LIFTING AN ENDOMORPHISM OF AN ELLIPTIC CURVE TO CHARACTERISTIC ZERO

BY

FRANS OORT *)

(Communicated by Prof. J. P. Murre at the meeting of June 30, 1973)

Theorem 1. Let k be a field of characteristic $p \neq 0$, C_0 an elliptic curve over k, and $\alpha_0 \in \operatorname{End}_k(C_0)$; the pair (C_0, α_0) can be lifted to characteristic zero in the following sense: there exists an integral characteristic zero domain R, a ring homomorphism $R \to k$, an abelian scheme $\mathscr{C}$ over Spec (R), and $\alpha \in \operatorname{End}_R(\mathscr{C})$ such that

$$(\mathscr{C}, \alpha) \otimes_R k \simeq (C_0, \alpha_0).$$

Remark 2. In case k is algebraically closed the result is due to Deuring (cf. [1], pp. 259–263).

Fact 3. Let K be a field, C an elliptic curve over K such that $\mathbb{Z} \subsetneqq \operatorname{End}_K(C)$ (and we then say C has complex multiplications over K); then C can be defined over a finite extension of the prime field of K (cf. [8], p. 108 for the case char $(K)=0$; cf. [1], p. 220; cf. [5], theorem on p. 217; cf. [7], 3.2).

Local moduli (4). Let k be a field, W a complete local noetherian ring with residue class field k; denote by $\mathbf{C}$ (or by $\mathbf{C}_W$) the category of local artinian W-algebras R, with residue class field k as a W-algebra (e.g. cf. [6], Section 2). We fix C_0, an elliptic curve over k, and $\alpha_0 \in \operatorname{End}_k(C_0)$, and define: M is the local moduli functor given by C_0, and $I, E\colon \mathbf{C} \to \mathrm{Ens}$ are given by:

$I(R) = \{\simeq$ classes of $(C, D, \alpha, \varphi_0) \mid C$ and D are abelian schemes over Spec (R), $\alpha\colon A \to B$ is an isogeny such that

$\varphi_0\colon ((A \xrightarrow{\alpha} B) \otimes k) \xrightarrow{\sim} (\alpha_0\colon C_0 \to C_0)\}$;

$E(R) = \{\simeq$ classes of $(C, \alpha, \varphi_0) \mid C$ is an abelian scheme over Spec (R), $\alpha \in \operatorname{End}_R(C)$ and $\varphi_0\colon ((C, \alpha) \otimes k) \xrightarrow{\sim} (C_0, \alpha_0)\}$.

We know that M is pro-representable by $W[[T]]$ (cf. [6], Theorem (2.2.1)), and it is easily seen that E and I are pro-representable and $E \subset I \subset M \times M$,

---

*) The Tata Institute of Fundamental Research, Bombay, and the University of Aarhus are gratefully thanked for hospitality and excellent working conditions.

thus (cf. [6], exercise on page 285):

$$\begin{array}{ccc} I & \hookrightarrow & M \times M \\ \uparrow\cup & & \uparrow \text{diag} \\ E & \hookrightarrow & M \end{array} \qquad \begin{array}{ccc} W[[T,S]]/\mathfrak{a} & \twoheadleftarrow & W[[T,S]] \\ \downarrow & & \downarrow \\ W[[U]]/\mathfrak{b} & \twoheadleftarrow & W[[U]]. \end{array}$$

Note that

$$W[[U]]/\mathfrak{b} \simeq W[[T,S]]/((T-S)+\mathfrak{a}).$$

Now suppose moreover W is an integral characteristic zero domain.

LEMMA 5. The conclusion of the theorem holds if and only if

$$p \notin \sqrt{\mathfrak{b}}.$$

PROOF. In case $\alpha_0 \in \mathbb{Z} = \mathbf{Q} \cap \mathrm{End}_k(C_0)$ the conclusion of the theorem is true (because C_0 can be lifted to characteristic zero), and $\mathfrak{b} = 0$. Thus suppose $\alpha_0 \notin \mathbb{Z}$. Consider the prime decomposition of the radical of $\mathfrak{b}$:

$$\mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_? = \sqrt{\mathfrak{b}}$$

(note that W, and hence $W[[U]]$ is noetherian); because $p \notin \sqrt{\mathfrak{b}}$ at least one of these prime ideals (call it $\mathfrak{p}$) does not contain p; then $R := [[U]]/\mathfrak{p}$ is a characteristic zero local integral domain; its residue class field is k because: $\mathfrak{p}$ is contained in the maximal ideal of $W[[U]]$, thus $\mathfrak{p} \otimes k$ is contained in the maximal ideal of $k[[U]]$; because $\alpha_0 \notin \mathbb{Z}$ we know by fact (3) that $\mathfrak{b} \neq 0$; thus $\mathfrak{p} \otimes k = U \cdot k[[U]]$. By the definition of E and its pro-representing object $W[[U]]/\mathfrak{b}$ the conclusion of the theorem follows.

