

FORMAL GROUPS AND ZETA-FUNCTIONS

TAIRA HONDA

(Received July 8, 1968)

Let $F(x, y)$ be a one-parameter formal group over the rational integer ring \mathbf{Z} . Then it is easy to see that there is a unique formal power series $f(x) = \sum_{n=1}^{\infty} n^{-1} a_n x^n$ with $a_n \in \mathbf{Z}$, $a_1 = 1$ satisfying

$$F(x, y) = f^{-1}(f(x) + f(y))$$

and that $f'(x)dx = \sum_{n=1}^{\infty} a_n x^{n-1} dx$ is the canonical invariant differential on F . Let C_1 be an elliptic curve over the rational number field \mathbf{Q} , uniformized by automorphic functions with respect to some congruence modular group $\Gamma_0(N)$. In the language of formal groups results of Eichler [3] and Shimura [14] imply that a formal completion \hat{C}_1 of C_1 (as an abelian variety) is isomorphic over \mathbf{Z} to a formal group whose invariant differential has essentially the same coefficients as the zeta-function of C_1 .

In this paper we prove that the same holds for any elliptic curve C over \mathbf{Q} (th. 5). This follows from general theorems which allow us explicit construction and characterization of certain important (one-parameter) formal groups over finite fields, p -adic integer rings, and the rational integer ring (th. 2 and th. 3). The proof of th. 5 depends only on the fact that the Frobenius endomorphism of an elliptic curve over a finite field is the inverse of a zero of the numerator of the zeta-function, and implies a general relation between the group law and the zeta-function of a commutative group variety. In fact it is remarkable that the p -factor of the zeta-function of C for bad p also can be given a clear interpretation from our point of view (cf. th. 5). Moreover, we prove that the Dirichlet L -function with conductor D has the same coefficients as the canonical invariant differential on a formal group isomorphic, over the ring of integers in $\mathbf{Q}(\sqrt{D})$, to the algebroid group $x+y+\sqrt{D}xy$ (th. 4). In this way the zeta-function of a commutative group variety may be characterized as the L -series whose coefficients give a normal form of its group law.

1. Preliminaries

Let R be a commutative ring with the identity 1. We denote by $R\{x\}$,

$R\{x, y\}$, etc. formal power series rings with coefficients in R . Two formal power series are said to be congruent (mod deg n) if and only if they coincide in terms of degree strictly less than n . A one-parameter formal group (or a group law) over R is a formal power series $F(x, y) \in R\{x, y\}$ satisfying the following axioms:

- (i) $F(z, 0) = F(0, z) = z$
- (ii) $F(F(x, y), z) = F(x, F(y, z))$.

If $F(x, y) = F(y, x)$ moreover, F is said to be commutative. Let G be another group law over R . By a homomorphism of F into G we mean a formal power series $\varphi(x) \in R\{x\}$ such that $\varphi(0) = 0$ and $\varphi \circ F = G \circ \varphi$, where we have written $G(\varphi(x), \varphi(y)) = (G \circ \varphi)(x, y)$. If φ has the inverse function φ^{-1} , φ^{-1} is also a homomorphism of G into F . In this case we say that G is (weakly) isomorphic to F and write $\varphi: F \sim G$. If there is an isomorphism φ of F onto G such that $\varphi(x) \equiv x \pmod{\deg 2}$, we say that G is strongly isomorphic to F and write $\varphi: F \approx G$. If G is commutative, the set $\text{Hom}_R(F, G)$, consisting of all the homomorphisms of F into G over R , has a structure of an additive group by defining $(\varphi_1 + \varphi_2)(x) = G(\varphi_1(x), \varphi_2(x))$ for $\varphi_1, \varphi_2 \in \text{Hom}_R(F, G)$. In particular $\text{End}_R(F)$ ($= \text{Hom}_R(F, F)$) forms a ring with the identity $[1](x) = x$. We call $[n]_F$ the image of $n \in \mathbb{Z}$ under the canonical homomorphism of \mathbb{Z} into $\text{End}_R(F)$.

Writing $A = R\{x\}$, we denote by $\mathfrak{D}(A; R)$ the space of R -derivations of A . It is a free A -module of rank 1 and is generated by $D = d/dx$. We denote by $\mathfrak{D}^*(A; R)$ the dual A -module of $\mathfrak{D}(A; R)$ and call its element a differential of A . For $f \in A$ the map $D \rightarrow Df$ of $\mathfrak{D}(A; R)$ into A defines a differential, which we denote by df . A differential of the form df with $f \in A$ is called an exact differential. It is easy to see that dx is an A -basis of $\mathfrak{D}^*(A; R)$ and $df = (Df)dx$ for any $f \in A$. Let $\omega = \psi(x)dx$ be a differential of A and let $\varphi(x) \in A$ with $\varphi(0) = 0$. Then $\psi(\varphi(x))d\varphi(x)$ is again a differential. We denote it by $\varphi^*(\omega)$. The map φ^* is an R -endomorphism of $\mathfrak{D}^*(A; R)$. Let $F(x, y)$ be a (one-parameter) formal group over R . Introducing a new variable t , F is considered a formal group over $R\{t\}$. Define the right translation T_t of F by $T_t(x) = F(x, t)$. A differential ω of A is said to be an invariant differential on F if and only if $T_t^*(\omega) = \omega$. The set of all the invariant differentials on F forms an R -module. We denote it by $\mathfrak{D}^*(F; R)$.

Proposition 1. Let $F(x, y)$ be a one-parameter formal group over R . Put $\psi(z) = \left(\frac{\partial}{\partial x} F(0, z) \right)^{-1}$ and $\omega = \psi(x)dx$. Then we have $\psi(0) = 1$ and $\mathfrak{D}^*(F; R)$ is a free R -module of rank one generated by ω .

