Abelian varieties

Davide Lombardo

Luxembourg Summer School on Galois representations

03-07 July 2018

Kummer surface of a genus 2 Jacobian

Contents

Disclaimer. The purpose of these notes is to give a quick, somewhat hands-on[1] introduction to the arithmetic theory of Abelian varieties from the point of view of their Galois representations. They are not intended as a course book or as a complete reference for the topic (far from it!): the reader is encouraged to complement them with the many great sources already available either in print or on the web. Some personal favourites of mine are Mumford's classic book on abelian varieties [**Mum70**], the notes by Edixhoven, van Geemen, and Moonen [**EMvG**], and Milne's course notes [**Mil12**].

Acknowledgments. Many thanks go to Andrea Maffei and Pietro Mercuri for the extensive feedback I received from them while writing these notes. I'd also like to thank Bas Edixhoven for an illuminating discussion about Jacobians, and Gabor Wiese, Antonella Perucca, Shaunak Deo, Ilker Inam and Alexander Rahm for the organisation of the summer school.

[1] at least, that was the intention. I'm afraid I might have failed...

CHAPTER 1

Introduction to abelian varieties

1. Preliminaries

1.1. Basic notation. We reserve the letter K to denote fields. When K is a *number field*, that is a finite extension of the field $\mathbb{Q}$ of rational numbers, we denote by $\mathcal{O}_K$ its ring of integers. The letters p and ℓ will usually denote rational primes (that is, usual prime numbers), while the symbol v will usually denote a prime ideal (a 'finite place') in the ring of integers of some number field. The completion of $\mathcal{O}_K$ at v will be denoted by $\mathcal{O}_{K,v}$ and the residue field at v by $\mathbb{F}_v$.

The symbol C will usually denote a curve, and J will be the associated Jacobian variety (to be defined later). We'll use the letters A and B for abelian varieties.

A *variety* over a field is a scheme of finite type over that field, separated and geometrically integral (that is, reduced and irreducible). In particular, varieties are geometrically connected. A *nice curve* is a smooth projective variety of dimension 1 (hence in particular geometrically connected).

1.2. Group schemes. The reader should be aware that the language of group schemes is essential in developing some of the more advanced parts of the arithmetic theory of abelian varieties. To keep these notes as elementary as possible we shall try to avoid this language as much as possible, but it is still useful to have at least a vague idea of what it is about:

DEFINITION 1.1. *Let S be a scheme. A* ***group scheme*** *over S is an S-scheme $\mathcal{G}$ together with three morphisms*

$$m : \mathcal{G} \times_S \mathcal{G} \to \mathcal{G}, \quad i : \mathcal{G} \to \mathcal{G}, \quad e : S \to \mathcal{G},$$

called respectively the ***multiplication****,* ***inverse****, and* ***unit*** *maps. They satisfy the obvious axioms to endow the set of points $\mathcal{G}(A)$ (for any S-scheme A) with the structure of a group; for example, associativity translates into the commutativity of the following diagram*

$$\begin{array}{ccc} \mathcal{G} \times_S \mathcal{G} \times_S \mathcal{G} & \xrightarrow{(m,\mathrm{id})} & \mathcal{G} \times_S \mathcal{G} \\ \downarrow{\scriptstyle (\mathrm{id},m)} & & \downarrow{\scriptstyle m} \\ \mathcal{G} \times_S \mathcal{G} & \xrightarrow[m]{} & \mathcal{G} \end{array}$$

and there are analogous diagrams that encode the fact that i gives the inverse and e the unit for the group law.

REMARK 1.2. More informally, when S is the spectrum of a field K, a group scheme over S is a K-variety G whose $\overline{K}$-points form a group, and such that:

(1) the identity element of $G(\overline{K})$ is K-rational;
(2) the functions $m : G(\overline{K}) \times G(\overline{K}) \to G(\overline{K})$ and $i : G(\overline{K}) \to G(\overline{K})$ that give the multiplication and inverse in the group are induced by algebraic morphisms $G \times G \to G$ and $G \to G$ (defined over K).

Group schemes over a field are often simply called **algebraic groups**.

REMARK 1.3. Roughly speaking, group schemes over S should be thought of as algebraic groups parametrised by points of S.

1.3. Abelian varieties. Let K be a field (not necessarily of characteristic 0). An **abelian variety over** K is a reduced, connected and projective algebraic group: since this seemingly innocuous definition hides quite a bit of sophisticated mathematics, let us spend some time making the acquaintance of these objects.

REMARK 1.4.
(1) In the definition, one may replace *projective* with *proper*. It is a theorem of Weil that the two definitions are equivalent (for a proof see [**Mil12**, §7]).
(2) Since abelian varieties by definition are connected and possess a K-rational point, they are also geometrically connected [**Sta18**, Tag 04KV].
(3) A theorem of Cartier shows that if $\mathrm{char}(K) = 0$ all group schemes over K are automatically reduced ([**EMvG**, Theorem 3.20]); this is not true in general over fields of positive characteristic.
(4) It is a well-known fact ([**EMvG**, Proposition 3.17]) that all *reduced* group schemes over a field are smooth. Combined with the previous remarks, this shows that if $\mathrm{char}(K) = 0$ one may simply define abelian varieties as connected, proper group schemes over K.

