GALOIS ENDOMORPHISMS OF THE TORSION SUBGROUP OF CERTAIN FORMAL GROUPS[1]

JONATHAN LUBIN

1. **The theorem.** The purpose of this paper is to give a short and elementary proof of the following

THEOREM. *Let A be the ring of integers in a field K of finite degree over the field $\mathbf{Q}_p$ of p-adic numbers, $\overline{K}$ an algebraic closure of K, and G the Galois group of $\overline{K}$ over K. Let F be a one-parameter formal group defined over A, of finite height, that has an $f\in\mathrm{End}_A(F)$ such that $f'(0)$ is a prime element of A, and let ϕ be a G-endomorphism of the group $\Lambda(F)$ of points of finite order of F. Then there is a $g\in\mathrm{End}_A(F)$ such that for every $\lambda\in\Lambda(F)$, $\phi(\lambda)=g(\lambda)$.*

(The reader may refer to [1] and [2] for all definitions not given below.)

REMARK. In [3] Tate has given a proof of the most general theorem of this nature, which applies to homomorphisms of formal groups of arbitrary dimension. It needs no such restrictive assumption as above on the existence of a special endomorphism f, which says roughly that F can be defined over an unramified extension of its endomorphism ring. Tate's proof makes use however of some deep results from class field theory and algebraic geometry; this weak version of the theorem is presented here in the hope that the methods, which are quite different from Tate's, may be of some interest in themselves. When they apply, they give more precise information than Tate's; cf. our last corollary.

2. **Preliminaries.** Let A, K, $\overline{K}$, G be as above, let M be the maximal ideal of A, and let $A[[x]]$ be the ring of power series over A in one indeterminate. Then if $f\in A[[x]]$, the *Weierstrass degree* of f, $\mathrm{wideg}(f)$, is defined to be the smallest degree in which a unit appears as a coefficient of f, ∞ if there is no unit coefficient. One sees immediately that if $f, g\in A[[x]]$, then $\mathrm{wideg}(f+g)\geqq\min(\mathrm{wideg}(f),\mathrm{wideg}(g))$, $\mathrm{wideg}(fg)=\mathrm{wideg}(f)+\mathrm{wideg}(g)$, and if $0<\mathrm{wideg}(g)$, then $\mathrm{wideg}(f\circ g)=\mathrm{wideg}(f)\ \mathrm{wideg}(g)$. The Weierstrass Preparation theorem says that if $\mathrm{wideg}(f)<\infty$, then f is the associate in $A[[x]]$ of a polynomial P with $\deg(P)=\mathrm{wideg}(P)=\mathrm{wideg}(f)$. If $f\in A[[x]]$ with $0<\mathrm{wideg}(f)<\infty$ and $f(0)$ is a prime element of A, then f is indecomposable in

Received by the editors September 2, 1967.

[1] This work was supported by NSF Grants GP-5098 and GP-5802.

$A[[x]]$. Such an f may be called an *Eisenstein power series*. One sees that in the maximal ideal $\overline{M}$ of the ring of integers $\overline{A}$ of $\overline{K}$, an Eisenstein power series $f \in A[[x]]$ has exactly wideg(f) roots, which form a complete set of conjugates over K; and if α is such a root then $A[\alpha]$ is the ring of integers in the field $K(\alpha)$, and α is a prime element of $A[\alpha]$.

Given the one-parameter formal group F over A, one may impose a group-structure on the set $\overline{M}$: for $\alpha, \beta \in \overline{M}$, $\alpha +_F \beta = F(\alpha, \beta)$. We call this group $F(\overline{A})$; it is a G-module. (Note that the group law F can be used in the same way for adding two power series in the maximal ideal (M, x) of the local ring $A[[x]]$.) The torsion subgroup $\Lambda(F)$ of $F(\overline{A})$ is just $\bigcup \ker([p^n]_F)$. Suppose now that F is of finite height. By [2, paragraph 1.2], the roots of any nonzero $f \in \mathrm{End}_A(F)$ are all simple; and since wideg$(f) < \infty$, a power series vanishing on $\ker(f)$ is divisible by f.

