Theory of abelian varieties and their moduli spaces

Damien Robert

March 2021

[Draft Version: Tuesday September 27, 2022 at 9:13]

CONTENTS

1 INTRODUCTION

chap:intro

This notes are meant as a complement of my hdr [Rob21], which is more focused on the algorithmic aspect of abelian varieties and modular forms.

This is a partial overview of some results about abelian varieties and their moduli spaces.

An outline to learn about the subject would be to first learn about complex abelian varieties: the first chapter of Mumford's book [Mum70a] and [BL04], along with Mumford's TATA lectures [Mum83], [Mum84]. Then learn about abeian varieties, via Milne's book [Mil91] and then Mumford's book [Mum70a], complemented by the articles [Mil86; Mil85]. Then go on to more advanced topics, like abelian schemes [MFK94], Néron models [BLR12] and compactifications [FC90].

These results about abelian varieties are completed by appendix chapters about some results from algebraic geometry, group schemes and the theory of algebraic stacks.

Unfortunately there are for now incomplete. So some chapters contain only a list of planned topic, with sometime a draft version that covers more or less these topics.

A big missing topic from this outline is on how to construct points on an abelian variety over a number field: descent [Sto06], Heegner points [Bir04; Gro84], the Chabauty method [MP12], quadratic Chabauty [BD18]…Another topic missing is a quick summary of heights [HS13], Raynaud's isogeny theorem [Ray85], Faltings theorems [FWG+84; Fal86; BSa; Con+11].

I restrict to topic interesting from an algorithmic point of view: abelian scheme allow to study families of abelian varieties, degenerations allow to study their reduction, lift allow to do the converse. Pairings are used a lot in cryptographic protocols. Moduli spaces encode interesting families of abelian varieties. I apologize to the experts in algebraic geometry from my probably naive point of view on these subjects.

One of the fascinating aspect of abelian varieties is that most of the results that hold for complex abelian varieties are true in any characteristic (with the appropriate reformulations). For instance the complex lattice Λ can be replaced in most case by the Tate modules $T_\ell A$ and $T_p A$. Analytically, Λ is the dual of the singular homology $H^1(A, \mathbb{Z})$, while the Tate module $T_\ell(A)$ is the dual of the étale cohomology $H^1_t(A, \mathbb{Z}_\ell)$ and $T_p(A)$ (which is already defined contragradiently) is given by the crystalline cohomology $H^1_{crys}(A_k/W(k), \mathbb{Z}_p)$, see Section 2.2.5. As a Galois module the Tate module $T_\ell A$ is also the module associated to the divisible group $A(\ell)$ by Grothendieck's étale Galois theory, while $T_p A$ is the (contragredient) crystal associated to $A(p)$, see Chapter 3.

It is remarkable that these two abstract cohomology theories, the étale cohomology and the crystalline cohomology allow in some sense to recover the lattice Λ of complex abelian varieties in the algebraic setting. Even more remarkable is the fact that these cohomologies can be efficiently computed for an abelian variety over a finite field, paving the way for efficient point counting. Indeed, Schoof algorithm [Sch85; Sch95] on elliptic curves and its generalisation to abelian varieties in [Pil90] can be seen as an explicit version of étale cohomology computation, and is useful when the characteristic is large. We refer to [Rob21, Section 5.4] for more details, in particular on how to adapt the improvements of Elkies [Elk92; Elk92] from the case of elliptic curves to abelian surfaces. In small characteristic, one can use Kedlaya's algorithm [Ked01], which is based on Monsky-Washnitzer cohomology. Alternatively, in small characteristic one can use Satoh's method of canonical lift [Sato0], whose existence can be seen as an application of crystalline cohomology. We refer to [Gau04; Col08] for surveys of point counting algorithms, [Con08] for a survey of rigid geometry (rigid cohomology is a common generalisation of Monsky-Washnitzer cohomology and crystalline cohomology), and [Ked16a; Ked16b; Ked04; Ked07] for good introductions to p-adic cohomology and its applications to point counting.

The fact that abstract constructions become so concrete and explicit for abelian variety has been a big factor in developing these theories: just to give an example abelian varieties were keys in the construction by Grothendieck of crystalline cohomology (as the story is very well told in [Ill15], see also [Gro66a]) and of course p-adic Hodge theory started with the p-adic Hodge decomposition of abelian varieties (and p-divisible groups). Conversely, the theory is very useful to develop algorithms, for instance to transfer results from complex abelian varieties to abelian varieties over general fields (eg see Section 2.3.6).

Part I

ABELIAN VARIETIES

2 ABELIAN VARIETIES

chap:thav

CONTENTS

2.1 ABELIAN VARIETIES OVER $\mathbb{C}$

sec:avC

References for this section are [Mum70a, Chapter 1], [BL04], and a more detailed summary of these results is in [Rob10, Chapitre 2]. Analytic theta functions are studied in details in [Mum83; Mum84; Mum91]. Complete abelian varieties are completely described from their period matrices. This give an easy description of their moduli space. Algorithmically, one can use complex approximation methods to compute class polynomials or modular polynomials, via for instance the Fourier series of the corresponding modular invariants.

2.1.1 *Complex torus and cohomology*

A complex abelian variety $A/\mathbb{C}$ is a connected algebraic compact complex lie group.

It is easy to see that a connected compact complex Lie group X of dimension g is a complex torus $X = V/\Lambda$ where $V \simeq \mathbb{C}^g$ can be identified to T_0X and $\Lambda \simeq \mathbb{Z}^{2g}$ is a lattice.

The proof goes in two steps: first one prove that X is commutative, then one can either construct the isomorphism $X = V/\Lambda$ using the exponential map as in [Mum70a, §1], or by seeing $\pi : V \to X$ as the universal covering as in [BL04, Lemma 1.1.1]. This shows that $\Lambda = H_1(X, \mathbb{Z}) = \pi^1(X, 0)$.

Algebraizability is more delicate. If X is algebraizable, then it is complete (since we assumed X compact), and then it is projective (since an abelian variety over a field is always projective). Such X is algebraic if and only if it is projective. It is equivalent to check for the existence of an ample line bundle $\mathcal{L}$ on A. We first recall some cohomological results.

Since V is the universal covering of X, $\pi_1(X) = \Lambda$, so the universal coefficient theorem gives $H^1(X, \mathbb{Z}) = \mathrm{Hom}(\Lambda, \mathbb{Z})$. Künneth formula then implies $H^n(X, \mathbb{Z}) = \bigwedge^n \Lambda^*$, and the universal coefficient theorem gives $H^n(X, \mathbb{C}) = H^n(X, \mathbb{Z}) \otimes \mathbb{C} = \bigwedge^n \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{C}) = \bigwedge^n (T \oplus \overline{T}) = \bigoplus_{p+q=n} \bigwedge^p T \otimes \bigwedge^q \overline{T}$, where $T = \mathrm{Hom}_{\mathbb{C}}(V, \mathbb{C})$ is the space of linear forms on V and $\overline{T} = \mathrm{Hom}_{\overline{\mathbb{C}}}(V, C)$ is the space of antilinear forms.

Alternatively, one can use De Rham's theorem to get $H^n(X, \mathbb{C})$ as the space $IF^n(X)$ of real differential forms of degree n on V invariant by translation. We have $IF^n(X) = \bigoplus_{p+q=n} IF^{p,q}(X)$, where $IF^{p,q}(X)$ is the space spanned by forms of the form $dv_1 \wedge \cdots \wedge dv_p \wedge d\overline{v}_1 \wedge \hat{\wedge} d\overline{v}_q$, so $IF^{p,q}(X) = \bigwedge^p T \otimes \bigwedge^q \overline{T}$.

We recover the Hodge decomposition, $H^n(X, \mathbb{C}) = \bigoplus_{p+q=n} H^q(X, \Omega_X^p)$ where Ω_X^p is the sheaf of p-differential holomorphic forms. Indeed, since $O_X \otimes_{\mathbb{C}} \bigwedge^p T \xrightarrow{\sim} \Omega_X^p$, $H^q(X, \Omega_X^p) = H^q(X, O_X) \otimes \bigwedge^p T$, and from Harmonic analysis $H^q(X, O_X) \simeq IF^{0,q}(X) \simeq \bigwedge^q \overline{T}$, so $H^q(X, \Omega_X^p) = \bigwedge^p T \otimes \bigwedge^q \overline{T}$.

We note that the morphisms $H^n(X, \mathbb{Z}) \to H^n(X, \mathbb{C}) \to H^n(X, O_X)$ are the natural ones via the above isomorphisms, and the decomposition is compatible with the cup product. We refer to [Rob10, Théorème 2.3.2] for more details.

2.1.2 Line bundles

cec:linebundlesC

Now we have the commutative diagram [Rob10, Proposition 2.3.3]

$$\begin{array}{ccccc}
H^1(\Lambda, \Gamma(O_V^*)) & \longrightarrow & H^2(\Lambda, \mathbb{Z}) & & \\
\downarrow \wr & & \downarrow \wr & & \\
H^1(X, O_X^*) & \xrightarrow{c_1} & H^2(X, \mathbb{Z}) & \xrightarrow{\gamma} & H^2(X, O_X) \\
 & & \downarrow \wr & & \downarrow \wr \\
 & & \bigwedge^2 \Lambda^* & \longrightarrow & \bigwedge^2 \overline{T}.
\end{array}$$

which show that if $\mathcal{L} \in H^1(X, O_X^*)$ is a line bundle on X, then its Chern class $c_1(\mathcal{L})$ is canonically identified with a symplectic form $E \in \mathrm{Alt}_{\mathbb{R}}^2(V, \mathbb{C})$, such that furthermore $E(\Lambda, \Lambda) \subset \mathbb{Z}$ and $E(ix, iy) = E(x, y)$ for all $x, y \in V$.

We get an Hermitian form $H(x, y) = E(ix, y) + iE(x, y)$ such that $\mathrm{Im}\, H(\Lambda, \Lambda) \subset \mathbb{Z}$. Thus two line bundles $\mathcal{L}_1$ and $\mathcal{L}_2$ are algebraically equivalent if and only if they have the same Hermitian form. Conversely by the diagram above, these type of Hermitian forms span the Néron-Severi group $\mathrm{NS}(X) := \ker H^2(X, \mathbb{Z}) \to H^2(X, O_X)$. Furthermore, given H, $\mathcal{L}$ can be recovered from a canonical choice of its automorphic factor $a_{\mathcal{L}} \in Z^1(\Lambda, \Gamma(O_V^*))$ as $a_{\mathcal{L}}(\lambda, v) = \chi(\lambda) e^{\pi H(v,\lambda) + \frac{\pi}{2} H(\lambda,\lambda)}$, where χ is a semi-character: $\chi(\lambda_1 + \lambda_2) = \chi(\lambda_1)\chi(\lambda_2) e^{i\pi E(\lambda_1, \lambda_2)}$. We call H, the polarisation associated to $\mathcal{L}$. From this we deduce [Rob10, Théorème 2.3.6]:

Theorem 2.1.1 (Appell-Humbert). *We have a commutative diagram:*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}(\Lambda, \mathbb{C}_1^*) & \longrightarrow & \textit{Group of } (H, \chi) & \longrightarrow & \begin{array}{l}\textit{Hermitian forms}\\ \textit{on } V \textit{ such that}\\ \mathrm{Im}\, H(\Lambda, \Lambda) \subset \mathbb{Z}.\end{array} & \longrightarrow & 0 \\
 & & \downarrow \wr & & \downarrow \wr & & \downarrow \wr & & \\
0 & \longrightarrow & \mathrm{Pic}_0(X) & \xrightarrow{c_1} & \mathrm{Pic}(X) & \longrightarrow & \mathrm{NS}(X) & \longrightarrow & 0.
\end{array}$$

n@appell@humbert

We will denote $H_{\mathcal{L}}$ (or $E_{\mathcal{L}}$), $\chi_{\mathcal{L}}$ the Hermitian form (or symplectic form) and quasi-character associated to the line bundle $\mathcal{L}$, and conversely $L(H,\chi)$ the line bundle associated to H and χ.

It remains to identify the ample line bundles.

schetzavc

Theorem 2.1.2 (Lefschetz). *A line bundle $\mathcal{L}$ is ample if and only if its associated Hermitian form H is positive. In this case $\mathcal{L}^3$ is very ample.*

Proof. See [Mum70a, p. 30] or [BL04, Theorem 4.5.1]. Here we implicitly use that by Chow's theorem a closed analytic subset of a complete complex algebraic variety is Zariski closed, hence an analytic embedding into the projective space give an algebraic embedding. □

polsquare

Remark 2.1.3. The case of $\mathcal{L}^2$ is detailed in [BL04, §4.4, §4.5, §4.8]. $(A,\mathcal{L}) \simeq (A_0,\mathcal{L}_0) \times_{i=1}^{k} (A_i,M_i)$ where M_i is principal and $\mathcal{L}_0$ is without fixed component. Then $\mathcal{L}_0^2$ is very ample, and M_i^2 descend to a very ample line bundle on the Kummer variety $K_{A_i} := A_i/\pm 1$. In particular, if A is indecomposable and $\mathcal{L}$ principal, $\mathcal{L}^2$ gives an embedding of the Kummer variety K_A.

In summary, a complex abelian variety $A/\mathbb{C}$ is given by three data

- *Linear data*: A complex vector space V of dimension g;
- *Arithmetic data*: A $\mathbb{Z}$-lattice Λ of rank $2g$ in V
- *Quadratic data*: A positive Hermitian form H.

2.1.3 Polarisations

The Hermitian form H is only intrinsic to A as a *polarized abelian variety*. In particular, H can essentially be seen as a way to embed A into projective space, or as an isogeny to its dual.

Indeed, whenever $\mathcal{L}$ is a non degenerate line bundle (meaning that $H = H_{\mathcal{L}}$ is non degenerate), then since the quotient of two quasicharacter is a character, we see that all the other quasi-characters are of the form $\chi = \chi_{\mathcal{L}} H(c,\cdot)$. In particular $L(H,\chi) = t_c^*\mathcal{L}$ is a translate of $\mathcal{L}$. So whenever $\mathcal{L}$ is very ample, the map $A \to \mathbb{P}^*(\Gamma(A,\mathcal{L}))$ is determined by H up to translation. Furthermore, if $\Lambda = \Lambda_1 \oplus \Lambda_2$ is a symplectic decomposition of Λ for E, $\chi_0(\lambda) = e^{i\pi E(\lambda_1,\lambda_2)}$ is a canonical symmetric semi-character, hence this decomposition induces a canonical symmetric line bundle $\mathcal{L}_0$ in the algebraic equivalence class of $\mathcal{L}$.

The dual abelian variety $\widehat{A}$ of A is $\mathrm{Pic}_A^0 = \mathrm{Hom}(\Lambda,\mathbb{C}_1^*) = \mathrm{Hom}_{\overline{\mathbb{C}}}(V,\mathbb{C})/\overline{\Lambda} = \overline{V}/\overline{\Lambda}$ where $\overline{\Lambda}$ is the $\mathbb{Z}$-dual of Λ for the canonical pairing $(v,f) \mapsto \Im f(v)$. This canonical pairing induces the Poincaré $\mathcal{P}$ bundle on $A \times \widehat{A}$, whose Hermitian form on $V \times \overline{V}$ is $H((v_1,f_1),(f_2,v_2) = f_2(v_1) + \overline{(}f_1(v_2))$[1]. In particular $\phi_H : A \to \widehat{A}, x \mapsto H(x,\cdot)$ is well defined and induce an isogeny from A to its dual. Algebraically, the point $\phi_H(x) \in \mathrm{Pic}_A^0$ corresponds to the degree 0, line bundle on A represented by the character $e^{2i\pi E(x,\cdot)}$, in other words $\phi_H(x) = t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$. We will also denote the last morphism as $\phi_{\mathcal{L}}$.

Pulling back the canonical pairing induced by the Poincarré bundle by $\mathrm{Id} \times \phi_H$ gives a pairing on $A \times A$; analytically this is the pairing induced by H on $V \times V$ (or by E on $\Lambda \times \Lambda$). This is the Weil pairing induced by the polarisation, which we will study in more details in Chapter 4.

The kernel $K(H)$ (also denoted $K(\mathcal{L})$) of ϕ_H is given by $\Lambda(H)/\Lambda$ where $\Lambda(H)$ is the $\mathbb{Z}$-dual of Λ for E: $\Lambda(H) = \{v \in V \mid E(v,\cdot) \subset \mathbb{Z}\}$. Algebraically, $K(\mathcal{L})$ is the set of translates of $\mathcal{L}$ isomorphic to it. When $\mathcal{L}$ is ample, its degree d of $\mathcal{L}$ can be defined via the degree of the g-fold intersection (of an effective divisor representing it) $d = (\mathcal{L}\cdot\mathcal{L}\cdots\mathcal{L})/g!$. The cardinal of $K(\mathcal{L})$ is then d^2, and the rank of $\Gamma(A,\mathcal{L})$ is d. An explicit basis of d sections is given by the analytic theta functions. It is easier to define them by looking at a period matrix of Λ.

2.1.4 Period matrix

Since E is integral on Λ, there is a "symplectic" basis such that the action of E is given by the matrix

$$M_\delta = \begin{pmatrix} 0 & D_\delta \\ -D_\delta & 0 \end{pmatrix}$$

[1] And $\mathcal{P}$ is the line bundle corresponding to the symplectic decomposition $\Lambda \oplus \overline{\Lambda}$

where D_δ is the diagonal matrix $\delta = (\delta_1, \delta_2, \dots, \delta_g)$, with $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_g$ and $\delta_i > 0$ for $i \in [1..g]$. We say that $\mathcal{L}$ is of type δ, since $K(\delta) \simeq (\mathbb{Z}^g/\delta\mathbb{Z}^g)^2$, the degree d of $\mathcal{L}$ is then $d = \prod \delta_i = \det D_\delta$. Taking the corresponding symplectic decomposition $\Lambda = \Lambda_1 \oplus \Lambda_2$, we may take a basis of V such that $\Lambda = D_\delta\mathbb{Z}^g \oplus \Omega'\mathbb{Z}^g$. Then $\Omega \in \mathfrak{H}_g$, the Siegel space of symmetric matrices Ω with $\Im\Omega > 0$. In this basis, $H = (\Im\Omega)^{-1}$, and $E(x_1 + \Omega x_2, y_1 + \Omega y_2) = x_1 y_2 - x_2 y_1$.

For $\Omega \in \mathfrak{H}_g$ and $a, b \in \mathbb{Q}^g$, analytic theta functions are defined as

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \Omega) = \sum_{n \in \mathbb{Z}^g} e^{\pi i {}^t(n+a)\Omega(n+a) + 2\pi i {}^t(n+a)(z+b)}. \tag{2.1}$$

{eq@theta

and a basis of section of $\mathcal{L}_0$ is given by $(\theta\left[\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right](\cdot, \Omega))_{a \in D^{-1}\mathbb{Z}^g/\mathbb{Z}^g}$. (More precisely these analytic functions are sections of a different factor of automorphy than $a_{\mathcal{L}_0}$, see [Rob10, § 2.6].)

Via the change of variable $z \mapsto D^{-1}z$, we have $\Lambda = \Omega'\mathbb{Z}^g \oplus \mathbb{Z}^g = \Omega_0 D \oplus \mathbb{Z}^g$, where $\Omega_0 \in \mathfrak{H}_g$, $\Omega = D\Omega_0 D$, $\Omega' = \Omega_0 D$. For these new coordinates, $H = (\Im\Omega_0)^{-1}$, the old basis is then $(\theta\left[\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right](D\cdot, D\Omega'))_{a \in D^{-1}\mathbb{Z}^g/\mathbb{Z}^g}$, and another basis is given by $(\theta\left[\begin{smallmatrix} 0 \\ b \end{smallmatrix}\right](\cdot, \Omega' D^{-1}))_{b \in D^{-1}\mathbb{Z}^g/\mathbb{Z}^g} = \theta\left[\begin{smallmatrix} 0 \\ b \end{smallmatrix}\right](\cdot, \Omega_0)$.

In particular, if $\mathcal{L}_0$ is of degree 1 (in other words $\mathcal{L}$ is a principal line bundle, and $(A, \mathcal{L})$ is a principally polarised abelian variety), with hermitian form H, then the hermitian form corresponding to $\mathcal{L}_0^n$ is nH, and if $n = n_1 n_2$ a basis of sections (called theta functions of level n) is given by $(\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](n_1\cdot, n_1\Omega_0/n_2))_{a,b \in \frac{1}{n_1}\mathbb{Z}^g/\mathbb{Z}^g \times \frac{1}{n_2}\mathbb{Z}^g/\mathbb{Z}^g}$.

2.1.5 *Isogenies*

A group morphism $f : A \to B$ between two abelian varieties is induced by the linear morphism $\rho(f) : T_0 A \to T_0 B$, f is an isogeny whenever $\rho(f)$ is bijective. The kernel of the isogeny is then $f^{-1}\Lambda_B/\Lambda_A$. If $\mathcal{M}$ is a polarisation on B with associated Hermitian form H_M, then $\mathcal{L} = f^*\mathcal{M}$ has associated Hermitian form $H_{\mathcal{L}}(\rho(f)(\cdot), \rho(f)(\cdot))$.

If $f : A \to B$ is an isogeny, the complex transpose $\rho(f)^* = \overline{{}^t\rho(f)}$ induce a dual isogeny $\hat{f} : \hat{B} \to \widehat{A}$. In particular, $\operatorname{Ker} f$ is the dual of $\operatorname{Ker} \hat{f}$, and description of $H_{\mathcal{L}}$ above show that we have $\Phi_{f^*\mathcal{M}} = \hat{f} \circ \Phi_M \circ f$, and

2.2 ABELIAN VARIETIES

sec:av

This is the core object of this work. The best reference on this subject is still [Mum70a], even 50 years after its publication! One can also consult [Mil85; Mil86] for the treatment of Jacobians and simplifications made by using the étale cohomology, Milne's course notes [Mil91] (which essentially restrict to separable isogenies) , Bhatt's course notes [Bha] and also the unfortunately still unfinished [MGE12]. A modern point of view via the Fourier-Mukai transform is in [Pol03].

Remark 2.2.1. In [Mum70a] Mumford works with an algebraically closed field. But his result generally hold for a perfect field k by Galois descent, or even for an arbitrary field by fpqc descent. (Essentially assuming k perfect allows to describe étale finite groups G via their $\bar{k}$-points $G(\bar{k})$, while for a general k we would use $G(k_s)$ instead where k_s is the separable closure of k.) The book [MGE12] gives explicit statements over any field.

2.2.1 *Definition*

av:def

Definition 2.2.2. An abelian variety A/k is a proper geometrically integral group scheme over k.

From the discussion on algebraic group Appendix B.1, we have:

prop:caracav

Proposition 2.2.3. *The following are equivalent:*

- *A/k is an abelian variety;*
- *A/k is a proper smooth (geometrically) connected[2] group scheme;*

[2] Since 0_A is rational, A connected $\Leftrightarrow$ A geometrically connected.

- *A/k is a proper group scheme, geometrically reduced[3] and (geometrically) connected;*
- *A/k is a connected group scheme locally of finite type, universally closed and whose neutral point 0_A is geometrically reduced[4];*

2.2.2 Basic properties of abelian varieties

As the name imply, we have [Mum70a, Chapter II]:

Proposition 2.2.4. *If A/k is an abelian variety, it is commutative and projective.*

Projectivity was not known to Weil when he developed the theory of abelian varieties to prove the Weil conjecture for curves, hence he had to introduce abstract algebraic varieties. It was then proved by Chow for Jacobians, and by Barsotti, Matsusaka and Weil for abelian varieties.

Quite a lot of the geometric theory of abelian varieties can be derived from Weil's theorem of the cube:

Theorem 2.2.5 ([Mum70a, §6, §10]). *Let $k = \overline{k}$ be an algebraically closed field. If X, Y are complete varieties and Z a connected scheme over k. Let $\mathcal{L}$ a line bundle on $X \times Y \times Z$ whose restriction to $\{x_0\} \times Y \times Z$, to $X \times \{y_0\} \times Z$, and $X \times Y \times \{z_0\}$ is trivial for some $x_0 \in X$, $y_0 \in Y$, $z_0 \in Z$. Then $\mathcal{L}$ is trivial.*

We get the following corollaries [Mum70a, § 6, Cor 2, 3, 4]:

th:square

Corollary 2.2.6.

- *If f, g, h are morphisms from a variety X to an abelian variety A, for all $\mathcal{L} \in \mathrm{Pic}(A)$,*

$$(f+g+h)^*\mathcal{L} \simeq (f+g)^*\mathcal{L} \otimes (f+h)^*\mathcal{L} \otimes (g+h)^*\mathcal{L} \otimes f^*\mathcal{L}^{-1} \otimes g^*\mathcal{L}^{-1} \otimes h^*\mathcal{L}^{-1}.$$

- *For all $n \in \mathbb{Z}$, $[n]^*\mathcal{L} \simeq \mathcal{L}^{\frac{n^2+n}{2}} \otimes [-1]^*\mathcal{L}^{\frac{n^2-n}{2}}$. In particular if $\mathcal{L}$ is symmetric, $[n]^*\mathcal{L} \simeq \mathcal{L}^{n^2}$ and if $\mathcal{L}$ is antisymmetric, $[n]^*\mathcal{L} \simeq \mathcal{L}^n$.*
- Theorem of the square: *$t_{x+y}^*\mathcal{L} \otimes \mathcal{L} \simeq t_x^*\mathcal{L} \otimes t_y^*\mathcal{L}$ where t_x denotes the translation by x.*

Another very nice property is that rational map to an abelian variety extends:

tensionav

Proposition 2.2.7. *A rational map XA from a regular variety X to an abelian variety is defined everywhere on X.*

Proof. This is [Mil91, Theorem 3.2] using that a rational map XY from a normal variety to a complete variety is defined everywhere except at a locus of codimension ≥ 2 [Mil91, Theorem 3.1] and that a rational map XG from a non singular variety to a group variety is defined everywhere except at a locus of pure codimension 1 (if non empty) [Mil91, Lemma 3.3].

See Proposition 2.3.16 and Proposition 3.1.7 for a generalisation of these theorems to abelian schemes and group schemes. □

2.2.3 Isogenies

isogenies

Definition 2.2.8. An isogeny of abelian varieties $f : A \to B$ is a finite surjective group morphism.

If $\dim A = \dim B$ and $f : A \to B$ is a group morphism, it suffices to check that $\mathrm{Ker} f$ is finite or that f is surjective. The isogeny is étale whenever it is separable. In fact, if A is an abelian variety and $\pi : X \to A$ is an étale cover by a connected scheme, then X is an abelian variety and π is a separable isogeny.

Commutativity of abelian varieties can also be seen as a corollary of the following rigidity theorem:

Theorem 2.2.9 (Rigidity of abelian varieties [Mum70a, Theorem p.44]). *If X is a complete variety with a point e and a morphism $m : X \times X \to X$ such that $m(x,e) = m(e,x) = x$ for all geometric points x, then (X, m) is an abelian variety.*

[3] If k is perfect, this is equivalent to A/k reduced

[4] Or just reduced if k is perfect

As a corollary, if A, B are abelian varieties, any morphism (as varieties) $f : A \to B$ which sends 0_A to 0_B is a group morphism, so a morphism of variety $f : A \to B$ is the composition of a group morphism and a translation.

If A is an abelian variety, there is a canonical structure of abelian variety on $\widehat{A} = \mathrm{Pic}^0(A)$, and there is a universal Poincare bundle $\mathcal{P}$ on $A \times \widehat{A}$ [Mum70a, §8, §13]. It is rigidified along the zero sections of A and $\widehat{A}$ and its universal property is that any line bundle $\mathcal{L}$ on $A \times S$ rigidified along the pullback $0_A \times S$ of the neutral point of A and such that $\mathcal{L}_s \in \mathrm{Pic}^0 A$ for all geometric point of s is the pullback of $\mathcal{P}$ by a unique morphism $\phi : S \to \widehat{A}$. By this universal property, the Poincare line bundle itself induces a canonical morphism $A \to \widehat{A}^\vee$, and it is an isomorphism by [Mum70a, §13].

If $f : A \to B$ is an isogeny, the morphism $f^* : \mathrm{Pic}^0(B) \to \mathrm{Pic}^0(A), \mathcal{M} \to f^*\mathcal{M}$ induce an isogeny $\hat{f} : \hat{B} \to \widehat{A}$. We call $\hat{f}$ the dual isogeny, and by biduality of A, $\mathrm{Ker}\hat{f}$ is the Cartier dual of $\mathrm{Ker} f$ [Mum70a, §14, §15 Theorem 1].

The degree $\deg f$ of an isogeny can be defined as the degree $\deg f$ (as a scheme) of its kernel $\ker f$, so by duality f and $\hat{f}$ have the same degree. We then have $\chi(f^*\mathcal{M}) = \deg f \chi(\mathcal{M})$ for any line bundle $\mathcal{M}$ on B.

If α is an endomorphism of A, its characteristic polynomial is defined by $\chi_\alpha(n) = \deg(\alpha - n)$ for $n \in \mathbb{Z}$. It is monic of degree $2g$, and can be computed as its characteristic polynomial acting on $V_\ell A := T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ [Mil91, Theorem 10.9] (see Section 2.2.5 for these definitions).

2.2.4 Line bundles

ec:avlinebundles

If $\mathcal{L}$ is a line bundle, then by the theorem of the square (Corollary 2.2.6) $t_{x+y}^*\mathcal{L} \otimes \mathcal{L} \simeq t_x^*\mathcal{L} \otimes t_y^*\mathcal{L}$ so $\Phi_\mathcal{L} : x \mapsto t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$ is a morphism from A to $\widehat{A}$, of kernel $K(\mathcal{L})$. If the line bundle $\mathcal{L}$ is ample then $\Phi_\mathcal{L}$ is an isogeny, it is the polarisation associated to $\mathcal{L}$.

th:polarisations

Theorem 2.2.10. *Let $\mathcal{L}$ be a line bundle on an abelian variety A.*

- *Riemann-Roch: if $\mathcal{L} = O_X(D)$, $\chi(\mathcal{L}) = (D^g)/g!$;*
- $\deg \Phi_\mathcal{L} = \chi(L)^2$;
- *Vanishing theorem: if $\mathcal{L}$ is non degenerate (which means $K(\mathcal{L})$ is finite), there is a unique integer $0 \leq i(\mathcal{L}) \leq g$ such that $H^i(A, \mathcal{L}) \neq 0$. Moreover $i(\mathcal{L}^{-1}) = g - i(\mathcal{L})$.*

And $\mathcal{L}$ is ample if and only if it is non degenerate and $i(\mathcal{L}) = 0$, if and only if $\Phi_\mathcal{L}$ is an isogeny and $\mathcal{L}$ is represented by an effective divisor.

Proof. See [Mum70a, §16]. The index $i(\mathcal{L})$ is equal to the number of positive roots of the polynomial $P(n) = \chi(\mathcal{L}^n \otimes M)$, M any non ample line bundle. In the complex case, this is the number of negative eigenvalues of $H_\mathcal{L}$. □

If $\mathcal{L}$ is degenerate, $\mathcal{L}$ and its sections descend to $A/K^\circ(\mathcal{L})$ where $K^\circ(\mathcal{L})$ is the connected component of 0_A in $K(\mathcal{L})$, so we reduce to the non degenerate case.

Lefschetz theorem still holds:

th:lefschetzav

Theorem 2.2.11 (Lefschetz)**.** *If $\mathcal{L}$ is ample, then $\mathcal{L}^2$ is base point free and induce a finite morphism into projective space, and $\mathcal{L}^3$ is very ample.*

Proof. See [Mum70a, §17]. □

2.2.5 Cohomology

ec:av:cohomology

By [Mum70a], some of the cohomology computations of Section 2.1 hold in the algebraic case. Let A/k be an abelian variety over an algebraically closed field $k = \bar{k}$. Then $H^q(A, \Omega^p) \simeq \bigwedge^p H^0(A, \Omega^1) \otimes_k \bigwedge^q H^1(A, O_{A_k})$. Furthermore Ω_A^1 is canonically isomorphic to $\Omega_0 \otimes_k O_X$ where $\Omega_0 = T_{A,0}^*$ is the cotangent space. Via this isomorphism, the image of Ω_0 are the translation invariants differential forms, and since $H^0(A, O_{A_k}) = k$ these are exactly the forms regular everywhere, ie the global sections of Ω_A^1: $T_0(A) = \mathrm{Lie}(A) \simeq H^0(A, \Omega^1)^\vee$. We also have a canonical isomorphism $\mathrm{Lie}(\widehat{A}) = T_0\widehat{A} \simeq H^1(A, O_{A_k})$.

Now let k be any field, p its characteristic, and let A/k be an abelian variety. Instead of a lattice, we can consider the divisible group $\varinjlim_{p\nmid n} A[n](k_s)$ or the Tate module $\varprojlim_{p\nmid n} A[n](k_s)$.

By the Chinese Remainder Theorem, it suffices to consider the ℓ-divisible group for $\ell \neq p$: $A(\ell) \coloneqq \varinjlim_n A[\ell^n](k_s)$ and the ℓ-Tate module $T_\ell A = \varprojlim_n A[\ell^n](k_s)$.

We recall that $[n]$, the multiplication by n is an isogeny of degree n^g, and is separable if and only if $p \nmid n$, in which case the kernel $A[n](k_s)$ is isomorphic to $\mathbb{Z}^{2g}/n\mathbb{Z}^{2g}$. The multiplication by p is never separable, and $A[p](k_s) = \mathbb{Z}^r/p\mathbb{Z}^r$ where $0 \leq r \leq g$ is called the p-rank of A. Then $A[p^m](k_s) = \mathbb{Z}^r/p^m\mathbb{Z}^r$.

An abelian variety is ordinary if its p-rank is 0. Be careful that unlike the elliptic case, an abelian variety of p-rank 0 may not be supersingular: for A to be supersingular we need that the only slope of its Newton polygon is $1/2$ (so in dimension 2, A is of p-rank 0 still imply that A is supersingular because there is only one possibility for its Newton polygon). In this case A is isogenous to a product of supersingular elliptic curves, it is called superspecial if it is isomorphic to such a product. We refer to [Prio8; AP15] for more details.

When $\ell \neq p$, the Tate module is a good substitute of the period lattice, because it is recovered by the étale cohomology:

:etalecoh

Theorem 2.2.12.

$$H^1_t(A_{k_s}, \mathbb{Z}_\ell) \simeq \mathrm{Hom}_Z(\bar{\ell})(T_\ell A, \mathbb{Z}_\ell)$$
$$H^q_t(A_{k_s}, \mathbb{Z}_\ell) \simeq \Lambda^q H^1_t(A, \mathbb{Z}_\ell)$$

where these isomorphisms are compatible with the Galois action, and the bottom isomorphism is induced by the first via the cup product.

Proof. See [Mil86], [Mil, §12]. By Galois theory, $H^1(A, Z(\bar{\ell})) = \mathrm{Hom}(\pi_1^t A, Z(\bar{\ell}))$, so $H^1(A, Z(\bar{\ell}))$ is the dual of the Galois module associated to $A(\ell)$, and this is exactly $T_\ell A$, see Section 3.3.2. □

In particular if $A/\mathbb{C}$ is a complex abelian variety, we get $H^1_t(A_{\mathbb{C}}, \mathbb{Z}_\ell) \simeq \Lambda^* \otimes \mathbb{Z}_\ell = H^1(A, \mathbb{Z}_\ell)$ as expected from Grothendieck's comparison theorem [Gro71, Exposé XII], [Art66].

If A/K is an abelian variety over a p-adic field K, we let $\overline{K}$ denote the algebraic closure and $\mathbb{C}_p$ the completion of $\overline{K}$. Seeing $\mathbb{C}_p$ as a $G_K = \mathrm{Gal}(\overline{K}/K)$-Galois module, we denote by $\mathbb{C}_p(1)$ the Tate twist. Then the Hodge decomposition $H^1(A, \mathbb{C}) = H^0(A, O_A) \oplus H^0(A, \Omega^1_A)$ of a complex abelian variety has a p-adic analogue:

Theorem 2.2.13 (Hodge-Tate decomposition)**.** *Let A/K be an abelian variety, $S = \mathrm{Spec}\, O_K$ and η its generic point, $\overline{\eta}$ the geometric point above η corresponding to $\overline{K}$. Then A can be seen as an abelian variety over η, and*

$$H^1_t(A_{\overline{\eta}}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{C}_p \simeq H^0(A, \Omega^1_{A/\eta}) \otimes_K \mathbb{C}_p(-1) \oplus H^1(A, O_A) \otimes_K \mathbb{C}_p$$

(the isomorphism is Galois equivariant).

Proof. If A/K has good reduction, this is proved by Tate in [Tat67] using the theory of p-divisible groups, see [Ser66, Théorème 3].

The general case is proved by Raynaud in [Gro72, Exposé 9, Théorème 3.6 et Proposition 5.6]. The general Hodge-Tate decomposition for a proper smooth scheme is proved by Faltings (among others) in [Fal88b], as a special case of the étale cohomologie and crystalline/De Rham cohomology comparison theorems using Fontaine's period rings [Fon82; Fal88b; Fal88a]. We refer to [ABB+19; Car19] for a good exposition of p-adic Hodge theory.

Dually: $H^0(A, \Omega^1_{A/K})^\vee \simeq \mathrm{Lie}(A)$ and $H^1(A, O_A) \simeq \mathrm{Lie}(A^\vee)$ and the Hodge-Tate decomposition is $T_p(A) \otimes_{\mathbb{Z}_p} \mathbb{C}_p \simeq (\mathrm{Lie}(A^\vee)^\vee \otimes_K \mathbb{C}_p) \oplus (\mathrm{Lie}(A) \otimes_K \mathbb{C}_p(1))$.

And since the Weil pairing induces a perfect pairing $T_pA \times T_p\widehat{A} \to \mathbb{Z}_p(1)$, we have $H^1_t(A_{\overline{\eta}}, \mathbb{Z}_p(1)) \simeq \mathrm{Hom}_{\mathbb{Z}_p}(T_p(A_\eta), \mathbb{Z}_p(1)) \simeq T_p\widehat{A}$, hence the Hodge-Tate decomposition gives isomorphisms $T_0\widehat{A} \simeq H^1(A, O_A) \simeq \mathrm{Hom}_{\mathbb{Z}_p[G_K]}(T_p(A_{\overline{\eta}}), \mathbb{C}_p)$ and $H^0(A, \Omega^1_{A/\eta}) \simeq \mathrm{Hom}_{\mathbb{Z}_p[G_K]}(T_p(A_{\overline{\eta}}), \mathbb{C}_p(1))$. □

When $\ell = p$, the Tate module is not enough to recover all the arithmetic information of A. We define instead T_pA to be the Dieudonné module of the p-divisible group. We recall that the crystalline cohomology of a smooth

proper scheme can be seen either as the sheaf cohomology of the crystalline site [Ill94], or as the hypercohomology of its De Rahm-Witt complex [Ill79], or as the De Rham (hyper)cohomology of any proper smooth lift [Ber06; BJ11].

As expected, crystalline cohomology is the correct one when $\ell = p$:

Theorem 2.2.14 (Mazur-Messing-Oda)**.**

$$H^1_{crys}(A_k/W(k), \mathbb{Z}_p) \simeq T_p(A)$$
$$H^q_{crys}(A_k/W(k), \mathbb{Z}_p) \simeq \Lambda^q H^1_{crys}(A_k/W(k), \mathbb{Z}_p).$$

2.2.6 *Abelian varieties over finite fields*

TODO: endomorphisms, classification, Honda-Tate.

2.3 ABELIAN SCHEMES

sec:abschemes

Algorithmically, abelian schemes allow to study families of abelian varieties (for instance to construct families of abelian surfaces with real multiplication). They are also useful to construct the moduli of abelian varieties (which as we will see in Section 2.3.6 allow us to extend results over $\mathbb{C}$ to results over any field), and to study reduction modulo p.

There is a surprising lack of textbooks on this subject. But as we will see, because of rigidity most of the theory reduce immediately to abelian varieties. Rigidity of abelian schemes is proved in [MFK94, Chapter 6] for projective abelian schemes. Projectivity[5] was needed to ensure the existence of the dual abelian scheme, this was later proven in the general case by Artin and Raynaud, see [FC90, Chapter 1]. Raynaud's book [Ray06] contains many wonderful result about projectivity of group schemes, and in particular abelian schemes. SGA 7 also contains a wealth of results on abelian schemes [Gro72] (like the semi-stable reduction theorem and a fine study of duality via the theory of biextensions), and SGA 3 [DA70] is also useful in the study of quotients (eg to construct isogenies).

2.3.1 *Definitions*

def:avscheme

Definition 2.3.1. Let S be a scheme. An abelian scheme A/S is a proper smooth group scheme $A \to S$ with geometrically connected fibers.

By Proposition 2.2.3, an abelian scheme has abelian varieties as its geometric fibers, so alternatively an abelian scheme A/S is a flat proper finitely presented group scheme with abelian varieties as geometric fibers. We refer to Section 2.3.5 for other characterisations.

Since an abelian scheme is flat by definition, a lot of properties can be checked fiberwise. For instance if $f : A \to B$ is an application between abelian schemes, it is

- Flat if and only if it is fiberwise flat [Stacks, Tag 039C];
- (Schematically) dense if it is fiberwise (schematically) dense [GD64, pp. IV.11.10.9, IV.11.10.10].

Furthermore, since A is proper, and $\mathcal{L}$ is a line bundle on A, then the locus U of $s \in S$ such that $\mathcal{L}_s$ is ample is open, and $\mathcal{L}_{|U}$ is ample over U [GD64, p. IV.9.6.5].

Sometimes abelian schemes are constructed étale locally, as in the construction of the dual abelian variety (see Section 2.3.2). The resulting algebraic space is actually a scheme.

th:algabelian

Theorem 2.3.2 (Raynaud)**.** *Let A/S be an abelian algebraic space. Then A is an abelian scheme. If S is affine, A/S is an AF-scheme*[6]*.*

[5] Unlike abelian varieties, an abelian scheme need not be projective

[6] See Appendix D for the definition.

Proof. We refer to [FC90, Theorem 1.9] for a proof. The affine finite condition will be useful to construct isogenies in Proposition 2.3.15. □

An abelian scheme needs not be projective (see [Ray06] for counterexamples). By a theorem of Murre [Mur64, p. 258], it is if the base S is integral and normal. More generally:

Theorem 2.3.3 (Grothendieck). *Let S be an integral scheme with generic point $\eta = \eta_S$ geometrically unibranch. Let A/S be an abelian scheme, and $\mathcal{L}_\eta$ invertible on A_η. Then there exists a symmetric line bundle $\mathcal{M}$ such that $\mathcal{M}_\eta$ is algebraically equivalent to $\mathcal{L}_\eta^2$. If $\mathcal{L}_\eta$ is ample then $\mathcal{M}$ is S-ample. In particular A/S is projective.*

Proof. This is [Ray06, Th XI.1.4]. □

2.3.2 The relative Picard functor and the dual abelian scheme

sec:picard

We begin by a disgression on the relative Picard functor. This will allow us to construct the dual abelian scheme, and also Jacobians of (relative) curves in Section 2.4 Much more details can be found in [BLR12, Chapter 8] (but beware of the missing hypotheses in some of their statements).

If X/S is a scheme, the Picard functor $\mathrm{Pic}(X)$ is the set of isomorphism classes of line bundles on X. Since a line bundle is the same as a $\mathbb{G}_m$-torsor, $\mathrm{Pic}(X) \simeq H^1(X, O_X^*)$. By fpqc descent of line bundles[7], this isomorphism is true in the Zariski, étale, fppf or even fpqc topology.

The relative Picard functor $\mathcal{P}ic_{X/S}$ is defined to be $Rf_{*,fppf}\mathbb{G}_m$ [BLR12, Definition 8.1.2], in other words it is the fppf-sheafication of the presheaf $\mathrm{Pic}_{X/S} : T/S \mapsto \mathrm{Pic}(X_T)$, where we denote by X_T the pullback $X_T := X \times_S T$. If X/S is proper, $\mathcal{P}ic_{X/S} = Rf_{*,tale}\mathbb{G}_m$ [BLR12, p. 203].By construction, it commutes with base change.

If X/S is qcqs, the Leray spectral sequence induces an exact sequence [BLR12, p. 203]

$$0 \to H^1(S, f_*(\mathbb{G}_m)) \to H^1(X, \mathbb{G}_m) \to \underset{X/S}{\mathcal{P}ic}(S) \to H^2(S, f_*\mathbb{G}_m) \to H^2(X, \mathbb{G}_m) \tag{2.2}$$

{eq:leray}

We say that f is an O-morphism when $f_*O_X = O_S$. In this case the pullback by a flat base change is still an O-morphism (ie, in the terminology of [MFK94] this notion is uniform). We say that f is an universal O-morphism if the pullback by an arbitrary morphism is an O-morphism. If f is an O-morphism, then for every $T \to S$ flat (resp. every $T \to S$ if f is an universal O-morphism), the exact sequence from Equation (2.2) can be interpreted as follow [BLR12, Proposition 8.1.4]

$$0 \to \mathrm{Pic}(T) \to \mathrm{Pic}(X_T) \to \underset{X/S}{\mathcal{P}ic}(T) \to \mathrm{Br}(T) \to \mathrm{Br}(X_T) \tag{2.3}$$

{eq:leray2}

So if the map $\mathrm{Br}(T) \to \mathrm{Br}(X_T)$ is injective, for instance if $X \to S$ has a section, then the exact sequence collapse to to

$$0 \to \mathrm{Pic}(T) \to \mathrm{Pic}(X_T) \to \underset{X/S}{\mathcal{P}ic}(T) \to 0 \tag{2.4}$$

{eq:leray3}

In particular, when X/S has a section e, then there is an alternative definition of $\mathcal{P}ic_{X/S}$ that is easier to describe than the sheafication process: $\mathcal{P}ic_{X/S}(T)$ is isomorphic to the group of isomorphism class of line bundles $\mathcal{L}$ on $X \times_S T$ rigidified along the pullback of e, ie there is an isomorphim $O_T \simeq e_T^*\mathcal{L}$. Indeed, up to an action of $\mathrm{Pic}(T)$ each line bundle on X_T can be rigidified, so since rigidified line bundles have no automorphism, the set of rigidified line bundles is isomorphic to $\mathrm{Pic}(X_T)/\mathrm{Pic}(T)$.

We have the following representability theorems of the relative Picard functor. First if $f : X \to S$ is proper flat and finitely presented with S reduced, then if $\mathcal{P}ic_{X/S}$ is representable by an algebraic space, f has to be cohomologically flat in dimension 0[8] by [BLR12, Remark 8.3.2].

Remarkably, cohomological flatness is enough for representability.

th:picard

Theorem 2.3.4. *Let $f : X \to S$ be a proper locally finitely presented flat morphism of algebraic spaces, cohomologically flat in dimension* 0.

[7] This is a special case of Grothendieck's fpqc descent of quasi-coherent modules, but for line bundles this can also be seen as an application of Hilbert 90

[8] We refer to Appendix A.2 for the definition of a morphism cohomologically flat in dimension 0.

th:picardi (i) *$\mathcal{P}ic_{X/S}$ is an (qs) algebraic space.*

th:picardii (ii) *If furthermore f is a universal O-morphism and admits a section, then $X \times_S \mathcal{P}ic_{X/S}$ has a universal rigidified line bundle.*

th:picardiii (iii) $\mathrm{Lie}(\mathcal{P}ic_{X/S}) \simeq R^1 f_* O_X$;

th:picardiv (iv) *If $H^2(X_s, O_{X_s}) = 0$ (for instance if X/S is a relative curve), $\mathcal{P}ic_{X/S}$ is formally smooth in a neighbourhood of s.*

th:picardv (v) *If the geometric fibers of f are integral, $\mathrm{Pic}_{X/S}$ is separated. If furthermore f is smooth, each closed subspace Z of $\mathcal{P}ic_{X/S}$ of finite type over S is proper.*

th:picardvi (vi) *If f is projective with integral geometric fibers, $\mathcal{P}ic_{X/S}$ is a disjoint union of quasi-projective spaces: $\mathcal{P}ic_{X/S} = \bigsqcup_{\Phi \in \mathbb{Q}[t]} \mathcal{P}ic^{\Phi}_{X/S}$, where $\mathcal{P}ic^{\Phi}_{X/S}$ is the subfunctor of line bundles whose Hilbert polynomial is Φ In particular $\mathcal{P}ic_{X/S}$ is a separated scheme, locally of finite presentation.*

Proof. If f is cohomologically flat in dimension 0, Artin proves the representability by algebraic space in [Art69b, Theorem 7.3] using his criterion for algebraicity. See also [BLR12, Theorem 8.3.1].

Raynaud also proves representability of the rigidified Picard functor when f admits a rigidificator, see [BLR12, Theorem 8.3.3]. This is in particular the case when f has a section, and if it is furthermore an universal O-morphism, then we have seen that the rigidified Picard functor is $\mathcal{P}ic_{X/S}$. The universal rigidified line bundle on $X \times_S \mathcal{P}ic_{X/S}$ comes from the universal property applied to $\mathrm{id} : \mathcal{P}ic_{X/S} \to \mathcal{P}ic_{X/S}$.

The third item is [BLR12, Theorem 8.4.1], and the fourth is [BLR12, Proposition 8.4.2, Theorem 8.4.3]

The last item was proved by Grothendieck, [Gro62, n°232, Theorem 3.1]: if X/S is projective, finitely presented, flat, with integral geometric fibers, then $\mathcal{P}ic_{X/S}$ is a separated scheme locally of finite presentation over S. See also [BLR12, Theorems 8.2.1 and 8.2.5], and [BLR12, Theorem 8.2.2] for Mumford's theorem which state that under the conditions above, but we only assume that the fibers are geometrically reduced and their irreducible components are geometrically irreducible, the $\mathcal{P}ic_{X/S}$ is a scheme (not necessarily separated) locally of finite presentation over S. □

cor:picardk **Corollary 2.3.5.** *If k is a field, and X/k is a proper geometrically reduced scheme over k.*

cor:picardki (i) *$\mathcal{P}ic_{X/k}$ is a scheme locally of finite type, and is separated if X is geometrically integral.*

cor:picardkii (ii) *If X is smooth and geometrically connected, the identity component $\mathcal{P}ic^0_{X/k}$ is a proper scheme over k, and is projective if X/k is projective.*

cor:picardkiii (iii) *$\dim_k \mathcal{P}ic_{X/k} \leq \dim_k H^1(X, O_X)$, with equality if and only if $\mathcal{P}ic_{X/k}$ is smooth over k (this is always the case in characteristic zero).*

Proof. If X/k is proper and geometrically reduced, it is cohomologically flat in dimension 0 by Lemma A.2.1, hence $\mathcal{P}ic_{X/k}$ is an qs algebraic space by Theorem 2.3.4.(i).

But a decent [Stacks, Tag 0318] (in particular quasi-separated) algebraic space X contains a dense open schematic locus U [Stacks, Tag 086U]. In particular a quasi-separated group algebraic space G/k contains a dense open schematic locus U, so by translation G is is a scheme. (This was already observed by Artin in the separated case in [Art69b].) So $\mathcal{P}ic_{X/k}$ is a scheme. In particular, we recover the Murre-Oor theorem that if X/k is proper and geometrically integral, $\mathcal{P}ic_{X/S}$ is a separated scheme [BLR12, Theoerem 8.2.1].

By Lemma B.1.1, a connected group scheme locally of finite type over k is of finite type, so $\mathcal{P}ic^0_{X/k}$ is a proper scheme by Theorem 2.3.4.(v).

Corollary 2.3.5.(iii) is immediate from Theorem 2.3.4.(iii). We refer to [BLR12, Theorems 8.4.1 and 8.4.3] for more details. □

rem:pictau **Remark 2.3.6.** In the situation above, we define $\mathrm{Pic}^{\tau}_{X/k}$ be the preimage of the torsion points in the Neron-Severi group $NS(X) = \mathrm{Pic}_X / \mathrm{Pic}^0_X$. More generally if X/S is proper locally of finite presentation over a qc S, we define $\mathcal{P}ic^{\tau}_{X/S}$ and $\mathcal{P}ic^0_{X/S}$ fiberwise. Then by [BLR12, Theorem 8.4.4], $\mathcal{P}ic^{\tau}_{X/S} \to \mathcal{P}ic_{X/S}$ is relatively representable by an open qc immersion, and $\mathcal{P}ic^{\tau}_{X/S}$ is of finite type. In particular if f is smooth with integral geometric fibers, $\mathcal{P}ic^{\tau}_{X/S}$ is proper by Theorem 2.3.4.(v), and projective if X/S is projective by Theorem 2.3.4.(vi). Furthermore if X/S is projective with geometric integral fibers, $\mathcal{P}ic^{\tau}_{X/S} \to \mathcal{P}ic_{X/S}$ is an open and closed immersion [BLR12, Theorem 8.4.4.(b)].

We can now prove that the dual abelian scheme exist (and is an abelian scheme):

biduality **Theorem 2.3.7** (Mumford). *If A/S is an abelian scheme, the relative Picard functor $\mathcal{P}ic^0_{A/S}$ is also an abelian scheme $\widehat{A}$, and is projective if A/S is projective. The Poincare sheaf $\mathcal{P}$ on $A \times_S \widehat{A}$ correspond to the line bundle associated to the map* $\mathrm{id} : \widehat{A} \to \widehat{A}$ *by the universal property of the relative Picard functor. It is symmetric and this is also the Poincare sheaf on $\widehat{A} \times_S A$, so A is canonically isomorphic to its bidual.*

Proof. Since A/S is proper smooth with connected fibers, it is cohomologically flat in dimension 0 by Lemma A.2.1, so $\mathcal{P}ic_{A/S}$ is a separated algebraic space by Theorems 2.3.4.(i) and 2.3.4.(v) and $\mathcal{P}ic^\tau_{A/S}$ is proper by Theorem 2.3.4.(v), and smooth by [MFK94, Proposition 6.7]. (The idea of the proof is as follow: to prove formal smoothness of $\mathcal{P}ic^\tau_{A/S}$ one need to lift line bundles, the obstruction to lifting is represented by an element in H^2, and by using the group law Mumford shows that this obstruction vanishes.) Hence it is an abelian algebraic space, so it is an abelian scheme by Theorem 2.3.2. It is projective if A/S is projective by Theorem 2.3.4.(vi). Finally since an abelian variety has no torsion, $\mathcal{P}ic^\tau_{A/S} = \mathcal{P}ic^0_{A/S}$, so $\widehat{A}$ is the identity component of $\mathcal{P}ic_{A/S}$. Since A/S is a group scheme, it has a section ϵ, so by Theorem 2.3.4.(ii) there is a universal rigidified Poincare bundle on $A \times_S \widehat{A}$ by Theorem 2.3.4.(ii). Biduality can be checked fiberwise, so result from biduality of abelian varieties (Section 2.2.3, [BLR12, Theorem 8.4.5]). □

2.3.3 *Rigidity*

Commutativity of abelian schemes can be proven by a similar rigidity argument as for abelian varieties.

:rigidity **Lemma 2.3.8** (Rigidity lemma). *Let $f : X \to S$ be a proper flat morphism, with S noetherian and connected and $H^0(X_s, O_{X_s}) = k(s)$ for all geometric points s. Let $g : Y \to S$ be separated and $h : X \to Y$ an S-morphism, such that $h_s : X_s \to Y_s$ is constant for some $s \in S$. Then h is constant, ie h factors through S.*

Proof. This is [MFK94, Proposition 6.1], [Bha, Corollary 2.2]. □

Remark 2.3.9. In the notations above, if $Y \to S$ is affine, then since f is an O-morphism by Lemma A.2.1 and $\mathrm{Hom}_S(X, Y) = \mathrm{Hom}_{O_S}(g_*Y, f_*X)$, h is also constant [Bha, Proposition 2.1].