Since we are all familiar with the notion of on abelian *group*, it would be quite disconcerting if abelian varieties (or rather, the groups consisting of their rational points) were not commutative. Luckily, the nomenclature is consistent:

PROPOSITION 1.5. *Any abelian variety is commutative, that is, the two maps*

$$\begin{array}{ccc} A \times A & \to & A \\ (x, y) & \mapsto & x \cdot y \end{array}$$

and

$$\begin{array}{ccc} A \times A & \to & A \\ (x, y) & \mapsto & y \cdot x \end{array}$$

coincide, where we (temporarily) denote by $\cdot$ the multiplication map on A.

PROOF. Since we are considering abelian varieties over a field, it suffices to work at the level of $\overline{K}$-points (notice that A is separated, so two morphisms are equal iff they are

equal at all closed points). It's enough to show that the image of the map

$$\begin{array}{ccc} A(\overline{K}) \times A(\overline{K}) & \to & A(\overline{K}) \\ (x, y) & \mapsto & y \cdot x \cdot y^{-1} \cdot x^{-1} \end{array}$$

is the identity element e_A of $A(\overline{K})$. Now notice that the restriction of this map to $\{e_A\} \times A(\overline{K})$ and to $A(\overline{K}) \times \{e_A\}$ is constantly equal to e_A, and apply the Rigidity Lemma (Lemma 1.7 below). □

NOTATION 1.6. *Because of the previous proposition we shall usually denote the group operation on an abelian variety additively, and we shall write 0_A (or simply 0) for the neutral element and $-x$ for the opposite of x with respect to the group law.*

LEMMA 1.7 (Rigidity lemma). *Let $f : A \times B \to C$ be a morphism of varieties over k. If A is proper and $f(A \times \{b_0\}) = f(\{a_0\} \times B) = \{c_0\}$ for some $a_0 \in A(k), b_0 \in B(k), c_0 \in C(k)$, then $f(A \times B) = \{c_0\}$.*

PROOF. Choose an open affine neighbourhood C_0 of c_0. By properness, $\pi : A \times B \to B$ is a closed map, hence $Z = \pi(f^{-1}(C \setminus C_0))$ is closed in B. A closed point b of B lies outside Z if and only if $f(A \times \{b\}) \subseteq C_0$; by assumption b_0 lies in $B \setminus Z$, which is therefore open and nonempty, hence dense (recall that our varieties are geometrically irreducible by definition). Now pick any point $b \in B \setminus Z$ and consider $f(A \times \{b\})$: on the one hand, the image of this map is contained in C_0 by what we just said, and on the other, since $A \times \{b\} \cong A$ is proper and C_0 is affine, $f(A \times \{b\})$ is a point. We also know *which* point it is: by assumption,

$$f(A \times \{b\}) \ni f(\{a_0\} \times \{b\}) \in f(\{a_0\} \times B) = \{c_0\},$$

hence $f(A \times \{b\}) = \{c_0\}$ for all b in the dense set $B \setminus Z$. In particular f is constantly equal to $\{c_0\}$ on the dense open set $A \times (B \setminus Z)$, hence it is constant as claimed. □

PROPOSITION 1.8. *Let $f : A \to B$ be an algebraic morphism of abelian varieties. Then f is the composition of a homomorphism with a translation.*

PROOF. Replacing f with $g(x) = f(x) - f(0)$, we are reduced to showing that an algebraic morphism $g : A \to B$ such that $f(0_A) = 0_B$ is a homomorphism of abelian varieties. Consider the map

$$\begin{array}{rccc} \varphi : & A \times A & \to & B \\ & (a_1, a_2) & \mapsto & g(a_1) + g(a_2) - g(a_1 + a_2) : \end{array}$$

by the rigidity lemma, noticing that $\varphi(\{0_A\} \times A) = \varphi(A \times \{0_A\}) = \{0_B\}$, we obtain that $\varphi(A \times A) = \{0_B\}$, that is, $g(a_1) + g(a_2) = g(a_1 + a_2)$ as desired. □

1.4. Examples. Our main source of examples will be *Jacobians*, a special class of abelian varieties canonically associated with curves. We will meet Jacobians soon; for now, we can only describe very basic examples of abelian varieties:

EXAMPLE 1.9. (1) elliptic curves are abelian varieties. In fact, the term *elliptic curve* is synonymous with *abelian variety of dimension 1.* Recall that an elliptic curve is a genus 1 curve *with a marked rational point*: the rational point is essential in defining the group law (in fact, Proposition 1.8 implies in particular that the group law is uniquely determined by the choice of the neutral element).

(2) Let $E_1, \ldots, E_k$ be elliptic curves: then $E_1 \times \cdots \times E_g$ is a group scheme which is connected, smooth and projective, hence an abelian variety (of dimension g). One can prove that not all g-dimensional abelian varieties are of this form: in what follows we shall see (many) examples of abelian varieties that are not products of elliptic curves.

