Reprinted from JOURNAL OF NUMBER THEORY
All Rights Reserved by Academic Press New York and London

Vol 56 No 2, February 1996
Printed in Belgium

Complex Multiplication Structure of Elliptic Curves

H W LENSTRA, JR

Department of Mathematics, 3840, University of California, Berkeley, California 94720-3840

Communicated by K Ribet

Received October 23, 1990, revised February 18, 1994

Let k be a finite field and let E be an elliptic curve over k In this paper we describe, for each finite extension l of k, the structure of the group $E(l)$ of points of E over l as a module over the ring R of endomorphisms of E that are defined over k If the Frobenius endomorphism π of E over k does not belong to the subring $\mathbf{Z}$ of R, then we find that $E(l) \cong R/R(\pi^t - 1)$ where n is the degree of l over k, and if π does belong to $\mathbf{Z}$ then $E(l)$ is, as an R-module, characterized by $E(l) \oplus E(l) \cong R/R(\pi^n - 1)$ The arguments used in the proof of these statements generalize to yield a description of the group of points of an elliptic curve over an algebraically closed field as a module over suitable subrings of the endomorphism ring of the curve It is shown that straightforward generalizations of the results of this paper to abelian varieties of dimension greater than 1 cannot be expected to exist © 1996 Academic Press Inc

1 INTRODUCTION

Let k be a field and let E be an elliptic curve over k In this paper we describe the structure of several groups of points of E as modules over suitable subrings of the ring $\mathrm{End}_k E$ of endomorphisms of E over k We shall view the ring $\mathbf{Z}$ of integers as a subring of $\mathrm{End}_k E$

Our first result is concerned with the case of finite fields

THEOREM 1 *Let k be a finite field, let E be an elliptic curve over k, and put $R = \mathrm{End}_k E$ Let $\pi \in R$ be the Frobenius endomorphism of E Further, let l be a finite field extension of k, and denote by $n = [l\ k]$ its degree*

(a) *Suppose that $\pi \notin \mathbf{Z}$ Then R has rank 2 over $\mathbf{Z}$, and there is an isomorphism $E(l) \cong R/R(\pi^n - 1)$ of R-modules*

(b) *Suppose that $\pi \in \mathbf{Z}$ Then R has rank 4 over $\mathbf{Z}$, we have $E(l) \cong \mathbf{Z}/\mathbf{Z}(\pi^n - 1) \oplus \mathbf{Z}/\mathbf{Z}(\pi^n - 1)$ as abelian groups, and this group has, up to isomorphism, exactly one left R-module structure Furthermore, one has $E(l) \oplus E(l) \cong R/R(\pi^n - 1)$ as R-modules*

This theorem is proved in Section 4, as a consequence of results obtained in Sections 2 and 3 We note that E is supersingular if we are in case (b), but not conversely

0022-314X/96 $12 00

In our other results we take k to be algebraically closed, and we let R be a subring of $\mathrm{End}_k E$ with the property that the abelian group $(\mathrm{End}_k E)/R$ is torsion-free, for example we can take $R = \mathrm{End}_k E$ if E is actually defined over some subfield k' of k (see 4.1). We shall give a complete description of $E(k)$ as a module over R. The following result expresses that the torsion subgroup of $E(k)$ is the only piece of interest. By $\mathbf{Q}$ we denote the field of rational numbers.

THEOREM 2. *Let k be an algebraically closed field and let E be an elliptic curve over k. Let R be a subring of $\mathrm{End}_k E$ for which the abelian group $(\mathrm{End}_k E)/R$ is torsion-free. Denote by $E(k)_{\mathrm{tor}}$ the torsion subgroup of $E(k)$. Then we have*

(a) *the exact sequence $0 \to E(k)_{\mathrm{tor}} \to E(k) \to E(k)/E(k)_{\mathrm{tor}} \to 0$ of R-modules splits,*

(b) *if k is algebraic over a finite field, then $E(k)/E(k)_{\mathrm{tor}} = 0$,*

(c) *if k is not algebraic over a finite field, then $E(k)/E(k)_{\mathrm{tor}}$ is, as a left R-module, isomorphic to the direct sum of $\#k$ copies of $R \otimes_{\mathbf{Z}} \mathbf{Q}$.*

The proof is given in Section 5. It depends on the injectivity of $E(k)_{\mathrm{tor}}$ as a left R-module (Proposition 5.1).

The structure of $E(k)_{\mathrm{tor}}$ as an abelian group is well-known (see [13]). If the characteristic char k of k equals 0 then we have $E(k)_{\mathrm{tor}} \cong (\mathbf{Q}/\mathbf{Z}) \oplus (\mathbf{Q}/\mathbf{Z})$, if char $k = p > 0$ and E is not supersingular, then we have $E(k)_{\mathrm{tor}} \cong (\mathbf{Q}/\mathbf{Z}) \oplus (\mathbf{Z}_{(p)}/\mathbf{Z})$, where $\mathbf{Z}_{(p)}$ denotes the localization of $\mathbf{Z}$ at p, and finally, if char $k = p > 0$ and E is supersingular, then $E(k)_{\mathrm{tor}} \cong (\mathbf{Z}_{(p)}/\mathbf{Z}) \oplus (\mathbf{Z}_{(p)}/\mathbf{Z})$.

The description of $E(k)_{\mathrm{tor}}$ as an R-module requires some notation. There is a ring homomorphism $R \to k$ that describes the action of the endomorphisms in R on the tangent space of E at the zero point O of $E(k)$ (see [13, Chapter III, Theorem 5.2]). Let $\mathfrak{p}$ denote the kernel of this map, it consists of the zero map together with all inseparable isogenies $E \to E$ that belong to R (see [13, Chapter II, Proposition 4.2(c)]). Clearly, char k belongs to $\mathfrak{p}$, and if char $k = 0$ then $\mathfrak{p} = 0$. We view R as a subring of the division ring $R_{\mathbf{Q}} = R \otimes_{\mathbf{Z}} \mathbf{Q}$, and we let $R_{\mathfrak{p}}$ denote the sub-left-R-module of $R_{\mathbf{Q}}$ generated by $\{s^{-1} : s \in R, s \notin \mathfrak{p}\}$. If R is commutative then $R_{\mathfrak{p}}$ is just the localization of R at $\mathfrak{p}$, and if char $k = 0$ then $R_{\mathfrak{p}} = R_{\mathbf{Q}}$.

We now distinguish cases as to the value of $[R\ \mathbf{Z}]$, the rank of the additive group of R as a $\mathbf{Z}$-module. By [13, Chapter III, Section 9], it equals 1, 2, or 4. If $[R\ \mathbf{Z}] = 1$ then we have $R = \mathbf{Z}$, and the $\mathbf{Z}$-module structure was discussed above. The following result deals with the case that $[R\ \mathbf{Z}] = 2$.

