J. reine angew. Math. **445** (1993), 109—160

Journal für die reine und angewandte Mathematik


# On the group of components of a Néron model

By *Dino J. Lorenzini*[1]) at Athens

## Introduction

Let $K$ be a complete field with a discrete valuation $v$. Let $\mathcal{O}_K$ denote the ring of integers of $v$, with algebraically closed residue field $k$ of characteristic $p \geqq 0$. The Néron model of an abelian variety $A/K$ is denoted by $\mathscr{A}/\mathcal{O}_K$. Its special fiber $\mathscr{A}_k/k$ is an extension of the finite étale group scheme $\pi_0(\mathscr{A})$ by the smooth connected group scheme $\mathscr{A}_k^0/k$, the connected component of zero in $\mathscr{A}_k$:

$$0 \to \mathscr{A}_k^0 \to \mathscr{A}_k \to \pi_0(\mathscr{A}) \to 0\,.$$

The group $\Phi_K(A) := \pi_0(\mathscr{A})(k)$ is called the group of components of $A/K$. When no confusion can result, we denote this group simply by $\Phi$. Let $\Phi^{(p)}$ denote the prime-to-$p$ part of the group $\Phi$; when the residue characteristic equals zero, we let $\Phi^{(p)} = \Phi$. By Chevalley's Theorem, the group $\mathscr{A}_k^0$ can be described by an exact sequence:

$$0 \to U \times \mathscr{T} \to \mathscr{A}_k^0 \to B \to 0\,,$$

where the group $U$ is a unipotent group scheme of dimension $u_K$, the group $\mathscr{T}$ is a torus of dimension $t_K$, and the quotient $B$ is an abelian variety of dimension $a_K$. We call $u_K$, $t_K$, and $a_K$ respectively the unipotent, toric, and abelian rank of $A/K$. The dimension of $A/K$ is denoted by $g := \dim A = u_K + t_K + a_K$.

We discuss in this paper the structure of the group $\Phi$. To provide a context for our results, let us recall the case of elliptic curves.

If $t_K = 0$, then $\Phi \in \{\{0\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\}$.

If $u_K = 0$, then $\Phi$ is a cyclic group and all cyclic groups can arise in this way.

[1]) Research partially supported by a grant from the Swiss National Science Foundation.

Lenstra and Oort [L-O], 1.15, have generalized the first fact for abelian varieties as follows:

$$\text{If} \quad t_K = a_K = 0, \quad \text{then} \quad \sum_{\ell \text{ prime}} \operatorname{ord}_\ell(|\Phi^{(p)}|)(\ell - 1) \leqq 2g .$$

This bound implies in particular that $|\Phi^{(p)}| \leqq 2^{2g}$, and that, if $\ell$ is a prime dividing $|\Phi^{(p)}|$, then $\ell \leqq 2g + 1$. It was known to Grothendieck (see [Lor2], 3.7) that:

$$\text{If} \quad u_K = 0, \quad \text{then} \quad \Phi \text{ is generated by } t_K \text{ elements} .$$

Silverman [Sil2] suggested that the general case might be a combination of these two "extreme" cases. We will show in this paper that this is indeed true for $\Phi^{(p)}$. Specifically, we will show that $\Phi^{(p)}$ contains a canonical subgroup, $\Theta^{(p)}$, whose order and group structure are bounded in a very precise manner in terms of the unipotent rank $u_K$, and such that the quotient $\Phi^{(p)}/\Theta^{(p)}$ can be generated by $t_K$ elements. We will also describe how the monodromy filtrations on the Tate modules $T_\ell(A)$ are reflected in the group structure of the subgroup $\Theta^{(p)}$. In the second part of this paper, we present an analogous description of the $p$-part of the group $\Phi$, when $A/K$ is the jacobian of a curve.

When $A/K$ has purely additive reduction (i.e., when $a_K = t_K = 0$), the group $\Phi^{(p)}$ is isomorphic to the prime-to-$p$ part of the torsion subgroup of $A(K)$. As a consequence of our study of $\Phi$, we obtain very severe restrictions on the possible finite abelian groups that can occur as the prime-to-$p$ part of the $K$-rational torsion subgroup of an abelian variety having purely additive reduction.

## 1. The main results

**1.1.** Let $A/K$ be an abelian variety. Recall that there exists a Galois extension, $L/K$, minimal with the property that the unipotent rank of $A_L/L$ is equal to zero (see for instance [Des], 5.15). For a prime $\ell \neq p$, let $K_\ell/K$ denote the unique (cyclic) extension of $K$ in $L$ of degree

$$[K_\ell : K] = \ell^{\operatorname{ord}_\ell([L:K])} .$$

We let $a_{K_\ell}$, $t_{K_\ell}$, and $u_{K_\ell}$ denote respectively the abelian, toric, and unipotent rank of $A_{K_\ell}/K_\ell$.

**1.2.** Let $G$ be any finite abelian group. We denote by $G_\ell$ its $\ell$-part. Write $G_\ell$ as a product of cyclic groups:

$$G_\ell := \prod_{i=1}^{s(\ell)} \mathbb{Z}/\ell^{a_i}\mathbb{Z}, \quad \text{with } a_1 \geqq \ldots \geqq a_{s(\ell)} ,$$

and define

$$\delta(G_\ell) := (\ell^{a_1} - 1) + \left(\sum_{i=2}^{s(\ell)} a_i\right)(\ell - 1) .$$

The following theorems summarize the main properties of the group $\Phi_{K,\ell}$, for $\ell$ prime, $\ell \neq p$.

**Theorem 2.15.** *Let $A/K$ be an abelian variety. There exist three subgroups*

$$\Sigma_{K,\ell}(A) \subseteqq \Sigma^{[2]}_{K,\ell}(A) \subseteqq \Sigma^{[3]}_{K,\ell}(A)$$

*of the $\ell$-part $\Phi_{K,\ell}(A)$ of $\Phi_K(A)$, having the following properties:*

(i) *The subgroup $\Sigma_{K,\ell}(A)$ can be generated by $t_K$ elements.*

(ii) *The quotient $\Phi_{K,\ell}/\Sigma^{[2]}_{K,\ell}$ is killed by $[K_\ell : K]$ and*

$$\delta(\Phi_{K,\ell}/\Sigma^{[2]}_{K,\ell}) \leqq 2(a_{K_\ell} - a_K) + t_{K_\ell} - t_K .$$

*Moreover,*

- $\delta(\Phi_{K,\ell}/\Sigma^{[3]}_{K,\ell}) \leqq t_{K_\ell} - t_K$.
- $\delta(\Sigma^{[3]}_{K,\ell}/\Sigma^{[2]}_{K,\ell}) \leqq 2(a_{K_\ell} - a_K)$.

(iii) *The quotient $\Sigma^{[2]}_{K,\ell}/\Sigma_{K,\ell}$ is killed by $[K_\ell : K]$ and $\delta(\Sigma^{[2]}_{K,\ell}/\Sigma_{K,\ell}) \leqq t_{K_\ell} - t_K$.*

**Theorem 3.21.**[2]) *Let $A/K$ be an abelian variety. Let $\ell \neq p$ be a prime. Assume that $A/K$ has a polarization whose degree is prime to $\ell$.*

(i) *Then there exists a nondegenerate pairing*

$$(\ ;\ ) : \Phi_{K,\ell} \times \Phi_{K,\ell} \to \mathbb{Q}_\ell/\mathbb{Z}_\ell .$$

(ii) *There exist three subgroups*

$$\Theta^{[3]}_{K,\ell}(A) \subseteqq \Theta^{[2]}_{K,\ell}(A) \subseteqq \Theta_{K,\ell}(A)$$

*of the $\ell$-part $\Phi_{K,\ell}(A)$ of $\Phi_K(A)$, which are functorial in the variable $A$ and whose existence does not depend on the choice of a polarization for $A$. These subgroups are equal to the orthogonals, under the pairing $(\ ;\ )$, of the subgroups*

$$\Sigma^{[3]}_{K,\ell}(A) \supseteqq \Sigma^{[2]}_{K,\ell}(A) \supseteqq \Sigma_{K,\ell}(A),$$

*respectively.*

(iii) *The pairing $(\ ;\ )$ restricts to a nondegenerate pairing on $\Theta_{K,\ell}(A)$, again denoted by $(\ ;\ )$. The subgroup $\Theta^{[2]}_{K,\ell}(A)$ is the orthogonal in $\Theta_{K,\ell}(A)$, under the restricted pairing, of the subgroup $\Theta^{[3]}_{K,\ell}(A)$. In particular,*

- *The groups $\Theta^{[3]}_{K,\ell}(A)$ and $\Theta_{K,\ell}(A)/\Theta^{[2]}_{K,\ell}(A)$ are isomorphic. Equivalently, the group $\Phi_{K,\ell}(A)/\Sigma^{[3]}_{K,\ell}(A)$ is isomorphic to $\Sigma^{[2]}_{K,\ell}(A)/\Sigma_{K,\ell}(A)$.*

[2]) The author wishes to thank a referee for a correction to an earlier version of Theorem 3.21.

As we shall see in the next section, the subgroups of $\Phi_{K,\ell}$ of the form "$\Sigma$" are easy to compute with. On the other hand, the subgroups of the form "$\Theta$" are more "natural", as we shall now see. The group $\Theta_{K,\ell}^{[2]}$ can be described in the following explicit way. Let $M/K$ be any finite extension. Let $a_M$, $t_M$, and $u_M$ denote respectively the abelian, toric, and unipotent rank of $A_M/M$. Denote by $\mathscr{A}_M/\mathcal{O}_M$ the Néron model of $A_M/M$. By the universal property of Néron models, there exists a unique map,

$$\gamma_{K,M} : (\mathscr{A}_K)_{\mathcal{O}_M} \to \mathscr{A}_M ,$$

which equals the identity map when restricted to the generic fibers. In particular, there is a natural map, again denoted by $\gamma_{K,M}$:

$$\gamma_{K,M} : \Phi_K \to \Phi_M .$$

We let

$$\Psi_{K,M} := \operatorname{Ker}(\gamma_{K,M}) \subseteqq \Phi_K .$$

**Theorem 3.22.** *The subgroup $\Theta_{K,\ell}^{[2]}$ is equal to the $\ell$-part of $\Psi_{K,L}$.*

In the last section of this paper, we will present examples of the filtration of the group of components

$$\Theta_{K,\ell}^{[3]}(A) \subseteqq \Theta_{K,\ell}^{[2]}(A) \subseteqq \Theta_{K,\ell}(A) \subseteqq \Phi_{K,\ell}(A)$$

introduced in Theorem 3.21. We will also describe the group of components of the jacobian of a Fermat curve.

**Remark 1.3.** Recall that when $A/K$ has *purely additive reduction* (i.e., when $a_K = t_K = 0$), the reduction map

$$\pi_K : A(K) \to \mathscr{A}_k(k)$$

induces an isomorphism from the prime-to-$p$ part $A(K)_{\text{tors}}^{(p)}$ of the torsion subgroup of $A(K)$ to $\Phi_K^{(p)}$. Using Lemma 2.17, we obtain the following corollary of Theorem 2.15, which is a sharpening of a result of Lenstra and Oort ([L-O], 1.13).

**Corollary 1.4.** *Let $A/K$ be an abelian variety of dimension g having purely additive reduction. If $A/K$ has potentially good reduction, then $A(K)_{\text{tors}}^{(p)}$ is killed by $[L:K]$ and*

$$\sum_{\ell \neq p} \delta(A(K)_{\text{tors},\ell}) \leqq 2g .$$

*If $A/K$ does not have potentially good reduction, then there exists a subgroup $A^{[2]}$ of $A(K)_{\text{tors}}^{(p)}$, such that both $A^{[2]}$ and $A(K)_{\text{tors}}^{(p)}/A^{[2]}$ are killed by $[L:K]$, and such that*

$$\sum_{\ell \neq p} \delta(A_\ell^{[2]}) + \delta(A(K)_{\text{tors},\ell}/A_\ell^{[2]}) \leqq 2g .$$

**Corollary 1.5.** *Let $A/K$ be a principally polarized abelian variety having purely additive reduction. If the semistable reduction of $A/K$ is purely toric (i.e., if $a_L = 0$), then the order of $A^{(p)}(K)_{\text{tors}}$ is a square.*

*Proof.* Since, by hypothesis, $t_K = 0$, it follows from part (i) of Theorem 2.15 that $\Sigma_{K,\ell} = (0)$ if $\ell \neq p$. Since $a_L = 0$, it follows from part (ii) of Theorem 2.15 that

$$\Sigma_{K,\ell}^{[2]} = \Sigma_{K,\ell}^{[3]} .$$

Hence, Theorem 3.21 shows that the group $A^{(p)}(K)_{\text{tors}}$ is an extension of the group $\Sigma_{K,\ell}^{[2]}$ by itself. The order of $A^{(p)}(K)_{\text{tors}}$ is therefore a square. Note that the pairing on $\Phi_{K,\ell}$ is not necessarily alternating. □

**Corollary 3.25.** *Let $A/K$ be an abelian surface having purely additive reduction. If $A/K$ has potentially good reduction, then $A(K)_{\text{tors}}^{(p)}$ is isomorphic to a subgroup of one of the following groups*:

$$\mathbb{Z}/5\mathbb{Z},\ (\mathbb{Z}/3\mathbb{Z})^2,\ (\mathbb{Z}/2\mathbb{Z})^4,\ \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z} .$$

*Except for the groups $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$, each group in the above list can be realized as the prime-to-p torsion subgroup of a product of elliptic curves. The group $\mathbb{Z}/5\mathbb{Z}$ can be realized as the prime-to-p torsion subgroup of an abelian surface. The group $\mathbb{Z}/4\mathbb{Z}$ cannot be realized as the prime-to-p torsion subgroup of a principally polarized abelian surface.*

*If $A/K$ does not have potentially good reduction, then $A(K)_{\text{tors}}^{(p)}$ is isomorphic to a subgroup of one of the following groups*:

$$\mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/9\mathbb{Z},\ \mathbb{Z}/12\mathbb{Z},\ (\mathbb{Z}/3\mathbb{Z})^2,\ (\mathbb{Z}/2\mathbb{Z})^4,\ \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z},\ (\mathbb{Z}/2\mathbb{Z})^2\oplus\mathbb{Z}/4\mathbb{Z},\ (\mathbb{Z}/4\mathbb{Z})^2 .$$

*Except for the groups $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/9\mathbb{Z}$, each group in the above list can be realized as the prime-to-p torsion subgroup of a product of elliptic curves. The groups $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/9\mathbb{Z}$ can be realized as the prime-to-p torsion subgroups of abelian surfaces.*

It is not known whether the group $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$ can be realized as the prime-to-$p$ part of the group of components of a principally polarized abelian surface with purely additive reduction and potentially good reduction.

**Remark 1.6.** Let $L_0/K$ denote the maximal tame subextension of $L$. We will show in Lemma 2.17 that

$$\sum_{\ell \neq p} (a_{K_\ell} - a_K) + (t_{K_\ell} - t_K) \leqq u_K - u_{L_0} .$$

Let

$$\Theta_K^{(p)} := \prod_{\ell \neq p} \Theta_{K,\ell} ,$$

and

$$\Psi_{K,L}^{(p)} := \prod_{\ell \neq p} \Psi_{K,L,\ell} .$$

Our next corollary follows directly from Theorem 2.15, Theorem 3.21 and Theorem 3.22, quoted above.

**Corollary 1.7.** *Let $A/K$ be a principally polarized abelian variety. The functorial subgroup $\Theta_K^{(p)}$ has the following properties:*

(i) *The quotient $\Phi_K^{(p)}/\Theta_K^{(p)}$ is generated by $t_K$ elements.*

(ii) $\sum_{\ell \neq p} \delta(\Psi_{K,L,\ell}^{(p)}) + \delta(\Theta_{K,\ell}^{(p)}/\Psi_{K,L,\ell}^{(p)}) \leqq 2(u_K - u_{L_0})$.

**Remark 1.8.** It is natural to wonder, in light of Corollary 1.7, and in view of the fact that the subgroup $\Psi_{K,L}$ has a well-defined functorial $p$-part, whether there exists a subgroup,

$$\Theta_{K,p}(A) \subseteqq \Phi_{K,p}(A),$$

having the following properties:

(i) The subgroup $\Theta_{K,p}(A)$ is functorial in the variable $A$.

(ii) The quotient $\Phi_{K,p}(A)/\Theta_{K,p}(A)$ is generated by $t_K$ elements.

(iii) The order of $\Theta_{K,p}(A)$ is bounded in terms of $u_{L_0}$.

We do not know whether there exists such a subgroup in general. However, when $A/K$ is a jacobian, we show in the following theorem that $\Phi_K$ contains a subgroup $G_p$ satisfying the properties (ii) and (iii) stated above. Even in the particular case of jacobians, we do not know whether there exists a subgroup $\Theta_{K,p}(A)$ satisfying property (i) as well as properties (ii) and (iii).

**Theorem 4.1.** *Let $X/K$ be a smooth proper geometrically connected curve having a $K$-rational point. Let $A/K$ denote the jacobian of $X/K$. The $p$-part $\Phi_{K,p}$ of the group of components of $A/K$ contains three subgroups,*

$$H'_p \subseteqq H_p \subseteqq G_p,$$

*having the following properties:*

1. *The group $\Phi_{K,p}/G_p$ is generated by $t_K$ elements.*

2. *The following inequality holds:*

$$\delta(H_p) + \delta(G_p/H_p) \leqq 2u_{L_0}.$$

3. *The group $G_p/H_p$ is isomorphic to the group $H'_p$.*

**Remark 1.9.** The semistable reduction theorem for abelian varieties states that, given an abelian variety $A/K$, there exists a finite extension $M/K$ such that the unipotent rank of $A_M/M$ is equal to zero. Corollary 1.7 might be better understood in light of the following proposition, which plays a crucial role in Artin and Winters' proof of the semistable reduction for abelian varieties [A-W], 2.8. We recall the proof of the proposition for the convenience of the reader.

**Proposition 1.10.** *The existence, for all abelian varieties $A/K$, of a subgroup $G(A)$ in $\Phi_K^{(p)}(A)$ having the properties:*

- *$\Phi_K^{(p)}/G$ is generated by $t_K$ elements, and*
- *$|G|$ is bounded by a constant $c = c(g)$ depending on the dimension of $A$ only,*

*implies the existence of a finite extension $M/K$ such that the Néron model $\mathscr{A}_M/\mathcal{O}_M$ of $A_M/M$ has unipotent rank $u_M = 0$.*

*Proof.* Let $\ell \neq p$ be a prime larger than $c(g)$. For any group or group scheme $G$, denote by ${}_\ell G$ the kernel of the multiplication by $\ell$ on $G$. Let $M$ denote the field of rationality of the points of ${}_\ell A(\bar{K})$. We are going to show that $u_M = 0$. To simplify our notations, we let $\mathscr{A}$, in this proof, denote the Néron model of $A_M/M$. Since $\ell \neq p$, the multiplication by $\ell$ is étale on $\mathscr{A}$ and, hence, we have an isomorphism of groups:

$$ {}_\ell A(M) = {}_\ell A(\bar{K}) \xrightarrow{\sim} {}_\ell \mathscr{A}_k(k) \, . $$

Since $\ell \neq p$, the group $\mathscr{A}_k^0(k)$ is $\ell$-divisible, that is, the map

$$ \text{“multiplication by } \ell\text{”} : \mathscr{A}_k^0(k) \to \mathscr{A}_k^0(k) $$

is surjective. We therefore have an exact sequence,

$$ 0 \to {}_\ell \mathscr{A}_k^0(k) \to {}_\ell \mathscr{A}_k(k) \to {}_\ell \Phi_M \to 0 \, . $$

We conclude the proof by counting the dimensions of these three $\mathbf{F}_\ell$-vector spaces. The group ${}_\ell \mathscr{A}_k(k)$ has dimension $2g = 2a_M + 2t_M + 2u_M$, by hypothesis. Since a unipotent group has no element of order $\ell$ if $\ell \neq p$, we find that

$$ \dim_{\mathbf{F}_\ell}({}_\ell \mathscr{A}_k^0(k)) = 2a_M + t_M \, . $$

Since $\ell > c(g)$, $\dim_{\mathbf{F}_\ell}({}_\ell \Phi_M) \leqq t_M$. We obtain the inequality

$$ 2a_M + 2t_M + 2u_M \leqq (2a_M + t_M) + t_M \, , $$

and therefore $u_M = 0$. □

**Remark 1.11.** Write $\Phi_K \cong \prod_{i=1}^{r} \mathbb{Z}/\varphi_i\mathbb{Z}$ with $\varphi_1 | \dots | \varphi_r$, $\varphi_i$ positive integers. If $r > t_K$, let

$$ \Upsilon_K := \prod_{i=1}^{r-t_K} \mathbb{Z}/\varphi_i\mathbb{Z} $$

so that $\Phi_K$ splits into a product

$$ \Phi_K \cong \Upsilon_K \times C_1 \times \dots \times C_{t_K} $$

where each group $C_i$ is cyclic. If $r \leqq t_K$, let $\Upsilon_K = \{0\}$.

