Formal Complex Multiplication in Local Fields

By JONATHAN LUBIN* and JOHN TATE

Let k be a field complete with respect to a discrete valuation, with a finite residue class field. Let A be the ring of integers in k, let π be a prime element in A, and let $q = (A:\pi A)$ be the number of elements in the residue class field. Let $\mathcal{F}_\pi$ denote the set of power series $f(T) \in A[[T]]$ which satisfy the two conditions

$$(1) \qquad f(T) \equiv \pi T \pmod{\deg 2} \quad \text{and} \quad f(T) \equiv T^q \pmod{\pi} .$$

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; they are congruent (mod π) if and only if each coefficient of their difference is divisible by π. For example, the simplest choice for an element $f \in \mathcal{F}_\pi$ is $f(T) = \pi T + T^q$. By Lemma 1 below, there exists for each $a \in A$ and each $f \in \mathcal{F}_\pi$ a unique series $[a]_f(T) \in A[[T]]$ satisfying the two conditions

$$[a]_f(T) \equiv aT \pmod{\deg 2} \quad \text{and} \quad [a]_f\big(f(T)\big) = f\big([a]_f(T)\big) .$$

Let $f(T)$ be any element of $\mathcal{F}_\pi$. For each integer $m \geqq 1$, let $f^m(T) = f(f(\cdots(f(T))\cdots))$ denote the m^{th} iterate of $f(T)$. Let $\Lambda_{f,m}$ denote the set of elements λ in an algebraic closure $\bar{k}$ of k such that ord $\lambda > 0$ and $f^m(\lambda) = 0$, and let $L_{f,m} = k(\Lambda_{f,m})$ be the field generated over k by these elements. We shall show:

$L_{f,m}$ is the totally ramified abelian extension of k whose norm group is the subgroup of k^* generated by π and by the units congruent to 1 (mod π^m). *For each unit u in k and each $\lambda \in \Lambda_{f,m}$ we have*

$$(2) \qquad (u, L_{f,m}/k)\lambda = [u^{-1}]_f(\lambda) ,$$

where $(u, L/k)$ is the automorphism of the abelian extension L/k associated to u by the reciprocity law of local class field theory.

One special case of this result is well known, namely that in which $k = \mathbf{Q}_p$ (the rational p-adic field), $\pi = p$, and $f(T) = (1 + T)^p - 1$. Then $f^m(T) = (1 + T)^{p^m} - 1$, the elements λ are those of the form $\zeta - 1$, where $\zeta^{p^m} = 1$, and $L_{f,m}$ is the field generated over $\mathbf{Q}_p$ by the p^m-th roots of unity. In this case we have $[u]_f(T) = (1 + T)^u - 1 = \sum_{n=1}^{\infty} \binom{u}{n} T^n$ for each p-adic integer u, hence $[u]_f(\zeta - 1) = \zeta^u - 1$, and (2) becomes the well-known cyclotomic reciprocity law, the first purely local proof of which was given by Dwork [1].

* This work was supported by a grant from the Research Corporation.

In the general case, we construct, for each π and each $f \in \mathcal{F}_\pi$, a formal Lie group law on one parameter, $F_f(X, Y) \in A[[X, Y]]$ (cf. [2]), which has A as a ring of endomorphisms in such a way that $T \mapsto f(T)$ is the endomorphism corresponding to π. Thus $\Lambda_{f,m}$ becomes an A-module. We show it is isomorphic to $A/\pi^m A$, thereby obtaining an isomorphism between the Galois group of the extension $L_{f,m}/k$ and the group of units in the ring $A/\pi^m A$; the procedure is familiar from the case of extensions generated by roots of unity, or by division points on elliptic curves with complex multiplication. In order to prove that the isomorphism obtained in this way is the opposite of the reciprocity law isomorphism, we make use of the fact that all the formal A-modules F_f, for all π and all f, become isomorphic over the complete maximal unramified extension of k. In the number field case, this follows from [3, Th. 4.3.2], because the formal groups F_f's are full, with endomorphism ring A.

