J. LUBIN

J. TATE

Formal moduli for one-parameter formal Lie groups

Bulletin de la S. M. F., tome 94 (1966), p. 49-59

<http://www.numdam.org/item?id=BSMF_1966__94__49_0>

Bull. Soc. math. France,
94, 1966, p. 49 à 60.

FORMAL MODULI FOR ONE-PARAMETER FORMAL LIE GROUPS

BY

JONATHAN LUBIN (1) AND JOHN TATE.

In this paper we study formal Lie groups using methods introduced by LAZARD [2]. This material was exposed in a preliminary form in a seminar at the Woods Hole Institute on Algebraic Geometry in July 1964. All formal groups discussed here are commutative formal Lie groups on *one* parameter, which we will frequently refer to as " group laws ". The reader is referred to [2] and [3] for all basic definitions.

Suppose that $\mathfrak{o}$ is a complete noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field $k = \mathfrak{o}/\mathfrak{m}$ of characteristic $p > 0$. If f is a power series with coefficients in $\mathfrak{o}$, let us call $f^\star$ the power series over k whose coefficients are those of f, reduced modulo $\mathfrak{m}$. Let us say that two group laws, i. e. one-parameter formal Lie groups, F and G, over $\mathfrak{o}$, are $\bigstar$*-isomorphic* if $F^\star = G^\star$ and there is an $\mathfrak{o}$-isomorphism φ between F and G such that $\varphi^\star(x) = x$. We shall show that if Φ is a group law of height $h < \infty$ over k, the set $\mathfrak{G}_{\mathfrak{o}}(\Phi)$ of $\bigstar$-isomorphism classes of group laws F over $\mathfrak{o}$ such that $F^\star = \Phi$ can be put into one-to-one correspondence with the (set-theoretic) product of $\mathfrak{m}$ with itself $(h-1)$ times, in a way that is compatible with extension of the ring $\mathfrak{o}$.

1. Generic group laws of height h.

We give here a construction of a group law Γ which will turn out to be (theorem 3.1) a generic lifting of a given group law Φ of height h. We recall that if $F(x, y)$ is an abelian $(r-1)$-bud over a ring R, i. e. a

(1) This work was supported by a grant from the Research Corporation.

polynomial that behaves modulo degree r like a group law over R (*see* [2], p. 255) then there is an abelian r-bud F' defined over R such that $F \equiv F'$ mod deg r; and if F'' is another such r-bud, then $F' \equiv F'' + aC_r$ mod deg$(r+1)$ for some $a \in R$, where C_r is the modified binomial form, *see* [2], definition 2.5 or [3], definition 3.2.1. We point out that if Φ is a group law defined over a field k of characteristic $p \neq 0$ and if Φ is of height $h < \infty$, then there is Φ' isomorphic to Φ over k such that

$$\Phi'(x, y) \equiv x + y + aC_q(x, y) \bmod \deg (q+1)$$

where $q = p^h$ and a is a non-zero element of k. This can be proved directly from [2], lemma 6 or by applying [3], lemma 3.2.2 to any group law F defined over an appropriate discrete valuation ring $\mathfrak{o}$ with residue field k, such that $F^* = \Phi$.

PROPOSITION 1.1. — *Let k be a field of characteristic $p \neq 0$, and let $\Phi(x, y) \in k[[x, y]]$ be a group law of height $h < \infty$, with $\Phi(x, y) \equiv x + y$ mod deg p^h. Let R be a ring with maximal ideal I, such that $R/I \simeq k$, and let $R[[t]] = R[[t_1, \ldots, t_{h-1}]]$ be the ring of formal power series in $h-1$ letters $t_1, \ldots, t_{h-1}$ over R. Then there is a group law $\Gamma(t_1, \ldots, t_{h-1})(x, y)$ defined over $R[[t_1, \ldots, t_{h-1}]]$ such that :*

1. $\Gamma(0, \ldots, 0)^*(x, y) = \Phi(x, y)$,
2. *For each* $i (1 \leq i \leq h-1)$,

$$\Gamma(0, \ldots, 0, t_i, \ldots, t_{h-1})(x, y) \equiv x + y + t_i C_{p^i}(x, y) \bmod \deg(p^i + 1).$$

Proof. — We start with the abelian 1-bud $x + y$ defined over $R[[t]]$ and complete it to a group law with the desired properties. Suppose for $r > 1$ that we have an abelian $(r-1)$-bud $\Gamma_{r-1}(t_1, \ldots, t_{h-1})$ such that :

1. $\Gamma_{r-1}(0, \ldots, 0)^*(x, y) \equiv \Phi(x, y)$ mod deg r,
2. For each i,

$$\Gamma_{r-1}(0, \ldots, 0, t_i, \ldots, t_{h-1})(x, y) \\ \equiv x + y + t_i C_{p^i}(x, y) \bmod \deg(\min(r, p^i + 1)).$$

Now let Γ'_r be any abelian r-bud defined over $R[[t]]$ such that $\Gamma'_r \equiv \Gamma_{r-1}$ mod deg r.