THEOREM 3 *Let k, E, R, and $E(k)_{\mathrm{tor}}$ be as in Theorem 2, and suppose that $[R\ \mathbf{Z}]=2$ Then there is an isomorphism $E(k)_{\mathrm{tor}}\cong R_{\mathrm{p}}/R$ of R-modules*

The proof of this theorem is given in Section 2 It uses—only implicitly, in the presentation below—that the ring R is a *Gorenstein ring* if $[R\ \mathbf{Z}]=2$ (see [2, Proposition (6 4)]) Rings of higher ranks need not be Gorenstein, and this indicates that no straightforward generalization of Theorem 3 to higher dimensional abelian varieties can be expected to exist Section 6 is devoted to the construction of counterexamples, in any characteristic and in any dimension exceeding 1

In the case that $[R\ \mathbf{Z}]=4$ we have the following result

THEOREM 4 *Let k, E, R, and $E(k)_{\mathrm{tor}}$ be as in Theorem 2, and suppose that $[R\ \mathbf{Z}]=4$ Then the number $p=\mathrm{char}\,k$ is non-zero, the group $E(k)_{\mathrm{tor}}$ has, up to isomorphism, exactly one left R-module structure, and we have $E(k)_{\mathrm{tor}}\oplus E(k)_{\mathrm{tor}}\cong R_{\mathrm{p}}/R$ as left R-modules*

This theorem is proved in Section 3 It follows in a straightforward way from the observation that for any integer n that is not divisible by p the ring R/Rn is isomorphic to the ring of 2×2 matrices over $\mathbf{Z}/\mathbf{Z}n$

The results above can be reformulated in terms of the Tate module TE Let the assumptions be as in Theorem 2 For a positive integer n let $E[n]=\{P\in E(k)\ nP=O\}$ For each multiple mn of n there is a map $E[mn]\to E[n]$ sending P to mP With these maps, the collection of groups $E[n]$ forms a projective system, and TE is defined to be their projective limit As a profinite abelian group, the structure of TE is as follows If $\mathrm{char}\,k=0$ then $TE\cong\hat{\mathbf{Z}}\oplus\hat{\mathbf{Z}}$, where $\hat{\mathbf{Z}}$ is the projective limit of the groups $\mathbf{Z}/\mathbf{Z}n$, $n\geqslant 1$, if $\mathrm{char}\,k=p>0$ and E is not supersingular, then $TE\cong\hat{\mathbf{Z}}\oplus\hat{\mathbf{Z}}'$, where $\hat{\mathbf{Z}}'$ denotes the projective limit of the groups $\mathbf{Z}/\mathbf{Z}n$, with n now ranging over the positive integers that are not divisible by p, and if $\mathrm{char}\,k=p>0$ and E is supersingular, then $TE\cong\hat{\mathbf{Z}}'\oplus\hat{\mathbf{Z}}'$ To describe TE as a profinite R-module in the case $[R\ \mathbf{Z}]>1$, we define $\hat{R}'$ to be the projective limit of the R-modules $R/\mathfrak{a}$, where $\mathfrak{a}$ ranges over the left ideals of R that are not contained in $\mathfrak{p}$, for $\mathfrak{a}\subset\mathfrak{b}$, the map $R/\mathfrak{a}\to R/\mathfrak{b}$ is the natural one Now if $[R\ \mathbf{Z}]=2$, then we have $TE\cong\hat{R}$ as a profinite R-module, and if $[R\ \mathbf{Z}]=4$, then TE has, up to isomorphism, only one left R-module structure, and it satisfies $TE\oplus TE\cong\hat{R}'$ This follows in a routine manner from Theorems 3 and 4 We note that $E(k)_{\mathrm{tor}}$ may be identified with the injective limit of the groups $TE/n\ TE$, where n ranges over the positive integers and the map $TE/n\ TE\to TE/mn\ TE$ is induced by multiplication by m Thus the R-module structure of $E(k)_{\mathrm{tor}}$ can be recovered from that of TE

Rings are supposed to have unit elements in this paper, and modules are left modules, unless stated otherwise For a prime number p, we denote by $\mathbf{F}_p$ the field $\mathbf{Z}/\mathbf{Z}p$

2 Rank Two

In this section k, E, and R are as in Theorem 3, in particular, k is algebraically closed, and $[R\ \mathbf{Z}]=2$ In this situation R is commutative, the division ring $R_{\mathbf{Q}}=R\otimes\mathbf{Q}$ is an imaginary quadratic field extension of $\mathbf{Q}$, and R is an order in $R_{\mathbf{Q}}$ (see [13, Chapter III, Section 9]) For $s\in R$ we let $E[s]=\{P\in E(k)\ sP=O\}$

Proposition 2 1 *Let the notation and hypotheses be as above Then for every separable element $s\in R$ there is an isomorphism $E[s]\cong R/Rs$ of R-modules*

The proof depends on two lemmas A module M over a ring A is called *faithful* if $aM\neq 0$ for each $a\in A$, $a\neq 0$ A *minimal* ideal or submodule is understood to be a minimal non-zero one

Lemma 2 2 *Let A be a finite commutative ring Then the following two statements are equivalent*

(i) *each faithful A-module M contains a submodule that is free of rank 1 over A,*

(ii) *the number of maximal ideals of A is equal to the number of minimal ideals of A*

Proof (i) $\Rightarrow$ (ii) Let $M=\mathrm{Hom}(A, \mathbf{Q}/\mathbf{Z})$ be the dual of the additive group of A The A-module structure on A induces an A-module structure on M It is clear that M is faithful and that $\#M=\#A$, so by (i) we have $M\cong A$ Hence the number of minimal ideals of A equals the number of minimal submodules of M By duality, the latter number equals the number of maximal ideals of A

(ii) $\Rightarrow$ (i) Let M be a faithful A-module We have $A\cong\prod_{\mathfrak{m}} A_{\mathfrak{m}}$, with $\mathfrak{m}$ ranging over the maximal ideals of A (see [1, Theorem 8 7]) It follows that $M\cong\prod_{\mathfrak{m}} M_{\mathfrak{m}}$, where each $M_{\mathfrak{m}}$ is faithful as an $A_{\mathfrak{m}}$-module Each $A_{\mathfrak{m}}$ has a unique maximal ideal, and clearly at least one minimal ideal, hence, by (ii), each $A_{\mathfrak{m}}$ has a *unique* minimal ideal Let $a_{\mathfrak{m}}$ be a non-zero element of the unique minimal ideal of $A_{\mathfrak{m}}$ Since $M_{\mathfrak{m}}$ is faithful, there exists $x_{\mathfrak{m}}\in M_{\mathfrak{m}}$ with $a_{\mathfrak{m}}x_{\mathfrak{m}}\neq 0$ Then the annihilator of $x_{\mathfrak{m}}$ in $A_{\mathfrak{m}}$ does not contain the unique minimal ideal of $A_{\mathfrak{m}}$, so this annihilator is zero Therefore the submodule $A_{\mathfrak{m}}x_{\mathfrak{m}}$ of $M_{\mathfrak{m}}$ is isomorphic to $A_{\mathfrak{m}}$ The direct sum of the modules $A_{\mathfrak{m}}x_{\mathfrak{m}}$ is isomorphic to A, as required This proves 2 2

