-coordinate of the corresponding point of J_ρ by $x(u)$; similarly for $y(u)$. We shall sometimes identify u with the corresponding point of J_ρ as long as it is different from the singular point. Then, for instance, we have

$$\pm u = (\pm x(u), y(u)) .$$

Furthermore, if n is an *odd* positive integer and if we put $x = x(u)$ and $y = y(u)$, we have

$$x(nu) = (-1)^{\frac{1}{2}(n-1)} \cdot x^{n^2} F_n(x^{-1}) F_n(x)^{-1} , \qquad y(nu) = G_n(x) F_n(x)^{-2} \cdot y ,$$

in which $F_n(X)$ and $G_n(X)$ are even polynomials in X with coefficients in $\boldsymbol{F}[\rho]$. If we denote $X^{n^2} F_n(X^{-1})$ by $T_n(X)$, we have

$$T_n(X) = \prod_{na=0} (X - x(a))^{p^e} ,$$

in which p^e is the inseparability degree of the endomorphism $n\delta$ of J_ρ. We call $T_n(X)$ the n-th *division polynomial* of J_ρ. It is of degree n^2 and is relatively prime to $F_n(X)$. We note also that, if a is a point of J_ρ of order n, we have $\boldsymbol{F}(\rho, a) = \boldsymbol{F}(\rho, x(a))$. More precisely, we have

$$y(a) = F_n(x(a))^2 \cdot G_n(x(a))^{-1} ,$$

in which $G_n(x(a)) \neq 0$. Therefore $y(a)$ is contained in $\boldsymbol{F}(\rho, x(a))$ and, in fact, in $\boldsymbol{F}(\rho, x^2(a))$. In the special case when $n = p$ with $p \neq 0$ and when ρ is assumed, for a moment, to be a variable over $\boldsymbol{F}$, we have

$$T_p(X) = X^p((X^p)^{p-1} + \sum_{0<2i<p-1} P(\rho)\gamma_i(\rho) \cdot (X^p)^{2i} + (-1)^{\frac{1}{2}(p-1)} P(\rho)) ,$$

in which $P(\rho)$ is the $\frac{1}{2}(p-1)$-th *Legendre polynomial* and $\gamma_i(\rho)$ are contained in $\boldsymbol{F}[\rho]$. We know that $P(\rho)$ is a polynomial in ρ of degree $\frac{1}{2}(p-1)$ with simple roots, and they are different from ± 1. If we compare the two expressions for $T_p(X)$, we see that ${}_pJ_\rho$ is a cyclic group of order p and

$$P(\rho)=(-1)^{\frac{1}{2}(p-1)}(\prod_{\substack{pa=0\\a\neq 0}} x(a))^p .$$

Therefore, by specializing ρ to ρ' different from ± 1 and ∞, we see that $P(\rho')=0$ if and only if ${}_pJ_{\rho'}$ reduces to the neutral element. We refer to (4) for a systematic treatment, especially for the proofs of some non-trivial statements that we have made so far.

Now, we shall find all Jacobi quartics which are "isomorphic" to J_ρ and we shall also find the isomorphisms themselves. Suppose that we have σ: $J_\rho \simeq J_{\rho'}$ for some ρ'. Then σ gives rise to an isomorphism not only of the corresponding function-fields but also of their subfields of even functions. We observe that these subfields are generated over the universal domain by (x^2, y) and $((x')^2, y')$ respectively if (x', y') denote the coordinate functions on $J_{\rho'}$. In this way, we get an isomorphism σ_0, say, of the non-singular conic C_ρ defined inhomogeneously by

$$Y^2=X^2-2\rho\cdot X+1$$

to a similarly defined $C_{\rho'}$. All these conics (forming a linear pencil) pass through four points (the base points) with homogeneous coordinates (0, 1, 1), (0, 1, -1), (1, 1, 0), (1, -1, 0). Since σ maps the neutral element of J_ρ to the neutral element of $J_{\rho'}$, necessarily σ_0 keeps the point (0, 1, 1) fixed. We recall that every isomorphism between two non-singular conics is a projective transformation. Therefore σ_0 determines an element S of PL_3 keeping (0, 1, 1) fixed. On the other hand, the Jacobi quartic J_ρ, or its non-singular model A, is ramified over C_ρ at the four points on C_ρ that we have mentioned above; similarly for $J_{\rho'}$ and $C_{\rho'}$. We know that S keeps (0, 1, 1) fixed. Therefore S has to permute the three remaining points. In this way, we get the following 3! possibilities