As with abelian varieties, we get the usual corollaries:

Corollary 2.3.10.
- *Any schematic morphism $g : A \to B$ of abelian schemes is the composition of a translation and a group morphism;*
- *An abelian scheme is commutative;*
- *If $A \to S$ is proper smooth with connected fibers, and given a section $\epsilon_{A/S}$, there is at most one structure of abelian scheme on A whose unit is $\epsilon_{A/S}$.*

Proof. See [MFK94, Corollaries 6.4 and 6.5], [Bha, Corollary 2.4]. For the first item we only need B/S to be a separated group scheme.

Note that these results hold if S is not noetherian. We may assume S is affine, and we invoke approximation [GD64, §IV.8, §IV.11]. □

In fact, rigidity of abelian varieties extends to an even stronger version for abelian schemes:

yavscheme **Theorem 2.3.11** (Rigidity of abelian schemes, Grothendieck-Mumford [MFK94, Theorem 6.14]). *Assume that S is connected, $f : X \to S$ proper smooth and $\epsilon : S \to X$ a section of f. If, for a geometric point s, the fiber X_s is an abelian variety of neutral point $\epsilon(s)$, then X/S is an abelian scheme, with identity ϵ.*

Theorem 2.3.11 extends a theorem of Koizumi [Koi+60] saying that if an abelian variety A over $K = \mathrm{Frac}\, R$, R a dvr extends to a smooth and proper scheme $\mathcal{A}$ over $\mathrm{Spec}\, R$, then $\mathcal{A}$ is an abelian scheme (ie the group structure extends). Furthermore $\mathcal{A}$ is unique [KG59] (this is now subsumed in the theory of Néron models [BLR12], see Section 3.1.2).

More Details 2.3.12. Milne version (Theorem 3.4): if $V \times W \to A$, $V \times W$ is geom irred and V,W non singular or one of them complete; then if the two axes collapse above a, the morphism is constant.

Rigidity allows us in most cases to generalize theorems from abelian varieties to abelian schemes by checking them fiberwise (rather than globally).

If $\mathcal{L}$ is a line bundle on A, it is straightforward to generalise the morphism $\Phi_{\mathcal{L}} : A \to \widehat{A}$ from Section 2.2.4; this only depends on the algebraic equivalence class of $\mathcal{L}$ (by rigidity, since this is true when $S = \operatorname{Spec} \bar{k}$) [MFK94, §6.2]. We recall that a line bundle $\mathcal{L}$ is algebraically equivalent to 0 if it is equal to 0 in each of the geometric fibers of the Néron-Severi group $\mathrm{NS}_{A/S}(s) := \mathrm{Pic}_{A_s/k(s)}(k(s))/\mathrm{Pic}^0_{A_s/k(s)}(k(s))$. In particular if $\mathcal{L}$ is relatively ample, $\Phi_{\mathcal{L}}$ is an isogeny, so it induces a polarisation $A \to \widehat{A}$.

One need to be careful that for abelian scheme the converse need not be true, a polarisation $f : A \to \widehat{A}$ need not come from a relatively ample line bundle A (indeed A may not even be locally projective). Instead we only require f to come locally from a relatively ample line bundle in the étale (or fppf or fpqc) topology. This means that étale locally, f is of the form $\Phi_{\mathcal{L}}$, but the different line bundles $\mathcal{L}$ may not glue together to a global line bundle on A (since we have seen that algebraically equivalent lines bundles induce the same polarisation). But by rigidity, it suffice to check that f comes from an ample line bundle fiberwise! In fact it suffice to check this at a point:

igidpolarisation

Proposition 2.3.13. *Let A/S be an abelian scheme, and $\lambda : A \to \widehat{A}$ be a morphism. Then the set of geometric points $s \in S$ such that λ_s is a polarisation is open and closed. In particular, if S is connected and λ_s is a polarisation for one geometric point s, then λ is a polarisation.*

Proof. We use the following criteria for polarisations. $\lambda : A \to \widehat{A}$ is a polarization if and only if:

(i) λ is symmetric with respect to biduality
(ii) The line bundle $(1,\lambda)^*(\mathcal{P}_A)$ on A is fiberwise ample.

Indeed by [MFK94, Proposition 6.10], if $\lambda : A \to \widehat{A}$ is a polarization and $\mathcal{L}_\lambda = (\lambda \times \mathrm{id})^* \mathcal{P}$, then $\Phi_{\mathcal{L}} = 2\lambda$. One can then check that these two criteria are open and closed in S. We refer to [nfd16] for more details. □

Let $\lambda : A \to \widehat{A}$ be a polarisation, and assume that it is represented by an ample line bundle $\mathcal{L}$ (this is always the case étale locally). Then we have the following properties:

p:lefchetzscheme

Proposition 2.3.14. *Let $\mathcal{L}$ be a relatively ample line bundle on an abelian scheme $f : A \to S$.*

(i) $R^i f_* \mathcal{L} = 0$ *if* $i > 0$, *and* $f_* \mathcal{L}$ *is locally free on S of rank r;*
(ii) $\Phi_{\mathcal{L}} : A \to \widehat{A}$ *is an isogeny of degree r^2 (where the degree of an isogeny ϕ is the rank of $\phi_* O_A$);*
Lefschetz *If $n \geq 2$, $f_* \mathcal{L}^n$ is base point free (ie its sections have no common zeroes in A, so induce a morphism $A \to \mathbb{P}(f_* \mathcal{L})$. If $n \geq 3$ this morphism is a closed immersion;*

Proof. This is [MFK94, Proposition 6.13]. Since $H^i(A_s, \mathcal{L}_s) = 0$ when $i > 0$ for all geometric points $s \in S$ by Theorem 2.2.10, the first item is a special case of the proper base change theorem, see Lemma A.1.1 below. This also shows that the sections of $H^0(A_s, \mathcal{L}_s)$ are generated by $f_* \mathcal{L}$. The second item can be checked fiberwise, and the third also by [GD64, p. III.6.7]. □

2.3.4 Isogenies

vschemeisogenies

We can also construct isogenies fiberwise (compare with Appendix B.4).

prop:isogeny

Proposition 2.3.15. *A morphism $f : A \to B$ of abelian schemes over S is projective of finite presentation, and is flat if f is surjective. If it is fiberwise an isogeny, its degree is locally constant and its kernel is a finite flat (over S) subgroup G. Conversely, if G is a finite flat subgroup of A, the quotient A/G is an abelian scheme.*

Proof. If f is any surjective morphism of group schemes $f : X \to Y$ over S, with X/S flat and Y/S smooth, then f is fiberwise flat by Proposition B.1.4, hence flat (see also [MFK94, Lemma 6.12]). If $f : A \to B$ is a morphism of abelian schemes, it is automatically proper of finite presentation by the usual cancellation properties, and its kernel G is the pullback of the zero section 0_B, which is a closed immersion in B since B/S is separated, so it is closed in A, hence proper over S. Since f is flat, G is also flat over S (see the discussion in Appendix B.4).

If f is fiberwise an isogeny, G is proper quasi-finite over S hence finite by Lemma B.4.1. Since G is finite flat, its rank is locally constant, so the degree of f is locally constant.

Raynaud proved that if S is affine, then A/S is an AF-scheme, so by Appendix D A/G exists as a scheme. Alternatively A/G exists a an algebraic space by Deligne's theorem (see Appendix D, so is an abelian scheme by Raynaud's theorem Theorem 2.3.2.

We refer to Proposition B.4.2 for more details. In fact, the same argument shows that a quotient A/A' by a subgroup scheme A' of A which is flat over S is an abelian scheme (since it is an abelian algebraic space). □

Biduality of abelian schemes Theorem 2.3.7 gives that a birational map from a nice scheme to an abelian scheme extends everywhere:

neronprop

Proposition 2.3.16 ([BLR12, Corollary 8.4.6].)**.** *If A/S is an abelian scheme, any rational S-morphism $g : TA$ from a regular scheme T is defined everywhere.*

In particular, if S is regular, a rational morphism $g : AB$ of abelian schemes is defined everywhere.

Proof. By considering the pullback over T, we may assume $T = S$ and we need to show that g extends to S. By biduality, the map g corresponds to a line bundle on $\widehat{A}_U$ where U is an open of S, and this line bundle extends to a line bundle on $\widehat{A}$ since $\widehat{A}$ is regular (being smooth over the regular S). □

As another striking illustration of rigidity of abelian schemes with respect to extension of isogenies, see [Gro66b]. See Section 3.1.5 for other examples of extending isogenies.

2.3.5 Characterisations of abelian schemes

c:avcarac

The definition of an abelian group scheme itself does not seems to be fibral, since flatness and properness are global conditions. But we will see that this will actually be the case, at least if S is reduced. Since I was not able to find references in the literature, I wrote an appendix section Appendix B.3 giving more details in the proofs than in the other sections of this summary.

Combining Proposition B.3.3 and Theorem 2.3.11, we get the following equivalent definitions of an abelian scheme, for an arbitrary connected base s.

hemecarac

Theorem 2.3.17. *Assume that S is a connected scheme. An abelian scheme $f : A \to S$ is either*

- *A proper group scheme with some conditions on all fibers:*
  - *(i) A proper smooth group scheme whose fibers are abelian varieties (ie are geometrically integral, or equivalently geometrically irreducible or connected).*
  - *(i') A proper flat finitely presented group scheme whose fibers are abelian varieties (ie are geometrically integral, or equivalently are smooth and geometrically connected, or geometrically reduced and geometrically connected).*
  - *(i") (If S is reduced) A proper finitely presented group scheme whose fibers are abelian varieties of the same dimension g (ie are geometrically integral of dimension g, or equivalently are smooth and geometrically connected of dimension g).*
- *A proper group scheme with a condition on one fiber:*
  - *(ii) A proper smooth group scheme with one fiber an abelian varieties (ie is geometrically integral/irreducible/connected).*
  - *(ii') A proper flat finitely presented group scheme whose fibers are smooth (or geometrically reduced) and one is an abelian variety (ie is geometrically connected).*
  - *(ii") (If S is reduced) A proper finitely presented group scheme whose fibers are smooth (or geometrically reduced) of the same dimension g and one is an abelian variety (ie is geometrically connected).*
- *A group scheme with conditions on all fibers:*

(iii) *A flat finitely presented group scheme, whose fibers are abelian varieties (ie are proper geometrically integral, or equivalently proper smooth geometrically connected).*

(iii") *(If S is reduced) A finitely presented group scheme whose fibers are abelian varieties of the same dimension g (ie are proper geometrically integral of dimension g, or equivalently are proper smooth and geometrically connected of dimension g).*

- *A/S admit a section $\epsilon : S \to A$ such that either:*

(iv) *a scheme $f : A \to S$ proper smooth, and with a section ϵ such that $A_s \to k(s)$ is an abelian variety with neutral point $\epsilon(s)$ at a point s.*

(iv') *a scheme $A \to S$ flat of finite presentation, whose fibers are proper, geometrically connected and smooth, and with a section ϵ such that $A_s \to k(s)$ is an abelian variety with neutral point $\epsilon(s)$ at a point s.*

(iv") *[If S is reduced] a scheme $A \to S$ proper of finite presentation, whose fibers are smooth of the same dimension g, and with a section ϵ such that $A_s \to k(s)$ is an abelian variety with neutral point $\epsilon(s)$ at a point s.*

(iv"') *[If S is reduced] a scheme $A \to S$ of finite presentation, whose fibers are proper, smooth, geometrically connected of the same dimension g, and with a section ϵ such that $A_s \to k(s)$ is an abelian variety with neutral point $\epsilon(s)$ at a point s.*

By Proposition 2.2.3 in the above we may replace "geometrically connected" by "connected", and by Lemma B.3.1 we may also replace "of finite presentation" by "locally of finite presentation".

Proof. The different characterisations of an abelian varieties come from Proposition 2.2.3. $(i) \Leftrightarrow (i')$ by definition of smooth. $(i) \Leftrightarrow (ii) \Leftrightarrow (ii') \Leftrightarrow (iii)$ by Proposition A.3.6. $(i) \Leftrightarrow (i'') \Leftrightarrow (ii'') \Leftrightarrow (iii'')$ by Proposition B.3.3. $(i) \Leftrightarrow (iv)$ by rigidity, Theorem 2.3.11. $(iv) \Leftrightarrow (iv')$ by Proposition A.3.6, $(iv') \Leftrightarrow (iv'') \Leftrightarrow (iv''')$ by Propositions B.3.3 and A.3.6. □

ngabelianschemes

2.3.6 *Using abelian schemes*

Assume that we have a property (P) of abelian varieties, and which we can prove for some abelian varieties (typically abelian varieties over $\mathbb{C}$). We explain some standard method to show that it is valid over all fields. Essentially all these methods involve extending (P) to abelian schemes, (eg so that it is defined on the universal abelian scheme, or at least on a Néron model so that we can reduce). The extension will typically be that (P) is true for all fibers of the abelian scheme, along some flatness condition.

Lifting arguments

Suppose that (P) involves a level n structure. We use that the universal abelian stack with a level n structure $\mathcal{X}_{g,n} \to \mathcal{A}_{g,n}$ is smooth over $\mathbb{Z}[1/n]$ Section 5.7. Since $\mathcal{A}_{g,n}$ is a DM stack, it has an étale cover by a scheme, so every property that is étale-local on target (see [Stacks, Tag 04QW], [Stacks, Tag 0CFY]) extends to $\mathcal{X}_{g,n} \to \mathcal{A}_{g,n}$, in particular all results of this Section hold for $\mathcal{X}_{g,n} \to \mathcal{A}_{g,n}$.

This can be used for lifting arguments. By the Lefschetz principle [FR86], (P) is true over a field of characteristic zero. Note that we don't really need to invoke the Lefschetz principle here, since the moduli stack of polarised abelian varieties is of finite type over $\mathbb{Z}$, an abelian variety A/k is the pullback of an abelian variety defined over a field of finite transcendance degree over the base field, hence embeds into $\mathbb{C}$ in case of characteristic zero.

If A is defined over a perfect field k, and k is of characteristic p prime to n, we can lift A to an abelian scheme $\widetilde{A}/W(k)$, ie to characteristic zero. Indeed, by smoothness of $\mathcal{A}_{g,n}$ over $\mathbb{Z}[1/n]$, we can lift A to the finite Witt vectors, and then we invoke that $\mathcal{A}_{g,n}$ if finitely presented, hence its functor of points commute with filtered limits, to lifts to the Witt vectors.

If $\widetilde{A} \to W(k)$ is a lift, the generic fiber is of characteristic zero so (P) holds. We can then typically use genericity arguments or property of Néron models to extend (P) to all of $\widetilde{A}$ (ie show that (P) has good reduction), so (P) holds for the special fiber $A = \widetilde{A}_k$.

Approximation arguments

Since $\mathcal{A}_{g,n}$ is smooth over $\mathbb{Z}[1/n]$, its connected components are normal, hence integral. The generic points of the connected components are of characteristic zero, and the associated fields are of finite transcendance degree $g(g+1)/2$ over $\mathbb{Q}$ hence embed into $\mathbb{C}$.

So (P) is valid over the generic fibers of $\mathcal{X}_{g,n}$, and we often will be able to use the approximation results of [GD64, §IV.8] to show that (P) is valid over an open containing these generic points, hence a dense open, hence valid everywhere if (P) is a closed property. (The same strategy holds if (P) is a property of ℓ-isogenies, and we apply this to the universal isogeny $\mathcal{X}_{g,\ell n} \to \mathcal{X}_{g,n} \times_{\mathcal{A}_{g,n}} \mathcal{A}_{g,\ell n}$, by using that $\mathcal{X}_{g,n}$ is separated and $\mathcal{X}_{g,\ell n}$ is reduced).

An essentially equivalent reformulation is that we can cover $\mathcal{A}_{g,n}$ by affine integral schemes whose fraction field embeds into $\mathbb{C}$. (The covers are étale covers if $\mathcal{A}_{g,n}$ is a stack, and can be taken to be Zariski covers when $\mathcal{A}_{g,n}$ is a scheme).

This is essentially a reformulation of the lifting argument, hidden in the fact that the connected components of $\mathcal{A}_{g,n}$ dominate $\mathbb{Z}[1/n]$, hence their generic points are of characteristic zero.

Flatness arguments

Since $\operatorname{Spec}\mathbb{C} \to \operatorname{Spec}\mathbb{Q}$ is faithfully flat, proving that (P) holds for $\mathcal{A}_{g,n} \otimes \mathbb{Q}$ is the same as proving it holds for $\mathcal{A}_{g,n} \otimes \mathbb{C}$ for all properties (P) which are fpqc-local (or just étale local) on the base.

Sometimes, this is enough to prove that (P) holds for $\mathcal{A}_{g,n}$ over $\mathbb{Z}[1/n]$. For instance, if we have a line bundle $\mathcal{L}$ on $\mathcal{A}_{g,n}$ and two sections s_1, s_2 of $\mathcal{L}$. Since $\mathcal{A}_{g,n}$ is smooth over $\mathbb{Z}[1/n]$, then $\mathcal{L}$ is torsion free over $\mathbb{Z}[1/n]$, hence we can test equality to the pullback over $\mathbb{Q}$.

More generally, if we have two morphisms $f_1, f_2 : \mathcal{A}_{g,n} \to T$ where T is separated, the locus where $f_1 = f_2$ is a closed subscheme. Since $\mathcal{A}_{g,n}$ has no embedded points, it suffices to check that it contains the generic points to show that $f_1 = f_2$ everywhere.

Rigidity arguments

We can use the rigidity lemma Lemma 2.3.8 on an abelian scheme. This apply in particular to the universal abelian stack $\mathcal{X}_{g,n} \to \mathcal{A}_{g,n}$. We can also apply Lemma 2.3.8 to suitable compactifications of $\mathcal{A}_g$, since its fibers are geometrically connected.

Let us give an exemple: suppose that A/S is an abelian scheme, and that we have a finite flat subgroup scheme K/S. We want to construct the isogeny $f : A \to B = A/K$.

Suppose that we know B and define a morphism $g : A \to B$ which is proper flat (and sends the zero section of A to the zero section of B). This is usually easy to check by the fiberwise criteria for flatness and the valuation property for properness. Then by the rigidity lemma it suffices to check that f and g coincide on one fiber to get that $f = g$.

A related argument can be made using Proposition 3.1.21. Assume that A/S and B/S are abelian schemes and S is (noetherian) and normal. Since S is in particular reduced, we recall that by Theorem 2.3.17 this just amount to say that there is a zero section $\epsilon : A \to S$ and that all fibers of A/S are abelian varieties of the same dimension g. (In fact it even suffices to check that the fibers are proper smooth geometrically connected of the same dimension g and that one of them is an abelian variety).

Let η be the generic point of S, and assume we have a surjective morphism $f_\eta : A_\eta \to B_\eta$ (eg an isogeny). Then f_η extends to a surjective morphism $f : A \to B$ by Proposition 3.1.21, hence a proper flat morphism by Proposition 2.3.15. If we have defined a proper flat candidate $g : A \to B$ above, it suffice to check equality on one fiber (eg the generic fiber) to get that $f = g$.

These arguments show that if we have a generic isogeny f, extending it is essentially just a matter of definition of f as a map of abelian schemes. It will automatically be an isogeny. Applying this to $\mathcal{A}_{g,n}$, this shows that if we have a candidate for an isogeny formula that is defined for every abelian scheme (in such a way that the resulting map on the universal abelian schemes is proper flat), then it suffices to check that it is valid in characteristic zero to know that it is valid everywhere.

2.4 JACOBIANS

sec:jacobians

References for this section are [Mil85; BLR12]. From the algorithmic point of view Jacobians varieties are easy to work with. We have Mumford coordinates on Jacobians of hyperelliptic curves, and more generally we can use the algorithms of [Hes02; Khu04; Khu07] to work on a Jacobian.

For instance, if k is a field, any indecomposable principally polarised abelian variety of dimension $g \leq 3$ is the Jacobian of a (smooth geometrically connected) curve C/k of genus g[9]. In particular any principally polarised abelian variety A/k of dimension $g \leq 3$ is a product of Jacobians [OU73]. Thus curves provide convenient models of abelian varieties of small dimension. In a similar vein: any abelian variety A/k over an infinite field is a quotient of a Jacobien [Mil85, Theorem 10.1].

2.4.1 *Curves*

subsec:curves

A curve $f : X \to S$ is a proper finitely presented scheme of relative dimension 1 (we do not yet impose smoothness conditions). We first recall the Riemann-Roch theorem. There is a 1-dualizing sheaf ω_f on X[10]. Then by definition, if L is an invertible sheaf on X, $H^0(X, L^\vee \otimes \omega_f) \simeq \mathrm{Hom}_{O_X}(L, \omega_f) \simeq H^1(X, L)^\vee$.

prop:projcurve

Proposition 2.4.1 ([BLR12, Remark 9.3.2]). *Let $f : X \to S$ be a proper flat curve whose geometric fibers are integral curves of genus g. Assume that X is a relative local complete intersection (l.c.i.) over S. Then the relative dualizing sheaf ω_f is a line bundle (since X is Gorenstein), which is ample if $g \geq 2$. If $g = 0$, ω_f^{-1} is ample. In both case X/S is projective. If $g = 1$, X/S is étale locally projective.*

th:riemannroch

th:riemannrochi

Theorem 2.4.2 (Riemann-Roch). *Let $f : C \to k$ be a proper curve, and D a Cartier divisor. Then*

(i) $\chi(O_C(D)) = \deg D + \chi(O_C)$, *where χ is the Euler-Poincare characteristic.In particular, if $D = \div f$ is principal,* $\deg(D) = 0$.

(ii) *The arithmetic genus $p_a(C)$ is defined by $\chi(O_C) = 1 - p_a(C)$. We thus get by duality* $\dim_k H^0(C, O_C(D)) - \dim_k H^0(C, \omega_f \otimes_{O_C} (-D)) = \deg D + 1 - p_a$.

(iii) *By duality, $H^0(C, \omega_f) \simeq H^1(C, O_C)^\vee$, $H^0(C, O_C) \simeq H^1(C, \omega_f)^\vee$. In particular, $\chi(\omega_f) = -\chi(O_C)$, so* $\deg(\omega_f) = 2(p_a - 1)$.
Thus if $\dim_k H^0(C, O_C) = 1$ *(for instance C is geometrically connected and geometrically reduced), $p_a(C) =$* $\dim_k H^1(C, O_C) = \dim_k H^0(C, \omega_f)$.

(iv) *If C is l.c.i., the (geometric) genus is $g(C) =$* $\dim_k H^0(C, \omega_C/k)$, *so since $\omega_{C/k} = \omega_f$ it is equal to the arithmetic genus if C is geometrically connected and geometrically reduced. If C is smooth, $\omega_{C/k} = \Omega^1_{C/k}$.*

Proof. See [Liu02, §7.3.2]. □

If X/S is a flat proper curve, and $\mathcal{L}$ a line bundle, since the Euler-Poincare characteristic is locally constant by [GD64, p. III.7.9.4], $\deg \mathcal{L}$ is locally constant by Theorem 2.4.2.(i) ([BLR12, Proposition 9.1.2]). In particular, $\dim_{k(s)} H^0(X_s, O_{X_s})$ is locally constant if and only if $\dim_{k(s)} H^1(X_s, O_{X_s})$ is locally constant. So if X/S is cohomologically flat in dimension 0, the arithmetic genus of the geometric fibers is locally constant, and conversely if S is reduced by Lemma A.2.1.

2.4.2 *The Jacobian of a curve*

th:jacobian

Theorem 2.4.3. *Let X/S be a proper smooth relative curve (which means that the fibers are of dimension 1) with connected geometric fibers. Then the Jacobian $J = J(X/S)$ is an abelian projective scheme over S representing the relative Picard functor $\mathcal{P}ic^0_{X/S}$. We have a canonical isomorphism* $\mathrm{Lie}(J) \simeq R^1 f_* O_X$.

[9] Be careful that we require the polarisation to be indecomposable, not only the abelian variety A. Indeed a Jacobian of an hyperelliptic curve of genus 2 can also be a product of two elliptic curves, but the polarisation is different. See [Kan94; Kan16; Kan19a] for a precise description of when this can happen.

[10] By [Kle80, Theorem 4], if $f : X \to S$ is proper finitely presented with fibers of dimension $\leq r$, a r-dualizing sheaf ω_f always exist and it is equal to $f^! O_Y$. (For full duality we need that each fiber is Cohen-Macauley [Kle80, Theorem 21]). If f is projective and a locally complete intersection, ω_f is the canonical line bundle $\omega_{X/S}$, so $\omega_f = \Omega^r_{X/S}$ if f is smooth [Liu02, § 6.4.3].

There is a canonical principal polarisation $\lambda : J \to \hat{J}$, the pullback of $\mathcal{P}$ by $\mathrm{id} \times \lambda$ is then a canonical S-ample rigidified line bundle $\mathcal{L}$ on J.

If X has a section, there is a canonical rigidified line bundle on $X \times_S J(X/S)$ which induces a morphism $X \to J$, and the canonical principal polarisation $\lambda : J \to \hat{J}$ comes from the Θ-divisor on J.

Finally, the connected components of $\mathcal{P}ic_{X/S}$ are given by $\mathcal{P}ic_{X/S} = \bigsqcup(\mathcal{P}ic_{X/S})^n$ where each $(\mathcal{P}ic_{X/S})^n$ is a torsor under $\mathcal{P}ic^0_{X/S}$ and $(\mathcal{P}ic_{X/S})^0 \simeq \mathcal{P}ic^0_{X/S}$. If X/S has a section, $(\mathcal{P}ic_{X/S})^n$ represents the (rigidified) line bundles of degree n.

Proof. This is [MFK94, Propositon 6.9] and [BLR12, Proposition 9.4.4] (see also [Mil85, §8]). By Theorem 2.3.4 and Remark 2.3.6 we know that $\mathcal{P}ic^\tau_{X/S}$ is a proper smooth group algebraic space, since formal smoothness is immediate from Theorem 2.3.4.(iii). But a curve has no torsion, so $\mathcal{P}ic^\tau_{X/S} = \mathcal{P}ic^0_{X/S}$ so the fibers are connected, hence $\mathcal{P}ic^0_{X/S}$ is an abelian algebraic space, hence an abelian scheme by Theorem 2.3.2.

If X/S is projective, J/S is projective by Remark 2.3.6. But a curve is étale locally projective by Proposition 2.4.1, so J/S is projective on an étale cover S' of S, and the canonical line bundle on J descend to S (since it is canonical), hence J is projective [BLR12, Theorem 6.1.7].

We have the decomposition into connected components $\mathcal{P}ic_{X/S} = \bigsqcup(\mathcal{P}ic_{X/S})^n$ where $(\mathcal{P}ic_{X/S})^n$ represents the line bundles of degree n by [BLR12, Theorem 9.3.1]. Indeed the degree of a line bundle is constant on a connected component. It remains to check that $(\mathcal{P}ic_{X/S})^n$ is connected. If X/S has a section, $(\mathcal{P}ic_{X/S})^n$ is isomorphic to $(\mathcal{P}ic_{X/S})^0$. Since X/S is flat it has a section fppf-locally, hence $(\mathcal{P}ic_{X/S})^n$ is a torsor under $(\mathcal{P}ic_{X/S})^0$. It remains to prove that $(\mathcal{P}ic_{X/S})^0 = \mathcal{P}ic^0_{X/S}$. We reduce to $S = \operatorname{Spec} k$ with $k = \overline{k}$ algebraically closed, and $X = C$ is a curve over k. We fix a point P on C. Then the map $C^{<g>} \to \mathcal{P}ic_{C/k}, (P_1, \dots, P_g) \mapsto \sum[P_i - P]$ (or precisely maps to the line bundle associated to this divisor) lands into $\mathcal{P}ic^0_{C/k}$ by connectedness. Hence the universal line bundle on $C \times \mathcal{P}ic^0_{C/k}$ has degree 0. Conversely by the Riemann-Roch theorem (Theorem 2.4.2), $C^{<g>} \to (\mathcal{P}ic_{C/k})^0$ is surjective. Hence $\mathcal{P}ic^0_{C/k} = (\mathcal{P}ic_{C/k})^0$. Hence the geometric points of $\mathcal{P}ic^0_{C/k}$ do correspond to line bundles of degree 0 on C.

The principal polarisation $J \to \hat{J}$ is constructed in [MFK94, Propositon 6.9]. If X has a section, since $X \to S$ is an universal O-morphism by Lemma A.2.1, we have the existence of the canonical rigidified line bundle by Theorem 2.3.4.(ii). This line bundle induces a morphism $X \to \hat{J}$ by the universal property of $\hat{J}$, hence a morphism $X \to J$ via the principal polarisation.

In fact Mumford proof is the other way around: X naturally maps to $\mathcal{P}ic^1_{X/S}$, so if X/S has a section σ we have a natural map to $\mathcal{P}ic^0_{X/S} = J$. We get a morphism from $\hat{J} \to J$ (induced by pulling back line bundles), which is an isomorphism fiberwise, hence an isomorphism by flatness of J and $\hat{J}$. This define the polarisation $\lambda : J \to \hat{J}$ when X/S has a section. It is principal by [Mil85, Theorem 6.6]. It is shown in [BLR12, Proposition 9.4.4] that λ is the polarisation induced by the usual theta divisor. Indeed the symmetric power $(X/S)^{<g-1>}$ naturally maps into $\mathcal{P}ic^{g-1}_{X/S}$ and using the section σ we get a map to $\mathcal{P}ic^0_{X/S}$. The schematic image W_{g-1} is birational to $(X/S)^{<g-1>}$ and is a translation of the theta divisor Θ_σ.

But X/S always have a section fppf locally (since X/S is flat and its pullback over itself admits a section), so we have fppf local maps $J_{S'} \to \hat{J}_{S'}$ which glue together, hence by descent they define the polarisation $J \to \hat{J}$.

If $\mathcal{L} = (1 \times \lambda)^* \mathcal{P}$, then $\mathcal{L}$ is ample. Indeed this can be checked fiberwise, so we reduce to the case of a Jacobian over a field, in which case the result is from Weil. Be careful that $\mathcal{L}$ does not induce λ, indeed $\Phi_{\mathcal{L}} = 2\lambda$ by the proof of Proposition 2.3.13. □

Remark 2.4.4. There are examples of smooth projective geometrically connected curves over $\mathbb{Q}$ such that the principal polarisation on their Jacobians J is not induced by a principal line bundle on J. Such curves necessarily have $C(\mathbb{Q}) = \emptyset$ by Theorem 2.4.3.

We recall that the relative Picard functor is the fppf sheafication of the relative Picard presheaf $\mathrm{Pic}_{X/S}$. In the case when $S = \operatorname{Spec} k$ is a field, and $X = C$ is a proper smooth connected curve over k, $\mathcal{P}ic^0_{X/S}(T) = \mathrm{Pic}^0_{X/S}(T)$ whenever $C(T)$ is non empty [Mil85, Theorem 1.1] (since $\mathcal{P}ic$ commutes with base change, this is a special case of Theorem 2.3.4.(ii)). In particular, $J(k) = \mathrm{Pic}^0_{C/k}$ if $C(k)$ is non empty.

There are several constructions of the Jacobians when $S = \operatorname{Spec} k$ and $k = \bar{k}$ is an algebraically closed field. One may glue together the symmetric powers $C^{<i>}$ for $i = 0, 1, \dots, g$. Chow's construction use the fact that if $r > 2g-2$, $C^{<r>} \to J$ is smooth with fibers isomorphic to $\mathbb{P}^{r-g}$ by the Riemann-Roch theorem (see Proposition 2.4.5)[11]. Weil's construction was to define a birational group law on $C^{<g>}$, and prove an extension theorem to extend the group law from $C^{<g>}$ to its birational J. We refer to [Mil85] for an overview of these constructions.

2.4.3 Properties of Jacobians

prop:symmetric

Proposition 2.4.5. *Let k be a field, C/k be a smooth proper connected curve and $P_0 \in C(k)$ a point. Let $f_P : C \to J$ be the map sending a point P to $[P - P_0]$.*

- *Since $T_0 J \simeq H^1(C, O_C)$, the pullback $f_P^* : \Gamma(J, \Omega^1_J) \to \Gamma(C, \Omega^1_C)$ is an isomorphism.*
- *The map f_P is a closed immersion.*
- *It induces a map $f_P^{<r>}$ from $C^{<r>}$ (the symmetric power of C, which is smooth) to J. Its image is a closed subvariety W_r of J and there is a stratification $J = \bigsqcup_{i=0}^{r} W_r$. The pullback $f_P^{<r>*} : \Gamma(J, \Omega^1_J) \to \Gamma(C^{<r>}, \Omega^1_{C^{<r>}})$ is an isomorphism.*
- *If $r \leq g$, $f_P^{<r>} : C^{<r>} \to W_r$ is birational, in particular, J is birational to $C^{<g>}$. The theta divisor Θ is a translation of W_{g-1} (to make it symmetric) and is principal and ample.*
- *If D is an effective divisor of degree r on C, and F is the fibre of $f_P^{<r>}$ at D, we have*

$$0 \to T_D(F) \to T_D(C^{<r>}) \to T_{f_P^{<r>}(D)} J$$

  Since F is the space of all effective divisors linearly equivalent to D, it is isomorphic to $|D|$, a projective space of dimension $m = h^0(D) - 1$.
- *The multiplicity of (the image of) D in W_r is $\binom{g-r+m}{m}$ (so is $m+1$ if $r = g-1$).*

Proof. The first four statements are mostly a corollary of Theorem 2.4.3 specialised to $S = \operatorname{Spec} k$. For more details, see [Mil85, §2, §5]. The last statement is Riemann-Kempf theorem [Rie65; Kem73]. Riemann's singularity theorem is useful to compute the order of vanishing of a theta function at the Θ divisor. □

Remark 2.4.6. If C/k is a proper smooth geometrically connected curve of Jacobian $J = \operatorname{Jac}(C)$ over a perfect field k, we may relate the rational points $J(k)$ and its Picard group $\operatorname{Pic}^0_{X/k}(k)$ as follow. Let X/k be a scheme of finite type over a perfect field k, $\bar{k}$ an algebraic closure and G the Galois-group. The Leray spectral sequence applied to $R(X \to k)_* \mathbb{G}_m$ gives the exact sequence:

$$0 \to H^1(G, \bar{k}[X]^*) \to \operatorname{Pic}(X) \to \operatorname{Pic}(\overline{X})^G \to H^2(G, \bar{k}[X]^*) \to \ker[\operatorname{Br}(X) \to \operatorname{Br}(\overline{X})^G] \to H^1(G, \operatorname{Pic}(\overline{X})) \to H^3(G, \bar{k}[X]^*)$$

since $\operatorname{Pic}(X) = H^1(X, G_m)$ and we denote by $Br(X) = H^2(X, G_m)$ the Brauer cohomological group. If X is proper, $\bar{k}[X]^* = \bar{k}^*$ so $H^1(G, \bar{k}^*) = 0$ by Hilbert 90, and the exact sequence becomes:

$$0 \to \operatorname{Pic}(X) \to \operatorname{Pic}(\overline{X})^G \to \operatorname{Br}(k) \to \ker[\operatorname{Br}(X) \to \operatorname{Br}(Xbar)^G] \to H^1(G, \operatorname{Pic}(\overline{X})) \to H^3(G, \bar{k}^*)$$

If X has point over k, then $\operatorname{Br}(k) \to \operatorname{Br}(X)$ has a section (via the evaluation on the point), so is injective. We get: $\operatorname{Pic}(X) \simeq \operatorname{Pic}(\overline{X})^G$ and there is an exact sequence:

$$0 \to \operatorname{Br}(k) \to \operatorname{Br}_1(X) \to H^1(G, \operatorname{Pic}(\overline{X})) \to 0$$

where $\operatorname{Br}_1(X) = \ker[\operatorname{Br}(X) \to \operatorname{Br}(\overline{X})^G]$.

Going back to our curve C, since $J(k) = J(\bar{k})^G = \operatorname{Pic}(\overline{X})^G$, we get that $\operatorname{Pic}_{C/k}(k) \to J(k)$ is always injective, and we recover that it is a bijection when C has a rational point, since in this case every rational linear equivalence class of divisors arise from a rational divisor on C.

[11] Khuri-Makdisi's algorithm [Khu07] is also based on this idea

Theorem 2.4.7 (Torelli). *Let C/k be a smooth geometrically connected curve,* $\mathrm{Jac}(C)$ *its Jacobian and Θ_C its canonical divisor. Then C is uniquely determined b* $(\mathrm{Jac}\, C, \Theta_C)$.

More precisely, for every isomorphism of (polarized) abelian varieties $F : (\mathrm{Jac}(C), \Theta_C) \xrightarrow{\sim} (\mathrm{Jac}(C'), \Theta_{C'})$, there exists a unique isomorphism $f : C \to C'$ and $e = \pm 1$ such that $F = e\,\mathrm{Jac}\, f$. Moreover if C is hyperelliptic, $e = 1$.

In particular, $\mathrm{Aut}(J, \Theta_C) = \mathrm{Aut}(C)$ *if C is hyperelliptic and* $\mathrm{Aut}(J, \Theta_C) = \pm 1 \times \mathrm{Aut}(C)$ *otherwise.*

Proof. This refined version is in [Sero1]. See also [Mil85, Theorem 12.1] for a proof of the standard Torelli theorem over $k = \overline{k}$. □

Remark 2.4.8. We recall that a smooth geometrically connected curve C/k of genus $g \geq 2$ is hyperelliptic if there is a degree 2 morphism to $\pi : C \to \mathbb{P}^1_k$. Alternatively, $k(C)$ is a quadratic cyclic extension of $k(\mathbb{P}^1)$, and the Galois action induce the hyperelliptic involution ι on C (such that $\pi(P) = \pi(Q)$ if and only if $P = Q$ or $P = \iota(Q)$.

Since ι is canonical, the cover $\pi : C \to \mathbb{P}^1_k$ is unique up to postcomposition by an automorphism of $\mathbb{P}^1_k$. The involution ι induces $[-1]$ on the Jacobian, and so it commutes with every automorphism of C, and we have an exact sequence $1 \to \langle \iota \rangle \to \mathrm{Aut}_k(C) \to \mathrm{Aut}_k \mathbb{P}^1$ [Liuo2, §7.4.3] and [CNPo5, §1.1].

2.4.4 Generalised Jacobians

If C/k is a smooth proper curve, its Jacobian $J(C) = \mathcal{P}ic^0_{C/k}$ is an abelian variety.

In general, when C/k is just a proper curve, $\mathcal{P}ic^0_{C/k}$ is still a smooth scheme by Corollary 2.3.5, it is sometimes called the generalised Jacobian $J(C)$. Concretely, $J(C)$ consists of all elements in $\mathcal{P}ic_{X/k}$ whose partial degree on each irreducible component of $X_{\overline{K}}$ is zero [BLR12, Proposition 9.2.13]. We refer to [BLR12, §9.2] and [Rom13, §3.3] for the structure of this generalised Jacobian.

Anticipating Sections 3.1 and 3.2, we note two important properties of $J(C)$, for a curve C/k reduced proper over a perfect field k:

- $J(C)$ contains no unipotent connected subgroup (ie is semi-abelian), if and only if C is weakly normal [BLR12, Proposition 9.2.9], and then singularities of $X_{\overline{k}}$ are analytically isomorphic to the crossing of the coordinates axes in $\mathbb{A}^n$ [BLR12, Corollary 9.2.12.(a)])
- If $J(C)$ is an abelian variety, then the irreducible components of X are smooth and the configuration of the irreducible components of $X_{\overline{k}}$ is tree like, ie $H^1(X_{\overline{k}}, \mathbb{Z}) = 0$ by [BLR12, Corollary 9.2.12.(c)]), and conversely if furthermore X is weakly normal by [BLR12, Propositions 9.2.9 and 9.2.10].

  In particular this provides a way to construct a product $\prod J(C_i)$ of Jacobians of smooth propers curves as the generalised Jacobian $J(\bigsqcup C_i)$.

We have the following important example:

Example 2.4.9 ([BLR12, Example 9.2.8]). Let C/k be a (weak) semistable curve. Then $J(C)$ is a semi-abelian variety, and if $C_1, \dots, C_r$ are its irreducible components, the canonical decomposition of $J(C)$ into an abelian part and a torus part

$$1 \to T \to J(C) = \underset{C/k}{\overset{0}{\mathcal{P}ic}} \to A \to 1$$

is given by $A = J(\widetilde{C_i})$ where $\widetilde{C_i}$ is the normalisation of C_i and $X(T) = H_1(\Gamma, \mathbb{Z})$, for the dual graph Γ of $C_{\overline{k}}$, so is of rank rank $H^1(\Gamma(X_{\overline{k}}), \mathbb{Z})$ [Con+11, Proposition 7.14].

We recall [Liuo2, §10.1.3] that the dual graph Γ has a vertice for each C_i, and its edges correspond to the singularities of C, the edge links C_i to C_j if the two analytic branches of the singularities belong to C_i and C_j respectively (hence is a loop if $C_i = C_j$).

We finish by a discussion on representability theorems of the generalised Jacobian over a general base. First if X/S is projective flat curve locally of finite presentation, with integral geometric fibers, then $\mathcal{P}ic_{X/S} = \bigsqcup (\mathcal{P}ic_{X/S})^n$ by Theorem 2.3.4.(vi). The same arguments as in Theorem 2.4.3 show that the $(\mathcal{P}ic_{X/S})^n$ are torsors under $(\mathcal{P}ic_{X/S})^0$, and the description of the generalised Jacobian $J(C/k)$ in [BLR12, Proposition 9.2.13] shows that $(\mathcal{P}ic_{X/S})^0 = \mathcal{P}ic^0_{X/S}$ since by assumption the geometric fibers of X/S are irreducible curve (see [BLR12, Theorem 9.3.1]).

More generally, we have:

obianssemistable

Theorem 2.4.10.

- *(Deligne, [BLR12, Theorem 9.4.1]): Let X/S be a (weak) semistable curve locally of finite presentation. Then $\mathcal{P}ic_{X/S}$ is a smooth algebraic space, and $\mathcal{P}ic^0_{X/S}$ is a semiabelian scheme (so in particular is a smooth separated scheme), and it has a canonical S-ample line bundle $\mathcal{L}$.*
- *(Raynaud, [BLR12, Theorem 9.4.2]): if S is the spectrum of a dvr, $f : X \to S$ proper flat curve and an O-morphism, and the gcd of the geometric multiplicities of the irreducible components of the special fiber is 1, then $\mathcal{P}ic_{X/S}$ is a smooth algebraic space, and $\mathcal{P}ic^0_{X/S}$ is a smooth separated scheme.*

More Details 2.4.11. Other representability theorem:

[BLR12, Theorem 9.3.7]: If S is a stricly henselian local scheme, X/S flat projective morphism whose geometric fibres are reduced and connected curves. Then smooth separated and coincide with $\mathcal{P}ic^0_{X/S}$ is a smooth and separated scheme.

Corollary of Raynaud's theorem [BLR12, Corollary 9.4.3]: if S dvr, X/S proper flat curve with connected generic fibre, X regular and there is a rational point in its generic fibre. Then $\mathcal{P}ic_{X/S}$ is an algebraic space and $\mathcal{P}ic^0_{X/S}$ a separated scheme.

3 DEGENERATIONS AND LIFTS

chap:lift

CONTENTS

In this Chapter we study two related topics: degenerations and lifts. Degenerations study what happen when we reduce an abelian variety A defined over a number field K modulo a prime ideal $\mathfrak{p}$. For this to make sense, we need a good model $\mathcal{A}$ of A over the maximal order O_K. This is provided by the theory of Neron models. This allow to construct modular varieties (like class polynomials or modular polynomials) by constructing them modulo $\mathfrak{p}$ a CRT approach

Degenerations also allow us to tackle what happen at the boundary of the moduli space of abelian varieties (suitably compactified). This is useful to show that certain spaces of modular form are finitely generated, or to construct modular forms from polynomial covariants of curves in small dimension.

3.1 SEMI-ABELIAN VARIETIES AND NÉRON MODELS

sec:semiab

3.1.1 *Semi-abelian varieties*

A good intuition for a commutative linear group scheme is that the unipotent part is "bad" (behaves badly) while the torus part is "good". So a semi-abelian variety is almost as nice as an abelian variety:

def:semiab

Definition 3.1.1. A semi-abelian variety G/k over a field k is a connected smooth commutative group scheme such that $G_{\overline{k}}$ is an extension of an abelian variety by a torus (equivalently $G_{\overline{k}}$ contains no nontrivial smooth connected unipotent group). A semi-abelian scheme G/S is a smooth separated commutative group scheme whose (geometric) fibers are semi-abelian varieties.

We leave as an exercice a fiberwise characterisation of semi-abelian schemes, as in Section 2.3.5, using Proposition B.3.3 and Lemma B.3.1.

Remark 3.1.2. Be careful that the definition from [BLR12, p. 178] does not requires G connected, contrary to the usual definitions (see eg [FC90, Definition 1.2.3]). We will call these varieties weakly semiabelian, likewise for weakly semiabelian schemes.

This notion is stable by isogeny [] and if $1 \to G' \to G \to G'' \to 1$ is an exact sequence, G is (weakly) semi-abelian if and only if G' and G'' are.

We have the following structure theorem, which show that commutativity is automatic and that the torus part descend over the base field:

th:structsemiab

Theorem 3.1.3 ([Con+11, L13, Theorem 3.1])**.** *Let G/k be a smooth connected group, such that the affine part of $G_{\overline{k}}$ is a torus. Then G is commutative, and there is a unique short exact sequence of k-groups:*

$$1 \to T \to G \to A \to 1$$

where T/k is a torus and A/k is an abelian variety.

3.1.2 Néron models

subsec:neron

Let S be a Dedekind connected scheme with field of fractions K, and let $G_K = \mathrm{Gal}(K) = \mathrm{Gal}(K_s/K)$ for a separably closed extension K_s of K. When S is affine, we denote $S = \mathrm{Spec}\, R$, and when R is furthermore local (so a dvr), we denote by $m = (\pi)$ its maximal ideal, π a uniformiser, v the corresponding place on K and by $k = R/m$ its residue field and p the characteristic of k. Implicitly, often when we mention R we assume that we are in the local case. (Most of what follows extend to a general Dedekind scheme S by looking at its connected components.)

Néron models are in some sense the best possible models $\mathcal{A}$ of an abelian variety A/K, and allow us to get what the best possible reduction $\mathcal{A}_k$ of A (sometimes denoted A_k by abuse of notation) we can obtain. These results will be extremely useful to reduce abelian varieties defined over a number field to abelian varieties defined over finite fields.

def:neronmodel

Definition 3.1.4. Let X/K be a smooth separated scheme of finite type (equivalently qc). A Néron model is a smooth separated scheme of finite type $\mathcal{X}/S$ such that $\mathcal{X}_K \simeq X$ and which satisfy the Néron mapping property: for any smooth scheme $\mathcal{Y}/S$ with a mapping $\mathcal{Y}_K \to X$ there is an extension to a mapping $\mathcal{Y} \to \mathcal{X}$.

See [Con+11, pp. L11, 1.3.12] and [BLR12, Definition 1.1.1] for the interpretation of the Néron mapping property as a version of a valuative criterion.

If R is local, we denote by $\mathcal{X}^\circ$ the open subscheme of $\mathcal{X}$ obtained from $\mathcal{X}$ by removing the non identity components of the special fiber X_k.

As an exemple of the Néron mapping property, if $\mathcal{X}$ is a Néron model of X, then if X is a group scheme, there is a unique structure of group scheme on $\mathcal{X}$ extending the one on X [BLR12, Proposition 1.2.6]. As another exemple, if R is local we have an isomorphism $\mathcal{X}(R) \simeq X(K)$[1], and if $\mathcal{Y}$ is a Néron model of Y, then $\mathrm{Hom}_S(\mathcal{X}, \mathcal{Y}) \simeq \mathrm{Hom}_K(X, Y)$.

Proposition 3.1.5.

- *The formation of Néron models commute with étale base change.*
- *If R is local, a smooth group scheme of finite type $\mathcal{G}/R$ is the Néron model of its generic fiber if and only if $G(R^{sh}) \to G(K^{sh})$ is an isomorphism where R^{sh} is the strict henselian completion of R (this is the Weak Néron property; equivalently $G(R') \to G(K')$ is an isomorphism for all R'/R étale local);*
- *If R is local and $R \subset R' \subset R^{sh}$, then a Néron model $\mathcal{G}'$ over R' descends to a Néron model $\mathcal{G}$ over R.*
- *More generally, if $R \subset R'$ is a local extension of dvr with ramification index 1*[2] *(in particular $R' = \hat{R}$ is the completion). Then a Néron model descends from R' to R and ascends from R to R'.*

[1] By definition of a pullback, we always have $\mathcal{X}(K) = \mathcal{X}_K(K) = X(K)$.

[2] This means that the uniformizer π of R induces a uniformizer on R', and the residue field $k' = R'/\pi R'$ is separable over $k = R/\pi R$. If R'/R is of finite type and furthermore K'/K is separable then $R \to R'$ is étale.

Proof. The first item is [BLR12, Proposition 1.2.2] (see also [Con+11, L11, Proposition 1.4.3]), the second is [BLR12, Criterion 1.2.9 and Theorem 7.1.1] (see also [Con+11, L11, Proposition 6.1.1]), the third [BLR12, Corollary 6.5.4] (see also [Con+11, L11, Proposition 6.2.1]), and the fourth [BLR12, §3.6 and Theorem 7.2.1] (see also [Con+11, L11, Proposition 6.2.2]).

Note that any weak Néron model $\mathcal{X}/S$ of X/K satisfy the weak Néron mapping property: given a smooth scheme $\mathcal{Z}/S$ with irreducible special fiber Z_k, a K-rational map $\mathcal{Z}_K\mathcal{X}_K$ extends to an R-rational map $\mathcal{Z}\mathcal{X}$ [Con+11, L11, Proposition 3.3.1]. □

th:neron **Theorem 3.1.6** (Néron [Nér64]). *An abelian variety A/K admits a Néron model $\mathcal{A}$ over S.*

Proof. This is [BLR12, Theorem 1.4.3]. By standard limit arguments (approximation) [GD64, §IV.8], an abelian variety extends to an abelian scheme over an open U of S [BLR12, Proposition 1.4.2]. By Néron's theorem [BLR12, Theorem 1.3.1 and Corollary 1.3.2], there exists a local Néron model $\mathcal{A}_s$ over each closed point $s \in S \setminus U$, and these glue together to a global Néron model $\mathcal{A}/S$. Conversely, a scheme $\mathcal{A}$ is a Néron model if and only if $\mathcal{A}_s$ is a Néron model of A over $O_{S,s}$ for each closed point $s \in S$ [BLR12, Proposition 1.2.4].

We refer to [BLR12] for the full proof (this is the canonical book on the subject), and to [Con+11, L11, Theorem 2.3.4] for an overview. See also [Liu02] for the case of elliptic curves. □

The proof of Theorem 3.1.6 use two crucial ingredients due to Weil. The first is an extension of rational map into group schemes:

omorphisms **Proposition 3.1.7** ([BLR12, Theorem 4.4.1]). *If $u : UG$ is a T-rational map from a smooth scheme U/T to a smooth and separated group scheme G/T, with the base T normal and noetherian, then if u is defined in codimension ≤ 1 it is defined everywhere.*

The second is that birational group laws extend to a group law [BLR12, Theorem 6.6.1].

chemeneron **Example 3.1.8.** By Proposition 2.3.16, an abelian scheme satisfy a stronger version of the Néron mapping property, so in particular is the Néron model of its generic fiber [BLR12, Proposition 1.2.8].

More generally, if A/K has a smooth and proper model $\mathcal{A}/S$, then $\mathcal{A}$ is an abelian scheme hence is the Néron model of A. (See [BLR12, Proposition 1.4.2] or use Theorem 2.3.11 together with the valuative criterion of properness to extend $\epsilon : \operatorname{Spec} K \to A$ to $\epsilon : S \to \mathcal{A}$.)

In fact for an abelian variety we have a stronger version of the Neron mapping property:

eniesneron **Proposition 3.1.9** ([BLR12, Proposition 1.4.4]). *Let A/K be an abelian variety and $\mathcal{A}/S$ its Néron model. Then for each smooth scheme Y/S each K-rational map $Y_K A$ extends to a unique S-map $Y \to \mathcal{A}$.*

Proof. This is immediate combining Proposition 2.2.7 and the mapping property of a Néron model. Alternatively this is an immediate application of Proposition 2.3.16 since the K-rational map extends to an open by [GD64, §IV.8]. □

3.1.3 *Good reduction*

dreduction With the same notations as above, an abelian variety A/K has good reduction if it extends to an abelian scheme $\mathcal{A}/R$. We recall by Example 3.1.8 that $\mathcal{A}/R$ is then the Néron model of its generic fiber.

dreduction **Theorem 3.1.10** (Good reduction). *An abelian variety A/K with Néron model $\mathcal{A}$ has good reduction if it satisfy one of these equivalent conditions:*

- *The Néron model $\mathcal{A}$ of A is an abelian scheme, or $\mathcal{A}^\circ$ is an abelian scheme;*
- *$\mathcal{A}$ or $\mathcal{A}^\circ$ is proper;*

And if R is local this is also equivalent to:

- *The identity component ${\mathcal{A}^\circ}_k$ of its special fiber is proper;*

- *The representation ρ_ℓ of G_K on the Tate module $T_\ell(A)$ is unramified (ie the inertia I_K acts trivially) for one (resp. any) $\ell \neq p$ (Néron-Ogg-Shafarevich). Equivalently $A[m]$ is not ramified for all m prime to p (resp. an infinite number of m prime to p).*

- *The ℓ-divisible group $A(\ell)$ has good reduction (if R is henselian this means that it extends to a ℓ-divisible subgroup over R), for one (resp. any) ℓ, including $\ell = p$.*

Proof. If $\mathcal{A}$ is an abelian scheme, it is proper, and if $\mathcal{A}$ or $\mathcal{A}^\circ$ is proper so is ${\mathcal{A}^\circ}_k$. The converse is Lemma A.3.3. In fact if we have a flat model $\mathcal{A}$ of A such that ${\mathcal{A}^\circ}_k$ is proper, then $\mathcal{A}^\circ$ is an abelian scheme by Lemma A.3.3 so is the Néron model of A.

The Néron-Ogg-Shafarevich condition is the main result of [ST68] (see [ST68, Theorem 1] and [BLR12, Theorem 7.4.5]). The inertia I_K is not strictly defined (it depends of a choice of place on K_s extending the place v representing m), but since all choice are conjugate to each other, the unramifiedness of the action does not depend on any choice. Grothendieck's theorem is in [Gro72, p. 5.10] in the case of mixed characteristic, and extended by de Jong in [Jon98, Theorem 2.5] to the case of equal characteristic (see [De 98, Theorem 3] for a summary). See [Con+11, L11, Corollary 2.2.7 and Theorem 5.3.1] for an overview of the proofs. □

As a corollary, this notion is stable by isogeny, and by exact extension: if $0 \to A' \to A \to A'' \to 0$ is an exact sequence, A has good reduction if and only if A' and A'' have good reduction.

Remark 3.1.11. If A has an ample line bundle $\mathcal{L}$ and has good reduction, then the polarisation $\Phi_{\mathcal{L}} : A \to \widehat{A}$ extend to a polarisation $\mathcal{A} \to \widehat{\mathcal{A}}$ of the Néron model. Since the base scheme S is normal, this polarisation is induced by a line bundle on $\mathcal{A}$. In otherwords, if R is local, $\mathcal{A}$ is the Zariski closure in $\mathbb{P}_R$ of the embedding of A into $\mathbb{P}_K$.