CASE 1 : $r > p^{h-1}$. — Then

$$\Gamma'_r(0, \ldots, 0)^*(x, y) \equiv \Phi(x, y) + a^* C_r(x, y) \bmod \deg (r+1)$$

for some $a \in R$, by [2], proposition 2, and so we set $\Gamma_r = \Gamma'_r - aC_r$.

CASE 2 : $p^{j-1} < r \leqq p^j$ for some $j \leqq h-1$. — Then our hypotheses on Γ_{r-1} imply that

$$\Gamma'_r(0, \ldots, 0, t_j, \ldots, t_{h-1})(x, y) \equiv x + y + bC_r(x, y) \bmod \deg (r+1) \qquad \text{for} \quad b \in R[[t_j, \ldots, t_{h-1}]]$$

and in this case we let $\Gamma_r = \Gamma'_r - bC_r$ if $r \neq p^j$ and $\Gamma_r = \Gamma'_r + (t_j - b)\, C_r$ if $r = p^j$.

In either case, Γ_r is an abelian r-bud congruent to Γ_{r-1} mod deg r such that:

1. $\Gamma_r(0, \ldots, 0)^*(x, y) \equiv \Phi(x, y)$ mod deg $(r+1)$,
2. For each i,

$$\Gamma_r(0, \ldots, 0, t_i, \ldots, t_{h-1})(x, y) \equiv x + y + t_i C_{p^i}(x, y) \bmod \deg (\min (r+1, p^i+1)).$$

Then if we let $\Gamma = \lim \Gamma_r$, we see that Γ has the desired properties.

2. **The 2-cohomology group of a formal group.**

DEFINITION 2.1. — *Let R be a ring and M an R-module. We denote by $M[[x_1, \ldots, x_n]]$ the module $M \hat{\otimes}_R R[[x_1, \ldots, x_n]]$.*

By this we mean the completion of $M \otimes_R R[[x_1, \ldots, x_n]]$ with respect to the family of submodules $M \otimes_R J^r$, where J is the ideal $(x_1, \ldots, x_n)$ of $R[[x_1, \ldots, x_n]]$. An element of $M[[x_1, \ldots, x_n]]$ can be represented as $\sum \alpha_\mu \mu$, where μ runs through all the monomials in the x's, and each α_μ belongs to M.

It should be observed that $M[[x_1, \ldots, x_n]]$ is not only an $R[[x_1, \ldots, x_n]]$-module, but also has a substitution operation: if $f(x_1, \ldots, x_n) \in M[[x_1, \ldots, x_n]]$ and if $g_1, \ldots, g_n \in R[[y_1, \ldots, y_m]]$ are such that $g_i(0, 0, \ldots, 0) = 0$ for each i, then $f(g_1, \ldots, g_n) \in M[[y_1, \ldots, y_m]]$.

DEFINITION 2.2. — *Let $F(x, y) \in R[[x, y]]$ be a group law and M be an R-module. If $f \in M[[x]]$, then $\delta_F f \in M[[x, y]]$ is defined by*

$$(\delta_F f)(x, y) = f(y) - f(F(x, y)) + f(x).$$

If $f \in M[[x, y]]$, then $\delta_F f \in M[[x, y, z]]$ is defined by

$$(\delta_F f)(x, y, z) = f(y, z) - f(F(x, y), z) + f(x, F(y, z)) - f(x, y).$$

Also, $B^2_M(F)$ is the set of all $f \in M[[x, y]]$ such that $f = \delta g$ for some $g \in M[[x]]$ and $Z^2_M(F)$ is the set of all $f \in M[[x, y]]$ such that $f(x, y) = f(y, x)$ and such that $\delta f = 0$. Since $B^2_M(F) \subset Z^2_M(F)$, we can define $H^2_M(F)$ as $Z^2_M(F)/B^2_M(F)$. Elements of B^2 and Z^2 are called coboundaries and cocycles, respectively.