The crucial step in Artin and Winters' proof of the semistable reduction theorem is to show that, when $A$ is the jacobian of a curve having a $K$-rational point, the order of the group $\Upsilon_K$ is bounded by a constant $c$ depending only on $g = \dim A$. This follows from [A-W], 1.16. Artin and Winters, however, did not make this statement explicit (there is no mention of groups of components in their work). One finds the first explicit statement of an analogous result in an article, published twelve years later, in which Silverman [Sil] shows that $\Phi_K^{(p)}$ is bounded by such a constant $c$ when $A/K$ has potentially good reduction. We provide an explicit bound for $|\Upsilon_K|$ in 4.16 and 4.21.

Note that the subgroup $\Upsilon_K$ is not "functorial" in $A$ since a morphism of abelian varieties $\alpha: A \to B$ does not always induce a commutative diagram

$$\begin{array}{ccc} \Upsilon_K(A) & \longrightarrow & \Upsilon_K(B) \\ \cap & & \cap \\ \Phi_K(A) & \xrightarrow{\alpha} & \Phi_K(B) . \end{array}$$

To show that such a commutative diagram does not always exist, let $E$ be an elliptic curve with additive reduction over $K$ and a non-trivial group of components. Let $\mathscr{E}$ be an elliptic curve with multiplicative reduction and a trivial group of components. Let $t$ and $u$ be two positive integers with $t > 2u$. Consider the natural map

$$\alpha: E^u \to E^u \times \mathscr{E}^t .$$

The induced map $\Phi_K(E^u) \to \Phi_K(E^u \times \mathscr{E}^t)$ is an injection while $\Upsilon_K(E^u) = \Phi_K(E^u)$ and the group $\Upsilon_K(E^u \times \mathscr{E}^t)$ is trivial.

This article will proceed as follows. In section two, we use the monodromy filtration on the Tate module $T_\ell(A)$ to define some subgroups of $\Phi_{K,\ell}(A)$ and to prove a bound for their orders. In the third section, we prove our main theorem describing a filtration on the $\ell$-part of the group of components $\Phi_{K,\ell}$ when $\ell \neq p$. In the fourth section, we recall Raynaud's description of the group $\Phi_K$ when the abelian variety $A/K$ is a jacobian. We then use our main theorem to deduce the existence of a nonfunctorial filtration on the $p$-part of the group of components of a jacobian. In the last section, we present some examples to illustrate the main properties of the group $\Phi_K$. In particular, we describe the group of components of the jacobian of a Fermat curve.

## 2. Description of the group $\Phi_{K,\ell}$

Let $A/K$ be an abelian variety. We let $T_\ell$, or simply $T$ when no confusion can result, denote the Tate module $T_\ell A$, $\ell \neq p$. In this section, we recall Grothendieck's description of the group $\Phi_{K,\ell}$. This description will enable us to associate to any submodule $X$ of $T_\ell$ a subgroup $s(X)$ of the group $\Phi_{K,\ell}$. The computation of the number of generators of $s(X)$ and of the order of $\Phi_{K,\ell}/s(X)$ will be reduced to linear algebra.

The Galois group $I_K := I(\bar{K}/K)$ acts on the Tate module $T_\ell = T_\ell A$ in a natural way. When $\ell$ is a prime different from the residue characteristic $p$, Grothendieck [Gro], IX, 11.2, describes the $\ell$-part $\Phi_{K,\ell}$ of $\Phi_K$ in terms of this action by showing the existence of a natural isomorphism

$$\phi_{K,\ell}\colon \Phi_{K,\ell} \to \frac{(T_\ell A \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell)^{I_K}}{(T_\ell A)^{I_K} \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell}.$$

Let $P$ denote the pro-$p$-Sylow subgroup of $I_K$ and let $\sigma$ denote a topological generator of $I_K/P \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$. For each $\ell \neq p$, let $\sigma_\ell$ denote the automorphism of $(T_\ell A)^P$ induced by $\sigma$. We may drop the subscript $\ell$ in $\sigma_\ell$ when no confusion may result. Let

$$\mathbb{D}_\ell := \mathbb{Q}_\ell/\mathbb{Z}_\ell\,.$$

Let

$$E := \frac{(T_\ell \otimes \mathbb{D}_\ell)^{I_K}}{T_\ell^{I_K} \otimes \mathbb{D}_\ell}\,.$$

**Lemma 2.1.** *The group $E$ is isomorphic to the torsion subgroup $F$ of $T_\ell^P/(\sigma_\ell - \mathrm{id})(T_\ell^P)$.*

*Proof.* Since $T_\ell$ is a free $\mathbb{Z}_\ell$-module, we have an exact sequence:

$$0 \to T_\ell \to T_\ell \otimes \mathbb{Q}_\ell \to T_\ell \otimes \mathbb{D}_\ell \to 0\,.$$

Lenstra and Oort remark, in [L-O], 1.2, that taking $P$-invariants is an exact functor. Consider then the diagram:

$$\begin{array}{ccccccccc} 0 & \to & T_\ell^P & \to & (T_\ell \otimes \mathbb{Q}_\ell)^P & \to & (T_\ell \otimes \mathbb{D}_\ell)^P & \to & 0 \\ & & \downarrow{\scriptstyle \sigma_\ell - \mathrm{id}} & & \downarrow{\scriptstyle \sigma_\ell - \mathrm{id}} & & \downarrow{\scriptstyle \sigma_\ell - \mathrm{id}} & & \\ 0 & \to & T_\ell^P & \to & (T_\ell \otimes \mathbb{Q}_\ell)^P & \to & (T_\ell \otimes \mathbb{D}_\ell)^P & \to & 0\,. \end{array}$$

Using the Snake Lemma, we obtain the exact sequence:

$$0 \to T_\ell^{I_K} \to (T_\ell \otimes \mathbb{Q}_\ell)^{I_K} \to (T_\ell \otimes \mathbb{D}_\ell)^{I_K} \xrightarrow{\partial_\sigma} T_\ell^P/\mathrm{Im}(\sigma_\ell - \mathrm{id}) \to (T_\ell^P \otimes \mathbb{Q}_\ell)/\mathrm{Im}(\sigma_\ell - \mathrm{id})\,.$$

Hence, we can write:

$$0 \to \frac{(T_\ell \otimes \mathbb{D}_\ell)^{I_K}}{T_\ell^{I_K} \otimes \mathbb{D}_\ell} \xrightarrow{\partial_\sigma} T_\ell^P/\mathrm{Im}(\sigma_\ell - \mathrm{id}) \xrightarrow{\mu} (T_\ell^P \otimes \mathbb{Q}_\ell)/\mathrm{Im}(\sigma_\ell - \mathrm{id})\,.$$

Since the kernel of $\mu$ is equal to the torsion subgroup of $T_\ell^P/\mathrm{Im}(\sigma_\ell - \mathrm{id})$, our lemma is proved. □

**Remark 2.2.** The isomorphism between the group $\Phi_{K,\ell}$ and the group $F$ greatly simplifies the computation of the group $\Phi_{K,\ell}$ when the matrix $\sigma_\ell$ is given explicitly. Indeed, a row and column reduction of the matrix $\sigma_\ell - \mathrm{id}$ reduces this matrix to a diagonal matrix $\mathrm{diag}(e_1, \dots, e_h, 0, \dots, 0)$, with $h \leqq 2g$. The group $\Phi_{K,\ell}$ is isomorphic to $\prod_{i=1}^{h} \mathbb{Z}_\ell/e_i\mathbb{Z}_\ell$.

**Lemma 2.3.** *The group $F$ does not depend on the choice of a generator $\sigma$ of $I_K/P$.*

*Proof.* The group $F$ is defined to be the torsion subgroup of the group

$$T_\ell^P/(\sigma_\ell - \mathrm{id})(T_\ell^P).$$

Let us show that the group $(\sigma_\ell - \mathrm{id})(T_\ell^P)$ does not depend on the choice of a generator of $I/P$. The module $T_\ell^P$ is compact and Hausdorff, and the map

$$\sigma_\ell - \mathrm{id}: T_\ell^P \to T_\ell^P$$

is continuous. Therefore, the image $(\sigma_\ell - \mathrm{id})(T_\ell^P)$ is closed in $T_\ell^P$. Let $\tau \in I_K/P$ and $x \in T_\ell^P$. The element $(\tau - \mathrm{id})(x)$ is in the closure of $(\sigma_\ell - \mathrm{id})(T_\ell^P)$ in $T_\ell^P$ because the map

$$I_K/P \to T_\ell^P,$$
$$\mu \mapsto (\mu - \mathrm{id})(x)$$

is continuous and because the subgroup generated by $\sigma$ is dense in $I_K/P$. Therefore, if $\tau$ is a topological generator of $I_K/P$, then $(\tau - \mathrm{id})(T_\ell^P) = (\sigma_\ell - \mathrm{id})(T_\ell^P)$. □

**2.4.** To any submodule $X$ of $T_\ell$, we may now associate a subgroup $s(X)$ of $F$ as follows:

$$s(X) := \text{torsion subgroup of } \frac{X^P + (\sigma_\ell - \mathrm{id})(T^P)}{(\sigma_\ell - \mathrm{id})(T^P)}.$$

Clearly, $s(X) = s(X^P)$. Note that the subgroup $s(X)$ does not depend on the choice of a polarization of $A$. It does not depend on the choice of a generator of $I_K/P$ either.

**2.5.** Before we can proceed any further, we need to recall some standard facts about abelian varieties. We refer the reader to [Gro], IX, § 2 and § 3, for the proofs of these facts. Fix a polarization of the abelian variety $A/K$. There exists a Galois-invariant skew-symmetric separating pairing:

$$\langle , \rangle : T_\ell A \times T_\ell A \to T_\ell \mathbb{G}_m \cong \mathbb{Z}_\ell.$$

For any submodule $X \subseteq T_\ell$, we let $X^\perp$ denote the orthogonal complement of $X$ under $\langle , \rangle$. We define

$$W_{\ell,K} := T_\ell^{I_K} \cap (T_\ell^{I_K})^\perp.$$

We may drop the index $\ell$ when no confusion can result.

The image of the wild ramification subgroup $P$ in $\mathrm{Aut}(T_\ell)$ is a finite $p$-group $P_0$. For any $\ell \neq p$, $|P_0|$ is invertible in $\mathbb{Z}_\ell$. Therefore, the following averaging map, introduced by Lenstra and Oort in [L-O], 1.1, is well defined:

$$x \in T_\ell \mapsto \Big(|P_0|^{-1} \sum_{\sigma \in P_0} \sigma(x)\Big) \in T_\ell^P.$$

The pairing $\langle , \rangle$ on $T_\ell A$ restricts to a non-degenerate pairing on $T_\ell^P$, denoted again by $\langle , \rangle$. We let $Y^\S$ denote the orthogonal complement of a submodule $Y \subseteq T_\ell^P$ under the restricted pairing. It is clear that for any submodule $X \subseteq T_\ell$,

$$(X^P)^\S = (X^\perp)^P .$$

In particular,

$$W_{\ell,K} = T_\ell^{I_K} \cap (T_\ell^{I_K})^\S .$$

For any extension $K \subseteq M \subseteq L$, we denote by $M_0$ the extension $K \subseteq M_0 \subseteq M$ corresponding to the inertia group

$$I_{M_0} = I_M \cdot P .$$

Let $a_M$, $t_M$, and $u_M$ denote respectively the abelian, toric, and unipotent rank of $A_M/M$. We indicate in the diagram below the rank over $\mathbb{Z}_\ell$ of the quotient of two successive modules:

$$0 \xrightarrow{t_M} W_{\ell,M} \xrightarrow{2a_M} T_\ell^{I_M} \xrightarrow{2u_M} W_{\ell,M}^\perp \xrightarrow{t_M} T_\ell .$$

Taking the $P$-invariant submodules in the above sequence, we obtain the following inclusions:

$$0 \to W_{M_0} \to T_\ell^{I_{M_0}} \to W_{M_0}^\S \to T_\ell^P .$$

By definition of $L$, the unipotent rank $u_L$ equals zero. Therefore, $W_L^\perp / T^{I_L}$ is a torsion module. Since $T/T^{I_M}$ is a free $\mathbb{Z}_\ell$-module for any $M \supseteq K$, we conclude that

$$W_L^\perp = T_\ell^{I_L} .$$

This equality implies in particular that:

$$(W_{L_0})^\S = T^{I_{L_0}} .$$

**2.6.** In the following diagram, all maps are inclusions. The rank of the cokernel of each map is indicated over the corresponding arrow.

$$\begin{array}{ccccccc}
0 & \xrightarrow{t_K} & W_K & \xrightarrow{2a_K} & T^{I_K} & \xrightarrow{2(u_K - u_{L_0})} & W_K^\S \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle t_K} \\
0 & \xrightarrow{t_{L_0}} & W_{L_0} & \xrightarrow{2a_{L_0}} & T^{I_{L_0}} & \xrightarrow{t_{L_0}} & T^P \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle 2u_{L_0}} \\
0 & \xrightarrow{t_L} & W_L & \xrightarrow{2a_L} & T^{I_L} & \xrightarrow{t_L} & T .
\end{array}$$

**Remark 2.7.** Assume that the residue characteristic $p$ is equal to zero. Let $q$ be any prime and denote by $Q$ the pro-$q$-Sylow subgroup of $I_K$. Let $L_q$ denote the extension of $K$ corresponding to the subgroup $I_L \cdot Q$, so that

$$L_q = (\bar{K})^{I_L \cdot Q} .$$

If $\ell \neq q$, the image $Q_0$ of $Q$ in $\mathrm{Aut}(T_\ell)$ is finite. The pairing $\langle ; \rangle$ on $T_\ell \times T_\ell$ restricts to a nondegenerate Galois invariant pairing, again denoted by $\langle ; \rangle$, on $T_\ell^Q \times T_\ell^Q$. If $X$ is any submodule of $T_\ell^Q$, let $X^\#$ denote its orthogonal in $T_\ell^Q$ under the restricted pairing $\langle ; \rangle$.

In the following diagram, all maps are inclusions:

$$\begin{array}{ccccccc}
0 & \xrightarrow{t_K} & W_K & \xrightarrow{2a_K} & T^{I_K} & \longrightarrow & W_K^{\#} \\
 & & \downarrow & & \downarrow & & \downarrow t_K \\
0 & \xrightarrow{t_{L_q}} & W_{L_q} & \xrightarrow{2a_{L_q}} & T^{I_{L_q}} & \xrightarrow{t_{L_q}} & T^Q \\
 & & \downarrow & & \downarrow & & \downarrow 2u_{L_q} \\
0 & \xrightarrow{t_L} & W_L & \xrightarrow{2a_L} & T^{I_L} & \xrightarrow{t_L} & T\,.
\end{array}$$

We note, for future use, that

$$\mathrm{rank}_{\mathbb{Z}_\ell}(T/T^Q) = 2u_{L_q}\,.$$

The following lemma provides a justification for the inclusions given in the first columns of the two diagrams above.

**Lemma 2.8.** *Let $M/K$ be any field extension contained in $L$. Then*

$$W_{\ell,K} = (W_{\ell,M})^{I_K}\,.$$

*In particular,* $W_{\ell,K} \subseteq W_{\ell,M} \subseteq W_{\ell,L}$.

*Proof.* It immediately follows from the definitions of $W_K$ and $T^{I_{M_0}}$ that

$$W_K \subseteq T^{I_{M_0}}\,.$$

To show that $W_K \subseteq (T^{I_{M_0}})^\S$, let $\tau$ be a generator of $\mathrm{Gal}(M_0/K)$. Let $x \in W_K$. Then

$$[M_0 : K]\langle x, y\rangle = \langle x, (1 + \tau + \cdots + \tau^{[M_0:K]-1})y\rangle = 0$$

for all $y \in T^{I_{M_0}}$. Indeed, $x \in (T^{I_K})^\S$ and $(1 + \tau + \cdots + \tau^{[M_0:K]-1})y \in T^{I_K}$. Therefore,

$$\langle x, y\rangle = 0 \quad \text{for all } y \in T^{I_{M_0}}, \text{ and } x \in (T^{I_{M_0}})^\S\,.$$

Hence, $W_K \subseteq W_{M_0}$. Note now that

$$\begin{aligned}
(W_M)^P &= [T^{I_M} \cap (T^{I_M})^\perp]^P \\
&= T^{I_{M_0}} \cap (T^{I_{M_0}})^\S \\
&= T^{I_{M_0}} \cap (T^{I_{M_0}})^\perp \\
&= W_{M_0}\,,
\end{aligned}$$

so that $W_M^{I_K} = W_{M_0}^{I_K}$.

Clearly, $W_K \subseteq W_{M_0}^{I_K}$. Since $(T^{I_{M_0}})^{\S} \subseteq (T^{I_K})^{\S}$, we find that

$$W_K \subseteq W_{M_0}^{I_K} = [(T^{I_{M_0}})^{\S}]^{I_K} \subseteq [(T^{I_K})^{\S}]^{I_K} = W_K .$$

This finishes the proof of our lemma. □

**Remark 2.9.** Let $\ell \neq p$ be a prime. The following description of the module $W_{\ell,K}$ shows that this module does not depend on the choice of a polarization of $A/K$. Let $\mathscr{A}/\mathcal{O}_K$ denote the Néron model of $A/K$. Let $\mathscr{T}_K$ denote the torus in the connected component of zero of the special fiber of $\mathscr{A}$. The module $W_{\ell,K}$ can be canonically identified to the Tate module $T_\ell(\mathscr{T}_K)$ ([Gro], IX, 2.3). Therefore, the modules

$$W_{\ell,K} \subseteq W_{\ell,L} \subseteq T_\ell^{I_L}$$

are canonical submodules of $T_\ell$, independent of a choice of a polarization. We define:

$$\Sigma_{K,\ell}(A) := s(W_{\ell,K}),$$
$$\Sigma_{K,\ell}^{[2]}(A) := s(W_{\ell,L}),$$
$$\Sigma_{K,\ell}^{[3]}(A) := s(T_\ell^{I_L}).$$

In the remainder of this section, we discuss some bounds for the order of a quotient of $\Phi_{K,\ell}$ of the form $\Phi_{K,\ell}/s(X)$.

**Lemma 2.10.** *If $X \subset T_\ell$ is any submodule, then*

$$s(X) := \textit{torsion of } \frac{X^P + (\sigma_\ell - \mathrm{id})(T^P)}{(\sigma_\ell - \mathrm{id})(T^P)}$$

*is isomorphic to*

$$\frac{X^P \cap (T_\ell^{I_K})^{\S}}{X^P \cap (\sigma_\ell - \mathrm{id})(T^P)}.$$

*Proof.* The sequence

$$0 \to \frac{X^P \cap (T^{I_K})^{\S}}{X^P \cap (\sigma_\ell - \mathrm{id})(T^P)} \to \frac{X^P}{X^P \cap (\sigma_\ell - \mathrm{id})(T^P)} \to \frac{X^P}{X^P \cap (T^{I_K})^{\S}} \to 0$$

is exact. Since $(T^{I_K})^{\S}$ and $(\sigma_\ell - \mathrm{id})(T^P)$ have the same rank, the left term of this sequence is a finite group. One easily checks that the right term of this sequence is a free $\mathbb{Z}_\ell$-module. □

**Lemma 2.11.** *The group $s(W_K)$ is generated by $t_K$ elements.*

*Proof.* Indeed, the $\mathbb{Z}_\ell$-module $W_K$ has rank $t_K$ and, therefore, the group

$$s(W_K) := \frac{W_K + (\sigma_\ell - \mathrm{id})(T^P)}{(\sigma_\ell - \mathrm{id})(T^P)} \cong \frac{W_K}{W_K \cap (\sigma_\ell - \mathrm{id})(T^P)}$$

is generated by $t_K$ elements. □

**Proposition 2.12.** *Let $Z \subseteqq X$ be two $\sigma_\ell$-invariant submodules of $(T_\ell^{I_K})^\S$ containing $W_{\ell,K}$. If the automorphism induced by $\sigma_\ell$ on the free $\mathbb{Z}_\ell$-module $X/Z$ has finite order $r$, then $s(X)/s(Z)$ is killed by $r$ and*

$$\delta(s(X)/s(Z)) \leqq \operatorname{rank}_{\mathbb{Z}_\ell}((X/Z)^{\langle \sigma_\ell^{r_\ell} \rangle}),$$

*where $r_\ell := \ell^{\operatorname{ord}_\ell(r)}$, and $\langle \sigma_\ell^{r_\ell} \rangle$ denote the group generated by $\sigma_\ell^{r_\ell}$. The operator $\delta(\ )$ is defined as in* 1.2.