A finite commutative ring A satisfies (ii) if and only if it is a Gorenstein ring, and if and only if it is a quasi-Frobenius ring (see [5, Chapter VIII, Section 58]) This will not be used in the sequel

We use a circumflex to denote the canonical involution of $\mathrm{End}_k E$, it maps R to R, since $s+\hat{s}=\deg(s+1)-\deg s-1\in\mathbf{Z}$ for all $s\in\mathrm{End}_k E$

LEMMA 2.3 *Let $s\in R$, $s\neq 0$ Then R/Rs is a finite ring of cardinality $s\hat{s}$, and the number of maximal ideals of R/Rs is equal to the number of minimal ideals of R/Rs*

Proof The canonical involution is the restriction to R of the unique non-trivial automorphism of $R_{\mathbf{Q}}$ One deduces that the determinant of the $\mathbf{Q}$-linear map $R_{\mathbf{Q}}\to R_{\mathbf{Q}}$ that sends every x to xs equals $s\hat{s}$, so that $\#R/Rs=s\hat{s}<\infty$

Write $A=R/Rs$, and let q be a prime number dividing $\#A$ To prove 2.3 it suffices to show that the number of maximal ideals $\mathfrak{m}\subset A$ with $Aq\subset\mathfrak{m}$ is equal to the number of minimal ideals $\mathfrak{n}\subset A$ with $q\mathfrak{n}=0$ Let $A_q=\{a\in A\ qa=0\}$ Since A is finite, we have $\#A_q=\#A/Aq$, and since R/Rq maps surjectively to A/Aq the number $\#A/Aq$ equals either q or q^2 If $\#A_q=\#A/Aq=q$, then the only $\mathfrak{m}$, $\mathfrak{n}$ as above are $\mathfrak{m}=Aq$, $\mathfrak{n}=A_q$, so the number of $\mathfrak{m}$'s and the number of $\mathfrak{n}$'s are both equal to 1 Suppose therefore that $\#A_q=\#A/Aq=q^2$ Then the map $R/Rq\to A/Aq$ is an isomorphism, so $s=rq$ for some $r\in R$ It follows that $A_q=(R\cap Rsq^{-1})/Rs=Rr/Rrq\cong R/Rq\cong A/Aq$ (as A-modules), and under this isomorphism the minimal ideals $\mathfrak{n}\subset A_q$ that we are counting map to the minimal ideals of A/Aq Thus it remains to prove that the ring A/Aq of cardinality q^2 has equally many maximal and minimal ideals If A/Aq has only trivial ideals (so that it is a field) that is clear, and in the other case an ideal is maximal if and only if it has cardinality q, and if and only if it is minimal, so that the statement is again clear This proves 2.3

Proof of 2.1 We put $A=R/Rs$ and $M=E[s]$ Clearly, M is an A-module, and we claim that it is a *faithful* A-module, that is, any $r\in R$ with $rM=0$ belongs to Rs Namely, let $r\in R$ annihilate $M=E[s]$ Since s is separable, the homomorphism theorem for elliptic curves (see [13, Chapter III, Corollary 4.11]) implies that $r=ts$ for some endomorphism t of E We have $t\ s\hat{s}=r\hat{s}\in R$, where $s\hat{s}$ is a positive integer Since $(\mathrm{End}_k E)/R$ is supposed to be torsion-free this implies that $t\in R$, so that $r\in Rs$, which proves the claim From 2.3 we see that A satisfies 2.2(ii) Applying 2.2 we thus find that M contains a free A-module of rank 1 By [13, Chapter III, Theorem 4.10(c) and Theorem 6.2(a)] we have $\#M=\deg s=s\hat{s}$, which by 2.3 is equal to $\#A$ Therefore M is free over A of rank 1 This proves 2.1

It will be useful to have a similar result for inseparable s To state such a result, we assume without loss of generality that $p=\mathrm{char}\,k>0$, and we introduce some additional notation We still assume that $[R\ \mathbf{Z}]=2$

For $s \in R$, $s \neq 0$, let $\deg_i s$ denote the inseparable degree of s (see [13, Chapter II, Section 2]), which is a power of p. We put $\deg_i 0 = \infty$. From the definition of $\deg_i$ it is clear that $\deg_i(st) = \deg_i s \cdot \deg_i t$ for all $s, t \in R$. We also have $\deg_i(s+t) \geqslant \min\{\deg_i s, \deg_i t\}$ for all $s, t \in R$, this follows easily from the fact that $\deg_i s$ is divisible by a given power q of p if and only if s factors via the qth power Frobenius morphism $E \to E^{(q)}$ (see [13, Chapter II, Corollary 2.12]). It follows that there is an exponential p-adic valuation v on $R_{\mathbf{Q}}$ such that $v(s) = \log(\deg_i s)/\log p$ for all $s \in R$. Let $V = \{x \in R_{\mathbf{Q}} \mid v(x) \geqslant 0\}$ be the valuation ring. Note that $R \subset V$.

PROPOSITION 2.4. *Let the notation and hypotheses be as above. Then for every non-zero element $s \in R$ there is an isomorphism $E[s] \oplus (V/Vs) \cong R/Rs$ of R-modules.*

Proof. We first show that $E[s] \oplus (V/Vs)$ is faithful as an R/Rs-module. Suppose that $r \in R$ annihilates both $E[s]$ and V/Vs. Then $\deg_i r \geqslant \deg_i s = q$ (say), so if F denotes the qth power Frobenius morphism then $r = r'F$, $s = s'F$ for certain r', s': $E^{(q)} \to E$, with s' separable. Now the homomorphism theorem for elliptic curves implies, as above, that $r' = ts'$ for some $t \in \mathrm{End}_k E$. Then $r = ts$, and as above one finds that $t \in R$, as desired.