Proof. Since $F(x, y) \equiv x + y \pmod{\deg 2}$, we have $\frac{\partial}{\partial x} F(0, z) \equiv 1 \pmod{\deg 1}$. Hence $\psi(z)$ is well-defined and $\psi(0) = 1$. A differential $\eta = \lambda(x)dx$ of A

is invariant on F if and only if $\lambda(x)dx = \lambda(F(x, z))\frac{\partial}{\partial x}F(x, z)dx$, or

$$(1) \quad \lambda(x) = \lambda(F(x, z))\frac{\partial}{\partial x}F(x, z).$$

From (1) we have

$$\lambda(0) = \lambda(z)\frac{\partial}{\partial x}F(0, z)$$

or

$$(2) \quad \lambda(z) = \lambda(0)\psi(z).$$

Define an R -homomorphism Φ of $\mathfrak{D}^*(F; R)$ into R by $\Phi(\eta) = \lambda(0)$. By (2) Φ is injective. Now differentiating $F(u, F(v, w)) = F(F(u, v), w)$ relative to u , we obtain

$$\frac{\partial}{\partial x}F(u, F(v, w)) = \frac{\partial}{\partial x}F(F(u, v), w)\frac{\partial}{\partial x}F(u, v),$$

and then

$$\frac{\partial}{\partial x}F(0, F(v, w)) = \frac{\partial}{\partial x}F(v, w)\frac{\partial}{\partial x}F(0, v),$$

or

$$(3) \quad (\psi(F(v, w)))^{-1} = \frac{\partial}{\partial x}F(v, w)\psi(v)^{-1}.$$

Now (3) implies that $\psi(x)$ satisfies (1). Therefore ω belongs to $\mathfrak{D}^*(F; R)$ and is clearly its R -basis.

We shall call this ω the *canonical invariant differential* on F .

Proposition 2. *Let F be a one-parameter formal group over a \mathbf{Q} -algebra R . Then we have $F(x, y) \approx x + y$ over R .*

Proof. As R is a \mathbf{Q} -algebra, all the differentials of A are exact. Let $\omega = df(x)$ with $f(x) \equiv x \pmod{\deg 2}$ be the canonical invariant differential on F . Then we have $df(F(x, t)) = df(x)$, i.e. $f(F(x, t)) - f(x) \in R\{t\}$. Put $f(F(x, t)) = f(x) + g(t)$. Then we have $f(F(0, t)) = 0 + g(t)$, or $g(t) = f(t)$. Since $f(x)$ is invertible, this completes the proof.

Prop. 2 was proved in Lazard [5] in an alternative way. More generally we can prove that a commutative formal group of arbitrary dimension over a \mathbf{Q} -algebra is strongly isomorphic to the vector group of the same dimension.

Now let R be an integral domain of characteristic 0 and let K be the fraction field of R . We note that, if $\varphi(x) \in R\{x\}$ satisfies the functional equation $\varphi(x+y) = \varphi(x) + \varphi(y)$, $\varphi(x)$ must be of the form ax with $a \in R$. Let F and G be group laws over R , let $\varphi \in \text{Hom}_R(F, G)$ and let $c(\varphi)$ be the first-degree coefficient of φ ,

The additive map $c: \varphi \rightarrow c(\varphi)$ of $\text{Hom}_R(F, G)$ into R , which is a unitary ring-homomorphism in the case $F=G$, is injective, because F (resp. G) $\approx x+y$ over K (cf. Lubin [6]). In particular the series $f(x) \in K\{x\}$ such that $f(x) \equiv x \pmod{\deg 2}$ and $F(x, y) = f^{-1}(f(x) + f(y))$ is uniquely determined by F . For this f and for $a \in R$ we put $[a]_F(x) = f^{-1}(af(x))$. It is clear that $[a]_F \in \text{End}_R(F)$ if and only if $[a]_F(x) \in R\{x\}$.

We now consider formal groups over a field k of characteristic $p > 0$.

Lemma 1. *Let F and G be group laws over k . If $\varphi \in \text{Hom}_k(F, G)$ and if $\varphi \neq [0]$, there is $q = p^r$ such that $\varphi(x) \equiv ax^q \pmod{\deg(q+1)}$ with $a \neq 0$. Moreover $\varphi(x)$ is a power series in x^q .*

Proof. See Lazard [5] or Lubin [6].

If $[p]_F(x) \equiv ax^q \pmod{\deg(q+1)}$ with $a \neq 0$ and $q = p^h$, h is called the height of F . If $[p]_F = 0$, then the height of F is said to be infinite (Lazard [5]). We denote by $h(F)$ the height of F . It is easy to see that, if $h(F) \neq h(G)$, then $\text{Hom}_k(F, G) = 0$.

Now it is well known that $k\{x\}$ has the structure of a topological ring if we take powers of its maximal ideal as a basis of neighbourhoods at 0. Endowed with the topology induced by it, $\text{Hom}_k(F, G)$ (resp. $\text{End}_k(F)$) becomes a complete topological group (resp. ring) (Lubin [6]). It is clear that $\text{End}_k(F)$ has no zero-divisor. Moreover it is easy to see that, if $h(F) < \infty$, the homomorphism $n \rightarrow [n]_F$ of \mathbb{Z} into $\text{End}_k(F)$ is injective and this imbedding is continuous relative to p -adic topology of \mathbb{Z} . Since $\text{End}_k(F)$ is complete, this extends to an imbedding of the p -adic integer ring \mathbb{Z}_p into $\text{End}_k(F)$. In this way $\text{End}_k(F)$ is a \mathbb{Z}_p -algebra and $\text{Hom}_k(F, G)$ is a \mathbb{Z}_p -module.

The following theorem is fundamental in the theory of one-parameter formal groups over a field of positive characteristic.

Theorem 1. (Lazard [5], Dieudonné [2] and Lubin [6].)

(i) *For every $h(1 \leq h \leq \infty)$ there is a formal group of height h over the prime field of characteristic $p > 0$.*

(ii) *Let k be an algebraically closed field of characteristic $p > 0$. If F and G are group laws over k and if $h(F) = h(G)$, then $F \sim G$ over k . Moreover, if $h(F) = h(G) = \infty$, then $F \approx G$ over k .*

(iii) *Let k be as in (ii) and let F be a group law over k . If $h = h(F) < \infty$, $\text{End}_k(F)$ is the maximal order in the central division algebra with invariant $1/h$ over \mathbb{Q}_p .*

Later we shall reprove (i) and (iii) as applications of our results in 2.

2. Certain formal groups over finite fields and p -adic integer rings

Let R be a complete discrete valuation ring of characteristic 0 such that the

residue class field $k=R/m$ is of characteristic $p>0$, where m denotes the maximal ideal of R . For a group law F over R we obtain a group law over k by reducing the coefficients of $F \bmod m$. We denote it by F^* . If G is another group law over R , we derive the reduction map $*$: $\text{Hom}_R(F, G) \rightarrow \text{Hom}_k(F^*, G^*)$. The following two lemmas are due to Lubin [6].

Lemma 2. *The map $c: \text{Hom}_R(F, G) \rightarrow R$ is an isomorphism onto a closed subgroup of R .*

This is Lemma 2.1.1. of [6].