*Proof.* Note that the group

$$s(X)/s(Z) = \frac{X + (\sigma - 1)(T^P)}{Z + (\sigma - 1)(T^P)} = \frac{X}{X \cap [Z + (\sigma - 1)(T^P)]}$$

is a quotient of the group

$$\frac{X}{Z + (\sigma - 1)(X)} = \operatorname{coker}(X/Z \xrightarrow{\sigma - 1} X/Z).$$

Therefore, in order to prove our proposition, we only need to show that $X/[Z + (\sigma - 1)(X)]$ is killed by $r$ and that

$$\delta\left(\frac{X}{Z + (\sigma - 1)(X)}\right) \leqq \operatorname{rank}_{\mathbb{Z}_\ell}((X/Z)^{\langle \sigma_\ell^{r_\ell} \rangle}).$$

The group $X/[Z + (\sigma - 1)(X)]$ is finite because $(\sigma - 1)$ is injective when restricted to $X/Z$. Indeed, it is injective on $(T^{I_K})^\S/W_K$ because this module is isomorphic to $W_K^\S/T^{I_K}$ and Lenstra and Oort have shown, in [L-O], 1.6, that the integer one is not an eigenvalue of $\sigma$ restricted to $W_K^\S/T^{I_K}$. Therefore, in order to prove our proposition, we only need to prove the following lemma.

**Lemma 2.13.** *Let $Y$ be a free $\mathbb{Z}_\ell$-module of finite rank. Let $\sigma$ be an automorphism of $Y$ of finite order $r$, and such that*

$$\bar{Y} := Y/(\sigma - \mathrm{id})(Y) \quad \textit{is a finite group}.$$

*Then $r$ kills $\bar{Y}$ and*

$$\delta(\bar{Y}) \leqq \operatorname{rank}_{\mathbb{Z}_\ell}(Y^{\langle \sigma^{r_\ell} \rangle}),$$

*where the operator $\delta(\ )$ is defined as in* 1.2.

*Proof.* Write

$$\bar{Y} = \prod_{i=1}^{s} \mathbb{Z}/\ell^{a_i}\mathbb{Z}.$$

Let $x_i \in Y$ be such that its image $\bar{x}_i$ in $\bar{Y}$ generates the subgroup

$$\{0\} \times \ldots \times \mathbb{Z}/\ell^{a_i}\mathbb{Z} \times \ldots \times \{0\}.$$

Let $p_{x_i}(t) \in \mathbb{Q}_\ell[t]$ denote the minimal polynomial of

$$x_i \otimes 1 \in Y \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell .$$

Since the characteristic polynomial $\mathrm{char}(\sigma)(t)$ of $\sigma$ is monic with coefficients in $\mathbb{Z}_\ell$, we conclude that

$$p_{x_i}(t) \in \mathbb{Z}_\ell[t] .$$

Since $\overline{\sigma(x_i)} = \bar{x}_i$ in $\bar{Y}$, we find that

$$\overline{p_{x_i}(\sigma)(x_i)} = 0 = p_{x_i}(1)\,\bar{x}_i \quad \text{in} \quad \bar{Y} .$$

Note that

$$p_{x_i}(1) \neq 0 ,$$

because $p_{x_i}(t)$ divides $1 + t + \ldots + t^{r-1}$. Hence,

$$\ell^{a_i} \text{ divides } p_{x_i}(1) .$$

Let $\phi_n(t)$ denote the minimal polynomial over $\mathbb{Z}$ of a primitive $n$-th root of unity. Recall that

$$\phi_n(1) = \begin{cases} 1 & \text{if} \quad n \text{ is a composite integer,} \\ \ell & \text{if} \quad n = \ell^{\mathrm{ord}_\ell(n)} . \end{cases}$$

In particular, if $n$ is a composite integer and $f(t)$ is a factor of $\phi_n(t)$, then $f(1)$ is a unit in $\mathbb{Z}_\ell$. Recall also that $\phi_{\ell^c}(t)$ is irreducible in $\mathbb{Z}_\ell[t]$. Therefore, since $\ell^{a_i}$ divides $p_{x_i}(1)$, the polynomial $p_{x_i}(t)$ must be divisible by a product of at least $a_i$ polynomials of the form $\phi_{\ell^{b_{ij}}}(t)$, $j = 1, \ldots, a_i$. Since the polynomial $p_{x_i}(t)$ divides $t^r - 1$, the integers $b_{ij}$ must all be distinct. It follows that

$$\deg(p_{x_i}(t)) \geqq \sum_{i=1}^{a_i} (\ell^{b_{ij}} - \ell^{b_{ij}-1}) \geqq \ell^{a_i} - 1 .$$

Note that

$$\prod_{i=1}^{s} \ell^{a_i} = |\bar{Y}| = u \cdot \mathrm{char}(\sigma)(1), \quad \text{where } u \text{ is a unit in } \mathbb{Z}_\ell .$$

Therefore, $\mathrm{char}(\sigma)(t)$ is divisible by the product of exactly $\left(\sum_{i=1}^{s} a_i\right)$ polynomials of the form

$$\phi_{\ell^{c_k}}(t), \quad \text{with } k = 1, \ldots, \sum_{i=1}^{s} a_i .$$

Without loss of generality, we may assume that $c_j = b_{1j}$ for $j = 1, \ldots, a_1$. It is obvious that

$$\deg(\phi_{\ell^{c_k}}(t)) \geqq \ell - 1 \quad \text{if } k > a_1 .$$

Hence,

$$\mathrm{rank}_{\mathbb{Z}_\ell}(Y^{\langle \sigma^{r_\ell} \rangle}) = \mathrm{ord}_{(t-1)}(\mathrm{char}(\sigma^{r_\ell})(t)) \geqq (\ell^{a_1} - 1) + \Big(\sum_{j \neq 1} a_j\Big)(\ell - 1) .$$

This concludes the proof of our lemma and of Proposition 2.12. □

**Corollary 2.14.** *Let $K \subseteqq M \subseteqq L$ be any Galois extension. Fix a prime $\ell \neq p$. From the inclusions*

$$W_{\ell,K} \subseteqq (T_\ell^{I_M})^\perp \subseteqq W_{\ell,M}^\perp \subseteqq W_{\ell,K}^\perp,$$

*we obtain the subgroups*

$$s(W_K) \subseteqq s((T^{I_M})^\perp) \subseteqq s(W_M^\perp) \subseteqq F.$$

*Consider the exact sequence*:

$$0 \to s(W_M^\perp)/s((T^{I_M})^\perp) \to F/s((T^{I_M})^\perp) \to F/s(W_M^\perp) \to 0.$$

*The following properties hold*:

(1) $\delta(s(W_M^\perp)/s((T^{I_M})^\perp)) \leqq 2(a_{M \cap K_\ell} - a_K)$.

(2) *The group $F/s((T^{I_M})^\perp)$ is killed by $[M:K]$ and*

$$\delta(F/s((T^{I_M})^\perp)) \leqq 2(a_{M \cap K_\ell} - a_K) + t_{M \cap K_\ell} - t_K.$$

(3) *The group $F/s(W_M^\perp)$ is killed by $[M:K]$ and*

$$\delta(F/s(W_M^\perp)) \leqq t_{M \cap K_\ell} - t_K.$$

*Proof.* Let

$$U_1 := [W_{M_0}^\S \cap (T^{I_K})^\S]/(T^{I_{M_0}})^\S,$$

$$U_2 := (T^{I_K})^\S/(T^{I_{M_0}})^\S, \quad \text{and}$$

$$U_3 := (T^{I_K})^\S/[W_{M_0}^\S \cap (T^{I_K})^\S].$$

The Galois invariant pairing $\langle ; \rangle$ on $T^P \times T^P$ induces an isomorphism

$$T^{I_{M_0}} \cong T^P/(T^{I_{M_0}})^\S.$$

Since $\sigma$ acts as $T^{I_{M_0}}$ with finite order $[M_0 : K]$, it also acts on the modules $U_i, i = 1, 2, 3$, with finite order dividing $[M_0 : K]$. We may therefore apply Proposition 2.12. To compute the ranks of the modules $U_i^{\langle \sigma^{r_\ell} \rangle}$, we proceed as follows.

The module $U_1$ is isomorphic to the dual of the module

$$V_1 := T^{I_{M_0}}/[W_{M_0}^\S \cap (T^{I_K})^\S]^\S.$$

The module $U_2$ is isomorphic to the dual of the module

$$V_2 := T^{I_{M_0}}/T^{I_K}.$$

The module $U_3$ is isomorphic to the dual of the module

$$V_3 := [W_{M_0}^\S \cap (T^{I_K})^\S]^\S/T^{I_K}.$$

Note that

$$W_{M_0} + T^{I_K} \subseteqq [W^{\S}_{M_0} \cap (T^{I_K})^{\S}]^{\S}$$

is a subgroup of finite index. Therefore

$$\begin{aligned}\operatorname{rank}_{Z_\ell}(([W^{\S}_{M_0} \cap (T^{I_K})^{\S}]^{\S})^{\langle \sigma''_\ell \rangle}) &= \operatorname{rank}_{Z_\ell}((W_{M_0} + T^{I_K})^{\langle \sigma''_\ell \rangle}) \\ &= \operatorname{rank}_{Z_\ell}(W_{M_0 \cap K_\ell} + T^{I_K}) \\ &= \operatorname{rank}_{Z_\ell}(W_{M_0 \cap K_\ell}) + \operatorname{rank}_{Z_\ell}(T^{I_K}) - \operatorname{rank}_{Z_\ell}(W_K).\end{aligned}$$

Since the cohomology group $H^1(G, N)$ is finite if $G$ is a finite group and $N$ is a finitely generated module, we can write:

$$\begin{aligned}\operatorname{rank}_{Z_\ell}(V_1^{\langle \sigma''_\ell \rangle}) &= \operatorname{rank}_{Z_\ell}(T^{I_{M_0 \cap K_\ell}}) - \operatorname{rank}_{Z_\ell}(([W^{\S}_{M_0} \cap (T^{I_K})^{\S}]^{\S})^{\langle \sigma''_\ell \rangle}) \\ &= 2a_{M_0 \cap K_\ell} + t_{M_0 \cap K_\ell} - (t_{M_0 \cap K_\ell} + (2a_K + t_K) - t_K) \\ &= 2(a_{M_0 \cap K_\ell} - a_K).\end{aligned}$$

Similarly,

$$\begin{aligned}\operatorname{rank}_{Z_\ell}(V_2^{\langle \sigma''_\ell \rangle}) &= \operatorname{rank}_{Z_\ell}(T^{I_{M_0 \cap K_\ell}}) - \operatorname{rank}_{Z_\ell}(T^{I_K}) \\ &= 2(a_{M_0 \cap K_\ell} - a_K) + t_{M_0 \cap K_\ell} - t_K,\end{aligned}$$

and

$$\begin{aligned}\operatorname{rank}_{Z_\ell}(V_3^{\langle \sigma''_\ell \rangle}) &= \operatorname{rank}_{Z_\ell}([(W^{\S}_{M_0} \cap (T^{I_K})^{\S})^{\S}]^{\langle \sigma''_\ell \rangle}) - \operatorname{rank}_{Z_\ell}(T^{I_K}) \\ &= t_{M_0 \cap K_\ell} - t_K.\end{aligned}$$

This concludes the proof of our corollary. □

**Theorem 2.15.** *Let $A/K$ be an abelian variety. There exist three subgroups*

$$\Sigma_{K,\ell}(A) \subseteqq \Sigma^{[2]}_{K,\ell}(A) \subseteqq \Sigma^{[3]}_{K,\ell}(A)$$

*of the $\ell$-part $\Phi_{K,\ell}(A)$ of $\Phi_K(A)$, having the following properties:*

(i) *The subgroup $\Sigma_{K,\ell}(A)$ can be generated by $t_K$ elements.*

(ii) *The quotient $\Phi_{K,\ell}/\Sigma^{[2]}_{K,\ell}$ is killed by $[K_\ell : K]$ and*

$$\delta(\Phi_{K,\ell}/\Sigma^{[2]}_{K,\ell}) \leqq 2(a_{K_\ell} - a_K) + t_{K_\ell} - t_K.$$

*Moreover,*

- $\delta(\Phi_{K,\ell}/\Sigma^{[3]}_{K,\ell}) \leqq t_{K_\ell} - t_K$,
- $\delta(\Sigma^{[3]}_{K,\ell}/\Sigma^{[2]}_{K,\ell}) \leqq 2(a_{K_\ell} - a_K)$.

(iii) *The quotient $\Sigma^{[2]}_{K,\ell}/\Sigma_{K,\ell}$ is killed by $[K_\ell : K]$ and $\delta(\Sigma^{[2]}_{K,\ell}/\Sigma_{K,\ell}) \leqq t_{K_\ell} - t_K$.*

*Proof.* The subgroups mentioned in the statement of our theorem were introduced in Remark 2.9. Part (i) follows from Lemma 2.11. Part (ii) follows from Corollary 2.14, applied to the submodules $W_{\ell,K} \subseteqq (T_\ell^{I_L})^\perp \subseteqq W_{\ell,L}^\perp \subseteqq W_{\ell,K}^\perp$. Let us now prove part (iii). Note that $s(W_L) = s(W_L^P) = s(W_{L_0})$. We claim that $W_{\ell,K} \subseteqq W_{\ell,L_0}$ are two submodules that satisfy all the hypotheses of Proposition 2.12. Indeed, both modules are $\sigma_\ell$-invariant and, since $W_{\ell,L_0}$ is contained in $T^{I_{L_0}}$, it follows that $\sigma_\ell$ has finite order $r := [L_0 : K]$ when restricted to $W_{L_0}/W_K$. To compute the rank of $(W_{L_0}/W_K)^{\langle\sigma_\ell^{r_\ell}\rangle}$, we proceed as in the proof of Corollary 2.14 and find that

$$\mathrm{rank}_{\mathbb{Z}_\ell}((W_{L_0}/W_K)^{\langle\sigma_\ell^{r_\ell}\rangle}) = \mathrm{rank}_{\mathbb{Z}_\ell}(W_{K_\ell}) - \mathrm{rank}_{\mathbb{Z}_\ell}(W_K) = t_{K_\ell} - t_K .$$

This concludes the proof of Theorem 2.15. □

**Remark 2.16.** Let $X/K$ be a smooth proper geometrically connected curve having a $K$-rational point. Let $A/K$ denote the jacobian of $X/K$. Assume that $t_{K_\ell} = 0$ for all primes $\ell \neq p$. Note that this implies in particular that $t_K = 0$. Write

$$\Phi_{K,\ell} = \prod_{i=1}^{s(\ell)} \mathbb{Z}/\ell^{a_i}\mathbb{Z} .$$

It follows from the above corollary and from the following lemma that

$$\sum_{\ell \neq p} \delta(\Phi_{K,\ell}) \leqq \sum_{\ell \neq p} 2(a_{K_\ell} - a_K) \leqq 2u_K - 2u_{L_0} .$$

Theorem 3.6 in [Lor3] states that

$$\sum_{\ell \neq p} \left( \sum_{i=1}^{s(\ell)} (\ell^{a_i} - 1) \right) \leqq 2u_K .$$

In view of this theorem, it is natural to wonder whether Lemma 2.13 could be sharpened to state:

$$\sum_{i=1}^{s} (\ell^{a_i} - 1) \leqq \mathrm{rank}_{\mathbb{Z}_\ell}(Y^{\langle\sigma^{r_\ell}\rangle}) .$$

We have not been able to prove or disprove this bound. In case this sharper inequality were always true, we would define the quantity $\delta'(G_\ell)$, for any finite abelian group

$$G_\ell \cong \prod_{i=1}^{s} \mathbb{Z}/\ell^{a_i}\mathbb{Z} ,$$

to be:

$$\delta'(G_\ell) := \sum_{i=1}^{s} (\ell^{a_i} - 1) .$$

All the theorems stated in this paper would then remain true if $\delta(\ )$ were replaced by $\delta'(\ )$.

**Lemma 2.17.** *Let $A/K$ be any abelian variety. Then*

$$\sum_{\ell \neq p} (a_{K_\ell} - a_K) + (t_{K_\ell} - t_K) \leqq u_K - u_{L_0}.$$

*Proof.* Fix a prime $\ell$ and let $q \neq p$ denote any prime. Consider the inclusions

$$T_\ell^{I_K} \subseteqq T_\ell^{I_{K_q}} \subseteqq W_{\ell,K_q}^{\S} \subseteqq W_{\ell,K}^{\S}.$$

We know that

$$2(a_{K_q} - a_K) + 2(t_{K_q} - t_K) = \mathrm{rank}_{Z_\ell}(T_\ell^{I_{K_q}}/T_\ell^{I_K}) + \mathrm{rank}_{Z_\ell}(W_{\ell,K}^{\S}/W_{\ell,K_q}^{\S}).$$

Let $f_q(x)$ denote the characteristic polynomial of $\sigma_\ell$ acting on $T_\ell^{I_{K_q}}/T_\ell^{I_K} \oplus W_{\ell,K}^{\S}/W_{\ell,K_q}^{\S}$. For each prime $q$, the polynomial $f_q(x)$ is a product of cyclotomic polynomials of the form $\phi_{q^c}(x)$. The integer one is not an eigenvalue of $\sigma_\ell$ restricted to $W_{\ell,K}^{\S}/T_\ell^{I_K}$ (see for instance [L-O], 1.3). Hence, we conclude that the polynomials $f_q(x)$ are relatively prime and, therefore,

$$\prod_{q \neq p} f_q(x) \quad \text{divides} \quad \frac{\mathrm{char}(\sigma_\ell)(x)}{(x-1)^{2a_K + 2t_K}}.$$

Hence,

$$2\Big(\sum_{q \neq p} (a_{K_q} + t_{K_q} - a_K - t_K)\Big) \leqq \mathrm{rank}_{Z_\ell}(W_{\ell,K}^{\S}/T_\ell^{I_K}).$$

It follows from 2.6 that

$$\mathrm{rank}_{Z_\ell}(W_{\ell,K}^{\S}/T_\ell^{I_K}) = 2(u_K - u_{L_0}). \quad \square$$

## 3. A pairing attached to the group $\Phi_{K,\ell}$

Let us state now the main theorem of this paper.

**Theorem 3.1.** *Let $A/K$ be an abelian variety. Let $L/K$ denote the unique extension of $K$, minimal with the property that $A_L/L$ has semistable reduction. Let $\Phi_K(A)$ denote the group of components of the Néron model of $A/K$. Let $\ell \neq p$ be a prime. Assume that $A/K$ has a polarization of degree prime to $\ell$. Then there exists a subgroup $\Theta_{K,\ell}(A)$ of $\Phi_K(A)$ such that:*

(1) *The subgroup $\Theta_{K,\ell}(A)$ is functorial in the variable $A$ and does not depend on the choice of a polarization for $A$.*

(2) *The quotient $\Phi_{K,\ell}(A)/\Theta_{K,\ell}(A)$ is generated by $t_K$ elements.*

*Let $K \subseteqq M \subseteqq L$ be any Galois extension. There exist three subgroups*

$$\Theta_{K,M,\ell}^{[3]}(A) \subseteqq \Theta_{K,M,\ell}^{[2]}(A) \subseteqq \Theta_{K,M,\ell}^{[1]}(A) \subseteqq \Theta_{K,\ell}(A)$$

*such that:*

(3) *The subgroups $\Theta_{K,M,\ell}^{[i]}$ are functorial in the variable $A$ for $i = 1, 2, 3$, and do not depend on the choice of a polarization for $A$.*

(4) $\Theta^{[3]}_{K,M,\ell}$ *is killed by* $[M:K]$, *and* $\delta(\Theta^{[3]}_{K,M,\ell}) \leqq t_{M\cap K_\ell} - t_K$.

