TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 311, Number 1, January 1989

TORSION POINTS OF GENERIC FORMAL GROUPS

MICHAEL ROSEN AND KARL ZIMMERMANN

ABSTRACT. Let F be a generic formal group of height h defined over $A = \mathbf{Z}_p[[t_1, \dots, t_{h-1}]]$. Let K be the quotient field of A. We show the natural map ρ_n: $\mathrm{Gal}(K(\ker[p^n])/K) \to GL_h(\mathbf{Z}/p^n\mathbf{Z})$ isomorphisms for all $n \geq 1$ provided $p \neq 2$.

0. INTRODUCTION

Let F be a one-dimensional formal group defined over a p-adic integer ring R; i.e. R is the maximal compact subring of a finite extension K of $\mathbf{Q}_p$. Much is known about the torsion subgroup of F. In particular, the only torsion is p-power torsion. Denote by $\ker[p^n]_F$ the points in the kernel of the formal group endomorphism $[p^n]_F$ considered as a subset of $\bar{K}$, the algebraic closure of K. If F has height h, it is known that there is a monomorphism ρ_n: $\mathrm{Gal}(K(\ker[p^n]_F)/K) \hookrightarrow GL_h(\mathbf{Z}/p^n\mathbf{Z})$. Let $\Lambda(F) = \bigcup_n \ker[p^n]_F$. The ρ_n piece together to yield a monomorphism ρ: $\mathrm{Gal}(K(\Lambda(F))/K) \hookrightarrow GL_h(\mathbf{Z}_p)$. If F has no complex multiplication (i.e. $\mathrm{End}(F) \cong \mathbf{Z}_p$), Serre has shown in [8] that the image of ρ is open. The main purpose of this paper is to prove a similar result when F is a generic formal group.

Generic formal groups were introduced by Lubin and Tate (see [5]) in order to classify liftings of formal groups defined over a finite field. A generic formal group Γ of height $h \geq 2$ is defined over a power series ring; for our purposes $\mathbf{Z}_p[[t_1, \dots, t_{h-1}]] = A$. (We remark that for a formal group G defined over a complete local Noetherian domain $(R, \mathscr{M})$ of characteristic 0 with residue characteristic p we may define $\ker[p^n]_G$ and $\Lambda(G)$ just as for formal groups defined over p-adic integer rings.) Motivated by Serre's result, and the analogy between a generic formal group and a generic elliptic curve one is led to the conjecture that the monomorphism

$$\mathrm{Gal}(K(\Lambda(\Gamma))/K) \hookrightarrow GL_h(\mathbf{Z}_p) \tag{1}$$

Received by the editors October 2, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 14L05; Secondary 13H05.
Key words and phrases. Generic formal group, Galois representation, local ring, Newton polygon.
The first author was partially supported by the National Science Foundation and the Vaughn Foundation.

(here K is the quotient field of A) is an isomorphism. When $p > 2$, this is exactly what we prove. It is likely that the result is also true when $p = 2$ but we have not succeeded in proving this as yet.

The first step in our proof is to recall that

$$\mathrm{Gal}(K(\ker[p]_\Gamma)/K) \hookrightarrow GL_h(\mathbf{Z}/p\mathbf{Z}) \tag{2}$$

is an isomorphism (see Zimmermann [9]). Secondly, a purely algebraic lemma, which we prove in §1, shows that to prove the monomorphism in (1) is an isomorphism, it suffices for $p > 2$ to show $\mathrm{Gal}(K(\ker[p^2]_\Gamma)/K) \hookrightarrow GL_h(\mathbf{Z}/p^2\mathbf{Z})$ is an isomorphism. This is proven in §2.

We remark that if $p = 2$, it will be shown that if the points of order 8 yield a $GL_h(\mathbf{Z}/8\mathbf{Z})$ extension, then our main result holds when $p = 2$ as well. The "points of order 8" problem is presently under investigation.

After a preliminary version of this paper was circulated, we received a letter from J. P. Serre in which he pointed out that for $p \geq 5$ our main result could be obtained using the isomorphism (2), an algebraic lemma in Serre's book [7] and a theorem of Raynaud on the determinant map for p-divisible groups [6, Theorem 4.2.1]. The advantage of the treatment given here, in addition to handling the case $p = 3$ and providing a method of attack for $p = 2$, is that we use elementary methods throughout. We would like to thank Professor Serre for his comments and for pointing out the case $p = 2$ remains open. (*Added in proof.* The second author has now shown that the monomorphism of equation (1) is also an isomorphism when $p = 2$.)

1. A lemma concerning $GL_h(\mathbf{Z}_p)$

Let π_n be the natural epimorphism from $GL_h(\mathbf{Z}_p)$ to $GL_h(\mathbf{Z}/p^n\mathbf{Z})$.

Lemma 1.1. *Let X be a closed subgroup of $GL_h(\mathbf{Z}_p)$. Suppose*

$$\pi_2(X) = GL_h(\mathbf{Z}/p^2\mathbf{Z}).$$

If $p > 2$ then $X = GL_h(\mathbf{Z}_p)$. If $p = 2$ and $\pi_3(X) = GL_h(\mathbf{Z}/8\mathbf{Z})$ then $X = GL_h(\mathbf{Z}_2)$.

Proof. For $i \geq 1$ define $U_i \subseteq GL_h(\mathbf{Z}_p)$ by $U_i = \{A : A \equiv I \pmod{p^i}\}$. U_i is the kernel of π_i. It is easy to see that $U_i/U_{i+1} \approx M_h(\mathbf{Z}/p\mathbf{Z})$ via the map $I + p^iB \to \widetilde{B}$ where the tilde denotes reduction $\bmod\, p$. It follows from this that

$$U_i = \varprojlim_{j>i} U_i/U_j$$

is a pro-p-group.

Assume that $p > 2$. In this case, we claim that U_2 is the Frattini subgroup of U_1.

