ANNALES DE L'INSTITUT FOURIER

KARL ZIMMERMANN

# Points of order $p$ of generic formal groups

*Annales de l'institut Fourier*, tome 38, nº 4 (1988), p. 17-32

<http://www.numdam.org/item?id=AIF_1988__38_4_17_0>

Ann. Inst. Fourier, Grenoble
**38**, 4 (1988), 17-32.

# POINTS OF ORDER $p$ OF GENERIC FORMAL GROUPS

by Karl ZIMMERMANN

## 0. Introduction.

Let $\mathbb{F}_p$ be the field with $p$ elements and let $\Phi(x,y) \in \mathbb{F}_p[[x,y]]$ be a one dimensional formal group of finite height $h$. The ring of $p$-adic integers will be denoted $\mathbb{Z}_p$. In their paper, « Formal moduli for one parameter formal Lie groups », Lubin and Tate [8] have classified $*$-isomorphism classes of liftings of $\Phi$ to complete local $\mathbb{Z}_p$-algebras $(S,\mathcal{N})$. In particular, they show the existence of a generic formal group $\Gamma_{t_1,\dots,t_{h-1}}(x,y) \in \mathbb{Z}_p[[t_1,\dots,t_{h-1}]][[x,y]]$ of height $h$ which satisfies $\Gamma_{0,\dots,0}(x,y) \times_{\mathbb{Z}_p} \mathbb{F}_p = \Phi(x,y)$ and a universal property which says, in effect, that $*$-isomorphism classes of liftings are determined by continuous homomorphisms $\Psi : \mathbb{Z}_p[[t_1,\dots,t_{h-1}]] \to S$, (each $\Gamma_{\Psi(t_1),\dots,\Psi(t_{h-1})}$ is a canonical representative of an equivalence class). Said two other ways, the isomorphism classes are in one-to-one correspondence with the set theoretic product of $\mathcal{N}$ with itself $(h-1)$-times, or, the formal spectrum of $\mathbb{Z}_p[[t_1,\dots,t_{h-1}]]$ may be thought of as a parameter space for liftings.

There are many similarities between the theory of formal groups of finite height and the theory of elliptic curves. If $h = 2$, the one parameter family of liftings given by $\Gamma_t$ corresponds to the $j$-line in elliptic curve theory. Even more is known in the case of elliptic curves. Let $n > 2$ be an integer and consider pairs $(E,P)$ where $P$ is a point of order exactly $n$ on the elliptic curve $E$. For rings $R$ containing $\frac{1}{n}$

*Key-words :* Generic formal group - Local ring - Newton polygon.

there is associated to this situation a projective curve $\chi_1(n)$ defined over $\mathbb{Z}$ which is almost a moduli space. It almost represents the functor

$$R \mapsto R\text{-isomorphism classes of pairs } (E,P)$$

where $E$ is defined over $R$ and $P \in E(R)$ has order $n$. Moreover, there is another curve, $\chi(n)$ which almost parametrizes triples, $(E,P,Q)$ where $E$ is an elliptic curve and $P$ and $Q$ are points on $E$ that form a $\mathbb{Z}/n\mathbb{Z}$-basis for the $n$-torsion points of $E$. It is the aim of this paper to study the formal group analogue (applied to points of order $p$ on formal groups) of this concept of level structure known in elliptic curve theory. This will involve studying the points of order $p$ of $\Gamma_{t_1,\ldots,t_{h-1}}$ in an algebraic closure of $\mathbb{Z}_p[[t_1,\ldots,t_{h-1}]]$. Using these results, we then define the formal group analogue of the $e_n$-pairing for elliptic curves. In our case, it will be an $\mathbb{F}_p$-multilinear map on the finite group scheme $(\ker[p]_{\Gamma_{t_1,\ldots,t_{h-1}}})^h$ (set theoretic product) with values in the finite groupscheme $\ker[p]_F$ where $F$ is a multiplicative formal group.

The material in this paper is a new example of work done earlier in a more abstract setting. To see the general framework, the reader might wish to consult the book of Katz and Mazur, *Arithmetic Moduli of Elliptic Curves* [4]. Also of interest is the paper of Drindfel'd [3] in which he introduces the theory of elliptic modules. These are but two of the excellent sources available.

Before beginning, I would like to express my gratitude to B. Gross, M. Rosen, and especially Jonathan Lubin for sharing their insights and suggestions with me during the writing of my dissertation (of which this paper is a part).

## 1. The polynomials.

The main object of study in this paper is a generic formal group $\Gamma_{t_1,\ldots,t_{h-1}}(x, y) \in \mathbb{Z}_p[[t_1,\ldots,t_{h-1}]]$ of finite height $h \geqslant 2$. As mentioned in the introduction this is a generic lifting introduced by Lubin and Tate in their paper « Formal moduli for one parameter formal Lie groups » [8]. The reader should consult this paper for all pertinent definitions, and constructions. A briefer, summary of the properties of $\Gamma_{t_1,\ldots,t_{h-1}}$, can be found in Lubin [9].

Key to our purposes is the fact that for a generic formal group defined over $\mathbb{Z}_p[[t_1, \ldots, t_{h-1}]]$ the endomorphism, multiplication by $p$, can be written

$$[p]_{\Gamma_{t_1,\ldots,t_{h-1}}}(x) = pxg_0(x) + \sum_{i=1}^{h-1} t_i x^{p^i} g_i(x) + x^{p^h} g_h(x)$$

where $g_0(x) \in \mathbb{Z}_p[[x]]^*$, $g_i(x) \in \mathbb{Z}_p[[t_1, \ldots, t_i]][[x]]^*$, $i = 1, \ldots, h-1$, and $g_h \in \mathbb{Z}_p[[t_1, \ldots, t_{h-1}]][[x]]^*$. As this notation is somewhat cumbersome, we will let $\mathbb{Z}_p[[t_1, \ldots, t_{h-1}]] = A$, and when refering to a generic formal group we will drop the subscripts altogether. Thus, we write $\Gamma(x, y) \in A[[x, y]]$ for a generic formal group of height $h \geqslant 2$ ($h$, although arbitrary, will be fixed throughout the paper) and refer to multiplication by $n$ on the formal group as $[n](x) \in A[[x]]$.

