Uniwersytet im. Adama Mickiewicza w Poznaniu
Wydział Matematyki i Informatyki

Jędrzej Garnek

Abelian varieties over p-adic fields

**A doctoral dissertation in mathematical sciences
in the area of mathematics.
Advisor: prof. dr hab. Wojciech Gajda
Associate advisor: dr Bartosz Naskręcki**

Rozmaitości abelowe nad ciałami p-adycznymi

**Rozprawa doktorska z nauk matematycznych w zakresie matematyki.
Promotor: prof. dr hab. Wojciech Gajda
Promotor pomocniczy: dr Bartosz Naskręcki**

Poznań 2020

Abstract

In the thesis we study three problems related to arithmetic of abelian varieties over p-adic fields. The first part of the thesis studies the arithmetic complexity of p-torsion of an abelian variety over the field of p-adic numbers. This is connected to an unproven conjecture of David and Weston from 2008. We establish a relation between this problem and the notion of the canonical lift of an abelian variety. We also try to verify this conjecture for elliptic curves with complex multiplication, which leads to looking for primes in some recurrence sequences.

In the next part of the thesis we investigate the equivariant behaviour of the Hodge–de Rham exact sequence of a curve with an action of a finite group in positive characteristic. We show that if its Hodge–de Rham sequence splits equivariantly then the group action is weakly ramified. We also discuss converse statements and link this problem to lifting coverings of curves to the ring of Witt vectors of length 2. This allows us to exhibit new examples of abelian varieties without canonical lifts.

In the last part of the thesis we are concerned with the division fields of abelian varieties defined over number fields. Using Kummer theory of abelian varieties and various p-adic methods (such as the theory of Néron models and the classification theorem for compact p-adic Lie groups), we prove a lower bound on the class numbers of the division fields. This lower bound depends on the Mordell-Weil rank of A and the reduction of p-torsion points modulo primes above p.

Abstrakt

Celem tej pracy jest przedstawienie wyników dotyczących trzech problemów związanych z rozmaitościami abelowymi nad ciałami p-adycznymi. W pierwszej części rozprawy badamy arytmetyczną złożoność p-torsji rozmaitości abelowej nad ciałem liczb p-adycznych. Jest to związane z otwartym problemem, postawionym przez David i Westona w 2008 r. W pracy wskazujemy na związek tego problemu z pojęciem kanonicznego podniesienia rozmaitości abelowej. Próbujemy również zweryfikować hipotezę David i Westona dla krzywych eliptycznych z mnożeniem zespolonym, co prowadzi do poszukiwania liczb pierwszych w ciągach zadanych rekurencyjnie.

W następnej części pracy badamy ekwiwariantne zachowanie ciągu Hodge'a–de Rhama dla krzywej z działaniem grupy skończonej w dodatniej charakterystyce. Pokazujemy między innymi, że jeżeli ciąg Hodge'a–de Rhama tej krzywej rozszczepia się, to działanie to musi być słabo rozgałęzione. Omawiamy również twierdzenia odwrotne oraz wskazujemy na powiązanie tego problemu z podnoszeniem nakryć do pierścienia wektorów Witta długości 2. Pozwala nam to na wskazanie nowych przykładów rozmaitości abelowych bez kanonicznych podniesień.

Ostatnia część rozprawy dotyczy ciał podziału rozmaitości abelowych zdefiniowanych nad ciałami liczbowymi. Korzystając z teorii Kummera rozmaitości abelowych oraz różnych metod p-adycznych (takich jak teoria modeli Nérona oraz twierdzenie klasyfikacyjne dla zwartych p-adycznych grup Liego), dowodzimy dolnego oszacowania na liczbę klas ciała podziału. Oszacowanie to zależy od rangi grupy Mordella–Weila rozmaitości abelowej oraz redukcji punktów p-torsyjnych modulo ideały pierwsze leżące nad p.

Contents

Podziękowania

„Wielkim kunsztem wykazuje się
nauczyciel, który potrafi sprawić, że
twórcze wyrażanie siebie i nabywanie
wiedzy staje się źródłem radości.”
Albert Einstein

Pracę tą chciałbym zadedykować wszystkim moim nauczycielom – nie tylko tym napotkanym w szkole. W szczególności chciałbym podziękować:

- prof. drowi hab. Wojciechowi Gajdzie za siedem lat wspólnej pracy, w tym za wprowadzenie mnie w świat geometrii arytmetycznej, za niezliczone godziny dyskusji i za wszelką inną udzieloną pomoc.
- nauczycielom ze wszystkich etapów mojej edukacji – przede wszystkim pani Annie Drygas, pani Magdalenie Paul oraz panu Janowi Sibilskiemu, którzy rozbudzili moją pasję do matematyki,
- innym osobom, które zafascynowały mnie matematyką, w tym prof. drowi hab. Krzysztofowi Pawałowskiemu, drowi Bartoszowi Naskręckiemu oraz drowi Bartłomiejowi Bzdędze,
- całej mojej Rodzinie, w tym moim pierwszym Nauczycielom – Rodzicom,
- oraz Oli – za całe okazane mi wsparcie, które dawało mi siły i chęć do pracy ♡

Świadomość posiadania w swoim otoczeniu tylu osób, które życzą Ci dobrze, jest naprawdę ważna i motywująca. Chciałbym wyrazić swoją wdzięczność dla niewymienionych jeszcze osób, które również przyczyniły się do powstania artykułów: drowi Piotrowi Achingerowi, dr Bernadecie Tomasz, a także anonimowym recenzentom.

Moje badania były wspierane przez grant PRELUDIUM Narodowego Centrum Nauki o numerze UMO-2017/27/N/ST1/00497 oraz przez stypendium doktorskie Uniwersytetu im. Adama Mickiewicza w Poznaniu.

Introduction

The main field of interest of algebraic geometry are **algebraic varieties**, i.e. sets of solutions of systems of polynomial equations. An **abelian variety** is a projective algebraic variety, such that the set of its points forms a group with the group law given by some rational functions. One dimensional abelian varieties are called **elliptic curves**. The first mathematician to consider elliptic curves was probably Diophantus of Alexandria (about 200 - 284 BC). He invented a method of "doubling" points on them. Elliptic curves and Jacobians of higher genus curves appeared also in the theory of complex functions, developed by nineteenth century mathematicians. The next big step in this theory was the problem posed by Henri Poincaré:

if E is an elliptic curve defined over $\mathbb{Q}$, is the abelian group $E(\mathbb{Q})$ finitely generated?

Poincaré's question was answered positively by Louis Mordell in 1922. This and other similar problems led to the development of the field called **arithmetic geometry**. Arithmetic geometry deals with polynomial equations over small sets, such as integers, rational numbers, finite fields or p-adic numbers. In this thesis we focus on the latter ring.

The initial motivation for introducing p-adic numbers was the **Hasse principle**, stated by Helmut Hasse in 1921. It turns out that a quadratic dipohantine equation has rational solutions if and only if it has real solutions and p-adic solutions for every prime p. Nowadays, p-adic geometry has many more arithmetic applications and is a vast subfield of arithmetic geometry. We mention only the most recent results of Scholze. He introduced a new type of p-adic varieties, called **perfectoid spaces**. Perfectoid spaces allow to compare objects in positive characteristic with objects in characteristic zero. This approach led for example to the proof of certain cases of the weight-monodromy conjecture. For these results Scholze was awarded the Fields Medal in 2018.

The interplay between algebraic varieties in positive characteristic and in characteristic zero is the main topic of this thesis. We consider three problems concerning abelian varieties over p-adic fields and over fields of positive characteristic.

History of the presented results. The inital motivation for all of the results included in this thesis was the following folklore conjecture.

Conjecture 1 (Local torsion conjecture)**.** *Let E be an elliptic curve over the field of rational numbers without complex multiplication. Then for all but finitely many primes p:*

$$E(\mathbb{Q}_p)[p] = 0.$$

We started our research by introducing the notion of the (n, d)-degree of an abelian variety, which measures the arithmetic complexity of the torsion. This enabled us to reformulate and generalize Conjecture 1 (cf. Question A.2). Also, we established a relation between the (n, d)-degree and the notion of the **canonical lift** of an abelian variety. Unfortunately, we weren't able to prove neither Conjecture 1 nor to describe the behaviour of the (n, d)-degree. The problem was that it was usually hard to answer the following question.

Question 2. *How often is an abelian variety $A/\mathbb{Q}$ the canonical lift* $\bmod p^2$ *of its reduction* $\bmod p$*?*

The answer to Question 2 is straightforward only for abelian varieties with complex multiplication. Any such abelian variety is the canonical lift of its reduction for any ordinary prime. This allowed us to compute the $(p, 1)$-degree for elliptic curves with complex multiplication. It turns out that the problems concerning local torsion of elliptic curves with complex mult-plication lead to classical problems of number theory: searching for prime values of quadratic polynomials and for primes in sequences given by a linear recursion.

In order to answer Question 2, we tried to distinguish an abelian variety from its canonical lift. It turns out that canonical lift of a jacobian is *usually* not a jacobian. We tried to construct a jacobian, whose canonical lift modulo any ordinary prime p is not a jacobian $\bmod p^2$. This lead us to studying the equivariant behaviour of the Hodge–de Rham exact sequence. Finally, we managed only to construct non-ordinary jacobians with no "canonical liftings" in a certain sense.

We tried also to understand the connection between the local torsion of an abelian variety and the class numbers of its division fields. Hiranouchi gave an estimate for the class number of p^n-th division field of an elliptic curve, assuming that it has no local torsion (cf. [Hir19]). We generalized this result to abelian varieties. It turns out that the assumption on the local torsion is superfluous.

We give now a more detailed overview of the results included in this thesis.

A. Lifts of ordinary abelian varieties.

Let k be a perfect field of characteristic $p > 0$ and let R be a local ring with k as a residue field. Recall that given an abelian scheme $\mathbf{B}$ over R we may reduce it and obtain an abelian variety B/k. We will say that $\mathbf{B}$ is a **lift** of B to R. The liftings of an abelian variety B to R are described by the Serre–Tate theory. The Serre–Tate theory takes a particularly pleasant form in the case when B is an ordinary abelian variety. The set of lifts of B to R has then a natural group structure. The neutral element of this group is the **canonical lift** of the abelian variety B to the ring R. Canonical lifts have a broad scope of applications in algorithmic algebraic number theory. They are used among other things for counting points on

elliptic curves over finite fields, constructing elliptic curves over finite fields with a prescribed number of points, computing Hilbert class polynomials and constructing hyperelliptic curves suitable for cryptography. One usually considers the ring R to be $W_n(k)$, the ring of Witt vectors of length n. It is also possible to define the canonical lift of B/k to $W(k)$.

In Chapter 2 we give the following characterization of canonical lifts via their torsion.

Theorem A.1 (Theorem 2.2.1)**.** *Let B be an abelian variety of dimension g over a perfect field k of characteristic $p > 0$. Suppose that*

$$B(k)[p^n] \cong (\mathbb{Z}/p^n)^g$$

as abelian groups. Let $\boldsymbol{B}$ be a lift of B to $W(k)$. The scheme $\boldsymbol{B}_{W_n(k)}$ is the canonical lift of B to $W_n(k)$, if and only if

$$\boldsymbol{B}(W(k))[p^n] \cong (\mathbb{Z}/p^n)^g.$$

We apply this result to the problem of the local torsion of abelian varieties. Define the (n,d)**-degree** of an abelian variety A over a field K to be the number:

$$D_{n,d}(A/K) = \min\{[L:K] : A(L) \text{ contains a subgroup isomorphic to } (\mathbb{Z}/n)^d\}.$$

This quantity measures the arithmetic complexity of the n-torsion of A. Investigating the (n,d)-degree is especially interesting when A is a fixed abelian variety over the field of rational numbers $\mathbb{Q}$, which we base change to $\mathbb{Q}_p$ for a varying p. In particular it is natural to ask about the asymptotic behaviour of the p-degree:

Question A.2. *Let A be an abelian variety over $\mathbb{Q}$. Fix two positive integers n, d. Does $D_{p^n,d}(A/\mathbb{Q}_p)$ tend to infinity as p becomes large?*

We discuss related conjectures in Section 2.3. Also, we prove a theorem, which ties the Question A.2 to the notion of the canonical lift. Let $A/\mathbb{Q}_p$ be an abelian variety of dimension g with good reduction. Denote by $A_{\mathbb{Z}/p^n}$ its reduction $\bmod p^n$.

Theorem A.3 (Theorem 2.3.6)**.** *Let A be an abelian variety over $\mathbb{Q}$ of dimension g. Suppose that n is a positive integer and p is a prime of good reduction for A. If*

$$D_{p^n,g}(A/\mathbb{Q}_p) < p - 1,$$

then $A_{\mathbb{F}_p}$ is ordinary and $A_{\mathbb{Z}/p^{n+1}}$ is the canonical lift of $A_{\mathbb{F}_p}$.

A version of Theorem A.3 for elliptic curves for $n = 1$ appeared in [DW08] and in [Gar18]. In Section 2.4 we compute the $(p,1)$-degree of elliptic curves with complex multiplication.

Theorem A.4 (Theorem 2.4.1)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with complex multplication by an order of discriminant $-D$ in an imaginary quadratic field. Then for any prime p of good reduction:*

$$D_{p,1}(E/\mathbb{Q}_p) = \begin{cases} \operatorname{ord}_p(\pm s), & \text{for } \left(\frac{-D}{p}\right) = 1, \\ p^2 - 1, & \text{for } \left(\frac{-D}{p}\right) = -1, \end{cases}$$

where for p satisfying $\left(\frac{-D}{p}\right) = 1$, s is defined by the equation

$$4p = s^2 + Dt^2 \tag{A.1}$$

and, for $D = -4$, by the equation (A.1) *and the additional condition $4 \nmid s$.*

Previously, it was known that the condition $D_{p,1}(E/\mathbb{Q}_p) \in \{1,2\}$ for elliptic curves with complex multiplication is related to the existence of specific prime values of a certain quadratic polynomial, cf. [Qin16] and [JQ14]. Our results show that the local torsion problem is also connected to searching for primes in a recurrence sequence.

Corollary A.5 (Corollary 2.4.5)**.** *Let E be an elliptic curve with complex multiplication by an order in $\mathbb{Q}(i)$. Then for any prime p of good reduction we have $D_{p,1}(E/\mathbb{Q}_p) = 8$ if and only if p is of the form $a_k^2 + a_{k+1}^2$ for some $k \geq 0$, where:*

$$a_0 = 0, \qquad a_1 = 1, \qquad a_{k+2} = 4a_{k+1} - a_k.$$

It seems natural to expect that the sequence $(a_k^2 + a_{k+1}^2)_k$ contains infinitely many primes. Therefore we expect that for elliptic curves as in Corollary A.5 the answer to Question A.2 is negative. Theorem A.4 and Corollary A.5 appeared already in [Gar16], but with a different proof, which used the main theorem of complex multiplication.

B. Lifts of non-ordinary abelian varieties.

The canonical lift of an ordinary abelian variety A/k to a ring R may be characterized as the unique lift $\mathbf{A}/R$ such that

$$\mathrm{End}_R(\mathbf{A}) \cong \mathrm{End}_k(A) \tag{B.2}$$

under the natural reduction map. In Chapter 3 of this thesis we provide new examples of non-ordinary abelian varieties A without "canonical lifts" to $W_2(k)$, i.e. lifts satisfying (B.2) for $R = W_2(k)$.

Theorem B.1 (Corollary 3.4.8 and Example 3.4.6)**.** *Suppose that k is an algebraically closed field of characteristic $p > 2$. Let X/k be a smooth projective curve with the affine part given by the equation:*

$$y^m = f(z^p - z),$$

where f is a separable polynomial, $p \nmid m$ and $m \nmid \deg f$. Let A/k be the Jacobian variety of X. Then A has no lift $\boldsymbol{A}$ to $W_2(k)$ satisfying the condition (B.2)*.*

Examples of abelian varieties without "canonical lifts" in the above sense existed previously in the literature, see e.g. [Nak86, Corollary, Sec. 4], [CCO14, Theorem 3.8.3.] or [Oor92, Theorem B]. However, most of this examples do not lift to characteristic 0, whereas our example does not lift modulo p^2. To the best of our knowledge, the technique that we use to provide this example is new. To prove Theorem B.1 we use a classical result of Deligne and Illusie concerning the de Rham cohomology. We briefly recall it now.

Let X be a smooth proper algebraic variety over a field k. Recall that its de Rham cohomology may be computed in terms of Hodge cohomology via the spectral sequence

$$E_1^{ij} = H^j(X, \Omega^i_{X/k}) \Rightarrow H^{i+j}_{dR}(X/k). \tag{B.3}$$

Suppose that the spectral sequence (B.3) degenerates at the first page. This is automatic if $\mathrm{char}\, k = 0$. For a field of positive characteristic, this happens for instance if X is a smooth projective curve or an abelian variety, or (by a celebrated result of Deligne and Illusie from [DI87]) if $\dim X > \mathrm{char}\, k$ and X lifts to $W_2(k)$. Under this assumption we obtain the following exact sequence:

$$0 \to H^0(X, \Omega_{X/k}) \to H^1_{dR}(X/k) \to H^1(X, \mathcal{O}_X) \to 0. \tag{B.4}$$

If X is equipped with an action of a finite group G, the terms of the sequence (B.4) become $k[G]$-modules. In case when $\operatorname{char} k \nmid \#G$, Maschke's theorem allows one to conclude that the sequence (B.4) splits equivariantly. However, this might not be true in case when $\operatorname{char} k = p > 0$ and $p|\#G$, as was shown in [KT18]. In fact we prove in our thesis that for curves the sequence (B.4) *usually* does not split equivariantly.

Let X be a curve over an algebraically closed field of characteristic $p > 0$ with an action of a finite group G. For $P \in X$, denote by $G_{P,n}$ the n-th ramification group of G at P. Following [Köc04], we say that the action of G on X is **weakly ramified** if $G_{P,2} = 0$ for every $P \in X$.

Theorem B.2 (Theorem 3.4.5)**.** *Suppose that X is a smooth projective curve over an algebraically closed field k of characteristic $p > 2$ with an action of a finite group G. If the sequence* (B.4) *for the curve X splits G-equivariantly, then the action of G on X is weakly ramified.*

As far as we are concerned, this criterion is new in the literature. Previous results in this direction apply only to hyperelliptic curves (cf. [Hor12] and [KT18]). The main idea of the proof of Theorem B.2 is to compare $H^1_{dR}(X/k)^G$ and $H^1_{dR}(Y/k)$, where $Y := X/G$. The discrepancy between those groups is measured by the sheafified version of group cohomology, introduced by Grothendieck in [Gro57]. This allows us to compute the defect

$$\begin{aligned} \delta(X,G) &:= \dim_k H^0(X,\Omega_{X/k})^G + \dim_k H^1(X,\mathcal{O}_X)^G \\ &- \dim_k H^1_{dR}(X/k)^G \end{aligned}$$

in terms of some local terms connected to Galois cohomology, cf. Proposition 3.2.1. We compute these local terms in case of Artin-Schreier coverings (cf. Corollary 3.3.7). This special case allows us to finish the proof of Theorem B.2.

The natural question arises: *to what extent is the converse of Theorem B.2 true?* We provide some partial answers. In characteristic 2, we were able to produce a counterexample (cf. Subsection 3.6). We also prove some positive results. In particular, we obtain the following theorem.

Theorem B.3 (Theorem 3.5.1)**.** *If the action of G on a smooth projective curve X over an algebraically closed field k is weakly ramified, then the sequence*

$$0 \to H^0(X,\Omega_{X/k})^G \to H^1_{dR}(X/k)^G \to H^1(X,\mathcal{O}_X)^G \to 0$$

is exact also on the right.

To derive Theorem B.3 we use the method of proof of Theorem B.2 and a result of Köck from [Köc04].

We were also able to show the splitting of the Hodge-de Rham exact sequence of a curve with a weakly ramified group action under some additional assumptions.

Theorem B.4 (Lemma 3.5.4, Corollary 3.4.7 and Corollary 3.4.4)**.** *Let X be a curve over an algebraically closed field of characteristic $p > 0$ with an action of a finite group G. The sequence* (B.4) *splits, provided that at least one of the following conditions holds:*

(1) the action of G on X is weakly ramified and the p-Sylow subgroup of G is cyclic,

(2) the action of G on X lifts to $W_2(k)$,

(3) X is ordinary.

Note that the conditions (1), (2), (3) of Theorem B.4 do not imply one another.

C. Class numbers of division fields.

In the final chapter we apply the methods from previous chapters in order to obtain lower bounds on class numbers of division fields of abelian varieties. Let us fix a prime p. Let A be an abelian variety of dimension g defined over $\mathbb{Q}$. Let us consider the p^n-th division field of A:

$$K_n := \mathbb{Q}(A[p^n]).$$

Let $\mathrm{Cl}(K_n)$ be the ideal class group of K_n, defined as the quotient of the group of fractional ideals of the ring of integers of K_n by the subgroup of principal ideals. Denote also the reduction of A to $\mathbb{F}_p$ by A_p.

Theorem C.1 (Corollary 4.1.5). *Let $A/\mathbb{Q}$ be an abelian variety of dimension g and rank r over $\mathrm{End}_{\mathbb{Q}}(A)$. If either of the following condition holds:*

- *$r \geq 1$ and A has good reduction at p with positive p-rank, i.e. $A_p(\overline{\mathbb{F}}_p)[p] \neq 0$, or*
- *$r > g$,*

then:

$$\lim_{n\to\infty} \#\,\mathrm{Cl}(K_n) = \infty.$$

In fact, we obtained estimates on $\#\,\mathrm{Cl}(K_n)$ for abelian varieties over arbitrary number fields (cf. Theorem 4.1.4). Previous estimates on class numbers of division fields were given in two cases:

- for abelian varieties with complex multiplication (cf. [Gre01] and [FKY07]),
- for elliptic curves over $\mathbb{Q}$ under some additional assumptions on p, including surjectivity of the Galois representation mod p and vanishing of p-torsion in $\mathbb{Q}_p$ (cf. [SY15], [SY18] and [Hir19]).

The article [Ohs20] (published after [Gar19b]) proves a bound similar to that in Theorem C.1 in a more general setting, for Galois representations satisfying certain conditions. The mentioned article uses a different method from ours, namely the theory of Selmer groups.

The basic idea of our proof of Theorem C.1 is to find a large unramified abelian extension of K_n inside the Kummer extension L_n (cf. Section 1.2.6 for the relevant definitions). The Bashmakov-Ribet theory of Kummer extensions (cf. [Bas72] and [Rib79]) provides us a monomorphism with bounded cokernel:

$$\Gamma^{(\infty)} : \mathrm{Gal}(L_\infty/K_\infty) \to T_p(A)^{\oplus r},$$

where $K_\infty = \bigcup_n K_n$, $L_\infty = \bigcup_n L_n$. This allows us to estimate the degree $[L_n : K_n]$. The rest of the proof of Theorem C.1 focuses on estimating inertia groups in Kummer extensions. The basic tools to this end are the classification theorem for compact p-adic Lie groups and the theory of Néron models. In order to illustrate our estimates of class numbers we offer a numerical example in Section 4.5.

Structure of the thesis. Chapter 1 presents some preliminaries for the convenience of the reader. Sections A, B, C of the Introduction summarize the results of Chapters 2, 3 and 4 respectively. Chapter 2 partially generalizes the results of the paper [Gar18]. The material presented in Chapters 3 and 4 follows closely the published article [Gar19b] and preprint [Gar19a] and differs only in exposition.

1 Preliminaries

In this chapter we present some preliminary results concerning algebra and geometry. First, in Section 1.1 we treat the basics of group objects and group schemes. Then, in Section 1.2 we recall a few necessary properties of abelian varieties and abelian schemes. Next, in Sections 1.3 and 1.4 we give a brief introduction to the de Rham cohomology and the group cohomology of sheaves. Finally, we present in Section 1.5 some basic results in algebraic number theory. The basic references for this chapter are [Tat97], [Sha86], [Mum08], [BLR90] and [Neu99].

Notations and conventions: by a ring we will always mean a commutative ring with unity. For a given category $\mathscr{A}$, $\mathrm{Ob}(\mathscr{A})$ denotes the class of its objects and $\mathrm{Hom}_{\mathscr{A}}(A, B)$ is the class of morphisms between two objects A and B of $\mathscr{A}$. Regarding algebraic geometry, we follow the notation of [Har77]. For a more complete list of notation, see page 69.

1.1. Group schemes

1.1.1. Definitions and examples

Let $\mathscr{A}$ be a category with an initial object 1 and with finite products.

Definition 1.1.1. We say that an object G of $\mathscr{A}$ together with morphisms

$$\mu \in \mathrm{Hom}_{\mathscr{A}}(G \times G, G), \quad \varepsilon \in \mathrm{Hom}_{\mathscr{A}}(1, G), \quad \mathrm{inv} \in \mathrm{Hom}_{\mathscr{A}}(G, G)$$

is a **group object** in the category $\mathscr{A}$, if for every $T \in \mathrm{Ob}(\mathscr{A})$ the set $G(T) := \mathrm{Hom}_{\mathscr{A}}(T, G)$ has a group structure given by $\mu, \varepsilon, \mathrm{inv}$.

Let S be a noetherian scheme. An **S-group scheme** is defined to be a group object in $\mathbf{Sch}/S$, the category of schemes over S. In case when $S = \operatorname{Spec} R$ for a ring R, we will refer to S-group schemes simply as **R-group schemes**. One may define a morphism of S-group schemes as a morphism of S-schemes commuting with μ, ε and inv. Below we give standard examples of group schemes:

- the **additive group scheme** $\mathbb{G}_{a,S}$ over S,
- the **multiplicative group scheme** $\mathbb{G}_{m,S}$ over S,
- the **constant group scheme** $\underline{\Gamma}_S$ with fiber Γ (where Γ is an abstract group),
- the **group scheme of n-th roots of unity** $\mu_{n,S}$.

By abuse of notation, we will write $\mathbb{G}_m$ instead of $\mathbb{G}_{m,S}$, etc. if no confusion can arise. Suppose that G is a commutative group scheme over a base scheme S and n is an integer. The **multiplication–by–n** morphism

$$[n] : G \to G$$

is defined by letting $[n] : G(T) \to G(T)$ to be the multiplication by n for any $T \in \mathrm{Ob}(\mathbf{Sch}/S)$. Its kernel is denoted by $G[n]$.

1.1.2. Algebraic groups

Let K be a field. A **K-algebraic group** is a group object in the category of algebraic varieties over K. The group schemes $\mathbb{G}_a$, $\mathbb{G}_m$, Gl_n are algebraic groups. Algebraic groups share many properties with Lie groups. In particular, one can define the Lie algebra $\mathrm{Lie}\, G$ of an algebraic group G. The dimension of $\mathrm{Lie}\, G$ as a K-vector space equals the dimension of G. The following lemma will be used in the sequel.

Lemma 1.1.2. *Let G be a connected commutative algebraic group over an algebraically closed field K. Then for any n relatively prime to* $\mathrm{char}\, K$ *the multiplication-by-n morphism*

$$[n] : G(K) \to G(K)$$

is surjective.

Proof. Let $H := [n]G$ be the image of G under the multiplication-by-n morphism. Note that H is a closed subgroup (images of morphisms of algebraic groups are closed, cf. [MT11, Proposition 1.5]). The differential $d[n] : \mathrm{Lie}(G) \to \mathrm{Lie}(G)$ is the multiplication by n on the Lie algebra of G. Since $\mathrm{char}\, K \nmid n$, it is an isomorphism on $\mathrm{Lie}(G)$ and thus:

$$\mathrm{Lie}(\ker d[n]) = \ker\left(d[n] : \mathrm{Lie}(G) \to \mathrm{Lie}(G)\right) = 0.$$

Hence $\dim \ker[n] = 0$ and $\dim H = \dim G$. This yields $H = G$. □

Affine algebraic groups are usually referred to as the **linear algebraic groups**. Every linear algebraic group is a closed subgroup of Gl_n for some n. An **abelian variety** is a projective algebraic group over K. It turns out that the group law on an abelian variety must be automatically commutative. We discuss more properties of abelian varieties in Section 1.2. By a theorem of Chevalley (cf. [Con02]) any connected algebraic group over an algebraically closed field is an extension of an abelian variety by a connected linear algebraic group.

1.1.3. Finite flat group schemes

Another important class of group schemes consists of those that are finite and flat over the base scheme S, since they share many properties with abstract finite groups. For example, for any finite flat group scheme G/S it is possible to define its rank, which we denote by $\#G$. We refer to [Tat97] or [Sha86] for relevant definitions. Here are two simple examples of finite flat group schemes:

- if Γ is a finite group then $\underline{\Gamma}$ is a finite flat group scheme and $\#\underline{\Gamma} = \#\Gamma$,
- μ_n is a finite flat group scheme of rank n.

From now on, we will focus on group schemes over an affine base scheme $S = \mathrm{Spec}\, R$. Also, we will use the following notation (unless stated otherwise).

Setup 1.1.3. R is a complete local ring with a maximal ideal $\mathfrak{p}$ and a perfect residue field k of characteristic $p > 0$.

Recall that if Γ is a topological group and its connected component of identity Γ^0 is open, then the group of components Γ/Γ^0 is discrete. A similar theorem might be stated for finite flat group schemes over R.