Since $U_1/U_2 \approx M_h(\mathbf{Z}/p\mathbf{Z})$, an elementary p-group, it follows that the Frattini subgroup of U_1 is contained in U_2. Since the dimension of $M_h(\mathbf{Z}/p\mathbf{Z})$

over $\mathbf{Z}/p\mathbf{Z}$ is h^2, to finish the proof of our claim, it suffices to find h^2 elements of U_1 which topologically generate U_1. For $\lambda \in \mathbf{Z}_p$, define $E_{ij}(\lambda)$ to be the identity plus the matrix which has all of its entries equal to zero except for a λ in the ij th place. For example, in the 2×2 case we have

$$E_{11}(\lambda) = \begin{pmatrix} 1+\lambda & 0 \\ 0 & 1 \end{pmatrix}, \qquad E_{12}(\lambda) = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix},$$
$$E_{21}(\lambda) = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}, \qquad E_{22}(\lambda) = \begin{pmatrix} 1 & 0 \\ 0 & 1+\lambda \end{pmatrix}.$$

We now show that the set $\{E_{ij}(p)\colon 1 \le i,\ j \le h\}$ topologically generates U_1. Let Y be the closed subgroup of U_1 generated by this set. Every diagonal matrix D in U_1 has the form $E_{11}(p\alpha_1)E_{22}(p\alpha_2)\cdots E_{hh}(p\alpha_h)$ with $\alpha_i \in \mathbf{Z}_p$. For $p > 2$, the principal units in $\mathbf{Z}_p$ are topologically generated by $1+p$. Thus for $\alpha \in \mathbf{Z}_p$ there is a $\beta \in \mathbf{Z}_p$ such that $1 + p\alpha = (1+p)^\beta$. It follows that $D = E_{11}(p)^{\beta_1}E_{22}(p)^{\beta_2}\cdots E_{hh}(p)^{\beta_h} \in Y$.

Recall that for $i \neq j$ multiplying a matrix B on the left by $E_{ij}(\lambda)$ has the effect of multiplying the j th row of B by λ and adding it to the i th row. Similarly, multiplication on the right by $E_{ij}(\lambda)$ has the effect of multiplying the i th column of B by λ and adding it to the j th column.

Suppose $B \in U_1$. We will show that a succession of left and right multiplications by matrices of the form $E_{ij}(px)$ will reduce B to a diagonal matrix. Since for $i \neq j$, $E_{ij}(px) = E_{ij}(p)^x$, this will complete the proof that $Y = U_1$. Note that $B = (b_{ij}) \in U_1$ if and only if $p|b_{ij}$ for $i \neq j$ and $b_{ij} \equiv 1 \pmod p$ for $i = j$. Multiply B on the right by $E_{12}(px_{12})$. The 12 entry of the resulting matrix is $b_{12} + pb_{11}x_{12}$. Since $p|b_{12}$ and b_{11} is a unit, we can choose x_{12} so that this expression is zero. Now multiply the resulting matrix on the right by $E_{13}(px_{13})$. By appropriate choice of x_{13}, we can make the 13 entry of the resulting matrix equal to zero. Continuing in this way, we obtain a matrix in U_1 with all entries on the first row to the right of b_{11} equal to zero. Starting with a right multiplication by $E_{23}(px_{23})$ we can in a similar fashion make all the entries on the second row to the right of b_{22} equal to zero. In finitely many steps we derive a lower triangular matrix in U_1. By an exactly analogous process using left multiplications by matrices of the form $E_{ij}(px_{ij})$ we reduce this lower triangular matrix to a diagonal matrix.

Having now shown that when $p > 2$ U_2 is the Frattini subgroup of U_1 we can proceed to the proof of Lemma 1.1. Consider the diagram

$$(3)\qquad \begin{array}{ccccccccc} (1) & \longrightarrow & X_1 & \longrightarrow & X & \longrightarrow & \pi_1(X) & \longrightarrow & (1) \\ & & \downarrow & & \downarrow & & \downarrow & & \\ (1) & \longrightarrow & U_1 & \longrightarrow & GL_h(\mathbf{Z}_p) & \longrightarrow & GL_h(\mathbf{Z}/p\mathbf{Z}) & \longrightarrow & (1). \end{array}$$

Here, $X_1 = X \cap U_1$ and all of the vertical arrows are inclusions. The right-hand arrow is an isomorphism by hypothesis. Thus, if $X_1 = U_1$ it would follow that $X = GL_h(\mathbf{Z}_p)$ which is what we want to prove.

From (3) we derive

$$(4)\qquad \begin{array}{ccccccccc} (1) & \longrightarrow & X_1 & \longrightarrow & X & \longrightarrow & \pi_1(X) & \longrightarrow & (1) \\ & & \downarrow & & \downarrow & & \downarrow & & \\ (1) & \longrightarrow & U_1/U_2 & \longrightarrow & GL_h(\mathbf{Z}/p^2\mathbf{Z}) & \longrightarrow & GL_h(\mathbf{Z}/p\mathbf{Z}) & \longrightarrow & (1). \end{array}$$

The right-hand vertical arrow is the identity map and by hypothesis the middle vertical arrow is an epimorphism. By the five lemma, $X_1 \to U_1/U_2$ is onto. Since U_2 is the Frattini subgroup of U_1 it follows that $X_1 \to U_1$ is onto, i.e. $X_1 = U_1$. The proof is now complete in the case $p > 2$.

If $p = 2$, the problem is that the group of principal units in $\mathbf{Z}_2$ is not pro-cyclic. However, it is true that $\{a \in \mathbf{Z}_2 \colon a \equiv 1 \pmod 4\}$ is pro-cyclic; in fact, it is topologically generated by the number 5. Using this, one can prove that U_3 is the Frattini subgroup of U_2. Then, as in the last part of the above proof, one can show that $\pi_3(X) = GL_h(\mathbf{Z}/8\mathbf{Z})$ implies $X = GL_h(\mathbf{Z}_2)$. We leave the details to the reader.

Corollary 1.2. *Suppose G is a compact topological group and*

$$\rho\colon G \to GL_h(\mathbf{Z}_p)$$

is a continuous homomorphism. If $p > 2$ and $\pi_2 \circ \rho\colon G \to GL_h(\mathbf{Z}/p^2\mathbf{Z})$ is onto, then ρ is onto. If $p = 2$ and $\pi_3 \circ \rho\colon G \to GL_h(\mathbf{Z}/8\mathbf{Z})$ is onto then ρ is onto.