Now, let $K$ be the field of fractions of $A$ and $\bar{K}$ an algebraic closure of $K$. As in the study of formal groups over a local field we let $\wedge(\Gamma) = \bigcup_{m=1}^{\infty} \{\alpha \in \bar{K} | [p^m](\alpha) = 0\}$, and refer to $\wedge(\Gamma)$ as the group of torsion points of $\Gamma$. The group structure is defined as follows: for $\alpha, \beta \in \wedge(\Gamma)$, $\alpha \oplus \beta = \Gamma(\alpha, \beta)$. This substitution makes sense because $\alpha$ and $\beta$ are non-units in $A[\alpha, \beta]$ which is finite as an $A$-module, hence complete. The formal group endomorphism $[p](x)$ induces a group endomorphism $[p] : \Lambda(\Gamma) \to \Lambda(\Gamma)$, and it is clear that $\ker[p]$ is equal to $\{\alpha \in \bar{K} : [p](\alpha) = 0\}$. The elements of the group $\ker[p]$ will be referred to as the points of order $p$ of $\Gamma$.

The ring $A$ is a complete local ring and therefore, we may apply the Weierstrass Preparation Theorem to the power series $[p](x)/x$. We write $[p](x)/x = P(x)\mu(x)$ where $\mu(x) \in A[[x]]^*$, and $P(x) \in A[x]$ is monic of degree $p^h - 1$ (since the height of $\Gamma$ is $h$). Note that $P(x)$ satisfies the Eisenstein criterion and is therefore irreducible. Furthermore, $\ker[p] = \{0\} \cup \{\alpha \in \bar{K} | P(\alpha) = 0\}$ and so has $p^h$ elements. It is in fact an $h$-dimensional vector space over $\mathbb{F}_p$.

$P(x)$ is one of several polynomials important in the study of the points of order $p$ of $\Gamma$. Let $\gamma_1 \in \bar{K}$ satisfy $P(\gamma_1) = 0$ and define

$$P^{\gamma_1}(x) = \frac{xP(x)}{\prod_{i_1=0}^{p-1} (x - [i_1](\gamma_1))}.$$

Similarly, if $\gamma_2 \in \bar{K}$ satisfies $P^{\gamma_1}(\gamma_2) = 0$, define

$$P^{\gamma_1,\gamma_2}(x) = \frac{xP(x)}{\prod_{i_1,i_2=0}^{p-1} (x-[i_1](\gamma_1))\oplus[i_2](\gamma_2))}.$$

Continuing in this fashion, if $P^{\gamma_1,\ldots,\gamma_{h-2}}(\gamma_{h-1}) = 0$, define

$$P^{\gamma_1,\gamma_2,\ldots,\gamma_{h-1}}(x) = \frac{xP(x)}{\prod_{i_1,\ldots,i_{h-1}=0}^{p-1} (x-[i_1](\gamma_1))\oplus \ldots \oplus[i_{h-1}](\gamma_{h-1}))}.$$

Finally, let $\gamma_h \in \bar{K}$ satisfy $P^{\gamma_1,\ldots,\gamma_{h-1}}(\gamma_h) = 0$ and observe that $\{\gamma_1, \ldots, \gamma_h\}$ is an $\mathbb{F}_p$-basis for the vector space $\ker[p]$. It is possible to shorten notation at this point; let $V_j$ be the vector subspace of $\ker[p]$ generated by $\{\gamma_1, \ldots, \gamma_j\}$. We have $P^{\gamma_1,\ldots,\gamma_j} = \dfrac{xP(x)}{\prod_{\alpha \in V_j}(x-\alpha)}$.

We will show below that for each $j = 1, \ldots, h$, the ring $A[\gamma_1, \ldots, \gamma_j]$ is a complete regular local ring and the polynomial $P^{\gamma_1,\ldots,\gamma_j}(x)$ is defined and irreducible over this ring.

## 2. Certain discrete valuation rings.

The proof of irreducibility of the polynomials introduced in the previous section will depend on the existence of certain rings $\mathcal{O}_i \supseteq A$ where each $\mathcal{O}_i$ is a complete discrete valuation ring. These rings will be constructed via

PROPOSITION 2.1. – *Let $R$ be a complete discrete valuation ring with valuation function $v$. Let $\pi$ be a uniformizer of $R$ with $v(\pi) = \frac{1}{r}$, $r \in \mathbb{N}$. Let $s \in \mathbb{N}$. The ring $R[[x]]$ may be embedded in a complete discrete valuation ring $\mathcal{O}$ whose valuation function extends the original function. Moreover, the element $x$ will be a uniformizer for $\mathcal{O}$, $v(x) = \frac{1}{rs}$.*

*Sketch of the proof.* – If $f(x) = \Sigma a_i x^i \in R[[x]]$ define

$$v(f(x)) = \mathrm{Inf}\left(v(a_i) + \frac{i}{rs}\right).$$

Let

$$\mathcal{O}' = \left\{\frac{f(x)}{g(x)} : f(x), g(x) \in R[[x]], g(x) \neq 0 \quad \text{and} \quad v(f(x)) \geqslant v(g(x))\right\}.$$

$\mathcal{O}'$ is a discrete valuation ring and may be completed to get the desired ring $\mathcal{O}$.

For our purposes, several applications of the proposition will be used to embed $A$ into a ring $\mathcal{O}_i$ satisfying :

$$\begin{aligned} v(t_1) &= 1/p \\ v(t_j) &= \frac{v(t_{j-1})}{p^j - p^{j-1} + 1}, \qquad 1 < j \leqslant i \\ v(t_j) &= v(t_i), \qquad j > i. \end{aligned}$$

## 3. Newton polygons.

We will be able to study the polynomials introduced in section 1 as polynomials defined over complete discrete valuation rings. In particular, we will study their Newton polygons and so a quick review of these polygons is in order.

Let $\mathcal{O}$ be a ring that is complete with respect to a discrete valuation $v$. Let $F$ be the field of fractions of $\mathcal{O}$ and $\bar{F}$ an algebraic closure of $F$. The unique extension of $v$ to $\bar{F}$ will still be referred to as $v$. If $f(z) = \sum_{i=0}^{n} a_i z^i \in F[z]$, the Newton polygon of $f$ is constructed by erecting vertical half-lines on all points $(i, v(a_i)) \in \mathbb{R} \times \mathbb{R}$, and taking the convex hull of the union of these lines. The boundary of this polygon, $\mathcal{N}_F(f)$, has the following property : if $\mathcal{N}_F(f)$ has a segment of width $w$ (length of the projection onto the axis of abscissas) and slope $\mu$, then in $\bar{F}$, there are, counting multiplicity, $\omega$ roots $\rho$ of $f$ with $v(p) = -\mu$. Moreover, a vertex of $\mathcal{N}_F(f)$ will indicate a factorization of $f$ over $F$. To see some details, and for further information about Newton polygons the reader should see Artin [1]. A more complete list of properties may be found in Lubin [10].