Proposition 1.1.4 (connected-étale exact sequence, [Sha86, p. 43])**.** *Let R and k be as defined in Setup 1.1.3. Let G be a commutative finite flat group scheme over R with the connected component of identity G^0. Then G^0 is a normal subgroup and the quotient $G^{et} := G/G^0$ is étale over R. The exact sequence:*

$$0 \to G^0 \to G \to G^{et} \to 0$$

is called the ***connected-étale exact sequence*** *of G. If $R = k$, then the sequence splits.*

Let $\mathbf{GS}/S$ denote the category of finite flat commutative S-group schemes. The category $\mathbf{GS}/S$ is abelian and thus we may define the Ext functors in the sense of Yoneda (cf. [Wei94, Vista 3.4.6]). Equivalently, one may compute Ext of commutative group schemes as the usual Ext in the category of abelian fppf-sheaves on S. The following result will be used in the sequel.

Proposition 1.1.5. *Let R be as in the Setup 1.1.3. Then for every $n \geq 1$:*

$$\mathrm{Ext}^1_{\boldsymbol{GS}/R}(\underline{\mathbb{Z}/n}, \mu_n) \cong R^\times/R^{\times n}.$$

Proof. Note that $\Gamma(\operatorname{Spec} R, -) = \operatorname{Hom}(\underline{\mathbb{Z}/n}, -)$ as functors on the category of n-torsion abelian fppf sheaves on R. Thus:

$$\mathrm{Ext}^1_{\mathbf{GS}/R}(\underline{\mathbb{Z}/n}, \mu_n) \cong R^1 \operatorname{Hom}(\underline{\mathbb{Z}/n}, -)(\mu_n) \cong R^1\Gamma(\operatorname{Spec} R, -)(\mu_n) \cong H^1_{fppf}(\operatorname{Spec} R, \mu_n)$$

and the proof follows by [Mil80, example II.2.18. (b), p. 66]. □

Let G be a commutative finite flat R-group scheme. The functor $\underline{Hom}(G, \mathbb{G}_m)$ is represented by a commutative finite flat group scheme $G^\vee$, called the **Cartier dual** of G. One checks that $(G^\vee)^\vee \cong G$ and that $\#G^\vee = \#G$. We say that a group scheme G is **of multiplicative type**, if $G^\vee$ is an étale group scheme. A crucial property of group schemes of multiplicative type is that they are "rigid", i.e. they can not be deformed in an appropriate sense.

Proposition 1.1.6 ([Lan13, Theorem 3.1.1.1])**.** *Let G be a group scheme of multiplicative type over a field k and let R be an Artin local ring with k as a residue field.*

(1) There exists (up to a unique isomorphism) a unique group scheme G^{can} over R such that $G^{can} \times_R k \cong G$. We call it the ***canonical lift*** *of G to R.*

(2) Let $\boldsymbol{H}$ be an R-group scheme and let $H := \boldsymbol{H} \times_R k$. Each morphism of k-group schemes $f : G \to H$ can be uniquely lifted to a morphism $\boldsymbol{f} : G^{can} \to \boldsymbol{H}$.

The following proposition is a consequence of results of Raynaud from [Ray74].

Proposition 1.1.7 ([Tat97, Theorem 4.5.1.])**.** *Let $L/\mathbb{Q}_p$ be a finite extension with the ramification index $e < p - 1$. Let $\boldsymbol{G}_1, \boldsymbol{G}_2$ be commutative finite flat $\mathcal{O}_L$-group schemes of p-power order. If $(\boldsymbol{G}_1)_K \cong (\boldsymbol{G}_2)_K$, then $\boldsymbol{G}_1 \cong \boldsymbol{G}_2$.*

We introduce now p-divisible groups. A p-divisible group is a special kind of formal group, that is a "limit" of finite flat group schemes of p-power order.

Definition 1.1.8. A **p-divisible group** of height h over R is a sequence $(G_n)_n$ of commutative finite flat group schemes over R such that $\#G_n = p^{nh}$, $G_n \subset G_{n+1}$ and $G_n = \ker([p^n] : G_{n+1} \to G_{n+1})$. We will denote the category of p-divisible groups over R by p-**div**$/R$.

The two most important examples of p-divisible groups, from our point of view, are $\underline{\mathbb{Q}_p/\mathbb{Z}_p} := (\underline{\mathbb{Z}/p^n})_n$ and $\mu_{p^\infty} := (\mu_{p^n})_n$. Many properties of finite flat group schemes may be generalized to p-divisible groups. A p-divisible group $(G_n)_n$ is étale (resp. connected, ...), if G_n is étale (resp. connected, ...) for all n. In particular, one may also define the **connected-étale exact sequence** for a p-divisible group.

1.1.4. Formal groups

For a reference of the mentioned facts see [Ser92]. Keep the Setup 1.1.3.

Definition 1.1.9. A **formal group** over R is a group object in the category of formal schemes over $\operatorname{Spf} R$, the formal spectrum of R. We say that a formal group $\mathcal{G}$ over R is **smooth** of dimension g, if its underlying formal scheme is isomorphic to $\operatorname{Spf} R[[x_1, \ldots, x_g]]$ for some $g \geq 0$.

Note that every smooth formal group $\mathcal{G}$ over R is given by a collection of g power series:

$$F_{\mathcal{G}} = (F_i(\mathbf{x}, \mathbf{y}))_{i=1,\ldots,g},$$

(where $F_i \in R[[\mathbf{x}, \mathbf{y}]]$, $\mathbf{x} = (x_1, \ldots, x_g)$ and $\mathbf{y} = (y_1, \ldots, y_g)$) such that:

- $F_{\mathcal{G}}(\mathbf{x}, \mathbf{y}) = \mathbf{x} + \mathbf{y} +$ terms of higher degree,
- (associativity) $F_{\mathcal{G}}(\mathbf{x}, F_{\mathcal{G}}(\mathbf{y}, \mathbf{z})) = F_{\mathcal{G}}(F_{\mathcal{G}}(\mathbf{x}, \mathbf{y}), \mathbf{z})$,
- (neutral element) $F_{\mathcal{G}}(\mathbf{x}, 0) = \mathbf{x}$, $F_{\mathcal{G}}(0, \mathbf{y}) = \mathbf{y}$,
- (inverse element) there exists a unique tuple of power series without constant terms $i(\mathbf{x}) = (i_1(\mathbf{x}), \ldots, i_g(\mathbf{x}))$ such that $F_{\mathcal{G}}(\mathbf{x}, i(\mathbf{x})) = F_{\mathcal{G}}(i(\mathbf{y}), \mathbf{y}) = 0$.

A smooth formal group $\mathcal{G}$ is commutative, if $F_{\mathcal{G}}(\mathbf{x}, \mathbf{y}) = F_{\mathcal{G}}(\mathbf{y}, \mathbf{x})$. It turns out that for a smooth formal group $\mathcal{G}$, the group $\mathcal{G}(R)$ has $\mathfrak{p}^{\oplus g}$ as the underlying set and the group law:

$$\mathbf{x} \oplus_{\mathcal{G}} \mathbf{y} := F_{\mathcal{G}}(\mathbf{x}, \mathbf{y}). \tag{1.1}$$

By abuse of notation, we denote by $\mathcal{G}(\mathfrak{p}^i)$ the topological group with the underlying space $(\mathfrak{p}^i)^{\oplus g}$ and the group law given by the formula (1.1), in particular $\mathcal{G}(R) = \mathcal{G}(\mathfrak{p})$.

Suppose now that G is a smooth group scheme over R. Then the completion of G along the identity section, denoted $\widehat{G}$, is a smooth formal group.

Proposition 1.1.10 ([CX08, 2.5])**.** *Keep the Setup 1.1.3 and let G, $\widehat{G}$ be as above. The kernel of the reduction homomorphism:*

$$G(R) \to G(R/\mathfrak{p}^n)$$

is topologically isomorphic to $\widehat{G}(\mathfrak{p}^n)$.

Suppose now that $\mathcal{G}$ is a commutative smooth formal group. Just as in the case of group schemes, one defines the **multiplication-by-n morphism** $[n] : \mathcal{G} \to \mathcal{G}$. For a future use we note the following properties.

(1.2) One has:

$$[n](\mathbf{x}) = n\mathbf{x} + \text{terms of higher degree.}$$

(1.3) If $p \nmid n$ then $[n] : \mathcal{G} \to \mathcal{G}$ is an isomorphism of formal groups. In particular, $\mathcal{G}(R)$ has no prime-to-p torsion.

(1.4) Suppose that v is a discrete valuation on R, $v(R \setminus \{0\}) = \{0\} \cup \mathbb{Z}_+$. Then for $i > \frac{v(p)}{p-1}$ we have an isomorphism of topological groups:

$$\mathcal{G}(\mathfrak{p}^i) \cong (\mathfrak{p}^i)^{\oplus g}.$$

We end this section with the following definition.

Definition 1.1.11. Let R be a ring of characteristic $p > 0$ and suppose that $\mathcal{G}$ is a commutative smooth formal group of dimension g over R. The **height of $\mathcal{G}$** is defined as the largest integer h such that:

$$[p](\mathbf{x}) = (H_1(\mathbf{x}^{p^h}), \ldots, H_g(\mathbf{x}^{p^h}))$$

for some $H_1, \ldots, H_g \in R[x_1, \ldots, x_g]$ (where $\mathbf{x}^n := (x_1^n, \ldots, x_g^n)$).

1.2. Abelian varieties and abelian schemes

The notion of an abelian variety may be generalized to an arbitrary base scheme S: an **abelian scheme over** S is a smooth group scheme over S, the fibres of which are abelian varieties. The goal of this section is to give a brief overview of the most important facts concerning abelian varieties and abelian schemes which we will use in the sequel. For a detailed account of the theory of abelian varieties we refer to [Mum08].

Setup 1.2.1. Throughout this section, A will be an abelian variety of dimension g over a field K, unless stated otherwise. In case when A_1, A_2 are abelian varieties over K, we will denote by $\mathrm{Hom}_K(A_1, A_2)$ the set of morphisms $A_1 \to A_2$ of algebraic groups over K. In particular, we denote $\mathrm{End}_K(A) := \mathrm{Hom}_K(A, A)$.

1.2.1. Abelian varieties over complete fields

In this subsection we discuss the structure of $A(K)$ for some complete fields K.

In case when $K = \mathbb{C}$ every abelian variety is isomorphic (as a complex Lie group) to a manifold of the form $\mathbb{C}^g/\Gamma$, where $\Gamma \subset \mathbb{C}^g$ is a lattice of a full rank. In particular, we may decribe the group structure of the n-torsion:

$$A[n] \cong (\mathbb{Z}/n)^{2g}. \tag{1.5}$$

Consider now the case $K = \mathbb{R}$. In this case $A(K)$ is a compact Lie group, and thus its identity component must be isomorphic to the group $(\mathbb{S}^1)^g$, where $\mathbb{S}^1$ denotes the unit circle. It turns out that it is possible to describe the group of components of $A(\mathbb{R})$.

Proposition 1.2.2 (cf. [GH81, Proposition 1.1 (c)]). *Suppose that A is an abelian variety over $\mathbb{R}$ of dimension g. Then, as Lie groups:*

$$A(\mathbb{R}) \cong (\mathbb{S}^1)^g \times (\mathbb{Z}/2)^t$$

for some $0 \leq t \leq g$.

Finally, we come to the case of the p-adic fields. In this case we can use the classification theorem of compact p-adic Lie groups (cf. [CL19, Thm. 21]) to deduce the following fact.

Theorem 1.2.3. *Let $K/\mathbb{Q}_p$ be a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}_K$. Let A be an abelian variety of dimension g. Then $A(K)_{tors}$ is a finite group and we have an isomorphism of topological groups:*

$$A(K) \cong A(K)_{tors} \oplus \mathcal{O}_K^g.$$

1.2.2. Torsion of abelian varieties

It turns out that for an algebraically closed field we have a description of torsion analogous to (1.5):

- if $\operatorname{char} K \nmid n$:
$$A[n](\overline{K}) \cong (\mathbb{Z}/n)^{2g},$$
- if $\operatorname{char} K = p > 0$, then there exists a number $0 \leq r(A) \leq g$ (the **p-rank of A**), such that for every $a \geq 1$:
$$A[p^a](\overline{K}) \cong (\mathbb{Z}/p^a)^{r(A)}. \tag{1.6}$$

Definition 1.2.4. Suppose that $\operatorname{char} K = p > 0$. We say that an abelian variety A is **ordinary**, if $r(A) = g$.

Lemma 1.2.5. *Let K be a field of characteristic $p > 0$. The following conditions are equivalent:*

(1) A is ordinary,

(2) $A[p^n]$ is a group scheme of multiplicative type for some (equivalently all) n,

(3) the étale-connected sequence for the finite flat group scheme $A_{\overline{K}}[p^n]$ is of the form:

$$0 \to \mu_{p^n}^{\oplus g} \to A_{\overline{K}}[p^n] \to (\underline{\mathbb{Z}/p^n})^{\oplus g} \to 0$$

for some (equivalently all) n,

(4) the étale-connected sequence for the p-divisible group $A_{\overline{K}}[p^\infty]$ is of the form:

$$0 \to \mu_{p^\infty}^{\oplus g} \to A_{\overline{K}}[p^\infty] \to (\underline{\mathbb{Q}_p/\mathbb{Z}_p})^{\oplus g} \to 0.$$

It turns out that a generic abelian variety over an algebraically closed field of characteristic $p > 0$ is ordinary, see e.g. [Pri08, §3.1] for a precise statement. An unproven conjecture of Serre asserts that for any abelian variety A over a number field K there exist infinitely many primes $\mathfrak{p}$ such that A has good ordinary reduction at $\mathfrak{p}$. This is known to be true for elliptic curves (cf. [Ser89]) and for abelian surfaces (cf. [Ogu81]).

The following definition allows to gather the information about the ℓ-primary torsion into one object.

Definition 1.2.6. Let ℓ be a prime. The **ℓ-adic Tate module** of an abelian variety A/K is defined as:

$$T_\ell A := \lim_{\leftarrow} A[\ell^n](\overline{K}).$$

Let $G_K := \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K. One easily checks that $T_\ell A$ is a G_K-module. Therefore we obtain the ℓ-adic representation of G_K:

$$\rho_\ell : G_K \to \mathrm{Aut}(T_\ell A)$$

Note that when $\ell \neq \mathrm{char}\, K$ and A is principally polarized, $\mathrm{Aut}(T_\ell A) \cong \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$. It turns out that in many cases the image of ρ_ℓ is as big as possible. Indeed, if one of the following conditions is satisfied:

- g equals 2, 6 or is odd and A is a principally polarized abelian variety of dimension g with $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$ (cf. [Ser13, Theorem 3]),

- $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$, K is finitely generated over its prime field and K has a discrete valuation at which A has a semistable reduction of toric dimension one (this follows from [Hal11] or [AdRGP13, Main Theorem] and [Lar95, Theorem 1.1]),

then $\rho_\ell(G_K)$ contains $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ for almost all ℓ. For elliptic curves and abelian surfaces with $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$ one can determine numerically the finite set of primes, outside of which the representation is surjective (cf. [Sut16] for elliptic curves and [Die02] for abelian surfaces).

1.2.3. Complex multiplication

Recall that a number field M is a **CM-field** if it is a totally imaginary quadratic extension of a totally real number field M^+. We say that an abelian variety A/K of dimension g has **complex multiplication** by M, if $\mathrm{End}_{\overline{K}}(A)$ is an order in M and $[M : \mathbb{Q}] = 2g$. In the sequel we will need the following two facts regarding abelian varieties with complex multiplication.

Lemma 1.2.7 (Deuring's criterion for abelian varieties, cf. [Bla14])**.** *Suppose that K is a finite field of characteristic $p > 0$ and that A/K has complex multiplication by a CM field M.*

(1) If p splits completely in M, then A is ordinary.

(2) If p splits completely in M^+ and every prime of M^+ above p stays inert in M, then $r(A) = 0$.

Lemma 1.2.8. *Let A be an abelian variety defined over a field K Galois over $\mathbb{Q}$ and with complex multiplication by the CM field $L \subset \overline{K}$. Then:*

$$\mathrm{End}_{\overline{K}}(A) = \mathrm{End}_{LK}(A).$$

Recall that there are finitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves $E/\mathbb{Q}$ with complex multiplication (cf. [Sil94, A §3] for a full list of them). Each of them has a complex multiplication by an order in an imaginary quadratic field of class number one.

1.2.4. Reduction of an abelian variety

The main reference for this subsection is [BLR90]. We will use the following notation.

Setup 1.2.9. Let K be a field of fractions of a Dedekind domain R with a maximal ideal $\mathfrak{p}$. Suppose that $k := R/\mathfrak{p}$ is a perfect field of characteristic $p > 0$.

Definition 1.2.10. A Néron model of A over R is a smooth group scheme $\mathcal{A}$ over R such that $\mathcal{A}_K \cong A$ and that the following **Néron mapping property** holds: for any smooth separated R-scheme $\mathbf{X}$, any K-morphism $\mathbf{X}_K \to A$ may be extended to a unique R-morphism $\mathbf{X} \to \mathcal{A}$.

Any abelian variety over K has a Néron model over R, which is unique up to an isomorphism. Let $\mathcal{A}/R$ be the Néron model of an abelian variety A/K. For any R-algebra B we will denote by abuse of notation $A_B := \mathcal{A}_B$. Also, let $A_\mathfrak{p} := A_{R/\mathfrak{p}}$ be the fiber of $\mathcal{A}$ over $\mathfrak{p}$. The scheme $A_\mathfrak{p}$ is an algebraic group over k. We denote the connected component of the identity in $A_\mathfrak{p}$ by $A_\mathfrak{p}^0$ and by $\Phi_{A_\mathfrak{p}} = A_\mathfrak{p}/A_\mathfrak{p}^0$ the group scheme of geometric components. The group $\Phi_{A_\mathfrak{p}}(\overline{\mathbb{F}}_\mathfrak{p})$ is finite and its order is called the Tamagawa number of A at $\mathfrak{p}$.

The Néron model allows us to reduce the points of A modulo any prime ideal $\mathfrak{p}$ of R. Note that using the Néron mapping property we obtain an isomorphism $A(K) \cong \mathcal{A}(R)$. Moreover, by the universal property of fiber product, $\mathcal{A}(k) \cong A_\mathfrak{p}(k)$. This allows us to define the **reduction homomorphisms:**

$$\mathrm{red}_\mathfrak{p} : A(K) \cong \mathcal{A}(R) \to \mathcal{A}(k) \cong A_\mathfrak{p}(k)$$

and

$$\mathrm{red}_{\mathfrak{p},n} : A(K) \cong \mathcal{A}(R) \to \mathcal{A}(R/\mathfrak{m}^n).$$

The following result is a geometric version of Hensel's lemma.

Lemma 1.2.11 ([BLR90, 2.3, Proposition 5])**.** *If R is a complete local ring, then the maps $\mathrm{red}_{\mathfrak{p},n}$ are surjective for all $n \geq 0$.*

Definition 1.2.12. If there exists an abelian scheme $\mathbf{A}/R$ with A as the generic fiber, we say that A/K has **good reduction** over R. We say that A has **good reduction at $\mathfrak{p}$**, if it has good reduction over $R_\mathfrak{p}$ (the localisation of R at $\mathfrak{p}$). Otherwise, we say that A/K has **bad reduction at $\mathfrak{p}$**.

Lemma 1.2.13 ([BLR90, 7.4, Theorem 5])**.** *The following conditions are equivalent:*

(1) A has good reduction at $\mathfrak{p}$,

(2) $A_\mathfrak{p}$ is an abelian variety,

(3) the Néron model of A over $R_\mathfrak{p}$ is proper,

(4) the Néron model of A over $R_\mathfrak{p}$ is an abelian scheme,

(5) (Néron-Ogg-Shafarevich criterion) *the inertia group*

$$I_K := \ker\left(G_{\widehat{K}_\mathfrak{p}} \to G_k\right)$$

(where $\widehat{K}_\mathfrak{p}$ is the completion of K at $\mathfrak{p}$) acts trivially on $T_\ell A$ for $\ell \neq p$.

Note also that any abelian scheme over R is the Néron model of its generic fiber.

Remark 1.2.14. *Let L/K be an algebraic extension of fields and let B be the integral closure of R in L. Let $\mathcal{P}$ be a prime ideal of B over $\mathfrak{p}$. Suppose that $\mathcal{A}_B$ is the Néron model of A_L over B. This happens for example if one of the following conditions holds:*

- *L/K is unramified (since the formation of the Néron model commutes with étale base change – cf. [BLR90, Proposition 1.2.2]),*
- *A has good reduction (since $\mathcal{A}_B$ is an abelian scheme over B).*

Under this assumption the reduction homomorphism extends to

$$\mathrm{red}_{\mathfrak{p}} : A(L) \cong \mathcal{A}(B) \to \mathcal{A}(B/\mathcal{P}) \cong A_{\mathfrak{p}}(B/\mathcal{P}).$$

In some cases we can describe the kernel of the reduction homomorphism, using the theory from Subsection 1.1.4. Let $\mathcal{A}/R$ be the Néron model of an abelian variety A/K and let $\widehat{\mathcal{A}}$ be the completion of $\mathcal{A}$ along the zero section. Then:

(1.7) if R is a complete discrete valuation ring, then by Proposition 1.1.10:

$$\ker \mathrm{red}_{\mathfrak{p},n} = \widehat{\mathcal{A}}(\mathfrak{p}^n),$$

(1.8) if $R = k$ is a perfect field of characteristic p, then the height of $\widehat{\mathcal{A}}/k$ equals:

$$2g - r(A)$$

(this may be proven using (1.7)).

1.2.5. Lifts of an abelian variety

Let A be an abelian variety of dimension g over a perfect field K of positive characteristic p. Denote by Art_K the category of local Artin rings with K as a residue field. We say that an abelian scheme A over $R \in \mathrm{Ob}(\mathrm{Art}_K)$ together with an isomorphism is

By a **lift** of A to a ring $R \in \mathrm{Ob}(\mathrm{Art}_K)$ we will understand any abelian scheme $\mathbf{A}$ over R together with an isomorphism $\mathbf{A} \times_R K \cong A$. In this way we obtain a functor:

$$\begin{array}{rcl} \mathrm{Def}_{A/K} : \mathrm{Art}_K & \longrightarrow & \mathrm{Set} \\ R & \longmapsto & \left\{ \begin{array}{c} \text{isomorphism classes} \\ \text{of lifts of } A \text{ to } R \end{array} \right\}. \end{array} \tag{1.9}$$

Let $\mathbf{A}$ be an abelian scheme over a ring R of relative dimension g. The group scheme $\mathbf{A}[n]$ is finite flat of rank n^{2g} over R. Thus for any prime p we can associate to $\mathbf{A}$ its **p-divisible group** $\mathbf{A}[p^\infty] := (\mathbf{A}[p^n])_n$. The height of $\mathbf{A}[p^\infty]$ equals $2g$. It turns out that the lifts of A/K to R are determined by the lifts of the p-divisible group of A. For an arbitrary p-divisible group G over K, we define the functor $\mathrm{Def}_{G/K} : \mathrm{Art}_K \to \mathrm{Set}$ in analogy with (1.9).

Theorem 1.2.15 (Serre-Tate, cf. [Kat81, Theorem 1.2.1])**.** *If A is an abelian variety over a perfect field K of characteristic p, then the natural transformation of functors:*

$$\begin{array}{rcl} \mathrm{Def}_{A/K} & \to & \mathrm{Def}_{A[p^\infty]/K} \\ \boldsymbol{A} & \mapsto & \boldsymbol{A}[p^\infty] \end{array}$$

is an isomorphism.

1.2.6. Kummer theory for abelian varieties

We fix a prime p. Denote by K a number field with the ring of integers $\mathcal{O}_K$. Let A be an abelian variety of dimension g defined over K. Let K_n denote the p^n-th division field of A:

$$K_n := K(A[p^n]).$$

For any point $P \in A(\overline{K})$ and $N \in \mathbb{N}$, the symbol $\frac{1}{N}P$ will denote an arbitrary point T, such that $NT = P$. Note that there are N^2 such points. Fix some points $P_1, \ldots, P_r \in A(K)$ linearly independent over $\mathrm{End}_K(A)$. We define:

$$L_n := K_n\left(\frac{1}{p^n}P_1, \ldots, \frac{1}{p^n}P_r\right).$$

Observe that the field L_n does not depend on the choice of the points $\frac{1}{p^n}P_1, \ldots, \frac{1}{p^n}P_r$.
The extension L_n/K_n is abelian, since there exists a monomorphism

$$\Gamma^{(n)} : \mathrm{Gal}(L_n/K_n) \to A[p^n]^{\oplus r}, \quad \Gamma^{(n)}(\sigma) = \bigoplus_{i=1}^{r} \kappa_n(P_i, \sigma),$$

where:

$$\kappa_n : A(\overline{K}) \times \mathrm{Gal}(L_n/K_n) \to A[p^n], \quad \kappa_n(P, \sigma) = \left(\frac{1}{p^n}P\right)^{\sigma} - \left(\frac{1}{p^n}P\right)$$

is the Kummer pairing. It turns out that for n large enough, the homomorphism $\Gamma^{(n)}$ is "almost an isomorphism". More precisely, consider the fields:

$$K_\infty = \bigcup_n K_n, \quad L_\infty = \bigcup_n L_n.$$

The inverse limit over n of homomorphisms $\Gamma^{(n)} : \mathrm{Gal}(L_n/K_n) \to A[p^n]^{\oplus r}$ is the monomorphism:

$$\Gamma^{(\infty)} : \mathrm{Gal}(L_\infty/K_\infty) \to T_p(A)^{\oplus r}.$$

The map $\Gamma^{(\infty)}$ is continuous if we endow $\mathrm{Gal}(L_\infty/K_\infty)$ and $T_p(A)^{\oplus r}$ with the usual profinite topologies. The following theorem is based on results of Bashmakov [Bas72] and Ribet [Rib79].

Theorem 1.2.16 ([BGK05, Lemma 2.13])**.** $\Gamma^{(\infty)}(\mathrm{Gal}(L_\infty/K_\infty))$ *is an open subgroup of finite index in* $T_p(A)^{\oplus r}$.

Define the integer m_p by the equality:

$$p^{m_p} := [T_p(A)^{\oplus r} : \Gamma^{(\infty)}(\mathrm{Gal}(L_\infty/K_\infty))] \tag{1.10}$$

(observe that this index must be a power of p, since $T_p(A)^{\oplus r}$ is a pro-p group).

Corollary 1.2.17.

$$p^{2grn - m_p} \leq [L_n : K_n] \leq p^{2grn}.$$

Proof. Note that $[L_n : K_n] \leq p^{2grn}$, since $\Gamma^{(n)}$ is injective. Let us denote $K'_n := L_n \cap K_\infty$. Observe that $K_n \subset K'_n$ and thus

$$\mathrm{Gal}(L_n/K'_n) \subset \mathrm{Gal}(L_n/K_n).$$

The commutative diagram:

$$\begin{array}{ccc} \mathrm{Gal}(L_\infty/K_\infty) & \xhookrightarrow{\Gamma^{(\infty)}} & T_p(A)^{\oplus r} \\ \downarrow & & \downarrow \\ \mathrm{Gal}(L_n/K'_n) & \xhookrightarrow{\Gamma^{(n)}|_{\mathrm{Gal}(L_n/K'_n)}} & A[p^n]^{\oplus r} \end{array}$$

implies that

$$T_p(A)^{\oplus r}/\Gamma^{(\infty)}(\mathrm{Gal}(L_\infty/K_\infty)) \twoheadrightarrow A[p^n]^{\oplus r}/\Gamma^{(n)}(\mathrm{Gal}(L_n/K_n)).$$

It follows that:

$$[L_n : K_n] \geq [L_n : K'_n] \geq \#A[p^n]^{\oplus r}/p^{m_p} = p^{2grn-m_p}.$$

□

1.3. The de Rham cohomology

Let $\mathscr{A}$ be an abelian category with enough injectives. Denote by $\mathcal{C}(\mathscr{A})$ the category of cochain complexes. This category is also abelian and has enough injectives (cf. [Rot09, Theorem 10.43. and the following Remark]). For an arbitrary $C^\bullet \in \mathrm{Ob}(\mathcal{C}(\mathscr{A}))$ we denote by $h^i(C^\bullet)$ the i-th cohomology of the complex $C^\bullet$. Also, if A is any object of $\mathscr{A}$, let $A[i] \in \mathrm{Ob}(\mathcal{C}(\mathscr{A}))$ denote the complex satisfying:

$$A[i]^j = \begin{cases} A, & j = i, \\ 0, & j \neq i. \end{cases}$$

We denote the category of non-negative complexes by $\mathcal{C}_+(\mathscr{A})$.