Proof. This follows immediately by applying Lemma 1.1 to $X =$ image of ρ.

Corollary 1.3. *Let R be a complete, Noetherian, local domain and K the quotient field of R. Suppose the residue class field of R has characteristic $p > 0$. Let F be a one-dimensional formal group of height h defined over R. If $p > 2$ and $\mathrm{Gal}(K(\ker[p^2]_F)/K) \approx GL_h(\mathbf{Z}/p^2\mathbf{Z})$, then $\mathrm{Gal}(K(\Lambda(F))/K) \approx GL_h(\mathbf{Z}_p)$. If $p = 2$ and $\mathrm{Gal}(K(\ker[8]_F)/K) \approx GL_h(\mathbf{Z}/8\mathbf{Z})$, then $\mathrm{Gal}(K(\Lambda(F))/K) \approx GL_h(\mathbf{Z}_2)$.*

Proof. Simply apply Corollary 1.2 to the group $G = \mathrm{Gal}(K(\Lambda F)/K)$.

2. Torsion points of generic formal groups

Let $\Gamma_{t_1, t_2, \dots, t_{h-1}}(x, y) \in \mathbf{Z}_p[[t_1, t_2, \dots, t_{h-1}]][[x, y]]$ be a one-dimensional generic formal group of height h. (For more information about generic formal groups, the reader should see Lubin and Tate [5] or Lubin [3].) To simplify notation, we will denote the formal group $\Gamma_{t_1, t_2, \dots, t_{h-1}}(x, y)$ by $\Gamma(x, y)$, the endomorphism $[p]_{\Gamma_{t_1, \dots, t_{h-1}}}(x)$ by $[p](x)$ and let $A = \mathbf{Z}_p[[t_1, \dots, t_{h-1}]]$. Denote by K, the field of fractions of A and let $\bar{K}$ be the algebraic closure of K.

Since p is a prime in $\mathbf{Z}_p$, multiplication by p on the formal group Γ can be written

$$[p](x) = pxg_0(x) + \sum_{i=1}^{h-1} t_i x^{p^i} g_i(x) + x^{p^h} g_h(x)$$

where $g_0(x)$ is a unit in $\mathbf{Z}_p[[x]]$, $g_i(x)$ is a unit in $\mathbf{Z}_p[[t_1, \dots, t_i]][[x]]$ for $i = 1, 2, \dots, h-1$, and $g_h(x)$ is a unit in $A[[x]]$. Our interest is in the zeros of this power series and its iterates.

Let $\Lambda(\Gamma) = \bigcup_{n=1}^{\infty}$ (zeros in $\bar{K}$ of $[p^n](x)$) and impose a group structure on $\Lambda(\Gamma)$ as follows: if $\alpha, \beta \in \Lambda(\Gamma)$, $\alpha \oplus \beta = \Gamma(\alpha, \beta)$. This substitution makes sense since α and β are nonunits in $A[\alpha, \beta]$ which is finite as an A-module, hence complete.

The formal group endomorphism $[p^n](x)$ determines a group endomorphism $[p^n]: \Lambda(\Gamma) \to \Lambda(\Gamma)$ defined by $\lambda \mapsto [p^n](\lambda)$. It is clear that $\ker([p^n])$ is equal to the set of zeros of $[p^n](x)$ in $\bar{K}$. The elements of $\Lambda(\Gamma)$ are called the torsion points of Γ.

Since A is a complete local ring, the Weierstrass preparation theorem applies. Let $P(x)$ be the polynomial associated to $[p](x)/x$ via the Weierstrass theorem. We observe that $\deg(P(x)) = p^h - 1$ (since the height is h) and of course, $P(x)$ is monic. Furthermore, the zeros of $P(x)$ are the nonzero elements of $\ker[p]$.

A natural first step in the study of $K(\Lambda(\Gamma))/K$ is the study of $K(\ker[p])/K$. In [9], it is shown that this extension is Galois, with Galois group isomorphic to $GL_h(\mathbf{Z}/p\mathbf{Z})$. The extension can be constructed as follows. First observe that $P(x)$ satisfies the Eisenstein criterion over A. Hence, if $P(\gamma_1) = 0$, $\gamma_1 \in \bar{K}$, we have $[K(\gamma_1) : K] = p^h - 1$. Now, define a polynomial

$$P^{\gamma_1}(x) = P(x) \div \sum_{i_1=1}^{p-1} (x - [i_1](\gamma_1)).$$

This polynomial is in $A[\gamma_1][x]$ and in fact it is irreducible over $A[\gamma_1][x]$. Since $A[\gamma_1]$ is integrally closed, $P^{\gamma_1}(x)$ is irreducible over $K(\gamma_1)$. Thus if $\gamma_2 \in \bar{K}$ satisfies $P^{\gamma_1}(x) = 0$, we have $[K(\gamma_1, \gamma_2) : K(\gamma_1)] = p^h - p$. One continues this process by defining

$$P^{\gamma_1\gamma_2}(x) = P^{\gamma_1}(x) \div \prod (x - [i_1](\gamma_1) \oplus [i_2](\gamma_2))$$

where $i_1 = 0, 1, \dots, p-1$, $i_2 = 1, 2, \dots, p-1$. If $\gamma_3 \in \bar{K}$ satisfies $P^{\gamma_1\gamma_2}(\gamma_3) = 0$, $[K(\gamma_1, \gamma_2, \gamma_3) : K(\gamma_1, \gamma_2)] = p^h - p^2$. After h steps we have constructed our extension $K(\gamma_1, \dots, \gamma_h)/K$ of degree $(p^h - 1)(p^h - p) \cdots (p^h - p^{h-1})$. One observes that by construction, $\{\gamma_1, \gamma_2, \dots, \gamma_h\}$ form a linearly independent subset of the h-dimensional $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$ vector space $\ker[p]$ whence it may be concluded $K(\gamma_1, \dots, \gamma_h) = K(\ker[p])$, and $\mathrm{Gal}(K(\ker[p])/K) \approx GL_h(\mathbf{F}_p)$.