We conclude this section with the statement of a lemma that will greatly facilitate the use of the Newton polygon in our situation. The proof is just an interpretation of the conditions in the hypothesis.

LEMMA 3.1. — *Let $\mathcal{O}$ be a complete discrete valuation ring, $f(x) = \sum_{j=0}^{\infty} a_j x^j \in \mathcal{O}[[x]]$. Let $P(x)\mu(x) = f(x)$ where $P(x) \in \mathcal{O}[x]$ and $\mu(x) \in \mathcal{O}[[x]]^*$ arise from the Weierstrass Preparation Theorem.*

*If $f(x)$ satisfies $a_j = 0$ for*

$$j < n_0, v(a_{n_0}) > v(a_{n_1}) > \cdots > v(a_{n_{h-1}}) > v(a_{n_h}) = 0$$

*and when $n_i < \ell < n_{i+1}, v(a_{n_i}) \leqslant v(a_\ell)$ then*

$$\mathcal{N}_{\mathcal{O}}(P(x)) = \mathcal{N}_{\mathcal{O}}\left(\sum_{j=0}^{n_h} a_j x^j\right).$$

It should be remarked that the monic polynomial $P(x)$ and $\sum_{j=0}^{n_h} a_j x^j$ are not likely equal. The lemma says they have the same Newton polygon.

DEFINITION 3.1. — *In the situation of the above lemma, the points $(a_{n_i}, v(a_{n_i})) \in \mathbb{R} \times \mathbb{R}$ will be called the critical points of $\mathcal{N}_{\mathcal{O}}(f)$.*

*Critical points need not be vertices of $\mathcal{N}_{\mathcal{O}}(f)$ although in our application of the lemma to $[p](x)/x$ and $P(x)$ they will be.*

## 4. The regularity of the rings.

In this section, we take a close look at the rings $A$ and $A[\gamma_1, \ldots, \gamma_j]$, $j = 1, 2, \ldots, h$, where $\gamma_1, \ldots, \gamma_h$ are as defined in section 1. The first observation is that $A$ is a complete, regular local ring of dimension $h$ with maximal ideal $M_0 = (p, t_1, \ldots, t_{h-1})$. Our goal is to prove.

THEOREM 4.1. — *Let $\gamma_1, \ldots, \gamma_h$ be chosen as above. For $1 \leqslant k \leqslant h$, $A[\gamma_1, \ldots, \gamma_k]$ is a complete regular local ring of dimension h with maximal ideal $M_k = (\gamma_1, \ldots, \gamma_k, t_k, \ldots, t_{h-1})$.*

*Note.* — The fact that $A[\gamma_1]$ is regular and local of dimension $h$ with maximal ideal $M_1 = (\gamma_1, t_1, \ldots, t_{h-1})$ follows from a general theorem about roots of Eisenstein polynomials over regular local rings (as well as from our proof below). The fact that $A$ is complete then implies $A[\gamma_1]$ is complete.

*Proof.* – We may start by assuming that for $j \leqslant i$ it has been shown that the ring $A[\gamma_1, \ldots, \gamma_j]$ is a complete regular local ring with maximal ideal $M_j = (\gamma_1, \ldots, \gamma_j, t_j, \ldots, t_{h-1})$. Observe that since $A[\gamma_1, \ldots, \gamma_i]$ is complete, terms of the form $[n_1](\gamma_1) \oplus \cdots \oplus [n_i](\gamma_i)$ are in it. We recall that $V_i$ denotes the subspace of $\ker[p]$ generated by $\gamma_1, \ldots, \gamma_i$ and let $g_i(x) = \prod_{0 \neq z \in V_i} (x-z)$. The remark above indicates that $g_i(x) \in A[\gamma_1, \ldots, \gamma_i][x]$. Moreover, since $P(x) = g_i(x) P^{\gamma_1, \ldots, \gamma_i}(x)$ and $P(x) \in A[x]$ it follows that $P^{\gamma_1, \ldots, \gamma_i}(x) \in A[\gamma_1, \ldots, \gamma_i][x]$. We will now show that $P^{\gamma_1, \ldots, \gamma_i}$ is irreducible over $A[\gamma_1, \ldots, \gamma_i]$ which will in turn give information about the ring in question, $A[\gamma_1, \ldots, \gamma_{i+1}]$.

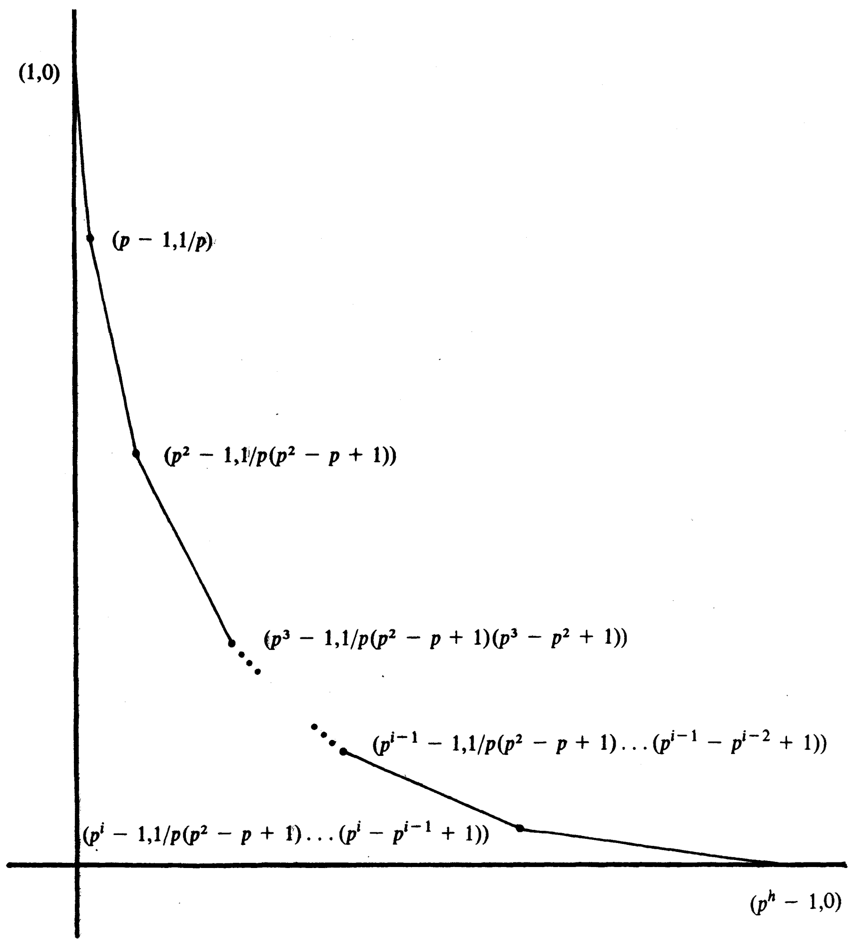


Fig. 1.

