CRYSTALLINE REPRESENTATIONS AND NÉRON MODELS

by

Susan Hammond Marshall

A Dissertation Submitted to the Faculty of the

DEPARTMENT OF MATHEMATICS

In Partial Fulfillment of the Requirements
For the Degree of

DOCTOR OF PHILOSOPHY

In the Graduate College

THE UNIVERSITY OF ARIZONA

2001

UMI Number: 3016487

Bell & Howell Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

THE UNIVERSITY OF ARIZONA ®
GRADUATE COLLEGE

As members of the Final Examination Committee, we certify that we have read the dissertation prepared by Susan Hammond Marshall

entitled Crystalline representations and Neron models

and recommend that it be accepted as fulfilling the dissertation requirement for the Degree of Doctor of Philosophy

Minhyong Kim	Date 5/3/01
Douglas Ulmer	Date 5/3/01
Daniel Madden	Date 5/3/01
Klaus Lux	Date 5/3/01
Douglas Pickrell	Date 5/3/01

Final approval and acceptance of this dissertation is contingent upon the candidate's submission of the final copy of the dissertation to the Graduate College.

I hereby certify that I have read this dissertation prepared under my direction and recommend that it be accepted as fulfilling the dissertation requirement.

Dissertation Director Minhyong Kim	Date 5-3-2001 5/3/01

STATEMENT BY AUTHOR

SIGNED: Susan H. Marshall

Acknowledgements

I would like to express my thanks to my advisor, Minhyong Kim, for sharing with me the beautiful world of mathematics and for the all the support and encouragement he gave me throughout my time at the University of Arizona.

The Department of Mathematics at the University of Arizona has been an enjoyable and stimulating place to study, thanks to many people (professors, staff and students alike). I would especially like to thank the Number Theory group, including Bill McCallum, Doug Ulmer, Kirti Joshi and Dinesh Thakur. I'm grateful to Bill McCallum for sharing his ideas and expertise in the subject of Fermat curves.

I would like to thank Doug Ulmer, Dan Madden and Dino Lorenzini for reading this thesis and sharing their comments and suggestions.

I'd also like to thank my friends and fellow graduate students for providing lodging, proof-reading services and general moral support during this past year, especially Alex, Sacha, Jenn, Guada, Jeff, my officemates, and the rest of the 7th floor gang. I would also like to express my gratitude for the moral support provided by my friend Teresa, even while navigating a very large speed bump in the road of her own life.

I would like to thank my family for their support, both this past year and throughout my life. I'd especially like to thank my parents and my big brother Bill, who was my first math teacher.

Finally, I'd like to thank my husband David who has been family, friend, and fellow graduate student to me. His help this past year has been invaluable, and I can't imagine having traversed this difficult road without it. I look forward to sharing many mathematical and non-mathematical pursuits in the years to come: I especially look forward to sharing an address again.

The figures in this thesis were drawn by Alexander R. Perlis, using Metapost. I am grateful for the financial support of the NSF, through Grant DMS9977116.

Table of Contents

Table of Contents—*Continued*

List of Tables

LIST OF FIGURES

Abstract

We define and study the *maximal crystalline subrepresentation functor*, $\mathrm{Crys}(-)$, defined on p-adic Galois representations of the absolute Galois group of a finite extension K of $\mathbb{Q}_p$. In particular, we define and study the derived functors, $R^i\,\mathrm{Crys}(-)$, of $\mathrm{Crys}(-)$.

We then apply these functors to the study of Néron models of abelian varieties defined over K. We extend a formula of Grothendieck expressing the component group of a Néron model in terms of Galois cohomology.

The extended formula is only valid for abelian varieties with semistable reduction defined over an unramified base. We explore the failure of the formula in the non-semistable case through the example furnished by Jacobians of Fermat curves.

Chapter 1. INTRODUCTION

1.1 Number Theory and Galois Representations

One way to study algebraic numbers is to study symmetry groups or *Galois groups* associated to them. By definition, an algebraic number α satisfies a polynomial equation with rational coefficients:

$$f(\alpha) = 0, \quad f(x) \in \mathbb{Q}[x].$$

The field obtained by adjoining to $\mathbb{Q}$ all the roots of the minimal such polynomial is a Galois extension of $\mathbb{Q}$ and we associate to α the Galois group of this extension. Properties of this Galois group translate into information about the number α. For example, if the Galois group associated to α is *abelian*, then α can be written as a finite sum

$$\sum_j a_j e^{2\pi i b_j}$$

with a_j and b_j rational numbers. This is the *Kronecker–Weber Theorem*, which asserts that every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension (i.e., an extension generated by roots of unity). For more on this theorem, see (for example) [Neu99, Chapter V], especially Theorem 1.10.

A convenient way to study the Galois groups associated to algebraic numbers is through their inverse limit

$$G_{\mathbb{Q}} := \varprojlim_K \mathrm{Gal}(K/\mathbb{Q})$$

where K runs over all finite extensions of $\mathbb{Q}$. This is the Galois group of the extension of $\mathbb{Q}$ obtained by adjoining *all* algebraic numbers. It is a huge and complicated group, encompassing information about *every* kind of algebraic number. In this sense, it seems quite unwieldy. But, it allows us to ask questions about certain classes of numbers in terms of group theory. For example, questions about all "abelian numbers" (i.e., all algebraic numbers whose associated Galois group is abelian) translate into questions about the maximal abelian quotient of $G_{\mathbb{Q}}$.

In studying $G_{\mathbb{Q}}$, one is naturally led to studying its representations

$$\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(R).$$

There is a natural topology on $G_{\mathbb{Q}}$, the *profinite topology*, arising from the structure of $G_{\mathbb{Q}}$ as an inverse limit of finite groups. As such, it is natural to consider coefficient spaces R which are also topological and to restrict to *continuous* representations. Such representations are usually called *Galois representations*. For example, R may be taken to be the complex numbers or the field of p-adic numbers. The coefficients need not be a field: for example, R could also be a complete local ring (such as the p-adic integers).

For a Galois representation $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(R)$, let L_ρ be the Galois extension of $\mathbb{Q}$ associated to the closed, normal subgroup $\ker\rho \subset G_{\mathbb{Q}}$ via the Galois correspondence for infinite extensions. The image of ρ is thus isomorphic to $\mathrm{Gal}(L_\rho/\mathbb{Q})$. Considering Galois representations with finite image thus leads us back to Galois groups associated to algebraic numbers.

1.2 Galois Representations arising from Geometry

The role of Galois representations in number theory is not limited to the study of $G_{\mathbb{Q}}$. These representations have played an important role in many recent advances in arithmetic geometry, such as the proof of Fermat's Last Theorem and the more general proof of the Shimura–Taniyama–Weil conjecture. This connection with arithmetic geometry stems from the fact that Galois representations arise naturally from algebro-geometric objects defined over arithmetically interesting bases, such as number fields or finite fields, and encode geometric information about these objects. To illustrate this, we shall now consider the example furnished by Tate modules of elliptic curves. Basic definitions and properties of elliptic curves are outlined below. See [Sil86] for more information.

1.2.1 Elliptic curves

Elliptic curves are non-singular projective curves that have a group structure. Over $\mathbb{Q}$, they can be given by Weierstrass equations of the form

$$E\colon y^2 = x^3 + Ax + B, \tag{1.1}$$

where $A, B \in \mathbb{Q}$ and $4A^3 + 27B^2 \neq 0$. The non-vanishing condition on the coefficients ensures that the resulting variety is non-singular. For K an extension of $\mathbb{Q}$, the K-*points of* E are the solutions of the above equation with coefficients in K, plus a "point at infinity" denoted O:

$$E(K) := \{(x_0, y_0) \in K \times K \mid y_0^2 = x_0^3 + Ax_0 + B\} \cup \{O\}.$$

The group structure on E gives rise to a group structure on each of these sets with O as the identity element; the conditions of non-singularity and projectivity force these group laws to be commutative. We briefly consider some examples for specific choices of K.

An example of the group of real points $E(\mathbb{R})$ is given in Figure 1.1 below. Also illustrated in the figure is the geometric interpretation of the group law on E, which is based on the demand that three collinear points should sum to zero. The sum of P and Q, denoted $P \oplus Q$, is defined to be the reflection about the x-axis of the third point of intersection of the line through P and Q with the curve $E(\mathbb{R})$.

The group $E(\mathbb{Q})$ is called the group of *rational points* of E. It is known to be a *finitely-generated* abelian group:

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus \text{Torsion}.$$

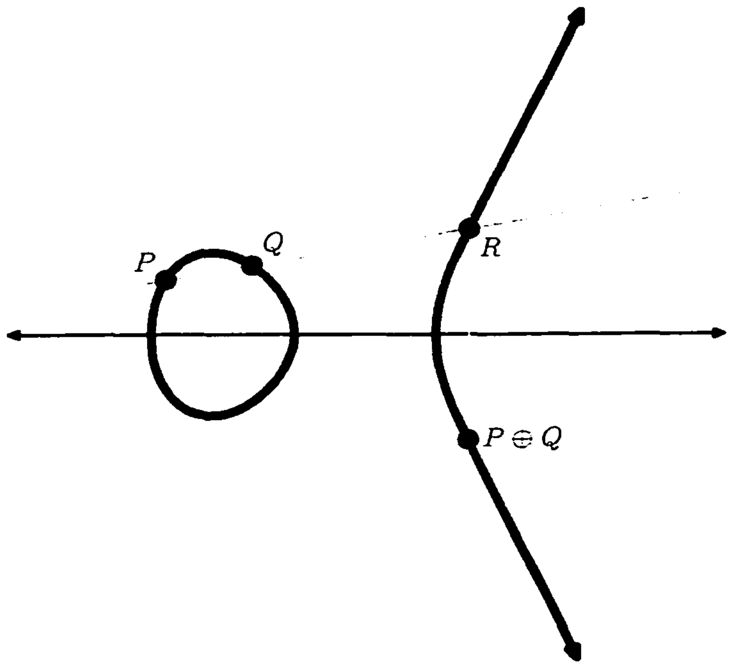

FIGURE 1.1. The real points of the elliptic curve given by $y^2 = x^3 - x$.

The torsion subgroup is known to come from a finite list of possibilities and there are methods available to determine its structure (see [Cre97, Section 3.3]); the rank r of E is more mysterious and is the subject of many open questions. For example, it is not known whether there exist elliptic curves over $\mathbb{Q}$ of arbitrarily large rank.

The group of complex points $E(\mathbb{C})$ is isomorphic to a complex torus, $\mathbb{C}/\Lambda$, where $\Lambda \cong \mathbb{Z}^2$ is a lattice in $\mathbb{C}$. The group law of $E(\mathbb{C})$ corresponds under this isomorphism to addition of complex numbers. One can easily describe the m-torsion points of $E(\mathbb{C})$, where m is a positive integer:

$$E(\mathbb{C})[m] \cong \left(\mathbb{C}/\Lambda\right)[m] = \tfrac{1}{m}\Lambda/\Lambda \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

We obtain the same result for the m-torsion of the $\overline{\mathbb{Q}}$-points (since the complex points of E are in fact algebraic):

$$E[m] := E(\overline{\mathbb{Q}})[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

It is sometimes convenient to also consider the "$\mathbb{F}_p$-points" of E, where $\mathbb{F}_p$ denotes the field with p elements for p a prime. This does not make sense since $\mathbb{F}_p$ is not an extension of $\mathbb{Q}$; what we really mean is to consider the $\mathbb{F}_p$-points of the "reduction of E modulo p", which we now describe. By making an appropriate change of coordinates, we can take the coefficients of the defining equation of E to be integers. Moreover, the integral coefficients can be chosen minimally, in a suitable sense. Then the *reduction of E modulo p* is the curve over $\mathbb{F}_p$ given by

$$\widetilde{E}_p\colon y^2 = x^3 + \overline{A}x + \overline{B}$$

where $\overline{A}$ and $\overline{B}$ denote the images of A and B in $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$. This curve may be singular since $4\overline{A}^3 + 27\overline{B}^2$ may vanish in $\mathbb{F}_p$; in this case, we do not have a group structure on the sets of points of $\widetilde{E}_p$. Let $\overline{\mathbb{F}}_p$ be an algebraic closure of $\mathbb{F}_p$. There are three possible reduction types:

1. E has *good reduction* at p if $\widetilde{E}_p(\overline{\mathbb{F}}_p)$ is non-singular. In this case, $\widetilde{E}_p$ is itself an elliptic curve, defined over $\mathbb{F}_p$.

2. E has *multiplicative bad reduction* at p if $\widetilde{E}_p(\overline{\mathbb{F}}_p)$ has a nodal singularity (see Figure 1.2 below).

3. E has *additive bad reduction* at p if $\widetilde{E}_p(\overline{\mathbb{F}}_p)$ has a cuspidal singularity (see Figure 1.2 below).

Even though there is no group structure on $\widetilde{E}_p(\overline{\mathbb{F}}_p)$ in the case of bad reduction, there is *always* a group structure on the set of non-singular points of $\widetilde{E}_p(\overline{\mathbb{F}}_p)$. The above terminology is explained by the fact that this group is isomorphic to the multiplicative (respectively, additive) group of $\overline{\mathbb{F}}_p$ when E has multiplicative (respectively, additive) bad reduction at p.

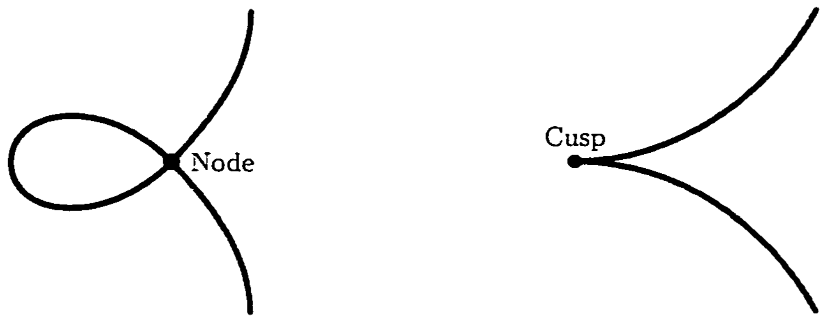

FIGURE 1.2. Multiplicative and Additive reduction

1.2.2 Galois representations arising from elliptic curves

Let ℓ be a prime number. The ℓ-power torsion subgroups $E[\ell^n]$ form an inverse system with respect to the multiplication-by-ℓ maps, $\ell\colon E[\ell^{n+1}] \to E[\ell^n]$. The inverse limit of this system, denoted $T_\ell E$, is called the *ℓ-adic Tate module* of E. By the description of the torsion subgroups in Section 1.2.1, we have an isomorphism of $T_\ell E$ with $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$, where $\mathbb{Z}_\ell$ denotes the ring of ℓ-adic integers.

Tate modules of elliptic curves give rise to Galois representations as follows. We consider the natural action of $G_{\mathbb{Q}}$ on the group of "geometric points" $E(\overline{\mathbb{Q}})$ given by:

$$\sigma(x, y) := \big(\sigma(x), \sigma(y)\big), \quad \sigma \in G_{\mathbb{Q}}.$$

The point $\big(\sigma(x), \sigma(y)\big)$ satisfies the defining equation of E (and hence lies in $E(\overline{\mathbb{Q}})$) since that equation has $\mathbb{Q}$-coefficients. The multiplication by ℓ^n maps are also defined over $\mathbb{Q}$, and so the Galois action commutes with multiplication by ℓ^n:

$$\ell^n\big(\sigma(x, y)\big) = \sigma\big(\ell^n(x, y)\big).$$

The action of $G_{\mathbb{Q}}$ on $E(\overline{\mathbb{Q}})$ thus restricts to an action on each of the $E[\ell^n]$. These actions give rise to an action on $T_\ell E$. The homomorphism giving this action

$$\rho_{E,\ell}\colon G_{\mathbb{Q}} \to \mathrm{Aut}(T_\ell E) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$$

is continuous for the natural topologies involved and is an example of an *ℓ-adic representation* of $G_{\mathbb{Q}}$.

We remark that the example of Galois representations arising from Tate modules of elliptic curves fits into a more general framework for constructing Galois representations from geometric objects. Representations often arise from the Galois action on *cohomology groups* associated to the geometric object. The representation on the ℓ-adic Tate module is *dual* to the representation on the first étale cohomology group of the elliptic curve.

1.2.3 Local properties

We now describe how "local properties" of the Tate module representations are related to "local properties" of the elliptic curve. For an elliptic curve E, "local" refers to behavior of the reduction of E modulo various primes p. For a representation $\rho_{E,\ell}$, "local" refers to the behavior of the restriction of $\rho_{E,\ell}$ to various local Galois groups, i.e., to fixed embeddings of $G_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ into $G_{\mathbb{Q}}$ for various primes p, where $\mathbb{Q}_p$ denotes the field of p-adic numbers and $\overline{\mathbb{Q}}_p$ an algebraic closure of $\mathbb{Q}_p$. For example, let I_p denote the inertia subgroup of $G_{\mathbb{Q}_p}$; that is, $I_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{ur})$, where $\mathbb{Q}_p^{ur}$ is the maximal unramified extension of $\mathbb{Q}_p$ in $\overline{\mathbb{Q}}_p$. The representation $\rho_{E,\ell}$ is said to be *unramified* at p if $\rho_{E,\ell}$ is trivial on I_p.

The following criterion of Néron–Ogg–Shafarevich is a beautiful example of this relationship (see [ST68, Theorem 1]):

$$E \text{ has good reduction at } p \iff \rho_{E,\ell} \text{ is unramified at } p \text{ for all } \ell \neq p.$$

The field extension $L_\ell = L_{\rho_{E,\ell}}$ associated to $\rho_{E,\ell}$ (see Section 1.1) is the extension of $\mathbb{Q}$ obtained by adjoining the coordinates of all ℓ-power torsion points of $E(\overline{\mathbb{Q}})$. The condition that $\rho_{E,\ell}$ be unramified at p is equivalent to p being unramified in the extension $L_\ell/\mathbb{Q}$, and we can rephrase the criterion as:

$$E \text{ has good reduction at } p \iff p \text{ is unramified in } L_\ell/\mathbb{Q}, \text{ for all } \ell \neq p.$$

There are similar representation-theoretic criteria for the other types of reduction as well.

This also highlights the fundamental difference between ℓ-adic ($\ell \neq p$) and p-adic representations of $G_{\mathbb{Q}_p}$. The Néron–Ogg–Shafarevich criterion is *false* for $\ell = p$: that is, $\rho_{E,p}$ may be *ramified* even though E has good reduction at p. In general, the p-adic representations of $G_{\mathbb{Q}_p}$ behave quite differently than their ℓ-adic counterparts and have a much richer structure. Their theory has been developed extensively by Fontaine, Messing, Faltings, and others. In particular, Fontaine's theory provides a p-adic analogue to *unramified* ℓ-adic representations in the notion of a *crystalline* representation. There is a p-adic version of the criterion of Néron–Ogg–Shafarevich (see [CI99, Part II, Theorem 4.7]):

$$E \text{ has good reduction at } p \iff \rho_{E,p} \text{ is crystalline at } p.$$

1.3 Galois representations and Néron Models

In this section, we explore another example of the difference between ℓ-adic ($\ell \neq p$) and p-adic representations of $G_{\mathbb{Q}_p}$, arising in the study of Néron models of abelian varieties.

1.3.1 Abelian varieties and Néron models

Much of the discussion of the previous section also holds for *abelian varieties*, the higher-dimensional analogues of elliptic curves. We will immediately focus on one prime by considering our abelian varieties defined over the p-adic numbers rather than $\mathbb{Q}$. Fix a prime p and consider an abelian variety A of dimension g defined over $\mathbb{Q}_p$.

When $g > 1$, we no longer have Weierstrass equations defining integral models of our variety; however, we do have a nice integral model, the *Néron model* of A, which allows us to consider the reduction of A modulo p. In Section 1.2.1, we saw that the reduction modulo p of the Weierstrass model of an elliptic curve may be singular and hence may not have a group structure; the reduction modulo p of the Néron model (denoted $\widetilde{A}_p$), on the other hand, is always non-singular and always has a group structure. However, this reduction may not be connected. Let $\widetilde{A}_p^0$ denote the connected component of the identity of $\widetilde{A}_p$ and Φ the group of connected components. The reduction $\widetilde{A}_p$ fits into the exact sequence:

$$0 \to \widetilde{A}_p^0 \to \widetilde{A}_p \to \Phi \to 0.$$

The $\overline{\mathbb{F}}_p$-points of the component group Φ form a finite abelian group. The component $\widetilde{A}_p^0$ is known to be an extension of an abelian variety B by a linear algebraic group L:

$$0 \to L \to \widetilde{A}_p^0 \to B \to 0.$$

Over $\overline{\mathbb{F}}_p$, L is a product of a torus T (a *multiplicative* group) and a unipotent group U (an *additive* group). The dimensions of U, T, and B sum to g and any combination is possible. Some specific situations include the following:

1. A has *good reduction* over $\mathbb{Z}_p$ if $\widetilde{A}_p^0$ is isomorphic to B. (In this case, the component group will be trivial and hence $\widetilde{A}_p$ is itself an abelian variety over $\mathbb{F}_p$.)