An abelian variety has potential stable reduction if it acquires good reduction over a finite field extension K'/K. Then by Theorem 3.1.10, A has potential good reduction if and only if the image $\rho_\ell(I_K)$ of the inertia I_K is finite in $T_\ell(A)$ for a $\ell \neq p$ (and in this case the restriction of ρ_ℓ to I is independent of ℓ in a sense made precise in [ST68, Theorem 2.ii]), if and only if the modular invariant of A is integral at v (the place corresponding to m) [ST68, §2].

op:potentialgood

Proposition 3.1.12 (Potential good reduction)**.** *Assume that R is local. If the action of G_K on $T_\ell(A)$ is commutative, or if A is CM, then A has potential good reduction.*

If A has potential good reduction, then the connected component ${\mathcal{A}_k}^\circ$ of the special fiber of its Néron model is an extension of an abelian variety by a unipotent group (hence the extension where it acquires good reduction is exactly the same extension where it acquires semi-stable reduction, in other words if A has both potential good reduction and semi-stable reduction, it has good reduction).

If A has potential good reduction, then if $m \geq 3$ is prime to p,

- *The inertia group of $K(A[m])/K$ is independent of m, and this extension is tamely ramified if $p > 2g + 1$;*

- *$K(A[m]/K)$ is unramified if and only if A has good reduction;*

- *If R is strictly henselian, $K(A[m])$ is the smallest extension of good reduction (so is independent of $m \geq 3$) and its Galois group is* $\operatorname{Ker} \rho_\ell$.

If furthermore the residue field k is a finite field $\mathbb{F}_q$, there exists an extension K'/K of good reduction with the same residue field. Moreover if σ represent the Frobenius in $G_K = \operatorname{Gal}(K)$, then the action of σ on $T_\ell(A)$ is the action of the Frobenius on $T_\ell(\mathcal{A}'_k) = T_\ell(A') = T_\ell(A)$, so its characteristic polynomial is the characteristic polynomial of the Frobenius acting on $\mathcal{A}'_k$.

Proof. This is [ST68, §2], except the part about CM abelian varieties which is [ST68, Theorem 6] and is developed in much more details in [ST68, §4 to 7]. See also [Con+11, L13, Proposition 6.5] for a proof using the semi-stable theorem. □

Remark 3.1.13. We use the potential good reduction of CM abelian varieties to develop a CRT algorithm to construct class polynomials in [Rob21, Chapter 7].

3.1.4 Semi-stable reduction

We continue with the notations from Section 3.1.2. We refer to [Cas13] for a more general overview of the topic of semi-stable reduction.

A group scheme G/S is said to have semi-abelian (or semi-stable) reduction at a closed point $s \in S$ if ${G^\circ}_s$ is a semi-abelian variety (in other words if G_s is a weak semi-abelian variety). We say that an abelian variety A/K has semi-stable reduction at s if its Néron model $\mathcal{A}$ has semi-abelian reduction at s [BLR12, §7.4].

elianneron

Proposition 3.1.14. *Let R be local, and A/K be an abelian variety with Néron model $\mathcal{A}/R$. Assume that A has a model G/R by a smooth separated group scheme which has semi-abelian reduction (ie G/R is weakly semi-abelian). Then the canonical morphism $G \to \mathcal{A}$ is an open immersion and restricts to an isomorphism on the identity components, so A has semi-stable reduction.*

In particular if A has semi-stable reduction, then the formation of $\mathcal{A}^\circ$ is compatible with local base change $R \to R'$ of dvrs.

Proof. This is [BLR12, Proposition 7.4.3 and Corollary 7.4.4], see also [Con+11, L13, Theorem 4.4 and Corollary 4.5]. □

As a corollary, a semi-abelian scheme $\mathcal{A}/S$ whose generic fiber is an abelian variety A is the identity component of the Néron model of A. When A has semi-stable reduction, its Néron model still does not commute with local base change (only its identity component does). In particular, the component group $\pi_0(\mathcal{N}(A))$ can increase. In fact, the limit of the component groups $\pi_0(\mathcal{N}(A_{K'}))$ is $\mathrm{Hom}(X(T_{\overline{k}}), \mathbb{Q}/\mathbb{Z})$ where T is the maximal torus of the semi-abelian $\mathcal{N}(A)_{\overline{k}}$ [Gro72, Exposé IX, §11.9].

The notion of semi-stable reduction is stable by isogeny, hence by exact extension [BLR12, Lemma 7.4.2]. More precisely:

Proposition 3.1.15. *Let R be local, $f : A \to B$ be an isogeny of abelian varieties over K, and let $\mathcal{A}, \mathcal{B}$ be their Néron model. Then if either ${\mathcal{A}^\circ}_k$ or ${\mathcal{B}^\circ}_k$ is semi-abelian then so is the other, and in this case ${f^\circ}_k$ is an isogeny. And furthermore $\mathrm{Hom}_K(A, B) \to \mathrm{Hom}_k({\mathcal{A}^\circ}_k, {\mathcal{B}^\circ}_k)$ is injective.*

Proof. The first part is immediate by the extension of isogenies to their Néron-models mentioned in Section 3.1.2 and the fact that semi-abelian varieties are stable under isogenies (of smooth group schemes). See [Con+11, L13, Proposition 4.1] and [BLR12, Corollary 7.3.7]. The injectivity of the reduction map is [Con+11, L13, Proposition 6.4]. □

Like potential good reduction, there is a notion of potential semi-stable reduction.

emistable

Theorem 3.1.16 (Potential semi-stable reduction)**.** *Every abelian variety A/K has potential semi-stable reduction everywhere. More precisely, if R is local, there is a finite separable field extension K'/K such that $A_{K'}$ has semistable reduction over R', the integral closure of R in K'.*

Proof. This is proved by Grothendieck in [Gro72]. From the potential semi-stable reduction of Jacobians we can deduce the potential semi-stable reduction of curves [DM69]. Nowadays the proof goes the other way around: potential semistability of curves is proved directly, from which we deduce potential semistability of Jacobians, and hence of any abelian variety (since they are always quotient of Jacobians). See [BLR12, Theorem 7.4.1] and [Con+11, L13, Theorem 4.2]. In characteristic different from 2 there is also a very nice proof due to Mumford using the theory of theta functions [Cha85, Appendix II]. □

Concretely an abelian variety A acquires semistable reduction at all places of the Galois splitting field $K(A[N])/K$ of $A[N]$ for any $N \geq 3$ not divisible by $p = \mathrm{char}\, k$ by Raynaud's theorem [Gro72, Exposé IX, Proposition 4.7] (see also [Con+11, L13, Proposition 6.5]) (compare with Proposition 3.1.12, we recall that if A has potential good reduction, it acquires good reduction whenever it acquires semistable reduction). By [SZ95], it also has semistable eduction whenever all points of a maximal isotropic subgroup of $A[N]$ are defined for a $N \geq 5$ not divisible by p.

We also have a criteria for semi-stability, proved by Grothendieck:

abcriteria

Theorem 3.1.17. *Let R be local, I_K the inertia group of G_K. Then A/K has semi-stable reduction if and only if it satisfy one of these equivalent condition:*

- *the action of I_K on one (resp. all) $T_\ell A$ with $\ell \neq p$ is unipotent. The unipotency index is then (at most)* 2.
- *The ℓ-divisible group $A(\ell)$ has semi-stable reduction, for one (resp. any) ℓ, including $\ell = p$.*

Proof. The first item is proven in [Gro72, p. IX.3.5], see [Con+11, L13, Theorem 5.8] for an overview of the proof or [BLR12, Theorem 7.4.6]. See [De 98, Theorem 2] and [Jon98, Theorem 2.5] for the second item. □

As a corollary, we recover that semistability is stable under isogenies or exact sequences.

Orthogonality

We finish by a discussion on duality and the orthogonality theorem. We refer to [Con+11, L13, §5] for more details. Let R be local and A be an abelian variety and assume that it has semi-stable reduction, and let $\mathcal{A}$ be its Néron model. Then since ${\mathcal{A}^\circ}_k$ is semi-abelian, by Theorem 3.1.3 there is an exact sequence

$$0 \to T \to {\mathcal{A}^\circ}_k \to B$$

with T/k a torus and B/k and an abelian variety. Since A is isogenous to its dual $\widehat{A}$, $\widehat{A}$ is also semistable. By [Gro72, §IX], in the decomposition $0 \to T' \to {\widehat{\mathcal{A}}^\circ}_k \to B'$ of the Néron model of $\widehat{A}$, B' is canonically dual to B and T' dual to T (which means that their Galois lattices $X(T)(k_s)$ and $X(T')(k_s)$ are dual).

Fix an integer N, then $\mathcal{A}[N]$ is flat quasi-finite by [BLR12, Lemma 7.3.2] (and is étale if N is prime to p). We remark that if $p \nmid N$, ${\mathcal{A}^\circ}_k[N]$ has order N^{t+2a} where $a = \dim B$ and t is the rank of T.

Assume that R is henselian, then by the structure theorem of quasi-finite morphisms Corollary A.4.5 we have $\mathcal{A}[N] = \mathcal{A}[N]_f \bigsqcup \mathcal{A}[N]_\eta$ with $\mathcal{A}[N]_f$ finite with special fiber $\mathcal{A}_k[N]$ and $\mathcal{A}[N]_\eta$ having empty special fiber (this is a special case of [GD64, p. III.5.5.2] or [Stacks, Tag 03GX]). Since R is henselian, the open and closed subgroups $T[N]$ and ${\mathcal{A}^\circ}_k[N]$ of ${\mathcal{A}^\circ}_N$ lift to $\mathcal{A}[N]_f$ into a filtration: $\mathcal{A}[N]_t \subset \mathcal{A}[N]_f^\circ \subset \mathcal{A}[N]$.

m:subgroupsneron

Lemma 3.1.18. *With the notations above, assume that R is henselian, and let $K^{un} = K_s^{I_K}$ be the maximal unramified extension of K, and R^{sh} the strict henselisation of R seen as the extension of v to K^{un}, its residue field is then k_s.*

Then if $p \nmid N$, $A[N](K) = \mathcal{A}[N]_f(K) = \mathcal{A}[N](R) = \mathcal{A}_k[N](k)$ and $A[N](K_s)^{I_K} = A[N](K^{un}) = \mathcal{A}[N]_f(K_s) = \mathcal{A}[N](R^{sh}) = \mathcal{A}_k[N](k_s)$.

In general, $A(K^{un}) = \mathcal{A}(R^{sh}) \to \mathcal{A}_k(k_s)$ is surjective.

Proof. If X is a scheme separated étale and quasi-finite over an henselian local ring R, $X(R) \simeq X_k(k)$. Indeed by the structure theorem of quasi-finite morphisms Corollary A.4.5 $X = X_f \bigsqcup X_\eta$ with X_f finite étale and use the Henselian property to get $X_f(R) = X_{f,k}(k) = X_k(k)$ But since R is connected, we have $X_f(R) = X(R)$ and since X_f is finite, $X_f(R) = X_f(K)$ by the valuative criterion of properness. In summary: $X_f(K) = X(R) = X_f(R) = X_k(k)$. (See also [BLR12, Proposition 7.3.3].)

We apply this to $\mathcal{A}[N]$, to get all the equalities of the first equation, except $A[N](K) = \mathcal{A}[N](R)$ which comes from the (weak) Néron mapping property: $A(K) = \mathcal{A}(K) = \mathcal{A}(R)$. The second equation comes from base changing $\mathcal{A}$ to $\mathcal{A}/R^{sh}$ (using commutativity of Néron models with étale extensions). The last surjection simply comes from the fact that $\mathcal{A}/R^{sh}$ is smooth.

Note also that if X is not étale, X_f is just finite, but we may form its largest finite étale quotient X_f^t (see the proof of Lemma B.1.2). Then $(X_f^t)_k(\bar{k}) \simeq (X_f)_k(\bar{k})$ and so $(X_f^t)_k(k) \simeq (X_f)_k(k) = X_k(k)$, so $X_k(k) \simeq X_f^t(R)$.

Thus, if we relax the condition $p \nmid N$, we can use the connected-étale sequence Lemma B.1.2 and Section 3.3.1 to get the reduction morphism: $A[N](K) = \mathcal{A}[N](R) = \mathcal{A}[N]_f(R) = \mathcal{A}[N]_f(K) \to \mathcal{A}[N]_f^t(K) = \mathcal{A}[N]_f^t(R) = \mathcal{A}_k^t[N](k) = \mathcal{A}_k[N](k)$ with the different reduction map from the left members to the right members all compatible. □

Passing to ℓ-divisible groups for $\mathcal{A}[\ell^n]_t$ and $\mathcal{A}[\ell^n]_f^\circ$ (which are of heights t and $t + 2a$), and viewing their generic fibers inside of the ℓ-divisible group of A, we get if $\ell \neq p$ (in fancy term by passing through their crystal, which in this case is just the Tate module) the filtration of G_K-stable saturated $\mathbb{Z}_\ell$ submodules:

$$T_\ell(A)_t \subset T_\ell(A)_f \subset T_\ell(A).$$

We have $T_\ell(A)_f = T_\ell(A)^{I_K}$ is the inertial fixed part, since $\mathcal{A}[N]_f(K_s) \subset \mathcal{A}[N](K_s)$ is exactly the unramified submodule, ie the K^{un} points by Lemma 3.1.18 or [Con+11, L13, Remark 5.3].

The *orthogonality theorem* (deduced from the duality of $\mathcal{A}$ and $\widehat{\mathcal{A}}$ or directly as in [Con+11, L13, Theorem 5.5]) then gives that under the Weil pairing $T_\ell(A) \times T_\ell(\widehat{A}) \to \mathbb{Z}_\ell(1)$, that $T_\ell(A)_f$ and $T_\ell(\widehat{A})_t$ are the exact annihilators of each others. In particular the Cartier dual of $T_\ell(\widehat{A})_t$ is $T_\ell(A)/T_\ell(A)_f$, hence has trivial I_K action. This gives one direction in Theorem 3.1.17.

3.1.5 *Extension of isogenies and morphisms*

isogenies

We have already seen some results about extension of morphisms and isogenies. Here T denotes a general base, and S a Dededking scheme.

1. If A/k is an abelian variety, any birational morphism from a regular variety Y/k is defined everywhere Proposition 2.2.7.

tensionii

2. More generally, Proposition 2.3.16: If A/T is an abelian scheme, any rational T-morphism $g : YA$ from a regular scheme Y is defined everywhere. (Note that if T is integral of generic point η, then any η-rational map $X_\eta Y_\eta$ of schemes finitely presented over T extend to an open of T by [GD64, §IV.8]. So in the proposition above it suffices to have an η-rational map YA, Y regular, for it to be defined everywhere.)

3. If T is normal and noetherian, a T-rational map YG from a smooth scheme Y/T to a smooth and separated group scheme G/T, is defined everywhere if it is defined in codimension ≤ 1 Proposition 3.1.7.

4. If A/K is abelian variety and $\mathcal{A}/S$ its Néron model, by Definition 3.1.4, for each smooth scheme Y/S each K-rational map $Y_K A$ extends to a unique S-map $Y \to \mathcal{A}$.

5. If $\mathcal{A}/S$ is an abelian scheme, it is the Néron model of $\mathcal{A}_K$, so for each smooth scheme Y/S, each K-rational map $Y_K A$ extends to a unique S-map $Y \to \mathcal{A}$ (this is a particular case of Item 2).

tensionvi

6. If S is local and $\mathcal{A}/S$ is a semi-abelian scheme whose generic fiber is abelian, it is the identity component of its Néron model Proposition 3.1.14, so for every smooth scheme Y/S such that Y_k is connected, every map $Y_K \to \mathcal{A}_K$ extends uniquely to $Y \to \mathcal{A}$.

The proof by [BLR12] of Item 6 uses as an intermediate result the following Proposition which is interesting in its own right: an isogeny of abelian varieties of degree prime to the residue characteristic extend to the Néron models.

agredient

Proposition 3.1.19. *An isogeny $f : A \to B$ of abelian varieties over K extend to an isogeny $\mathcal{A} \to \mathcal{B}$ of their Néron models over a local R if A has semi-stable reduction or* $\deg f$ *is prime to the residue characteristic.*

Proof. This is [BLR12, §7.3]. The proof goes as follow. First assume we are over a general base S, and let G/S be a smooth commutative group scheme of finite type. Then if ℓ does not divide the residual characteristics of S, the multiplication by ℓ $[\ell] : G \to G$ is étale, so the ℓ-torsion subgroup $G[\ell]$ is étale. In general, provided that G is (weakly) semi-abelian, $G[\ell]$ is always flat quasi-finite [BLR12, Lemma 7.3.2].

Secondly, if $f : G \to G'$ is an isogeny of smooth commutative algebraic groups over a field k, and that either $\operatorname{char} k \nmid \deg f$ or G is (weakly) semi-abelian, then there is a contragredient isogeny $g : G' \to G$ such that $g \circ f = [\deg f]$ [BLR12, Lemma 7.3.5].

So going back to $S = \operatorname{Spec} R$ Dedekind local, if G/S and G'/S are Néron models of their generic fibers G_K and G'_K (smooth commutative algebraic groups), and $f_K : G_K \to G'_K$ is an isogeny such that either G is (weakly) semi-abelian or $\deg f$ does not divide p, then f_K and its contragredient isogeny g_K extends [BLR12, Proposition 7.3.6].

As a corollary, G is weakly semi-abelian if and only if G' is weakly semi-abelian [BLR12, Corollary 7.3.7]. □

Remark 3.1.20. Conversely, if $f : A \to B$ is a morphism of abelian varieties over K, and we denote $f : \mathcal{A} \to \mathcal{B}$ the induced map on their Néron models, then if $f^\circ{}_k : \mathcal{A}^\circ{}_k \to \mathcal{B}^\circ{}_k$ is an isogeny, then f is an isogeny [Con+11, L13, Proposition 4.1.(2)].

We can strengthen Proposition 3.1.19 to a normal base (and also not requiring the generic fiber to be abelian) as follow:

tendingisogenies

Proposition 3.1.21. *If $\mathcal{A}/T$ and $\mathcal{B}/T$ are two semiabelian schemes over a normal locally Noetherian scheme T, and $f : \mathcal{A}|U \to \mathcal{B}|U$ a morphism (of groups) defined over a dense open U of T, then f extends uniquely to T.*

Proof. This is [Fal86, Lemma 2.1], see also [Con+11, L12, Lemma 35]. By [BLR12, §10.1], a smooth algebraic group G_K over admits a Néron model (resp. an lft Néron model) over R (strictly henselian excellent) if and only if G_K does not contains $\mathbb{G}_a$ and $\mathbb{G}_m$ (resp. G_K does not contains $\mathbb{G}_a$). In particular, if R is a complete dvr with algebraically closed residue field, it is excellent and strictly henselian, so a semi-abelian scheme A/K has an lft Néron model (which is only locally of finite type). But the same reasoning as in Proposition 3.1.14 show that if $\mathcal{A}/R$ is a semi-abelian scheme, it is the identity component of its Néron model. So in particular, f extends by the property of lft Néron models (since the special fiber of $\mathcal{A}$ is connected). Of course, if the generic fibers are abelian, this is juste Item 6.

For the general case, we consider the closure X of the graph of f, and we need to show that $p_1 : X \to \mathcal{A}$ is an isomorphism. We may then reduce to the case treated above by using [Stacks, Tag 0CM1] and [GD64, Inew.5.5.2]. Indeed, since the map extends above excellent strictly henselian local rings, and the extension is unique because torsion points are dense, this shows that the map p_1 is a bijection (hence is quasi-finite). Since it is birational due to the existence of f_0 it is an isomorphism by ZMT since T is normal. □

A related result is that if we have an isogeny over a separable field extension of $k(T)$, the isogeny extends over an étale cover of T:

endingisogenies2

Proposition 3.1.22. *If $\mathcal{A}/T$ and $\mathcal{B}/T$ are two abelian schemes over a normal integral locally Noetherian scheme T, L a separable extension of $K = k(T)$ and $f : \mathcal{A}_L \to \mathcal{B}_L$ a morphism (of groups), then f extends to a morphism $f : \mathcal{A}_{T'} \to \mathcal{B}_{T'}$ for an étale cover (ie an étale finite map) $T' \to T$.*

Proof. This is [Sta17]. The idea is that $\mathcal{H}om_T(\mathcal{A}, \mathcal{B})$ has connected components proper (by Weil's extension theorem [**prop:extendinggroupmorphisms**]) and unramified (by the rigidity Lemma Lemma 2.3.8). If T is normal, then any finite unramified dominant morphism to T is étale, hence the components of $\mathcal{H}om_T(\mathcal{A}, \mathcal{B})$ that dominate T are finite étale. □

If the degree is invertible, then we can extend the isogeny as well as the target semiabelian variety:

nsionofisogenies

Proposition 3.1.23. *If T is normal and locally noetherian, and U is an open of T, then if $f_0 : A_0 \to B_0$ is an isogeny of semi-abelian schemes over U of degree invertible in $\mathcal{O}_T$, and A_0/U extends to a semi-abelian scheme A/S, then f_0 extends to an isogeny $f : A \to B$ over S.*

If A is abelian, then B too (and we only need T to be geometrically unibranch locally noetherian for this result).

Proof. This is [Ore20]. We first only assume that T is geometrically unibranch locally noetherian. We may reduce to T connected by working on each connected component. Then we take the kernel of f to be the closure $\overline{K}$ of the kernel K of f_0 in $A[m]$, m the degree of f (which is constant since T is connected). Since T is geometrically unibranch, $A[m]$ too (since it is étale over T), and this shows that $\overline{K}$ is étale over T. Then we may define $B = A/\overline{K}$. This is a semiabelian algebraic space.

If A is abelian, B is an abelian algebraic space, hence an abelian scheme by Theorem 2.3.2. Otherwise, if S is normal, B is a semiabelian scheme by Proposition B.3.4. □

See [FC90, §V.6] for more on extending semi-abelian schemes: an abelian scheme over a dense open subscheme of a regular local ring whose complement is a divisor with normal crossing extends to a semi-abelian scheme provided the ℓ-adic monodromy is unipotent and the generic characteristic is zero.

See also [FC90, p. 192] for an example of an isogeny $f_0 : A_0 \to B_0$ of abelian schemes over U such that A_0 extends over S but B_0 does not.

More Details 3.1.24. By [BLR12, Theorem 7.5.4] (see also [Con+11, L11, Theorem 6.3.1]): if $0 \to A' \to A \to A" -> 0$ is an exact sequence of abelian varieties, R of characteristic $(0, p)$ and absolute ramification $e < p - 1$, A has good reduction, then the Néron models are abelian schemes and satisfy $0 \to \mathcal{A}' \to \mathcal{A} \to \mathcal{A}" \to 0$. If A has only semiabelian reduction, the sequence are formed by semiabelian schemes and is still left exact.

From the purity result of [FC90, §V.6], the authors deduce that any morphism from the complement of a divisor with normal crossings in a regular scheme to $\mathcal{A}^*_{g,n}$ automatically extends (uniquely) to S provided the generic characteristic of S is zero.

3.2 REDUCTION OF CURVES

c:sscurves

3.2.1 *Minimal regular models and canonical models*

We briefly detail the link between stability of curves and their Jacobians. A good references for curves is [Liu02], a good summary is in [Rom13] and [Con+11, p. L12].We continue with the notations of Section 3.1.2.

We recall that if C/k is a curve, a nodal singularity (or an ordinary double point) is a point x such that $\hat{O}_{C,x} \simeq k[[u,v]]/uv$. By Artin's approximation theorem [Art69a], this means that étale locally around x, the curve look like the intersection of the x coordinate and the y coordinate in the plane at 0.

Definition 3.2.1. A curve $C/\bar{k}$ is semistable (resp. stable) if it is proper, reduced, connected of dimension 1, with only nodal singularities, and whose irreducible components isomorphic to $\mathbb{P}^1$ meet the other components in at least 2 points (resp. 3 points).

A proper flat (relative) curve $\mathcal{C}/S$ is stable (resp. semistable) if it has stable (resp. semistable) geometric fibers.

Stable curves were introduced in [DM69], to construct a smooth proper compactification of $\mathcal{M}_g$ the moduli stack of smooth curves of genus g. The terminology comes from [MFK94], and if we exclude curves of arithmetic genus 1, the condition of stability (resp. semistability) becomes equivalent to $C/\bar{k}$ is complete connected with only ordinary double points as singularities and $\mathrm{Aut}(C)$ is finite (resp. is reductive), see [Rom13, Lemmas 4.2.1 and 4.2.2]. For semistable curves, sometime only the condition on nodal singularities is required, as in [BLR12, Definition 9.2.6]. We call these weak semistable curves.

If $C/\bar{k}$ is a stable curve, then $H^1(C, \omega^n_{C/\bar{k}}) = 0$ if $n \geq 2$ and $\omega^n_{C/\bar{k}}$ is very ample if $n \geq 3$ [DM69, Theorem 1.2]. So if $\mathcal{C}/S$ is a proper flat stable curve, $\omega^n_{\mathcal{C}/S}$ is relatively very ample for $n \geq 3$ (since this is a fibral condition) and its pushforward is locally free by Lemma A.1.1. In particular it is projective.

Note that if $\mathcal{C}/S$ is a proper flat relative curve, since S is of dimension 1 we may also see $\mathcal{C}$ as an arithmetic surface. By Lipman's resolution of singularities of an arithmetic surface (ie an excellent reduced noetherian scheme of dimension 2) [Liu02, §8.3.4], a curve X/S has a birational proper regular model. We can then develop a theory of intersection.

For simplicity, assume for now that R is local and $k = \bar{k}$. and if E_i are the irreducible components of X_k, then $E_i \cdot E_j$ is the number of intersections of points in $E_i \cap E_j$, and $E_i \cdot E_i$ is the opposite of the number of points where E_i meets another component [Rom13, Example 2.3.3]. Hence X/S is semistable (resp. stable) if and only if it does not contains a projective line with self intersection -2 (resp. -1) or less. By the adjonction formula, if E is a vertical effective divisor with $0 < E \leq X_k$, $-2\chi(E) = E \cdot (E + K_{X/S})$ where $K_{X/S}$ is a canonical divisor representing the canonical sheaf $\omega_{X/S}$ (see Section 2.4.1) [Rom13, Theorem 2.3.4].

One important tool in order to construct "minimal models" is contractions and blow downs. Indeed, when we have a regular model X/S of C/k, a blow up $\widetilde{X}/S$ is still a regular model of C/k.

Example 3.2.2 ([Rom13, Example 2.4.2])**.** Let x be a nodal singularity in the special fibre of a normal arithmetical surface. The completed local ring is $R[[a,b]]/(ab - \pi^n)$. Blowing up at x, we get that if $n = 1$ the exceptional divisor is a projective line with self intersection -1, if $n = 2$ it is a smooth conic over k with self intersection -2, and if $n > 2$ its gives two projective lines intersecting in a nodal singularity of thickness $n - 2$, each meeting the rest of the special fibre at one point.

Contractions exist by [Rom13, Theorem 2.4.5]. For blow downs, we want to contract a component E into a point $e \in X_0$ such that the resulting contraction is still regular, and E is the exceptional divisor of the blowup at e in X_0. If E is a vertical prime divisor, a blow down exists if and only if $E \simeq \mathbb{P}^1$ and $E^2 = -1$ [Rom13, Theorem 2.4.6].

More generally, if k is non necessarily algebraically closed, a vertical divisor $E \subset X_s$ is an exceptional divisor if and only if $E \simeq \mathbb{P}^1$ and $E^2 = -[H^0(E, O_E) : k(s)]$ [Liu02, Theorem 9.3.8], [Con+11, L12, Theorem 6]. This is Castelnuovo's criterion, and E is said to be an exceptional divisor.

Going back to the general case, using blow downs, we get

rveminimal

Theorem 3.2.3 (Lichtenbaum-Shafarevich)**.** *Let C/K be a smooth geometrically connected curve of genus $g \geq 1$. Then there is a unique (up to unique isomorphism) minimal proper regular model X/S (resp. minimal regular model with normal crossings, which means that the reduced special fibre is a normal crossing divisor) of C over S. This minimal model is projective, and* $\mathrm{Aut}_S(X) \simeq \mathrm{Aut}_K(C)$.

Proof. This is [Rom13, Theorems 2.5.1 and 2.5.2] or [DM69, §2] or [Liu02, Theorem 9.3.21] or [Con+11, L12, Theorem 14]. If we start with a regular model X and blow down exceptional divisors, we get a relative regular minimal model, and one can show that this model is actually minimal. By the same proof, every regular arithmetic surface X whose generic fiber of arithmetic genus $p_a(X_K) \geq 1$ has a unique minimal model.

The assertions on automorphism is from the minimality [Con+11, L12, Proposition 12]. □

One can also construct canonical models using the canonical dualizing sheaf $\omega_{X/S}$ represented by its divisor $K_{X/S}$:

Theorem 3.2.4 (Canonical model)**.** *Let X/S be a regular arithmetic surface, such that the arithmetic genus of the generic fiber is greater or equalt to 2: $p_a(X_K) \geq 2$. Let $\mathcal{E}$ be the list of all a vertical divisors such that $K_{X/S}.D = 0$. Then*

- *$\mathcal{E}$ is finite, and there is a birational morphism $X \to Y$ that contracts all the divisors in $\mathcal{E}$.*
- *the dualizing sheaf $\omega_{Y/S}$ is relatively ample;*
- *There is a m such that $\omega_{X/S}^m$ is base point free, and then if ϕ is the morphism $X \to \mathbb{P}_S^N$ associated to a generating system, $\phi(X) = Y$.*

Proof. This is [Liu02, Proposition 4.20]. See also [Con+11, L12, §3]. If D is a vertical divisor over s, and $k' = \Gamma(D)$, the condition $K_{X/S}.D = 0$ is equivalent to D/k' is a conic and $\deg_{k'} O_X(D) \mid D = -2$, or that $H^1(D, O_D) = 0$ and $D^2 = -2[k' : k(s)]$ by [Liu02, Proposition 9.4.8]. The intersection matrix $(D_i \cdot D_j)$ of all $D_i \in \mathcal{E}$ is then definite negative, and the contraction exists by Artin's theorem [Liu02, Theorem 9.4.2 and Corollary 9.4.7]. □

3.2.2 Stable reduction of curves

A curve C/K has good reduction if there exists a smooth proper model X/S; since C/K is smooth it always have good reduction almost everywhere.

A curve C/K has stable (resp. semistable) reduction if there exists a regular model X/S, proper and flat over S, such that its special fiber is a stable (resp. semistable) curve. Semistability is stable by dominant base change of Dedekind scheme [Liu02, Proposition 10.3.15], and descends from étale morphisms or completions [Liu02, Corollary 10.3.36].

Proposition 3.2.5. *Let C/K be a smooth geometrically connected curve of genus $g \geq 1$, and let X be its minimal regular model.*

Then C has good reduction over S if and only if X/S is smooth, and in this case X/S is the only smooth model of X. And C has semistable reduction $\Leftrightarrow$ its minimal regular model X/S is semistable $\Leftrightarrow$ X_k is reduced and has only ordinary double points (ie is weakly semistable).

If $g \geq 2$, and let Y/S is the canonical model, then we also have that C has semistable reduction $\Leftrightarrow$ C has stable reduction $\Leftrightarrow$ Y/S is stable (and in this case it is the unique stable model).

Proof. The assertion on good reduction is [Liu02, Proposition 10.1.21], for semistability and stability this is [Liu02, Theorem 10.3.34]. See also [Con+11, Propositions 25 and 26, Theorem 30] and [Rom13, Proposition 3.1.1].

If X/R is a semistable model, by blow downs we may assume that it has no exceptional divisor. The singular points of X_k has for completed ring $\hat{O}_{X,x} = R[[a,b]]/(ab - \pi^n)$. Blowing-up this singularity $[n/2]$ times yields a regular scheme X' whose special fibre has $n-1$ new projective lines of self intersection -2. This is the minimal regular model by the proof of Theorem 3.2.3, so it is semistable.

Conversely if the minimal model is semistable, contracting all the projective lines of self intersection -2 in the special fiber gives a normal surface with nodal singularities [Liu02, Theorem 9.4.15] (using that $g \geq 2$), hence a stable model. See also [DM69, Proposition 2.3]. □

If X/S is a semistable curve whose generic fiber is smooth and geometrically irreducible, we may construct the Néron model $\mathcal{J}$ of the Jacobian $J(X_K)$ or the generalised Jacobian of X/S, which is then semiabelian by Theorem 2.4.10. As expected, the two are related:

enjacobian

Proposition 3.2.6. *Let X/S be a proper flat and normal semistable curve whose generic fiber X_K is geometrically irreducible. Let $\mathcal{J}$ be the Néron model of* $\mathrm{Jac}(X_K)$. *Then $\mathcal{J}^0 \simeq \mathcal{P}ic^0_{X/S}$.*

Proof. Since $\mathcal{P}ic^0_{X/S}$ is semiabelian by Theorem 2.4.10, it is the connected component of the Néron model of its generic fiber $\mathcal{P}ic^0_{X_K}$ by Proposition 3.1.14. See also [BLR12, Corollary 9.7.2] for another proof. □

Remark 3.2.7. There are other cases where the Néron model $\mathcal{J}$ of the Jacobian $J(X_K)$ of the generic fiber coincide with the generalised Jacobian $\mathcal{P}ic^0_{X/S}$ of X/S:

- If X/S is regular, flat, projective and has geometrically integral fibres, then $\mathcal{J} \simeq \mathcal{P}ic^0_{X/S}$ [BLR12, Theorem 9.5.1], so the special fiber of $\mathcal{J}$ is connected.
- If X/S is a regular, proper flat curve, whose generic fibre is geometrically irreducible, and k is perfect (or the spécial fibre is geometrically reduced), and the gcd of the geometric multiplicities of the irreducible components of the special fiber is 1 (so that we can apply Theorem 2.4.10), then $\mathcal{J}^0 \simeq \mathcal{P}ic^0_{X/S}$. See also [BLR12, Theorem 9.7.1] for a generalisation of both this result and Proposition 3.2.6.

ecurvejac

Corollary 3.2.8. *Let C/K be a smooth geometrically connected curve of genus $g \geq 2$, and X/S be its minimal regular model. Then C has stable reduction over R if and only if $J(C/K)$ has semistable reduction over R if and only if $\mathcal{P}ic^0(X_k)$ is a semi-abelian variety (ie has no unipotent subgroup).*

Proof. One direction is clear by Proposition 3.2.6. For the converse, see [DM69, Theorem 2.4]. By descent, they reduce to the case where $C(K)$ has a rational point. See also [Rom13, Theorem 3.4.1] for a summary of the proof in this case. And in this case, the rational point extends to a point over X by the valuative criterion of properness, hence a rational point of X_k, so C/K has stable reduction if and only if $\mathrm{Pic}^0(X_k)$ is semiabelian. □

Remark 3.2.9 (Good reduction of C and its Jacobian)**.** If C/K has good reduction over R, then its minimal regular model X is smooth, so $\mathrm{Pic}^0_{X/S}$ is an abelian scheme, and so is the Néron model of $J = J(C)$: $\mathcal{J} = \mathrm{Pic}^0_{X/S}$. In particular $J(C)$ has good reduction.

Conversely, if $J(C)$ has good reduction, then C has stable reduction by Corollary 3.2.8, and $J(C)_k = J(X_k)$ by functoriality of $\mathcal{P}ic$. Since $J(C)_k$ is abelian, X_k is a curve of compact type. But X_k may not be smooth, hence C may not have good reduction. It will have good reduction if and only if $J(C)_k$ is absolutely simple [Rou17].

tablecurve

Theorem 3.2.10 (Potential stable reduction of curves)**.** *Let C/K be a proper smooth geometrically connected curve. Then it has potential semistable reduction (hence potential stable reduction if $g \geq 2$), ie there is a separate field extension K'/K and a (semi)stable model (which can be chosen regular) X'/R of $X_K \otimes_K K'$. This stable model is unique.*

Proof. Using Corollary 3.2.8, this is deduced from the potential semistable reduction of abelian varieties Theorem 3.1.16 if $g \geq 2$. See [BLR12, Theorem 9.2.7] and [Rom13, Theorem 3.4.2].

If $g = 1$, then C is an elliptic curve (if it has a rational point), so we can directly use the theory of Néron models, see Section 3.2.3.

There are also direct proofs (which can then be used to give a proof of the potential semistable reduction theorem for abelian varieties), see the references in [Stacks, Tag 0C2Q] and [Liu02, Theorem 10.4.3]. □

gconnected

Remark 3.2.11. Theorem 3.2.10 is exactly the valuative criterion of properness for $\overline{\mathcal{M}}_g$, the moduli stack of stable curves of genus $g \geq 2$ by [Stacks, Tags 0CLY and 0CLK]. Hence this stack is proper ([Rom13, § 4.1]). By Zariski main theorem, since $\overline{\mathcal{M}}_g \otimes_{\mathbb{Z}} \mathbb{C}$ is connected, every fibers of $\overline{\mathcal{M}}_g/\mathbb{Z}$ are geometrically connected [Stacks, Tag 0AY8], hence geometrically irreducible since $\overline{\mathcal{M}}_g/\mathbb{Z}$ is smooth. This is the proof in [DM69, §5] (see [DM69, Theorem 5.2] where they show it is a proper smooth Deligne-Mumford stack), see also [DM69, §3] for an algebraic proof.

See also [MFK94, Appendix 5.D p.228] for an analog proof using the fact that the coarce moduli $\overline{\mathrm{M}}_g$ of $\overline{\mathcal{M}}_g$ is a projective variety with geometrically unibranch fibers. (Note that the geometric irreductibility of the $\overline{\mathcal{M}}_g \otimes_{\mathbb{Z}} \mathbb{F}_p$ implies the one of their coarse moduli space since they have the same topological space.)

Note that curves of genus 1 have too many automorphisms so the moduli stack is constructed by fixing some points.

3.2.3 Elliptic curves

subsec:elliptic

An elliptic curve is both a smooth proper curve and an abelian variety. Hence we can relate its Néron model with its proper minimal regular model.

Theorem 3.2.12. *Let E/K an elliptic curve, then the Néron model $\mathcal{N}$ of E is the smooth locus of its minimal regular proper model $\mathcal{E}$, and the smooth locus of a minimal Weierstrass model $\mathcal{W}$ is isomorphic to $\mathcal{E}^0$.*

Proof. This is [Liu02, Theorem 10.2.14] (see also [BLR12, Proposition 1.5.1]). Moreover $H^0(\mathcal{E}, \omega_{\mathcal{E}/S}) = H^0(\mathcal{N}, \omega_{\mathcal{N}/S}) = H^0(\mathcal{W}, \omega_{\mathcal{W}/S}) \subset H^0(E, \omega_{E/S}))$. Note that there are effective algorithms (Tate algorithm) to construct the minimal Weierstrass model $\mathcal{W}$ (assuming S affine), and $\mathcal{E}$ is then the minimal desingularisation of $\mathcal{W}$. □

As an application, we recover the reduction map: $r : E(K) = \mathcal{N}(R) \to \mathcal{N}_k(k) \subset \mathcal{N}_k^0(k) = \mathcal{W}^{sm}(k)$. Using this reduction map, we define a filtration of abelian groups $E(K)^1 \subset E(K)^0 \subset E(K)$ such that $E(K)^1 = ker(r) \subset E(K)^0 := r^{-1}(\mathcal{N}_k^0(k)) \subset E(K)$. The reduction map r then induces isomorphisms $E(K)^0/E(K)^1 \simeq \mathcal{N}_k^0(k)$, $E(K)/E(K)^0 \simeq \Phi_E(k) = \mathcal{N}_k/\mathcal{N}_k^0$ by [Liu02, Proposition 10.2.26].

3.3 p-DIVISIBLE GROUPS

sec:pdivisible

Planned topics

3.3.1 Finite flat group schemes

ubsec:finiteflat

Grothendieck's Galois theory gives an equivalence of category between finite etale covers over S and $\pi_1(S,s)$-finite sets given by the fiber (s a geometric point of the connected locally noetherian S): [Gro71]. This induces an equivalence between finite etale groups and $\pi := \pi_1(S,s)$-finite groups.

Finite flat group schemes (Deligne theorem: a commutative finite flat group schemes is killed by its order).

The (functorial) connected-étale exact sequence $0 \to G^0 \to G \to G^t$ [Tat97, p. 3.7] over an Henselian local ring R. (This extends Lemma B.1.2 by using Proposition A.4.1.)

- If $G = \operatorname{Spec} A$ is affine then G^t is the spectrum of the largest étale quotient of A, so in general a morphism from G to an étale H factors through G^t.
- The order of G^0 is a power of p (in characteristic zero: $G = G^t$).
- If $R = k$, then G is killed by its order, and if k is perfect the connected-étale exact sequence splits (via $G_{\text{red}} \simeq G^t$).
- $G^t(\bar{k}) \simeq G(\bar{k})$

See also the very nice application to elliptic curves in [BCn10].

Generalisation to an arbitrary base: the connected-étale sequence of a finite flat group scheme G/S exists if and only if the separable rank is locally constant [Mes72, Lemma 4.8][3].

Warning: for a general base, the connected component of the identity does not commute with (non local) base change (eg passage to the generic fiber). See the discussion at [TJC16].

Prolongations [Tat97, §4], Classification?

Dieudonne module: if G/k is a finite commutative algebraic k-group, $M(G) = \operatorname{Hom}(G, CW)$ where CW is the fppf sheaf of Witt covectors. This defines an anti-equivalence from the category of finite commutative algebraicp-groups over k to that of Dieudonné modules of finite length over $W(k)$ (ie with an action of F and V).

Dieudonné-Manin classification theorem.

[3] Let me quote Messing about this proof: "Apologies are offered in advance to the reader for the proof in the following lemma".

3.3.2 Barsotti-Tate groups

c:BTgroups

p-divisible/Barsotti-Tate groups, fppf groups sheaves [Con+11, pp. Lo9, L10], [Rio03].

Connected-étale exact sequence by going to the limit. Also the equivalence of category on finite étale group above (ie by Grothendieck's Galois theory) gives an equivalence of category between étale p-divisible groups and free $\mathbb{Z}_p$-modules with a continuous action of π.

Example: For A/R an abelian scheme (R henselian local), the module associated to $A(\ell)$ ($\ell \neq p$) is $T_\ell(A)$ with the action of $\pi_1(R)$. Rem: $A(\ell)$ also encode the ℓ-covers of A. By Galois theory we have $H^1(A, Z(\bar{\ell})) = \mathrm{Hom}(\pi_1^t A, Z(\bar{\ell}))$. So this proves that $H^1(A, Z(\bar{\ell})) = T_\ell(A)^\vee$ as in Theorem 2.2.12.

Extension of $M(G)$ to formal group and to p-divisible groups. The contravariant Dieudonné functor induces an anti-equivalence between p-divisible groups and Dieudonné modules free of finite rank over $W(k)$. (The Dieudonné module can be seen as the "limit" $\mathbb{D}(G/W(k))_{W(k)}$ of the crystal $\mathbb{D}(G/W(k))$ associated to it, [CO09, Remark 4.34].) For an étale p-divisible group the associated Dieudonné module/crystal is the free $\mathbb{Z}_p$ module with its Galois action from the Galois theory above. (When G is étale, F is bijective and so induces V; eg V is zero if we are in characteristic p.)

Hodge-Tate decomposition of p-divisible groups [Ser66, Théorèmes 2 et 3]: $T_pG \otimes \mathbb{C}_p \simeq t_G \otimes \mathbb{C}_p(1) \oplus \mathrm{Hom}(t_{G^\vee}, \mathbb{C}_p)$. Proof: Logarithm: $L : G(R) \otimes \mathbb{Q}_p \simeq t_G \otimes_R K$ where t_G is the tangent space to G°. We have isomorphisms $\alpha : G(R) \to \mathrm{Hom}_\pi(T_pG^\vee, U_{\mathbb{C}_p})$ and $d\alpha : t_G \otimes_R K \to \mathrm{Hom}_\pi(T_pG^\vee, U_{\mathbb{C}_p})$. Where $U_{\mathbb{C}_p}$: inversibles elements of $O_{\mathbb{C}_p}$ congruent to 1.

Equivalence between connected p-divisible groups and formal lie algebra [Ser66, §1.4]. (By seeing them both as fppf group sheaves). The Cartier module of the formal group is isomorphic to the Dieudonne module of the connected p-divisible group [CO09, Theorem 4.33].

Formal smoothness of p-divisible groups [Ill15, Theorem 4.2.1], [Ill85, §4.4], [CO09, Theorem 2.4].

Crystals [Mes72] (= extension of the Dieudonné functor to schemes). Fully faithfull embedding [De 98, §2]. Surjectivity (hence bijectivity) of the reduction of morphisms to the generic fiber (Tate [Tat67], [Ser66, Théorème 1] for number fields and De Jong) [De 98, §3], [Jon98, Theorem 1.1] for function fields). Deforming divisible groups = lifting the Hodge filtration (in an admissible way) [Mes72, Theorem V.1.6]. See also the nice summary in [CN90, § 2].

Newton polygons (and lift under specialization): [Ill15, §5], [Oor01b], [CO09, Theorem 1.22].

3.3.3 Applications to abelian varieties

The crystal of $A(\ell)$ is exactly $T_\ell(A)$ (both for $\ell \neq p$ and $\ell = p$). If $\ell = p$, this is also the first crystalline cohomology group. If A_0/R_0 lift to A/R (R $\mathfrak{p}$-adically complete separated), then the crystalline cohomology (for the crystalline site induced by R) of A_0 is $H^1_{DR}(A/R)$. The Hodge filtration induces a Hoge filtration on the crystalline cohomology (ie the crystal), which is exactly the filtration corresponding to the deformation of $\mathbb{D}(A_0(p))$ from Section 3.3.2.

The connected-étale exact sequence for an abelian variety. The connected part of its p-divisible group corresponds to the formal group law of A. Compatibility with Cartier duality.

Application to Tate's isogeny theorem (via equivalence between isogenies of abelian varieties and of their p-divisible groups, and then using crystals which are their Tate modules), both for finite fields (Tate) [WM71, Theorem 6], number fields (Faltings [Fal86]), and function fields (Zarhin [Zar75] and Morin [Mor78] for T_ℓ , De Jong for T_p [De 98, Theorem 4], [Jon98, Theorem 2.6]). (Warning: this is not true over $\mathbb{Q}_p$)

Application: if we have a morphism F between Tate modules of abelian schemes A, B over S (reduced and connected), such that F_s is realised by an isogeny $f : A_s \to B_s$, then mF is realised by an isogeny $f : A \to B$ for a suitable power $m = p^e$ of p (so $m = 1$ if $p = 0$), see [Gro66a; Per13].

Recall we have seen: A/R has good/semi-stable reduction iff $A(\ell)$ has (even if $\ell = p$), [De 98].

Serre-Tate local coordinates [Kat81; CN90, § 3].

3.4 LIFTS OF ABELIAN VARIETIES

sec:lifts

3.4.1 General theory

Lifting schemes to artinian rings and obstructions (in H^2) via the cotangent complex [Stacks, Tag 08V3], [Ill72], [FGI05, §8.5.7]. For a smooth scheme this is just the tangent space.

Formal schemes [FGI05, §8.1], [Stacks, Tag 0AHW]. Grothendieck criterion of formal representability [Oor71a], Schlessinger criterion [Stacks, Tags 06G7 and 06JK], versality [Stacks, Tag 06SX].

Grothendieck's existence/algebraicity theorem [FGI05, §8.4], [Stacks, Tags 087V, 0886, 0CYW].

3.4.2 Lifting abelian varieties

For an abelian variety, lifting as a scheme lift the group structure by rigidity, and the obstruction vanishes using the group law [FGI05, Theorem 8.5.23].

Pro-representability of the functor of lifts of an abelian variety: non polarised case (Grothendieck) [Oor71a, Theorem 2.2.1] and polarised case (Mumford) [Oor71a, Theorem 2.3.3].

Application to algebraicity of polarised abelian varieties: algebraicity when the when the polarisation is separable (hence lift), in particular for principally polarised abelian varieties [Oor71a, Theorem 2.4.1 and Corollary 2.4.2].

An abelian variety always lift in characteristic zero [Oor79; NO80] (possibly over a ramified extension if the polarisation is non separable).

See also the surveys [Oor95; Oor15] about lifting abelian varieties. For the particular case of lifting CM abelian varieties, see the book [CCO13] (and its survey [Oor09]).

3.4.3 Serre-Tate theorem and canonical lifts

Serre-Tate theorem [LST64], [Ser66, Théorème 4] (Drinfeld's proof as exposed in [Kat81] and the nice surveys [Dos; You15]). Good references are [Mes72, § V.3.4 and Appendix; Kat81]; see also [MS87, Appendix] for an extension to smooth projective varieties.

See also the alternative proof by Grothendieck [Ill85] using the refined version of BT lifting [Ill15, Theorem 4.2.1]

So we reduce to lifting BT groups, which reduces (in nice cases) to lifting the Hodge filtration of their crystals $D(G)$ (if $p > 2$) [Mes72, Theorem V.1.6].

Canonical lifts of ordinary abelian varieties over a perfect field k (the connected-étale sequence split and we take the unique lift that still split[4]), canonical coordinates on the moduli space [Mes72, Appendix; Kat81]. See also [Rob21, Section 6.2.1].

Canonical lifting is a fully faithful functor compatible with the Galois action. They are characterized by $\mathrm{End}(\widetilde{A}) = \mathrm{End}(A)$ or by lifting of the Frobenius. [Mes72, Appendix, Corollaries 1.2 and 1.3].

[4] If R is henselian local and k perfect, if G° is of multiplicative type, there is a unique lift of a p-divisible G/k to G/R such that the connected-étale exact sequence stays split. Indeed, G^t lifts uniquely to an étale p-divisible group, so G° too by duality, and we have a bijection between lifts G/R and $\mathrm{Ext}^1(G^\circ/R, G^t/R)$. So we have a group structure on lifts, and the zero element corresponds to the split connected-étale exact-sequence; this is the canonical lift

4 PAIRINGS IN ABELIAN VARIETIES

ch:pairings

CONTENTS

4.1 THE WEIL PAIRING

sec:weil

4.1.1 *The many facets of the Weil pairing*

pairingdef

There is many instance of the Weil pairing. We describe some of these. Note that if e_W is a bilinear application with value the multiplicative group, e_W^n is still bilinear but certainly cannot be non-degenerate (hence a pairing) in characteristic $p \mid n$. So since the Weil pairing is universal over $\mathbb{Z}$, there is essentially only a sign ambiguity in defining the Weil pairing[1].

Let us first give the philosophy behind the Weil pairing. If A/k is an abelian variety, the dual abelian variety $\widehat{A}$ is the scheme representing the connected component of the Picard sheaf. (This coincides with the definition of $\mathrm{Pic}^0(A)$ as the line bundles algebraically equivalent to zero, and this extends to abelian scheme using the relative Picard sheaf. We refer to Section 2.3.2 for more details.) Since A has a rational point 0_A, this allow us to describe $\widehat{A}(T)$ as the set of line bundles fiberwise algebraically equivalent to zero and rigidified along the pullback of the zero section. In particular, $\widehat{A}(k)$ are the rational line bundles over A algebraically equivalent to zero. There is a canonical/universal Poincare sheaf $\mathcal{P}$ on $A \times \widehat{A}$. For instance this is the line bundle induced by the universal property of $\widehat{A}$ on the identity morphism $\mathrm{id} : \widehat{A} \to \widehat{A}$. Using the Poincare bundle, one can show that A is canonically isomorphic to its bidual [Mum70a].

This means that $\widehat{A} \simeq \mathrm{Hom}_k(A, B\mathbb{G}_m)$ where $B\mathbb{G}_m$ is the classifying stack of $\mathbb{G}_m$ over k (hence represents line bundles). So $\widehat{A}$ is the dual of A in a somewhat abstract manner, and the Weil pairing can be seen as a way to make this duality "concrete", at last on finite subgroups of A, eg by showing that $\widehat{A}[m]$ is the Cartier dual of $A[m]$ (canonically). Alternatively, we will see that[2] we may also interpret $\widehat{A}$ as the Ext-sheaf $\mathrm{Ext}^1_k(A, \mathbb{G}_m) \simeq \tau_{\leq 1} R\,\mathrm{Hom}_k(A, \mathbb{G}_m)[1]$ (where $R\,\mathrm{Hom}$ is in the derived category and the isomorphism comes from the fact that $\mathrm{Hom}_k(A, \mathbb{G}_m) = 0$ since A/k is projective and $\mathbb{G}_m$ is affine). Once again this somewhat abstract duality is made concrete by the Weil pairing.

Let us close this philosophical parenthese, and go back to the concrete definition of the Weil pairing. References for these definitions are [Mum70a; Mil91, §16; Sil10] The Weil pairing is geometric (it does not depends on the field extension), and commutes with the Galois action. So we might as well assume that A is defined over $\overline{k}$.

[1] This raises the interesting question of whether the Weil pairing is the only pairing on abelian schemes satisfying suitable functorial like properties and defined over $\mathbb{Z}$

[2] I am told that this also follow formally from the Dold-Kan correspondance. There is also probably a way to define a derived dual abelian scheme as $\mathbb{R}\widehat{A} = R\,\mathrm{Hom}(A, B\mathbb{G}_m)$, so that $\mathbb{R}\widehat{A}$ corresponds to $R\,\mathrm{Hom}(A, \mathbb{G}_m)$, but my knowledge of this subject is far too limited to hasard such a statement.

- If $f : A \to B$ is an isogeny, $K = \operatorname{Ker} f$, then if $\widehat{K}$ is the kernel of the dual isogeny $\hat{f} : \widehat{A} \to \hat{B}$, $\widehat{K}$ is canonically identified with the Cartier dual of K: $\widehat{K} \simeq \operatorname{Hom}(K, \mathbb{G}_m)$. Hence there is a canonical non degenerate pairing (often called the Weil-Cartier pairing): $e_f : K \times \widehat{K} \to \mathbb{G}_m$.

  We can compute e_f as follow. Let $Q \in \hat{K}(\bar{k})$, Q then correspond to a line bundle $\mathcal{L}_Q$ algebraically equivalent to 0 on $B_{\bar{k}}$. Concretely, if $\mathcal{P}$ is the Poincare bundle on $B \times \hat{B}$, $\mathcal{L}_Q = \mathcal{P}_Q$ where $\mathcal{P}_Q$ is the pullback of $\mathcal{P}$ by $B \to B \times \hat{B}, P \mapsto (P, Q)$. Then $\hat{f}(Q) = f^*\mathcal{L}_Q = 0 \in \widehat{A} = \operatorname{Pic}^0(A_{\bar{k}})$, so f^*Q is isomorphic to the trivial bundle $O_{A_{\bar{k}}}$ on $A_{\bar{k}}$. In other words, $O_{A_{\bar{k}}}$ descend via f to the line bundle $\mathcal{L}_Q$, by descent theory this correspond to a section $K \to G(O_{A_{\bar{k}}})$ associated to such an isomorphism $\psi_Q : f^*Q \to O_{A_{\bar{k}}}$. Then $e_f(P, Q)$ is the scalar that makes the following diagram commute:

$$\begin{array}{ccc} f^*\mathcal{L}_Q & \xrightarrow{\psi_Q} & O_A \\ \| & & \| e_f(P,Q) \\ \tau_P^* f^* \mathcal{L}_Q & \xrightarrow{\tau_P^*\psi_Q} & \tau_P^* O_A. \end{array} \tag{4.1}$$

  {eq@pairi

  We can reformulate this diagram as follow: since $O_{A_{\bar{k}}} \in \operatorname{Pic}_0(A_{\bar{k}})$, $G(O_{A_{\bar{k}}}) = A_{\bar{k}} \times \bar{k}$ is commutative (because $e_{O_{A_{\bar{k}}}}$ is trivial on $A_{\bar{k}}$). The action of $G(O_{A_{\bar{k}}})$ on the trivial line bundle $A_{\bar{k}} \times \mathbb{A}^1_{\bar{k}}$ is given by $(x, \lambda).(y, \gamma) = (x + y, \lambda\gamma)$. So the section $K \to G(O_{A_{\bar{k}}})$ corresponds to a character χ such that K acts on the trivial line bundle via $x.(y, \gamma) = (y + x, \chi(x)\gamma)$ and $\mathcal{L}_Q$ is the quotient of $A_{\bar{k}} \times \mathbb{A}^1_{\bar{k}}$ by this action. Then [Mum70a, p. 183; MGE12, (11.12)]:

$$e_f(P, Q) = \chi(P).$$

  More geometrically, if D_Q is a divisor representing $\mathcal{L}_Q$, f^*D_Q is principal, so is the divisor of a rational function $g_{f,Q}$. Then $g_{f,Q}/t_P^* g_{f,Q} = \chi(P)$ so that [Mum70a, p. 184; MGE12, (11.13)]

$$e_f(P, Q) = g_{f,Q}(X)/g_{f,Q}(X + P) \tag{4.2}$$

  {eq:pairi

  where X is any point of $A_{\bar{k}}$ such that $g(X + P)$ is well defined.

