PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 102, Number 1, January 1988

GALOIS ENDOMORPHISMS OF THE TORSION SUBGROUP OF ONE-PARAMETER GENERIC FORMAL GROUPS

KARL ZIMMERMANN

(Communicated by William C. Waterhouse)

ABSTRACT. Let $\mathbf{Z}_p$ be the ring of p-adic integers and let Γ be a one-parameter generic formal group of finite height h defined over $\mathbf{Z}_p[[t_1, \ldots, t_{h-1}]] = A$. Let K be the field of fractions of A, $G = \mathrm{Gal}(\overline{K}/K)$ and $T(\Gamma)$ the Tate module of Γ. The purpose of this paper is to give an elementary proof that the map $\mathrm{End}_A(\Gamma) \to \mathrm{End}_G(T(\Gamma))$ is a surjection.

1. Introduction. In [**4**], using some deep results from class field theory and algebraic geometry, Tate proved the following

THEOREM. *Let R be an integrally closed, noetherian, integral domain whose field of fractions K is of characteristic zero. Let F and H be p-divisible groups defined over R, and let $T(F)$, $T(H)$ be the Tate modules of F and H respectively. The map* $\mathrm{Hom}_R(F, H) \to \mathrm{Hom}_G(T(F), T(H))$ *is bijective, where* $G = \mathrm{Gal}(\overline{K}/K)$.

Subsequently, in [**2**], Lubin presented a short, elementary proof of a special case of the above theorem which applies to certain one-parameter formal groups defined over the ring of integers in a finite dimensional extension of the field of p-adic numbers. In this paper, we will show that Lubin's method of proof can be used in a slightly more general situation which will apply directly to one-parameter generic formal groups of height h, $\Gamma_{t_1,\ldots,t_{h-1}}(x,y)$ defined over $\mathbf{Z}_p[[t_1, \ldots, t_{h-1}]][[x,y]]$ where $\mathbf{Z}_p$ is the ring of p-adic integers. (See [**1**] for definitions and notation regarding generic formal groups.) In particular, we will prove

THEOREM 1. *Let A be a complete regular local ring of characteristic* 0 *with residue field k of characteristic $p > 0$. Let $K = \mathrm{Frac}(A)$ be the field of fractions of A and $\overline{K}$ an algebraic closure of K with $G = \mathrm{Gal}(\overline{K}/K)$. Let F be a one- parameter formal group defined over A, of finite height h, that has $f \in \mathrm{End}_A(F)$ such that $f'(0)$ is a parameter of A. If ϕ is a G-endomorphism of the group $\Lambda(F)$ of points of finite order of F then there exist $g \in \mathrm{End}_A(F)$ such that for every $\lambda \in \Lambda(F)$, $g(\lambda) = \phi(\lambda)$.*

Parts of the proof are based on properties of regular local rings (see for example [**3**]). Specifically we will refer to

($*$) If (A, M) is a regular, local ring and $f(x) \in A[x]$ satisfies $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ with $a_i \in M$ and $a_0 \in M \backslash M^2$, then $f(x)$ (which is called an Eisenstein polynomial) is irreducible over the field of fractions of A. Moreover, if

Received by the editors October 12, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 14L05; Secondary 13H05.
Key words and phrases. One parameter formal group, local ring.
This paper appears as part of the author's dissertation written at Brown University.

$f(\alpha) = 0$ then $A[\alpha]$ is regular local ring and if N is the maximal ideal, $\alpha \in N \backslash N^2$, i.e. α is a parameter of $A[\alpha]$.

Continuing with preliminary notions, if we now take A to be complete in the M-adic topology, the Weierstrass preparation theorem applies. More precisely, if $f(x) \in A[[x]]$ with $\text{wideg}(f) < \infty$[1] and $f(0)$ a parameter of A, then $f(x) = P(x)u(x)$ where $P(x)$ is an Eisenstein polynomial in $A[x]$ and $u(x)$ is a unit in $A[[x]]$. Such an $f(x)$ will be called an Eisenstein power series. Clearly $f(x)$ is indecomposable in $A[[x]]$, and in $\overline{K}$ (an algebraic closure of $K = \text{Frac}(A)$), $f(x)$ has $\text{wideg}(f)$ distinct roots which form a complete set of conjugates over K.