(5) $\Theta^{[2]}_{K,M,\ell}$ *is killed by* $[M:K]$, *and* $\delta(\Theta^{[2]}_{K,M,\ell}) \leqq 2(a_{M\cap K_\ell} - a_K) + (t_{M\cap K_\ell} - t_K)$.

(6) $\delta(\Theta^{[2]}_{K,M,\ell}/\Theta^{[3]}_{K,M,\ell}) \leqq 2(a_{M\cap K_\ell} - a_K)$.

*Moreover, the group* $\Phi_{K,\ell}(A)$ *is equipped with a nondegenerate pairing*

$$(\,;\,): \Phi_{K,\ell}(A) \times \Phi_{K,\ell}(A) \;\to\; \mathbb{Q}_\ell/\mathbb{Z}_\ell$$

*that restricts to a nondegenerate pairing*

$$(\,;\,): \Theta_{K,\ell}(A) \times \Theta_{K,\ell}(A) \;\to\; \mathbb{Q}_\ell/\mathbb{Z}_\ell\,.$$

(7) *The group* $\Theta^{[1]}_{K,M,\ell}(A)$ *is the orthogonal in* $\Theta_{K,\ell}(A)$, *under the above pairing, of the group* $\Theta^{[3]}_{K,M,\ell}(A)$. *In particular,*

(8) *The groups* $\Theta^{[3]}_{K,M,\ell}$ *and* $\Theta_{K,\ell}/\Theta^{[1]}_{K,M,\ell}$ *are isomorphic.*

*The natural map* $\gamma_{K,M}: \Phi_K \to \Phi_M$ *does not induce, in general, a map from* $\Theta_{K,\ell}$ *to* $\Theta_{M,\ell}$. *However,*

(9) $\gamma_{K,M}(\Theta^{[1]}_{K,M,\ell}) \subseteqq \Theta_{M,\ell}$.

(10) *The subgroup* $\Theta^{[2]}_{K,M,\ell}$ *is equal to the* $\ell$-*part* $\Psi_{K,M,\ell}$ *of the kernel of* $\gamma_{K,M}$. *In particular, the group* $\Theta^{[1]}_{K,M,\ell}/\Theta^{[2]}_{K,M,\ell}$ *injects into the group* $\Theta_{M,\ell}$.

(11) *When* $M = L$, *the groups* $\Theta^{[2]}_{K,M,\ell}$ *and* $\Theta^{[1]}_{K,M,\ell}$ *are equal. We therefore obtain a bound for the order of* $\Theta_{K,\ell}$ *in the form of:*

- $\delta(\Theta_{K,\ell}/\Psi_{K,L,\ell}) + \delta(\Psi_{K,L,\ell}) \leqq 2(a_{K_\ell} - a_K) + 2(t_{K_\ell} - t_K)$, *and*
- $\Theta_{K,\ell}$ *is killed by* $[K_\ell : K]^2$.

Most of this section will be devoted to proving the above theorem. Fix a prime $\ell$, $\ell \neq p$. Let

$$\mathbb{D}_\ell := \mathbb{Q}_\ell/\mathbb{Z}_\ell\,.$$

Define

$$E := \frac{(T_\ell \otimes \mathbb{D}_\ell)^{I_K}}{T_\ell^{I_K} \otimes \mathbb{D}_\ell}\,.$$

Recall that Grothendieck, [Gro], IX, 11.2, constructed a functorial isomorphism

$$\phi_{K,\ell}: \Phi_{K,\ell} \;\to\; E\,.$$

Let

$$F := \text{torsion subgroup of } \frac{T_\ell^P}{(\sigma - \mathrm{id})(T_\ell^P)}\,.$$

We showed in 2.1 that the groups $E$ and $F$ are isomorphic. Given the submodules

$$W_K \subseteqq W_M \subseteqq (T_\ell^{I_M})^\perp \subseteqq W_M^\perp \subseteqq W_K^\perp ,$$

we can define as in 2.4 the subgroups:

$$s(W_K) \subseteqq s(W_M) \subseteqq s((T^{I_M})^\perp) \subseteqq s(W_M^\perp) \subseteqq F .$$

We will show below the existence of a pairing

$$( \,;\, ) : E \times F \to \mathbb{D}_\ell .$$

Denote by $H^\#$ the orthogonal under $( \,;\, )$ of a subgroup $H$ of $F$. We will define the subgroups $\Theta_{K,\ell}$ and $\Theta^{[i]}_{K,M,\ell}$ for $i = 1,2,3$, in 3.8. When the pairing on $E \times F$ is perfect, we will show in 3.11 that

$$\begin{aligned} \phi_{K,\ell}(\Theta_{K,\ell}) &= s(W_K)^\# , \\ \phi_{K,\ell}(\Theta^{[1]}_{K,M,\ell}) &= s(W_M)^\# , \\ \phi_{K,\ell}(\Theta^{[2]}_{K,M,\ell}) &= s((T^{I_M})^\perp)^\# , \quad \text{and} \\ \phi_{K,\ell}(\Theta^{[3]}_{K,M,\ell}) &= s(W_M^\perp)^\# . \end{aligned}$$

Therefore, when the pairing on $E \times F$ is perfect, part (2) of Theorem 3.1 follows from 2.11. Parts (4), (5), and (6) follow from 2.14. Part (11) follows from the definitions and from parts (4), (5), and (8).

**3.2. Existence of a pairing on $\Phi_{K,\ell}$.** We define a pairing

$$( \,;\, ) : E \times F \to \mathbb{D}_\ell$$

as follows. If $x \in E$, let $\tilde{x}$ denote a preimage of $x$ under the natural map

$$T_\ell^P \otimes \mathbb{Q}_\ell \to (T_\ell \otimes \mathbb{D}_\ell)^P .$$

If $y \in F$, let $\tilde{y}$ denote a preimage of $y$ under the natural map

$$(T_\ell^{I_K})^\S \to (T_\ell^{I_K})^\S / (\sigma_\ell - \mathrm{id})(T_\ell^P) .$$

Choose a polarization on $A$ and denote by $\langle ; \rangle$ the associated pairing on $T_\ell^P \times T_\ell^P$. The pairing $\langle ; \rangle : T_\ell^P \times T_\ell^P \to \mathbb{Z}_\ell$ extends to a pairing

$$\langle ; \rangle : (T_\ell^P \otimes \mathbb{Q}_\ell) \times (T_\ell^P \otimes \mathbb{Q}_\ell) \to \mathbb{Q}_\ell .$$

We define

$$(x; y) \in \mathbb{Q}_\ell / \mathbb{Z}_\ell$$

to be the image of $\langle \tilde{x}, \tilde{y} \rangle$ under the natural map $\mathbb{Q}_\ell \to \mathbb{Q}_\ell / \mathbb{Z}_\ell$. It is clear that

$$\langle \tilde{x} + z; \tilde{y} \rangle = \langle \tilde{x}, \tilde{y} \rangle \quad \text{if} \quad z \in T_\ell^{I_K} \otimes \mathbb{Q}_\ell .$$

To check that

$$\langle \tilde{x}, \tilde{y} + z \rangle \in \mathbb{Z}_\ell \quad \text{if} \quad z \in (\sigma_\ell - \mathrm{id})(T_\ell^P),$$

we need the following description of $(T_\ell \otimes \mathbb{D}_\ell)^{I_K}$.

**3.3.** Any element $z$ in $T_\ell A$ can be written as

$$z := \{z_i\}_{i=1}^{\infty},$$

where $z_i$ is a point of order $\ell^i$ in $A(\bar{K})$, and $z_i = \ell z_{i+1}$ for all $i \in \mathbb{N}$. Let $X \subset T_\ell$ be any $I_K$-invariant submodule such that $T_\ell/X$ is torsion free. Let

$$\alpha(X) := \{x \in A(K) \mid \exists \{x_i\}_{i=1}^{\infty} \in X \text{ and } j \in \mathbb{N} \text{ such that } x = x_j\}.$$

**Lemma 3.4.** *The set $\alpha(X)$ is a subgroup of $A(K)$ isomorphic to $(X \otimes \mathbb{D}_\ell)^{I_K}$.*

*Proof.* Let $x, y \in \alpha(X)$. Let $\{x_i\}_{i=1}^{\infty} \in X$ be such that there exists $j \in \mathbb{N}$ with $x = x_j$. Similarily, let $\{y_i\}_{i=1}^{\infty}$ be such that there exists $k \in \mathbb{N}$ with $y = y_k$. We may assume without loss of generality that $k \leq j$. Then

$$x + y \in \alpha(X)$$

because

$$x + y = z_j,$$

where

$$\{z_i\}_{i=1}^{\infty} := \{x_i\}_{i=1}^{\infty} + \ell^{j-k}\{y_i\}_{i=1}^{\infty} \in X.$$

We define a map

$$f: \alpha(X) \to (X \otimes \mathbb{D}_\ell)^{I_K}$$

as follows. If $x \in \alpha(X)$, let $\{x_i\}_{i=1}^{\infty}$ be such that $x = x_j$ for some $j \in \mathbb{N}$. Then set

$$f(x) := \{x_i\}_{i=1}^{\infty} \otimes \ell^{-j}.$$

Let us first check that $f(x) \in (X \otimes \mathbb{D}_\ell)^{I_K}$. Since $\sigma(x_j) = x_j$ for all $\sigma \in I_K$,

$$\{x_i\}_{i=1}^{\infty} - \sigma(\{x_i\}_{i=1}^{\infty}) \text{ is divisible by } \ell^j \text{ in } T,$$

and hence, is also divisible by $\ell^j$ in $X$ because $T/X$ is free. Let

$$\{y_i\}_{i=1}^{\infty} := \ell^{-j}(\{x_i\} - \sigma(\{x_i\})), \quad \text{with } \{y_i\}_{i=1}^{\infty} \in X.$$

Then

$$[\{x_i\} - \sigma(\{x_i\})] \otimes \ell^{-j} = (\ell^j\{y_i\}) \otimes \ell^{-j} = 0,$$

which shows that

$$\{x_i\}_{i=1}^{\infty} \otimes \ell^{-j} \quad \text{is fixed by } I_K.$$

To show that the map $f$ is well defined, we let $\{x_i\}_{i=1}^{\infty} \in X$ be such that $x = x_j$ for some $j$ and we let $\{y_i\}_{i=1}^{\infty}$ be such that $y_k = x$ for some $k$. Without loss of generality, we may assume that $j \geqq k$. Then,

$$\{x_i\} - \ell^{j-k}\{y_i\} \quad \text{is divisible by } \ell^j \text{ in } X.$$

Hence,

$$[\{x_i\} \otimes \ell^{-j}] - [\{y_i\} \otimes \ell^{-k}] = 0 \quad \text{in } X \otimes \mathbb{D}_\ell.$$

We leave it to the reader to check that the map is an isomorphism, recalling only that $\{x_i\} \otimes \ell^{-j} = 0$ in $X \otimes \mathbb{D}_\ell$ if and only if $\{x_i\} = \ell^j\{y_i\}$ for some $\{y_i\} \in X$. This concludes the proof of Lemma 3.4. □

**3.5.** Let $x \in (T_\ell \otimes \mathbb{D}_\ell)^{I_K}$. We claim that we may assume that there exists a lift

$$\tilde{x} \in T_\ell^P \otimes \mathbb{Q}_\ell$$

of $x$ of the form

$$\{x_i\}_{i=1}^{\infty} \otimes \ell^{-j}, \quad \text{with} \quad \{x_i\} \in T_\ell^P \quad \text{and} \quad x_j = x.$$

Indeed, by the above lemma, we can find a lift of $x$ in $T_\ell \otimes \mathbb{Q}_\ell$ of the form $\{z_i\} \otimes \ell^{-j}$, with $z_j = x$. Applying the averaging map

$$S : T_\ell \to T_\ell^P,$$

$$v \to \frac{1}{|P_0|} \sum_{\sigma \in P_0} \sigma(v)$$

to $\{z_i\}$, we obtain a lift of $x$ in $T_\ell^P \otimes \mathbb{Q}_\ell$:

$$\tilde{x} := S(\{z_i\}) \otimes \ell^{-j}, \quad \text{with} \quad x = (S(\{z_i\}))_j.$$

**3.6.** Let us now conclude the proof of the existence of the pairing ( ; ). Let $x \in (T_\ell \otimes \mathbb{D}_\ell)^{I_K}$ and choose

$$\tilde{x} \in T_\ell^P \otimes \mathbb{Q}_\ell$$

such that $\tilde{x} = \{x_i\}_{i=1}^{\infty} \otimes \ell^{-j}$ with $x_j \in A(K)$ and $x_j$ mapping to $x$ under the isomorphism of $\alpha(T_\ell)$ with $(T_\ell \otimes \mathbb{D}_\ell)^{I_K}$. Note that, since $\{x_i\}_{i=1}^{\infty} \otimes \ell^{-j} = \tilde{x}$ is such that $x_j \in A(K)$,

$$(\sigma_\ell^{-1} - \mathrm{id})(\{x_i\}) \quad \text{is divisible by } \ell^j \text{ in } T_\ell^P.$$

Write then $(\sigma_\ell^{-1} - \mathrm{id})(\{x_i\}) = \ell^j\{y_i\}$ for some $\{y_i\} \in T_\ell^P$. Let $z := (\sigma_\ell - \mathrm{id})(u)$ be any element of $(\sigma_\ell - \mathrm{id})(T_\ell^P)$. Then

$$\begin{aligned} \langle \tilde{x}, z \rangle &= \langle (\sigma_\ell^{-1} - \mathrm{id})(\tilde{x}), u \rangle \\ &= \langle \ell^j\{y_i\} \otimes \ell^{-j}, u \rangle \\ &= \langle \{y_i\}, u \rangle \\ &\in \mathbb{Z}_\ell \end{aligned}$$

because both $u$ and $\{y_i\}$ are in $T_\ell^P$. This shows that the pairing ( ; ) is well defined.

Lemma 2.3 shows that $F$ does not depend on the choice of a generator $\sigma$ of $I_K/P$. It is then easy to check that the pairing

$$(\,;\,): E \times F \to \mathbb{D}_\ell$$

also does not depend on the choice of a generator. □

**Remark 3.7.** Let $\Phi'_{K,\ell}$ denote the group of components of the abelian variety dual to $A$. In [Gro], IX, 1.2 and in IX, 11.3, Grothendieck defines two pairings between $\Phi_{K,\ell}$ and $\Phi'_{K,\ell}$. We do not know how Grothendieck's pairings relate to the pairing $(\,;\,)$ introducted in this section. Grothendieck conjectured that the pairing that he defined in IX, 1.2, was perfect. This was proved by Artin and Mazur (see for instance [McC 3], Theorem 4.8).

**3.8.** Given a submodule $X \subseteq T_\ell$, let

$$f_X : X \otimes \mathbb{Q}_\ell \to T_\ell \otimes \mathbb{D}_\ell$$

denote the natural map. We denote by $t(X)$ the subgroup of $E$ generated by the elements $x \in (T_\ell \otimes \mathbb{D}_\ell)^{I_K}$ such that there exists $\tilde{x} \in X \otimes \mathbb{Q}_\ell$ with $f_X(\tilde{x}) = x$. It follows from 3.5 that $t(X) = t(X^P)$.

Note that if $Y \subseteq X$ is such that $X/Y$ is finite, then

$$t(Y) = t(X)\,.$$

Note also that, for any submodule $X$,

$$t(X) = t(X + T^{I_K})\,.$$

We define the subgroups $\Theta_{K,\ell}$ and $\Theta^{[i]}_{K,M,\ell}$, $i = 1, 2, 3$, as follows:

$$\phi_{K,\ell}(\Theta_{K,\ell}) := t\big((\sigma - \mathrm{id})(T_\ell^P)\big)\,,$$

$$\phi_{K,\ell}(\Theta^{[1]}_{K,M,\ell}) := t\big(T_\ell^{I_M} + (\sigma^{[M_0:K]} - \mathrm{id})(T_\ell^P)\big)\,,$$

$$\phi_{K,\ell}(\Theta^{[2]}_{K,M,\ell}) := t(T_\ell^{I_M}), \quad \text{and}$$

$$\phi_{K,\ell}(\Theta^{[3]}_{K,M,\ell}) := t(W_{\ell,M})\,.$$

It follows from these definitions that the subgroups $\Theta_{K,\ell}(A)$ and $\Theta^{[i]}_{K,M,\ell}(A)$, for $i = 1, 2, 3$, do not depend on the choice of a polarization of $A$. Lemma 2.3 shows that these subgroups do not depend on the choice of a generator $\sigma$. It is clear that these subgroups are functorial in the variable $A$. Therefore, parts (1) and (3) of Theorem 3.1 hold.

Let us note that

$$\phi_{K,\ell}(\Theta_{K,\ell}) := t\big((\sigma - \mathrm{id})(T_\ell^P)\big) = t(W^{\S}_{\ell,K})\,,$$

since the module $T_\ell^{I_K} + (\sigma - \mathrm{id})(T_\ell^P)$ has finite index in $W_{\ell,K}^{\S}$. Similarly,

$$\phi_{K,\ell}(\Theta_{K,M,\ell}^{[1]}) := t(T_\ell^{I_M} + (\sigma^{[M_0:K]} - \mathrm{id})(T_\ell^P)) = t(W_{\ell,M}^{\S}) .$$

Therefore, we find the following inclusions:

$$\Theta_{K,M,\ell}^{[3]}(A) \subseteqq \Theta_{K,M,\ell}^{[2]}(A) \subseteqq \Theta_{K,M,\ell}^{[1]}(A) \subseteqq \Theta_{K,\ell}(A) .$$

Proposition 3.11 below describes the orthogonals of the groups $\Theta_{K,M,\ell}^{[i]}(A)$, $i = 1, 2, 3$, and of the group $\Theta_{K,\ell}(A)$ under the pairing ( ; ) constructed above, provided that $A$ has a polarization of degree prime to $\ell$.