2.3. — In case F is defined over a field k and M is a finite-dimensional k-vector space, $M[[x_1, \ldots, x_n]]$ is canonically isomorphic to $M \otimes_k k[[x_1, \ldots, x_n]]$. Also, $Z^2_M(F) \cong M \otimes_k Z^2_k(F)$, and similarly for $B^2_M(F)$ and $H^2_M(F)$.

Suppose $f(x, y) \in Z^2_k(F)$ and $f(x, y) \equiv 0 \bmod \deg r$. Then

$$0 = (\delta f)(x, y, z) \equiv f(y, z) - f(x+y, z) + f(x, y+z) - f(x, y) \bmod \deg (r+1)$$

so that by [2], lemma 3, $f(x, y) \equiv aC_r(x, y) \bmod \deg (r+1)$ for some $a \in R$. Similarly, if M is a finite-dimensional vector space over a field k over which F is defined, for each nonzero $f(x, y) \in Z^2_M(F)$, there is an integer r and a nonzero element a of M such that

$$f(x, y) \equiv aC_r(x, y) \bmod \deg (r+1).$$

In the next proposition, we show how the second cohomology group H^2 measures the " infinitesimal deformations " of a formal group. If $\mathfrak{o}$ is a local ring with maximal ideal $\mathfrak{m}$ and residue field $k = \mathfrak{o}/\mathfrak{m}$, let us call ν_r the canonical homomorphism of $\mathfrak{m}^r$ onto the k-vector space $M_r = \mathfrak{m}^r/\mathfrak{m}^{r+1}$, and we will use the same symbol, ν_r, for the corresponding homomorphism between the power-series modules in n variables, over $\mathfrak{m}^r$ and M_r, respectively. We will be dealing with a group law $\Phi(x, y) \in k[[x, y]]$, and we will denote by Φ_1 and Φ_2 the first partial derivatives of Φ with respect to the left- and the right-hand arguments, respectively. Observe that Φ_1 has constant term 1, so that $\Phi_1(0, x)$ has a reciprocal in $k[[x]]$.

Proposition 2.4. — *Let $\mathfrak{o}$, $\mathfrak{m}$, M_r, and Φ be as above. Let F and G be group laws over $\mathfrak{o}$ such that $F^* = G^* = \Phi$. Suppose $\varphi(x) \in \mathfrak{o}[[x]]$ is a power series such that :*

1. $\varphi^*(x) = x$,
2. $\varphi(F(x, y)) \equiv G(\varphi x, \varphi y) \bmod \mathfrak{m}^r$.

Let $\Delta(x, y) \in M_r[[x, y]]$ be defined by

$$\Delta(x, y) = [\Phi_1(0, \Phi(x, y))]^{-1} \cdot \nu_r[\varphi(F(x, y)) - G(\varphi x, \varphi y)].$$

Then $\Delta(x, y) \in Z^2_{M_r}(\Phi)$. Furthermore, $\Delta(x, y) \in B^2_{M_r}(\Phi)$ if and only if there is $\varphi'(x) \in \mathfrak{o}[[x]]$ such that :

1. $\varphi'(x) \equiv \varphi(x) \bmod \mathfrak{m}^r$,
2. $\varphi'(F(x, y)) \equiv G(\varphi' x, \varphi' y) \bmod \mathfrak{m}^{r+1}$.

Finally, such a φ' is unique modulo $\mathfrak{m}^{r+1}$, if Φ is of finite height.

Proof. — We will use the simplifying notation $x \star y$ for $\Phi(x, y)$ and make use of the facts that $\Phi_1(0, x) = \Phi_2(x, 0)$ and $\Phi_1(x, y) \cdot \Phi_1(0, x) = \Phi_1(0, x \star y)$, which are proved by differentiating the identities expressing the commutativity and associativity of Φ, and then setting one of the variables equal to zero.

By abuse of notation, we can say, modulo $\mathfrak{m}^{r+1}$,

$$\varphi(F(x, y)) \equiv G(\varphi x, \varphi y) + \Delta(x, y)\,\Phi_1(o, x \star y) \qquad (\operatorname{mod} \mathfrak{m}^{r+1}).$$