Embed the ring $A$ in the complete discrete valuation ring $\mathcal{O}_i$ described in section 2. Observe that $[p](x)/x$ and $P(x)$ satisfy the criteria of lemma 3.1 with critical points $(0,1)$, $(p-1, v(t_1))$, $\ldots$, $(p^i-1, v(t_i))$, and $(p^h-1, 0)$. Thus, we may graph $\mathcal{N}_{\mathcal{O}_i}(P)$ where $P$ is considered a polynomial with coefficients in $\mathcal{O}_i$. (A quick computation, (check the slopes), will show that each critical point is a vertex.) See figure 1.

The breaks in $\mathcal{N}_{\mathcal{O}_i}(P)$ indicate that $P(x)$ factors over $\mathcal{O}_i[x]$ as $P(x) = s_1(x)s_2(x), \ldots, s_i(x)s_{i+1}(x)$. Let $\beta_1, \beta_2, \ldots, \beta_i$ be roots of $s_1(x), \ldots, s_i(x)$ respectively. Each root $\zeta_j$ of $s_j(x)$ satisfies $v(\zeta_j) = v(\beta_j)$ and if $j_1 < j_2$, $v(\zeta_{j_1}) > v(\zeta_{j_2})$. Notice also that all roots of $s_{i+1}(x)$ have value less than the roots of $s_1(x), \ldots, s_i(x)$. A computation shows that $s_j(x) = \Pi(x - [i_1](\beta_1) \oplus \cdots \oplus [i_j](\beta_j))$ where $i_1, \ldots, i_j = 0, 1, \ldots, p-1$ and $i_j = 1, 2, \ldots, p-1$. It therefore must be the case that $s_{i+1}(x) = P^{\beta_1, \ldots, \beta_i}(x)$.

The valuation on $\mathcal{O}_i$ may be extended to $\overline{\mathcal{O}}_i$ and then restricted to $\mathcal{O}_i[\beta_1, \ldots, \beta_i]$. Note that if $\beta \in \mathcal{O}[\beta_1, \ldots, \beta_i]$ then $v(\beta) \geqslant v(\beta_i) = v(P^{\beta_1, \ldots, \beta_i}(0))$. However, all coefficients of $P^{\beta_1, \ldots, \beta_i}(x)$, except that of $x^{p^h-p^i}$, lie in a maximal ideal of $\mathcal{O}_i[\beta_1, \ldots, \beta_i]$ and thus $P^{\beta_1, \ldots, \beta_i}(x)$ satisfies an Eisenstein criterion over that ring and therefore is irreducible. Note that since $A[\beta_1, \ldots, \beta_i] \subseteq \mathcal{O}_i[\beta_1, \ldots, \beta_i]$ we see that $P^{\beta_1, \ldots, \beta_i}(x)$ is irreducible over $A[\beta_1, \ldots, \beta_i]$. Because there is an isomorphism $A[\beta_1, \ldots, \beta_i] \to A[\gamma_1, \ldots, \gamma_i]$ we finally conclude $P^{\gamma_1, \ldots, \gamma_i}$ is irreducible over $A[\gamma_1, \ldots, \gamma_i]$.

Since $P^{\gamma_1, \ldots, \gamma_i}(\gamma_{i+1}) = 0$ and $A[\gamma_1, \ldots, \gamma_i]$ is a unique factorization domain, we have that

$$A[\gamma_1, \ldots, \gamma_{i+1}] \cong A[\gamma_1, \ldots, \gamma_i][x]/(P^{\gamma_1, \ldots, \gamma_i}(x))$$

whence it is complete and local. All that remains to show is regularity. Clearly $M_{i+1} = (\gamma_1, \ldots, \gamma_{i+1}, t_i, \ldots, t_{h-1})$ and it will be shown that $t_i$ can be written in terms of $\gamma_1, \ldots, \gamma_{i+1}, t_{i+1}, \ldots, t_{h-1}$. To this end, we argue as in the beginning of the proof that $P^{\gamma_1, \ldots, \gamma_{i-1}}(x) \in A[\gamma_1, \ldots, \gamma_{i+1}]$. In particular, since

$$P(x) = P^{\gamma_1, \ldots, \gamma_{i+1}}(x) g_{i+1}(x), \left( g_{i+1}(x) = \prod_{0 \neq z \in V_{i+1}} (x - z) \right),$$

we deduce that the first $p^{i+1} - 2$ coefficients of $P$ are in the ideal of $A[\gamma_1, \ldots, \gamma_{i+1}]$ generated by $\gamma_1, \ldots, \gamma_{i+1}$. Now, we will use the fact that $P(x)\mu(x) = [p](x)/x$ and compare coefficients of $x^{p^i-1}$.

Recall that,

$$P(x)\mu(x) = pg_0(x) + t_1x^{p-1}g_1(x) + \cdots + t_ix^{p^i-1}g_i(x) + \cdots + x^{p^h}g_h(x).$$

Let the coefficient of $x^{p^i-1}$ on the left hand side of the above equation be $c$. By remarks above, $c \in (\gamma_1, \ldots, \gamma_{i+1})$. We have $t_iu = c - pb_0 - \sum_{n=1}^{i-1} b_nt_n$ where $b_n \in \mathbb{Z}_p[[t_1, \ldots, t_{h-1}]]$ and $u \in \mathbb{Z}_p^*$. For $j \leqslant i-1$ we may assume $t_j \in (\gamma_1, \ldots, \gamma_{j+1})$ in $A[\gamma_1, \ldots, \gamma_{j+1}]$ and therefore $t_j \in (\gamma_1, \ldots, \gamma_{j+1})$ in $A[\gamma_1, \ldots, \gamma_{i+1}]$. It follows that $t_i \in (\gamma_1, \ldots, \gamma_{i+1})$ in $A[\gamma_1, \ldots, \gamma_{i+1}]$ and so $M_{i+1} = (\gamma_1, \ldots, \gamma_{i+1}, t_{i+1}, \ldots, t_{h-1})$. This completes the proof.