1. The formal Lie A-modules

These can be constructed efficiently by means of the following

LEMMA 1. *Let $f(T)$ and $g(T)$ be elements of $\mathcal{F}_\pi$, and let $L(X_1, \cdots, X_n) = \sum_{i=1}^n a_i X_i$ be a linear form with coefficients in A. There exists a unique series $F(X_1, \cdots, X_n)$ with coefficients in A such that*

$$(3)\qquad \begin{gathered} F(X_1, \cdots, X_n) \equiv L(X_1, \cdots, X_n) \pmod{\deg 2}\ , \\ \textit{and} \\ f\big(F(X_1, \cdots, X_n)\big) = F\big(g(X_1), \cdots, g(X_n)\big)\ . \end{gathered}$$

Writing $X = (X_1, \cdots, X_n)$ and $g(X) = \big(g(X_1), \cdots, g(X_n)\big)$, we show by induction on r that the congruences

$$F_r(X) \equiv L(X) \pmod{\deg 2} \quad \text{and} \quad f\big(F_r(X)\big) \equiv F_r\big(g(X)\big) \big(\text{mod deg } (r+1)\big)$$

have a solution $F_r(X) \in A[X]$ which is unique (mod deg $(r+1)$). This is true for $r = 1$, with $F_1(X) = L(X)$. Suppose it is true for some $r \geqq 1$. Then the next solution, F_{r+1}, must be of the form $F_{r+1} = F_r + \Delta_r$, where $\Delta_r \equiv 0$ (mod deg $(r+1)$), and the equations

$$\left.\begin{aligned} f\big(F_{r+1}(X)\big) &\equiv f\big(F_r(X)\big) + \pi\Delta_r(X) \\ F_{r+1}\big(g(X)\big) &\equiv F_r\big(g(X)\big) + \pi^{r+1}\Delta_r(X) \end{aligned}\right\} \big(\text{mod deg } (r+2)\big)$$

show that we must take

$$\Delta_r(X) \equiv \frac{f\big(F_r(X)\big) - F_r\big(g(X)\big)}{\pi^{r+1} - \pi} \big(\text{mod deg } (r+2)\big)\ .$$

The coefficients are in A because

$$f\big(F_r(X)\big) - F_r\big(g(X)\big) \equiv \big(F_r(X)\big)^q - F_r(X^q) \equiv 0 \pmod{\pi}\ .$$

Now $F(X) = \lim F_r(X) \in A[[X]]$ is obviously the unique solution of (3).

Remarks. The completeness of A was not used in the proof. Moreover, the proof shows that F is the only power series with coefficients in any overfield of A satisfying (3).

For each $f \in \mathcal{F}_\pi$, we let $F_f(X, Y)$ be the unique solution of

$$F_f(X, Y) \equiv X + Y \pmod{\deg 2}\,, \quad \text{and} \quad f(F_f(X, Y)) = F_f(f(X), f(Y))\,, \tag{4}$$

For each $a \in A$, and $f, g \in \mathcal{F}_\pi$ we let $[a]_{f,g}(T)$ be the unique solution of

$$[a]_{f,g}(T) \equiv aT \pmod{\deg 2}\,, \quad \text{and} \quad f([a]_{f,g}(T)) = [a]_{f,g}(g(T))\,. \tag{5}$$

We shall write $[a]_f$ instead of $[a]_{f,f}$ to simplify the typography.