  The functoriality of the dual isogeny induce the following functoriality on the Weil-Cartier pairing: if $\alpha : U \to A$ and $\beta : B \to V$ are isogenies, then for $P \in \alpha^{-1}(K(\bar{k}))$ and $Q \in \hat{\beta}^{-1}\hat{K}(\bar{k})$ we have

$$e_{\alpha \circ f \circ \beta}(P, Q) = e_f(\alpha P, \hat{\beta} Q). \tag{4.3}$$

  {eq:pairi

- A particular case is the isogeny $[n]$ of multiplication by n, this gives a non degenerate pairing $e_n : A[n] \times \widehat{A}[n] \to \mu_n$, usually called the Weil pairing.

  We have the following compatibility: if $P \in A[nm_1](\bar{k})$, $Q \in \widehat{A}[nm_2]$, $e_{nm_1m_2}(P, Q) = e_n(m_1P, m_2Q)$. So the Weil pairings glue to form a pairing $\hat{e}_\ell : T_\ell A \times T_\ell \widehat{A} \to Z(\bar{\ell})(1)$ where $Z(\bar{\ell})(1) = \varprojlim \mu_{\ell^n}$ is the Tate twist.

- If $\mathcal{L}$ is an ample line bundle (or even simply a non degenerate line bundle), then the associated polarisation $\Phi_{\mathcal{L}} : A \to \widehat{A}$ is an isogeny. $\Phi_{\mathcal{L}}$ is autodual (using that A is canonically isomorphic to its bidual), hence the pairing associated to this isogeny is: $e_{\mathcal{L}} : K(\mathcal{L}) \times K(\mathcal{L}) \to \mathbb{G}_m$.

  As a particular case of a Weil-Cartier pairing, we have that the following diagram is commutative up to the action of $e_{\phi(\mathcal{L})}(P, Q)$:

$$\begin{array}{ccc} \mathcal{L} & \xrightarrow{\psi_P} & \tau_P^*\mathcal{L} \\ \downarrow \psi_Q & & \downarrow \tau_P^*\psi_Q \\ \tau_Q^*\mathcal{L} & \xrightarrow{\tau_Q^*\psi_P} & \tau_{P+Q}^*\mathcal{L}. \end{array}$$

We have the following functorial compatibilities (see [Mum70a, p. 228]):

risation1

1. If $f : A \to B$ is an isogeny and $\mathcal{M}$ is ample on B,
$$e_{f^*\mathcal{M}}(x,y) = e_{\mathcal{M}}(f(x),f(y))$$
for all $x,y \in f^{-1}(K(\mathcal{M}))$.

arisation

2. If $\mathcal{L}_1$ and $\mathcal{L}_2$ are ample on A, $e_{\mathcal{L}_1\otimes\mathcal{L}_2}(x,y) = e_{\mathcal{L}_1}(x,y)e_{\mathcal{L}_2}(x,y)$ for all $x,y \in K(\mathcal{L}_1)\bigcap K(\mathcal{L}_2)$.
Indeed, $\Phi(\mathcal{L}_1 \otimes \mathcal{L}_2) = \Phi(\mathcal{L}_1) + \Phi(\mathcal{L}_2)$, so $\Phi_{\mathcal{L}_1\otimes\mathcal{L}_2}$ so this result can be seen by looking at the composition $A \to A \times A \to \widehat{A} \times \widehat{A} \to \widehat{A}$ given by $x \mapsto (x,x) \mapsto (\Phi_{\mathcal{L}_1}(x), \Phi_{\mathcal{L}_2}(x)) \mapsto \Phi_{\mathcal{L}_1}(x) + \Phi_{\mathcal{L}_2}(x)$.

risation3

3. $e_{\mathcal{L}^\ell}(x,y) = e_{\mathcal{L}}(x,\ell y)$ for all $x \in K(\mathcal{L})$ and $y \in [\ell]^{-1}(K(\mathcal{L}))$.

- If $\mathcal{L}$ is an ample line bundle, the theta group $G(\mathcal{L})$ is a central extension of $K(\mathcal{L})$ by $\mathbb{G}_m$. The associated commutator pairing (which can also be defined in term of the 2-cocycle associated to the extension, see [Rob21, Section 2.4]) gives a pairing $e_{\mathcal{L}} : K(\mathcal{L}) \times K(\mathcal{L}) \to \mathbb{G}_m$. This is exactly the same pairing as above, as the commutative diagram above shows.

- On the other side of the spectrum, if $\mathcal{L}$ is algebraically equivalent to 0, then $G(\mathcal{L})$ is commutative and an extension of A by $\mathbb{G}_m$. This provide a canonical identification of $\widehat{A}$ with $\mathrm{Ext}^1(A,\mathbb{G}_m)$ [Mum70a].

  Then if $f : A \to B$ is an isogeny, the standard long cohomological sequence gives gives $0 \to \mathrm{Hom}(\mathrm{Ker}f,\mathbb{G}_m) \to \mathrm{Ext}^1(B,\mathbb{G}_m) \to \mathrm{Ext}^1(A,\mathbb{G}_m) \to 0$ using that $\mathrm{Hom}(A,\mathbb{G}_m) = 0$ and $\mathrm{Ext}^1(\mathrm{Ker}f,\mathbb{G}_m) = 0$. We recover this way the dual isogeny $\hat{f}$ and a canonical identification $\mathrm{Ker}\hat{f} = \mathrm{Hom}(\mathrm{Ker}f,\mathbb{G}_m)$, which induces the Weil-Cartier pairing e_f.

  Concretely the identification of $\widehat{A}$ with $\mathrm{Ext}^1(A,\mathbb{G}_m)$ is as follow. First we identify $\widehat{A}$ with Pic^0_A. Then if $[D] \in \mathrm{Pic}^0_A$, then all $P \in A(\bar{k})$, $\tau_P^*D - D$ is principal, of the form $g_{D,P}$, hence we get an element of $\mathrm{Ext}^1(A,\mathbb{G}_m)$ by $(P,Q) \mapsto g_{D,P}(x+Q)/g_P(x)$ for any x where this is well defined. Plugging this identification into e_f, we recover Equation (4.2).

- If $\mathcal{L}$ is an ample line bundle, then $\mathcal{L}^n$ is ample and $K(\mathcal{L}^n) = [n]^{-1}K(\mathcal{L})$. The pairing corresponding to the isogeny $\Phi_{\mathcal{L}^n}$ $e_{\mathcal{L}^n} : K(\mathcal{L}^n) \times K(\mathcal{L}^n) \to \mathbb{G}_m$ is also the Weil-Cartier pairing associated to the isogeny $\Phi_{\mathcal{L}} \circ [n]$.

  Its relationship with the Weil pairing e_n is as follow:
$$e_{\mathcal{L}^n}(x,y) = e_n(x,\phi_{\mathcal{L}}(y))$$
for all $x \in A[n]$ and $y \in [n]^{-1}K(\mathcal{L}) = \phi_{\mathcal{L}}^{-1}(\widehat{A}[n])$.
So the $e_{\mathcal{L}^n}$ glue together to form a pairing $\hat{e}_{\mathcal{L},\ell}$ on $T_\ell A$, and we have $\hat{e}_{\mathcal{L},\ell}(x,y) = \hat{e}_\ell(x,\Phi_{\mathcal{L}}(y))$.

- The Poincare line bundle $\mathcal{P}$ is principal on $A\times\widehat{A}$, hence $\mathcal{P}^n$ induce a pairing on $A[n]\times A[n]\times\widehat{A}[n]\times\widehat{A}[n]$, which is given by $e_{\mathcal{P}^n}(x_1,x_2,y_1,y_2) = e_n(x_1,y_2)e_n^{-1}(x_2,y_1)$.

  In particular we may recover the Weil pairing e_n from $e_{\mathcal{P}^n}$.

- If X is a complex curve of genus g, there is a period map $H_1(X,\mathbb{Z}) \times \Omega^1_X \to \mathbb{C}, (\gamma,\omega) \mapsto \int_\gamma \omega$, where $\Omega^1_X = H^0(X,\Omega^1)$. The Jacobian of X is then $J(X) = {\Omega^1_X}^\vee/H_1(X,\mathbb{Z}) \simeq \mathbb{C}^g/\Lambda$. We also have a dual construction: $H_1(X,\mathbb{Z})$ embeds into $H_1(X,\mathbb{R})$, which is dual to $H^1(X,\mathbb{R})$ by Poincare duality. The complex structure on $H^1(X,\mathbb{R})$ is compatible with the Hodge decomposition $H^1(X,\mathbb{C}) = H^1_{dR}(X,\mathbb{C}) = H^{0,1}(X,\mathbb{C}) \oplus H^{1,0}(X,\mathbb{C}) = H^0(X,\Omega^1) \oplus H^1(X,O_X)$. So we may also dually construct $J(X)$ as $J(X) = H^1(X,O_X)/H^1(X,\mathbb{Z})$.

  The intersection product yields an alternate pairing $H_1(X,\mathbb{Z}) \times H_1(X,\mathbb{Z}) \to \mathbb{Z}$, hence $H_1(X,\mathbb{Z}/n\mathbb{Z}) \times H_1(X,\mathbb{Z}/n\mathbb{Z}) \to \mathbb{Z}/n\mathbb{Z}$, hence a pairing $J(X)[n] \times J(X)[n] \to \mathbb{Z}/n\mathbb{Z}$. This is exactly the Weil pairing on the principally polarised $J(X)$.

- If $X/\mathbb{C}$ is a complex abelian variety, we have seen that an ample polarisation corresponds to an hermitian form H (and a symplectic form $E = \Im H$ on the lattice Λ). Then for $x, y \in K(H)$, $e_H(x,y) = e^{-2i\pi E(x,y)}$.

  The pairing corresponding to the polarisation nH is then for $x, y \in K(nH) = [n]^{-1}K(H)$, $e_{nH}(x,y) = e^{-2i\pi nE(x,y)}$. So the Weil pairing induced by all $nH, n \in \mathbb{N}$ encode the symplectic form E on Λ.

  If $X = V/\Lambda$, the dual abelian variety $\widehat{X}$ is $\widehat{X} = \mathrm{Hom}(\Lambda, \mathbb{C}_1^*) = \mathrm{Hom}_{\overline{\mathbb{C}}}(V, \mathbb{C})/\Lambda^\star$ where $\Lambda^\star = \{f \in \mathrm{Hom}_{\overline{\mathbb{C}}}(V, \mathbb{C}), \Im f \subset \mathbb{Z}\}$, [Rob10, p. 29]. The polarisation corresponding to the Poincare bundle on $X \times \widehat{X}$ is then $(v_1, v_2, f_1, f_2) \mapsto f_1(v_2) + \overline{f_2(v_1)}$.

- For an abelian variety A over $\overline{k}$, given a polarisation (induced by a line bundle) $\mathcal{L}$, one may also recover a symplectic form on the Tate module $T_\ell A$ when $\ell \neq p$ imitating the procedure to get the symplectic form E on Λ in the complex case (see Section 2.1.2), as follow: the Kummer exact sequence $1 \to \mu_{\ell^n} \to \mathbb{G}_m \xrightarrow{\ell^n} \mathbb{G}_m \to 1$ yields the following exact sequence in étale cohomology, using that $\mathrm{Pic}(A) = H^1(A, \mathbb{G}_m)$:

$$0 \to \mathrm{Pic}(A_{\overline{k}})/\ell^n \mathrm{Pic}(A_{\overline{k}}) \to H^2(A_{\overline{k}}, \mu_{\ell^n}) \to H^2(A_{\overline{k}}, \mathbb{G}_m)_{\ell^n} \to 0.$$

  Passing to the inverse limit using that $\mathrm{Pic}(A_{\overline{k}})/\ell^n \mathrm{Pic}(A_{\overline{k}}) = \mathrm{NS}(A_{\overline{k}})/\ell^n \mathrm{NS}(A_{\overline{k}})$ yields

$$0 \to \mathrm{NS}(A_{\overline{k}}) \otimes Z(\overline{\ell})(1) \to H^2(A_{\overline{k}}, Z(\overline{\ell})(1)) \to T_\ell H^2(A_{\overline{k}}, \mathbb{G}_m) \to 0.$$

  In other words, a polarisation $\mathcal{L}$ induces a symplectic form $E_{\mathcal{L},\ell}$ on $T_\ell(A)$.

  We have that $E_{\mathcal{L},\ell} = -\hat{e}_\ell$ [Mil91, §16].

  See also [Mil91, Proposition 16.6] for a characterisation of when a morphism $\lambda : A \to \widehat{A}$ is a polarisation, ie comes from an ample line bundle $\mathcal{L}$. This is exactly when e_λ is skew-symmetric (in characteristic different from 2) on $T_\ell(A)$.

weilpolarisation

Example 4.1.1 (Polarisation and pairings)**.** If $f : A \to B$ we have the Weil-Cartier pairing $e_f : \mathrm{Ker} f \times \mathrm{Ker} \hat{f} \to \mathbb{G}_m$. If B has a polarisation $\mathcal{L}$, we have an isogeny $\Phi_{\mathcal{L}} \circ f : A \to B \to \hat{B}$, and the Weil-Cartier pairing gives a pairing on $e_{\mathcal{L},f} : f^{-1}(K(\mathcal{L})) \times \Phi_{\mathcal{L}}^{-1} \mathrm{Ker} \hat{f} \to \mathbb{G}_m$.

If $P \in \mathrm{Ker} f$ and $Q \in \Phi_{\mathcal{L}}^{-1} \mathrm{Ker} \hat{f}$, then by compatibility of the Weil-Cartier pairing with isogenies Equation (4.3), $e_{\mathcal{L},f}(P,Q) = e_f(P, \Phi_{\mathcal{L}}(Q))$. Also if $\mathcal{L} = {\mathcal{L}_0}^n$, $\Phi_{\mathcal{L}} = \Phi_{\mathcal{L}_0}^n$, so if $Q \in \Phi_{\mathcal{L}_0}^{-1} \mathrm{Ker} \hat{f}$, $e_{\mathcal{L},f}(P,Q) = e_{\mathcal{L}_0,f}(P,Q)^n$.

4.1.2 *Weil's reciprocity and alternative definitions of the Weil pairing*

:weilreciprocity

Let $(A, \mathcal{L})$ be a (separably) polarised abelian variety, and ℓ prime to p. By Section 4.1.1, we have a pairing $e_{\mathcal{L}^\ell}$ on $K(\mathcal{L}^\ell)$ which may be defined as follow. Let Θ be a divisor corresponding to $\mathcal{L}$ (the pairing $e_{\mathcal{L}}$ only depends on the isomorphism class of $\mathcal{L}$, hence any divisor will do. In fact it only depends on $\Phi_{\mathcal{L}}$, hence on the algebraic equivalence class). For a 0-cycle $Z = \sum n_i(P_i)$ we associate the divisor $D_Z = \sum n_i t_{P_i}^* \Theta$ (we call this $D_{\Theta,Z}$ when we want to make the dependency on Θ explicit) (see also [Rob21, Section 2.9]). This divisor is of degree zero if Z is of degree zero, and in this case it is principal whenever its realisation $S(Z) = \sum n_i P_i \in K(\mathcal{L})$. In this case we let f_Z (or $f_{\Theta,Z}$) be a function associated to D_Z, this function f_Z is only defined up to a multiple, but evaluating it at a 0-cycle Z' (where this is well defined) does not depend on the representative f_Z.

Now let $P, Q \in K(\mathcal{L}^\ell)$, and let Z_Q be the cycle $(Q) - (0_A)$, $D_Q = t_Q^*\Theta - \Theta$ (this can be seen as a convenient generalisation of the notation D_Z above applied to a cycle Z which is not linearly equivalent to 0: D_Z means $D_{Z'}$ where $Z' = Z - (S(Z)) - (\deg Z - 1)(0_A)$). Following the recipe in Section 4.1.1, and using that $\Phi_{\mathcal{L}^\ell} = \Phi_{\mathcal{L}} \circ [\ell]$, we have that $[\ell]^* D_Q$ is principal. If $g_{\ell,Q}$ is a function representing this principal divisor, $e_{\mathcal{L}^\ell}(P,Q) = g_{\ell,Q}(P + x)/g_{\ell,Q}(x)$, for any point x where this is well defined.

The divisor $[\ell]^* D_Q$ corresponds to the cycle $[\ell]^* Z_Q = \sum_{T \in A[\ell](\overline{k})} (Q_0 + T) - (T)$ where $\ell Q_0 = Q$. We could in principle compute the Weil pairing using this equation, but this would be costly. For elliptic curves or more generally Jacobians of curves, and $\mathcal{L}$ the principal polarisation given by the Theta divisor, there is an alternative definition of the Weil pairing expressed in term of the divisor ℓD_Q. The equivalence with the above definition rest on Weil's reciprocity for curves. For abelian varieties, we can use a version proved by Lang.

First we introduce some notations: if $\mathcal{P}$ is a divisor on $A \times B$, then to a point $Q \in B$ we may associate the pullback of $\mathcal{P}$ via the morphism $A \to A \times B$ given by $\mathrm{Id} \times Q$. We may then extend this construction to 0-cycles on B. We call $\mathcal{P}(Z)$ the divisor associate to a cycle. If Z_B is a cycle on B of degree 0 such that its realisation $S(Z_B) = 0$, then $\mathcal{P}(Z_B)$ is principal. If f_{Z_B} is a function representing it, and Z_A a cycle on A of degree zero, the value $f_{Z_B}(Z_A)$ (if it is well defined, that is different from 0 and ∞) does not depend on the choice of f_{Z_B}, and we write this value as $\mathcal{P}(Z_B)(Z_A)$.

Let us give two examples: if $\mathcal{P}$ is (a suitably normalised divisor representing) the Poincare line bundle on $A \times \widehat{A}$, and $Q \in \widehat{A}$, $\mathcal{P}(Q)$ is simply the line bundle algebraically equivalent to 0 on A represented by Q. Thus if $\mathcal{P}_{\mathcal{L}}$ is the pullback of $\mathcal{P}$ by the morphism $A \times A \to A \times \widehat{A}$ given by $\mathrm{Id} \times \Phi_{\mathcal{L}}$, then if $Q \in A$, $\mathcal{P}_{\mathcal{L}}(Q)$ is the line bundle represented by $\Phi_{\mathcal{L}}(Q)$, ie it is $t_Q^*\mathcal{L} \otimes \mathcal{L}^{-1}$. (By duality of $\Phi_{\mathcal{L}}$, and biduality of A, $\mathcal{P}_{\mathcal{L}}$ is equal to its own transpose, so the pullback is the same whether we pull back by $Q \times \mathrm{Id}$ or $\mathrm{Id} \times Q$.) In particular, if Z is a cycle on A, $\mathcal{P}_{\mathcal{L}}(Z)$ is simply $D_{\Theta,Z}$ from above, up to a change of Θ.

Theorem 4.1.2 (Lang's reciprocity)**.** *If $\mathcal{P}$ is a divisor on $A \times B$, Z_A and Z_B two cycles of degree 0 on A and B respectively such that $S(Z_A) = 0_A$, $S(Z_B) = 0_B$ (by analogy with divisors on elliptic curves we say that the two cycles are linearly equivalent to zero) and no pair of points in the respective support is contained in D. Then $\mathcal{P}(Z_B)(Z_A)$ and ${}^t\mathcal{P}(Z_A)(Z_B)$ (where ${}^t\mathcal{P}$ is just the transposition of the two projections) are well defined, and $\mathcal{P}(Z_B)(Z_A) = \mathcal{P}(Z_A)(Z_B)$.*

In particular, if we apply this to $\mathcal{P}_{\mathcal{L}}$ on $A \times A$, we get that if Z_1 and Z_2 are two cycle linearly equivalent to zero, then $f_{\Theta,Z_2}(Z_1) = f_{Theta,Z_1}(Z_2)$.

Proof. This is [Lan58, Theorem 5]. Thus the last assertion is valid up to a change of Θ, but the equality does not depend on the linear equivalence class (as long as we use the same divisor on the LHS and RHS).

In [LR15, Proposition 4] we gave a slightly less streamlined proof based on Lang's reciprocity for the Poincare bundle applied to $Z_1' = \Phi_{\mathcal{L}}(Z_1)$ and Z_2. □

Lang recover Weil's reciprocity from this theorem in [Lan58, Corollary p.436]. It should be clear that the alternative definition of the Weil and Tate pairing showed for elliptic curves using Weil's reciprocity hold for abelian variety using Lang's reciprocity. In particular:

iringweil

Corollary 4.1.3. *Let $(A, \mathcal{L})$ be a polarised abelian variety, Θ a divisor representing $\mathcal{L}$ and let $P, Q \in A[\ell]$. Let Z_P, Z_Q be two cycles linearly equivalent to $(P) - (0)$ and $(Q) - (0)$, and D_P, D_Q the corresponding divisors D_{Θ,Z_P}, D_{Θ,Z_Q}. Then $e_{\mathcal{L}^\ell}(P, Q) = \frac{f_{\Theta,\ell D_P}(Z_Q)}{f_{\Theta,\ell D_Q}(Z_P)}$.*

Proof. This is proven in [Lan58, Theorem 6], see also [LR15, Theorem 2];

The result does not depend on the (algebraic class) of Θ, but once it is fixed the same one should be used for the numerator and denominator (and similarly for Z_P and Z_Q). □

We remark that if $\mathcal{L} = \mathcal{L}_0^n$ is the n-power of a principal line bundle, then for P, Q as above, $e_{\mathcal{L}^\ell}(P, Q) = e_{\mathcal{L}_0^\ell}(P, Q)^n$. So we get a power of the standard Weil pairing associated to the principal polarisation $\mathcal{L}_0$, and $e_{\mathcal{L}^\ell}$ is non degenerate when restricted on $A[\ell]$ if ℓ is prime to n.

When A is the Jacobian $\mathrm{Jac}(C)$ of a curve, with the principal polarisation coming from the Θ divisor, we can compute the Weil pairing on A by working with functions and divisors on the curve C. Indeed assume that C/k has a rational point $O \in C(k)$. Let f be a function on C, with divisor $\sum(P_i) - \sum(Q_i)$. Then it induces a function on $\mathrm{Jac}(C)$ by letting for $x \in \mathrm{Jac}(C)$ not in $\Theta_{P_i - O}$, $f(x) = f(D_x)$ where D_x is the (unique) effective divisor of degree g such that $D_x - gO$ represents x (see [CE14, § 2.2]).

Then seen on $\mathrm{Jac}(C)$, $\mathrm{Div}(f) = \sum \Theta_{P_i - O} - \sum \Theta_{Q_i - O}$. Thus we can construct functions associated to cycles via Θ directly on the curve. In other words: if we have a divisor $D = \sum n_i(P_i)$ of degree 0 on the curve, it is principal whenever its realisation $[D] \in J$ in the Jacobian is trivial, hence whenever the cycle $Z_D = \sum n_i(P_i - O)$ is trivial on J. If we let f_D with divisor D, D' another degree zero divisor on C, then by definition the extension of f_D to the Jacobian satisfy $f_D(D') = f_D(Z_{D'})$. Conversely, any degree zero cycle on J is equivalent to a cycle coming from a degree 0 divisor D on C. So for pairings, it is enough to work with divisors and functions on curves.

In particular, both interpretations of the Weil pairing can be reformulated in terms of divisors on the curve, and Weil's reciprocity for curves is enough to show that they give the same definition. This is the usual setting looked

at in cryptography. We argue however that restricting to curves provide less flexibility (even when working on Jacobian), we will see for instance that the pairing induced by a small multiple $n\Theta$ of the theta divisor has the big advantage that there is no point where the intermediate Miller steps are not well defined.

Lets record how to translate Corollary 4.1.3 to Jacobians:

rop:weiljacobian

Proposition 4.1.4. *Let $J = \mathrm{Jac}(C)/k$ be the Jacobian of a curve, and $O \in C(k)$ be a rational point. The Weil pairing $e_\ell : J[\ell] \times J[\ell] \to \mu_\ell$ associated to its principal polarisation coming from the theta divisor Θ may be defined by letting D_P and D_Q be any divisors on C linearly equivalent to $(P) - (O)$ and $(Q) - (O)$ respectively, $f_{\ell D_P}$ (resp. $f_{\ell D_Q}$) a function representing the principal divisor ℓD_P (resp. ℓD_Q), and setting*

$$e_\ell(P, Q) = \frac{f_{\ell D_P}(D_Q)}{f_{\ell D_Q}(D_P)}.$$

4.1.3 *Restricting the Weil pairing to subgroups*

subsec:G1G2

For an elliptic curve E over $\mathbb{F}_q$, the Weil pairing is a pairing $e_\ell : E[\ell] \times E[\ell] \to \mu_\ell$. It is customary in cryptography to work in the setting where $E(\mathbb{F}_q)$ has a rational point P of ℓ-torsion, and the embedding degree d such that $\mu_\ell \subset \mathbb{F}_{q^d}$ satisfy $d > 1$. Then $E[\ell] \subset \mathbb{F}_{q^d}$.

We recall that the embedding degree d is the smallest extension $\mathbb{F}_{q^d}$ such that $\mu_\ell(\overline{\mathbb{F}}_q) \subset \mathbb{F}_{q^d}$. This is the order of π acting on a primitive ℓ-root of unity ζ, so this is the order of q in $\mathbb{Z}/\ell\mathbb{Z}$.

The Frobenius action on $E[\ell]$ has then two eigenvalues, 1 and q, and it is customary to define $\mathbf{G}_1$ and $\mathbf{G}_2$ as the two corresponding eigencomponents. We have $\mathbf{G}_1 = E[\ell](\mathbb{F}_q)$ while $\mathbf{G}_2 = \{Q \in E[\ell] \mid \pi(Q) = qQ\}$ is exactly the kernel of the trace of π, since $\ell \mid q^d - 1$ by definition of the embedding degree. We have $E[\ell] = \mathbf{G}_1 \oplus \mathbf{G}_2$, and since e_ℓ is alternate we get that its restriction to $\mathbf{G}_1 \times \mathbf{G}_2$ or to $\mathbf{G}_2 \times \mathbf{G}_1$ is non degenerate. (The same hold when replacing $\mathbf{G}_2$ by any supplement $\mathbf{G}_3$ of $\mathbf{G}_1$, this as the benefit that if $\mathbf{G}_3 \cap \mathbf{G}_2 = 0$, the trace induces an isomorphism $\mathbf{G}_3 \simeq \mathbf{G}_1$, hence e_ℓ restrict to a pairing of type II.)

For a principally polarised abelian variety $A/\mathbb{F}_q$, if we let $\mathbf{G}_1'$ and $\mathbf{G}_2'$ be the characteristic spaces of $A[\ell]$ related to the eigenvalues 1 and q (assuming they are not empty and that $q \neq 1 \mod \ell$, ie the embedding degree $d > 1$, so that $\mathbf{G}_1' \neq \mathbf{G}_2'$), then since $A[\ell]$ is its own Cartier dual (as a Galois module), $\mathbf{G}_2'$ is the Cartier dual of $\mathbf{G}_1'$, and furthermore by writing $A[\ell]$ as a direct sum of indecomposable modules $A[\ell] = \mathbf{G}_1' \oplus \mathbf{G}_2' \oplus \cdots$, we see that e_ℓ is non degenerate on $\mathbf{G}_1' \times \mathbf{G}_2'$ and on $\mathbf{G}_2' \times \mathbf{G}_1'$. Be careful that even if we let $\mathbf{G}_1, \mathbf{G}_2$ be the eigenvectors for the eigenvalues 1 and q respectively, then $\mathbf{G}_2$ is the Cartier dual of $\mathbf{G}_1$ but the Weil pairing may not be non degenerate on $\mathbf{G}_1 \times \mathbf{G}_2$.

We give below an elementary proof of this, not relying on Cartier duality (except of course for the existence of e_ℓ itself).

We start by a general lemma on symplectic decomposition.

lem:symplectic

Lemma 4.1.5. *Let M be a symplectic matrix in a vector space V/k. Let χ_M be its characteristic polynomial, since M is symplectic χ_M is a reciprocal polynomial. Let Q be a reciprocal polynomial dividing χ_M. Then denoting by V_Q the characteristic space of Q, we have that M restricted to V_Q is symplectic.*

In particular, if Q_1 is a prime factor of χ_M, Q_2 its reciprocal polynomial, and $Q_2 \neq Q_1$, then M restricted to $V_{Q_1} \oplus V_{Q_2}$ is symplectic.

Proof. (With help from Jérôme Plût.) Write $\chi_M = Q^d R$ with R prime to Q. Then V_Q is the image of V by $R(M)$. If $v_1 \in V_Q$, we want to find $v_2 = R(M)v_2'$ such that $\langle v_1, v_2\rangle \neq 0$ where $\langle v_1, v_2\rangle = {}^t v_1 J v_2$ is the symplectic action. But $\langle v_1, R(M)v_2'\rangle = \langle \widetilde{R(M)} v_1, v_2'\rangle$ where $\widetilde{R(M)} = R(M^{-1})$ is the symplectic transpose (where we use here that M is symplectic). But since both χ_M and Q are reciprocal, R too, so $R(M^{-1}) = M^e R(M)$ where $e = \deg R$. So $M^e R(M) v_1 \neq 0$ since $v_1 \in V_Q$, so there do exist a v_2'. □

lem:symplectic2

Lemma 4.1.6. *If Q is an irreducible divisor of χ_M which is not a reciprocal polynomial, then its characteristic space is isotropic. If Q_1, Q_2 are two distinct irreducible divisors of χ_M which are not reciprocal, then the Q_i characteristic spaces are orthogonal.*

Proof. If $\chi_M = Q^e R$ with R prime to Q, then $\operatorname{Ker} Q^e = \mathfrak{I}R$, so if x, y are in $\operatorname{Ker} Q^e$, $(x|y) = (Ru|Rv) = (u|\widetilde{R}Rv)$ where $\widetilde{R}$ is the reciprocal of R by the same reasoning as in the proof of Lemma 4.1.5. So the Q characteristic space is isotopic whenever $\widetilde{Q}^e \mid R$, eg when Q is irreducible and not reciprocal. Likewise, the Q_1-characteristic space is orthogonal to the Q_2-characteristic space if $\widetilde{Q_2}^{e_2} \mid R_1$. □

By the same reasoning: if Q_1 and Q_2 are two distinct irreducibles divisors of χ_M such that Q_2 is the reciprocal of Q_1, and we assume that $M \mid Q_i$ is cyclic of minimal polynomial Q_i^e, then the orthogonal of $\operatorname{Ker} Q_1^f$ in $\operatorname{Ker} Q_2^e$ is given by $\operatorname{Ker} Q_2^{e-f}$.

Corollary 4.1.7. *Let $A/\mathbb{F}_q$ be a principally polarised abelian variety of dimension g over a finite field $\mathbb{F}_q$. Let ℓ be a prime, χ_π be the characteristic polynomial of the Frobenius on $A[\ell]$, and assume that $A[\ell](\mathbb{F}_q) \neq 0$ and that the embedding degree $d > 1$. Let $\mathbf{G}_1'$ and $\mathbf{G}_2'$ be the characteristic spaces related to the eigenvalues 1 and q. Then the Weil pairing e_ℓ restricted to $\mathbf{G}_1' \times \mathbf{G}_2'$ and to $\mathbf{G}_2' \times \mathbf{G}_1'$ is non degenerate.*

Proof. By Lemma 4.1.5 above, using the obvious adaptation to the case that π is q-symplectic, we get that e_ℓ is non degenerate on $\mathbf{G}_1' \oplus \mathbf{G}_2'$. But $\mathbf{G}_1'$ and $\mathbf{G}_2'$ are isotropic by Lemma 4.1.6, so $\mathbf{G}_1' \oplus \mathbf{G}_2'$ is a symplectic decomposition of $\mathbf{G}_1' + \mathbf{G}_2'$, hence the Weil pairing is non degenerate on $\mathbf{G}_1' \times \mathbf{G}_2'$ and $\mathbf{G}_2' \times \mathbf{G}_1'$.

It is instructive, if a bit tedious, to try to prove the isotropy directly. First we show that $e_\ell(\mathbf{G}_1', \mathbf{G}_1') = 1$. Indeed, if P is an eigenvalue, then $e_\ell(P, Q)^\pi = e_\ell(P, \pi(Q))$, so $e_\ell(P, Q)^{(\pi-1)^k} = e_\ell(P, (\pi-1)^k Q) = 1$ if $Q \in \mathbf{G}_1'$ for k-big enough. So $e_\ell(P, Q)$ is rational, but since $\mathbb{F}_q \cap \mu_\ell = 1$ by our assumption (here we need that ℓ is prime), then $e_\ell(P, Q) = 1$ if $Q \in \mathbf{G}_1$. And then if $\pi(P') = P' + P$, we also have $e_\ell(P', Q)^\pi = e_\ell(P', Q)$, and we conclude by induction on an Jordan-Holder basis that $e_\ell(\mathbf{G}_1', \mathbf{G}_1') = 1$.

Likewise, if P is an eigenvalue for q, $e_\ell(P, Q)^\pi = e_\ell(\pi P, \pi Q) = e_\ell(qP, \pi Q) = e_\ell(P, \pi Q)^q = e_\ell(P, \pi Q)^\pi$. So $e_\ell(P, Q) = e_\ell(P, \pi Q)$, hence if Q is also an eigenvalue for q,$e_\ell(P, Q)$ is rational so is equal to 1. We conclude as above by double induction on P and Q that $e_\ell(\mathbf{G}_2', \mathbf{G}_2') = 1$.

□

4.2 THE TATE PAIRING

sec:tate

The Tate pairing is derived from the Weil pairing using cup product and Galois cohomology (or étale cohomology for abelian schemes). There are several different variants, the Tate-Lichtenbaum pairing [Lic69] which is better suited for finite fields, and the Tate pairing [Tat57] which is better suited for number fields.

4.2.1 *The Tate-Cartier pairing*

tecartier

Assume that k is perfect for simplicity, and let G_k be its absolute Galois group. We denote by $H^i(k, M)$ the Galois cohomology $H^i(G_k, M)$ [3]. Then by Hilbert 90, $H^1(k, \overline{k}^*) = 0$, so the long exact sequence associated to the Kummer exact sequence $1 \to \mu_n \to \overline{k}^* \to \overline{k}^* \to 1$ yield $H^1(k, \mu_n) \simeq k^*/k^{*,n}$.

Let $f : A \to B$ be a separable isogeny of exponent n, with kernel K and let $\widehat{K}$ be the kernel of the dual isogeny $\hat{f}$. Then applying Galois cohomology we get a map $H^0(k, B)/H^0(k, A) \to H^1(k, K)$, so we have a mapping $B(k)/A(k) \times \widehat{K}(k) = H^0(k, B)/H^0(k, A) \times H^0(k, \widehat{K}) \to H^1(k, K) \times H^0(k, \widehat{K}) \to H^1(k, K \otimes \widehat{K}) \to H^1(k, \mu_n) \simeq k^*/k^{*,n}$. Here we used the cup product to go to $K \otimes \widehat{K}$, followed by the Cartier-Weil pairing e_f, and the fact that $H^1(k, k^*) = 0$ by Hilbert 90 so that $H^1(k, \mu_n) \simeq k^*/k^{*,n}$.

We now specialize this to finite fields. So let $k = \mathbb{F}_q$ be a finite field. Since the Galois group is procyclic, Galois cohomology is easy to describe. If M is a finite G_k module, then by the inflation-restriction sequence, there is an extension k'/k such that $H^1(k, M) = H^1(\operatorname{Gal}(k'/k), M)$ (it suffice to take k' such that the restriction map $H^1(k, M) \to H^1(k', M)$ in the inflation-restriction sequence $0 \to H^1(\operatorname{Gal}(k'/k), M(k')) \to_{inf} H^1(k, M) \to_{res} H^1(k', M)^{\operatorname{Gal}(k'/k} \to H^2(\operatorname{Gal}(k'/k), M(k')) \to_{inf} H^2(k, M)$ is zero). Now G is a cyclic group. It is convenient here

[3] We have $H^i(G_k, M) = H^i_t(k, M)$. So when looking at the Tate pairing for abelian schemes A/S the discussion would extend using étale cohomology instead (or even flat cohomology to handle inseparable isogenies). We refer to [Milo6a] for more details.

to use Tate's cohomology groups. We recall that they are defined by: $\widehat{H}^1(G,M) = H^1(G,M)$ and $\widehat{H}^0(G,M) = H^0(G,M)/\operatorname{Tr}$, where $\operatorname{Tr} : H_0(G,M) \to H^0(G,M)$ sends a to $\sum_{g\in G} g.a$. The group $\widehat{H}^0$ allows to glue the long exact sequence coming from homology with the long exact sequence coming from cohomology.

Since G is cyclic, taking a generator g we have an explicit description as $\widehat{H}^0(G,M) = M^G/\operatorname{Tr}$ and $\widehat{H}^1(G,M) = \operatorname{Tr}_0/\langle g-1\rangle$ where $\operatorname{Tr}_0 = \operatorname{Ker}\operatorname{Tr}$ are the elements of trace 0 in M. Furthermore, since the Herbrandt quotient is 1, both groups have the same cardinality. Increasing the field k' if needed, we may also assume that $\operatorname{Tr} = 0$. Furthermore we can take for g the Frobenius σ. In this case, $\widehat{H}^0(G,M) = M^G = M(k)$ and $\widehat{H}^1(G,M) = M/\langle\sigma-1\rangle$

Let $\widehat{M}$ be the Cartier dual of M, and assume that M is of exponent n. Then we have $H^1(k,M) \simeq M/\langle\sigma-1\rangle$ while $H^0(k,\widehat{M}) = \widehat{M}(k) = \operatorname{Hom}(M,\overline{k}^*)^G = \operatorname{Hom}(M,\mu_n)^G = \operatorname{Hom}(M,\mu_n)[\sigma-1]$ where G acts by conjugation, ie the rational maps $f : M \to \mu_n$ are precisely those that commute with the Frobenius: $\sigma f\sigma^{-1} = f$. Since $H^1(k,\mu_n) \simeq \mu_n/\langle\sigma-1\rangle$, we see that the application $H^1(k,M)\times H^0(k,\widehat{M}) \to H^1(k,\mu_n)$ given by composing the cup product with the Cartier duality is given by the (well defined) natural restriction $M/\langle\sigma-1\rangle \times \operatorname{Hom}(M,\mu_n)[\sigma-1] \to \mu_n/\langle\sigma-1\rangle$ of the Cartier duality $M\times\widehat{M}\to\mu_n$. Explicitly we get a pairing as follow: if M is of exponent n, $f\in\widehat{M}(k) = \operatorname{Hom}(M,k^*)^G$ and $[x]\in H^1(k,M) = M/\langle\sigma-1\rangle$, we associate $[f(x)]\in H^1(k,\mu_n) = \mu_n/\langle\sigma-1\rangle$.

As an example, the isomorphism $H^1(k,\mu_n)\simeq k^*/k^{*,n}$ can be described explicitly as follow. Let $x\in\mathbb{F}_q^*$, and $y\in\overline{\mathbb{F}}_q$ such that $x = y^n$. Then $\sigma(y)/y$ is an element of μ_n, well defined from x up to the action of $\sigma\zeta/\zeta$ for $\zeta\in\mu_n$. The Cartier dual of μ_n is $\mathbb{Z}/n\mathbb{Z}$, so the duality above shows that $k^*/k^{*,n}$ is dual to $\mathbb{Z}/n\mathbb{Z}$: we recover Kummer theory. If $\mu_n\subset k$, then $H^1(k,\mu_n) = \mu_n$ and the identification above is simply $x\mapsto x^{\frac{q-1}{n}}$. In other words this is exactly the final exponentiation in the Tate pairing as used in cryptography.

When $\mu_n(\overline{k})\subset k^*$, the pairing above is a duality (in particular is non degenerate): $H^0(k,\widehat{M}) = \widehat{M}(k) = \operatorname{Hom}(M,\overline{k}^*)^G = \operatorname{Hom}(M,k^*)^G = \operatorname{Hom}(M/\langle\sigma-1\rangle,k^*) = \operatorname{Hom}(H^1(k,M),k^*)$. Alternatively, we may also see the duality as follow: M is dual to $\widehat{M}$ by definition, so $\widehat{M}[\sigma-1]$ is dual to $M/\langle\sigma-1\rangle$ (using that $\sigma-1$ is trivial on μ_n). But the first element is $\widehat{M}(k)$ while the second is $H^1(k,M)$.

Applying this to an isogeny yields the following.

prop:tatecartier

Proposition 4.2.1 (Tate-Cartier pairing)**.** *Let $f : A\to B$ be a separable isogeny of abelian varieties of exponent n over a finite field $k = \mathbb{F}_q$. Let K be the kernel of f and let $\widehat{K}$ be the kernel of the dual isogeny $\hat{f}$. Then the pairing $e_{T,f} : B(k)/A(k)\times\widehat{K}(k)\to H^1(k,\mu_n)$, given via the identification $H^1(k,\mu_n)\simeq\mu_n/(\pi-1)$, by $e_{T,f}(P,Q) = e_f(\pi(P')-P',Q)$ where P' is any point in $A(\overline{k})$ such that $f(P') = P$, is isomorphic to the canonical pairing $K(\overline{k})/\langle\sigma-1\rangle\times\widehat{K}(k)\to\mu_n/\langle\sigma-1\rangle$ induced by Cartier duality.*

In particular, if $\mu_n(\overline{k})\subset k^*$ the Tate-Cartier pairing is non degenerate.

Proof. We have constructed a pairing $H^1(k,K)\times H^0(k,\widehat{K})\to H^1(k,\mu_n)$. But by Lang's theorem [Lan56], $H^1(k,A) = 0$ when k is a finite field (ie A has no non trivial torsors, ie every torsor of A over a finite field $\mathbb{F}_q$ has a rational point over $\mathbb{F}_q$), so by the long exact sequence of Galois-cohomology $H^1(k,K)\simeq B(k)/A(k)$. The formula is then just an unraveling of the definition, using the fact that e_f is induced by the Cartier pairing. □

We recover [Bru11] in the case that $n\mid q-1$ so that $H^1(k,\mu_n) = \mu_n$. See also [Bru11, Remark p.2] for a more direct proof due to Lenstra not needing cohomology: the Weil-Cartier pairing $\ker f\times\ker\hat{f}\to\mathbb{G}_m$ restricts to a non degenerate pairing $\ker f/(\pi-1)\times\ker[\pi-1]\to\mathbb{G}_m$. But $\pi-1$ induces an isomorphism $A[f\circ(\pi-1)]/(A[f]+A[\pi-1])\simeq A[f]/(\pi-1) = \ker f/(\pi-1)$ and f induces an isomorphism $A[f\circ(\pi-1)]/(A[f]+A[\pi-1])\simeq B[\pi-1]/f(A[\pi-1]) = B(k)/f(A(k))$, so $B(k)/f(A(k))\simeq\ker f/(\pi-1)$.

When $n=\ell$ is prime, if the embedding degree is not one then $\mu_n/\langle\sigma-1\rangle$ is trivial, so the general case of Proposition 4.2.1 is not really useful. However the general case is useful when n is not prime and μ_n is only partly rational, to identify subgroups on which the Tate-Cartier pairing is non degenerate.

rem:tatevsweil

Remark 4.2.2.

- Both the Tate-Cartier and Weil-Cartier are equivariant under Galois, by construction.
- The Tate-Cartier pairing does not really depend on the isogeny (if everything is well defined): if $f : A\to B$, $g : B\to C$, then $e_{T,g\circ f}(P,Q) = e_{T,g}(P,Q)$ if $Q\in\operatorname{Ker}\hat{g}\subset\operatorname{Ker}\hat{g\circ f}$ and $P\in C(k)$.

  Indeed, if $g\circ f(P_0) = P$, then $e_{T,g\circ f}(P,Q) = e_{g\circ f}(\pi P_0 - P_0,Q) = e_g(f(\pi P_0-P_0,Q) = e_{T,g}(P,Q)$ by Equation (4.3).

- We have the following compatibility of the Tate-Cartier pairing with endomorphisms: if $f : A \to B$, $g : C \to D$ and $\alpha_1 : A \to C$, $\alpha_2 : C \to D$ makes the diagram commute, then $e_{T,g}(\alpha_2 P, Q) = e_{T,f}(P, \hat{\alpha}_2 Q)$, for $P \in A(k)$ and $Q \in \ker \hat{g}$ such that $\hat{\alpha_2} Q \in \ker \hat{f}$.

  Indeed, if $f(P_0) = P$, then $g(\alpha_1(P_0) = \alpha_2(P)$, so the LHS is given by $e_g(\pi\alpha_1(P_0) - \alpha_1(P_0), Q)$ while the RHS is given by $e_f(\pi P_0 - P_0, \hat{\alpha_2} Q)$ so by compatibility of the Weil pairing with isogenies, both term are equal to $e_{g\circ\alpha_1=\alpha_2\circ f}(\pi P_0 - P_0, Q)$.

  In particular, $e_{T,\ell}(\alpha P, Q) = e_{T,\ell}(P, \hat{\alpha} Q)$.

- There is an important difference between the Weil pairing and the Tate pairing: the Weil pairing is *geometric*, in particular does not depends on the base field, so we may work over $\overline{k}$. The Tate pairing is arithmetic, changing the field will change the pairing, and it is trivial over $\overline{k}$ (since $H^1(\mu_n, \overline{k}) = 1$). For instance, if $f : A \to B$ is an isogeny of exponent ℓ with $\mu_\ell \subset \mathbb{F}_q$, the reduced Tate-Cartier pairing $e_{T,f}^{\mathbb{F}_{q^m}}(P, Q)$ over $\mathbb{F}_{q^m}$ is equal to $e_{T,f}^{\mathbb{F}_q}(P, Q)^m$ for $P \in B(k)$ and $Q \in \mathrm{Ker}\hat{f}(k)$.

  Indeed, $e_{W,f}(\pi^m P_0 - P_0, Q) = e_{W,f}(\pi P_0 - P_0, Q)^{1+q+\cdots+q^{m-1}}$ and $1 + q + \cdots + q^{m-1} = q - 1 + \cdots + q^{m-1} - 1 + d = d \mod \ell$.

- On the other hand we have seen that the Tate pairing does not depend on the isogeny, for instance $e_{T,\ell^2}(P, Q) = e_{T,\ell}(P, Q)$ (if both terms are defined), while $e_{W,\ell^2}(P, Q) = e_W(P, Q)^\ell$ (if both terms are defined). Using the results above, we do have $e_{T,\ell^2}^{\mathbb{F}_{q^\ell}}(P, Q) = e_{T,\ell}^{\mathbb{F}_q}(\ell P, Q)$.

- The Weil pairing is alternate, so $e_\ell(P, P) = 1$ (in characteristic different from 2). The Tate pairing may satisfy $e_\ell(P, P) \neq 1$. One of the original motivation for the Tate pairing in cryptography [FR94] was for this case: if $E/\mathbb{F}_q$ is an elliptic curve where $E[\ell](\mathbb{F}_q) = \langle P \rangle$ is of rank 1 and the embedding degree is 1, then $e_\ell(P, P) = 1$ but $e_{T,\ell}(P, P) \neq 1$ since the Tate pairing is non degenerate on $E[\ell](\mathbb{F}_q) \times E[\ell](\mathbb{F}_q) \to \mu_\ell$ since $\mu_\ell \subset \mathbb{F}_q$ here (in this cryptographic setting, $E(\mathbb{F}_q)$ has no points of ℓ^2-torsion).

- If ℓ is prime, the final exponentiation in the Tate pairing kills any element in a subfield of $\mathbb{F}_{q^d}$ (since no subfield contains μ_ℓ by definition). For instance for elliptic curve, if $d = 2d'$ is even then points in $Q \in \mathbf{G}_2$ satisfy $\pi^{d'}(Q) = -Q$, hence $x_Q \in \mathbb{F}_q^{d'}$. During Miller's algorithm to compute the Tate pairing on $\mathbf{G}_1 \times \mathbf{G}_2$ (see Section 4.2.3), the denominators involve $x_Q - x_P$ where $Q \in \mathbf{G}_2$ and $P \in \mathbf{G}_1$, hence are in $\mathbb{F}_q^{d'}$ so are killed by the final exponentiation. This is one of the reason Tate's pairing is faster to compute than Weil's pairing for elliptic curves.

arisation

Example 4.2.3 (Tate-Cartier pairing and polarisations)**.** If $f : A \to B$ is an isogeny, the Tate-Cartier pairing is a pairing $e_{T,f}$ on $B(k)/A(k) \times \mathrm{Ker}\hat{f}(k)$. If B has a polarisation $\mathcal{L}$, the isogeny $\Phi_\mathcal{L} \circ f : A \to B \to \hat{B}$ induce a Tate-Cartier pairing on $e_{T,\mathcal{L},f} : \hat{B}(k)/A(k) \times \Phi_\mathcal{L}^{-1}(\mathrm{Ker}\hat{f}(k))$. By definition of the Tate-Cartier pairing, we have, if $P \in B(k)$, $e_{T,\Phi_\mathcal{L}\circ f}(\Phi_\mathcal{L}(P), Q) = e_{\mathcal{L},f}(\pi(P') - P', Q)$ for any P' such that $f(P') = P$. So if we define a pairing $e_{T,\mathcal{L},f}$ on $B(k)/A(k) \times \mathrm{Ker}\hat{f}$ as in Proposition 4.2.1 by simply replacing e_f by $e_{\mathcal{L},f}$ in the definition, then we have $e_{T,\mathcal{L},f}(P, Q) = e_{T,\Phi_\mathcal{L}\circ f}(\Phi_\mathcal{L}(P), Q)$. (In particular, if $f = [\ell]$, then this is the pairing induced by $\Phi_{\mathcal{L}^\ell}$, ie $e_{T,\mathcal{L},\ell} = e_{T,\Phi_{\mathcal{L}^\ell}}(\Phi_\mathcal{L}(P), Q) = e_{\mathcal{L}^\ell}(\pi(P') - P', Q)$ where $\ell P' = P$.)

If $\mathcal{L} = \mathcal{L}_0^n$, and $Q \in \Phi_{\mathcal{L}_0}^{-1}(\mathrm{Ker}\hat{f}(k))$, then by compatibility of the Weil-Cartier pairing with isogenies or the fact that the Tate pairing does not depends on the isogeny Remark 4.2.2, $e_{T,\Phi_\mathcal{L}\circ f}(\Phi_\mathcal{L}(P), Q) = e_{T,\Phi_{\mathcal{L}_0}\circ[n]\circ f}(\Phi_\mathcal{L}(P), Q) = e_{T,\Phi_{\mathcal{L}_0}\circ f}(\Phi_{\mathcal{L}_0}(P_0), Q)$ if $\Phi_{\mathcal{L}_0}(P_0) = \Phi_\mathcal{L}(P)$.

Since $\Phi_\mathcal{L}(P) = n\Phi_{\mathcal{L}_0}(P)$, we get that $e_{T,\mathcal{L},f}(P, Q) = e_{T,\mathcal{L}_0,f}(P, Q)^n$.

More generally, since $\Phi_{\mathcal{L}\otimes\mathcal{M}} = \Phi_\mathcal{L} + \Phi_\mathcal{M}$, we have $e_{T,\mathcal{L}\otimes\mathcal{M},f}(P, Q) = e_{T,\mathcal{L},f}(P, Q) e_{T,\mathcal{M},f}(P, Q)$ by Item 2.

Example 4.2.4. Let $A/\mathbb{F}_q$ be a polarised abelian variety, and let $f = \pi - 1$ where π is the Frobenius. Then the Weil-Cartier pairing is a pairing on $A(\mathbb{F}_q) \times \widehat{A}[\pi \widehat{-} 1]$. The Tate-Cartier pairing is a pairing on $A(\mathbb{F}_q)/(\pi -$

$1)A(\mathbb{F}_q) \times \widehat{A}[\pi \hat{-} 1](\mathbb{F}_q)$. Looking at the definition in Proposition 4.2.1, $\pi(P') - P' = P$, so in this case the Tate-Cartier pairing is equal to the Weil-Cartier pairing.

In [Garo2], the author applies this to an elliptic curve $E/\mathbb{F}_q$ such that $E(\mathbb{F}_q)$ is a prime ℓ, and the trace $a_q = 2$ (in particular the embedding degree is one). In this case, we get that $\pi \hat{-} 1 = \hat{\pi} - 1$, and using the principal polarisation to go to E we have that $\hat{\pi}$ is the Verschiebung (see [MGE12, Proposition 7.34]). The condition on the trace shows that $E[\hat{\pi} - 1] = E(\mathbb{F}_q)$, so there is a non degenerate pairing on $E(\mathbb{F}_q) \times E(\mathbb{F}_q)$. Plugging the formula for the Weil-Cartier pairing, the author recovers in this particular case the formula of the Tate pairing from Proposition 4.2.5. See also [Scho5, § 6].

4.2.2 The Tate-Lichtenbaum pairing

Let $A/\mathbb{F}_q$ be an abelian variety, d the embedding degree for μ_ℓ. One usually apply the Tate-Cartier pairing for the isogeny $[\ell] : A \to A$, this yield a (reduced) pairing $e_{T,\ell} : A(\mathbb{F}_{q^d})/\ell A(\mathbb{F}_{q^d}) \times \widehat{A}[\ell](\mathbb{F}_{q^d}) \to \mu_\ell$.

If $\mathcal{L}$ is a polarisation, plugging $e_{\mathcal{L}\ell}$ instead of e_ℓ in the definition of the Tate pairing (see Example 4.2.3) yield the following definition:

prop:reducedtate

Proposition 4.2.5 (Explicit versions of the Tate-Lichtenbaum pairing)**.** *The (reduced) Tate-Lichtenbaum pairing $e_{T,\ell} : A(\mathbb{F}_{q^d})/\ell A(\mathbb{F}_{q^d}) \times A[\ell](\mathbb{F}_{q^d}) \to \mu_\ell$ may be computed for $P \in A(\mathbb{F}_{q^d})$ and $Q \ni A[\ell](\mathbb{F}_{q^d})$ as $e_{\mathcal{L}^\ell}(\pi P' - P', Q)$ where P' is any point in A such that $\ell P' = P$.*

Using the notations of Corollary 4.1.3, the non reduced Tate-Lichtenbaum pairing $A(\mathbb{F}_{q^d})/\ell A(\mathbb{F}_{q^d}) \times A[\ell](\mathbb{F}_{q^d}) \to \mathbb{F}^*_{q^d}/\mathbb{F}^{*,\ell}_{q^d}$ is given by $f_{\Theta,\ell D_P}(Z_Q)$, hence the reduced Tate pairing as $f_{\Theta,\ell D_P}(Z_Q)^{(q^k-1)/\ell}$.

If $A = \mathrm{Jac}(C)$ is the Jacobian of a curve and $\mathcal{L}$ is the polarisation coming from the theta divisor, then this time using the notations of Proposition 4.1.4, the non reduced Tate pairing is also given by $f_{\ell D_P}(D_Q)$.

Proof. The first equation is just the definition of the Tate-Cartier pairing applied to $[\ell]$. It then suffices to plug the definition of the Weil pairing to get the second equation, see for instance [LR15, Theorem 3]. This equation is the one used algorithmically in practice.