For the convenience of the reader we recall the theory of de Rham cohomology over an arbitrary field k. See e.g. [Wei94, 5.7], [Har75] or [Wed08] for a precise treatment. Let X be an algebraic variety and let $\mathcal{O}_X$-mod denote the category of $\mathcal{O}_X$-modules. The **i-th hypercohomology group** $\mathbb{H}^i(X, \mathcal{F}^\bullet)$ of a complex $\mathcal{F}^\bullet \in \mathrm{Ob}(\mathcal{C}_+(\mathcal{O}_X\text{-mod}))$ is defined as the i-th derived functor of

$$\mathbb{H}^0 : \mathcal{C}_+(\mathcal{O}_X\text{-mod}) \to k\text{-mod}, \quad \mathbb{H}^0(X, \mathcal{F}^\bullet) := h^0(H^0(X, \mathcal{F}^\bullet)) = H^0(X, h^0(\mathcal{F}^\bullet)).$$

The hypercohomology may be computed in terms of the usual cohomology using the spectral sequences

$$ {}_IE_1^{ij} = H^j(X, \mathcal{F}^i) \quad \Rightarrow \quad \mathbb{H}^{i+j}(X, \mathcal{F}^\bullet), \tag{1.11}$$

$$ {}_{II}E_2^{ij} = H^i(X, h^j(\mathcal{F}^\bullet)) \quad \Rightarrow \quad \mathbb{H}^{i+j}(X, \mathcal{F}^\bullet). \tag{1.12}$$

One defines **the de Rham cohomology $H^i_{dR}(X/k)$ of the variety** X/k as the hypercohomology of the de Rham complex:

$$\Omega^\bullet_{X/k} := (\ldots \to 0 \to \mathcal{O}_X \to \Omega_{X/k} \xrightarrow{d} \Omega^2_{X/k} \xrightarrow{d} \ldots).$$

In particular, we obtain from (1.11) and (1.12) **the Hodge–de Rham spectral sequence** and **the conjugate spectral sequence**:

$$ {}_IE_1^{ij} = H^j(X, \Omega^i_{X/k}) \quad \Rightarrow \quad H^{i+j}_{dR}(X/k), \tag{1.13}$$

$$ {}_{II}E_1^{ij} = H^i(X, h^j(\Omega^\bullet_{X/k})) \quad \Rightarrow \quad H^{i+j}_{dR}(X/k). \tag{1.14}$$

Let k be a perfect field of characteristic $p > 0$ and let X/k be a smooth projective variety. Denote by X' the Frobenius twist of X and by $F : X \to X'$ the relative Frobenius. For any k-vector space V, let the symbol V' denote the k-vector space with the same underlying abelian group as V and the scalar multiplication $(\lambda, v) \mapsto \lambda^p \cdot v$. Then one easily checks that $H^i(X', \Omega^j_{X'}) \cong H^i(X, \Omega^j_X)'$. Cartier proved in [Car57] that there exists an isomorphism of $\mathcal{O}_{X'}$-modules:

$$\mathcal{C}^{-1} : \Omega^i_{X'} \to h^i(F_*\Omega^\bullet_X)$$

(note the strange convention – it is denoted $\mathcal{C}^{-1}$ rather then $\mathcal{C}$). Therefore the spectral sequence (1.14) becomes:

$$_{II}E^{ij} = H^i(X, \Omega^j_X)' \Rightarrow H^{i+j}_{dR}(X/k). \tag{1.15}$$

Using the classical Hodge–de Rham decomposition of compact Kähler manifolds (cf. [Voi02, §6]), one can prove that for $\operatorname{char} k = 0$ the spectral sequence (1.13) degenerates at the first page. A celebrated theorem proven by Deligne and Illusie in [DI87] provides an analogous statement in positive characteristic under certain liftability condition. To state this theorem, we need the notion of Witt vectors.

The **ring of Witt vectors** $W(k)$ is the cartesian product $\prod_{n=0}^{\infty} k$ with addition and multiplication given by Witt polynomials (cf. [Ser79, II §6] for definitions). In particular, if $k/\mathbb{F}_p$ is a finite extension, $W(k)$ is the ring of integers in the unique unramified extension of $\mathbb{Q}_p$ having k as the residue field. The **ring of Witt vectors of length** n, $W_n(k)$, is defined as $W_n(k) := W(k)/p^n W(k)$.

Theorem 1.3.1 ([DI87, Théoréme 2.1])**.** *Keep the above notation and suppose that* $\dim X < p$. *For every smooth lifting* $\widetilde{X}$ *of* X *to* $W_2(k)$ *there exists an isomorphism:*

$$\varphi^\bullet_{\widetilde{X}} : F_*\Omega^\bullet_{X/k} \cong \bigoplus_i \Omega^i_{X'/k}[-i],$$

in the derived category of coherent $\mathcal{O}_{X'}$*-modules. This isomorphism is functorial with respect to* $\widetilde{X}$.

It is a folklore result that for an abelian variety the spectral sequence (1.13) always degenerates on the first page (cf. [Oda69, Prop. 5.1]).

Suppose that X/k is an algebraic variety, for which the spectral sequence (1.13) degenerates on the first page. Then, in particular, we obtain the exact sequence:

$$0 \to H^0(X, \Omega_{X/k}) \to H^1_{dR}(X/k) \to H^1(X, \mathcal{O}_X) \to 0.$$

We refer to this sequence as **the Hodge–de Rham exact sequence**. Similarly, if the spectral sequence (1.15) degenerates on the second page, we obtain **the conjugate Hodge–de Rham exact sequence**:

$$0 \to H^1(X, \mathcal{O}_X)' \to H^1_{dR}(X/k) \to H^0(X, \Omega_{X/k})' \to 0.$$

1.4. Group cohomology of sheaves

Let R be any ring and G a finite group. We define the **i-th group cohomology**, $H^i_R(G, -)$, as the i-th derived functor of the functor

$$(-)^G : R[G]\text{-mod} \to R\text{-mod}, \quad M \mapsto M^G := \{m \in M : g \cdot m = m\}.$$

One checks that if $R \to B$ is a homomorphism of rings and M is a $B[G]$-module then $H^i_B(G,M)$ and $H^i_R(G,M)$ are isomorphic R-modules for all $i \geq 0$ (cf. [Sta16, Lemma 0DVD]). Thus without ambiguity we drop the index from notation and write $H^i(G,M)$. For a future use we note the following properties of group cohomology.

(1.16) If $M = \mathrm{Ind}_H^G N$ is an induced module (which for finite groups is equivalent to being a coinduced module), then

$$H^i(G,M) \cong H^i(H,N).$$

This property is known as **Shapiro lemma**, cf. [Ser79, Proposition VIII.2.1].

(1.17) If M is a $\mathbb{F}_p[G]$-module and G has a normal p-Sylow subgroup P then:

$$H^i(G,M) \cong H^i(P,M).$$

For a proof observe that $H^i(G/P,N)$ is killed by multiplication by p for any $\mathbb{F}_p[G]$-module N and use [Ser79, Theorem IX.2.4.] to obtain $H^i(G/P,N) = 0$ for $i \geq 1$. Then use Lyndon–Hochschild–Serre spectral sequence for group cohomology.

(1.18) Suppose that R is a finitely generated algebra over a field k and that R is a local ring with maximal ideal $\mathfrak{p}$. If M is a finitely generated R-module then

$$H^i(G,M) \cong H^i(G,\widehat{M_{\mathfrak{p}}}),$$

where $\widehat{M_{\mathfrak{p}}}$ denotes the completion of M with respect to $\mathfrak{m}$ (cf. proof of [BM00, Lemme 3.3.1] for a brief justification).

Properties of group cohomology described above extend to sheaves, as explained in [Gro57] and [BM00]. We briefly recall this theory. Let $(Y,\mathcal{O})$ be a ringed space and let G be a finite group. By an $\mathcal{O}[G]$-sheaf on $(Y,\mathcal{O})$ we understand a sheaf $\mathcal{F}$ equipped with an $\mathcal{O}$-linear action of G on $\mathcal{F}(U)$ for every open subset $U \subset Y$, compatible with respect to the restrictions. The $\mathcal{O}[G]$-sheaves form a category $\mathcal{O}[G]$-mod, which is abelian and has enough injectives. For any $\mathcal{O}[G]$-sheaf $\mathcal{F}$ one may define a sheaf $\mathcal{F}^G$ by the formula

$$U \mapsto \mathcal{F}(U)^G := \{f \in \mathcal{F}(U) : \forall_{g \in G} \quad g \cdot f = f\}.$$

We denote the i-th derived functor of

$$(-)^G : \mathcal{O}[G]\text{-mod} \to \mathcal{O}\text{-mod}$$

by $\mathcal{H}^i_{(Y,\mathcal{O})}(G,-)$. Similarly as in the case of modules, one may neglect the dependence on the sheaf $\mathcal{O}$ and write simply $\mathcal{H}^i(G,M)$. If $\mathcal{F} = \widetilde{M}$ is a quasicoherent $\mathcal{O}[G]$-module coming from a $\mathcal{O}(Y)[G]$-module M, one may compute the group cohomology of sheaves via the standard group cohomology:

$$\mathcal{H}^i(G,\mathcal{F}) \cong \widetilde{H^i(G,M)}.$$

In particular, group cohomology of a quasicoherent $\mathcal{O}[G]$-sheaf is a quasicoherent $\mathcal{O}$-module. Moreover for any $Q \in Y$ we have the following isomorphism:

$$\mathcal{H}^i(G,\mathcal{F})_Q \cong H^i(G,\mathcal{F}_Q). \tag{1.19}$$

1.5. Number theory preliminaries

We refer to [Neu99] for all the quoted facts. Let $\mathcal{O}_K$ be the ring of integers in a number field K. Recall that the **class group** of $\mathcal{O}_K$ (denoted by $\mathrm{Cl}(\mathcal{O}_K)$) is defined as the quotient of the group of non-zero fractional ideals of $\mathcal{O}_K$ by the subgroup of principal ideals. By abuse of notation we often write $\mathrm{Cl}(K) := \mathrm{Cl}(\mathcal{O}_K)$. The group $\mathrm{Cl}(K)$ is finite and abelian; its rank is called the **class number of** K.

Definition 1.5.1. An **absolute value** on K is a map $|\cdot| : K \to \mathbb{R}$ satisfying the following conditions:

(1) $|x| \geq 0$ for all $x \in K$, with an equality if and only if $x = 0$,

(2) $|x \cdot y| = |x| \cdot |y|$ for all $x, y \in K$,

(3) $|x + y| \leq |x| + |y|$ for all $x, y \in K$.

Two absolute values on K are **equivalent** if they give rise to the same topology. The **trivial absolute value** is given by $|0| = 0$ and $|x| = 1$ for all $x \in K^\times$. An equivalence class of non-trivial absolute values on K is called a **place** of K.

There are three types of places:

- **finite places**, i.e. places corresponding to non-archimedean absolute values. They are in bijection with the maximal ideals in $\mathcal{O}_K$,
- **infinite complex places**, which are in bijection with pairs $\{\sigma, \overline{\sigma}\}$ of conjugated embeddings of K into $\mathbb{C}$, such that $\sigma \neq \overline{\sigma}$,
- **infinite real places**, which correspond to embeddings of K into $\mathbb{R}$.

We say that an extension of number fields L/K is **unramified** at a place v of K, if one of the following conditions holds:

- v is a finite place, corresponding to a prime ideal $\mathfrak{p}_v$, which factors in $\mathcal{O}_L$ as $\mathcal{P}_1 \dots \mathcal{P}_g$ for distinct finite prime ideals $\mathcal{P}_i$ of $\mathcal{O}_L$,
- v is an infinite complex place,
- v is an infinite real place corresponding to $\sigma : K \hookrightarrow \mathbb{R}$ and σ might be extended to an embedding $\sigma_L : L \hookrightarrow \mathbb{R}$.

An extension L/K is called **abelian**, if it is Galois and the group $\mathrm{Gal}(L/K)$ is abelian.

Theorem 1.5.2. *Let K be a number field. There exists a maximal abelian unramified extension of K, called the **Hilbert class field** of K. Its degree over K equals $\#\,\mathrm{Cl}(K)$.*

In the sequel we will need also the notion of the power residue symbol. Fix an integer $n > 1$. Suppose that K contains that contains a primitive n-th root of unity ζ_n. Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_K$ and assume that $\mathfrak{p} \nmid n$ and $\#(\mathcal{O}_K/\mathfrak{p}) \equiv 1 \pmod{n}$.

Definition 1.5.3. The **n-th power residue symbol** for $\alpha \bmod \mathfrak{p}$, denoted $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$ is the unique n-th root of unity ζ_n^s such that:

$$\alpha^{\frac{\#(\mathcal{O}_K/\mathfrak{p})-1}{n}} \equiv \zeta_n^s \pmod{\mathfrak{p}}.$$

2

Lifts of ordinary abelian varieties

In this chapter we focus on ordinary abelian varieties. In Sections 2.1 and 2.2 we consider the deformation theory of an ordinary abelian variety B of dimension g over a perfect field k of characteristic $p > 0$. We recall the notion of canonical lift of an ordinary abelian variety and characterize canonical lifts via their p-primary torsion (Theorem 2.2.1). In Section 2.3 we apply the characterization of canonical lifts to the problem of local torsion of abelian varieties. In particular, we will study the local torsion of an abelian variety A of dimension g over $\mathbb{Q}_p$ with good reduction. For this purpose, we introduce the notion of (n, d)-degree and tie it to the canonical lift of A (Theorem 2.3.6). In Section 2.4 we compute the $(p, 1)$-degree of an elliptic curve $E/\mathbb{Q}$ with complex multplication (Theorem 2.4.1). This chapter partially extends the results of [Gar18] to abelian varieties.

Setup 2.0.1. Let p, k, B, A, g be as above. Let also:

- R denote an Artin local ring with residue field k and $\mathbf{B}$ be a lift of B to R,
- $\mathcal{A}$ be an abelian scheme over $\mathbb{Z}_p$, whose generic fiber is A. We will use the notation introduced in Subsection 1.2.4.
- $\mathcal{O} := \mathrm{End}_{\overline{\mathbb{Q}}} E$ be an order of discriminant $-D$ in a quadratic imaginary field. We suppose also that E has good reduction at p and that $p \nmid D$.

2.1. Serre–Tate theory

It turns out that ordinary abelian varieties have particularly nice deformation theory. Let us assume that k, R, B, $\mathbf{B}$ are objects defined in Setup 2.0.1. One can prove that the connected–étale sequence of $\mathbf{B}[p^\infty]$ is of the form:

$$0 \to G^0 \to \mathbf{B}[p^\infty] \to G^{et} \to 0,$$

where G^0 is the canonical lift of $B[p^\infty]^0$ (in the sense of Subsection 1.1.3) and G^{et} is the Cartier dual of G^0. Thus, by Theorem 1.2.15:

$$\mathrm{Def}_{B/k}(R) \cong \mathrm{Ext}_{p\text{-}\mathbf{div}/R}(G^{et}, G^0). \tag{2.1}$$

Therefore the set $\mathrm{Def}_{B/k}(R)$ has a natural structure of a group. This observation allows us to pick a "distinguished" lift of B to R.

Definition 2.1.1. A lift $\mathbf{B}/R$ corresponding to the neutral element of the group $\mathrm{Def}_B(R)$ is called the **canonical lift of B to R**.

One easily proves that the canonical lift is functorial, i.e. for any ordinary abelian varieties B_1, B_2 over k with canonical lifts $\mathbf{B}_1$, $\mathbf{B}_2$ to R:

$$\mathrm{Hom}_R(\mathbf{B}_1, \mathbf{B}_2) \cong \mathrm{Hom}_k(B_1, B_2).$$

In particular, if $\mathbf{B}$ is the canonical lift of B to R, the natural monomorphism:

$$\mathrm{End}_R \mathbf{B} \to \mathrm{End}_k B \tag{2.2}$$

becomes an isomorphism. It follows from [Mes72, Appendix, Corollary (1.3)] that this condition characterizes the canonical lift completely. For a finite field $k = \mathbb{F}_q$ one can prove a stronger statement. Let π_B denote the Frobenius endomorphism of B, i.e. the endomorphism of B induced by the map $x \mapsto x^q$ on k.

Lemma 2.1.2 ([dJN91, Lemma 3.3])**.** *Keep the Setup 2.0.1 and suppose that $k = \mathbb{F}_q$ is a finite field. Then $\mathbf{B}$ is the canonical lift of B if and only if the image of (2.2) contains π_B.*

We want now to see what happens, if we allow the ring R to vary. Recall that a functor $F : \mathrm{Art}_k \to \mathrm{Set}$ is **pro-represented by a formal scheme $\mathcal{M}$** defined over $W(k)$, if it is isomorphic to the functor

$$R \mapsto \mathcal{M}(R) := \mathrm{Hom}(\mathrm{Spf}\, R, \mathcal{M}).$$

Using the isomorphism (2.1) one can prove that the functor $\mathrm{Def}_{B/k} : \mathrm{Art}_k \to \mathrm{Set}$ is pro-represented by a formal torus $\mathcal{M}_{B/k}$ defined over $W(k)$, i.e. by a formal group satisfying:

$$(\mathcal{M}_{B/k})_{W(\overline{k})} \cong \widehat{\mathbb{G}}^d_{m, W(\overline{k})}$$

for some $d \geq 0$ (cf.[Kat81, Theorem 2.1]).

We consider now the lifts of an ordinary abelian variety to the ring of Witt vectors. One easily sees that the canonical lifts $\mathbf{B}_n$ of B to $W_n(k)$ are compatible in the sense that

$$\mathbf{B}_{n+1} \times_{W_{n+1}(k)} W_n(k) \cong \mathbf{B}_n.$$

Thus, by taking a limit, we obtain a formal abelian scheme $\widehat{\mathbf{B}} \to \mathrm{Spf}\, W(k)$. Every polarization of B/k canonically lifts to its canonical lift. Thus, by the Grothendieck's algebraization theorem (cf. [GD71, 5.4.5]) $\widehat{\mathbf{B}}$ comes from a unique abelian scheme $\mathbf{B} \to \mathrm{Spec}\, W(k)$. We will refer both to the abelian scheme $\mathbf{B}/W(k)$ and to its generic fiber as the **canonical lift** of B to $W(k)$.

Lemma 2.1.3. *Let $\mathcal{A}$, A be as in the Setup 2.0.1. Suppose that $\mathcal{O} := \mathrm{End}_{\overline{\mathbb{Q}}_p}(A)$ is an order in a CM-field M and that p splits completely in M. Then $\mathcal{A}$ is the canonical lift of $A_{\mathbb{F}_p}$.*

Proof. Since p splits completely in M, $A_{\mathbb{F}_p}$ is ordinary by Lemma 1.2.8. Moreover, $M \hookrightarrow \mathbb{Q}_p$ and by Lemma 1.2.7 we have $\mathcal{O} = \mathrm{End}_{\mathbb{Q}_p}(A)$. Let $\mathcal{M} := \mathcal{M}_{A_{\mathbb{F}_p}/\mathbb{F}_p}$. Suppose that $\mathcal{A} \in \varprojlim \mathrm{Def}_A(\mathbb{Z}/p^n)$ corresponds to $q \in \mathcal{M}(\mathbb{Z}_p)$. Let $\pi_{A_{\mathbb{F}_p}} \in \mathrm{End}_{\mathbb{F}_p} A_{\mathbb{F}_p}$ be the Frobenius element of A. Let $m \in \mathbb{Z} \setminus \{0\}$ be such that

$$m \cdot \pi_{A_{\mathbb{F}_p}} \in \mathcal{O}$$

(note that $\mathcal{O}$ and $\mathrm{End}_{\mathbb{F}_p} A_{\mathbb{F}_p}$ are both orders in M – therefore $[\mathrm{End}_{\mathbb{F}_p} A_{\mathbb{F}_p} : \mathcal{O}]$ is finite). Let $\mathcal{A}' \in \varprojlim \mathrm{Def}_A(\mathbb{Z}/p^n)$ be the (formal) lift corresponding to $q^m \in \mathcal{M}$. Then, since $m \cdot \pi_{A_{\mathbb{F}_p}} \in \mathcal{O}$, by functoriality of $\mathcal{M}$, $\pi_{A_{\mathbb{F}_p}}$ lifts to $\mathcal{A}'$. Thus, by Lemma 2.1.2, $\mathcal{A}'$ is the canonical lift of A and $q^m = 1$. But $\mathcal{M}$ has no non-trivial torsion elements, since

$$\widehat{\mathbb{G}}_m(W(\overline{\mathbb{F}}_p)) = 1 + pW(\overline{\mathbb{F}}_p)$$

is torsion-free. Thus, since $p \nmid m$, $q = 1$ and $\mathcal{A}$ is the canonical lift of $A_{\mathbb{F}_p}$. □

We will also need the following lemma in the sequel.

Lemma 2.1.4. *Let B, k be as in the Setup 2.0.1. Let also $\boldsymbol{B}_1, \boldsymbol{B}_2 \in \mathrm{Def}_{B/k}(W_n(k))$. If $(\boldsymbol{B}_1)_{W_n(\overline{k})} \cong (\boldsymbol{B}_2)_{W_n(\overline{k})}$ then $\boldsymbol{B}_1 \cong \boldsymbol{B}_2$.*

Proof. We want to show that the natural map:

$$\mathrm{Def}_{B/k}(W_n(k)) \to \mathrm{Def}_{B_{\overline{k}}/\overline{k}}(W_n(\overline{k})), \qquad \mathbf{B} \mapsto \mathbf{B}_{W_n(\overline{k})}$$

is injective. One easily proves that $(\mathcal{M}_{B/k})_{W(\overline{k})} \cong \mathcal{M}_{B_{\overline{k}}/\overline{k}}$. Therefore we are left with proving that the map:

$$\mathcal{M}(W_n(k)) \to \mathcal{M}(W_n(\overline{k})) \cong \mathcal{M}_{W(\overline{k})}(W_n(\overline{k}))$$

is injective, which is immediate. □

2.2. Characterisation of canonical lifts via torsion

The goal of this section is to prove the following characterisation of the canonical lift of an ordinary abelian variety in terms of its p-primary torsion.

Theorem 2.2.1. *We use the Setup 2.0.1. Suppose that*

$$B(k)[p^n] \cong (\mathbb{Z}/p^n)^g$$

as abelian groups. Let $\boldsymbol{B}$ be a lift of B to $W(k)$. Then $\boldsymbol{B}_{W_n(k)}$ is the canonical lift of B to $W_n(k)$ if and only if

$$\boldsymbol{B}(W(k))[p^n] \cong (\mathbb{Z}/p^n)^g.$$

In order to prove this, we will need the following auxilliary result.

Lemma 2.2.2. *Keep the Setup 2.0.1. The natural maps:*

$$\mathrm{Ext}^1_{\boldsymbol{GS}/W(k)}(\underline{\mathbb{Z}/p^n}, \mu_{p^n}) \to \mathrm{Ext}^1_{\boldsymbol{GS}/W_{n+1}(k)}(\underline{\mathbb{Z}/p^n}, \mu_{p^n}) \tag{2.3}$$

$$\mathrm{Ext}^1_{p\text{-}\boldsymbol{div}/W_{n+1}(k)}(\underline{\mathbb{Q}_p/\mathbb{Z}_p}, \mu_{p^\infty}) \to \mathrm{Ext}^1_{\boldsymbol{GS}/W_{n+1}(k)}(\underline{\mathbb{Z}/p^n}, \mu_{p^n}) \tag{2.4}$$

are isomorphisms.

Proof. In order to prove that the map (2.3) is an isomorphism, it suffices to check that the reduction map:

$$W(k)^\times / W(k)^{\times p^n} \to W_{n+1}(k)^\times / W_{n+1}(k)^{\times p^n}$$

is an injection. Let $a \in W(k)^\times$ and suppose that $a \equiv b^{p^n} \pmod{p^{n+1}}$. We will show that for $i \geq n$

$$a \equiv b_i^{p^n} \pmod{p^{i+1}}$$

for some $b_i \in W(k)^\times$ by induction on i. For $i = n$ this is immediate. Suppose now that $a = b_i^{p^n} + p^{i+1} \cdot c$. Consider the equation:

$$(b_i + p^{i-n} \cdot x)^{p^n} \equiv a \pmod{p^{i+2}}$$

with a variable x. Recall that by a theorem of Kummer (cf. [Kum52]) for $1 \leq j \leq p^n - 1$:

$$v_p\left(\binom{p^n}{j}\right) = n - v_p(j). \tag{2.5}$$

Let us expand the left hand side using (2.5):

$$\begin{aligned}(b_i + p^{i-n} \cdot x)^{p^n} &= \sum_{j=0}^{p^n} \binom{p^n}{j} b_i^{p^n - j} (p^{i-n}x)^j \\ &\equiv b_i^{p^n} + p^i \cdot b_i^{p^n - 1} x \pmod{p^{i+2}},\end{aligned}$$

since by (2.5) for $j \geq 2$:

$$v_p\left(\binom{p^n}{j} b_i^{p^n - j} p^{j \cdot (i-n)}\right) \geq i + 2.$$

Thus we may take $x \equiv c \cdot (b_i^{p^n - 1})^{-1}$ and define:

$$b_{i+1} := b_i + p^{i-n} \cdot x.$$

This ends the proof of (2.3). In order to show (2.4), it suffices to prove that the projection:

$$\varphi : \varprojlim_i W_{n+1}(k)^\times / W_{n+1}(k)^{\times p^i} \to W_{n+1}(k)^\times / W_{n+1}(k)^{\times p^n}$$

is an injection. Let $(a_i) \in \varprojlim_i W_{n+1}(k)^\times / W_{n+1}(k)^{\times p^i}$ and suppose that $\varphi(([a_i])_i) = 1$, i.e. that $a_n = 1$. We will show inductively that

$$a_i \equiv b_i^{p^i} \pmod{p^{n+1}} \tag{2.6}$$

for $i \geq n$ and some $b_i \in W_i(k)^\times$. Indeed, suppose that the equality (2.6) is true. Note that since k is perfect, $b_i \equiv b_{i+1}^p \pmod{p}$ for some $b_{i+1} \in W_i(k)^\times$, i.e. $b_i = b_{i+1}^p + p \cdot c$ for some c. Then:

$$\begin{aligned}a_i &\equiv (b_{i+1}^p + p \cdot c)^{p^i} \\ &\equiv b_{i+1}^{p^{i+1}} + \sum_{j \geq 1} \binom{p^i}{j} b_{i+1}^{p \cdot (p^i - j)} \cdot (pc)^j \\ &\equiv b_{i+1}^{p^{i+1}} \pmod{p^{n+1}},\end{aligned}$$

since by (2.5):

$$v_p\left(\binom{p^i}{j} b_{i+1}^{p \cdot (p^i - j)} \cdot (pc)^j\right) \geq n + 1$$

for $j \geq 1$. This ends the induction. Therefore $([a_i])_i = ([b_i^{p^i}])_i$ is trivial in $\varprojlim_i W_{n+1}(k)^\times / W_{n+1}(k)^{\times p^i}$ and φ is injective. □

Proof of Theorem 2.2.1. Note that by assumption, $B[p^n] \cong (\underline{\mathbb{Z}/p^n})^{\oplus g} \oplus (\mu_{p^n})^{\oplus g}$.

($\Rightarrow$) The assumption implies that the class of $\mathbf{B}[p^n]_{W_{n+1}(k)}$ is trivial in

$$\mathrm{Ext}^1_{\mathbf{GS}/W_{n+1}(k)}(\mathbf{B}[p^n]^{et}_{W_{n+1}(k)}, \mathbf{B}[p^n]^0_{W_{n+1}(k)}) \cong \mathrm{Ext}^1_{\mathbf{GS}/W_{n+1}(k)}(\underline{\mathbb{Z}/p^n}, \mu_{p^n})^{\oplus g^2}.$$

Therefore the isomorphism (2.3) implies that the class of $\mathbf{B}[p^n]_{W(k)}$ is trivial in

$$\mathrm{Ext}^1_{\mathbf{GS}/W(k)}(\mathbf{B}[p^n]^{et}, \mathbf{B}[p^n]^0) \cong \mathrm{Ext}^1_{\mathbf{GS}/W(k)}(\underline{\mathbb{Z}/p^n}, \mu_{p^n})^{\oplus g^2},$$

i.e. that $\mathbf{B}[p^n] \cong (\underline{\mathbb{Z}/p^n})^{\oplus g} \oplus \mu_{p^n}^{\oplus g}$. This implies the desired result.

($\Leftarrow$) By Lemma 2.1.4 we can replace k by $\overline{k}$. Then, by (2.1):

$$\mathrm{Def}_{B/k}(W_n(k)) \cong \mathrm{Ext}^1_{p\text{-}\mathbf{div}/W_n(k)}(\underline{\mathbb{Q}_p/\mathbb{Z}_p}, \mu_{p^\infty})^{\oplus g^2}.$$

The assumption implies that we have an embedding $(\underline{\mathbb{Z}/p^n})^{\oplus g} \to \mathbf{B}[p^n]_{W(k)[1/p]}$. Let G be the scheme–theoretic closure of the image of this embedding in $\mathbf{B}[p^n]$. Then, by Raynaud's theorem (cf. Proposition 1.1.7), $G \cong (\underline{\mathbb{Z}/p^n})^{\oplus g}$ and we obtain an embedding $\varphi : (\underline{\mathbb{Z}/p^n})^{\oplus g} \to \mathbf{B}[p^n]$. By modifying φ by an automorphism of $(\underline{\mathbb{Z}/p^n})^{\oplus g}$, we may assume that φ is a section of the connected-étale exact sequence for $\mathbf{B}[p^n]$. Thus $\mathbf{B}[p^n] \cong \mu_{p^n}^{\oplus g} \oplus \underline{\mathbb{Z}/p^n}^{\oplus g}$ and in particular, the class of $\mathbf{B}[p^n]_{W_{n+1}(k)}$ is trivial in $\mathrm{Ext}^1_{\mathbf{GS}/W_{n+1}(k)}(\underline{\mathbb{Z}/p^n}, \mu_{p^n})^{\oplus g^2}$. By using isomorphism (2.4), we see that $\mathbf{B}[p^\infty]_{W_{n+1}(k)}$ corresponds to the trivial extension of $\underline{\mathbb{Q}_p/\mathbb{Z}_p}$ by μ_{p^∞}. Thus $\mathbf{B}_{W_{n+1}(k)}$ is the canonical lift of $\mathbf{B}_k$.