THEOREM 1. *For series $f, g, h \in \mathcal{F}_\pi$, and elements $a, b \in A$, the following identities hold*:

$$F_f(X, Y) = F_f(Y, X)\,, \tag{6}$$

$$F_f(F_f(X, Y), Z) = F_f(X, F_f(Y, Z))\,, \tag{7}$$

$$F_f([a]_{f,g}(X), [a]_{f,g}(Y)) = [a]_{f,g}(F_g(X, Y))\,, \tag{8}$$

$$[a]_{f,g}([b]_{g,h}(T)) = [ab]_{f,h}(T)\,, \tag{9}$$

$$[a + b]_{f,g}(T) = F_f([a]_{f,g}(T), [b]_{f,g}(T))\,, \tag{10}$$

$$[\pi]_f(T) = f(T),\ [1]_f(T) = T\,. \tag{11}$$

In each case one checks immediately that both the left side and the right side of the identity to be proved are solutions to a problem of the type discussed in Lemma 1, whose solution is unique. Sample: both sides of (8) are congruent to $aX + aY$ (mod deg 2); and if we replace X by $g(X)$ and Y by $g(Y)$ in either side, we see using (4) and (5) that the result is the same as if we substitute the given side in f.

Equations (6) and (7) show that F_f is a commutative formal Lie group on one parameter, defined over A. From (8), we see that $[a]_{f,g}$ is a formal homomorphism of F_g into F_f. By (9), the composition of two such homomorphisms is reflected in the multiplication of the corresponding elements of A; and by (10), the addition of the homomorphisms is reflected in the addition of the corresponding elements in A. Taking $f = g$ in these equations, we see that the map $a \mapsto [a]_f$ is an injective ring homomorphism of A into $\mathrm{End}_A(F_f)$, the ring of endomorphisms of F_f over A, and by (11) we see that this ring homomorphism is unitary, and associates f with π. Thus, we may view the F_f's not only as formal groups, but as *formal A-modules*. From (9), with $g = f$ resp. $g = h$, we see that $[a]_{f,g}$ is a homomorphism of formal A-modules, not only of formal groups. Finally, the F_f's, for $f \in \mathcal{F}_\pi$, are canonically isomorphic by means of the isomorphisms $[1]_{f,g}$; the isomorphism class of the F_f's depends only on π, not on the choice of $f \in \mathcal{F}_\pi$. By (1), a formal group over A is in this isomorphism class if and only if it has an endomorphism reducing mod π to the Frobenius, $T \mapsto T^q$, whose derivative at the origin is π.

Let L be an algebraic extension of k, and let $M(L)$ be the maximal ideal in the ring of integers of L. Given elements $x_1, \cdots, x_n$ in $M(L)$ and a formal series $G(X_1, \cdots, X_n) \in A[[X_1, \cdots, X_n]]$, the series $G(x_1, \cdots, x_n)$ is convergent to an element of $M(L)$ if the constant term of G is zero. Moreover the identities (6)–(11) will hold true after substitution of elements x, y, z, t in $M(L)$ for the variables X, Y, Z, T. These identities show that each series f satisfying (1) determines an A-module structure on the set $M(L)$, for which the addition and scalar multiplication are defined by

$$x + y = F_f(x, y) \tag{12}$$

$$ax = [a]_f(x)\ . \tag{13}$$

We shall denote the resulting A-module by $M_f(L)$.

If $L_1 \subset L$, it is clear that $M_f(L_1)$ is an A-submodule of $M_f(L)$. If L/L_1 is Galois with group $G = G(L/L_1)$, then by its ordinary operation on the underlying set $M(L)$ an element $\tau \in G$ induces an automorphism of the A-module $M_f(L)$; this results from the fact that τ acts continuously on L, and that the operations in $M_f(L)$ are defined by convergent series (12) and (13) whose coefficients are in k, and hence are left fixed by τ. For different f and g, the map $x \mapsto [1]_{f,g}(x)$ is an A-isomorphism of $M_g(L)$ onto $M_f(L)$, and this isomorphism commutes with the inclusions $L_1 \subset L$, and with the operations of G in the Galois case.