Incidentally, to get the second equation it is easier to use the definition of the Weil pairing with the function $g_{\ell,Q}$ (see [LR15, Theorem 3]) rather than the definition in Corollary 4.1.3 using the functions $f_{\ell,Q}$, but using Weil-Lang's reciprocity we can also recover the formula for the Tate pairing using the second definition of the Weil pairing (see [Bru11, Theorem 2.1]).

The case of Jacobians follow by the same reasoning as in Proposition 4.1.4. □

4.2.3 Restricting the Tate-Lichtenbaum pairing to subgroups

subsec:tateg1g2

We can also restrict the Tate-Lichtenbaum pairing to subgroups, as for the Weil pairing. Let $\mathbf{G}_1$ and $\mathbf{G}_2$ be the eigenvalue subgroups for 1 and q respectively, and assume that they are not empty and that $d > 1$. Then $\mathbf{G}_1$ is of type $(\mathbb{Z}/\ell)^r$ as an $\mathbb{F}_q$-module, hence by duality $\widehat{A}$ contains has a $\widehat{G}_2$ of type μ_ℓ^r. Let $\hat{f} : \widehat{A} \to \hat{B} = \widehat{A}/\widehat{G}_2$ be the corresponding isogeny, and let $f : B \to A$ be the dual of $\hat{f}$.

Then the Tate-Cartier pairing yields a pairing $A(\mathbb{F}_{q^d})/B(\mathbb{F}_{q^d}) \times \widehat{G}_2(\mathbb{F}_{q^d}) \to \mu_\ell$. We have $A(\mathbb{F}_{q^d})/B(\mathbb{F}_{q^d}) \simeq H^1(\mathbb{F}_{q^d}, \mathrm{Ker} f)$, with $\mathrm{Ker} f$ the Cartier dual of $\widehat{G}_2$, hence is of type $(\mathbb{Z}/\ell\mathbb{Z})^r$ over $\mathbb{F}_q$. Hence $H^1(\mathbb{F}_{q^d}, \mathrm{Ker} f) = H^1(\mathbb{F}_q, \mathrm{Ker} f) = \mathrm{Ker} f(\mathbb{F}_q)$. So $A(\mathbb{F}_{q^d})/B(\mathbb{F}_{q^d}) \simeq A(\mathbb{F}_q)/B(\mathbb{F}_q) \simeq A(\mathbb{F}_q)/\ell A(\mathbb{F}_q)$ since $A(\mathbb{F}_q)/B(\mathbb{F}_q)$ is a quotient of $A(\mathbb{F}_q)/\ell A(\mathbb{F}_q)$ and since $A(\mathbb{F}_q)/\ell A(\mathbb{F}_q) \simeq H^1(k, A[\ell])$ it has cardinal $h^1(k, A[\ell]) = h^0(k, A[\ell]) = \#A[\ell](k) = \ell^r$ (using that the Herbrandt quotient is one).

We thus get a pairing $A(\mathbb{F}_q)/\ell A(\mathbb{F}_q) \times \widehat{G}_2(\mathbb{F}_{q^d}) \to \mu_\ell$. If $A(\mathbb{F}_q)$ does not contains a point of ℓ^2-torsion, then $\mathbf{G}_1 \to A(\mathbb{F}_q)/\ell A(\mathbb{F}_q)$ is an isomorphism since it is injective and the LHS has the same cardinal as the RHS.

Looking at the quotient $\widehat{A} \to C = \widehat{A}/\widehat{G}_1$ instead, we get a pairing $A(\mathbb{F}_{q^d})/C(\mathbb{F}_{q^d}) \times \widehat{G}_1 \to \mu_\ell$. Whenever $\mathbf{G}_2 \to A(\mathbb{F}_{q^d})/C(\mathbb{F}_{q^d})$ is a monomorphism (eg if $A(\mathbb{F}_{q^d})$ does not contain a point of ℓ^2-torsion), then it is an isomorphism (by cardinality consideration).

4.2.4 The Tate pairing

There is a related pairing, called the Tate pairing, with values in $H^2(k, \mathbb{G}_m)$: by Hilbert 90, we have that $H^2(k, \mu_n) \simeq H^2(k, \mathbb{G}_m)[n] \simeq \mathrm{Br}(k)[n]$ where $\mathrm{Br}(k)$ is the Brauer group. If $f : A \to B$ is a separable isogeny of exponent n as above, with kernel K and dual kernel $\widehat{K}$, Galois cohomology yield exact sequences $H^0(k, B)/H^0(k, A) \to H^1(k, K) \to H^1(k, A)[f]$, and $H^0(k, \widehat{A})/H^0(k, \widehat{B}) \to H^1(k, \widehat{K}) \to H^1(k, \widehat{B})[\hat{f}]$, where $H^1(k, A)$ is the kernel of $H^1(k, A) \to H^1(k, B)$.

Given a point $P \in B(k)/A(k)$ we then have a 1-cocycle $F_P : \mathrm{Gal}(k) \to K$. Likewise, given $\xi \in H^1(k, \widehat{B})[\hat{f}]$, we can lift it to a 1-cocycle $F_\xi : \mathrm{Gal}(k) \to \widehat{K}$. The cup product of F_P and F_ξ gives an element of $H^2(k, K \times \widehat{K})$, and composing with the Cartier-Weil pairing gives a 2-cocycle $\mathrm{Gal}(k) \times \mathrm{Gal}(k) \to \mu_n, (\sigma, \tau) \mapsto e_m(F_P(\sigma), F_\xi(\tau)^\sigma)$. This defines a pairing $B(k)/A(k) \times H^1(k, \widehat{B})[\hat{f}] \to \mathrm{Br}(k)[n]$, the Tate pairing.

This pairing is not interesting for finite fields since $\mathrm{Br}(k) = 0$, but it is for p-adic local fields. Indeed, if K is such a field, $\mathrm{Br}(K) = \mathbb{Q}/\mathbb{Z}$, so $H^2(K, \mu_n) \simeq \mathbb{Z}/n\mathbb{Z}$. Taking for the isogeny the multiplication by $[n]$, Tate proves in [Tat57] that $A(K)/nA(K) \times H^1(K, \widehat{A})[n] \to \mathbb{Z}/n\mathbb{Z}$ is non degenerates, and that these pairings glue to form a pairing $A(K) \times H^1(K, \widehat{A}) \to \mathrm{Br}(K) \simeq \mathbb{Q}/\mathbb{Z}$.

In [FR94], Frey and Rück show how reducing the Tate pairing on $\mathbb{Q}_q$ modulo p recover the Tate-Lichtenbaum pairing $A(k)/\ell A(k) \times A[n]_0 \to \mu_\ell$ where $A[n]_0 = \mathbf{G}_2$ is the trace zero subgroup. They thus deduce that this induced pairing is non degenerate from the non degeneracy of the Tate pairing on $\mathbb{Q}_q$. This recovers Section 4.2.3.

Alternative proofs of the non degeneracy of the Tate-Lichtenbaum (or related) pairings are [Heß04; Sch05]. However they only give the formula of Proposition 4.2.5 in the case of Jacobians either by relating it to the Lichtenbaum pairing in [FR94] or using Weil's reciprocity in [Heß04; Sch05] (but unlike [FR94] these do not deal with restricting the Tate pairing to subgroups).

Part II

MODULI OF ABELIAN VARIETIES

5 MODULI SPACES OF ABELIAN VARIETIES

CONTENTS

ap:moduli

PLANNED TOPICS

5.1 MODULI SPACES FROM THE ANALYTIC POINT OF VIEW

5.1.1 *Siegel spaces*

Explicit description of Siegel spaces [BL04, §8], [Rob10, §2.5]. Modular forms [BGH+08; CS17].

Satake compactification. as a particular case of the Baily Borel compactification [BB66] of Hermitian symmetric spaces [Mil05].

Interpretation of the Siegel operator in term of this boundary.

Toroidal compactifications. Interpretation of the Fourier-Jacobi coefficients. Note: semi abelian variety of toric rank 1, extension of A = a point on $\widehat{A} = H^1(A, \mathbb{G}_m)$

Analytic theta functions as modular forms [Igu72a; Igu66; Igu72b].

5.1.2 *Hilbert spaces*

Hilbert moduli space [BL04, §9.2]. Hilbert modular forms [Van12; BGH+08].

5.1.3 Shimura varieties

PEL Shimura varieties [Milo5], Deligne torus, how to recover the previous examples as special cases of Shimura varieties [Kie20].

5.2 MODULI SPACES FROM THE ALGEBRAIC POINT OF VIEW

5.2.1 Algebraic stacks of abelian varieties

Global construction by Mumford [MFK94], construction via Artin's representability theorem (cf the introduction of [FC90]).

Compactifications [FC90] minimal and toroidal over $\mathbb{Z}$. Toroidal compactification = smooth proper stack over $\mathbb{Z}$, so we get irreductibility of $\mathcal{A}_g \otimes_{\mathbb{Z}} \mathbb{F}_p$ by the same argument as in Remark 3.2.11.

Modular forms from an algebraic point of view (section of the Hodge bundle) [Kat73], algebraic Koecher principle and Fourier expansions (ie the q-expansion principle to get the ring of definition of a modular form), [Kat73, §1.12], [FC90, Chapter V].

Kodaira-Spencer, Gauss-Manin connection.

5.2.2 The structure of the moduli space

The structure of the moduli space [Mum70b; Jon93a]: $\overline{\mathcal{A}}_{g,d}$, $\overline{\mathcal{A}}_{g,\delta}$, the geometric fibres of $\overline{\mathcal{A}}_{g,\delta} \to \mathbb{Z}$ are irreducible.

Local coordinates [Jon93a].

5.2.3 Stratifications of the moduli space

Stratification via the p-rank: [NO80]. The stratification of p-rank V_f is of dimension $g(g+1)/2 - g + f$, the generic point of each irreducible composant is ordinary.

Refinement via Newton polygon: [Oor01b] (this solves a conjecture by Grothendieck on the possible deformations of a BT-group). Application to density of Hecke orbits [CO09].

Via a finer invariant of $A[p]$: [Oor01a]. This gives a purely algebraic proof (compared to [FC90] of the geometric irreductibility of $\mathcal{A}_g \otimes_{\mathbb{Z}} \mathbb{F}_p$.

5.3 MODULAR SPACE OF LEVEL $\Gamma_0(p)$

The construction of [DR73] for modular curves (which extends readily to $\mathcal{A}_g$). Modular interpretation of the stack of generalised elliptic curves using Drinfeld's structure [KM85; Ces17].

Genus 2: [CN90]. Decomposition of $_{\Gamma_0(p)\otimes_{\mathbb{Z}}\mathbb{F}_p}$: [Jon91; Yu04a].

5.3.1 Hilbert-Blumenthal algebraic stacks

Construction and properties: [Rap78; Cha90], compactification, we get a smooth proper stack.

CURRENT DRAFT VERSION

A lot of this is essentially copy-pasted from [KPR20].

5.4 SIEGEL MODULI SPACE

sec:siegelC

If $A/\mathbb{C}$ is a principally polarised complex abelian variety, by Section 2.1 we have $A = \mathbb{C}^g/(\mathbb{Z}^g \oplus \Omega\mathbb{Z}^g)$ with Ω in the Siegel space $\mathfrak{H}_g$ and the polarisation is given by $(\Im\Omega)^{-1}$. Here the lattice is given by a symplectic basis, and

acting by $\gamma = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z})$ changes Ω by $(a\Omega + b)(c\Omega + d)^{-1}$. This describe the Siegel moduli space as the orbifold $\mathcal{A}_{g,\mathbb{C}} = \mathfrak{H}_g / \mathrm{Sp}_{2g}(\mathbb{Z})$ (see [Rob10, p. 2.5] for the case of polarisations of type δ).

A modular function is a function on this orbifold. More generally a modular form f is a function $f : \mathfrak{H}_g \to V$ satisfying some (automorphic) transformation formula under the action of $\mathrm{Sp}_{2g}(\mathbb{Z})$. Typically a scalar modular form of weight k takes values in $\mathbb{C}$ and satisfy $f(\gamma \cdot \Omega) = \det(a\Omega + b)^k f(\Omega)$. We will need in [Rob21, Section 5.4] more general modular forms (called vectorial modular form) where the transformation formula is given by a representation $\rho : \mathrm{Gl}_g \to V$. In fact g should be defined on some compactification of $\mathbf{H}_g$, (if $g = 1$ this is the cusp at infinity), but by Koecher principle this is automatic if $g \geq 2$. Like in $g = 1$, we can also look at Siegel modular forms for a congruence subgroup Γ of $\Gamma(1) := \mathrm{Sp}_{2g}(\mathbb{Z})$. In this will be particularly interested in the standard level subgroups $\Gamma(n)$ and $\Gamma_0(n)$ which encode principally polarised abelian varieties with a symplectic basis of $A[n]$ or a kernel of an n-isogeny respectively. Thus $\mathcal{A}_{g,\Gamma_0(n),\mathbb{C}} = \mathfrak{H}_g/\Gamma_0(n)$ parametrize n-isogenies. There are several ways to represent this: via the cover $\mathcal{A}_{g,\Gamma_0(n),\mathbb{C}} \to \mathcal{A}_{g,\mathbb{C}}$, via the modular correspondance $\mathcal{A}_{g,\Gamma_0(n),\mathbb{C}} \to \mathcal{A}_{g,\mathbb{C}} \times \mathcal{A}_{g,\mathbb{C}}$ given by $\tau \mapsto (\tau, \tau/n)$, via modular polynomials which essentially give the birational version of these morphisms, ie describe the extension $\mathbb{C}(\mathcal{A}_{g,\Gamma_0(n),\mathbb{C}})/\mathbb{C}(\mathcal{A}_{g,\mathbb{C}})$ which can also be seen as the image of the generic point by the modular correspondance.

A Siegel modular form has Fourier coefficients indexed by positive semi-definite half-integral matrices. There is a Siegel operator which gives a modular form for $\mathfrak{H}_{g-1}$ and essentially comes from the restriction of f on the boundary given by the Satake compactification (if $g = 1$ this is the value at the cusp). We can also look at the canonical partial toroidal compactification (there are several extensions to full toroidal compactification) which parametrizes on the boundary semi-abelian schemes of dimension g with torus rank 1. To give such a semi-abelian $\widetilde{A}$: $1 \to \mathbb{G}_m \to \widetilde{B} \to B \to 0$ is the same as to give B (an abelian variety of dimension $g-1$) and an element of $\mathrm{Ext}^1(B, \mathbb{G}_m)$, ie a point in $P \in \widehat{B}$ (this is not quite the same because there is an extra involution $P \to \pm P$ involved). Restricting f to this boundary gives its Fourier-Jacobi series decomposition (see the excellent survey [Van08, § 5, 8 and 11]).

5.5 HILBERT MODULI SPACE

::hilbertC

If A has real multiplication by a maximal totally real order O_K, then Λ is an O_K module, and we can write $\Lambda = O_K \oplus M$ for some locally free rank 1 O_K-module M. The existence of a polarisation shows that we can write $\Lambda = I \oplus O_K\tau$ where $\tau \in \mathfrak{H}_1^g$ and I is a fractional ideal [BL04, § 9.2]. The polarisation is given by $H_\lambda(z,w) = \sum \lambda_i \frac{z_i \overline{w_i}}{\tau_i}$ where $\lambda \in K$ is totally positive and we denote by λ_i the g embeddings of K in $\mathbb{R}$. We have $\Lambda \otimes \mathbb{Q} = K \oplus K\tau$, so we can see the polarisation as given by $E_\lambda(x + y\tau, x' + y'\tau') = \mathrm{Tr}_{K/\mathbb{Q}}(\lambda(xy - yx'))$ where $x, y, x', y' \in K$. Since we want $E_\lambda(\Lambda, \Lambda) \subset \mathbb{Z}$, we need to take $\lambda \in I^*$, the dual of I for the trace. If $I \subset O_K$, we can take $\lambda = 1$, the orthogonal lattice is then given by $O_K^\star \oplus I^\star\tau$ (recall that for any ideal we have $II^\star = R(I)^*$ where $R(I)$ is its order), so to get a principal polarisation we need $I = O_K^\star = \partial_K^{-1}$. More generally the polarisation types are indexed by the narrow class group $\mathrm{Cl}^+(O_K)$, the ideal I above giving a polarisation of type I^*.

Let us focus on the principally polarised case (ie polarisation of type O_K, ie $I = O_K^*$), we then have that the Hilbert moduli space of principally polarised abelian varieties with real multiplication by O_K is given by $\mathfrak{H}_1^g/\Gamma$ where $\Gamma := \mathrm{Sl}_2(O_K \oplus \partial_K^{-1})$ with the notations of [BGH+08, Eq. 1.6]. (When $g = 2$ see also [MR20, § 2.2 and § A.2] for alternative descriptions of the Hilbert moduli surfaces where the quotient is given by $\mathfrak{H}_1^g/\Gamma$ with $\Gamma = \mathrm{Sl}_2(O_K)$.)

We can then define Hilbert modular forms as functions f on $\mathfrak{H}_1^g$ satisfying a suitable automorphic transformation, given by a representation of GL_1^g (one for each embedding of K in $\mathbb{R}$). So the weight of a Hilbert modular form is given by a g-tuple of weights $(k_1, \dots, k_g)$ such that $f(\gamma \cdot \tau) = \prod \det(c_i\tau_i + d_i)^{k_i} f(\tau)$. A Baily-Borel compactification is given by adding a finite number of cusps $\mathbb{P}^1(K)/\Gamma$. If $O_K^\star$ is isomorphic to O_K (ie if O_K is Gorenstein), then this set is in bijection with $\mathrm{Cl}(K)$ [BGH+08, Lemma 1.3]. Like in the Siegel case, a Hilbert modular form is automatically holomorphic at the cusps if $g > 1$. It has Fourier coefficients indexed by the totally positive elements of O_K (and eventually a constant coefficients). We refer to [BGH+08] for more details.

We also can define level subgroups $\Gamma(I)$ and $\Gamma_0(I)$. We will be mainly interested in the case $I = (\beta)$ with $\beta \gg 0$. Indeed in this case the β-isogeny preserve the polarisation type, otherwise we have a modular correspondance

between Hilbert component of different polarisation type.

We have a canonical map $\mathfrak{H}_1^g \to \mathfrak{H}_g$ by forgetting the real multiplication structure, which is compatible with the action of $\mathrm{Sl}_2(O_K \oplus \partial_K^{-1})$ and $\mathrm{Sp}_{2g}(\mathbb{Z})$ respectively. Concretely if $\Lambda = O_K^\star \oplus \tau O_K$, let $(e_1, \dots, e_g)$ be a $\mathbb{Z}$-basis of τ, and R_{O_K} the matrix given by the g-embeddings of the e_i. Let $(f_1, \dots, f_g)$ be the dual basis for the trace, this is a basis for $O_K^\star$ and we let $R_{O_K^\star}$ be the matrix of the g-embeddings. Then we check that $t_{R_{O_K}} R_{O_K^\star} = \mathrm{Id}$, so $\Lambda = \mathbb{Z}^g \oplus \Omega\mathbb{Z}^g$ with $\Omega = t_{R_{O_K}}^{-1} \tau R_{O_K}$.

The Galois action on K permutes the g embedding, and we say that a Hilbert modular form is symmetric if it is invariant under these permutations. The image in Siegel space is called the Humbert variety (this is essentially the quotient of the Hilbert space under the Galois action), and it is clear that the pullback of a Siegel modular form is symmetric.

5.6 SHIMURA VARIETIES

sec:shimura

More generally we can define a Shimura variety of PEL type as $\mathrm{Sh}_K(G, X_+)(\mathbb{C}) = G(\mathbb{Q})_+ \backslash (X_+ \times G(\mathsf{A}_f))/K = G(\mathbb{Q})_+ \backslash (G(\mathbb{R})_+ \times G(\mathsf{A}_f))/K_\infty \times K$ where X_+ is the hermitian symmetric domain given by the orbit of $G(\mathbb{R})_+$ on a complex structure h on V, (V, ψ) is a faithful symplectic $(B, \star)$-module, $(B, \star)$ a simple algebra with positive involution which can appear as an endomorphism algebra of a principally polarised abelian variety (with the Rosati involution), and G reductive group such that $G(\mathbb{Q})$ are (essentially) the B-symplectic automorphisms of V. We refer to [Mil05] for more details on Shimura variety, and to [Kie20, § 2.2] for the modular interpretation of $\mathrm{Sh}_K(G, X_+)$ as parametrizing abelian varieties with Polarisation, Endomorphisms and Level. We can then define a Hecke correspondance and so modular polynomials in this general setting. The Siegel moduli correspond to $B = \mathbb{Q}$ and $G = \mathrm{GSp}_{2g}(\mathbb{Q})$ and the Hilbert case is $B = K$ (K totally real), and $G = \mathrm{GL}_2(K)$. We refer to [Kie20] for more details.

5.7 SIEGEL MODULI SPACE OVER $\mathbb{Z}$

sec:siegelZ

Since we want to compute modular polynomials over finite field, we need integral models of the corresponding Shimura varieties. First $\mathcal{A}_g := \mathcal{A}_g$, the moduli space of principally polarised abelian varieties is a smooth separated Deligne-Mumford stack with affine diagonal of finite type over $\mathbb{Z}$ (so in practice a very "tame" moduli space). The corresponding coarse moduli space is a quasi-projective scheme by the results of [MFK94]. Indeed Mumford shows that $\mathcal{A}_g$ can be constructed as a (stacky) quotient of a locally closed subscheme of a Hilbert scheme by the reductive group PGL_n, so the coarse moduli space is the corresponding GIT quotient. Algebraicity of the stack $\mathcal{A}_g$ can also be shown directly using Artin criterion.

Integral toroidal (hence smooth) and Baily-Borel-Satake compactifications $\overline{\mathcal{A}}_g$ are constructed in [FC90] (here a compactification is a dense open embedding into a proper stack). This shows as a corollary (using ZMT) that the geometric fibers $\mathcal{A}_g \otimes \overline{\mathbb{F}}_p$ are connected (hence irreducible) since $\overline{\mathcal{A}}_g \otimes \overline{\mathbb{Q}}$ is (as shown by the analytic compactifications of the Siegel moduli space). A purely algebraic proof of the irreducibility of the geometric fibers is given in [Oor01a].

More generally, if we do not want to restrict to principally polarised abelian varieties[1] , we can look at $\mathcal{A}_g^\delta$ [Mum70b], the stack of abelian varieties with a polarisation of type δ, ie such that $K(\mathcal{L}) \simeq \prod_{i=1}^g \mathbb{Z}/\delta_i\mathbb{Z} \times \mu_{\delta_i}$ (after faithfully flat base change if needed). Their geometric fibers are irreducible (and non empty) by [Jon93b]. We also have $\mathcal{A}_g^d$ which parametrizes polarisation of degree d^2 (unlike the $\mathcal{A}_g^\delta$ this includes non ordinary abelian varieties). The ordinary points are dense in each geometric fiber [NO80], so the irreducible components of a geometric fiber at $x \in \mathrm{Spec}\,\mathbb{Z}$ are given by the closure of the geometric fibers of $\mathcal{A}_g^\delta$ at x for δ such that $d = \prod \delta_i$. While $\mathcal{A}_g^d$ is only smooth over $\mathbb{Z}[1/d]$ (because separably polarised abelian varieties lift), the $\mathcal{A}_g^\delta$ are smooth over $\mathbb{Z}$ (essentially because ordinary abelian varieties lift).

[1] Even if we only want to explore the isogeny graph of principally polarised abelian varieties, it is sometime convenient to use intermediate non principally polarised abelian varieties.

For modular correspondances, we need to describe moduli with level subgroups. We stick to the principally polarised case for simplicity. Let us first describe the moduli $\mathcal{A}_{g,\Gamma(n)}$: this is the algebraic stack of principally polarised abelian variety with a level n structure. If we define such a structure on A as an isomorphism $A[n] \simeq (\mathbb{Z}/n\mathbb{Z})^g \times \mu_n^g$, this gives a smooth stack over $\mathbb{Z}$ with irreducible geometric fibers. (Smoothness over $\mathbb{Z}[1/n]$ comes from the fact that $A[n]$ is then étale hence lift, and over Z_p with $p \mid n$ this is because the level n structure impose that A is ordinary.) A word of warning: the stack $\mathcal{A}_{g,\Gamma(n)}$ is often considered over $\mathbb{Z}[1/n, \zeta_n]$ so that the level structure is $A[n] \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$. The geometric fibers of this pullback are then defined over $k(\zeta_n)$ ($k = \mathbb{F}_p$ with $p \nmid n$ or $k = \mathbb{Q}$), hence they decompose into $\phi(n)$ disjoint irreducible components over k. In characteristic $p \mid n$, the stack $\mathcal{A}_{g,\Gamma(n)}$ misses the non ordinary points, hence the forgetting map $\mathcal{A}_{g,\Gamma(n)} \to \mathcal{A}_g$ is quasi-finite, and it is only finite above $\mathbb{Z}[1/n]$. A convenient way to fix this is to consider the normalisation of $\mathcal{A}_g$ in $\mathcal{A}_{g,\Gamma(n)}[1/n]$ (or simply in its generic point). The resulting stack is not smooth at non ordinary points however. This also allows us to define compactifications of $\mathcal{A}_{g,\Gamma(n)}$ as normalisation of a compactification $\overline{\mathcal{A}_g}$ in $\mathcal{A}_{g,\Gamma(n)}[1/n]$. Looking at the normalisation of $\overline{\mathcal{A}_g}$ in $\mathcal{A}_{g,\Gamma(n)}[1/n]$ also allows to construct compactifications of $\mathcal{A}_{g,\Gamma(n)}$. If $n \geq 3$ the inertia stack of $\mathcal{A}_{g,\Gamma(n)}$ is trivial, hence $\mathcal{A}_{g,\Gamma(n)}$ is a space, and in fact a quasi-projective scheme by [MFK94]. If $n \leq 2$, the generic automorphisms are given by $\mathbb{Z}/2\mathbb{Z}$, and the map from $\mathcal{A}_g$ to its coarse space factor through the quotient by the generic automorphisms. The quotient $\mathcal{A}_g \to [\mathcal{A}_g/\pm 1]$ is a $\mathbb{Z}/2\mathbb{Z}$-gerbe, hence is still smooth. This shows that if A is a point of $\mathcal{A}_g$ which only has generic automorphisms, there is an étale open U around A where this holds, and the smooth quotient $[U/\pm 1]$ is a space, ie the coarse space of $\mathcal{A}_g$ is smooth around A.

Anyway over $\mathbb{Z}[1/n]$, the forgetful map $\mathcal{A}_{g,\Gamma(n)} \to \mathcal{A}_g$ is finite étale representable. Moreover the finite group $\Gamma(1)/\Gamma(n) = \mathrm{Sp}_{2g}(\mathbb{Z}/n\mathbb{Z})$ acts on $\mathcal{A}_{g,\Gamma(n)}$ and $\mathcal{A}_g$ is exactly the stack quotient by this action. Now if $\Gamma \subset \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$ is a level subgroup containing $\Gamma(n)$, we can construct $\mathcal{A}_{g,\Gamma}$ as the stack quotient of $\mathcal{A}_{g,\Gamma(n)}$ by $\Gamma/\Gamma(n)$. A T-point of $\mathcal{A}_{g,\Gamma} := [\mathcal{A}_{g,n}/\tilde{\Gamma}]$ then corresponds to an abelian scheme A/T which is étale-locally (since $A[n]$ is étale we just need an étale cover rather than an fppf cover here) endowed with a level n structure modulo the action of $\tilde{\Gamma}$ [DR73, §IV.3.1]. The maps $\mathcal{A}_{g,\Gamma(n)} \to \mathcal{A}_{g,\Gamma}$ and $\mathcal{A}_{g,\Gamma} \to \mathcal{A}_g$ are finite, étale, and representable [DR73, §IV.2, §IV.3]. As for $\mathcal{A}_{g,n}$, we can extend $\mathcal{A}_{g,\Gamma}$ to $\mathbb{Z}$ by normalization. We can also check as in [DR73, §IV.3.6] that the definition does not depend on the integer n such that $\Gamma(n) \subset \Gamma$. Indeed, if m is another integer such that $\Gamma(m) \subset \Gamma$, and we define $\mathcal{A}'_{g,\Gamma}/\mathbb{Z}[1/m] := [\mathcal{A}_{g,m}/\tilde{\Gamma}]$. Then $\mathcal{A}_{g,\Gamma}/\mathbb{Z}[1/n]$ and $\mathcal{A}'_{g,\Gamma}/\mathbb{Z}[1/m]$ are isomorphic over $\mathbb{Z}/[1/nm]$, and since $\mathcal{A}'_{g,\Gamma}/\mathbb{Z}[1/m]$ is smooth, it coincides with the normalization $\mathcal{A}_{g,\Gamma}/\mathbb{Z}$ over $\mathbb{Z}[1/m]$.

We apply this construction to $\Gamma = \Gamma_0(\ell)$ (ℓ prime for simplicity). We then have an algebraic modular correspondance $\mathcal{A}_{g,\Gamma_0(\ell)} \to \mathcal{A}_g \times \mathcal{A}_g$ [KPR20, Proposition 4.9] which we will study over $\mathbb{Z}[1/\ell]$ since we restrict to étale isogenies for simplicity.

We also have the following algebraic interpretation of Siegel modular forms: let $\pi : \mathcal{X}_g \to \mathcal{A}_g$ be the universal abelian scheme, with unit section ϵ. The vector bundle

$$\mathcal{H} = \pi_* \Omega^1_{\mathcal{X}_g/\mathcal{A}_g} = \epsilon^* \Omega^1_{\mathcal{X}_g/\mathcal{A}_g}$$

over $\mathcal{A}_g$, which is dual to $\mathrm{Lie}_{\mathcal{X}_g/\mathcal{A}_g}$, is called the *Hodge bundle*. If ρ is a representation of GL_g, a Siegel modular form of weight ρ is a section of $\rho(\mathcal{H})$; in particular, a scalar-valued modular form of weight k is a section of $\Lambda^g \mathcal{H}^{\otimes k}$. In other words, a Siegel modular form f can be seen as a map

$$(A, \omega) \mapsto f(A, \omega)$$

where A is a point of $\mathcal{A}_g$ and ω is a basis of differential forms on A, with the following property: if $\eta \colon A \to A'$ is an isomorphism, and $r \in \mathrm{GL}_g$ is the matrix of η^* in the bases ω', ω, then $f(A', \omega) = \rho(r) f(A, \omega')$. The link with classical modular forms over $\mathbb{C}$ is the following: if $\tau \in \mathbb{H}_g$, then we let

$$f(\tau) = f(\mathbb{C}^g/(\mathbb{Z}^g + \tau\mathbb{Z}^g), (2\pi i\, dz_1, \dots, 2\pi i\, dz_g)).$$

This choice of basis is made so that the q-expansion principle holds [FC90, p. 141]. The canonical line bundle $\mathfrak{h} = \Lambda^g \mathcal{H}$ is ample (it gives the Baily-Borel compactification), so modular forms give local coordinates on $\mathcal{A}_g$.

5.8 HILBERT MODULI SPACE OVER $\mathbb{Z}$

sec:hilbertZ

We can apply the same method to Hilbert–Blumenthal stacks. [Rap78; Cha90] Let K be a real number field of dimension g, and let O_K be its maximal order. An abelian scheme $A \to S$ has *real multiplication by* O_K if it is endowed with a morphism $\iota\colon O_K \to \mathrm{End}(A)$ such that $\mathrm{Lie}(A)$ is a locally free $O_K \otimes O_S$-module of rank 1. This last condition can be checked on geometric fibers [Rap78, Rem. 1.2] and is automatic on fibers of characteristic zero [Rap78, Prop. 1.4].

Warning: Rapoport defines a compactification of this moduli space in [Rap78], and state that it is smooth over $\mathbb{Z}$. However this "compactification" is not proper. A real compactification is constructed in [DP94] by enlarging the moduli space (at primes dividing the discriminant Δ), however it is smooth only over $\mathbb{Z}[\Delta^{-1}]$. The Rapoport moduli space is fiberwise dense inside the Deligne-Pappas moduli space.

We let $\mathcal{H}_g$ be the Rapoport stack of principally polarized abelian schemes with real multiplication by O_K. It is algebraic and smooth of relative dimension g over $\mathrm{Spec}\,\mathbb{Z}$ [Rap78, Thm. 1.14]. Moreover, $\mathcal{H}_g$ is connected and its generic fiber is geometrically connected [Rap78, Thm. 1.28]. Forgetting ι yields a map $\mathcal{H}_g \to \mathcal{A}_g$, called the *Hilbert embedding*, which is an $\mathrm{Isom}(O_K, O_K) \simeq \mathrm{Gal}(K)$-gerbe over its image, the *Humbert stack*. The map from $\mathcal{H}_g \to \mathcal{A}_g$ is finite over its image by [GD64, EGA IV.15.5.9], [DR73, Lem 1.19] (or by looking at the compactifications of [Rap78], [FC90]).

One can define the stack $\mathcal{H}_{g,n} \to \mathbb{Z}[1/n]$ of RM abelian schemes with a level n structure in the usual way. The map $\mathcal{H}_{g,n} \to \mathcal{H}_g$ is étale over $\mathbb{Z}[1/n]$ [Rap78, Thm. 1.22], its generic fiber is connected, and geometrically has $\phi(n)$ components defined over $\mathbb{Q}(\zeta_n)$ [Rap78, Thm. 1.28]. If β is a totally positive prime of O_K, this allows us to construct, in a similar fashion to $\mathcal{A}_g(\ell)$, the stack $\mathcal{H}_g(\beta) = \mathcal{H}_{g,\Gamma_0(\beta)}$ of RM abelian schemes endowed with a subgroup K which is maximal isotropic for the β-pairing. We have a map

$$\Phi_\beta = (\Phi_{\beta,1}, \Phi_{\beta,2})\colon \mathcal{H}_g(\beta) \to \mathcal{H}_g \times \mathcal{H}_g$$

given by forgetting the extra structure and taking the isogeny respectively. The condition on β ensures that $\Phi_{\beta,2}$ sends $\mathcal{H}_g(\beta)$ to $\mathcal{H}_g$.

If A has real multiplication, there is always a polarization compatible with $\iota\colon O_K \to \mathrm{End}(A)$ [Rap78, Proposition 1.10]. In fact the possible compatible polarizations form a projective O_K-module P of rank 1 with positivity. The stack $\mathcal{H}_g^{\mathrm{pol}}$ of polarized abelian schemes with real multiplication is algebraic and smooth of relative dimension g over $\mathrm{Spec}\,\mathbb{Z}$ [Rap78, Théorème 1.14]. Isomorphisms classes of polarization modules P as above are indexed narrow class group $\mathrm{Cl}^+(\mathbb{Z}_K)$. Therefore $\mathcal{H}_g^{\mathrm{pol}}$ decomposes as $\mathcal{H}_g^{\mathrm{pol}} = \coprod_{P \in \mathrm{Cl}^+(\mathbb{Z}_K)} \mathcal{H}_g^{\mathrm{pol},P}$ where $\mathcal{H}_g^{\mathrm{pol},P}$ is the open substack of abelian schemes with real multiplication and polarization type P [Cha90, §1], [Rap78, Preuve du thm. 1.28]. Over $\mathbb{C}$, the analytification of $\mathcal{H}_g^{\mathrm{pol},P}$ is given by $\mathbb{H}_1^g / \mathrm{Sl}_2(O_K \oplus P^\vee)$, where a point $(t_1, \dots, t_g) \in \mathbb{H}_1^g$ represents the abelian variety $\mathbb{C}^g / (\Sigma(P^\vee) \oplus \mathrm{Diag}(t_1, \dots, t_g)\Sigma(O_K))$, where $\Sigma\colon K \to \mathbb{R}^g$ is the collection of the g real embeddings of K. For any $\lambda \in P$ the corresponding hermitian form of the polarization is given by $H_\lambda(z, w) = \sum_{i=1}^g \lambda_i z_i \overline{w}_i / \Im t_i$.

Then $\mathcal{H}_g = \mathcal{H}_g^{\mathrm{pol},O_K}$ is the substack which corresponds to principally polarizable abelian schemes, $\mathcal{H}_{g,n} \otimes \mathbb{Q}(\zeta_n)$ is geometrically connected.

We can also construct $\mathcal{H}^{\mathrm{pol}}_{g,\Gamma^0(I)}$ for any ideal I of O_K, but in this case the corresponding $\Phi_{\beta,2}$ isogeny map would map $\mathcal{H}^{\mathrm{pol}}_{g,\Gamma^0(I)}{}^P$ to $\mathcal{H}_g^{\mathrm{pol}^{I\otimes P}}$ [Kie20, §3.4].

5.9 ALGEBRAIC MODULAR FORMS

subsec:mf-ZZ

5.9.1 *Siegel modular forms*

Let $\pi : \mathcal{X}_g \to \mathcal{A}_g$ be the universal abelian variety. The vector bundle

$$\mathcal{H} = \pi_* \Omega^1_{\mathcal{X}_g/\mathcal{A}_g}$$

over $\mathcal{A}_g$, which is dual to $\mathrm{Lie}_{\mathcal{X}_g/\mathcal{A}_g}$, is called the *Hodge bundle*. If ρ is a representation of GL_g, a Siegel modular form of weight ρ is a section of $\rho(\mathcal{H})$; in particular, a scalar-valued modular form of weight k is a section of $\Lambda^g\mathcal{H}^{\otimes k}$. In other words, a Siegel modular form f can be seen as a map

$$(A,\omega)\mapsto f(A,\omega)$$

where A is a point of $\mathcal{A}_g$ and ω is a basis of differential forms on A, with the following property: if $\eta\colon A\to A'$ is an isomorphism, and $r\in\mathrm{GL}_g$ is the matrix of η^* in the bases ω',ω, then $f(A',\omega)=\rho(r)f(A,\omega')$. The link with classical modular forms over $\mathbb{C}$ is the following: if $\tau\in\mathbb{H}_g$, then we let

$$f(\tau)=f(\mathbb{C}^g/(\mathbb{Z}^g+\tau\mathbb{Z}^g),(2\pi i\,dz_1,\dots,2\pi i\,dz_g)).$$

This choice of basis is made so that the q-expansion principle holds [FC90, p. 141]. The canonical line bundle $\mathfrak{h}=\Lambda^g\mathcal{H}$ is ample, so modular forms give local coordinates on $\mathcal{A}_g$.

The canonical line bundle $\mathfrak{h}=\Lambda^g\mathcal{H}$ is ample, and can be used to construct the Satake-Baily-Borel compactification $\mathcal{A}_g^*$ of $\mathcal{A}_g$ over $\mathbb{Z}$. The stack $\mathcal{A}_g^*$ is normal but not smooth, one can also construct smooth toroidal compactifications $\overline{\mathcal{A}}_g$ over $\mathbb{Z}$. If $g>1$, the Koecher principle is still valid over $\mathbb{Z}$, and a scalar modular form defined over $\mathcal{A}_g$ extends to $\mathcal{A}_g^*$ and $\overline{\mathcal{A}}_g$. The boundary components have interpretations in terms of the Fourier coefficients, in term of the Siegel operator or the Fourier-Jacobi development respectively. Finally the q-expansion principle give a convenient way to find the ring of definition of a modular form. For all this and much more, we refer to [FC90, Ch. V].

Let j be a modular function, that is a section of $\mathcal{O}_{\mathcal{A}_g}$. Then if A/k is in the open of definition of j, one can evaluate j at every deformation A_ϵ of A. If t_ϵ is the tangent vector at A to $\mathcal{A}_g$ corresponding to A_ϵ, writing $j(A_\epsilon)=j(A)+dj(\epsilon)\epsilon$ defines an application $dj:\mathrm{Sym}^2T_{0_A}A\to k$ (where we used the Kodaira-Spencer isomorphism). More generally this holds for abelian schemes, so we see that dj is a section of $\mathrm{Sym}^2\mathcal{H}$, in other words a modular form of weight Sym^2.

5.9.2 *Hilbert modular forms*

For the algebraic interpretation of Hilbert modular forms as sections of the Hodge bungle on $\mathcal{H}_g$, the Koecher principle and the q-expansion principle for Hilbert modular forms, we refer to [Cha90, §4] and [Rap78, Thm. 6.7].

More precisely, the Hilbert Hodge bundle $\mathfrak{h}=\pi_*\Omega^1_{\mathcal{X}_g/\mathcal{H}_g}$ is a locally free $\mathbb{Z}_K\otimes\mathcal{H}_g$-module, and Hilbert modular forms of weight χ are sections of the line bundle $\mathfrak{h}^\chi$ where the weights are given by $\chi\in G_{\mathbb{Z}_K}=Res_{\mathbb{Z}_K/\mathbb{Z}}\mathbb{G}_{m,\mathbb{Z}_K}\times\mathbb{Z}_K$ [AG05, Defs. 5.1 and 5.4], [Rap78, §6]. If K' is the normal closure of K, it splits $\mathbb{Z}_K$, and a choice of trivialization of $\mathbb{Z}_K\otimes K'$ induce a splitting of the torus $G_{K'}$, hence a basis of g characters $\chi_1,\dots,\chi_g$. An Hilbert modular form of weight $\chi_1^{a_1}\dots\chi_g^{a_g}$ corresponds to a form of weight $(a_1,\dots a_g)$ in the notations of Section 5.5 [AG05, p. 2].

5.10 THE KODAIRA-SPENCER ISOMORPHISM

The Kodaira-Spencer morphism was first introduced in [KS58]; we refer to [FC90, §III.9] and [And17, §1.3] for more details.

Let $p\colon A\to S$ be a proper abelian scheme, and assume for simplicity that S is smooth. Then, using the Gauss-Manin connection

$$\nabla\colon R^1p_*\Omega_{A/S}\to R^1p_*\Omega_{A/S}\otimes\Omega^1_S,$$

one can define the *Kodaira–Spencer morphism*

$$\kappa\colon T_S\to R^1p_*T_{A/S},$$

where $T_{A/S}$ is the dual of $\Omega^1_{A/S}$. {{ Note that S smooth is enough for our purpose since we will apply this to $\mathcal{A}_g$, or rather to an étale presentation S of $\mathcal{A}_g$). }}

Recall that $\mathrm{Lie}_S A = p_* T_{A/S}$ is the dual of $p_* \Omega^1_{A/S}$, and is canonically identified with $s^* T_{A_S}$ where $s\colon S \to A$ is the zero section [MGE12, Prop. 3.15]. By the projection formula [FGI+05, Thm. 8.3.2], [Stacks, Tag 0943], we have

$$R^1 p_* T_{A/S} = \mathrm{Lie}_S(A) \otimes_{O_S} R^1 p_* O_A.$$

Moreover, $R^1 p_* O_A$ is naturally isomorphic to $\mathrm{Lie}_S(A^\vee)$, where $A^\vee \to S$ is the dual of A. Therefore, we can also write the Kodaira–Spencer map as

$$\kappa\colon T_S \to R^1 p_* T_{A/S} \simeq \mathrm{Lie}_S(A) \otimes_{O_S} \mathrm{Lie}_S(A^\vee).$$

The Kodaira-Spencer map κ is invariant by duality. A polarization $A \to A^\vee$ induces another version of the Kodaira–Spencer map:

$$\kappa\colon T_S \to \mathrm{Sym}^2 \mathrm{Lie}_S(A) = \mathrm{Hom}_{\mathrm{Sym}}(\Omega^1_{A/S}, \Omega^{1\,\vee}_{A^\vee/S}) = \mathrm{Hom}_{\mathrm{Sym}}(\mathrm{Lie}_S(A)^\vee, \mathrm{Lie}_S(A^\vee)).$$

If we apply this construction to the universal abelian scheme $\mathcal{X}_g \to \mathcal{A}_g$ (or rather, the pullback of $\mathcal{X}_g$ to an étale presentation S of $\mathcal{A}_g$), the Kodaira–Spencer map is an isomorphism [And17, §2.1.1]. Its analytification can be described explicitly.

analytic_kodaira

Proposition 5.10.1. *Let V be the trivial vector bundle $\mathbb{C}^g$ on $\mathbb{H}_g$, identified with the tangent space at 0 of the universal abelian variety $A(\tau)$ over $\mathbb{H}_g$. Then the pullback of the Kodaira–Spencer map $\kappa\colon T_{\mathcal{A}_g} \to \mathrm{Sym}^2 \mathrm{Lie}_S \mathcal{X}_g$ by $\mathbb{H}_g \to \mathcal{A}_g^{an}$ is an isomorphism $T_{\mathbb{H}_g} \simeq \mathrm{Sym}^2 V$ given by*

$$\kappa\Big(\frac{1+\delta_{jk}}{2\pi i}\frac{\partial}{\partial \tau_{jk}}\Big) = \frac{1}{(2\pi i)^2}\frac{\partial}{\partial z_j} \otimes \frac{\partial}{\partial z_k}.$$

for each $1 \le j,k \le g$, where δ_{jk} is the Kronecker symbol.

Proof. The fact that the pullback is an isomorphism is [And17, §2.2]. The identification itself can be derived by looking at the deformation of a section s of the line bundle on $\mathcal{X}_g$ giving the principal polarization. {{ Precisely, if $(A, \mathcal{L})$ is a principally polarized abelian variety, and s a non zero section of $\mathcal{L}$, each deformation $(A_\epsilon, \mathcal{L}_\epsilon)$ gives a deformation s_ϵ. }} On $\mathbb{H}_g \times \mathbb{C}^g \to \mathbb{H}_g$, we can take the theta function θ as a section, and its deformation along τ is given by the heat equation [Cvoo, p. 9]:

$$2\pi i(1+\delta_{jk})\frac{\partial \theta}{\partial \tau_{jk}} = \frac{\partial^2 \theta}{\partial z_j \partial z_k}.$$

□

When identifying the tangent space at τ with the symmetric matrices, the action of Sym^2 at a matrix U on the tangent space is given by $M \mapsto MUM^t$. It is then easy to check that this action is indeed compatible with the action of $\mathrm{Sp}_{2g}(\mathbb{Z})$ on τ and U. From Proposition 5.10.1, we recover that derivatives of Siegel modular invariants have weight Sym^2.

To sum up, if $x : \mathrm{Spec}\, k \to \mathcal{A}_g$ is a point represented by a principally polarized abelian variety A/k, we have a canonical isomorphism $T_x \mathcal{A}_g \simeq \mathrm{Sym}^2(T_0(A))$.

In the Hilbert case, the Kodaira–Spencer isomorphism is as follows.

:kodaira_hilbert

Proposition 5.10.2. *Let $A \to S$ be an abelian scheme in $\mathcal{H}_g$. Then we have canonical isomorphisms*

$$T_A(\mathcal{H}_g) \simeq \mathrm{Hom}_{\mathbb{Z}_K \otimes O_S}(\mathrm{Lie}(A)^\vee, \mathrm{Lie}(A^\vee)) = \mathrm{Lie}(A^\vee) \otimes_{\mathbb{Z}_K \otimes O_S} \mathrm{Lie}(A) \otimes_{\mathbb{Z}_K} \mathbb{Z}_K^\vee.$$

Proof. Combine [Rap78, Prop. 1.6] with [Rap78, Prop. 1.9]. □

Remark 5.10.3. By the above Propositions of [Rap78], the functor of formal deformations of RM abelian schemes with or without polarization are the same; in other words, all deformations which preserve the real multiplication automatically preserve the polarization. By contrast for an abelian scheme with a separable polarization, the formal functor of deformations (without polarization) is represented by $W(k)[[[t_{11}, \dots, t_{gg}]]$[Oor71b, Thm. 2.2.1] and the one with polarization by $W(k)[[[t_{11}, \dots, t_{gg}]]/(t_{ij} - t_{ji})$ [Oor71b, Thm. 2.3.3 and Rem. p. 288].

Proposition 5.10.2 shows that for Hilbert–Blumenthal stacks, the deformation map is actually represented by an element of $\mathbb{Z}_K \otimes O_S$ rather than by a matrix in O_S. The action of the Hilbert embedding on tangent spaces is also easy to describe.

embedding

Proposition 5.10.4. *Let A be a k-point of $\mathcal{H}_g$. Then the map $T_A(\mathcal{H}_g) \to T_A(\mathcal{A}_g)$ induced by the forgetful functor fits in the commutative diagram*

$$\begin{array}{ccc} T_A(\mathcal{H}_g) & \longrightarrow & T_A(\mathcal{A}_g) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathbb{Z}_K \otimes O_k}(\mathrm{Lie}(A)^\vee, \mathrm{Lie}(A^\vee)) & \longrightarrow & \mathrm{Hom}_{\mathrm{Sym}}(\mathrm{Lie}(A)^\vee, \mathrm{Lie}(A^\vee)). \end{array}$$

where the vertical arrows are the Kodaira–Spencer isomorphisms. {{ As a reformulation: the forgetful functor $\mathcal{H}_g \to \mathcal{A}_g$ induces the following map on tangent spaces. If $A \to k$ represents the geometric point $\mathrm{Spec}\, k \to \mathcal{H}_g$, then $T_{A,\mathcal{H}_g} \to T_{A,\mathcal{A}_g}$ is given by the natural map $\mathrm{Lie}(A) \otimes_{\mathbb{Z}_K \otimes O_k} \mathrm{Lie}(A) \otimes_{\mathbb{Z}_K} \mathbb{Z}_K^\vee \simeq \mathrm{Hom}_{\mathbb{Z}_K \otimes O_k}(\mathrm{Lie}(A)^\vee, \mathrm{Lie}(A^\vee)) \to \mathrm{Sym}^2 \mathrm{Lie}(A) \simeq \mathrm{Hom}_{\mathrm{Sym}}(\mathrm{Lie}(A)^\vee, \mathrm{Lie}(A^\vee))$. }}

Proof. The bottom arrow is well-defined: $\mathrm{Lie}(A)$ is a projective $\mathbb{Z}_K \otimes O_k$-sheaf of rank 1, so its image in $\mathrm{Hom}_{O_k}(\mathrm{Lie}(A)^\vee, \mathrm{Lie}(A^\vee))$ obtained by forgetting the $\mathbb{Z}_K$-structure is automatically symmetric. We omit the proof of commutativity. □

Combining Proposition 5.10.4 with the analytic description of the Kodaira–Spencer in the Siegel case (Proposition 5.10.1) and the analytic description of the forgetful map (Section 5.5), we obtain the following analytic description of the Kodaira–Spencer isomorphism in the Hilbert case.

Corollary 5.10.5. *The pullback of $\kappa\colon T_{\mathcal{H}_g} \to \mathrm{Sym}^2 \mathit{Lie}_S X_g$ by $\mathbb{H}_1^g \to \mathcal{H}_g^{an}$ is given by*

$$\kappa\Big(\frac{1}{\pi i}\frac{\partial}{\partial t_j}\Big) = \frac{1}{(2\pi i)^2}\frac{\partial}{\partial z_j} \otimes \frac{\partial}{\partial z_j}$$

for every $1 \le j \le g$.

6 MODULI SPACES VIA THETA FUNCTIONS

CONTENTS

Planned topics

6.1 EQUATIONS FOR THE MODULI

Explicit structure of moduli spaces with level structure via Mumford's theory of algebraic theta functions [Mum66; Mum67a; Mum67b; Mum69; Mum91; Kem89a].

6.2 EQUATIONS FOR THE UNIVERSAL ABELIAN SCHEME

Equations for abelian varieties [Mum66; Kem89a; Kem89b; Kem90], equations for Kummer varieties [Kem92] relation between projective normality of Kummer varieties and surjectivity of the multiplication map [Koi76; Kem88].

6.3 THETA AS MODULAR FORMS

Algebraic interpretation of theta as modular forms. Determinant (line) bundle [Mor85, Appendice 2], [FC90, Theorem 5.1]. Improved bounds via analytic methods [Kou00] or algebraic methods [Pol00; MR08]. Applications to Riemann's functional equation [Mor90; Can20; Can16].

Curiously, I have not seen a direct proof that the canonical line bundle $\mathcal{L}$ constructed by Mumford for embedding the moduli spaces of abelian variety with a level $(n, 2n)$ structure satisfy $\mathcal{L}^2 = \mathcal{H}$. (Analytic interpretation: θ constants of level n are analytic modular forms of level $\Gamma(n, 2n)$). This is easily derived from [Can16, Theorem 4.2.1], but should be simpler to prove directly.

7 MODULI SPACE OF CURVES

CONTENTS

PLANNED TOPICS

7.1 COMPACTIFICATION

Deligne-Mumford: construction of $\overline{\mathcal{M}}_g$ [DM69]. Semistable curves, compact curves.

7.2 THE TORELLI MORPHISM

The torelli morphism $\mathcal{M}_g \to \mathcal{A}_g$ is an injection. Cf [Zur09] for the construction.

On algebraic stack, its restriction to $\mathcal{M}_g \setminus \mathcal{H}_g$ is unramified, and also its restriction on $\mathcal{H}_g$ is unramified [VA09]. Unramified locus on the coarse space: [OS79; Ric20; Lan20]

Extension to compact curves, and to the compactifications $\overline{\mathcal{M}}_g \to \overline{\mathcal{A}}_g$ (warning: Torelli is no longer injective) [MO11].

7.3 TEICHMULLER MODULAR FORMS.

CURRENT DRAFT VERSION

7.4 THE TORELLI MORPHISM

The link between modular forms and covariants comes from the Torelli morphism

$$\tau_g : \mathcal{M}_g \to \mathcal{A}_g$$

where $\mathcal{M}_g$ denotes the moduli stack of smooth curves of genus g. Let $\mathbb{C}_g \to \mathcal{M}_g$ denote the universal curve; then the pullback $\tau_g^* \mathcal{H}$ of the Hodge bundle by the Torelli morphism is $\pi_* \Omega^1 \mathbb{C}_g / \mathcal{M}_g$, with both having canonical action by GL_g. In other words a Siegel modular form of weight ρ induces a Teichmuller modular form of weight ρ.

The isomorphism $T_0 \operatorname{Jac} C \simeq H^1(C, O_C) \simeq H^0(C, \Omega_C)$ for a curve C shows that the pullback $\tau_g^* \mathcal{H}$ of $\mathcal{H}$ by the Torelli morphism $\tau_g : \mathcal{M}_g \to \mathcal{A}_g$ is indeed given by the bundle $\pi_* \Omega^1 \mathbb{C}_g / \mathcal{M}_g$, with both having canonical action by Gl_g. In other words a Siegel modular form of weight ρ induces a Teichmuller modular form of weight ρ.

The Torelli morphism is radicial on $\mathcal{M}_g$, and unramified when restricted to $\mathcal{M}_g \setminus \mathcal{H}_g$ and to $\mathcal{H}_g$, where $\mathcal{H}_g$ is the locus of hyperelliptic curves. If $\overline{\mathcal{M}}_g$ is the moduli space of stable curves of genus g, then the Torelli morphisms extends to morphisms (no longer injective) $\mathcal{M}_g^* \to \mathcal{A}_g$ and $\overline{\mathcal{M}}_g \to \overline{\mathcal{A}}_g$, where $\mathcal{M}_g^*$ denotes the locus of stable curves.

8 MODULI SPACES OF SMALL DIMENSION

CONTENTS

PLANNED TOPICS

8.1 MODULI OF ELLIPTIC CURVES

8.2 MODULI OF CURVES OF GENUS 2 AND ABELIAN SURFACES

sec:ag2

8.2.1 *Moduli of hyperelliptic curves of genus* 2

The coarse moduli of M_2 is $(\operatorname{Proj} \mathbb{Z}[J_2, J_4, J_6, J_8, J_{10}])_{J_{10}} \simeq \mathbb{Z}[y_1, y_2, y_3, y_4]^{\mu_5}$ [Igu60]. Smooth points, automorphisms.

Description of twists over a finite field [CQ05; CNP05].

Links between the J-invariants and the Igusa-Clebsh invariants I_2, I_4, I_6, I_{10}, link with modular forms. The different type of curve equations: (long) Weierstrass equation, Artin-Schreier equation in characteristic two (type $(1,1,1)$, $(3,1)$, (5) and link with the 2-rank), Igusa's universal normal form, absolute invariants.