Lemma 3. *If $h(F^*) < \infty$, the reduction map $*$: $\text{Hom}_R(F, G) \rightarrow \text{Hom}_k(F^*, G^*)$ is injective.*

This is lemma 2.3.1. of [6].

From now on until the end of 2 we denote by \mathfrak{o} the integer ring in an extension field K of \mathbb{Q}_p , of finite degree n , and by \mathfrak{p} the maximal ideal of \mathfrak{o} . Let e and d be the ramification index and the degree of \mathfrak{p} respectively. The residue class field $\mathfrak{o}/\mathfrak{p}$ is the finite field F_q with q elements, where $q=p^d$. The following two lemmas play essential roles in our further investigation.

Lemma 4. *Let π be a prime element of \mathfrak{o} . For any integers $v \geq 0$, $a \geq 1$ and $m \geq 1$ we have*

$$\pi^{-v}(X + \pi Y)^{mp^{av}} \equiv \pi^{-v} X^{mp^{av}} \pmod{\mathfrak{p}}.$$

Proof. It suffices to prove our lemma for $a=m=1$. We have to prove

$$(4) \quad \binom{p^v}{i} \pi^{i-v} \equiv 0 \pmod{\mathfrak{p}} \quad \text{for } 1 \leq i \leq p^v.$$

This is trivial if $i \geq v$. Assume $i < v$. Let $p^\mu | i!$, but $p^{\mu+1} \nmid i!$. Then we see

$$\mu = [i/p] + [i/p^2] + \dots < i/p + i/p^2 + \dots = i/(p-1) \leq i.$$

Hence we have

$$\binom{p^v}{i} p^{i-v} = (p^v - 1) \cdots (p^v - i + 1) \cdot p^i / i! \equiv 0 \pmod{\mathfrak{p}},$$

and a fortiori (4).

The following lemma is a trivial generalization of [7], lemma 1.

Lemma 5. *Let π be a prime element of \mathfrak{o} and let $a \geq 1$ be an integer. Let $f(x)$ and $g(x)$ be power series in $\mathfrak{o}\{x\}$ such that*

$$(5) \quad f(x) \equiv g(x) \equiv \pi x \pmod{\deg 2} \quad \text{and} \quad f(x) \equiv g(x) \equiv x^{qa} \pmod{\mathfrak{p}}.$$

Moreover, let $L(z_1, \dots, z_n)$ be a linear form with coefficients in \mathfrak{o} . Then there exists a unique power series $F(z_1, \dots, z_n)$ with coefficients in \mathfrak{o} such that

$$(6) \quad \begin{aligned} F(z_1, \dots, z_n) &\equiv L(z_1, \dots, z_n) \pmod{\deg 2} \\ &\text{and} \\ f(F(z_1, \dots, z_n)) &= F(g(z_1), \dots, g(z_n)). \end{aligned}$$

Proof. See Lubin-Tate [7]. Note that F is the only power series with coefficients in any overfield of \mathfrak{o} satisfying (6).

Denote by \mathfrak{O} the ring of integers in the maximal unramified extension of K . We are now ready to prove the following:

Theorem 2. *Let π be a prime element of \mathfrak{o} and let $a \geq 1$ be an integer. Put $f(x) = \sum_{v=0}^{\infty} \pi^{-v} x^{q^{av}}$ and $F(x, y) = f^{-1}(f(x) + f(y))$. Then we have the following:*

- (i) *F is a group law over \mathfrak{o} and $\text{End}_{\mathfrak{O}}(F)$ is the integer ring of the unramified extension of K of degree a .*
- (ii) *F^* is a group law of height a over \mathbf{F}_q . Denoting by ξ_{F^*} the q -th power endomorphism of F^* (i.e. $\xi_{F^*}(x) = x^q$), we have*

$$(7) \quad [\pi]_F^* = \xi_{F^*}^a.$$

- (iii) *If G is another group law over \mathfrak{o} such that $[\pi]_G \in \text{End}_{\mathfrak{O}}(G)$ and such that $[\pi]_G^* = \xi_{G^*}^a$, then $F \approx G$ over \mathfrak{o} .*

Proof. We define $u(x) \in K\{x\}$ by

$$(8) \quad [\pi]_F(x) = f^{-1}(\pi f(x)) = x^{q^a} + \pi u(x).$$

We shall prove $u(x) \in \mathfrak{o}\{x\}$. From (8) we have

$$\begin{aligned} \pi f(x) &= f(x^{q^a} + \pi u(x)), \\ \pi x + \sum_{v=0}^{\infty} \pi^{-v} x^{q^{a(v+1)}} &= x^{q^a} + \pi u(x) + \sum_{v=1}^{\infty} \pi^{-v} (x^{q^a} + \pi u(x))^{q^{av}} \end{aligned}$$

and

$$(9) \quad \pi(x - u(x)) = \sum_{v=1}^{\infty} [\pi^{-v} (x^{q^a} + \pi u(x))^{q^{av}} - \pi^{-v} x^{q^{a(v+1)}}].$$

Put $u(x) = x + \sum_{i=2}^{\infty} b_i x^i$ and assume $b_2, \dots, b_{k-1} \in \mathfrak{o}$. Since b_k is written as a polynomial of b_2, \dots, b_{k-1} by (9), we have $b_k \in \mathfrak{o}$ by applying lemma 4 to (9). This proves $u(x) \in \mathfrak{o}\{x\}$.

This being proved, we can apply lemma 5 to $[\pi]_F(x)$ as is seen from (8). First $F(x, y) \in \mathfrak{o}\{x, y\}$ follows from $[\pi]_F \circ F = F \circ [\pi]_F$ by lemma 5. The equality (7) follows directly from (8). Now put $p = \varepsilon \pi^e$. Then ε is a unit in \mathfrak{o} . We have

$$[p]_F = [\varepsilon]_F \circ [\pi]_F^e.$$

and hence, by (7),

$$[p]_{F^*} = (\text{automorphism of } F^*) \circ \xi_{F^*}^{ae}$$

Since $\xi_{F^*}^{ae}(x) = x^{p^{dae}}$, we have $h(F^*) = dae = an$, which completes the proof of (ii). Let G be as in (iii). By prop. 2 there is $\varphi(x) \in K\{x\}$ with $\varphi(x) \equiv x \pmod{\deg 2}$ such that $\varphi \circ F = G \circ \varphi$. Then we have $\varphi \circ [\pi]_F = [\pi]_G \circ \varphi$. Hence φ has coefficients in \mathfrak{o} by lemma 5.