We will do a similar analysis of the points of order p^2 of Γ but since many results about the extension of fields $K(\ker[p^2])/K$ are obtained using Newton polygons we will quickly review the construction and the key property of these polygons. Let $\mathscr{O}$ be a ring, complete with respect to a discrete valuation v. Let F be the field of fractions of $\mathscr{O}$ and $\bar{F}$ the algebraic closure of F. The unique extension of v to $\bar{F}$ will also be referred to as v. If $f(z) = \sum a_i z^i \in \mathscr{O}[[z]]$, the Newton polygon of f is constructed by erecting vertical half-lines on all points $(i, v(a_i)) \in \mathbf{R} \times \mathbf{R}$ and taking the convex hull of the union of these lines. The boundary of this polygon $\mathscr{N}_{\mathscr{O}}(f)$, has the following property: if $\mathscr{N}_{\mathscr{O}}(f)$ has a segment of width ω (length of the projection onto the horizontal axis) and slope μ, then in $\bar{F}$, there are, counting multiplicity, ω zeros ρ of f with $v(\rho) = -\mu$. For more information about the Newton polygon the reader may see Lubin [4], Artin [1], or Koblitz [2].

The power series that we are concerned with in this paper are defined over finite extensions of the ring $A = \mathbf{Z}_p[[t_1, \dots, t_{h-1}]]$. To be able to use the power of the Newton polygon we embed A into certain (specifically chosen) complete discrete valuation rings. In fact, the rings will be chosen in a way that will make it easy to observe that certain polynomials, whose zeros are elements of $\ker[p^2]$, are irreducible using the Eisenstein criterion. In particular, we will use

Proposition 2.1. *Let R be a complete discrete valuation ring with valuation function v. Let π be a uniformizer of R with $v(\pi) = 1/r$, $r \in \mathbf{N}$. Let $s \in \mathbf{N}$. The ring $R[[t]]$ may be embedded in a complete discrete valuation ring $\mathscr{O}$ with valuation function (still denoted v) satisfying v restricted to R is unchanged and $v(t) = 1/rs$. The element t will be a uniformizer for $\mathscr{O}$.*

Sketch of the proof. If $f(t) = \sum a_i t^i \in R[[t]]$, define

$$v(f(t)) = \operatorname{Inf}(v(a_i) + i/rs).$$

Let

$$\mathscr{O}' = \{f(t)/g(t) : f(t), g(t) \in R[[t]], g(t) \neq 0, v(f(t)) \geq v(g(t))\}.$$

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

As mentioned before, the above proposition will be used as a tool to study certain polynomials defined over integral extensions of $\mathbf{Z}_p[[t_1, \dots, t_{h-1}]] = A$. Specifically, with several applications of Proposition 2.1, we embed A into the complete discrete valuation right $\mathscr{O}_i$ satisfying:

$$v(t_1) = 1/p^2,$$
$$v(t_j) = \frac{v(t_{j-1})}{p^{2j} - p^{2j-1} + p^j - p^{j-1} + 1} \quad \text{for } 1 < j \leq i,$$
$$v(t_j) = v(t_i) \quad \text{for } i < j \leq h-1.$$

The points of order p^2 on the generic formal group Γ are the zeros in the field $\bar{K}$ of the power series $[p^2](x)$. Of course one of these points is the zero element in $\bar{K}$ and if we let $P_2(x)$ be the polynomial associated to $[p^2](x)/x$ via the Weierstrass preparation theorem, the nonzero points of $\ker[p^2]$ are just the zeros of $P_2(x)$. Our first task will be to determine the Newton polygon of $[p^2](x)$ (and hence $P_2(x)$) considered as a power series over the discrete valuation ring $\mathscr{O}_i$ (defined above).

Recall that since Γ is defined over A,

$$[p](x) = pxg_0(x) + \sum_{i=1}^{h-1} t_i x^{p^i} g_i(x) + x^{p^h} g_h(x)$$

where $g_0(x) \in \mathbf{Z}_p[[x]]^*$, for $L = 1, 2, \ldots, h-1$, $g_i(x) \in \mathbf{Z}_p[[t_1, \ldots, t_i]]^*$, and $g_h(x) \in A[[x]]^*$. It is readily seen that $\mathscr{N}_{\mathscr{O}_i}([p])$ has the shape shown in Figure 1.

Let γ_j be any zero of $[p](x)$ associated to the segment whose vertices are $(p^{j-1}, v(t_{j-1}))$ and $(p^j, v(t_j))$. As in Zimmermann [9], $\gamma_1, \ldots, \gamma_i$ are linearly independent in the $\mathbf{F}_p$-vector space $\ker[p]$. Let γ be associated to the remaining nontrivial segment. To see what values the zeros of $[p^2](x)$ can take on in an algebraic closure of the field of fractions of $\mathscr{O}_i$ (the zeros are actually elements of $\bar{K}$) we need only compute $\mathscr{N}_{\mathscr{O}_i}([p] - \gamma_j)$ and $\mathscr{N}_{\mathscr{O}_i}([p] - \gamma)$. We will then count the number of zeros assuming each value. Since we know that $\mathscr{N}_{\mathscr{O}_i}([p^2])$ has vertices at $(1, 2)$ and $(p^{2h}, 0)$ this completely determines $\mathscr{N}_{\mathscr{O}_i}([p^2])$.