□

2.3. Local torsion of abelian varieties

Define the (n,d)**-degree** of an abelian variety A over a field K to be the number:

$$D_{n,d}(A/K) = \min\{[L:K] : A(L) \text{ contains a subgroup isomorphic to } (\mathbb{Z}/n)^d\}$$

(we put $D_{n,d}(A/K) = \infty$ if $(\mathbb{Z}/n)^d$ is not a subgroup of $A(\overline{K})$). Note that for any abelian variety A/K, $D_{n,1}(A/K) \leq n^{2g} - 1$. A classical result of Faltings and Zarhin (cf. [Zar85], [FWG+86, p. 118, p. 204]) implies that if $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$, then for sufficiently large p the $\mathbb{F}_p[G_K]$-module $A[p]$ is irreducible (cf. [AdRGP13, Proposition 3.1]) and therefore, if $p \neq \mathrm{char}\, K$, then $D_{p,1}(A/K) = p^{2g} - 1$. However, if we allow the field of definition to vary, the behaviour of torsion is not easy to predict. We say that p is a *local torsion prime* for an abelian variety $A/\mathbb{Q}$, if $A(\mathbb{Q}_p)[p] \neq 0$. The following conjecture is part of the folklore:

Conjecture 2.3.1. *An elliptic curve $E/\mathbb{Q}$ without complex multiplication has only finitely many local torsion primes.*

Note that p is a local torsion prime for $A/\mathbb{Q}$ if and only if $D_{p,1}(A/\mathbb{Q}_p) = 1$. Hence the following natural question arises:

Question 2.3.2. *Fix an abelian variety $A/\mathbb{Q}$ of dimension g and natural numbers n and $1 \leq d \leq 2g$. What is the asymptotic behaviour of $D_{p^n,d}(A/\mathbb{Q}_p)$ as p tends to infinity over primes?*

The following conjecture treats the case $(n, d) = (1, 1)$.

Conjecture 2.3.3 ([Gam14, Conjecture 1.1]). *Let A be an abelian variety over $\mathbb{Q}$ with an endomorphism ring that embeds into a totally real field. Then:*

$$\lim_{p\to\infty} D_{p,1}(A/\mathbb{Q}_p) = \infty,$$

where the limit is taken over prime numbers.

This conjecture was proposed by David and Weston in [DW08] for elliptic curves and by Gamzon in [Gam14] in general. Both articles justified Conjecture 2.3.3 by some simple heuristics and averaging results. The primary motivation for Conjecture 2.3.3 is the theory of deformations of Galois representations. Let E be an elliptic curve over $\mathbb{Q}$. If the representation $\rho_{E,p}$ is absolutely irreducible, then one can associate to $\rho_{E,p}$ its universal deformation ring $R^{univ}_{E,p}$, parameterizing all lifts of $\rho_{E,p}$ to Artinian local rings with the residue field $\mathbb{F}_p$. Mazur in [Maz97] asked if the deformation theory of $\rho_{E,p}$ is unobstructed (so that $R^{univ}_{E,p}$ is non-canonically isomorphic to a power series ring in three variables over $\mathbb{Z}_p$) for all but finitely many primes p. He showed that this is the case as long as one excludes those primes p for which E has a point of order p over a quadratic extension of $\mathbb{Q}_p$, which leads to Conjecture 2.3.3. The whole reasoning may be repeated for an arbitrary abelian variety (cf. [Gam14, Proposition 2.4.]).

We will show now that the Question 2.3.2 may be easily answered for $d > g$. To this end we need to tie the (p, d)-degree of an abelian variety to the p-rank of its reduction.

Lemma 2.3.4. *Let $A/\mathbb{Q}_p$ be an abelian variety of dimension g with good reduction. Then for $d > r(A_p)$:*

$$D_{p,d}(A/\mathbb{Q}_p) \geq p^{2g} - 1.$$

In particular, if $r(A_p) = 0$ then $D_{p,1}(A/\mathbb{Q}_p) = p^{2g} - 1$.

Proof. Suppose that $K/\mathbb{Q}_p$ is a finite field extension such that $(\mathbb{Z}/p)^{r(A_p)+1} \leq A(K)[p]$. We will give a lower bound for $[K : \mathbb{Q}_p]$. Let $\mathcal{O}_K$ be the ring of integers in K with the maximal ideal $\mathfrak{p}$. Then there exists $P \in A(K)[p]$, $P \neq 0$, such that

$$P \in \ker\left(\mathrm{red}_{\mathfrak{p}} : A(K) \to A_p(\mathcal{O}_K/\mathfrak{p})\right) = \widehat{\mathcal{A}}(\mathfrak{p})$$

(here we used (1.7)). Note that the multiplication-by-p morphism on $\widehat{\mathcal{A}}$ must be of the form:

$$[p](\mathbf{x}) = p(F_1(\mathbf{x}), \ldots, F_g(\mathbf{x})) + (G_1(\mathbf{x}^{p^g}), \ldots, G_g(\mathbf{x}^{p^g}))$$

where $F_i, G_i \in R[\![\mathbf{x}]\!]$, $G_i(0) = 0$, $F_i(\mathbf{x}) = x_i + \ldots$, cf. (1.2) and (1.8). Thus P corresponds to some $\mathbf{a} = (a_1, \ldots, a_g) \in \mathfrak{p}^g$, $\mathbf{a} \neq 0$, satisfying:

$$0 = [p](\mathbf{a}) = p \cdot (F_1(\mathbf{a}), \ldots, F_g(\mathbf{a})) + (G_1(\mathbf{a}^{p^{2g}}), \ldots, G_g(\mathbf{a}^{p^{2g}})).$$

Let v be a discrete valuation on K, satisfying $v(K^\times) = \mathbb{Z}$. Let $e := v(p)$ be the ramification index of K. Suppose that i is such that $v(a_i) = \min_j v(a_j)$. Then:

$$e + v(a_i) = v(pF_i(\mathbf{a})) = v(-G_i(\mathbf{a}^{p^{2g}})) \geq v(a_i^{p^{2g}}) = p^{2g} \cdot v(a_i).$$

Thus we obtain:

$$[K : \mathbb{Q}_p] \geq e \geq (p^{2g} - 1) \cdot v(a_i) \geq p^{2g} - 1.$$

This ends the proof of the first claim. The second claim is immediate. □

Since $r(A_p) \leq g$, we obtain the following corollary.

Corollary 2.3.5. *Let $A/\mathbb{Q}$ be an abelian variety of dimension g. Then:*

$$\lim_{p\to\infty} D_{p,g+1}(A/\mathbb{Q}_p) = \infty.$$

We will now focus on the (p,d)-degree for the "boundary" value $d = g$. The goal of this Section is to prove the following Theorem, which ties the (p^n, g)-degree of an abelian variety of dimension g with its canonical lift.

Theorem 2.3.6. *Keep the Setup 2.0.1. Consider the following conditions:*

(1) $D_{p^n,g}(A/\mathbb{Q}_p) < p-1$,

(2) $(\mathbb{Z}/p^n)^g \leq A(\mathbb{Q}_p^{un})$,

(3) $A_{\mathbb{F}_p}$ *is ordinary and* A *is the canonical lift of* $A_{\mathbb{F}_p} \pmod{p^{n+1}}$,

(4) $A_{\mathbb{F}_p}$ *is ordinary and* $D_{p^n,g}(A/\mathbb{Q}_p) \leq D_{p^n,g}(A_{\mathbb{F}_p}/\mathbb{F}_p)$.

Then (1) *implies* (2), (2) *and* (3) *are equivalent, and* (3) *implies* (4).

Lemma 2.3.7. *Let A be as in the Setup 2.0.1 and let $K/\mathbb{Q}_p$ be a finite extension with the ramification index $e < p-1$. Then the following groups are equal:*

$$A(K)[p^\infty] = A(K \cap \mathbb{Q}_p^{un})[p^\infty].$$

Proof. We mimic the proof of [Gam14, Lemma 4.10]. Keep the Setup 2.0.1. Suppose that $A(K)[p^\infty] = A(K)[p^d]$ and let $G := A(K)[p^d]$ be an abstract group. We will show that $\mathcal{A}[p^d]$ contains a finite étale subgroup scheme $\mathbf{G}$ such that $\mathbf{G}(K) \cong A(K)[p^d]$. Let L be the Galois closure of K over $\mathbb{Q}_p$. Note that by Abhyankar's lemma (cf. [Sti93, Proposition III.8.9]) its ramification index equals e as well. The $\mathrm{Gal}(L/\mathbb{Q}_p)$-orbit of $A(K)[p^d]$ corresponds to an étale group scheme $\mathcal{G} \leq \mathcal{A}[p^d]_{\mathbb{Q}_p}$. Let $\mathbf{G}$ be the scheme-theoretic closure of $\mathcal{G}$ in $\mathcal{A}[p^d]$. By the assumption, $\mathbf{G}_L$ is a constant group scheme. Thus, by Raynaud theorem (cf. Proposition 1.1.7), since $e < p-1$, $\mathbf{G}_{\mathcal{O}_L}$ is a constant group scheme. Hence $\mathbf{G}$ is an étale group scheme. On the other hand, the category of étale group schemes over $\mathbb{Z}_p$ is equivalent to the category of étale group schemes over $\mathbb{F}_p$ (cf. [Mil80, Proposition I.4.4]). Thus, since $\mathbf{G}_{\mathcal{O}_K}$ contains a finite étale subgroup isomorphic to $\underline{A[p^d](K)}$, $\mathbf{G}_{W(k)}$ must also contain such a subgroup. This ends the proof. □

Proof of Theorem 2.3.6.

(1) ⇒ (2): Suppose that $K/\mathbb{Q}_p$ is a finite extension such that $[K : \mathbb{Q}_p] < p-1$ and $A(K)[p]$ contains a subgroup isomorphic to $(\mathbb{Z}/p^n)^g$. Then by Lemma 2.3.7

$$A(K \cap \mathbb{Q}_p^{ur})[p^\infty] = A(K)[p^\infty],$$

which implies (2).

(2) ⇒ (3): Suppose that $(\mathbb{Z}/p^n)^g \leq A(\mathbb{Q}_p^{un})$. By Theorem 2.2.1, $A_{W_{n+1}(\overline{\mathbb{F}}_p)}$ is the canonical lift of $A_{\overline{\mathbb{F}}_p}$. Using Lemma 2.1.4, we deduce that $A_{\mathbb{Z}/p^{n+1}}$ is the canonical lift of $A_{\mathbb{F}_p}$.

(3) ⇒ (2): By assumption, $A_{\mathbb{Q}_p^{ur}}$ is the canonical lift of $A_{\overline{\mathbb{F}}_p} \pmod{p^n}$. Thus the proof follows by Theorem 2.2.1.

(3) $\Rightarrow$ (4): Suppose that A is the canonical lift of $A_{\mathbb{F}_p}$ (mod p^{n+1}) and that for a finite extension $k/\mathbb{F}_p$ we have $A(k)[p^n] \cong (\mathbb{Z}/p^n)^g$. Then, by Theorem 2.2.1 we obtain: $A(W(k))[p^\infty] \cong (\mathbb{Z}/p^n)^g$. The equality $[W(k) : \mathbb{Q}_p] = [k : \mathbb{F}_p]$ concludes the proof. □

Theorem 2.3.6 naturally leads to the following question, which appeared already in [AWZ17, Remark 4.4.2].

Question 2.3.8. *Fix an abelian variety $A/\mathbb{Q}$. Are there infinitely many primes p such that $A_{\mathbb{Z}/p^2}$ is the canonical lift of $A_{\mathbb{F}_p}$?*

Note that Question 2.3.8 may be positively answered for abelian varieties with complex multiplication.

Proposition 2.3.9. *Suppose that $A/\mathbb{Q}$ has complex multiplication by an order $\mathcal{O} := \mathrm{End}_{\overline{\mathbb{Q}}} A$ in a CM-field M. Then there exist infinitely many primes p such that $A/\mathbb{Q}_p$ is the canonical lift of $A_{\mathbb{F}_p}$.*

Proof. Let p be a prime of good reduction for A that splits completely in M. Then A is the canonical lift of $A_{\mathbb{F}_p}$ by Lemma 2.1.3. □

We explain now the relation between Conjecture 2.3.3 and Question 2.3.8. Suppose that for an abelian variety $A/\mathbb{Q}$ of dimension g without complex multiplication the answer to Question 2.3.8 is negative. Then, for almost all primes p, $A_{\mathbb{Z}/p^2}$ is not the canonical lift of $A_{\mathbb{F}_p}$ and by Theorem 2.3.6 $D_{p,g}(A/\mathbb{Q}_p) \geq p-1$. In particular, $D_{p,g}(A/\mathbb{Q}_p)$ tends to infinity with p tending to infinity.

2.4. $(p,1)$-degree of elliptic curves

The goal of this section is to compute the $(p,1)$-degree of elliptic curves with complex multiplication.

Theorem 2.4.1. *Keep the Setup 2.0.1, in particular E has complex multiplication by an order $\mathcal{O}$ of discriminant $-D$ in a quadratic imaginary field. Then:*

$$D_{p,1}(E/\mathbb{Q}_p) = \begin{cases} \mathrm{ord}_p(\pm s), & \text{for } \left(\frac{-D}{p}\right) = 1, \\ p^2 - 1, & \text{for } \left(\frac{-D}{p}\right) = -1, \end{cases}$$

where for p satisfying $\left(\frac{-D}{p}\right) = 1$, s is defined by the equation

$$4p = s^2 + Dt^2 \tag{2.7}$$

and, for $D = -4$, by the equation (2.7) and the additional condition $4 \nmid s$.

Theorem 2.4.1 is a consequence of Theorem 2.3.6 and of the following lemma.

Lemma 2.4.2. *Let $E/\mathbb{Q}_p$ be an elliptic curve with good ordinary reduction.*

(1) Let us denote by $a_{p^d}(E_{\mathbb{F}_p})$ the p^d-Frobenius trace of $E_{\mathbb{F}_p}$ for any $d \geq 1$. Let also $\mathrm{ord}_p a$ be the multiplicative order of $a \in \mathbb{F}_p^\times$. Then $D_{p,1}(E_{\mathbb{F}_p}/\mathbb{F}_p) = \mathrm{ord}_p\, a_p(E_{\mathbb{F}_p})$.

(2) If $E_{\mathbb{Z}/p^2}$ is the canonical lift of $E_{\mathbb{F}_p}$, then we have:

$$D_{p,1}(E/\mathbb{Q}_p) = D_{p,1}(E_{\mathbb{F}_p}/\mathbb{F}_p).$$

Proof. (1) It suffices to prove that

$$E_{\mathbb{F}_p}(\mathbb{F}_{p^d})[p] \neq 0 \quad \text{if and only if} \quad a_p(E_{\mathbb{F}_p})^d \equiv 1 \pmod{p}.$$

Recall that

$$\#E_{\mathbb{F}_p}(\mathbb{F}_{p^d}) = p^d + 1 - (\alpha_1^d + \alpha_2^d)$$

where $\alpha_1, \alpha_2 \in \mathbb{C}$ are the roots of the characteristic polynomial $x^2 - a_p(E_{\mathbb{F}_p})x + p$. After muliplying the equality $\alpha_i^2 = a_p(E_{\mathbb{F}_p}) \cdot \alpha_i - p$ by α_i^{d-2} we obtain for $d \geq 2$:

$$\begin{aligned} a_{p^d}(E_{\mathbb{F}_p}) &= \alpha_1^d + \alpha_2^d = a_p(E_{\mathbb{F}_p}) \cdot (\alpha_1^{d-1} + \alpha_2^{d-1}) - p \cdot (\alpha_1^{d-2} + \alpha_2^{d-2}) \\ &= a_p(E_{\mathbb{F}_p}) \cdot a_{p^{d-1}}(E_{\mathbb{F}_p}) - p \cdot a_{p^{d-2}}(E_{\mathbb{F}_p}) \\ &\equiv a_p(E_{\mathbb{F}_p}) \cdot a_{p^{d-1}}(E_{\mathbb{F}_p}) \pmod{p}. \end{aligned}$$

By repeating this calculation we obtain: $a_{p^d}(E_{\mathbb{F}_p}) \equiv a_p(E_{\mathbb{F}_p})^d \pmod{p}$. Therefore:

$$\begin{aligned} E_{\mathbb{F}_p}(\mathbb{F}_{p^d})[p] \neq 0 \quad &\Leftrightarrow \quad p | \#E_{\mathbb{F}_p}(\mathbb{F}_{p^d}) = p^d + 1 - a_{p^d}(E_{\mathbb{F}_p}) \\ &\Leftrightarrow \quad p | (a_p(E_{\mathbb{F}_p})^d - 1). \end{aligned}$$

(2) By Theorem 2.3.6 and part (1):

$$D_{p,1}(E/\mathbb{Q}_p) \leq D_{p,1}(E_{\mathbb{F}_p}/\mathbb{F}_p) = \operatorname{ord}_p a_p(E). \tag{2.8}$$

Suppose to the contrary that the inequality (2.8) is strict. Then:

$$D_{p,1}(E/\mathbb{Q}_p) < \operatorname{ord}_p a_p(E) \leq p - 1.$$

Therefore $E(K)[p] \neq 0$ for some extension $K/\mathbb{Q}_p$ of degree $D_{p,1}(E/\mathbb{Q}_p)$. By (1.4) and Lemma 1.2.11, $E[p](K) \cong E_{\mathbb{F}_p}[p](k)$, where k is the residue field of $\mathcal{O}_K$. Thus $E_{\mathbb{F}_p}[p](k) \neq 0$ and:

$$D_{p,1}(E_{\mathbb{F}_p}/\mathbb{F}_p) \leq [k : \mathbb{F}_p] \leq [K : \mathbb{Q}_p] = D_{p,1}(E/\mathbb{Q}_p).$$

This contradiction ends the proof.

□

Proof of Theorem 2.4.1. Suppose firstly that $\left(\frac{-D}{p}\right) = -1$. Then p stays inert in $\mathcal{O}$ and thus by Deuring's criterion (cf. Lemma 1.2.7), E has supersingular reduction at p. Therefore, by Lemma 2.3.4:

$$D_{p,1}(E/\mathbb{Q}_p) = p^2 - 1.$$

Suppose now that $\left(\frac{-D}{p}\right) = 1$. By analogous reasoning, E has an ordinary reduction at p. Moreover, E is the canonical lift of $E_{\mathbb{F}_p}$ by Lemma 2.1.3. Therefore by Lemma 2.4.2 $D_{p,1}(E/\mathbb{Q}_p) = \operatorname{ord}_p a_p(E_{\mathbb{F}_p})$. Observe that $4p$ is of the form (2.7), since it splits in the quadratic order of discriminant $-D$ with class number equal to one (cf. Subsection 1.2.3). The proof follows by [Ish04, p. 126], which gives an explicit formula for $a_p(E_{\mathbb{F}_p})$. □

Remark 2.4.3. *Theorem 2.4.1 may also be proven using the main theorem of complex multiplication, cf. [Gar16, Theorem 3.2.2].*

We apply now Theorem 2.4.1 to investigate Question 2.3.2 for elliptic curves with complex multiplication.

Corollary 2.4.4. *Keep the Setup 2.0.1 and suppose that $p \geq 5$. Then $D_{p,1}(E/\mathbb{Q}_p) \in \{1,2\}$ if and only if for some $t \in \mathbb{N}$:*

$$p = \frac{1}{4}(1 + D \cdot t^2).$$

Proof. By Theorem 2.4.1, the condition $D_{p,1}(E/\mathbb{Q}_p) \in \{1,2\}$ holds if and only if $\left(\frac{-D}{p}\right) = 1$ and

$$s^2 \equiv 1 \pmod{p} \tag{2.9}$$

(recall that s, t are defined by (2.7)). The condition (2.9) is easily seen to be equivalent to the equality $p = \frac{1}{4}(1 + Dt^2)$. □

Corollary 2.4.5. *Keep the Setup 2.0.1 and suppose that $D = -4$ and $p \geq 5$. Then $D_{p,1}(E/\mathbb{Q}_p) = 8$ if and only if p is of the form $a_k^2 + a_{k+1}^2$ for some $k \geq 0$, where:*

$$a_0 = 0, \qquad a_1 = 1, \qquad a_{k+2} = 4a_{k+1} - a_k.$$

Proof. Note that $D_{p,1}(E/\mathbb{Q}_p) < p^2 - 1$ implies that $p \equiv 1 \pmod{4}$. Let s, t be defined by (2.7). Then $D_{p,1}(E/\mathbb{Q}_p) = 8$ if and only if $\mathrm{ord}_p(s) = 8$. The proof follows now from [CD14, Theorem 3, Corollary 1]. □

A version of Corollary 2.4.4 may be found in [Qin16] and in [JQ14]. Corollary 2.4.5 was proven in [Gar16] and [Gar18].

Therefore we see that Question 2.3.2 for elliptic curves with complex multiplication leads to two classical problems of number theory:

- looking for prime values of a quadratic polynomial,
- looking for primes in sequences, given by a linear recurrence.

Both problems are in general very hard. The first problem has not been solved even for a single quadratic polynomial. For example, at present, we do not know whether the polynomial x^2+1 represents infinitely many primes. This is one of Landau's four problems which were presented at the 1912 International Congress of Mathematicians, all of which remain unsolved today. See [Qin16] for related statements. Regarding the second problem, note that it is still not known whether Fibbonacci sequence contains infinitely many primes. Numerical computations show that the elements of the sequence $(a_k^2 + a_{k+1}^2)_k$ for $1 \leq k \leq 100000$ are prime for:

$$k \in \{1, 2, 3, 4, 5, 131, 200, 296, 350, 519, 704, 950, 5598, 6683, 7445, 8775, 8786, 11565, 12483\}.$$

It turns out that for $4p = s^2 + t^2$ one has $s \equiv (\frac{p-1}{4})! \pmod{p}$, which was proven by Gauss. The proof of this fact and other facts related to computing $\mathrm{ord}_p(s)$ for $\mathcal{O} = \mathbb{Z}[i]$ may be found in [CD14].

3

Lifts of non-ordinary abelian varieties

In this chapter we will consider a smooth projective curve X with an action of a finite group G over an algebraically closed field k of characteristic $p > 0$. We would like to investigate the G-equivariant behaviour of the Hodge–de Rham and conjugate exact sequences:

$$0 \to H^0(X, \Omega_{X/k}) \to H^1_{dR}(X/k) \to H^1(X, \mathcal{O}_X) \to 0, \tag{3.1}$$
$$0 \to H^1(X, \mathcal{O}_X)' \to H^1_{dR}(X/k) \to H^0(X, \Omega_{X/k})' \to 0 \tag{3.2}$$

defined in Section 1.3. The main result concerning this problem is Theorem 3.4.5. This theorem will allow us to construct non-ordinary abelian varieties without "canonical lifts" to $W_2(k)$, cf. Corollary 3.4.8. This chapter of the thesis is based on the article [Gar19a], which has been submitted for publication.

Setup 3.0.1. We will keep the above assumptions on k, G and X. Let $Y := X/G$ be the quotient of X by the action of G and let $\pi : X \to Y$ be the quotient morphism. Note that Y is a smooth projective curve. Its underlying space is the topological quotient X/G and its structure sheaf is given by $\pi_*^G(\mathcal{O}_X)$. Additionally, we will use the following notation (unless stated otherwise):

- g_Y is the genus of the curve Y,
- $R \in \mathrm{Div}(X)$ is the ramification divisor of π,
- $R' := \left[\frac{\pi_* R}{\#G}\right] \in \mathrm{Div}(Y)$, where for $\delta \in \mathrm{Div}(Y) \otimes_{\mathbb{Z}} \mathbb{Q}$, we denote by $[\delta]$ the integral part taken coefficient by coefficient,
- $k(X)$, $k(Y)$ are the function fields of X and Y,
- $v_Q(f)$ denotes the order of vanishing of a function f at a point Q,
- $\underline{R}_X$ denotes the constant sheaf on X associated to a ring R.

Fix now a (closed) point P in X. Denote:

- $G_{P,i}$ – the i-th ramification group of π at P, i.e.

$$G_{P,i} := \{g \in G : g(f) \equiv f \pmod{\mathfrak{m}_{X,P}^{i+1}} \quad \text{for all } f \in \mathcal{O}_{X,P}\}.$$

Note that (since k is algebraically closed) the inertia group $G_{P,0}$ coincides with the decomposition group at P, i.e. the stabilizer of P in G. Define also:

$$d_P = \sum_{i \geq 0} (\#G_{P,i} - 1).$$

Then (by [Ser79, IV §1, Proposition 4]) $R = \sum_{P \in X} d_P \cdot (P)$.

- e_P – the ramification index of π at P, i.e. $e_P = \#G_{P,0}$.
- n_P is given by the formula:

$$n_P := \max\{n : G_{P,n} \neq 0\}.$$

Also, by abuse of notation, for $Q \in Y$ we write $e_Q := e_P$, $d_Q := d_P$, $n_Q := n_P$ for any $P \in \pi^{-1}(Q)$. Note that these quantities don't depend on the choice of P, since the covering $\pi : X \to Y$ is Galois.

Finally, recall that for any k-vector space V, V' denotes the k-vector space with the same underlying abelian group as V and the scalar multiplication $(\lambda, v) \mapsto \lambda^p \cdot v$.

3.1. G-sheaves on a curve

Keep the Setup 3.0.1. In order to investigate the equivariant behaviour of the sequences (3.1) and (3.2), we consider the following "defect":

$$\delta(X, G) \quad := \quad \dim_k H^0(X, \Omega_{X/k})^G + \dim_k H^1(X, \mathcal{O}_X)^G - \dim_k H^1_{dR}(X/k)^G.$$

Observe that if either of the exact sequences (3.1) and (3.2) splits G-equivariantly, then we have $\delta(X, G) = 0$. Thus $\delta(X, G)$ may be considered as an 'obstruction to the splitting'.

In order to compute $\delta(X, G)$, we need to work with the group cohomology of sheaves (cf. Section 1.4). We start by investigating the G-sheaves on Y coming from G-coverings. Let $\mathcal{F}$ be an $\mathcal{O}_X$-module with a G-action compatible with that on X. Then $\pi_*\mathcal{F}$ is an $\mathcal{O}_Y[G]$-module. It is natural to try to relate the group cohomology of $\pi_*\mathcal{F}$ to the ramification of π. Suppose for a while that the action of G on X is free, i.e. that $\pi : X \to Y$ is unramified. In this case the functors

$$\begin{array}{rcl} \mathcal{F} & \mapsto & \pi_*^G(\mathcal{F}), \\ \pi^*(\mathcal{G}) & \leftarrow\!\shortmid & \mathcal{G} \end{array}$$

are exact and provide an equivalence between the category of coherent $\mathcal{O}_Y$-modules and coherent $\mathcal{O}_X$-modules (cf. [Mum08, Proposition II.7.2, p. 70]). In particular, $\mathcal{H}^i(G, \pi_*\mathcal{F}) = 0$ for all $i \geq 1$ and every coherent $\mathcal{O}_X$-module $\mathcal{F}$. The following Proposition treats the general case of not necessarily free G-action.

Proposition 3.1.1. *Keep the Setup 3.0.1. Let $\mathcal{F}$ be a coherent $\mathcal{O}_X$-module with a G-action lifting that on X. Then, for every $i \geq 1$, $\mathcal{H}^i(G, \pi_*\mathcal{F})$ is a torsion sheaf supported on the wild ramification locus of π.*

Recall that the wild ramification locus of π is the set of points $Q \in Y$ with $n_Q \geq 1$. To prove Proposition 3.1.1 we shall need the following lemma involving group cohomology of modules over Dedekind domains.

Lemma 3.1.2. *Let k be an algebraically closed field of an arbitrary characteristic. Let B be a finitely generated k-algebra, which is a Dedekind domain equipped with a k-linear action of the group G. Suppose that $A := B^G$ is a principal ideal domain with a maximal ideal $\mathfrak{q}$. Let $G_{\mathfrak{p},i}$ denote the i-th higher ramification group of a prime ideal $\mathfrak{p} \in \operatorname{Spec} B$ over $\mathfrak{q}$. Then for every B-module M we have an isomorphism of B-modules:*

$$H^i(G, M) \cong H^i(G_{\mathfrak{p},1}, M_{\mathfrak{p}}),$$

where $M_{\mathfrak{p}}$ denotes the localisation of M at $\mathfrak{p}$.

