A normal basis theorem for infinite Galois extensions

by H.W. Lenstra, Jr.

Mathematisch Instituut, University of Amsterdam, Roetersstraat 15, 1018 WB Amsterdam, the Netherlands

Communicated at the meeting of November 26, 1984

ABSTRACT

The normal basis theorem from Galois theory is generalized to infinite Galois extensions

INTRODUCTION

Let K be a field, L a Galois extension of K, and G the Galois group of L over K. We consider G as a topological group with the topology defined by Krull [4; 1, Chapitre V, Appendice II].

The *normal basis theorem* asserts that if L is finite over K there exists $x \in L$ such that the elements $\sigma(x)$, $\sigma \in G$, form a basis for L as a vector space over K, see [5; 3]. If L is infinite over K then no such basis exists, since for every $x \in L$ the set $\{\sigma(x) : \sigma \in G\}$ is finite. Hence if we wish to generalize the normal basis theorem to infinite Galois extensions we must look for an alternative formulation.

Let L be finite over K, and write (G,K) for the K-vector space of all functions $f: G \to K$. We let G operate on (G,K) by $(\sigma f)(\tau) = f(\sigma^{-1}\tau)$, for σ, $\tau \in G$. We can now reformulate the normal basis theorem by saying that there is an isomorphism $\varphi : (G,K) \to L$ of K-vector spaces that respects the action of G. Namely, if $(\sigma(x))_{\sigma \in G}$ is a basis of L over K, then we can define φ by $\varphi(f) = \sum_{\sigma \in G} f(\sigma)\sigma(x)$. Conversely, if $\varphi : (G,K) \to L$ is an isomorphism as above, and $h: G \to K$ is defined by $h(1) = 1$, $h(\tau) = 0$ ($\tau \in G$, $\tau \neq 1$), then $x = \varphi(h)$ has the property that $(\sigma(x))_{\sigma \in G}$ is a basis of L over K.

It turns out that this version of the normal basis theorem is valid for *infinite*

Galois extensions as well, provided that we only consider *continuous* functions $G \to K$.

THEOREM 1. *Let $K \subset L$ be a Galois extension of fields, with group G, and denote by $C(G, K)$ the K-vector space of all continuous functions $f: G \to K$; here G is provided with the Krull topology and K with the discrete topology. Let G operate on $C(G, K)$ by $(\sigma f)(\tau) = f(\sigma^{-1}\tau)$, for σ, $\tau \in G$. Then there exists an isomorphism $C(G, K) \to L$ of K-vector spaces that respects the action of G.*

The proof of this theorem is given in Section 3 of this paper.

We can also express the normal basis theorem by saying that, for L finite over K, the additive group of L is free on one generator as a left module over the group ring $K[G]$. This assertion can be generalized to the infinite case as follows.

Denote by U the set of open normal subgroups of G. We order U by letting $N' \leq N$ if and only if $N \subset N'$. For N, $N' \in U$, $N \subset N'$, let the ring homomorphism $\varrho_{N'/N}: K[G/N] \to K[G/N']$ be induced by the natural group homomorphism $G/N \to G/N'$. We write $K[[G]] = \varprojlim_{N \in U} K[G/N]$, the projective limit being taken with respect to the maps $\varrho_{N'/N}$ (see Section 1 for our conventions about projective limits). Observe that $K[[G]]$ contains the group ring $K[G]$ in a natural way, and is equal to it if G is finite.

For $N \in U$, let the subfield L^N of L be defined by $L^N = \{y \in L : \sigma(y) = y$ for all $\sigma \in N\}$; this is a finite Galois extension of K with group G/N. For N, $N' \in U$, $N \subset N'$, the *trace* map $\mathrm{Tr}_{N'/N}: L^N \to L^{N'}$ is defined by $\mathrm{Tr}_{N'/N}(y) = \sum_{\sigma \in N'/N} \sigma(y)$. The projective limit $\varprojlim_{N \in U} L^N$, taken with respect to the maps $\mathrm{Tr}_{N'/N}$, is in a natural way a left module over $K[[G]]$.

THEOREM 2. *For any Galois extension of fields $K \subset L$ with group G, the left $K[[G]]$-module $\varprojlim_{N \in U} L^N$ is free on one generator.*

The proof of this theorem is given in Section 3 of this paper.

1. PROJECTIVE LIMITS

A *preordered* set is a set I with a binary relation $\leq$ on I that is transitive and reflexive. A *directed* set is a preordered set I with the property that for any two α, $\beta \in I$ there exists $\gamma \in I$ with $\alpha \leq \gamma$ and $\beta \leq \gamma$. A *projective system* consists of a directed set I, a set E_α for each $\alpha \in I$, and a map $f_{\alpha\beta}: E_\beta \to E_\alpha$ for each pair α, $\beta \in I$ with $\alpha \leq \beta$, such that $f_{\alpha\alpha}$ equals the identity on E_α for each $\alpha \in I$, and $f_{\alpha\beta} f_{\beta\gamma} = f_{\alpha\gamma}$ for all $\alpha, \beta, \gamma \in I$ with $\alpha \leq \beta$ and $\beta \leq \gamma$. The *projective limit* of such a system, denoted by $\varprojlim E_\alpha$ or $\varprojlim_{\alpha \in I} E_\alpha$, is defined by

$$\varprojlim E_\alpha = \{(x_\alpha)_{\alpha \in I} \in \prod_{\alpha \in I} E_\alpha : f_{\alpha\beta}(x_\beta) = x_\alpha \text{ for all } \alpha,\ \beta \in I \text{ with } \alpha \leq \beta\}.$$

The projective limit may be empty, even if all E_α are non-empty and all $f_{\alpha\beta}$ are surjective [6]. We recall from Bourbaki [2, III.7.4] sufficient conditions for a projective system to have a non-empty projective limit.

Let I, $(E_\alpha)_{\alpha\in I}$, $(f_{\alpha\beta})_{\alpha,\beta\in I,\alpha\leq\beta}$ be a projective system in which all E_α are *non-empty*. We suppose that for each $\alpha\in I$ we are given a collection $\mathscr{S}_\alpha$ of subsets of E_α, such that the following four conditions are satisfied.

(1.1) If $\alpha\in I$ and $\mathscr{F}\subset\mathscr{S}_\alpha$ then $\bigcap_{M\in\mathscr{F}} M\in\mathscr{S}_\alpha$.

In particular, taking $\mathscr{F}=\emptyset$, we see that $E_\alpha\in\mathscr{S}_\alpha$.

(1.2) If $\alpha\in I$, and $\mathscr{F}\subset\mathscr{S}_\alpha$ is such that $\bigcap_{M\in\mathscr{F}'} M\neq\emptyset$ for all finite subsets $\mathscr{F}'\subset\mathscr{F}$, then $\bigcap_{M\in\mathscr{F}} M\neq\emptyset$.

(1.3) If α, $\beta\in I$, $\alpha\leq\beta$ and $x\in E_\alpha$, then $f_{\alpha\beta}^{-1}x\in\mathscr{S}_\beta$.

(1.4) If α, $\beta\in I$, $\alpha\leq\beta$ and $M\in\mathscr{S}_\beta$, then $f_{\alpha\beta}[M]\in\mathscr{S}_\alpha$.

In the following proposition we write $E=\varprojlim E_\alpha$. For $\alpha\in I$, we denote the natural map $E\to E_\alpha$ by f_α, and we put $E'_\alpha=\bigcap_{\beta\in I,\alpha\leq\beta} f_{\alpha\beta}[E_\beta]$; so $E'_\alpha\subset E_\alpha$, and $E'_\alpha=E_\alpha$ if all $f_{\alpha\beta}$ are surjective.

(1.5) PROPOSITION *With the above hypotheses and notation, we have.*

(a) $E\neq\emptyset$;

(b) $f_\alpha[E]=E'_\alpha$ *for each* $\alpha\in I$;

(c) *if* $J\subset I$ *is directed with respect to the restriction of* $\leq$ *to* J, *then the image of the natural map* $\varprojlim_{\alpha\in I} E_\alpha\to\varprojlim_{\alpha\in J} E_\alpha$ *is* $\varprojlim_{\alpha\in J} E'_\alpha$.

PROOF We need a few facts from the proof of [2, III.7 4, Theoreme 1]. Let Σ denote the set of all families $(A_\alpha)_{\alpha\in I}$ for which

$$A_\alpha\neq\emptyset \text{ and } A_\alpha\in\mathscr{S}_\alpha, \text{ for all } \alpha\in I,$$

$$f_{\alpha\beta}[A_\beta]\subset A_\alpha \text{ for all } \alpha,\ \beta\in I,\ \alpha\leq\beta.$$

Let $(A_\alpha)_{\alpha\in I}\leq(A'_\alpha)_{\alpha\in I}$ if and only if $A'_\alpha\subset A_\alpha$ for each $\alpha\in I$. This makes Σ into a partially ordered set. In [2, *loc cit*] it is shown that Σ satisfies the conditions of Zorn's lemma, and that the map $E\to\Sigma$ sending $(x_\alpha)_{\alpha\in I}$ to $(\{x_\alpha\})_{\alpha\in I}$ establishes a bijection between E and the set of maximal elements of Σ.