From 2.2 and 2.3 it now follows that $E[s] \oplus (V/Vs)$ contains a submodule isomorphic to R/Rs. By 2.3 we have $\#R/Rs = s\hat{s}$, and by [13, Chapter III, Theorem 4.10(a) and Theorem 6.2(a)] we have $\#E[s] = s\hat{s}/\deg_i s$. Hence we obtain $\#V/Vs \geqslant \deg_i s$, and to prove 2.4 it suffices to show that we have equality. Since each of $\#V/Vs$ and $\deg_i s$ is a constant power of $p^{v(s)}$, it suffices to prove equality for a single choice of s with $v(s) \neq 0$. We choose $s = p$. Because V is contained in a two-dimensional $\mathbf{Q}$-vector space, we have $\#V/Vp \leqslant p^2$, which finishes the proof if $\deg_i p = p^2$. Hence suppose that $\deg_i p < p^2$. Then $\deg_i p = p$, and the p-adic Tate module $T_p E$, which is the projective limit of the groups $E[p^n]$ $(n \geqslant 1)$, is free of rank 1 over $\mathbf{Z}_p$. The action of R on $T_p E$ induces a ring homomorphism $R \to \mathbf{Z}_p$, and therefore a $\mathbf{Q}_p$-algebra homomorphism $R_{\mathbf{Q}} \to \mathbf{Q}_p$. By elementary algebraic number theory, the existence of such a homomorphism implies that p splits completely in $R_{\mathbf{Q}}$, so that p is a prime element of V and the residue class field V/Vp has p elements. This completes the proof of 2.4.

Remark. From 2.4 and its proof it follows easily that there is a $\mathbf{Z}_p$-algebra isomorphism $R \otimes_{\mathbf{Z}} \mathbf{Z}_p \cong V \otimes_{\mathbf{Z}} \mathbf{Z}_p$ or $R \otimes_{\mathbf{Z}} \mathbf{Z}_p \cong \mathbf{Z}_p \times \mathbf{Z}_p$, according as $\deg_i p = p^2$ or $\deg_i p = p$. This implies that the index of R in the maximal order of $R_{\mathbf{Q}}$ is not divisible by p, which is a result of Deuring.

We now prove Theorem 3. Let $S = R - \mathfrak{p}$ be the set of separable endomorphisms in R. First we show that $E(k)_{\mathrm{tor}} = \bigcup_{s \in S} E[s]$, the inclusion

$\supset$ being obvious For the other inclusion, suppose that $P \in E(k)_{tor}$, and let $m \in \mathbf{Z} \subset R$ be the order of P If $m \notin \mathfrak{p}$ then $s = m$ satisfies $s \in S$ and $P \in E[s]$ If $m \in \mathfrak{p}$, then $p = \operatorname{char} k \neq 0$, and any $s \in R$ for which $s \bmod Rm$ maps to $(O, 1 \bmod Vm)$ under some isomorphism $R/Rm \cong E[m] \oplus V/Vm$ as in 2 4 is separable and annihilates P

Reformulating 2 1, we see that for each $s \in S$ there is an isomorphism $E[s] \xrightarrow{\sim} Rs^{-1}/R$ of R-modules, let W_s be the set of such isomorphisms If t divides s, then passing to the largest submodules annihilated by t we see that any isomorphism $E[s] \xrightarrow{\sim} Rs^{-1}/R$ maps the submodule $E[t]$ of $E[s]$ isomorphically to Rt^{-1}/R, so there is a restriction map $W_s \to W_t$ Since the projective limit of a system of non-empty finite sets is non-empty (see [3, Chapitre III, paragraphe 7 4, Theoreme 1]), the projective limit of the sets W_s is non-empty Therefore we can make a simultaneous choice of isomorphisms $E[s] \xrightarrow{\sim} Rs^{-1}/R$ that commute with the inclusions $E[t] \subset E[s]$, $Rt^{-1}/R \subset Rs^{-1}/R$ Taking the union over s, we conclude that $E(k)_{tor} \cong R_{\mathfrak{p}}/R$ as R-modules This proves Theorem 3

3 Rank Four

In this section k, E, and R are as in Theorem 4, in particular, k is algebraically closed, and $[R\ \mathbf{Z}] = 4$ In this situation R is non-commutative (see [13, Chapter III, Section 9]) Hence the ring homomorphism $R \to k$ with kernel $\mathfrak{p}$ that was defined in the introduction is not injective, so $\mathfrak{p} \neq 0$, and therefore $\operatorname{char} k = p \neq 0$ For $n \in \mathbf{Z}$ we write $E[n] = \{P \in E(k)\ nP = O\}$

Proposition 3 1 *Suppose that* $[R\ \mathbf{Z}] = 4$, *and let* $n \in \mathbf{Z}$, $n \not\equiv 0 \bmod p$ *Then there is an isomorphism* $E[n] \cong \mathbf{Z}/\mathbf{Z}n \oplus \mathbf{Z}/\mathbf{Z}n$ *as abelian groups, and this group has up to isomorphism exactly one left* R*-module structure Furthermore, one has* $E[n] \oplus E[n] \cong R/Rn$ *as left* R*-modules*

Proof It is well-known that there is an isomorphism $E[n] \cong \mathbf{Z}/\mathbf{Z}n \oplus \mathbf{Z}/\mathbf{Z}n$ (see [13 Chapter III Corollary 6 4(b)]) The endomorphism ring $\operatorname{End} E[n]$ of this abelian group is isomorphic to the ring $M(2, \mathbf{Z}/\mathbf{Z}n)$ of 2×2 matrices over $\mathbf{Z}/\mathbf{Z}n$, and has order n^4

As in the proof of 2 1 we see that $E[n]$ is a faithful module over the ring R/Rn, so the map $R/Rn \to \operatorname{End} L[n]$ that describes the module structure is injective Since both rings have cardinality n^4 this implies that it is an isomorphism

To prove that $\mathbf{Z}/\mathbf{Z}n \oplus \mathbf{Z}/\mathbf{Z}n$ has, up to isomorphism, only one left R-module structure, it suffices to show that it has, up to isomorphism, only one left module structure over the ring $M(2, \mathbf{Z}/\mathbf{Z}n)$ By Morita

equivalence (see [9, Section 3 12]), each left $M(2, \mathbf{Z}/\mathbf{Z}n)$-module P is isomorphic to one of the form $(\mathbf{Z}/\mathbf{Z}n \oplus \mathbf{Z}/\mathbf{Z}n) \otimes_{\mathbf{Z}/\mathbf{Z}n} Q$, where Q is a $\mathbf{Z}/\mathbf{Z}n$-module that is uniquely determined by P, up to isomorphism (namely, $Q = F \otimes_{M(2, \mathbf{Z}/\mathbf{Z}n)} P$, where F is the right $M(2, \mathbf{Z}/\mathbf{Z}n)$-module $\mathrm{Hom}(\mathbf{Z}/\mathbf{Z}n \oplus \mathbf{Z}/\mathbf{Z}n, \mathbf{Z}/\mathbf{Z}n)$) In this situation, P and $Q \oplus Q$ are isomorphic as abelian groups, and the statement to be proved is therefore equivalent to the easily proven fact that $Q \oplus Q \cong \mathbf{Z}/\mathbf{Z}n \oplus \mathbf{Z}/\mathbf{Z}n$ implies that $Q \cong \mathbf{Z}/\mathbf{Z}n$