It remains to determine $\text{End}_{\mathfrak{D}}(F)$. Let w be a primitive $(q^a - 1)$ -th root of unity in \mathfrak{D} . By definition of $f(x)$ we have $f(wx) = wf(x)$ and so $F(wx, wy) = wF(x, y)$. Hence we have $wx = [w]_F[x] \in \text{End}_{\mathfrak{D}}(F)$. This implies that the fraction field L of $\text{End}_{\mathfrak{D}}(F)$ contains the unramified extension of \mathbf{Q}_p of degree ad . Moreover, since $[\pi]_F \in \text{End}_{\mathfrak{D}}(F)$, the ramification index of L/\mathbf{Q}_p is a multiple of e . Thus we have $[L : \mathbf{Q}_p] \geq ade = an$. On the other hand, as $h(F^*) = an$, we have $[L : \mathbf{Q}_p] \leq an$ by th. 1, (iii) and by lemma 3. Hence we have $[L : \mathbf{Q}_p] = an$. Since $\mathbf{Z}_p[w, \pi]$ is the integer ring of L , this proves (ii) and completes the proof of th. 2.

The existence of a formal group F with the properties (i), (ii) in th. 2 was proved by Lubin ([6], th. 5.1.2.). But his construction of F is not explicit as ours.

Corollary. *Let F be a formal group over \mathbf{Z}_p such that $h(F^*) = 1$. Then we can find a prime element π of \mathbf{Z}_p such that $[\pi]_F^*(x) = x^p$. The map $\pi : F \rightarrow \pi$ gives a bijection $\Phi : \{\text{strong isomorphism classes of formal groups } F \text{ over } \mathbf{Z}_p \text{ such that } h(F^*) = 1\} \rightarrow \{\text{prime elements of } \mathbf{Z}_p\}$.*

Proof. Since $h(F^*) = 1$, the map $*$: $\text{End}_{\mathbf{Z}_p}(F) \rightarrow \text{End}_{F^p}(F^*)$ is bijective by th. 1, (iii). As $\xi_{F^*}(x) = x^p \in \text{End}_{F^p}(F^*)$, this proves the first assertion. The injectivity of Φ follows from th. 2, (iii) and the surjectivity from th. 2, (ii).

We now prove th. 1, (iii) assuming th. 1, (ii). Applying th. 2 to $\mathfrak{o} = \mathbf{Z}_p$ and $f(x) = \sum_{v=0}^{\infty} p^{-v} x^{p^{hv}}$, we obtain a group law F^* over \mathbf{F}_p , of height h . Let k be the algebraic closure of \mathbf{F}_p . Since $\text{End}_k(F^*)$ contains $[w]_F^*$ and ξ_{F^*} , $\text{End}_k(F^*)$ contains the maximal order M_h in the central division algebra D_h of rank h^2 over \mathbf{Q}_p , and invariant $1/h$. (For details see [6], 5.1.3.) We shall prove $\text{End}_k(F^*) = M_h$. In the following we write ξ instead of ξ_{F^*} for simplicity. Let \mathfrak{u}_h be the integer ring in the unramified extension of degree h over \mathbf{Q}_p and let S be a system of representatives of \mathfrak{u}_h modulo its maximal ideal. For $\beta \in S$, we write $[\beta]$ instead of $[\beta]_F^*$ for brevity. Then we have $[\beta](x) \equiv \beta^* x \pmod{\deg 2}$. Let φ be any element of $\text{End}_k(F^*)$ and let $\varphi(x) \equiv \alpha_0 x \pmod{\deg 2}$. Comparing the r -th degree coefficients of $\varphi \circ [p]_F^* = [p]_F^* \circ \varphi$, where $r = p^h$, we have $\alpha_0 = \alpha_0^r$, i.e. $\alpha_0 \in \mathbf{F}_r$. Hence we can find $\beta_0 \in S$ such that $(\varphi - [\beta_0])(x) \equiv 0 \pmod{\deg 2}$. Then, by lemma 1, there is $\varphi_1 \in \text{End}_k(F^*)$ such that $\varphi - [\beta_0] = \varphi_1 \circ \xi$. Applying the same argument to φ_1 , we obtain $\beta_1 \in S$ and $\varphi_2 \in \text{End}_k(F^*)$ such that $\varphi_1 - [\beta_1] = \varphi_2 \circ \xi$. By repeating the same procedure n -times we derive $\beta_0, \beta_1, \dots, \beta_{n-1} \in S$ and $\varphi_1, \varphi_2, \dots, \varphi_n \in \text{End}_k(F^*)$ such that $\varphi_i - [\beta_i] = \varphi_{i+1} \circ \xi$ for $0 \leq i \leq n-1$, where $\varphi_0 = \varphi$. Then

we have

$$\varphi = [\beta_0] + [\beta_1]\xi + \cdots + [\beta_{n-1}]\xi^{n-1} + \varphi_n \xi^n.$$

Hence the series $[\beta_0] + [\beta_1]\xi + \cdots + [\beta_{n-1}]\xi^{n-1} + \cdots$ converges and coincides with φ . Since $[\beta_i] \in M_h$, this proves $\varphi \in M_h$.

REMARK. Formal groups F^* constructed in th. 2 do not exhaust all the formal groups over finite fields (cf. Serre [13], p. 9).

3. Certain formal groups over \mathbb{Z}

We now give explicit global construction of certain formal groups over \mathbb{Z} . The method is based on lemma 4 and lemma 5 as in 2.

Lemma 6. *Let p be a prime number and let $a_1, a_2, \dots, a_n, \dots$ be rational integers satisfying the following conditions:*

- (i) *If $n = p^\nu m$ with $p \nmid m$, then $a_n = a_p^\nu a_m$*
- (ii) *$a_1 = 1$. $p \nmid a_p$.*

$$a_{p^{\nu+2}} - a_p a_{p^{\nu+1}} + p a_p^\nu = 0 \quad \text{for } \nu \geq 0.$$

Let π be the prime element of \mathbb{Z}_p satisfying the equation

$$(10) \quad X^2 - a_p X + p = 0.$$

Put $f(x) = \sum_{n=1}^{\infty} n^{-1} a_n x^n$ and $F(x, y) = f^{-1}(f(x) + f(y))$. Then we have $F(x, y) \in \mathbb{Z}_p\{x, y\}$, $[\pi]_F(x) \in \mathbb{Z}_p\{x\}$ and $[\pi]_F(x) \equiv x^p \pmod{p}$.