We use this to prove (c). Let $J\subset I$ be directed. It is trivial that the image of E in $\varprojlim_{\alpha\in J} E_\alpha$ is contained in $\varprojlim_{\alpha\in J} E'_\alpha$. To prove the other inclusion, let $(x_\alpha)_{\alpha\in J}\in\varprojlim_{\alpha\in J} E'_\alpha$. For $\beta\in I$, let $A_\beta=\bigcap_{\alpha\in J,\alpha\leq\beta} f_{\alpha\beta}^{-1}x_\alpha$. We claim that $A_\beta\neq\emptyset$. To prove this, it suffices by (1 3) and (1.2) to show that $\bigcap_{\alpha\in K,\alpha\leq\beta} f_{\alpha\beta}^{-1}x_\alpha\neq\emptyset$ for every *finite* subset $K\subset J$. Let K be such We may assume that $K\neq\emptyset$ Since J is directed, we can choose $\gamma\in J$ such that $\alpha\leq\gamma$ for all $\alpha\in K$, and since I is directed we can choose $\delta\in I$ such that $\beta\leq\delta$, $\gamma\leq\delta$. We have $x_\gamma\in E'_\gamma\subset f_{\gamma\delta}[E_\delta]$, so $x_\gamma=f_{\gamma\delta}(z)$ for some $z\in E_\delta$, and it is now readily verified that $f_{\beta\delta}(z)\in$ $\in\bigcap_{\alpha\in K,\alpha\leq\beta} f_{\alpha\beta}^{-1}x_\alpha$. This proves that $A_\beta\neq\emptyset$. It follows that $(A_\beta)_{\beta\in I}\in\Sigma$ The results about Σ quoted above imply that Σ has a maximal element $(\{y_\beta\})_{\beta\in I}$ with $(\{y_\beta\})_{\beta\in I}\geq(A_\beta)_{\beta\in I}$. Then $y_\beta\in A_\beta$, and since $A_\alpha=\{x_\alpha\}$ for $\alpha\in J$ this implies that $y_\alpha=x_\alpha$ for all $\alpha\in J$. Hence $(y_\beta)_{\beta\in I}\in E$ maps to $(x_\alpha)_{\alpha\in J}\in\varprojlim_{\alpha\in J} E_\alpha$. This proves (c).

PROOF With Zorn's lemma, choose $W\subset V$ maximal among all subsets $W'\subset V$ for which the sum $N+\bigoplus_{w\in W} M_w$ is direct. Then for $v\in V$ the sum $(N+\bigoplus_{w\in W}M_w)+M_v$ is not direct, by the maximality of W, so $(N+\bigoplus_{w\in W}M_w)\cap M_v\neq 0$; but M_v is simple, so $(N+\bigoplus_{w\in W}M_w)\cap M_v=M_v$, and $M_v\subset N+\bigoplus_{w\in W}M_w$ This implies that $M=N+\bigoplus_{w\in W}M_w$, and the lemma follows easily This proves (2 3).

(2.4) LEMMA *Let R be an Artin ring, and $x\in R$ Then we have:*

(a) *x is a unit if and only if it is a left unit, and if and only if it is a right unit;*

(b) *R has only finitely many maximal two-sided ideals.*

(c) *$x\in R^*$ if and only if $(x \bmod \mathfrak{m})\in(R/\mathfrak{m})^*$ for every maximal two-sided ideal $\mathfrak{m}$ of R.*

PROOF (a) It suffices to show that $yz=1$ implies $zy=1$. The descending chain condition implies that $Ry^n=Ry^{n+1}$ for some $n\geq 0$, so $y^n=wy^{n+1}$ for some $w\in R$ Then $1=y^nz^n=wy^{n+1}z^n=wy$ and $w=wyz=z$.

(b) Let $\mathfrak{m}_1,\mathfrak{m}_2,\dots,\mathfrak{m}_k$ be distinct maximal two-sided ideals. Then $\mathfrak{m}_i+\mathfrak{m}_j=R$ for $i\neq j$, so the map $R\to\prod_{i=1}^k R/\mathfrak{m}_i$ is surjective with kernel $\bigcap_{i=1}^k\mathfrak{m}_i$. This proves that $\bigcap_{i=1}^k\mathfrak{m}_i$ is properly contained in $\bigcap_{i=1}^{k-1}\mathfrak{m}_i$. The descending chain condition now implies a bound on k.

(c) "Only if" is clear. To prove "if", suppose that $x\notin R^*$. Then $Rx\neq R$ by (a), so $Rx\subset L$ for some maximal left ideal $L\subset R$. Let $\mathfrak{m}=\text{Ann}\,(R/L)\subset R$ be the annihilator of the simple R-module R/L. Then $\mathfrak{m}\subset L$ so $(R/\mathfrak{m})(x \bmod \mathfrak{m})\subset L/\mathfrak{m}\neq R/\mathfrak{m}$ and consequently $(x \bmod \mathfrak{m})\notin(R/\mathfrak{m})^*$. Hence to prove (c) it suffices to show that $\mathfrak{m}$ is maximal as a two-sided ideal. We have $\mathfrak{m}=\bigcap_{y\in R-L}L_y$ where $L_y=\{r\in R\colon ry\in L\}$; considering the map $R\to R/L$ sending 1 to y one finds that $R/L_y\cong R/L$ as R-modules. By the descending chain condition we have $\mathfrak{m}=\bigcap_{y\in T}L_y$ for some *finite* set $T\subset R-L$. Then $R/\mathfrak{m}$ is a submodule of $\prod_{y\in T}R/L_y\cong(R/L)^{\#T}$, so $R/\mathfrak{m}\cong(R/L)^m$ for some $m>0$, by (2.3) Let now $\mathfrak{n}$ be a two-sided ideal of R containing $\mathfrak{m}$. Then $R/\mathfrak{n}\cong(R/L)^n$ for some $n\geq 0$, by (2 3). If $n=0$ then $\mathfrak{n}=R$, and if $n>0$ then $\mathfrak{n}=\text{Ann}\,(R/\mathfrak{n})=\text{Ann}\,(R/L)=\mathfrak{m}$

This proves (2 4).

(2.5) LEMMA *Let $g: R_0\to R_1$ be a surjective ring homomorphism from an Artin ring R_0 to a ring R_1, and let $\mathfrak{a}\subset R_0$ be a two-sided ideal. Then* $g[(1+\mathfrak{a})\cap R_0^*]=(1+g[\mathfrak{a}])\cap R_1^*$

PROOF The inclusion $\subset$ is obvious. To prove $\supset$ we first suppose that $\mathfrak{a}\subset\mathfrak{m}$ for every maximal two-sided ideal $\mathfrak{m}$ of R_0 that does not contain $\ker g$. Let $x=1+g(y)\in(1+g[\mathfrak{a}])\cap R_1^*$, with $y\in\mathfrak{a}$. Using (2 4)(c) we prove that $1+y\in R_0^*$. Let $\mathfrak{m}$ be a maximal two-sided ideal of R_0 If $\ker g\subset\mathfrak{m}$ then the natural map $R_0\to R_0/\mathfrak{m}$ factors via g, so $x=g(1+y)\in R_1^*$ implies that $(1+y \bmod \mathfrak{m})\in(R_0/\mathfrak{m})^*$. If $\ker g\not\subset\mathfrak{m}$ then $y\in\mathfrak{a}\subset\mathfrak{m}$ by hypothesis, so $(1+y \bmod \mathfrak{m})=(1 \bmod \mathfrak{m})\in(R_0/\mathfrak{m})^*$. This proves that $1+y\in R_0^*$, so $x=g(1+y)\in g[(1+\mathfrak{a})\cap R_0^*]$.

Assertions (b) and (a), which form [2, III.7.4, Théorème 1], follow from (c) by putting $J=\{\alpha\}$ and $J=\emptyset$, respectively. This proves (1.5).

2. ARTIN RINGS

Rings are supposed to have unit elements, and ring homomorphisms are supposed to preserve these. The group of units of a ring R is denoted by R^*. A *projective system of rings* is a projective system I, (R_α), $(g_{\alpha\beta})$ in which each R_α carries the structure of a ring and each $g_{\alpha\beta}$ is a ring homomorphism. The projective limit of such a system carries a natural ring structure.

The following proposition is not needed in the sequel, but its proof motivates the approach taken later.

(2.1) PROPOSITION. *Let I, (R_α), $(g_{\alpha\beta})$ be a projective system of rings in which each R_α satisfies the descending chain condition on two-sided ideals and each $g_{\alpha\beta}$ is surjective. Put $R=\varprojlim R_\alpha$. Then the natural map $R\to R_\alpha$ is surjective for every $\alpha\in I$.*

PROOF. We apply (1.5) with $E_\alpha=R_\alpha$, $f_{\alpha\beta}=g_{\alpha\beta}$ and

$$\mathscr{S}_\alpha=\{\emptyset\}\cup\{x+\mathfrak{a}.\ x\in R_\alpha,\ \mathfrak{a}\subset R_\alpha \text{ is a two-sided ideal}\}.$$

It is clear that $E_\alpha\neq\emptyset$ and that (1.1), (1.3) and (1.4) are satisfied. To prove (1.2), we note that the descending chain condition on two-sided ideals of R_α implies the existence of a minimal element among all finite intersections of sets $M\in\mathscr{S}$; this minimal element must then be $\bigcap_{M\in\mathscr{S}}M$.

Since the $g_{\alpha\beta}$ are surjective we have $E'_\alpha=E_\alpha=R_\alpha$ in (1.5), so (2.1) follows from (1.5)(b). This proves (2.1).

An *Artin ring* is a ring that satisfies the descending chain condition on left ideals.

(2.2) PROPOSITION. *Let I, (R_α), $(g_{\alpha\beta})$ be a projective system of rings in which each R_α is an Artin ring and each $g_{\alpha\beta}$ is surjective. Put $R=\varprojlim R_\alpha$. Then the natural map $R^*\to R_\alpha^*$ is surjective for each $\alpha\in I$.*

The properties of Artin rings needed in the proof are listed in Lemma (2.4). This lemma can easily be derived from the structure of semisimple Artin rings and properties of the Jacobson radical. We give a direct proof, starting from the following well-known lemma. By a *module* we mean a left module on which the unit element acts as the identity, and a module is called *simple* if it is nonzero and has no submodules except itself and $\{0\}$.