From now on we restrict our attention to subfields L of a fixed separable algebraic closure k_s of k. For each $f \in \mathcal{F}_\pi$ and each integer $m \geqq 1$ we let $\Lambda_{f,m}$ denote the A-submodule of $M_f(k_s)$ consisting of the elements λ such that $\pi^m\lambda = 0$. For $f, g \in \mathcal{F}_\pi$ we have $\lambda \in \Lambda_{f,m}$ if and only if $[1]_{g,f}(\lambda) \in \Lambda_{g,m}$. Hence the field extension $k(\Lambda_{f,m})/k$ depends only on π, not on $f \in \mathcal{F}_\pi$; we denote it by $L_{\pi,m}/k$, and its Galois group by $G_{\pi,m}$. We let $\Lambda_f = \bigcup_{m=1}^{\infty} \Lambda_{f,m}$, $L_\pi = k(\Lambda_f)$, and $G_\pi =$ proj lim $(G_{\pi,m})$.

THEOREM 2. *Let π be a prime element of A and let $f \in \mathcal{F}_\pi$.*

(a) *The A-module $M_f(k_s)$ is divisible.*

(b) *For each m, the A-module $\Lambda_{f,m}$ is isomorphic to $A/\pi^m A$.*

(c) *The A-module Λ_f is isomorphic to k/A.*

(d) *For each $\tau \in G_\pi$ there exists a unique unit u in A such that $\tau\lambda = [u]_f(\lambda)$*

for every λ *in* Λ_f.

(e) *The map* $\tau \mapsto u$ *is an isomorphism of* G_π *onto the group* U *of units in* A, *under which the quotients* $G_{\pi,m}$ *of* G *correspond to the quotients* $U/(1 + \pi^m A)$ *of* U.

(f) *The element* π *is a norm from the extension* $L_{\pi,m}/k$ *for each* m.

In view of the isomorphisms $[1]_{f,g}$, we may suppose $f(T) = T^q + \pi T$. For $x \in M(k_s)$ the polynomial $T^q + \pi T - x$ has all its zeros in $M(\bar{k})$, the maximal ideal in the algebraic closure $\bar{k}$ of k, and they are distinct because the derivative $f'(T)$ is $qT^{q-1} + \pi$, which has no zero in $M(\bar{k})$. Thus the roots of $f(T) = T^q + \pi T = x$ are in $M(k_s)$, and so $M_f(k_s)$ is divisible. The A-module $\Lambda_{f,1}$, which consists of the roots of the equation $f(T) = T^q + \pi T = 0$, has q elements, and is therefore a one-dimensional vector space over the residue class field $A/\pi A$. Statements (b) and (c) now follow, being true for any divisible torsion module Λ over a valuation ring A, such that the kernel Λ_1 of $\pi\colon \Lambda \to \Lambda$ is one-dimensional over $A/\pi A$. An automorphism $\tau \in G_\pi$ induces an automorphism of the A-module Λ_f, and for a module $\Lambda \approx k/A$ over a *complete* valuation ring A, the only automorphisms of Λ are those of the form $\lambda \mapsto u\lambda$, where u is a unit in A. This proves (d). As for (e), the map $\tau \mapsto u$ is injective because Λ_f generates L_π over k. More precisely, the unit u is congruent to 1 (mod $\pi^m A$), i.e., multiplication by u is identity on $(A/\pi^m A) \simeq \Lambda_{f,m}$, if and only if τ is identity on $L_{\pi,m} = k(\Lambda_{f,m})$. Thus the map $\tau \mapsto u$ induces an injection: $G_{\pi,m} \to U/(1 + \pi^m A)$ for every m. The surjectivity follows by counting: $L_{\pi,m}$ contains the roots of the polynomial

$$f^m(X) = f(f(\cdots(f(X))\cdots)) = X^{q^m} + \cdots + \pi^m X\,,$$

and hence those of the polynomial

$$\Phi_m(X) = \frac{f^m(X)}{f^{m-1}(X)} = \frac{f(f^{m-1}(X))}{f^{m-1}(X)} = (f^{m-1}(X))^{q-1} + \pi\,,$$