Hence, computing modulo $\mathfrak{m}^{r+1}$ we have :

$$\begin{aligned} \varphi(F(F(x, y), z)) &\equiv G(G(\varphi x, \varphi y) + \Delta(x, y)\cdot\Phi_1(o, x \star y), \varphi z) \\ &\quad + \Delta(x \star y, z)\cdot\Phi_1(o, x \star y \star z) \\ &\equiv G(G(\varphi x, \varphi y), \varphi z) + \Phi_1(x \star y, z) \\ &\qquad \times \Delta(x, y)\cdot\Phi_1(o, x \star y) + \Delta(x \star y, z)\cdot\Phi_1(o, x \star y \star z) \\ &\equiv G(G(\varphi x, \varphi y), \varphi z) + \Phi_1(o, x \star y \star z) \\ &\qquad \times [\Delta(x, y) + \Delta(x \star y, z)]. \end{aligned}$$

Symmetrically,

$$\varphi(F(x, F(y, z))) \equiv G(\varphi x, G(\varphi y, \varphi z)) + \Phi_1(o, x \star y \star z)\cdot[\Delta(y, z) + \Delta(x, y \star z)].$$

Then, since both F and G are associative, we see immediately that $\Delta \in Z^2_{M_r}(\Phi)$.

If we have $\varphi'(x) \in \mathfrak{o}[[x]]$ such that $\varphi'(x) \equiv \varphi(x) \bmod \mathfrak{m}^r$, let us set $\psi(x) = \Phi_1(o, x)^{-1}\cdot\nu_r(\varphi x - \varphi' x)$. Then, again by abuse of notation, we have, modulo $\mathfrak{m}^{r+1}$,

$$\varphi(x) \equiv \varphi'(x) - \Phi_1(o, x)\,\psi(x),$$

and

$$\begin{aligned} \Phi_1(o, x \star y).\Delta(x, y) &\equiv \varphi'(F(x, y)) - \Phi_1(o, x \star y)\cdot\psi(x \star y) \\ &\quad - G(\varphi' x - \Phi_1(o, x)\cdot\psi(x), \varphi' y - \Phi_1(o, y)\cdot\psi(y)) \\ &\equiv \varphi'(F(x, y)) - G(\varphi' x, \varphi' y) - \Phi_1(o, x \star y)\,\psi(x \star y) \\ &\quad + \Phi_1(o, x)\cdot\psi(x)\cdot\Phi_1(x, y) \\ &\quad + \Phi_1(y, o)\cdot\psi(y)\cdot\Phi_1(x, y) \qquad (\operatorname{mod} \mathfrak{m}^{r+1}). \end{aligned}$$

Thus $\Delta(x, y) = \Phi_1(o, x \star y)^{-1}\cdot\nu_r[\varphi'(F(x, y)) - G(\varphi' x, \varphi' y)] + (\delta\psi)(x, y)$.

This shows that $\Delta \in B^2_{M_r}(\Phi)$ is a necessary and sufficient condition for the existence of a series $\varphi'(x)$ satisfying conditions 1 and 2 of the proposition. It remains only to prove the unicity of such a φ' in case Φ is of finite height. If φ'' is another such series, then the difference of φ' and φ'' in $\operatorname{Hom}_{\mathfrak{o}/\mathfrak{m}^{r+1}}(F, G)$ is a homomorphism $\rho \equiv o \bmod \mathfrak{m}^r$. Such a ρ satisfies

$$\rho(F(x, y)) \equiv G(\rho x, \rho y) \equiv \rho x + \rho y \qquad (\operatorname{mod} \mathfrak{m}^{r+1}).$$

Hence the series $h(x) = \nu_{r'}(\rho(x))$ satisfies

$$h(\Phi(x, y)) = h(x) + h(y).$$

By iteration, this implies $h([p](x)) = ph(x) = 0$, where

$$[p](x) = x \star x \ldots \star x$$

is the p-fold endomorphism for the group Φ. Since $[p](x) \neq 0$ for Φ of finite height, we can conclude $h = 0$, and consequently $\varphi' \equiv \varphi'' \bmod \mathfrak{m}^{r'+1}$ in that case.

2.5 Remark. — It should be noted that under the hypotheses of the preceding proposition, Δ is congruent modulo degree n to a coboundary if and only if there is $\varphi(x) \in \mathfrak{o}[[x]]$ such that :

1. $\varphi'(x) \equiv \varphi(x) \bmod \mathfrak{m}^{r}$, and
2. $\varphi'(F(x, y)) \equiv G(\varphi' x, \varphi' y) \bmod \mathfrak{m}^{r+1}$, mod deg n.