(2.3) LEMMA. *Let R be a ring, $(M_v)_{v\in V}$ a collection of simple R-modules, $M=\bigoplus_{v\in V}M_v$, and $N\subset M$ a submodule. Then there is a subset $W\subset V$ such that $M/N\cong\bigoplus_{v\in W}M_v$ and $N\cong\bigoplus_{v\in V-W}M_v$.*

In the general case, let $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_k$ be the maximal two-sided ideals of R_0 that do not contain ker g. Then $\mathfrak{m}_i + \ker g = R_0$ for each i, so some $z_i \in \mathfrak{m}_i$ satisfies $z_i \equiv 1 \bmod \ker g$. Then $z = z_1 z_2 \ldots z_k$ satisfies $z \in \mathfrak{m}_1 \mathfrak{m}_2 \ldots \mathfrak{m}_k$ and $g(z) = 1$. Therefore $g[\mathfrak{a}] = g[\mathfrak{b}]$ for $\mathfrak{b} = \mathfrak{a}\mathfrak{m}_1\mathfrak{m}_2 \ldots \mathfrak{m}_k$. Applying the previous case to $\mathfrak{b}$ we see that $(1 + g[\mathfrak{a}]) \cap R_1^* = g[(1+\mathfrak{b}) \cap R_0^*] \subset g[(1+\mathfrak{a}) \cap R_0^*]$.

This proves (2.5).

(2.6) LEMMA. *Let $g: R_0 \to R_1$ be a surjective ring homomorphism from an Artin ring R_0 to a ring R_1. Then the map $R_0^* \to R_1^*$ induced by g is surjective.*

PROOF. Put $\mathfrak{a} = R_0$ in (2.5). This proves (2.6).

PROOF OF (2.2). We apply (1.5) with $E_\alpha = R_\alpha^*$ and $f_{\alpha\beta}: R_\beta^* \to R_\alpha^*$ the map induced by $g_{\alpha\beta}$. For $\mathscr{S}_\alpha$ we take

$$\mathscr{S}_\alpha = \{\emptyset\} \cup \{(x + \mathfrak{a}) \cap R_\alpha^*: \ x \in R_\alpha^*, \ \mathfrak{a} \subset R_\alpha \text{ is a two-sided ideal}\}.$$

It is clear that $E_\alpha \neq \emptyset$. We check conditions (1.1)–(1.4).

(1.1) If $\bigcap_{M \in \mathscr{F}} M \neq \emptyset$ then with $x \in \bigcap_{M \in \mathscr{F}} M$ each $M \in \mathscr{F}$ has the form $(x + \mathfrak{a}_M) \cap R_\alpha^*$ for some two-sided ideal $\mathfrak{a}_M \subset R_\alpha$, and then $\bigcap_{M \in \mathscr{F}} M = (x + \mathfrak{a}) \cap R_\alpha^*$ where $\mathfrak{a} = \bigcap_{M \in \mathscr{F}} \mathfrak{a}_M$.

(1.2) Using (1.1) we may assume that $\mathscr{F}$ is closed under taking finite intersections. For $M \in \mathscr{F}$, let $\mathfrak{b}_M$ be the two-sided ideal of R_α generated by $\{y - z: y, z \in M\}$; then $M = (x + \mathfrak{b}_M) \cap R_\alpha^*$ for each $x \in M$. Choose $M' \in \mathscr{F}$ such that $\mathfrak{b}_{M'}$ is minimal among all ideals $\mathfrak{b}_M$, $M \in \mathscr{F}$. It then follows that $M' = \bigcap_{M \in \mathscr{F}} M$.

(1.3) This is clear.

(1.4) If $M = (x + \mathfrak{a}) \cap R_\beta^* \in \mathscr{S}_\beta$ then by (2.5) we have

$$f_{\alpha\beta}[M] = f_{\alpha\beta}[x((1+\mathfrak{a}) \cap R_\beta^*)] = f_{\alpha\beta}(x) \cdot ((1 + g_{\alpha\beta}[\mathfrak{a}]) \cap R_\alpha^*) =$$
$$= (f_{\alpha\beta}(x) + g_{\alpha\beta}[\mathfrak{a}]) \cap R_\alpha^* \in \mathscr{S}_\alpha.$$

From (2.6) we see that the maps $f_{\alpha\beta}$ are surjective, so $E'_\alpha = R_\alpha^*$ in (1.5). The proposition now follows from (1.5)(b).

This proves (2.2).

(2.7) PROPOSITION. *Let I, (R_α), $(g_{\alpha\beta})$ be a projective system of rings in which each R_α is an Artin ring and each $g_{\alpha\beta}$ is surjective. Let further I, (M_α), $(h_{\alpha\beta})$ be a projective system in which each M_α is a free R_α-module on one generator and each $h_{\alpha\beta}$ is a surjective R_β-module homomorphism; here M_α is considered as an R_β-module via the map $R_\beta \to R_\alpha$. Put $R = \varprojlim R_\alpha$ and $M = \varprojlim M_\alpha$. Then M is a free R-module on one generator, which can be chosen of the form $(x_\alpha)_{\alpha \in I}$, where each x_α generates M_α as an R_α-module.*

PROOF. Without loss of generality we may assume that $M_\alpha = R_\alpha$, for each $\alpha \in I$. By (2.4)(a) we then have $h_{\alpha\beta}(1) \in R_\alpha^*$, and $h_{\alpha\beta}(x) = g_{\alpha\beta}(x) h_{\alpha\beta}(1)$ for all

$x \in R_\beta$. Let $f_{\alpha\beta}: R_\beta^* \to R_\alpha^*$ be the map induced by $h_{\alpha\beta}$; then the statement of (2.7) is equivalent to the assertion that $\varprojlim R_\alpha^* \neq \emptyset$, the projective limit being taken with respect to the maps $f_{\alpha\beta}$.

To prove that $\varprojlim R_\alpha^* \neq \emptyset$ we apply (1.5) with the same E_α and $\mathscr{S}_\alpha$ as in the proof of (2.2); but $f_{\alpha\beta}$ differs from the map $f_{\alpha\beta}$ used for (2.2) by a unit factor $h_{\alpha\beta}(1)$ on the right. Since $\mathscr{S}_\alpha$ is transformed into itself by multiplication by units conditions (1.1)–(1.4) are still satisfied. The proposition now follows from (1.5)(a).

This proves (2.7).

3. GALOIS EXTENSIONS

In this section we use the notation from the Introduction.

PROOF OF THEOREM 2. We apply (2.7) to the projective system U, $(K[G/N])$, $(\varrho_{N'/N})$ of rings and the projective system U, (L^N), $(\mathrm{Tr}_{N'/N})$ of modules. Each $K[G/N]$ is finite dimensional over K and therefore an Artin ring. Each L^N is free over $K[G/N]$ on one generator, by the normal basis theorem. The remaining conditions are easy to check. Theorem 2 now follows from (2.7).

PROOF OF THEOREM 1. From (2.7) we obtain an element $(x_N)_{N \in U} \in \prod_{N \in U} L^N$ such that

(3.1) $\quad (\sigma(x_N))_{\sigma \in G/N}$ is a basis of L^N over K, for each $N \in U$,

(3.2) $\quad \mathrm{Tr}_{N'/N}(x_N) = x_{N'}$ for $N, N' \in U$, $N \subset N'$.

To define $\varphi: C(G,K) \to L$, let $f \in C(G,K)$. Since K is discrete, there is for every $\sigma \in G$ an $N \in U$ such that f is constant on σN. By compactness of G, we can choose the same N for all σ. Let $f_N: G/N \to K$ be the map induced by f. We now put

$$\varphi(f) = \sum_{\sigma \in G/N} f_N(\sigma)\sigma(x_N).$$

From (3.2) it easily follows that the expression on the right does not depend on the choice of N, so φ is well-defined. It is also K-linear, and it respects the action of G. Finally, (3.1) implies that it is bijective.

This proves Theorem 1.

Let L be finite over K, and let M be an intermediate field that is also Galois over K. Applying the trace from L to M one obtains, from every normal basis of L over K, a normal basis of M over K. In addition, every normal basis of M over K can be obtained in this way, since the natural map $K[G]^* \to K[G/N]^*$ is surjective (Lemma (2.6)); here $M = L^N$.

The extension of these results to the general case is as follows. Let L again be arbitrary, and let M be an intermediate field that is also Galois over K. Then $M = L^N$ for a unique closed normal subgroup N of G. From any isomorphism

$C(G,K)\to L$ as in Theorem 1 one obtains, upon taking invariants under N, an isomorphism $C(G/N,K)\to M$ such that the diagram

$$\begin{tikzcd} C(G/N,K) \arrow[r] \arrow[d] & M \arrow[d] \\ C(G,K) \arrow[r] & L \end{tikzcd}$$

is commutative; here the first vertical arrow is induced by the canonical map $G\to G/N$, and $M\to L$ is the inclusion. Conversely, given an isomorphism $C(G/N,K)\to M$ of K-vector spaces that respects the action of G/N one can find an isomorphism $C(G,K)\to L$ as in Theorem 1 such that the above diagram commutes This is a consequence of (1.5)(c), with $I=U$ and J equal to the set of open normal subgroups of G that contain N.

REFERENCES

1 Bourbaki, N – Algebre, Chapitres 4 et 5, Hermann, Paris, 1959

2 Bourbaki, N – Theorie des ensembles, Hermann, Paris, 1970

3 Deuring, M – Galoissche Theorie und Darstellungstheorie, Math Ann **107**, 140–144 (1933)

4 Krull, W – Galoissche Theorie der unendlichen algebraischen Erweiterungen, Math Ann **100**, 687–698 (1928)

5 Noether, E – Normalbasis bei Korpern ohne hohere Verzweigung, J reine angew Math **167**, 147–152 (1932)

6 Waterhouse, W C – An empty inverse limit, Proc Amer Math Soc **36**, 618 (1972)

Journal of Pure and Applied Algebra 36 (1985) 281-298
North Holland

ABELIAN VARIETIES HAVING PURELY ADDITIVE REDUCTION

H.W LENSTRA, Jr.