2. A has *multiplicative reduction* over $\mathbb{Z}_p$ if $\widetilde{A}_p^0$ is isomorphic to T.

3. A has *additive reduction* over $\mathbb{Z}_p$ if $\widetilde{A}_p^0$ is isomorphic to U.

In the elliptic curve case, we have only one dimension. Thus the connected component of the identity of the Néron model has only three possible structures: an elliptic curve, a multiplicative group, or an additive group. This is reminiscent of the

Weierstrass model situation. In fact, the connected component of the identity in the reduction modulo p of a Néron model of an elliptic curve $E/\mathbb{Q}_p$ is isomorphic to the non-singular locus of the reduction modulo p of a minimal Weierstrass model of E.

We can define the ℓ-adic Tate module of A as in the case of elliptic curves by

$$T_\ell A := \varprojlim A[\ell^n],$$

where $A[\ell^n]$ denotes the ℓ^n-torsion subgroup of $A(\overline{\mathbb{Q}}_p)$ and ℓ is a prime, possibly equal to p. In this case, the $A[\ell^n]$ are isomorphic to $(\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$ and for each ℓ, we obtain a representation

$$\rho_{A,\ell}\colon G_{\mathbb{Q}_p} \to \mathrm{Aut}(T_\ell A) \cong \mathrm{GL}_{2g}(\mathbb{Z}_\ell).$$

The analogues of the criterion of Néron–Ogg–Shafarevich and its p-adic version also hold in this case:

$$\begin{aligned} A \text{ has good reduction over } \mathbb{Z}_p \quad &\Longleftrightarrow \quad \rho_{A,\ell} \text{ is unramified at } p \text{ for all } \ell \neq p, \\ &\Longleftrightarrow \quad \rho_{A,p} \text{ is crystalline at } p. \end{aligned}$$

1.3.2 Grothendieck's formula and a p-complement

We have seen how the Tate module representations associated to an abelian variety $A/\mathbb{Q}_p$ relate to the structure of the identity component of the reduction modulo p of the Néron model of A. In [Gro72], Grothendieck explains how to relate these representations to the component group Φ. Let $\Phi(\ell)$ denote the ℓ-primary subgroup of the $\overline{\mathbb{F}}_p$-points of Φ; that is, $\Phi(\ell)$ is the subgroup of $\Phi(\overline{\mathbb{F}}_p)$ composed of elements of ℓ-power order. For a prime $\ell \neq p$, Grothendieck relates $\Phi(\ell)$ to the first Galois cohomology group (with respect to inertia) of the ℓ-adic Tate module. He proves (page 135, [Gro72])

$$\Phi(\ell) \cong \mathrm{H}^1(I_p, T_\ell A)_{\mathrm{tors}},$$

where I_p denotes the inertia subgroup of $G_{\mathbb{Q}_p}$ and the subscript "tors" indicates the torsion subgroup.

This formula does not hold for $\ell = p$; the Galois cohomology of T_pA is not "large enough" for the p-primary subgroup of Φ. In [KM00], we give an analogous cohomological formula for the p-primary subgroup of Φ. The crucial idea is to view the inertia invariants functor as picking out the *maximal unramified subrepresentation* of a given representation. The obvious candidate for a p-adic analogue of this is the functor picking out the *maximal crystalline subrepresentation*. Its right-derived functors $R^i\,\mathrm{Crys}(-)$ then play the p-adic role of Galois cohomology with respect to inertia. In the case of semistable abelian varieties, i.e., for abelian varieties for which $U = 0$ (see Section 1.3.1), we have

$$\Phi(p) \cong R^1\,\mathrm{Crys}(T_pA)_{\mathrm{tors}}.$$

The main purpose of this dissertation is to develop the theory of these functors, as well as to explore the situation when A has non-semistable reduction.

1.4 Synopsis of Chapters

Let p be a fixed prime and let K be a finite extension of $\mathbb{Q}_p$. Let $\overline{K}$ denote a fixed algebraic closure of K and let $G_K := \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K. A $\mathbb{Q}_p$*-representation* of G_K is a finite-dimensional $\mathbb{Q}_p$-vector space V on which G_K acts linearly and continuously. In Chapter 2, we review the definition and basic properties of a *crystalline* $\mathbb{Q}_p$-representation of G_K, as defined by Fontaine. However, in order to apply the notion of a "maximal crystalline subrepresentation functor" to Néron models of abelian varieties defined over K, we need a notion of crystalline in a wider context. In particular, we define the notion of crystalline for discrete G_K-modules, as well as finitely-generated $\mathbb{Z}_p$-modules on which G_K acts linearly and continuously (see Definitions 2.4, 2.5, and 2.6.) We remark that our definitions differ from those of [KM00]; in particular, they do not require us to restrict to K unramified over $\mathbb{Q}_p$.

In Section 2.3, we review the homological algebra necessary to define "derived functors" of the maximal crystalline subrepresentation functor. We use a technique of Jannsen, which he applied to define continuous étale cohomology in [Jan88].

In Chapter 3, we define the *maximal crystalline subrepresentation functor*, denoted $\mathrm{Crys}(-)$. We also define the $R^i\,\mathrm{Crys}(-)$, as right-derived functors of $\mathrm{Crys}(-)$ where possible and using the technique of Jannsen otherwise (see Section 3.2). We then study basic functorial properties of the $R^i\,\mathrm{Crys}(-)$. For example, in Section 3.3, we show the existence of a long-exact sequence:

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Crys}(M) \arrow[r] & \mathrm{Crys}(M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \arrow[r] & \mathrm{Crys}(M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p) \arrow[dll, rounded corners] \\ & R^1\,\mathrm{Crys}(M) \arrow[r] & R^1\,\mathrm{Crys}(M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \arrow[r] & R^1\,\mathrm{Crys}(M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p) \arrow[r] & \cdots \end{tikzcd}$$

when M is a free, finite-rank $\mathbb{Z}_p$-module with linear and continuous G_K-action; see Proposition 3.2. In Section 3.4, we exhibit a spectral sequence relating the $R^i\,\mathrm{Crys}(-)$ to Galois cohomology.

In Chapter 4, we discuss applications of these functors to component groups of Néron models. After a review of Néron models in Section 4.1, we prove in Section 4.2 the formulae stated in Section 1.3.2 for the ℓ-primary part $\Phi(\ell)$ of the component group of a Néron model associated to an abelian variety A defined over K. In order to prove the formula

$$\Phi(p) \cong R^1\,\mathrm{Crys}(T_pA)_{\mathrm{tors}},$$

we must restrict to K unramified over $\mathbb{Q}_p$, $p \neq 2$, and A semistable. In Section 4.3, we explore these restrictions. In particular, we consider the example furnished by Jacobians of Fermat curves to study the situation in the non-semistable case.

Chapter 2. GALOIS REPRESENTATIONS

In Section 2.1, we fix notation and define the notion of a p-adic Galois representation. We then define *crystalline* p-adic Galois representations in Section 2.2. Finally, in Section 2.3, we summarize the necessary facts from homological algebra that will be needed in Chapter 3.

2.1 Definitions and Notations

Let p be a prime number, and let $\mathbb{Q}_p$ and $\mathbb{Z}_p$ denote the field of p-adic numbers and the ring of p-adic integers, respectively. Let K be a fixed finite extension of $\mathbb{Q}_p$, with ring of integers $\mathcal{O}_K$ and residue field k. Let $\overline{K}$ denote a fixed algebraic closure of K and let K^{ur} denote the maximal unramified subextension of $\overline{K}/K$. These extensions have the same residue field, denoted $\overline{k}$, which is an algebraic closure of k. For any algebraic extension L of K, denote the ring of integers of L by $\mathcal{O}_L$. For example, $\mathcal{O}_{\overline{K}}$ is the ring of integers of $\overline{K}$.

Let $G := \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K and let $I := \mathrm{Gal}(\overline{K}/K^{ur})$ be the inertia subgroup of G. The group G is a profinite group:

$$G \cong \varprojlim_{L/K} \mathrm{Gal}(L/K),$$

where L runs over all finite Galois extensions of K. As such, G has a natural topology, the *profinite* topology, making G a compact, totally disconnected topological group.

Throughout this paper, we will be interested in objects on which G acts. For example, an *abstract G-module* is an abelian group equipped with a linear action of G. The category of abstract G-modules is equivalent to the category of modules over the group ring $\mathbb{Z}[G]$.

Since G is a topological group, it is natural to consider G-modules that also have a topological structure. A *topological G-module* is an abelian topological group equipped with a continuous, linear action of G. A *discrete G-module* is a topological G-module whose topology is discrete. For any topological G-module V, the continuous action of G gives rise to a continuous homomorphism

$$\rho: G \longrightarrow \mathrm{Aut}(V).$$

We often refer to topological G-modules as *representations* of G (which is perhaps an abuse of terminology).

Suppose M is an abstract G-module. One can consider M as a topological group by giving it the discrete topology. The action of G will be continuous for the discrete topology on M if and only if the following equivalent properties hold:

(a) For every $m \in M$, the stabilizer $\mathrm{Stab}_m(G) := \{g \in G \mid g \cdot m = m\}$ is an open subgroup of G.

(b) $M = \bigcup M^U$, where U runs through the open subgroups of G and $M^U = \{m \in M \mid u \cdot m = m, \ \forall u \in U\}$.

Let ℓ be a prime number (possibly equal to p). An *ℓ-adic representation* of G is a topological G-module V, where V also has the structure of a $\mathbb{Z}_\ell$-module and the module structure is compatible with the topological structure. (That is, we require the scalar multiplication morphism $\mathbb{Z}_\ell \times V \to V$ to be continuous, where $\mathbb{Z}_\ell$ is given the usual topology.) We are particularly interested in *p-adic representations* of G (i.e., in the case $\ell = p$). We denote the abelian category of p-adic representations of G by $\mathbf{Rep(G)}$. The morphisms are continuous $\mathbb{Z}_p$-module homomorphisms that commute with the G-action of the representations. From now on, we will write "representation" to mean "p-adic representations of G", unless explicitly stated otherwise. We describe below various types of representations that will play a large role in what follows.

A *discrete* representation is a representation whose underlying topological group structure is discrete. The category of discrete representations will be denoted by $\mathbf{Mod(G)}$. It is an abelian category, where kernels and cokernels of morphisms are kernels and cokernels as $\mathbb{Z}_p$-module homomorphisms. A *discrete torsion representation* is a discrete representation whose underlying $\mathbb{Z}_p$-module is torsion. The category of discrete torsion representations, also abelian, will be denoted by $\mathbf{Mod_t(G)}$.

Example 2.1. Consider $\mathbb{Q}_p/\mathbb{Z}_p$ as a representation by equipping it with trivial G-action. Then $\mathbb{Q}_p/\mathbb{Z}_p$ is a discrete torsion representation.

A $\mathbb{Q}_p$*-representation* is a representation whose underlying $\mathbb{Z}_p$-module has the structure of a finite-dimensional $\mathbb{Q}_p$-vector space. Given a finite-dimensional $\mathbb{Q}_p$-vector space V, there is a unique topological structure on V for which the vector space structure is compatible with the usual topology on $\mathbb{Q}_p$. The category of $\mathbb{Q}_p$-representations will be denoted by $\mathbf{Rep}_{\mathbb{Q}_p}\mathbf{(G)}$. Since any $\mathbb{Q}_p$-linear map between topological $\mathbb{Q}_p$-vector spaces is continuous, the morphisms are $\mathbb{Q}_p$-vector space maps commuting with the G-action. This is an abelian category, with various linear algebra constructions available. Given V and W in $\mathbf{Rep}_{\mathbb{Q}_p}\mathbf{(G)}$, we can form the $\mathbb{Q}_p$-representations $V \oplus W$, $V \otimes_{\mathbb{Q}_p} W$, and $V^* = \mathrm{Hom}_{\mathbb{Q}_p}(V, \mathbb{Q}_p)$, where the underlying vector spaces are given by the usual definitions and the G-actions are given by:

$$\begin{aligned} g \cdot (v, w) &= (g \cdot v, g \cdot w), \\ g \cdot v \otimes w &= g \cdot v \otimes g \cdot w, \\ g \cdot \phi(v) &= \phi(g \cdot v), \end{aligned}$$

for all $g \in G$ and for all $v \in V$, $w \in W$, and $\phi \in V^*$.

Remark. We warn the reader that our terminology is not consistent with some of the literature, where "p-adic representation" often refers to what we call a $\mathbb{Q}_p$-representation.

A $\mathbb{Z}_p$*-representation* is a representation whose underlying $\mathbb{Z}_p$-module is of finite-type (that is, finitely-generated as a module). We will denote the category of $\mathbb{Z}_p$-

representations by $\mathbf{Rep}_{\mathbb{Z}_p}(\mathbf{G})$, where morphisms are $\mathbb{Z}_p$-module homomorphisms commuting with the G-action. This is an abelian category with various linear algebra constructions available, as in the $\mathbb{Q}_p$-representation case. If M and N lie in $\mathbf{Rep}_{\mathbb{Z}_p}(\mathbf{G})$, we can form the $\mathbb{Z}_p$-representations $M \oplus N$, $M \otimes_{\mathbb{Z}_p} N$, and $M^* = \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Z}_p)$ as indicated above.

A *finite-length* representation is a representation whose underlying $\mathbb{Z}_p$-module is of finite-length. These are exactly the *torsion $\mathbb{Z}_p$-representations* and hence their underlying $\mathbb{Z}_p$-module structure is actually finite. (We call them finite-length rather than finite to avoid confusion with another possible definition for the phrase "finite representation".) We will denote by $\mathbf{Rep}_{\mathbb{Z}_p,\mathbf{t}}(\mathbf{G})$ the abelian category of finite-length representations.

See Table 2.1 below for a quick reference of the different categories of representations defined above.

Category name	*Description of objects*
$\mathbf{Mod}(\mathbf{G})$	discrete $\mathbb{Z}_p$-modules with continuous, linear G-action
$\mathbf{Mod}_{\mathbf{t}}(\mathbf{G})$	discrete torsion $\mathbb{Z}_p$-modules with continuous, linear G-action
$\mathbf{Rep}(\mathbf{G})$	topological $\mathbb{Z}_p$-modules with continuous, linear G-action
$\mathbf{Rep}_{\mathbb{Q}_p}(\mathbf{G})$	finite-dimensional $\mathbb{Q}_p$-vector spaces with continuous, linear G-action; called $\mathbb{Q}_p$-representations
$\mathbf{Rep}_{\mathbb{Z}_p}(\mathbf{G})$	finite-type $\mathbb{Z}_p$-modules with continuous, linear G-action; called $\mathbb{Z}_p$-representations
$\mathbf{Rep}_{\mathbb{Z}_p,\mathbf{t}}(\mathbf{G})$	finite torsion $\mathbb{Z}_p$-modules with continuous, linear G-action; called finite-length representations

TABLE 2.1. Table of categories of representations

Example 2.2. Consider $\mathbb{Z}/p^n\mathbb{Z}$ (for fixed $n \geq 1$), $\mathbb{Z}_p$, and $\mathbb{Q}_p$ as representations with trivial G-action. These are examples of finite-length, $\mathbb{Z}_p$-, and $\mathbb{Q}_p$-representations, respectively.

Example 2.3. Let μ_{p^n} denote the group of p^nth roots of unity in $\overline{K}$. The natural action of G transforms these groups into finite-length representations. We can obtain a $\mathbb{Z}_p$-representation from these by defining $\mathbb{Z}_p(1) := \varprojlim_{n\in\mathbb{N}} \mu_{p^n}$, where the limit is taken with respect to the p-power maps, $\zeta \mapsto \zeta^p$. The homomorphism giving the action of G on $\mathbb{Z}_p(1)$

$$\chi \colon G \longrightarrow \operatorname{Aut}(\mathbb{Z}_p(1)) \cong \mathbb{Z}_p^\times$$

(where $\mathbb{Z}_p^\times$ denotes the units of $\mathbb{Z}_p$) is usually referred to as the *cyclotomic character* of G. It is often convenient to consider the $\mathbb{Q}_p$-representation $\mathbb{Z}_p(1) := \mathbb{Z}_p(1) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ as well.

Example 2.4. Let A be an abelian variety defined over K. The natural G-action on the p^n-torsion points $A[p^n]$ of $A(\overline{K})$ gives rise to finite-length representations. As in Example 2.3, we obtain a $\mathbb{Z}_p$-representation, $T_pA := \varprojlim_{n\in\mathbb{N}} A[p^n]$, which in turn gives rise to a $\mathbb{Q}_p$-representation, $T_pA \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. (See Sections 1.2.2 and 1.3.1 for more details.)

2.2 Crystalline Galois representations

In this section, we define the notion of a crystalline representation in the general context of p-adic representations (in particular, we define crystalline for discrete and $\mathbb{Z}_p$-representations). In Section 2.2.1, we begin by reviewing the definitions and basic properties in the $\mathbb{Q}_p$-representation case. Then in Section 2.2.2, we extend the definition to all p-adic representations.

2.2.1 Crystalline $\mathbb{Q}_p$-representations

The definition of a *crystalline* $\mathbb{Q}_p$-representation fits into a more general framework designed by Fontaine to pick out certain classes of representations from the full category $\mathbf{Rep}_{\mathbb{Q}_p}(\mathbf{G})$. The motivation for these definitions originates in geometry and the notion of crystalline is the representation-theoretic analogue of good reduction. That is, representations arising from varieties with good reduction are crystalline (see Examples 2.7 and 2.8 below). The basic idea of the definition is to attach to a representation V a purely algebraic object $D_{crys}(V)$ (see below). The representation V is "crystalline" if V and $D_{crys}(V)$ have the same dimension. By attaching different purely algebraic objects to V, one can define other types of representations. We will restrict our discussion to the crystalline case. The definitions are quite technical, and we give an overview below. See the original papers of Fontaine [Fon79, Fon82, Fon94a, Fon94b] for more detailed information.

We will need to consider a subextension K_0 of $K/\mathbb{Q}_p$ with the property that K_0 is an unramified extension of $\mathbb{Q}_p$ with residue field k. These properties determine K_0 up to isomorphism. For example, we may take K_0 to be the fraction field of the ring $W(k)$ of Witt vectors with coefficients in k (see [Ser79, Chapter II, Sections 5 and 6]). In particular, the Frobenius morphism $x \mapsto x^p$ on k lifts uniquely to an automorphism of $W(k)$, which in turn gives rise to an automorphism of K_0. We denote these automorphisms all by σ and refer to them as the *Frobenius* on k, K_0, or $W(k)$.

The purely algebraic object $D_{crys}(V)$ is a "filtered K_0-module", as described below.

Definition 2.1. A *filtered K_0-module* is a finite-dimensional K_0-vector space D equipped with

(i) a bijective map $F\colon D \to D$ that is σ-semilinear: that is, $F(\lambda d) = \sigma(\lambda)F(d)$, for all $\lambda \in K_0$ and $d \in D$);

(ii) a filtration $(D_K^i)_{i\in\mathbb{Z}}$ of $D_K := D \otimes_{K_0} K$ by K-subspaces that is decreasing, separated, and exhaustive; that is, for all $i \in \mathbb{Z}$, $D_K^{i+1} \subset D_K^i$, $\bigcap_{i\in\mathbb{Z}} D_K^i = 0$, and $\bigcup_{i\in\mathbb{Z}} D_K^i = D_K$.

The map F is usually referred to as "a Frobenius" on D. We denote the category of filtered K_0-modules by $\mathbf{MF_K}$, where the morphisms are K_0-vector space morphisms that commute with F and (after extending scalars to K) respect the filtration. For more details on filtered modules, see [Fon79, Section 1.2], for example.

In order to attach a filtered K_0-module to a representation V, we use the K_0-algebra "B_{crys}". On the one hand, B_{crys} is a p-adic representation of $G = \mathrm{Gal}(\overline{K}/K)$, with G-invariants $(B_{crys})^G = \{b \in B_{crys} \mid g \cdot b = b, \forall g \in G\}$ equal to K_0. On the other hand, it has the structure of a filtered K_0-module. That is, it has a σ-semilinear Frobenius $F\colon B_{crys} \to B_{crys}$ as well as a decreasing, separated, and exhaustive filtration of $B_{crys} \otimes_{K_0} K$. These two structures are compatible with each other (i.e., the automorphisms induced by the action of G on B_{crys} are *filtered module* automorphisms) and B_{crys} provides a bridge between the world of p-adic representations of G and that of filtered K_0-modules. See [Fon82] and [Fon94a] for details on the construction of B_{crys}.