Proof. By Hensel's lemma and by the assumption $p \nmid a_p$ the equation (10) has solutions in \mathbb{Z}_p . Let π' be the other root of (10). It is a unit in \mathbb{Z}_p . Since

$$a_{p^{\nu+2}} - (\pi + \pi') a_{p^{\nu+1}} + \pi \pi' a_p^\nu = 0,$$

we have

$$(11) \quad a_{p^{\nu+2}} - \pi' a_{p^{\nu+1}} = \pi(a_{p^{\nu+1}} - \pi' a_p^\nu) \quad \text{for } \nu \geq 0.$$

Define $u(x) \in \mathbb{Q}_p\{x\}$ by

$$(12) \quad [\pi]_F(x) = f^{-1}(\pi f(x)) = x^p + \pi u(x).$$

The point of the proof is to prove $u(x) \in \mathbb{Z}_p\{x\}$ as in th. 2. From (12) we obtain

$$\pi \sum_{n=1}^{\infty} n^{-1} a_n x^n = x^p + \pi u(x) + \sum_{n=2}^{\infty} n^{-1} a_n (x^p + \pi u(x))^n,$$

or

$$(13) \quad \pi(x - u(x)) = x^p + \sum_{n=2}^{\infty} n^{-1} a_n (x^p + \pi u(x))^n - \pi \sum_{n=2}^{\infty} n^{-1} a_n x^n.$$

Put $u(x) = \sum_{i=1}^{\infty} b_i x^i$, where $b_1 = 1$. Assuming $b_2, \dots, b_{k-1} \in \mathbb{Z}_p$, we shall prove $b_k \in \mathbb{Z}_p$. By lemma 4 we have

$$n^{-1}(x^p + \pi \sum_{i=1}^{k-1} b_i x^i)^n \equiv n^{-1} x^{pn} \pmod{p}.$$

Hence by (13), we have only to prove that the k -th degree coefficient c_k in

$$(14) \quad \sum_{n=1}^{\infty} n^{-1} a_n x^{pn} - \pi \sum_{n=2}^{\infty} n^{-1} a_n x^n$$

is a multiple of p . If $p \nmid k$, this is clear. Assume $k = p^\nu m$ with $\nu \geq 1$, $p \nmid m$. We have

$$\begin{aligned} c_k &= p^{-(\nu-1)} m^{-1} a_{n/p} - p^{-\nu} m^{-1} \pi a_n \\ &= p^{-\nu} m^{-1} a_m (p a_{p^{\nu-1}} - \pi a_{p^\nu}) \end{aligned}$$

or

$$(15) \quad c_k = p^{-\nu} m^{-1} a_m \pi (\pi' a_{p^{\nu-1}} - a_{p^\nu}).$$

Applying (11) to (15) repeatedly we have

$$\begin{aligned} c_k &= p^{-\nu} m^{-1} a_m \pi^\nu (\pi' a_1 - a_p) \\ &= -p^{-\nu} m^{-1} a_m \pi^{\nu+1} \\ &\equiv 0 \pmod{p}. \end{aligned}$$

This proves $b_k \in \mathbb{Z}_p$ and by induction we see in fact $u(x) \in \mathbb{Z}_p\{x\}$. The fact $F(x, y) \in \mathbb{Z}_p\{x, y\}$ follows from this by Lemma 5. (cf. The proof of th. 2)

Lemma 7. *Let p be a prime number, let $\varepsilon = +1$ or -1 , and let $h \geq 1$ be an integer. Let $a_1, a_2, \dots, a_n, \dots$ be rational integers satisfying the following conditions:*

- (i) *If $n = p^\nu m$ with $p \nmid m$, then $a_n = a_{p^\nu} a_m$.*
- (ii) *$a_1 = 1$. $a_p = \dots = a_{p^{h-1}} = 0$.
 $a_{p^{\nu+h}} = \varepsilon p^{h-1} a_{p^\nu}$ for $\nu \geq 0$.*

Put $f(x) = \sum_{n=1}^{\infty} n^{-1} a_n x^n$ and $F(x, y) = f^{-1}(f(x) + f(y))$. Then we have $F(x, y) \in \mathbb{Z}_p\{x, y\}$ and $[\varepsilon p]_F(x) \equiv x^{p^h} \pmod{p}$.

Proof. Repeat the same reasoning as in the proof of lemma 6. The point is to prove $u(x) \in \mathbb{Z}_p\{x\}$, where $u(x)$ is defined by $[\varepsilon p]_F(x) = x^{p^h} + pu(x)$. The details will be left to the reader.

Theorem 3. *Assume that to every prime number p there is given a local L -series $L_p(s)$ of the type:*

$$(a) \quad L_p(s)=1,$$

$$(b) \quad L_p(s)=(1-a_p p^{-s}+p^{1-2s})^{-1} \text{ with } a_p \in \mathbf{Z}, p \nmid a_p,$$

or

$$(c) \quad L_p(s)=(1-\varepsilon_p p^{h-1-hs})^{-1} \text{ with } \varepsilon_p=+1 \text{ or } -1, h=h_p \geq 1.$$

Define the global (formal) L -series $L(s)=\sum_{n=1}^{\infty} a_n n^{-s}$ by $L(s)=\prod_p L_p(s)$ and put $f(x)=\sum_{n=1}^{\infty} n^{-1} a_n x^n$. Then the formal group $F(x, y)=f^{-1}(f(x)+f(y))$ has coefficients in \mathbf{Z} . Denote by F^* the reduction of $F \bmod p$. Then we have:

Case (a): $F \approx x+y$ over \mathbf{Z}_p .

Case (b): $h(F^*)=1$ and the p -th power endomorphism of F^* is a root of the equation

$$X^2 - a_p X + p = 0.$$

Case (c): $h(F^*)=h$ and $[\varepsilon_p p]_F(x) \equiv x^{p^h} \pmod{p}$.

Proof. If $L_p(s)=1$, the coefficients of $f(x)$ are p -integral and we have $F(x, y) \approx x+y$ over \mathbf{Z}_p . If $L_p(s)$ is of type (b) (resp. (c)), it is easily verified that the sequence $a_1, a_2, \dots, a_n, \dots$ satisfies the assumptions of lemma 6 (resp. lemma 7). Therefore the coefficients of $F(x, y)$ are p -integral for every p . This proves $F(x, y) \in \mathbf{Z}\{x, y\}$. The other assertions of our theorem follow from lemma 6 and lemma 7.