Mathematisch Instituut, Roetersstraat 15, 1018 WB Amsterdam, The Netherlands

F. OORT

Mathematisch Instituut, Budapestlaan 6, 3584 CD Utrecht, The Netherlands

Communicated by F Oort
Received 30 November 1983
Revised 11 April 1984

Let E be an elliptic curve over a field K with a discrete valuation v with residue class field k. Suppose E has 'additive reduction' at v, i.e. the connected component A_0^0 of the special fibre A_0 of the Néron minimal model is isomorphic to $\mathbb{G}_a$. Then the order of $A_0(k)/A_0^0(k)$ is at most 4 as can be seen by inspection of the usual tables, cf. [9, pp. 124–125] and [5, p. 46]. Thus it follows that if the order of the torsion subgroup Tors($E(K)$) is at least 5 and prime to $p = \text{char}(k)$, the reduction cannot be additive. This note arose from an attempt to see whether an explicit classification really is necessary to achieve this result This attempt turned out to be successful: we prove a generalization for abelian varieties (cf. 1.15). The proof does not use any specific classification, but it relies on monodromy arguments. It explains the special role of prime numbers l with $l \leq 2g+1$ in relation with abelian varieties of dimension g. Note that Serre and Tate already pointed out the importance of such primes, cf. [14, p. 498, Remark 2]. In their case, and in the situation considered in this paper the representation of the Galois group on T_lA has dimension $2g$, hence primes l with $l \leq 2g+1$ play a special role

We give the theorem and its proof in Section 1. Further we show that the bound in the theorem in sharp (Section 2), and we give examples in Section 3 which show that the restriction $l \neq \text{char}(k)$ in the theorem is necessary. In Section 4 we indicate what can happen under the reduction map $E(K) \to E_0(k)$ with points of order p in case of additive reduction.

K. Ribet made several valuable suggestions on an earlier draft of this paper The elegant methods of proof in Section 2 were suggested by him. We thank him heartily for his interest in our work and for his stimulating remarks

1. Torsion points on an abelian variety having purely additive reduction

Let K be a field and v a discrete valuation of K. We denote the residue class field of v by k; we assume k is perfect. Let K_s be a separable closure of K and $\bar{v}$ an extension of v to K_s. We denote the inertia group and first ramification group of $\bar{v}$ by I and J, respectively. These are closed subgroups of the Galois group $\mathrm{Gal}(K_s/K)$. If the residue characteristic $\mathrm{char}(k)=p$ is positive, then J is a pro-p-group; if $\mathrm{char}(k)=0$, then J is trivial. The group J is normal in I, and the group I/J is pro-cyclic:

$$I/J \cong \prod_{l \text{ prime}, l\neq \mathrm{char}(k)} \mathbb{Z}_l.$$

Let A be an abelian variety of dimension g over K, and $\mathscr{A}$ the Néron minimal model of A at v, cf. [9]. We write A_0 for the special fibre: $A_0=\mathscr{A}\otimes_R k$, where R is the valuation ring of v. We denote by A_0^0 the connected component of A_0. Let

$$0\to L_s\oplus L_u\to A_0^0\to B\to 0$$

be the 'Chevalley decomposition' of the k-group variety A_0^0, i.e., B is an abelian variety, L_s is a torus, and L_u is a unipotent linear group. We write

$$\alpha=\dim B, \qquad \mu=\dim L_s.$$

We say that A has *purely additive reduction* at v if $L_u=A_0^0$, so if $\alpha=\mu=0$ (and we say *additive reduction* if $\dim A=1=\dim L_u$).

Throughout this paper, l will stand for a prime number different from $\mathrm{char}(k)$. If G is a commutative group scheme over K, and $n\in\mathbb{Z}$, we write $G[n]$ for the group scheme $\mathrm{Ker}(n\cdot 1_G: G\to G)$, and

$$T_lG=\varprojlim G[l^r](K_s).$$

This is a module over the ring $\mathbb{Z}_l$ of l-adic integers, and it has a continuous action of $\mathrm{Gal}(K_s/K)$. For $G=\mathbb{G}_m$, the multiplicative group, T_lG is free of rank 1 over $\mathbb{Z}_l$, and the subgroup $I\subset\mathrm{Gal}(K_s/K)$ acts trivially on $T_l\mathbb{G}_m$. We write

$$U_l=T_lA.$$

This is a free module of rank $2g$ over $\mathbb{Z}_l$.

Let M be a finitely generated $\mathbb{Z}_l$-module. By the *eigenvalues* of an endomorphism of M we mean the eigenvalues of the induced endomorphism of the vector space $M\otimes_{\mathbb{Z}_l}\mathbb{Q}_l$ over the field $\mathbb{Q}_l$ of l-adic numbers. Suppose now that M has a continuous action of I. If $I'\subset I$ is a subgroup, we write

$$M^{I'}=\{x\in M: \tau x=x \text{ for all } \tau\in I'\}.$$

We claim that the image J_0 of J in $\mathrm{Aut}(M)$ is *finite*. If $\mathrm{char}(k)=0$ this is trivial, so suppose that $\mathrm{char}(k)=p>0$. Then J_0 is a pro-p-group, and the kernel of the natural map $\mathrm{Aut}(M)\to\mathrm{Aut}(M/lM)$ is a pro-l-group. From $p\neq l$ it follows that J_0

has trivial intersection with this kernel, so J_0 is isomorphic to a subgroup of $\mathrm{Aut}(M/lM)$ and therefore finite. This proves our claim.

We define, in the above situation, the *averaging map* $N_J: M \to M^J$ by

$$N_J(x) = (\# J_0)^{-1} \sum_{\sigma \in J} \sigma x.$$

This map is the identity on M^J, so gives rise to a splitting

$$M = M^J \oplus \ker N_J. \tag{1.1}$$

It follows that the functor $(\ )^J$ is exact:

$$(M_1/M_2)^J = M_1^J/M_2^J. \tag{1.2}$$

Notice that M^J has a continuous action of the pro-cyclic group I/J. This is in particular the case for

$$X_l = U_l^J.$$

We denote by σ a topological generator of I/J.

1.3. Proposition. *The multiplicity of* 1 *as an eigenvalue of the action of* σ *on* $X_l = U_l^J$ *is equal to* $2\mu + 2\alpha$. *In particular, it does not depend on the choice of the prime number* $l \neq \mathrm{char}(k)$.

Proof. We begin by recalling the results from [*SGA*, 7.I, exp. IX] that we need, see also [11]. Let a polarization of A over k be fixed. Then we obtain a skew-symmetric pairing

$$\langle\ ,\ \rangle: U_l \times U_l \to T_l \mathbb{G}_{\mathrm{m}} \cong \mathbb{Z}_l,$$

which is *separating* in the sense that the induced map $U_l \to \mathrm{Hom}_{\mathbb{Z}_l}(U_l, T_l\mathbb{G}_{\mathrm{m}})$ becomes an isomorphism when tensored with $\mathbb{Q}_l$. The pairing is Galois-invariant in the sense that

$$\begin{aligned} \langle \tau u, \tau v \rangle &= \tau \langle u, v \rangle \quad \text{for } \tau \in \mathrm{Gal}(K_s/K),\ u, v \in U_l, \\ &= \langle u, v \rangle \quad \text{if } \tau \in I. \end{aligned}$$

We write

$$V = U_l^I, \qquad W = V \cap V^{\perp},$$

where $\perp$ denotes the orthogonal complement in U_l with respect to $\langle\ ,\ \rangle$. We have

$$\mathrm{rank}_{\mathbb{Z}_l} W = \mu, \qquad \mathrm{rank}_{\mathbb{Z}_l} V/W = 2\alpha. \tag{1.4}$$

Since A has potentially stable reduction, there is an open normal subgroup $I' \subset I$ such that the module $V' = U_l^{I'}$ satisfies

$$V'^{\perp} \subset V'. \tag{1.5}$$

Notice that $V \subset V'$.

We now take J-invariants. The Galois-invariance of $\langle\cdot,\cdot\rangle$ implies that $X_l = U_l^J$ is orthogonal to the complement of U_l^J in U_l defined in (1.1). Therefore $\langle\cdot,\cdot\rangle$ gives rise to a separating Galois-invariant pairing

$$X_l \times X_l \to T_l\mathbb{G}_{\mathrm{m}}$$

which will again be denoted by $\langle\cdot,\cdot\rangle$. We let § denote the orthogonal complement in X_l with respect to $\langle\cdot,\cdot\rangle$.

There is a diagram of inclusions

$$\begin{tikzcd}
& & V \arrow[dr, hook] & & \\
0 \arrow[r, hook, "\mu"] & W \arrow[ur, hook, "2\alpha"] \arrow[dr, hook] & & W^{\S} \arrow[r, hook, "\mu"] & X_l \\
& & V^{\S} \arrow[ur, hook, "2\alpha"'] & &
\end{tikzcd}$$

where μ and 2α indicate the $\mathbb{Z}_l$-ranks of the quotients of two successive modules in the diagram; here we use (1.4) and the equalities

$$\mathrm{rank}_{\mathbb{Z}_l}(X_l/W^{\S}) = \mathrm{rank}_{\mathbb{Z}_l}(W), \qquad \mathrm{rank}_{\mathbb{Z}_l}(W^{\S}/V^{\S}) = \mathrm{rank}_{\mathbb{Z}_l}(V/W),$$

which follow by duality.

All eigenvalues of σ on V are 1, and by duality the same is true for $X_l/V^{\S}$, hence for $X_l/W^{\S}$. We have

$$\mathrm{rank}_{\mathbb{Z}_l} V + \mathrm{rank}_{\mathbb{Z}_l} X_l/W^{\S} = 2\mu + 2\alpha,$$

so in order to prove the proposition it suffices to show that

$$\text{no eigenvalue of } \sigma \text{ on } W^{\S}/V \text{ equals } 1. \tag{1.6}$$

Let $Y = V'^J$. We first prove that

$$\text{no eigenvalue of } \sigma \text{ on } Y/V \text{ equals } 1. \tag{1.7}$$

Suppose in fact, that $y \in Y$ satisfies $\sigma y = y + v$ for some $v \in V$. Then $\sigma^n y = y + nv$ for all positive integers n. Choosing n such that $\sigma^n \in I'$ we also have $\sigma^n y = y$, since $y \in V'$, so we find that $v = 0$ and $y \in V$. This proves (1.7).