Given a $\mathbb{Q}_p$-representation V, define:

$$D_{crys}(V) := (B_{crys} \otimes_{\mathbb{Q}_p} V)^G.$$

$D_{crys}(V)$ is a filtered K_0-module; it inherits its Frobenius and filtration from that of B_{crys}. Moreover, its dimension as a K_0-vector space is known to be less than or equal to the dimension of V as a $\mathbb{Q}_p$-vector space [Fon79, Proposition 3.2.1].

Definition 2.2. A $\mathbb{Q}_p$-representation V is *crystalline* if

$$\dim_{\mathbb{Q}_p} V = \dim_{K_0} D_{crys}(V).$$

We denote the category of crystalline $\mathbb{Q}_p$-representations by $\mathbf{Rep}_{\mathbb{Q}_p,\mathbf{crys}}(\mathbf{G})$. It is an abelian, strictly full subcategory of $\mathbf{Rep}_{\mathbb{Q}_p}(\mathbf{G})$, which is stable under subobject, quotient, direct sum, dual and tensor product [Fon79, Section 3.4].

The correspondence $V \rightsquigarrow D_{crys}(V)$ defines a functor from $\mathbf{Rep}_{\mathbb{Q}_p}(\mathbf{G})$ to the category of filtered K_0-modules. Its restriction to the crystalline $\mathbb{Q}_p$-representations is an exact, fully-faithful functor [Fon79, Proposition 3.4.1], and induces an equivalence between $\mathbf{Rep}_{\mathbb{Q}_p,\mathbf{crys}}(\mathbf{G})$ and the essential image of D_{crys} [Fon79, Theorem 3.6.5]. A long-conjectured concrete description of this image as "weakly admissible" filtered modules has recently been given by Colmez and Fontaine [CF00].

Example 2.5. Suppose V is a $\mathbb{Q}_p$-representation with trivial G-action. Then it follows easily from the definition that V is crystalline.

Example 2.6. A $\mathbb{Q}_p$-representation V is *unramified* if the inertia subgroup $I \subset G$ acts trivially on V. Unramified $\mathbb{Q}_p$-representations are crystalline [Fon79, Proposition 3.3.1].

Example 2.7. Let A be an abelian variety defined over K. The associated $\mathbb{Q}_p$-representation $T_pA \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is crystalline if and only if A has good reduction. (The "if" follows from Theorem A, page 183 of [FM87]; the "only if" is Theorem 4.7, page 201 of [CI99].)

Example 2.8. Let X be a smooth, proper variety defined over K having good reduction (i.e., for which there exists a smooth, proper model $\mathcal{X}$ over $\mathcal{O}_K$). Then the ith étale cohomology group $\mathrm{H}^i_{\acute{e}t}(X_{\overline{K}}, \mathbb{Q}_p)$ is crystalline for all $i \geq 0$. Moreover,

$$D_{crys}\big(\mathrm{H}^i_{\acute{e}t}(X_{\overline{K}}, \mathbb{Q}_p)\big) \cong \mathrm{H}^i_{crys}(\mathcal{X}_k) \otimes_W K_0,$$

where $\mathrm{H}^i_{crys}(\mathcal{X}_k)$ denotes the ith crystalline cohomology group of the special fiber of $\mathcal{X}$. (This is proved in Faltings [Fal89], extending results of [FM87]).

Example 2.9. Let $\mathcal{G}$ be a Barsotti–Tate group (also known as a p-divisible group) defined over $\mathcal{O}_K$ (see [Tat67]). The associated Tate module representation $T_p(\mathcal{G}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is crystalline and $D_{crys}\big(T_p(\mathcal{G}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p\big)$ is the Dieudonné module of the special fiber of $\mathcal{G}$ [Fon79, Fon82].

Remark 2.1. The theory of crystalline representations stems from Example 2.9. See the introduction of [Fon79].

We will also need the notion of an "h-crystalline" $\mathbb{Q}_p$-representation.

Definition 2.3. Let V be a $\mathbb{Q}_p$-representation and let $D = D_{crys}(V)$. For a non-negative integer h, we say V is *h-crystalline* if V is crystalline and $D_K^i/D_K^{i+1} = 0$ for all i not in the interval $[0, h]$.

Remark 2.2. This is equivalent to V being crystalline with Hodge–Tate weights in the interval $[0, h]$ (see [Fon79, Corollary, page 23]).

If V is an h-crystalline representation and $D = D_{crys}(V)$, then D_K has filtration length less than or equal to h; moreover $D_K^0 = D_K$ and $D_K^{h+1} = 0$.

Proposition 2.1. *Let*

$$0 \longrightarrow V_1 \longrightarrow V_2 \longrightarrow V_3 \longrightarrow 0$$

be a short exact sequence of $\mathbb{Q}_p$-representations and let h be a non-negative integer.

(i) If V_2 is h-crystalline, then V_1 and V_3 are also h-crystalline.

(ii) If V_1 and V_3 are h-crystalline and V_2 is crystalline, then V_2 is in fact h-crystalline.

Proof. In the first statement, we know that V_1 and V_3 are crystalline by the stability of $\mathbf{Rep}_{\mathbb{Q}_p,\mathbf{crys}}(\mathbf{G})$ under subobject and quotient. Let $D_j = D_{crys}(V_j)$ for $j = 1, 2$, and 3. Since D_{crys} is an exact functor on crystalline representations, we have in both statements an exact sequence of filtered modules (see [Fon79, Paragraph 1.2.3]):

$$0 \longrightarrow D_1 \longrightarrow D_2 \longrightarrow D_3 \longrightarrow 0.$$

In particular, we have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & D_1^{i+1} & \longrightarrow & D_2^{i+1} & \longrightarrow & D_3^{i+1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & D_1^{i} & \longrightarrow & D_2^{i} & \longrightarrow & D_3^{i} & \longrightarrow & 0.
\end{array}$$

Both statements then follow from the Snake Lemma. $\square$

We denote the strictly full subcategory of $\mathbf{Rep}_{\mathbb{Q}_p,\mathbf{crys}}(\mathbf{G})$ consisting of h-crystalline $\mathbb{Q}_p$-representations by $\mathbf{Rep}^{h}_{\mathbb{Q}_p,\mathbf{crys}}(\mathbf{G})$. By Proposition 2.1, it is stable under subobject, quotient, and direct sum (and is thus an abelian category).

The category of h-crystalline representations is not stable under tensor product or duals. For example, if V is h-crystalline and W is h'-crystalline, then $V \otimes_{\mathbb{Q}_p} W$ is $(h+h')$-crystalline. This follows from the fact that $D_{crys}(V \otimes_{\mathbb{Q}_p} W) = D_{crys}(V) \otimes D_{crys}(W)$ (where the tensor product is taken in the category of filtered modules), and the filtration of $(D_1 \otimes D_2)_K$ for any D_1 and D_2 in $\mathbf{MF_K}$ is given by

$$(D_1 \otimes D_2)^i_K = \sum_{j+k=i} (D_1)^j_K \otimes (D_2)^k_K$$

for all $i \in \mathbb{Z}$.

Example 2.10. Unramified $\mathbb{Q}_p$-representations are 0-crystalline (see [Fon79, Remark 3.3.4]).

Example 2.11. Let $\mathcal{G}$ be a Barsotti-Tate group defined over $\mathcal{O}_K$ (see also Example 2.9). Then the Tate module representation $T_p(\mathcal{G}) \otimes \mathbb{Q}_p$ is 1-crystalline.

2.2.2 Crystalline p-adic representations

To define the notion of a crystalline representation in general, we first define crystalline finite-length representations in terms of crystalline $\mathbb{Q}_p$-representations and then extend the definition to arbitrary representations using limits. These definitions may seem a little arbitrary at first glance, but they allow us to discuss the notion of crystalline compatibly across the different types of representations and they allow us to use the technique of Jannsen discussed in Section 2.3.4. We say a finite-length representation T is a *subquotient* of a $\mathbb{Q}_p$-representation V if a subrepresentation $M \subset V$ surjects onto T. In that case, M must be a free $\mathbb{Z}_p$-representation (i.e., a $\mathbb{Z}_p$-representation whose underlying $\mathbb{Z}_p$-module is free).

Definition 2.4. A finite-length representation is *crystalline* if it is a subquotient of a crystalline $\mathbb{Q}_p$-representation.

The property of crystalline for finite-length representations is stable under subobject, quotient, and direct sum. This follows from the similar statement for crystalline $\mathbb{Q}_p$-representations. For example, suppose $V_1 \to V_2$ is a surjective map of finite-length representations with V_1 crystalline, i.e., V_1 is a subquotient of a crystalline $\mathbb{Q}_p$-representation W:

$$\begin{tikzcd} U \arrow[r, hook] \arrow[d, two heads] & W \\ V_1 \arrow[r, two heads] & V_2 \end{tikzcd}$$

Clearly V_2 is also a subquotient of W and hence crystalline as well. We denote the abelian category of crystalline finite-length representations by $\mathbf{Rep}_{\mathbb{Z}_p,\mathbf{t},\mathbf{crys}}(\mathbf{G})$.

Definition 2.5. A discrete representation is *crystalline* if it is the direct limit of finite-length crystalline representations.

The property of crystalline for discrete representations is stable under subobject, quotient, and direct sum. This follows from the similar statement for finite-length representations and from the properties of the direct limit. For example, let $W \subset V$ be discrete representations with V crystalline, that is, $V \cong \varinjlim V_i$, where the V_i are finite-length crystalline representations. Then, $W \cong \varinjlim f_i^{-1}(W)$, where the $f_i\colon V_i \to V$ are the maps given by the definition of the direct limit. We denote the abelian category of crystalline discrete representations by $\mathbf{Mod}_{\mathbf{crys}}(\mathbf{G})$. We will also consider the abelian category of crystalline discrete torsion representations, $\mathbf{Mod}_{\mathbf{t},\mathbf{crys}}(\mathbf{G})$.

Definition 2.6. An arbitrary representation is *crystalline* if it is an inverse limit of discrete crystalline representations, where the topology is given by the inverse limit.

Once again, the property of crystalline is stable under subobject, quotient, and direct sum. The category of crystalline representations will be denoted by $\mathbf{Rep}_{\mathbf{crys}}(\mathbf{G})$.

We now consider what these definitions mean in the specific cases of $\mathbb{Z}_p$-representations and $\mathbb{Q}_p$-representations.

Proposition 2.2. *Suppose M is a $\mathbb{Z}_p$-representation. Then*

(i) M is crystalline if and only if M is an inverse limit of finite-length crystalline representations.

(ii) M is crystalline if and only if M/p^nM is crystalline for all $n \geq 1$.

Proof. For statement (i), first suppose M is an inverse limit of crystalline finite-length representations. Then, in particular, M is an inverse limit of crystalline *discrete* representations and is crystalline by definition. For the other direction, suppose $M \cong \varprojlim M_n$, where the M_n are crystalline discrete representations. Let $f_n\colon M \to M_n$ be the projection maps given by the inverse limit. Then, $M \cong \varprojlim f_n(M)$ and moreover, the images $f_n(M)$ are crystalline *finite-length* representations. This follows from the fact that these images are compact *and* discrete, and hence finite.

For the second statement, first suppose M/p^nM is crystalline for all $n \geq 1$. Then $M \cong \varprojlim_{n\in\mathbb{N}} M/p^nM$ is crystalline by definition.

For the other direction, suppose M is crystalline. Then, by the first statement, $M \cong \varprojlim_{m\in\mathbb{N}} M_m$, where the M_m are crystalline finite-length representations. We may assume the projection maps $\phi_m\colon M \to M_m$ are surjective; otherwise, replace M_m by the image of ϕ_m. Let K_m denote the kernel of ϕ_m. Then for each $n \geq 1$, p^nM contains K_m for some m, since p^nM is open and the K_m form a base for the topology of M. Hence, the map $M \to M/p^nM$ factors through M_m, inducing a surjection $M_m \to M/p^nM$. This implies M/p^nM is crystalline. □

We now have two definitions for crystalline $\mathbb{Q}_p$-representations. These definitions are in fact equivalent.

Proposition 2.3. *Let V be a $\mathbb{Q}_p$-representation. Then V is crystalline in the sense of Section 2.2.1 if and only if V is crystalline in the sense of Definition 2.6.*

Proof. Suppose V is crystalline in the sense of Section 2.2.1. Let $L \subset V$ be a G-invariant lattice, guaranteed to exist by the compactness of G, and write V as

$$V \cong \varprojlim_{\mathbb{N}} (L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p),$$

where the inverse limit is taken with respect to the multiplication by p maps

$$L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\ p\ } L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p.$$

Since

$$L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \cong \varinjlim (L \otimes_{\mathbb{Z}_p} \tfrac{1}{p^n}\mathbb{Z}_p/\mathbb{Z}_p) \cong \varinjlim L/p^n L,$$

is crystalline, V is also crystalline in the sense of Definition 2.6.

For the other direction, suppose V is crystalline in the sense of Definition 2.6; that is, suppose $V \cong \varprojlim V_n$, where each V_n is a crystalline discrete representation. Let $L \subset V$ be a G-invariant lattice. Then, $L \cong \varprojlim L_n$, where $L_n := f_n(L)$ and $f_n \colon V \to V_n$ is the canonical projection. Each L_n is in fact a finite-length crystalline representation, i.e., a subquotient of a crystalline (in the sense of Section 2.2.1) $\mathbb{Q}_p$-representation. This implies that L itself is crystalline and hence by Proposition 2.2, we can take the L_n to be $L/p^n L$. Let W_n denote the crystalline (in the sense of Section 2.2.1) $\mathbb{Q}_p$-representation for which $L/p^n L$ is a subquotient and denote by U_n the free $\mathbb{Z}_p$-submodule of W_n surjecting onto $L/p^n L$:

$$\begin{tikzcd}
\cdots \arrow[r] & L/p^{n+1}L \arrow[r, "d_n"] & L/p^n L \arrow[r] & \cdots \arrow[r, "d_2"] & L/p^2 L \arrow[r, "d_1"] & L/pL \\
\cdots & U_{n+1} \arrow[u] & U_n \arrow[u, "f_n"] & \cdots & U_2 \arrow[u, "f_2"] & U_1 \arrow[u, "f_1"]
\end{tikzcd}$$

We may assume that, for all n, $\mathrm{rank}_{\mathbb{Z}_p} U_n = \mathrm{rank}_{\mathbb{Z}_p} L = \dim_{\mathbb{Q}_p} V$. Indeed, since U_n surjects onto $L/p^n L$, we have $\mathrm{rank}_{\mathbb{Z}_p} U_n \geq \mathrm{rank}_{\mathbb{Z}_p} L$. If the rank is strictly larger, we may replace U_n by the subrepresentation generated by a set of lifts of generators of $L/p^n L$.

A priori, there is no relationship between the U_n; however, we can make the following adjustment. Define

$$U_2' := \{(x, y) \in U_1 \times U_2 \mid f_1(x) = d_1(f_2(y))\},$$

where d_1 and f_1 are as in the above diagram. Then, U_2' is contained in the crystalline (in the sense of Section 2.2.1) $\mathbb{Q}_p$-representation $W_1 \times W_2$ and U_2' surjects onto L/p^2L. Furthermore, U_2' surjects onto U_1, and we may assume that $\operatorname{rank}_{\mathbb{Z}_p} U_2' = \operatorname{rank}_{\mathbb{Z}_p} L$. If the rank is strictly larger, replace U_2' by the subrepresentation generated by a set of lifts of generators of L/p^2L. We claim that we still have a surjection onto U_1. Indeed, this new U_2' will surject onto L/pL, which is isomorphic to U_1/pU_1 by rank considerations, and hence by Nakayama's Lemma also surjects onto U_1. Similarly, we can inductively define $U_n' \subset U_n \times U_{n-1}'$ and obtain a system of U_n' with surjective maps $U_{n+1}' \to U_n$, for all n (we let $U_1' = U_1$):

$$\begin{tikzcd}
\cdots \arrow[r] & L/p^{n+1}L \arrow[r, "d_n"] & L/p^nL \arrow[r] & \cdots \arrow[r, "d_2"] & L/p^2L \arrow[r, "d_1"] & L/pL \\
\cdots \arrow[r] & U_{n+1}' \arrow[u] \arrow[r] & U_n' \arrow[u, "f_n"] \arrow[r] & \cdots \arrow[r] & U_2' \arrow[u, "f_2"] \arrow[r] & U_1' \arrow[u, "f_1"]
\end{tikzcd}$$

Since $\operatorname{rank}_{\mathbb{Z}_p} U_n' = \operatorname{rank}_{\mathbb{Z}_p} L$ for all n, this implies that the U_n' are in fact all isomorphic. Let $U = U_n'$ for any n and let W be a crystalline (in the sense of Section 2.2.1) $\mathbb{Q}_p$-representation that contains U. The above diagram induces a map $U \cong \varprojlim U_n \to L$, which must be injective since the ranks are the same. Tensoring with $\mathbb{Q}_p$, we find that $V \cong U \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \subset W$ and hence V is crystalline in the sense of Section 2.2.1. □

We can similarly define h-crystalline ($h \geq 0$) for all p-adic representations. We summarize below, noting that the proofs are just as above.

Definition 2.7.

(i) A finite-length representation is *h-crystalline* if it is a subquotient of an h-crystalline $\mathbb{Q}_p$-representation.

(ii) A discrete representation is *h-crystalline* if it is the direct limit of finite-length h-crystalline representations.

(iii) An arbitrary representation is *h-crystalline* if it is an inverse limit of discrete h-crystalline representations, where the topology is given by the inverse limit.

The property of h-crystalline is stable under subobject, quotient, and direct sum. We indicate categories of h-crystalline representations with a superscript "h". For example, the category of h-crystalline discrete representations is denoted by $\mathbf{Mod}^{\mathbf{h}}_{\mathbf{crys}}(\mathbf{G})$. The analogues of Propositions 2.2 and 2.3, stated below, also hold for h-crystalline representations.

Proposition 2.4. *Suppose M is a $\mathbb{Z}_p$-representation. Then*

(i) M is h-crystalline if and only if M is an inverse limit of finite-length h-crystalline representations.

(ii) M is h-crystalline if and only if M/p^nM is h-crystalline for all $n \geq 1$.

Proposition 2.5. *Let V be a $\mathbb{Q}_p$-representation. Then V is h-crystalline in the sense of Section 2.2.1 if and only if V is h-crystalline in the sense of Definition 2.7.*

In the case of h-crystalline finite-length representations (at least for $0 \leq h \leq p-1$), we still have a filtered module description when K is *unramified* over $\mathbb{Q}_p$ (and hence equal to K_0). This description arises from Fontaine–Laffaille theory [FL82]; we will follow the treatment of Wach [Wac97]. We will also use the notation K_0 and $W = W(k)$ to emphasize that this description only holds when K is unramified.

Definition 2.8. A *filtered W-module* is a W-module M equipt with

(i) a decreasing, separated, and exhaustive filtration $(M^i)_{i\in\mathbb{Z}}$ by sub-W-modules,

(ii) a σ-semilinear morphism $\phi^i \colon M^i \to M$ for each $i \in \mathbb{Z}$ such that

$$\phi^i|_{M^{i+1}} = p\phi^{i+1}.$$

The filtered W-modules form an additive category, where the morphisms are W-linear morphisms respecting the filtration and commuting with the ϕ^i.

Let $\mathbf{MF^h_{W,tors}}$ denote the category composed of filtered W-modules M satisfying the following conditions:

(i) the underlying W-module is of finite-length;

(ii) $M^0 = M$ and $M^{h+1} = \{0\}$;

(iii) $M = \sum_{i \in \mathbb{Z}} \phi^i(M^i)$.

This is an abelian category.

The connection to Galois representations is achieved, as in the $\mathbb{Q}_p$-representation case, by means of a ring ($A_{crys,\infty}$ in the terminology of [Wac97]), which has both a Galois module structure and a filtered module structure. More precisely, one can define a contravariant functor,

$$\begin{array}{llll} V^*_{crys}: & \mathbf{MF^h_{W,tors}} & \longrightarrow & \mathbf{Rep_{\mathbb{Z}_p,t}(G)} \\ & M & \longmapsto & \mathrm{Hom}_{\mathbf{MF}}(M, A_{crys,\infty}), \end{array}$$

which is exact and fully-faithful for $0 \le h \le p-2$ and induces an anti-equivalence of categories between $\mathbf{MF^h_{W,tors}}$ and the essential image of V^*_{crys}. For $h = p-1$, one must consider a slightly different category of filtered modules. (See Theorem 2 of [Wac97].) The essential image of V^*_{crys} consists of exactly the subquotients of h-crystalline representations.

Using this description, we can show: if

$$0 \to V' \to V \to V'' \to 0$$

is a short exact sequence of crystalline finite-length representations with V' and V'' both h-crystalline, then V is also h-crystalline.

Example 2.12. If K is unramified over $\mathbb{Q}_p$, unramified finite-length representations of G are 0-crystalline.