The following proposition is useful in the study of algebroid commutative formal groups over \mathbf{Q} .

Proposition 3. Let p be a prime number and let \mathfrak{o} be the integer ring of the quadratic unramified extension of \mathbf{Q}_p . Put $f_1(x)=\sum_{v=0}^{\infty} p^{-v} x^{p^v}$, $f_2(x)=\sum_{v=0}^{\infty} (-p)^{-v} x^{p^v}$ and $F_i(x, y)=f_i^{-1}(f_i(x)+f_i(y))$ for $i=1, 2$. Then we have the following:

(i) $F_1^* \sim F_2^*$ over \mathbf{F}_{p^2} , but $F_1^* \not\sim F_2^*$ over \mathbf{F}_p . If p is odd, then $F_1 \sim F_2$ over \mathfrak{o} .

(ii) Let F be a group law over \mathbf{Z}_p such that $F^*(x, y) \sim x+y+xy$ over \mathbf{F}_{p^2} . Then we have either $F \approx F_1$ or $F \approx F_2$ over \mathbf{Z}_p according as $F^*(x, y) \sim x+y+xy$ over \mathbf{F}_p or not.

Proof. By th. 3 F_i ($i=1, 2$) has coefficients in \mathbf{Z} and $[p]_{F_i}(x) \equiv [-p]_{F_i}(x) \equiv x^p \pmod{p}$. Let k be the algebraic closure of \mathbf{F}_p . Since $h(F_1^*)=h(F_2^*)=1$, there is an invertible series $\varphi(x) \in k\{x\}$ such that $\varphi \circ F_1^* = F_2^* \circ \varphi$ by th. 1, (ii). Then we have $\varphi \circ [p]_{F_1}^* = [p]_{F_2}^* \circ \varphi$, i.e. $\varphi(x^{p^2}) = \varphi(x)^{p^2}$. This implies $\varphi(x) \in \mathbf{F}_{p^2}\{x\}$ and $F_1^* \sim F_2^*$ over \mathbf{F}_{p^2} . If $\varphi(x) \in \mathbf{F}_p\{x\}$, we should have

$$\begin{aligned} ([p]_{F_2}^* \circ \varphi)(x) &= \varphi(x)^p = \varphi(x^p) \\ &= (\varphi \circ [p]_{F_1}^*)(x) = ([p]_{F_2}^* \circ \varphi)(x), \end{aligned}$$

and then

$$[-p]_{F_2}^* = [p]_{F_2}^*,$$

a contradiction. Hence $F_1^* \sim F_2^*$ over F_p . If p is odd, \mathfrak{o} contains the primitive (p^2-1) -th root of unity and there is $w \in \mathfrak{o}$ such that $w^{p-1} = -1$. Then we have $w^{p^2} = (-1)^p w$. Hence $f_1(wx) = wf_2(x)$ and then $F_1(wx, wy) = wF_2(x, y)$, which proves (i). Now the p -th power endomorphism of F^* comes from an endomorphism of F , say $[\pi]_F$, since $h(F^*) = 1$. As the p -times endomorphism of the multiplicative group $x+y+xy$ over F_p is $(1+x)^p - 1 = x^p$, we have $F_1^*(x, y) \sim x+y+xy$ over F_p by th. 1, (ii) and so $F^* \sim x+y+xy \sim F_1^*$ over F_{p^2} . Let ψ be an invertible element of $F_{p^2}\{x\}$ such that $\psi \circ F^* = F_1^* \circ \psi$. Then

$$\begin{aligned} (\psi \circ [\pi^2]_{F_1}^*)(x) &= \psi(x^{p^2}) = \psi(x)^{p^2} = ([p^2]_{F_1}^* \circ \psi)(x) \\ &= (\psi \circ [p^2]_F^*)(x), \end{aligned}$$

which implies $\pi^2 = p^2$. Then by th. 2, (iii) we have $F \approx F_1$ or $F \approx F_2$ over Z_p according as $\pi = p$ or $-p$, i.e. according as $F^* \sim x+y+xy$ or not.

4. Group laws and zeta-functions of group varieties of dimension one

We now interpret zeta-functions of certain commutative group varieties from our point of view. Let $F(x, y)$ be a group law over Z . Then there is unique $f(x) \in Q\{x\}$ such that $f(x) \equiv x \pmod{\deg 2}$ and $F(x, y) = f^{-1}(f(x) + f(y))$ (cf. 1). It is clear that $df(x) = f'(x)dx$ is the canonical invariant differential ω on F . Let $f'(x) = \sum_{n=1}^{\infty} a_n x^{n-1}$ and define a (formal) L -series $L(s)$ by $L(s) = \sum_{n=1}^{\infty} a_n n^{-s}$. If each one of F, f, ω and $L(s)$ is given, the rests are uniquely determined from it.

Theorem 4. *Let K be a quadratic number field, let \mathfrak{o} be the integer ring of K and let D be the discriminant of K . Then the Dirichlet L -function $\sum_{n=1}^{\infty} \left(\frac{D}{n}\right) n^{-s}$ is obtained from a group law $G(x, y)$ over Z . Moreover, let $F(x, y) = x + y + \sqrt{D}xy$. Then we have $F \approx G$ over \mathfrak{o} .*

Proof. Let $\chi(n) = \left(\frac{D}{n}\right)$ be the Kronecker symbol and define

$$(16) \quad P(u) = \prod_{\substack{a \bmod D \\ \chi(a) = 1}} (1 - \zeta^a u), \quad \text{where } \zeta = \exp(2\pi\sqrt{-1}/|D|).$$

It is easy to see $P(u) \in \mathfrak{o}[u]$. Let σ be the non-trivial automorphism of K and put

$$(17) \quad \varphi(u) = (P^\sigma(u) - P(u))/\sqrt{D}P(u).$$

We have only to prove that $\varphi(u) = u + \dots \in \mathfrak{o}\{u\}$ and

$$(18) \quad d\varphi(u)/(1+\sqrt{D}\varphi(u)) = \sum_{n=1}^{\infty} \chi(n)u^{n-1} du ,$$

since $dx/(1+\sqrt{D}x)$ is the canonical invariant differential on F . We recall

$$(19) \quad \sum_{r \bmod D} \chi(r) \zeta^{nr} = \chi(n) \sqrt{D} \quad \text{for any } n \in \mathbf{Z}$$