**3.9.** The groups $E$ and $F$ are finite and isomorphic. Therefore, in order to show that the pairing

$$( \, ; \,) : E \times F \to \mathbb{Q}_\ell/\mathbb{Z}_\ell$$

is perfect, we need only to show that the induced map

$$E \to \mathrm{Hom}(F, \mathbb{Q}_\ell/\mathbb{Z}_\ell)$$

is injective or, equivalently, that the orthogonal of $F$ in $E$ under ( ; ) is trivial. This will be shown in Proposition 3.11, after a preparatory lemma. Let

$$\pi_n : T_\ell \to T_\ell/\ell^n T_\ell = A[\ell^n](\bar{K})$$

denote the natural quotient map. The pairing

$$e_n : A[\ell^n](\bar{K}) \times A[\ell^n](\bar{K}) \to \mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell$$

induced by $\langle ; \rangle$ is perfect when the polarization used to define the pairing on $T_\ell \times T_\ell$ has degree prime to $\ell$. We claim that the pairing

$$e_{n,P} : \pi_n(T_\ell^P) \times \pi_n(T_\ell^P) \to \mathbb{Z}/\ell^n\mathbb{Z}$$

is also perfect. Indeed, let $\bar{x} \in \pi_n(T_\ell^P)$ and $x \in T_\ell^P$ such that $\pi_n(x) = \bar{x}$. Since the pairing $e_n$ is perfect, there exists $y \in T_\ell$ such that

$$e_n(\bar{x}, \pi_n(y)) \neq 0 .$$

Hence,

$$\langle x, y \rangle \notin \ell^n \mathbb{Z}_\ell .$$

Therefore,

$$\langle x, S(y) \rangle = \frac{1}{|P_0|} \sum_{\sigma \in P_0} \langle \sigma(x), \sigma(y) \rangle = \langle x, y \rangle \notin \ell^n \mathbb{Z}_\ell .$$

Hence,

$$e_{n,P}(\bar{x}, \pi_n(S(y))) \neq 0, \quad \text{with} \quad \pi_n(S(y)) \in \pi_n(T_\ell^P) .$$

**Lemma 3.10.** *Let $X \subset T^P$ be any submodule. The group $\pi_n(X^\S)$ is the orthogonal of the group $\pi_n(X)$ under the pairing $e_{n,P}$.*

*Proof.* Since $X^\S$ is orthogonal to $X$ under $\langle ; \rangle$, it is clear that the orthogonal of $\pi_n(X)$ under $e_{n,P}$ contains $\pi_n(X^\S)$. This inclusion is an equality because both groups have the same order. Indeed, $\pi_n(X^\S)$ has order $(\ell^n)^{\mathrm{rank}(X^\S)}$ and the orthogonal of $\pi_n(X)$ has order $(\ell^n)^{\mathrm{rank}(T^P)-\mathrm{rank}(X)}$. □

**Proposition 3.11.** *Let $X$ be an $I_K$-invariant submodule of $T_\ell$ such that $T_\ell/X$ is free. Then $t(X^\perp)$ is the orthogonal of $s(X)$ under the pairing $( ; )$ on $E \times F$. In particular, the pairing $( ; )$ is perfect.*

*Proof.* Let $H^\# \subset E$ denote the orthogonal of a subgroup $H \subset F$ under the pairing $( ; ): E \times F \to \mathbb{Q}_\ell/\mathbb{Z}_\ell$. It is easy to check that

$$t(X^\perp) \subseteq s(X)^\# .$$

To prove the reverse inclusion, let $x \in s(X)^\#$. By assumption,

$$\langle \tilde{x}, \tilde{y} \rangle \in \mathbb{Z}_\ell$$

for all lifts $\tilde{x} = \{x_i\} \otimes \ell^{-j} \in T_\ell^P \otimes \mathbb{Q}_\ell$ with $x = x_j$, and for all elements $\tilde{y} \in X^P \cap (T_\ell^{I_K})^\S$. We claim that we can find a lift $\tilde{x}$ with $\{x_i\} \in [X^P \cap (T^{I_K})^\S]^\S$. Indeed,

$$e_{j,P}(\pi_j(\tilde{x}), \pi_j(\tilde{y})) = 0$$

for all $\tilde{y} \in X^P \cap (T^{I_K})^\S$. Therefore, $\pi_j(\tilde{x})$ is in the orthogonal of $\pi_j(X^P \cap (T^{I_K})^\S)$ under $e_{j,P}$, which was shown in 3.10 to be equal to $\pi_j([X^P \cap (T^{I_K})^\S]^\S)$.

Note now that

$$(X^P)^\S + T^{I_K} \subseteq [X^P \cap (T^{I_K})^\S]^\S$$

is a subgroup of finite index. Therefore, the image in $T_\ell^P \otimes \mathbb{D}_\ell$ of

$$[(X^P)^\S + T^{I_K}] \otimes \mathbb{Q}_\ell$$

is equal to the image of

$$[X^P \cap (T^{I_K})^\S]^\S \otimes \mathbb{Q}_\ell .$$

Therefore, we can find two elements

$$\tilde{z} = \{z_i\} \otimes \ell^{-a} \quad \text{with } \{z_i\} \in (X^P)^\S ,$$

and

$$\tilde{y} = \{y_i\} \otimes \ell^{-b} \quad \text{with } \{y_i\} \in T_\ell^{I_K}$$

such that

$$\tilde{x} = \tilde{z} + \tilde{y} \quad \text{in} \quad T_\ell \otimes \mathbb{D}_\ell .$$

Since the image of both $\tilde{x}$ and $\tilde{y}$ in $T_\ell \otimes \mathbb{D}_\ell$ are in $(T_\ell \otimes \mathbb{D}_\ell)^{I_K}$, it follows that the image of $\tilde{z}$ in $T_\ell \otimes \mathbb{D}_\ell$ is in $((X^P)^\S \otimes \mathbb{D}_\ell)^{I_K}$. Since $\tilde{x}$ and $\tilde{z}$ map to the same element in $E$, we conclude that

$$x \in t((X^P)^\S) = t(X^\perp). \quad \square$$

**3.12.** Fix a generator $\sigma$ of $I/P$. Let $\partial_\sigma : E \to F$ denote the isomorphism described in 2.1 and let

$$(\ ;\ )_\sigma : E \times E \to \mathbb{Q}_\ell/\mathbb{Z}_\ell$$

be defined by

$$(x, y)_\sigma := (x, \partial_\sigma(y)).$$

**Proposition 3.13.** *The pairing* $(\ ;\ )_\sigma : E \times E \to \mathbb{Q}_\ell/\mathbb{Z}_\ell$ *restricts to a nondegenerate pairing*

$$(\ ;\ )_\sigma : t(W_K^\perp) \times t(W_K^\perp).$$

*If* $W_K \subseteq X \subseteq W_K^\perp$ *is any* $I_K$*-invariant submodule such that* $W_K^\perp/X$ *is free, then the orthogonal of* $t(X)$ *in* $t(W_K^\perp)$ *under the pairing* $(\ ;\ )_\sigma$ *is equal to the subgroup* $t(X^\perp)$.

**Corollary 3.14** (Parts (7) and (8) of 3.1). *The group* $\Theta_{K,M,\ell}^{[1]}$ *is the orthogonal in* $\Theta_{K,\ell}$ *of the group* $\Theta_{K,M,\ell}^{[3]}$.

*Proof.* Recall that $W_K \subseteq W_M \subseteq W_M^\perp \subseteq W_K^\perp$. Recall also that

$$\phi_{K,\ell}(\Theta_{K,M,\ell}^{[1]}) = t(W_{\ell,M}^\perp),$$

and

$$\phi_{K,\ell}(\Theta_{K,M,\ell}^{[3]}) = t(W_{\ell,M}).$$

Hence, the corollary follows immediately from Proposition 3.13. $\square$

*Proof of Proposition* 3.13. The fact that the restricted pairing is nondegenerate follows from the fact that the orthogonal of $t(W_{\ell,K}^\perp)$ is equal to $t(W_{\ell,K})$, and that $t(W_{\ell,K}) = \{0\}$. To prove that the orthogonal of $t(X)$ in $t(W_K^\perp)$ under the pairing $(\ ;\ )_\sigma$ is equal to the subgroup $t(X^\perp)$, we need the following lemmas.

**Lemma 3.15.** *The subgroup* $X^{I_K} + (\sigma - 1)(X^P)$ *has finite index in* $X^P$. *Equivalently,*

$$X^{I_K} \cap (\sigma - 1)(X^P) = \{0\}.$$

*Proof.* Let $y \in X^P$ be such that $(\sigma - 1)(y) \in X^{I_K}$. It follows that

$$(\sigma - 1)^2(y) = 0.$$

In [L-O], 1.3, it is shown that the integer one is not an eigenvalue of $\sigma$ restricted to $W_K^\S/T^{I_K}$. Hence, since $X^P \subseteq W_K^\S$,

$$(\sigma - 1)(y) = 0,$$

and, therefore,

$$X^{I_K} \cap (\sigma - 1)(X^P) = \{0\}.$$

Our lemma follows because

$$\operatorname{rank}(X^{I_K}) + \operatorname{rank}(\sigma - 1)(X^P) = \operatorname{rank}(X^P). \quad \square$$

**Lemma 3.16.** *The subgroup $W_K + [(\sigma - 1)(X^P)]^{\S\S}$ has finite index in $X^P \cap (T^{I_K})^{\S}$.*

*Proof.* Since $W_K \subseteqq X$,

$$W_K = X^{I_K} \cap (T^{I_K})^{\S}.$$

Since $(\sigma - 1)(X^P) \subseteqq (T^{I_K})^{\S}$, it follows that

$$W_K + (\sigma - 1)(X^P) = [X^{I_K} + (\sigma - 1)(X^P)] \cap (T^{I_K})^{\S}.$$

It therefore follows from the previous lemma that $W_K + (\sigma - 1)(X^P)$ has finite index in $X^P \cap (T^{I_K})^{\S}$. Since $T^P/X^P$ is free, we have $X^P = (X^P)^{\S\S}$ and, therefore,

$$[(\sigma - 1)(X^P)]^{\S\S} \subseteqq (X^P)^{\S\S} \cap (T^{I_K})^{\S\S\S} = X^P \cap (T^{I_K})^{\S}.$$

Hence, our lemma follows. $\square$

**3.17.** We are now ready to begin the proof of 3.13. It is clear that $t(X^{\perp})$ is contained in the orthogonal of $t(X)$ under $(\,;\,)_\sigma$. We therefore need only to prove the reverse inclusion. Let $\lambda \in t(W_K^{\S})$ be such that

$$(\zeta, \partial_\sigma(\lambda)) = 0 \quad \text{for all} \quad \zeta \in t(X).$$

Since $\lambda \in t(W_K^{\S})$, we can find a lift $\tilde{z}$ of $\lambda$ in $T_\ell^P \otimes \mathbb{Q}_\ell$ of the form

$$\tilde{z} = z \otimes \ell^{-j} \quad \text{with} \quad z \in W_K^{\S}.$$

**Lemma 3.18.** *Let $\tilde{z} = z \otimes \ell^{-j}$ be as above. Then*

$$\langle y, z \rangle \in \ell^j \mathbb{Z}_\ell \quad \textit{for all} \quad y \in [(\sigma - 1)(X^P)]^{\S\S}.$$

*Proof.* Recall that, if $Y$ is any submodule of $T^P$, then

$$Y^{\S\S} = \{y \in T^P \mid \exists\, m \in \mathbb{N} \quad \text{with } \ell^m y \in Y\}.$$

Let $y \in [(\sigma - 1)(X^P)]^{\S\S}$. Let $m \in \mathbb{N}$ and $x \in X^P$ such that

$$\ell^m y = (\sigma^{-1} - 1)(x).$$

This equality shows that the image of the element

$$x \otimes \ell^{-m} \in T_\ell^P \otimes \mathbb{Q}_\ell$$

in $T_\ell^P \otimes \mathbb{D}_\ell$ is $I_K$-invariant. Hence, $x \otimes \ell^{-m}$ defines an element $\zeta \in t(X)$. Therefore,

$$\begin{aligned}(\zeta, \lambda)_\sigma &= \langle x \otimes \ell^{-m}, (\sigma - 1)(\tilde{z})\rangle \bmod \mathbb{Z}^\ell \\ &= \langle (\sigma^{-1} - 1)(x) \otimes \ell^{-m}, \tilde{z}\rangle \\ &= \langle y \otimes 1, z \otimes \ell^{-j}\rangle .\end{aligned}$$

But, by hypothesis,

$$(\zeta, \lambda)_\sigma = 0 \quad \text{in } \mathbb{D}_\ell .$$

Hence, $\langle y; z\rangle \in \ell^j \mathbb{Z}_\ell$. □

Let $e_{j,P}$ denote the pairing induced by $\langle ; \rangle$ on $\pi_j(T^P) \times \pi_j(T^P)$. Lemma 3.18 shows that $\pi_j(z)$ belongs to the orthogonal of the group $\pi_j((\sigma - 1)(X^P)^{\S\S})$. It follows from Lemma 3.10 that

$$\pi_j(z) \in \pi_j((\sigma - 1)(X^P)^{\S\S\S}) = \pi_j((\sigma - 1)(X^P)^{\S}) .$$

Since, by construction, $\pi_j(z) \in \pi_j(W_K^{\S})$, it follows that

$$\pi_j(z) \in \pi_j(W_K^{\S}) \cap \pi_j((\sigma - 1)(X^P)^{\S}) .$$

**Lemma 3.19.** $\pi_j(z) \in \pi_j([W_K + (\sigma - 1)(X^P)^{\S\S}]^{\S})$.

*Proof.* Let $G$ be any group endowed with a perfect pairing. Let $A^*$ denote the orthogonal of $A$ under this pairing. Recall that, if $A = A^{**}$ and $B = B^{**}$ and

$$A^* + B^* = (A^* + B^*)^{**} ,$$

then

$$(A \cap B)^* = A^* + B^* .$$

This last equality always holds when $G$ is finite. Hence, using this fact and Lemma 3.10, we conclude that:

$$\begin{aligned}[\pi_j(W_K^{\S}) \cap \pi_j((\sigma - 1)(X^P)^{\S})]^* &= \pi_j(W_K) + \pi_j((\sigma - 1)(X^P)^{\S\S}) \\ &= \pi_j(W_K + (\sigma - 1)(X^P)^{\S\S}) .\end{aligned}$$

The last equality comes from the fact that $\pi_j$ is linear. Taking the orthogonals of these groups and using Lemma 3.10 again proves our lemma. □

It follows from Lemma 3.19 that

$$z \otimes \ell^{-j} \quad \text{defines an element in} \quad t([W_K + (\sigma - 1)(X^P)^{\S\S}]^{\S}) .$$

Lemma 3.16 shows that $W_K + (\sigma - 1)(X^P)^{\S\S}$ has finite index in $X \cap (T^{I_K})^{\S}$. Recall that, if $Y$ and $Z$ are two submodules of $T_\ell$ such that $Y \subseteq Z$ and $Z/Y$ is finite, then $Y^{\S} = Z^{\S}$. Therefore, we find that

$$t([W_K + (\sigma - 1)(X^P)^{\S\S}]^{\S}) = t([X \cap (T^{I_K})^{\S}]^{\S}) .$$

Recall also that if $Y$ and $Z$ are any submodules of $T_\ell$, then

$$Y^{\S} + Z^{\S} \subseteq [Y \cap Z]^{\S} \text{ is a submodule of finite index}.$$

Therefore, as noted in 3.8, we find that

$$t([X \cap (T^{I_K})^{\S}]^{\S}) = t(X^{\S} + T^{I_K}) = t(X^{\S}).$$

Since $z \otimes \ell^{-j}$ is a lift of $\lambda$, it follows that $\lambda \in t(X^{\S})$. □

**3.20. Proof of parts (9) and (10) of 3.1.** The natural isomorphism

$$\phi_{K,\ell}: \Phi_{K,\ell} \to \frac{(T_\ell \otimes \mathbb{D}_\ell)^{I_K}}{T_\ell^{I_K} \otimes \mathbb{D}_\ell}$$

is functorial in the following sense. Any extension $M/K$ induces a map of Néron models

$$(\mathscr{A}_K)_{\mathcal{O}_M} \to \mathscr{A}_M.$$

This map induces, in turn, a map

$$\gamma_{K,M,\ell}: \Phi_{K,\ell} \to \Phi_{M,\ell}.$$

The natural map

$$\xi_{K,M,\ell}: (T_\ell \otimes \mathbb{D}_\ell)^{I_K}/(T_\ell^{I_K} \otimes \mathbb{D}_\ell) \to (T_\ell \otimes \mathbb{D}_\ell)^{I_M}/(T_\ell^{I_M} \otimes \mathbb{D}_\ell),$$

induced by the inclusion

$$(T_\ell \otimes \mathbb{D}_\ell)^{I_K} \to (T_\ell \otimes \mathbb{D}_\ell)^{I_M}$$

coming from the inclusion

$$A(K) \subseteq A(M),$$

is such that the following diagram is commutative:

$$\begin{array}{ccc} \Phi_{K,\ell} & \xrightarrow{\gamma_{K,M,\ell}} & \Phi_{M,\ell} \\ \downarrow{\scriptstyle \phi_{K,\ell}} & & \downarrow{\scriptstyle \phi_{M,\ell}} \\ (T_\ell \otimes \mathbb{D}_\ell)^{I_K}/(T_\ell^{I_K} \otimes \mathbb{D}_\ell) & \xrightarrow{\xi_{K,M,\ell}} & (T_\ell \otimes \mathbb{D}_\ell)^{I_M}/(T_\ell^{I_M} \otimes \mathbb{D}_\ell). \end{array}$$

Let $X \subseteq T_\ell$ be any submodule. Let

$$t_K(X) := \text{subgroup of } \frac{(T_\ell \otimes \mathbb{D}_\ell)^{I_K}}{(T_\ell^{I_K} \otimes \mathbb{D}_\ell)} \text{ generated by } (X \otimes \mathbb{D}_\ell)^{I_K},$$

and

$$t_M(X) := \text{subgroup of } \frac{(T_\ell \otimes \mathbb{D}_\ell)^{I_M}}{(T_\ell^{I_M} \otimes \mathbb{D}_\ell)} \text{ generated by } (X \otimes \mathbb{D}_\ell)^{I_M}.$$

Note that this is the only place in this paper where $t_K$ and $t_M$ do not denote toric ranks. It is clear that

$$\xi_{K,M,\ell}(t_K(X)) \subseteqq t_M(X).$$

Therefore, to prove part (9), i.e., to show that

$$\gamma_{K,L,\ell}(\Theta^{[1]}_{K,M,\ell}) \subseteqq \Theta_{M,\ell},$$

we simply need to note that

$$\phi_{K,\ell}(\Theta^{[1]}_{K,M,\ell}) = t_K(W_M^{\S})$$

and that

$$\phi_{M,\ell}(\Theta_{M,\ell}) = t_M(W_M^{\S}).$$

Let us now prove part (10). By definition,

$$\phi_{K,\ell}(\Psi_{K,M,\ell}) = \operatorname{Ker}(\xi_{K,M,\ell}).$$

Since $\operatorname{Ker}(\xi_{K,M,\ell})$ is generated by

$$(T_\ell^{I_M} \otimes \mathbb{D}_\ell) \cap (T_\ell \otimes \mathbb{D}_\ell)^{I_K} = (T_\ell^{I_M} \otimes \mathbb{D}_\ell)^{I_K},$$

we find that

$$t_K(T_\ell^{I_M}) = \operatorname{Ker}(\xi_{K,M,\ell}).$$

Since

$$t_K(T_\ell^{I_M}) =: \phi_{K,\ell}(\Theta^{[2]}_{K,M,\ell}),$$

part (10) is proved. This concludes the proof of Theorem 3.1. □

Let us now restate two of the theorems announced in the first section of this paper.

**Corollary 3.21.** *Let $A/K$ be an abelian variety. Let $\ell \neq p$ be a prime. Assume that $A/K$ has a polarization whose degree is prime to $\ell$.*

(i) *Then there exists a nondegenerate pairing*

$$(\;;\;): \Phi_{K,\ell} \times \Phi_{K,\ell} \to \mathbb{Q}_\ell/\mathbb{Z}_\ell.$$

(ii) *There exists three subgroups*

$$\Theta^{[3]}_{K,\ell}(A) \subseteqq \Theta^{[2]}_{K,\ell}(A) \subseteqq \Theta_{K,\ell}(A)$$

*of the $\ell$-part $\Phi_{K,\ell}(A)$ of $\Phi_K(A)$, which are functorial in the variable $A$ and whose existence does not depend on the choice of a polarization for $A$. These subgroups are equal to the orthogonals, under the pairing ( ; ), of the subgroups*

$$\Sigma^{[3]}_{K,\ell}(A) \supseteqq \Sigma^{[2]}_{K,\ell}(A) \supseteqq \Sigma_{K,\ell}(A),$$

*respectively.*

(iii) *The pairing* ( ; ) *restricts to a nondegenerate pairing on* $\Theta_{K,\ell}$, *again denoted by* ( ; ). *The subgroup* $\Theta^{[2]}_{K,\ell}(A)$ *is the orthogonal in* $\Theta_{K,\ell}(A)$, *under the restricted pairing, of the subgroup* $\Theta^{[3]}_{K,\ell}(A)$. *In particular,*

• *The groups* $\Theta^{[3]}_{K,\ell}(A)$ *and* $\Theta_{K,\ell}(A)/\Theta^{[2]}_{K,\ell}(A)$ *are isomorphic. Equivalently, the group* $\Phi_{K,\ell}(A)/\Sigma^{[3]}_{K,\ell}(A)$ *is isomorphic to* $\Sigma^{[2]}_{K,\ell}(A)/\Sigma_{K,\ell}(A)$.