8.2.2 *Moduli of abelian surfaces*

Description of A_2 using the fact that all principally polarised abelian surface is a generalised Jacobian [Liu93]. Generators of modular forms over $\mathbb{C}$ [Igu62], with levels [Igu64], and over $\mathbb{Z}$ [Igu79].

8.2.3 *Real multiplications*

Humbert varieties, generalised Humbert [Kan19b; Kan19a].

8.2.4 Examples of Hilbert surface

Over $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$, explicit invariants (Gundlach [Gun63; Gun65]).

Current draft version

For now, this draft version is essentially extracted from [KPR20; MR22].

8.3 Covariants of hyperelliptic curves of genus 2

8.3.1 Covariants

def:cov **Definition 8.3.1.** Denote by $k_6[x]$ the space of polynomials of degree at most 6. Let $\rho\colon \mathrm{GL}_2(k) \to \mathrm{GL}(V)$ be a finite-dimensional holomorphic representation of $\mathrm{GL}_2(k)$. A *covariant*, or *polynomial covariant*, of weight ρ is a map

$$C\colon k_6[x] \to V$$

which is polynomial in the coefficients, and such that the following transformation rule holds: for every $r \in \mathrm{GL}_2(k)$ and $W \in k_6[x]$,

$$C(\det{}^{-2}\,\mathrm{Sym}^6(r)\,W) = \rho(r)\,C(W).$$

If $\dim V \geq 2$, then C is said to be *vector-valued*, and otherwise *scalar-valued*. A *fractional covariant* is a map satisfying the same transformation rule which is only required to have a fractional expression in terms of the coefficients.

In characteristic 0, let f and g be binary forms of degrees n and m. To compute covariants of sextic forms, Clebsh introduced [Cle72] the *Ueberschiebung* operation defined by :

$$(fg)_k = \frac{(m-k)!(n-k)!}{m!n!}\left(\frac{\partial f}{\partial x}\frac{\partial g}{\partial y} - \frac{\partial f}{\partial y}\frac{\partial g}{\partial x}\right)^k$$

where in the binomial expression $\left(\frac{\partial f}{\partial x}\right)^r\left(\frac{\partial f}{\partial y}\right)^s$ means $\frac{\partial^{r+s} f}{\partial x^r \partial y^s}$.

Using the Ueberschiebung, Clebsh showed that the algebra of scalar covariants is generated by fives covariants denoted A, B, C, D and R of respective degrees 2, 4, 6, 10 and 15 [Cle72]. Since R^2 admits a polynomial expression in function of A, B, C and D then these four invariants suffice to characterize the linear equivalence classification of sextic forms. They are called *Clebsh invariants*.

Now let's consider a hyperelliptic model a of genus 2 curves $C\colon y^2 = f(x) = u_0x^6 + u_1x^5 + \ldots + u_5x + u_6$ and $\alpha_1, \cdots, \alpha_6$ the distinct roots of f. If we denote by (ij) the difference $(\alpha_{\sigma(i)} - \alpha_{\sigma(j)})$ such that :

$$I_2 = u_0^2 \sum_{15} (12)^2(34)^2(56)^2\ ,$$

$$I_4 = u_0^4 \sum_{10} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2\ ,$$

$$I_6 = u_0^6 \sum_{60} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2\ ,$$

$$I_{10} = u_0^{10} \prod_{i<j} (\alpha_i - \alpha_j)^2$$

where every α_i appears in each expression m times equal to the power of u_0. Then J.Igusa has shown in [Igu60, p. 620] that I_2, I_4, I_6 and I_{10} are homogenous invariants of degree 2, 4, 6 and 10 with integers coefficients . They are called *Igusa-Clebsh invariants* because of the following relations with Clebsh invariants :

$$
\begin{aligned}
I_2 &= -120A\,,\\
I_4 &= -720A^2 + 6750B\,,\\
I_6 &= 8640A^3 - 108000AB + 202500C\,,\\
I_{10} &= -62208A^5 + 972000A^3B + 1620000A^2C - 3037500AB^2 - 6075000BC - 4556250D.
\end{aligned}
$$

8.3.2 *Algebraic interpretation*

Over $\mathbb{Z}[1/2]$, the moduli stack $\mathcal{M}_2$ of hyperelliptic curves is identified with the moduli stack of nondegenerate binary forms of degree 6. Let $V = \mathbb{Z}x \oplus \mathbb{Z}y$, let $X = \det^{-2} V \otimes \mathrm{Sym}^6 V$, and let U be the open locus determined by the discriminant. Then $U \to \mathcal{M}_2$ is naturally identified with the Hodge frame bundle on $\mathcal{M}_2$: in other words, U is the moduli space of genus 2 hyperelliptic curves $\pi : C \to S$ endowed with a rigidification $\mathcal{O}_S^{\oplus 2} \simeq \pi_*\Omega^1_{C/S}$. In this identification, we send the binary form $f(x,y)$ to the curve $v^2 = f(u,1)$ with a basis of differential forms given by $(u\,du/v, du/v)$ [CFv17, §4]. The natural action of GL_2 on the Hodge bundle corresponds to the action of GL_2 on U that we describe in Definition 8.3.1. This shows why a Siegel modular form of weight ρ pulls back to a fractional covariant of weight ρ, at least over $\mathbb{Z}[1/2]$. In fact, one can show, by considering suitable compactifications, that a Siegel modular form pulls back to a polynomial covariant over any ring R in which 2 is invertible. Using Igusa's universal form [Igu60, §2], one can also use binary forms of degree 6 to describe the moduli stack of genus 2 curves even in characteristic two.

8.3.3 *Arithmetic invariants*

sec:artinv

We present Igusa's results [Igu60] about the construction of the moduli of genus 2 curves. In characteristic 0 the knowledge of the quadruplet (A,B,C,D) (equivalently I_{2i}'s) in the weighted projective space corresponds exactly to a genus 2 curve in the coarse moduli space $\mathcal{M}$.

However those invariants have bad reduction in characteristic 2. In fact, the Clebsh invariants (A,B,C,D) have bad reduction in characteristic $2,3,5$, and the Igusa-Clebsh invariants only have bad reduction in characteristic $2,3$ (their reduction is well defined, but they do not classify genus 2 curves anymore).

Igusa shows that hyperelliptic curves of genus 2 admit a *universal normal form* [Igu60, p. 617]

$$XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0$$

such that in characteristic different from 2, the Weierstrass points of the associated sextic form are the roots of the equation :

$$(1 + aX + bX^2)^2 - 4X^3(c + dX + X^2) = 0.$$

Igusa defines the following integral arithmetical invariants:

$$
\begin{aligned}
J_2 = 2^{-3}I_2, \quad J_4 = 2^{-5}3^{-1}(4J_2^2 - I_4),\\
J_6 = 2^{-6}3^{-2}(8J_2^3 - 160J_2J_4 - I_6),\\
J_8 = 2^{-2}(J_2J_6 - J_4^2), \quad J_{10} = 2^{-12}I_{10}.
\end{aligned}
$$

as arithmetic invariants associated to the curves of equation :

$$XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0$$

[Igu60, p. 621]. So every J_{2i} reduces well modulo 2, and $J_{10} \neq 0$.

Indeed, J_{10} encode the fact that C is smooth (for instance in characteristic different from 2, I_{10} is the discriminant), so is invertible on $\mathcal{M}$, since a curve is smooth over its base. If we express J_{2i}, as polynomials in a, b, c, d, we get a quantity that depends only on the bi-rational class of the genus 2 curves. In characteristic different from 2, it

is a consequence of the invariance property of J_{2i}, and in the characteristic 2, it is a consequence of the explicit relations Equations (8.5) to (8.7).

Reciprocally Igusa shows that from the quintuplet $(J_2, J_4, J_6, J_8, J_{10})$, with $J_{10} \neq 0$, one can construct a normal form with arithmetic invariants those J_{2i}'s (possibly under a field extension) [Igu60, §3, §5]. For the characteristic different from two this can be done algorithmically using the Igusa-Clebsh construction [Mes91] and in characteristic 2 it is a consequence of the three relations from Section 8.3.3 and Equation (8.5) below. Also by considering the relation $J_2J_6 - J_4^2 - 4J_8 = 0$ the invariant J_8 can be disregarded in characteristic different from 2 (but it is crucial in characteristic 2).

Let us consider the graded ring generated over $\mathbb{Z}$ by J_{2i}, $i = 1, 2, 3, 4, 5$ and localized at J_{10}. We denote by $\mathcal{R}$ the integral domain generated by its homogeneous elements of degree zero. Then Igusa shows [Igu60, §7] that $\mathcal{R}$ is generated over $\mathbb{Z}$ by the elements of the form $J_2^{e_1}J_4^{e_2}J_6^{e_3}J_8^{e_4}J_{10}^{-e_5}$ with e_i a non negative integers verifying $e_1 + 2e_2 + 3e_3 + 4e_4 = 5e_5$.

In particular, if y_1, y_2, y_3 and y_4 are an independent variables with $4y_4 = y_1y_3 - y_2^2$, then the correspondence :

$$J_2^{e_1}J_4^{e_2}J_6^{e_3}J_8^{e_4}J_{10}^{-e_5} \longmapsto y_1^{e_1}y_2^{e_2}y_3^{e_3}y_4^{e_4}$$

from $\mathcal{R}$ to $\mathbb{Z}[y_1, y_2, y_3, y_4]^{\mu_5}$ defines an isomorphism between $\mathcal{R}$ and the elements of $\mathbb{Z}[y_1, y_2, y_3, y_4]$ that are invariant under the transformation $y^i \to \zeta_5^i y_i$ for $i = 1, 2, 3, 4$, where ζ_5 is a primitive fifth root of unity.

By considering the condition $J_2J_6 - J_4^2 - 4J_8 = 0$, Igusa shows that the monoid of the powers of e_i's appearing in the elements of $\mathbb{Z}[y_1, y_2, y_3, y_4]^{\mu_5}$ is generated by ten elements (only eight are needed in characteristics different form 2) [Igu60, §7]. Therefore $\mathcal{R}$ is generated by ten elements called γ_i in [GL12]:

$$\gamma_1 = J_2^5/J_{10}, \quad \gamma_2 = J_2^3J_4/J_{10}, \quad \gamma_3 = J_2^2J_6/J_{10}, \quad \gamma_4 = J_2J_8/J_{10},$$
$$\gamma_5 = J_2J_6/J_{10}, \quad \gamma_6 = J_4J_8^2/J_{10}^2, \quad \gamma_7 = J_6^2J_8/J_{10}^2, \quad \gamma_8 = J_6^5/J_{10}^3,$$
$$\gamma_9 = J_6J_8^3/J_{10}^3, \quad \gamma_{10} = J_8^5/J_{10}^4.$$

In summary, we have:

thm:igusa

Theorem 8.3.2. *Let μ_5 be the group of the fifth root of unity, the moduli space $\mathcal{M}_2$ of the genus 2 curves is isomorphic to* Proj $(\mathbb{Z}[J_2, J_4, J_6, J_8, J_{10}])_{(J_{10})}$ = Spec $(\mathbb{Z}[y_1, y_2, y_3, y_4]^{\mu_5})$ = Spec $(\mathbb{Z}[\gamma_1, \dots, \gamma_{10}])$ *[Igu60, Theorem 2] (with a weighted grading on the* Proj*). And the variety $\mathcal{M}_2$ can be embedded as a subvariety of an affine space over $\mathbb{Z}$ of dimension ten and not less than ten [Igu60, Theorem 6].*

Corollary 8.3.3. *Let $\gamma_i(C)$ be the evaluation of γ_i at a representative model of C.*

- *If C is a curve defined over a number field $\mathbb{K}$, then C has good reduction modulo a prime $\mathfrak{p}$ of $\mathbb{K}$ if and only if :*
$$ord_{\mathfrak{p}}(\gamma_i(C)) \geq 0, \quad i = 1, \cdots, 10.$$
- *And if C_1 and C_2 are curves over $\overline{\mathbb{k}}$, then [Igu60, Corollary p.632] :*
$$C_1 \simeq C_2 \iff (\gamma_1(C_1), \cdots, \gamma(C_1)) = (\gamma_1(C_2), \cdots, \gamma(C_2))$$
$$\iff (J_2(C_1) : J_4(C_1) : J_6(C_1) : J_8(C_1) : J_{10}(C_1)) = (J_2(C_2) : J_4(C_2) : J_6(C_2) : J_8(C_2) : J_{10}(C_2))$$
(with the weighted gradings).

8.3.4 *The case of characteristic* 2

In characteristic 2, a genus 2 curve can also be defined via an Artin-Schreier equation: $y^2 - y = R(x)$, where R is a rational function in x with pole divisors. The isomorphism classes of these curves are in bijection with the orbits of $R(x)$ under the double actions by the Artin-Schreier group $AS(\mathbb{k}(x))$ and the linear projective group $PGL_2(\mathbb{k})$ [Igu60; GNP]. From the ramifications of the Weierstrass points one deduces three types $(1, 1, 1)$, $(3, 1)$, (5) of birationnally equivalence classes defined by the following affine equations [Igu60, p. 618]:

$$Y^2 - Y = \begin{cases} \alpha X + \beta X^{-1} + \gamma(X-1)^{-1}, & \alpha\beta\gamma \neq 0 \qquad (1,1,1) \\ X^3 + \alpha X + \beta X^{-1}, & \beta \neq 0 \qquad (3,1) \\ X^5 + \alpha X^3, & \qquad (5) \end{cases}$$

8.3.5 Covariants and modular forms

TODO: in these formula the χ_i are not normalised in the same way.

structure

Theorem 8.3.4 ([Igu62; Igu67]). *The graded $\mathbb{C}$-algebra of scalar-valued even-weight Siegel modular forms in genus 2 is generated by four algebraically independent elements $\psi_4, \psi_6, \chi_{10}$, and χ_{12} of respective weights 4, 6, 10, 12, and q-expansions*

$$\begin{aligned}
\psi_4(\tau) &= 1 + 240(q_1 + q_3) \\
&\quad + (240q_2^2 + 13440q_2 + 30240 + 13340q_2^{-1} + 240q_2^{-2})q_1q_3 + O(q_1^2, q_3^2), \\
\psi_6(\tau) &= 1 - 504(q_1 + q_3) \\
&\quad + (-504q_2^2 + 44352q_2 + 166320 + 44352q_2^{-1} - 504q_2^{-2})q_1q_3 + O(q_1^2, q_3^2), \\
\chi_{10}(\tau) &= (q_2 - 2 + q_2^{-1})q_1q_3 + O(q_1^2, q_3^2), \\
\chi_{12}(\tau) &= (q_2 + 10 + q_2^{-1})q_1q_3 + O(q_1^2, q_3^2).
\end{aligned}$$

The graded $\mathbb{C}$-algebra of scalar-valued Siegel modular forms in genus 2 is

$$\mathbb{C}[\psi_4, \psi_6, \chi_{10}, \chi_{12}] \oplus \chi_{35}\mathbb{C}[\psi_4, \psi_6, \chi_{10}, \chi_{12}]$$

where χ_{35} is a modular form of weight 35 and q-expansion

$$\chi_{35}(\tau) = q_1^2q_3^2(q_1 - q_3)(q_2 - q_2^{-1}) + O(q_1^4, q_3^4).$$

We can express these modular forms in term of theta constants. Let $\mathcal{D} = \{0, 1, 2, 3, 4, 6, 8, 9, 12, 15\}$, and define:

$$h_4 = \sum_{i \in \mathcal{D}} \theta_i^8, \quad h_6 = \sum_{60\ tuples\ (i,j,k) \in \mathcal{D}^3} (\theta_i\theta_j\theta_k)^4$$

$$h_{10} = \prod_{i \in \mathcal{D}} \theta_i^2, \quad h_{12} = \sum_{15\ tuples\ (i,j,k,l,m,n) \in \mathcal{D}^6} (\theta_i\theta_j\theta_k\theta_l\theta_m\theta_n)^4$$

and $h_{16} = \frac{1}{3}(h_{12}h_4 - 2h_6h_{10})$. These are modular forms of weight i, and we have:

$$h_4 = 2^2\psi_4, \quad h_6 = 2^2\psi_6, \quad h_{10} = -2^{14}\chi_{10} \quad \text{and} \quad h_{12} = 2^{17}3\chi_{12}.$$

where ψ_k are the Eisenstein series of weight $k \geq 4$ defined by:

$$\psi_k(\Omega) = \sum_{\gamma \in \Gamma_2} \det(C\Omega + D)^{-k}$$

and χ_{10}, χ_{12} are cusp forms, expressed in function of ψ_k with $k \in \{4, 6, 10, 12\}$.

Igusa covariants:

$$\begin{aligned}
4\ \mathrm{Cov}(\psi_4) &= I_4, \\
4\ \mathrm{Cov}(\psi_6) &= I_6', \\
2^{12}\ \mathrm{Cov}(\chi_{10}) &= I_{10}, \\
2^{15}\ \mathrm{Cov}(\chi_{12}) &= I_2I_{10}, \\
2^{37}3^{-9}5^{-10}\ \mathrm{Cov}(\chi_{35}) &= I_{10}^2R.
\end{aligned}$$

A standard set of invariants used for computation of class or modular polynomials was $I_2^5/I_{10}, I_2^3I4/I_{10}, I_2^2I_6/I_{10}$, the corresponding U is $I_2 \neq 0$. To reduce the size of these polynomials, Streng introduced the absolute invariants $I_4I_6'/I_{10}, I_2I_4^2/I_{10}, I_4^5/I_{10}^2$ where $I_6' = 1/2(I_2I_4 - 3I_6)$. The corresponding U is given by $I_4 \neq 0$. They correspond (up to a constant) to the modular forms defined in terms of theta constants h_4, h_6, h_{10}, h_{12}.

Streng's version of Igusa invariants in terms of modular forms:

$$j_1 = 2^{-8}\frac{\psi_4\psi_6}{\chi_{10}}, \quad j_2 = 2^{-5}\frac{\psi_4^2\chi_{12}}{\chi_{10}^2}, \quad j_3 = 2^{-14}\frac{\psi_4^5}{\chi_{10}^2}.$$

8.3.6 Absolute invariants

In characteristic different from 2

One can define absolute invariants [CQ05, § 1], hence coordinates on the moduli space using the invariants J_{2i}'s. Knowing that the invariant J_{10} defines the discriminant of the curve, so is not null, we obtain that:

- The class of genus 2 curves with a nonzero J_2, is an open set of $\mathcal{M}_2$ on which we have the tuple of absolute invariants : $\left(J_2^5/J_{10}, J_2^3J_4/J_{10}, J_2^2J_6/J_{10}\right)$.
- The genus 2 curves that annihilate in J_2 with a nonzero J_4, is a subspace of $\mathcal{M}_2$ where coordinates can be defined by : $\left(0, J_4^5/J_{10}^2, J_4J_6/J_{10}\right)$.
- The others curves lie in set with coordinates defined by : $\left(0,\ 0, J_6^5/J_{10}^3\right)$.

Then the set of points of $\mathcal{M}_2 \otimes \Bbbk$ is in bijection with the set of tuples defined previously, so in bijection with $\mathbb{A}^3_{\Bbbk}$. In other words, these invariants (k_1, k_2, k_3) on the above stratification are optimal.

In characteristic 2

We recall that every hyperelliptic curves of genus 2 is birationally equivalent to one of the three following types according to the number and the degree of the ramified Weierstrass points:

$$Y^2 - Y = \begin{cases} \alpha X + \beta X^{-1} + \gamma (X-1)^{-1}, & (1,1,1) \\ X^3 + \alpha X + \beta X^{-1}, & (3,1) \\ X^5 + \alpha X^3, & (5) \end{cases}$$

When $\Bbbk$ has q elements the number $\overline{\Bbbk}$-isomorphism classes of smooth projective curves of genus two defined over $\Bbbk$ is given in the following table according to the type [GNP, Th 20]:

tab:table

Type	Number
(1,1,1)	$q^3 - q^2$
(3,1)	$q^2 - q$
(5)	q

Let's consider the normal form equation :

$$XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0.$$

sym_funct1

If ab is different from 0, we get three Weierstrass points; it corresponds to the type $(1,1,1)$. After a technical variable change in [Igu60, §3], one can obtain :

$$\alpha = ab^{-3}, \tag{8.1}$$
$$\beta = a^{-3}b\xi^{-2}\left(c + \xi^{-2} + a(c\xi + d + \xi^{-1})^{1/2}\right), \tag{8.2}$$
$$\gamma = a^{-3}b\eta^{-2}\left(c + \eta^{-2} + a(c\eta + d + \eta^{-1})^{1/2}\right) \tag{8.3}$$

in which $\xi + \eta = a$, $\eta\xi = b$;
But if a or b is nonzero and $ab = 0$, it corresponds the type $(3,1)$; and if $a \neq 0$ and $b = 0$, one can transform :

$$XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0$$

into

$$Y^2 - Y = X^3 + \alpha X + \beta X^{-1}$$

ym_funct2

with

$$\alpha = a^{5/3}\left(a^{-3}c + (a^{-5} + a^{-4}d)^{1/2}\right), \quad \beta = a^{-5/3}\left(a^{-5} + a^{-3}c + (a^{-5} + a^{-4}d + a^{-3}c)^{1/2}\right). \tag{8.4}$$

If $b \neq 0$ and $a = 0$, we obtain α, β in terms of b, c, d via a more complicated expressions for which we refer to Igusa. The type (5) corresponds to $a = b = 0$ and the associated normal form $XY^2 + Y + X^2(c + dX + X^2) = 0$ can be transformed into $Y^2 - Y = X^5 + \alpha X^3$ with $\alpha = c$.

The open set $\mathcal{M}_2[J_2^{-1}] \otimes \Bbbk$ describes in $\mathcal{M} \otimes \Bbbk$, the curves birationaly equivalent to a curve of type $(1,1,1)$. It is characterized by the non vanishing of J_2 modulo 2, and can be defined using the following three absolute arithmetic invariants: $\mathfrak{a}_1 = J_4/J_2^2$, $\mathfrak{a}_2 = J_8/J_2^4$ and $\mathfrak{a}_3 = J_{10}/J_2^5$. Indeed one can recover these invariants from the coefficients of the normal form using the following relation [Igu60, §3]:

$$\left\{ \begin{array}{ccc} \alpha^2 + \beta^2 + \gamma^2 & = & J_4/J_2^2, \\ \alpha^2\beta^2\gamma^2 & = & J_{10}/J_2^5, \\ \alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2 & = & J_8/J_2^4 + (J_4/J_2^2)^3 + (J_4/J_2^2)^4 \end{array} \right. \tag{8.5}$$

{abcd1}

And Igusa shows in [Igu60, §2] that birational invariants are given by the three standard symmetric invariants: $\alpha + \beta + \gamma, \alpha\beta + \beta\gamma + \gamma\alpha, \alpha\beta\gamma$, they are also used by Cardona and al. in [GNP, §2]: Although they are ramified over the symmetric invariants, there is one important advantage to the three invariants $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$: they come from modular functions over $\mathbb{C}$ and are actually defined over $\mathbb{Z}$. By contrast, the symmetric invariants do not lift to modular forms (without characters) in characteristic 0. More precisely, it is proven in [MR22, Theorem 2.4] that these invariants $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$ describe $\mathcal{M}[J_2^{-1}]$ over $\mathbb{Z}$. In particular, over $\mathbb{Z}_2$ these invariants describe the open set $\mathcal{M}[J_2^{-1}]$ of $\mathcal{M}$ that reduces to $\mathcal{M}_2[J_2^{-1}] \otimes \Bbbk$ modulo 2, in other words of curves with good reduction modulo 2, and whose reduction is of type $(1,1,1)$.

The type $(3,1)$ is characterized by $J_2 = 0$ and the non-vanishing of J_6 over $\Bbbk$, this corresponds to a closed subscheme of $\mathcal{M}_2[J_6^{-1}] \otimes \Bbbk$, hence a locally closed subscheme in $\mathcal{M}_2 \otimes \Bbbk$, of curves birationally equivalent to that type. Coordinates on this subscheme are defined using the following tuple of absolute invariants: $(0, J_8J_{10}/J_6^3, J_{10}^3/J_6^5)$. Indeed from the equation $(3,1)$, one recovers this tuple using:

$$\left\{ \begin{array}{ccc} \alpha^6 & = & J_8^{3/4}/J_6^1, \\ \beta^6 & = & J_{10}^3/J_6^5, \\ \alpha^2\beta^2 & = & J_8^{1/4}J_{10}/J_6^2. \end{array} \right. \tag{8.6}$$

{abcd2}

And birational invariants are given by $\alpha^3, \alpha\beta$ [Igu60, §2].

The type (5) is characterized by $J_2 = J_6 = 0$. The corresponding closed subset of $\mathcal{M} \otimes \Bbbk$, can be defined using the tuple $(0, 0, J_8^5/J_{10}^4)$ of invariants. And the following relation holds :

$$\left\{ \ \alpha^{10} = J_8^{5/4}/J_{10}. \right. \tag{8.7}$$

{abcd3}

And α^5 is a birational invariant [Igu60, §2].

From this discussion, we see that the invariants $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3) = (J_4/J_2^2, J_8/J_2^4, J_{10}/J_2^5)$ when $J_2 \neq 0$, $(0, J_8J_{10}/J_6^3, J_{10}^3/J_6^5)$ when $J_2 = 0, J_6 \neq 0$, and $(0, 0, J_8^5/J_{10}^4)$ induces a bijection between the set of points of $\mathcal{M}_2 \otimes \Bbbk$ and $\mathbb{A}^3_{\Bbbk}$, hence are optimal. Indeed the above formula show how to recover α, β, γ from these invariants.

9 COMPLEX MULTIPLICATION

CONTENTS

clabapoly

PLANNED TOPICS

9.1 THE FUNDAMENTAL THEOREM OF COMPLEX MULTIPLICATION

[Milo6b; Milo7].

9.2 CM LIFTING

A CM abelian variety is defined over a number field in characteristic zero, and is p-isogenous to an abelian variety defined over a finite field in characteristic p (Grothendieck [Oor73], and [Yu04b] for an elementary proof).

Algorithmic survey: [ER13].

CURRENT DRAFT VERSION

References for this e [Milo6b; Str10] See also [ER13] for algorithmic aspects.

9.3 CM FIELDS AND THE SHIMURA CLASS GROUP

Let K be a CM field, K_0 be its real subfield. So K_0 is a totally real field of degree g and K/K_0 is an imaginary quadratic extension. There are g real embeddings $\phi_1, \dots, \phi_g$ of K_0, which each split into 2 complex embedding $\Phi_i, \overline{\Phi}_i$. A CM type Φ is a choice of one among $\{\Phi_i, \overline{\Phi}_i\}$ for each i. Two CM types are said to be equivalent if they differ by an automorphism of K (acting on the righ), in particular Φ is equivalent to $\overline{\Phi}$. A CM pair (K, Φ) is said to be primitive if it is not an induced by a smaller CM field.

An abelian variety A/k (k of characteristic 0) has complex multiplication by O_K with CM type Φ if there is an embedding $O_K \to \mathrm{End}(A)$ such that the action of O_K on T_0A is diagonal induced by the CM type. If A is absolutely simple, (K, Φ) is primitive.

A CM type Φ induce the type trace Tr_Φ and type norm N_Φ (the trace and product respectively of the elements of Φ). If K'/K is an extension, we will denote by $N_{K',\Phi}$ or simply still N_Φ the function $N_\Phi \circ N_{K'/K}$. The field generated over $\mathbb{Q}$ by the type traces of K is also a CM field, called the reflex CM field K^r, and the CM type Φ induces a reflex CM type Φ^r on K^r (hence a reflex type norm and type trace). The CM pair (K^r, Φ^r) is primitive, and its reflex under Φ^r is K if (K, Φ) is primitive. If we let L a Galois closure of K, then K^r may also be described as the subfield invariant under all automorphisms of L leaving Φ invariant (when acting on the left). Even if K is primitive, the reflex K^r may be of different dimension. This does not happen if $g \leq 2$. Changing the CM type conjugates K^r.

The Shimura class group is given by

$$\mathfrak{C} = \{(\mathfrak{a}, u) : \mathfrak{a} \text{ a fractional ideal of } O_K, \mathfrak{a}\bar{\mathfrak{a}} = uO_K, \text{ and } u \in K_0 \text{ totally positive}\}/\sim \tag{9.1}$$ {eq:shimu

The equivalence relation denoted $\sim$ above is the one induced by principal ideals, more precisely the equivalence modulo the subgroup given by the $(vO_K, v\bar{v})$ with $v \in K^*$ and $v\bar{v} \in K_0$ totally positive.

It fits into the exact sequence

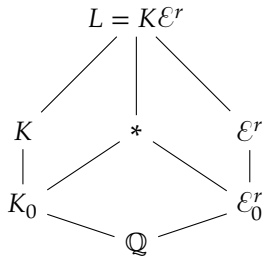
$$1 \longrightarrow O_{K_0}^+/N_{K/K_0}(O_K^*) \xrightarrow{u\mapsto(O_K,u)} \mathfrak{C} \xrightarrow{(\mathfrak{a},\alpha)\mapsto\mathfrak{a}} \mathrm{Cl}_K \xrightarrow{N_{K/K_0}} \mathrm{Cl}_{K_0}^+ \longrightarrow 1, \tag{9.2}$$ {eq:exact

where $O_{K_0}^+$ is the subgroup of totally positive units in O_{K_0} and $\mathrm{Cl}_{K_0}^+$ is the narrow class group of K_0.

The type norm gives a natural morphism $\mathrm{Cl}_{\mathcal{E}^r} \to \mathfrak{C}, I \mapsto (N_{\Phi^r}(I), N_{\mathcal{E}^r/\mathbb{Q}}(I))$.

Example 9.3.1. In dimension $g = 2$, there are two type of quartic primitive CM field: the Galoisian whose Galois group is cyclic, and the non Galoisian whose Galoisian closure has the Dihedral group D_4 of order 8 as Galois group. There is also a non primitive case with Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

In the cyclic case there is only one equivalence class of CM type, and K is its own reflex field. In the Dihedral case there are two equivalence class, which both give the same reflex field K^r, and fit into the following diagram:



Let's assume that the only roots of unity of K are ± 1 (this is always the case if K is primitive, but in the bicyclic case we would have the fourth-root of unity), so if we let ϵ be a fundamental unit, $U_K = \pm 1 \times \langle\epsilon\rangle$. Let ϵ_0 be a fundamental unit of K_0, $U_{K_0} = \pm 1 \times \langle\epsilon_0\rangle$, and $U_{K_0}^+$ be the totally positive units of K_0. We let $\#\mathrm{Cl}_{K_0} = h_0$ and $\#\mathrm{Cl}_K = h_0h_1$.

There are two cases: if $\epsilon_0 = \epsilon$, then $N_{K/K_0}(\epsilon) = \epsilon_0^2$, so $\langle\epsilon^2\rangle = N_{K/K_0}(U_K)$, and $U_K = U_{K_0}$. If K is primitive we are always in this case by [Str10, § II.3.3]. We then have two subcases: if ϵ_0 (or $-\epsilon_0$) is totally positive (so $N_{K_0/\mathbb{Q}}(\epsilon_0) = 1$), then $N_{K/K_0}(U_K)$ is of index 2 in $U_{K_0}^+$ which is of index 2 in U_{K_0}. In this case, $\#O_{K_0}^+/N_{K/K_0}(O_K^*) = 2, \#\mathfrak{C} = h_1, \#\mathrm{Cl}_{K_0}^+ = 2h_0$. So $\mathfrak{C}$ is represented by $h_1/2$ classes of Cl_K with principal totally positive norm, for each element $(\mathfrak{a}, \alpha)$ there is a second one $(\mathfrak{a}, \alpha\epsilon_0)$.

Otherwise $N_{K_0/\mathbb{Q}}(\epsilon_0) = -1$, $N_{K/K_0}(U_K) = U_{K_0}^+$ is of index 4 in U_{K_0}. In this case, $\#O_{K_0}^+/N_{K/K_0}(O_K^*) = 1$, $\#\mathfrak{C} = h_0h_1, \#\mathrm{Cl}_{K_0}^+ = h_0$. By multiplying with ϵ_0 if necessary, any principal ideal in $O_{\mathcal{F}}$ has a totally positive generator, so $\mathfrak{C}$ is represented by the classes of Cl_K with principal relative norm.

Finally if $\epsilon_0 = \epsilon^2$, then $N_{K/K_0}(\epsilon) = -\epsilon_0$ (so $-\epsilon_0$ is totally positive and $N_{K_0/\mathbb{Q}}(\epsilon_0) = 1$), and $\langle\epsilon_0^2\rangle$ is of index 2 in $N_{K/K_0}(U_K) = U_{K_0}^+$ which is of index 2 in U_{K_0} which is of index 2 in U_K. In this case, $\#O_{K_0}^+/N_{K/K_0}(O_K^*) = 1$, $\#\mathfrak{C} = h_1/2, \#\mathrm{Cl}_{K_0}^+ = 2h_0$. So $\mathfrak{C}$ is represented by $h_1/2$ classes of Cl_K with principal totally positive norm.

Finally, in the primitive cases, then the image of $N_{\Phi^r}(\mathrm{Cl}_{K^r})$ in $\mathfrak{C}$ is of index a power of 2 [Str10, Theorem 2.2; BGL11, Lemma 6.5].

9.4 Abelian varieties with complex multiplication over a number field

The action of the Shimura class group on CM abelian varieties is summarized in [Str10, Theorem I.5.2].

Fix a CM type (K, Φ). Let $\mathfrak{a}$ be a fractional O_K-ideal such that $(\mathfrak{a}\bar{\mathfrak{a}}fD_{K/\mathbb{Q}})^{-1} = (\xi)$ with ξ totally imaginary positive. Then we have a polarisation E on $A = \mathbb{C}^g/\Phi(\mathfrak{a})$ given by the $\mathbb{R}$-linear extension of $E(\Phi(x), \Phi(y)) = \mathrm{Tr}_{K/\mathbb{Q}}(\xi\bar{x}y)$. Then (A, E) is a principally polarised abelian variety with CM by O_K and CM type Φ, it is simple if and only if Φ is primitive (in which case $K = \mathrm{End}(A) \otimes \mathbb{Q}$), and every abelian varieties satisfying these conditions

are of this form. Furthermore if $\mathfrak{a}' = \gamma\mathfrak{a}$ and $\xi' = \gamma\overline{\gamma}^{-1}\xi$ for $\gamma \in K^*$, then (A', E') is isomorphic to (A, E). The converse is true if Φ is primitive.

Letting $\mathcal{A}_{g,\Phi}$ be the dimension 0 subspace of $\mathcal{A}_g \otimes_{\mathbb{Q}} \mathbb{C}$ of principally polarised abelian varieties with CM by (K, Φ) we get that if Φ is primitive, $\mathcal{A}_{g,\Phi}$ is a torsor under the Shimura class group $\mathfrak{C}$, where $(\mathfrak{a}, u)$ acts on $(\mathfrak{b}, \xi)$ by $(\mathfrak{ab}, u\xi)$. In particular, $(\mathfrak{a}, u) \cdot A = A/A[\mathfrak{a}]$.

The main theorem of complex multiplication then states that evaluating a modular parameter J on $(\mathfrak{a}, \xi)$ then gives an abelian extension of $\mathcal{E}^r$, and the Galois action comes from the action of the type norm:

h:maincm0 **Theorem 9.4.1** (Main Theorem of Complex Multiplication)**.** *Let $A/\mathbb{C}$ be an abelian variety with primitive complex multiplication by (K, Φ) represented by $(\mathfrak{a}, \xi)$, and let $P \in A$ be a point with annihilator $\mathfrak{b}$, $P = \Phi(x)$, $x \in K/\mathfrak{a}$. Let J be a modular parameter for (A, P) (by which I mean coordinates on the corresponding moduli space). Then $\mathcal{E}^r(J(A))$ is a class field extension of $\mathcal{E}^r$ with corresponding ideal class group $I_{\mathcal{E}^r}(b)/\{I \mid N_\Phi(I) = \mu O_{\mathcal{E}^r}, \mu\overline{\mu} = N_{K/\mathbb{Q}}(I), \mu = 1 \bmod {}^*\mathfrak{b}\}$ where $I_{\mathcal{E}^r}(b)$ are the invertible ideals of $\mathcal{E}^r$ prime to $b = \mathfrak{b} \cap \mathbb{Z}$. The Galois action represented by the class of I on $(\mathfrak{a}, \xi, x)$ is $(N_\Phi(I)^{-1}\mathfrak{a}, N_{K/\mathbb{Q}}(I)\xi, x \mod N_\Phi(I)^{-1}\mathfrak{a})$.*

Proof. This is [Str10, Theorem I.9.1 and Lemma 9.2]. The statement of the complex theorem of complex multiplication becomes more streamlined when switching to the adélic point of view of class field theory. See [Milo6b] for an overview of different reformulations, and an extension of the main theorem stated over $\mathbb{Q}$ rather than over $\mathcal{E}^r$. See also [Milo7] for a condensed proof.

In fact the main theorem of complex multiplication is a corollary of Shimura's general reciprocity theorem that gives the adélic Galois action on modular function of any level. See [Str] for a reformulation of Shimura's reciprocity expressed in terms of ideals. This is used by Streng to find class invariants giving smaller class polynomials than J. □

Using that the action of complex conjugation is $\overline{J(\mathfrak{a}, \xi)} = J(\mathfrak{a}, \overline{\xi})$ by [Str10, Lemma 9.2], we obtain by setting $b = 1$ in Theorem 9.4.1:

th:maincm **Corollary 9.4.2.** *If $A \in \mathcal{A}_{g,\Phi}$, and J are modular parameters, then $\mathfrak{H} = \mathcal{E}^r(J(A))$ is an abelian extension of $\mathcal{E}^r$ corresponding to the class group $N_{\Phi^r}(\mathrm{Cl}_{\mathcal{E}^r})$.*

Moreover, the field $\mathfrak{H}_0 = \mathcal{F}^r(J(A))$ is linearly disjoint from $\mathcal{E}^r$ over $\mathcal{F}^r$ and we have $\mathfrak{H} = \mathfrak{H}_0\mathcal{E}^r$. The extension $\mathfrak{H}/\mathcal{F}^r$ is Galois, and $\mathfrak{H}_0$ is the real subfield of the CM field $\mathfrak{H}$.

The moduli space $\mathcal{A}_{g,\Phi}$ splits into K-irreducible components under the action of $\mathrm{Gal}(\mathfrak{H}/K)$. These components correspond to the orbits of the action of $N_{\Phi^r}(\mathrm{Cl}_{\mathcal{E}^r})$ in $\mathfrak{C}$, and are defined over $\mathcal{F}^r$. The action of $\sigma \in \mathrm{Gal}(\mathcal{F}^r/\mathbb{Q})$ sends an irreducible component of $\mathcal{M}_\Phi$ to an irreducible component of $\mathcal{M}_{\sigma\Phi}$. This describes the splitting of $\mathcal{A}_{g,\Phi}$ into $\mathbb{Q}$-irreducible components.

:shimura1 *Proof.* This is [ER13, Theorem 1.3.1] which uses the references [Str10, Theorem I.9.1 and Chapter III]. The main point is that by Theorem 9.4.1 the Galois action is given by the image of $\mathrm{Cl}(\mathcal{E}^r)$ in the Shimura class group by the type norm. □

This imply in particular that if A/K' has CM by (K, Φ) (K' a number field), then A is defined over an abelian extension of $\mathcal{E}^r$.

9.5 ABELIAN VARIETIES WITH COMPLEX MULTIPLICATION OVER FINITE FIELDS

bsec:CMFq If A/L (L a local field of characteristic 0 with maximal ideal m) has complex multiplication by (K, Φ), it has potential good reduction at m. Furthermore, by general theory [ST68] it acquires good reduction whenever it acquires semi-stable reduction, so eg when adding the points of n torsion ($n \geq 3$ prime to p). By [ST68] there is an extension L'/L with the same residue field k/m such that $A_{L'}$ has good reduction, and this does not depend on the chosen L'. We refer to Section 3.1.3 for more details.

Assuming that A/L has good reduction at m, and writing $k = O_L/m$, by the theory of Néron models and rigidity, $\mathrm{End}(A_L) = \mathrm{End}(A) \subset \mathrm{End}(A_k)$, so A_k has CM by O_K. Furthermore the reduction of O_K-isogenies behaves well (ie is an equivalence of categories) by [Milo6b, Proposition 7.42] since they are given by $\mathfrak{a}$-multiplications (possibly over finite extensions).

The Taniyama-Shimura formula describes the characteristic polynomial of the Frobenius.

Theorem 9.5.1. *Let A/L be an abelian variety with CM by (K, Φ), L a Galoisian number field, $\mathfrak{P}$ a prime of O_L over which A has good reduction. Let $\mathfrak{p} = \mathfrak{P} \cap O_{\mathcal{E}^r}$, $p = \mathfrak{P} \cap \mathbb{Z}$, and assume that p is unramified in O_K and $\mathfrak{P}$ is unramified over $O_{\mathcal{E}^r}$.*

Then the action of the Frobenius $\pi \in O_K$ acting on $\mathsf{A}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{P}}$ is given by $(\pi_{\mathfrak{P}}) = N_{L,\Phi}(\mathfrak{P})$. Note that since the endomorphisms of A are defined over L, L contains $\mathcal{E}^r$ by [Milo6b, Proposition 7.11]. We also have $\pi_{\mathfrak{P}}\overline{\pi_{\mathfrak{P}}} = p^{f_{\mathfrak{P}}} = N_{L/\mathbb{Q}}(\mathfrak{P})$, which determines $\pi_{\mathfrak{P}}$ up to roots of unity.

Furthermore the Artin symbol $\left(\frac{\mathfrak{P}}{\mathfrak{p}}\right)$ corresponds to the action of the Frobenius π_q of $\mathbb{F}_q := \mathbb{F}_{\mathfrak{p}}$ (ie $q = N_{\mathcal{E}^r/\mathbb{Q}}(\mathfrak{p})$) on $A_{\mathfrak{P}}$. This Frobenius action is given by the action of the type norm $\mathfrak{a} = N_{\Phi}(\mathfrak{p})$ in the Shimura class group (via the $\mathfrak{a}$-multiplication).

th:shimura2

In particular if $\mathfrak{a}$ is of order n, then $A_{\mathfrak{P}}$ is defined over $\mathbb{F}_{q^n}$, and $\mathfrak{a}^n = (\pi_{q^n})$.

Proof. See [Milo6b, Theorem 8.1 and Corollary 8.7] and also [ER13, Theorem 3.1.1] and the references cited there. □

We will mainly use this theorem when Φ is primitive, taking $L = \mathfrak{H}$ (this is a field of definition, not only a field of moduli).

We say that $\mathfrak{p}$ is an ordinary prime (of degree n) if there exists $L, \mathfrak{P}$ as above such that $A_{\mathfrak{P}}$ is ordinary (and $\mathfrak{a} = N_{\Phi}(\mathfrak{p})$ is of order n, ie $A_{\mathfrak{P}}$ is defined over $\mathbb{F}_{\mathfrak{p}^n}$). Since the p-rank of an abelian variety over $\mathbb{F}_q$ can be read off from the Newton polygon of χ_π we can check this condition directly on $\mathfrak{a}^n$. This is in particular the case if p splits completely in K [Sug14, Theorem 1.2]. See also [GL12] for refinements of this result when K is a quartic CM field.

We also have by [Milo6b, Corollary 8.3] that $\mathrm{ord}_v(\pi_{\mathfrak{P}})/\mathrm{ord}_v(p^{f_{\mathfrak{P}}}) = |\Phi \cap H_v|/|H_v|$ where v is a place of K above p and H_v are the morphisms $K \to L_{\mathfrak{P}}$ which factor through K_v, hence is of cardinal $K_v : \mathbb{Q}_p$. Hence if p splits completely in K, $\#H_v = 1$ and Φ is given by the element of H_v for the primes v such that $v \mid \pi O_K$.

If A has CM by (K, Φ) and Φ is primitive, then A is simple so $\mathrm{End}(A) = O_K$. In the ordinary case the reduction then gives a bijection between abelian varieties with complex multiplication in $\mathbb{C}$ and those in $\mathbb{F}_{\mathfrak{p}^n}$. Indeed in the ordinary case we have $\mathrm{End}(A_{\mathfrak{P}}) = O_K = \mathrm{End}_k(A) = \mathrm{End}_{\overline{k}}(A)$ (in particular $A_{\mathfrak{P}}$ is absolutely simple) so canonical lifts provide the reverse direction: A is the canonical lift of $A_{\mathfrak{P}}$, and every abelian varieties over $\mathbb{F}_{\mathfrak{p}^n}$ with CM by K is isogenous to $A_{\mathfrak{P}}$ hence is ordinary hence its canonical lift to characteristic zero belongs in $\mathcal{A}_{g,\Phi}$.

Part III

TOPICS IN ALGEBRAIC GEOMETRY

A RESULTS FROM ALGEBRAIC GEOMETRY

dixgeoalg

CONTENTS

A.1 THE PROPER BASE CHANGE THEOREM

roperbase

Let $f : X \to Y$ be a proper map of noetherian schemes. The map f is said to be cohomologically flat in dimension p if $R^p f_* O_X$ commutes with base change (it suffice to test on each fibers) and is locally free (The original definition is but [GD64, p. III.7.8.4] show that this is equivalent).

roperbase

Lemma A.1.1 (Proper base change theorem). *Let $f : X \to Y$ be a proper map of noetherian schemes, F a coherent sheaf on X flat over Y. Then $K = Rf_*F$ is perfect and $H^p(X_y, F_y) = H^p(K \otimes^L_{O_Y} \kappa(y))$.*

(a) $\varphi^p(y) : R^p f_* F \otimes_{O_Y} \kappa(y) \to H^p(X_y, F_y)$ *is surjective if and only if it is an isomorphism.*

Then there is an open U around y, such that (a) holds for U and the formation of $R^p f_* F$ commutes with arbitrary base change on U.

(b) In this case, The following are equivalent:

a) $\varphi^{p-1}(y)$ *is also surjective ie* $R^{p-1} f_* F \otimes_{O_Y} \kappa(y) \to H^{p-1}(X_y, F_y)$ *is an isomorphism*

b) $R^p f_* F$ *is a free sheaf in a neighborhood of y.*

By definition, f is cohomologically flat in dimension p at y if we have (a)+(b). In this case $y \mapsto \dim_k(y) H^p(X_y, F_y)$ is a locally constant function around y. The converse is true if Y is reduced.

So if Y is reduced, $y \mapsto \dim_k(y) H^p(X_y, F_y)$ is locally constant on $S \Leftrightarrow F$ is cohomologically flat in dimension p.

As a corollary:

- *If $R^k f_*(F)_y = (0)$ for $k > b$, $H^k(X_y, F_y) = (0)$ for $k > b$,*
- *If $H^{b+1}(X_y, F_y) = (0)$, then $R^{b+1} f_* F_y = 0$ and $R^b f_* F \otimes_O Yk(y) \simeq H^b(X_y, F_y)$ is an isomorphism.*
- *Taking $b = 0$ above yields that if $H^1(X_y, F_y) = (0)$, then $R^1 f_* F_y = 0$ and $R^0 f_* F \otimes_{O_Y} \kappa(y) \simeq H^0(X_y, F_y))$, hence the formation of $f_* F$ commutes with arbitrary base change (locally around y). Then $f_* F$ is locally free around y, ie f is cohomologically flat in dimension 0 around y.*

Proof. The proper base change theorem is developped in [GD64, §III.7.7, §III.7.8]. See also [Stacks, Tag 0E62], [Har13, Chapter III]. A reformulation of Grothendieck's base change theorem simplified by the language of derived categories is in [FGI05, §8.3, Corollary 8.3.6.5]. An elementary proof, sufficient for what we need, can be found in [Mum70a, §5] completed by [Ten13]. A summary of this criteria for cohomological flatness of dimension 0 is in [MFK94, §0.5][1]

[1] I cannot resist to cite Mumford here: "The first topic is a theorem in EGA 3, § 7, which is extremely useful, but which is unfortunately buried there in a mass of generalizations".

For the corollary, the first item is by recursion via (b ii). For the second item, if $H^{b+1}(X_y, F_y) = (0)$ then by (a) and Nakayama (which we can apply since $R^{b+1}f_*F$ is coherent by Serre's theorem), $R^{b+1}f_*F_y = 0$, and the conclusion follow by (b ii). The last item comes from the second, except for the final conclusion which comes from applying (b i) to $H^{-1}(X_y, F_y) = 0$. □

A.2 COHOMOLOGICAL FLATNESS IN DIMENSION 0

sec:cohflat

We recall that f is cohomologically flat in dimension 0 if the formation of f_*O_X commutes with base change.

Indeed by Lemma A.1.1 (or [BLR12, Theorem 8.1.7]), f_*O_X is then automatically locally free, hence this is coherent with the definition from Appendix A.1.

For instance an universal O-morphism is cohomologically flat in dimension 0. If the base S is reduced, f is cohomologically flat if and only if $s \mapsto \dim_{k(s)}(H^0(X_s, O_{X_s})$ is locally constant on S by Lemma A.1.1.

lem:cohflat

Lemma A.2.1. *Let $f : X \to S$ be proper flat of finite presentation. Let $s \in S$ be a point such that $H^0(X_s, O_{X_s})$ is an étale algebra over $k(s)$ (for instance X_s is geometrically reduced by [Stacks, Tag 0BUG]). Then f is cohomologically flat in dimension 0 over an open U containing s.*

If furthermore $k(s) = H^0(X_s, O_{X_s})$ (for instance X_s is geometrically connected and geometrically reduced), then f is an universal O-morphism over U (by shrinking U if necessary).

In particular, if f has geometrically reduced fibers, f is cohomologically flat in dimension 0, and in its Stein factorisation $X \to X' = \mathrm{Spec} f_*O_X \to S$, X' is finite étale over X. If furthermore the geometric fibers are connected, f is an universal O-morphism. If f is surjective, it suffices to check that the generic fibers are geometrically connected, then all geometric fibers are connected.

Proof. The first statement is [GD64, Proposition III.7.8.6], an application of the proper base change theorem Lemma A.1.1. The second statement then follows immediatly (see [GD64, Cor III.7.8.7]).

The remark in parenthesis in the second statement comes from the fact that a proper geometrically reduced scheme of finite type X over a field k satisfy $H^0(X, O_X) = k$ if and only if it is geometrically connected [Stacks, Tag 0F2D].

Finally the last statement is a corollary of the first, except for the fact that it suffices to check geometric connectedness of the generic fibers. By [GD64, p. IV.15.5.9], the number of geometrically connected components is lower semi-continuous on S, so if it is equal to one on the generic fibers it is equal to one (by surjectivity) everywhere. □

A.3 PROPER MORPHISMS AND CONNECTED FIBERS

We want to give fibral criterions for a map to be proper. For the next four lemmas, the proofs in [GD64] assume that the base scheme S (locally) noetherian. But these hold for general scheme if we assume $f : X \to S$ to be finitely presented by the usual approximations techniques of [GD64, p. IV.8]. By Zariski connectedness theorem, there is a link between being a proper morphisms and having geometrically connected fibers.

omconnectedfiber

Lemma A.3.1. *If $f : X \to S$ a proper flat morphism of finite presentation, then it has proper fibers, and if furthermore the generic fibers are geometrically connected all its fibers are, by semi-continuity [GD64, p. IV.15.5.4][2].*

There is a converse:

a:converseproper

Lemma A.3.2. *If f is flat (or even just universally submersive), separated of finite presentation, has proper and geometrically connected fibers then it is proper [GD64, p. IV.15.7.10].*

If S is (the Spec of) a discrete valuation ring (in French the standard terminology is that S is "un trait"), there is an intermediate result:

lemma:serretate

Lemma A.3.3. *Let $f : X \to S$ be flat separated of finite type, S the* Spec *of a dvr (discrete valuation ring). If the special fiber is proper and the generic fiber is geometrically connected then f is proper. Hence the special fiber is geometrically connected by Lemma A.3.1.*

[2] This is a corollary of Zariski connectedness theorem [GD64, p. III.4.3]

Proof. This is [ST68, Lemma 3]. In their Lemma they assume that f is smooth but they only use that it is universally open: If $S = \operatorname{Spec} R$, since $R \mapsto \hat{R}$ is fpqc, and since geometrical connectedness (of X_{η_S}) ascend and properness (of X) descend, we may assume $R = \hat{R}$. By [GD64, p. III.5.5.2], $X = Y \bigsqcup Z$ with Y proper and $X_s \subset Y$. Since X/S is open, $Y \cap X_K$ is not empty, but since X_K is connected, $Z \cap X_K = \emptyset$ so $X = Y$ and X is proper. □

nserretate **Corollary A.3.4.** *If $f : X \to S$ is flat separated, of finite presentation with geometrically connected generic fibers. If the fiber at s is proper, then f proper at s (which mean that it is proper above a neighborhood of s, [GD64, p. IV.15]).*

Proof. Indeed since this is a topological condition we may assume that X and S are reduced. Since f is separated, it suffices to prove that f is proper at s at each irreducible component of X. We may assume that X and S are irreducible, and by approximation that S is Noetherian. So we reduce to S and X integral and f dominant. By [GD64, p. IV.15.7.1], it suffices to check the valuative criterion for S' a dvr whose generic point η maps to the generic point of X, hence also to the generic point of S, and the closed point s' of S' maps to s. We are reduced to Lemma A.3.3. □

nconnected **Lemma A.3.5** ([GD64, p. IV.15.5.7])**.** *Let $f : X \to S$ be a proper morphism of finite presentation, s a point of S and assume that the fiber X_s at s is geometrically reduced, and f is universally open at X_s. Then $t \mapsto n(t)$, the number of geometrically connected components, is locally constant at s.*

We can now state a fiberwise criterion for a smooth map to be proper:

iseproper **Proposition A.3.6.** *Let $f : X \to S$ be a morphism The following are equivalent:*

(i) f is proper, flat of finite presentation, with smooth and geometrically connected fibers (since a smooth map is by definition a flat map, locally of finite presentation and with smooth fibers, equivalently f is proper smooth of finite presentation with geometrically connected fibers);

(i') f is proper, flat of finite presentation, with smooth fibers and geometrically connected generic fibers;

(i") (If S connected) f is proper, flat of finite presentation, with smooth fibers and one geometrically connected fiber;

(ii) f is flat of finite presentation, with fibers smooth, proper and geometrically connected;

(ii') f is flat of finite presentation, with fibers smooth and proper, and with geometrically connected generic fibers.

Proof. By definition, a smooth morphism is a flat morphism (locally of finite presentation), with smooth fibers. (i) ⇒ (i') is trivial, the converse holds because if f is proper flat with geometrically connected generic fibers, then all fibers are geometrically connected by semi-continuity of $n(t)$ [GD64, p. IV.15.5.4]. (i) ⇔ (i") is Lemma A.3.5, since a flat finitely presented morphism is universally open.

(i) ⇒ (ii) is trivial since a proper morphism has proper fibers, the converse is Lemma A.3.2, which use the fact that a flat finitely presented morphism, with proper and geometrically connected fibers is proper by [GD64, p. IV.15.7.10], using the local properness criteria.