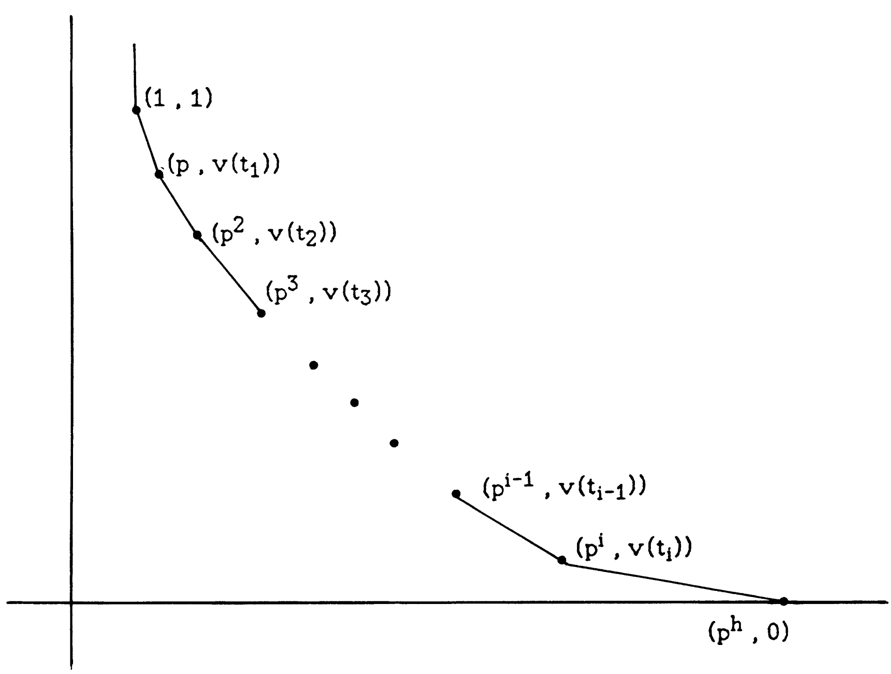

FIGURE 1

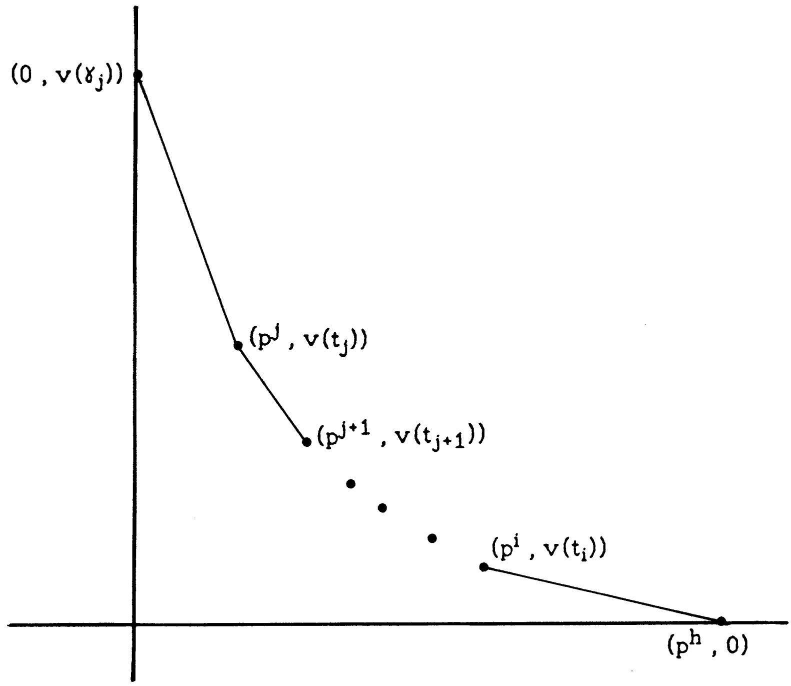

FIGURE 2

The computation of $\mathcal{N}_{\mathcal{O}_i}([p]-\gamma_j)$ is trivial since $[p](x)$ has no constant term. See Figure 2. Let α_j be a zero associated to the leftmost nontrivial segment of the polygon. Note that

$$v(\alpha_j)=\frac{v(t_{j-1})-(p^j-p^{j-1}+1)v(t_j)}{p^{2j}-p^{2j-1}}$$

and by checking $v([p](\alpha_j))$ it is seen we may choose α_j satisfying $[p](\alpha_j)=\gamma_j$. A similar computation using γ will yield elements of $\ker[p^2]$ each having value $v(t_i)/p^{2h}-p^{h+i}$. Thus we may list the possible values for the points of order p^2 of Γ.

$$\begin{aligned}\frac{1-v(t_1)}{p-1}&>\frac{1-pv(t_1)}{p^2-p}>\frac{v(t_1)-v(t_2)}{p^2-p}>\frac{v(t_1)-(p^2-p+1)v(t_2)}{p^4-p^3}\\&>\frac{v(t_2)-v(t_3)}{p^3-p^2}>\cdots>\frac{v(t_{i-1})-v(t_i)}{p^i-p^{i-1}}\\&>\frac{v(t_{i-1})-(p^i-p^{i-1}+1)v(t_i)}{p^{2i}-p^{2i-1}}>\frac{v(t_i)}{p^h-p^i}>\frac{v(t_i)}{p^{2h}-p^{h+i}}.\end{aligned}$$

We observe that there are $2i+2$ possible values for the zeros of $[p^2](x)$ and so $\mathcal{N}_{\mathcal{O}_i}([p^2])$ will have $2i+2$ nontrivial segments. Let S_j, $1 \le j \le 2i+2$, denote the segments corresponding to the values listed above, (i.e. a zero associated to S_1 will have value $1 - v(t_1)/p - 1$ while a zero associated to S_{2i+2} will have value $v(t_i)/p^{2h} - p^{h+i}$.