We have $Y^{\S} \subset Y$, by (1.5), so (1.7) implies that

$$\text{no eigenvalue of } \sigma \text{ on } (Y^{\S} + V)/V \text{ equals } 1. \tag{1.8}$$

By duality, (1.7) implies that no eigenvalue of σ on $V^{\S}/Y^{\S}$ equals 1, and therefore

$$\text{no eigenvalue of } \sigma \text{ on } (V^{\S} + V)/(Y^{\S} + V) \text{ equals } 1. \tag{1.9}$$

From $W = V \cap V^{\S}$ it follows that $V^{\S} + V$ is of finite index in $W^{\S}$, so (1.8) and (1.9) imply the desired conclusion (1.6). This proves Proposition 1.3. □

1.10. Corollary. *The abelian variety A has purely additive reduction at v if and only if σ has no eigenvalue equal to* 1 *on X.*

Proof. Clear from Proposition 1.3. It is easy to prove the corollary directly, using that $\mathrm{rank}_{\mathbb{Z}_l} V = \mu + 2\alpha$. □

Let $I' \subset I$ and $Y = (U_l^{I'})^J \subset X_l$ be as in the proof of Proposition 1.3, and n a positive integer for which $\sigma^n \in I'$. Then σ^n acts as the identity on Y, and by duality also on $X_l/Y^{\S}$. By $Y^{\S} \subset Y$ this implies that all eigenvalues of σ^n on X_l are 1. Thus we find that all eigenvalues of σ on X_l are *roots of unity.* These roots of unity are of order not divisible by $\mathrm{char}(k) = p$, since the pro-p-part of the group I/J is trivial. Let $a_l(m)$ denote the number of eigenvalues of σ on X_l that are m-th roots of unity, counted with multiplicities.

1.11. Proposition. *For any two prime numbers l, l' different from* $\mathrm{char}(k)$ *and any positive integer m we have $a_l(m) = a_{l'}(m)$.*

Proof. We may assume that m is not divisible by $\mathrm{char}(k)$. Let L be a totally and tamely ramified extension of K of degree m. Replacing K by L has no effect on J, but σ should be replaced by σ^m. Since $a_l(m)$ is the multiplicity of 1 as an eigenvalue of σ^m on X_l, the proposition now follows by applying Proposition 1.3 with base field L. □

1.12. Corollary. *The number* $\mathrm{rank}_{\mathbb{Z}_l} X_l$ *does not depend on l.*

Proof. This follows from Proposition 1.11, since

$$\mathrm{rank}_{\mathbb{Z}_l} X_l = \sup_m a_l(m). \qquad \square$$

Remark. Proposition 1.11 and Corollary 1.12 can also easily be deduced from the fact that, for each $\tau \in I$, the coefficients of the characteristic polynomial of the action of τ on U_l are rational integers independent of l, see [*SGA*, 7 I, exp. IX, Théorème 4.3].

1.13. Theorem. *Suppose that A has purely additive reduction at v. Then for every prime number $l \neq$* $\mathrm{char}(k)$ *the number $b(l) \in \{0, 1, 2, \dots, \infty\}$ defined by*

$$\sup_{N \geq 0} \# A[l^N](K) = l^{b(l)}$$

is finite, *and*

$$\sum_{l \text{ prime},\, l \neq \mathrm{char}(k)} (l-1) b(l) \leq 2g.$$

Proof. First let l be a fixed prime, $l \neq \mathrm{char}(k)$, and let N be a positive integer. We have

$$\begin{aligned}\# A[l^N](K) &\leq \# A[l^N](K_s)^I \\ &= \#(\text{kernel of } \sigma - 1 \text{ on } A[l^N](K_s)^I) \\ &= \#(\text{cokernel of } \sigma - 1 \text{ on } A[l^N](K_s)^I),\end{aligned}$$

the last equality because $A[l^N](K_s)$ is finite. By (1.2) the natural map

$$X_l = U_l^I \to (U_l / l^N U_l)^I = A[l^N](K_s)^I$$

is *surjective*, so the above number is

$$\leq \#(\text{cokernel of } \sigma - 1 \text{ on } X_l).$$

Let us write $|\ |_l$ for the normalized absolute value on an algebraic closure $\bar{\mathbb{Q}}_l$ of $\mathbb{Q}_l$ for which $|l|_l = l^{-1}$. Then by a well-known and easily proved formula we have

$$\begin{aligned}\#(\text{cokernel of } \sigma - 1 \text{ on } X_l) &= |\det(\sigma - 1 \text{ on } X_l)|_l^{-1} \\ &= \prod |\zeta - 1|_l^{-1},\end{aligned}$$

where ζ ranges over the eigenvalues of σ on X_l.

Letting N tend to infinity we see that we have proved

$$l^{b(l)} \leq \prod |\zeta - 1|_l^{-1}. \tag{1.14}$$

By Corollary 1.10 the right hand side of (1.14) is finite. This proves the claim that $b(l)$ is finite.

Next we exploit the fact that the eigenvalues ζ of σ are roots of unity. It is well known that for a root of unity $\zeta \neq 1$ we have

$$\begin{aligned}|\zeta - 1|_l &\geq l^{-1/(l-1)} && \text{if } \zeta \text{ has } l \text{ power order,} \\ |\zeta - 1|_l &= 1 && \text{otherwise.}\end{aligned}$$

Write $a_l(l^\infty) = \max_N a_l(l^N)$. Then (1.14) implies that

$$b(l) \leq a_l(l^\infty)/(l-1),$$

so there is a number $d(l)$ such that

$$(l-1)b(l) \leq a_l(l^{d(l)}).$$

Now let q be an arbitrary prime number different from char(k). Using Proposition 1.11 we deduce

$$\begin{aligned}\sum_{l \text{ prime},\, l \neq \mathrm{char}(k)} (l-1)b(l) &\leq \sum_l a_l(l^{d(l)}) \\ &= \sum_l a_q(l^{d(l)}) \\ &\leq \mathrm{rank}_{\mathbb{Z}_l}(X_q) \qquad (\text{since } a_q(1) = 0) \\ &\leq \mathrm{rank}_{\mathbb{Z}_l}(U_q) = 2g.\end{aligned}$$

This completes the proof of Theorem 1.13. □

1.15. Corollary. *Suppose that A has purely additive reduction at v. Denote by m the number of geometric components of the special fibre A_0 of the Néron minimal model of A at v. Then*

$$\sum_{l \text{ prime}, l \neq \mathrm{char}(k)} (l-1)\,\mathrm{ord}_l(m) \leq 2g$$

where $\mathrm{ord}_l(m)$ denotes the number of factors l in m.

Proof. Analogous to the proof of [11, 2.6]. □

We shall see in Section 3 that the restriction $l \neq \mathrm{char}(k)$ is essential in Theorem 1.13. We do not know whether this is also the case for Corollary 1.15.

1.16. Remark. In [17] we find a weaker version of the result mentioned in Corollary 1.15.

2. An example which shows the bound in Theorem 1.13 to be sharp

2.1. Example. Let l be an *odd* prime number, and $g=(l-1)/2$. We construct an abelian variety A of dimension g over a field K with a point of order l rational over K such that A has purely additive reduction at a given place of K.

Let $\zeta=\zeta_l$ be a primitive l-th root of unity (in $\mathbb{C}$), and $F:=\mathbb{Q}(\zeta)$. We write $D=\mathbb{Z}[\zeta]$ for the ring of integers of F. The field $F_0:=\mathbb{Q}(\zeta+\bar{\zeta})$ is totally real of degree g over $\mathbb{Q}$ and F is a totally imaginary quadratic extension of F_0, i.e. F is a CM field. We choose

$$\phi_j : F \to \mathbb{C}, \qquad \phi_j(\zeta)=e^{j2\pi i/l}, \quad 1 \leq j \leq g;$$

in this way, cf. [15, 6.2 and 8.4(1)], we obtain an abelian variety

$$B=\mathbb{C}^g/\Gamma, \qquad \Gamma=(\phi_1,\dots,\phi_g)(D),$$

with $\mathrm{End}(B)=D$, with a polarization $\lambda : B \to B^t$ (defined by a Riemann form, cf. [15, p. 48]):

$$\mathrm{Aut}(B,\lambda)=\langle\zeta\rangle \times \{\pm 1\} \cong \mathbb{Z}/2l;$$

in fact by a theorem of Matsusaka, cf. [3, VII.2, Proposition 8], we know that $\mathrm{Aut}(B,\lambda)$ is a finite group, hence only the torsion elements of the group of units of $\mathbb{Z}[\zeta]$ can be automorphisms of (B,λ), moreover complex multiplication by ζ leaves the Riemann form invariant (use [15, p. 48, line 8]), and the result follows. Let $P \in B$ be the point

$$P=\left\{\phi_j\left(\frac{1}{1-\zeta}\right) : 1 \leq j \leq g\right\} \bmod \Gamma \in \mathbb{C}^g/\Gamma;$$

note that $1-\zeta$ divides $l\in\mathbb{Z}[\zeta]$, hence P is an l-torsion point; moreover

$$\zeta\frac{1}{1-\zeta}=-1+\frac{1}{1-\zeta},$$

hence complex multiplication by ζ leaves P invariant; thus

$$\mathrm{Aut}(B,\lambda,P)=\langle\zeta\rangle\cong\mathbb{Z}/l.$$

By [15, p. 109, Proposition 26], we can choose a number field K such that B is defined over K, such that $P\in B(K)$, and such that $\mathrm{Aut}_K(B,P)\cong\mathbb{Z}/l$. We choose a prime number p such that

$$p\equiv 1 \pmod{l}, \quad\text{and}\quad p\nmid \mathrm{discriminant}(K/\mathbb{Q})$$