Proof. By (1.18) we have: $H^i(G, M) \cong H^i(G, \widehat{M}_{\mathfrak{q}})$. One easily sees that we have an isomorphism of $B[G]$-modules:

$$\widehat{M}_{\mathfrak{q}} \cong \operatorname{Ind}_{G_{\mathfrak{p},0}}^{G} \widehat{M}_{\mathfrak{p}}$$

(see [Ser79, II §3, Proposition 4] for a proof for $M = B$. The general case follows by tensoring both sides by M). Therefore by (1.16) and (1.18) $H^i(G, M) \cong H^i(G_{\mathfrak{p},0}, \widehat{M}_{\mathfrak{p}}) \cong H^i(G_{\mathfrak{p},0}, M_{\mathfrak{p}})$. Moreover, $G_{\mathfrak{p},1}$ is a normal p-Sylow subgroup of $G_{\mathfrak{p},0}$ (cf. [Ser79, Corollary 4.2.3., p. 67]). Hence the proof follows by (1.17). □

Proof of Proposition 3.1.1. Denote by ξ the generic point of Y. Recall that by the normal base theorem (cf. [Jac85, sec. 4.14]), $k(X) = \operatorname{Ind}^G k(Y)$ is an induced G-module. Therefore $(\pi_* \mathcal{F})_\xi$ is also an induced G-module (since it is a $k(X)$-vector space of finite dimension) and by (1.16):

$$\mathcal{H}^i(G, \pi_* \mathcal{F})_\xi = H^i(G, (\pi_* \mathcal{F})_\xi) = 0 \qquad \text{for } i \geq 1.$$

Thus, since the sheaf $\mathcal{H}^i(G, \pi_* \mathcal{F})$ is coherent, it must be a torsion sheaf. Note that if a point $Q \in Y$ is tamely ramified then $G_{P,1} = 0$ for any $P \in \pi^{-1}(Q)$ and thus $\mathcal{H}^i(G, \pi_* \mathcal{F})_Q = 0$ by Lemma 3.1.2. This concludes the proof. □

We will recall now a standard formula describing G-invariants of an $\mathcal{O}_Y[G]$-module coming from an invertible $\mathcal{O}_X$-module. For a proof see [BM00, Proposition 5.3.2].

Lemma 3.1.3. *For any G-invariant divisor $D \in \operatorname{Div}(X)$:*

$$\pi_*^G(\mathcal{O}_X(D)) = \mathcal{O}_Y\left(\left[\frac{\pi_* D}{\#G}\right]\right),$$

where for $\delta \in \operatorname{Div}(Y) \otimes_{\mathbb{Z}} \mathbb{Q}$, we denote by $[\delta]$ the integral part taken coefficient by coefficient.

Corollary 3.1.4. *Keep the Setup 3.0.1. Let:*

$$R' = \left[\frac{\pi_* R}{\#G}\right] \in \operatorname{Div}(Y).$$

Then:

$$\pi_*^G \Omega_{X/k} = \Omega_{Y/k} \otimes \mathcal{O}_Y(R').$$

In particular:

$$\dim_k H^0(X, \Omega^1_{X/k})^G = \begin{cases} g_Y, & \text{if } R' = 0, \\ g_Y - 1 + \deg R', & \text{otherwise.} \end{cases}$$

Proof. The first claim follows from Lemma 3.1.3 if one takes for D the canonical divisor of X and uses the Riemann-Hurwitz formula. To prove the second claim we observe that

$$H^0(X, \Omega_{X/k})^G = H^0(Y, \pi_*^G \Omega_{X/k}) = H^0(Y, \Omega_{Y/k} \otimes \mathcal{O}_Y(R'))$$

and apply the Riemann-Roch theorem (cf. [Har77, Theorem IV.1.3]). □

We end this section with one more elementary observation.

Lemma 3.1.5. *The divisor R' vanishes, if and only if, the morphism $\pi : X \to Y$ is tamely ramified.*

Proof. Recall that $R = \sum_{P \in X} d_P \cdot (P)$. Hence

$$\begin{aligned} R' &= \sum_{Q \in Y} \left[\frac{d_Q \cdot \#\pi^{-1}(Q)}{\#G} \right] (Q) \\ &= \sum_{Q \in Y} \left[\frac{d_Q}{e_Q} \right] (Q). \end{aligned}$$

On the other hand, we have: $d_Q \geq e_Q - 1$ with an equality if and only if π is tamely ramified at Q. This completes the proof. □

3.2. Computing the defect

The goal of this section is to compute the defect $\delta(X, G)$ in terms of cetain group cohomologies.

Proposition 3.2.1. *Keep the Setup 3.0.1. We have:*

$$\delta(X, G) = \sum_{Q \in Y} \dim_k \operatorname{im} \Big(H^1(G, (\pi_* \mathcal{O}_X)_Q) \to H^1(G, (\pi_* \Omega_{X/k})_Q) \Big),$$

where

$$H^1(G, (\pi_* \mathcal{O}_X)_Q) \to H^1(G, (\pi_* \Omega_{X/k})_Q)$$

is the map induced by the derivation map $\mathcal{O}_X \to \Omega_{X/k}$.

Note that π is an affine morphism. Therefore π_* is an exact functor on the category of quasi-coherent sheaves. Thus using the spectral sequence (1.11) we obtain:

$$H^i_{dR}(X/k) = \mathbb{H}^i(X, \Omega^\bullet_{X/k}) = \mathbb{H}^i(Y, \pi_* \Omega^\bullet_{X/k}).$$

We start with the following observation.

Lemma 3.2.2. *The spectral sequence*

$$E_1^{ij} = H^j(Y, \pi_*^G \Omega^i_{X/k}) \Rightarrow \mathbb{H}^{i+j}(Y, \pi_*^G \Omega^\bullet_{X/k})$$

degenerates at the first page.

Proof. We have a morphism of complexes $\Omega^\bullet_{Y/k} \to \pi_*^G \Omega^\bullet_{X/k}$, which is an isomorphism on the zeroth term. Thus for $j = 0, 1$ we obtain a commutative diagram:

$$\begin{array}{ccc} H^j(Y, \mathcal{O}_Y) & \xrightarrow{\cong} & H^j(Y, \pi_*^G \mathcal{O}_X) \\ \downarrow & & \downarrow \\ H^j(Y, \Omega_{Y/k}) & \longrightarrow & H^j(Y, \pi_*^G \Omega_{X/k}), \end{array} \tag{3.3}$$

where the upper arrow is an isomorphism. Note also that the left arrow in the diagram (3.3) is zero for $j = 0, 1$. Indeed, this is immediate for the map:

$$d : k \cong H^0(Y, \mathcal{O}_Y) \to H^0(Y, \Omega_{Y/k}) \tag{3.4}$$

(since the differential of a constant is zero) and the map $d : H^1(Y, \mathcal{O}_Y) \to H^1(Y, \Omega_{Y/k})$ is the dual of (3.4). Therefore the diagram (3.3) shows that for $j = 0, 1$ the maps

$$H^j(Y, \pi_*^G \mathcal{O}_X) \to H^j(Y, \pi_*^G \Omega_{X/k})$$

are zero. This implies the desired conclusion. □

Corollary 3.2.3.

$$\begin{aligned} \delta(X, G) &= \Big(\dim_k \mathbb{H}^1(Y, \pi_*^G \Omega^\bullet_{X/k}) - \dim_k \mathbb{H}^1(Y, \pi_* \Omega^\bullet_{X/k})^G \Big) \\ &- \Big(\dim_k H^1(Y, \pi_*^G \mathcal{O}_X) - \dim_k H^1(Y, \pi_* \mathcal{O}_X)^G \Big). \end{aligned}$$

Proof. By Lemma 3.2.2 we obtain an exact sequence:

$$0 \to H^0(Y, \pi_*^G \Omega_{X/k}) \to \mathbb{H}^1(Y, \pi_*^G \Omega^\bullet_{X/k}) \to H^1(Y, \pi_*^G \mathcal{O}_{X/k}) \to 0.$$

Recall also that (since π is affine) $H^1(X, \mathcal{O}_X) \cong H^1(Y, \pi_* \mathcal{O}_X)$ and $H^1_{dR}(X/k) \cong \mathbb{H}^1(Y, \pi_* \Omega^\bullet_{X/k})$. Hence:

$$\begin{aligned} \delta(X, G) &= \dim_k H^0(X, \Omega_{X/k})^G + \dim_k H^1(X, \mathcal{O}_X)^G - \dim_k H^1_{dR}(X/k)^G \\ &= \Big(\dim_k \mathbb{H}^1(Y, \pi_*^G \Omega^\bullet_{X/k}) - \dim_k H^1(Y, \pi_*^G \mathcal{O}_X) \Big) \\ &+ \dim_k H^1(X, \mathcal{O}_X)^G - \dim_k H^1_{dR}(X/k)^G \\ &= (\dim_k \mathbb{H}^1(Y, \pi_*^G \Omega^\bullet_{X/k}) - \dim_k \mathbb{H}^1(Y, \pi_* \Omega^\bullet_{X/k})^G) \\ &- (\dim_k H^1(Y, \pi_*^G \mathcal{O}_X) - \dim_k H^1(Y, \pi_* \mathcal{O}_X)^G). \end{aligned}$$

□

Corollary 3.2.3 implies that we need to compare the hypercohomology groups

$$\mathbb{H}^i(Y, (\mathcal{F}^\bullet)^G) \text{ and } \mathbb{H}^i(Y, \mathcal{F}^\bullet)^G.$$

for $\mathcal{F}^\bullet = \pi_* \mathcal{O}_X[0]$ and $\mathcal{F}^\bullet = \pi_* \Omega^\bullet_{X/k}$ (note that the latter is a complex of $\underline{k}_Y[G]$-modules rather than $\mathcal{O}_Y[G]$-modules, since the differentials in the de Rham complex are not $\mathcal{O}_Y$-linear). Consider the commutative diagram of functors:

$$\begin{array}{ccc} \underline{k}_Y[G]\text{-mod} & \xrightarrow{(-)^G} & \underline{k}_Y\text{-mod} \\ \downarrow{\scriptstyle \Gamma(Y,-)} & & \downarrow{\scriptstyle \Gamma(Y,-)} \\ k[G]\text{-mod} & \xrightarrow{(-)^G} & k\text{-mod}\,. \end{array}$$

By applying the Grothendieck spectral sequence to compositions of the functors in the diagram, we obtain two spectral sequences:

$$
\begin{aligned}
{}_{I}E_2^{ij} &= \mathbb{H}^i(Y, \mathcal{H}^j(G, \mathcal{F}^\bullet)) \Rightarrow \mathbb{R}^{i+j}\Gamma^G(\mathcal{F}^\bullet), && (3.5)\\
{}_{II}E_2^{ij} &= H^i(G, \mathbb{H}^j(Y, \mathcal{F}^\bullet)) \Rightarrow \mathbb{R}^{i+j}\Gamma^G(\mathcal{F}^\bullet)., && (3.6)
\end{aligned}
$$

Note that here $\mathcal{H}^j(G, \mathcal{F}^\bullet)$ denotes a complex of $\underline{k}_Y$-modules with the l-th term being $\mathcal{H}^j(G, \mathcal{F}^l)$. For motivation, suppose at first that the 'obstructions'

$$\mathcal{H}^i(G, \mathcal{F}^l) \quad \text{and} \quad H^i(G, \mathbb{H}^l(Y, \mathcal{F}^\bullet))$$

vanish for all $i \geq 1$ and $l \geq 0$ (this happens e.g. if $\operatorname{char} k = 0$). Then the spectral sequences (3.5) and (3.6) lead us to the isomorphisms:

$$\mathbb{H}^i(Y, (\mathcal{F}^\bullet)^G) \cong \mathbb{R}^i\Gamma^G(\mathcal{F}^\bullet) \cong (\mathbb{H}^i(Y, \mathcal{F}^\bullet))^G.$$

In general, the relation between $\mathbb{H}^i(Y, (\mathcal{F}^\bullet)^G)$ and $\mathbb{H}^i(Y, \mathcal{F}^\bullet)^G$ is more complicated. However, in the case of the first hypercohomology group, one can extract some information from the low-degree exact sequences of spectral sequences (3.5) and (3.6):

$$
\begin{aligned}
0 &\to \mathbb{H}^1(Y, (\mathcal{F}^\bullet)^G) \to \mathbb{R}^1\Gamma^G(\mathcal{F}^\bullet) \to && (3.7)\\
&\to \mathbb{H}^0(Y, \mathcal{H}^1(G, \mathcal{F}^\bullet)) \to \mathbb{H}^2(Y, (\mathcal{F}^\bullet)^G) \to\\
&\to \mathbb{R}^2\Gamma^G(\mathcal{F}^\bullet)
\end{aligned}
$$

and respectively:

$$
\begin{aligned}
0 &\to H^1(G, \mathbb{H}^0(Y, \mathcal{F}^\bullet)) \to \mathbb{R}^1\Gamma^G(\mathcal{F}^\bullet) \to && (3.8)\\
&\to \mathbb{H}^1(Y, \mathcal{F}^\bullet)^G \to H^2(G, \mathbb{H}^0(Y, \mathcal{F}^\bullet)) \to\\
&\to \mathbb{R}^2\Gamma^G(\mathcal{F}^\bullet).
\end{aligned}
$$

This will be done separately in the case of wild and tame ramification.

Proof – the wild case. Consider first the case when π is wildly ramified, i.e. by Lemma 3.1.5 when $R' \neq 0$. Then, as one easily sees by Lemma 3.2.2:

$$\mathbb{H}^2(Y, \pi_*^G \Omega^\bullet_{X/k}) \cong H^1(Y, \pi_*^G \Omega_{X/k}).$$

Therefore, using Corollary 3.1.4 and Riemann–Roch theorem (cf. [Har77, Theorem IV.1.3]):

$$\mathbb{H}^2(Y, \pi_*^G \Omega^\bullet_{X/k}) \cong H^1(Y, \Omega_{Y/k} \otimes \mathcal{O}_Y(R')) \cong 0. \tag{3.9}$$

By (3.7) and (3.9) we see that

$$
\begin{aligned}
\dim_k \mathbb{R}^1\Gamma^G(\pi_*\Omega^\bullet_{X/k}) &= \dim_k \mathbb{H}^1(Y, (\pi_*\Omega^\bullet_{X/k})^G) && (3.10)\\
&+ \dim_k \mathbb{H}^0(Y, \mathcal{H}^1(G, \pi_*\Omega^\bullet_{X/k})).
\end{aligned}
$$

On the other hand, (3.8) yields:

$$
\begin{aligned}
\dim_k \mathbb{R}^1\Gamma^G(\pi_*\Omega^\bullet_{X/k}) &= \dim_k H^1(G, \mathbb{H}^0(Y, \pi_*\Omega^\bullet_{X/k})) && (3.11)\\
&+ \dim_k \mathbb{H}^1(Y, \pi_*\Omega^\bullet_{X/k})^G - c_1,
\end{aligned}
$$

where

$$c_1 \;=\; \dim_k \ker\Big(H^2(G,\mathbb{H}^0(Y,\pi_*\Omega^\bullet_{X/k})) \to \mathbb{R}^2\Gamma^G(\pi_*\Omega^\bullet_{X/k})\Big). \tag{3.12}$$

Thus by comparing (3.10) and (3.11):

$$\begin{aligned}\dim_k \mathbb{H}^1(Y,\pi_*\Omega^\bullet_{X/k})^G &= \dim_k \mathbb{H}^1(Y,(\pi_*\Omega^\bullet_{X/k})^G) \\ &+ \dim_k \mathbb{H}^0(Y,\mathcal{H}^1(G,\pi_*\Omega^\bullet_{X/k})) \\ &- \dim_k H^1(G,\mathbb{H}^0(Y,\pi_*\Omega^\bullet_{X/k})) + c_1.\end{aligned} \tag{3.13}$$

By repeating the same argument for $\pi_*\mathcal{O}_X$, we obtain:

$$\begin{aligned}\dim_k H^1(Y,\pi_*\mathcal{O}_X)^G &= \dim_k H^1(Y,(\pi_*\mathcal{O}_X)^G) \\ &+ \dim_k H^0(Y,\mathcal{H}^1(G,\pi_*\mathcal{O}_X)) \\ &- \dim_k H^1(G,H^0(Y,\pi_*\mathcal{O}_X)) + c_2,\end{aligned} \tag{3.14}$$

where:

$$c_2 \;=\; \dim_k \ker\Big(H^2(G,H^0(Y,\pi_*\mathcal{O}_X)) \to R^2\Gamma^G(\pi_*\mathcal{O}_X)\Big). \tag{3.15}$$

By combining (3.13), (3.14) and Corollary 3.2.3 we obtain:

$$\begin{aligned}\delta(X,G) &= \dim_k \operatorname{im}\Big(H^0(Y,\mathcal{H}^1(G,\pi_*\mathcal{O}_X)) \to H^0(Y,\mathcal{H}^1(G,\pi_*\Omega_{X/k}))\Big) \\ &+ (c_2 - c_1).\end{aligned}$$

Note that since $\mathcal{H}^1(G,\pi_*\mathcal{O}_X)$, $\mathcal{H}^1(G,\pi_*\Omega_{X/k})$ are torsion sheaves, we can compute their sections by taking stalks and using (1.19):

$$\begin{aligned}&\dim_k \operatorname{im}\Big(H^0(Y,\mathcal{H}^1(G,\pi_*\mathcal{O}_X)) \to H^0(Y,\mathcal{H}^1(G,\pi_*\Omega_{X/k}))\Big) = \\ &\sum_{Q\in Y} \dim_k \operatorname{im}\Big(H^1(G,(\pi_*\mathcal{O}_X)_Q) \to H^1(G,(\pi_*\Omega_{X/k})_Q)\Big).\end{aligned}$$

Thus we are left with showing that $c_1 = c_2$. This will be done at the end of this Section.

Proof – the tame case. Consider now the case of tame ramification, i.e. $R' = 0$. Then by Propostion 3.1.1 we see that $\mathcal{H}^i(G,\pi_*\Omega^j_{X/k}) = 0$ for $i \geq 1$, $j \geq 0$. Thus it is evident by (3.5) that

$$\mathbb{R}^i\Gamma^G(\pi_*\Omega^\bullet_{X/k}) \cong \mathbb{H}^i(Y,(\pi_*\Omega^\bullet_{X/k})^G).$$

Therefore the exact sequence (3.8) implies that:

$$\dim_k \mathbb{H}^1(Y,\pi_*\Omega^\bullet_{X/k})^G \;=\; \dim_k \mathbb{H}^1(Y,\pi_*^G\Omega^\bullet_{X/k}) + \dim_k H^1(G,k) + c_1,$$

where c_1 is given by (3.12). One proceeds analogously as in the wildly ramified case to obtain:

$$\delta(X,G) = (c_2 - c_1).$$

Again, it remains to prove that $c_1 = c_2$.

Proof – the end. Recall that in order to prove Proposition 3.2.1 we have to investigate the map

$$H^2(G, \mathbb{H}^0(Y, \mathcal{F}^\bullet)) \to \mathbb{R}^2\Gamma^G(\mathcal{F}^\bullet) \tag{3.16}$$

arising in the exact sequence (3.8).

Lemma 3.2.4. *Let $\mathcal{F}^\bullet$ be complex of $\mathcal{O}[G]$-sheaves on a ringed space $(Y, \mathcal{O})$, which is a noetherian topological space of dimension 1. Suppose that $\mathcal{F}^j = 0$ for $j \neq 0, 1$ and that the support of the sheaf $\mathcal{H}^i(G, \mathcal{F}^j)$ is a finite subset of Y for $i \geq 1$ and $j \in \{0, 1\}$. There exists a natural monomorphism*

$$\mathbb{H}^0(Y, \mathcal{H}^2(G, \mathcal{F}^\bullet)) \hookrightarrow \mathbb{R}^2\Gamma^G(\mathcal{F}^\bullet).$$

It is an isomorphism, provided that $\mathcal{F}^\bullet$ is a complex concentrated in degree 0.

Proof. Note that for $i \geq 2$, $j \geq 1$ in the spectral sequence (3.5):

$${}_IE_2^{ij} = \mathbb{H}^i(Y, \mathcal{H}^j(G, \mathcal{F}^\bullet)) = 0.$$

Indeed, this follows from (1.11), since for every l, $H^i(Y, \mathcal{H}^j(G, \mathcal{F}^l)) = 0$ for $i, j \geq 1$ (cf. [Har77, Theorem III.2.7]), for $i \geq 2$ and for $j \geq 2$. Thus it is evident that there exists a natural monomorphism

$$\mathbb{H}^0(Y, \mathcal{H}^2(G, \mathcal{F}^\bullet)) = {}_IE_2^{02} = {}_IE_\infty^{02} \hookrightarrow \mathbb{R}^2\Gamma^G(\mathcal{F}^\bullet).$$

Suppose now that $\mathcal{F}^\bullet$ is concentrated in degree 0. Then ${}_IE_2^{ij} = 0$ for $i, j \geq 1$ and for $i \geq 2$. Therefore ${}_IE_\infty^{11} = {}_IE_2^{11} = 0$ and ${}_IE_\infty^{20} = {}_IE_2^{20} = 0$, which leads to the conclusion. □

Corollary 3.2.5. *There exists a commutative diagram*

$$\begin{array}{ccc} H^2(G, \mathbb{H}^0(Y, \mathcal{F}^\bullet)) & \longrightarrow & \mathbb{R}^2\Gamma^G(\mathcal{F}^\bullet) \\ \downarrow & \nearrow & \\ \mathbb{H}^0(Y, \mathcal{H}^2(G, \mathcal{F}^\bullet)), & & \end{array}$$

where the upper arrow is (3.16)*, and the diagonal arrow is as in Lemma 3.2.4.*

Proof. The morphism $\mathcal{F}^\bullet \to \mathcal{F}^0[0]$ yields by functoriality the commutative diagram:

$$\begin{array}{ccccc} H^2(G, \mathbb{H}^0(Y, \mathcal{F}^\bullet)) & \longrightarrow & \mathbb{R}^2\Gamma^G(\mathcal{F}^\bullet) & \longleftarrow & \mathbb{H}^0(Y, \mathcal{H}^2(G, \mathcal{F}^\bullet)) \\ \downarrow & & \downarrow & & \downarrow \\ H^2(G, H^0(Y, \mathcal{F}^0)) & \longrightarrow & R^2\Gamma^G(\mathcal{F}^0) & \xleftarrow{\cong} & H^0(Y, \mathcal{H}^2(G, \mathcal{F}^0)). \end{array}$$

By composing the maps from the diagram we obtain a map

$$\begin{array}{rcl} H^2(G, \mathbb{H}^0(Y, \mathcal{F}^\bullet)) & \to & H^2(G, H^0(Y, \mathcal{F}^0)) \\ \to R^2\Gamma^G(\mathcal{F}^0) & \cong & H^0(Y, \mathcal{H}^2(G, \mathcal{F}^0)). \end{array} \tag{3.17}$$

One easily checks that the image of the map (3.17) lies in the image of

$$\mathbb{H}^0(Y, \mathcal{H}^2(G, \mathcal{F}^\bullet)) \hookrightarrow H^0(Y, \mathcal{H}^2(G, \mathcal{F}^0)).$$

This clearly completes the proof. □

We are now ready to finish the proof of Proposition 3.2.1. Recall that we are left with showing that $c_1 = c_2$ (where c_1 and c_2 are given by (3.12) and (3.15) respectively). By using Corollary 3.2.5 for $\mathcal{F}^\bullet = \pi_*\Omega^\bullet_{X/k}$, Lemma 3.2.4 and the equality

$$\mathbb{H}^0(Y, \pi_*\Omega^\bullet_{X/k}) = H^0(Y, \pi_*\mathcal{O}_X) = k$$

we obtain:

$$\begin{aligned} c_1 &= \dim_k \ker\left(H^2(G, \mathbb{H}^0(Y, \pi_*\Omega^\bullet_{X/k})) \to \mathbb{R}^2\Gamma^G(\pi_*\Omega^\bullet_{X/k})\right) \\ &= \dim_k \ker\left(H^2(G, \mathbb{H}^0(Y, \pi_*\Omega^\bullet_{X/k})) \to \mathbb{H}^0(Y, \mathcal{H}^2(G, \pi_*\Omega^\bullet_{X/k}))\right) \\ &= \dim_k \ker\left(H^2(G, \mathbb{H}^0(Y, \pi_*\mathcal{O}_X)) \to H^0(Y, \mathcal{H}^2(G, \pi_*\mathcal{O}_X))\right) \\ &= \dim_k \ker\left(H^2(G, \mathbb{H}^0(Y, \pi_*\mathcal{O}_X)) \to R^2\Gamma^G(\pi_*\mathcal{O}_X)\right) \\ &= c_2. \end{aligned}$$

3.3. Local terms for the Artin-Schreier coverings

The main goal of this section is to compute the local terms occuring in Proposition 3.2.1 in case when $G = \mathbb{Z}/p$. We start by recalling the most important facts concerning Artin–Schreier coverings. For a reference see e.g. [PZ12, sec. 2.2]. Let X be a smooth algebraic curve with an action of $G = \mathbb{Z}/p$ over an algebraically closed field k of characteristic p and let $Y := X/G$. By Artin–Schreier theory, the function field of X equals $k(Y)(z)$, where:

$$z^p - z = f \tag{3.18}$$

for some $f \in k(Y)$. The action of $G = \langle\sigma\rangle \cong \mathbb{Z}/p$ is then given by $\sigma(z) := z + 1$. Let $\mathcal{P} \subset Y$ denote the branch locus of the quotient morphism $\pi : X \to Y$. Note that $\mathcal{P}$ is contained in the set of poles of f and moreover for any $Q \in Y$:

$$\#\pi^{-1}(Q) = \begin{cases} p, & \text{for } Q \notin \mathcal{P}, \\ 1, & \text{otherwise.} \end{cases}$$

Lemma 3.3.1. *Keep the above setting. Fix a point $Q \in \mathcal{P}$ and let $\pi^{-1}(Q) = \{P\}$. Suppose that $p \nmid n := v_Q(f)$. Then for some $t \in \widehat{\mathcal{O}}_{X,P}$ and $x \in \widehat{\mathcal{O}}_{Y,Q}$:*

- $\widehat{\mathcal{O}}_{X,P} = k[[t]]$, $\widehat{\mathcal{O}}_{Y,Q} = k[[x]]$,
- $t^{-np} - t^{-n} = x^{-n}$,
- *the action of $G \cong \mathbb{Z}/p$ on t is given by an automorphism:*

$$\sigma(t) = \frac{t}{(1+t^n)^{1/n}} = t - \frac{1}{n}t^{n+1} + \text{ (terms of order } \geq n+2\text{).} \tag{3.19}$$

In particular, n is equal to n_Q as defined in the Setup 3.0.1.

Proof. Let x, t be arbitrary uniformizers at Q and P respectively. Then $\widehat{\mathcal{O}}_{Y,Q} = k[[x]]$ and $\widehat{\mathcal{O}}_{X,P} = k[[t]]$. Before the proof observe that for $h \in k[[x]]$ the equation $u^m = h(x)$ has a solution $u \in k[[x]]$, whenever $p \nmid m$ and $m | v_Q(h)$ (this follows easily from Hensel's lemma). We will denote a fixed solution by $h(x)^{1/m}$. Note that:

$$f^{-1} = \frac{z^{-p}}{1 - z^{1-p}}.$$

By comparing the valuations we see that $v_P(z) = -n$. Thus we may replace t by $z^{-1/n}$ to ensure that $z = t^{-n}$. Then:

$$\begin{aligned} \sigma(t)^n &= \sigma(t^n) = \sigma\left(\frac{1}{z}\right) \\ &= \frac{1}{z+1} = \frac{1}{t^{-n}+1} = \frac{t^n}{1+t^n} \end{aligned}$$

and thus we can assume without loss of generality (by replacing σ by its power if necessary) that $\sigma(t) = \frac{t}{(1+t^n)^{1/n}}$. Finally, we replace x by $f(x)^{-1/n}$ to ensure that $t^{-np} - t^{-n} = x^{-n}$. $\square$

Example 3.3.2. *Let X/k be the smooth projective curve with the affine part given by the equation:*

$$y^m = f(z^p - z),$$

where f is a separable polynomial and $p \nmid m$. Denote by $\mathcal{P}$ the set of points of X at infinity (i.e. of points of X that do not belong to the affine part). One checks that $\#\mathcal{P} = \mathrm{GCD}(m, \deg f) =: \delta$ (cf. [Tow96, Section 1]). The group $G = \mathbb{Z}/p$ acts on X via the automorphism $\varphi(z, y) = (z + 1, y)$. Then X is a $\mathbb{Z}/p$-covering of a curve Y with the affine equation:

$$y^m = f(x).$$

The function field of X is $k(Y)(z)$, where $z^p - z = x$. As proven in [Tow96] the function $x \in k(Y)$ has δ poles, each of them of order m/δ. This establishes the formula:

$$n_P = \begin{cases} m/\delta, & \text{if } P \in \mathcal{P}, \\ 0, & \text{otherwise.} \end{cases} \tag{3.20}$$

In particular, the action of G on X is weakly ramified if and only if $m | \deg f$.