Q.E.D.

The rings of the above theorem, $A[\gamma_1, \ldots, \gamma_j]$, give us the formal group analogue of level structure as mentioned in the introduction. In particular, let $\Phi(x,y) \in \mathbb{F}_p[[x,y]]$ be a formal group of finite height $h$ and let $p$ be the set of all pairs $(F,P)$ where $F$ is a formal group defined over a complete, local $\mathbb{Z}_p$-algebra $(S,\mathcal{N})$ satisfying $Fx_SS/\mathcal{N} = \Phi$ with $P$ a point of $F$ of order $p$. Define an equivalence relation on $p$ as follows: $(F,P) \sim (G,Q)$ if and only if there is a $*$-isomorphism $f: F \to G$ with $f(P) = Q$. Note that if a $*$-isomorphism exists, it will be unique.

Now, note that a continuous homomorphism

$$\Psi: A[\gamma_1] \cong A[x]/(P(x)) \cong A[[x]]/(([p](x) \div x) \to S$$

is determined by the images of $t_1, \ldots, t_{h-1}$ and $x$ in $S$. Thus, the formal spectrum of $A[\gamma_1]$ may be thought of as a parameter space for $p/\sim$ with each equivalence class having a unique representative of the form $(\Gamma_{\psi(t_1), \ldots, \psi(t_{h-1})}, \psi(x))$. The rings $A[\gamma_1, \ldots, \gamma_j]$, $j = 2, \ldots, h$ will play similar roles. Moreover, the fact that the rings are regular indicates that we have smooth families

$$S_pf(A[\gamma_1, \ldots, \gamma_h]) \to S_pf(A[\gamma_1, \ldots, \gamma_{h-1}]) \to \cdots \to S_pf(A).$$

It would be nice to know a bit about the rings $A[\gamma_1, \ldots, \gamma_j]$. It has been conjectured, for example, that in the case $h = 2$, $p = 2$, $A[\gamma_1, \gamma_2] \cong \mathbb{Z}_2[[a,b,c]]/(abc - 2, a+b+c)$ because of the action of $S_3$ on the latter group. I have been unable to show this.

## 5. The Galois group of $K(\ker[p])/K$.

Let $K$ denote the field of fractions of the ring $A$. We may deduce a great deal about the extension of fields $K(\ker[p])/K$ from our previous work. The results of this section will then allow us to define the multilinear map referred to in the introduction.

PROPOSITION 5.1. — *Let $\gamma_1, \ldots, \gamma_h$ be chosen as before. Then $K(\ker[p]) = K(\gamma_1, \ldots, \gamma_h)$. Moreover, $K(\gamma_1, \ldots, \gamma_h)$ is a Galois extension of $K$ of degree $(p^h - 1)(p^h - p) \ldots (p^h - p^{h-1})$.*

*Proof.* — First observe that for $j = 1, 2, \ldots, h$, $K(\gamma_1, \ldots, \gamma_j)$ is the field of fractions of the unique factorization domain $A[\gamma_1, \ldots, \gamma_j]$ and so $p^{\gamma_1, \ldots, \gamma_j}(x)$ is irreducible over $K(\gamma_1, \ldots, \gamma_j)[x]$. Similarly $P(x)$ is irreducible over $K[x]$. To get the final assertion, consider the tower of fields, $K \subseteq K(\gamma_1) \subseteq \ldots \subseteq K(\gamma_1, \ldots, \gamma_h)$.

Now observe that $A[\gamma_1, \ldots, \gamma_h]$ is complete and therefore contains $\ker[p]$. It follows that $K(\ker[p]) = K(\gamma_1, \ldots, \gamma_h)$. Finally note that $K(\gamma_1, \ldots, \gamma_h)$ is a Galois extension of $K$ since it is the splitting field of $P(x)$ over $K$.

Q.E.D.

Let $G$ denote the Galois group of $K(\ker[p])$ over $K$ (or $K(\gamma_1, \ldots, \gamma_h)$ over $K$). There is an injection of groups, $G \hookrightarrow GL_h(\mathbb{F}_p)$ which arises by associating to each $\sigma \in G$, the matrix $(a_{ij})$ where $\sigma(\gamma_i) = \sum_{j=1}^{h} [a_{ij}]\gamma_j$. Since the order of $GL_h(\mathbb{F}_p)$ is precisely $(p^h - 1)(p^h - p) \ldots (p^h - p^{h-1})$ this injection is actually an isomorphism.

Our attention now shifts to the fixed field, $L$, of $SL_h(\mathbb{F}_p)$ in $K(\gamma_1, \ldots, \gamma_h)$. Several properties of $L$ are immediate due to properties of $SL_h(\mathbb{F}_p)$ and the Galois correspondence. In particular, $L$ is a cyclic extension of $K$ of degree $p - 1$. It will be shown that $L$ is the field of fractions of $\mathbb{Z}_p[\pi][[t_1, \ldots, t_{h-1}]]$ where $\pi$ is integral over $\mathbb{Z}_p$.

It is necessary to do some preliminary work before proving the above claim. To that end, let $V$ be an arbitrary vector space of dimension $h$ over $\mathbb{F}_p$. Projective $(h-1)$-space over $\mathbb{F}_p$, $\mathbb{P}^{h-1}(\mathbb{F}_p)$ may be thought of as the dimension one subspaces of $V$. Let $S \subseteq V$ be a complete set of representatives for $\mathbb{P}^{h-1}(\mathbb{F}_p)$. Such a set is characterized by two properties:

i) $S$ contains $p^h - 1/p - 1$ elements (exactly one for each point of $\mathbb{P}^{h-1}(\mathbb{F}_p)$).

ii) Any two distinct elements of $S$ are linearly independent.