Example 2.13. A finite-length representation V is said to be *finite-flat* if V is isomorphic (as a Galois representation) to the $\overline{K}$-points of a finite-flat group scheme defined over $\mathcal{O}_K$. If K is unramified over $\mathbb{Q}_p$, then the finite-flat representations are exactly the 1-crystalline finite-length representations. (See Section 9 of [FL82].)

2.3 Homological Algebra

In this section, we summarize the homological algebra needed to define and study cohomology theories on p-adic representations. In Section 2.3.1, we review the notion of an injective object in an abelian category. In Section 2.3.2, we review the definitions and properties of right-derived functors constructed via injective resolutions. In Section 2.3.3, we review the basic cohomological tool of spectral sequences. Finally, in Section 2.3.4, we review a technique of Jannsen for constructing derived functors by means other than injective resolutions.

2.3.1 Injective Objects

Let $\mathfrak{A}$ be an abelian category. For example, $\mathfrak{A}$ could be the category **Ab** of abelian groups or the category of R-modules, where R is a ring.

Definition 2.9. An object I of $\mathfrak{A}$ is *injective* if one of the following equivalent properties holds:

1. Given an inclusion $i\colon N \hookrightarrow M$ of objects in $\mathfrak{A}$ and a morphism $\phi\colon N \to I$, there exists a morphism $\widetilde{\phi}\colon M \to I$ such that $\phi = \widetilde{\phi} \circ i$.

2. The functor $\mathrm{Hom}_{\mathfrak{A}}(-, I)$ is an exact functor.

For many abelian categories $\mathfrak{A}$, injective objects are difficult to write down explicitly, even though they can be shown to exist in plenty. However, in the category **Ab** of abelian groups, the injective objects are a more familiar type of object: they are exactly the *divisible groups* (see [Eis95, Proposition A3.5, page 626]), those groups for which multiplication by m is surjective for all nonzero integers m. This allows us to write down explicit examples of injective abelian groups, such as $\mathbb{Q}$ or $\mathbb{Q}/\mathbb{Z}$.

Definition 2.10. The category $\mathfrak{A}$ is said to *have enough injectives* if every object of $\mathfrak{A}$ embeds into an injective object of $\mathfrak{A}$.

Examples:

1. The category **Ab** of abelian groups has enough injectives (see [Lan93, Chapter XX, Section 4]).

2. More generally, the category of modules over an arbitrary ring has enough injectives [Lan93, Chapter XX, Theorem 4.1].

3. The category of abstract p-adic representations of G (i.e., $\mathbb{Z}_p$-modules with a linear action of G) has enough injectives. This is just a specific instance of Example 2, since this category is equivalent to the category of $\mathbb{Z}_p[G]$-modules, where $\mathbb{Z}_p[G]$ denotes the group ring of G over $\mathbb{Z}_p$.

4. The category $\mathbf{Mod(G)}$ of *discrete* p-adic representations of G has enough injectives (see [NSW00, Lemma 2.2.5, page 101]).

5. It follows easily from Example 4 that the category $\mathbf{Mod_t(G)}$ of discrete torsion representations also has enough injectives. The key observation is that for any injective discrete representation I, the torsion submodule I_{tors} is an injective object of $\mathbf{Mod_t(G)}$. Thus the embedding of M into an injective object I of $\mathbf{Mod(G)}$ guaranteed by Example 4 yields an embedding of M in the injective discrete torsion representation I_{tors}.

The usefulness of the property of having enough injectives lies in the fact that any object A in a category with enough injectives can be resolved by injective objects.

(The usefulness of such resolutions will be illustrated in the next section.) An *injective resolution* of A is an exact sequence

$$0 \longrightarrow A \xrightarrow{d_0} I^0 \xrightarrow{d_1} I^1 \longrightarrow \cdots$$

where the I^n are injective objects of $\mathfrak{A}$ for all $n \geq 0$. We often denote resolutions more concisely as $A \hookrightarrow I^\bullet$. The existence of injective resolutions follows easily from the existence of enough injectives.

2.3.2 Derived Functors

Suppose that

$$F\colon \mathfrak{A} \to \mathfrak{B}$$

is a covariant functor of abelian categories which is *additive* (that is, preserves the group law on morphisms) and *left-exact*, so that F takes short exact sequences in $\mathfrak{A}$

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

to left-exact sequences in $\mathfrak{B}$

$$0 \longrightarrow F(A) \longrightarrow F(B) \longrightarrow F(C).$$

It is often useful to know "what comes next" in the above left-exact sequence. One can answer this question in a functorial way when the category $\mathfrak{A}$ has enough injectives.

Proposition 2.6. *Let $F\colon \mathfrak{A} \to \mathfrak{B}$ be a covariant, additive, left-exact functor of abelian categories and suppose $\mathfrak{A}$ has enough injectives. Then there exists a family of covariant, additive functors*

$$\{R^iF\colon \mathfrak{A} \to \mathfrak{B}\}_{i \geq 0}$$

satisfying the following properties:

1. *$R^0F \cong F$, as functors.*

2. Given a short exact sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

in $\mathfrak{A}$, there exists a long exact sequence

$$\begin{tikzcd} 0 \arrow[r] & R^0F(A) \arrow[r] & R^0F(B) \arrow[r] & R^0F(C) \arrow[dll, rounded corners] \\ & R^1F(A) \arrow[r] & R^1F(B) \arrow[r] & R^1F(C) \arrow[r] & \cdots \end{tikzcd}$$

in $\mathfrak{B}$.

We refer to the R^iF as the *right-derived functors* of F. Combining both properties given in Proposition 2.6, we get the answer to "what comes next" in the sequence

$$0 \longrightarrow F(A) \longrightarrow F(B) \longrightarrow F(C).$$

We include below the construction of the right-derived functors via injective resolutions. See [Lan93, Chapter XX, Theorem 6.1] for a proof that this construction satisfies the statements of Proposition 2.6.

Let A be an object of $\mathfrak{A}$.

- STEP 1: Choose an injective resolution

$$0 \longrightarrow A \longrightarrow I^0 \longrightarrow I^1 \longrightarrow \ldots$$

- STEP 2: Apply the functor F to the resolution and consider the resulting complex

$$0 \longrightarrow F(I^0) \longrightarrow F(I^1) \longrightarrow F(I^2) \longrightarrow \ldots$$

- STEP 3: Define

$$R^iF(A) := h^i(F(I^\bullet)),$$

where for a general complex $C^\bullet$,

$$h^i(C^\bullet) := \mathrm{Ker}(C^i \to C^{i+1}) / \mathrm{Im}(C^{i-1} \to C^i),$$

and

$$h^0(C^\bullet) := \mathrm{Ker}(C^0 \to C^1).$$

We now define the R^iF on morphisms. Suppose that $f \colon A \to B$ is a morphism in $\mathfrak{A}$. Let $A \hookrightarrow I_A^\bullet$ and $B \hookrightarrow I_B^\bullet$ be injective resolutions of A and B respectively. By the definition of an injective object, the morphism f will extend to a morphism of resolutions; that is, the morphism f extends to a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & I_A^0 & \longrightarrow & I_A^1 & \longrightarrow & \cdots \\ & & {\scriptstyle f}\big\downarrow & & {\scriptstyle f_0}\big\downarrow & & {\scriptstyle f_1}\big\downarrow & & \\ 0 & \longrightarrow & B & \longrightarrow & I_B^0 & \longrightarrow & I_B^1 & \longrightarrow & \cdots \end{array}$$

Then, the morphisms

$$R^nF(f) \colon R^nF(A) \to R^nF(B)$$

are the maps induced by $F(f_n)$.

These definitions are in fact independent of the choice of injective resolution (see [Lan93, Chapter XX, Theorem 6.1(i)]).

As an easy example, we can compute the $R^iF(I)$ when I is an injective object of $\mathfrak{A}$. The sequence

$$0 \longrightarrow I \xrightarrow{Id} I \longrightarrow 0$$

is an injective resolution of I and thus

$$R^iF(I) = \begin{cases} F(I) & \text{if } i = 0, \\ 0 & \text{for all } i > 0, \end{cases}$$

for any functor F.

More generally, an object A is called F*-acyclic* if the $R^iF(A)$ vanish for all $i \geq 1$. One can in fact compute the R^iF using F-acyclic resolutions in place of injective resolutions [Lan93, Chapter XX, Theorem 6.2]. While the notion of injective object is useful theoretically, explicit acyclic resolutions are generally easier to write down than their injective counterparts.

Example 2.14 (The Hom and Ext functors). The category of modules over a ring R has enough injectives (see Section 2.3.1). Fix an R-module M. The functor

$$N \rightsquigarrow \mathrm{Hom}_R(M, N)$$

from the category of R-modules to the category of abelian groups is additive and left-exact. The right-derived functors of $\mathrm{Hom}_R(M, -)$ are denoted $\mathrm{Ext}^i_R(M, -)$.

Given two R-modules M and N, an *extension* of M by N is another R-module E and a short exact sequence:

$$0 \longrightarrow N \longrightarrow E \longrightarrow M \longrightarrow 0. \tag{2.1}$$

Given such an extension, one obtains an element of $\mathrm{Ext}^1(M, N)$ in the following way. Apply $\mathrm{Hom}_R(M, \cdot)$ to (2.1) and consider the resulting homomorphism:

$$\mathrm{Hom}_R(M, M) \longrightarrow \mathrm{Ext}^1_R(M, N).$$

The associated element of $\mathrm{Ext}^1_R(M, N)$ is the image of the identity homomorphism on M. This association is in fact a bijection (up to a suitable notion of equivalence of extensions). See [Lan93, Exercise 27, page 831].

Example 2.15 (Galois cohomology). The category of discrete representations has enough injectives (see Section 2.3.1). The G-invariants functor

$$M \rightsquigarrow M^G = \{m \in M \mid g \cdot m = m, \ \forall g \in G\}$$

from $\mathbf{Mod(G)}$ to the category of abelian groups is additive and left-exact. The right-derived functors of $(-)^G$ are denoted $\mathrm{H}^i(G, -)$ and are referred to as *Galois cohomology*.

Galois cohomology can be computed in terms of a specific acyclic resolution. After applying G-invariants, this complex becomes the "standard cochain complex".

Galois cohomology is actually a special case of Example 2.14: the G-invariants functor is isomorphic to the functor $\mathrm{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p, -)$. Hence, we can interpret elements of $\mathrm{H}^1(G, M)$ as extensions (in the category of $\mathbb{Z}_p[G]$-modules) of $\mathbb{Z}_p$ by M.

One can also consider *Galois cohomology with respect to inertia*, the right-derived functors $\mathrm{H}^i(I, -)$ of the I-invariants functor, where I is the inertia subgroup of G.

2.3.3 Spectral sequences

Given an additive, left-exact functor F that can be written as a composition

$$\mathfrak{A} \xrightarrow{F_1} \mathfrak{B} \xrightarrow{F_2} \mathfrak{C}.$$

of additive, left-exact functors, it is possible to compute the derived functors of F in terms of the derived functors of the F_i (provided the categories involved are nice enough) using the cohomological tool of *spectral sequences*. We give the basic definitions and properties of spectral sequences (see also [NSW00, Chapter 2, Section 1]).

A *spectral sequence* $E = (E_r^{ij}, E^n)$ in an abelian category $\mathfrak{A}$ consists of the following data. First, we have

- for each integer $r \geq 2$, a collection of objects E_r^{ij} of $\mathfrak{A}$ indexed by $(i, j) \in \mathbb{Z} \times \mathbb{Z}$.
- for $r \geq 2$ and $(i, j) \in \mathbb{Z} \times \mathbb{Z}$, differentials $d_r^{ij} : E_r^{ij} \to E_r^{i+r, j-r+1}$ whose compositions (where they make sense) are zero, and
- for $r \geq 2$ and $(i, j) \in \mathbb{Z} \times \mathbb{Z}$, isomorphisms

$$\alpha_r^{ij} : \mathrm{Ker}(d_r^{ij}) \,/\, \mathrm{Im}(d_r^{i-r, j+r-1}) \xrightarrow{\cong} E_{r+1}^{ij}.$$

  (Otherwise said, we have isomorphisms between the $(r+1)$st term E_{r+1} and the cohomology of the rth term of the spectral sequence E.)

Second, we have for each $n \in \mathbb{Z}$ a filtered object E^n of $\mathfrak{A}$, i.e., an object E^n together with a decreasing filtration by subobjects of $\mathfrak{A}$:

$$\ldots \supset F^iE^n \supset F^{i+1}E^n \supset \ldots$$

Third, the relationship between the two sets of data is as follows. We assume for fixed i and j, there exists an r_0 such that $E_r^{ij} = E_{r_0}^{ij}$ for all $r \geq r_0$. (For example, this would happen if the differentials were 0 after the r_0th term.) We denote the limit object $E_{r_0}^{ij}$ by E_∞^{ij}. Then we also assume given isomorphisms

$$\beta^{ij} \colon E_\infty^{ij} \xrightarrow{\cong} gr_iE^{i+j},$$

where $gr_iE^n := F^iE^n/F^{i+1}E^n$ denotes the ith graded piece of E^n.

Spectral sequences are usually viewed as a means of computing the E^n. We write this relationship as

$$E_2^{ij} \Longrightarrow E^{i+j},$$

where the arrow is spoken as "abuts to". Spectral sequences are often described as pages of an infinite book, where the rth page contains the E_r^{ij} and the maps d_r (see Figure 2.1), and each page is the cohomology of the previous page. In this analogy, the E^n are on the last "infinite" page. (Of course, the degeneration of the spectral sequence tells us that we can "get to the last page" in a finite number of steps.)

A *first quadrant* or *cohomological* spectral sequence is one in which the E_r^{ij} are zero whenever either i or j is less than 0. The following proposition tells us exactly when we have a spectral sequence relating composite functors, as alluded to in the beginning of this section. See [NSW00, Theorem 2.2.6, page 101].

Proposition 2.7 (Grothendieck spectral sequences). *Suppose that $\mathfrak{A}$, $\mathfrak{B}$, and $\mathfrak{C}$ are abelian categories and that $\mathfrak{A}$ and $\mathfrak{B}$ have enough injectives. Let*

$$\mathfrak{A} \xrightarrow{F_1} \mathfrak{B} \xrightarrow{F_2} \mathfrak{C}$$

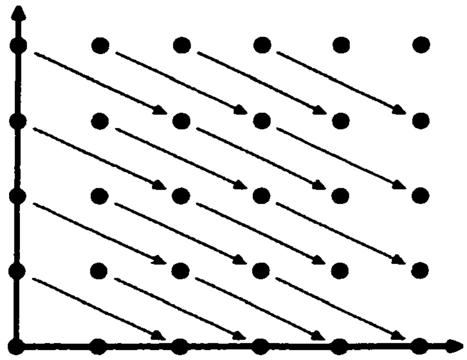

FIGURE 2.1. The E_2 term of a spectral sequence

be additive, left-exact functors and assume that F_1 maps injective objects of $\mathfrak{A}$ to F_2-acyclic objects of $\mathfrak{C}$. Then there exists a first-quadrant spectral sequence

$$E_2^{ij} = R^i F_2\big(R^j F_1(A)\big) \implies R^{i+j}(F_2 \circ F_1)(A).$$

2.3.4 The Technique of Jannsen

Not all abelian categories have enough injectives; for example, the categories of $\mathbb{Z}_p$-representations and $\mathbb{Q}_p$-representations do not have enough injectives. Thus, we cannot always construct right-derived functors via the method of injective resolutions. Jannsen employs another approach to circumvent this difficulty in order to define "continuous étale cohomology" [Jan88]. We will use this technique in Chapter 3 and describe it below.

For an abelian category $\mathfrak{A}$, we define $\mathfrak{A}^{\mathbb{N}}$ to be the category of inverse systems of objects in $\mathfrak{A}$ indexed by the natural numbers $\mathbb{N}$. Thus objects of $\mathfrak{A}^{\mathbb{N}}$ are inverse systems:

$$(A_n, d_n) \colon \; \dots \longrightarrow A_{n+1} \xrightarrow{d_n} A_n \longrightarrow \dots \xrightarrow{d_2} A_2 \xrightarrow{d_1} A_1,$$

and morphisms $\phi\colon (A_n, d_n) \to (B_n, f_n)$ are commutative diagrams:

$$\begin{tikzcd} \dots \arrow[r] & A_{n+1} \arrow[r, "d_n"] \arrow[d] & A_n \arrow[r] \arrow[d, "\phi_n"'] & \dots \arrow[r, "d_2"] & A_2 \arrow[r, "d_1"] \arrow[d, "\phi_2"'] & A_1 \arrow[d, "\phi_1"'] \\ \dots \arrow[r] & B_{n+1} \arrow[r, "f_n"] & B_n \arrow[r] & \dots \arrow[r, "f_2"] & B_2 \arrow[r, "f_1"] & B_1 . \end{tikzcd}$$

The category $\mathfrak{A}^{\mathbb{N}}$ is also an abelian category, taking kernels and cokernels componentwise. The relationship between injective objects of $\mathfrak{A}$ and those of $\mathfrak{A}^{\mathbb{N}}$ is given by the following lemma (see [Jan88, Proposition 1.1]).

Lemma 2.1.

1. *The category $\mathfrak{A}$ has enough injectives if and only if the category $\mathfrak{A}^{\mathbb{N}}$ has enough injectives.*

2. *An object (A_n, d_n) is an injective object of $\mathfrak{A}^{\mathbb{N}}$ if and only if each A_n is an injective object of $\mathfrak{A}$ and each d_n is a split surjection.*

Given a left-exact, additive functor $F\colon \mathfrak{A} \to \mathfrak{B}$ of abelian categories, there is an associated left-exact, additive functor $F^{\mathbb{N}}\colon \mathfrak{A}^{\mathbb{N}} \to \mathfrak{B}^{\mathbb{N}}$ defined by

$$F^{\mathbb{N}}(A_n, d_n) := \big(F(A_n), F(d_n)\big).$$

If $\mathfrak{A}$ (and hence $\mathfrak{A}^{\mathbb{N}}$) has enough injectives, we can construct the right-derived functors of both F and $F^{\mathbb{N}}$ via injective resolutions as in Section 2.3.2. We denote these as R^iF and $R^i(F^{\mathbb{N}})$, respectively. For all $i \geq 0$ [Jan88, Proposition 1.2],

$$R^i(F^{\mathbb{N}})(A_n, d_n) = \big(R^iF(A_n), R^iF(d_n)\big).$$

Let $\mathfrak{C}$ be a category in which inverse limits of objects in $\mathfrak{B}^{\mathbb{N}}$ exist. For example, if $\mathfrak{B} = \mathbf{Ab}$, we can take $\mathfrak{C} = \mathbf{Ab}$. On the other hand, if $\mathfrak{B} = \mathbf{Mod(G)}$, we would need to take $\mathfrak{C} = \mathbf{Rep(G)}$. The functor

$$\varprojlim_{n\in\mathbb{N}}\colon \mathfrak{B}^{\mathbb{N}} \longrightarrow \mathfrak{C}$$

is a left-exact, additive functor. If $\mathfrak{B}$ has enough injectives, we can construct the right-derived functors of $\varprojlim$, denoted $\varprojlim^i$, via injective resolutions. If countable products exist and are exact in $\mathfrak{C}$, then $\varprojlim^i = 0$ for all $i \geq 2$ (see [Jan88, page 211]).

Define $\varprojlim F : \mathfrak{A}^{\mathbb{N}} \to \mathfrak{C}$ as the composition

$$\mathfrak{A}^{\mathbb{N}} \xrightarrow{F^{\mathbb{N}}} \mathfrak{B}^{\mathbb{N}} \xrightarrow{\varprojlim} \mathfrak{C}.$$

If F is left-exact and additive, so is $\varprojlim F$ and hence, if $\mathfrak{A}$ has enough injectives, we can construct the right-derived functors $R^i(\varprojlim F)$ of $\varprojlim F$ via injective resolutions. If $\mathfrak{B}$ has enough injectives and $F^{\mathbb{N}}$ takes injective objects of $\mathfrak{A}^{\mathbb{N}}$ to $\varprojlim$-acyclic objects, then we have a Grothendieck spectral sequence associated to the above composition:

$$E_2^{ij} = \varprojlim{}^i(R^j F^{\mathbb{N}}(A_n, d_n)) \implies R^{i+j}(\varprojlim F)(A_n, d_n),$$

for all $(A_n, d_n) \in \mathfrak{A}^{\mathbb{N}}$. Combining this with the vanishing of $\varprojlim^i$ for $i \geq 2$, we get the following short exact sequences for all $i \geq 1$ and all $(A_n, d_n) \in \mathfrak{A}^{\mathbb{N}}$ (see [Jan88, Proposition 6]):

$$0 \to \varprojlim{}^1(R^{i-1}F(A_n)) \to R^i(\varprojlim F)(A_n, d_n) \to \varprojlim(R^i F(A_n)) \to 0, \tag{2.2}$$

where the limits are taken with respect to the $R^i F(d_n)$.

