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.