Notice that if $\beta_1, \beta_2 \in \Lambda(\Gamma)$, $v([i](\beta_1)) = v(\beta_1)$, $i = 1, \dots, p-1$; and

$$v(\beta_1 \oplus \beta_2) \ge \min\{v(\beta_1), v(\beta_2)\}.$$

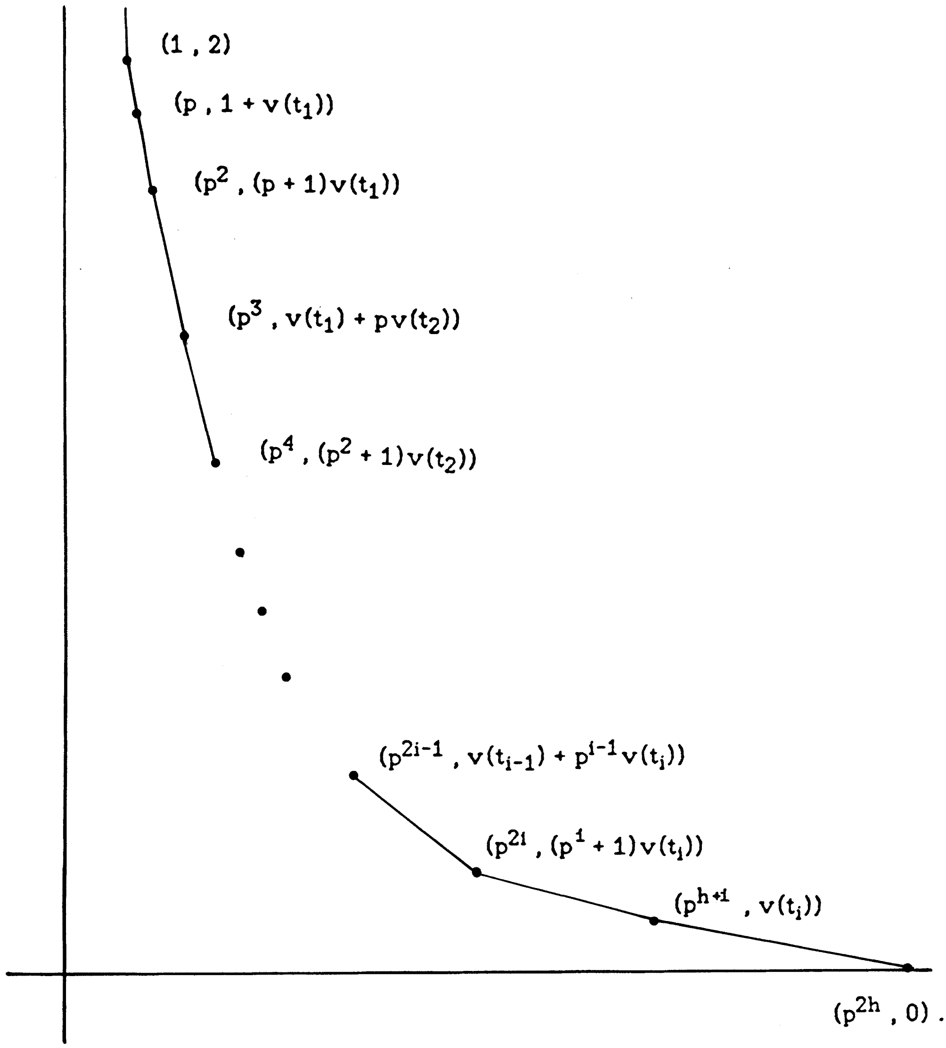

FIGURE 3

Thus if β is a zero associated to S_{2j}, $j = 1, 2, \dots, i$, $\beta = [m_1](\gamma_1) \oplus \cdots \oplus [m_j](\gamma_j) \oplus [n_1](\alpha_1) \oplus \cdots \oplus [n_j](\alpha_j)$ where $n_j = 1, 2, \dots, p-1$ and all other coefficients vary from 0 to $p-1$. Thus, there are $p^{2j} - p^{2j-1}$ zeros associated to S_{2j}. Similarly, one sees that the zeros associated to S_{2j-1}, $j = 1, 2, \dots, i$, are $\beta = [m_1](\gamma_1) \oplus \cdots \oplus [m_j](\gamma_j) \oplus [n_1](\alpha_1) \oplus \cdots \oplus [n_{j-1}](\alpha_{j-1})$ where $m_j \neq 0$ but all other coefficients may vary from 0 to $p-1$. Thus there are $p^{2j-1} - p^{2j-2}$ zeros associated to S_{2j-1}. If we let γ be a zero of $[p](x)$ with $v(\gamma) = v(t_i)/(p^h - p^i)$ (there are $p^h - p^i$ such γ's) then any root associated to S_{2i+1} will have the form $\beta = \gamma \oplus [n_1](\alpha_1) \oplus \cdots \oplus [n_i](\alpha_i)$. Thus, there are $p^i(p^h - p^i)$ such β. The number of zeros associated to S_{2i+2} must be $p^{2h} - p^{h+i}$.

Since we know that $[p^2](x) \in \mathscr{O}_i[[x]]$, and the initial vertex of $\mathscr{N}_{\mathscr{O}_i}([p^2](x))$ is $(1, 2)$ while $(p^{2h}, 0)$ is the first potential vertex which lies on the horizontal axis, we can construct the Newton polygon of $[p^2](x)$ as in Figure 3. We remark that with γ_j, $j = 1, 2, \dots,$ i chosen as above, it is shown in [9] that

$$[K(\gamma_1, \dots, \gamma_j) : K(\gamma_1, \dots, \gamma_{j-1})] = p^h - p^{j-1}.$$

Now, to set notation, let $s_k(x)$, $k = 1, 2, \dots, 2i+2$, be the polynomial associated to segment S_k of $\mathscr{N}_{\mathscr{O}_i}([p^2])$. We may write these polynomials explicitly. For $k = 1, 2, \dots, 2i$ we observe that $s_k = \prod(x - \beta)$ where β runs through the zeros associated to S_k. We will be slightly more explicit in the case $k = 2i-1$. Let $\gamma_{i+1}, \gamma_{i+2}, \dots, \gamma_h$ be chosen so that $\{\gamma_1, \dots, \gamma_h\}$ is a basis for the $\mathbf{F}_p$-vector space $\ker[p]$. Then

$$s_{2i+1}(x) = \prod(x - [m_1](\gamma_1) \oplus \cdots \oplus [m_h](\gamma_h) \oplus [n_1](\alpha_1) \oplus \cdots \oplus [n_i](\alpha_i))$$

where all coefficients vary from 0 to $p-1$ but $\sum_{k=1}^{h-i} m_{i+k} \neq 0$.