Remark 3.3.3. *Suppose that $\pi : X \to Y$ is an Artin-Schreier covering. For every point $Q \in \mathcal{P}$ we can find functions $f_Q \in k(Y)$, $z_Q \in k(X)$ such that the function field of X is given by the equation $z_Q^p - z_Q = f_Q$ and either $f_Q \in \mathcal{O}_{Y,Q}$ or $p \nmid v_Q(f_Q)$. Indeed, in order to obtain f_Q one can repeatedly subtract from f a function of the form $h^p - h$, where h is a power of a uniformizer at Q.*

Example 3.3.4. *It might not be possible to find a function f such that the function field of X is given by (3.18) and for any pole Q of f one has $p \nmid v_Q(f)$. Take for example an ordinary elliptic curve $X/\overline{\mathbb{F}}_p$. Let $\tau : X \to X$ be the translation by a p-torsion point. Consider the action of $G = \langle \tau \rangle \cong \mathbb{Z}/p$ on X. This group action is free and hence $n_P = 0$ for all $P \in X$. Thus, if $k(X)$ would have an equation of the form $z^p - z = f$, where $p \nmid v_Q(f)$ for all $Q \in \mathcal{P}$, then f would have no poles. This easily leads to a contradiction.*

Keep the notation of Lemma 3.3.1. Fix an integer $a \in \mathbb{Z}$ and denote:

- $B := \widehat{\mathcal{O}}_{Y,Q} = k[[t]]$, $L := k((t))$, $I := t^a B$,
- $A := \widehat{\mathcal{O}}_{X,P} = k[[x]]$, $K := k((x))$.

In the Lemma below we will compute $H^1(G, I)$. The dimension of $H^1(G, I)$ is computed also in [BM00, Théoréme 4.1.1] and [Kon07, formula (18)]. However, we need an explicit description of a basis of $H^1(G, I)$.

Lemma 3.3.5. *Keep the notation introduced in Lemma 3.3.1 and above.*

(1) $H^1(G, I)$ *may be identified with*

$$M := \operatorname{coker}(L^G \to (L/I)^G).$$

(2) A basis of $H^1(G, I)$ *is given by the images of the elements* $(t^i)_{i\in J}$ *in* M*, where*

$$J := \{a - n \leq i \leq a - 1 : p \nmid i\}.$$

(3) $\dim_k H^1(G, I) = n - \left[\frac{a-1}{p}\right] + \left[\frac{a-1-n}{p}\right]$.

(4) The images of the elements:

$$t^i \qquad \text{for } a - n \leq i \leq a - 1 \text{ where } p|i$$

are zero in M*.*

Proof. For any $h \in L$, we will denote its images in L/I and M by $[h]_{L/I}$ and $[h]_M$, respectively.

(1) The proof follows by taking the long exact sequence of cohomology for the short exact sequence of $k[G]$-modules:

$$0 \to I \to L \to L/I \to 0$$

and using the Normal Base Theorem (cf. [Jac85, sec. 4.14]).

(2) Note that for any $a - n \leq i \leq a - 1$, we have $[t^i]_{L/I} \in (L/I)^G$, since

$$\begin{aligned} \sigma([t^i]_{L/I}) &= [\sigma(t^i)]_{L/I} = [(t - \frac{1}{n}t^{n+1} + O(t^{2n}))^i]_{L/I} = \\ &= [t^i - \frac{i}{n}t^{i+n} + O(t^{2n})]_{L/I} = [t^i]_{L/I}. \end{aligned}$$

We will show now that the set $([t^i]_M)_{i\in J}$ spans M. Note that $L^G = K$. Therefore it suffices to show that for any $[h]_{L/I} \in (L/I)^G$, one has

$$h \in K + \bigoplus_{i\in J} k \cdot t^i. \tag{3.21}$$

Let $h = \sum_{i=N}^{a-1} a_i t^i \in L$, where $a_N \neq 0$. Observe that if $p|j$ and $a_j \neq 0$, then we may replace h by $h - c \cdot x^{j/p}$ for a suitable constant $c \in k$, since valuation of x in L equals p. Thus without loss of generality we may assume that $a_j = 0$ for $p|j$ and that $p \nmid N$. The equality $\sigma([h]_{L/I}) = [h]_{L/I}$ is equivalent to

$$\sum_{i=N}^{a-1} a_i \sigma(t)^i = \sum_{i=N}^{a-1} a_i t^i + \sum_{i=a}^{\infty} b_i t^i$$

for some $b_a, b_{a+1}, \ldots \in k$. By using equality (3.19) this implies:

$$\sum_{i=N}^{a-1} a_i t^i \cdot \left(1 - \frac{i}{n} t^n + O(t^{2n})\right) = \sum_{i=N}^{a-1} a_i t^i + \sum_{i=a}^{\infty} b_i t^i.$$

By comparing coefficients of t^{N+n}, we see that either $N+n \geq a$, or

$$a_N \cdot \left(-\frac{N}{n}\right) + a_{N+n} = a_{N+n}.$$

The second possibility easily leads to a contradiction. This proves (3.21). We check now linear independence of the considered elements. Suppose that for some $a_i \in k$ not all equal to zero:

$$\sum_{i \in J} a_i [t^i]_M = 0$$

or equivalently,

$$\sum_{i \in J} a_i t^i = \sum_{j \geq N} b_j x^j + \sum_{j \geq a} c_j t^j \tag{3.22}$$

for some $b_j, c_j \in k$, $b_N \neq 0$. Consider the coefficient of t^{pN} in (3.22). Observe that $x = t^p + O(t^{p+1})$, since $v_P(x) = p$. We see that either $pN \geq a$ (which is impossible, since $\sum_{i \in J} a_i t^i \notin I$) or $0 = b_N + 0$, which also leads to a contradiction. This ends the proof.

(3) Follows immediately from (2).

(4) Note that

$$\begin{aligned} x &= \frac{1}{(t^{-np} - t^{-n})^{1/n}} = \frac{t^p}{(1 - t^{n \cdot (p-1)})^{1/n}} \\ &= t^p \cdot (1 + O(t^{n \cdot (p-1)})) \end{aligned}$$

and thus for any $a - n \leq i \leq a - 1$, $p | i$:

$$x^{i/p} = t^i \cdot (1 + O(t^{n \cdot (p-1)})) = t^i + O(t^a)$$

and $[t^i]_{L/I} = [x^{i/p}]_{L/I}$, which shows that $[t^i]_M = 0$. □

Proposition 3.3.6. *Keep the Setup 3.0.1 and suppose that $G \cong \mathbb{Z}/p$. Then for any $Q \in Y$ the dimension of*

$$\operatorname{im}\left(H^1(G, (\pi_* \mathcal{O}_X)_Q) \to H^1(G, (\pi_* \Omega_{X/k})_Q)\right)$$

equals

$$\left[\frac{(n_Q + 1) \cdot (p-1)}{p}\right] - 1 - \left[\frac{n_Q - 1}{p}\right].$$

Proof. Fix a point $Q \in \mathcal{P}$ and keep the above notation. Note that $\widehat{(\pi_* \mathcal{O}_X)_Q} \cong B$, $\widehat{\pi_* \Omega_{X/k}} = B\,dt$. Moreover, note that $\frac{dt}{t^{n+1}}$ is a G-invariant form, since from the equation $t^{-np} - t^{-n} = x^{-n}$ one obtains:

$$\frac{dt}{t^{n+1}} = -\frac{dx}{x^{n+1}}.$$

Thus we have the following isomorphism of $B[G]$-modules:

$$\begin{array}{rcl} B\,dt & \longrightarrow & t^{n+1}B \\ h(t)\,dt = t^{n+1}h(t)\cdot\dfrac{dt}{t^{n+1}} & \longmapsto & t^{n+1}h(t) \end{array}$$

(cf. [Kon07, proof of Lemma 1.11.] for the "dual" version of this isomorphism). Lemma 3.3.5 implies that $H^1(G,B)$ and $H^1(G,B\,dt)$ may be identified with

$$M_1 := \operatorname{coker}(L^G \to (L/B)^G) \quad \text{and} \quad M_2 := \operatorname{coker}((L\,dt)^G \to (L\,dt/B\,dt)^G),$$

respectively. One easily checks that the morphism $d : H^1(G,B) \to H^1(G,B\,dt)$ corresponds to

$$d : M_1 \to M_2, \quad d([h(t)]_{M_1}) = [dh(t)]_{M_2} = [h'(t)\,dt]_{M_2}.$$

By using Lemma 3.3.5 (2), (4) for $a = 0$ and $a = n+1$ we see that the basis of $\operatorname{im}(d : M_1 \to M_2)$ is

$$[dt^i]_{M_2} = [it^{i-1}\,dt]_{M_2} \quad \text{for } i = -n, -n+1, \dots, -1, \quad p \nmid i, \quad i+n \not\equiv 0 \pmod{p}.$$

An elementary calculation allows one to compute the dimension of this space. □

Corollary 3.3.7. *Suppose that X is a smooth projective curve over an algebraically closed field k of characteristic $p > 0$ with an action of the group $G = \mathbb{Z}/p$. Then:*

$$\delta(X,G) = \sum_{P\in X}\left(\left[\frac{(p-1)\cdot(n_P+1)}{p}\right] - 1 - \left[\frac{n_P-1}{p}\right]\right).$$

Proof. Corollary 3.3.7 follows immediately by combining Propositions 3.2.1 and 3.3.6. □

3.4. Equivariant splitting of the Hodge–de Rham exact sequence

Let X be a smooth algebraic variety over k equipped with an action of a finite group G. We say that the pair (X,G) lifts to $W_2(k)$, if there exists a smooth scheme $\widetilde{X}$ over $W_2(k)$ and a homomorphism $G \to \operatorname{Aut}_{W_2(k)}(\widetilde{X})$ such that

$$(\widetilde{X}, G \to \operatorname{Aut}_{W_2(k)}(\widetilde{X})) \times_{W_2(k)} k = (X, G \to \operatorname{Aut}_k(X)).$$

The following proposition is a G-equivariant version of Theorem 1.3.1 and follows easily from the functoriality of the result of Deligne and Illusie.

Theorem 3.4.1. *Suppose that the pair (X,G) lifts to $W_2(k)$ and that $\dim X < p$. Then the exact sequence (3.2) of $k[G]$-modules splits.*

Proof. Since $\dim X < p$, we can apply Theorem 1.3.1 to obtain the isomorphism:

$$\varphi^{\bullet}_{\widetilde{X}} : \bigoplus_i \Omega^i_{X'/k}[-i] \to F_*\Omega^{\bullet}_{X/k}. \tag{3.23}$$

By tracing through the proof of [DI87, Théoréme 2.1], one sees that $\varphi^0_{\widetilde{X}}$, the zeroth component of $\varphi^{\bullet}_{\widetilde{X}}$, is the composition of maps:

$$\mathcal{O}_{X'}[0] \overset{C^{-1}}{\to} h^0(F_*\,\Omega^{\bullet}_{X/k})[0] \hookrightarrow F_*\,\Omega^{\bullet}_{X/k}.$$

Thus, by applying the first cohomology to (3.23) we obtain an isomorphism:

$$\phi_{\widetilde{X}} : H^0(X', \Omega^1_{X'/k}) \oplus H^1(X', \mathcal{O}_{X'}) \to H^1(X', F_* \Omega^\bullet_{X/k}) \cong H^1(X, \Omega^\bullet_{X/k}) \tag{3.24}$$

which yields a splitting of (3.2). Now, observe that $\varphi_{\widetilde{X}}$ and $\phi_{\widetilde{X}}$ are functorial with respect to $\widetilde{X}$. Thus, if (X, G) lifts to $W_2(k)$, (3.24) becomes an isomorphism of $k[G]$-modules. □

Remark 3.4.2. *If G is a cyclic p-group and V is a $k[G]$-module with $\dim_k V < \infty$, one may easily prove that $V \cong V'$ as $k[G]$-modules.*

The following important question remains open.

Question 3.4.3. *Suppose that the pair (X, G) lifts to $W_2(k)$. Does it follow that the exact sequence of $k[G]$-modules* (3.1) *splits?*

Corollary 3.4.4. *Suppose that a finite group G acts on an ordinary curve X. Then the exact sequences* (3.1) *and* (3.2) *split G-equivariantly and*

$$H^0(X, \Omega_{X/k})' \cong H^0(X, \Omega_{X/k}), \quad H^1(X, \mathcal{O}_X)' \cong H^1(X, \mathcal{O}_X).$$

as $k[G]$-modules.

Proof. Let A be the Jacobian variety of X. Observe that the Abel-Jacobi map induces an isomorphism between the Hodge-de Rham sequences of X and A (cf. [Mil08, Proposition III.2.1, Lemma III.9.5.]). The same applies to the conjugate Hodge-de Rham sequence. Moreover, A is ordinary, and thus the natural inclusions:

$$H^0(A, \Omega_{A/k}) \to H^1_{dR}(A/k), \quad H^1(A, \mathcal{O}_A)' \to H^1_{dR}(A/k)$$

induce an isomorphism $H^1_{dR}(A/k) \cong H^0(A, \Omega_{A/k}) \oplus H^1(A, \mathcal{O}_A)'$ (cf. [Wed08, §2.1]). This isomorphism is clearly functorial and thus is an isomorphism of $k[G]$-modules. The remaining statement is clear. □

Let X be a curve. Following [Köc04], we say that the action of G on X is **weakly ramified** if $n_P \in \{0, 1\}$ for every $P \in X$.

Theorem 3.4.5. *Keep the Setup 3.0.1. If $p > 2$ and either of the sequences* (3.1) *and* (3.2) *splits G-equivariantly, then the action of G on X is weakly ramified.*

Proof. We start by proving the result for the exact sequence (3.1). We consider first the case $G = \mathbb{Z}/p$. An easy computation shows that for any $n \geq 1$, $p \geq 3$ one has:

$$\left[\frac{(p-1)\cdot(n+1)}{p}\right] \geq 1 + \left[\frac{n-1}{p}\right]$$

with an equality only for $n = 1$ (here is where we use the assumption $p > 2$). Thus by Corollary 3.3.7, $\delta(X, G) = 0$ holds if and only if π is weakly ramified.

Suppose now that G is arbitrary and $G_{P,2} \neq 0$ for some $P \in X$. Note that $G_{P,2}$ is a finite p-group (cf. [Ser79, Corollary 4.2.3., p. 67]) and thus contains a subgroup H of order p. Observe that $\pi : X \to X/H$ is an Artin-Schreier covering and it is not weakly ramified, since $H_{P,2} = H \neq 0$. Therefore by the first paragraph of the proof, the sequence (3.1) does not split H-equivariantly and therefore it cannot split as a sequence of $k[G]$-modules.

Note that for a $k[G]$-module V of finite k-dimension, $\dim V^G = \dim(V')^G$. Thus for the sequence (3.2) the proof is analogous. □

The example below is a direct generalization of results proven in [KT18].

Example 3.4.6. *Let X be the curve considered in Example 3.3.2. If the Hodge–de Rham exact sequence of X splits G-equivariantly, then by Theorem 3.4.5 and the formula* (3.20) *we have either $p = 2$, or $m|\deg f$.*

We give now some applications of Theorem 3.4.5. The following is an immediate consequence of Theorem 3.4.5 and Theorem 3.4.1.

Corollary 3.4.7. *Suppose that $p > 2$, X is a smooth projective curve over k and the pair (X, G) lifts to $W_2(k)$. Then the action of G on X is weakly ramified.*

Note that it was known previously that non-weakly ramified actions on curves do not lift to $W(k)$ (cf. [Nak86, Corollary, Sec. 4]). Observe also that Corollary 3.4.4 and Theorem 3.4.5 imply that ordinary curves admit only weakly ramified group actions. This follows also from the Deuring-Shafarevich formula (cf. [Sub75]). We will show now that the Jacobian of a curve with a non-weakly ramified group action has no "canonical lifting".

Corollary 3.4.8. *In the above notation, suppose that the action of G on X is non-weakly ramified. Then the Hodge–de Rham exact sequence of $A := \mathrm{Jac}(X)$ does not split G-equivariantly. In particular, A has no lifting $\boldsymbol{A}$ to $W_2(k)$ such that the natural map:*

$$\mathrm{End}_{W_2(k)}(\boldsymbol{A}) \to \mathrm{End}_k(A)$$

is an isomorphism.

Proof. To prove the first statement, it suffices to note that the Abel-Jacobi map induces an isomorphism between the Hodge-de Rham sequences of a curve and its Jacobian variety (cf. [Mil08, Proposition III.2.1, Lemma III.9.5.]). The second statement follows from Theorem 3.4.1. □

3.5. The G-fixed subspaces

This section will be devoted to proving a partial converse statement to Theorem 3.4.5.

The methods used to prove Theorem 3.4.5 seem to be insufficient to obtain a positive result regarding splitting of the exact sequence (3.1). However, we may say something about the G-fixed subspaces of the vector spaces in the sequence (3.1).

Theorem 3.5.1. *Keep the Setup 3.0.1. If the action of G is weakly ramified then the sequence*

$$0 \to H^0(X, \Omega_{X/k})^G \to H^1_{dR}(X/k)^G \to H^1(X, \mathcal{O}_X)^G \to 0$$

is exact also on the right.

Proof. By Proposition 3.2.1 it is sufficient to show that the map

$$H^1(G, (\pi_* \mathcal{O}_X)_{\pi(P)}) \to H^1(G, (\pi_* \Omega_{X/k})_{\pi(P)})$$

is zero for every $P \in X$. Just as in the proof of Proposition 3.7.1 we observe that

$$H^1(G, (\pi_* \mathcal{O}_X)_{\pi(P)}) \cong H^1(G_{P,0}, k) \oplus H^1(G_P, \mathfrak{m}_{X,P}).$$

However, the map $d : k \to \Omega_{X/k}$ is zero and thus the induced map

$$d : H^1(G_{P,0}, k) \to H^1(G, (\pi_* \Omega_{X/k})_{\pi(P)})$$

is also zero. Moreover, since π is weakly ramified, by a result of Köck (cf. [Köc04, Theorem 1.1]), $H^1(G_{P,0}, \mathfrak{m}_{X,P}) = 0$. This ends the proof. □

Note that if an action of a finite group G on X is weakly ramified then the action of any subgroup of G on X is also weakly ramified. Therefore the condition imposed by Theorem 3.5.1 on the Hodge–de Rham exact sequence of X seems to be strong from the group theoretical point of view. This raises the following question:

Question 3.5.2. *Suppose that k is a field of characteristic $p > 0$ and G is a finite group. Let*

$$0 \to A \to B \to C \to 0 \tag{3.25}$$

be an exact sequence of $k[G]$-modules of finite dimension over k. Assume that for every subgroup $H \leq G$ the sequence

$$0 \to A^H \to B^H \to C^H \to 0$$

is exact. Does it follow that the exact sequence (3.25) *splits G-equivariantly?*

We will show in the next subsection that the answer to the Question 3.5.2 is negative for $\operatorname{char} k = 2$. The following lemma reduces the Question 3.5.2 to the case of p-groups.

Lemma 3.5.3. *Let k be a field of characteristic $p > 0$ and let G be a finite group with a p-Sylow subgroup P. Suppose that*

$$0 \to A \to B \to C \to 0 \tag{3.26}$$

is an exact sequence of $k[G]$-modules. Then (3.26) *splits as an exact sequence of $k[G]$-modules if and only if it splits as an exact sequence of $k[P]$-modules.*

Proof. The proof is adapted from the proof of Maschke's theorem. Suppose that $s : C \to B$ is a $k[P]$-equivariant section of the map $B \to C$. Let $P \setminus G = \{Pg_1, \ldots, Pg_m\}$, where $p \nmid m = [G : P]$. Then, as one easily checks

$$\widetilde{s} : C \to B, \quad \widetilde{s}(x) := \frac{1}{m} \sum_{i=1}^{m} g_i^{-1} s(g_i x)$$

is a $k[G]$-equivariant section of $B \to C$. □

Unfortunately we are able to answer Question 3.5.2 only for the class of groups that have 'tame' modular representation theory, i.e. for groups with a cyclic p-Sylow subgroup.

Lemma 3.5.4. *Suppose that k is a field of characteristic $p > 0$ and G is a finite group with a cyclic p-Sylow subgroup. Let*

$$0 \to A \to B \to C \to 0 \tag{3.27}$$

be an exact sequence of $k[G]$-modules. If the sequence

$$0 \to A^G \to B^G \to C^G \to 0$$

is exact on the right, then the exact sequence (3.27) *splits G-equivariantly.*

Proof. Without loss of generality we can assume that $G = \mathbb{Z}/p^n$ is a cyclic p-group (by Lemma 3.5.3). Note that $k[\mathbb{Z}/p^n] \cong k[x]/(x-1)^{p^n}$. The classification theorem of finitely generated modules over the principal ideal domain $k[x]$ (cf. [DF04, Theorem 12.1.5]) implies that every finitely generated indecomposable $k[\mathbb{Z}/p^n]$-module is of the form:

$$J_i = k[x]/(x-1)^i \qquad \text{for some } i = 1, \ldots, p^n.$$

Let also J_0 denote the zero module. Using the Smith's normal form theorem (cf. [DF04, Theorem 12.1.4]) we obtain a commutative diagram:

$$\begin{array}{ccc} A & \hookrightarrow & B \\ \cong\downarrow & & \cong\downarrow \\ \bigoplus_{i=1}^{l} J_{a_i} & \hookrightarrow & \bigoplus_{i=1}^{m} J_{b_i}, \end{array}$$

where $l \leq m$, $a_i \leq b_i$ and $J_{a_i} \hookrightarrow J_{b_i}$ is the natural inclusion. Hence, we are reduced to proving the claim for the exact sequence:

$$0 \to J_a \to J_b \to J_c \to 0,$$

where $a + b = c$, $0 \leq a, b, c \leq p^n$. However, the equality

$$\dim_k J_s^G = \begin{cases} 1, & \text{if } s \neq 0, \\ 0, & \text{otherwise} \end{cases}$$

makes it obvious that $a = 0$ or $c = 0$. This finishes the proof.

□

3.6. A counterexample

In this section we give an example of an elliptic curve over a field of characteristic 2 with a weakly ramified group action, for which the sequence (3.1) does not split equivariantly. It remains unclear whether similar counterexamples will arise over fields of odd characteristic.

Consider an elliptic curve X over the field $k := \overline{\mathbb{F}}_2$ with the affine part U_0 given by the equation:

$$y^2 + y = x^3.$$

Note that $X \setminus U_0 = \{\mathcal{O}\}$, where $\mathcal{O}$ is the point at infinity. The group G of automorphisms of X that fix $\mathcal{O}$ is of order 24 and is isomorphic to $\mathrm{Sl}_2(\mathbb{F}_3)$. In particular its 2-Sylow subgroup is isomorphic to the quaternion group Q_8. This group action may be given explicitly, cf. [Sil09, Appendix A] or [KST17, Section 3]. Let:

$$A := \{(u, r, t) : u \in \mathbb{F}_4^\times, \quad t \in \mathbb{F}_4, \quad t^2 + t + r^3 = 0\}.$$

Define for any $(u, r, t) \in A$ an automorphism $g_{u,r,t} \in \mathrm{Aut}(X)$ by:

$$g_{u,r,t} \cdot (x, y) := (u^2 x + r, y + u^2 r^2 x + t).$$

We will compute $H^1_{dR}(X/k)$ using Čech cohomology. Recall that if a curve X may be covered by affine subsets U_0, U_∞, then:

$$H^1_{dR}(X/k) \quad \cong \quad \frac{\{(\omega_0, \omega_\infty, f_{0\infty}) : df_{0\infty} = \omega_0 - \omega_\infty\}}{\{(df_0, df_\infty, f_0 - f_\infty) : f_i \in \mathcal{O}_X(U_i)\}},$$

where we take $\omega_i \in \Omega_X(U_i)$ for $i = 0, \infty$ and $f_{0\infty} \in \mathcal{O}_X(U_0 \cap U_\infty)$. In our case, we may take U_0 as above and $U_\infty = X \cap \{x \neq 0\}$. Then, by [KT18, Theorem 2.2.], one sees that $H^1_{dR}(X/k)$ is a k-vector space of dimension 2, generated by $v_1 := [(dx, dx, 0)]$ and $v_2 := [(x\,dx, \frac{y\,dx}{x^2}, \frac{y}{x})]$.

Lemma 3.6.1. *In the above situation:*

(1) $H^1_{dR}(X/k)$ is an indecomposable $k[G]$-module,

(2) the action of G on X is weakly ramified.

Proof. (1) Suppose that V is a G-invariant proper subspace of $H^1_{dR}(X/k)$. We will show that $V = \mathrm{Span}_k(v_1)$. Indeed, otherwise we would have $V = \mathrm{Span}_k(v)$ for some $v = \alpha \cdot v_1 + v_2$ and $\alpha \in k$. Note that for $g = g_{u,r,t}$:

$$\begin{aligned} gv_1 &= u^2 v_1 \\ gv_2 &= u^2 t v_1 + u v_2. \end{aligned}$$

Thus:

$$g \cdot v = (\alpha \cdot u^2 + u^2 \cdot t) \cdot v_1 + u v_2.$$

Therefore $g \cdot v \in V$ if and only if $\alpha \cdot u^2 + u^2 \cdot t = u\alpha$, which leads to the equation:

$$(1 - u) \cdot \alpha = ut.$$

The last equality is however impossible to hold for all $(u, r, t) \in A$ and a fixed $\alpha \in k$. Indeed, one can take e.g. $(u, r, t) = (1, 0, 1), (1, 1, \zeta)$ for any $\zeta \in \mathbb{F}_4 \setminus \mathbb{F}_2$ to obtain a desired contradition.

(2) One easily sees that if $gP = P$ and $g \neq \mathrm{id}$ then $P = \mathcal{O}$. Thus we are left with showing that $G_{\mathcal{O},2} = 0$. Observe that $\mathrm{ord}_{\mathcal{O}}(x) = -2$ and $\mathrm{ord}_{\mathcal{O}}(y) = -3$. Hence the function $t := \frac{x}{y}$ is the uniformizer at $\mathcal{O}$. For $g = g_{u,r,t}$ one has:

$$g(t) - t = \frac{(u^2 + 1) \cdot xy + u^2 r^2 \cdot x^2 + r \cdot y + t \cdot x}{y \cdot (y + u^2 r^2 x + t)}$$

and

$$\mathrm{ord}_{\mathcal{O}}(g(t) - t) = \begin{cases} 2, & \text{if } u = 1, \\ 1, & \text{if } u \neq 1. \end{cases}$$

Therefore $G_{\mathcal{O},2} = 0$ and

$$G_{\mathcal{O},1} = \{g_{1,r,s} : (1, r, s) \in A\} \cong Q_8.$$

□

3.7. Computing the dimension of $H^1(X, \mathcal{O}_X)^G$

For completeness we include also the following proposition, which allows in many situations to compute dimensions of $H^0(X, \Omega_{X/k})^G$, $H^1(X, \mathcal{O}_X)^G$ and $H^1_{dR}(X/k)^G$ in terms of invariants of Y and group cohomology of sheaves. Note that by Corollary 3.1.4 and Proposition 3.2.1 we are left with computing the dimension of $H^1(X, \mathcal{O}_X)^G$.

Proposition 3.7.1. *Keep the Setup 3.0.1, in particular G acts on X and $\pi : X \to Y$ is the quotient map. Suppose that there exists $Q_0 \in Y$ such that $p \nmid \#\pi^{-1}(Q_0)$. Then:*

$$\begin{aligned} \dim_k H^1(X, \mathcal{O}_X)^G &= g_Y + \sum_{Q \in Y} H^1(G, (\pi_* \mathcal{O}_X)_Q) \\ &- \dim_k H^1(G, k). \end{aligned}$$

Proof. By substituting $\mathcal{F}^0 = \pi_*\mathcal{O}_X$ in the formula (3.14) and using Lemma 3.2.4 and Corollary 3.2.5 it suffices to prove that the natural map

$$H^2(G,k) \cong H^2(G, H^0(Y, \pi_*\mathcal{O}_X)) \to H^0(Y, \mathcal{H}^2(G, \pi_*\mathcal{O}_X)) \tag{3.28}$$

is injective. One easily sees that

$$\mathcal{H}^2(G, \pi_*\mathcal{O}_X) \;\cong\; \bigoplus_{Q\in Y} (i_Q)_*\Big(H^2(G, (\pi_*\mathcal{O}_X)_Q)\Big)$$

is a direct sum of skyscraper sheaves. Choose any $P_0 \in \pi^{-1}(Q_0)$. Observe that by Lemma 3.1.2 we have:

$$H^2(G, (\pi_*\mathcal{O}_X)_Q) \cong H^2(G_{P_0,1}, \mathcal{O}_{X,P_0}).$$

But $\mathcal{O}_{X,P_0} \cong k \oplus \mathfrak{m}_{X,P_0}$ as a $k[G_{P_0,1}]$-module and therefore

$$H^2(G_{P_0,1}, \mathcal{O}_{X,P_0}) \cong H^2(G_{P_0,1}, k) \oplus H^2(G_{P_0,1}, \mathfrak{m}_{X,P_0}).$$

One easily sees that the map (3.28) factors as

$$H^2(G,k) \to H^2(G_{P_0,1}, k) \hookrightarrow H^2(G_{P_0,1}, k) \oplus H^2(G_{P_0,1}, \mathfrak{m}_{X,P_0}),$$

where the first map is the restriction $\mathrm{res}^G_{G_{P_0,1}}$. Note that $p \nmid \#\pi^{-1}(Q_0) = [G : G_{P_0}]$ and thus $G_{P_0,1}$ is a p-Sylow subgroup of G by [Ser79, Corollary 4.2.3., p. 67]. Thus by (1.17) $\mathrm{res}^G_{G_{P_0,1}}$ is an isomorphism. This ends the proof. □

Example 3.7.2. *Keep the Setup 3.0.1 and suppose that $G \cong \mathbb{Z}/p$. Then by Lemma 3.3.1, one has $d_Q = (n_Q+1)\cdot p$ for all $Q \in Y$ and therefore:*

$$R' = \sum_{Q\in Y} \left[\frac{(n_Q+1)\cdot(p-1)}{p}\right](Q). \tag{3.29}$$

Moreover, by Lemma 3.3.5:

$$\dim_k H^1(G, (\pi_*\mathcal{O}_X)_Q) = \left[\frac{(n_Q+1)\cdot(p-1)}{p}\right].$$

Suppose that the action of G on X is not free. Then by Corollary 3.1.4, Proposition 3.7.1 and (3.29) we obtain:

$$\begin{aligned}\dim_k H^0(X, \Omega_{X/k})^G &= \dim_k H^1(X, \mathcal{O}_X)^G \\ &= g_Y - 1 + \sum_{Q\in Y}\left[\frac{(n_Q+1)\cdot(p-1)}{p}\right].\end{aligned}$$

Moreover, by previous computations and by Proposition 3.2.1 we obtain:

$$\begin{aligned}\dim_k H^1_{dR}(X/k)^G &= 2(g_Y-1) \\ &+ \sum_{Q\in Y}\left(\left[\frac{(n_Q+1)\cdot(p-1)}{p}\right] + 1 + \left[\frac{n_Q-1}{p}\right]\right).\end{aligned}$$

If the action of G is free, then a similar reasoning leads to the formulas:

$$\begin{aligned}\dim_k H^0(X, \Omega_{X/k})^G &= \dim_k H^1(X, \mathcal{O}_X)^G = g_Y, \\ \dim_k H^1_{dR}(X/k)^G &= 2g_Y.\end{aligned}$$

4

Class numbers of division fields

Let A be an abelian variety of dimension g over a number field K. Fix a rational prime p. Denote by $K_n := K(A[p^n])$ the p^n-th division field of A. We define the number k_n by the equality:

$$\#\operatorname{Cl}(K_n)[p^\infty] = p^{k_n}.$$

The goal of this chapter is to prove a lower bound for k_n. In order to achieve this, we use Kummer theory of abelian varieties to produce large unramified abelian extensions of abelian varieties. In order to bound inertia groups in the Kummer extension we will base change a given abelian variety to a p-adic field and then use methods such as the theory of Néron models and classification theorem for compact p-adic Lie groups. This chapter is based on the article [Gar19b].