which is of degree $q^m - q^{m-1}$, and is irreducible over k by Eisenstein's criterion. Thus the order of $G_{\pi,m}$ is $q^m - q^{m-1}$, the same as the order of $U/(1 + \pi^m A)$, and the surjectivity follows. Passing to the inverse limit over m, we obtain $G_\pi \simeq U$ because both groups are compact. Finally, if λ is a root of the Eisenstein polynomial $\Phi_m(X)$, we have $L_{\pi,m} = k(\lambda)$, hence π is the norm of $-\lambda$ for the extension $L_{\pi,m}/k$.

2. The reciprocity law

Let T be the maximal unramified extension of k, and let σ be the Frobenius automorphism of T over k. Since L_π is totally ramified over k, it is linearly disjoint from T over k, and the Galois group $G(L_\pi T/k)$ is the product of

$G_\pi = G(L_\pi/k)$ and $G(T/k)$. For each prime element π in A, we can therefore define a homomorphism $r_\pi\colon k^* \to G(L_\pi T/k)$ such that

(a) For each unit $u \in U$, the automorphism $r_\pi(u)$ is identity on T, and on L_π is the reciprocal τ^{-1} of the element $\tau \in G_\pi$ corresponding to u by the isomorphism of Theorem 2; and

(b) $r_\pi(\pi)$ is identity on L_π and is the Frobenius automorphism σ on T. Thus for an arbitrary element $a = u\pi^m \in k^*$ we have, by definition:

$$r_\pi(a) = \sigma^m \text{ on } T\,, \tag{14}$$

and

$$\lambda^{r_\pi(a)} = [u^{-1}]_f(\lambda)\,, \qquad \text{for } \lambda \in \Lambda_f\,. \tag{15}$$

THEOREM 3. *The field $L_\pi T$ and the homomorphism r_π are independent of π.*

For a separable algebraic extension $K \subset k_s$ of k we let $\hat{K}$ denote the completion of K, inside a fixed completion $\hat{k}_s$ of k_s. If K/k is Galois, then the automorphisms of K over k extend uniquely, by continuity, to automorphisms of $\hat{K}$ over k. Let π and $\omega = u\pi$, $u \in U$, be two prime elements in A, and let $f \in \mathcal{F}_\pi$ and $g \in \mathcal{F}_\omega$ be two series of the type we have been considering, belonging to π and to ω, respectively. Let us admit the following lemma whose proof we give later.

LEMMA 2. *Let $\hat{B}$ be the completion of the ring of integers B in the maximal unramified extension T of k. There exists a formal series $\theta(X)$ with coefficients in $\hat{B}$ such that $\theta(X) \equiv \varepsilon X$* (mod deg 2) *with ε a unit, and*

$$\theta^\sigma(X) = \theta\big([u]_f(X)\big)\,, \tag{16}$$

$$\theta\big(F_f(X, Y)\big) = F_g\big(\theta(X), \theta(Y)\big)\,, \tag{17}$$

$$\theta\big([a]_f(X)\big) = [a]_g\big(\theta(X)\big)\,, \qquad \text{for all } a \in A\,. \tag{18}$$

Equations (17) and (18) express the fact that θ is a homomorphism of the formal A-module F_f into the formal A-module F_g. Since $\theta'(0) = \varepsilon$ is a unit, the inverse series $\theta^{-1}(X)$ has coefficients in $\hat{B}$, so $\theta\colon F_f \xrightarrow{\sim} F_g$ is in fact an isomorphism, defined over $\hat{B}$. Hence the map $\lambda \mapsto \theta(\lambda)$ is an isomorphism of Λ_f, the torsion submodule of $M_f(\hat{k}_s)$, onto Λ_g, the torsion submodule of $M_g(\hat{k}_s)$. Thus, $\Lambda_g = \theta(\Lambda_f) \subset \widehat{T(\Lambda_f)} = \widehat{TL_\pi}$, and, by symmetry, $\widehat{TL_\pi} = \widehat{TL_\omega}$. We conclude that $TL_\pi = TL_\omega$, both being the separable algebraic closure of k in $\widehat{TL_\pi}$.