(by Dirichlet's theorem there exist infinitely many prime numbers satisfying the first condition). Let v be a place of K dividing p. If B has bad reduction at v we choose $A=B$; if B has good reduction at v we proceed as follows. We have

$$\mathrm{Gal}(K(\zeta_p)/K)\cong(\mathbb{Z}/p)^*,$$

thus there exists a (unique) field L with

$$K\subset L\subset K(\zeta_p), \quad\text{and}\quad \mathrm{Gal}(L/K)\cong\mathbb{Z}/l.$$

We choose an isomorphism

$$\alpha:\mathrm{Gal}(L/K)\xrightarrow{\sim}\mathrm{Aut}_K(B,P)=H\cong\mathbb{Z}/l.$$

By [12, p. 121] we know

$$H^1(G=\mathrm{Gal}(L/K),H=\mathrm{Aut}_K(B,P))=\mathrm{Hom}(G,H),$$

thus by [13, p. III-6, Proposition 5] this element α corresponds to a pair (A,Q) defined over K such that

$$(A,Q)\otimes_K L\cong(B,P)\otimes_K L.$$

We note that A has bad reduction at v: the extension $L\supset K$ is totally ramified at v, we assumed that B has good reduction at v, hence the inertia group I at v operates trivially on T_pB, and by twisting with (the non-trivial) α we see that I operates non-trivially on T_pA. Note that $A\otimes_K L$ has CM, thus A has potentially good reduction at all places of K. From these facts we deduce that A (in both cases considered) has purely additive reduction at v as follows; let A_0^0 be the connected component of the special fibre of the Néron minimal model of A at v; then

$$0\to L_s\oplus L_u\to A_0^0\to C\to 0$$

is exact. It is easily seen that $L_s\neq 0$ leads to a contradiction with the fact that A has potentially good reduction. Because A has bad reduction at v we know $L_u\neq 0$. The special fibre C' of the Néron minimal model at a place of L over v of $A\otimes_K L$ has $\mathbb{Z}[\zeta]\subset\mathrm{End}(C')$, thus C' is indecomposable, hence $L_u\neq 0$ implies $C=0$; thus $L_u=A_0^0$, i.e. A has purely additive reduction at v.

2.2. Remark. One can also construct an example with residue-characteristic zero. Consider (B, P) as constructed above (say over $k=\mathbb{C}$), choose a deformation of this over $k[[T]]$ on which $H=\mathbb{Z}/l$ acts; then we obtain an abelian variety A defined over $K=k((T))^H$, and $P\in A(K)$ of order l; it is not difficult to see it has bad reduction (at $T^l \mapsto 0$). We leave the details to the reader.

2.3. Remark. We make (2.1) more explicit. Let l be an odd prime, $l=2g+1$, let p be an odd prime, $p\neq l$, let $K=\mathbb{Q}(\zeta_l)$ and suppose a curve C is given by the two affine curves defined by the equations

$$Y^2=X^l+p^2, \qquad \eta^2=\xi+p^2\xi^{l+1},$$

which are identified along the open sets $(x\neq 0)$ and $(\xi\neq 0)$ by

$$X=1/\xi, \qquad Y=\eta/\xi^{g+1}.$$

Thus we have a complete (hyperelliptic) algebraic curve of genus g and

$$X\mapsto \zeta X, \qquad Y\mapsto Y, \qquad \zeta=\zeta_l$$

$$\xi\mapsto \xi/\zeta, \qquad \eta\mapsto\zeta^g\eta$$

is an automorphism ϕ of order l. The points

$$\alpha=(x=0, y=p), \qquad \beta=(\xi=0, \eta=0)$$

define

$$P:=\mathrm{Cl}(\alpha-\beta)\in A:=\mathrm{Jac}(C).$$

We see that α and β are invariant under ϕ, thus $P\in\mathrm{Jac}(C)$ is invariant under $\phi^*\in\mathrm{Aut}(A)$. Note that $Y-p$ defines a rational function on C; this function has $l\cdot\alpha$ as set of zeros, its poles are not on the first affine curve, hence $l\cdot\beta$ is the set of poles; thus $l\alpha-l\beta\sim 0$, i.e. $l\cdot P=0$. The points of order 2 on A are generated by the points $\mathrm{Cl}(\gamma-\beta)$, where $\gamma=(x,0)$ and $x^l+p^2=0$; thus we see that

$$\mathrm{Gal}(K(\sqrt[l]{-p^2})/K)$$

operates non-trivially on points of order 2 on A, and because this extension is ramified above each place v dividing p, and because $p\neq 2$, we conclude that A does not have good reduction at v. Moreover

$$\mathbb{Z}[\zeta]\subset\mathrm{End}_K(A)$$

and we conclude as before. The last step can also be made explicit; choose a zero x of $X^l+p^2=0$; then $\gamma\in\{\zeta^i x \mid i=1,\dots,l\}$, write $Q_i=\mathrm{Cl}((\zeta^i x, 0)-\beta)$, and denote by ζ the generator

$$\langle\zeta\rangle=\mathrm{Gal}(K(\sqrt[l]{-p^2})/K), \qquad \zeta\cdot(\zeta^i x)=\zeta^{i+1}x;$$

$A[2](\bar{K})\cong(\mathbb{Z}/2)^{2g}$ is generated by $Q_1, \quad , Q_l$ and the only relation is $Q_1 + \quad + Q_l = 0$ Thus the action of ζ on $A[2](\bar{K})$ is given by

$$Q_i \mapsto Q_{i+1}, \quad 1 \le i \le 2g-1 = l-2$$

$$Q_{l-1} \mapsto Q_l = -(Q_1 + \quad + Q_{2g}),$$

the matrix

$$\begin{pmatrix} 0 & 0 & & 0 & -1 \\ 1 & 0 & & 0 & -1 \\ 0 & 1 & & 0 & -1 \\ & & & & \\ 0 & 0 & & 1 & -1 \end{pmatrix}$$

has no eigenvalues equal to $+1$ and by Corollary 1 10 (applied with the prime 2) we conclude that A has purely additive reduction

3. Points of order p on elliptic curves having additive reduction

Let K, v, and k be as in Section 1, and suppose $\mathrm{char}(k)=p>0$ Let A be an abelian variety over K having additive reduction at v, we have seen in Theorem 1 13 that the prime-to-p torsion in $A(K)$ is very limited in this case What about the p power torsion in this case? With the help of some examples we show this torsion can be arbitrarily large

First we give equal-characteristic examples

3.1. Example. Let $p\equiv 5 \pmod 6$ and suppose given an integer $i\ge 1$ We construct *K, v, k, E such that char(K)$=p=$char(k), E has additive reduction at v and*

$$p^i \text{ divides } \#(E[p^i](K))$$

Consider $k=\mathbb{F}_p$ and $L=k(t)$, define an elliptic curve C over L by the equation

$$Y^2 = X^3 + aX + a, \qquad a = \frac{27}{4}\,\frac{t}{1728-t},$$

note that

$$j(C) = 1728\,\frac{4a^3}{4a^3+27a^2} = t,$$

and that its discriminant equals

$$\Delta = -16(4a^3+27a^2) = \alpha t^2,$$

here w is the valuation on L with $w(t)=1$, with valuation ring $R=k[t]_{(t)}$ and $\alpha\in R^*$ (note that 2 and 3 are invertible in k), thus C has potentially good reduction at w

(its j-invariant being integral), and it has bad reduction at w, because its discriminant satisfies

$$0 < w(\Delta) = 2 < 12;$$

note further that for any extension $K \supset L$ of degree not divisible by 6 and for any extension v of w to K the reduction at v is additive (note that C is of type $\mathrm{II} = C_1$ at w, cf. [5, p. 46]). Let ϕ be the i-th iterate of the Frobenius homomorphism, and let M be its kernel:

$$0 \to M \to C \xrightarrow{\phi} E := C^{(p^i)} \to 0,$$

thus E is given by the equation

$$Y^2 = X^3 + a^q X + a^q, \qquad q = p^i,$$

and M is a local group scheme of rank q. Note that C is not a super-singular elliptic curve (because its j-invariant is not algebraic over k), thus

$$M \otimes_L L_s \cong \mu_q.$$

By duality we obtain

$$M^D = N \subset E, \quad N \otimes_L L_s \cong \mathbb{Z}/q.$$

We take for $K \supset L$ the smallest field of rationality for the points in N, and we extend w to a discrete valuation v on K. Note that $K \supset L$ is a Galois extension and the degree

$$[K:L] \text{ divides } \#(\mathrm{Aut}(\mathbb{Z}/q)) = (p-1)p^{i-1};$$

thus 3 does not divide $[K:L]$, we conclude $E \otimes_L K$ has additive reduction at v; moreover

$$\mathbb{Z}/p^i \subset E(K)$$

by construction, and the Example 3.1 is established.

3.2. Example. Take $p = 2$, the other data as in Example 3.1, and we construct E so that

$$2^i \text{ divides } \#(E[2^i](K)).$$

Define C over $L = k(t)$, $k = \mathbb{F}_2$, by the equation

$$Y^2 + tXY = X^3 + t^5;$$

well-known formulas (cf. [5, p. 36]) yield:

$$\Delta = t^{11}, \qquad j = t;$$

note that 3 does not divide

$$\#(\mathrm{Aut}(\mathbb{Z}/2^i)) = 2^{i-1}, \quad i \geq 1,$$

and the methods of the previous example carry over.

Now we construct some examples in which $\mathrm{char}(K) = 0 < p = \mathrm{char}(k)$.