*Proof.* Set $\Theta^{[i]}_{K,\ell} := \Theta^{[i]}_{K,L,\ell}$, for $i = 1, 2, 3$. Our corollary follows immediately from Theorem 3.1 and from Proposition 3.11. □

**Corollary 3.22.** *The subgroup* $\Theta^{[2]}_{K,\ell}$ *is equal to the* $\ell$*-part* $\Psi_{K,L,\ell}$ *of the kernel of* $\gamma_{K,L}$.

*Proof.* In Corollary 3.21, we defined the subgroup $\Theta^{[2]}_{K,\ell}$ to be equal to the group $t(T_\ell^{I_L})$. Corollary 3.22 follows immediately from the proof of part (10) in Theorem 3.1, a proof which does not depend on the choice of a polarization of $A$. □

**Remark 3.23.** Let $A/K$ be a simple abelian variety. Let $L/K$ be the minimal extension such that $A_L/L$ has semistable reduction. If $A/K$ has real or complex multiplication defined over $K$, then the abelian variety $A_M/M$ has purely additive reduction over any extension $K \subseteq M \subset L$ (see for instance [Oor], 2.4, for a proof in the case of complex multiplication). The following corollary provides a bound for the exponent of the prime-to-$p$ part $A(K)^{(p)}_{\text{tors}}$ of the torsion subgroup of such an abelian variety.

**Corollary 3.24.** *Let* $A/K$ *be a principally polarized abelian variety such that* $A_M/M$ *has purely additive reduction over any extension* $K \subseteq M \subset L$. *If* $A(K)^{(p)}_{\text{tors}} \neq \{0\}$, *then* $[L:K]$ *is a power of a single prime* $\ell \neq p$ *and* $A(K)^{(p)}_{\text{tors}}$ *is killed by* $\ell^2$. *Moreover, if* $A/K$ *has potentially good reduction, then* $A(K)^{(p)}_{\text{tors}}$ *is killed by* $\ell$.

*Proof.* If $A(K)$ contains a point of order $\ell$, then the group $\Theta_{K,\ell}$ is nontrivial. Therefore, part (11) of Theorem 3.1 implies that the integer

$$2(a_{K_\ell} - a_K) + 2(t_{K_\ell} - t_K)$$

must be strictly positive. It follows then from our hypothesis on $A/K$ that $K_\ell = L$.

Assume now that $A(K)$ contains a point of order $\ell^3$. Then $\Psi_{K,L}$ contains a point of order $\ell^2$. Indeed, if $\Phi_K/\Psi_{K,L}$ contains a point of order $\ell^2$, then parts (8) and (11) of Theorem 3.1 imply that $\Psi_{K,L}$ must also contain a point of order $\ell^2$. In the case where $A/K$ has potentially good reduction and $A(K)$ contains a point of order $\ell^2$, the group $\Psi_{K,L}$, which equals $\Phi_K$, also contains a point of order $\ell^2$. We will show that, regardless of the type of semistable reduction of $A_L/L$, the group $\Psi_{K,L}$ cannot contain a point of order $\ell^2$. Consider the field extensions

$$K \subseteq E \subset K_\ell = L\,,$$

with $[K_\ell : E] = \ell$. Recall that our hypothesis on $A/K$ implies that $a_E = t_E = 0$. Therefore, part (5) of Theorem 3.1 implies that the group $\Psi_{K,E,\ell}$ must be trivial. It follows that the group $\Psi_{E,L}$ contains a point of order $\ell^2$. We have obtained a contradiction since part (5) of Theorem 3.1 implies that the group $\Psi_{E,L,\ell}$ is killed by $[K_\ell : E] = \ell$. □

**Corollary 3.25.** *Let $A/K$ be an abelian surface having purely additive reduction. If $A/K$ has potentially good reduction, then $A(K)^{(p)}_{\mathrm{tors}}$ is isomorphic to a subgroup of one of the following groups:*

$$\mathbb{Z}/5\mathbb{Z},\ (\mathbb{Z}/3\mathbb{Z})^2,\ (\mathbb{Z}/2\mathbb{Z})^4,\ \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}.$$

*Except for the groups $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$, each group in the above list can be realized as the prime-to-p torsion subgroup of a product of elliptic curves. The group $\mathbb{Z}/5\mathbb{Z}$ can be realized as the prime-to-p torsion subgroup of an abelian surface. The group $\mathbb{Z}/4\mathbb{Z}$ cannot be realized as the prime-to-p torsion subgroup of a principally polarized abelian surface.*

*If $A/K$ does not have potentially good reduction, then $A(K)^{(p)}_{\mathrm{tors}}$ is isomorphic to a subgroup of one of the following groups:*

$$\mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/9\mathbb{Z},\ \mathbb{Z}/12\mathbb{Z},\ (\mathbb{Z}/3\mathbb{Z})^2,\ (\mathbb{Z}/2\mathbb{Z})^4,\ \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z},$$
$$(\mathbb{Z}/2\mathbb{Z})^2\oplus\mathbb{Z}/4\mathbb{Z},\ (\mathbb{Z}/4\mathbb{Z})^2.$$

*Except for the groups $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/9\mathbb{Z}$, each group in the above list can be realized as the prime-to-p torsion subgroup of a product of elliptic curves. The groups $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/9\mathbb{Z}$ can be realized as the prime-to-p torsion subgroups of abelian surfaces.*

*Proof.* Assume that $A/K$ has purely additive reduction and potentially good reduction. It follows immediately from Theorem 2.15 that $\Phi_K^{(p)}$ must be isomorphic to one of the following groups:

$$\{0\},\ \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/5\mathbb{Z},\ \mathbb{Z}/6\mathbb{Z},\ (\mathbb{Z}/2\mathbb{Z})^2,\ (\mathbb{Z}/2\mathbb{Z})^3,\ (\mathbb{Z}/2\mathbb{Z})^4,$$
$$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z},\ (\mathbb{Z}/3\mathbb{Z})^2,\ \mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}.$$

By taking products of elliptic curves, it is easy to show that each of the groups

$$\{0\},\ \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/6\mathbb{Z},\ (\mathbb{Z}/2\mathbb{Z})^2,\ (\mathbb{Z}/2\mathbb{Z})^3,\ (\mathbb{Z}/2\mathbb{Z})^4,$$
$$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z},\ (\mathbb{Z}/3\mathbb{Z})^2,$$

arises as the group of components of an abelian surface having purely additive reduction and potentially good reduction. Let $K=\mathbb{C}((t))$ and let $X/K$ denote the curve given by the equation

$$y^2=x^5-t^2.$$

The jacobian of $X/K$ has purely additive reduction and potential good reduction. One easily checks that this abelian surface has a $K$-rational point of order 5 and that, therefore, the associated group of components $\Phi$ also has a point of order 5. Theorem 2.15 implies then that $\Phi$ is cyclic of order 5.

We proceed now to show that the prime-to-$p$ part of the group of components of a principally polarized abelian surface with purely additive reduction and potentially good reduction cannot be cyclic of order 4. Indeed, if the prime-to-$p$ part were cyclic of order 4, then the characteristic polynomial $\operatorname{char}(\sigma_2)(x)$ would be equal either to:

$$(x^2+1)(x^2-1), \quad \text{or to } (x^2+1)^2, \quad \text{or to } (x+1)^2(x^2-x+1),$$
$$\text{or } \operatorname{rank}_{\mathbb{Z}_\ell}(T^P)=2 \text{ and } \operatorname{char}(\sigma_2)(x)=(x+1)^2.$$

Recall that the multiplicity of the integer one as an eigenvalue of a symplectic matrix must be even. Therefore, $\operatorname{char}(\sigma_2)(x)$ cannot be equal to $(x^2+1)(x^2-1)$. Suppose now that $\operatorname{char}(\sigma_2)(x)=(x^2+1)^2$. Let $M/K$ be an extension of degree 2. Since

$$\operatorname{char}(\sigma_2^2)(x)=(x+1)^4,$$

it follows that the abelian rank of $A_M/M$ is trivial. Therefore, part (5) of Theorem 3.1 implies that $\Psi_{K,M}$ is trivial. On the other hand, it also follows from the fact that

$$\operatorname{char}(\sigma_2^2)(x) = (x+1)^4$$

that $\Phi_M$ is killed by 2, contradicting the fact that $\Psi_{K,M}$ is trivial. Suppose then that

$$\operatorname{char}(\sigma_2)(x)=(x+1)^2(x^2-x+1).$$

It follows immediately that $[K_2:K]=2$ and, therefore, 2 must kill $\Phi_{K,2}$, which is a contradiction. The last case is similar and we omit it.

Assume now that $A/K$ does not have potentially good reduction. It follows immediately from Theorem 2.15 that the group of components of such an abelian surface must be isomorphic to a subgroup of one of the groups listed in the corollary. It is clear that, except for the cyclic groups of order 8 and 9, each subgroup listed in the corollary arises as the group of components of a product of elliptic curves. Examples 5.6 and 5.2 show that the groups $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/9\mathbb{Z}$ also arise as groups of components of abelian surfaces with purely additive reduction and $t_L \neq 0$. □

**Remark 3.26.** Let $A/K$ be a principally polarized abelian surface with purely additive reduction and potentially good reduction. We proved in the previous corollary that $\Phi_{K,2}$ cannot be isomorphic to $\mathbb{Z}/4\mathbb{Z}$. Therefore, when $\ell=2$, there exists an abelian group satisfying the bound for $\Phi_{K,\ell}$ given in Theorem 3.1 but which cannot occur as the group of components of a principally polarized abelian surface with purely additive reduction and potentially good reduction. In fact, it is likely that our bound for $\Phi_{K,2}$ is not best possible for such abelian varieties. We believe that the prime-to-$p$ part of the group of components of $A/K$ cannot be isomorphic to $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$. Since Lemma 2.1 implies that the group $\Phi_{K,2}$ is isomorphic to $T_2^P/(\sigma_2-\mathrm{id})(T_2^P)$, one could show that $\Phi_{K,2}$ cannot be isomorphic to $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$ by showing that there does not exist any matrix $S$ in $\mathrm{GL}_4(\mathbb{Z}_2)$ with the following properties:

(1) $\operatorname{char}(S)(x) = (x^2+1)(x+1)^2$.

(2) $(\mathbb{Z}_2)^4/\operatorname{Im}(S - \mathrm{id}) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

(3) The matrix $S$ is *symplectic*.

It is interesting to note that the bound for $\Phi_{K,\ell}$ obtained in Lemma 2.13 does not depend on the fact that the matrix $\sigma_\ell$, acting on $T_\ell(A)$, is symplectic. On the other hand, a proof that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ cannot arise as a group of components would rely on the fact that $\sigma_2$ is symplectic, since the following matrix $S$ does satisfy both properties (1) and (2) above but is not symplectic.

$$S = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

## 4. The $p$-part of the group $\Phi_K$

Let $A/K$ be a jacobian variety, and denote by $\Phi_K$ its group of components. In the following theorem, we describe, for the group $\Phi_{K,p}$, a nonfunctorial analogue to the filtration of $\Phi_{K,\ell}$ introduced in Theorem 3.1 when $\ell \neq p$.

**Theorem 4.1.** *Let $X/K$ be a smooth proper geometrically connected curve having a $K$-rational point. Let $A/K$ denote its jacobian. The $p$-part $\Phi_{K,p}$ of the group of components of $A/K$ contains three subgroups,*

$$H'_p \subseteqq H_p \subseteqq G_p\,,$$

*having the following properties*:

1. *The group $\Phi_{K,p}/G_p$ is generated by $t_K$ elements.*

2. *The following inequality holds*:

$$\delta(H_p) + \delta(G_p/H_p) \leqq 2u_{L_0}(A)\,.$$

3. *The group $G_p/H_p$ is isomorphic to the group $H'_p$.*

*Proof.* To prove our theorem, we must begin by recalling how to compute $t_K(A)$ and $\Phi_K(A)$ using a good regular model $\mathscr{X}/\mathcal{O}_K$ of $X/K$. The special fiber $\mathscr{X}_k$ of $\mathscr{X}/\mathcal{O}_K$ is an effective Cartier divisor and, as such, we write it as

$$\mathscr{X}_k = \sum_{i=1}^{n} r_i C_i\,,$$

where $r_i$ is the multiplicity of the irreducible component $C_i$. Let

$$M := ((C_i \cdot C_j))$$

be the intersection matrix associated to $\mathscr{X}_k$ and set

$${}^tR := (r_1, \ldots, r_n).$$

The vector $R$ is in the kernel of the matrix $M$ or, equivalently, $M \cdot R = 0$. When we need to emphasize the dependence of $M$ and $R$ on $\mathscr{X}$, we write $M(\mathscr{X})$ and $R(\mathscr{X})$.

**4.2.** The integer $\gcd(r_1, \ldots, r_n)$ does not depend on the choice of a regular model of $X/K$. The fact that $X$ has a $K$-rational point implies that

$$\gcd(r_1, \ldots, r_n) = 1.$$

Raynaud [Ray] (see also [BLR], 9.6) has proven that, when $\gcd(r_1, \ldots, r_n) = 1$, the group of components $\Phi_K$ of $\mathrm{Jac}(X)/K$ is isomorphic to

$$\mathrm{Ker}({}^tR)/\mathrm{Im}(M),$$

where $M: \mathbb{Z}^n \to \mathbb{Z}^n$ and ${}^tR: \mathbb{Z}^n \to \mathbb{Z}$ are the linear transformations associated to the matrices $M$ and ${}^tR$. In particular, the group $\Phi_K$ can be computed explicitly using a row and column reduction of the matrix $M$ (see [Lor1], 1.4).

**4.3.** We call a regular model $\mathscr{X}/\mathcal{O}_K$ of $X/K$ a *good model* if the following additional properties hold:

- The components $C_i$ are smooth of genus $g(C_i)$.
- If $i \neq j$, the intersection number $(C_i \cdot C_j)$ is equal to zero or one.

To the model $\mathscr{X}$ we associate a graph $G(\mathscr{X})$ defined as follows: the vertices of $G$ are the curves $C_i$, and a vertex $C_h$ is linked to $C_j$ by $(C_h \cdot C_j)$ edges. We let $\beta(G)$ denote the first Betti number of $G$.

Raynaud (see [BLR], Theorem 4 on page 267 and Propositions 9 and 10 on pages 248–249, or [Lor2], 1.3) has shown that, if $\mathscr{X}/\mathcal{O}_K$ is a good model of $X/K$, then:

$$\sum_{i=1}^{n} g(C_i) = a_K,$$

and

$$\beta(G) = t_K.$$

**4.4.** Let $\mathscr{X}/\mathcal{O}_K$ be a good model of a curve $X/K$. Let

$$T(\mathscr{X}) := (g(C_1), \ldots, g(C_n))$$

denote the vector whose coordinates are the genera of the components $C_i$. In the terminology of Artin and Winters [A-W], the quadruple $(G(\mathscr{X}), M(\mathscr{X}), R(\mathscr{X}), T(\mathscr{X}))$ is called a *type*. Winters' Theorem [Win], 4.3, states that, given any type

$$(G, M, R, T),$$

one can find a field $F$ with a discrete valuation $v$, having residue characteristic equal to zero, and such that

- there exists a smooth proper geometrically irreducible curve $Y/F$ having a regular model $\mathscr{Y}/\mathcal{O}_F$ whose associated type $(G(\mathscr{Y}), M(\mathscr{Y}), R(\mathscr{Y}), T(\mathscr{Y}))$ is equal to the given type $(G, M, R, T)$.

**4.5.** We are now ready to begin the proof of Theorem 4.1. We want to use Winters' Existence Theorem to "reduce our situation to a situation in equicharacteristic zero" that will enable us to apply Theorem 3.1. Let $X/K$ be a curve having a $K$-rational point. Choose a good model $\mathscr{X}/\mathcal{O}_K$ of the curve $X/K$. Let

$$(G(\mathscr{X}), M(\mathscr{X}), R(\mathscr{X}), T(\mathscr{X}))$$

be the type associated to $\mathscr{X}/\mathcal{O}_K$. Winters' Theorem, when applied to the type

$$(G(\mathscr{X}), M(\mathscr{X}), R(\mathscr{X}), T(\mathscr{X})),$$

implies the existence of a curve, $Y/F$, having the properties listed in 4.4. Let $B/F$ denote the jacobian of $Y/F$. It follows from the facts recalled in 4.3 that

$$t_K(A) = t_F(B),$$

and

$$a_K(A) = a_F(B).$$

It follows from the facts recalled in 4.2 that there exists an isomorphism

$$\varphi : \Phi_K(A) \to \Phi_F(B).$$

Since $\mathcal{O}_F$ has equicharacteristic zero and since $B/F$ is principally polarized, Theorem 3.1 shows the existence of three $p$-subgroups of $\Phi_{F,p}(B)$,

$$\Theta_{F,p}^{[3]}(B) \subseteqq \Psi_{F,p}(B) \subseteqq \Theta_{F,p}(B).$$

Define three subgroups of $\Phi_K(A)$ as follows.

$$G_p := \varphi^{-1}(\Theta_{F,p}),$$

$$H_p := \varphi^{-1}(\Psi_{F,p}),$$

and

$$H_p' := \varphi^{-1}(\Theta_{F,p}^{[3]}).$$

Part (2) of Theorem 3.1 implies part 1 of Theorem 4.1. Similarly, part 3 of Theorem 4.1 follows immediately from part (8) of Theorem 3.1.

Let $E/F$ denote the unique extension of $F$, minimal with the property that $B_E/E$ has semistable reduction. Let $F \subseteqq F_p \subseteqq E$ be such that

$$[F_p : F] = p^{\operatorname{ord}_p([E:F])}.$$

It follows from part (11) of Theorem 3.1 that

$$\delta(\Psi_{F,p}) + \delta(\Theta_{F,p}/\Psi_{F,p}) \leqq 2\big(a_{F_p}(B) - a_F(B)\big) + 2\big(t_{F_p}(B) - t_F(B)\big).$$

Let

$$F \subseteqq E_p \subseteqq E$$

denote the unique extension of $F$ such that

$$[E : E_p] = [F_p : F].$$

It follows from Lemma 4.8 below that

$$\delta(H_p) + \delta(G_p/H_p) \leqq 2\big(a_{F_p}(B) - a_F(B)\big) + 2\big(t_{F_p}(B) - t_F(B)\big) \leqq 2u_{E_p}(B).$$

Therefore, to complete the proof of Theorem 4.1, we only need to show that

$$u_{L_0}(A) = u_{E_p}(B).$$

**4.6.** Recall from Diagram 2.6 that, if $A/K$ is any abelian variety and $p > 0$ is the residue characteristic, then

$$2u_{L_0}(A) = \operatorname{rank}_{Z_\ell}\big(T_\ell A/(T_\ell A)^P\big).$$

When $A$ is the jacobian of a curve $X/K$, the rank of $(T_\ell A)^P$ can be computed in terms of a good regular model of $X/K$ (see [Lor4], 2.1). Namely, let

$$d_i = \sum_{i \neq j} (C_i \cdot C_j).$$

For any integer $r$, let

$$r^{(p)} := r \cdot p^{-\operatorname{ord}_p(r)}.$$

Then

$$\operatorname{rank}_{Z_\ell}(T_\ell A)^P = 2a_K(A) + 2t_K(A) + \sum_{i=1}^{n} (r_i^{(p)} - 1)(d_i - 2) + 2\sum_{i=1}^{n} (r_i^{(p)} - 1)g(C_i).$$

**4.7.** When $F$ has equicharacteristic zero and $q$ is any prime, let $Q$ denote the pro-$q$-Sylow subgroup of $\operatorname{Gal}(\bar{F}/F)$. Let

$$E_q := (\bar{F})^{I_E Q}.$$

We noted in Remark 2.7 that

$$2u_{E_q}(B) = \operatorname{rank}_{Z_\ell}(T_\ell B/(T_\ell B)^Q).$$

We showed in [Lor4], 2.1, that

$$\operatorname{rank}_{Z_\ell}(T_\ell B)^Q = 2a_F(B) + 2t_F(B) + \sum_{i=1}^{n} (r_i^{(q)} - 1)(d_i - 2) + 2\sum_{i=1}^{n} (r_i^{(q)} - 1)g(C_i).$$

Hence, we may apply this formula for $\operatorname{rank}_{Z_\ell}(T_\ell B)^Q$ in the case $q = p$ and obtain that

$$2u_{E_p}(B) = 2g - \operatorname{rank}_{Z_\ell}(T_\ell B)^Q = 2g - \operatorname{rank}_{Z_\ell}(T_\ell A)^P = 2u_{L_0}(A).$$