Setup 4.0.1. Keep the above setting. Denote by r the rank of $A(K)$ over $\operatorname{End}_K(A)$. Let L_n be the Kummer extension of K_n, κ_n be the Kummer pairing and $\Gamma^{(n)}$ be the Kummer map, as defined in Subsection 1.2.6. Let $I(\mathcal{P})$ denote the inertia group of the extension L_n/K_n at a prime $\mathcal{P} \in \operatorname{Spec}(\mathcal{O}_{L_n})$. Let us fix $\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_K)$. We introduce the following notation:

- $\mathbb{F}_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$ – a finite field of characteristic ℓ (in the sequel we will consider two separate cases: $\ell \neq p$ and $\ell = p$),
- $\widehat{K}_\mathfrak{p}$ – completion of K at $\mathfrak{p}$ with the ring of integers $\mathcal{O}_{\widehat{K}_\mathfrak{p}}$,
- $I_\mathfrak{p}^{(n)} := \langle \bigcup_\mathcal{P} I(\mathcal{P}) \rangle$ – the subgroup of $\operatorname{Gal}(L_n/K_n)$ generated by the inertia groups of all primes $\mathcal{P}$ of L_n over $\mathfrak{p}$,
- $\mathcal{A}$ – the Néron model of A over $\widehat{K}_\mathfrak{p}$ with the special fiber $A_\mathfrak{p}$, the connected component of the identity $A_\mathfrak{p}^0$ and the group of geometric components $\Phi_{A_\mathfrak{p}}$ (cf. Subsections 1.2.4 and 1.1.4 for the relevant definitions),
- $p^{\alpha_\mathfrak{p}}$ – the exponent of the group $\Phi_{A_\mathfrak{p}}(\overline{\mathbb{F}}_\mathfrak{p})[p^\infty]$,
- $p^{\beta_\mathfrak{p}}$ – the exponent of the group $A(\widehat{K}_\mathfrak{p})[p^\infty]$,
- $h_\mathfrak{p} := 2g - r(A_\mathfrak{p})$, if A has good reduction at $\mathfrak{p}$ (where $r(A_\mathfrak{p})$ is defined by (1.6)) and $h_\mathfrak{p} := 2g$, if A has bad reduction at $\mathfrak{p}$,
- m_p is defined by the condition (1.10).

Note that $\alpha_{\mathfrak{p}} = 0$ whenever A has good reduction at $\mathfrak{p}$. Also, $\beta_{\mathfrak{p}}$ is finite, since $A(\widehat{K}_{\mathfrak{p}})$ contains a subgroup of finite index isomorphic to $\mathcal{O}_{\widehat{K}_{\mathfrak{p}}}^d$, cf. Theorem 1.2.3. However, it is unknown whether $\beta_{\mathfrak{p}} = 0$ holds for almost all p, even in the case of elliptic curves over $\mathbb{Q}$, cf. Conjecture 2.3.1.

Finally, define $I^{(n)}$ to be the subgroup of $\mathrm{Gal}(L_n/K_n)$, generated by all the subgroups $I_{\mathfrak{p}}^{(n)}$:

$$I^{(n)} := \left\langle \bigcup_{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)} I_{\mathfrak{p}}^{(n)} \right\rangle.$$

4.1. Proof of the bounds

In this Section we prove a lower bound for k_n, assuming some bounds on inertia groups, which will be proven later. The main idea behind the proof is to control the ramification in L_n/K_n. A standard argument used in the proof of the weak Mordell-Weil theorem shows that the only possible ramified primes of L_n/K_n, are the primes lying over primes of bad reduction for A or primes over p (see e.g. [HS00, Proposition C.1.5]). We need to bound the inertia group for those primes. We will estimate the order of interia groups $I_{\mathfrak{p}}^{(n)}$ separately for $\mathfrak{p} \nmid p$ and for $\mathfrak{p}|p$. In order to do this, we will work in the local setting. Keep the Setup 4.0.1. We have the following proposition:

Proposition 4.1.1. *If $\mathfrak{p} \nmid p$, then:*

$$\#I_{\mathfrak{p}}^{(n)} \leq p^{2gr \min\{\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}}\}}.$$

Note that in particular this bound is independent of n and that it equals 1 for primes $\mathfrak{p}$ of good reduction for A. Proposition 4.1.1 will be proven in Section 4.2. In Section 4.3 we will estimate the order of $I_{\mathfrak{p}}^{(n)}$ for $\mathfrak{p}|p$ and will prove the following result.

Proposition 4.1.2. *If $\mathfrak{p}|p$, then:*

$$\#I_{\mathfrak{p}}^{(n)} \leq p^{h_{\mathfrak{p}} \cdot \min\{d \cdot [\widehat{K}_{\mathfrak{p}} : \mathbb{Q}_p], r\} \cdot n + r h_{\mathfrak{p}} \beta_{\mathfrak{p}}}.$$

Before the proof of the bound on k_n we need one more lemma:

Lemma 4.1.3. *The field K_n has no real embeddings for $(p, n) \neq (2, 1)$.*

Proof. Suppose to the contrary that $\sigma : K_n \hookrightarrow \mathbb{R}$ is a real place of K_n. Then one may view A as an abelian variety over the field $\mathbb{R}$, satisfying $A(\mathbb{R})[p^n] = (\mathbb{Z}/p^n)^{2g}$. On the other hand, we have by Proposition 1.2.2:

$$A(\mathbb{R}) \cong (\mathbb{S}^1)^g \times (\mathbb{Z}/2)^t$$

for some integer $0 \leq t \leq g$. Thus:

$$A(\mathbb{R})[p^n] \cong (\mathbb{Z}/p^n)^g \times (\mathbb{Z}/2)^t[p^n],$$

which leads to a contradiction for $(p, n) \neq (2, 1)$. □

The result proved below may be considered as the main theorem of this chapter.

Theorem 4.1.4. *Let A/K be an abelian variety of dimension g. Denote by r the maximal possible number of $\mathrm{End}_K(A)$-independent points of $A(K)$. Then:*

$$k_n \geq \left(2rg - \sum_{\mathfrak{p}|p} h_{\mathfrak{p}} \cdot \min\left\{ [\widehat{K}_{\mathfrak{p}} : \mathbb{Q}_p] \cdot g, r \right\} \right) \cdot n - C,$$

where the constant C depends on K, A and p.

Proof. Let $\widetilde{L_n}$ be the maximal unramified extension of K_n inside L_n. Then it must be a subfield of the Hilbert class field of K_n. The degree of the Hilbert class field of K_n is $\#\,\mathrm{Cl}(K_n)$ and thus:

$$[\widetilde{L_n} : K_n] \text{ divides } \#\,\mathrm{Cl}(K_n). \tag{4.1}$$

Note that by Propositions 4.1.1 and 4.1.2:

$$\begin{aligned} \#I^{(n)} &\leq \prod_{\mathfrak{p}} \#I_{\mathfrak{p}}^{(n)} = \prod_{\mathfrak{p}|p} \#I_{\mathfrak{p}}^{(n)} \cdot \prod_{\mathfrak{p}\nmid p} \#I_{\mathfrak{p}}^{(n)} \leq \\ &\leq p^{\sum_{\mathfrak{p}|p}(h_{\mathfrak{p}} \min\{g\cdot[\widehat{K}_{\mathfrak{p}}:\mathbb{Q}_p], r\}\cdot n + r h_{\mathfrak{p}} \beta_{\mathfrak{p}}) + 2gr \cdot \sum_{\mathfrak{p}\nmid p} \min\{\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}}\}}. \end{aligned} \tag{4.2}$$

By Lemma 4.1.3 K_n has no real places and thus any extension of K_n is unramified at infinite places. Therefore $\widetilde{L_n} = (L_n)^{I^{(n)}}$, which yields (using Corollary 1.2.17):

$$\begin{aligned} [\widetilde{L_n} : K_n] &= [L_n : K_n]/\#I^{(n)} \geq p^{2gnr - m_p}/\#I^{(n)} \\ &\overset{(4.2)}{\geq} p^{\left(2gr - \sum_{\mathfrak{p}|p} h_{\mathfrak{p}} \min\{g\cdot[\widehat{K}_{\mathfrak{p}}:\mathbb{Q}_p], r\}\right)\cdot n - C}, \end{aligned} \tag{4.3}$$

where for $(p, n) \neq (2, 1)$ one can take:

$$C := 2gr \sum_{\mathfrak{p}\nmid p} \min\{\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}}\} + r \sum_{\mathfrak{p}|p} h_{\mathfrak{p}} \beta_{\mathfrak{p}} + m_p. \tag{4.4}$$

The proof follows by combining (4.1), (4.3) and noting that $[\widetilde{L}_n : K_n]$ must be a power of p, since $[L_n : K_n]$ is a power of p. □

Corollary 4.1.5. *Let $A/\mathbb{Q}$ be an abelian variety of dimension g. If either of the following condition holds:*

- *$r \geq 1$, A has good reduction at p and $r(A_{\mathfrak{p}}) > 0$,*
- *$r > g$,*

then:

$$\lim_{n\to\infty} \#\,\mathrm{Cl}(K_n) = \infty.$$

Proof. By Theorem 4.1.4:

$$k_n \geq (2rg - h_p \min\{g, r\}) \cdot n.$$

If any of the above conditions holds then the right-hand side tends to infinity. □

4.2. Inertia groups over $\ell \neq p$

In this section we estimate the order of the inertia group $I_{\mathfrak{p}}^{(n)}$ for a prime $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$, $\mathfrak{p} \nmid p$. We use the Setup 4.0.1.

Proposition 4.2.1. *If $\mathfrak{p} \nmid p$, then*

$$\#I_{\mathfrak{p}}^{(n)} \leq p^{2gr\beta_{\mathfrak{p}}}.$$

Proof. Let us fix a point $P \in A(\widehat{K}_{\mathfrak{p}})$. Recall that ℓ is the rational prime below $\mathfrak{p}$. By the classification theorem of compact ℓ-adic Lie groups (cf. Theorem 1.2.3):

$$A(\widehat{K}_{\mathfrak{p}}) \cong \mathcal{O}_{\widehat{K}_{\mathfrak{p}}}^{g} \times A(\widehat{K}_{\mathfrak{p}})_{tors} \cong \mathbb{Z}_{\ell}^{g\cdot[\widehat{K}_{\mathfrak{p}}:\mathbb{Q}_{\ell}]} \times A(\widehat{K}_{\mathfrak{p}})_{tors}$$

as topological groups. Note that multiplication by p is an isomorphism on $\mathbb{Z}_{\ell}$. Therefore and by the definition of $\beta_{\mathfrak{p}}$:

$$p^{\beta_{\mathfrak{p}}} A(\widehat{K}_{\mathfrak{p}}) \cong \mathbb{Z}_{\ell}^{g\cdot[\widehat{K}_{\mathfrak{p}}:\mathbb{Q}_{\ell}]} \times T,$$

where T is a finite group satisfying $p \nmid \#T$. This implies that multiplication by p on $p^{\beta_{\mathfrak{p}}} A(\widehat{K}_{\mathfrak{p}})$ is an isomorphism and

$$p^{\beta_{\mathfrak{p}}} P = p^n R$$

for some $R \in A(\widehat{K}_{\mathfrak{p}})$. Thus for the Kummer map κ_n:

$$\begin{aligned} p^{\beta_{\mathfrak{p}}} \kappa_n(P,\sigma) = \kappa_n(p^{\beta_{\mathfrak{p}}} P, \sigma) = \kappa_n(p^n R, \sigma) = \\ = R^{\sigma} - R = 0 \end{aligned}$$

for any $\sigma \in I_{\mathfrak{p}}$. In particular, taking $P = P_i$ for $i = 1, \ldots, r$ we obtain:

$$\Gamma^{(n)}(I_{\mathfrak{p}}^{(n)}) \subset A[p^{\beta_{\mathfrak{p}}}]^{\oplus r}.$$

This ends the proof, since $\Gamma^{(n)}$ is injective. □

We now move on to prove the second estimate on the order of $I_{\mathfrak{p}}^{(n)}$. Let $\widehat{K}_{\mathfrak{p}}^{ur}$ be the maximal unramified extension of $\widehat{K}_{\mathfrak{p}}$ inside $\overline{\mathbb{Q}}_{\ell}$. We denote its ring of integers by $\mathcal{O}^{ur}$ and the maximal ideal of $\mathcal{O}^{ur}$ by $\mathfrak{m}^{ur}$. Recall that the reduction morphism extends to $\widehat{K}_{\mathfrak{p}}^{ur}$ (cf. Remark 1.2.14).

Proposition 4.2.2. *If $\mathfrak{p} \nmid p$ then*

$$\#I_{\mathfrak{p}}^{(n)} \leq p^{2gr\alpha_{\mathfrak{p}}}.$$

Proof. Consider $\mathcal{A}$ as the Néron model for A over $\mathcal{O}^{ur}$. Let $\alpha := \alpha_{\mathfrak{p}}$ and

$$c := \#\Phi_{A_{\mathfrak{p}}}(\overline{\mathbb{F}}_{\mathfrak{p}}).$$

Fix $P \in A_{\mathfrak{p}}(\widehat{K}_{\mathfrak{p}})$. We have $c \cdot \mathrm{red}_{\mathfrak{p}}(P) \in A_{\mathfrak{p}}^0(\overline{\mathbb{F}}_{\mathfrak{p}})$. But $A_{\mathfrak{p}}^0$ is a connected commutative group scheme over $\overline{\mathbb{F}}_{\mathfrak{p}}$, an algebraically closed field of characteristic $\ell \neq p$ and thus by Lemma 1.1.2:

$$c \cdot \mathrm{red}_{\mathfrak{p}}(P) = p^n R'$$

for some $R' \in A_{\mathfrak{p}}^0(\overline{\mathbb{F}}_{\mathfrak{p}})$. But the reduction homomorphism is surjective (cf. Lemma 1.2.11) and thus $R' = \mathrm{red}_{\mathfrak{p}}(R)$ for some $R \in \mathcal{A}(R')$, i.e.

$$cP - p^n R \in \ker\left(\mathrm{red}_{\mathfrak{p}} : A(K^{ur}) \to A_{\mathfrak{p}}(\overline{\mathbb{F}}_{\mathfrak{p}})\right) = \widehat{\mathcal{A}}(\mathfrak{m}^{ur})$$

(cf. (1.7) for the last equality). Note that p is invertible in $\mathcal{O}^{ur}$. Thus the multiplication by p is an automorphism of the formal group $\widehat{\mathcal{A}}(\mathfrak{m}^{ur})$ (cf. Lemma 1.3) and $\widehat{\mathcal{A}}(\mathfrak{m}^{ur})$ is p-divisible. Therefore (modifying R by some element of $\widehat{\mathcal{A}}(\mathfrak{m}^{ur})$ if necessary) we can assume that $cP = p^n R$. Note that $c = p^\alpha \cdot c'$, where $p \nmid c'$. Thus we can modify R by a multiple of P to obtain:

$$p^\alpha P = p^n R,$$

where $R \in A(\widehat{K}_\mathfrak{p}^{ur})$. This implies for the Kummer map κ_n:

$$\begin{aligned} p^\alpha \kappa_n(P,\sigma) = \kappa_n(p^\alpha P,\sigma) = \kappa_n(p^n R,\sigma) = \\ = R^\sigma - R = 0 \end{aligned}$$

for any $\sigma \in I_\mathfrak{p}^{(n)}$. Therefore $\Gamma^{(n)}(I_\mathfrak{p}^{(n)}) \subset A[p^\alpha]^{\oplus r}$ and we are done. □

Proof of Proposition 4.1.1. It follows by combining Propositions 4.2.1 and 4.2.2. □

Remark 4.2.3. *The form of the bound in Proposition 4.1.1 raises a natural question: are both inequalities $\alpha_\mathfrak{p} < \beta_\mathfrak{p}$ and $\alpha_\mathfrak{p} > \beta_\mathfrak{p}$ possible? The answer is* yes. *It turns out that in the case of elliptic curves with split multiplicative reduction both cases are possible.*

- *Let $v_p(x)$ denote the p-adic valuation of x. We choose primes ℓ, p such that $v_p(\ell - 1) = k \geq 2$. Consider the Tate curve $E_q/\mathbb{Q}_\ell$, where $q = \ell$. Then by [Sil94, Corollary IV.9.2.(d)] $\Phi_\ell(\overline{\mathbb{F}}_\ell)$ is trivial. On the other hand, one easily checks that*

  $$E_q(\mathbb{Q}_\ell)[p] \cong (\mathbb{Q}_\ell/q^\mathbb{Z})[p] = \langle \zeta_{p^k} \rangle \cong \mathbb{Z}/p^k,$$

  thus $\alpha_\ell = 0 < \beta_\ell = k$.

- *Let ℓ, p be primes such that $v_p(\ell - 1) = 1$. Note that not every element of $\mathbb{Q}_\ell^\times$ is a p-th power, since $\mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^p \neq 1$. Let $a \in \mathbb{Q}_\ell^\times \setminus (\mathbb{Q}_\ell^\times)^p$ and $q := \ell^{p^k} \cdot a$ for some $k \geq 2$. Consider the Tate curve $E_q/\mathbb{Q}_\ell$. Using again [Sil94, Corollary IV.9.2.(d)] we obtain:*

  $$\Phi_\ell(\overline{\mathbb{F}}_\ell) \cong \mathbb{Z}/(v_\ell(q)) \cong \mathbb{Z}/p^k.$$

  On the other hand, one easily checks that

  $$E_q(\mathbb{Q}_\ell)[p] \cong (\mathbb{Q}_\ell/q^\mathbb{Z})[p] = \langle \zeta_p \rangle \cong \mathbb{Z}/p,$$

  thus $\beta_\ell = 1 < \alpha_\ell = k$.

However, it turns out that it is possible to compare the exponents of $\Phi_\ell(\overline{\mathbb{F}}_\ell)[p^\infty]$ and $A(\widehat{K}_\mathfrak{p}^{ur})[p^\infty]$.

Proposition 4.2.4. *Let p^{γ_p} be the exponent of $A(\widehat{K}_\mathfrak{p}^{ur})[p^\infty]$. Then*

$$\alpha_p \leq \gamma_p.$$

Proof. Let $\mathbb{F}/\mathbb{F}_\mathfrak{p}$ be a finite field extension such that $\Phi_{A_\mathfrak{p}}(\mathbb{F}) = \Phi_{A_\mathfrak{p}}(\overline{\mathbb{F}}_\mathfrak{p})$ and let $\widehat{K}'_\mathfrak{p}$ be the finite unramified extension of $\widehat{K}_\mathfrak{p}$ with $\mathbb{F}$ as the residue field. By a similar argument as in proof of Proposition 4.2.1 the group $p^{\gamma_\mathfrak{p}} A(\widehat{K}'_\mathfrak{p})$ is p-divisible. Therefore $p^{\gamma_\mathfrak{p}} \Phi_{A_\mathfrak{p}}(\mathbb{F})$ must also be p-divisible and thus (since it is a finite group) it contains no p-torsion. It follows that $\alpha_p \leq \gamma_p$. □

4.3. Inertia groups over p

In this section we estimate the order of $I_{\mathfrak{p}}^{(n)}$ in the remaining case when $\mathfrak{p}|p$. Again, we use the Setup 4.0.1. Assume for a while that A has good reduction at p. In this case we can extend the reduction homorphism to the algebraic closure $\overline{K}_{\mathfrak{p}}$ of $\widehat{K_{\mathfrak{p}}}$ (cf. Remark 1.2.14). Let:

$$H_n := \begin{cases} \ker\left(\mathrm{red}_{\mathfrak{p}} : A(\overline{K}_{\mathfrak{p}})[p^n] \to A_{\mathfrak{p}}(\overline{\mathbb{F}}_{\mathfrak{p}})\right), & \text{if } A \text{ has good reduction at } \mathfrak{p}, \\ A[p^n], & \text{otherwise.} \end{cases}$$

One easily sees that $|H_n| = p^{nh_{\mathfrak{p}}}$.

Proof of Proposition 4.1.2. Observe that $\Gamma^{(n)}(I_{\mathfrak{p}}^{(n)}) \subset H_n^{\oplus r}$. If A has bad reduction at $\mathfrak{p}$, then this obviously holds true. If A has good reduction at $\mathfrak{p}$, then for all $\sigma \in I_{\mathfrak{p}}^{(n)}$:

$$\mathrm{red}_{\mathfrak{p}}(\kappa_n(P_i, \sigma)) = \mathrm{red}_{\mathfrak{p}}(P_i)^{\sigma} - \mathrm{red}_{\mathfrak{p}}(P_i) = 0$$

by Néron–Ogg–Shafarevich criterion (cf. Lemma 1.2.13). This yields the bound:

$$\#I_{\mathfrak{p}}^{(n)} \leq \#H_n^{\oplus r} = p^{h_{\mathfrak{p}} r n}.$$

We put $b := g \cdot [\widehat{K_{\mathfrak{p}}} : \mathbb{Q}_p]$. Using the classification theorem of compact p-adic Lie groups (cf. Theorem 1.2.3) we obtain:

$$A(\widehat{K_{\mathfrak{p}}}) \cong \mathcal{O}_{\widehat{K_{\mathfrak{p}}}}^{g} \times A(\widehat{K_{\mathfrak{p}}})_{tors} \cong \mathbb{Z}_p^b \times A(\widehat{K_{\mathfrak{p}}})_{tors}.$$

Let G be the group generated by the images of $p^{\beta_{\mathfrak{p}}} P_1, \ldots, p^{\beta_{\mathfrak{p}}} P_r$ inside the group

$$p^{\beta_{\mathfrak{p}}} A(\widehat{K_{\mathfrak{p}}}) / p^{n+\beta_{\mathfrak{p}}} A(\widehat{K_{\mathfrak{p}}}) \cong (\mathbb{Z}/p^n)^b.$$

The group G is generated by images of at most b elements $Q_1, \ldots, Q_b \in A(\widehat{K_{\mathfrak{p}}})$. Suppose

$$p^{\beta_{\mathfrak{p}}} P_i \equiv \sum_j a_{ij} Q_j \pmod{p^n A(\widehat{K_{\mathfrak{p}}})} \qquad \text{for some } a_i \in \mathbb{Z}.$$

Then for $\sigma \in I_{\mathfrak{p}}^{(n)}$ we have:

$$p^{\beta_{\mathfrak{p}}} \kappa_n(P_i, \sigma) = \sum_j a_{ij} \kappa_n(Q_j, \sigma). \tag{4.5}$$

Consider the homomorphism $\Psi^{(n)} : I_{\mathfrak{p}}^{(n)} \to H_n^{\oplus b}, \quad \Psi^{(n)}(\sigma) = \bigoplus_{i=1}^{b} \kappa_n(Q_i, \sigma)$. Note that the equality (4.5) implies that $\Gamma^{(n)}(\ker \Psi^{(n)}) \subset H_{\beta_{\mathfrak{p}}}^{\oplus r}$ and thus, since $\Gamma^{(n)}$ is injective, $\#(\ker \Psi^{(n)}) \leq p^{h_{\mathfrak{p}} r \beta_{\mathfrak{p}}}$. Finally we obtain:

$$\begin{aligned} \#I_{\mathfrak{p}}^{(n)} &= \#\Psi^{(n)}(I_{\mathfrak{p}}^{(n)}) \cdot \#(\ker \Psi^{(n)}) \leq \\ &\leq p^{h_{\mathfrak{p}} b n} \cdot p^{h_{\mathfrak{p}} r \beta_{\mathfrak{p}}} = p^{h_{\mathfrak{p}} b n + h_{\mathfrak{p}} r \beta_{\mathfrak{p}}}. \end{aligned}$$

□

4.4. Kummer theory and the surjectivity of $\rho_{A,p}$

The results presented in previous sections are insufficient to obtain any effective bound on m_p. We will prove a criterion for m_p to vanish. This will allow us to give an explicit numerical example in Section 4.5.

Theorem 4.4.1. *Suppose that the image of the p-adic representation*

$$\rho_{A,p} : G_K \to \mathrm{GSp}_{2g}(\mathbb{Z}_p)$$

associated to the abelian variety A contains $\mathrm{Sp}_{2g}(\mathbb{Z}_p)$. *Then the map* $\Gamma^{(\infty)}$ *is an isomorphism.*

The proof of Theorem 4.4.1 will occupy the rest of this section. First, we need few preliminary lemmas concerning the symplectic groups. Recall that for any commutative unital ring R:

$$\mathrm{GSp}_{2g}(R) := \{M \in M_{2g}(R) : M\Omega M^T = \lambda(M) \cdot \Omega \quad \text{for some } \lambda(M) \in R^\times\},$$

where $\Omega = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$. Note that $\lambda(M)$ may be considered as a surjective homomorphism $\mathrm{GSp}_{2g}(R) \to R^\times$. Its kernel is denoted by $\mathrm{Sp}_{2g}(R)$. For any local ring R with the maximal ideal $\mathfrak{m}$ we introduce the following notation:

$$\begin{aligned}\mathrm{GSp}_{2g}(R)_n &:= \{M \in \mathrm{GSp}_{2g}(R) : M \equiv I_{2g} \pmod{\mathfrak{m}^n}\} \\ &= \ker\left(\mathrm{GSp}_{2g}(R) \to \mathrm{GSp}_{2g}(R/\mathfrak{m}^n)\right).\end{aligned}$$

We define $\mathrm{Sp}_{2g}(R)_n$ in a similar manner.

Lemma 4.4.2. *If R is a local ring, then for any positive integers* m, n*:*

$$[\mathrm{GSp}_{2g}(R)_n, \mathrm{GSp}_{2g}(R)_m] = [\mathrm{Sp}_{2g}(R)_n, \mathrm{Sp}_{2g}(R)_m] = \mathrm{Sp}_{2g}(R)_{n+m}.$$

Proof. The first equality is immediate. The second equality follows from [Sos78, Theorem, page 843] by taking $\mathfrak{b}_r := \mathfrak{m}^r$, $f(i,j,k) = k$ and by noting that a maximal ideal in a local ring must be quasi-regular. □

Lemma 4.4.3. *The representation of* $\mathrm{Sp}_{2g}(\mathbb{F}_p)$ *on the* $\mathbb{F}_p$*-vector space:*

$$\mathfrak{sp}_{2g}(\mathbb{F}_p) = \{M \in M_{2g}(\mathbb{F}_p) : M\Omega + \Omega M^T = 0\}$$

(given by conjugation) is irreducible.

Proof. Let $S(2)$ be the space of symmetric matrices in $M_{2g}(\mathbb{F}_p)$ with an action of $\mathrm{Sp}_{2g}(\mathbb{F}_p)$ given by:

$$(A, M) \mapsto AMA^T$$

Note that one may also identify $S(2)$ with the space of quadratic forms over $\mathbb{F}_p$ in $2g$ variables. The maps:

$$\begin{aligned} S(2) &\to \mathfrak{sp}_{2g}(\mathbb{F}_p), \quad M \mapsto M\Omega \\ \mathfrak{sp}_{2g}(\mathbb{F}_p) &\to S(2), \quad N \mapsto -N\Omega \end{aligned}$$

provide isomorphisms of $\mathbb{F}_p[\mathrm{Sp}_{2g}(\mathbb{F}_p)]$-modules. It suffices now to note that $S(2)$ is a simple $\mathbb{F}_p[\mathrm{Sp}_{2g}(\mathbb{F}_p)]$-module by [SZ, Proposition 2.2.]. □

The following proposition is a generalization of [SY15, Lemma 2.2] to the case of abelian varieties.

