A CLASSIFICATION OF ALMOST FULL FORMAL GROUPS

WILLIAM C. WATERHOUSE

1. **Introduction.** Let A be a complete discrete valuation ring in characteristic zero with algebraically closed residue field of characteristic p. Let F be a one-parameter formal group law defined over A. Then there is an injection c of $\mathrm{End}_A F$ onto a subring of A. If height $(F)=h<\infty$, $c(\mathrm{End}_A F)$ is a free $\boldsymbol{Z}_p$-module of rank $\leqq h$. We call F *almost full over* A if $c(\mathrm{End}_A F)$ has rank h; in this case all the endomorphisms of F are defined over A, and we write simply End F. F is *full over* A if it is almost full over A and in addition $c(\mathrm{End}\ F)$ is integrally closed in its fraction field Σ_F.

The main theorem of the paper by Lubin [2] which contains the above results is a uniqueness theorem: If F and G are both full over A and $c(\mathrm{End}\ F)=c(\mathrm{End}\ G)$ (equivalently, $\Sigma_F=\Sigma_G$), then F and G are isomorphic over A. I will show that this result is a particular case of a classification theorem for formal groups almost full over A.

2. **Statement of the theorem.** The basic idea is to use the theory of the Tate module $T(F)$, as developed in [3]. (The reader should note that the theorems there remain true under our hypotheses.) $T(F)$ is a free $\boldsymbol{Z}_p$-module of rank h, and is a module over $R=c(\mathrm{End}\ F)$. $V(F)=T(F)\otimes\boldsymbol{Q}_p$ is therefore a vector space over Σ_F, and must be of dimension one if F is almost full. In this case, $T(F)$ is isomorphic as an R-module to a lattice in Σ_F. Furthermore, by [3, 3.1] R is the order of this lattice, i.e., $R=\{x\in\Sigma_F: xT(F)\subseteq T(F)\}$.

THEOREM. *Two groups F and G almost full over A with $c(\mathrm{End}\ F)=c(\mathrm{End}\ G)=R$ are isomorphic if and only if $T(F)$ and $T(G)$ are isomorphic as R-modules. Furthermore, the isomorphism classes of R-modules occurring are precisely those of the lattices in Σ_F with order R.*

In particular, the number of nonisomorphic such formal groups is finite and equals the class number of R, i.e., the number of isomorphism classes of such lattices.

3. **Proof.** All formal groups from now on will be almost full over A.

PROPOSITION 3.1 (LUBIN). *F and G are isogenous if and only if $\Sigma_F=\Sigma_G$.*

PROOF. The necessity of the condition is [3, 3.0]. Conversely, if $\Sigma_F=\Sigma_G$, F and G are both isogenous to full groups with the same Σ

Received by the editors November 19, 1967.

by [**3**, 3.2], and these in turn are isomorphic by the uniqueness theorem.

LEMMA 3.2. *There is an H with $c(\text{End } H)=R$ such that $T(H)$ is free of rank one as an R-module.*

PROOF. We view $T(F)$ as a lattice in $V(F)$. Let k be the fraction field of A, K its algebraic closure. The Galois group $\mathcal{G}=\text{Gal }(K/k)$ acts on $T(F)$ and commutes with the action of A-endomorphisms, so it acts Σ_F-linearly on $V(F)$. Since $V(F)$ is one-dimensional over Σ_F, the action is given by a homomorphism $\rho\colon \mathcal{G}\to\Sigma_F^*$. As $T(F)$ is stable under $\mathcal{G}$, and R is the order of $T(F)$, we have $\rho(\mathcal{G})\subseteq R$. Hence for any $b\in T(F)$, Rb is a lattice stable under $\mathcal{G}$. Therefore it defines an H isogenous to F over A, with $T(H)$ isomorphic to Rb as an R-module [**3**, 2.3] and $c(\text{End } H)$ equal to the order of $T(H)$, i.e., R.

Now let L be any sublattice of $T(H)$ with order R. As before, $\rho(\mathcal{G})\subseteq R$, so L is stable under $\mathcal{G}$; hence L defines a formal group G isogenous to H over A and having $T(G)\simeq L$. Conversely, if G is any formal group with $c(\text{End } G)=R$, then as we saw G is isogenous to H and hence [**3**, 2.2] occurs as the group associated to some such lattice L. Now since $T(H)$ is free of rank one over R, the lattices in it with order R correspond precisely to the ideals I of R with order R. We now must prove that such ideals are isomorphic if and only if the corresponding groups are; this will complete the proof of the theorem, since any lattice in Σ_H is isomorphic (under multiplication by an integer) to one lying in R.