We are now in a position to compute $H_k^2(\Phi)$ for Φ a group law of finite height over a field k of characteristic $p \neq 0$:

Proposition 2.6. — *If Φ is a group law of height $h < \infty$, defined over a field k of characteristic $p \neq 0$, then $H_k^2(\Phi)$ is a k-vector space of dimension $h - 1$. If $\Phi(x, y) \equiv x + y$ mod deg p^h, and $\Gamma(t)(x, y)$ is any group law over $k[[t_1, \ldots, t_{h-1}]]$ satisfying the conditions of proposition 1.1 with $R = k$, then the functions*

$$f_i(x, y) = (\Phi_1(0, x\star y))^{-1} \frac{\partial \Gamma}{\partial t_i}(0, \ldots, 0)(x, y) \qquad (1 \leqq i \leqq h - 1),$$

are cocycles satisfying

$$f_i(x,y) \equiv C_{p^i}(x, y) \text{ mod deg } p^i + 1,$$

whose classes form a base for $H_k^2(\Phi)$.

Let $\Phi(x, y)$ and $\Gamma(t)(x, y)$ be as in proposition 1.1, with $R = k$. Apply proposition 2.4 with $\mathfrak{o} = k[\tau]/(\tau^2)$, with $r = 1$, with $\varphi(x) = x$, with $G(x, y) = \Phi(x, y) = \Gamma(0, \ldots, 0)\ (x, y)$ and with $F(x, y) = \Gamma(0, \ldots, 0, \tau, 0, \ldots, 0)\ (x, y)$, where the τ is in the i-th place. Since then

$$F(x, y) = G(x,y) + \tau \frac{\partial \Gamma}{\partial t_i}(0, \ldots, 0)(x, y),$$

we conclude that $f_i(x, y)$ is a cocycle. The fact that

$$f_i(x, y) \equiv C_{p^i}(x, y) \text{ mod deg } p^i + 1$$

is obvious from the definition of f_i, and using this we will now show that the classes of the f_i form a base for $H_k^2(\Phi)$.

For each j, let $g_j(x) = x^j$. Then if j is not a power of p,

$$(\delta g_j)(x, y) \equiv B_j(x, y) \mod \deg (j+1)$$

where $B_j = \lambda C_j$ for λ some nonzero element of k. And if $j = p^s$ for $s \geq 0$, then

$$(\delta g_j)(x, y) \equiv y^j - (\Phi(x, y))^j + x^j \equiv -\alpha^j (C_{p^h}(x, y))^j \mod \deg (jp^h+1),$$

since $\Phi(x, y) \equiv x + y + \alpha C_{p^h}(x, y) \mod \deg (p^h + 1)$ for some $\alpha \neq 0$. But $(C_q(x, y))^p = C_{pq}(x, y)$ in characteristic p, so that $(\delta g_j)(x, y) \equiv \lambda C_{jp^h}(x, y)$ mod deg (jp^h+1), for $\lambda \neq 0$, if j is a power of p. With these facts, we can now show that if $\psi \in Z_k^2(\Phi)$, ψ is equal to a linear combination of the f_i, $(1 \leq i < h)$, plus a coboundary.

Indeed, suppose

$$\psi \equiv \sum \lambda_i f_i + \delta\gamma_{n-1} \mod \deg n,$$

for $\lambda_i \in k$ and $\gamma_{n-1} \in k[[x]]$. It then follows that

$$\psi \equiv \sum \lambda_i f_i + \delta\gamma_{n-1} + aC_n \mod \deg (n+1),$$

for $a \in k$, by 2.3.

Case 1 : $n = p^j$ for $j < h$. — Then since

$$aC_n \equiv af_j \mod \deg (n+1),$$

$\psi \equiv af_j + \sum \lambda_i f_i + \delta\gamma_{n-1}$ so that we can let $\gamma_n = \gamma_{n-1}$.

Case 2 : $n = p^j$ for $j \geq h$. — Let $m = n/p^h = p^{j-h}$. Then

$$aC_n \equiv b\delta g_m \mod \deg (n+1) \text{ for some } b \in k,$$
$$\text{and so we let } \gamma_n = \gamma_{n-1} + bg_m.$$

Case 3 : n is not a power of p. — Then

$$aC_n \equiv b\delta g_n \mod \deg (n+1) \text{ for some } b \in k$$

and so we let $\gamma_n = \gamma_{n-1} + bg_n$.