The final assertion of 3 1 is equivalent to the statement that $M(2, \mathbf{Z}/\mathbf{Z}n)$ is, as a left module over itself, isomorphic to $(\mathbf{Z}/\mathbf{Z}n \oplus \mathbf{Z}/\mathbf{Z}n) \oplus (\mathbf{Z}/\mathbf{Z}n \oplus \mathbf{Z}/\mathbf{Z}n)$, which is obvious This proves 3 1

Remark From the proof of 3 1 one easily derives that $R \otimes_{\mathbf{Z}} \mathbf{Z}_l \cong M(2, \mathbf{Z}_l)$ for every prime number $l \neq p$ Using the map $\deg_i$ as in the previous section, one can show that $R \otimes_{\mathbf{Z}} \mathbf{Z}_p$ is the "valuation ring" of a non-commutative division algebra of degree 4 over $\mathbf{Q}_p$ From these statements it follows that R is a maximal order in the division algebra $R \otimes_{\mathbf{Z}} \mathbf{Q}$, a result that is due to Deuring

We now prove Theorem 4 Above we saw already that the characteristic p of k is non-zero By a theorem of Deuring (see [13, Chapter V, Theorem 3 1]) there are no elements of order p in $E(k)_{\mathrm{tor}}$, so $E(k)_{\mathrm{tor}} = \bigcup_n E[n]$, with n ranging over $\mathbf{Z} - \mathbf{Z}p$ It also follows that for each non-zero $s \in R$ the order $s\hat{s}/\deg_i s$ of the subgroup $\{P \in E(k) \mid sP = O\}$ of $E(k)_{\mathrm{tor}}$ is not divisible by p Therefore an element s of R belongs to $\mathfrak{p}$ if and only if the integer $s\hat{s}$ is divisible by p This implies that the group $R_{\mathfrak{p}}$ defined in the introduction is, as a sub-left-R-module of $R_{\mathbf{Q}}$, generated by $\{n^{-1} \mid n \in \mathbf{Z} - \mathbf{Z}p\}$

As in the proof of Theorem 3, the isomorphisms $E[n] \cong (\mathbf{Z}n^{-1}/\mathbf{Z}) \oplus (\mathbf{Z}n^{-1}/\mathbf{Z})$ and $E[n] \oplus E[n] \cong Rn^{-1}/R$ can be glued together to isomorphisms $E(k)_{\mathrm{tor}} \cong (\mathbf{Z}_{(p)}/\mathbf{Z}) \oplus (\mathbf{Z}_{(p)}/\mathbf{Z})$ (as abelian groups) and $E(k)_{\mathrm{tor}} \oplus E(k)_{\mathrm{tor}} \cong R_{\mathfrak{p}}/R$ (as R-modules) Also, two R-module structures on $(\mathbf{Z}_{(p)}/\mathbf{Z}) \oplus (\mathbf{Z}_{(p)}/\mathbf{Z})$ give rise to two R-module structures on $(\mathbf{Z}n^{-1}/\mathbf{Z}) \oplus (\mathbf{Z}n^{-1}/\mathbf{Z})$ for each n, which by 3 1 are isomorphic, and again by the projective limit argument from the proof of Theorem 3 such isomorphisms can be glued together This proves Theorem 4

4 Finite Fields

In this section we prove Theorem 1 We let k, E, R, π, l, and n be as in Theorem 1, in particular, k is now a finite field, and $R = \mathrm{End}_k E$ We choose an algebraic closure $\bar{k}$ of k containing l We write $\bar{R} = \mathrm{End}_{\bar{k}} E$, which is the ring of endomorphisms of E defined over $\bar{k}$ A theorem of Deuring (see [13, Chapter V, Theorem 3 1]) states that $\bar{R} \otimes_{\mathbf{Z}} \mathbf{Q}$ is a definite quaternion algebra if E is supersingular and an imaginary quadratic field otherwise

An endomorphism in $\bar{R}$ belongs to R if and only if it commutes with the action of the Frobenius automorphism Since the latter acts in the same way as π, we have $R=\{r\in\bar{R}\ \pi r=\pi r\}$ It also follows that the additive group $\bar{R}/R$ is torsion-free

Let it now first be assumed that $\pi\notin\mathbf{Z}$ We have $\pi\in R$, so $[R\ \mathbf{Z}]\neq 1$ Since π belongs to the center of R, we have $[R\ \mathbf{Z}]\neq 4$ Therefore we have $[R\ \mathbf{Z}]=2$

To prove part (a) of Theorem 1, we note that $E(l)=E[\pi^n-1]$, in the notation of 2 1, here π^n-1 is separable because $\pi\in\mathfrak{p}$ From 2 1, applied with k as the base field, it now follows that $E(l)\cong R/R(\pi^n-1)$ as R-modules, as required

Next suppose that $\pi\in\mathbf{Z}$ From $\pi^2=\pi\hat{\pi}=\#k$ it follows that k has even degree over its prime field, and that $\pi=\pm\sqrt{\#k}$ For each positive integer m, the integer π^m-1 annihilates $E(k_m)$, where k_m is the unique intermediate field of $k\subset\bar{k}$ with $[k_m\ k]=m$ Since π^m-1 is coprime to p, it follows that $E(k_m)$ does not contain an element of order p, and the same is then true for $E(\bar{k})=\bigcup_m E(k_m)$ By a theorem of Deuring (see [13, Chapter V, Theorem 3 1]) this implies that E is supersingular, so that $\bar{R}$ is an order in a definite quaternion algebra From $\pi\in\mathbf{Z}$ we see that $R=\{r\in\bar{R}\ \pi r=\pi r\}=\bar{R}$ In particular, we have $[R\ \mathbf{Z}]=4$

To prove part (b) of Theorem 1, it now suffices to note that $E(l)=E[\pi^n-1]$ and to invoke Proposition 3 1 This proves Theorem 1

4 1 *Remark* The observation, in the proof above, that $\bar{R}/R$ is torsion-free, carries over to arbitrary base fields, that is, if E is an elliptic curve over any field k, and l denotes any extension field of k, then $(\mathrm{End}_l E)/(\mathrm{End}_k E)$ is torsion-free To prove this, it suffices to consider (i) the case that l is Galois over k, and (ii) the case that every element of l that is algebraic over k is purely inseparable over k In the first case one uses, as in the proof above, that $\mathrm{End}_k E$ consists of the elements of $\mathrm{End}_l E$ that are fixed under the action of the Galois group In the second case one has in fact $\mathrm{End}_l E=\mathrm{End}_k E$ (apply [10, Chapter II, Theorem 5], with B equal to the graph of an endomorphism)