(Gauss sum). The first-degree coefficient of $\varphi(u)$ is

$$\begin{aligned} & (- \sum_{\substack{b \bmod D \\ \chi(b)=-1}} \zeta^b + \sum_{\substack{a \bmod D \\ \chi(a)=1}} \zeta^a) / \sqrt{D} \\ &= (\sum_{r \bmod D} \chi(r) \zeta^r) / \sqrt{D} = 1 \end{aligned}$$

by (19). Let α_i be the i -th degree coefficient of $P^\sigma - P$. We shall prove $\alpha_i \equiv 0 \pmod{\sqrt{D}}$. Since $(P^\sigma - P)^\sigma = -(P^\sigma - P)$, α_i is of the form $c_i \sqrt{D}$ with $2c_i \in \mathbf{Z}$. If D is odd, we have at once $c_i \in \mathbf{Z}$. If D is even, we have $D \equiv 0 \pmod{4}$. In this case we can easily check

$$\chi(r+D/2) = -\chi(r) \quad \text{for any } r \in \mathbf{Z}$$

and so $\{\zeta^a \mid a \bmod D, \chi(a)=1\}$ coincide with $\{-\zeta^b \mid b \bmod D, \chi(b)=-1\}$ as a whole. Hence $\alpha_i=0$ or twice an integer according as i is even or odd. This shows $c_i \in \mathbf{Z}$ and $\varphi(u) \in v\{u\}$. Let us compute $d\varphi(u)/(1+\sqrt{D}\varphi(u))$. We have

$$\begin{aligned} d\varphi(u) &= \sqrt{D}^{-1} d(P^\sigma/P) \\ &= \frac{1}{\sqrt{D}} \frac{P^\sigma}{P} \left(\sum_b \frac{-\zeta^b}{1-\zeta^b u} - \sum_a \frac{-\zeta^a}{1-\zeta^a u} \right) du \\ &= \frac{1}{\sqrt{D}} \frac{P^\sigma}{P} \left(\sum_{r \bmod D} \frac{\chi(r) \zeta^r}{1-\zeta^r u} \right) du \\ &= \sqrt{D}^{-1} P^{\sigma-1} \sum_{n=1}^{\infty} \sum_{r \bmod D} \chi(r) \zeta^{nr} u^{n-1} du \\ &= P^{\sigma-1} \sum_{n=1}^{\infty} \chi(n) u^{n-1} du \quad (\text{by (19)}) . \end{aligned}$$

Hence we have

$$\begin{aligned} \frac{d\varphi(u)}{1+\sqrt{D}\varphi(u)} &= \frac{P^{\sigma-1} \sum_{n=1}^{\infty} \chi(n) u^{n-1} du}{1+(P^\sigma-P)/P} \\ &= \sum_{n=1}^{\infty} \chi(n) u^{n-1} du . \end{aligned}$$

This completes the proof of our theorem.

Now the Dirichlet L -function $L(s, \chi)$ has an Euler product of the form $\prod_p (1 - \varepsilon_p p^{-s})^{-1}$ where $\varepsilon_p = \chi(p)$. By th. 3 ε_p is uniquely determined by the group law F . From this point of view $L(s, \chi)$ can be characterized as the L -series attached to a normal form over \mathbf{Z} of the algebroid group F . The Euler product

implies that the group law F is "the direct product" of group laws over \mathbf{Z}_p 's attached to p -factors of $L(s, \chi)$.

Quite the same holds for elliptic curves over \mathbf{Q} . In the following we mean by an elliptic curve an abelian variety of dimension one. Let C be an elliptic curve over \mathbf{Q} . Néron [10] shows that there is an essentially unique (affine) model for C of the form

$$(20) \quad Y^2 + \lambda XY + \mu Y = X^3 + \alpha X^2 + \beta X + \gamma$$

where $\lambda, \mu, \alpha, \beta, \gamma$ are integers and the discriminant of the equation (18) is as small as possible. For this model $C_p = C \bmod p$ is an irreducible curve for every prime number p . Then local L -series $L_p(s)$ of C are defined as follows.

(I) If C_p is of genus 1, we put

$$L_p(s) = (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

where $1 - a_p U + p U^2$ is the numerator of the zeta-function of C_p .

(II) If C_p has an ordinary double point, we put $\varepsilon_p = +1$ or -1 according as the tangents at the double point are rational over \mathbf{F}_p or not and write

$$L_p(s) = (1 - \varepsilon_p p^{-s})^{-1}$$

(III) If C_p has a cusp, we put

$$L_p(s) = 1.$$

In case (II) the reduction of the group law of C is isomorphic to the multiplicative group over \mathbf{F}_{p^2} and is isomorphic to it over \mathbf{F}_p if and only if $\varepsilon_p = +1$. In case (III) the reduction of the group law of C is the additive group ([10], Chap. III, prop. 3).

Now, we take $t = X/Y$ as a local parameter at the origin. By [15], Chap. III, prop. 4 t is a local parameter at the origin of C_p for every p . Writing down the group law of C as a formal power series relative to the variable t , we obtain a formal group $F(x, y)$ over \mathbf{Z} . (The fact $F(x, y) \in \mathbf{Z}\{x, y\}$ can be verified also by direct computation.) We shall call a formal group over \mathbf{Z} , strongly isomorphic to this F over \mathbf{Z} , a *formal minimal model* for C over \mathbf{Z} .

Theorem 5. *Let $C, C_p, L_p(s)$ and F be as above. Let S be any set of prime numbers which does not contain $p=2$ or 3 , if C_p has genus one and $a_p = \pm p$, and put $\mathbf{Z}_S = \bigcap_{p \in S} (\mathbf{Z}_p \cap \mathbf{Q})$. Write $\prod_{p \in S} L_p(s) = \sum_{n=1}^{\infty} a_n n^{-s}$, $g(x) = \sum_{n=1}^{\infty} n^{-1} a_n x^n$ and $G(x, y) = g^{-1}(g(x) + g(y))$. Then $G(x, y)$ is a formal group over \mathbf{Z} and $F \approx G$ over \mathbf{Z}_S .*