$$S=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix} \qquad \begin{pmatrix}1&-1&1\\2&0&-2\\-1&-1&-1\end{pmatrix} \qquad \begin{pmatrix}1&1&-1\\-2&0&-2\\1&-1&-1\end{pmatrix}$$

$$\rho'=\rho \qquad (\rho-3)(\rho+1)^{-1} \qquad -(\rho+3)(\rho-1)^{-1}$$

$$\begin{pmatrix}1&0&0\\0&-1&0\\0&0&-1\end{pmatrix} \qquad \begin{pmatrix}1&-1&1\\-2&0&2\\1&1&1\end{pmatrix} \qquad \begin{pmatrix}1&1&-1\\2&0&2\\-1&1&1\end{pmatrix}$$

$$-\rho \qquad -(\rho-3)(\rho+1)^{-1} \qquad (\rho+3)(\rho-1)^{-1} .$$

All these cases are possible. We note that σ determines σ_0 uniquely and σ_0 determines σ up to the sign of x. We have thus obtained the information that we shall use later.

We can consider those six values of moduli as defining a transformation group on a projective straight line over $\boldsymbol{F}$. The orbits consist of six points in general except for the degenerate case $\{\pm 1, \infty\}$, the harmonic case $\{0, \pm 3\}$ and the equianharmonic case $\{\pm(-3)^{\frac{1}{2}}\}$ with respective multiplicities 2, 2 and 3. We can identify these orbits to single points of another projective straight line over $\boldsymbol{F}$. Up to a projective transformation, the identification morphism is given by

$$j = 2^6(\rho^2+3)^3(\rho^2-1)^{-2}.$$

This j is called the *absolute invariant* of J_ρ and also of any curve which is birationally equivalent to J_ρ. Actually, we know how to characterize j up to the Kroneckerian transformation $j \to \pm j +$integer (cf. 5). We note that the three exceptional orbits are mapped respectively to ∞, 12^3 and 0. We also note that the $\frac{1}{2}(p-1)$ simple roots of $P(\rho)$ are divided into orbits. These orbits are mapped to *supersingular invariants* on the j-line (cf. 2). For instance 0 is the only supersingular invariant for $p=3$. Using the Kronecker symbol, we can write down the number h of supersingular invariants in general, and it is as follows

$$h = (1/12)(p-1) + (1/3)(1-(-3/p)) + (1/4)(1-(-4/p)).$$

2. The field $\boldsymbol{F}(\rho, Ku({}_nJ_\rho))$ for $n=p^e$. First of all, suppose that A is an elliptic curve defined over a field K of characteristic $p \neq 0$. Then, for $n=p^e$ we have

$$[K({}_nA) : K]_s \leqq p^{e-1}(p-1), \qquad [K({}_nA) : K]_i \leqq p^e,$$

provided that ${}_pA$ is cyclic of order p for the second inequality. We leave the proof as an exercise to the reader. We say that an "irreducibility theorem" holds for A and n over K if we have equality signs. In this case, clearly the Galois group of the separable part of $K({}_nA)$ over K is isomorphic to $GL_1(\boldsymbol{Z}/n\boldsymbol{Z})$, i.e., to the Galois group of $\boldsymbol{Q}(e^{2\pi i/n})$ over $\boldsymbol{Q}$.