The polynomial $s_{2i+2}(x)$ is of key importance at this stage and to emphasize this, and its dependence on i we will rename it, $s_{2i+2}(x) = f_i(x)$. It is our claim that $f_i(x)$ is irreducible over $A[\alpha_1, \dots, \alpha_i]$ but it first must be shown that $f_i(x) \in A[\alpha_1, \dots, \alpha_i][x]$. Initially, we will use Galois theory to show $f_i(x) \in K(\alpha_1, \dots, \alpha_i)[x]$.

To that end, consider the following diagram of field extensions

$$K(\alpha_1, \dots, \alpha_i, \gamma_{i+1}, \dots, \gamma_h) = L_i$$

$$F_i = K(\alpha_1, \dots, \alpha_i) \qquad K(\gamma_1, \dots, \gamma_h) = K(\ker[p]).$$

$$K$$

As mentioned before, $K(\gamma_1, \dots, \gamma_h)$ is Galois over K, so by extension of the base, L_i is Galois over F_i. Let $g_i(x) = \prod_{j=1}^{2i} s_j(x) s_{2i+1}(x)$, and observe

$$g_i(x) = \prod(x - [m_1](\gamma_1) \oplus \cdots \oplus [m_h](\gamma_h) \oplus [n_1](\alpha_1) \oplus \cdots \oplus [n_i](\alpha_i))$$

where m_i, $n_i = 0, \dots, p-1$. Clearly, $g_i(x)$ splits in L_i. Now, let $\sigma \in \mathrm{Gal}(L_i/F_i)$ and observe that if $\beta_1, \beta_2 \in \Lambda(\Gamma)$, $\sigma(\beta_1 \oplus \beta_2) = \sigma(\beta_1) \oplus \sigma(\beta_2)$ and $\sigma([i](\beta_1)) = [i]\sigma(\beta_1)$. Since σ fixes $\alpha_1, \dots, \alpha_i$ and σ must take a point of order p (of Γ) to a point of order p, $g_i^\sigma(x) = g_i(x)$ whence $g_i(x) \in K(\alpha_1, \dots, \alpha_i)$. However, $g_i(x) f_i(x) = xP_2(x)$ and since $g_i(x)$, $xP_2(x) \in K(\alpha_1, \dots, \alpha_i)$ it follows that $f_i(x) \in K(\alpha_1, \dots, \alpha_i)[x]$.

Proposition 2.2. *The ring $A[\alpha_1, \dots, \alpha_i]$ is a complete regular local ring of dimension h, with maximal ideal $\mathscr{M}_i = (\alpha_1, \alpha_2, \dots, \alpha_i, t_i, \dots, t_{h-1})$. Moreover $f_i(x) \in A[\alpha_1, \dots, \alpha_i][x]$ and is irreducible over $A[\alpha_1, \dots, \alpha_i]$.*

Proof. The proof depends on the fact (proved in [9]) that $A[\gamma_1, \dots, \gamma_i]$ is a complete regular local ring of dimension h with maximal ideal $(\gamma_1, \gamma_2, \dots, \gamma_i, t_i, t_{i+1}, \dots, t_{h-1})$. First observe that $A[\alpha_1]$ is a complete regular local ring of dimension h with maximal ideal $\mathscr{M}_1 = (\alpha_1, t_1, \dots, t_{h-1})$ since α_1 satisfies $P_2(x)/P(x)$ which is an Eisenstein polynomial defined over A. ($P(x)$ is the polynomial associated to $[p](x)/x$ via the Weierstrass preparation theoerm). In particular, $A[\alpha_1]$ is integrally closed in a field of fractions $K(\alpha_1)$. However, $f_1(x) \in K(\alpha_1)[x]$ and all roots of $f_1(x)$ are integral over A whence $f_1(x) \in A[\alpha_1][x]$. Furthermore, $A[\alpha_1][x] \subseteq \mathscr{O}_1[\alpha_1][x]$ and $f_1(x)$ satisfies the Eisenstein criterion over $\mathscr{O}_1[\alpha_1][x]$. This follows because $v(f_1(0)) = v(t_1)$ which is the least value of any element in $\mathscr{O}_1[\alpha_1]$. (Note that if $i \neq j$ the valuation function on $\mathscr{O}_i$ is not equal to the valuation function on $\mathscr{O}_j$. Since no confusion should arise we will however write the valuation on all rings $\mathscr{O}_i$ as v.) Thus $f_1(x)$ is irreducible over $A[\alpha_1]$, and so $A[\alpha_1, \alpha_2] \cong A[\alpha_1][x]/(f_1(x))$. This shows that $A[\alpha_1, \alpha_2]$ is complete and local. If it can be shown that $A[\alpha_1, \alpha_2]$ is regular of dimension h, Proposition 2.2 will follow by continuing in the manner we have indicated thus far. To show regularity, we note that $M_2 = (M_1, \alpha_2) = (\alpha_1, \alpha_2, t_1, \dots, t_{h-1})$. However, $t_1 \in (\gamma_1, \gamma_2, t_2, \dots, t_{h-1})$, the maximal ideal in $A[\gamma_1, \gamma_2]$ and so certainly t_1 can be expressed in terms of $\alpha_1, \alpha_2, t_2, \dots, t_{h-1}$ in $A[\alpha_1, \alpha_2]$.

Corollary 2.3. *$f_i(x)$ is irreducible over $K(\alpha_1, \dots, \alpha_i)[x]$, for $i = 1, 2, \dots, h-1$.*

Proof. The corollary follows since $A[\alpha_1, \dots, \alpha_i]$ is a regular local ring and hence a unique factorization domain.

The results thus far, will allow us to complete our study of $K(\ker[p^2])/K$.

Theorem 2.4. *With notation as above,* $[K(\alpha_1, \dots, \alpha_{i+1}) : [K(\alpha_1, \dots, \alpha_i)] = p^{2h} - p^{h+i}$.

Corollary 2.5. $[K(\alpha_1, \dots, \alpha_i)] : K(\gamma_1, \dots, \gamma_i)] = p^{ih}$.

We record the following as a special case.

Corollary 2.6. $[K(\alpha_1, \dots, \alpha_h) : K(\gamma_1, \dots, \gamma_h)] = p^{h^2}$.