The ring $A[[x]]$ is complete under the (M, x)-adic topology. If $f, g \in A[[x]]$ and $f(0)=0$, then if $f \in (M, x)^i$ and $g \in (M, x)^j$ with $j \geqq 1$, we have $f \circ g \in (M, x)^{i+j-1}$. In particular if f is any nonunit in $\mathrm{End}_A(F)$, then $f \in (M, x)^2$; consequently the nth iterate of f, $f^{(n)}$, is in $(M, x)^n$. Because of this if f is a nonunit endomorphism of F, and $\{g_n\}$ is a sequence of elements of $A[[x]]$ such that for all positive n and r, g_n and g_{n+r} agree on the zero-set of $f^{(n)}$ in $\overline{M}$, then $\{g_n\}$ is an (M, x)-adic Cauchy sequence in $A[[x]]$ and so converges to a power series $g \in A[[x]]$ such that for all $n \geqq 1$, g and g_n agree on the zero-set of f in $\overline{M}$.

3. **Proof of the theorem.** We use the same notation as in the statement of the theorem, §1. First we find a power series $g \in A[[x]]$ such that for every $\lambda \in \Lambda(F)$, $\phi(\lambda) = g(\lambda)$. Because of the remarks in §2, it is enough to find for each n a power series $g_n \in A[[x]]$ such that g_n agrees with ϕ on $\ker([p^n]_F)$. Let α be a root in $\overline{M}$ of the Eisenstein power series $f(x)/x \in A[[x]]$. Let $K(\alpha) = L$ and let B be the ring of integers in L. Then $B = A[\alpha]$ and α is a prime element of B, and $[p^n]_F(x) - \alpha$ is an Eisenstein power series in $B[[x]]$. If β is a root of $[p^n]_F - \alpha$ in $\overline{M}$, then the set of all L-conjugates of β is just $\beta +_F \ker([p^n]_F)$. Now $\phi(\beta) \in L(\beta) \cap \overline{M} \subset B[\beta]$, so that there is a polynomial $\gamma \in B[x]$ such that $\chi(\beta) = \phi(\beta)$ and whose constant coefficient is a nonunit; thus we may define a power series $g_*(x) \in B[\beta][[x]]$ by $g_*(x) \gamma(\beta +_F x) -_F \phi(\beta)$. Then for any $\lambda \in \ker[p^n]_F$,

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

since $\beta +_F \lambda$ is L-conjugate to β. Now, by the Weierstrass preparation theorem, $g_* \equiv g_n \bmod([p^n]_F)$, where g_n is a polynomial with coefficients in $B[\beta]$ and of degree less than $\text{wideg}([p^n]_F) = p^{nh}$, where h is the height of F. Since for every one of the p^{nh} elements λ of $\ker([p^n]_F)$ and for every $\sigma \in G$ we have $\sigma(g_n(\lambda)) = g_n(\sigma(\lambda))$, it must follow that $g_n \in K[x]$, so that $g_n \in A[[x]]$, as desired.

Thus there is a $g \in A[[x]]$ such that for every $\lambda \in \Lambda(F)$, $g(\lambda) = \phi(\lambda)$. Then the power series $g \circ [p]_F - [p]_F \circ g \in A[[x]]$ has an infinite zero-set (since $\Lambda(F)$ is infinite) and must necessarily be zero, so $g \in \text{End}_A(F)$ by [**1**, Lemma 4.2.1], q.e.d.

The above proof also yields the following fact, stronger, in the cases when it applies, than the results of [**3**]:

COROLLARY. *If A and F are as in the statement of the above 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 is an $f(x) \in A[[x]]$ such that for all* $\lambda \in \ker([p^n]_F)$, $\phi(\lambda) = f(\lambda)$.

REFERENCES

1. Jonathan Lubin, *One-parameter formal Lie groups over p-adic integer rings*, Ann. of Math. **80** (1964), 464–484.

2. ———, *Finite subgroups and isogenies of one-parameter formal Lie groups*, Ann. of Math. **85.** (1967), 296–302.

3. John Tate, *p-divisible groups*, Proc. Dreibergen Summer School on Local Fields, 1966, Springer, Berlin, 1967.

BOWDOIN COLLEGE, INSTITUTE FOR ADVANCED STUDY AND
BROWN UNIVERSITY