Now, we take an algebraically closed field k containing $\boldsymbol{F}$ for $p \neq 2$ and also a variable ρ over k. We shall show that the irreducibility theorem holds for J_ρ and $n=p^e$ over $k(\rho)$. We choose a sequence of points

$$\cdots a_{m+1}, \qquad a_m, \cdots, \qquad a_1 \neq 0, \qquad a_0 = 0$$

of J_ρ with the property $pa_{m+1} = a_m$ for $m = 0, 1, 2, \cdots$. Then we have $\boldsymbol{F}(\rho, {}_nJ_\rho) = \boldsymbol{F}(\rho, x(a_e))$. In fact ${}_nJ_\rho$ is a cyclic group of order n and a_e is one of the generators. Since the law of composition of J_ρ is defined over $\boldsymbol{F}(\rho)$, we have $\boldsymbol{F}(\rho, {}_nJ_\rho) = \boldsymbol{F}(\rho, a_e)$, and, as we have seen, this coincides with $\boldsymbol{F}(\rho, x(a_e))$. After this remark, we take a root ρ' of the Legendre polynomial $P(\rho)$. We shall show that: (1) there exists only one point P_e in $K_e = k(\rho, x(a_e))$ lying over ρ';

(2) $x(a_e)$ is a local parameter of K_e at P_e; and (3) the order of $\rho-\rho'$ at P_e is $p^{2e-1}(p-1)$. We shall prove (1), (2), (3) by an induction on e.

We observe that $x(a_1)$ is a root of

$$T_p(X)X^{-p}=(X^p)^{p-1}+P(\rho)\cdot U_0(\rho, X),$$

in which

$$U_0(\rho, X)=\sum_{0<2i<p-1}\gamma_i(\rho)\cdot(X^p)^{2i}+(-1)^{\frac{1}{2}(p-1)}.$$

Let t_1 denote a local parameter of a point of K_1 lying over ρ'. We shall compute orders of elements of K_1 with respect to t_1. Since $U_0(\rho, x(a_1))$ is a unit at $t_1=0$, we have

$$p(p-1)\cdot \mathrm{ord}\,(x(a_1))=\mathrm{ord}\,(\rho-\rho').$$

Since we have

$$\mathrm{ord}\,(x(a_1))\geqq 1, \qquad \mathrm{ord}\,(\rho-\rho')\leqq [K_1:K_0]\leqq p(p-1),$$

we get equality signs everywhere. This proves (1), (2), (3) for $e=1$. Suppose next that (1), (2), (3) are verified up to $e=m\geqq 1$. We shall proceed to prove them for $e=m+1$. We observe that $x(a_{m+1})$ is a root of

$$\begin{aligned} &T_p(X)-(-1)^{\frac{1}{2}(p-1)}\,x(a_m)\cdot F_p(X)\\ &\qquad =X^{p^2}+P(\rho)\cdot X^p\cdot U_m(\rho, X)-(-1)^{\frac{1}{2}(p-1)}\,x(a_m),\end{aligned}$$

in which $U_m(\rho, X)-U_0(\rho, X)$ is given by

$$-(-1)^{\frac{1}{2}(p-1)}\,x(a_m)\cdot\Big(\sum_{0<2i<p-1}\gamma_i(\rho)\cdot(X^p)^{p-2i-2}+(-1)^{\frac{1}{2}(p-1)}(X^p)^{p-2}\Big).$$

Let t_{m+1} denote a local parameter of a point of K_{m+1} lying over P_m. We shall compute orders of elements of K_{m+1} with respect to t_{m+1}. Since $U_m(\rho\cdot x(a_{m+1}))$ is a unit at $t_{m+1}=0$ and since $P(\rho)\cdot x(a_{m+1})^p$ clearly has a larger order than $x(a_m)$, we have

$$p^2\cdot\mathrm{ord}\,(x(a_{m+1}))=\mathrm{ord}\,(x(a_m)).$$

Since we have

$$\mathrm{ord}\,(x(a_{m+1}))\geqq 1, \qquad \mathrm{ord}\,(x(a_m))\leqq [K_{m+1}:K_m]\leqq p^2,$$

we get equality signs everywhere. This proves (1), (2), (3) for $e=m+1$, and the induction is complete. We observe also that the polynomial for $x(a_e)^p$ with coefficients in K_{e-1} is separable. Therefore, we get $[K_e:K_{e-1}]_s=p$ for $e>1$ and $=p-1$ for $e=1$, and hence

$$[K_e:K_0]_s=p^{e-1}(p-1), \qquad [K_e:K_0]_i=p^e.$$

This shows that the irreducibility theorem holds for J_ρ and $n=p^e$ over $k(\rho)$, hence a fortiori over $\boldsymbol{F}(\rho)$. In particular $\boldsymbol{F}(\rho, {}_nJ_\rho)$ is a regular extension of $\boldsymbol{F}$