5 Algebraically Closed Fields

In this section we let k, E, R, and $E(k)_{\mathrm{tor}}$ be as in Theorem 2

Proposition 5 1 *As a left R-module, $E(k)_{\mathrm{tor}}$ is injective*

Proof For background on injective and projective modules, see [9, 3 10 and 3 11] We distinguish three cases, according to the value of

$[R\ \mathbf{Z}]$ If $[R\ \mathbf{Z}]=1$ then $R=\mathbf{Z}$, and in this case the injectivity of $E(k)_{\text{tor}}$ follows from the fact that it is divisible as an abelian group

Next suppose that $[R\ \mathbf{Z}]=2$ We first show that for any non-zero $s\in R$ the ring R/Rs is injective as a module over itself The category of finite R/Rs-modules has a duality that sends any module M to $\mathrm{Hom}_{\mathbf{Z}}(M, \mathbf{Q}/\mathbf{Z})$ Since it is a duality, it interchanges injective and projective objects From 2 2 and 2 3 it also follows that the dual of a free module of rank one is free of rank one (cf the proof of 2 2, (i) $\Rightarrow$ (ii)), so that the dual of a projective module is projective Hence the projective and injective objects of this category are the same In particular, R/Rs is injective, also in the category of *all* R/Rs-modules (by [9, Proposition 3 15]) The same applies to the isomorphic module Rs^{-1}/R

We deduce that $R_{\mathbf{Q}}/R$ is injective as an R-module By [9, Proposition 3 15] it suffices to show that any R-linear map f from a non-zero R-ideal a to $R_{\mathbf{Q}}/R$ can be extended to a map $R\to R_{\mathbf{Q}}/R$ Since $R_{\mathbf{Q}}/R$ is torsion we can find a non-zero element $s\in\ker f$ Then f induces an R/Rs-linear map $a/Rs\to Rs^{-1}/R$, which by injectivity of Rs^{-1}/R can be extended to an R/Rs-linear map $R/Rs\to Rs^{-1}/R$ The latter map induces an extension of f to a map $R\to R_{\mathbf{Q}}/R$, as required

If $\mathrm{char}\ k=0$ then we have $R_{\mathbf{Q}}=R_p$, so Theorem 3 tells us that $E(k)_{\text{tor}}\cong R_{\mathbf{Q}}/R$ If $\mathrm{char}\ k>0$ then 2 4 and the projective limit argument in the proof of Theorem 3 show that $E(k)_{\text{tor}}\oplus(R_{\mathbf{Q}}/V)\cong R_{\mathbf{Q}}/R$ as R-modules In both cases the injectivity of $R_{\mathbf{Q}}/R$ implies that of $E(k)_{\text{tor}}$

The argument in the case that $[R\ \mathbf{Z}]=4$ is similar but simpler If $n\in\mathbf{Z}, n\neq 0$, then as above one deduces from 2 2 that all finite projective $\mathbf{Z}/\mathbf{Z}n$-modules are injective By Morita equivalence, the same is true for finite projective $M(2, \mathbf{Z}/\mathbf{Z}n)$-modules As above it follows that $R_{\mathbf{Q}}/R$ is injective as a left R-module Removing the p-primary part, which is a direct summand, and applying the isomorphism $E(k)_{\text{tor}}\oplus E(k)_{\text{tor}}\cong R_p/R$ from Theorem 4, one concludes that $E(k)_{\text{tor}}$ is injective as well This proves 5 1

We now prove Theorem 2 It is clear that 5 1 implies part (a) of the theorem From the divisibility of $E(k)$ as an abelian group it follows that the R-module $E(k)/E(k)_{\text{tor}}$ may be identified with the vector space $E(k)\otimes_{\mathbf{Z}}\mathbf{Q}$ over the division ring $R_{\mathbf{Q}}$ So to prove the remaining assertions of Theorem 2 it suffices to show that $\dim_{R_{\mathbf{Q}}}\otimes_{\mathbf{Z}}\mathbf{Q}$ equals 0 or $\#k$, according as k is algebraic over a finite field or not

First suppose that k is algebraic over a finite field Then E is defined over some finite subfield k' of k, and $E(k)$ is the union of the finite subgroups $E(l)$, with l ranging over the finite subfields of k that contain k' Therefore $E(k)\otimes_{\mathbf{Z}}\mathbf{Q}=0$

Now suppose that k is not algebraic over a finite field, and let $k_0\subset k$ be a subfield that is either $\mathbf{Q}$ or $\mathbf{F}_p(t)$ for some t that is transcendental over

$\mathbf{F}_p$. It is easy to see that $\#E(k) = \#k$, and for cardinality reasons it follows that $\dim_{R_\mathbf{Q}} E(k) \otimes_\mathbf{Z} \mathbf{Q}$ is equal to $\#k$ if $\#k$ is uncountable, and at most $\#k$ if k is countable. Therefore it suffices to show that $E(k) \otimes_\mathbf{Z} \mathbf{Q}$ is not finite dimensional over $R_\mathbf{Q}$, or over $\mathbf{Q}$, which by $\dim_\mathbf{Q} R_\mathbf{Q} < \infty$ is the same.

Suppose that $E(k) \otimes_\mathbf{Z} \mathbf{Q}$ is finite dimensional over $\mathbf{Q}$, and choose finitely many points $P_i \in E(k)$ that give a basis. Also, choose a finitely generated subfield k_1 of k, containing k_0, such that E can be defined over k_1 and such that the coordinates of the points P_i belong to k_1. Then the inclusion $E(k_1) \subset E(k)$ induces an isomorphism $E(k_1) \otimes_\mathbf{Z} \mathbf{Q} \cong E(k) \otimes_\mathbf{Z} \mathbf{Q}$. Hence, if one first adjoins to k_1 all the torsion points of $E(k)$ and next the points $(1/m)P_i$ for all positive integers m and all i, then one obtains the field $k_1(E(k))$, which is the same as the algebraically closed field k. Looking at the Galois groups of these extensions, and consulting the list of subgroups of the group $PSL_2\mathbf{F}_q$ (for q prime) (see [8, Kapitel II, 8.27]), one concludes that the non-cyclic composition factors of any finite Galois group over k_1 are among the groups $PSL_2\mathbf{F}_q$, for $q \geqslant 5$ prime. Since the image of the natural map of the absolute Galois group of k_1 to the absolute Galois group of k_0 has finite index in the latter, it follows that the finite Galois groups over k_0 are built up from the same composition factors, plus possibly finitely many additional simple groups. This is absurd, since k_0 has for each positive integer n a Galois extension with group isomorphic to the full symmetric group of degree n (see [14, section 66] for $k_0 = \mathbf{Q}$, the case $k_0 = \mathbf{F}_p(t)$ can be done in a similar manner).