(ii) ⇒ (ii') is trivial, and (ii') ⇒ (i) by Corollary A.3.4. □

A.4 MORPHISMS OVER AN HENSELIAN LOCAL RING

Since an isogeny is an étale cover (ie an étale finite morphism), it is interesting to have conditions when two schemes have the same étale covers (ie have the same fundamental étale group).

quivalence **Proposition A.4.1.** *Let S be the spectrum of a Henselian local ring with closed point s. Let X/S be proper. Then the pair (X, X_s) is 0-Henselian and 1-Henselian.*

Proof. The pair (X, X_s) is 0-Henselian means that closed and open subsets of X_s lifts uniquely. This is proved in [GD64, p. IV.18.5.19]. It is 1-Henselian means that the category of finite étale covers of X_s is equivalent to the category of finite étale covers of X. This is proved in [AGV72, Exposé XII, Corollary 5.5]. See also [Ryd10, Proposition A.7] for equivalent conditions, and [Ryd10, Theorems A.11 and A.13]. □

Remark A.4.2. When $f : X \to Y$ is a universal homeomorphism of schemes[3] that is an integral, universally injective and surjective morphism then there is an equivalence of category between étale spaces over X and étale spaces over Y [Stacks, Tag 05ZG] and [Ryd10, Theorem 5.21].

Example A.4.3. If A/S and B/S are abelian schemes over an Henselian local S (with closed point s), étale isogenies $g : A_s \to B_s$ lift uniquely to $A \to B$. Of course in this case we can directly lift $\operatorname{Ker} g/s$ to $\operatorname{Ker} f/S$ by the properties of Henselian rings.

We will also need the structure theorem of quasi-finite morphisms over an Henselian local ring.

prop:henselpair

Proposition A.4.4. *Let (A, I) be an henselian pair, $S = \operatorname{Spec} A$, $S_0 = \operatorname{Spec} A/I$, $X \to S$ separated of finite type, and $X_0 = X_{S_0}$. Then open and closed subschemes of X_0 which are proper lift to X. In particular, if X_0 is proper over S_0 then $X = Y \bigsqcup Z$ such that Y/S is proper and contains X_0 and all the closed subschemes X' of X that are proper over S.*

Proof. This is [Stacks, Tag 03GX]. See also [GD64, p. III.5.5.1] for a proof when (A, I) is a noetherian I-adically complete ring and [GD64, p. III.5.5.2] for the corollary. □

ifinitestructure

Corollary A.4.5. *Let X be quasi-finite and separated over a henselian local ring A. There is a unique decomposition $X = X_f \coprod X_\eta$ where X_f is A-finite and X_η has empty special fiber. The formation of the "finite part" X_f is functorial in X and commutes with products, so it is an A-subgroup when X is an A-group.*

Proof. This is Proposition A.4.4, indeed the reduction X_0 is quasi-finite over a field, hence finite. See also [Con+11, L13, Theorem 4.10] for a beautiful direct proof using Zariski's main theorem. □

See [Con04] for an application to the classification of a quasi-finite étale separated scheme over a Dedekind scheme.

[3] or even of algebraic spaces if we ask f to be furthermore separated; this is automatic for schemes

B ALGEBRAIC GROUPS AND GROUP SCHEMES

adixgroups

CONTENTS

B.1 ALGEBRAIC GROUPS

:alggroup

Let k be a field, $\overline{k}$ an algebraic closure of k. We denote by k_s the separable closure of k in $\overline{k}$. For our algorithmic applications we are mainly interested in perfect fields, in which case $k_s = \overline{k}$.

A locally algebraic group G/k is a group scheme over k which is locally of finite type. It is said to be algebraic whenever G/k is of finite type (ie an algebraic group is a locally algebraic group that is quasi-compact).

Since the diagonal is the base change of the identity section, which by definition of a group scheme is a rational point 0_G over k, a group scheme G/k is always separated. Furthermore an algebraic group G is quasi-projective [Stacks, Tag 0B7F] hence is an AF-scheme.

An algebraic group scheme G/k over a perfect field k (which mean a group scheme of finite type over k) is smooth whenever G is reduced [Stacks, Tag 047P]. In fact, for a general k, if G has a geometrically reduced point, it is smooth by [GD64, 15.6.10.(iii)]. Conversely, if G is smooth it is of course geometrically reduced, and punctually geometrically integral (so is geometrically integral whenever it is geometrically connected). And if k if of characteristic 0, G is always smooth (Cartier, [Stacks, Tag 04TN]).

There exists a maximal smooth (or equivalently geometrically reduced) closed sub-scheme $G^\dagger$ of G, it commutes with separable base change. It is equal to the closure of $G(k_s)$ if $k = k_s$ is separably closed and equal to G_{red} if k is perfect [Gil14, Corollary 3.3.3].

onentgroup

Lemma B.1.1. *Let G/k be a group scheme locally of finite type. Then its connected neutral component G° is geometrically irreducible and of finite type.*

Proof. This is [DA70, Prop VIa.2.4] where the statement is more generally proved for a group scheme locally of finite type over an Artinian ring see also [Stacks, Tag 0B7R]). Since the neutral point is rational, the fact that G° is geometrically connected can also be seen from the fact that a connected scheme X/k with a point x such that k is algebraically closed in $k(x)$ (in particular if x is rational) is geometrically connected by [GD64, p. IV.4.5.14] or [Stacks, Tag 04KV]. It is then geometrically irreducible by [Stacks, Tag 0B7Q]. □

ctedetale

Lemma B.1.2 (The connected-étale sequence)**.** *Let G/k be an algebraic group. The quotient $\pi(G) = G/G^\circ$ is an étale finite group. The formation of $\pi(G)$ commutes with fields extension, and a morphism from G to an étale finite group factorizes through $\pi(G)$. The connected components of G that are geometrically connected (for instance who contains a rational point) correspond bijectively to k-points of G/G°.*

Proof. Since $G^\circ \to G$ is a flat and closed immersion by [Stacks, Tag 0B7R], it is open by [Stacks, Tag 025G] (since it is locally of finite presentation), hence the quotient $\pi(G) = G/G^\circ$ (which exists by Appendix D) is a finite group scheme over k.

The rest of the assertions are proved in [Liu02, Proposition 10.2.18 and Corollary 10.2.21]: For an algebraic scheme X/k, we may define $\pi_0(X)$, the largest finite étale quotient $X \to \pi_0(X)$, as the largest finite étale subalgebra of $\Gamma(X)$. If X/k is finite, we may describe it as follow: $X = \operatorname{Spec} A$ where $A = \prod A_i$ is a product of Artinian local rings, and $\pi_0(X) = \operatorname{Spec} A^t$, where $A^t = \prod A_i^t$, and A_i^t is the lift to A_i of the separable closure of k in the residue field $k_i = A_i/m_i$. The morphism $X \to \pi_0(X)$ is faithfully flat, its fiber $X_{f(x)}$ corresponds to the connected component of x. Its formation is functorial, commutes with field extension and product. For a group G, $\pi_0(G)$ coincide with the quotient G/G° as above [Liu02, Corollary 10.2.21.b].

The connected components of G that are geometrically connected correspond bijectively to k-points of G/G° [Liu02, Corollary 10.2.21.a]. See [use14] for an example where some connected components are not geometrically connected. See also Section 3.3.1 for an extension to a more general base. □

In summary:

Proposition B.1.3. *Let G/k be a locally algebraic group.*

- *G/k is always separated and is quasi-projective (hence is an AF-scheme).*
- *G/k is smooth whenever it has a geometrically reduced point (hence a reduced point if k is perfect). This is always the case if k is of characteristic zero.*
- *Its connected neutral component G° is a geometrically irreducible algebraic group.*

Quotients of algebraic groups behave well:

p:morphismgroups

Proposition B.1.4. *Let G/k be an algebraic group.*

- *If H is a closed subgroup of G, the fppf quotient (that is the quotient as fppf sheaves) is represented by an algebraic group: $q : G \to G/H$ (so q is fppf). The map q is finite if and only if it is quasi-finite if and only if H is finite.*

  If G is smooth the quotient G/H too, and if both G and H are smooth the quotient is characterized by $G/H(\bar{k}) = G(\bar{k})/H(\bar{k})$ and $T_q : \mathfrak{g} \to \mathfrak{g}/\mathfrak{h}$ is surjective (where $\mathfrak{g}$ and $\mathfrak{h}$ are the Lie algebra of G and H).
- *If H is a normal closed subgroup (if G and H are smooth this is equivalent to $H(\bar{k})$ normal in $G(\bar{k})$), then G/H has a (unique) structure of group scheme making q a morphism, and then $H = \ker q$. If G is affine then G/H too.*
- *Let $f : G \to G'$ be a morphism of algebraic groups. The image $f(G)$ is closed in G', and is a closed immersion if and only if $\ker f = 1$. In particular a monomorphism is a closed immersion, in other words a subgroup is automatically closed.*

  If G' is reduced, then f is faithfully flat $\Leftrightarrow$ f is surjective $\Leftrightarrow$ f is dominant; and f is flat $\Leftrightarrow$ $f \mid G^\circ : G^\circ \to G'^\circ$ is surjective. In particular, $f(G) \simeq G/\operatorname{Ker} f$, and $G \to f(G) \subset G'$ is fppf. This is the case if G and G' are smooth, $f(G) \simeq G/\operatorname{Ker} f$ is then a smooth subgroup of G'.
- *If G and G' are connected, the map f is an isogeny if it is a finite flat surjection, or equivalently is faithfully flat with finite kernel. If G and G' are smooth, this is equivalent to f is surjective and $\dim G = \dim G'$, or f is surjective with finite kernel, or f has finite kernel and $\dim G = \dim G'$.*

  More generally, if G and G' are not necessarily connected, we say that f is an isogeny if it is an isogeny on the connected components.

Proof. These are essentially particular cases of [DA70, Exposés VIA et VIB]. See [Con+11, L13, Proposition 2.1] and [Con14, p. 6].

To construct G/H, we may also construct it as the coarse moduli of the stack quotient $[G/H]$, this is then a separated algebraic group space over a field k, hence a group scheme, see Appendix D.

The pullback of the projection map $q : G \to G/H$ by itself is $G \times H \to G$ (this is a general fact about an fppf groupoid quotient $[U/R]$, see Appendix D). So if $\operatorname{Ker} f$ is finite (or equivalently quasi-finite, ie $\operatorname{Ker} f(\bar{k})$ is finite since we are over a field), q is finite. The converse is immediate.

For the third item, if $f : G \to G'$ is a morphism and G' is reduced, by generic flatness and transitivity f is fppf if it is surjective (and it is surjective if it is dominant since its image is closed). If f is flat, then $f(G^\circ)$ is closed, open, and connected, so has to contain G'°. Conversely if $f(G^\circ) = G'^\circ$, then $f|G^\circ$ is fppf over G'°, so flat over G', hence f is flat by transitivity. Moreover $G/\operatorname{Ker} f \to f(G)$ is an fppf monomorphism, so an isomorphism.

The part on isogenies is [Con+11, L13, p.4], see also [BLR12, Lemma 7.3.1]. □

B.2 STRUCTURE OF ALGEBRAIC GROUPS

B.2.1 *The Chevalley decomposition*

There are two important classes of algebraic group: affine groups and abelian variety.

An affine group automatically embeds into $\mathrm{GL}(V)$ for a finite dimensional k-vector space V[1]. Be careful that the usual terminology is to say that G is an affine linear group (or simply linear group) if it is a *smooth* affine group. If G is affine but not smooth (so k is of characteristic $p > 0$), there is an n such that $G/G[\pi^n]$ is smooth (where $G[\pi^n]$ is the kernel of the Frobenius) [DA70, VIIA.8.3], [Gil14, Proposition 9.7.1].

These two classes are orthogonal to each other: there is no nonconstant morphism between an abelian variety A and a connected affine algebraic group G (since the image of A is proper and affine, it is finite hence constant) and conversely from G to A (since likewise the image of G is proper and affine by Proposition B.1.4).

Theorem B.2.1 (Chevalley)**.** *If G/k is a connected algebraic group, there exists a smallest connected subgroup G_1 of G such that G/G_1 is an abelian variety and G_1 embeds into GL_n (but may not be smooth, hence not linear according to our terminology).*

If k is perfect, G_1 is smooth (so is linear) and its formation is compatible with extension of the base field. The formation of the affine part and the abelian part is then functorial, and if $G \to G'$ is surjective (resp. an isogeny), then so is the induced map on the affine and abelian parts.

Proof. See [BLR12, Theorem 9.2.1], and [Con+11, L13 Theorem 2.6]. The functoriality comes from the orthogonality of these two classes. The last statement is [Con+11, L13, Proposition 2.8]. □

We now briefly detail the structure of linear groups. If G is a linear group over a *perfect field* k, for every $g \in G(k)$ there is a canonical *functorial* Jordan decomposition $g = g_{ss}g_u$ with g_{ss} and g_u in $G(k)$ commuting with each others, such that for every linear representation $j : G \to \mathrm{GL}_N$, $j(g) = j(g_{ss})j(g_u)$ is the classical Jordan decomposition. Over $\bar{k}$, every 1-dimensional linear group is isomorphic to either $\mathbb{G}_m$ or $\mathbb{G}_a$. Using these as building block yield two different type of algebraic groups.

B.2.2 *Torus*

A *torus* T/k is a linear group such that $T_{\bar{k}} \simeq \mathbb{G}_m^r$ (and the torus is split if the isomorphism descends to k). Equivalently, T is a torus when all its $\bar{k}$-points $T(\bar{k})$ are semi-simple. A torus is completely determined by its lattice of characters $X^*(T) = \operatorname{Hom}_{k_s}(T_{k_s}, \mathbb{G}_{m,k_s})$ together its Galois action. Indeed, if $k = \bar{k}$ the lattice of cocharacters $X_*(T) = \operatorname{Hom}_{\bar{k}}(\mathbb{G}_{m,\bar{k}}, T_{\bar{k}})$ is the $\mathbb{Z}$-dual of $X^*(T)$ (via the canonical pairing $X^*(T) \times X_*(T) \to \operatorname{End}(\mathbb{G}_m) = \mathbb{Z}$, and $T(\bar{k}) \simeq X_*(T) \otimes_Z \bar{k}^*$, hence the quasi-inverse of X^* is given by $M \mapsto M^\vee \otimes_Z \mathbb{G}_m$. If k is not algebraically closed, and T is a split torus, then the same map yields a quasi-inverse of $X_k(T) = \operatorname{Hom}_k(T, \mathbb{G}_m)$.

In fact more generally [Mil12a, §9], a group G is said to be *diagonalisable* if $G = D(M)$ for a finitely generated abelian group M. If G where $D(M)$ is the algebraic group functorially defined by $D(M)(R) = \operatorname{Hom}(M, R^*)$. Then M can be recovered from $G = D(M)$ via $M = X(G) = \operatorname{Hom}(G, \mathbb{G}_m)$. For instance $\mathbb{G}_m = D(\mathbb{Z})$, so a split torus is of the form $D(\mathbb{Z}^r)$. A group is diagonalisable if and only if every finite dimensional representation is

[1] More generally an affine algebraic group scheme over a Dedekind ring is linear [Mil12b, Aside 9.4], see [Gro10] for other examples

diagonalisable. A group G is said to be of multiplicative type if G_{k_s} is diagonalisable. In this case $G \to X^*(G) = \mathrm{Hom}_{k_s}(T_{k_s}, \mathbb{G}_{m,k_s})$ is an equivalence of category between groups of multiplicative type and the category of finitely generated commutative groups equipped with a continuous action of $\mathrm{Gal}(k)$. The quasi-inverse is given by, if $K \subset k_s$, $G(K) = \mathrm{Hom}(X^*(G), {k_s}^*)^{\mathrm{Gal}(k)}$. The torus then correspond to free $\mathbb{Z}$-modules. We have the equivalences, if p is the characteristic of k: $D(M)$ is connected $\Leftrightarrow$ the only torsion in M is p-torsion; $D(M)$ is smooth $\Leftrightarrow$ M has no p-torsion; so a torus is exactly a smooth and connected algebraic group of multiplicative type. Every representation of a group G of multiplicative type is semi-simple: the simple objects correspond to an orbit ξ of $\mathrm{Gal}(k)$ acting on $X^*(G)$, to such an orbit ξ correspond a vector space V_ξ such that $V_\xi \otimes k_s \simeq \oplus_{\chi \in \xi} V_\chi$, and $\mathrm{End}(V_\xi) = k_\chi$ the fixed subfield of k_s by $\mathrm{Gal}(k)$ leaving $\chi \in \xi$ invariant.

We have the following rigidity result [Mil12a, pp. 9.9, 9.10]: an action of a connected algebraic group G on a multiplicative group H is trivial, so every normal subgroup of multiplicative type of a connected algebraic group is central. And if G is a smooth connected algebraic group and H is of multiplicative type, a morphism of scheme $G \to H$ is an homomorphism if it sends 1_G to 1_H.

B.2.3 Unipotent groups

A connected affine algebraic group U is *unipotent* if $U_{\bar{k}}$ admits a finite composition series whose successive quotients are $\mathbb{G}_a$ (in fact for a general algebraic group U such a condition imply that U is affine)[2]. Equivalently (for a non necessarily connected U), U can be embedded into some k-group of strictly upper triangular matrices, or equivalently each linear representation of U has a fixed point [DA70, pp. XVII.3.5, XVII.4.11], [Gil14, Proposition 10.1.3]. If U is linear, this is equivalent to the standard definition that $g = g_u$ for all $g \in U(\bar{k})$ [DA70, pp. XVII, 2.1]. An unipotent algebraic group is always split (meaning that we have a composition series over k whose successive quotients are $\mathbb{G}_a$) over an inseparable extension of k, so is always k-split if k is perfect [Gil14, Corollary 10.1.4].

More Details B.2.2. Stable by image or closed subgroup.

The k-split property is inherited by quotients [Bo, 15.4(i)], but is not inherited by smooth connected closed subgroups in general when k is imperfect. Classic counterexample: $\mathbb{G}_a^2$ over an arbitrary imperfect field.

In summary:

- G° the connected component is normal, and G/G° is finite;
- If G is connected, it has a normal affine subgroup G_1 such that G/G_1 is an abelian variety;
- If G is affine connected, it is linear, and has a largest solvable normal subgroup $R(G)$ (its radical). Then $G/R(G)$ is semi-simple.
- G affine connected solvable has a largest normal unipotent subgroup $R(G)_u$, and $G/R(G)_u$ is a torus.

B.2.4 The structure of commutative affine groups

Like abelian varieties and affine groups, torus and unipotent groups are orthogonal.

Lemma B.2.3 ([Con+11, L13, Lemma 2.15])**.** *Let T/k be a torus and U/k a smooth connected unipotent group. There are no nontrivial morphisms between T and U.*

Proposition B.2.4. *Let G be a commutative smooth connected affine k-group.*

- *There is a unique maximal tori T, and $U = G/T$ is unipotent, and the formation of T and U commutes with field extension;*
- *If k is perfect, $U \simeq R_u(G)$ so the exact sequence $1 \to T \to G \to U \to 1$ splits uniquely as $G = T \times U$;*
- *The formation of T and U is functorial, and if $G \to G'$ is surjective (resp. an isogeny), then so is $T \to T'$ and $U \to U'$. In particular if $G \to G'$ is an isogeny, G is a torus (resp. is nilpotent) if and only if G' is one.*

Proof. This is [Con+11, L13, Proposition 2.16]. See also [Gil14, Theorem 10.2.2], [DG70, pp. IV.1.2.2, IV.3.3.1] for the more general version with G just commutative affine, and the torus T replaced by a group of multiplicative type. □

[2] more generally a non necessarily connected algebraic group is unipotent when $U_{\bar{k}}$ admits a finite composition series whose successive quotients are subgroups of $\mathbb{G}_a$ [DA70, p. XVII 1.3].

B.2.5 *The structure of reductive linear groups*

For completude, we briefly detail some of the theory of reductive linear groups. This won't be used in the text.

A linear connected group G always contains a k-torus T such that $T_{\overline{k}}$ is maximal in $G_{\overline{k}}$, and a torus T is k-maximal if and only if T_K is K-maximal in G_K for any extension K/k. In particular the (reductive) rank of G defined as the dimension of a maximal torus does not depend on the base field [Con14, Appendix A]. A connected linear group either contains a tori, or is unipotent [Con14, p. 14], so the reductive rank is 0 if and only if G is unipotent.

If T is a torus, then $Z_G(T)$ is of finite index in $N_G(T)$ (they are both smooth group), and is connected if G is connected. The quotient $W_G = N_G(T)/Z_G(T)$ is then finite étale, this is the Weyl group of T. A Cartan subgroup is $C = Z_G(T)$ for any maximal torus T, they commute with field extension and are conjugate over $\overline{k}$. If G is connected and reductive then so is $Z_G(T)$, hence if T is maximal then $T = Z_G(T)$ [Con14, Theorem 1.1.19].

If G/k is an affine algebraic group, it is solvable (resp. k-solvable) if it admits a composition series whose successive quotients are commutative affine algebraic groups (resp $\mathbb{G}_a$ or $\mathbb{G}_m$). If G is solvable then so is G_K for any field extension, so G is solvable if $G(\overline{k})$ is solvable. If G is connected and solvable, every representation of G can be conjugated to have image inside the upper triangular matrices (Lie-Kolchin). Every connected solvable linear algebraic group is a semidirect product of a torus with a unipotent group, $G = T \ltimes U$ [Bor12, 10.6(4)] or alternatively an extension of a torus $T = G/R_u(G)$ by a unipotent subgroup $U = R_u(G)$ [DA70, pp. XVII, 3.11].

Theorem B.2.5 ([Con14, Theorems 1.1.8 and 1.1.9])**.** *Let $G/\overline{k}$ be a linear algebraic group over an algebraically closed field $\overline{k}$. The maximal connected solvable linear algebraic-subgroups of G are all $G(k)$-conjugate to each other, and these are precisely the connected solvable linear algebraic groups B that are parabolic (which mean that the quasi-projective quotient scheme G/B is projective). A subgroup P of G is parabolic if and only if it contains a Borel subgroup B.*

If $G/\overline{k}$ is connected and P is parabolic, P is connected and $N_G P = P$.

If G is a linear group, it has a unipotent radical $R_u(G)$ (the unique maximal connected normal unipotent linear algebraic subgroup of G), and a radical $R(G)$ (the maximal connected normal solvable subgroup of G). These radicals commute with quotients, and normal subgroups (ie $R(H) = (H \cap R(G))^\circ_{\mathrm{red}}$).

We also have a split version $R_{u,s}(G)$ and $R_s(G)$ of these radicals. The radicals R_u, $R_{u,s}$ and R commutes with separable field extensions, so in particular $R_u(G_{\overline{k}})$ and $R(G_{\overline{k}})$ descend to k if k is perfect [Gil14, §11].

The linear group G is said to be reductive (resp. pseudo-reductive) if $R_u(G_{\overline{k}}) = 1$ (resp. $R_u(G) = 1$), and is semi-simple if $R(G_{\overline{k}}) = 1$. And G is pseudo-semi simple if it is pseudo-reductive with $D(G) = G$. By compatibility with quotients, $G/R_u(G)$ (resp. $G/R(G)$) is always reductive (resp. semisimple), and by compatibility with separable field extension, if k is perfect then G is reductive whenever it is pseudo-reductive. If G is connected and has a faithful semi-simple representation then it is reductive [Mil12a, p. 17.13], and conversely in characteristic zero every then all representations of a connected reductive linear group are semi-simple [Con14, Remark 1.1.14].

If G is connected and reductive, then $R(G)$ is the largest subtorus of $Z(G)$ so is a central torus and $G/R(G)$ is semi-simple. We also have that $D(G)$ is semi-simple and the torus $G/D(G)$ is isogenous to $R(G)$, so G is canonically an extension of a torus by a connected semi-simple group (and $D(D(G)) = D(G)$ since $D(G)$ is connected and semi-simple). And $Z \times D(G) \to G$ is an isogeny. See [Con14, Example 1.1.16] when $k = \overline{k}$ and [Mil12a, p. 17.28] for the general case. A semisimple group is then central isogenous to a product of (Weil restriction) of simply connected almost simple linear groups [Mil12a, p. 17.27].

We refer to [DA70; Mil12a; Mil17; Con14; CGP15; CP17] for the classification of (pseudo)-reductive groups, in particular the classification of split reductive groups via root data (a generalisation of Dynkin diagrams used when $k = \overline{k}$). To study the structure of a general group, it helps to have a Levi subgroup. Over a perfect field k, a Levi subgroup is a subgroup L of G such that $L \to G/R_u(G)$ is an isomorphism. They always exist in characteristic zero and are conjugated under $G(k)$ [Gil14, Definition 11.0.9].

B.3 GROUP SCHEMES

upschemes

In this section, if S is a scheme, a group scheme G/S will always be assumed to be flat and locally of finite presentation.

We have the following generalisation of Lemma B.1.1:

lem:lfpisfp **Lemma B.3.1.** *Let G/S be a flat locally finitely presented group scheme with connected fibers. Then G/S is qcqs, that is it is finitely presented.*

Proof. This is [Sta19]. □

If S is a regular scheme, and X/S is a Cohen-Macauley scheme, then "miracle flatness" give a fibral criterion for X/S to be flat over S (namely that all fibers are of the same dimension if S is connected). This can be strengthened in the case of a group scheme G/S, using the existence of a section $\epsilon : S \to G$: for a geometrically reduced group scheme over a reduced base scheme, flatness is equivalent to the fact that the dimension of the fibers is locally constant, see Proposition B.3.3.

The section ϵ also allows to check properness fibrally (compare with Proposition A.3.6).

For a group scheme G/S with section ϵ, ${G^\circ}_s$ denotes the identity component of G at $\epsilon(s)$, and G° is the union of all ${G^\circ}_s$.

connectedsection **Lemma B.3.2.** *Let $f : X \to S$ be a morphism of finite presentation, with a section $\epsilon : S \to X$. For $s \in S$, let X^0_s denote the connected composant of $\epsilon(s)$ in X_s.*

Then if X is separated and a fiber X_s is proper over $k(s)$, then X is proper over S at the point s (which means that X_U it is proper over an open U containing s).

Assume that X^0_s is geometrically integral for all s. Then the following conditions are equivalent:

- *$s \to \dim(X^0_s)$ is locally constant;*
- *f_{red} is flat on X^0;*
- *(If S is locally noetherian) f is universally open on X^0.*

And in this case X^0, the union of all X^0_s is open in X.

Proof. The first statement is [GD64, p. IV.15.6.8]. The second statement is [GD64, p. IV.15.6.7]. See [GD64, p. IV.15.6.6] for a more precise statement. □

Combining Lemma B.3.2 with the results from Appendix B.1, we get

op:fiberwiseflat **Proposition B.3.3** ([GD64, p. IV.15.6.10.iii])**.** *Let $f : G \to S$ be a group scheme of finite presentation.*

- *G/S is separated if and only if the unit section $\epsilon : S \to G$ is a closed immersion.*
- *If G/S is separated and ${G^\circ}_s$ is proper over s then G° is proper over S at s.*
- *G°_s (the connected component at the neutral point of the fiber) is always geometrically irreducible (in particular geometrically connected) and $\dim G^\circ_s = \dim G_s$.*
- *f is universally open on ${G^\circ}_s$ if and only if $z \mapsto \dim(G_z)$ is locally constant at s. In particular, if G/S is smooth or flat, then $z \mapsto \dim(G_z)$ is locally constant (so constant if S is connected).*
- *If G_s is geometrically reduced at a point, then G_s is smooth over $k(s)$. If furthermore f is universally open on ${G^\circ}_s$ and $O_{S,s}$ is reduced, then f is smooth at all points of ${G^\circ}_s$.*
- *In particular, if S is reduced and G_s is smooth (equivalently geometrically reduced) at all $s \in S$ and the dimension of the fibers is locally constant, then G° is open in G and G°/S is smooth.*

Proof. The first statement is [BLR12, Lemma 7.1.2], and the second [GD64, § 15.6.8]. The rest is [GD64, § IV.15.6.10.iii], using [GD64, § IV.15.6.6 and IV.15.6.4]. □

Under some conditions, a group scheme is quasi-projective:

audlocprojective **Proposition B.3.4** (Raynaud)**.** *Let G/S be a smooth group scheme over a normal base S, with connected fibers. Let X be an homogeneous space under X. Then X is locally quasi-projective.*

If S is locally noetherian and regular of dimension 1, then X is projective, and all line bundle $\mathcal{L}$ which is ample on the generic points of S is S-ample.

Proof. This is the main result of [Ray06]. □

B.4 MORPHISMS AND ISOGENY OF GROUP SCHEMES

isogenies

Let G/S and G'/S be flat locally finitely presented group schemes. We will consider flat morphisms $f : G \to G'$, since G and G' are flat over the base, the morphism f is flat if and only if it is flat over each fiber.

If $f : G \to G'$ is a morphism, we let $\mathrm{Ker} f \to G$ be the pullback of the zero section of G'. So it is closed if G'/S is separated. Then $\mathrm{Ker} f \to S$ is the composition $\mathrm{Ker} f \to G \to S$, so is proper if $G \to S$ is proper and G'/S is separated of finite type. But $\mathrm{Ker} f \to S$ is also the pullback of $G \to G'$ via the identity section $\epsilon_{G'} : S \to G'$, so it is flat whenever f is flat. If $\mathbf{G} \to S$ is proper and G'/S is separated of finite type, then $G \to G'$ is proper[3], so we recover that $\mathrm{Ker} f \to S$ is proper in this case.

Conversely we may try to construct quotients of G by finite flat subgroups.

finiteflat

Lemma B.4.1. *Let G/S be a separated flat group scheme. A (finitely presented) subgroup H of G is finite over S whenever it is quasi-finite and proper. If S is reduced, it is finite flat over $S \Leftrightarrow$ it is finite of locally constant rank $\Leftrightarrow$ it is flat quasi-finite of locally constant rank $\Leftrightarrow$ it is locally free of constant (finite) rank. It is also finite flat if it is flat quasi-finite with a locally constant number of geometric points on its fibers, and conversely if the fibers are geometrically reduced.*

Proof. A proper quasi-finite H/S is finite by [GD64, p. IV.8.11.1] or [Stacks, Tag 02LS].[4]

It is well known that a finite module over a reduced base is flat if and only if its rank is locally constant. If H is locally finitely presented, quasi-finite and flat, and its rank is locally constant it is finite by [DR73, §II.1.19] (the finitely presented condition allows us to use approximation to reduced to their noetherian base S). Likewise, if H is locally finitely presented, quasi-finite and flat, and the number of geometric points of its fibers is locally constant it is finite by [GD64, p. IV.15.5.9.i], the converse is [GD64, p. IV.15.5.9.ii].

Note that in particular, if H is the kernel of a finite étale separated isogeny $f : G \to G'$, this number of geometric points is locally constant by [GD64, pp. IV.15.5.9.ii, IV.18.2.8]. □

entbygroup

Proposition B.4.2. *Let G/S be a flat group scheme of finite presentation. If H/S is a subgroup of G, flat over S, then G/H exists as an algebraic space, and as a scheme if G is an AF scheme. Furthermore $G \to G/H$ is an fppf morphism, G/H is flat over S, and the construction of this quotient commutes with arbitrary base change. And if G/S is smooth, G/H too.*

Proof. This is a particular case of the results of Appendix D. Indeed the stack quotient $[G/H]$ has trivial inertial, so is an algebraic space.

Since $G \to G/H$ is an fppf cover and $G \to S$ if flat, $G/H \to S$ is flat. If G/S is smooth, the fibers $(G/H)_s = G_s/H_s$ are smooth, so G/H is smooth over S (since it is flat over S). □

If H is as in Proposition B.4.2, since $H \to S$ is the pullback of $G \to G/H$, the properties of $H \to S$ reflect the properties of $G \to G/H$. But the converse is true: the pullback of $G \to G/H$ by itself is $G \times_S H \to G$, so is a pullback of $H \to S$. By descent, $G \to G/H$ has all properties of $H \to S$ that are stable by base change and fppf local on the base. In particular, $G \to G/H$ is proper if and only if $H \to S$ is proper.

[3] By the usual cancellation properties, if g, f are separated of finite type and $g \circ f$ is proper, then f is proper, and g is proper if f is surjective.

[4] Grothendieck proved that a proper quasi-finite morphism locally of finite presentation is finite as a corollary of his version of ZMT (Zariski's main theorem) [GD64, p. IV.8.12], and Deligne extended this result to the case to f quasi-finite universally closed separated locally of finite type.

C | ALGEBRAIC STACKS

CONTENTS

ap:stacks

References: [Stacks] (the canonical reference), [LM18; Ols16].

C.1 RINGS

Rings = locally presentable category, so equivalence with torsors on rings of finite presentation (by Diaconescu) = classifying topos of rings. Zariski topos = classifying topos of local ring (internally in the topos).

Applied to topological spaces: an internal ring = sheaf (of rings), an internal local ring = a locally ringed space.

The functor of global sections from locally ringed space to rings has an adjoint (by the adjoint functor theorem for presentable categories), which is fully faithful.

By the coyoneda lemma, there is an adjonction between presheafs on rings and locally ringed space. Schemes = locus where this is an equivalence of category (point of view of [DG70]).

C.2 SCHEMES

Schemes = Zariski locally affine = quotient of an affine by an open equivalence relation.

Three methods to see what it means to be covered by affine opens:

1. Can be seen via the embedding into locally ringed space (see the discussion above).

2. Purely functorialy: open immersion = finite presentation (this is functorial = commute with filtered limit) + formally étale + monomorphism (or finite presentation + flat + monomorphism).

   So can define an open immersion for a sheaf (in the Zariski topology) representable by affine space (we get exactly the schemes with affine diagonal). Disgression on equivalence of representability via pullbacks and representability of the diagonal (easy from the point of view of the internal logic of a category with pullbacks, this is the same proof as in Set).

   Bootstrap a second time to get schemes.

   Trick to get schemes in one step: by pullback we need to explain when $F \to \operatorname{Spec} A$ is open, but since an open immersion is a monomorphism we can cheat and say that it is so when its image coincide with the union of the image of a bunch of open morphisms $\operatorname{Spec} A_i \to \operatorname{Spec} A$.

3. The Zariski topos has a subobject classifier Ω (since it is a topos). We simply have $\Omega(A) = \{\text{the set of ideals}\}$, and a morphism $X \to Y$ is an open immersion (resp. a closed immersion) if it is the pullback of $1 \to \Omega$ (resp. $0 \to \Omega$).

C.3 ALGEBRAIC SPACES

Algebraic spaces = étale locally affine = quotient of an affine scheme by an étale equivalence relation. Bootstrap: fppf locally affine is already an algebraic space.

Explain why this is useful:

- fpqc descent of modules.
- fpqc descent of morphisms: fpqc = stable effective (regular) epimorphism so $\mathrm{Hom}(\cdot, X)$ is a sheaf in the fpqc topology, ie if $T' \to T$ is fpqc to give a morphism from T to X is the same as giving a morphism from T' to X which satisfy gluing conditions.

  This is also a descent morphism (by the monadic descent theorem [JT94; JT97; JT04]) so if $T' \to T$ is fpqc, to give a morphism from X to Y above T is the same as giving a morphism from $X_{T'}$ to $Y_{T'}$ above T' satisfying suitable compatibility conditions.

  Application: construct morphism fppf locally (map from $A \to \widehat{A}$, the Torelli morphism, we can thus suppose there is a base point).
- No fpqc descent of schemes

We can construct algebraic spaces étale or fppf locally! In some cases, algebraic spaces are automatically schemes:

algspaceisscheme

Example C.3.1.

- A quasi-separated group algebraic space over a field is a quasi-projective scheme [Art69b] (See also the proof of Corollary 2.3.5.)
- An abelian algebraic space is a scheme (Raynaud), cf Theorem 2.3.2. More generally, a proper commutative group algebraic space, which is locally of finite presentation, flat and cohomologically flat in dimension 0 is a scheme.
- A curve over a field (ie a proper algebraic space of dimension 1 over k) is a proper scheme.

C.4 ALGEBRAIC STACKS

Stacks (in groupoid) = internally a groupoid in the topos. Deligne-Mumford algebraic stack = stack with an étale cover by an algebraic space = quotient by an étale groupoid (ie as an étale presentation) = the inertia is unramified. Point of view of étendues [Pro96].

Artin algebraic stack = quotient by a smooth groupoid = quotient by an fppf groupoid = smooth or fppf cover by an étale space. An algebraic stack with trivial inertia is an algebraic space.

Representability by schemes vs by algebraic spaces.

If $f : X \to Y$ is representable, every notion that is fppf local on the base and stable by pullback behave well (even étale local for DM stacks) [Stacks, Tag 03YJ]. For a more general morphism this still work for morphisms which are smooth local on the source and target [Stacks, Tag 0CFY] (or even just étale local on the base and smooth local on target for DM morphisms [Stacks, Tag 06F7]).

C.4.1 *Artin's representability theorem*

Explain the results of [Art69b; Art74], extending the earlier Grothendieck-Murre result on representability of unramified functors [Mur64].

Key aspect played by Artin's approximation theorem: [Art69a], extended to general G-rings via the Neron-Popescu desingularisation theorem [Pop85], [Stacks, Tag 07BX]. This allows to approximate versal deformations: [CJ02]. For more aspects of Artin's approximation, see this nice survey [Gui11].

The representability theorem uses several steps:

1. existence of formally versal deformations;

2. algebraization of formally versal deformations;
3. openness of formal versality; and
4. formal versality implies formal smoothness.

As we have seen in Section 3.4, step 1 is solved by Schlessinger's criterion (for algebraic spaces) and Rim's extension (for algebraic stack) [Gro72, Exposé VI], cf [Stacks, Tag 06G7] for an excellent presentation. These conditions are elegantly reinterpreted as homogeneity conditions in [HR19]. They also require that the Deformation and Automorphism functors are coherent.

Step 2, algebraization is done by combining Grothendieck's existence/algebraicity theorem [FGI05, §8.4], [Stacks, Tag 087V], [Stacks, Tag 0886], [Stacks, Tag 0CYW] to get effectivity over the complete ring, and then Artin approximation [CJ02] to descend to an Henselian ring. By standard approximation [GD64, §IV.8] we have a cover which is (formally) versal at a point.

Step 3 ensures that the cover is formally versal in an open, so is formally smooth by Step 4. The functorial criterion for finite presentation allows to check that we are of finite presentation, hence smooth, hence we have found a smooth cover. Step 4 is automatic over a noetherian base by [GD64, p. IV.17.4.2], [Stacks, Tag 02HW]

Openness of formal versality is the hardest to check in practise, so several theories have been developed to deal with it: generally by constructing nice obstruction theories. Cf Artin [Art69b; Art74], the approach by the stack project [Stacks, Tag 07YF], see also [Hal13] for another approach and [HR19] for a comparison of all these methods.

Good surveys are [Ray71] for algebraic space and [Alp15] for algebraic stacks.

D COARSE MODULI SPACES AND QUOTIENTS

rsemoduli

Planned topics

D.1 QUOTIENTS

Description of quotients (Zariski quotients, geometric quotients, categorical quotients, GC quotients), quotients of finite groups, quotients of groupoids (and equivalence relations).

Particular case of quotients of AF scheme is a scheme:

An affine finite scheme (AF scheme) means that every finite set of points is contained in an affine open subscheme. See [Ryd13, Appendix B] for more on AF schemes.

This allows to construct quotient by a finite group by G by gluing together the affine case (in which case the quotient is simply given by taking the invariant sections) [Gro62, No 212, Theorem 5.1], [DA70, Exposés V et VIA], [Ryd13, Theorems 4.1 and 4.4]. See also the surveys by Raynaud: [Ray67a; Ray67b].

Case of a finite group acting on an algebraic space. Deligne proved that a (good) quotient of a separated algebraic space X by a finite locally free group scheme G acting on it always exist [Ryd13, Corollary 5.4].

Recover the construction of quotients of group schemes and abelian schemes as a special case (since algebraic group spaces over a field and abelian algebraic spaces are schemes), so refer to this section from Propositions 2.3.15 and B.1.4 and Appendix B.4.

Summary of all quotient constructions and their properties (eg when the quotient is simply the fppf sheafication, …).

D.2 COARSE MODULI SPACE

Link with the construction of coarse moduli spaces (for a finite inertia) [KM97; Con05; Ryd13]. This allows to construct quotients in algebraic spaces of fppf groupoids whose inertia is finite.

Note: also if the inertia of $\mathcal{X}$ is flat (locally of finite presentation), the coarse moduli space is just the associated fppf sheaf X since $\mathcal{X} \to X$ is a gerbe by [Stacks, Tag 06QB]. This is in particular the case for a quotient $[G/H]$ where H is a flat subgroup scheme of G, since the inertia $G \times G \times_G H \simeq H$.

Quotients by linear reductive groups [MFK94; Ses77] (linearly reductive vs geometrically reductive) and the stacky interpretation (good and adequate moduli spaces) [Alp13; Alp+14]. The étale local structure of separated Deligne Mumford stacks [AOV08; Ols+06], étale local structure of tame stacks [AOV08], extension of Luna's theorem [Lun73] and the étale local structure to non finite inertia [Alp10; AHR20; AHR19].

Current draft version

D.3 COARSE MODULI SPACES

Let $\mathcal{X}$ be a Deligne-Mumford stack of finite type over a Noetherian base S (from now on all our stacks will be assumed to be of finite type over a Noetherian base). In our settings, $\mathcal{X}$ will typically be a stack of abelian varieties of PEL type. In this section we summarize well known result on the geometry of $\mathcal{X}$ and its coarse moduli space.

By a point x of $\mathcal{X}$, we mean a point of the underlying topological space $|\mathcal{X}|$, and we implicitly take a representative $\operatorname{Spec} k \to \mathcal{X}$ of x. A T-point of $\mathcal{X}$ means a morphism $T \to \mathcal{X}$. We denote by $I_{\mathcal{X}}$ the inertia stack of $\mathcal{X}$, and if x is a point of $\mathcal{X}$, we usually denote I_x the pullback of $I_{\mathcal{X}}$ to x, this is simply the space $\operatorname{Aut}(x)$ of automorphisms (or stabilisers) of x. Since we assume $\mathcal{X}$ separated, I_x is in fact finite. The stabiliser I_x does not really depend on the

representative chosen since I_x is a pullback of the residual gerbe $G_x \to k(\xi)$ at x through $\operatorname{Spec} k \to k(\xi)$. We recall that a map $f : \mathcal{X} \to \mathcal{Y}$ is representable if and only if the induced map $I_{\mathcal{X}} \to \mathcal{X} \times_{\mathcal{Y}} I_{\mathcal{Y}}$ is a monomorphism, and that if f is unramified, then its diagonal is étale, hence $I_{\mathcal{X}} \to \mathcal{X} \times_{\mathcal{Y}} I_{\mathcal{Y}}$ is étale. So if f is representable and unramified, $I_{\mathcal{X}} \to \mathcal{X} \times_{\mathcal{Y}} I_{\mathcal{Y}}$ is an open immersion. Finally we identify open substacks of $\mathcal{X}$ with the underlying open topological spaces of $|\mathcal{X}|$.

A coarse moduli space X of $\mathcal{X}$ is an algebraic space X with a map $\pi : \mathcal{X} \to X$ such that π is categorical and induces a bijection $\pi : \mathcal{X}(k) \to X(k)$ for any algebraically closed field k. A coarse moduli space always exists:

Theorem D.3.1 (Keel-Mori)**.** *Let $\mathcal{X}$ be an Artin stack with finite inertia of finite type over a Noetherian base scheme S. Then there is a coarse moduli space $\pi : \mathcal{X} \to X$, where X is of finite type over S. The map π is a GC quotient, is proper, quasi-finite and separated if $\mathcal{X}$ is separated over S, and the construction is stable by flat base change.*

Proof. The original proof is in [KM97]. A proof relying on the language of stacks rather than groupoids is given in [Con05] where the Noetherian hypothesis on S is relaxed, and $\mathcal{X}$ is assumed to be locally of finite presentation. This last condition is relaxed in [Ryd13]. Since our $\mathcal{X}$ is a separated Deligne-Mumford stack, then its inertia I_X is finite so the Keel-Mori theorem applies.

We recall the following terminology from [MFK94] (see also [KM97, Definition 1.8] and [Ryd13, Definitions 2.2 and 6.1]): a map $q : \mathcal{X} \to Z$ is topological if q is a universal homeomorphism, and geometric if it is topological and furthermore $\mathcal{O}_Z \to q_*\mathcal{O}_{\mathcal{X}}$ is an isomorphism. A GC quotient is a geometric quotient that is also (uniformly) categorical, in particular it is a coarse moduli ([KM97, Definition 1.8] and [Ryd13, Definition 3.17 and Remark 3.18]).

Note that by Zarsiki Main Theorem, X is characterised by the fact that $\pi : \mathcal{X} \to X$ is proper quasi-finite such that $\mathcal{O}_X \simeq \pi_\star \mathcal{O}_{\mathcal{X}}$ on the étale site [Con05, §1]. □

When $\mathcal{X}$ is separated Deligne-Mumford, we can describe the coarse moduli space $\pi : \mathcal{X} \to X$ étale locally (since it is stable by flat pullback), as follow:

th:localstruct **Theorem D.3.2.** *Let $\mathcal{X}$ be a separated Deligne-Mumford stack, $\pi : \mathcal{X} \to X$ its coarce moduli. Let $x \in X(k)$ a point and I_x be the stabilizer of any point in $\mathcal{X}$ above x. Then étale-locally around x, there is an affine open U and a finite morphism $V \to U$ such that $\mathcal{X}_U := \mathcal{X} \times_X U = [V/I_x]$ is a I_x-gerbe, and $U = V/I_x$.*

Proof. See [AV02, Lemma 2.2.3] which shows that $\mathcal{X}$ is locally a quotient, and [Ols+06, Theorem 2.12] which shows that we can take the quotient to be by I_x. If $V = \operatorname{Spec} R$, then V/I_x is the affine scheme R^{I_x}. The fact that $U = \operatorname{Spec} R/I_x$ then follow easily from the theory of quotients on affine scheme, see for instance [Ryd13, §4] or [DR73, §I.8.2.2]. □

cor:hensellocal **Corollary D.3.3.** *Let $\mathcal{X}$ be a separated Deligne-Mumford stack, and $x \in \mathcal{X}(k)$ a point. Let $\widehat{\mathcal{O}}_{\mathcal{X},x}$ be the strict Hensel ring of $\mathcal{X}$ at x, then*

$$\widehat{\mathcal{O}}_{X,x} = \widehat{\mathcal{O}}^{I_x}_{\mathcal{X},x} \tag{D.1}$$ {eq:stric

Proof. This is an immediate application of Theorem D.3.2. See also [DR73, §I.8.2.1], which states that the kernel of the action of I_x acting on $\widehat{\mathcal{O}}_{\mathcal{X},x}$ is exactly given by the automorphisms of x that can be extended to $\operatorname{Spec} \widehat{\mathcal{O}}_{\mathcal{X},x} \to \mathcal{X}$. □

cor:genericiso **Corollary D.3.4.** *Let $\mathcal{X}$ be a separated Deligne-Mumford stack. Then the set U of points x such that I_x is trivial is an open substack (which may be empty), and $\pi : U \to \pi(U)$ is an isomorphism.*

cor:normal **Corollary D.3.5.** *Let $\mathcal{X}$ be a normal separated Deligne-Mumford stack. Then its coarce moduli space is normal.*

We will apply the Keel-Mori theorem to get the coarse moduli space $\mathcal{A}_{g,n}$ of $\mathcal{A}_{g,n}$. Mumford constructed $\mathcal{A}_{g,n}$ directly in [MFK94] using Geometric Invariant Theory and proved that it is a quasi-projective variety, so in particular a scheme (and not just an algebraic space).

Some care must be taken that the formation of coarse moduli spaces do commute with flat base change, but not with arbitrary base change. In particular the coarse moduli $\mathcal{A}_{g,n,p}$ of $\mathcal{A}_{g,n,p} := \mathcal{A}_{g,n} \otimes \mathbb{F}_p$ is not equal to $\mathcal{A}_{g,n} \otimes \mathbb{F}_p$.

In practice, this is not really a problem for two reasons. First the two spaces are topologically homeomorphic. Indeed let $T \to S$ be a morphism of algebraic spaces, $\mathcal{X}_T$ the base change of $\mathcal{X}$ to T and X_T the coarse moduli space

of $\mathcal{X}_T$. Then the natural map $\mathsf{X}_T \to X_T$ is an adequate homeomorphism in the sense of [Alp+14], and in particular is a universal homeomorphism [Alp+14, Main Theorem].

D.4 THE LOCAL STRUCTURE OF TAME STACKS

Furthermore, [AOV08] shows that there is an open set of tame points where the formation of the coarse moduli space commutes with arbitrary pullback. We recall [AOV08] that an Artin stack $\mathcal{X}$ with finite inertia is said to be tame if the map $\pi : \mathcal{X} \to X$ is cohomologically affine (see [Alp13]). And a finite fppf group scheme G/S is said to be linearly reductive if $BG \to S$ is tame ([AOV08, Definition 2.4], [Alp13, Definition 12.1]). In [AOV08], it is shown that a finite fppf group scheme G/S is linearly reductive if and only if its geometric fibers are geometrically reductive, if and only if its geometric fibers are locally (in the fppf topology) a split extension of a constant tame group by a group of multiplicative type.

A characterisation and the local structure of tame stacks is given by

ruct_tame

Theorem D.4.1. *Let $\mathcal{X}$ be a tame Artin stack with finite inertia. The stack $\mathcal{X}$ is tame if every geometric point $x \in \mathcal{X}(k)$ has a linearly reductive stabiliser $I_x \to \operatorname{Spec} k$. Furthermore if $\mathcal{X}$ is tame, then the formation of its coarse moduli space commutes with arbitrary base change.*

Conversely if a point $x \in \mathcal{X}(k)$ has linearly reductive stabiliser I_x, there exist an étale morphism $U \to X$ with U affine and whose image contains x, and a finite morphism $V \to U$ such that $\mathcal{X}_U \simeq [V/I_x]$ as algebraic stacks. In particular there is an open tame substack of $\mathcal{X}$ containing x. Furthermore, the image of U in X is Cohen-Macauley.

Proof. The étale local structure of a tame stack $\mathcal{X}$ is the main result of [AOV08]. Note that by contrast to Theorem D.3.2, this applies to Artin stack with finite inertia and not only to separated Deligne-Mumford stacks, but only at points with linearly reductive stabilizers. See the references in Remark D.5.2 for a generalisation to adequate moduli spaces.

Hochster-Roberts theorem [MFK94, Appendix 1.E] then shows that $U = V/I_x$ is Cohen-Macauley, so its image in X is Cohen-Macauley since this notion is local for the syntomic, hence étale, topology. □

In particular, if $\mathcal{X} = \mathcal{A}_g$, then since $\mathcal{A}_g = [\mathcal{A}_{g,n}/\operatorname{Sp}(n,\mathbb{Z})]$ is a $\operatorname{Sp}(n,\mathbb{Z})$ gerbe and $\mathcal{A}_{g,n}$ has trivial inertia for $n \geq 3$, this shows that there is a p_0 such that $\mathcal{A}_g$ is tame at every abelian variety defined over a field of characteristic $p > p_0$.

D.5 ÉTALE SLICES

We need one last result on when an étale map between algebraic stacks induce an étale map on their coarse moduli spaces.

rongetale

Theorem D.5.1. *Let $f : \mathcal{X} \to \mathcal{Y}$ be a representable and unramified morphism of algebraic stacks with finite inertia. Then the set of points where f is stabilizer preserving (meaning that the monomorphism on inertia $I_x \to I_{f(x)}$ induced by f is an isomorphism) is an open $\mathcal{U}$, and the canonical morphism $I_{\mathcal{U}} \to I_{\mathcal{Y}} \times_{\mathcal{Y}} \mathcal{U}$ is an isomorphism.*

If f is étale and $\mathcal{U} = \mathcal{X}$, that is if f is stabilizer preserving at every point, then the induced map $f_0 : X \to Y$ is étale, and even strongly étale (meaning that $\mathcal{X} = X \times_Y \mathcal{Y}$).

Proof. If $\mathcal{X}$ and $\mathcal{Y}$ are separated Deligne-Mumford stack, the fact that the induced map is étale comes from Corollary D.3.3. The general case is in [Ryd13, Proposition 6.5 and Theorem 6.10]. In loc. cit. stabilizer preserving is called fixed point reflecting, but we have prefered to use the terminology of [Stacks]. The fact that f_0 is strongly étale comes from the cartesian diagram in [Ryd13, Theorem 6.10], see also [AHR19, Theorem 3.14] where this is proved more generally for adequate moduli spaces. □

te_moduli

Remark D.5.2. In [MFK94] and [Ses77], Mumford and Seshadri study quotients of schemes by (linearly) reductive groups. This has been generalised in the context of stacks by Alper, which introduces the notion of good moduli spaces in [Alp13] (this includes GIT quotients by linearly reductive groups), and the notion of adequate moduli

space in [Alp+14] (this includes GIT quotients by geometrically reductive groups). In particular if $\mathcal{X}$ is an Artin stack with finite inertia, its coarse moduli is adequate [Alp+14, Proposition 8.2.1].

Most of the results of this section can be extended to good and adequate moduli spaces. For instance adequate moduli spaces are stable by flat base change [Alp+14], while good moduli spaces are stable by arbitrary base change [Alp13]. Alper defines in [Alp13, §7] a tame moduli spaces $\pi : \mathcal{X} \to X$ as a good moduli which induces a bijection on geometric points. This extends the notion of tame spaces from [AOV08].

The local structure and characterisation of Theorem D.4.1 is still valid for good moduli spaces, but much more difficult to prove: see [AHR20, Theorem 1.2] and [AHR19, Theorem 1.1 and Proposition 13.4].

Finally Luna's étale slice theorem [Lun73] can be used to study the local structure of the quotient of a scheme by a linearly reductive group scheme. See also the generalisation to stacks and the relative setting in [AHR20, Theorem 1.1] and [AHR19, Theorem 19.4], and the generalisation of Luna's fundamental lemma in [AHR19, Theorem 3.14].

The coarse moduli of principally polarised abelian varieties is constructed by Mumford as a quotient of a locally closed subscheme of the Hilbert scheme by the reductive group PGL_n (and its coarse moduli space as the corresponding GIT quotient). Over $\mathbb{Z}[1/2]$, the coarse moduli of hyperelliptic curves can be constructed as the quotient of the open subvariety of $\mathbb{P}^{2g+2}$ given by the discriminant by PGL_2 (since the map from stack of hyprelliptic curves to its coarse space factorize through $[\mathbb{P}^{2g+2}/\mathrm{PGL}_2]$). One can then use Luna's étale slice theorem to study the local structure of these spaces.

ch2008tame [AOV08] D. Abramovich, M. Olsson, and A. Vistoli. "Tame stacks in positive characteristic". In: *Annales de l'institut Fourier*. Vol. 58. 4. 2008, pp. 1057–1091 (cit. on pp. 97, 99, 100).

actifying [AV02] D. Abramovich and A. Vistoli. "Compactifying the space of stable maps". In: *Journal of the American Mathematical Society* 15.1 (2002), pp. 27–75 (cit. on p. 98).

erspecial [AP15] J. D. Achter and R. Pries. "Superspecial rank of supersingular abelian varieties and Jacobians". In: *Journal de théorie des nombres de Bordeaux* 27.3 (2015), pp. 605–624 (cit. on p. 11).

4adequate [Alp+14] J. Alper et al. "Adequate moduli spaces and geometrically reductive group schemes". In: (2014) (cit. on pp. 97, 99, 100).

2010local [Alp10] J. Alper. "On the local quotient structure of Artin stacks". In: *Journal of Pure and Applied Algebra* 214.9 (2010), pp. 1576–1591 (cit. on p. 97).

r2013good [Alp13] J. Alper. "Good moduli spaces for Artin stacks". In: *Annales de l'Institut Fourier*. Vol. 63. 6. 2013, pp. 2349–2402 (cit. on pp. 97, 99, 100).

2015artin [Alp15] J. Alper. *Artin algebraization and quotient stacks*. 2015. arXiv: 1510.07804 [math.AG] (cit. on p. 95).