Suppose first that I and J are isomorphic R-modules. As the isomorphism extends to a Σ_H vector space automorphism of Σ_H, it is given by a scalar multiplication, so $I=\lambda J$. If $\lambda\in R$, let $f\colon G\to H$ be the isogeny with $f(T(G))=J\,T(H)$. Then $[\lambda]_H\circ f\colon G\to H$ is an isogeny with $[\lambda]_H\circ f(T(G))=[\lambda]_H(J\,T(H))=\lambda J\,T(H)=I\,T(H)$, and so G serves also as the formal group corresponding to I. If $\lambda\notin R$, choose an integer n with $n\lambda\in R$; then the group for I is isomorphic to that for $nI=(n\lambda)J$, which is in turn isomorphic to that for J.

Conversely, suppose the groups for I and J are isomorphic. Then we have a G and two isogenies f, $g\colon G\to H$ with $f(T(G))=I\,T(H)$, $g(T(G))=J\,T(H)$. Replacing I by an integer multiple of itself if necessary, we may assume $I\subseteq J$. Then by [**3**, 2.2] there is an isogeny $h\colon G\to G$ such that $f=g\circ h$. If $h=[x]_G$ for $x\in R$, then $g\circ h=[x]_H\circ g$, since c of these two maps is the same (see [**2**, 2.1.1]). Hence $I\,T(H)$ $=f(T(G))=x\,g(T(G))=xJ\,T(H)$. As $T(H)$ is free, $I=xJ$ and the modules are isomorphic.

4. **Remarks.** 1. The uniqueness theorem of Lubin is of course a

particular case of our theorem, since the unique integrally closed order in a local field Σ is a discrete valuation ring and hence has just one ideal class. We have not, however, given an independent proof of that theorem; it was used in the proof of Proposition 3.1.

2. Our theorem assumes that R occurs as $c(\text{End } F)$ for some F defined over A. Lubin has shown in [3, 3.2] that for any R there is some A over which R occurs, but for a fixed A not all R are possible. To be more specific, let us fix Σ and take the unique group F with $c(\text{End } F)$ maximal in Σ; this group is full over $c(\text{End } F)$ [4, Theorem 1], and so is available whenever k contains Σ. The argument of Lemma 3.2 applied to F shows then that those R which occur are precisely those which contain the group $\rho(\mathcal{G})$.

3. If we take the integral closure of A in a finite extension of k, we get another ring satisfying our hypotheses. This extension reduces $\rho(\mathcal{G})$ and thus makes more orders possible, but the theorem implies that it can have no other effect. Once a single group F with $c(\text{End } F) = R$ is defined over A, so are all the others; expanding k cannot introduce any new isomorphism types, nor can any nonisomorphic groups become isomorphic over the larger ring.

4. The technique used here resembles that of a standard theorem on the isomorphism types of elliptic curves with complex multiplication. Serre [5] has drawn attention to the fact that that result can be interpreted as saying that the isomorphism classes of curves with endomorphism ring R are a principal homogeneous space over the group of rank one projective R-modules. Similar results have been proved for certain abelian varieties when the endomorphism ring is a maximal order. It may therefore be useful to point out that no such formulation is possible here: the modules occurring in the theorem need not be projective, nor need they form a group. (An example is easily constructed following Exercise 18 [1, p. 94].) A similar example shows that the use of Lemma 3.2 cannot be avoided; there is an almost full group G and ideals $I \neq J$ of $c(\text{End } G)$ with $I\,T(G) = J\,T(G)$.

References

1. Z. Borevich and I. Shafarevich, *Number theory*, Academic Press, New York, 1966.

2. J. Lubin, *One-parameter formal Lie groups over p-adic integer rings*, Ann. of Math. (2) **80** (1964), 464–484.

3. ———, *Finite subgroups and isogenies of one-parameter formal Lie groups*, Ann. of Math. (2) **85** (1967), 293–302.

4. J. Lubin and J. Tate, *Formal complex multiplication in local fields*, Ann. of Math. (2) **81** (1965), 380–387.

5. J.-P. Serre, *Algèbre et géométrie*, Ann. Coll. France, Paris, 1964–1965.

Harvard University