2. Abelian schemes over arbitrary bases

For arithmetic applications it is extremely useful to have a notion of abelian variety also over arbitrary bases – that is, we want to treat the general situation of an abelian variety defined over an arbitrary base scheme S and not just over the spectrum of a field. We will not dwell much on this topic, but here is the general definition:

DEFINITION 2.1 (Abelian schemes over general bases). *Let S be a scheme. A g-dimensional abelian scheme over S is a group scheme $\mathcal{A} \to S$ such that the structure morphism $\mathcal{A} \to S$ is of finite presentation, proper, smooth, with all fibers geometrically connected and of dimension g.*

REMARK 2.2. If S is noetherian (which is the case in most arithmetic applications!) then *finite presentation* can be replaced by *finite type*, a property that holds for any reasonable morphism. Recall that $\pi : \mathcal{A} \to S$ is of finite type if the following holds: there is a cover of S by open affine subschemes $S_i = \mathrm{Spec}(R_i)$ and a cover of every $\pi^{-1}(S_i)$ by open affine subschemes $\mathcal{A}_{ij} = \mathrm{Spec}(B_{ij})$, such that B_{ij} is a finitely generated R_i-algebra for every i, j.

This somewhat abstract definition essentially amounts to asking for a family of abelian varieties A_s that varies algebraically with respect to the (geometric) point $s \in S$. The usefulness of the definition lies in its ability to give a geometric framework for the notion of *reduction modulo p*, which can be defined in concrete terms (e.g. using equations) for elliptic curves, but is much harder to describe in such elementary terms for higher-dimensional abelian varieties. It is of course also very useful to study the more geometrical problem of understanding families of abelian varieties depending algebraically on some parameters (a typical example being the Jacobian scheme of a family of curves).

REMARK 2.3. Let A be an abelian variety over a number field K. It is not true in general that A extends to an abelian scheme over $\mathcal{O}_K$ (in fact, this *almost never* happens): in particular, it is a famous theorem due to Fontaine [**Fon85**] and Abrashkin that there are no abelian varieties over $\mathrm{Spec}(\mathbb{Z})$. On the other hand, there are *some* abelian varieties that extend to the full ring of integers of a number field: one of the most famous and (to my knowledge) earliest examples is the elliptic curve E over $K = \mathbb{Q}(\sqrt{29})$ with equation

$$y^2 + xy + a^2 y = x^3,$$

where $a = \frac{5+\sqrt{29}}{2} \in \mathcal{O}_K^\times$. This elliptic curve extends to an abelian scheme over all of $\mathcal{O}_K$, or equivalently, in more classical language, it has good reduction at all the primes of $\mathcal{O}_K$.

3. Two technical tools: the theorems of the square and of the cube

We collect in this section some technical results that will be useful in what follows. The reader is not expected to spend much time meditating on these theorems, which are only included for completeness (proofs of all these statements can be found in [**Mum70**]). For the notation $[n]$ see definition 5.11.

THEOREM 3.1 (Theorem of the cube). *Let U, V, W be complete geometrically irreducible varieties over K, and let $u_0 \in U(K)$, $v_0 \in V(K)$, $w_0 \in W(K)$ be base points. Then an invertible sheaf $\mathcal{L}$ on $U \times V \times W$ is trivial if its restrictions to*

$$U \times V \times \{w_0\}, U \times \{v_0\} \times W, \{u_0\} \times V \times W$$

are all trivial.

THEOREM 3.2 (Theorem of the square). *For all line bundles $\mathcal{L}$ on A and for all points $a, b \in A(k)$ we have*

$$\tau_{a+b}^*\mathcal{L} \otimes \mathcal{L} \cong \tau_a^*\mathcal{L} \otimes \tau_b^*\mathcal{L},$$

where τ_x denotes translation by x.

COROLLARY 3.3. *The following formula holds for all line bundles $\mathcal{L}$ and all integers n:*

$$[n]^*\mathcal{L} \cong \mathcal{L}^{\otimes \frac{n^2+n}{2}} \otimes [-1]^*\mathcal{L}^{\otimes \frac{n^2-n}{2}}$$

Furthermore, if $[\mathcal{L}] \in \mathrm{Pic}^0(A)$, then $[-1]^*\mathcal{L} \cong \mathcal{L}^{-1}$, so that $[n]^*\mathcal{L} \cong \mathcal{L}^{\otimes n}$.