(cf. 8). We shall calculate the genus of its subfield $\boldsymbol{F}(\rho, Ku({}_nJ_\rho))$.

First of all, we may take $Ku(u)$ to be $(x^2(u), y(u))$. Then, we have $\boldsymbol{F}(\rho, Ku({}_nJ_\rho))=\boldsymbol{F}(\rho, x^2(a_e))$, and hence we have only to calculate the genus of $\boldsymbol{F}(\rho, x^2(a_e))^{p^e}=\boldsymbol{F}(\rho, (x^{2p^e})(a_e))$ or of $L_e=k(\rho, (x^{2p^e})(a_e))$. Suppose that ρ' is an arbitrary element of k. If ρ' is not a root of ρ^2-1, the specialization $\rho\rightarrow\rho'$ over k extends uniquely to a specialization $(J_\rho, {}_nJ_\rho)\rightarrow(J_{\rho'}, {}_nJ_{\rho'})$. If further ρ' is not a root of $P(\rho)$, the specialization ${}_nJ_\rho\rightarrow{}_nJ_{\rho'}$ is an isomorphism of the two cyclic groups. Therefore $(K_e)^{p^e}$ is ramified over $k(\rho)$ at most at the roots of $(\rho^2-1)P(\rho)$ and at ∞. Suppose that ρ' is a root of $P(\rho)$. We shall first compute the contribution to the different of $(K_e)^{p^e}$ over $k(\rho)$ of the unique point of $(K_e)^{p^e}$ lying over ρ'. Since $s_e=x(a_e)^{p^e}$ is a local parameter of $(K_e)^{p^e}$ at this point, we have only to compute the order of $d\rho/ds_e$ with respect to s_e. By applying the chain rule and using the equation for $x(a_{m+1})^{p^{m+1}}$ over $(K_m)^{p^m}$ for $m=0, 1, \cdots, e-1$, we get

$$(p-2)p^{e-1}+p^{e-1}(p-1)\sum_{m=1}^{e-1}p^m=p^{e-1}(p^e-2)\,.$$

Therefore, applying again the chain rule to $(K_e)^{p^e}\supset L_e\supset k(\rho)$, we see that the contribution to the different of L_e over $k(\rho)$ of the unique point of L_e lying over ρ' is

$$\frac{1}{2}(p^{e-1}(p^e-2)-1)=\frac{1}{2}(p^{2e-1}-1)-p^{e-1}\,.$$

On the other hand, as we shall see presently in the next section, the contribution coming from the points of L_e lying over $\rho'=\pm1$ and ∞ are same. We shall show that they are all 0. For this purpose, we take a variable ρ_0 over $\boldsymbol{Q}$ and consider the field $\boldsymbol{Q}(\rho_0, {}_nJ_{\rho_0})$ for $n=p^e$. We know that ${}_nJ_{\rho_0}$ is an abelian group of type (n, n). Therefore, it is generated by two elements a_0, b_0, say. Consider

$$\xi=\prod_{m \bmod n}x(ma_0+b_0)\,.$$

Then ξ can be expanded into a power-series in ρ_0-1 (with coefficients in the principal order of $\boldsymbol{Q}(e^{2\pi i/n})$). This follows from the fact that ξ is invariant by one of the local Galois groups of $\boldsymbol{Q}(\rho_0, {}_nJ_{\rho_0})$ over $\boldsymbol{Q}(e^{2\pi i/n}, \rho_0)$ at $\rho_0=1$. Therefore, if we take the reduction modulo a prime factor of $x(b_0)$, we see that $x(a)^n$ has a power-series expansion in $\rho-1$ (with coefficients in $\boldsymbol{F}$). This proves the assertion. Therefore, the genus $g(L_e)$ of L_e is given by

$$2g(L_e)-2=\frac{1}{2}(p-1)\Big(\frac{1}{2}(p^{2e-1}-1)-p^{e-1}\Big)-p^{e-1}(p-1)\,.$$

As we have seen, $g(L_e)$ is also the genus of $\boldsymbol{F}(\rho, Ku({}_nJ_\rho))$.