2019etale [AHR19] J. Alper, J. Hall, and D. Rydh. "The étale local structure of algebraic stacks". 2019. arXiv: 1912.06162 (cit. on pp. 97, 99, 100).

r2020luna [AHR20] J. Alper, J. Hall, and D. Rydh. "A Luna étale slice theorem for algebraic stacks". In: *Annals of Mathematics* 191.3 (2020), pp. 675–738 (cit. on pp. 97, 100).

erMap2017 [And17] Y. André. "On the Kodaira–Spencer map of abelian schemes". In: *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)* 17.4 (2017), pp. 1397–1416 (cit. on pp. 59, 60).

Forms2005 [AG05] F. Andreatta and E. Z. Goren. "Hilbert modular forms: mod p and p-adic aspects". In: *Mem. Amer. Math. Soc.* 173.819 (2005), pp. vi+100 (cit. on p. 59).

adichodge [ABB+19] F. Andreatta, R. Brasca, O. Brinon, X. Caruso, B. Chiarellotto, G. F. i Montplet, S. Hattori, N. Mazzari, S. Panozzo, M. Seveso, and G. Yamashita. *An excursion into p-adic Hodge theory: from foundations to recent trends*. Vol. 54. Panoramas et synthèses. SMF, 2019, pp. xii+268. ISBN: 978-2-85629-913-5 (cit. on p. 11).

72theorie [AGV72] M. Artin, A. Grothendieck, and J. Verdier. *Théorie des topos et cohomologie étale des schémas. (SGA4)*. 1972 (cit. on p. 83).

1966etale [Art66] M. Artin. "The étale topology of schemes". In: *Proc. Internat. Congr. Math.(Moscow, 1966)*. 1966, pp. 44–56 (cit. on p. 11).

algebraic [Art69a] M. Artin. "Algebraic approximation of structures over complete local rings". In: *Publications Mathématiques de l'Institut des Hautes Études Scientifiques* 36.1 (1969), pp. 23–58 (cit. on pp. 33, 94).

raization [Art69b] M. Artin. "Algebraization of formal moduli. I". In: *Global analysis (papers in honor of K. Kodaira)* (1969), pp. 21–71 (cit. on pp. 14, 94, 95).

974versal [Art74] M. Artin. "Versal deformations and algebraic stacks". In: *Inventiones mathematicae* 27.3 (1974), pp. 165–189 (cit. on pp. 94, 95).

ients1966 [BB66] W. L. Baily Jr. and A. Borel. "Compactification of Arithmetic Quotients of Bounded Symmetric Domains". In: *Ann. of Math. (2)* 84 (1966). https://mathscinet.ams.org/mathscinet-getitem?mr=216035, pp. 442–528. ISSN: 0003-486X. DOI: 10.2307/1970457 (cit. on p. 53).

hnan_2018 [BD18] J. S. Balakrishnan and N. Dogra. "Quadratic Chabauty and rational points, I: p-adic heights". In: *Duke Mathematical Journal* 167.11 (Aug. 2018), pp. 1981–2038. ISSN: 0012-7094. DOI: 10.1215/00127094-2018-0013. URL: http://dx.doi.org/10.1215/00127094-2018-0013 (cit. on p. 1).

mo16136 [BCn10] BCnrd. *Example of connected-etale sequence for group schemes over a Henselian field?* MathOverflow. Feb. 23, 2010. URL: https://mathoverflow.net/q/16136 (cit. on p. 36).

t2006cohomologie [Ber06] P. Berthelot. *Cohomologie Cristalline des Schemas de Caracteristique $p > 0$*. Vol. 407. Springer, 2006 (cit. on p. 12).

bhattav [Bha] B. Bhatt. *Math 731: topics in algebraic geometry I – Abelian varieties*. Course notes. URL: http://www-personal.umich.edu/~stevmatt/abelian_varieties.pdf (cit. on pp. 8, 15).

t2011crystalline [BJ11] B. Bhatt and A. J. de Jong. *Crystalline cohomology and de Rham cohomology*. 2011. arXiv: 1110.5001 [math] (cit. on p. 12).

umim_mordellweil [BSa] B. Bhatt, A. Snowden, and al. *Faltings's Proof of the Mordell Conjecture*. URL: https://web.math.princeton.edu/~takumim/Mordell.pdf (cit. on p. 1).

birch2004heegner [Bir04] B. Birch. "Heegner points: the beginnings". In: *Special values of Rankin L-series, Math. Sci. Res. Inst. Publications* 49 (2004), pp. 1–10 (cit. on p. 1).

BiLaCAV [BL04] C. Birkenhake and H. Lange. *Complex abelian varieties*. Second. Vol. 302. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Berlin: Springer-Verlag, 2004, pp. xii+635. ISBN: 3-540-20488-1 (cit. on pp. 1, 5, 7, 53, 55).

borel2012linear [Bor12] A. Borel. *Linear algebraic groups*. Vol. 126. Springer Science & Business Media, 2012 (cit. on p. 89).

bosch2012neron [BLR12] S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron models*. Vol. 21. Springer Science & Business Media, 2012 (cit. on pp. 1, 13–15, 17, 20, 21, 23, 24, 26–33, 35, 36, 82, 87, 90).

lauterIsogenies [BGL11] R. Bröker, D. Gruenewald, and K. Lauter. "Explicit CM theory for level 2-structures on abelian surfaces". In: *Algebra & Number Theory* 5.4 (2011), pp. 495–528. arXiv: 0910.1848 (cit. on p. 76).

bruin2011tate [Bru11] P. Bruin. "The Tate pairing for abelian varieties over finite fields". In: *J. de theorie des nombres de Bordeaux* 23.2 (2011), pp. 323–328 (cit. on pp. 46, 48).

er2008modular123 [BGH+08] J. H. Bruinier, G. van der Geer, G. Harder, and D. Zagier. *The 1-2-3 of modular forms: lectures at a summer school in Nordfjordeid, Norway*. Springer Science & Business Media, 2008 (cit. on pp. 53, 55).

16transformation [Can16] L. Candelori. "The transformation laws of algebraic theta functions". 2016. arXiv: 1609.04486 (cit. on p. 63).

bri2020algebraic [Can20] L. Candelori. "The algebraic functional equation of Riemann's theta function". In: *Annales de l'Institut Fourier*. Vol. 70. 2. 2020, pp. 809–830. arXiv: 1512.04415 (cit. on p. 63).

ardona2005curves [CNP05] G. Cardona, E. Nart, and J. Pujolàs. "Curves of genus two over fields of even characteristic". In: *Mathematische Zeitschrift* 250.1 (2005), pp. 177–201 (cit. on pp. 23, 67).

cardona2005field [CQ05] G. Cardona and J. Quer. "Field of moduli and field of definition for curves of genus 2". In: *Computational aspects of algebraic curves*. World Scientific, 2005, pp. 71–83 (cit. on pp. 67, 72).

2019introduction [Car19] X. Caruso. *An introduction to p-adic period rings*. 2019. arXiv: 1908.08424 [math.NT] (cit. on p. 11).

hamartin2013tour [Cas13] S. Casalaina-Martin. *A tour of stable reduction with applications*. 2013. arXiv: 1207.1048 [math.AG] (cit. on p. 29).

vcius2017modular [Čes17] K. Česnavičius. "A modular description of $X_0(n)$". In: *Algebra & Number Theory* 11.9 (2017), pp. 2001–2089 (cit. on p. 54).

compactification [Cha85] C.-L. Chai. *Compactification of Siegel moduli schemes*. Vol. 107. Cambridge University Press, 1985 (cit. on p. 29).

chai1990appendix [Cha90] C.-L. Chai. "Appendix to" The Iwasawa Conjecture for Totally Real Fields": Arithmetic Minimal Compactification of the Hilbert-Blumenthal Moduli Spaces". In: *Annals of Mathematics* 131.3 (1990), pp. 541–554 (cit. on pp. 54, 58, 59).

chai2013complex [CCO13] C.-L. Chai, B. Conrad, and F. Oort. *Complex multiplication and lifting problems*. Vol. 195. American Mathematical Soc., 2013 (cit. on p. 38).

hai1990bad [CN90] C.-L. Chai and P. Norman. "Bad reduction of the Siegel moduli scheme of genus two with Γo (p)-level structure". In: *American Journal of Mathematics* (1990), pp. 1003–1071 (cit. on pp. 37, 54).

2009moduli [CO09] C.-L. Chai and F. Oort. "Moduli of abelian varieties and p-divisible groups". In: *Arithmetic Geometry. Clay Math. Proc* 8 (2009), pp. 441–536 (cit. on pp. 37, 54).

belian2000 [Cv00] C. Ciliberto and G. van der Geer. "The moduli space of abelian varieties and the singularities of the theta divisor". In: *Surveys in differential geometry*. Vol. 7. Surv. Differ. Geom. Int. Press, Somerville, MA, 2000, pp. 61–81 (cit. on p. 60).

Clebsh [Cle72] A. Clebsh. "Theorie der Binärien Algebraischen Formen". In: *Verlag von B. G.* (1872) (cit. on p. 68).

extics2017 [CFv17] F. Cléry, C. Faber, and G. van der Geer. "Covariants of binary sextics and vector-valued Siegel modular forms of genus two". In: *Math. Ann.* 369.3-4 (2017), pp. 1649–1669 (cit. on p. 69).

017modular [CS17] H. Cohen and F. Strömberg. *Modular forms*. Vol. 179. American Mathematical Soc., 2017 (cit. on p. 53).

_317__39_0 [Colo8] Collectif. "Compter (rapidement) le nombre de solutions d'équations dans les corps finis". fr. In: *Séminaire Bourbaki - Volume 2006/2007 - Exposés 967-981*. Astérisque 317. talk:968. Société mathématique de France, 2008, pp. 39–90. URL: http://www.numdam.org/item/AST_2008__317__39_0 (cit. on p. 1).

sification [Cono4] B. Conrad. *Classification of quasi-finite étale separated schemes*. 2004. URL: http://math.stanford.edu/~conrad/vigregroup/vigre03/zmt.pdf (cit. on p. 84).

ad2005keel [Cono5] B. Conrad. "Keel–Mori theorem via stacks". In: *preprint* (2005) (cit. on pp. 97, 98).

008several [Cono8] B. Conrad. "Several approaches to non-archimedean geometry". In: *p-adic geometry*. 2008, pp. 9–63 (cit. on p. 1).

ellSeminar [Con+11] B. Conrad et al. *Mordell Seminar*. Number theory learning seminar. 2011. URL: http://virtualmath1.stanford.edu/~conrad/mordellsem/ (cit. on pp. 1, 23, 26–34, 37, 84, 86–88).

-reductive [Con14] B. Conrad. "Reductive group schemes". In: *Autour des schémas en groupes* 1 (2014), pp. 93–444 (cit. on pp. 86, 89).

2015pseudo [CGP15] B. Conrad, O. Gabber, and G. Prasad. *Pseudo-reductive groups*. Vol. 26. Cambridge University Press, 2015 (cit. on p. 89).

roximation [CJo2] B. Conrad and A. J. de Jong. "Approximation of versal deformations". In: *Journal of Algebra* 255.2 (2002), pp. 489–515 (cit. on pp. 94, 95).

structure [CP17] B. Conrad and G. Prasad. "Structure and classification of pseudo-reductive groups". In: *Proc. Symp. Pure Math*. Vol. 94. 2017, pp. 127–276 (cit. on p. 89).

computing [CE14] J.-M. Couveignes and T. Ezome. "Computing functions on Jacobians and their quotients". In: *LMS Journal of Computation and Mathematics* 18.1 (2014), pp. 555–577. arXiv: 1409.0481 (cit. on p. 43).

98barsotti [De 98] A. De Jong. "Barsotti-Tate groups and crystals". In: *Proceedings of the International Congress of Mathematicians*. Vol. 2. 1998, pp. 259–265 (cit. on pp. 28, 30, 37).

ourbes1973 [DR73] P. Deligne and M. Rapoport. "Les schémas de modules de courbes elliptiques". In: *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*. 1973, 143–316. Lecture Notes in Math., Vol. 349 (cit. on pp. 54, 57, 58, 91, 98).

ducibility [DM69] P. Deligne and D. Mumford. "The irreducibility of the space of curves of given genus". In: *Publications Mathématiques de l'Institut des Hautes Études Scientifiques* 36.1 (1969), pp. 75–109 (cit. on pp. 29, 33–35, 65).

gularites [DP94] P. Deligne and G. Pappas. "Singularités des espaces de modules de Hilbert, en les caractéristiques divisant le discriminant". In: *Compositio Mathematica* 90.1 (1994), pp. 59–79 (cit. on p. 58).

970schemas [DA70] M. Demazure and M. Artin. *Schémas en groupes (SGA3)*. Springer Berlin, Heidelberg, New York, 1970 (cit. on pp. 12, 85–89, 97).

970groupes [DG70] M. Demazure and P. Gabriel. *Groupes algébriques*. Vol. 1. Masson et Cie, 1970 (cit. on pp. 88, 93).

ospinesculifting [Dos] G. Dospinescu. *Lifting abelian schemes: theorems of Serre-Tate and Grothendieck*. URL: http://perso.ens-lyon.fr/gabriel.dospinescu/Serre-Tate.pdf (cit. on p. 38).

kies1992explicit [Elk92] N. Elkies. "Explicit isogenies". In: *manuscript, Boston MA* (1992) (cit. on p. 1).

DRreportClassCRT [ER13] A. Enge and D. Robert. "Computing class polynomials in genus 2". Apr. 2013. URL: http://www.normalesup.org/~robert/pro/publications/reports/2013-04-class_poly_g2.pdf (cit. on pp. 75, 77, 78).

gs1986finiteness [Fal86] G. Faltings. "Finiteness theorems for abelian varieties over number fields". In: *Arithmetic geometry*. Springer, 1986, pp. 9–26 (cit. on pp. 1, 32, 37).

s1988crystalline [Fal88a] G. Faltings. "Crystalline cohomology and p-adic Galois-representations". In: *Algebraic analysis, geometry, and number theory* (1988) (cit. on p. 11).

gs1988padichodge [Fal88b] G. Faltings. "p-adic Hodge theory". In: *Journal of the American Mathematical Society* 1.1 (1988), pp. 255–299 (cit. on p. 11).

ianVarieties1990 [FC90] G. Faltings and C.-L. Chai. *Degeneration of abelian varieties*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) 22. Springer-Verlag, Berlin, 1990 (cit. on pp. 1, 12, 13, 26, 32, 54, 56–59, 63).

ings1984rational [FWG+84] G. Faltings, G. Wüstholz, F. Grunewald, N. Schappacher, and U. Stuhler. *Rational points*. Springer, 1984 (cit. on p. 1).

fgaexplained [FGI05] B. Fantechi, L. Gottsche, and L. Illusie. *Fundamental algebraic geometry: Grothendieck's FGA explained*. 123. American Mathematical Soc., 2005 (cit. on pp. 38, 81, 95).

raicGeometry2005 [FGI+05] B. Fantechi, L. Göttsche, L. Illusie, S. L. Kleiman, N. Nitsure, and A. Vistoli. *Fundamental algebraic geometry*. Mathematical Surveys and Monographs 123. American Mathematical Society, Providence, RI, 2005 (cit. on p. 60).

aine1982certains [Fon82] J.-M. Fontaine. "Sur certains types de représentations p-adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate". In: *Annals of Mathematics* 115.3 (1982), pp. 529–577 (cit. on p. 11).

frey1986strong [FR86] G. Frey and H.-G. Rück. "The strong Lefschetz principle in algebraic geometry". In: *manuscripta mathematica* 55.3-4 (1986), pp. 385–401 (cit. on p. 18).

frey1994remark [FR94] G. Frey and H.-G. Rück. "A remark concerning $\mathfrak{m}$-divisibility and the discrete logarithm in the divisor class group of curves". In: *Mathematics of computation* 62.206 (1994), pp. 865–874 (cit. on pp. 47, 49).

CardonaNart [GNP] C. Gabriel, E. Nart, and J. Pujolàs. "Curves of genus two over fields of even characteristic". In: () (cit. on pp. 70, 72, 73).

s2002generalized [Gar02] T. Garefalakis. "The generalized Weil pairing and the discrete logarithm problem on elliptic curves". In: *LATIN 2002: Theoretical Informatics*. Springer, 2002, pp. 118–130 (cit. on p. 48).

rySurveyComptage [Gau04] P. Gaudry. "Algorithmes de comptage de points d'une courbe définie sur un corps fini". 2004. URL: http://www.loria.fr/~gaudry/publis/pano.pdf (cit. on p. 1).

2014introduction [Gil14] P. Gille. *Introduction to affine algebraic groups in positive characteristic*. 2014. URL: http://math.univ-lyon1.fr/homes-www/gille/prenotes/lyon_pg2014.pdf (cit. on pp. 85, 87–89).

goren2012genus [GL12] E. Z. Goren and K. E. Lauter. "Genus 2 curves with complex multiplication". In: *International Mathematics Research Notices* 2012.5 (2012), pp. 1068–1142 (cit. on pp. 70, 78).

gross1984heegner [Gro84] B. Gross. *Heegner points on Xo (N)*. 1984 (cit. on p. 1).

mo22955 [Gro10] P. Gross. *Smooth linear algebraic groups over the dual numbers*. MathOverflow. Apr. 29, 2010. URL: https://mathoverflow.net/q/22955 (cit. on p. 87).

ieck1964elements [GD64] A. Grothendieck and J. Dieudonné. "Eléments de géométrie algébrique". In: *Publ. math. IHES* 20.24 (1964), p. 1965 (cit. on pp. 12, 15, 16, 19, 20, 27, 30–32, 58, 81–85, 90, 91, 95).

ck1962fondements [Gro62] A. Grothendieck. *Fondements de la géométrie algébrique: extraits du Séminaire Bourbaki, 1957-1962*. Secrétariat mathématique, 1962 (cit. on pp. 14, 97).

6theoreme [Gro66a] A. Grothendieck. "Un théorème sur les homomorphismes de schémas abéliens". In: *Inventiones mathematicae* 2.1 (1966), pp. 59–78 (cit. on pp. 1, 37).

6avscheme [Gro66b] A. Grothendieck. "Un théorème sur les homomorphismes de schémas abéliens". In: *Inventiones mathematicae* 2.1 (1966), pp. 59–78 (cit. on p. 17).

evetement [Gro71] A. Grothendieck. "Revêtement étales et groupe fondamental (SGA1)". In: *Lecture Note in Math.* 224 (1971) (cit. on pp. 11, 36).

72groupes [Gro72] A. Grothendieck. *Groupes de Monodromie en Géométrie Algébrique: SGA 7*. Springer-Verlag, 1972 (cit. on pp. 11, 12, 28–30, 95).

aumeartin [Gui11] R. Guillaume. "Artin Approximation". In: (2011). URL: http://iml.univ-mrs.fr/~rond/Artin_survey.pdf (cit. on p. 94).

Gundlach63 [Gun63] K.-B. Gundlach. "Die Bestimmung der Funktionen zur Hilbertschen Modulgruppe des Zahlkörpers $\mathbb{Q}(\sqrt{5})$". In: *Math. Annalen* 152 (1963), pp. 226–256 (cit. on p. 68).

Gundlach65 [Gun65] K.-B. Gundlach. "Die Bestimmung der Funktionen zu einigen Hilbertschen Modulgruppen". In: *Journal für die reine und angewandte Mathematik* 220 (1965) (cit. on p. 68).

3openness [Hal13] J. Hall. *Openness of versality via coherent functors*. 2013. arXiv: 1206.4182 [math.AG] (cit. on p. 95).

Hall_2019 [HR19] J. Hall and D. Rydh. "Artin's criteria for algebraicity revisited". In: *Algebra & Number Theory* 13.4 (May 2019), pp. 749–796. ISSN: 1937-0652. DOI: 10.2140/ant.2019.13.749. URL: http://dx.doi.org/10.2140/ant.2013.13.749 (cit. on p. 95).

algebraic [Har13] R. Hartshorne. *Algebraic geometry*. Vol. 52. Springer Science & Business Media, 2013 (cit. on p. 81).

ss2004note [Heß04] F. Heß. "A note on the Tate pairing of curves over finite fields". In: *Archiv der Mathematik* 82.1 (2004), pp. 28–32 (cit. on p. 49).

2computing [Hes02] F. Hess. "Computing Riemann–Roch spaces in algebraic function fields and related topics". In: *Journal of Symbolic Computation* 33.4 (2002), pp. 425–445 (cit. on p. 20).

iophantine [HS13] M. Hindry and J. H. Silverman. *Diophantine geometry: an introduction*. Vol. 201. Springer Science & Business Media, 2013 (cit. on p. 1).

ective1967 [Igu67] J.-I. Igusa. "Modular forms and projective invariants". In: *Amer. J. Math.* 89 (1967), pp. 817–855 (cit. on p. 71).

rithmetic [Igu60] J.-i. Igusa. "Arithmetic variety of moduli for genus two". In: *Annals of Mathematics* (1960), pp. 612–649 (cit. on pp. 67–70, 72, 73).

962siegel [Igu62] J.-i. Igusa. "On Siegel modular forms of genus two". In: *American Journal of Mathematics* 84.1 (1962), pp. 175–200 (cit. on pp. 67, 71).

964siegel [Igu64] J.-i. Igusa. "On Siegel modular forms of genus two (II)". In: *American Journal of Mathematics* 86.2 (1964), pp. 392–412 (cit. on p. 67).

966graded [Igu66] J.-i. Igusa. "On the graded ring of theta-constants (II)". In: *American Journal of Mathematics* 88.1 (1966), pp. 221–236 (cit. on p. 53).

972graded [Igu72a] J.-i. Igusa. "Graded Rings of Theta Constants". In: *Theta Functions*. Springer, 1972, pp. 173–224 (cit. on p. 53).

gusaTheta [Igu72b] J.-i. Igusa. *Theta functions*. Die Grundlehren der mathematischen Wissenschaften, Band 194. New York: Springer-Verlag, 1972, pp. x+232 (cit. on p. 53).

a1979ring [Igu79] J.-i. Igusa. "On the ring of modular forms of degree two over Z". In: *American Journal of Mathematics* 101.1 (1979), pp. 149–183 (cit. on p. 67).

2cotangent [Ill72] L. Illusie. "Cotangent complex and deformations of torsors and group schemes". In: *Toposes, algebraic geometry and logic*. Springer, 1972, pp. 159–189 (cit. on p. 38).

79complexe [Ill79] L. Illusie. "Complexe de de Rham-Witt et cohomologie cristalline". In: *Annales scientifiques de l'École Normale Supérieure*. Vol. 12. 4. 1979, pp. 501–661 (cit. on p. 12).

illusie127exp [Ill85] L. Illusie. "Déformations de groupes de Barsotti-Tate, d'après A. Grothendieck". In: *Astérisque* 127 (1985). Exp. VI in: Séminaire sur les pinceaux arithmétiques: la conjecture de Mordell (L. Szpiro), pp. 151–198 (cit. on pp. 37, 38).

e1994crystalline [Ill94] L. Illusie. "Crystalline cohomology". In: *Motives (Seattle, WA, 1991)* 55 (1994), pp. 43–70 (cit. on p. 12).

2015grothendieck [Ill15] L. Illusie. "Grothendieck at Pisa: crystals and Barsotti-Tate groups". In: *Colloquium De Giorgi 2013 and 2014*. Springer. 2015, pp. 79–107 (cit. on pp. 1, 37, 38).

elidze1994facets [JT94] G. Janelidze and W. Tholen. "Facets of descent, I". In: *Applied Categorical Structures* 2.3 (1994), pp. 245–281 (cit. on p. 94).

elidze1997facets [JT97] G. Janelidze and W. Tholen. "Facets of descent, II". In: *Applied Categorical Structures* 5.3 (1997), pp. 229–248 (cit. on p. 94).

elidze2004facets [JT04] G. Janelidze and W. Tholen. "Facets of Descent III: Monadic descent for rings and algebras". In: *Applied Categorical Structures* 12.5-6 (2004), pp. 461–477 (cit. on p. 94).

dejong1991moduli [Jon91] A. J. de Jong. *The Moduli Spaces of Principally Polarized Abelian Varieties with $\Gamma_0(p)$-level Structure*. Rijksuniversiteit Utrecht. Mathematisch Instituut, 1991 (cit. on p. 54).

dejong1993moduli [Jon93a] A. J. de Jong. "The moduli spaces of polarized abelian varieties". In: *Mathematische Annalen* 295.1 (1993), pp. 485–503 (cit. on p. 54).

998homomorphisms [Jon98] A. J. de Jong. "Homomorphisms of Barsotti-Tate groups and crystals in positive characteristic". In: *Inventiones mathematicae* 134.2 (1998), pp. 301–333 (cit. on pp. 28, 30, 37).

jong1993moduli [Jon93b] A. de Jong. "The moduli spaces of polarized abelian varieties". In: *Mathematische Annalen* 295.1 (1993), pp. 485–503. ISSN: 0025-5831 (cit. on p. 56).

kani1994elliptic [Kan94] E. Kani. "Elliptic curves on abelian surfaces". In: *manuscripta mathematica* 84.1 (1994), pp. 199–223 (cit. on p. 20).

kani2016moduli [Kan16] E. Kani. "The moduli spaces of Jacobians isomorphic to a product of two elliptic curves". In: *Collectanea mathematica* 67.1 (2016), pp. 21–54 (cit. on p. 20).

kani2019elliptic [Kan19a] E. Kani. "Elliptic subcovers of a curve of genus 2. I. The isogeny defect". In: *Annales mathématiques du Québec* 43.2 (2019), pp. 281–303 (cit. on pp. 20, 67).

kanigeneralized [Kan19b] E. Kani. *Generalized Humbert Schemes and Intersections of Humbert Surfaces*. 2019. URL: https://mast.queensu.ca/~kani/papers/interHum11.pdf (cit. on p. 67).

katz1981serre [Kat81] N. Katz. "Serre-Tate local moduli". In: *Surfaces algébriques*. Springer, 1981, pp. 138–202 (cit. on pp. 37, 38).

katz1973padic [Kat73] N. M. Katz. "P-adic properties of modular schemes and modular forms". In: *Modular functions of one variable III*. Springer, 1973, pp. 69–190 (cit. on p. 54).

tz1985arithmetic [KM85] N. M. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*. 108. Princeton University Press, 1985 (cit. on p. 54).

laya2001counting [Ked01] K. Kedlaya. "Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology". 2001. arXiv: math/0105031 (cit. on p. 1).

aya2004computing [Ked04] K. S. Kedlaya. "Computing zeta functions via p-adic cohomology". In: *International Algorithmic Number Theory Symposium*. Springer. 2004, pp. 1–17 (cit. on p. 1).

a2007padicschool [Ked07] K. S. Kedlaya. "p-adic cohomology: from theory to practice". In: *Arizona Winter School* (2007) (cit. on p. 1).

kedlaya2004padic [Ked16a] K. S. Kedlaya. *p-adic cohomology*. 2016. arXiv: math/0601507 (cit. on p. 1).

notesisocrystals [Ked16b] K. S. Kedlaya. *Notes on isocrystals*. 2016. arXiv: 1606.01321 [math.NT] (cit. on p. 1).

eel1997quotients [KM97] S. Keel and S. Mori. "Quotients by groupoids". In: *Annals of mathematics* 145.1 (1997), pp. 193–213 (cit. on pp. 97, 98).

plication [Kem88] G. Kempf. "Multiplication over abelian varieties". In: *American Journal of Mathematics* 110.4 (1988), pp. 765–773 (cit. on p. 63).

989linear [Kem89a] G. Kempf. "Linear systems on abelian varieties". In: *American Journal of Mathematics* 111.1 (1989), pp. 65–94 (cit. on p. 63).

992kummer [Kem92] G. Kempf. "Equations of Kümmer Varieties". In: *American Journal of Mathematics* 114.1 (1992), pp. 229–232 (cit. on p. 63).

3geometry [Kem73] G. Kempf. "On the geometry of a theorem of Riemann". In: *Annals of Mathematics* (1973), pp. 178–185 (cit. on p. 22).

rojective [Kem89b] G. Kempf. "Projective coordinate rings of abelian varieties". In: *Algebraic analysis, geometry and number theory* (1989), pp. 225–236 (cit. on p. 63).

f1990some [Kem90] G. R. Kempf. "Some wonderful rings in algebraic geometry". In: *Journal of Algebra* 134.1 (1990), pp. 222–224 (cit. on p. 63).

2004linear [Khu04] K. Khuri-Makdisi. "Linear algebra algorithms for divisors on an algebraic curve". In: *Mathematics of Computation* 73.245 (2004), pp. 333–357 (cit. on p. 20).

totically [Khu07] K. Khuri-Makdisi. "Asymptotically fast group operations on Jacobians of general curves". In: *Mathematics of Computation* 76.260 (2007), pp. 2213–2239 (cit. on pp. 20, 22).

2020degree [Kie20] J. Kieffer. "Degree and height estimates for modular equations on PEL Shimura varieties". Accepté à London Mathematical Society. 2020. arXiv: 2001.04138 [math.AG]. HAL: hal-02436057. (Cit. on pp. 54, 56, 58).

ogeniesg2 [KPR20] J. Kieffer, A. Page, and D. Robert. "Computing isogenies from modular equations between Jacobians of genus 2 curves". Oct. 2020. arXiv: 2001.04137 [math.AG]. URL: http://www.normalesup.org/~robert/pro/publications/articles/modular_isogenies_g2.pdf. HAL: hal-02436133. (Cit. on pp. 54, 57, 68).

0relative [Kle80] S. L. Kleiman. "Relative duality for quasi-coherent sheaves". In: *Compositio Mathematica* 41.1 (1980), pp. 39–60 (cit. on p. 20).

lytic1958 [KS58] K. Kodaira and D. C. Spencer. "On deformations of complex analytic structures, I". In: *Ann. of Math. (2)* 67 (1958), pp. 328–401 (cit. on p. 59).

1976theta [Koi76] S. Koizumi. "Theta relations and projective normality of abelian varieties". In: *American Journal of Mathematics* (1976), pp. 865–889 (cit. on p. 63).

alization [Koi+60] S. Koizumi et al. "On specialization of the Albanese and Picard varieties". In: *Memoirs of the College of Science, University of Kyoto. Series A: Mathematics* 32.3 (1960), pp. 371–382 (cit. on p. 15).

lizations [KG59] S. Koizumi and S. Goro. "On specializations of abelian varieties". In: *Scientific Papers of the College of General Education, University of Tokyo* 9 (1959), pp. 187–211 (cit. on p. 15).

2000theta [Kou00] A. Kouvidakis. "Theta line bundles and the determinant of the Hodge bundle". In: *Transactions of the American Mathematical Society* 352.6 (2000), pp. 2553–2568 (cit. on p. 63).

20torelli [Lan20] A. Landesman. "The Torelli map restricted to the hyperelliptic locus". 2020. eprint: 1911.02084 (arXiv) (cit. on p. 65).

ciprocity [Lan58] S. Lang. "Reciprocity and Correspondences". In: *American Journal of Mathematics* 80.2 (1958), pp. 431–440 (cit. on p. 43).

algebraic [Lan56] S. Lang. "Algebraic groups over finite fields". In: *American Journal of Mathematics* 78.3 (1956), pp. 555–563 (cit. on p. 46).

2018champs [LM18] G. Laumon and L. Moret-Bailly. *Champs algébriques*. Vol. 39. Springer, 2018 (cit. on p. 93).

969duality [Lic69] S. Lichtenbaum. "Duality theorems for curves over p-adic fields". In: *Inventiones mathematicae* 7.2 (1969), pp. 120–136 (cit. on p. 45).

993courbes [Liu93] Q. Liu. "Courbes stables de genre 2 et leur schéma de modules". In: *Mathematische Annalen* 295.1 (1993), pp. 201–222 (cit. on p. 67).

liu2002algebraic [Liu02] Q. Liu ⊠⊠. *Algebraic geometry and arithmetic curves*. Vol. 6. Oxford University Press on Demand, 2002 (cit. on pp. 20, 23, 27, 33–36, 86).

DRoptimal [LR15] D. Lubicz and D. Robert. "A generalisation of Miller's algorithm and applications to pairing computations on abelian varieties". In: *Journal of Symbolic Computation* 67 (Mar. 2015), pp. 68–92. DOI: 10.1016/j.jsc.2014.08.001. URL: http://www.normalesup.org/~robert/pro/publications/articles/optimal.pdf. HAL: hal-00806923, eprint: 2013/192. (Cit. on pp. 43, 48).

LST1964 [LST64] J. Lubin, J.-P. Serre, and J. Tate. *Elliptic Curves and formal groups*. 1964. URL: http://ma.utexas.edu/users/voloch/lst.html (cit. on p. 38).

luna1973slices [Lun73] D. Luna. "Slices étales". In: *Bull. Soc. Math. France* 33 (1973), pp. 81–105 (cit. on pp. 97, 100).

anonicalliftg2p2 [MR22] A. Maiga and D. Robert. "Computing the 2-adic canonical lift of genus 2 curves". Mar. 2022. DOI: 10.1007/978-981-16-6890-6_48. URL: http://www.normalesup.org/~robert/pro/publications/articles/canonical_lift_g2_p2.pdf. HAL: hal-03119147. (Cit. on pp. 68, 73).

t2008determinant [MR08] V. Maillot and D. Rössler. "On the determinant bundles of abelian schemes". In: *Compositio Mathematica* 144.2 (2008), pp. 495–502 (cit. on p. 63).

callum2012method [MP12] W. McCallum and B. Poonen. "The method of Chabauty and Coleman". In: *Explicit methods in number theory* 36 (2012), pp. 99–117 (cit. on p. 1).

nta1987varieties [MS87] V. B. Mehta and V. Srinivas. "Varieties in positive characteristic with trivial tangent bundle". In: *Compositio Mathematica* 64.2 (1987), pp. 191–212 (cit. on p. 38).

sing1972crystals [Mes72] W. Messing. "The crystals associated to Barsotti-Tate groups". In: *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*. Springer, 1972, pp. 112–149 (cit. on pp. 36–38).

Mestre91 [Mes91] J. Mestre. "Construction de Courbes de Genre 2 à partir de leurs Modules". In: *In Effective Methods in Algebraic Geometry (Castiglioncello, 1990)* (1991), pp. 313–334 (cit. on p. 70).

DRmodularcyclic [MR20] E. Milio and D. Robert. "Modular polynomials on Hilbert surfaces". In: *Journal of Number Theory* 216 (Nov. 2020), pp. 403–459. DOI: 10.1016/j.jnt.2020.04.014. URL: https://www.sciencedirect.com/science/article/abs/pii/S0022314X20301402. HAL: hal-01520262, Reproducible archive: https://data.mendeley.com/datasets/yy3bty5ktk/1. (Cit. on p. 55).

ilne1985jacobian [Mil85] J. Milne. "Jacobian varieties". In: *Arithmetic geometry (G. Cornell and JH Silverman, eds.)* (1985), pp. 167–212 (cit. on pp. 1, 8, 20–23).

milne-abelian [Mil91] J. Milne. *Abelian varieties*. 1991. URL: http://www.jmilne.org/math/CourseNotes/av.html (cit. on pp. 1, 8–10, 39, 42).

milnebookav [Mil] J. Milne. *Abelian varieties*. URL: https://www.jmilne.org/math/CourseNotes/av.html (cit. on p. 11).

2005introduction [Mil05] J. S. Milne. "Introduction to Shimura varieties". In: *Harmonic analysis, the trace formula, and Shimura varieties* 4 (2005), pp. 265–378 (cit. on pp. 53, 54, 56).

ne2006arithmetic [Mil06a] J. S. Milne. *Arithmetic duality theorems*. Vol. 20. Citeseer, 2006 (cit. on p. 45).

milne2006complex [Mil06b] J. S. Milne. *Complex multiplication*. 2006. URL: https://www.jmilne.org/math/CourseNotes/cm.html (cit. on pp. 75, 77, 78).

e2007fundamental [Mil07] J. S. Milne. *The fundamental theorem of complex multiplication*. 2007. arXiv: 0705.3446 (cit. on pp. 75, 77).

lne2012reductive [Mil12a] J. S. Milne. *Reductive groups*. Courses Notes. 2012. URL: https://www.jmilne.org/math/CourseNotes/RG.pdf (cit. on pp. 87–89).

lne2017algebraic [Mil17] J. S. Milne. *Algebraic groups: The theory of group schemes of finite type over a field*. Vol. 170. Cambridge University Press, 2017 (cit. on p. 89).

milne1986abelian [Mil86] J. Milne. "Abelian varieties". In: *Arithmetic geometry (G. Cornell and JH Silverman, eds.)* (1986), pp. 103–150 (cit. on pp. 1, 8, 11).

roupscheme [Mil12b] J. Milne. "Basic Theory of Affine Group Schemes". In: (2012). URL: https://www.jmilne.org/math/CourseNotes/AGS.pdf (cit. on p. 87).

012abelian [MGE12] B. Moonen, G. van der Geer, and B. Edixhoven. *Abelian varieties*. Book project, 2012. URL: https://www.math.ru.nl/~bmoonen/research.html#bookabvar (cit. on pp. 8, 40, 48, 60).

011torelli [MO11] B. Moonen and F. Oort. *The Torelli locus and special subvarieties*. 2011. eprint: 1112.0933 (arXiv) (cit. on p. 65).

85pinceaux [Mor85] L. Moret-Bailly. *Pinceaux de variétés abéliennes*. Société mathématique de France, 1985 (cit. on p. 63).

90equation [Mor90] L. Moret-Bailly. "Sur l'équation fonctionnelle de la fonction thêta de Riemann". In: *Compositio Mathematica* 75.2 (1990), pp. 203–217 (cit. on p. 63).

ri1978tate [Mor78] S. Mori. "On Tate conjecture concerning endomorphisms of abelian varieties". In: *Proceedings of International Symposium on Algebraic Geometry*. Kinokuniya. 1978, pp. 219–230 (cit. on p. 37).

fordOEDAV1 [Mum66] D. Mumford. "On the equations defining abelian varieties. I". In: *Invent. Math.* 1 (1966), pp. 287–354 (cit. on p. 63).

fordOEDAV2 [Mum67a] D. Mumford. "On the equations defining abelian varieties. II". In: *Invent. Math.* 3 (1967), pp. 75–135 (cit. on p. 63).

fordOEDAV3 [Mum67b] D. Mumford. "On the equations defining abelian varieties. III". In: *Invent. Math.* 3 (1967), pp. 215–244 (cit. on p. 63).

varieties [Mum69] D. Mumford. "Varieties defined by quadratic equations". In: *Questions on Algebraic Varieties (CIME, III Ciclo, Varenna, 1969)* (1969), pp. 29–100 (cit. on p. 63).

MumfordAV [Mum70a] D. Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970, pp. viii+242 (cit. on pp. 1, 5, 7–10, 39–41, 81).

structure [Mum70b] D. Mumford. *The structure of the moduli spaces of curves and abelian varieties*. Mathematics Institute, University of Warwick, 1970 (cit. on pp. 54, 56).

mfordTata1 [Mum83] D. Mumford. *Tata lectures on theta I*. Vol. 28. Progress in Mathematics. With the assistance of C. Musili, M. Nori, E. Previato and M. Stillman. Boston, MA: Birkhäuser Boston Inc., 1983, pp. xiii+235. ISBN: 3-7643-3109-7 (cit. on pp. 1, 5).

mfordTata2 [Mum84] D. Mumford. *Tata lectures on theta II*. Vol. 43. Progress in Mathematics. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura. Boston, MA: Birkhäuser Boston Inc., 1984, pp. xiv+272. ISBN: 0-8176-3110-0 (cit. on pp. 1, 5).

mfordTata3 [Mum91] D. Mumford. *Tata lectures on theta III*. Vol. 97. Progress in Mathematics. With the collaboration of Madhav Nori and Peter Norman. Boston, MA: Birkhäuser Boston Inc., 1991, pp. viii+202. ISBN: 0-8176-3440-1 (cit. on pp. 5, 63).

-geometric [MFK94] D. Mumford, J. Fogarty, and F. Kirwan. *Geometric invariant theory*. Vol. 34. Springer Science & Business Media, 1994 (cit. on pp. 1, 12, 13, 15, 16, 21, 33, 35, 54, 56, 57, 81, 97–99).

esentation [Mur64] J. Murre. "Representation of unramified functors. Applications". In: *Séminaire Bourbaki, Exp* 294 (1964), p. 65 (cit. on pp. 13, 94).

064modeles [Nér64] A. Néron. "Modeles minimaux des variétés abéliennes sur les corps locaux et globaux". In: *Publications Mathématiques de l'Institut des Hautes Études Scientifiques* 21.1 (1964), pp. 5–125 (cit. on p. 27).

mo243414 [nfd16] nfdc23. *Is a polarization on an abelian scheme an open condition?* MathOverflow. June 30, 2016. URL: https://mathoverflow.net/q/243414 (cit. on p. 16).

980moduli [NO80] P. Norman and F. Oort. "Moduli of abelian varieties". In: *Annals of Mathematics* 112.2 (1980), pp. 413–439 (cit. on pp. 38, 54, 56).

algebraic [Ols16] M. Olsson. *Algebraic spaces and stacks*. Vol. 62. American Mathematical Society, 2016 (cit. on p. 93).

olsson2006hom [Ols+06] M. C. Olsson et al. "Hom-stacks and restriction of scalars". In: *Duke Mathematical Journal* 134.1 (2006), pp. 139–164 (cit. on pp. 97, 98).

t1973principally [OU73] F. Oort and K. Ueno. "Principally polarized abelian varieties of dimension two or three are Jacobian varieties". In: *Journal of the Faculty of Science, the University of Tokyo: Tōkyō Daigaku Rigakubu kiyō. Dai 1-rui, Sūgaku. Mathematics* (1973), p. 377 (cit. on p. 20).

oort1971finite [Oor71a] F. Oort. "Finite group schemes, local moduli for abelian varieties, and lifting problems". In: *Compositio Mathematica* 23.3 (1971), pp. 265–296 (cit. on p. 38).

GroupSchemes1971 [Oor71b] F. Oort. "Finite group schemes, local moduli for abelian varieties, and lifting problems". In: *Compositio Math.* 23 (1971), pp. 265–296 (cit. on p. 60).

oort1973isogeny [Oor73] F. Oort. "The isogeny class of a CM-type abelian variety is defined over a finite extension of the prime field". In: *Journal of pure and applied algebra* 3.4 (1973), pp. 399–408 (cit. on p. 75).

oort1979abelian [Oor79] F. Oort. "Abelian varieties: moduli and lifting properties". In: *Algebraic Geometry*. Springer, 1979, pp. 477–495 (cit. on p. 38).

oort1995some [Oor95] F. Oort. "Some questions in algebraic geometry". In: (1995). URL: https://www.semanticscholar.org/paper/Some-questions-in-algebraic-geometry-Oort/7a1aa78e86e9afb6987184912439ffcd930 (cit. on p. 38).

01stratification [Ooro1a] F. Oort. "A stratification of a moduli space of abelian varieties". In: *Moduli of abelian varieties*. Springer, 2001, pp. 345–416 (cit. on pp. 54, 56).

oort2001newton [Ooro1b] F. Oort. "Newton polygon strata in the moduli space of abelian varieties". In: *Moduli of abelian varieties*. Springer, 2001, pp. 417–440 (cit. on pp. 37, 54).

oort2009cm [Ooro9] F. Oort. *CM-liftings of abelian varieties*. 2009. URL: https://webspace.science.uu.nl/~oort0109/Biel3-VI-2009.pdf (cit. on p. 38).

oort2015lifting [Oor15] F. Oort. *Lifting questions*. 2015. URL: https://webspace.science.uu.nl/~oort0109/Aug2015Lift.pdf (cit. on p. 38).

oort1979local [OS79] F. Oort and J. Steenbrink. "The local Torelli problem for algebraic curves". In: *Journées de Géometrie Algébrique d'Angers* 1979 (1979), pp. 157–204 (cit. on p. 65).

mo370025 [Ore20] G. Orecchia. *Extensions of (semi-)abelian schemes*. MathOverflow. Aug. 25, 2020. URL: https://mathoverflow.net/q/370025 (cit. on p. 32).

mo123454 [Per13] K. M. Pera. *Status of Grothendiecks conjecture on homomorphisms of abelian schemes*. MathOverflow. Mar. 3, 2013. URL: https://mathoverflow.net/q/123454 (cit. on p. 37).

ila1990frobenius [Pil90] J. Pila. "Frobenius maps of abelian varieties and finding roots of unity in finite fields". In: *Mathematics of Computation* 55.192 (1990), pp. 745–763 (cit. on p. 1).

k2000determinant [Poloo] A. Polishchuk. "Determinant bundles for abelian schemes". In: *Compositio Mathematica* 121.3 (2000), pp. 221–245 (cit. on p. 63).

nchuk2003abelian [Polo3] A. Polishchuk. *Abelian varieties, theta functions and the Fourier transform*. Vol. 153. Cambridge University Press, 2003 (cit. on p. 8).

pescu1985general [Pop85] D. Popescu. "General Néron desingularization". In: *Nagoya Mathematical Journal* 100 (1985), pp. 97–126 (cit. on p. 94).

pries2008short [Prio8] R. Pries. "A short guide to p-torsion of abelian varieties in characteristic p". In: *Computational arithmetic geometry* 463 (2008), pp. 121–129 (cit. on p. 11).

ronk1996etendues [Pro96] D. A. Pronk. "Etendues and stacks as bicategories of fractions". In: *Compositio Mathematica* 102.3 (1996), pp. 243–303 (cit. on p. 94).

ompactifications [Rap78] M. Rapoport. "Compactifications de l'espace de modules de Hilbert-Blumenthal". In: *Compositio Mathematica* 36.3 (1978), pp. 255–335 (cit. on pp. 54, 58–60).

ynaud1967passage [Ray67a] M. Raynaud. "Passage au quotient par une relation d'équivalence plate". In: *Proceedings of a Conference on Local Fields*. Springer. 1967, pp. 78–85 (cit. on p. 97).

ompterendu [Ray67b] M. Raynaud. "Passage au quotient par une relation par un groupoide plat". In: vol. 265. Compte rendu de l'Académie des Sciences. Springer. 1967, pp. 384–387 (cit. on p. 97).

971travaux [Ray71] M. Raynaud. "Travaux récents de M. Artin". In: *Séminaire Bourbaki vol. 1968/69 Exposés 347-363*. Springer, 1971, pp. 279–295 (cit. on p. 95).

85hauteurs [Ray85] M. Raynaud. "Hauteurs et isogénies". In: *Astérisque* 127 (1985), pp. 199–234 (cit. on p. 1).

06faisceaux [Ray06] M. Raynaud. *Faisceaux amples sur les schémas en groupes et les espaces homogenes*. Vol. 119. Springer, 2006 (cit. on pp. 12, 13, 90).

colfi_2020 [Ric20] A. T. Ricolfi. "The Hilbert scheme of hyperelliptic Jacobians and moduli of Picard sheaves". In: *Algebra & Number Theory* 14.6 (July 2020), pp. 1381–1397. ISSN: 1937-0652. DOI: 10.2140/ant.2020.14.1381. URL: http://dx.doi.org/10.2140/ant.2020.14.1381 (cit. on p. 65).

rschwinden [Rie65] B. Riemann. "Über das Verschwinden der Theta-Functionen". In: *Borchardt's [= Crelle's] J. für reine und angew. Math* 65 (1865), pp. 214–224 (cit. on p. 22).

divisibles [Rio03] J. Riou. *Groupes p-divisibles*. 2003. URL: https://www.math.u-psud.fr/~riou/doc/tate.ps.gz (cit. on p. 37).

DRphd [Rob10] D. Robert. "Theta functions and cryptographic applications". PhD thesis. Université Henri-Poincarré, Nancy 1, France, July 2010. URL: http://www.normalesup.org/~robert/pro/publications/academic/phd.pdf. Slides: 2010-07-Phd-Nancy.pdf (1h, Nancy), TEL: tel-00528942. (Cit. on pp. 5, 6, 8, 42, 53, 55).

DRhdr [Rob21] D. Robert. "Efficient algorithms for abelian varieties and their moduli spaces". HDR thesis. Université Bordeaux, June 2021. URL: http://www.normalesup.org/~robert/pro/publications/academic/hdr.pdf. Slides: 2021-06-HDR-Bordeaux.pdf (1h, Bordeaux). (Cit. on pp. 1, 28, 38, 41, 42, 55).

2013models [Rom13] M. Romagny. "Models of curves". In: *Arithmetic and geometry around Galois theory*. Springer, 2013, pp. 149–170 (cit. on pp. 23, 33–35).

mo253621 [Rou17] X. Roulleau. *A Jacobian with a good reduction, which is simple : how is the reduction of the curve?* MathOverflow. Apr. 13, 2017. URL: https://mathoverflow.net/q/253621 (cit. on p. 35).

ubmersions [Ryd10] D. Rydh. "Submersions and effective descent of étale morphisms". In: *Bulletin de la Société mathématique de France* 138.2 (2010), pp. 181–230. ISSN: 2102-622X. DOI: 10.24033/bsmf.2588. URL: http://dx.doi.org/10.24033/bsmf.2588 (cit. on pp. 83, 84).

ence_2013 [Ryd13] D. Rydh. "Existence and properties of geometric quotients". In: *Journal of Algebraic Geometry* 22.4 (May 13, 2013), pp. 629–669. ISSN: 1056-3911, 1534-7486. DOI: 10.1090/S1056-3911-2013-00615-3. arXiv: 0708.3333. URL: http://arxiv.org/abs/0708.3333 (visited on 07/02/2020) (cit. on pp. 97–99).

Scanonical [Satoo] T. Satoh. "The canonical lift of an ordinary elliptic curve over a finite field and its point counting". In: *J. Ramanujan Math. Soc.* 15.4 (2000), pp. 247–270 (cit. on p. 1).

fer2005new [Sch05] E. F. Schaefer. "A new proof for the non-degeneracy of the Frey-Rück pairing and a connection to isogenies over the base field". In: *Computational aspects of algebraic curves* 13 (2005), pp. 1–12 (cit. on pp. 48, 49).

85elliptic [Sch85] R. Schoof. "Elliptic curves over finite fields and the computation of square roots mod p". In: *Mathematics of computation* 44.170 (1985), pp. 483–494 (cit. on p. 1).

95counting [Sch95] R. Schoof. "Counting points on elliptic curves over finite fields". In: *J. Théor. Nombres Bordeaux* 7.1 (1995), pp. 219–254 (cit. on p. 1).

966groupes [Ser66] J.-P. Serre. "Groupes p-divisibles". In: *Séminaire Bourbaki* 10 (1966), pp. 73–86 (cit. on pp. 11, 37, 38).

re1968good [ST68] J.-P. Serre and J. Tate. "Good reduction of abelian varieties". In: *Annals of Mathematics* (1968), pp. 492–517 (cit. on pp. 28, 77, 83).

erre2001appendix [Ser01] J. Serre. "Appendix to Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields, by K". In: *Lauter. J. Algebraic Geom* 10.1 (2001), pp. 30–36 (cit. on p. 23).

dri1977geometric [Ses77] C. S. Seshadri. "Geometric reductivity over arbitrary base". In: *Advances in Mathematics* 26.3 (1977), pp. 225–274 (cit. on pp. 97, 99).

rg1995semistable [SZ95] A. Silverberg and Y. G. Zarhin. "Semistable reduction and torsion subgroups of abelian varieties". In: *Annales de l'institut Fourier*. Vol. 45. 2. 1995, pp. 403–420 (cit. on p. 29).

verman2010survey [Sil10] J. H. Silverman. "A survey of local and global pairings on elliptic curves and abelian varieties". In: *International Conference on Pairing-Based Cryptography*. Springer. 2010, pp. 377–396 (cit. on p. 39).

stacks-project [Stacks] T. Stacks Project Authors. *Stacks Project*. https://stacks.math.columbia.edu. 2018 (cit. on pp. 12, 14, 18, 30, 32, 35, 38, 60, 81, 82, 84–86, 91, 93–95, 97, 99).

mo265553 [Sta17] J. Starr. *Extending homomorphisms of Abelian schemes*. MathOverflow. Mar. 25, 2017. URL: https://mathoverflow.net/q/265553 (cit. on p. 32).

mo326136 [Sta19] J. Starr. *Given a semi-abelian scheme, is the set of points such that the fibres are abelian varities open?* MathOverflow. Mar. 23, 2019. URL: https://mathoverflow.net/q/326136 (cit. on p. 90).

stoll2006descent [Sto06] M. Stoll. *Descent on elliptic curves*. 2006. arXiv: math/0611694 (cit. on p. 1).

Streng10 [Str10] M. Streng. "Complex multiplication of abelian surfaces". Proefschrift. Universiteit Leiden, 2010 (cit. on pp. 75–77).

reng2011explicit [Str] M. Streng. "An explicit version of Shimura's reciprocity law for Siegel modular functions". arXiv: 1201.0020 (cit. on p. 77).

14generalization [Sug14] K.-i. Sugiyama. "On a generalization of Deuring□s results". In: *Finite Fields and Their Applications* 26 (2014), pp. 69–85 (cit. on p. 78).

tate1957wc [Tat57] J. Tate. "WC-groups over p-adic fields". In: *Séminaire Bourbaki* 4 (1957), pp. 265–277 (cit. on pp. 45, 49).

tate1997finite [Tat97] J. Tate. "Finite flat group schemes". In: *Modular forms and Fermat's last theorem*. Springer, 1997, pp. 121–154 (cit. on p. 36).

te1967pdivisible [Tat67] J. T. Tate. "p-Divisible groups". In: *Proceedings of a conference on Local Fields*. Springer. 1967, pp. 158–183 (cit. on pp. 11, 37).

tengan2013proof [Ten13] E. Tengan. *A proof of Grothendieck's base change theorem*. 2013. arXiv: 1312.7320 (cit. on p. 81).

mo47149 [TJC16] TJCM. *Quotient of an algebraic group by the connected component containing identity*. MathOverflow. May 26, 2016. URL: https://mathoverflow.net/q/47149 (cit. on p. 36).

mo190718 [use14] user63961. *Geometrically connected components of an algebraic group*. MathOverflow. Dec. 14, 2014. URL: https://mathoverflow.net/q/190718 (cit. on p. 86).

mo9338 [VA09] VA. *Is the Torelli map an immersion?* MathOverflow. Dec. 19, 2009. URL: https://mathoverflow.net/q/9338 (cit. on p. 65).

ergeer2008siegel [Van08] G. Van Der Geer. "Siegel modular forms and their applications". In: *The 1-2-3 of modular forms*. Springer, 2008, pp. 181–245 (cit. on p. 55).

geer2012hilbert [Van12] G. Van Der Geer. *Hilbert modular surfaces*. Vol. 16. Springer Science & Business Media, 2012 (cit. on p. 53).

house1971abelian [WM71] W. C. Waterhouse and J. S. Milne. "Abelian varieties over finite fields". In: *Proc. Sympos. Pure Math.* Vol. 20. 1971, pp. 53–64 (cit. on p. 37).

ayoucisserretate [You15] A. Youcis. *p-divisible groups, formal groups, and the Serre-Tate theorem*. 2015. URL: https://ayoucis.wordpress.com/2015/08/10/p-divisible-groups-formal-groups-and-the-serre-tate-theorem/ (cit. on p. 38).

04irreducibility [Yu04a] C.-F. Yu. "Irreducibility of the Siegel moduli spaces with parahoric level structure". In: *International Mathematics Research Notices* 2004.48 (2004), pp. 2593–2597 (cit. on p. 54).

somorphism [Yu04b] C.-F. Yu. "The isomorphism classes of abelian varieties of CM-type". In: *Journal of Pure and Applied Algebra* 187.1-3 (2004), pp. 305–319 (cit. on p. 75).

omorphisms [Zar75] J. G. Zarhin. "Endomorphisms of Abelian varieties over fields of finite characteristic". In: *Mathematics of the USSR-Izvestiya* 9.2 (1975), p. 255 (cit. on p. 37).

mo7513 [Zur09] D. Zureick-Brown. *Are Jacobians principally polarized over non-algebraically closed fields?* MathOverflow. Dec. 1, 2009. URL: https://mathoverflow.net/q/7513 (cit. on p. 65).