4. Abelian varieties over $\mathbb{C}$

The theory of complex abelian varieties (that is, abelian varieties over the complex numbers) is already very rich, but the existence of the *analytic uniformisation* (see below) makes it much more intuitive than the theory over general fields, so we start with this case. Let $A/\mathbb{C}$ be an abelian variety. Notice that $A(\mathbb{C})$ is a compact complex manifold of dimension g endowed with a group structure compatible with the differential structure; in other words, it is a compact complex Lie group of dimension g. We now show that – from the point of view of differential geometry – this group has a very simple form:

THEOREM 4.1 (Analytic uniformisation of complex abelian varieties). *Let A be a g-dimensional abelian variety over the complex numbers. Then there exists a lattice $\Lambda \subseteq \mathbb{C}^g$ such that $A(\mathbb{C})$ is isomorphic (as a Lie group) to $\mathbb{C}^g/\Lambda$.*

PROOF. Write $V = T_0A$ for the tangent space at identity. From the differential geometry of Lie groups we know that for every $v \in V$ there is a unique analytic group homomorphism

$$\varphi_v : \mathbb{C} \to A$$

with $d\varphi_v(0) = v$. One knows that $\varphi : V \times \mathbb{C} \to A$ is analytic. The **exponential map** is

$$\begin{array}{rccc} \exp: & V & \to & A \\ & v & \mapsto & \varphi_v(1). \end{array}$$

It is clear that $\varphi_v(t) = \exp(tv)$ (by uniqueness of φ_v we have $\varphi_v(st) = \varphi_{tv}(s)$, so the formula follows setting $s = 1$). Moreover, $\exp : V \to A$ is a group homomorphism: indeed

$$t \mapsto \exp(tx)\exp(ty)$$

is a group homomorphism (because A is abelian); taking the derivative at 0 and using the uniqueness of φ_{x+y} we obtain $\exp(tx)\exp(ty) = \exp(t(x+y))$ as claimed. Finally, exp is surjective because $\exp(V)$ is a subgroup of $A(\mathbb{C})$ that contains a neighbourhood of the identity (and A is connected). Now define Λ to be the kernel of exp: on the one hand it is discrete, because exp is a local homeomorphism, and on the other Λ must have full rank since $\mathbb{C}^g/\Lambda \cong A$ is compact. □

Definition 4.2 (Complex tori). *A **complex torus** is any complex analytic variety of the form $\mathbb{C}^g/\Lambda$ for some $g \geq 1$ and for some full-rank lattice Λ.*

Remark 4.3. It is **not** true that every complex torus is an abelian variety. The precise conditions under which this happens are known as **Riemann relations** (see remark 4.9 for a characterisation of abelian varieties among complex tori); the problem is that the general complex torus does **not** admit an analytic embedding in projective space.

Remark 4.4. Notwithstanding the previous remark, every complex torus of dimension 1 is an abelian variety (hence in particular an elliptic curve: the marked point is given by the class in $\mathbb{C}/\Lambda$ of the zero vector in $\mathbb{C}$). The Riemann conditions are automatic for 1-dimensional tori: see example 4.12.

Proposition 4.5 (Torsion points of complex abelian varieties). *Let n be a positive integer. The group*

$$A[n] = \{x \in A(\mathbb{C}) : nx = \underbrace{x + \cdots + x}_{n \text{ times}} = 0\}$$

is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g}$.

Proof. By analytic uniformisation it suffices to understand the n-torsion points of the group $\mathbb{C}^g/\Lambda \cong \mathbb{R}^{2g}/\Lambda$. As an abstract group, this is isomorphic to $\mathbb{R}^{2g}/\mathbb{Z}^{2g}$, because up to a change of basis in $\mathbb{R}^{2g}$ we can assume that Λ is the standard lattice[1] $\mathbb{Z}^{2g}$. Thus the group of n-torsion points of A is isomorphic to

$$(\mathbb{R}/\mathbb{Z})^{2g}[n] \cong \left(\frac{\mathbb{R}}{\mathbb{Z}}[n]\right)^{2g} \cong \left(\mathbb{S}^1[n]\right)^{2g} \cong (\mathbb{Z}/n\mathbb{Z})^{2g},$$

where we have denoted by $G[n]$ the n-torsion points of an abstract abelian group G. □

[1] notice that this statement is not true if we want to also preserve the complex structure! This is the reason why we replaced $\mathbb{C}^g$ with $\mathbb{R}^{2g}$

REMARK 4.6. Implicit in this proof is the fact that any complex abelian variety is isomorphic to $(\mathbb{S}^1)^g$ as a topological space, and in fact also as a real analytic variety. All the richness of the theory comes from the complex structure!

We now come to the existence of an embedding in projective space. In the interest of concreteness, we describe only one of the many possible definitions of a polarisation[2] and of the dual abelian variety:

DEFINITION 4.7 (Dual abelian variety, analytic setting). *Let $V = \mathbb{C}^g$ and write $A = V/\Lambda$. Let $\overline{V}^\vee$ be the space of $\mathbb{C}$-antilinear functionals $V \to \mathbb{C}$. The vector space $\overline{V}^\vee$ contains a natural lattice, namely*[3]

$$\Lambda^\vee = \left\{ \psi \in \overline{V}^\vee : \Im\psi(\Lambda) \subseteq \mathbb{Z} \right\},$$

*and one can check that the rank of $\Lambda^\vee$ is maximal, so that $\overline{V}^\vee/\Lambda^\vee$ is again an abelian variety, called the **dual abelian variety** of A.*

DEFINITION 4.8 (Polarisation, analytic setting). *We continue with the notation of definition 4.7. Let $H : V \times V \to \mathbb{C}$ be a Hermitian form (linear in the first argument, antilinear in the second). We say that H is a **polarisation** if it is positive-definite and $\Im H|_{\Lambda\times\Lambda}$ is integer-valued.*

REMARK 4.9. A complex torus $\mathbb{C}^g/\Lambda$ is a complex abelian variety if and only if it admits at least one polarisation.