3.3. Example. Take $p = 2$, let $i \geq 1$ be an integer. We construct K, v, k, E as before, such that E has additive reduction at v, and such that $\mathrm{char}(K) = 0$, $\mathrm{char}(k) = 2$, and

$$E[2^i] \subset E(K).$$

Let $m \geq 1$ be an integer, define

$$L = \mathbb{Q}(\pi), \qquad \pi^{m+1} = 2, \qquad w(\pi) = 1,$$

choose $a \in L$, and let E be given over L by the equation

$$Y^2 + \pi^m XY = X^3 + \pi^2 a X^2 + aX;$$

the point

$$P = (-1/\pi^2, 1/\pi^3) \in E(L)$$

is a point of order 2, because it is on the line $2Y + \pi^m X = 0$, and the same holds for $(0, 0) \in E(L)$; thus $E[2] \subset E(L)$.

Suppose $w(a) \geq 1$; because

$$\Delta = (\pi^{2m} + 4\pi^2 a)^2 a^2 - 64a^3$$

we conclude $w(\Delta) = 4m + 2w(a)$; suppose

$$m = 1 \quad \text{and} \quad w(a) = 2, \quad \text{thus} \quad w(\Delta) = 8 \quad \text{and} \quad w(j) = 0,$$

or

$$m = 2 \quad \text{and} \quad w(a) = 1, \quad \text{thus} \quad w(\Delta) = 10 \quad \text{and} \quad w(j) > 0;$$

then the equation is minimal, the curve E has additive reduction at w and the reduction is potentially good. Let $K \supset L$ be the smallest field of rationality for the points of $E[2^i]$; note that

$$\mathrm{Gal}(K/L) \subset \mathrm{Aut}((\mathbb{Z}/2^i)^2) = \mathrm{GL}(2, \mathbb{Z}/2^i)$$

is in the kernel of

$$\mathrm{GL}(2, \mathbb{Z}/2^i) \rightarrow \mathrm{GL}(2, \mathbb{Z}/2)$$

(because $E[2] \subset E(K)$ by construction), thus the degree $[K : L]$ is a power of 2, hence it is not divisible by 3. This implies that $v(\Delta)$ is not divisible by 12 (where v is some extension of w to K), thus the reduction of $E \otimes_L K$ at v is additive (because of $w(j) \geq 0$ it cannot become $\mathbb{G}_{\mathrm{m}}$-type). Hence over K we have

$$E[2^i] \subset E(K), \quad \text{and} \quad E \text{ has additive reduction at } v.$$

3.4. Example. Let $p \equiv 5 \pmod 6$, and let $i \geq 1$ be an integer. We construct K, v, k, E as above with $\mathrm{char}(K) = 0 < \mathrm{char}(k) = p$, with E having additive reduction at v, and

$$E[p^i] \subset E(K).$$

Consider over $\mathbb{Q}$ the modular curve $X_0(p)_{\mathbb{Q}}$; this is a coarse moduli scheme of pairs $N \subset E$ where E is an elliptic curve and N a subgroup scheme over a field K such that $N(K_s) \cong \mathbb{Z}/p$; consider the scheme $M_0(p)$ over $\mathrm{Spec}(\mathbb{Z})$ (cf. [4, p. DeRa-94, Théorème 1.6] and [6, p. 63]), and consider the point $x_0 \in M_0(p)(\mathbb{F}_p)$ given by $j = 0$. Note that $p \equiv 2 \pmod 3$ implies that the curve E_0 with $j = 0$ is supersingular in characteristic p, hence it has a unique subgroup scheme $\alpha_p \cong N_0 \subset E_0$, the kernel of Frobenius on E_0. Let $\mathcal{O}$ be the local ring of $M_0(p) \otimes_{\mathbb{Z}} W$ at x_0, where $W = W_\infty(\mathbb{F}_{p^2})$ (i.e. W is the unique unramified quadratic extension of $\mathbb{Z}_p$). We know: the local deformation space of $\alpha_p = N_0 \subset E_0$ is isomorphic to the formal spectrum of

$$\mathbb{Z}_p[[X, Y]]/(XY - p),$$

the automorphism group $\mathrm{Aut}(E \otimes \mathbb{F}_{p^2}) = A'$ acts via

$$A'/\pm 1 = \mathbb{Z}/3$$

on $W[[X, Y]]/(XY - p)$, and the completion of $\mathcal{O}$ is canonically isomorphic to the ring of invariants

$$\hat{\mathcal{O}} \cong W[[S, T]]/(ST - p^3), \qquad S = X^3, \quad T = Y^3.$$

(cf. [6, p. 63] and [4, VI.6]). Let L be the field of fractions of W (i.e. L is the unramified quadratic extension of $\mathbb{Q}_p$), and construct

$$\mathcal{O} \to \hat{\mathcal{O}} \to L \quad \text{by} \quad S \mapsto p^2, \ T \mapsto p;$$

this is a point $x \in X_0(p)(L)$; by results by Serre and Milne (cf. [4, p. DeRa-132, Proposition 3.2]) we know there exists a pair

$$N \subset E \text{ defined over } L, \quad N \otimes L_s \cong \mathbb{Z}/p,$$

with moduli-point x. Let K be the smallest field containing L such that all points of $E[p^i]$ are rational over K. Note that the degree $[K : L]$ divides $(p-1)^2 p^?$, thus it is not divisible by 3; hence

$$\begin{tikzcd}
\mathcal{O} \arrow[r] \arrow[d, hook] & L \arrow[d, hook] \\
W[[X, Y]]/(XY - p) \arrow[r, dashed, "\nexists"] & K
\end{tikzcd}$$

the pair $(N \subset E) \otimes K$ does not extend to a deformation of $\alpha_p \subset E_0$; it follows that E does not have good reduction at the discrete valuation v of K (if so, N would extend flatly, reduce to a subgroup scheme of rank p of E_0, hence to $\alpha_p = N_0 \subset E_0$). Thus E has additive reduction at v, and by construction

$$E[p^i] \subset E(K).$$

3.4 bis. Example. Consider $p=11$, take 121.H of [5, p. 97]. This is a curve E over $L=\mathbb{Q}$ with additive reduction at $w=v_{11}$, with $w(\Delta)=2$, with $w(j)\geq 0$ and which has a subgroup scheme of order 11. Now proceed as before: $K=L(E[11^i])$, etc., and we obtain a curve E over K with additive reduction at v (a valuation lying over w), and with $E[11^i]\subset E(K)$.

3.5. Remark. We have not been able to produce examples analogous to Example 3.4 in case $p\equiv 1 \pmod 3$. Hence for these primes the situation is not clear; we did not get beyond an example of the following type:

3.6. Example. Take $p=7$, consider a curve with conductor 49 over $\mathbb{Q}$, cf. [5, p. 86]. Then $w(\Delta)=3$ or $w(\Delta)=9$ (with $w=v_7$), and the curve has potentially good reduction (because of CM); furthermore it has a subgroup scheme $N\subset E$ over $\mathbb{Q}$ of rank 7. Thus $K:=\mathbb{Q}(N)$ has degree dividing 6, we see that $v(\Delta)$ is not divisible by 12 (where v lies over w) thus E has additive reduction at v and

$$\mathbb{Z}/7\subset E(K)$$

3.7. Example. Consider $p=3$, and let $i\geq 1$ be an integer. We constuct K, v, k, E as before with $\operatorname{char}(K)=0$, $\operatorname{char}(k)=3$ and $E[3^i]\subset E(K)$. We start with $L=\mathbb{Q}$, $w=v_3$, and we choose an elliptic curve E over $\mathbb{Q}$ with minimal equation f such that:

$$E \text{ has additive reduction at } w, \qquad w(j)\geq 0,$$

$$w(\Delta_f)\equiv 1 \pmod 2, \quad \text{and} \quad (\mathbb{Z}/3)\subset E(\mathbb{Q});$$

such examples exist, e.g. see [5, p. 87], the curve 54 A has $w(\Delta)=3$, $w(j)\geq 0$, and $\mathbb{Z}/3\cong E(\mathbb{Q})$. Let $K=\mathbb{Q}(E[3^i])$, then $[K:\mathbb{Q}]$ divides $2\cdot 3^{?}$, thus $v(\Delta)\not\equiv 0 \pmod 4$ for any v lying over $w=v_3$; thus

$$E \text{ has additive reduction at } v, \quad \text{and} \quad E[3^i]\subset E(K)$$

4. *The image of a point of order p under the reduction map*

Let A be an abelian variety over a field K, let $R\subset K$ be the ring defined by a discrete valuation v on K, and let $\mathcal{A}$ be the Neron minimal model of A over $\operatorname{Spec}(R)$. At first suppose $n\geq 1$ is an integer such that $\operatorname{char}(k)$ does not divide n (here k is the residue class field of v, i.e. $k=R/\mathfrak{m}$). Let $\mathcal{A}[n]$ denote the kernel of multiplication by n on $\mathcal{A}$. Note that

$$\mathcal{A}[n]\rightarrow \operatorname{Spec}(R)$$

is etale and quasi-finite. Thus we see that $A(K)[n]$ injects in $A_0(k)$ (here $A_0=\mathcal{A}\otimes_R k$ is the special fibre), and all torsion points of $A_0(\bar{k})$ lift to torsion points of A defined over an extension of K which is unramified at v. In short: for n-torsion the relation between $A(K)$ and $A_0(\bar{k})$ is clear (as long as $\operatorname{char}(k)$ does not divide n).

We give some examples what happens if we consider points whose order is divisible by $\mathrm{char}(k)=p>0$. Also in case of stable reduction it is not so difficult to describe the situation ($\mathscr{A}[p]\to\mathrm{Spec}(R)$ is quasi-finite in that case). Thus we suppose the reduction is *purely additive*; in that case all points on the connected component A_0^0 of the special fibre A_0 are p-power torsion, and $\mathscr{A}[p]\to\mathrm{Spec}(R)$ need not be quasi-finite. We use the filtration on $E(K)$ as introduced in [5, Section 4],

$$E(K)\supset E(K)_0\supset E(K)_1$$

where

$$E(K)_m=\{(x,y)\in E(K)\mid v(x)\leq -2m, v(y)\leq -3m\}$$

after having chosen a minimal equation for E.