We aim now to show that $r_\omega(\omega) = r_\pi(\omega)$. This will complete the proof of Theorem 3, because, π being arbitrary, it will show that all of the homomorphisms r_π coincide on a given prime element ω, and hence since ω was arbitrary also, and the prime elements ω generate the multiplicative group k^*, that the homomorphisms r_π coincide on k^*. On the field T, the automorphisms $r_\omega(\omega)$ and

$r_\pi(\omega)$ both induce the Frobenius automorphism σ. It will therefore suffice to show that our two automorphisms have the same effect on L_ω. By definition, $r_\omega(\omega)$ is identity on L_ω, and since $L_\omega = k(\Lambda_g)$ is generated over k by the elements $\mu = \theta(\lambda)$ for $\lambda \in \Lambda_f$, we are reduced to showing

$$(19) \qquad \big(\theta(\lambda)\big)^{r_\pi(\omega)} = \theta(\lambda)\,, \qquad \text{for } \lambda \in \Lambda_f\,.$$

Now $r_\pi(\omega) = r_\pi(u)\cdot r_\pi(\pi) = \tau\sigma$, say, where σ is the Frobenius on $\hat{T}$ and is identity on λ, whereas τ is trivial on $\hat{T}$ and carries λ into $[u^{-1}]_f(\lambda)$. Since the series θ has coefficients in $\hat{T}$, we have

$$\theta(\lambda)^{r_\pi(\omega)} = \big(\theta(\lambda)\big)^{\tau\sigma} = \theta^\sigma(\lambda^\tau) = \theta^\sigma\big([u^{-1}]_f(\lambda)\big) = \theta(\lambda)\,,$$

the last equality resulting from (16). This completes the proof of Theorem 3.

COROLLARY. *$L_\pi T$ is the maximal abelian extension of k, and r_π is the reciprocity law homomorphism for it,* i.e. *$r_\pi(a) = (a, L_\pi T/k)$ for $a \in k^*$.*

The first assertion follows from the second, because $L_\pi T$ contains T, and the restriction of r_π to U is injective. (If $u \in U$, and $r_\pi(u) = 1$ on $L_{\pi,m}$, then $u \equiv 1 \pmod{\pi^m}$). Let s: $k^* \to G(L_\pi T/T)$ be the reciprocity law homomorphism, i.e., let $s(a) = (a, L_\pi T/k)$, for $a \in k^*$. If π is a prime element in A, then $s(\pi)$ is identity on $L_\pi = \bigcup L_{\pi,m}$, because π is a norm from $L_{\pi,m}$ for each m, and $s(\pi)$ is the Frobenius automorphism of T. Thus we have $s(\pi) = r_\pi(\pi) = r(\pi)$, where $r = r_\pi$ for all π by Theorem 3. Since the primes π generate k^* this shows $s = r$ and completes the proof of the corollary.

We must still prove Lemma 2. In the number field case, we can use [3, Th. 4.3.2] to get a power series $\theta(X)$ with coefficients in $\hat{B}$ which is an isomorphism between the two formal groups F_f and F_g, so that (17) and (18) are satisfied. It is immediate that $\theta^{-1}\theta^\sigma \in \operatorname{End}(F_f)$, with (say) first-degree coefficient $v \in U$; and since $\theta^{-1}\theta^\sigma[\pi]_f = \theta^{-1}\theta^\sigma f$ and $[\omega]_f = \theta^{-1}[\omega]_g\theta = \theta^{-1}g\theta$ are two endomorphisms of F_f which are congruent (mod π), they are equal (cf. [3]), so that $v\pi = \omega$ and $v = u$, which implies $\theta^{-1}\theta^\sigma = [u]_f$, that is, formula (16).