DEFINITION 4.10 (Type of a polarisation). *Linear algebra over $\mathbb{Z}$ (essentially the elementary divisors theorem) shows that in a suitable basis of Λ the matrix representation of $\Im H|_{\Lambda\times\Lambda}$ takes the form*

$$\begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix}, \quad \text{where} \quad D = \begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_g \end{pmatrix}$$

*with the d_i positive integers such that $d_1 \mid d_2 \mid \cdots \mid d_g$. The vector $(d_1, \ldots, d_g)$ is called the **type** of the polarisation; one also sets $d(H) = \prod d_i$.*

REMARK 4.11. A polarisation induces a map

$$\begin{array}{rccc} \lambda_H : & V & \to & \overline{V}^\vee \\ & v & \mapsto & H(v, \cdot) \end{array}$$

[2]this is a fairly ill-defined term, in the sense that in different contexts it might mean very different things: an ample divisor on A, a certain bilinear form, or an isogeny from A to $A^\vee$ (see below) might all be reasonably called *polarisations*. We shall not describe the equivalence between the various notions in detail: the interested reader may consult, for example, the book by Birkenhake and Lange [**BL04**, §4.1], which gives a very clear picture of the situation over the complex numbers.

[3]here $\Im$ denotes the imaginary part

which is surjective and satisfies $\lambda_H(\Lambda) \subseteq \Lambda^\vee$. In particular, it induces a surjective analytic homomorphism $\lambda_H : V/\Lambda \to \overline{V}^\vee/\Lambda^\vee$ which is easily seen to have finite kernel (we will soon call such morphism **isogenies**). The polarisation H is said to be **principal** if λ_H is an isomorphism; this happens precisely when $d(H) = 1$.

Example 4.12 (Canonical polarisation of an elliptic curve). We now show that every elliptic curve over $\mathbb{C}$ admits a canonical principal polarisation. Up to a $\mathbb{C}$-linear change of variables, we may assume that the lattice Λ is $\mathbb{Z} \cdot 1 \oplus \mathbb{Z} \cdot \tau$, with τ in the upper half-plane. To define a polarisation we need to define a positive-definite Hermitian form $\mathbb{C} \times \mathbb{C}$ whose imaginary part takes integer values on 1 and $\tau = a + bi$. A Hermitian scalar product on $\mathbb{C}$ is uniquely defined by its value on $(1, 1)$, so we look for a polarisation of the form

$$\begin{array}{rccc} H: & \mathbb{C} \times \mathbb{C} & \to & \mathbb{C} \\ & (z_1, z_2) & \mapsto & \gamma z_1 \overline{z_2}; \end{array}$$

in order for H to be Hermitian and positive definite, γ needs to be real and positive.

Write $E := \Im H$; one checks that E is skew-symmetric (this is always true: if H is a polarisation, $E := \Im H$ is skew-symmetric), hence we have $E(1, 1) = E(\tau, \tau) = 0$; the only requirement is then $E(\tau, 1) \in \mathbb{Z}$, that is, $\gamma \Im\tau \in \mathbb{Z}$. Since $\Im\tau > 0$, we can choose $\gamma := \frac{1}{\Im\tau}$. We then obtain the polarisation

$$H(z_1, z_2) = \frac{z_1 \overline{z_2}}{\Im\tau}.$$

It is also easy to see that H is a principal polarisation (and in fact it's the *unique* principal polarisation of E). Assuming the previous remark it would be enough to notice that in the basis $\{\tau, 1\}$ the matrix of $\Im H$ is $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ to deduce that $d(H) = 1$ and that H is a principal polarisation. We check this by hand by finding the lattice $\Lambda^\vee$. A linear functional ψ lies in $\Lambda^\vee$ if and only if $\Im\psi(1) \in \mathbb{Z}$ and $\Im\psi(\tau) \in \mathbb{Z}$. Clearly ψ is determined by $\psi(1) = a + bi$ with $b \in \mathbb{Z}$; writing $\tau = \Re\tau + i\Im\tau$ we have

$$\begin{aligned} \psi(\tau) &= \psi(\Re\tau + i\Im\tau) = \Re\tau\psi(1) - i\Im\tau\psi(1) \\ &= \Re\tau(a + bi) - i\Im\tau(a + bi) = (a\Re\tau + b\Im\tau) + i(b\Re\tau - a\Im\tau), \end{aligned}$$

so that $\Im\psi(\tau) = b\Re\tau - a\Im\tau$. This is equal to an integer n if and only if

$$a = \frac{b\Re\tau - n}{\Im\tau}.$$

Hence $\psi(1) = a + bi = \dfrac{b\Re\tau + bi\Im\tau - n}{\Im\tau} = \dfrac{b\tau - n}{\Im\tau}$, and therefore $\psi = H(\lambda, \cdot)$ for $\lambda = b\tau - n \in \Lambda$. This implies that $\lambda_H : V \to \overline{V}^\vee$ induces an isomorphism of Λ with $\Lambda^\vee$, hence an isomorphism $\lambda_H : V/\Lambda \cong \overline{V}^\vee/\Lambda^\vee$ as claimed.