4.1.1. Remark. We take $p>3$. If $P\in E(K)$ (and $\mathrm{ord}(P)=p=\mathrm{char}(k)$, and E has additive reduction at v), then $P\in E(K)_0$ (because $p>3$ does not divide the number of connected components of E_0, and $E(K)_0\to E_0^0(k)$, use p. 46, table of [5]). We show that both cases $P\notin E(K)_1$ and $P\in E(K)_1$ indeed occur:

4.1.2. Example. Take $p>3$, we construct $P\in E(K)$, $\mathrm{ord}(P)=p$ and $P\notin E(K)_1$. Let E be the curve 150.C (cf. [5, p. 103]), thus the curve given by the minimal equation

$$Y^2+XY=X^3-28X+272;$$

it has additive reduction at $v=v_5$ (because 5^2 divides its conductor 150), and it has a point of order 5 (indeed $\#E(\mathbb{Q})=10$). We claim

$$P\in E(\mathbb{Q})_0, \qquad P\notin E(\mathbb{Q})_1$$

(relative the valuation v_5). This we can prove as follows: by Remark 4.1.1 we know $P\in E(\mathbb{Q})_0$, thus the group $\langle P\rangle=N\subset E$ extends flatly to a finite group scheme $\mathscr{N}\subset\mathscr{E}$ over $\mathrm{Spec}(\mathbb{Z}_{(5)})$ (one can work with the Néron minimal model $\mathscr{E}$, but also with the (plane) Weierstrass minimal model, and then $\mathscr{N}\otimes\mathbb{F}_5$ is not the singular point because of $P\in E(\mathbb{Q})_0$). If we would have $P\in E(\mathbb{Q})_1$, then it would follow $\alpha_5\cong\mathscr{N}\otimes\mathbb{F}_5$ (because of additive reduction), but α_5 over $\mathbb{F}_5$ does not lift to the unramified situation $\mathbb{Z}_{(5)}\to\mathbb{F}_5$ (cf. [18, Section 5]), thus

$$P\notin E(\mathbb{Q})_1.$$

One can avoid the abstract proof by an explicit computation:

$$P=(-4,20)\in E(\mathbb{Q}), \qquad P\notin E(\mathbb{Q})_1,$$

the tangent line at P is $y=20$, so $-2P=(8,20)$; the tangent line at $-2P$ is $3X-Y-4=0$, so $4P=(-4,-16)=-P$, thus $\langle P\rangle\cong\mathbb{Z}/5$; the singular point on $E \bmod 5$ is $(x=2,\ y=-1) \bmod 5$, thus $P\in E(\mathbb{Q})_0$, and the example is established.

4.1.3. Remark. Take $p>3$, and construct $Q\in E(K)_1$ with $\mathrm{ord}(Q)=p$. Indeed, take $i>1$, and use Example 3.4; then $\mathrm{ord}(P)=p^i$, and $P\in E(K)_0$ (because of Remark

4.1.1), thus $p\cdot P\in E(K)_1$ (because E has additive reduction), thus $Q:=p^{t-1}P\in E(K)_1$ and $\operatorname{ord}(Q)=p$.

Next we choose $p=3$, and we show various possibilities indeed occur:

4.2.1. Example. We construct $P\in E(\mathbb{Q})$, with $\operatorname{ord}(P)=3$, $P\notin E(\mathbb{Q})_0$. Let E be given by the equation

$$Y^2+3aXY+3bY=X^3;$$

by well-known formulas (cf. [5, p. 36]) one computes

$$\Delta=3^6b^3(a^3-3b).$$

If 3^6 does not divide $b^3(a^3-3b)$, this equation is minimal (e.g. take $a=1=b$). Furthermore $P=(0,0)$ is a flex on E (hence $\operatorname{ord}(P)=3$), and E mod 3 has a cusp at $(0,0)$. Thus $P\notin E(\mathbb{Q})_0$.

4.2.2. Example. It is very easy to give $P\in E(K)$ with $\operatorname{ord}(P)=3$, $P\in E(K)_0$ and $P\notin E(K)_1$. E.g.

$$P=(0,2) \quad \text{on} \quad Y^2=X^3+4$$

(cf. 108.A in [5, p. 95]) has this property, because $(x=-1,\ y=0)$ mod 3 is the singular point on E mod 3, thus P reduces to a point on E_0^0 but not to the identity. Another example:

$$P=(0,0) \quad \text{on} \quad Y^2+Y=X^3$$

(cf. 27.A in [5, p. 83]) is a flex, which does not reduce to the cusp $(x=1,\ y=1)$ mod 3 on E mod 3.

4.2.3. Example. We construct $P\in E(K)$ with $\operatorname{ord}(P)=9$, $P\notin E(K)_0$ and $3P\notin E(K)_1$. Indeed consider $K=\mathbb{Q}$, $v=v_3$, and take 54.B (cf. [5, p. 87]), a curve which has additive reduction at 3 such that $\#E(\mathbb{Q})=9$. Note that $\mathbb{Q}$ does not contain a primitive cube root of unity, thus $E(\mathbb{Q})$ does not contain $(\mathbb{Z}/3)\times(\mathbb{Z}/3)$, hence

$$E(\mathbb{Q})\cong\mathbb{Z}/9;$$

let P be a generator for this group. Note that α_3 over $\mathbb{F}_3$ does not lift to $\mathbb{Z}_{(3)}$, thus P and $3P$ do not reduce to the identity under reduction modulo 3, hence

$$E(\mathbb{Q})\to E(\mathbb{Q})/E(\mathbb{Q})_1$$

is injective, thus

$$\operatorname{ord}(P)=9, \qquad 3P\notin E(\mathbb{Q})_1, \qquad P\notin E(\mathbb{Q})_0,$$

and note that the extension

$$0\to E(\mathbb{Q})_0\to E(\mathbb{Q})\to\mathbb{Z}/3\to 0$$

is non-split.

4.2.4. Remark. Take $i=3$ in Example 3.7; then

$$p=3, \qquad P\in E(K), \qquad \operatorname{ord}(P)=3^3$$

and E has additive reduction at v. Then

$$3P\in E(K)_0, \qquad 0\neq 9P\in E(K)_1,$$

thus $Q:=9P$ has the property

$$\operatorname{ord}(Q)=3, \qquad Q\in E(K)_1.$$

4.3. Example. We conclude by an example with $p=2$. Consider 48.E (cf. [5, p. 86]), i.e

$$Y^2=X^3+X^2+16X+180;$$

the right hand side factors over $\mathbb{Q}$ in the irreducible factors

$$(X+5)(X^2-4X+36),$$

hence $E[2](\mathbb{Q})=\mathbb{Z}/2$ Because $\#E(\mathbb{Q})=8$ we conclude

$$E(\mathbb{Q})\cong\mathbb{Z}/8$$

(of course it is well-known that such examples exist, e g cf. [6, p. 35, Theorem 8]). Thus

$$E(\mathbb{Q})_1=0, \qquad E(\mathbb{Q})_0=\mathbb{Z}/2=\langle Q=(5,0)\rangle$$

and

$$E(\mathbb{Q})/E(\mathbb{Q})_0\cong\mathbb{Z}/4$$

(because $(0,0)$ mod 2 is the cusp on E mod 2, and Q mod 2 is smooth on E mod 2).

References

[1] A Frohlich, Local fields, in J W S Cassels and A Frohlich, eds , Algebraic Number Theory (Academic Press, New York, 1967)

[2] A Grothendieck, M Raynaud and D S Rim, Seminaire de Geometrie Algebrique, SGA 7 I, 1967-1969, Lecture Notes in Math 288 (Springer, Berlin, 1972)

[3] S Lang, Abelian Varieties (Interscience, New York, 1959)

[4] Modular functions of one variable II (Antwerp, 1972), Lecture Notes in Math 349 (Springer, Berlin, 1973) Especially P Deligne and M Rapoport, Les schemas de modules de courbes elliptiques, pp 143-316

[5] Modular functions of one variable IV (Antwerp, 1972), Lecture Notes in Math 476 (Springer, Berlin, 1975) Especially J Tate, Algorithm for determining the type of a singular fibre in an elliptic pencil, pp 33-52, Table 1, pp 81-113

[6] B Mazur, Modular curves and the Eisenstein ideal, Publ Math IHES 47 (1978)

[7] D Mumford, Geometric Invariant Theory, Ergebnisse 34 (Springer, Berlin, 1965)

[8] M Nagata, Complete reducibility of rational representations of a matrix group, J Math Kyoto Univ 1 (1961) 87-99

[9] A Neron, Modeles minimaux des varietes abeliennes sur les corps locaux et globaux Publ Math No 21, IHES 1964

[10] F Oort, Finite group schemes, local moduli for abelian varieties and lifting problems, Compositio Math 23 (1971) 265–296 Also in Algebraic Geometry, Oslo 1970 (Wolters-Noordhoff, Groningen, 1972)

[11] F Oort, Good and stable reduction of abelian varieties, Manuscr Math 11 (1974) 171–197

[12] J P Serre, Corps Locaux, Act Sc Ind 1296 (Hermann, Paris, 1962)

[13] J P Serre, Cohomologie Galoisienne Lecture Notes in Math 5 (Springer, Berlin, 1964)

[14] J P Serre and J Tate, Good reduction of abelian varieties, Ann of Math 88 (1968) 492–517

[15] G Shimura and Y Taniyama, Complex multiplication of abelian varieties and its applications to number theory, Math Soc Japan (1961)

[16] G Shimura, On the field of rationality for an abelian variety, Nagoya Math J 45 (1972) 167–178

[17] J H Silverman, The Neron fiber of abelian varieties with potential good reduction, Math Ann 264 (1983) 1–3

[18] J Tate and F Oort, Group schemes of prime order, Ann Sc Ecole Norm Sup 4me serie, 3 (1970) 1–21