Proposition 4.4.4. *If the image of* $\rho_{A,p} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GSp}_{2g}(\mathbb{Z}_p)$ *contains* $\mathrm{Sp}_{2g}(\mathbb{Z}_p)$ *then* $L_1 \cap K_\infty = K_1$.

Proof. Let $N := L_1 \cap K_\infty$. Let $K_1^{(p)}$ be the maximal abelian extension of exponent p of K_1 inside of K_∞. Then obviously $N \subset K_1^{(p)}$. Moreover, both $\mathrm{Gal}(K_1^{(p)}/K_1)$ and $\mathrm{Gal}(N/K_1)$ are $\mathbb{F}_p[\mathrm{Gal}(K_1/K)]$-modules. We will compare their structure as $\mathbb{F}_p[\mathrm{Sp}_{2g}(\mathbb{F}_p)]$-modules. Note that by assumption

$$\mathrm{Sp}_{2g}(\mathbb{Z}_p)_1 \subset \mathrm{Gal}(K_\infty/K_1) \subset \mathrm{GSp}_{2g}(\mathbb{Z}_p)_1.$$

By Lemma 4.4.2 we see that

$$\begin{aligned}[\mathrm{Gal}(K_\infty/K_1), \mathrm{Gal}(K_\infty/K_1)] &= [\mathrm{Sp}_{2g}(\mathbb{Z}_p)_1, \mathrm{Sp}_{2g}(\mathbb{Z}_p)_1] \\ &= [\mathrm{GSp}_{2g}(\mathbb{Z}_p)_1, \mathrm{GSp}_{2g}(\mathbb{Z}_p)_1] \\ &= \mathrm{Sp}_{2g}(\mathbb{Z}_p)_2.\end{aligned}$$

Therefore we have:

$$\mathrm{Sp}_{2g}(\mathbb{Z}_p)_1^{ab} \leq \mathrm{Gal}(K_\infty/K_1)^{ab} \leq \mathrm{GSp}_{2g}(\mathbb{Z}_p)_1^{ab}$$

and

$$\begin{aligned}\mathrm{GSp}_{2g}(\mathbb{Z}_p)_1^{ab} &\cong \mathrm{GSp}_{2g}(\mathbb{Z}_p)_1 / \mathrm{Sp}_{2g}(\mathbb{Z}_p)_2 \\ &\cong \mathrm{Sp}_{2g}(\mathbb{Z}/p^2)_1 \times (1 + p\mathbb{Z}_p) \\ &\cong \mathfrak{sp}_{2g}(\mathbb{F}_p) \times \mathbb{Z}_p,\end{aligned}$$

where:

- the isomorphism $\mathrm{GSp}_{2g}(\mathbb{Z}_p)_1 / \mathrm{Sp}_{2g}(\mathbb{Z}_p)_2 \cong \mathrm{Sp}_{2g}(\mathbb{Z}/p^2)_1 \times (1 + p\mathbb{Z}_p)$ is given by

$$A \mapsto (\lambda(A)^{-1} \cdot A, \lambda(A)),$$

- the isomorphism $\mathrm{Sp}_{2g}(\mathbb{Z}/p^2)_1 \cong \mathfrak{sp}_{2g}(\mathbb{F}_p)$ is given by $I + pM \mapsto M$.

Analogously, we have: $\mathrm{Sp}_{2g}(\mathbb{Z}_p)_1^{ab} \cong \mathfrak{sp}_{2g}(\mathbb{F}_p)$. This implies easily that

$$\mathrm{Gal}(K_1^{(p)}/K_1) \cong \mathfrak{sp}_{2g}(\mathbb{F}_p) \times (\mathbb{Z}/p)^i \qquad \text{for } i \in \{0, 1\}$$

as $\mathbb{F}_p[\mathrm{Sp}_{2g}(\mathbb{F}_p)]$-modules (with trivial action on $\mathbb{Z}/p$ and action on $\mathfrak{sp}_{2g}(\mathbb{F}_p)$ given by conjugation). The assumption implies that $A[p]$ is an irreducible $\mathrm{Sp}_{2g}(\mathbb{F}_p)$-module. Thus $\mathrm{Gal}(L_1/K_1) \cong A[p]^{\oplus r'}$ for some $r' \leq r$. Moreover, since

$$\mathrm{Gal}(L_1/K_1) \cong A[p]^{\oplus r'} \twoheadrightarrow \mathrm{Gal}(N/K_1),$$

we obtain $\mathrm{Gal}(N/K) \cong A[p]^{\oplus s}$ for some $s \leq r'$. On the other hand:

$$\mathrm{Gal}(K_1^{(p)}/K_1) \cong \mathfrak{sp}_{2g}(\mathbb{F}_p) \times (\mathbb{Z}/p)^i \twoheadrightarrow \mathrm{Gal}(N/K_1),$$

and since $\mathfrak{sp}_{2g}(\mathbb{F}_p)$ and $\mathbb{Z}/p$ are simple $\mathbb{F}_p[\mathrm{Sp}_{2g}(\mathbb{F}_p)]$-modules, which are non-isomorphic to $A[p]$, we obtain $s = 0$ and $N = K_1$. □

Proof of Theorem 4.4.1. It suffices to check that $\Gamma^{(\infty)}$ is surjective. One easily checks that $\mathrm{Sp}_{2g}(\mathbb{Z}_p) \subset \rho_p(G_K)$ implies that the axioms B_1, B_2 and B_3 from [Rib79] are satisfied. Thus by [Rib79, Theorem 1.2] $\Gamma^{(1)}$ is an isomorphism. By Proposition 4.4.4 we obtain $L_1 \cap K_\infty = K_1$. Consider the commutative diagram:

$$\begin{array}{ccc} \mathrm{Gal}(L_\infty/K_\infty) & \xhookrightarrow{\quad\Gamma^{(\infty)}\quad} & T_p(A)^{\oplus r} \\ \big\downarrow & & \big\downarrow \\ \mathrm{Gal}(L_1/L_1\cap K_\infty) = \mathrm{Gal}(L_1/K_1) & \xrightarrow[\cong]{\quad\Gamma^{(1)}\quad} & A[p]^{\oplus r}. \end{array}$$

Note that the $\mathbb{Z}_p$-modules

$$M := \Gamma^{(\infty)}(\mathrm{Gal}(L_\infty/K_\infty)) \quad \text{and} \quad N := T_p(A)^{\oplus r}$$

satisfy $M \subset N$ and

$$M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p/p\mathbb{Z}_p = \Gamma^{(1)}(\mathrm{Gal}(L_1/K_1)) \cong A[p]^{\oplus r} = N \otimes_{\mathbb{Z}_p} \mathbb{Z}_p/p\mathbb{Z}_p.$$

Therefore $M = N$ by Nakayama's lemma, which ends the proof. □

4.5. A numerical example

In order to illustrate our estimates of class numbers we offer a numerical example. Consider the genus two curve over $\mathbb{Q}$ with label 25913.a.25913 in [LMF20]. Its affine part is given by the equation:

$$X : y^2 + (x^3 + x + 1)y = x^3 - x^2 - 2x.$$

Let $A = \mathrm{Jac}(X)$ be the Jacobian variety of X. Its endomorphism ring $\mathrm{End}_{\overline{\mathbb{Q}}}(A)$ equals $\mathbb{Z}$. By using Magma we compute that $A(\mathbb{Q}) \cong \mathbb{Z}^3$. By Theorem 4.1.4 for each prime we have the following estimate (since $h_p \leq 4$):

$$k_n \geq 2 \cdot (2 \cdot 3 - 4) \cdot n - C = 4n - C,$$

where $C = C(p)$ is a constant. We compute now the constant C for almost all primes p. The conductor of A is 25913, which is a prime number. Let p be a prime outside of the set $S := \{2, 3, 5, 7, 25913\}$.

- Using algorithm described in [Die02], we check that the Galois representation $\rho_\ell : G_{\mathbb{Q}} \to \mathrm{GSp}_4(\mathbb{Z}_\ell)$ is surjective for primes ℓ outside S (note that the primality of the conductor simplifies the calculations – cf. [Die02, Remark 5.14]). Thus by Theorem 4.4.1 we have $m_p = 0$.
- Using Magma we check that for every prime p the Tamagawa number of A at p is trivial and thus $\alpha_p = 0$.
- By (1.4) the formal group $\widehat{\mathcal{A}}(p\mathbb{Z}_p) \cong \ker(\mathrm{red}_p : A(\mathbb{Q}_p) \to A_p(\mathbb{F}_p))$ is torsion-free and thus p^{β_p} divides the exponent of $A_p(\mathbb{F}_p)$. Therefore by Weil's estimate we obtain $\beta_p \leq 2$.

Finally, using (4.4) it follows that we may take $C = 24$ in this case, i.e.

$$k_n \geq 4n - 24.$$

Notation

- categories:
  - $\mathrm{Ob}(\mathscr{A})$ – the class of objects in a category $\mathscr{A}$ ..... p. 15
  - $\mathrm{Hom}_{\mathscr{A}}(A, B)$ – the class of morphisms between two objects of $\mathscr{A}$ ..... p. 15
  - $\mathbf{Sch}/S$ – the category of schemes over a base scheme S ..... p. 15
  - $\mathbf{GS}/S$ – the category of finite flat commutative group schemes over S ..... p. 17
  - p-$\mathbf{div}/S$ – the category of p-divisible groups over S ..... p. 18
  - $\mathbf{Sch}/R$ (resp. $\mathbf{GS}/R$, etc.) – the category of schemes (resp. group schemes, etc.) over $\operatorname{Spec} R$
  - Art_k – the category of local Artin rings with k as a residue field ..... p . 23
  - R-mod – the category of modules over a ring R
  - $\mathcal{O}$-mod – the category of modules over a sheaf $\mathcal{O}$
  - $\mathrm{Ext}^i_{\mathscr{A}}(A, B)$ – the i-th Ext functor in a category $\mathscr{A}$ ..... p . 17
  - R^iF – the i-th derived functor of a functor F
- homological algebra:
  - $\mathcal{C}(\mathscr{A})$ – the category of cochain complexes of an abelian category $\mathscr{A}$ ..... p. 25
  - $\mathcal{C}_+(\mathscr{A})$ – the category of non-negative cochain complexes ..... p. 25
  - $h^i(C^\bullet)$ – the i-th cohomology of a complex $C^\bullet \in \mathrm{Ob}(\mathcal{C}(\mathscr{A}))$ ..... p. 25
  - $A[i]$ – the cochain complex satisfying

$$A[i]^j = \begin{cases} A, & j = i \\ 0, & j \neq i. \end{cases}$$

    for a fixed object $A \in \mathrm{Ob}(\mathscr{A})$ ..... p. 25
- schemes:
  - X_T – the base change of an S-scheme X via a morphism $T \to S$
  - $\Omega^\bullet_{X/k}$ – the de Rham complex of a k-scheme X ..... p. 25

- $\mathrm{End}_K(A) := \mathrm{Hom}_K(A, A)$ ..... p. 19
- $T_\ell A$ – the ℓ-adic Tate module of A ..... p. 21
- ρ_ℓ – the ℓ-adic Galois representation of A ..... p. 21
- $r(A)$ – the p-rank of an abelian variety ..... p. 20
- π_A – the Frobenius endomorphism of $A/\mathbb{F}_q$ ..... p. 30
- $K_n := K(A[p^n])$ – the p^n-th divison field of A/k ..... p. 24
- L_n – the p^n-th Kummer field of A/k (for some fixed $P_1, \ldots, P_r \in A(K)$) ... p. 24
- $K_\infty = \bigcup_n K_n$, $L_\infty = \bigcup_n L_n$ ..... p. 24
- κ_n – the Kummer pairing ..... p. 24
- $\Gamma^{(n)}$ – the Kummer representation of A ..... p. 24
- m_p – the number defined by $p^{m_p} = [T_p(A)^{\oplus r} : \Gamma^{(\infty)}(\mathrm{Gal}(L_\infty/K_\infty))]$ ..... p. 24
- $\mathcal{A}$ – the Néron model of A ..... p. 22
- $A_B := \mathcal{A}_B$ ..... p. 22
- $A_\mathfrak{p} := \mathcal{A}_{R/\mathfrak{p}}$ – the fiber of $\mathcal{A}$ over $\mathfrak{p}$ ..... p. 22
- $\Phi_{A_\mathfrak{p}}$ – the group scheme of geometric components ..... p. 22
- $\widehat{\mathcal{A}}$ – the formal group associated to $\mathcal{A}$ ..... p. 22
- $\mathrm{red}_\mathfrak{p}, \mathrm{red}_{\mathfrak{p},n}$ – reduction homomorphisms ..... p. 22
- $\mathrm{Def}_{A/k}(R)$ – deformations of an abelian variety A/k to R ..... p. 23
- $\mathcal{M}_{A/k}$ – the formal torus pro-representing $\mathrm{Def}_{A/k}$ ..... p. 30
- $D_{n,d}(A/K)$ – the (n,d)-degree of A over K ..... p. 33
- $a_{p^d}(E)$ – the p^d-Frobenius trace of an elliptic curve $E/\mathbb{F}_p$ ..... p. 36
- $p^{\alpha_\mathfrak{p}}$ – the exponent of the group $\Phi_{A_\mathfrak{p}}(\overline{\mathbb{F}}_\mathfrak{p})[p^\infty]$ ..... p. 59
- $p^{\beta_\mathfrak{p}}$ – the exponent of the group $A(K_\mathfrak{p})[p^\infty]$ ..... p. 59
- $h_\mathfrak{p} := 2g - r(A_\mathfrak{p})$, if A has good reduction at $\mathfrak{p}$ and $h_\mathfrak{p} := 2g$, if A has bad reduction at $\mathfrak{p}$ ..... p. 59

- abstract algebra:

  - $H \leq G$ – H is a subgroup of G
  - $G[n]$ – the n-torsion subgroup of an abelian group G
  - G_{tors} – the subgroup of torsion elements of an abelian group G
  - Q_8 – the quaternion group on 8 elements ..... p. 55
  - $\widehat{M}$ – the completion of a module over a local ring w.r.t. its maximal ideal .. p. 27
  - M^G – the set of G-fixed points for an $R[G]$-module M ..... p. 26
  - $H^i(G, M)$ – group cohomology of a G-module M ..... p. 26
  - $\mathrm{Ind}_H^G M$ – G-module induced from an H-module M ..... p. 27
  - $G_K := \mathrm{Gal}(K^{sep}/K)$ – the absolute Galois group of a field K ..... p. 21
  - $\mathrm{Sp}_{2g}(R)$ – the symplectic group of dimension $2g$ over a ring R ..... p. 65
  - $\mathrm{GSp}_{2g}(R)$ – the general symplectic group of dimension $2g$ over a ring R .... p. 65
  - $\mathrm{GSp}_{2g}(R)_n = \ker\left(\mathrm{GSp}_{2g}(R) \to \mathrm{GSp}_{2g}(R/\mathfrak{m}^n)\right)$ ..... p. 65

- $\mathfrak{sp}_{2g}$ – the Lie algebra of Sp_{2g}
- V' – the k-vector space with the same underlying abelian group as V and the scalar multiplication $(\lambda, v) \mapsto \lambda^p \cdot v$ ..... p. 26
- $R^\times$ – the subgroup of units in a ring R

- coverings of curves:
  - $\pi : X \to Y := X/G$ – the quotient morphism by an action of a group G ..... p. 39
  - g_Y – the genus of the curve Y ..... p. 39
  - $R = \sum_{P \in X} d_P \cdot (P)$ – the ramification divisor of π ..... p. 39
  - $R' := \left[\frac{\pi_* R}{\#G}\right] \in \mathrm{Div}(Y)$ (the integral part taken coefficient by coefficient) ..... p. 39
  - $G_{P,i}$ – the i-th ramification group of π at P ..... p. 39
  - e_P – the ramification index of π at $P \in X$ ..... p. 39
  - $n_P := \max\{n : G_{P,n} \neq 0\}$ ..... p. 39

Bibliography

[AdRGP13] S. Arias-de Reyna, W. Gajda, and S. Petersen. Big monodromy theorem for abelian varieties over finitely generated fields. *J. Pure Appl. Algebra*, 217(2):218–229, 2013.

[AWZ17] P. Achinger, J. Witaszek, and M. Zdanowicz. Liftability of the Frobenius morphism and images of toric varieties, 2017.

[Bas72] M. I. Bashmakov. The cohomology of abelian varieties over a number field. *Russian Mathematical Surveys*, 27(6):25, 1972.

[BGK05] G. Banaszak, W. Gajda, and P. Krasoń. Detecting linear dependence by reduction maps. *J. Number Theory*, 115(2):322–342, 2005.

[Bla14] C. Blake. A Deuring criterion for abelian varieties. *Bull. Lond. Math. Soc.*, 46(6):1256–1263, 2014.

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.

[BM00] J. Bertin and A. Mézard. Déformations formelles des revêtements sauvagement ramifiés de courbes algébriques. *Invent. Math.*, 141(1):195–238, 2000.

[Car57] P. Cartier. Une nouvelle opération sur les formes différentielles. *C. R. Acad. Sci. Paris*, 244:426–428, 1957.

[CCO14] Ch.-L. Chai, B. Conrad, and F. Oort. *Complex multiplication and lifting problems*, volume 195 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2014.

[CD14] J. B. Cosgrave and K. Dilcher. The Gauss-Wilson theorem for quarter-intervals. *Acta Math. Hungar.*, 142(1):199–230, 2014.

[CL19] P. L. Clark and A. Lacy. There are genus one curves of every index over every infinite, finitely generated field. *J. Reine Angew. Math.*, 749:65–86, 2019.

[Con02] B. Conrad. A modern proof of Chevalley's theorem on algebraic groups. *J. Ramanujan Math. Soc.*, 17(1):1–18, 2002.

[CX08] P. L. Clark and X. Xarles. Local bounds for torsion points on abelian varieties. *Canad. J. Math.*, 60(3):532–555, 2008.

[DF04] D. S. Dummit and R. M. Foote. *Abstract algebra.* John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[DI87] P. Deligne and L. Illusie. Relèvements modulo p^2 et décomposition du complexe de de Rham. *Invent. Math.*, 89(2):247–270, 1987.

[Die02] L. V. Dieulefait. Explicit determination of the images of the Galois representations attached to abelian surfaces with $\mathrm{End}(A) = \mathbb{Z}$. *Experiment. Math.*, 11(4):503–512 (2003), 2002.

[dJN91] J. de Jong and R. Noot. Jacobians with complex multiplication. In *Arithmetic algebraic geometry (Texel, 1989)*, volume 89 of *Progr. Math.*, pages 177–192. Birkhäuser Boston, Boston, MA, 1991.

[DW08] Ch. David and T. Weston. Local torsion on elliptic curves and the deformation theory of Galois representations. *Math. Res. Lett.*, 15(3):599–611, 2008.

[FKY07] T. Fukuda, K. Komatsu, and Sh. Yamagata. Iwasawa λ-invariants and Mordell-Weil ranks of abelian varieties with complex multiplication. *Acta Arith.*, 127(4):305–307, 2007.

[FWG+86] G. Faltings, G. Wüstholz, F. Grunewald, N. Schappacher, and U. Stuhler. *Rational points.* Aspects of Mathematics, E6. Friedr. Vieweg & Sohn, Braunschweig, second edition, 1986. Papers from the seminar held at the Max-Planck-Institut für Mathematik, Bonn/Wuppertal, 1983/1984.

[Gam14] A. Gamzon. Local torsion on abelian surfaces with real multiplication by $\mathbf{Q}(\sqrt{5})$. *Int. J. Number Theory*, 10(7):1807–1827, 2014.

[Gar16] J. Garnek. Arytmetyka krzywych eliptycznych. *Master Thesis*, 2016.

[Gar18] J. Garnek. On p-degree of elliptic curves. *Int. J. Number Theory*, 14(3):693–704, 2018.

[Gar19a] J. Garnek. Equivariant splitting of the Hodge–de Rham exact sequence. *arXiv e-prints*, page arXiv:1904.05074, April 2019.

[Gar19b] J. Garnek. On class numbers of division fields of abelian varieties. *J. Théor. Nombres Bordeaux*, 31(1):227–242, 2019.

[GD71] A. Grothendieck and J. A. Dieudonné. *Eléments de géométrie algébrique. III*, volume 166 of *Pub. Math. IHES*. Springer-Verlag, Berlin, 1971.

[GH81] B. H. Gross and J. Harris. Real algebraic curves. *Annales scientifiques de l'École Normale Supérieure*, 14(2):157–182, 1981.

[Gre01] R. Greenberg. Iwasawa theory—past and present. In *Class field theory—its centenary and prospect (Tokyo, 1998)*, volume 30 of *Adv. Stud. Pure Math.*, pages 335–385. Math. Soc. Japan, Tokyo, 2001.

[Gro57] A. Grothendieck. Sur quelques points d'algèbre homologique. *Tôhoku Math. J. (2)*, 9:119–221, 1957.

[Hal11] Ch. Hall. An open-image theorem for a general class of abelian varieties. *Bull. Lond. Math. Soc.*, 43(4):703–711, 2011. With an appendix by Emmanuel Kowalski.

[Har75] R. Hartshorne. On the De Rham cohomology of algebraic varieties. *Inst. Hautes Études Sci. Publ. Math.*, (45):5–99, 1975.

[Har77] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[Hir19] T. Hiranouchi. Local torsion primes and the class numbers associated to an elliptic curve over $\mathbb{Q}$. *Hiroshima Math. J.*, 49(1):117–127, 2019.

[Hor12] R. Hortsch. On the canonical representation of curves in positive characteristic. *New York J. Math.*, 18:911–924, 2012.

[HS00] M. Hindry and J. H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[Ish04] N. Ishii. Trace of Frobenius endomorphism of an elliptic curve with complex multiplication. *Bulletin of the Australian Mathematical Society*, 70(1):125–142, 2004.

[Jac85] N. Jacobson. *Basic algebra. I.* W. H. Freeman and Company, New York, second edition, 1985.

[JQ14] Q. Ji and H. Qin. CM elliptic curves and primes captured by quadratic polynomials. *Asian J. Math.*, 18(4):707–726, 2014.

[Kat81] N. M. Katz. Serre-Tate local moduli. In *Algebraic surfaces (Orsay, 1976–78)*, volume 868 of *Lecture Notes in Math.*, pages 138–202. Springer, Berlin-New York, 1981.

[Köc04] B. Köck. Galois structure of Zariski cohomology for weakly ramified covers of curves. *Amer. J. Math.*, 126(5):1085–1107, 2004.

[Kon07] A. Kontogeorgis. On the tangent space of the deformation functor of curves with automorphisms. *Algebra Number Theory*, 1(2):119–161, 2007.

[KST17] M. Kronberg, M. A. Soomro, and J. Top. Twists of elliptic curves. *SIGMA Symmetry Integrability Geom. Methods Appl.*, 13:Paper No. 083, 13, 2017.

[KT18] B. Köck and J. Tait. On the de-Rham cohomology of hyperelliptic curves. *Res. Number Theory*, 4(2):4:19, 2018.

[Kum52] E. E. Kummer. Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen. *J. Reine Angew. Math.*, 44:93–146, 1852.

[Lan13] K.-W Lan. *Arithmetic compactifications of PEL-type Shimura varieties*, volume 36 of *London Mathematical Society Monographs Series*. Princeton University Press, Princeton, NJ, 2013.

[Lar95] M. Larsen. Maximality of Galois actions for compatible systems. *Duke Math. J.*, 80(3):601–630, 1995.

[LMF20] The LMFDB Collaboration. The l-functions and modular forms database. `http://www.lmfdb.org`, 2020. [Online; accessed 13 March 2020].

[Maz97] B. Mazur. An "infinite fern" in the universal deformation space of Galois representations. *Collect. Math.*, 48(1-2):155–193, 1997. Journées Arithmétiques (Barcelona, 1995).

[Mes72] W. Messing. *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes.* Lecture Notes in Mathematics, Vol. 264. Springer-Verlag, Berlin-New York, 1972.

[Mil80] J. S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series.* Princeton University Press, Princeton, N.J., 1980.

[Mil08] J. S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/.

[MT11] G. Malle and D. Testerman. *Linear algebraic groups and finite groups of Lie type*, volume 133 of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, Cambridge, 2011.

[Mum08] D. Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics.* Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.

[Nak86] S. Nakajima. Action of an automorphism of order p on cohomology groups of an algebraic curve. *J. Pure Appl. Algebra*, 42(1):85–94, 1986.

[Neu99] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Oda69] T. Oda. The first de Rham cohomology group and Dieudonné modules. *Ann. Sci. École Norm. Sup. (4)*, 2:63–135, 1969.

[Ogu81] A. Ogus. *Hodge Cycles and Crystalline Cohomology*, pages 357–414. Springer Berlin Heidelberg, Berlin, Heidelberg, 1981.

[Ohs20] T. Ohshita. Asymptotic lower bound of class numbers along a Galois representation. *Journal of Number Theory*, 211:95 – 112, 2020.

[Oor92] F. Oort. CM-liftings of abelian varieties. *J. Algebraic Geom.*, 1(1):131–146, 1992.

[Pri08] R. Pries. A short guide to p-torsion of abelian varieties in characteristic p. In *Computational arithmetic geometry*, volume 463 of *Contemp. Math.*, pages 121–129. Amer. Math. Soc., Providence, RI, 2008.

[PZ12] R. Pries and H. J. Zhu. The p-rank stratification of Artin-Schreier curves. *Ann. Inst. Fourier (Grenoble)*, 62(2):707–726, 2012.

[Qin16] H. Qin. Anomalous primes of the elliptic curve $E_D\colon y^2 = x^3 + D$. *Proc. Lond. Math. Soc. (3)*, 112(2):415–453, 2016.

[Ray74] M. Raynaud. Schémas en groupes de type $(p, \dots, p)$. *Bull. Soc. Math. France*, 102:241–280, 1974.

[Rib79] K. A. Ribet. Kummer theory on extensions of abelian varieties by tori. *Duke Math. J.*, 46(4):745–761, 1979.

[Rot09] J. J. Rotman. *An introduction to homological algebra*. Universitext. Springer, New York, second edition, 2009.

[Ser79] J.-P. Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[Ser89] J.-P. Serre. *Abelian l-adic representations and elliptic curves*. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, second edition, 1989. With the collaboration of Willem Kuyk and John Labute.

[Ser92] J.-P. Serre. *Lie algebras and Lie groups*, volume 1500 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, second edition, 1992. 1964 lectures given at Harvard University.

[Ser13] J.-P. Serre. *Oeuvres/Collected papers. IV. 1985–1998*. Springer Collected Works in Mathematics. Springer, Heidelberg, 2013. Reprint of the 2000 edition.

[Sha86] S. S. Shatz. Group schemes, formal groups, and p-divisible groups. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 29–78. Springer, New York, 1986.

[Sil94] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sil09] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Sos78] Ju. V. Sosnovskiĭ. Commutator structure of symplectic groups. *Mat. Zametki*, 24(5):641–648, 734, 1978.

[Sta16] The Stacks Project Authors. *Stacks Project*. `http://stacks.math.columbia.edu`, 2016.

[Sti93] H. Stichtenoth. *Algebraic function fields and codes*. Universitext. Springer-Verlag, Berlin, 1993.

[Sub75] D. Subrao. The p-rank of Artin-Schreier curves. *Manuscripta Math.*, 16(2):169–193, 1975.

[Sut16] A. V. Sutherland. Computing images of Galois representations attached to elliptic curves. *Forum Math. Sigma*, 4:e4, 79, 2016.

[SY15] F. Sairaiji and T. Yamauchi. On the class numbers of the fields of the p^n-torsion points of certain elliptic curves over $\mathbb{Q}$. *J. Number Theory*, 156:277–289, 2015.

[SY18] F. Sairaiji and T. Yamauchi. On the class numbers of the fields of the p^n-torsion points of elliptic curves over $\mathbb{Q}$. *J. Théor. Nombres Bordeaux*, 30(3):893–915, 2018.

[SZ] I. D. Supunenko and A. E. Zalesskii. Reduced symmetric powers of natural realizations of the groups $SL_m(p)$ and $Sp_m(p)$ and their restrictions to subgroups. *Siberian Math. J.*, 31(4):33–46.

[Tat97] J. Tate. *Modular Forms and Fermat's Last Theorem*, chapter Finite Flat Group Schemes, pages 121–154. Springer New York, New York, NY, 1997.

[Tow96] Ch. Towse. Weierstrass points on cyclic covers of the projective line. *Trans. Amer. Math. Soc.*, 348(8):3355–3378, 1996.

[Voi02] C. Voisin. *Hodge theory and complex algebraic geometry. I*, volume 76 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2002. Translated from the French original by Leila Schneps.

[Wed08] T. Wedhorn. De Rham cohomology of varieties over fields of positive characteristic. In *Higher-dimensional geometry over finite fields*, volume 16 of *NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur.*, pages 269–314. IOS, Amsterdam, 2008.

[Wei94] Ch. A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994.

[Zar85] Yu. G. Zarhin. A finiteness theorem for unpolarized abelian varieties over number fields with prescribed places of bad reduction. *Invent. Math.*, 79(2):309–321, 1985.