Finally, we remark that it is a general fact that an elliptic curve over any field K admits precisely one polarisation of degree d^2 for every $d \geq 1$ (see e.g. [**Con04**]).

We conclude this section with a result which is actually valid over any algebraically closed field, but that is easier to prove over $\mathbb{C}$:

THEOREM 4.13. *Every abelian variety $A/\mathbb{C}$ is $\mathbb{C}$-isogenous to a principally polarisable abelian variety, that is, there is a surjective analytic homomorphism φ from A to a principally polarisable abelian variety A' such that φ has finite kernel.*

PROOF. Write $A = \mathbb{C}^g/\Lambda$, choose any polarisation H (at least one exists, because A is an abelian variety and not just a complex torus), and fix a $\mathbb{Z}$-basis $\tau_1, \ldots, \tau_g, \tau_{g+1}, \ldots, \tau_{2g}$ of Λ such that the matrix of $\Im H$ is of the form

$$\Im H = \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix}$$

with $D = \mathrm{diag}(d_1, \ldots, d_g)$. Now consider the lattice $\Lambda' := \bigoplus_{i=1}^g \mathbb{Z} \cdot \frac{1}{d_i}\tau_i \oplus \bigoplus_{i=1}^g \mathbb{Z} \cdot \tau_{g+i}$. It is immediate to see that Λ' is an over-lattice of Λ, and that with respect to the obvious basis $\{\frac{1}{d_i}\tau_i, \tau_{g+i}\}_{i=1,\ldots,g}$ of Λ' the matrix representing $\Im H$ is $\begin{pmatrix} 0 & \mathrm{I}_g \\ -\mathrm{I}_g & 0 \end{pmatrix}$, so that the abelian variety $A' = \mathbb{C}^g/\Lambda'$ is principally polarised. Now simply observe that there is an isogeny $A = \mathbb{C}^g/\Lambda \to \mathbb{C}^g/\Lambda' = A'$ induced by the identity of $\mathbb{C}^g$ (the kernel is the finite group Λ'/Λ). □

5. Isogenies

DEFINITION 5.1 (Group scheme homomorphism, $\mathrm{Hom}(A, B)$). *Let $(\mathcal{G}_1, m_1, i_1, e_1)$ and $(\mathcal{G}_2, m_2, i_2, e_2)$ be group schemes over a common base S. A **homomorphism of group schemes** $f : \mathcal{G}_1 \to \mathcal{G}_2$ is a morphism of S-schemes such that $f \circ e_1 = e_2$, $m_2 \circ (f \times f) = f \circ m_1$ and $i_2 \circ f = f \circ i_1$. If $f : \mathcal{G}_1 \to \mathcal{G}_2$ is a group scheme homomorphism then one defines* $\ker f$ *in the obvious way, namely as the fiber product*

$$\begin{array}{ccc} \ker f & \longrightarrow & \mathcal{G}_1 \\ \downarrow & & \downarrow{\scriptstyle f} \\ S & \xrightarrow[e_2]{} & \mathcal{G}_2 \end{array}$$

$\ker f$ *is then a subgroup scheme of $\mathcal{G}_1$ (with the obvious definition: a subscheme which inherits a structure of group scheme when endowed with the suitable base changes of the maps m_1, i_1, e_1).*

*When A, B are abelian varieties we shall say that f is a **homomorphism of abelian varieties**, or simply a **homomorphism**. The set of all K-homomorphisms $A \to B$ is a group in the obvious way, and is denoted by* $\mathrm{Hom}_K(A, B)$.

DEFINITION 5.2. *Let $f : X \to Y$ be a finite surjective morphism between algebraic varieties over a field K. The **degree** of f is the degree of the finite field extension of the function field $K(X)$ over $f^*K(Y)$.*

DEFINITION 5.3. *Let A, B be abelian varieties over the field K. A **K-isogeny** between A and B is a homomorphism $A \to B$ defined over K and such that* $\ker A$ *is finite. The **degree** of an isogeny φ is its degree in the sense of the previous definition (see proposition 5.5 below).*

REMARK 5.4. The degree of an isogeny φ agrees with the order of $\ker\varphi$, where *order* means *rank as a finite group scheme*. When the isogeny is separable (which is always the case in characteristic zero), the order of $\ker\phi$ is really the number of geometric points of $\ker\phi$.