Note that it suffices to prove the theorem for *separable* isogenies (in case α_0 is not separable, $\beta_0 = 1 + \alpha_0$ is separable, lift β_0 to β, and define $\alpha = \beta - 1$). For W we choose $W = W_\infty(k)$, the ring of Witt vectors of infinite length over k. Suppose there exists an integer $n \geqslant 2$ such that $p^{n-1} \in \mathfrak{b}$; then

$$p^{n-1} \in \mathfrak{a} + (T-S),$$

and we are going to derive a contradiction; from now on we suppose $\alpha_0 \notin \mathbb{Z}$.

Take $\mathscr{C}$, the universal deformation in characteristic p of C_0, thus $\mathscr{C}$ is a formal abelian scheme of relative dimension one over $k[[U]] = k[[T]]$; by EGA.IV^4.18.1.2 there exists an étale finite group scheme $\mathscr{N} \to \mathscr{C}$ over $k[[T]]$ such that

$$(\mathscr{N} \subsetneq \mathscr{C}) \otimes k = \mathrm{Ker}\,(\alpha_0);$$

we define $\mathscr{D} = \mathscr{C}/\mathscr{N}$, and the quotient morphism $\mathscr{C} \to \mathscr{D}$ is an isogeny α lifting α_0, thus α defines an element of the functor I; because $k[[T,S]]$

pro-represents I, we thus obtain a homomorphism of complete local rings

$$d\colon k[[T, S]] \to k[[T]],$$

$dT = T$, so that $(\mathscr{C}, \mathscr{D}, \alpha)$ comes from the universal object over $k[[T, S]]$ via d; note that $(dS)(0) = 0$. Moreover note that $d(S) \neq T$ (use $\alpha_0 \notin \mathbb{Z}$ and the fact 3). Fix an integer m so that

$$T \not\equiv dS \pmod{T^m},$$

define

$$M := 1 + m(1 + p + \dots + p^{n-2}),$$

and write

$$R_1 := k[T]/(T^M), \ R_i := W_i(R_1)$$

(Witt vectors of length $i \geqslant 1$ over R_1); R_1 is a local artin ring with residue class field k, and the same holds for the rings R_i (e.g. use [3], page 132, Theorem 12). Let $C_1 = \mathscr{C} \otimes R_1$, lift C_1 in some way to C_n over R_n; let $N_1 = N \otimes R_1$, lift this to $N_n \subsetneq C_n$ over R_n (cf. EGA.IV^4.18.1.2), and define $D_n := C_n$; the isogeny $C_n \to D_n$ is a lift of α_0 to R_n, thus we obtain

$$\begin{array}{ccc} W[[T, S]] & \xrightarrow{\ d_n\ } & R_n \\ \downarrow & & \downarrow \\ k[[T, S]] & \xrightarrow{\ d_1\ } & R_1 \end{array}$$

with $d_n(\mathfrak{a}) = 0$. Because we assumed $p^{n-1} \in \mathfrak{a} + (T - S)$, there should exist $H \in W[[T, S]]$ with $(p^{n-1} - H(T - S)) \in \mathfrak{a}$, which however is a contradiction because of:

LEMMA 5. Notations as before, i.e. k is a field, char $(k) = p$, $n \geqslant 2$, $m > 0$, $M = 1 + m(1 + p + \dots + p^{n-2})$, $T - dS =: u_1 \not\equiv 0 \bmod T^m$; then there does not exist $h \in R_n = W_n(R_1)$ such that $hu_n = p^{n-1}$, $u_n \in R_n$.

PROOF. Assume $hu_n = p^{n-1}$; let $u_1 \equiv \lambda_1 T^m (\bmod T^{m+1})$, $\lambda_1 \in k^* \subset R_1{}^*$; lift this to $\lambda \in R_n{}^*$, and write $a = \lambda h$, $b = \lambda^{-1} u_n$,

$$\begin{aligned} a &= (a_0, a_1, \dots, a_{n-1}), \\ b &= (b_0, b_1, \dots, b_{n-1}),\ b_0 = T^m + T^{m+1}(\dots), \\ ab &= p^{n-1} = (0, 0, \dots, 0, 1). \end{aligned}$$

Note that $(ab)_0 = a_0 b_0 = 0 \in R_1$, and because $b_0 = T^m + T^{m+1}(\dots)$, and $R_1 = k[T]/T^M$, we obtain

$$a_0 \equiv 0 \bmod T^{M-m}.$$

Thus the following induction hypothesis is satisfied for $j=0$: assume $0<j<n-2$

$$\left.\begin{array}{l} a_0 \equiv 0 \\ \vdots \\ a_j \equiv 0 \end{array}\right\} \bmod T^{1+m(p^{j+1}+\ldots+p^{n-2})}.$$

Because of the Witt multiplication

$$(a\cdot b)_{j+1} \equiv a_{j+1} b_0^{p^{j+1}} \pmod{a_0 R_1+\ldots+a_j R_1},$$

thus the induction hypothesis implies

$$a_{j+1} \equiv 0 \bmod T^{1+m(p^{j+1}+\ldots+p^{n-2})-mp^{j+1}}.$$

Thus by induction on j we have proved:

$$\left.\begin{array}{l} a_0 \equiv 0 \\ \vdots \\ a_{n-2} \equiv 0 \end{array}\right\} \bmod T.$$

Thus

$$((a_0, \ldots, a_{n-2}, a_{n-1})\cdot(b_0, \ldots))_n \equiv 0 \bmod T,$$

which contradicts $ab=p^{n-1}=(0, \ldots, 0, 1)$, and the lemma is proved.