Proof. If C_p has genus one and $p \mid a_p$, we see easily $a_p = 0$ or $a_p = \pm p$ with $p=2$ or 3 by Riemann hypothesis $|a_p| < 2\sqrt{p}$. The latter cases being excluded,

we can apply th. 3 to $\prod_{p \in S} L_p(s)$ and obtain $G(x, y) \in \mathbb{Z}\{x, y\}$. In order to show $F \approx G$ over \mathbb{Z}_S , we have only to prove $F \approx G$ over \mathbb{Z}_p for every $p \in S$, since a power series $\varphi(x)$ such that $\varphi(x) \equiv x \pmod{\deg 2}$ and $\varphi \circ F = G \circ \varphi$ is unique. If C_p has genus one for $p \in S$, then $F \approx G$ over \mathbb{Z}_p by th. 3 and th. 2, (iii), since $X^2 - a_p X + p$ is the characteristic polynomial of the p -th power endomorphism of C_p . In case (II) $F \bmod p$ is isomorphic to the multiplicative group $x + y + xy$ over \mathbb{F}_{p^2} and isomorphic to it over \mathbb{F}_p is and only if $\varepsilon_p = +1$. Hence we have $F \approx G$ over \mathbb{Z}_p by prop. 3, (ii), by th. 3 and by th. 2, (iii). In case (III) it is clear $F \approx G$ over \mathbb{Z}_p . This completes our proof.

REMARK. It seems that the assumption on S in th. 5 would be superfluous. But I have not been able to get rid of it.

Corollary 1. *Notations being as in th. 5, assume that $a_p \neq \pm p$ for $p=2, 3$. Then the formal group attached to the zeta-function $L(s; C) = \prod_p L_p(s)$ of C has coefficients in \mathbb{Z} and is a formal minimal model for C .*

Corollary 2. *Let C and C' be elliptic curves over \mathbb{Q} and let S be a set of primes satisfying the assumption in th. 5 for each curve. Then formal minimal models of C and C' are isomorphic over \mathbb{Z}_S , if and only if p -factors of $L(s; C)$ and $L(s; C')$ coincide for every $p \in S$.*

Corollary 3. *Let notations be as in th. 5. If C_p has genus one for $p \in S$, $a_p \bmod p$ is the Hasse invariant of C_p .*

Proof. Take $f(x) \in \mathbb{Q}\{x\}$ such that $f(x) \equiv x \pmod{\deg 2}$ and $F(x, y) = f^{-1}(f(x) + f(y))$. Then $f'(t)dt$ is the canonical invariant differential on F , i.e. the t -expansion of an differential of the 1st kind on C . Hence our assertion follows from definition of Hasse invariant and from th. 5.

REMARK. Coroll. 3 is a special case of th. 1 of Manin [9]. So his theorem is suggestive for generalization of th. 5 to an abelian variety of higher dimension over an algebraic number field.

Corollary 4. *Let C be an elliptic curve over \mathbb{Q} and assume $a_p = 0$ for a prime number p . Denote by \mathfrak{o} the integer ring of the quadratic unramified extension of \mathbb{Q}_p . Then C has formal complex multiplications over \mathfrak{o} , i.e. $\text{End}_{\mathfrak{o}}(F) = \mathfrak{o}$.*

Proof. Let H be the formal group over \mathbb{Z} attached to the L -series $(1 + p^{1-2s})^{-1}$. We have $H(x, y) = h^{-1}(h(x) + h(y))$ where $h(x) = \sum_{v=0}^{\infty} (-p)^{-v} x^{p^{2v}}$. If $a_p = 0$, then $F \approx H$ over \mathbb{Z}_p by th. 5, and our assertion follows from th. 2, (i).

REMARK. Existence of elliptic curves, which have no complex multiplication but have formal complex multiplications over p -adic integer rings, was proved by

Lubin-Tate [8]. But they did not give an explicit example. Our result has a meaning in the study of l -adic Lie groups attached to elliptic curves over \mathbb{Q} . (cf. Remark on p. 246 of Serre [12].)

There are some questions concerned with our results. How can we generalize th. 4 to more general L -functions? Let F and G be as in th. 5 with $S =$ the set of all the prime numbers. What is the power series $\varphi(x) \in Z\{x\}$ such that $\varphi(x) \equiv x \pmod{\deg 2}$ and $F \circ \varphi = \varphi \circ G$? How can we generalize th. 5 to an abelian variety of higher dimension over an algebraic number field?

OSAKA UNIVERSITY.

References

- [1] M. Deuring: *Algebren*, Ergebnisse der Math., Berlin, 1935.
- [2] J. Dieudonné: *Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$* (VII), Math. Ann. **134** (1957), 114–133.
- [3] M. Eichler: *Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion*, Arch. Math. **5** (1954), 355–366.
- [4] E. Hecke: *Über die Modulfunktionen und die Dirichletschen Reihen mit Eulerschen Produktentwicklung I, II*, Math. Ann. **114** (1937), 1–28, 316–351.
- [5] M. Lazard: *Sur les groupes de Lie formels à un paramètre*, Bull. Soc. Math. France **83** (1955), 251–274.
- [6] J. Lubin: *One parameter formal Lie groups over \mathfrak{p} -adic integer rings*, Ann. of Math. **80** (1964), 464–484.
- [7] J. Lubin and J. Tate: *Formal complex multiplication in local fields*, Ann. of Math. **81** (1965), 380–387.
- [8] J. Lubin and J. Tate: *Formal moduli for one-parameter formal Lie groups*, Bull. Soc. Math. France **94** (1966), 49–60.
- [9] Ju. I. Manin: *On Hasse-Witt matrix of an algebraic curve* (in Russian), Izv. Akad. Nauk **25** (1961), 153–172. (= Amer. Math. Soc. Trans. (2) **45**, 245–264.)
- [10] A. Néron: *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*, Publ. Math. I.H.E.S., **21** (1964).
- [11] I.R. Šafarevič: *Algebraic number fields* (in Russian), Proceedings of the International Congress of Mathematicians in Stockholm, 1962, 163–176 (= Amer. Math. Soc. Trans. (2), **31**, 25–39).
- [12] J. -P. Serre: *Groupes de Lie l -adiques attachés aux courbes elliptiques*, Les tendances géométriques en algèbre et théorie des nombres, Clermont-Ferrand, 1964, Centre National de la Recherche Scientifique, 1966, 239–256.
- [13] J. -P. Serre: *Courbes elliptiques et groupes formels*, Extrait de l'Annuaire du Collège de France, 1966–67.
- [14] G. Shimura: *Correspondances modulaires et les fonctions ζ de courbes algébriques*, J. Math. Soc. Japan **10** (1958), 1–28.
- [15] G. Shimura and Y. Taniyama: *Complex multiplication of abelian varieties and its applications to number theory*, Math. Soc. Japan, Tokyo, 1961.