In the case at hand, that is $V = \ker[p]$, we have the following,

*Example* 5.1. — Let $\gamma_1, \ldots, \gamma_h$ be as chosen before. Consider

$$I_1 = \{\gamma_1\} \cup \{[i_1](\gamma_1) \oplus \gamma_2\} \cup \ldots \cup \{[i_1](\gamma_1) \oplus \ldots \oplus [i_{h-1}](\gamma_{h-1}) \oplus \gamma_h\}$$

where $i_k = 0, 1, \ldots, p-1$. Clearly the elements of $I_1$ are pairwise linearly independent and there are $p^h - 1/p - 1$ of them. Thus $I$ is a complete set of representatives for $\mathbb{P}^{h-1}(\mathbb{F}_p)$ in $\ker[p]$.

Note that $\ker[p] \subseteq \bar{K}$ and so, given $\alpha$, $\beta \in \ker[p]$ we can multiply them in $\bar{K}$, (actually in $K(\gamma_1, \ldots, \gamma_h)$).

DEFINITION. — *Let* $r = p^h - 1/p - 1$. $X \in \bar{K}$ *is a* $\mathbb{P}$*-mult if* $X = \prod_{j=1}^{r} s_j$ *where* $\{s_1, \ldots, s_r\} \subseteq \ker[p]$ *is a complete set of representatives for* $\mathbb{P}^{h-1}(\mathbb{F}_p)$.

To study $\mathbb{P}$-mults in $\bar{K}$, (clearly they exist) we will use « Lubin's Lemma » (see [6], [5]) essentially as it appeared in his thesis.

LEMMA (Lubin). — *Let $n$ be an integer which is not divisible by $p$ and let $\omega$ be an $n^{th}$ root of unity with $\omega \in R$ (a commutative ring with identity). Let $f(T) \in R[[T]]$ be such that $f^n(T) = T$. Suppose $f(T) = \omega T \bmod \deg 2$. Then there exists $u(T) \in R[[T]]$ such that $u^{-1}(T) \in R[[T]]$ and $f^u(T) = ufu^{-1}(T) = \omega T$.*

The Lemma will be used as follows. Note that the $(p-1)^{st}$ roots of unity are contained in $\mathbb{Z}_p \subseteq A$. Let $\eta$ be a primitive $(p-1)^{st}$ root of unity in $\mathbb{Z}_p$ and observe that $\{1, \eta, \ldots, \eta^{p-2}\}$ form a complete set of multiplicative representatives for $(\mathbb{Z}_p/p\mathbb{Z}_p)^*$ in $\mathbb{Z}_p$. Thus, for every $\alpha \in \ker[p]$, we see that $[\eta](\alpha) = [j](\alpha)$ for some $j = 1, 2, \ldots, p-1$. It is clear that $[\eta](x) = \eta$ mod degree 2, and $[\eta]^{p-1}(x) = x$. There exists, according to the lemma, $u(x) \in A[[x]]$ satisfying $[\eta]^u(x) = u[\eta]u^{-1}(x) = \eta x$. Reparametrize $\Gamma(x,y)$ via $u$, that is, let $\Gamma^u(x,y) = u(\Gamma(u^{-1}(x), u^{-1}(y)))$. If $\alpha \in \ker[p]_\Gamma$ then $u(\alpha) \in \ker[p]_{\Gamma^u}$. Since

$K(\gamma_1, \ldots, \gamma_h) = K(u(\gamma_1), \ldots, u(\gamma_h))$ we may assume without any loss of generality that $\Gamma(x, y)$ satisfies $[\eta]_\Gamma(x) = \eta x$. Letting $\omega_k$ be the $(p-1)^{st}$ root of unity in $\mathbb{Z}_p$ satisfying $\omega_k \equiv k \bmod p$ we have, for each $\alpha \in \ker[p]$, $[k](\alpha) = \omega_k \alpha$. We can now prove

LEMMA 5.1. – *There are exactly $p - 1$ $\mathbb{P}$-mults in $\bar{K}$.*

*Proof.* – Consider the set $I_1$ of example 5.1. To simplify notation, let the elements of $I_1$ be represented by $s_1, \ldots, s_r$ where $r = p^h - 1/p - 1$. Let $I_j = \{[j](s_k) : s_k \in I_1\}$ and observe that for $j = 1, 2, \ldots, p-1$, $I_j \subseteq \ker[p]$ is a complete set of representatives for $\mathbb{P}^{h-1}(\mathbb{F}_p)$. Now consider the following array which lists all non-zero elements of $\ker[p]$:

$$\begin{array}{lccccc}
I_1 & : & s_1 & s_2 & \ldots & s_r \\
I_2 & : & [2](s_1) & [2](s_2) & \ldots & [2](s_r) \\
\vdots & & & & & \\
I_{p-1} & : & [p-1](s_1) & [p-1](s_2) & \ldots & [p-1](s_r)
\end{array}$$

If $X$ is an arbitrary $\mathbb{P}$-mult then it is the product of $r$-elements and clearly no two can come from the same column. Therefore, $X = \prod_{i=1}^{r} [j_i](s_i)$, $j_i = 1, \ldots, p-1$. However, in light of the discussion preceeding this lemma, $X = \prod_{i=1}^{r} \omega_{j_i} \cdot s_i$ where $\cdot$ denotes multiplication in $\bar{K}$. Hence $X = \omega_k \prod_{i=1}^{r} s_i$ for some $k = 1, \ldots, p-1$. Since there are $p - 1$ such $\omega_k$, there are at most $p - 1$ $\mathbb{P}$-mults. Finally, to see that there are exactly $p - 1$ $\mathbb{P}$-mults let $X_j = [j]\, s_1 \prod_{i=2}^{r} s_i$.

Q.E.D.

We will set notation as follows: let $\Delta(\gamma_1, \ldots, \gamma_h) = \prod_{i=1}^{r} s_i$ be the $\mathbb{P}$-mult associated to $I_1$ and for $j = 2, \ldots, p-1$, $\Delta_j(\gamma_1, \ldots, \gamma_h)$ be the $\mathbb{P}$-mult associated to $I_j$; i.e. $\Delta_j(\gamma_1, \ldots, \gamma_h) = \prod_{i=1}^{h} [j](s_i)$.

There is a direct relationship between the $\mathbb{P}$-mults and the polynomial $P(x)$. In particular,

$$P(0) = \prod_{0 \neq z \in \ker[p]} z = \Delta(\gamma_1, \ldots, \gamma_h) \prod_{j=2}^{p-1} \Delta_j(\gamma_1, \ldots, \gamma_h).$$

Since each $\Delta_j(\gamma_1, \ldots, \gamma_h) = \omega_{\ell_j}\Delta(\gamma_1, \ldots, \gamma_h)$ we have $P(0) = \omega_\ell \Delta(\gamma_1, \ldots, \gamma_h)^{p-1}$ for some $\ell = 1, 2, \ldots, p-1$.