6. Abelian Varieties

In this section we show that straightforward generalizations of the results of this paper to higher dimensional abelian varieties cannot be expected to exist. We restrict attention to the situation of Theorem 3, in which $[R\ \mathbf{Z}] = 2$. It may not be obvious what the proper generalization of the condition $[R\ \mathbf{Z}] = 2$ to higher dimensional abelian varieties is, however, any reasonable generalization would seem to include at least those abelian varieties A over an algebraically closed field k that satisfy the following conditions, in which we put $g = \dim A$.

(6.1) if we put $R = \mathrm{End}_k A$, then $R_\mathbf{Q} = R \otimes_\mathbf{Z} \mathbf{Q}$ is a complex CM field of degree $2g$ over $\mathbf{Q}$,

(6.2) A is ordinary, i.e., if $p = \mathrm{char}\, k \neq 0$ then $\dim_{\mathbf{F}_p} \{P \in A(k) \mid pP = O\} = g$,

(6.3) A has a principal polarization.

Condition (6 1) means that $R_{\mathbf{Q}}$ is a number field that is a totally imaginary quadratic extension of a totally real field of degree g over $\mathbf{Q}$ For the notion of a principal polarization, see [4, Chapters IV and V]

We show that even when we restrict to abelian varieties satisfying these conditions the direct analogue of Proposition 2 1 is false

PROPOSITION 6 4 *Let k be either the field $\mathbf{C}$ of complex numbers or, for some prime number p, an algebraic closure of the field $\mathbf{F}_p$ Let g be an integer with $g > 1$, and let Q be a finite set of prime numbers different from* char k *Then there exists an abelian variety A over k with* dim $A = g$ *satisfying* (6 1), (6 2), *and* (6 3), *such that for each $q \in Q$ the R-modules $A[q] = \{P \in A(k)\ qP = O\}$ and R/Rq are non-isomorphic, here we put $R = \mathrm{End}_k A$*

Proof We give only a sketch of the proof

Let it first be supposed that $k = \mathbf{C}$ In [4, Chapter IV] one finds a description of the category of abelian varieties over $\mathbf{C}$ in terms of lattices (see also [11, Chapter 1]) In addition, one finds that both condition (6 3) and the structure of $A[q]$ as an R-module can be described in terms of the corresponding lattice Thus one can translate the entire problem into a problem about lattices Doing this, one finds that the conclusion of 6 4 is, in the case $k = \mathbf{C}$, equivalent to the existence of a totally real number field K_0 of degree g over $\mathbf{Q}$, a totally imaginary quadratic extension K of K_0, a set Φ of field embeddings $K \to \mathbf{C}$, an additive subgroup $\mathfrak{a} \subset K$ that is free of rank $2g$, and an element $\xi \in K$, such that the following conditions are satisfied

(6 5) $\bar{\xi} = -\xi \neq 0$, where the overhead bar denotes the non-trivial automorphism of K over K_0,

(6 6) Φ is the set of those field homomorphisms $\varphi\ K \to \mathbf{C}$ for which $\varphi(\xi)$ has positive imaginary part,

(6 7) if Tr denotes the trace function of K over $\mathbf{Q}$, then $\mathfrak{a} = \{x \in K\ \mathrm{Tr}(\xi x \bar{y}) \in \mathbf{Z}$ for all $y \in \mathfrak{a}\}$,

(6 8) if R denotes the subring $\{x \in K\ x\mathfrak{a} \subset \mathfrak{a}\}$ of K, then for each $q \in Q$ one has $\mathfrak{a}/\mathfrak{a}q \cong R/Rq$ as R-modules

To construct such objects one starts from an arbitrary totally real number field K_0 of degree g over $\mathbf{Q}$ and an arbitrary totally imaginary quadratic extension K of K_0 Next one lets $\alpha \in K$ be an algebraic integer satisfying $\alpha + \bar{\alpha} \in \mathbf{Z}$ and $K = \mathbf{Q}(\alpha)$, it is easy to show that such α exist (one may, for the moment, even take $\alpha + \bar{\alpha} = 0$) Now we put $m = \prod_{q \in Q} q$, and

$$A = \mathbf{Z}[\alpha] = \mathbf{Z} + \mathbf{Z}\alpha + \cdots + \mathbf{Z}\alpha^{2g-1},$$
$$R = \mathbf{Z} + Am = \mathbf{Z} + \mathbf{Z}m\alpha + \cdots + \mathbf{Z}m\alpha^{2g-1},$$
$$\mathfrak{a} = (\mathbf{Z} + \mathbf{Z}\alpha)^{g-1} \cdot (\mathbf{Z} + \mathbf{Z}m\alpha^g)$$
$$= \mathbf{Z} + \mathbf{Z}\alpha + \cdots + \mathbf{Z}\alpha^{g-1} + \mathbf{Z}m\alpha^g + \cdots + \mathbf{Z}m\alpha^{2g-1}.$$

We have $R \subset \mathfrak{a} \subset A$, and R, A are rings, while $\mathfrak{a}$ is an R-module. To define ξ, we let $f: K \to \mathbf{Q}$ be the $\mathbf{Q}$-linear map defined by $f(\alpha^i) = 0$ $(0 \leqslant i < 2g-1)$, $f(\alpha^{2g-1}) = 1/m$. There is a unique element $\xi \in K$ such that for all $x \in K$ one has $f(x) = \mathrm{Tr}(\xi x)$. From $\alpha + \bar{\alpha} \in \mathbf{Z}$ it follows that $f(x) = -f(\bar{x})$ and hence that $\bar{\xi} = -\xi$; this proves (6.5). Condition (6.6) is taken as the definition of Φ. The verification of (6.7) is straightforward. To show that R is the same as the ring defined in (6.8), we note that the subring $R' = \{x \in K: x\mathfrak{a} \subset \mathfrak{a}\}$ of K satisfies $R \subset R' \subset \mathfrak{a}$; the only such ring is R itself, so $R' = R$. Suppose that for some $q \in Q$ one has $\mathfrak{a}/\mathfrak{a}q \cong R/Rq$ as R-modules. Then $\mathfrak{a} = Ra + \mathfrak{a}q \subset \mathbf{Z}a + Aq$ for some $a \in \mathfrak{a}$, so the image of $\mathfrak{a}$ in A/Aq is at most one-dimensional over $\mathbf{F}_q$. However, inspection shows that it has dimension equal to g, which contradicts our assumption that $g > 1$. This proves 6.4 in the case $k = \mathbf{C}$.