Let (B_n, f_n) be an inverse system in $\mathfrak{B}^{\mathbb{N}}$ and let $f_{m,n}\colon B_{m+n} \to B_n$ denote the composition of transition maps $f_n \circ \ldots \circ f_{m-n+1}$. The inverse system (B_n, f_n) is said to satisfy the *Mittag-Leffler condition* if for each n, the images of the $f_{m,n}$ are constant for all m sufficiently large. Examples of inverse systems satisfying the Mittag-Leffler condition include inverse systems whose transition maps are all surjective. If $\mathfrak{B} =$ **Ab**, then any inverse system of *finite* abelian groups will satisfy the Mittag-Leffler condition.

If (B_n, f_n) satisfies the Mittag-Leffler condition and countable products exist and are exact functors in $\mathfrak{C}$, then $\varprojlim^1(B_n, f_n) = 0$ (see Lemma 1.15 of [Jan88]). In particular, if $\left(R^{i-1}F(A_n), R^{i-1}F(d_n)\right)$ satisfies the Mittag-Leffler condition, then the short exact sequence (2.2) tells us that

$$R^i(\varprojlim F)(A_n, d_n) \cong \varprojlim\left(R^i F(A_n)\right).$$

Example 2.16 (Galois Cohomology). Jannsen's technique gives a method for defining Galois cohomology groups for $\mathbb{Z}_p$-representations, even though $\mathbf{Rep}_{\mathbb{Z}_p}(\mathbf{G})$ does not have enough injectives. In the above formalism, let $\mathfrak{A} = \mathbf{Mod(G)}$, $\mathfrak{B} = \mathfrak{C} = \mathbf{Ab}$ and let F be the G-invariants functor. To a given $\mathbb{Z}_p$-representation M, let M_f be the associated "formal" inverse system where $M_n = M/p^n M$ and d_n is the canonical projection $M/p^{n+1}M \to M/p^n M$. Since $M^G \cong \varprojlim_{n\in\mathbb{N}}\left(M/p^n M\right)^G$, it is natural to define:

$$\mathrm{H}^i(G, M) := R^i\left(\varprojlim(-)^G\right)(M_f).$$

Note that by the above comments regarding Mittag-Leffler conditions, when $i = 0$ or $i = 1$ we have an isomorphism

$$\mathrm{H}^i(G, M) \cong \varprojlim_{n\in\mathbb{N}} \mathrm{H}^i(G, M/p^n M)$$

for any $\mathbb{Z}_p$-representation M. We get similar isomorphisms for $i \geq 2$ whenever the system (indexed by n) of $\mathrm{H}^{i-1}(G, M/p^n M)$ satisfies the Mittag-Leffler condition.

One can also define the *continuous* Galois cohomology groups of Tate [Tat76] for a $\mathbb{Z}_p$-representation M. This is achieved without resorting to injective resolutions at all; instead, one simply defines $\mathrm{H}^i_{cont}(G, M)$ to be the cohomology of the *continuous* cochain complex associated to M. These two definitions are compatible (see Theorem 2.2 of [Jan88]):

$$\mathrm{H}^i(G, M) \cong \mathrm{H}^i_{cont}(G, M)$$

for all $i \geq 0$ and all $\mathbb{Z}_p$-representations M.

CHAPTER 3. MAXIMAL CRYSTALLINE SUBREPRESENTATION FUNCTORS

In this chapter, we define and study the *maximal crystalline subrepresentation functors*. In Section 3.1, we define the maximal crystalline subrepresentation functors. In Section 3.2, we discuss the "derived functors" of these functors. For $\mathbb{Z}_p$- and $\mathbb{Q}_p$-representations, we must use the technique of Jannsen. In Sections 3.3 and 3.4, we study the functorial properties of the derived functors.

We retain the notations of Chapter 2; see especially Section 2.1.

3.1 The Functors $\mathrm{Crys}(-)$ and $\mathrm{Crys}_h(-)$

Let V be a p-adic representation of G. The *maximal crystalline subrepresentation* of V, denoted $\mathrm{Crys}(V)$, is the sum of all crystalline subrepresentations of V. Since the property of being crystalline is stable under quotients and direct sums, it is also stable under sums and so $\mathrm{Crys}(V)$ is itself crystalline. Furthermore, every crystalline subrepresentation of V is contained in $\mathrm{Crys}(V)$, justifying the terminology "maximal".

Let $f\colon V_1 \to V_2$ be a morphism of p-adic representations. The image $f\big(\mathrm{Crys}(V_1)\big)$ is crystalline (by the stability of crystalline representations under quotients), and so contained in $\mathrm{Crys}(V_2)$ by maximality. Thus, we get an induced morphism

$$f|_{\mathrm{Crys}(V_1)}\colon \mathrm{Crys}(V_1) \to \mathrm{Crys}(V_2)$$

and $\mathrm{Crys}(-)$ defines an additive functor

$$\mathrm{Crys}\colon \mathbf{Rep(G)} \to \mathbf{Rep_{crys}(G)}.$$

The stability under quotients implies that $\mathrm{Crys}(-)$ is the right adjoint functor to the simple functor $F\colon \mathbf{Rep_{crys}(G)} \to \mathbf{Rep(G)}$, which takes objects and morphisms of $\mathbf{Rep_{crys}(G)}$ and "thinks of them" as objects and morphisms of $\mathbf{Rep(G)}$; that is, we have natural isomorphisms

$$\mathrm{Hom}_{crys}(W, \mathrm{Crys}(V)) \cong \mathrm{Hom}(F(W), V)$$

for all crystalline representations W and all arbitrary representations V. This, in particular, implies that $\mathrm{Crys}(-)$ is a *left-exact functor*.

The left-exactness can also be seen directly from the observation that

$$W \subset V \implies \mathrm{Crys}(W) = \mathrm{Crys}(V) \cap W,$$

which follows from the stability of crystalline representations under subobjects.

Since the category of h-crystalline representations is also stable under subobjects, quotients, and direct sums, we can similarly define the left-exact, additive functors

$$\mathrm{Crys}_h \colon \mathbf{Rep(G)} \to \mathbf{Rep^h_{crys}(G)}$$

where $\mathrm{Crys}_h(V)$ is the maximal *h-crystalline* subrepresentation of V.

3.2 Derived Functors

Since the functors $\mathrm{Crys}(-)$ and Crys_h are additive and left-exact, we would like to discuss their right-derived functors. However, the full category of p-adic representations does not have enough injectives so we cannot use the formalism of Section 2.3.2 to guarantee the existence of derived functors. In fact, we will only be able to define $R^i\,\mathrm{Crys}(-)$ and $R^i\,\mathrm{Crys}_h(-)$ for certain p-adic representations. We will use the technique of Jannsen developed in [Jan88] (see Section 2.3.4) in the case of $\mathbb{Z}_p$-representations and $\mathbb{Q}_p$-representations. We discuss the method for the functor $\mathrm{Crys}(-)$; the definitions work in exactly the same way for the $\mathrm{Crys}_h(-)$.

We begin by restricting $\mathrm{Crys}(-)$ to a subcategory of $\mathbf{Rep}(G)$ which *does* have enough injectives, namely the discrete torsion representations, $\mathbf{Mod_t(G)}$ (see Section

2.3.1). For all $i \geq 0$, we define

$$R^i \operatorname{Crys}(-)\colon \mathbf{Mod_t}(\mathbf{G}) \to \mathbf{Mod_{t,crys}}(\mathbf{G})$$

to be the ith derived-functor of Crys(−) in the sense of Section 2.3.2; that is, constructed via injective resolutions.

Now let V be a $\mathbb{Z}_p$-representation. The right-adjoint property of Crys(−) gives an isomorphism

$$\operatorname{Crys}(V) \cong \varprojlim_{n\in\mathbb{N}} \operatorname{Crys}(V/p^n V),$$

inspiring us to define the $R^i \operatorname{Crys}(V)$ in terms of the derived functors of $\varprojlim \operatorname{Crys}(-)$ (see Section 2.3.4).

The functor $\varprojlim \operatorname{Crys}(-)$ is the composition

$$\varprojlim \operatorname{Crys}\colon \mathbf{Mod_t}(\mathbf{G})^{\mathbb{N}} \xrightarrow{\operatorname{Crys}^{\mathbb{N}}} \mathbf{Mod_{t,crys}}(\mathbf{G})^{\mathbb{N}} \xrightarrow{\varprojlim} \mathbf{Rep_{crys}}(\mathbf{G}).$$

By Proposition 2.1, $\mathbf{Mod_t}(\mathbf{G})^{\mathbb{N}}$ has enough injectives and so we define, for all $i \geq 0$,

$$R^i(\varprojlim \operatorname{Crys})\colon (\mathbf{Mod_t}(\mathbf{G}))^{\mathbb{N}} \to \mathbf{Rep_{crys}}(\mathbf{G})$$

to be the ith right-derived functor of $\varprojlim \operatorname{Crys}(-)$ (constructed via injective resolutions).

Lemma 3.1.

1. *If I is an injective object of $\mathbf{Mod_t}(\mathbf{G})$, then $\operatorname{Crys}(I)$ is an injective object of $\mathbf{Mod_{t,crys}}(\mathbf{G})$.*

2. *The category $\mathbf{Mod_{t,crys}}(\mathbf{G})$ has enough injectives.*

Proof. The first statement follows from the right adjoint property of Crys(−) since

$$\operatorname{Hom}_{crys}(-, \operatorname{Crys}(I)) \cong \operatorname{Hom}(G(-), I)$$

is exact. The second statement follows from the first. Let W be a crystalline discrete torsion representation. and embed $F(W)$ in an injective object I of $\mathbf{Mod_t(G)}$. As noted in Section 3.1, the image of $F(W)$ must actually land in $\mathrm{Crys}(I)$, giving an embedding of W in an injective object of $\mathbf{Mod_{t,crys}(G)}$. □

We thus have a spectral sequence

$$E_2^{ij} = \varprojlim{}^i(R^j \operatorname{Crys}^{\mathbb{N}}(M_n, d_n)) \implies R^{i+j}(\varprojlim \operatorname{Crys})(M_n, d_n),$$

from which we deduce the following (see Section 2.3.4).

Proposition 3.1. *For each $i \geq 1$, there are exact sequences*

$$0 \to \varprojlim{}^1(R^{i-1} \operatorname{Crys}(M_n)) \to R^i(\varprojlim \operatorname{Crys})(M_n, d_n) \to \varprojlim(R^i \operatorname{Crys}(M_n)) \to 0$$

for all (M_n, d_n) in $\mathbf{Mod_t(G)}^{\mathbb{N}}$.

We can embed the category of discrete torsion representations as a full-subcategory of $\mathbf{Mod_t(G)}^{\mathbb{N}}$ by associating to a discrete torsion representation V the inverse system $\underline{V}$ with V in each term and with transition maps all equal to the identity. We note that $V \cong \varprojlim(\underline{V})$ and for all $i \geq 0$

$$R^i \operatorname{Crys}(V) \cong R^i(\varprojlim \operatorname{Crys})(\underline{V}),$$

since $V \rightsquigarrow \underline{V}$ is an exact functor preserving injective objects.

We now return to our $\mathbb{Z}_p$-representation M. Define M_f to be the inverse system whose nth term is given by M/p^nM and whose transition maps are the canonical projections $M/p^{n+1}M \to M/p^nM$. Then, $M \cong \varprojlim M_f$ and we call M_f the "formal inverse system associated to M" (see also Example 2.16).

Definition 3.1. Let M be an object of $\mathbf{Rep_{\mathbb{Z}_p}(G)}$. For all $i \geq 0$, define

$$R^i \operatorname{Crys}(M) := R^i(\varprojlim \operatorname{Crys})(M_f).$$

Recall that $\mathrm{Crys}(M) \cong \varprojlim_{n\in\mathbb{N}} \mathrm{Crys}(M/p^nM)$, so $R^0\,\mathrm{Crys}(M) = \mathrm{Crys}(M)$. If M is a finite-length representation, this definition agrees with the previous definition (via injective resolutions) for discrete torsion representations, since the terms M_n of M_f are equal to M for n sufficiently large.

Finally, we turn our attention to the case of $\mathbb{Q}_p$-representations. Given a $\mathbb{Q}_p$-representation V, the compactness of G ensures that we can always find G-invariant lattice L of V. As noted in Section 3.1,

$$\mathrm{Crys}(V) \cap L = \mathrm{Crys}(L).$$

Tensoring both sides with $\mathbb{Q}_p$, we find

$$\mathrm{Crys}(V) \cong \mathrm{Crys}(L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

This leads to our next definition.

Definition 3.2. Let V be an object of $\mathbf{Rep}_{\mathbb{Q}_p}(\mathbf{G})$. For all $i \geq 0$, define

$$\begin{aligned} R^i\,\mathrm{Crys}(V) &:= R^i\,\mathrm{Crys}(L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \\ &= R^i(\varprojlim \mathrm{Crys})(L_f) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p. \end{aligned}$$

This definition is independent of the choice of lattice L. Suppose L' and L are two G-invariant lattices of V. It will suffice to check the case where $L' \subset L$, since the intersection of two lattices is still a lattice. In that case, we have an exact sequence

$$0 \to L' \to L \to L/L' \to 0$$

where L/L' is a finite-length representation. From this we get an associated exact sequence of "formal" inverse systems

$$L'_f \to L_f \to (L/L')_f \to 0,$$

which is not in general left-exact. Let K (respectively Q) be the kernel (respectively image) of $L'_f \to L_f$. Then we have two short exact sequences of inverse systems:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & L'_f & \longrightarrow & Q & \longrightarrow & 0, \\ 0 & \longrightarrow & Q & \longrightarrow & L_f & \longrightarrow & (L/L')_f & \longrightarrow & 0. \end{array}$$

The nth term of K is given by $K_n = \mathrm{Ker}(L'/p^nL' \to L/p^nL)$ and thus for n sufficiently large, $K_n = 0$. This implies that $R^i(\varprojlim \mathrm{Crys})(K) = 0$ for all $i \geq 0$. From the long exact sequence of $R^i(\varprojlim \mathrm{Crys})$ associated to the first short exact sequence, we get

$$R^i \,\mathrm{Crys}(L') \cong R^i(\varprojlim \mathrm{Crys})(Q).$$

From the long exact sequence associated to the second short exact sequence, we get

$$\dots \longrightarrow R^i \,\mathrm{Crys}(L') \longrightarrow R^i \,\mathrm{Crys}(L) \longrightarrow R^i(\varprojlim \mathrm{Crys})(L/L')_f \longrightarrow \dots$$

Tensoring with $\mathbb{Q}_p$ then gives

$$R^i \,\mathrm{Crys}(L') \otimes_{Z_p} \mathbb{Q}_p \cong R^i \,\mathrm{Crys}(L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

since $R^i(\varprojlim \mathrm{Crys})(L/L')_f \cong R^i \,\mathrm{Crys}(L/L')$ is torsion.

Summary. We now have a definition for $R^i \,\mathrm{Crys}(V)$ if V is a

- discrete torsion representation (via injective resolutions);
- $\mathbb{Z}_p$-representation (via the technique of Jannsen);
- $\mathbb{Q}_p$-representation (via tensor products).

We reiterate that we have similar definitions for $R^i \,\mathrm{Crys}_h(V)$ $(h \geq 0)$ for the above types of V. We study the functorial properties of the $R^i \,\mathrm{Crys}(-)$ in the next sections.

3.3 Long exact sequences

For the $R^i \,\mathrm{Crys}$ constructed via injective resolutions, we get the usual long exact sequences associated to short exact sequences guaranteed by Proposition 2.6. However, we do not in general get long exact sequences associated to short exact sequences involving, for example, $\mathbb{Q}_p$-representations, $\mathbb{Z}_p$-representations or some mixture of different types of representations. We prove below the existence of long exact sequences associated to short exact sequences of a specific type (cf. Lemma 5.2 and Theorem 5.14 in [Jan88]). Again, for simplicity of notation, we write down only the case for $\mathrm{Crys}(-)$, but the same proof works verbatim for the $\mathrm{Crys}_h(-)$.

Lemma 3.2. *Let I be an injective discrete torsion representation. Then:*

1. *I is p-divisible;*
2. *$\mathrm{Crys}(I)$ is p-divisible;*
3. *For all $i \geq 1$ and $n \geq 0$, $R^i\,\mathrm{Crys}(I[p^n]) = 0$.*

Proof. For the first statement, let $x \in I$ and suppose $p^m x = 0$. Consider the inclusion of discrete torsion representations $\mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p} \mathbb{Z}/p^m\mathbb{Z} \hookrightarrow \mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p} \mathbb{Z}/p^{m+1}\mathbb{Z}$ given by multiplication by p and the map $\mathbb{Z}/p^m\mathbb{Z} \to I$ given by $e \otimes 1 \mapsto x$, where e denotes the identity of G. Let $\phi\colon \mathbb{Z}/p^{m+1}\mathbb{Z} \to I$ be the extension guaranteed by the injectivity of I. Then $x = \phi(e \otimes p) = p\phi(e \otimes 1)$, giving the desired divisibility.

For the second statement, let $v \in \mathrm{Crys}(I)$. We want to show that $v = pv'$ for some $v' \in \mathrm{Crys}(I)$. Let N be the $\mathbb{Z}_p[G]$-submodule of $\mathrm{Crys}(I)$ generated by v. This is a finite-length crystalline representation and hence a subquotient of a crystalline $\mathbb{Q}_p$-representation: $W \supset U \to N$. Let K be the kernel of the morphism $U \to N$ and consider the commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & K & \longrightarrow & U & \longrightarrow & N & \longrightarrow & 0 \\
 & & \| & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K & \longrightarrow & \frac{1}{p}U & \xrightarrow{\phi} & N' & \longrightarrow & 0
\end{array}$$

where N' is the quotient $\frac{1}{p}U/K$ and the map $N \to N'$ is the obvious one. By the Snake Lemma, N injects into N'. Inside N', v is a p-multiple: $v = p\phi(\frac{1}{p}u)$, where u is any lift of v in U. By the injectivity of $\mathrm{Crys}(I)$ (see Lemma 3.1), there exists an extension of the injection $N \subset \mathrm{Crys}(I)$ to a map $\psi\colon N' \to \mathrm{Crys}(I)$. Thus in $\mathrm{Crys}(I)$,

$$v = \psi(v) = p\psi(\phi(\frac{1}{p})).$$

For the last statement, if $n = 0$, this follows from the injectivity of I. If $n \geq 1$, then

$$0 \longrightarrow I[p^n] \longrightarrow I \xrightarrow{p^n} I \longrightarrow 0$$

is an injective resolution of $I[p^n]$ and the statement follows. $\square$

Proposition 3.2. *Let M be a free $\mathbb{Z}_p$-representation. Let*

$$0 \longrightarrow M \longrightarrow M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \longrightarrow M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0$$

be the short exact sequence obtained from tensoring

$$0 \longrightarrow \mathbb{Z}_p \longrightarrow \mathbb{Q}_p \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0$$

with M. Then there exists an associated long exact sequence:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Crys}(M) \arrow[r] & \mathrm{Crys}(M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \arrow[r] & \mathrm{Crys}(M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p) \arrow[dll, rounded corners] & \\
& R^1\,\mathrm{Crys}(M) \arrow[r] & R^1\,\mathrm{Crys}(M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \arrow[r] & R^1\,\mathrm{Crys}(M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p) \arrow[r] & \cdots
\end{tikzcd}$$

Proof. Given a discrete torsion representation V, define inverse systems $T(V)$ and (V, p) as follows:

- $T(V)$ is the inverse system whose nth term is given by $V[p^n]$ and whose transition maps are given by multiplication by p, $V[p^n] \xrightarrow{p} V[p^{n-1}]$;
- (V, p) is the inverse system all of whose terms are V and all of whose transition maps are given by multiplication by p, $V \xrightarrow{p} V$.

If V is p-divisible, then the following sequence of inverse systems

$$0 \longrightarrow T(V) \longrightarrow (V, p) \longrightarrow \underline{V} \longrightarrow 0 \tag{3.1}$$

is exact, where we recall that $\underline{V}$ is the inverse system all of whose terms are V and all of whose transition maps are the identity.

Let $V = M \otimes \mathbb{Q}_p/\mathbb{Z}_p$. We claim that our desired long exact sequence is just the one arising from (3.1) above:

$$\ldots \longrightarrow R^i(\varprojlim \mathrm{Crys})(T(V)) \longrightarrow R^i(\varprojlim \mathrm{Crys})(V, p) \longrightarrow R^i(\varprojlim \mathrm{Crys})(\underline{V}) \longrightarrow \ldots$$

We noticed that $R^i(\varprojlim \mathrm{Crys})(\underline{V}) \cong R^i \mathrm{Crys}(V)$ for all $i \geq 0$ in Section 3.1. The isomorphisms

$$R^i(\varprojlim \mathrm{Crys})(T(V)) \cong R^i \mathrm{Crys}(M)$$

for all $i \geq 0$ follow from the fact that. by the freeness of M. $T(V)$ is isomorphic to M_f. the "formal inverse system associated to M" arising in the definition of $R^i \mathrm{Crys}_h(M)$ (Definition 3.1).