Another method, which works in the general case, is first to construct, coefficient by coefficient, a series $\theta(X)$ satisfying (16). The construction uses the well known fact that the endomorphism $(\sigma - 1)$ is surjective on the additive group of $\hat{B}$, and also on the multiplicative group of units in $\hat{B}$; (see [4, p 209, cor.] for example). Let ε be a unit in $\hat{B}$ such that $\varepsilon^\sigma = \varepsilon u$, and let $\theta_1(X) = \varepsilon X$. Then, supposing that

$$\theta_r^\sigma(X) \equiv \theta_r\big([u]_f(X)\big) \;\big(\mathrm{mod\ deg}\ (r+1)\big)\,,$$

we try to find b in $\hat{B}$ such that the series $\theta_{r+1}(X) = \theta_r(X) + bX^{r+1}$ satisfies the same congruence to one higher degree. Writing $b = a\varepsilon^{r+1}$, the condition on a becomes

$a-a^{\sigma}=c/\varepsilon^{\sigma(r+1)}$, where c is the coefficient of X^{r+1} in the series $\theta_r^{\sigma}(X)-\theta_r\big([u]_f(X)\big)$. Such an a always exists, and so we obtain a series $\theta = \lim \theta_r$ satisfying (16).

Next, consider the series

$$h = \theta^{\sigma} f \theta^{-1} = \theta[u]_f f \theta^{-1} = \theta[\omega]_f \theta^{-1} .$$

It has coefficients in A, because

$$h^{\sigma} = \theta^{\sigma}[\omega]_f^{\sigma}\theta^{-\sigma} = \theta^{\sigma} f [u]_f \theta^{-\sigma} = \theta^{\sigma} f \theta^{-1} = h .$$

Moreover,

$$h(X) \equiv \varepsilon\omega\varepsilon^{-1}X = \omega X \pmod{\deg 2} ,$$

and

$$h(X) \equiv \theta^{\sigma}\big(f\big(\theta^{-1}(X)\big)\big) \equiv \theta^{\sigma}\big(\big(\theta^{-1}(X)\big)^{q}\big) \equiv \theta^{\sigma}\big(\theta^{-\sigma}(X^{q})\big) \equiv X^{q} \pmod{\pi} .$$

Hence, $h \in \mathcal{F}_{\omega}$. If we replace θ by $[1]_{gh}\theta$, then (16) still holds, but now $g = \theta^{\sigma} f \theta^{-1} = \theta[\omega]_f\theta^{-1}$. To show that (17) holds, we verify that the series $F(X, Y) = \theta\big(F_f(\theta^{-1}(X), \theta^{-1}(Y))\big)$ has the properties characterizing $F_g(X, Y)$: Since F_f "commutes" with $[\omega]_f$, it is obvious that $F = \theta F_f \theta^{-1}$ "commutes" with $g = \theta[\omega]_f\theta^{-1}$; it is equally obvious that $F \equiv X + Y \pmod{\deg 2}$. The remark after Lemma 1 shows that F has coefficients in A. We verify (18) in the same way, by noting that the series $\theta[a]_f\theta^{-1}$ has the properties which characterize $[a]_g$.

BOWDOIN COLLEGE
HARVARD UNIVERSITY

REFERENCES

1. BERNARD DWORK, *Norm residue symbol in local number fields.* Abh. Math. Sem. Hamburg, 22 (1958), 180-190.
2. MICHEL LAZARD, *Sur les groupes de Lie formels à un paramètre.* Bull. Soc. Math. France, 83 (1955), 251-274.
3. JONATHAN LUBIN, *One parameter formal Lie groups over p-adic integer rings,* Ann. of Math., 80 (1964), 464-484.
4. JEAN-PIERRE SERRE, Corps locaux, Hermann, Paris, 1962.

(Received July 6, 1964)