Suppose F is a one-parameter formal group defined over the complete, regular, local ring A (with field of fractions K). Let $\Lambda(F) = \bigcup_{m=1}^{\infty}$ (zeros in $\overline{K}$ of $[p^m]_F(x)$), and note that the set $\Lambda(F)$ can be endowed with a group structure with addition defined as follows: if α, $\beta \in \Lambda(F)$, $\alpha +_F \beta = F(\alpha, \beta)$. This substitution makes sense because α and β are nonunits in $A[\alpha, \beta]$ which is finite as an A-module, hence complete. The formal group endomorphism $[p^m]_F$ induces a group endomorphism $[p^m]_F \colon \Lambda(F) \to \Lambda(F)$ defined by $\lambda \to [p^m]_F(\lambda)$. It is clear that $\ker([p^m]_F)$ is equal to the set of zeros of $[p^m]_F(x)$ in $\overline{K}$.

2. Proof of Theorem 1. The notation to be used was introduced in the statement of Theorem 1. The first step in the proof is to find a power series $g \in A[[x]]$ such that for every $\lambda \in \Lambda(F)$, $g(\lambda) = \phi(\lambda)$. The reader is referred to remarks in Lubin [**2**] to see that it is enough to find a power series $g_n \in A[[x]]$ for each n such that for every $\lambda \in \text{Ker}[p^n]_F$, $\phi(\lambda) = g_n(\lambda)$. To that end, let α be a root of the Eisenstein power series $f(x)/x$, $K(\alpha) = L$ and B the ring of integers in L. Recalling $(*)$, it is clear that $A[\alpha]$ is a regular local ring (hence integrally closed) and α is a parameter. Moreover, since $\text{Frac}(A[\alpha]) = K(\alpha) = L$, it may be concluded that $A[\alpha] = B$. We note that $[p^n]_F(x) - \alpha \in B[[x]]$ is an Eisenstein power series and if β is a root of this power series then a complete set of L-conjugates of β is given by $\beta +_F \ker[p^n]_F$.

Now consider the tower of fields $K \subseteq L \subseteq L(\beta) \subseteq \overline{K}$. Let $H = \text{Gal}(\overline{K}/L(\beta))$, and note that for $\sigma \in H$, $\sigma(\phi(\beta)) = \phi(\sigma(\beta)) = \phi(\beta)$. We see that $\phi(\beta)$ is in the fixed field of H, namely $L(\beta)$. $\phi(\beta) \in \Lambda(F)$ by definition and so $\phi(\beta) \in L(\beta) \cap \Lambda(F)$. However, using $(*)$, we see that the ring of integers in $L(\beta)$ is $B[\beta]$. Consequently, $\phi(\beta) \in L(\beta) \cap \Lambda(F) \subseteq B[\beta]$ implies there exists $\gamma(x) \in B[x]$ with $\gamma(\beta) = \phi(\beta)$. Clearly $\gamma(0)$ is a nonunit.

At this point we note that the remarks thus far will allow us to apply Lubin's methods directly to our more general situation. Specifically, define $g_*(x) \in B[\beta][[x]]$ by $g_*(x) = \gamma(\beta +_F x) -_F \phi(\beta)$ and observe that for $\lambda \in \ker[p^n]_F$,

$$g_*(\lambda) = \gamma(\beta +_F \lambda) -_F \phi(\beta) = \phi(\beta +_F \lambda) -_F \phi(\beta) = \phi(\lambda).$$

The second equality follows because $\beta +_F \lambda$ is an L-conjugate of β; thus there exists $\sigma \in \text{Gal}(\overline{K}/L)$ with $\sigma(\beta) = \beta +_F \lambda$. Therefore

$$\phi(\beta +_F \lambda) = \phi(\sigma(\beta)) = \sigma(\phi(\beta)) = \sigma(\gamma(\beta)) = \gamma(\sigma(\beta)) = \gamma(\beta +_F \lambda).$$

By the Weierstrass preparation theorem,

$$[p^n]_F(x) = xP_n(x)u_n(x) \quad \text{where } \deg P_n(x) = p^{nh} - 1.$$

[1] Let $\overline{f}(x)$ be obtained by reducing the coefficients of f modulo M. $\text{Wideg}(f) = n$ if and only if $\bar{f}(x) = \bar{a}_n x^n + \cdots + \bar{a}_0$, $\bar{a}_n \neq 0$.