Once again we call upon the fact that $[p](x)/(x) = \mathrm{P}(x)\mu(x)$ and comparing the coefficients of the constant term we have $pg_0(0) = \omega_\ell \Delta(\gamma_1, \ldots, \gamma_h)^{p-1}\mu(0)$ where $g_0(0) \in \mathbb{Z}_p^*$ and $\mu(0) \in A^*$. Thus $p = \Delta(\gamma_1, \ldots, \gamma_h)^{p-1}(g(t_1, \ldots, t_{h-1})^{-1})$ where $g(t_1, \ldots, t_{h-1})^{-1} \in A^*$. Let $f(x) = x^{p-1} - \Delta(\gamma_1, \ldots, \gamma_h)^{p-1} = x^{p-1} - g(t_1, \ldots, t_{h-1})p$. This polynomial has as roots, $\omega_k \Delta(\gamma_1, \ldots, \gamma_h)$, $k = 1, 2, \ldots, p-1$, that is, the roots of $f(x)$ are exactly the $\mathbb{P}$-mults. Moreover, since $g(t_1, \ldots, t_{h-1})$ is a unit in $A$, $f(x)$ is irreductible over $A$ by the Eisenstein criterion. We can now prove.

THEOREM 5.1. — *The fixed field of $Sl_h(\mathbb{F}_p)$ in $K(\gamma_1, \ldots, \gamma_h)$ is $L = K(\Delta(\gamma_1, \ldots, \gamma_h))$.*

*Proof.* — Clearly, $K \subseteq K(\Delta(\gamma_1, \ldots, \gamma_h)) \subseteq K(\gamma_1, \ldots, \gamma_h)$ and referring to the discussion preceeding the theorem, we see that

$$[K(\Delta(\gamma_1, \ldots, \gamma_h)) : K] = p - 1 .$$

If $p \neq 2$, $SL_h(\mathbb{F}_p)$ is the commutator subgroup of $GL_h(\mathbb{F}_p)$ (see for example [2]). If $\sigma, \tau \in \mathrm{Gal}(K(\gamma_1, \ldots, \gamma_h)/K)$ then

$$\sigma\tau\sigma^{-1}\tau^{-1}(\Delta(\gamma_1, \ldots, \gamma_h)) = \Delta(\gamma_1, \ldots, \gamma_h)$$

since $\sigma(\Delta(\gamma_1, \ldots, \gamma_h)) = \omega_k(\Delta(\gamma_1, \ldots, \gamma_h))$ for some $k = 1, 2, \ldots, p-1$. Hence the commutators of $G$ are contained in $\mathrm{Gal}(K(\gamma_1, \ldots, \gamma_h)/K(\Delta(\gamma_1, \ldots, \gamma_h)))$. A comparison of dimensions gives the desired result. Finally, when $p = 2$, $\Delta(\gamma_1, \ldots, \gamma_h) = P(0) \in K$.

Q.E.D.

THEOREM 5.2. — *$L$ is a constant field extension. In particular, there exists $\pi \in \overline{\mathbb{Q}}_p$ such that $L = K(\Delta(\gamma_1, \ldots, \gamma_h)) = K(\pi)$ where $\pi \in \overline{\mathbb{Q}}_p$ generates a totally ramified extension of $\mathbb{Q}_p$.*

*Proof.* — We have seen that $L$ is the splitting field of $f(x) = x^{p-1} - pg(t_1, \ldots, t_{h-1})$ where $g(t_1, \ldots, t_{h-1}) \in A^*$. We may write $g(t_1, \ldots, t_{h-1}) = a_0 + r(t_1, \ldots, t_{h-1})$ where $a_0 \in \mathbb{Z}_p^*$ and $r(0, \ldots, 0) = 0$. Thus we have $f(x) = x^{p-1} - a_0 ps(t_1, \ldots, t_{h-1})$ and $s(t_1, \ldots, t_{h-1}) \equiv 1 \bmod \deg 2$. Arguing modulo degree $n$ one constructs $q(t_1, \ldots, t_{h-1}) \in A^*$ with $s(t_1, \ldots, t_{h-1}) = q(t_1, \ldots, t_{h-1})^{p-1}$. Let $\pi$ be a $(p-1)^{st}$ root of $a_0 p$. Then $f(q(t_1, \ldots, t_{h-1})\pi) = 0$ whence $L = K(q(t_1, \ldots, t_{h-1})\pi) = K(\pi)$. To complete the proof, note that $\pi$ satisfies an Eisenstein polynomial with coefficients in $\mathbb{Z}_p$.

Q.E.D.

The following is a corollary of the proof and will be used in the next section. It says, in effect, that $\Delta(\gamma_1, \ldots, \gamma_h)$ is almost an element of $\mathbb{Z}_p[\pi]$.

COROLLARY. — *There exists* $v(t_1, \ldots, t_{h-1}) \in A^*$ *satisfying* $v(t_1, \ldots, t_{h-1})\Delta(\gamma_1, \ldots, \gamma_h) = \pi$.

*Proof.* — This follows easily from the fact that

$$\Delta(\gamma_1, \ldots, \gamma_h)^{p-1} = (\pi q(t_1, \ldots, t_{h-1}))^{p-1}.$$

Q.E.D.

## 6. The multilinear map.

The object at this point is to construct a non-degenerate, alternating multilinear map on the finite groupscheme $\ker[p] \times \cdots \times \ker[p]$ ($h$-times) with values in a finite groupscheme $\ker[p]_F$, where $F$ is a height 1 formal group.

To begin, consider the set $D$ of power series in $A[[x_1, \ldots, x_h]]$ defined below,

$$D = \{x_1\} \cup \{[i_1](x_1) \oplus (x_2)\} \cup \cdots \cup \{[i_1](x_1) \oplus \cdots \oplus [i_{h-1}](x_{h-1}) \oplus x_h\}$$

where $i_k = 0, 1, \ldots, p-1$ and $\oplus$ denotes $+_\Gamma$.

DEFINITION 6.1.

$$\hat{\Delta}(x_1, \ldots, x_h) = v(t_1, \ldots, t_{h-1}) \prod_{d \in D} d \in A[[x_1, \ldots, x_h]].$$

Observe that the result of substituting $\gamma_1, \ldots, \gamma_h$ for $x_1, \ldots, x_h$ *is* $\hat{\Delta}(\gamma_1, \ldots, \gamma_h) = \pi$. We will show that $\hat{\Delta}$ is the multilinear map we seek.