3. The field $\boldsymbol{F}(j, Ku({}_nA_j))$ for $n=p^e$. We shall assume, using the same notation as before, that ρ is a variable over k. The absolute invariant j of J_ρ is given explicitly as a rational function of ρ with coefficients in $\boldsymbol{F}$. We choose an elliptic curve A_j, defined over $\boldsymbol{F}(j)$, which is birationally equivalent to J_ρ (cf. 1, 5). We also choose a Kummer morphism for A_j defined over $\boldsymbol{F}(j)$. Then, if w and u are biregularly corresponding points of A_j and J_ρ, we have $\boldsymbol{F}(\rho, Ku(w))=\boldsymbol{F}(\rho, Ku(u))$. This implies $\boldsymbol{F}(\rho, Ku({}_nA_j))=\boldsymbol{F}(\rho, Ku({}_nJ_\rho))$ for $n=p^e$. Therefore $\boldsymbol{F}(\rho, Ku({}_nJ_\rho))$ is the compositum of $\boldsymbol{F}(j, Ku({}_nA_j))$ and $\boldsymbol{F}(\rho)$ over $\boldsymbol{F}(j)$. Consequently, $\boldsymbol{F}(j, Ku({}_nA_j))$ is a regular extension of $\boldsymbol{F}$ and over $\boldsymbol{F}(j)$, the separable and the inseparable degrees are respectively $\frac{1}{2}p^{e-1}(p-1)$ and p^e. The situation remains same even if we replace $\boldsymbol{F}$ by k. Since ± 1 and ∞ on the ρ-line are conjugate over $k(j)$, this settles a minor point left at the end of the previous section.

LEMMA. *If $j'\neq\infty$ is not a supersingular invariant, no point of $k(j, Ku({}_nA_j))$ lying over j' is ramified in $k(\rho, Ku({}_nJ_\rho))$.*

PROOF. Suppose that there is a ramification. Then there exists a point P of $k(\rho, Ku({}_nJ_\rho))$ lying over j' and an automorphism σ of $k(\rho, Ku({}_nJ_\rho))$ over $k(j, Ku({}_nA_j))$, different from the identity, satisfying $\sigma P=P$. Now, the morphism $A_j\rightarrow J_\rho$ gives rise to a unique isomorphism of their Kummer varieties over $\boldsymbol{F}(\rho)$, hence over $k(\rho)$. Applying σ to the graph of this isomorphism, we get an isomorphism of the Kummer variety of A_j to the Kummer variety of $J_{\rho\sigma}$. If we compose the inverse of the first isomorphism with the second isomorphism, using the notation of Section 1, we will get an isomorphism of the conic C_ρ to the conic $C_{\rho\sigma}$. Therefore, for every a in ${}_nJ_\rho$, the image $(x^2(a)^\sigma, y(a)^\sigma)$ of $(x^2(a), y(a))$ under the automorphism σ is precisely the image of $(x^2(a), y(a))$ under the isomorphism $C_\rho \simeq C_{\rho\sigma}$ determined as above. On the other hand, because of $\sigma P=P$, we have

$$(\rho^\sigma, x^2(a)^\sigma, y(a)^\sigma)(P)=(\rho, x^2(a), y(a))(P).$$

If we combine this fact with the explicit expression for $x^2(a)^\sigma$ obtained in Section 1, we immediately get a contradiction. In fact, for $a\neq 0$, $x^2(a)(P)$ satisfies a quadratic equation when $j'=0$ and a linear equation when $j'=12^3$. Therefore, the only possibilities are $n=p=3$ and $n=p=5$. On the other hand, since j' is not supersingular, we have $j'\neq 0$ in both cases. This will bring a contradiction. q. e. d.