Secondly, we consider the case that k is an algebraic closure of $\mathbf{F}_p$, for some prime number p. In [6] one finds a description of the category of ordinary abelian varieties over finite fields in terms of lattices. Again, one can describe the R-module structure of $A[q]$ in terms of the lattice corresponding to A, and the same applies to the existence of polarizations (see [7, Section 4]). One finds that the conclusion of 6.4, in the present case, is equivalent to the existence of K_0, K, Φ, $\mathfrak{a}$, ξ satisfying all the conditions above, together with an element $\pi \in R$ for which

(6.9) $\pi\bar{\pi} = p^n$ for some positive integer n, and $K = \mathbf{Q}(\pi^m)$ for all positive integers m;

(6.10) there is an exponential valuation v on $\mathbf{C}$ such that Φ consists of those field homomorphisms $\varphi: K \to \mathbf{C}$ for which $v(\varphi\pi) > 0$.

(The valuation in (6.10) is, by (6.9), necessarily a p-adic one. Also, from the fact that Φ consists of 'half' the embeddings $K \to \mathbf{C}$ and (6.10) one deduces that π is, as an algebraic integer, coprime to $\bar{\pi}$.)

For the construction of π it is convenient to suppose that K_0 and K are chosen so that the following conditions are satisfied:

(6.11) p is totally ramified in the extension $\mathbf{Q} \subset K_0$, and the prime of K_0 lying over p splits completely in the extension $K_0 \subset K$;

(6.12) the Galois closure M of K over $\mathbf{Q}$ has degree $2^g g!$ over $\mathbf{Q}$.

Note that the degree $2^g g!$ in (6.12) is largest possible, and that it is achieved if and only if the Galois closure M_0 of K_0 over $\mathbf{Q}$ has the full

symmetric group of degree g as its Galois group and $[M\ M_0]=2^g$ It is easy to construct K and K_0 such that (6 11) and (6 12) hold (cf the technique used in [12]) Also, we shall suppose that the algebraic integer $\alpha\in K$ chosen above satisfies

(6 13) the index $\langle \mathcal{O}\ A\rangle$ of $A=\mathbf{Z}[\alpha]$ in the ring of integers $\mathcal{O}$ of K is coprime to p,

in addition to the two conditions $\alpha+\bar{\alpha}\in\mathbf{Z}$ and $K=\mathbf{Q}(\alpha)$ This is, again, easy to achieve, because of (6 11) (but if $p=2$ we cannot have $\alpha+\bar{\alpha}=0$ any more)

Let A, R, $\mathfrak{a}$, ξ, and Φ now be chosen as above From (6 11) it follows that there is a prime ideal $\mathfrak{p}$ of $\mathcal{O}$ such that $\mathfrak{p}\neq\bar{\mathfrak{p}}$ and $\mathfrak{p}^g\bar{\mathfrak{p}}^g=\mathcal{O}p$ Some power of $\mathfrak{p}^g$ is principal, so we have $\mathcal{O}\pi\bar{\pi}=\mathcal{O}p^n$ for some positive integer n and some $\pi\in\mathcal{O}$ that is coprime to $\bar{\pi}$ Replacing π by $\pi p^n/\bar{\pi}$ and n by $2n$ we may in fact assume that $\pi\bar{\pi}=p^n$ From (6 13) it follows that $\langle \mathcal{O}\ R\rangle$ is coprime to π, so there is some power of π that is congruent to 1 modulo $\mathcal{O}\langle \mathcal{O}\ R\rangle$ and therefore belongs to R If we replace π by that power, and n by its corresponding multiple, then we obtain an element $\pi\in R$ that is coprime to $\bar{\pi}$ and satisfies $\pi\bar{\pi}=p^n$ For any positive integer m the subfield $\mathbf{Q}(\pi^m)$ of K is imaginary, and (6 12) implies that the only such subfield is K itself This proves (6 9)

From (6 12) it follows that all primes of M_0 lying over p split completely in the elementary abelian extension $M_0\subset M$ of degree 2^g Viewing M_0 and M as subfields of the field of complex numbers one deduces from this that any p-adic valuation of M_0 can be extended to a unique valuation v of M such that $v(\varphi\pi)>0$ for all $\varphi\in\Phi$ Extending v to $\mathbf{C}$ we then find that (6 10) holds, since π is coprime to $\bar{\pi}$

This completes the proof of Proposition 6 4

In the situation of 6 4 the R-module $A(k)_{\mathrm{tor}}$ cannot be embedded in $R_{\mathbf{Q}}/R$, so that the higher-dimensional analogue of Theorem 3 breaks down Also, when $\mathrm{char}\ k\neq 0$, then we can replace k by a finite subfield over which A can be defined, and take for l any finite extension of k over which all points of $A[q]$ are defined, for some $q\in Q$ This yields counterexamples to higher-dimensional analogues of Theorem 1(a)

Acknowledgments

The author was supported by NSF under Grants DMS 90 02939 and DMS 92-24205, and by NSA/MSP under Grant MDA90-H-4043 The hospitality and support of the Institute for Advanced Study (Princeton) are gratefully acknowledged Part of the work reported in this paper was done while the author was on appointment as a Miller Research Professor in the Miller Institute for Basic Research in Science I thank S Edixhoven, E W Howe, and F Oort for helpful advice

REFERENCES

1 M F ATIYAH AND I G MACDONALD, "Introduction to Commutative Algebra," Addison-Wesley, Reading, MA, 1969
2 H BASS, On the ubiquity of Gorenstein rings, *Math Z* **82** (1963), 8–28
3 N BOURBAKI, "Theorie des ensembles," Diffusion C C L S, Paris, 1970
4 G CORNELL AND J H SILVERMAN (Eds), "Arithmetic Geometry," Springer-Verlag, New York, 1986
5 C W CURTIS AND I REINER, "Representation Theory of Finite Groups and Associative Algebras," Interscience, New York, 1962
6 P DELIGNE, Varietes abeliennes ordinaires sur un corps fini, *Invent Math* **8** (1969), 238–243
7 E W HOWE, Principally polarized ordinary abelian varieties over finite fields, *Trans Amer Math Soc* **347** (1995), 2361–2401
8 B HUPPERT, "Endliche Gruppen I," Springer Verlag, Berlin, 1967
9 N JACOBSON, "Basic Algebra II," 2nd ed, Freeman, New York, 1989
10 S LANG, "Abelian Varieties," Interscience, New York, 1959
11 S LANG, "Complex Multiplication," Springer-Verlag, New York, 1983
12 H W LENSTRA, JR AND F OORT, Simple abelian varieties having a prescribed formal isogeny type, *J Pure Appl Algebra* **4** (1974), 47–53
13 J H SILVERMAN, "The Arithmetic of Elliptic Curves," Springer-Verlag, New York, 1986
14 B L VAN DER WAERDEN, "Algebra, Erster Teil," 7th ed, Springer-Verlag, Berlin, 1966

Printed by Catherine Press, Ltd, Tempelhof 41, B-8000 Brugge, Belgium