The isomorphisms $R^i(\varprojlim \mathrm{Crys})(V, p) \cong R^i \mathrm{Crys}(M \otimes \mathbb{Q}_p)$ for all $i \geq 0$ are also straightforward, but require a bit more work.

Suppose that $V \hookrightarrow I^\bullet$ is an injective resolution in the category of discrete torsion representations. Then we claim that both $T(V) \hookrightarrow T(I^\bullet)$ and $(V, p) \hookrightarrow (I^\bullet, p)$ are $(\varprojlim \mathrm{Crys})$-acyclic resolutions in the category of inverse systems of discrete torsion representations. The exactness of the first alleged resolution follows from the p-divisibility of V and the I^n; the exactness of second is straightforward.

To see the vanishing of the $R^i(\varprojlim \mathrm{Crys})(T(I))$ for all $i \geq 1$ when I is an injective object of $\mathbf{Mod_t(G)}$, consider the exact sequences

$$0 \to \varprojlim{}^1 (R^{i-1} \mathrm{Crys}(I[p^n])) \to R^i(\varprojlim \mathrm{Crys})(T(I)) \to \varprojlim (R^i \mathrm{Crys}(I[p^n])) \to 0.$$

By part 3 of Lemma 3.2, we get the desired vanishing for $i \geq 2$. For $i = 1$, we need the further observation that part 2 of Lemma 3.2 implies that the system $(\mathrm{Crys}(I[p^n]), p)$ satisfies the Mittag-Leffler condition.

The vanishing of the $R^i(\varprojlim \mathrm{Crys})(I, p)$ for all $i \geq 1$ when I is an injective object of $\mathbf{Mod_t(G)}$ is similar, using the fact that injective objects are always acyclic and, in this case, are p-divisible by part 1 of Lemma 3.2.

We can thus compute

$$R^i(\varprojlim \mathrm{Crys})(V,p) = h^i\Big(\varprojlim(\mathrm{Crys}(I^\bullet),p)\Big),$$

and

$$\begin{array}{rcl} R^i\,\mathrm{Crys}(M\otimes\mathbb{Q}_p) & := & R^i(\varprojlim \mathrm{Crys})(M_f)\otimes\mathbb{Q}_p \\ & \cong & R^i(\varprojlim \mathrm{Crys})\big(T(V)\big)\otimes\mathbb{Q}_p \\ & = & h^i\big(\varprojlim_n \mathrm{Crys}(I^\bullet[p^n])\big)\otimes\mathbb{Q}_p \\ & = & h^i\big(\varprojlim_n \mathrm{Crys}(I^\bullet[p^n])\otimes\mathbb{Q}_p\big) \end{array}$$

where the last equality follows from the flatness of $\mathbb{Q}_p$ over $\mathbb{Z}_p$.

But,

$$\varprojlim(\mathrm{Crys}(I^\bullet),p) \cong \varprojlim(\mathrm{Crys}(I^\bullet[p^n]),p)\otimes\mathbb{Q}_p$$

as complexes (since we are working in a torsion category), giving us the desired isomorphisms $R^i(\varprojlim \mathrm{Crys})(V,p) \cong R^i\,\mathrm{Crys}(M\otimes\mathbb{Q}_p)$ and completing the proof.

□

3.4 Spectral sequences

For V any p-adic representation of G, we have an equality

$$V^G = \big(\mathrm{Crys}(V)\big)^G,$$

where the inclusion $\big(\mathrm{Crys}(V)\big)^G \subset V^G$ comes from the inclusion of $\mathrm{Crys}(V)$ into V and the opposite inclusion comes from the maximality of $\mathrm{Crys}(V)$, since V^G is a crystalline subrepresentation of V (see Example 2.5). Thus, we expect a Grothendieck spectral sequence relating the $R^i\,\mathrm{Crys}(-)$ functors to Galois cohomology. We derive these spectral sequences in this section.

We need to first discuss the derived functors of the G-invariants functor restricted to crystalline representations. By Lemma 3.1, $\mathbf{Mod_{t,crys}(G)}$ has enough injectives, so we define

$$\mathrm{H}^i_{crys}(G,-)\colon \mathbf{Mod_{t,crys}(G)} \longrightarrow \mathbf{Ab}$$

to be the derived functors of $(-)^G_{crys}$, constructed via injective resolutions. (Note, this should not be confused with crystalline cohomology.)

Applying Jannsen's technique, we define

$$R^i\big(\varprojlim(-)^G_{crys}\big) : \mathbf{Mod_{t,crys}(G)}^{\mathbb{N}} \longrightarrow \mathbf{Ab}$$

to be the derived functors of

$$\varprojlim(-)^G_{crys}\colon \big(\mathbf{Mod_{t,crys}(G)}\big)^{\mathbb{N}} \xrightarrow{\mathrm{Crys}^{\mathbb{N}}} \mathbf{Ab}^{\mathbb{N}} \xrightarrow{\varprojlim(-)^G_{crys}} \mathbf{Ab}.$$

Let M be a crystalline $\mathbb{Z}_p$-representation. Similar to the case of usual Galois cohomology and that of the $R^i\,\mathrm{Crys}(-)$, we define

$$\mathrm{H}^i_{crys}(G, M) := R^i\big(\varprojlim(-)^G_{crys}\big)(M_f)$$

where M_f denotes the formal inverse system associated to M.

Remark 3.1. We note that for a discrete representation M, $\mathrm{H}^1_{crys}(G, M)$ classifies extensions of $\mathbb{Z}_p$ by M which are crystalline, and hence $\mathrm{H}^1_{crys}(G, M)$ coincides with the $\mathrm{H}^1_f(G, M)$ of Mokrane [Mok98, Section I.4], when M is a finite-length representation. (Compare also to [BK90] and [FPR94].) It is not clear if they coincide for $i \geq 2$.

Proposition 3.3. *For all V in $\mathbf{Mod_t(G)}$, there exists a spectral sequence:*

$$E_2^{ij} = \mathrm{H}^i_{crys}(G, R^j\,\mathrm{Crys}(V)) \Rightarrow \mathrm{H}^{i+j}(G, V).$$

Proof. By Lemma 3.1, the functor $\mathrm{Crys}(-)$ takes injective objects of $\mathbf{Mod_t(G)}$ to injective objects of $\mathbf{Mod_{t,crys}(G)}$. Thus the composition

$$\mathbf{Mod_t(G)} \xrightarrow{\mathrm{Crys}} \mathbf{Mod_{t,crys}(G)} \xrightarrow{(-)^G_{crys}} \mathbf{Ab}$$

satisfies the hypotheses of Proposition 2.7, giving the desired spectral sequence. $\square$

We can extend this to $\mathbb{Z}_p$-representations as well, by first extending the spectral sequence to inverse systems.

Proposition 3.4. *For all $(M_n, d_n) \in \mathbf{Mod_t(G)}^{\mathbb{N}}$, there exists a spectral sequence:*

$$E_2^{ij} = R^i(\varprojlim(-)^G_{crys})\left(R^j(\mathrm{Crys})^{\mathbb{N}}\right)(M_n, d_n) \Rightarrow R^{i+j}\left(\varprojlim(-)^G\right)(M_n, d_n).$$

Proof. The equality $(V)^G = \left(\mathrm{Crys}(V)\right)^G$ implies that $\varprojlim(-)^G$ is equal to the following composition:

$$\mathbf{Mod_t(G)}^{\mathbb{N}} \xrightarrow{\mathrm{Crys}^{\mathbb{N}}} \mathbf{Mod_{t,crys}(G)}^{\mathbb{N}} \xrightarrow{\varprojlim(-)^G_{crys}} \mathbf{Ab}.$$

Combining Lemmas 2.1 and 3.1, we see that $\mathbf{Mod_{t,crys}(G)}^{\mathbb{N}}$ has enough injectives. Moreover, if (I_n, d_n) is an injective object of $\mathbf{Mod_t(G)}^{\mathbb{N}}$, then $\mathrm{Crys}^{\mathbb{N}}(I_n, d_n)$ is an $\varprojlim(-)^G_{crys}$-acyclic object of $\mathbf{Mod_{t,crys}(G)}^{\mathbb{N}}$. The vanishing of

$$R^i(\varprojlim(-)^G_{crys})(\mathrm{Crys}(I_n), d_n)$$

for all $i \geq 2$ follows from the short exact sequence for $R^i(\varprojlim(-)^G_{crys})$ given by Proposition 3.1 and the fact that $\mathrm{Crys}(I_n)$ is an injective object (Lemma 3.1). The vanishing for $i = 1$ follows from the combination of this same short exact sequence, together with the fact that $\left((\mathrm{Crys}(I_n))^G_{crys}, d_n\right) = \left((I_n)^G, d_n\right)$ has surjective transition maps. This follows from the description given in Lemma 2.1 of injective objects in inverse system categories; in particular, it follows from the fact that the d_n are *split* surjections. □

Proposition 3.5. *Let M be a $\mathbb{Z}_p$-representation and suppose that $R^j\,\mathrm{Crys}(M/p^nM)$ is a finite-length representation for all $j \geq 0$ and for all $n \geq 1$. Then there exists a spectral sequence:*

$$\varprojlim \mathrm{H}^i_{crys}(G, R^j\,\mathrm{Crys}_h(M/p^nM)) \Longrightarrow \mathrm{H}^{i+j}_{conts}(G, M).$$

Proof. Consider the spectral sequence for the formal inverse system M_f associated to M given by Proposition 3.4:

$$R^i(\varprojlim(-)^G_{crys})\left(R^j(\mathrm{Crys})^{\mathbb{N}}\right)(M_f) \Rightarrow R^{i+j}\left(\varprojlim(-)^G\right)(M_f).$$

As we saw in Section 2.3.4,

$$R^{i+j}(\varprojlim(-)^G)(M_f) \cong \mathrm{H}^i_{cont}(G, M).$$

By hypothesis, for all $j \geq 0$, the inverse system of the $R^j\,\mathrm{Crys}\,M/p^nM$ satisfies the Mittag-Leffler condition. Thus, we have

$$R^i(\varprojlim(-)^G_{crys})(R^j\,\mathrm{Crys}^{\mathbb{N}}(M_f)) \cong \varprojlim \mathrm{H}^i_{crys}(G, R^j\,\mathrm{Crys}(M/p^nM).$$

$\square$

Chapter 4. APPLICATIONS TO COMPONENT GROUPS OF NÉRON MODELS

In this chapter, we apply the functors defined in Chapter 3 to the study of Néron models of abelian varieties. In Section 4.1, we review the basic definitions and properties of Néron models. In Section 4.2, we prove two cohomological formulae for the component group of a Néron model, one valid only for semistable abelian varieties. In Section 4.3, we explore the non-semistable case through the example furnished by Fermat curves.

4.1 Néron models of abelian varieties

We continue to use the notations of Section 2.1. Thus p is a fixed prime and K is a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}_K$ and residue field k. The absolute Galois group of K is denoted by G and its inertia subgroup by I.

An *abelian variety* A of dimension g defined over K is a non-singular projective variety with an algebraic group law. The projectivity of A forces the group law to be commutative (and in fact, the group law forces A to be non-singular). It is often quite useful to extend A to a geometric object defined over $\mathcal{O}_K$, where one can make use of "reduction modulo p" type arguments. Néron models, first defined by Néron in [Nér64], provide a natural way of doing this, as they are smooth models which extend the group structure of A. However, one pays a price for a smooth model preserving the group structure: $\mathcal{A}$ is not in general a *proper* model (i.e., the special fiber may have "holes").

More precisely, a *Néron model* $\mathcal{A}$ of A is a smooth, separated group scheme of finite-type over $\operatorname{Spec} \mathcal{O}_K$ whose generic fiber $\mathcal{A} \times_{\mathcal{O}_K} K$ is isomorphic to A. It must also satisfy the following universal property:

Suppose $\mathcal{X}$ is a smooth $\mathcal{O}_K$-scheme with generic fiber X. Then given a morphism $\phi\colon X \to A$ of K-schemes, there exists a unique morphism $\widetilde{\phi}\colon \mathcal{X} \to \mathcal{A}$ of $\mathcal{O}_K$-schemes extending ϕ. See Figure 4.1 below.

$$\begin{tikzcd}
A \arrow[r] & \mathcal{A} \\
\operatorname{Spec} K \arrow[u] \arrow[r] & \operatorname{Spec} \mathcal{O}_K \arrow[u] \\
X \arrow[u] \arrow[r] \arrow[uu, bend left=60, "\phi"] & \mathcal{X} \arrow[u] \arrow[uu, bend right=60, "\widetilde{\phi}"']
\end{tikzcd}$$

FIGURE 4.1. The Néronian property of $\mathcal{A}$

The universal property (often referred to as the *Néronian property* of $\mathcal{A}$) can be viewed as a replacement for properness. If $\mathcal{A}$ were a proper model of A, the valuative criterion of properness would give a bijection between the K-rational points of A and the $\mathcal{O}_K$-valued points of $\mathcal{A}$:

$$A(K) \cong \mathcal{A}(\mathcal{O}_K).$$

If we set $\mathcal{X} = \operatorname{Spec} \mathcal{O}_K$ in the above definition, then the Néronian property establishes the desired bijection of points even though $\mathcal{A}$ is generally *not* proper over $\mathcal{O}_K$. In particular, this gives a reduction map

$$A(K) \xrightarrow{red} A_k(k),$$

where A_k denotes the special fiber $\mathcal{A} \times_{\mathcal{O}_K} k$ of the Néron model.

The universal property also implies that Néron models, when they exist, are unique up to unique isomorphism. Néron showed the existence of Néron models in the case of abelian varieties defined over finite extensions of $\mathbb{Q}_p$, the situation of interest to us, in his original paper [Nér64]. For a thorough treatment of Néron models in modern language, see [BLR90].

The first examples of abelian varieties are of dimension one, namely *elliptic curves*. Their Néron models can be constructed from minimal, regular, proper models (see

Chapter IV [Sil94]). Let E be an elliptic curve defined over K and let $\mathcal{C}$ denote its minimal, regular, proper model defined over $\mathcal{O}_K$. (Such models are guaranteed to exist; see Theorem 4.5, Chapter IV [Sil94], for example.) The special fiber $\mathcal{C}_k$ of $\mathcal{C}$ consists of finitely-many irreducible components C_i, possibly with multiplicity:

$$\mathcal{C}_k = \sum_i n_i C_i.$$

The Néron model $\mathcal{E}$ is given by the non-singular locus of $\mathcal{C}$. The generic fiber of $\mathcal{E}$ is E itself, whereas the special fiber E_k is obtained by discarding from $\mathcal{C}_k$ all components of multiplicity greater than one, all points of singularity on each component, and all points of intersection between components. See Figure 4.2 below.

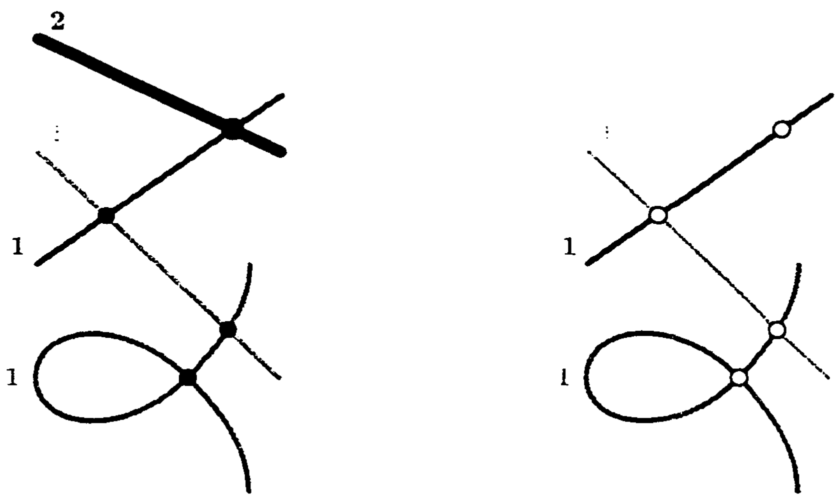

FIGURE 4.2. The special fibers of $\mathcal{C}$ and $\mathcal{E}$.

Jacobian varieties provide another large class of examples of abelian varieties. Let C be a curve of genus g defined over K. The *Jacobian variety* $\mathrm{Jac}(C)$ of C is an abelian variety defined over K of dimension g whose group of K-rational points is isomorphic to the *Picard group* of degree zero divisor classes on C:

$$\mathrm{Jac}(C)(K) \cong Pic^0(X/K).$$

In [Ray70], Raynaud shows that Néron models of Jacobian varieties can be constructed using the relative Picard functor associated to a regular, proper model of C over $\mathcal{O}_K$. See also [BLR90, Chapters 8 and 9].

For a general abelian variety A, the special fiber $\mathcal{A}_k$ of the Néron model of A is a smooth group scheme defined over the residue field k. It is not necessarily connected. Let $\mathcal{A}_k^0$ denote the connected component of the identity in $\mathcal{A}_k$ and let $\pi_0(\mathcal{A}_k) := \mathcal{A}_k/\mathcal{A}_k^0$ be the component group, so that we have the following exact sequence:

$$0 \longrightarrow \mathcal{A}_k^0 \longrightarrow \mathcal{A}_k \longrightarrow \pi_0(\mathcal{A}_k) \longrightarrow 0.$$

As a smooth, *connected* group scheme over k, $\mathcal{A}_k^0$ has a Chevalley decomposition as an extension of an abelian variety B by a linear algebraic group L:

$$0 \longrightarrow L \longrightarrow \mathcal{A}_k^0 \longrightarrow B \longrightarrow 0.$$

Furthermore, over the algebraic closure of k, L is canonically isomorphic to a product of a unipotent group U and an algebraic torus T. The torus T is isomorphic to a product of finitely many copies of the multiplicative group $\mathbb{G}_m$; the unipotent group U, however, may not split into a product of additive groups $\mathbb{G}_a$. Let u, t, and b denote the dimensions of U, T, and B respectively. Then

$$u + t + b = g,$$

and any such triple (u, t, b) is possible. The *reduction type* of A is determined by this triple. For example, A is said to have *good reduction* if $\mathcal{A}$ is proper over $\mathcal{O}_K$. In this case, the special fiber $\mathcal{A}_k$ is an abelian variety over k and so $(u, t, b) = (0, 0, g)$. More generally, A is said to have *semistable reduction* if $u = 0$.

In the example of elliptic curves, the connected component of the identity E_k^0 in the special fiber of the Néron model $\mathcal{E}$ is isomorphic to the non-singular locus of the special fiber of a minimal Weierstrass model of E. In particular, if E has good reduction, then the Weierstrass model is already a Néron model. Since the dimension of E is one, the only possibilities for E_k^0 are an elliptic curve over k, the multiplicative group $\mathbb{G}_m$, or the additive group $\mathbb{G}_a$.

In the case of the Jacobian variety of a curve C, the connected component of the identity in the special fiber of the Néron model is isomorphic to the connected component of the identity of the (scheme representing the) relative Picard functor associated to a regular, proper model $\mathcal{C}$ of C over $\mathcal{O}_K$. Thus, points of the identity component can be interpreted as divisors on $\mathcal{C}$.

For a general abelian variety A, the component group $\pi_0(A_k)$ is a finite, étale group scheme over k. Let $\Phi := \pi_0(A_k)(\overline{k})$ denote the *finite* abelian group of $\overline{k}$-points. The group structure of Φ is dependent on the reduction type of A. For example, in the case of elliptic curves, we have:

(i) If $u = 0$, then Φ is a cyclic group (of order equal to the valuation of the minimal discriminant of E);

(ii) If $t = 0$, then the order of Φ is bounded by 4 (and all groups of order less than or equal to 4 occur this way).

This structure is also reflected in the higher dimensional case, at least for the prime-to-p part of Φ. If $u = 0$, then Φ can be generated by t elements. If $t = 0$, bounds for the prime-to-p part of Φ depending only on the dimension of A were found by Silverman [Sil83], Lenstra-Oort [LO85], and Lorenzini [Lor90]. The general case was shown to be a mixture of these "extreme" cases by Lorenzini in [Lor93]. There he exhibits a filtration of the prime-to-p part $\Phi^{(p)}$ which in particular includes a functorial subgroup Σ^3 satisfying:

(i) Σ^3 can be generated by t elements;

(ii) The order of the quotient $\Phi^{(p)}/\Sigma^3$ is bounded by a constant depending only on the dimension of A.

Edixhoven [Edi95] uses this to classify all possible prime-to-p parts of component groups with fixed u, t, and b.