We shall, now, proceed to determine the contributions of the points of $k(j, Ku({}_nA_j))^{p^e}$ lying over $j'\neq\infty$ to the different relative to $k(j)$. Suppose first that j' is not supersingular. If j' is different from 0 and 12^3, the contribution is 0. If $j'=0$, using the previous lemma, we get $(2/3)N$ for

$$N=\frac{1}{2}p^{e-1}(p-1).$$

Similarly, if $j'=12^3$, we get $(1/2)N$. Suppose next that j' is supersingular. If j' is different from 0 and 12^3, the contribution is clearly equal to

$$W=\frac{1}{2}(p^{2e-1}-2p^{e-1}-1).$$

If $j'=0$ and $p\neq 3$, since $k(\rho, Ku({}_nJ_\rho))^{pe}$ is tamely ramified over $k(j, Ku({}_nA_j))^{pe}$ with 3 as its ramification index, calculating the derivative of j with respect to the local parameter of $k(\rho, Ku({}_nJ_\rho))^{pe}$ at any one of the points lying over j' in two different ways, we get $(1/3)(W+2N-2)$. Similarly, if $j'=12^3$ and $p\neq 3$, we get $(1/2)(W+N-1)$. On the other hand, if $j'=0=12^3$ and $p=3$, we proceed as follows: There is only one point P, say, of $k(\rho, Ku({}_nJ_\rho))^{pe}$ lying over j. The second ramification group of P is the subgroup which corresponds to $k(\rho)$. Consequently, although $k(\rho, Ku({}_nJ_\rho))^{pe}$ is wildly ramified over $k(j, Ku({}_nA_j))^{pe}$, the second ramification group of P for this extension reduces to the identity. The rest is the same as before, and we get $(1/6)(W+7N-7)$.

Finally, in the case when $j'=\infty$, we can show as before that it is not ramified in $k(j, Ku({}_nA_j))^{pe}$. Therefore, the genus g of this field, which is equal to that of $\boldsymbol{F}(j, Ku({}_nA_j))$, is given by

$$2g-2=(1/24)(p-1)(p^{2e-1}-12p^{e-1}+1)-h,$$

in which h is the number of supersingular invariants. In the case when $p=3$, it is necessary to subtract 1/3 from the right-hand side.

We shall, also, discuss the case when $p=2$. Assuming that j is a variable over k, we consider a plane curve defined inhomogeneously by

$$Y^2-XY=j^{-1}X^3+j.$$

This cubic curve is absolutely irreducible and non-singular, hence it is of genus 1. Therefore, it becomes an elliptic curve with the point at infinity, say, as its neutral element. We shall use this elliptic curve as A_j because it has j as its absolute invariant. We observe that, if $j\rightarrow j'$ is a specialization over k, the elliptic curve A_j has a similarly defined elliptic curve $A_{j'}$ as its unique specialization for $j'\neq 0, \infty$. Moreover, as we can see by using a different model, $j'=0$ is supersingular and, in fact, the only one in characteristic 2 (cf. 1, 2). On the other hand, if $u=(x(u), y(u))$ is a point of A_j, we have $x(-u)=x(u)$ and $y(-u)=x(u)+y(u)$. Therefore, we may take $Ku(u)$ to be $x(u)$. Furthermore, if we put $x=x(u)$, we have the following duplication formula

$$x(2u)=j^{-1}x^2+j^2x^{-2}.$$

We shall show that $\boldsymbol{F}(j, Ku({}_nA_j)$ for $n=2^e$ is a regular extension of $\boldsymbol{F}$ and over $\boldsymbol{F}(j)$, the separable and the inseparable degrees are respectively 2^{e-2} and 2^e provided $e \geqq 2$. We have only to prove the second part replacing $\boldsymbol{F}$ by k.