This induces an isomorphism between the rings $B[\beta][[x]]/([p^n]_F(x))$ and $B[\beta][x]/(xP_n(x))$ and the isomorphism yields $g_n(x) \in B[\beta][x]$ with $g_*(x) \cong g_n(x)$ mod $[p^n]_F(x)$ and $\deg(g_n(x)) < p^{nh}$. If $\sigma \in G$ then for every $\lambda \in \ker[p^n]_F$

$$(g_n(\lambda)) = \sigma(g_*(\lambda)) = \sigma(\phi(\lambda)) = \phi(\sigma(\lambda)) = g_*(\sigma(\lambda)) = g_n(\sigma(\lambda)).$$

However, $\deg(g_n^\sigma(x) - g_n(x)) < p^{nh}$; but for every $\sigma \in G$, $g_n^\sigma(x) - g_n(x)$ has p^{nh} roots and so $g_n^\sigma(x) = g_n(x)$. Thus $g_n(x) \in A[[x]]$ as desired. Letting $g(x) = \lim g_n(x)$ yields $g(x) \in A[[x]]$ and for every $\lambda \in \Lambda(F)$, $g(\lambda) = \phi(\lambda)$.

Note now that the power series $g \circ [p]_F(x) - [p]_F \circ g(x)$ has an infinite zero set (since $\Lambda(F)$ is infinite), whence $g \circ [p]_F = [p]_F \circ g$ which implies $g \in \mathrm{End}_A(F)$. Q.E.D.

COROLLARY 1. *Let $\Gamma_{t_1,\ldots,t_{h-1}}(x,y) \in \mathbf{Z}_p[[t_1,\ldots,t_{h-1}]][[x,y]] = A$ be a generic formal group of height h. Let $\overline{K}$ be an algebraic closure of $\mathrm{Frac}(A) = K$ and ϕ a $\mathrm{Gal}(\overline{K}/K)$ endomorphism of $\Lambda(\Gamma_{t_1,\ldots,t_{h-1}})$. Then there exists $g \in \mathrm{End}_A(\Gamma_{t_1,\ldots,t_{h-1}})$ such that for all $\lambda \in \Lambda(\Gamma_{t_1,\ldots,t_{h-1}})$, $g(\lambda) = \phi(\lambda)$.*

PROOF. A is a complete regular local ring of characteristic 0 with residue field characteristic $p > 0$. The endomorphism $[p]_{\Gamma_{t_1,\ldots,t_{h-1}}}(x) = f(x)$ has the property that $f'(0) = p$, a parameter of A. Q.E.D.

We remark that the claim made in the abstract of this paper is an easy consequence of Corollary 1.

Finally, we observe that as is the case in Lubin [**2**], the proof of Theorem 1 yields the following result which is stronger (when it applies) than the result in [**4**].

COROLLARY 2. *If A and G are as in the statement of the theorem, and if ϕ is a G-endomorphism of $\ker[p^{n+1}]_F$, then the restriction of ϕ to $\ker[p^n]_F$ is analytic, i.e. there exists $f(x) \in A[[x]]$ such that for all $\lambda \in \ker[p^n]_F$, $\phi(\lambda) = f(\lambda)$.*

The author would like to thank Professor Jonathan Lubin for many enlightening discussions on the subject of formal groups and for his helpful suggestions concerning this paper.

BIBLIOGRAPHY

1. J. Lubin and J. Tate, *Formal moduli for one parameter formal Lie groups*, Bull. Soc. Math. France **94** (1966), 49–60.
2. J. Lubin, *Galois endomorphisms of the torsion subgroup of certain formal groups*, Proc. Amer. Math. Soc. **20** (1969), 229–231.
3. M. Nagata, *Local rings*, Interscience, New York, 1962.
4. J. Tate, *p-divisible groups*, Proc. Dreibergen Summer School on Local Fields, 1966, Springer-Verlag, Berlin and New York, 1967.

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