The assumption $p^{n-1} \in \mathfrak{a}+(T-S)$ leads to a contradiction, hence $p \notin \sqrt{\mathfrak{b}}$, and Lemma 5 proves the theorem.

REMARK 6. In case C_0 has points of order p (i.e. the general case, and if C_0 has complex multiplications, the case of the singular j-invariant), the Serre-Tate theory of canonical lifts proves the theorem (e.g. cf. [4], page 178, Corollary 1.3). In case C_0 has no points of order p (the supersingular case), it might be that the theory of crystals (as in [4], page 151, Theorem 1.6) can be used to prove the theorem.

REMARK 7. The conclusion of the theorem does not hold for abelian varieties of higher dimension, as can be seen as follows. Choose a field k of characteristic $p\neq 0$, and an abelian variety B_0 over k such that B_0 is absolutely simple and of CM-type over k, and such that B_0 cannot be defined over a finite field (cf. [7], 3.3); let α_0 be an element which generates over $\mathbf{Q}$ a field of complex multiplications of B_0. If (B_0, α_0) would be liftable to characteristic zero, the lifted abelian variety B would be of CM-type in characteristic zero, hence defined over a finite extension of $\mathbf{Q}$, and one easily arrives at a contradiction.

REMARK 8. Two abelian varieties over a finite field k are k-isogenous if and only if their Frobenius endomorphisms relative to k have the same characteristic polynomial f (cf. [10], Theorem 1.C). For elliptic curves this can be proved using the theorem above (cf. [9], page 294), but as this proof is not available in the litterature we sketch it here. Let C_0 and D_0 be elliptic curves over a finite field k, such that $f_{C_0}=f=f_{D_0}$. Suppose first f is irreducible, let π_0, respectively φ_0, be the Frobenius of C_0, respectively of D_0, relative to k. Lift (C_0, π_0) and (D_0, φ_0) to a complete local characteristic zero integral domain R, with field of fractions L, a finite extension of $\mathbf{Q}_p$. Because f mod p factors, we can take a totally ramified extension L' of L in which f factors. The two lifted curves have $\mathbf{Q}[T]/(f)$ as field of complex multiplications, hence they are isogenous, and by [8], page 117, Theorem (5.4) one concludes this isogeny to be defined over L'. Thus we conclude C_0 and D_0 to be k-isogenous. In case f is reducible, then $f=(T \pm p^a)^2$, with $|k|=p^{2a}$, and both curves are supersingular. Choose a finite extension l of k such that $[E_{\mathbf{Q}}:\mathbf{Q}]=4$, where $E=\mathrm{End}_l(C_0)=\mathrm{End}_l(D_0)$, and $E_{\mathbf{Q}}=E\otimes\mathbf{Q}$ (we know we can choose $l=k$, but we do not use that). Suppose there exists an l-isogeny β between C_0 and D_0; this isogeny commutes with $\mp p^a$, which is the Frobenius of both C_0 and D_0 over k, thus we see β is a k-isogeny; in order to prove C_0 and D_0 are l-isogenous, choose $\alpha_0 \in E$ whose minimal polynomial is reducible mod p, and argue as before.

Mathematisch Instituut
Roeterssträat 15
Amsterdam

REFERENCES

1. DEURING, M., Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Hamburg **14**, 197–272 (1941).
2. GROTHENDIECK, A. and J. DIEUDONNÉ, Éléments de géométrie algébrique, IV4 (Étude locale des schémas et des morphismes de schémas). Publ. Math. No. 32, IHES, 1967. Cited as EGA.
3. JACOBSON, N., Lectures in abstract algebra III. van Nostrand, 1964.
4. MESSING, W., The crystals associated to Barsotti-Tate groups: with applications to abelian schemes. Lect. N. Math. 264, Springer Verlag, 1972.
5. MUMFORD, D., Abelian varieties. Tata Inst. F. R. Stud. in Math. No. 5, Oxford Univ. Press, 1970.
6. OORT, F., Finite group schemes, local moduli for abelian varieties, and lifting problems. Comp. Math. 23, 265–296 (1961) (also: Algebraic geometry, Oslo 1970, Wolters-Noordhoff, 1972).
7. ———, The isogeny class of a *CM*-type abelian variety is defined over a finite extension of the prime field. To appear (Aarhus Preprint Series 1972/73, No. 32).
8. SHIMURA, G., Introduction to the arithmetic theory of automorphic functions. Publ. Math. Soc. Japan No. 11, Iwanami Shoten and Princeton Univ. Press, 1971.
9. TATE, J., Duality theorems in Galois cohomology over number fields. Proc. ICM, Stockholm 1962, pp. 288–295, Almqvist & Wiksells, 1963.
10. ———, Endomorphisms of abelian varieties over finite fields. Invent. Math. 2, 134–144 (1966).