This concludes the proof of Theorem 4.1. □

**Lemma 4.8.** *Let $p = 0$ and let $q$ be any prime. Let $K_q$ and $L_q$ be the extensions of $K$ defined in* 1.1 *and* 2.7 *respectively, with* $\operatorname{Gal}(K_q/K) = \operatorname{Gal}(L/L_q) =$ *q-part of* $\operatorname{Gal}(L/K)$. *Then*

$$(a_{K_q} - a_K) + (t_{K_q} - t_K) \leqq u_{L_q}.$$

*Proof.* Let $\ell \neq q$. Let $[L:K] = \alpha \cdot \beta$ with $\gcd(q, \beta) = 1$ and $\alpha = q^{\operatorname{ord}_q(\alpha)}$. Recall that

$$2(a_K + t_K) = \operatorname{ord}_{(x-1)}(\operatorname{char}(\sigma_\ell)(x)),$$
$$2(a_{K_q} + t_{K_q}) = \operatorname{ord}_{(x-1)}(\operatorname{char}(\sigma_\ell^\alpha)(x)),$$
$$2(a_{L_q} + t_{L_q}) = \operatorname{ord}_{(x-1)}(\operatorname{char}(\sigma_\ell^\beta)(x)), \quad \text{and}$$
$$2(a_L + t_L) = \operatorname{ord}_{(x-1)}(\operatorname{char}(\sigma_\ell^{\alpha\beta})(x)).$$

Hence,

$$a_L + t_L \geqq (a_{L_q} + t_{L_q}) + (a_{K_q} + t_{K_q}) - (a_K + t_K).$$

Since, by definition,

$$a_L + t_L = a_{L_q} + t_{L_q} + u_{L_q} = g,$$

our lemma is proved. □

**Remark 4.9.** Let $A/K$ be any abelian variety. McCallum shows in [McC], Theorem 1, that

$$\Psi_{K,L} \text{ is killed by } [L:K].$$

In light of Theorem 3.1, it is natural to wonder whether a subgroup $\Theta_{K,p}$ of $\Phi_{K,p}$, satisfying the properties (ii) and (iii) of Remark 1.8, is killed by $[L:K]^2$. In this regard, we can show:

**Corollary 4.10.** *Let $X/K$ be a smooth proper geometrically connected curve having a $K$-rational point. Let $A/K$ be its jacobian. If $L/K$ is tame, then $u_{L_0}(A) = 0$ and, therefore, the group $G_p$ introduced in Theorem* 4.1 *is trivial.* □

**Remark 4.11.** Let $\ell \neq p$ be any prime. Parts (5) and (10) of Theorem 3.1 imply that, given any Galois extension $K \subseteq M \subseteq L$, the following bound holds for $\Psi_{K,M}$:

$$\delta(\Psi_{K,M,\ell}) \leqq 2(a_M - a_K) + (t_M - t_K)\,.$$

The following example shows that this bound does not hold when $\ell = p$. Consider the jacobian $A/K$ of a wild Fermat quotient $C$ over $K = \mathbb{Q}_p^{\mathrm{unr}}(\xi)$, with $\xi$ a primitive $p$-th root of 1 (see Example 5.1). McCallum shows in [McC2], Theorem 6, that $\Phi_K$ is cyclic of order $p = 2g+1$. Coleman and McCallum have shown in [C-M] (4.6 and following remark) that the extension $L/K$, minimal with the property that $A_L/L$ has good reduction, has degree $[L:K] = 2p$. The extension $L/K$ is abelian because $C$ has complex multiplication defined over $K$ ([Se-Ta], corollary 2 on page 502). Let

$$K \subset M \subset L\,,$$

with $[L:M] = 2$. The abelian rank $a_M$ and the toric rank $t_M$ of the jacobian of $C_M/M$ are both equal to zero because this abelian variety has complex multiplication over $M$ and does not have good reduction over $M$ ([Oor], 2.4). Since $L/M$ is tame and $t_M = 0$, Theorem 4.1 implies that the group $\Phi_M$ has order prime to $p$. In particular, the group $\Psi_{K,M}$ must be cyclic of order $p$. Hence,

$$\delta(\Psi_{K,M,p}) = p - 1 > 0 = 2(a_M - a_K) + (t_M - t_K)\,.$$

**Remark 4.12.** Let $A/K$ be an abelian variety with purely additive reduction. Let $\ell \neq p$ be any prime. As we recalled in Remark 1.3, the reduction map of the Néron model of $A/K$ induces an isomorphism of the $\ell$-part of the torsion subgroup of $A(K)$ with $\Phi_{K,\ell}$. We illustrate in the following remarks the extent to which the reduction map fails to be an isomorphism on the $p$-part of $A(K)_{\mathrm{tors}}$. The following example shows that $|\Phi_K|$ may be divisible by $p$ while the abelian variety $A/K$ has purely additive reduction and no point of order $p$ defined over $K$.

Let $K$ denote the completion of the maximal unramified extension of $\mathbb{Q}_2$. The curve $88A$ in [AnIV], given by the equation $y^2 = x^3 - 4x + 4$, has reduction $I_1^*$ at $p = 2$ ($\Phi = \mathbb{Z}/4\mathbb{Z}$). The group $E(\mathbb{Q})$ has rank one. We claim that $E(K)$ has no point of order 2. It is sufficient to check that the polynomial $x^3 - 4x + 4$ is irreducible over a field where the valuation $v(2)$ equals 1. Assume that there exists $z \in K$ such that $z^3 - 4z + 4 = 0$. Then $z \in \mathcal{O}_K$ and, in fact, the equality $z^3 = 4(z-1)$ implies that $v(z) > 0$. Therefore, $1 - z$ is a unit or, equivalently, $v(z-1) = 0$. The equality $z^3 = 4(z-1)$ implies, then, that $3v(z) = 2v(2) = 2$, which contradicts the fact that $v(z)$ is an integer.

**Remark 4.13.** Let $A/K$ denote an abelian variety of dimension $g$ with purely additive reduction over $\mathcal{O}_K$. Assume that the integer $2g+1$ is prime and consider the following assertions:

(i) $A(K)$ contains a point of order $2g+1$.

(ii) $|\Phi_K|$ is divisible by $2g+1$.

(iii) $[L:K]$ is divisible by $2g+1$.

(iv) $A/K$ has potentially good reduction (i.e. $t_L = 0$).

When $p \neq 2g+1$, the following implications hold:

$$\text{(i)} \Leftrightarrow \text{(ii)} \Rightarrow \text{(iii)} \Rightarrow \text{(iv)}.$$

The implication (ii) ⇒ (iii) follows from part (11) of 3.1. The implication (iii) ⇒ (iv) follows from Proposition 3.1 in [Lor2]. Note that parts (4), (5), and (6) of Theorem 3.1, together, also shows that (ii) implies (iv). When $p = 2g+1$, the situation is quite different and

$$\text{(i)} \not\Rightarrow \text{(ii)}, \quad \text{(i)} \not\Rightarrow \text{(iii)}, \quad \text{and} \quad \text{(i)} \not\Rightarrow \text{(iv)}.$$

The tame Fermat quotients (see 5.1) provide examples where the implications (i) ⇒ (ii) and (i) ⇒ (iii) do not hold (see [Gr-Ro] or [Gre] for the existence of points of order $p$ on the jacobians of Fermat quotients). The implication (i) ⇒ (iv) does not hold in general because there exist elliptic curves with $\mathbb{Q}$-rational points of order 3 that have potentially multiplicative reduction (e.g., the curve $90G$ on page 92 in [AnIV]). Note that such curves are twists of Tate curves and, therefore, their torsion points are well understood.

**Remark 4.14.** From the description of the structure of the group $\Phi_{K,q}$, obtained in Theorem 3.1 when $q \neq p$ ($q$ prime) and in Theorem 4.1 when $q = p$ and $A/K$ is a jacobian, we can deduce an explicit bound for the order of the subgroup $\Upsilon_{K,q}$ introduced in 1.11. Recall that, when $\Phi$ is any abelian group written as

$$\Phi \cong \mathbb{Z}/\varphi_1\mathbb{Z} \times \ldots \times \mathbb{Z}/\varphi_r\mathbb{Z} \quad \text{with} \quad \varphi_1 | \ldots | \varphi_r,$$

and $t \geq 0$ is any integer, we let

$$\Upsilon(t) := \begin{cases} \{0\} & \text{if} \quad t \geq r, \\ \mathbb{Z}/\varphi_1\mathbb{Z} \times \ldots \times \mathbb{Z}/\varphi_{r-t}\mathbb{Z} & \text{if} \quad r > t. \end{cases}$$

**Proposition 4.15.** *Let $\Phi$ be any abelian group and let $q$ be any prime. Suppose that $G_q$ is a subgroup of $\Phi_q$ and that $\Phi_q/G_q$ can be generated by $t$ elements. If $H_q$ is any subgroup of $G_q$, then there exists a subgroup $U_q$ in $\Upsilon_q(t)$ such that:*

- $\delta(U_q) \leq \delta(H_q)$, *and*
- $\delta(\Upsilon_q(t)/U_q) \leq \delta(G_q/H_q)$.

**Corollary 4.16.** *Let $A/K$ be any abelian variety and $\ell \neq p$ be any prime. Then there exists a subgroup $U_\ell \subseteq \Upsilon_{K,\ell}$ such that:*

- $\delta(U_\ell) \leq 2(a_{K_\ell} - a_K) + (t_{K_\ell} - t_K)$, *and*
- $\delta(\Upsilon_{K,\ell}/U_\ell) \leq (t_{K_\ell} - t_K)$.

*If $A/K$ is the jacobian of a smooth proper geometrically irreducible curve $X/K$ having a $K$-rational point, then there exists a subgroup $U_p \subseteqq \Upsilon_{K,p}$ such that:*

$$\delta(U_p) + \delta(\Upsilon_{K,p}/U_p) \leqq 2u_{L_0}.$$

*Proof.* The corollary follows immediately from Proposition 4.15 and Theorems 2.15 and 4.1. □

*Proof of* 4.15. Before proving Proposition 4.15, we need first to prove the following lemmas.

**Lemma 4.17.** *Let $\Phi$ be any abelian group and $G \subset \Phi$ be any subgroup such that $\Phi/G$ can be generated by $t$ elements. Then the exponent of $\Upsilon(t)$ divides the exponent $e$ of $G$.*

*Proof.* If $S$ is any group, we denote by $S[e]$ the kernel of the multiplication by $e$ on $S$. Since $G \subset \Phi[e]$, the group $\Phi/G$ surjects onto the group $\Phi/\Phi[e]$. Therefore, since $\Phi/G$ can be generated by $t$ elements, so can $\Phi/\Phi[e]$.

Recall now that, by definition,

$$\Phi \cong \Upsilon \oplus \Phi/\Upsilon,$$

and that the exponent of $\Upsilon$ divides the exponent of $\Phi/\Upsilon$. In particular, if $e$ does not kill $\Upsilon$, then both groups

$$\Upsilon/\Upsilon[e] \quad \text{and} \quad (\Phi/\Upsilon)/(\Phi/\Upsilon)[e]$$

are not trivial. It follows from the definitions that the minimal number of generators of the latter group is equal to $t$. Hence, the minimal number of generators of the group

$$\Phi/\Phi[e]$$

equals at least $t+1$, which is a contradiction, and our lemma is proved. □

**Lemma 4.18.** *Let $\Phi$ be any abelian group and $G \subset \Phi$ be any subgroup such that $\Phi/G$ can be generated by $t$ elements. The subgroup $\Upsilon(t)$ is a "lower approximation" of $G$ in the following sense: write*

$$G_q = \prod_{i=1}^{s(q)} \mathbb{Z}/q^{a_i}\mathbb{Z} \quad \text{with} \quad a_1 \geqq \ldots \geqq a_{s(q)}$$

*and*

$$\Upsilon_q(t) = \prod_{i=1}^{r(q)} \mathbb{Z}/q^{b_i}\mathbb{Z} \quad \text{with} \quad b_1 \geqq \ldots \geqq b_{r(q)}.$$

*Then,*

$$\forall i, \quad a_i \geqq b_i.$$

*Proof.* Define

$$G_{q,j} := \prod_{i=j}^{s(q)} \mathbb{Z}/q^{a_i}\mathbb{Z}$$

and

$$\Upsilon_{q,j} := \prod_{i=j}^{r(q)} \mathbb{Z}/q^{b_i}\mathbb{Z}.$$

By construction,

$$\Upsilon_{q,j} = \Upsilon_q(t+j-1),$$

and $\Phi_q/G_{q,j}$ is generated by $t+j-1$ elements. We may therefore apply the previous lemma to show that $q^{b_j}$ divides $q^{a_j}$. □

Let us return to the proof of our proposition. It is always possible to find generators for $H_q$ and $G_q$ such that the following properties hold:

- $H_q \cong \prod_{i=1}^{h} \mathbb{Z}/q^{a_i}\mathbb{Z}$ with $a_1 \geqq \ldots \geqq a_h$.
- $G_q \cong \prod_{i=1}^{g} \mathbb{Z}/q^{b_i}\mathbb{Z}$ with $b_1 \geqq \ldots \geqq b_g$.
- There exists an injection $s: \{1, \ldots, h\} \to \{1, \ldots, g\}$ and a commutative diagram

$$\begin{array}{ccc} H & \subseteq & G \\ \downarrow & & \downarrow \\ \prod_{i=1}^{h} \mathbb{Z}/q^{a_i}\mathbb{Z} & \xrightarrow{\eta} & \prod_{i=1}^{g} \mathbb{Z}/q^{b_i}\mathbb{Z} \end{array}$$

such that

$$a_i \leqq b_{s(i)} \quad \forall i = 1, \ldots, h,$$

and such that the map $\eta$ is the product of the inclusions

$$\mathbb{Z}/q^{a_i}\mathbb{Z} \to \mathbb{Z}/q^{b_{s(i)}}\mathbb{Z}, \quad \forall i = 1, \ldots, h.$$

Write

$$\Upsilon_q(t) = \prod_{i=1}^{r} \mathbb{Z}/q^{c_i}\mathbb{Z} \quad \text{with} \quad c_1 \geqq \ldots \geqq c_r.$$

Set

$$U_q := \prod_{i=1}^{\min(r,h)} \mathbb{Z}/q^{\min(a_i, c_{s(i)})}\mathbb{Z}.$$

Clearly,

$$\delta(U_q) \leqq \delta(H_q).$$

It follows from the previous lemma that

$$\delta(\Upsilon_q(t)/U_q) \leqq \delta(G_q/H_q). \quad □$$

Let $X/K$ be a smooth proper geometrically irreducible curve having a $K$-rational point. We keep the notations introduced in the proof of Theorem 4.1. In particular, let $A/K$ denote the jacobian of $X/K$. Let $\mathscr{X}/\mathcal{O}_K$ be any good regular model of $X/K$, and let

$$\mathscr{X}_k = \sum_{i=1}^{n} r_i C_i$$

denote its special fiber. Let

$$d_i := \sum_{j \neq i} (C_i \cdot C_j),$$

and let

$$v(\mathscr{X}) := \prod_{i=1}^{n} r_i^{d_i - 2}.$$

We claim that the rational number $v(\mathscr{X})$ is an integer independent of the choice of a good model of $X/K$. Indeed, we showed in [Lor4], 1.2, that the rational function

$$f_G(x) = \prod_{i=1}^{n} [(x^{r_i} - 1)/(x - 1)]^{d_i - 2}$$

is a polynomial independent of the choice of a good model of $X/K$. Since

$$f_G(1) = v(\mathscr{X}),$$

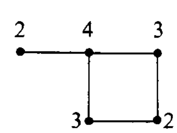
our claim follows. We denote the integer $v(\mathscr{X})$ by $v(X)$, or simply by $v$ when no confusion may result.

**Proposition 4.19.** *Let $A/K$ be the jacobian of a smooth proper geometrically connected curve $X/K$ having a $K$-rational point. Let $\ell$ be a prime, $\ell \neq p$. Then*:

(i) *If $a_K = 0$, then $|\Theta_{K,\ell}(A)|$ divides $v(X)$.*

(ii) *If $t_K = 0$, then $|\Theta_{K,\ell}(A)| = |\Phi_{K,\ell}|$ and $|\Phi_K| = v(X)$.*

**Remark 4.20.** It seems quite possible that the integer $|\Theta_{K,\ell}(A)|$ divides the integer $v(X)$ even when $a_K \neq 0$. On the other hand, if $t_K \neq 0$, then $|\Theta_{K,\ell}|$ is not always equal to the $\ell$-part of $v(X)$. Indeed, the following graph has a trivial group of components, while $v = 2$.




Note that the symbol $\overset{m}{\bullet}$ is used to denote a vertex/curve of multiplicity $m$.

*Proof of* 4.19. Fix a prime $\ell$, $\ell \neq p$. Recall that

$$|\Theta_{K,\ell}(A)| = |\Phi_{K,\ell}| / |s(W_{\ell,K})|.$$

It follows from the definition of the group $s(W_K)$ that

$$F/s(W_K) \cong \frac{(T_\ell^{I_K})^\S}{W_K + (\sigma_\ell - 1)(T_\ell^P)}.$$

This quotient injects into the group

$$\frac{W_K^\S}{T^{I_K} + (\sigma - 1)(T^P)},$$

which is a quotient of the group

$$\frac{W_K^\S}{T^{I_K} + (\sigma - 1)(W_K^\S)}.$$

This last group is the cokernel of the (injective) map:

$$\sigma - 1 : W_K^\S / T^{I_K} \to W_K^\S / T^{I_K}.$$

It follows from Theorem 2.1 in [Lor4] that the characteristic polynomial of $\sigma_\ell$ acting on $W_K^\S / T^{I_K}$ is equal to

$$\operatorname{char}(\sigma)(x) := \prod_{i=1}^{n} \left( \frac{x^{r_i^{(p)}} - 1}{x - 1} \right)^{d_i - 2 + 2g(C_i)}.$$

Therefore,

$$\text{order of } \frac{W_K^\S}{T^{I_K} + (\sigma - 1)(W_K^\S)} = \ell\text{-part of } \operatorname{char}(\sigma)(1).$$

Hence, when

$$\sum_{i=1}^{n} (r_i^{(p)} - 1)\, g(C_i) = 0,$$

it follows that

$$|F/s(W_K)| \text{ divides } \prod_{i=1}^{n} r_i^{d_i - 2} = v(X).$$

We recalled in 4.3 that $a_K = \sum g(C_i)$. Since, by hypothesis, $a_K = 0$, part (i) of our Proposition follows.

Part (ii) of our Proposition was proved in [Lor2]. Indeed, when $t_K = 0$, Theorem 3.1 implies that $\Theta_{K,\ell} = \Phi_{K,\ell}$. We showed in [Lor2], 1.5, that $|\Phi_K| = v(X)$ when $t_K = 0$. □

Note that, when $a_K = 0$ and $t_K = 0$, the method used to prove part (i) shows that

$$\begin{aligned} |\Phi_{K,\ell}| = |F/s(W_K)| &= |T/(\sigma - 1)(T)| \\ &= \ell\text{-part of } \operatorname{char}(\sigma)(1) \\ &= \ell\text{-part of } v(X), \end{aligned}$$

and, thereby, provides a new proof of [Lor2], 1.5, when $a_K = t_K = 0$.

As we recalled in the above proof, we showed in [Lor2] that:

$$\text{if} \quad t_K = 0, \quad \text{then} \quad |\Phi_K| = v(X).$$

We have also shown in [Lor1], 6.3, that, for a large class of simple graphs $(G, M, R)$,

$$|\Upsilon_K| \quad \text{divides} \quad v.$$

The following proposition implies that $|\Upsilon_K|$ divides $v$ for all simple graphs $(G, M, R)$, since Winters' Existence Theorem implies that every simple graph can be realized as the dual graph associated to a curve.

**Proposition 4.21.** *Let $X/K$ be a smooth proper geometrically connected curve having a K-rational point. Let $A/K$ be its jacobian. Then $|\Upsilon_K(A)|$ divides $v(X)$.*

*Proof.* Lemma 4.18 shows that, in order to prove our proposition, we only need to show the existence, for all primes $q$, of a subgroup $G_q \subseteqq \Phi_K$ such that

(i) $\Phi_{K,q}/G_q$ can be generated by $t_K$ elements, and

(ii) $|G_q|$ divides $v(X)$.