We choose a sequence of points

$$\cdots a_{m+1}, \qquad a_m, \cdots, \qquad a_1 \neq 0, \qquad a_0 = 0$$

of A_j with the property $2a_{m+1} = a_m$ for $m = 0, 1, 2, \cdots$. Since the group law is defined over $\boldsymbol{F}(j)$ and since ${}_nA_j$ is a cyclic group of order n generated by a_e, we have $\boldsymbol{F}(j, {}_nA_j) = \boldsymbol{F}(j, x(a_e), y(a_e))$, and $\boldsymbol{F}(j, Ku({}_nA_j)) = \boldsymbol{F}(j, x(a_e))$. On the other hand, we have $x(a_0) = \infty$, $x(a_1) = 0$ and $x(a_2)^4 = j^3$. Moreover, if we introduce

$$x_e = (x(a_{e+3})^2 (jx(a_{e+2}))^{-1})^{2^{e+1}}$$

for $e = 0, 1, 2, \cdots$, we have $(x_0)^2 - x_0 = j^{-1}$, and in general x_e is a root of $X^2 - X = R_{e-1}$ with

$$R_{e-1} = (x_0(x_0 - 1))^{2^{e+1}-1} \cdot (x_0 \cdots x_{e-1})^{-2}$$

for $e = 1, 2, \cdots$. We shall show that: (1) there exists only one point P_{e-1} in $k(x_0, \cdots, x_{e-1})$ lying over $x_0 = \infty$; (2) the order of x_{e-1} at P_{e-1} is -2^{2e-2}; and (3) if t_{e-1} is a local parameter of $k(x_0, \cdots, x_{e-1})$ at P_{e-1} and if we replace x_e by a suitable

$$\theta_e = x_e + \text{const.}\,(t_{e-1}{}^{-1})^{2^{2e-1}} + \text{lower powers},$$

the equation for θ_e will take the form

$$(\theta_e)^2 - \theta_e = \text{const.}\,(t_{e-1}{}^{-1})^{\varepsilon_e} + \text{lower powers}$$

with

$$\varepsilon_e = (2/3)(2^{2e} - 1) + 1,$$

in which the constants are both different from 0. We observe that (1), (2), (3) can be verified easily for $e = 1$. Therefore, we shall assume that they are true up to $e = m \geqq 1$. Since ε_m is an *odd* positive integer, we see that θ_m generates a separable quadratic extension of $k(x_0, \cdots, x_{m-1})$ ramified at P_{m-1} (cf. 3), and this extension is $k(x_0, \cdots, x_m)$. In particular, there exists only one point P_m in $k(x_0, \cdots, x_m)$ lying over P_{m-1}, hence over $x_0 = \infty$, and the order of t_{m-1} at P_m is 2. Since we have $2^{2m} - \varepsilon_m = (1/3)(2^{2m} - 1) \geqq 1$, the order of x_m at P_m is -2^{2m}. Therefore, the order of R_m at P_m is -2^{2m+2}. Moreover, we have

$$dR_m/dt_m = (x_0(x_0 - 1))^{2^{m+2}-2} \cdot (x_1 \cdots x_m)^{-2} \cdot (dt_0/dt_m)$$

for $t_0 = x_0{}^{-1}$, and the order of the coefficient of dt_0/dt_m at P_m is -2^{2m+2}. On the other hand, the order of dt_0/dt_m at P_m can be calculated by the chain rule using (3) for $e = 1, 2, \cdots, m$ (cf. 3), and we get

$$\sum_{e=1}^{m} 2^{m-e}(\varepsilon_e + 1) = (2^2/3)(2^{2m} - 1).$$

Therefore, the order of dR_m/dt_m at P_m is equal to

$$-(2/3)(2^{2m+2}+2)=-(\varepsilon_{m+1}+1)\,.$$

Consequently, if we expand R_m into a series of powers of t_m, the highest negative *odd* exponent will be precisely $-\varepsilon_{m+1}$. Since we have $\varepsilon_{m+1}-2^{2m+1}=(1/3)(2^{2m+1}+1)\geqq 3$, it is certainly possible to replace x_{m+1} by a suitable

$$\theta_{m+1}=x_{m+1}+\text{const.}\,(t_m{}^{-1})^{2^{2m+1}}+\text{lower powers}$$

so that the equation for θ_{m+1} takes the form

$$(\theta_{m+1})^2-\theta_{m+1}=\text{const.}\,(t_m{}^{-1})^{\varepsilon_{m+1}}+\text{lower powers}\,;$$

in which the constants are both different from 0. We have thus proved (1), (2), (3) for $e=m+1$, and the induction is complete.