THEOREM 6.1. — *Let* $a_0 \in \mathbb{Z}_p$ *be as defined in Theorem* 5.2. $\hat{\Delta}$ *defines a function whose domain is* $\ker[p] \times \ldots \times \ker[p]$ (*h-times*) *and whose image is* $\ker[p]_F$ *where $F$ is the Lubin-Tate formal group associated to* $-a_0px + x^p$.

*Proof.* — As usual, we consider the basis $\{\gamma_1, \ldots, \gamma_h\}$ for the vector space $\ker[p]$. Identify $(\ker[p])^h$ with $M_h(\mathbb{F}_p)$ in the following manner $(v_1, \ldots, v_h) \leftrightarrow \begin{pmatrix} (v_1) \\ \vdots \\ (v_h) \end{pmatrix}$ where if $v_i = a_{i_1}\gamma_1 + \cdots + a_{ih}\gamma_h$, $(v_i)$ lists the coordinates of $v_i$.

Let $\phi : \mathbb{F}_p \to \mathbb{Z}_p$ be the function $\phi(j) = \omega_j$ if $\omega_j \equiv j \bmod p$ and $\phi(0) = 0 = \omega_0$. Thus the image of $\phi$ is $\{0\} \cup \{(p-1)^{st}$ roots of unity$\} \subseteq \mathbb{Z}_p$. We will show that $\hat{\Delta}(v_1, \ldots, v_h) = \phi \quad \det \begin{pmatrix} (v_1) \\ \vdots \\ (v_h) \end{pmatrix} \quad \pi$. Observe that $\ker[p]_F = \{\phi(j)\pi : j \in \mathbb{F}_p\}$.

*Case i :* $(v_1, \ldots, v_h) \leftrightarrow \begin{pmatrix} (v_1) \\ \vdots \\ (v_h) \end{pmatrix} = M$ and $\det M = 0$.

In this case, the coordinate vectors $(v_1), \ldots, (v_h)$ are linearly dependent. However this is true if and only if $v_1, \ldots, v_h \in \ker[p]$ are linearly dependent. The result follows.

*Case ii :* $(v_1, \ldots, v_h) \leftrightarrow M \in SL_h(\mathbb{F}_p)$.

Here we observe that $M \leftrightarrow \sigma \in \mathrm{Gal}\,(K(\gamma_1, \ldots, \gamma_h)/K(\Delta(\gamma_1, \ldots, \gamma_h))$

$$\begin{aligned} \hat{\Delta}(v_1, \ldots, v_h) &= \hat{\Delta}(\sigma(\gamma_1), \ldots, \sigma(\gamma_h)) \\ &= \sigma(\hat{\Delta}(\gamma_1, \ldots, \gamma_h)) = \hat{\Delta}(\gamma_1, \ldots, \gamma_h) = \pi . \end{aligned}$$

*Case iii :* $(v_1, \ldots, v_h) \leftrightarrow M$, $\det M = j \in \mathbb{F}_p$.

Since any two matrices of determinant $j$ differ by an element of $SL_h(F_p)$, the image of $(v_1, \ldots, v_h)$ is that of $([j](\gamma_1), \ldots, \gamma_h)$. Indeed letting $M_1$ be the matrix associated to $([j](y_1), \ldots, \gamma_h)$, $M = M_1 M_2$ with $M_2 \in SL_h(\mathbb{F}_p)$. Let $\sigma, \sigma_1, \sigma_2$ be the elements of $G$ corresponding to $M, M_1, M_2$.

$$\begin{aligned} \hat{\Delta}(v_1, \ldots, v_h) = \hat{\Delta}(\sigma(\gamma_1), \ldots, \sigma(\gamma_h)) &= \sigma(\hat{\Delta}(\gamma_1, \ldots, \gamma_h)) \\ &= \sigma_1\sigma_2(\hat{\Delta}(\gamma_1, \ldots, \gamma_h)) = \sigma_1(\hat{\Delta}(\gamma_1, \ldots, \gamma_h) \\ &= \hat{\Delta}([j](\gamma_1), \ldots, \gamma_h). \end{aligned}$$

An easy but tedious computation shows $\hat{\Delta}([j](\gamma_1), \ldots, \gamma_h) = \omega_j\pi$.

Q.E.D.

THEOREM 6.2. — *$\hat{\Delta}$ is a multilinear, alternating, non-degenerate map on the finite groupscheme* $(\ker [p])^h$ *with values in* $\ker [p]_F$ *where $G$ is the Lubin-Tate formal group associated to* $- a_0 x + x^p$.

*Proof.* — First observe that if $\dot{+}$ denotes the addition in the $\mathbb{F}_p$-vector space $\ker [p]_F$, we have $\omega_k \pi \dot{+} \omega_\ell \pi = \omega_{k+\ell} \pi$. The proof then follows from Theorem 6.1 and properties of the determinant.

Q.E.D.

## BIBLIOGRAPHIE

[1] E. ARTIN, Algebraic Numbers and Algebraic Functions, Gordon and Breach, New york, 1967.
[2] E. ARTIN, Geometric Algebra, Interscience Publishers, New York, 1957.
[3] V. G. DRINFEL'D, Elliptic modules, Math. USSR Sbornik, Vol. 23, N° 4, (1974), 561-592.
[4] N. KATZ and B. MAZUR, Arithmetic Moduli of Eliptic Curves, Princeton University Press, New Jersey, 1985.
[5] S. LANG, Elliptic curves : Diophantine analysis, Springer Verlag 1978.
[6] J. LUBIN, One parameter formal Lie groups over $p$-adic integer rings, Ann. of Math., 81 (1965), 380-387.
[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 group, Bull. Soc. Math. France, 94 (1966), 49-60.
[9] J. LUBIN, Canonical subgroups of formal groups, Trans. Amer. Math. Soc., 251 (1979), 103-127.
[10] J. LUBIN, The local Kronecker-Weber Theorem, Trans. Amer. Math. Soc., 267 (1981), 133-138.
[11] M. NAGATA, Local Rings, Interscience Publishers, New York, 1962.

Manuscrit reçu le 18 septembre 1987.

Karl ZIMMERMANN,
Union College
Dept. of Mathematics
Schenectady, N.Y. 12308 (USA).