Let $\mathscr{X}/\mathcal{O}_K$ be any good regular model of $X/K$. Winters' Existence Theorem [Win], recalled in 4.4, implies that there exists a discrete valuation field $F$ of equicharacteristic zero, and a curve $Y/F$ having a (good) regular model $\mathscr{Y}/\mathcal{O}_F$ such that

$$(G(\mathscr{Y}), M(\mathscr{Y}), R(\mathscr{Y}), (0, \ldots, 0)) = (G(\mathscr{X}), M(\mathscr{X}), R(\mathscr{X}), \ldots, 0)).$$

Let $B/F$ denote the jacobian of $Y/F$. By construction,

$$T(\mathscr{Y}) = (0, \ldots, 0),$$

which implies that

$$a_F(B) = 0.$$

Therefore, Proposition 4.19 implies that

$$|\Theta_{F,q}(B)| \quad \text{divides} \quad v(Y) \quad \text{for all primes } q.$$

It follows from the facts recalled in 4.3 that

$$t_K(A) = t_F(B),$$

and

$$v(X) = v(Y).$$

It follows from the facts recalled in 4.2 that there is an isomorphism

$$\varphi : \Phi_K(A) \xrightarrow{\sim} \Phi_F(B).$$

The subgroups

$$G_q := \varphi^{-1}(\Theta_{F,q}(B)), \quad q \text{ prime},$$

are the subgroups needed to prove our proposition. □

## 5. Examples

**Example 5.1.** *The Fermat curve* $F_p$. Let $p$ be an odd prime. Denote by $k$ the algebraic closure of the finite field $\mathbb{F}_p$. Let $F_p$ be the smooth plane curve defined by the equation

$$x^p + y^p + z^p = 0.$$

The special fiber of the regular minimal model of $F_p$ over $\mathbb{Z}_p$ has been computed by Chang in [Cha], Theorem 4 and figure on page 255. Since the graph associated to this special fiber satisfies the hypothesis of Theorem 2.1 in [Lor3], we can use Theorem 2.1 to compute explicitly the group of components of the jacobian of $F_p/\mathbb{Q}_p$ using this special fiber. Our computations show that:

$$\Phi_{\mathbb{Q}_p}(F_p)(k) \cong (\mathbb{Z}/2\mathbb{Z})^\tau \times (\mathbb{Z}/p\mathbb{Z})^w,$$

for some integers $\tau$ and $w$ with

$$\tau + w = p - 2.$$

Let $\mathbb{Q}_p^{\text{unr}}$ denote the maximal unramified extension of $\mathbb{Q}_p$. Let $d$ be a divisor of $p-1$. It is possible to use Chang's result to compute the minimal model of $F_p$ over the unique extension $K_d/\mathbb{Q}_p^{\text{unr}}$ of degree $d$. Once the computation of a model for $(F_p)_{K_d}/K_d$ is made, one may check that Theorem 2.1 of [Lor3] can again be applied to show that

$$\Phi_{K_d}(F_p)(k) \cong (\mathbb{Z}/2\mathbb{Z})^{d\tau} \times (\mathbb{Z}/p\mathbb{Z})^w, \quad \text{if } d \text{ divides } p-1.$$

Mc Callum has computed the special fiber of a regular model of $F_p$ over $K_{p-1}$ in [McC2], diagram 3, page 69.

The curve $F_p$ has genus equal to

$$g(F_p) = (p-2) \cdot (p-1)/2.$$

Hence, over $K_{p-1}$, the group $\Phi := \Phi_{K_{p-1}}(F_p)$ has "maximal order" in the sense that

$$\delta(\Phi_2) + \delta(\Phi_p) = \tau(p-1) + w(p-1) = 2g(F_p).$$

The integers $\tau$ and $w$ may be interpreted geometrically as follows. Let $C_s$, $s = 1, \ldots, p-2$, be the smooth projective curve of genus $(p-1)/2$, birational to

$$y^p = x^s(1-x).$$

Each curve $C_s$ is a quotient of $F_p$ and the jacobian of $F_p$ is isogeneous over $\mathbb{Q}$ to the product of the jacobians $\operatorname{Jac}(C_s)$, $s = 1, \ldots, p-2$ ([Fad]). Let $L$ denote the minimal extension of $K_{p-1}$ over which $\mathrm{Jac}(F_p)$ has semistable reduction. Since each quotient $C_s$ has complex multiplication, the reduction of $\mathrm{Jac}(F_p)$ over $L$ is in fact good ([Oor], 2.2). Let $L_0$ denote the field of elements in $L$ fixed by the Sylow $p$-subgroup of $\mathrm{Gal}(L/K_{p-1})$. The abelian rank of $\mathrm{Jac}(F_p)_{L_0}/L_0$ is equal to $u_K - u_{L_0}$. Theorem 3.1 implies that

$$\delta(\Phi_2) = \tau(p-1) \leqq 2(u_K - u_{L_0}).$$

On the other hand, Theorem 4.1 implies that

$$\delta(\Phi_p) = w(p-1) \leqq 2u_{L_0}.$$

Therefore, we conclude that

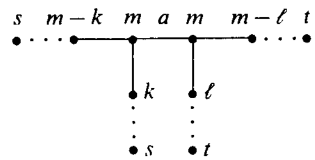
$$u_K - u_{L_0} = \tau(p-1)/2.$$

We claim that exactly $\tau$ jacobians $\mathrm{Jac}(C_s)$ have good reduction over $L_0$. First, note that, if $\mathrm{Jac}(C_s)$ contains a proper abelian subvariety $A$ defined over $L_0$, then $\mathrm{Jac}(C_s)$ must have good reduction over $L_0$. Indeed, $T_\ell(A)$ has rank smaller than $p-1$ and, therefore, an element $\sigma$ of $\mathrm{Gal}(L/K_{p-1})$ of order $p$ cannot act in a nontrivial manner on $T_\ell(A)$. On the other hand, if $\mathrm{Jac}(C_s)$ is simple, then it has either purely additive reduction or good reduction over $L_0$ since the complex multiplication is defined over $K_{p-1}$ ([Oor], 2.4). Therefore, all jacobians $\mathrm{Jac}(C_s)_{L_0}/L_0$ have dimension equal to $(p-1)/2$ and have either purely additive reduction or good reduction. Since the abelian rank of $\prod \mathrm{Jac}(C_s)$ is equal to $\tau(p-1)/2$, our claim is proved. We call the $\tau$ quotients whose jacobian has good reduction over $L_0$ the *tame* Fermat quotients; the other ones are said to be *wild*. There are $w$ such wild quotients.

In an unpublished result, D. Rohrlich (see [Lim], corollary 3.4) shows that the kernel of the isogeny from $\mathrm{Jac}(F_p)$ to $\prod_{s=1}^{p-2} \mathrm{Jac}(C_s)$ consists only of $p$-torsion points. Since $\mathrm{Jac}(F_p)/\mathbb{Q}_p$ has purely additive reduction, we conclude that the prime-to-$p$ torsion subgroup of $\prod \mathrm{Jac}(C_s)(\mathbb{Q}_p^{\mathrm{unr}})$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^\tau$. It is easy to show that, if $C_s$ is wild, then the prime-to-$p$ torsion of $\mathrm{Jac}(C_s)(\mathbb{Q}_p^{\mathrm{unr}})$ must be trivial. It is therefore natural to wonder whether the prime-to-$p$ torsion of $\mathrm{Jac}(C_s)(\mathbb{Q}_p^{\mathrm{unr}})$ is cyclic of order 2 when $C_s$ is tame. When $p-1$ is a power of 2 and $C_s$ is tame, it is indeed true that the prime-to-$p$ torsion of $\mathrm{Jac}(C_s)(\mathbb{Q}_p^{\mathrm{unr}})$ is cyclic of order 2. The general case could be proved (or disproved) by computing explicitly a regular model of $C_s$ over $\mathbb{Z}_p$.

Given any positive integer $g$, the reader will find examples, in [Lor3], 4.1, of abelian varieties of dimension $g$, with potentially good reduction, for which the bound for $\Theta_{K,\ell}$ recalled in Remark 2.16 is achieved ($\ell$ odd). The following examples discuss the case where the semistable reduction of the abelian variety is not good. Once again, we will produce examples of degenerating abelian varieties using Winters' Existence Theorem [Win].

**Example 5.2.** Let $a, m, k$, and $\ell$ be integers such that $1 \leqq k, \ell \leqq m$. Set $s := \gcd(m,k)$ and $t := \gcd(m,\ell)$ and assume that $\gcd(s,t) = 1$. Consider the following graph $G(a,m,k,\ell)$:




The symbol $\overset{m}{\bullet}$ is used to denote a vertex/curve of multiplicity $m$. The notation $\bullet\overset{a}{\text{—}}\bullet$ indicates that the given vertices are linked by $a$ edges; when $a = 1$, the superscript $a$ is dropped. We use the notation


to show that the chain is continued using Euclid's algorithm as follows:

$$
\begin{aligned}
r &= c_1 r_1 - r_2 \quad \text{with} \quad r_2 < r_1 , \\
r_1 &= c_2 r_2 - r_3 \quad \text{with} \quad r_3 < r_2 , \\
\vdots &\quad \vdots \\
r_? &= \gcd(r, r_1) .
\end{aligned}
$$

The integer $-c_i$ is then the "self-intersection" of the vertex having multiplicity $r_i$.

**5.3.** We claim that the group of components associated to the graph $G(a, m, \ell, k)$ is cyclic of order $am^2/s^2t^2$. This claim can be easily proved by computing a row and column reduction of the associated intersection matrix (see Raynaud's Theorem recalled in 4.2). We leave this computation to the reader.

**5.4.** Fix an integer $n \geqq 1$ and two integers $k, \ell \leqq n$ such that

$$\gcd(k, n) = \gcd(\ell, n) = 1 .$$

Let $(G, M, R)$ denote the graph $G(1, n, k, \ell)$ with its associated intersection matrix $M$ and vector of multiplicities $R$. Let $T := (0, \ldots, 0)$ be a null vector having as many entries as the number of vertices in the graph $G$. The quadruple

$$(G, M, R, T)$$

is a *type* and, hence, Winters' Existence Theorem, recalled in 4.4, implies that there exists a field $K$ with a discrete valuation of equicharacteristic zero, and a smooth proper curve $X/K$ having a regular model $\mathscr{X}/\mathcal{O}_K$ such that:

$$(G(\mathscr{X}), M(\mathscr{X}), R(\mathscr{X}), T(\mathscr{X})) = (G, M, R, T) .$$

**Lemma 5.5.** *The curve $X/K$ has genus $n-1$ and achieves semistable reduction over a cyclic extension $L/K$ of degree $n$. If $d$ is any divisor of $n$, let $K_d$ denote the unique cyclic extension of $K$ of degree $d$. Then $X_{K_d}/K_d$ has a regular model whose reduced special fiber is the union of smooth rational curves and whose associated graph is of the form*

$$G\left(d, \frac{n}{d}, k(d), \ell(d)\right)$$

*for some positive integers $k(d)$ and $\ell(d)$ depending on $d$, and prime to $n/d$. In particular, the special fiber of the minimal (semistable) model of $X_L/L$ is the union of two rational curves intersecting transversally in $n$ points.*

*Proof.* A regular model of $X_{K_d}/K_d$ can be explicitly described using a given regular model of $X/K$. We refer the reader to Theorem 11.2 in [BPV], or to 1.9 and 1.11 in [Lor3]. The explicit computations of the base change are omitted. □

Let $A/K$ denote the jacobian of $X/K$ and let $d|n$. The group $\Phi_{K_d}(A)$ can be computed explicitly by applying 5.3 to the special fiber of the regular model of $X_{K_d}/K_d$ provided in Lemma 5.5. We then find that

$$\Phi_{K_d} = \mathbb{Z}/\left(n \cdot \frac{n}{d}\right)\mathbb{Z}.$$

The group $\Theta_{K_d}(A) := \prod_{\ell \text{ prime}} \Theta_{K_d,\ell}(A)$ can also be computed explicitly. Let $\Psi_{K_d,L}$ denote the kernel of the map $\Phi_{K_d} \to \Phi_L$. We claim that

$$\begin{array}{ccccccc} \Psi_{K_d,L} & \subseteqq & \Theta_{K_d} & \subseteqq & \Phi_{K_d} & \to & \Phi_L \\ \| & & \| & & \| & & \| \\ \mathbb{Z}/(\frac{n}{d})\mathbb{Z} & \subseteqq & \mathbb{Z}/(\frac{n}{d})^2\mathbb{Z} & \subseteqq & \mathbb{Z}/(n\cdot\frac{n}{d})\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z}. \end{array}$$

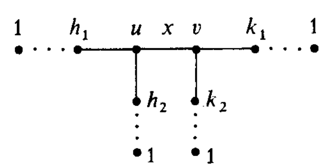
Indeed, the groups $\Phi_{K_d}$ and $\Phi_L$ are cyclic of order $n^2/d$ and $n$ respectively. Part (5) of Theorem 3.1 implies that the group $\Psi_{K_d,L}$ is killed by $[L:K_d] = n/d$. Therefore, $\Psi_{K_d,L}$ is cyclic of order $n/d$.

Since Lemma 5.5 implies that $a_{K_d} = 0$, it follows from Theorem 3.1 that

$$\Theta^{[3]}_{K_d,L} = \Theta^{[2]}_{K_d,L} = \Psi_{K_d,L}.$$

It follows from the fact that $\Theta_{K_d}/\Psi_{K_d,L}$ is isomorphic to $\Theta^{[3]}_{K_d,L}$ that $\Theta_{K_d}$ is cyclic of order $(n/d)^2$.

**Example 5.6.** We conclude this paper with a variation on the previous example. Consider the arithmetical graph $(G, M, R)$ whose graph $G = G(x, u, v, h_1, h_2, k_1, k_2)$ is as follows:




Implied in the above picture is the fact that $\gcd(u, h_i) = \gcd(v, k_i) = 1$. A row and column reduction of the matrix $M$ associated to $G$ shows that the group of components $\Phi(G)$ is cyclic of order $xuv$. We leave this computation to the reader.

**Lemma 5.7.** *Let $d \geqq c$ be any positive integers. Let $\Phi := \mathbb{Z}/\ell^{c+d}\mathbb{Z}$. Let $\Theta^{[3]} := \mathbb{Z}/\ell^c\mathbb{Z}$, and let $\Psi := \mathbb{Z}/\ell^d\mathbb{Z}$ be two subgroups of $\Phi$. There exists a discrete valuation field $K$ of equi-characteristic zero and a jacobian $A/K$ with the following properties:*

- *$A/K$ has purely additive reduction and has dimension $g = (\ell^d + \ell^c - 2)/2$.*
- *The group $\Phi_K(A)$ is isomorphic to $\Phi$.*
- *The group $\Psi_{K,L}(A)$ is isomorphic to $\Psi$ and $\delta(\Psi) = \ell^d - 1 = t_{K_\ell}(A) + 2a_{K_\ell}(A)$.*
- *The group $\Theta^{[3]}_{K,L}(A)$ is isomorphic to $\Theta^{[3]}$ and $\delta(\Theta^{[3]}) = \ell^c - 1 = t_{K_\ell}(A)$.*
- *$[L:K] = |\Psi| = \ell^d$.*

*Sketch of Proof.* We use Winters' Existence Theorem to show the existence of a curve $X/K$ having a regular model $\mathscr{X}/\mathcal{O}_K$ whose associated graph is of the form:

$$G(1, \ell^c, \ell^d, \ell^c - 1, 1, \ell^d - \ell^c - 1, 1)\,.$$

A regular model of $X_M/M$ can be computed explicitly for all extensions $K \subseteqq M$. One easily checks by direct computations that $K_\ell = L$ with $[K_\ell : K] = \ell^d$. The group $\Phi_L$ can be computed using a regular model of $X_L/L$ (4.2). The groups $\Psi_{K,L}$ and $\Theta^{[3]}_{K,L}$ are then determined with the help of Theorem 3.1. □

Note that Lemma 5.7 shows that, in general, the group $\Theta_{K,\ell}$ is not isomorphic to the direct sum

$$\Theta^{[3]}_{K,L,\ell} \oplus \Theta^{[2]}_{K,L,\ell}/\Theta^{[3]}_{K,L,\ell} \oplus \Theta_{K,\ell}/\Theta^{[2]}_{K,L,\ell}\,.$$

## References


[AnIV] Modular Functions of One Variable IV, edited by B. Birch and W. Kuyk, Lect. Notes Math. **476**, Berlin–Heidelberg–New York 1975.

[A-W] *M. Artin* and *G. Winters*, Degenerate fibers and stable reduction of curves, Topology **10** (1971), 373–383.

[BPV] *W. Barth*, *C. Peters* and *A. Van de Ven*, Compact Complex Surfaces, Berlin–Heidelberg–New York 1984.

[BLR] *S. Bosch*, *W. Lütkebohmert* and *M. Raynaud*, Néron Models, Berlin–Heidelberg–New York 1990.

[Cha] *H. Chang*, On the singularities of the Fermat scheme over $\mathbb{Z}$, Chin. J. Math. **17** no. 3 (1989), 243–257.

[C-M] *R. Coleman* and *W. McCallum*, Stable reduction of Fermat curves and Jacobi sum Hecke characters, J. reine angew. Math. **385** (1988), 41–101.

[Des] *M. Deschamps*, Réduction semistable, in: Séminaire sur les pinceaux de courbes de genre au moins deux, Astérisque **86** (1981), 1–34.

[Fad] *D. Faddeev*, Invariants of divisor classes for the curves $x^k(1-x) = y^l$ in an $\ell$-adic cyclotomic field, Tr. Mat. Inst. Steklova **64** (1961), 284–283.

[Gre] *R. Greenberg*, On the Jacobian variety of some algebraic curves, Comp. Math. **42** (1981), 345–359.

[Gr-Ro] *B. Gross* and *D. Rohrlich*, Some results on the Mordell-Weil group of the Jacobian of the Fermat Curve, Invent. Math. **44** (1978), 201–224.

[Gro] *A. Grothendieck*, Séminaire de géometrie algébrique SGA 7, I, Lect. Notes Math. **288**, Berlin–Heidelberg–New York 1970.

[L-O] *H. Lenstra* and *F. Oort*, Abelian varieties having purely additive reduction, J. Pure Appl. Alg. **36** (1985), 281–298.

[Lim] *C.H. Lim*, Endomorphisms of Jacobian varieties of Fermat curves, Comp. Math. **80** (1991), 85–110.

[Lor 1] *D. Lorenzini*, Arithmetical graphs, Math. Ann. **285** (1989), 481–501.

[Lor 2] *D. Lorenzini*, Groups of components of Néron models of Jacobians, Comp. Math. **73** (1990), 145–160.

[Lor 3] *D. Lorenzini*, Jacobians with potentially good $\ell$-reduction, J. reine angew. Math. **430** (1992), 151–177.

[Lor 4] *D. Lorenzini*, On the characteristic polynomial of a monodromy transformation attached to a family of curves, Com. Math. Helv. **68** (1993), 111–137.

[McC] *W. McCallum*, The component group of a Néron model, Preprint (1988).

[McC 2] *W. McCallum*, The Degenerate Fiber of the Fermat Curve, in: Number Theory Related to Fermat's Last Theorem, Boston 1982.

[McC 3] *W. McCallum*, Duality theorems for Néron models, Duke Math. J. **53** (1986), 1093–1124.

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

[Ray] *M. Raynaud*, Spécialisation du foncteur de Picard, Publ. Inst. Hautes Etudes Sci. **38** (1970), 27–76.

[Se-Ta] *J.-P. Serre* and *J. Tate*, Good reduction of abelian varieties, Ann. Math. **88** (1968), 492–517.

[Sil] *J. Silverman*, The Néron fiber of abelian varieties with potential good reduction, Math. Ann. **264** (1983), 1–3.

[Sil 2] *J. Silverman*, Discussion with the author, April 1988.

[Win] *G. Winters*, On the existence of certain families of curves, Amer. J. Math. **96** (1974), 215–228.


---

Department of Mathematics, University of Georgia, Athens, GA 30602

Eingegangen 9. November 1992