If we observe that $k(j, x(a_e))$ contains $k(x_0, \cdots, x_{e-3})$ for $e\geqq 3$ and that $k(x_0)$ is a separable quadratic extension of $k(j)$, which incidentally is ramified only at $j=0$, we see that the separable degree of $k(j, x(a_e))$ over $k(j)$ is 2^{e-2} and that $k(x_0, \cdots, x_{e-3})$ is the maximal separable subfield of $k(j, x(a_e))$ over $k(j)$. Furthermore, because of

$$x(a_e)^{2^e}=j^3\cdot(\prod_{m=0}^{e-3} j^{2^{m+1}}x_m)^2\,,$$

we see that $x(a_e)^{2^e}$ but not $x(a_e)^{2^{e-1}}$ is separable over $k(j)$ for $e\geqq 3$. Consequently, the inseparability degree of $k(j, x(a_e))$ over $k(j)$ is 2^e. In view of the fact that $k(j, x(a_2))=k(j^{1/4})$, we have completed the proof of the irreducibility statement that we made in the beginning.

We can also determine the genus of $\boldsymbol{F}(j, Ku({}_nA_j))$, which is equal to that of $k(x_0, \cdots, x_{e-3})$, for $e\geqq 3$. We observe that the contributions to the different of $k(x_0, \cdots, x_{e-3})$ relative to $k(x_0)$ come only from those points lying over $j=0$ and ∞. The contribution coming from the unique point lying over $j=0$, i.e., over $x_0=\infty$, has already been calculated in proving (1), (2), (3). We shall show that $j=\infty$ is not ramified in $k(x_0, \cdots, x_{e-3})$. At any rate, over $j=\infty$ we have two points $x_0=0$ and 1 in $k(x_0)$. Suppose that $k(x_0, \cdots, x_m)$ but not $k(x_0, \cdots, x_{m-1})$ is ramified over $k(j)$ at $j=\infty$. Then $k(x_0, \cdots, x_m)$ is ramified over $k(x_0, \cdots, x_{m-1})$ at every one of the 2^m points lying over $j=\infty$ (because they are conjugate over $k(j)$). Now, there is one point P, say, where we have $x_0=\cdots=x_{m-1}=1$. Then R_{m-1} is finite at P, and hence the extension of $k(x_0, \cdots, x_{m-1})$ generated by x_m is unramified at P. This is a contradiction. In this way, we get

$$2g-2=(2^2/3)(2^{2e-6}-1)-2^{e-2}\,,$$

and this is a special case of the general formula if we make an adjustment by subtracting 3/8 from the right-hand side (of the general formula).

The Johns Hopkins University

References

[1] M. Deuring, Invarianten und Normalformen elliptischer Funktionenkörper, Math. Z., **47** (1941), 47-56.

[2] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hamb. Univ., **14** (1941), 197-272.

[3] H. Hasse, Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper, J. Reine Angew. Math., **172** (1934), 37-54.

[4] J. Igusa, On the transformation theory of elliptic functions, Amer. J. Math., **81** (1959), 436-452.

[5] J. Igusa, Fiber systems of Jacobian varieties III, Amer. J. Math., **81** (1959), 453-476.

[6] J. Igusa, Kroneckerian model of fields of elliptic modular functions, Amer. J. Math., **81** (1959), 561-577.

[7] L. Kronecker, Zur Theorie der elliptischen Functionen, Collected Works, Vol. 4, 1929, 345-495.

[8] A. Weil, Foundations of Algebraic Geometry, Providence, 1962.