As stated earlier, there is a monomorphism

$$\mathrm{Gal}(K(\ker[p^2])/K) \to GL_h(\mathbf{Z}/p^2\mathbf{Z}).$$

We now see that $[K(\ker[p^2]) : K] = |GL_h(\mathbf{Z}/p^2\mathbf{Z})|$.

Theorem 2.7. *If* Γ *is a generic formal group defined over* $\mathbf{Z}_p[[t_1, \dots, t_{h-1}]]$, *then* $\mathrm{Gal}(K(\ker[p^2])/K) \cong GL_h(\mathbf{Z}/p^2\mathbf{Z})$.

3. Concluding remarks

We begin this section with a restatement of the main results proven in this paper. Following this will be some remarks and acknowledgments.

Theorem 3.1. *Let* $\Gamma_{t_1, \dots, t_{h-1}}(x, y) \in \mathbf{Z}_p[[t_1, \dots, t_{h-1}]][[x, y]]$ *be a generic formal group of height* $h \geq 2$. *Let* K *be the field of fractions of* $\mathbf{Z}_p[[t_1, \dots, t_{h-1}]]$ *and* $\bar{K}$ *an algebraic closure of* K. *Denote by* $\Lambda(\Gamma) \subset \bar{K}$ *the group of torsion points of* $\Gamma_{t_1, \dots, t_{h-1}}(x, y)$. *Then* $\mathrm{Gal}(K(\Lambda(\Gamma))/K) \cong GL_h(\mathbf{Z}_p)$.

Corollary 3.2. *With notation as in Theorem* 3.1,

$$\mathrm{Gal}(K(\ker[p^m]_\Gamma)/K) \cong GL_h(\mathbf{Z}/p^m\mathbf{Z}).$$

1. The results about generic formal groups depend on the fact that

$$[p]_\Gamma(x) = pg_0(x) + \sum_{i=1}^{h-1} x^{p^i} t_i g_i(x) + x^{p^h} g_h(x).$$

Multiplication by p on Γ has this form if Γ is defined over $\mathscr{O}[[t_1, \dots, t_{h-1}]]$ where $\mathscr{O}$ is an unramified extension of $\mathbf{Z}_p$. Thus our results could be stated in a slightly more general form replacing $\mathbf{Z}_p$ with θ.

2. $\mathrm{Gal}(K(\Lambda(\Gamma))/K)$ and $\mathrm{End}_A(\Gamma)$ both act on $T(\Gamma) = \varprojlim \ker[p^m]_\Gamma \cong \mathbf{Z}_p^h$ and the actions commute. It follows easily from this and Theorem 3.1 that $\mathrm{End}_A(\Gamma) \cong \mathbf{Z}_p$.

3. It follows from Corollary 3.2 that the groups $GL_h(\mathbf{Z}/p^m\mathbf{Z})$ occur as Galois groups of Galois extensions of K, the quotient field of $\mathscr{O}[[t_1, \dots, t_{h-1}]]$. This does not seem to be readily apparent on other grounds.

4. Lemma 1.1 can be viewed as a generalization of the fact that for p an odd prime, a primitive root $\bmod p^2$ is a primitive root modulo all higher powers of p. For, suppose $X \subseteq GL_1(\mathbf{Z}_p) = \mathbf{Z}_p^*$ is a closed subgroup mapping into $GL_1(\mathbf{Z}/p^2\mathbf{Z}) \cong (\mathbf{Z}/p^2\mathbf{Z})^*$. Then there is an integer $b \in X$ which is a primitive root $\bmod p^2$ and thus a primitive root $\bmod p^n$ for all $n \geq 1$. Thus b topologically generates $\mathbf{Z}_p^*$ and so $X = \mathbf{Z}_p^*$ since X is closed.

5. Let $H \subseteq GL_h(\mathbf{Z}_2)$ be the subgroup of matrices of determinant ± 1. Then $\pi_2(H) = GL_h(\mathbf{Z}/4\mathbf{Z})$. This shows we must consider π_3 when $p = 2$. (This was pointed out by J. P. Serre.) Nevertheless, it seems extremely likely that our main result is also true for $p = 2$.

6. The authors would like to thank L. Tatevossian, S. Shatz, and J. Lubin for many helpful discussions about this paper. In particular, it was Professor Lubin who suggested the straightforward method used to compute $\mathscr{N}_{\mathscr{O}_i}([p^2])$, replacing our original calculation which was quite complicated and somewhat tedious. Also, we would like to thank J. P. Serre for his helpful comments, mentioned above and in the Introduction.

BIBLIOGRAPHY

1. E. Artin, *Algebraic numbers and algebraic functions*, Gordon and Breach, New York, 1967.
2. N. Koblitz, *p-adic numbers, p-adic analysis, and zeta functions*, Springer-Verlag, New York, 1977.
3. J. Lubin, *Canonical subgroups of formal groups*, Trans. Amer. Math. Soc. **251** (1979), 103–127.
4. ——, *The local Kronecker-Weber Theorem*, Trans. Amer. Math. Soc. **267** (1981), 133–138.
5. J. Lubin and J. Tate, *Formal moduli for one parameter formal Lie groups*, Bull. Soc. Math. France **94** (1966), 49–60.
6. M. Raynaud, *Schemas en groups de type* $(p, \dots, p)$, Bull. Soc. Math. France **102** (1974), 241–280.
7. J. P. Serre, *Abelian l-adic representations and elliptic curves*, Benjamin, New York and Amsterdam, 1968.
8. ——, *Sur les group de Galois attaché aux groups p-divisible*, Proc. Conf. on Local Fields, Driebergen, Springer-Verlag, Berlin and New York, 1967, pp. 113–131.
9. K. Zimmermann, *Points of order p of generic formal groups*, Ann. Inst. Fourier (to appear).

DEPARTMENT OF MATHEMATICS, BROWN UNIVERSITY, PROVIDENCE, RHODE ISLAND 02912

DEPARTMENT OF MATHEMATICS, UNION COLLEGE, SCHENECTADY, NEW YORK 12308