The p-part of Φ has been more mysterious. It is conjectured that the same sort of phenomena should hold, i.e., there should exist a filtration with analogous properties for the p-part of Φ. Using methods of rigid-analytic geometry, Bosch and Xarles [BX96] recover Lorenzini's filtration in a way which extends to the p-part. However, it has not yet been shown that this filtration has the desired properties. Lorenzini [Lor93] has proved the conjecture in the case of Jacobian varieties (using methods independent of [BX96]). It is hoped that the main result of Section 4.2 below will eventually shed more light on the situation.

We remark that the Jacobian variety case is more accessible due to Raynaud's description in terms of the relative Picard functor. If A is the Jacobian of a curve C, then the component group can be computing using linear algebraic data associated to the special fiber of a regular, proper model of C.

4.2 Cohomological Formulae

In this section, we discuss two cohomological formulae for the component group Φ of the Néron model of an abelian variety A defined over K. The formulae describe the ℓ-primary subgroup of Φ, denoted $\Phi(\ell)$, where ℓ is a prime. The first, proved by Grothendieck in [Gro72], is valid for $\ell \neq p$ (see Theorem 4.1 below) and plays a large role in the results discussed in the previous section concerning the prime-to-p part of Φ. The second fills in the gap at $\ell = p$ in limited circumstances (see Theorem 4.2 below). This formula uses the functors developed in Chapter 3 and was the original motivation for their definition. Both proofs are included to underscore the strong analogy between the two formulae.

4.2.1 The finite part

As discussed in the previous section, the Néronian property of $\mathcal{A}$ implies every K-rational point of A extends (uniquely) to an $\mathcal{O}_K$-valued point of $\mathcal{A}$. However, we do *not* always have such an extension for a point in $A(\overline{K})$. Such a point will be defined over some finite extension L/K and hence defines a morphism $\operatorname{Spec} L \to A$, but we can only apply the Néronian property of $\mathcal{A}$ to get an extension to $\operatorname{Spec} \mathcal{O}_L$ if $\operatorname{Spec} \mathcal{O}_L$ is *smooth* over $\operatorname{Spec} \mathcal{O}_K$. This will be true if and only if L/K is an unramified extension.

We do however have an injection

$$i \colon \mathcal{A}(\mathcal{O}_{\overline{K}}) \hookrightarrow A(\overline{K})$$

given by restricting points to the generic fiber. We denote the image of $\mathcal{A}(\mathcal{O}_{\overline{K}})$ under i by $A(\overline{K})^f$. (The superscript "f" stands for *finite* and will be explained below.) Thus, $A(\overline{K})^f$ is the subgroup of $A(\overline{K})$ consisting of those points which extend to an $\mathcal{O}_{\overline{K}}$-valued point of $\mathcal{A}$. By the above discussion, we see that $A(K^{ur}) \subset A(\overline{K})^f$, where K^{ur} denotes the maximal unramified subextension of $\overline{K}/K$. For these points, it makes sense to talk about a "reduction" map to the special fiber:

$$A(\overline{K})^f \xrightarrow{red} A_k(\overline{k}).$$

Let $\mathcal{A}^0$ denote the identity component of $\mathcal{A}$. We denote by $A(\overline{K})^{f,0}$ the image of $\mathcal{A}^0(\mathcal{O}_{\overline{K}})$ under the above inclusion i. Thus, $A(\overline{K})^{f,0}$ is the subgroup of $A(\overline{K})^f$ consisting of those points which reduce to the identity component of $A_k(\overline{k})$.

For an integer $m > 0$, let $A[m]$ denote the kernel of multiplication by m on $A(\overline{K})$. Let $A[m]^f$ (respectively, $A[m]^{f,0}$) denote the kernel of multiplication by m on $A(\overline{K})^f$ (respectively, $A(\overline{K})^{f,0}$). These are the subgroups of $A[m]$ consisting of those points which extend to points of the Néron model and those points which reduce to the identity component, respectively. These groups have another interpretation that clarifies the choice of terminology "finite". We now explain that interpretation.

Lemma 4.1. *Let $m > 0$ be an integer.*

1. *If m and p are relatively prime, then multiplication by m on $\mathcal{A}$ is étale.*

2. *If A has semistable reduction, then multiplication by m on $\mathcal{A}$ is quasi-finite and flat.*

3. *The following are equivalent:*

   (a) *Multiplication by m on $\mathcal{A}^0$ is flat.*

   (b) *Multiplication by m on $\mathcal{A}^0$ is surjective.*

   (c) *Multiplication by m on $\mathcal{A}^0$ is quasi-finite.*

   (d) *m and p are relatively prime or A has semistable reduction.*

Proof. For the first two statements regarding $\mathcal{A}$, see [BLR90, Lemma 2, page 179]. For the third statement regarding $\mathcal{A}^0$, see [Gro72, Lemma 2.2.1, page 11]. □

For an integer $m > 0$, let $\mathcal{A}[m]$ and $\mathcal{A}^0[m]$ denote the kernel subgroup schemes of multiplication by m on $\mathcal{A}$ and $\mathcal{A}^0$, respectively. If m is prime to p or A has semistable reduction, then Lemma 4.1 implies that $\mathcal{A}[m]$ and $\mathcal{A}^0[m]$ are quasi-finite, flat, separated group schemes over $\mathcal{O}_K$. If m is prime to p, $\mathcal{A}[m]$ is moreover étale.

In general, a quasi-finite, separated group scheme $\mathcal{X}$ over $\mathcal{O}_K$ decomposes canonically into a disjoint sum

$$\mathcal{X} = \mathcal{X}^f \sqcup \mathcal{X}'$$

where $\mathcal{X}'$ has trivial special fiber and $\mathcal{X}^f$ is a finite subgroup scheme with special fiber identical to that of $\mathcal{X}$ and generic fiber consisting of those points of the generic fiber of $\mathcal{X}$ which extend to points of $\mathcal{X}$. Moreover, if $\mathcal{X}$ is flat or étale then $\mathcal{X}^f$ inherits those properties. The group scheme $\mathcal{X}^f$ is the maximal finite subgroup scheme in $\mathcal{X}$, and is called the *finite part* of $\mathcal{X}$. See [Gro72, page 13] or [BLR90, page 179].

Suppose ℓ is prime and assume that either

(i) $\ell \neq p$;

(ii) $\ell = p$ and A has semistable reduction.

Then, $\mathcal{A}[\ell^n]$ and $\mathcal{A}^0[\ell^n]$ are quasi-finite and separated group schemes by Lemma 4.1. We denote their finite parts by $\mathcal{A}[\ell^n]^f$ and $\mathcal{A}^0[\ell^n]^f$ respectively. These are finite-flat group schemes over $\mathcal{O}_K$ (and $\mathcal{A}[\ell^n]^f$ is étale if $\ell \neq p$) and we have

$$\mathcal{A}[\ell^n]^f(\overline{K}) = A[\ell^n]^f \text{ and } \mathcal{A}^0[\ell^n]^f(\overline{K}) = A[\ell^n]^{f,0}.$$

In the terminology of Example 2.13, the representations $A[\ell^n]^f$ and $A[\ell^n]^{f,0}$ are *finite-flat representations*. Moreover, $A[\ell^n]^f$ is the *maximal* finite-flat subrepresentation of $A[\ell^n]$ whose prolongation is a subgroup scheme of the Néron model. This interpretation of the finite part justifies the terminology "finite" and will be useful later, especially in the case of $\ell \neq p$.

We give one more definition before explaining the connection between finite parts and component groups. Recall that the ℓ-adic Tate module of A is given by $T_\ell A := \varprojlim_{n\in\mathbb{N}} A[p^n]$ (see Sections 1.2.2 and 1.3.1). We define the *finite part* $(T_\ell A)^f$ of $T_\ell A$ to be inverse limit of the $A[\ell^n]^f$ with respect to the multiplication by ℓ maps:

$$(T_\ell A)^f := \varprojlim_{n\in\mathbb{N}} A[\ell^n]^f.$$

The following lemma will play a key role in what follows.

Lemma 4.2. *Let ℓ be a prime number satisfying one of the following conditions:*

(i) $\ell \neq p$,

(ii) $\ell = p$ and A has semistable reduction.

Then the ℓ^n-torsion of the component group Φ can be expressed as:

$$\Phi[\ell^n] \cong \frac{(T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Z}/\ell^n\mathbb{Z})^f}{(T_\ell A)^f \otimes_{\mathbb{Z}_\ell} \mathbb{Z}/\ell^n\mathbb{Z}}.$$

Proof. The map

$$A(\overline{K})^f \longrightarrow \Phi$$

given by composing the reduction map $A(\overline{K})^f \to A_k(\overline{k})$ with the natural projection $A_k(\overline{k}) \to \Phi$ is surjective with kernel $A(\overline{K})^{f,0}$. By Lemma 4.1, multiplication by ℓ^n is surjective on $A^0(\overline{K})^f$. Thus, the bottom row of the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(\overline{K})^{f,0} & \longrightarrow & A(\overline{K})^f & \longrightarrow & \Phi & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & A[\ell^n]^{f,0} & \longrightarrow & A[\ell^n]^f & \longrightarrow & \Phi[\ell^n] & & \end{array}$$

is also surjective by the Snake Lemma. Hence, we have

$$\Phi[\ell^n] \cong A[\ell^n]^f / A[\ell^n]^{f,0}.$$

Clearly, $A[\ell^n]^f$ can be rewritten as $(T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Z}/\ell^n\mathbb{Z})^f$, so it just remains to show that $A[\ell^n]^{f,0}$ is equal to $(T_\ell A)^f \otimes \mathbb{Z}/\ell^n\mathbb{Z}$. Consider the map

$$(T_\ell A)^f \longrightarrow A[\ell^n]^f$$

which sends a compatible sequence (P_m) to its nth component P_n. Any point P_n in the image is infinitely ℓ-divisible since $P_n = \ell^m P_{m+n}$ for all $m > 0$. As Φ is a *finite* group, the image of this map must actually lie in $A[\ell^n]^{f,0}$; that is, the composition with $A[\ell^n]^f \to \Phi$ must be zero. The image surjects onto $A[\ell^n]^{f,0}$ by the surjectivity of ℓ^n on $A^0(\overline{K})^f$. Since the kernel is clearly $\ell^n(T_\ell A)^f$, this completes the proof. □

Remark 4.1. Our terminology differs from that of [Gro72]; there the "finite part" is called the "fixed part" due to its description in the case of $\ell \neq p$ (see below). However, since this description is not valid for $\ell \neq p$, we use the terminology "finite".

It is here that the paths for $\ell \neq p$ and p diverge. We treat each case separately.

4.2.2 The case of $\ell \neq p$

We now assume ℓ is different from p. In this case, the finite part of $A[\ell^n]$ coincides with the more familiar subrepresentation of inertia invariants:

$$A[\ell^n]^f = \left(A[\ell^n]\right)^I.$$

This follows from the fact that $\mathcal{A}[\ell^n]^f$ is finite and *étale* over $\mathcal{O}_K$ (see [Gro72, Proposition 2.2.5]). Combining this description of the finite part with Lemma 4.2 and taking direct limits, we find

$$\Phi(\ell) \cong \frac{(T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell/\mathbb{Z}_\ell)^I}{(T_\ell A)^I \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell/\mathbb{Z}_\ell}, \tag{4.1}$$

where $\Phi(\ell)$ denotes the ℓ-primary subgroup of Φ (cf. [Gro72, Proposition 11.2]). This leads to our first cohomological formula, relating the ℓ-primary subgroup of Φ to Galois cohomology with respect to inertia invariants.

Theorem 4.1 (Grothendieck, page 135 of [Gro72]). *Let A be an abelian variety defined over a finite extension K of $\mathbb{Q}_p$. Let Φ denote the component group of the Néron model of A. Then for $\ell \neq p$,*

$$\Phi(\ell) \cong \mathrm{H}^1(I, T_\ell A)_{\mathrm{tors}}.$$

Proof. Applying the inertia invariants functor to the short exact sequence

$$0 \longrightarrow T_\ell A \longrightarrow T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \longrightarrow T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell/\mathbb{Z}_\ell \longrightarrow 0,$$

we obtain the long exact sequence of cohomology:

$$\begin{tikzcd} 0 \arrow[r] & (T_\ell A)^I \arrow[r] & (T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)^I \arrow[r] & (T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell/\mathbb{Z}_\ell)^I \arrow[dll, rounded corners] & \\ & \mathrm{H}^1(I, T_\ell A) \arrow[r] & \mathrm{H}^1(I, T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell) \arrow[r] & \mathrm{H}^1(I, T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell/\mathbb{Z}_\ell) \arrow[r] & \cdots \end{tikzcd}$$

Since $(T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)^I = (T_\ell A)^I \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, the kernel of $\mathrm{H}^1(I, T_\ell A) \to \mathrm{H}^1(I, T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)$ is

$$\frac{(T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell/\mathbb{Z}_\ell)^I}{(T_\ell A)^I \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell/\mathbb{Z}_\ell}.$$

Thus, by the formula (4.1), there is an injection

$$\Phi(\ell) \hookrightarrow \mathrm{H}^1(I, T_\ell A).$$

Since $\mathrm{H}^1(I, T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)$ is torsion-free, $\Phi(\ell)$ is the full torsion subgroup of $\mathrm{H}^1(I, T_\ell A)$, as claimed. □

4.2.3 The case of $\ell = p$

We now treat the case of $\ell = p$. In order to use Lemma 4.2, we must assume that our abelian variety A has *semistable reduction.* In this case, the finite part of $A[p^n]$ does *not* coincide with the inertia fixed part. However, if K is *unramified* over $\mathbb{Q}_p$ and $p \neq 2$, then the finite part of $A[p^n]$ coincides with the *crystalline part*: $\mathrm{Crys}(A[p^n])$. We restrict to $p \neq 2$ in order to use certain results requiring the ramification index e of $K/\mathbb{Q}_p$ to be less than $p-1$.

Lemma 4.3. *Let A be an abelian variety defined over an unramified finite extension K of $\mathbb{Q}_p$. Suppose that A has semistable reduction and that $p \neq 2$. For all $n > 0$,*

$$A[p^n]^f = \mathrm{Crys}(A[p^n]).$$

Proof. We first show that $A[p^n]^f = \mathrm{Crys}_1(A[p^n])$. Since we are assuming K unramified over $\mathbb{Q}_p$, we have the Fontaine-Laffaille description of $\mathrm{Crys}_1(A[p^n])$ as the *maximal finite-flat subrepresentation* of $A[p^n]$ (see Example 2.13). Since $A[p^n]^f$ is a finite-flat representation (in fact, the *maximal* finite-flat subrepresentation with prolongation inside the Néron model), we have an inclusion

$$A[p^n]^f \subset \mathrm{Crys}_1(A[p^n]).$$

Equality will follow if we show that the prolongation of $\mathrm{Crys}_1(A[p^n])$ lies inside the Néron model. There is only one possible prolongation of $\mathrm{Crys}_1(A[p^n])$ by [Ray74, Theorem 3.3.3], since we are assuming that $e < p-1$.

Let $\mathcal{V}$ denote the prolongation of $\mathrm{Crys}_1(A[p^n])$ over $\mathcal{O}_K$. Thus, $\mathcal{V}$ is a finite-flat group scheme over $\mathcal{O}_K$ whose generic fiber V satisfies $V(\overline{K}) \cong \mathrm{Crys}_1(A[p^n])$. To show that $\mathcal{V}$ lies inside the Néron model, we essentially follow the argument of [Rib90, Lemma 6.2].

The inclusion $\mathrm{Crys}_1(A[p^n]) \subset A[p^n]$ induces a morphism of K-schemes

$$V \to A[p^n] \to A$$

(where by abuse of notation, $A[p^n]$ also denotes the scheme given by the generic fiber of $\mathcal{A}[p^n]$). Our goal is to extend this to a morphism of $\mathcal{O}_K$-schemes $\mathcal{V} \to \mathcal{A}$.

Let

$$0 \to V^0 \to V \to V^{\acute{e}t} \to 0$$

denote the *connected-étale sequence* for V (see [Tat97, page 138]). As $A[p^n]/A[p^n]^f$ is étale (see [Gro72, Proposition 5.6]), the morphism

$$V \to A[p^n] \to A[p^n]/A[p^n]^f$$

factors through $V^{\acute{e}t}$. In other words, the image of V^0 under $V \to A[p^n]$ lands in $A[p^n]^f$. The morphism $V^0 \to A[p^n]^f$ extends to a morphism $\mathcal{V}^0 \to \mathcal{A}[p^n]^f$ by [Ray74, Corollary 3.3.6]. (Note that this result requires $e < p-1$.) Viewing this morphism as a morphism $\mathcal{V}^0 \to \mathcal{A}$, we get our desired morphism $\mathcal{V} \to \mathcal{A}$ by [Gro72, Lemma 5.9.2].

We have shown

$$A[p^n]^f = \mathrm{Crys}_1(A[p^n]),$$

(where $A[p^n]^f$ again denotes the representation and not the scheme). We now show that $\mathrm{Crys}(A[p^n]) = \mathrm{Crys}_1(A[p^n])$. Consider the exact sequence of representations:

$$0 \to \mathrm{Crys}_1(A[p^n]) \to \mathrm{Crys}(A[p^n]) \to \mathrm{Crys}(A[p^n])/\mathrm{Crys}_1(A[p^n]) \to 0.$$

Since $\mathrm{Crys}(A[p^n])/\mathrm{Crys}_1(A[p^n])$ is a subrepresentation of the unramified representation $A[p^n]/A[p^n]^f = A[p^n]/\mathrm{Crys}_1(A[p^n])$, the outer terms of the sequence are both

1-crystalline, implying that $\mathrm{Crys}(A[p^n])$ is in fact 1-crystalline as well (see Section 2.2). $\square$

As in the $\ell \neq p$ case, we combine this description with Lemma 4.2. Since $\mathrm{Crys}(T_pA) \cong \varprojlim_{n\in N} \mathrm{Crys}(A[p^n])$ and $\mathrm{Crys}(-)$ commutes with direct limits, we obtain the p-analogue of formula (4.1):

$$\Phi(p) \cong \frac{\mathrm{Crys}(T_pA \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)}{\mathrm{Crys}(T_pA) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p}. \tag{4.2}$$

We are again led to a cohomological formula.

Theorem 4.2. *Let A be an abelian variety defined over an unramified extension K of $\mathbb{Q}_p$. Suppose that A has semistable reduction and that $p \neq 2$. Then*

$$\Phi(p) \cong R^1\,\mathrm{Crys}(T_pA)_{\mathrm{tors}}.$$

Proof. Applying $\mathrm{Crys}(-)$ to the short exact sequence

$$0 \longrightarrow T_pA \longrightarrow T_pA \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \longrightarrow T_pA \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0,$$

we obtain the long exact sequence (see Proposition 3.2):

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Crys}(T_pA) \arrow[r] & \mathrm{Crys}(T_pA \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \arrow[r] & \mathrm{Crys}(T_pA \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p) \arrow[dll] & \\
& R^1\,\mathrm{Crys}(T_pA) \arrow[r] & R^1\,\mathrm{Crys}(T_pA \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \arrow[r] & R^1\,\mathrm{Crys}(T_pA \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p) \arrow[r] & \cdots
\end{tikzcd}$$

Since $\mathrm{Crys}(T_pA \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) = \mathrm{Crys}(T_pA) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, the kernel of $R^1\,\mathrm{Crys}(T_pA) \to R^1\,\mathrm{Crys}(T_pA \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$ is

$$\frac{\mathrm{Crys}(T_pA \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)}{\mathrm{Crys}(T_pA) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p}.$$

Thus, by the formula (4.2), there is an injection

$$\Phi(p) \hookrightarrow R^1\,\mathrm{Crys}(T_pA).$$

Since $R^1\,\mathrm{Crys}(T_pA \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$ is torsion-free, $\Phi(p)$ is the full torsion subgroup of $R^1\,\mathrm{Crys}(T_pA)$ as claimed. $\square$

4.3 More on finite-flat representations

The restriction of semistability in Theorem 4.2 is rather serious. Without it, we lose the information furnished by Lemma 4.1. In particular, we lose the surjectivity in

$$A[p^n]^f/A[p^n]^{f,0} \hookrightarrow \Phi[p^n].$$

Moreover, it is no longer clear what the relationship between the component group and the maximal finite-flat subrepresentation of $A[p^n]$ will be. In an attempt to understand what relationship remains in the non-semistable case, we explore the question of when the p-torsion representation of an abelian variety is a finite-flat representation.