Since $\gamma = \lim \gamma_n$ exists in $k[[x]]$, we see that ψ is equal to $\delta\gamma$ plus a linear combination of the f_i, which shows that $H_k^2(\Phi)$ is spanned by the classes $\xi_1, \ldots, \xi_{h-1}$ of $f_1, \ldots, f_{h-1}$. But since $\sum \lambda_i f_i(x, y) = (\delta g)(x, y)$ is impossible unless each λ_i is zero, as one sees by considering the equation mod deg (p^i+1) successively for $i = 1, 2, \ldots, h-1$, the ξ_i are linearly independent and so form a basis for $H_k^2(\Phi)$.

2.7. — In the above proposition, we showed that $\dim(H_k^2(\Phi)) \geqq h - 1$ by using $\Gamma(t)$ to find for each $i < h$ a cocycle

$$f_i(x, y) \equiv C_{p^i}(x, y) \bmod \deg(p^i + 1).$$

Such cocycles can be constructed by another method, which we outline here :

If f is a cocycle modulo degree r, then the *r-degree* form φ of δf is a polynomial 3-cocycle in the sense of [1], i. e.

$$\varphi(y, z, w) - \varphi(x + y, z, w) + \varphi(x, y + z, w) - \varphi(x, y, z + w) + \varphi(x, y, z) = 0,$$

and furthermore, φ is " symmetric " in the sense that

$$\varphi(x, y, z) - \varphi(x, z, y) + \varphi(z, x, y) = 0.$$

By [1], page 272, any such 3-cocycle is the coboundary of a symmetric form $\psi(x, y)$:

$$\varphi(x, y, z) = (\partial\psi)(x, y, z) = \psi(y, z) - \psi(x + y, z) + \psi(x, y + z) - \psi(x, y),$$

so that $\delta(f - \psi) \equiv 0 \bmod \deg(r + 1)$. Thus f can be completed to a cocycle in $Z_k^2(\Phi)$, and to construct our f_i, we start off with $C_{p^i}(x, y)$ which is a cocycle modulo degree $(p^i + 1)$.

3. The formal moduli.

THEOREM 3.1. — *Let R, I, k, Φ, and Γ be as in proposition* 1.1. *Let $\mathfrak{o}$ be a complete noetherian local R-algebra, with maximal ideal $\mathfrak{m}$ containing $I\mathfrak{o}$ and residue field $K \supset k$. Let $F(x, y) \in \mathfrak{o}[[x, y]]$ be a group law such that $F^* = \Phi$. Then there is a unique $(h - 1)$-tuple $(\alpha_1, \ldots, \alpha_{h-1})$ of elements of $\mathfrak{m}$, such that F is $\bigstar$-isomorphic to $\Gamma(\alpha)$. Furthermore, there is only one $\bigstar$-isomorphism $\varphi : F \to \Gamma(\alpha)$.*

Proof. — By induction on r we will show that the conclusion is true for the ring $\mathfrak{o}/\mathfrak{m}^r$: there is a unique vector $(\alpha^{(r)})$ of elements of $\mathfrak{m}/\mathfrak{m}^r$ such that F is $\bigstar$-isomorphic modulo $\mathfrak{m}^r$ to $\Gamma(\alpha^{(r)})$, and there is only one $\bigstar$-isomorphism $\varphi^{(r)} : F \to \Gamma(\alpha^{(r)})$, $\varphi^{(r)} \in (\mathfrak{o}/\mathfrak{m}^r)[[x]]$. Uniqueness then implies immediately that $(\alpha) = \lim(\alpha^{(r)})$ and $\varphi = \lim \varphi^{(r)}$ exist and are unique, so that the conclusion is true for the ring $\mathfrak{o}$.

For $r = 1$ there is nothing to be proved. Suppose now that we have $(\alpha) \in (\mathfrak{m})^{h-1}$ and $\varphi \in \mathfrak{o}[[x]]$ such that

$$\varphi^*(x) = x \qquad \text{and} \qquad \varphi(F(x, y)) \equiv \Gamma(\alpha)(\varphi x, \varphi y) \bmod \mathfrak{m}^r,$$

and that such (α) and φ are unique modulo $\mathfrak{m}^r$. We will now construct φ' and (α') such that $\varphi'(x) \equiv \varphi(x) \bmod \mathfrak{m}^r$, for each i, $\alpha'_i \equiv \alpha_i \bmod \mathfrak{m}^r$, and

$$\varphi'(\mathrm{F}(x, y)) \equiv \Gamma(\alpha')(\varphi' x, \varphi' y) \bmod \mathfrak{m}^{r+1}.$$

For each $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_{h-1}) \in (\mathfrak{m}^r)^{h-1}$, let Δ_ε be the cocycle

$$\Delta_\varepsilon(x, y) = (\Phi_1(0, x \bigstar y))^{-1} \nu_r[\varphi(F(x, y)) - \Gamma(\alpha + \varepsilon)(\varphi x, \varphi y)],$$

as in proposition 2.4, where ν_r is the canonical projection of $\mathfrak{m}^r$ onto $M_r = \mathfrak{m}^r/\mathfrak{m}^{r+1}$. Since

$$\Gamma(\alpha + \varepsilon)(\varphi x, \varphi y) - \Gamma(\alpha)(\varphi x, \varphi y) \equiv \sum_{i=1}^{h-1} \frac{\partial \Gamma}{\partial t_i}(\alpha)(\varphi x, \varphi y)\varepsilon_i \bmod \mathfrak{m}^{r+1},$$

we have, on subtracting, and noting $\alpha^\star = 0$, and $\varphi^\star x = x$,

$$\begin{aligned}\Delta_0(x, y) - \Delta_\varepsilon(x, y) &= (\Phi_1(0, x \bigstar y))^{-1} \sum_{i=1}^{h-1} \frac{\partial \Gamma^\star}{\partial t_i}(\alpha^\star)(\varphi^\star x, \varphi^\star y)\, \nu_r(\varepsilon_i) \\ &= \sum_{i=1}^{h-1} f_i(x, y)\, \nu_r(\varepsilon_i),\end{aligned}$$

where the $f_i(x, y)$ are cocycles by proposition 2.6 applied to $\Gamma^\star$. The same proposition shows that there is a family $\varepsilon = (\varepsilon_i)$ such that $\Delta_\varepsilon = 0$, and that such an ε is unique modulo $\mathfrak{m}^{r+1} = \operatorname{Ker} \nu_r$. Putting $\alpha' = \alpha + \varepsilon$ and applying proposition 2.4 we see then that there is a φ' such that $\varphi' \equiv \varphi \bmod \mathfrak{m}^{r+1}$ and

$$\varphi'(F(x, y)) \equiv \Gamma(\alpha')(\varphi' x, \varphi' y) \bmod \mathfrak{m}^{r+1}$$

and that such a φ' is unique mod $\mathfrak{m}^{r+1}$.

3.2. — Thus we see that if Φ is a one-parameter formal group over k, of height $h < \infty$, the set $\mathfrak{G}_{\mathfrak{o}}(\Phi)$ of all $\bigstar$-isomorphism classes of group laws F over $\mathfrak{o}$ such that $F^\star = \Phi$ is in one-to-one correspondence with the set-theoretic product of $\mathfrak{m}$ with itself $(h - 1)$ times.

This correspondence is obviously functorial; the functor $\mathfrak{o} \mapsto \mathfrak{G}_{\mathfrak{o}}(\Phi)$ is isomorphic to the functor $\mathfrak{o} \mapsto (\mathfrak{m})^{h-1}$, for $\mathfrak{o}$ running through the category of complete local noetherian R-algebras, R being a fixed local ring with residue field $k = R/I$.

Proposition 3.3. — *Under the hypotheses of* theorem 3.1, *if* $u \in \operatorname{Aut}_k(\Phi)$, *there is a unique* $(h - 1)$-tuple (α) *of elements of* $\mathfrak{m}$ *and a unique isomorphism* $\varphi \in \operatorname{Hom}_{\mathfrak{o}}(F, \Gamma(\alpha))$ *such that* $\varphi^\star(x) = u(x)$.

Proof. — Let $g(x) \in \mathfrak{o}[[x]]$ be any power series such that $g^{\star}(x) = u^{-1}(x)$. Let $G(x, y) = g^{-1}(F(gx, gy))$. Then since $G^{\star} = \Phi$, we can use theorem 3.1 to get an $(h-1)$-vector (α) of elements of $\mathfrak{m}$ and a $\star$-isomorphism ψ from G to $\Gamma(\alpha)$. Then $\psi \circ g^{-1} = \varphi$ is the isomorphism we want. Uniqueness is clear.