This question is more tractable in the case of semistable reduction. If A moreover has good reduction, the representation $A[p]$ is known to be finite-flat with prolongation $\mathcal{A}[p]$ (see [Con97, Theorem 1.2], for example). For an elliptic curve with split multiplicative reduction (i.e., the tangent directions of the nodal singularity are defined over k), $E[p]$ will be finite-flat if p divides the order of the component group Φ (see [Con97, Example 1.3 (i)] and [Ell01, Corollary 1.2]). Recall in this situation, the order of Φ is given by the valuation of the minimal discriminant of E. Ellenberg [Ell01] gives analogous results for Hilbert-Blumenthal abelian varieties with multiplicative reduction, based on divisibility conditions associated to a set of Hilbert modular cuspforms attached to the variety.

Jacobians of Fermat curves provide examples of abelian varieties with non-semistable reduction. We study these examples in more detail.

We assume that p is an odd prime and let ζ_p denote a primitive pth root of unity. We fix $K = \mathbb{Q}_p(\zeta_p)$ and thus have $\mathcal{O}_K = \mathbb{Z}_p[\zeta_p]$ and $k = \mathbb{F}_p$. We denote by π the uniformizer $1 - \zeta_p$ of $\mathcal{O}_K$.

For each integer a between 1 and $p-2$, let C_a denote the non-singular projective curve over K associated to

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

This is a curve of genus $\frac{p-1}{2}$ and is a quotient of the p-th Fermat curve given by

$$x^p + y^p = 1.$$

Let $J_a = \mathrm{Jac}(C_a)$ denote the Jacobian variety of C_a. Thus, J_a is a dimension $\frac{p-1}{2}$ abelian variety defined over K. It has complex multiplication by $\mathbb{Z}[\zeta_p]$.

The complex multiplication of J_a gives rise to a filtration of $J_a[p]$:

$$0 \subset J_a[\pi] \subset J_a[\pi^2] \subset \ldots \subset J_a[\pi^{p-1}] = J_a[p],$$

where $J_a[\pi^m]$ denotes the kernel of the endomorphism on $J_a(\overline{K})$ given by π^m. The successive quotients of the filtration are isomorphic (as Galois representations) to $J_a[\pi]$. As a group, $J_a[\pi^m]$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^m$.

We are interested in computing finite-flat subrepresentations of $J_a[p]$. Suppose that $J_a[\pi^m]$ is *rational*, by which we mean $J_a[\pi^m] \subset J_a(K)$ (and not that $J_a[\pi^m]$ is a $\mathbb{Q}_p$-representation). Then $J_a[\pi^m]$ is finite-flat. In this case, $J_a[\pi^m] \cong (\mathbb{Z}/p\mathbb{Z})^m$ as a *Galois representation* and $(\mathbb{Z}/p\mathbb{Z})^m_{\mathcal{O}_K}$ and $(\mu_p)^m_{\mathcal{O}_K}$ are two examples of prolongations.

Let n be the maximal integer such that $J_a[\pi^n]$ is rational. Given a specific choice of a and p, one can be quite explicit about what n is (see [Gre81, page 11]). For example, if $p = 3$ then all of the 3-torsion is rational. If $p \geq 5$, then $J_a[p]$ is *not* rational. However, $J_a[\pi^3]$ is always rational and hence n is always greater than or equal to 3 when $p \geq 5$. More specific information is given by in terms of p-divisibility of certain Bernoulli numbers and congruence conditions on a.

By the above comments, we know that $J_a[\pi^n]$ is finite-flat. In fact, we can say more.

Proposition 4.1. *Let J_a be as defined above. Let n be the maximal integer such that $J_a[\pi^n] \subset J_a(K)$. Then $J_a[\pi^{n+1}]$ is finite-flat.*

Proof. The representation $J_a[\pi^{n+1}]$ is an extension of finite-flat representations:

$$0 \longrightarrow J_a[\pi^n] \longrightarrow J_a[\pi^{n+1}] \xrightarrow{\pi^n} J_a[\pi] \longrightarrow 0.$$

Let c_{n+1} denote the corresponding extension class in $\mathrm{Ext}^1(J_a[\pi], J_a[\pi^n])$. The basic idea is to show that c_{n+1} is in the image of

$$\mathrm{Ext}^1(\widetilde{J_a[\pi]}, \widetilde{J_a[\pi^n]}) \xrightarrow{\text{“}generic\ fiber\text{”}} \mathrm{Ext}^1(J_a[\pi], J_a[\pi^n])$$

for some choice of prolongations $\widetilde{J_a[\pi]}$, $\widetilde{J_a[\pi^n]}$ of $J_a[\pi]$, $J_a[\pi^n]$ respectively. The map "generic fiber" associates to an extension of $\mathcal{O}_K$-group schemes

$$0 \longrightarrow \widetilde{J_a[\pi^n]} \longrightarrow \mathcal{E} \longrightarrow \widetilde{J_a[\pi]} \longrightarrow 0$$

the extension

$$0 \longrightarrow J_a[\pi^n] \longrightarrow E(\overline{K}) \longrightarrow J_a[\pi] \longrightarrow 0$$

where E is the generic fiber of $\mathcal{E}$. Thus, if c_{n+1} corresponds to the class of $\mathcal{E}$ in $\mathrm{Ext}^1(\widetilde{J_a[\pi]}, \widetilde{J_a[\pi^n]})$, then $J_a[\pi^n]$ is finite-flat with prolongation $\mathcal{E}$.

Step 1. We choose $\widetilde{J_a[\pi]} = \mathbb{Z}/p\mathbb{Z}_{\mathcal{O}_K}$. We also fix a choice of prolongation $\widetilde{J_a[\pi^n]}$, but we do not make the choice of prolongation explicit, as yet.

Identify $J_a[\pi]$ with $\mathbb{Z}/p\mathbb{Z}$ and apply $\mathrm{Hom}(\cdot, J_a[\pi^n])$ to the short exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{p} \mathbb{Z} \xrightarrow{proj} \mathbb{Z}/p\mathbb{Z} \cong J_a[\pi] \longrightarrow 0.$$

From the resulting long exact sequence of Ext-groups, one obtains the short exact sequence:

$$0 \longrightarrow J_a[\pi^n] \longrightarrow \mathrm{Ext}^1(J_a[\pi], J_a[\pi^n]) \xrightarrow{proj^*} \mathrm{Ext}^1(\mathbb{Z}, J_a[\pi^n]) \longrightarrow 0.$$

We have made the identification $\mathrm{Hom}(\mathbb{Z}, J_a[\pi^n]) \cong J_a[\pi^n]^G = J_a[\pi^n]$, and both injectivity and surjectivity follow from the fact that $J_a[\pi^n]$ is killed by multiplication by p. Similarly, we apply $\mathrm{Hom}(\cdot, \widetilde{J_a[\pi^n]})$ to

$$0 \longrightarrow \mathbb{Z}_{\mathcal{O}_K} \xrightarrow{p} \mathbb{Z}_{\mathcal{O}_K} \xrightarrow{proj} \mathbb{Z}/p\mathbb{Z}_{\mathcal{O}_K} = \widetilde{J_a[\pi]} \longrightarrow 0$$

and combine with the above to obtain the commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & J_a[\pi^n] \arrow[r] & \mathrm{Ext}^1(J_a[\pi], J_a[\pi^n]) \arrow[r, "proj^*"] & \mathrm{Ext}^1(\mathbb{Z}, J_a[\pi^n]) \arrow[r] & 0 \\
0 \arrow[r] & J_a[\pi^n] \arrow[r] \arrow[u, equal] & \mathrm{Ext}^1(\widetilde{J_a[\pi]}, \widetilde{J_a[\pi^n]}) \arrow[r] \arrow[u] & \mathrm{Ext}^1(\mathbb{Z}_{\mathcal{O}_K}, \widetilde{J_a[\pi^n]}) \arrow[r] \arrow[u] & 0
\end{tikzcd}$$

We again have injectivity and surjectivity in the bottom row because $\widetilde{J_a[\pi^n]}$ is killed by multiplication by p and we have make the identification

$$\mathrm{Hom}(\mathbb{Z}_{\mathcal{O}_K}, \widetilde{J_a[\pi^n]}) \cong \widetilde{J_a[\pi^n]}(\mathcal{O}_K) \cong J_a[\pi^n].$$

It follows from a simple diagram-chase that

$$c_{n+1} \in \mathrm{Im}\big(\mathrm{Ext}^1(\widetilde{J_a[\pi]}, \widetilde{J_a[\pi^n]})\big) \iff proj^*(c_{n+1}) \in \mathrm{Im}\big(\mathrm{Ext}^1(\mathbb{Z}, \widetilde{J_a[\pi^n]})\big).$$

The problem is thus reduced to showing that $proj^*(c_{n+1}) \in \mathrm{Im}\big(\mathrm{Ext}^1(\mathbb{Z}, \widetilde{J_a[\pi^n]})\big)$.

Step 2. We wish to show that $proj^*(c_{n+1})$ actually lies in $\mathrm{Ext}^1(\mathbb{Z}, J_a[\pi])$. Apply $\mathrm{Hom}(\mathbb{Z}, \cdot)$ to the short exact sequence:

$$0 \longrightarrow J_a[\pi] \longrightarrow J_a[\pi^n] \xrightarrow{\pi} J_a[\pi^{n-1}] \longrightarrow 0.$$

We will show that $proj^*(c_{n+1})$ maps to 0 in the resulting long exact sequence:

$$\ldots \longrightarrow \mathrm{Ext}^1(\mathbb{Z}, J_a[\pi]) \longrightarrow \mathrm{Ext}^1(\mathbb{Z}, J_a[\pi^n]) \xrightarrow{\pi^*} \mathrm{Ext}^1(\mathbb{Z}, J_a[\pi^{n-1}]) \longrightarrow \ldots$$

and hence comes from an extension class in $\mathrm{Ext}^1(\mathbb{Z}, J_a[\pi])$, which we continue to denote by $proj^*(c_{n+1})$.

To show that $proj^*(c_{n+1})$ maps to 0, we will show that $\pi^*(proj^*(c_{n+1})) = proj^*(c_n)$, where c_n is the extension class in $\mathrm{Ext}^1(J_a[\pi], J_a[\pi^{n-1}])$ corresponding to

$$0 \longrightarrow J_a[\pi^{n-1}] \longrightarrow J_a[\pi^n] \longrightarrow J_a[\pi] \longrightarrow 0.$$

This extension is trivial, since $J_a[\pi^n]$ is assumed to be rational and hence c_n is zero.

To show that $\pi^*(proj^*(c_{n+1})) = proj^*(c_n)$, first notice that the following square commutes:

$$\begin{array}{ccc} \mathrm{Ext}^1(J_a[\pi], J_a[\pi^n]) & \xrightarrow{proj^*} & \mathrm{Ext}^1(\mathbb{Z}, J_a[\pi^n]) \\ {\scriptstyle \pi^*}\downarrow & & {\scriptstyle \pi^*}\downarrow \\ \mathrm{Ext}^1(J_a[\pi], J_a[\pi^{n-1}]) & \xrightarrow{proj^*} & \mathrm{Ext}^1(\mathbb{Z}, J_a[\pi^{n-1}]) \end{array}$$

Thus we need only show that $\pi^*(c_{n+1}) = c_n$. The extension corresponding to $\pi^*(c_{n+1})$ is the pushout of the diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J_a[\pi^n] & \longrightarrow & J_a[\pi^{n+1}] & \longrightarrow & J_a[\pi] & \longrightarrow & 0 \\ & & {\scriptstyle \pi}\downarrow & & & & \| & & \\ 0 & \longrightarrow & J_a[\pi^{n-1}] & \longrightarrow & & \longrightarrow & J_a[\pi] & \longrightarrow & 0 \end{array}$$

and this push-out is $J_a[\pi^n]$.

Recall that we fixed a prolongation $\widetilde{J_a[\pi^n]}$. There exist unique prolongations $\widehat{J_a[\pi]}$ and $\widehat{J_a[\pi^{n-1}]}$ such that

$$0 \longrightarrow \widehat{J_a[\pi]} \longrightarrow \widetilde{J_a[\pi^n]} \longrightarrow \widehat{J_a[\pi^{n-1}]} \longrightarrow 0$$

is exact with generic fiber

$$0 \longrightarrow J_a[\pi] \longrightarrow J_a[\pi^n] \longrightarrow J_a[\pi^{n-1}] \longrightarrow 0.$$

(See [Mil86, Lemma B.1, page 390].) From these sequences we get the commutative diagram with exact rows

$$\begin{array}{ccccc} \mathrm{Ext}^1(\mathbb{Z}, J_a[\pi]) & \longrightarrow & \mathrm{Ext}^1(\mathbb{Z}, J_a[\pi^n]) & \longrightarrow & \mathrm{Ext}^1(\mathbb{Z}, J_a[\pi^{n-1}]) \\ \uparrow & & \uparrow & & \uparrow \\ \mathrm{Ext}^1(\mathbb{Z}_{\mathcal{O}_K}, \widehat{J_a[\pi]}) & \longrightarrow & \mathrm{Ext}^1(\mathbb{Z}_{\mathcal{O}_K}, \widetilde{J_a[\pi^n]}) & \longrightarrow & \mathrm{Ext}^1(\mathbb{Z}_{\mathcal{O}_K}, \widehat{J_a[\pi^{n-1}]}). \end{array}$$

Thus, the problem is further reduced to showing that $proj^*(c_{n+1})$ is in the image of $\mathrm{Ext}^1(\mathbb{Z}_{\mathcal{O}_K}, \widehat{J_a[\pi]})$.

Step 3. We now choose our prolongation $\widetilde{J_a[\pi^n]}$ to be $(\mu_p)^n_{\mathcal{O}_K}$. This forces $\widehat{J_a[\pi]}$

to be $(\mu_p)_{\mathcal{O}_K}$. We then have identifications:

$$\begin{array}{ccccc}
\mathrm{Ext}^1(\mathbb{Z}, J_a[\pi]) & \cong & H^1(G, \mu_p) & \cong & K^\times/(K^\times)^p \\
\uparrow & & \uparrow & & \uparrow \\
\mathrm{Ext}^1(\mathbb{Z}_{\mathcal{O}_K}, \widetilde{J_a[\pi]}) & \cong & H^1_{fl}(\mathcal{O}_K, (\mu_p)_{\mathcal{O}_K}) & \cong & \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p
\end{array}$$

where $H^1_{fl}(\mathcal{O}_K, -)$ denotes flat cohomology.

Let $P_1, \ldots, P_{n+1}$ be generators of $J_a[\pi^{n+1}]$ so that P_1 generates $J_a[\pi]$ and $\pi \cdot P_i = P_i - 1$ for $i = 2, \ldots, n+1$. Then the cocycle corresponding to $proj^*(c_{n+1})$ under the above identification is

$$\sigma \mapsto \sigma(P_{n+1}), \ \forall \sigma \in G.$$

This cocycle corresponds to the class $[\alpha] \in K^*/(K^*)^p$, where $\alpha^{1/p}$ generates the fixed field of the above cocycle over K. Thus, $K(J_a[\pi^{n+1}]) = K(\alpha^{1/p})$. However, by [Gre81, Theorem 4], this extension is generated by pth roots of real cyclotomic *units*, and hence we get our desired result. □

References

[BK90] Spencer Bloch and Kazuya Kato. L-functions and Tamagawa numbers of motives. In *The Grothendieck Festschrift, Vol. I*, pages 333–400. Birkhäuser Boston, Boston, MA, 1990.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*. Springer-Verlag, Berlin, 1990.

[BX96] Siegfried Bosch and Xavier Xarles. Component groups of Néron models via rigid uniformization. *Math. Ann.*, 306(3):459–486, 1996.

[CF00] Pierre Colmez and Jean-Marc Fontaine. Construction des représentations p-adiques semi-stables. *Invent. Math.*, 140(1):1–43, 2000.

[CI99] Robert Coleman and Adrian Iovita. The Frobenius and monodromy operators for curves and abelian varieties. *Duke Math. J.*, 97(1):171–215, 1999.

[Con97] Brian Conrad. The flat deformation functor. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 373–420. Springer, New York, 1997.

[Cre97] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[Edi95] Bas Edixhoven. On the prime-to-p part of the groups of connected components of Néron models. *Compositio Math.*, 97(1-2):29–49, 1995. Special issue in honour of Frans Oort.

[Eis95] David Eisenbud. *Commutative algebra*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[Ell01] Jordan S. Ellenberg. Finite flatness of torsion subschemes of Hilbert-Blumenthal abelian varieties. *J. Reine Angew. Math.*, 532:1–32, 2001.

[Fal89] Gerd Faltings. Crystalline cohomology and p-adic Galois-representations. In *Algebraic analysis, geometry, and number theory (Baltimore, MD, 1988)*, pages 25–80. Johns Hopkins Univ. Press, Baltimore, MD, 1989.

[FL82] Jean-Marc Fontaine and Guy Laffaille. Construction de représentations p-adiques. *Ann. Sci. École Norm. Sup. (4)*, 15(4):547–608 (1983), 1982.

[FM87] Jean-Marc Fontaine and William Messing. p-adic periods and p-adic étale cohomology. In *Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985)*, pages 179–207. Amer. Math. Soc., Providence, RI, 1987.

[Fon79] Jean-Marc Fontaine. Modules galoisiens, modules filtrés et anneaux de Barsotti-Tate. In *Journées de Géométrie Algébrique de Rennes. (Rennes, 1978), Vol. III*, pages 3–80. Soc. Math. France, Paris, 1979.

[Fon82] Jean-Marc Fontaine. Sur certains types de représentations p-adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate. *Ann. of Math. (2)*, 115(3):529–577, 1982.

[Fon94a] Jean-Marc Fontaine. Le corps des périodes p-adiques. *Astérisque*, (223):59–111, 1994. With an appendix by Pierre Colmez, Périodes p-adiques (Bures-sur-Yvette, 1988).

[Fon94b] Jean-Marc Fontaine. Représentations p-adiques semi-stables. *Astérisque*, (223):113–184, 1994. Périodes p-adiques (Bures-sur-Yvette, 1988).

[FPR94] Jean-Marc Fontaine and Bernadette Perrin-Riou. Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L. In *Motives (Seattle, WA, 1991)*, pages 599–706. Amer. Math. Soc., Providence, RI, 1994.

[Gre81] Ralph Greenberg. On the Jacobian variety of some algebraic curves. *Compositio Math.*, 42(3):345–359, 1980/81.

[Gro72] A. Grothendieck. Modeles de Néron et monodromie. In *Lecture Notes in Mathematics*, volume 288. Springer-Verlag, 1972. SGA 7, Exposé IX.

[Jan88] Uwe Jannsen. Continuous étale cohomology. *Math. Ann.*, 280(2):207–245, 1988.

[KM00] Minhyong Kim and Susan H. Marshall. Crystalline subrepresentations and Néron models. *Math. Res. Lett.*, 7(5-6):605–614, 2000.

[Lan93] Serge Lang. *Algebra*. Addison-Wesley Publishing Company, Reading, MA, third edition, 1993.

[LO85] H. W. Lenstra, Jr. and F. Oort. Abelian varieties having purely additive reduction. *J. Pure Appl. Algebra*, 36(3):281–298, 1985.

[Lor90] Dino J. Lorenzini. Groups of components of Néron models of Jacobians. *Compositio Math.*, 73(2):145–160, 1990.

[Lor93] Dino J. Lorenzini. On the group of components of a Néron model. *J. Reine Angew. Math.*, 445:109–160, 1993.

[Mil86] J. S. Milne. *Arithmetic duality theorems*. Academic Press Inc., Boston, MA, 1986.

[Mok98] A. Mokrane. Quelques remarques sur l'ordinarité. *J. Number Theory*, 73(2):162–181, 1998.

[Nér64] André Néron. Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. *Inst. Hautes Études Sci. Publ.Math. No.*, 21:128, 1964.

[Neu99] Jürgen Neukirch. *Algebraic number theory.* Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[NSW00] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields.* Springer-Verlag, Berlin, 2000.

[Ray70] M. Raynaud. Spécialisation du foncteur de Picard. *Inst. Hautes Études Sci. Publ. Math.*, (38):27–76, 1970.

[Ray74] Michel Raynaud. Schémas en groupes de type $(p, \ldots, p)$. *Bull. Soc. Math. France*, 102:241–280, 1974.

[Rib90] K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[Ser79] Jean-Pierre Serre. *Local fields.* Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[Sil83] Joseph H. Silverman. The Néron fiber of abelian varieties with potential good reduction. *Math. Ann.*, 264(1):1–3, 1983.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves.* Springer-Verlag, New York, 1986.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves.* Springer-Verlag, New York, 1994.

[ST68] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[Tat67] J. T. Tate. *$p-$divisible groups.*. In *Proc. Conf. Local Fields (Driebergen, 1966)*, pages 158–183. Springer, Berlin, 1967.

[Tat76] John Tate. Relations between K_2 and Galois cohomology. *Invent. Math.*, 36:257–274, 1976.

[Tat97] John Tate. Finite flat group schemes. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 121–154. Springer, New York, 1997.

[Wac97] Nathalie Wach. Représentations cristallines de torsion. *Compositio Math.*. 108(2):185–240, 1997.