3.4. — If in particular R is a complete noetherian local ring and $\mathfrak{o}$ is $R[[t_1, \ldots, t_{h-1}]]$, then for each $u \in \mathrm{Aut}_k(\Phi)$ there is a unique substitution

$$u^{\cdot} : \quad t_i \mapsto u_i^{\cdot}(t_1, \ldots, t_{h-1})$$

where each $u_i^{\cdot}(t)$ is in the maximal ideal of $R[[t]]$, and a unique isomorphism $\varphi_u \in \mathrm{Hom}_{\mathfrak{o}}(\Gamma(t), \Gamma(u^{\cdot}(t)))$ such that $\varphi_u^{\star} = u$. One sees readily, using uniqueness, that if u and v are k-automorphisms of Φ, then $u^{\cdot}(v^{\cdot}(t)) = (u \circ v)^{\cdot}(t)$ so that $\mathrm{Aut}_k(\Phi)$ has a representation by analytic transformations of the " analytic variety " $\mathfrak{G}_R(\Phi)$. By our construction, $\Gamma(\alpha)$ has an automorphism reducing to u modulo the maximal ideal if and only if for each i, we have $u_i^{\cdot}(\alpha) = \alpha_i$. Thus $u^{\cdot}$ is the identity substitution if and only if $u \in \mathbf{Z}_p$, since by [3], 5.2.1 there are group laws of all heights with endomorphism ring $\mathbf{Z}_p$.

3.5. — We can use this operation of $\mathrm{Aut}_k(\Phi)$ on $\mathfrak{G}_R(\Phi)$ to find an elliptic curve E without complex multiplications but whose associated formal group does have complex multiplications, i. e. endomorphisms not in $\mathbf{Z}_p$.

Take the case $p = 2$, $R =$ the ring of integers of the quadratic unramified extension of $\mathbf{Q}_2$, $k =$ the field with four elements. Consider the elliptic curve E_t defined over $R[[t]]$ which is given by $Y^2 + tXY + Y = X^3$, which has j-invariant equal to $t^3(t^3 - 24)^3/(t^3 - 27)$. The point $(0, 0)$ is an inflection point of E_t, and we can take this as zero-point to make E_t an Abelian variety. If the function X is used as local uniformizing parameter at $(0, 0)$, the group law associated with E_t turns out to be congruent modulo degree 5 to $x + y + txy + 2x^3y + 3x^2y^2 + 2xy^3$ and is therefore a $\Gamma(t)(x, y)$ as in paragraph 1, if we call Φ the height-two group law $\Gamma(0)^{\star}(x, y) \in k[[x, y]]$.

Now consider E_0 which is an Abelian variety with endomorphism ring isomorphic to $\mathbf{Z}[\omega]$ where ω is a primitive cube root of 1. The endomorphism ring of the group law $\Gamma(0)$ contains a subring isomorphic to $\mathbf{Z}[\omega]$ and thus $\mathrm{End}(\Gamma(0)) \cong R$; in other words $\Gamma(0)$ is full in the sense of [3].

Now for $u \in \mathrm{Aut}_k(\Phi)$, we have $u^{\cdot}(0) = 0$ if and only if there is $\varphi \in \mathrm{Aut}_R(\Gamma(0))$ such that $\varphi^{\star} = u$. Thus under the action of $\mathrm{Aut}_k(\Phi)$ on the set $pR \cong \mathfrak{G}_R(\Phi)$, the orbit of 0 is in one-to-one correspondence with the set of left cosets of $(\mathrm{Aut}_R(\Gamma(0)))^{\star}$ in $\mathrm{Aut}_k(\Phi)$. But $\mathrm{Aut}_k(\Phi)$ is isomorphic to the group U of invertible elements in the maximal order of a central division algebra D of rank four over $\mathbf{Q}_2$, and $(\mathrm{Aut}_A(\Gamma(0)))^*$ corresponds to the intersection of U with a commutative subfield of D, so that the index is uncountable. Therefore, there are uncountably many distinct values of $u^*(0)$, and so (in virtue of the j-invariant) uncountably many non-isomorphic elliptic curves $E_{u^*(0)}$ whose formal groups $\Gamma(u^*(0))$ are full. But of course only countably many of these elliptic curves can have complex multiplications.

REFERENCES.

[1] HEATON (R.). — Polynomial 3-cocycles over fields of characteristic p, *Duke. math. J.*, t. 26, 1959, p. 269-275.

[2] LAZARD (Michel). — Sur les groupes de Lie formels à un paramètre, *Bull. Soc. math. France*, t. 83, 1955, p. 251-274.

[3] LUBIN (Jonathan). — One-parameter formal Lie groups over $\mathfrak{p}$-adic integer rings, *Annals of Math.*, t. 80, 1964, p. 464-484.

(Manuscrit reçu le 28 juillet 1965.)

Jonathan LUBIN,
Bowdoin College,
Brunswick, Maine (États-Unis).

John TATE,
Harvard University,
Cambridge, Mass. (États-Unis).