It is useful to know that isogenies can be characterised in many equivalent ways: the following standard result can be found for example in [**Mil12**, Proposition 8.1].

PROPOSITION 5.5. *For a homomorphism $f : A \to B$ of abelian varieties, the following statements are equivalent:*

(1) *f is an isogeny;*
(2) *$\dim A = \dim B$ and f is surjective;*
(3) *$\dim A = \dim B$ and $\ker f$ is a finite group (scheme);*
(4) *f is finite, flat, and surjective.*

REMARK 5.6. Notice in particular that a K-isogeny $\varphi : A \to B$ can only exist if A and B have the same dimension, see also definition 5.13 and remark 5.14.

REMARK 5.7. It is often useful to think about isogenies in geometric/topological terms: over $\mathbb{C}$, for example, an isogeny $\varphi : A \to B$ induces a covering map $\varphi : A(\mathbb{C}) \to B(\mathbb{C})$, and this map is Galois with group $\ker\varphi$. More generally, over a field of characteristic 0 isogenies are étale[4] maps. Even more generally, an isogeny of degree n is étale over any field K such that $(n, \operatorname{char} K) = 1$. The reason for this is that the group structure allows one to carry étaleness from one point to another, and étaleness at zero follows from the fact that $[n]$ (see definition 5.11) induces multiplication by n on the tangent space at 0 of any abelian variety, and an isogeny of degree n is a factor of $[n]$.

REMARK 5.8. It is clear that the degree is multiplicative: if $f : A \to B$ and $g : B \to C$ are isogenies we have

$$\deg(g \circ f) = \deg(g)\deg(f).$$

DEFINITION 5.9 (Endomorphism ring). *The (K-rational) endomorphism ring of A is*

$$\operatorname{End}_K(A) = \left\{ f : A \to A \;\middle|\; \begin{array}{c} f \text{ homomorphism} \\ \text{defined over } K \end{array} \right\}.$$

For $f \in \operatorname{End}_K(A)$ we define $\deg(f)$ as before in case f is an isogeny, and we set $\deg(f) = 0$ otherwise.

REMARK 5.10. Notice that a homomorphism $f : A \to A$ that is not an isogeny cannot be surjective, and that the composition of two endomorphisms, at least one of which fails to be surjective, cannot be surjective. This implies that $\deg : \operatorname{End}_K(A) \to \mathbb{N}$ satisfies

$$\deg(fg) = \deg(f)\deg(g)$$

for every pair of elements $f, g \in \operatorname{End}_K(A)$.

[4]recall that *étale* is the algebro-geometric version of *covering map*

DEFINITION 5.11 (Action of $\mathbb{Z}$ on A). *The ring* $\mathrm{End}_K(A)$ *contains a canonical copy of the integers: indeed, for every* $n \in \mathbb{N}$ *the map*

$$\begin{array}{rccc} [n]: & A & \to & A \\ & x & \mapsto & \underbrace{x + \cdots + x}_{n \text{ times}} \end{array}$$

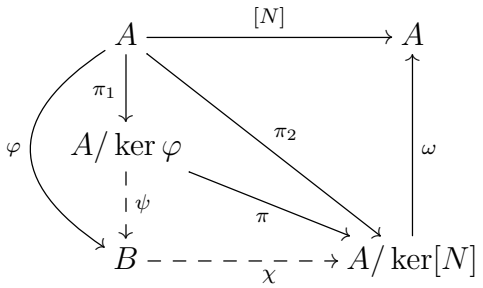
is an endomorphism of A*. We further define* $[-1]$ *to be the map giving the inverse for the group law, and for* $n > 1$ *we define* $[-n]$ *as the composition of* $[n]$ *and* $[-1]$*. This gives a canonical identification* $n \mapsto [n]$ *of* $\mathbb{Z}$ *with a subring of* $\mathrm{End}_K(A)$*. One often says that* A *has* ***trivial endomorphisms over*** K *if* $n \mapsto [n]$ *induces an isomorphism* $\mathbb{Z} \cong \mathrm{End}_K(A)$*.*

Once we have the isogenies $[n]$ we can look at their kernels; these will play an important role in what is to follow:

DEFINITION 5.12. *Let* A *be an abelian variety over the field* K *and let* n *be a positive integer. We define* $A[n]$ *to be the kernel of* $[n] : A(\overline{K}) \to A(\overline{K})$*. We call* $A[n]$ *the* ***group of*** n***-torsion points of*** A*.*

DEFINITION 5.13 (Isogenous abelian varieties). *We say that* A *is isogenous to* B*, and write* $A \sim B$*, if there exists an isogeny* $\varphi : A \to B$*.*

REMARK 5.14 (Isogeny is an equivalence relation). $\sim$ induces an equivalence relation. Indeed, it is clear that $\sim$ is reflexive and transitive[5], and it suffices to check that it is symmetric. Suppose that $\varphi : A \to B$ is an isogeny: we want to construct an isogeny $B \to A$ in the opposite direction. Since $\ker\varphi$ is a finite group (scheme), it is in particular of finite exponent N, so $\ker\varphi \subseteq \ker[N]$ (also as group schemes). Consider the following commutative diagram:



We notice that ψ exists and is an isomorphism because of the universal property of the quotient $A \to A/\ker\varphi$; moreover, since $\ker\varphi$ is contained in $\ker[N]$, one sees that there is a homomorphism π as in the diagram (in fact, it is nothing but the canonical projection from $A/\ker\varphi$ to $\frac{A/\ker\varphi}{A[N]/\ker\varphi}$). In particular we may define $\chi := \pi \circ \psi^{-1}$. Finally, using again the universal property of the quotient one also sees that ω is an isomorphism. Putting everything together we may define a homomorphism $B \to A$ as the composition $\omega \circ \chi = \omega \circ \pi \circ \psi^{-1}$; this homomorphism is in fact an isogeny because ω and ψ^{-1} are isomorphisms and π is an isogeny.

[5]if $A \sim B$ and $B \sim C$, then we have isogenies $\varphi_1 : A \to B$ and $\varphi_2 : B \to C$, so $\varphi_2 \circ \varphi_1$ is an isogeny $A \to C$

The argument in the previous remark implies in particular:

PROPOSITION 5.15. *Let $f : A \to B$ be an isogeny of degree d. There exists an isogeny $g : B \to A$ such that $g \circ f = f \circ g = [d]$.*

REMARK 5.16. It is sometimes useful to work in the *category $\mathcal{S}$ of abelian varieties (over K) up to isogeny*. This is the category whose objects are abelian varieties over K and such that $\mathrm{Hom}_{\mathcal{S}}(A, B) = \mathrm{Hom}_K(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}$. The previous remark, together with Poincaré's complete reducibility theorem (see theorem 7.1), implies that $\mathcal{S}$ is a *semisimple category*: every object is a direct sum of simple objects. In less fancy language, this simply means that every abelian variety is isogenous to the direct product of simple abelian varieties.

PROPOSITION 5.17. *For every positive integer $[n]$, the degree of $[n]$ is n^{2g}.*

PROOF. In order to compute the degree of $[n]$ we look at its action on a very ample line bundle $\mathcal{L}$.One can always find a *symmetric* ample line bundle, namely an ample $\mathcal{L}$ such that $[-1]^*\mathcal{L} \cong \mathcal{L}$: indeed, if $\mathcal{M}$ is any ample line bundle, $\mathcal{L} := \mathcal{M} \otimes [-1]^*\mathcal{M}$ is ample and symmetric. Taking a sufficiently large power will make it very ample; we still call $\mathcal{L}$ the resulting line bundle.

Corollary 3.3 implies that $[n]^*\mathcal{L} \cong \mathcal{L}^{\otimes n^2}$ – notice that this is in particular compatible with the assumption $[-1]^*\mathcal{L} \cong \mathcal{L}$. It follows that $[n]^*\mathcal{L}|_{\ker[n]} \cong \mathcal{L}^{\otimes n^2}|_{\ker[n]}$ is both trivial and very ample, which is only possible if $\ker[n]$ is zero-dimensional (hence $[n]$ is an isogeny). Furthermore, writing $\mathcal{L}$ as $\mathcal{O}(D)$, we have

$$\deg[n]\,(D, \dots, D) = ([n]^*D, \cdots, [n]^*D) = \left(n^2D, \cdots, n^2D\right) = n^{2g}\,(D, \dots, D)$$

where $(D, \dots, D)$ denotes the intersection product (of divisors). In order to conclude it suffices to show that $(D, \dots, D)$ is nonzero, but this is easy, because since $\mathcal{L}$ is very ample (hence it induces an embedding $A \hookrightarrow \mathbb{P}^N$) we may compute this intersection product as the intersection product of g general hyperplane sections of $A \hookrightarrow \mathbb{P}^N$, and this is clearly positive. □

DEFINITION 5.18 (Abelian subvarieties). *Let A/K be an abelian variety. An **abelian subvariety** is a connected subgroup scheme $B \subseteq A$, that is, a subvariety of A that is itself an abelian variety with the induced operations. An abelian variety A/K is said to be **simple** (or K-simple, if we want to stress the field of definition) if the only abelian subvarieties of A are A itself and $\{0_A\}$. When $A \times_K \overline{K}$ is simple, one says that A is **geometrically simple** or **absolutely simple**: clearly absolutely simple implies simple, but the converse implication does not hold (for an example see section 1.2).*

6. The dual abelian variety, polarisations, and the Weil pairing

We now introduce the **dual abelian variety** of an abelian variety A. The reader familiar with elliptic curves may never have heard of the notion, because for an elliptic curve E the dual abelian variety is E itself, and the distinction is almost never made. With varieties of higher dimension, however, A and its dual are often not isomorphic and it becomes important to distinguish them.

Roughly speaking, the dual abelian variety of A parametrises (certain kinds of) line bundles on A. More precisely, we define $\mathrm{Pic}^0(A)$ as the set of line bundles $\mathcal{L}$ on A which satisfy $\tau_a^*\mathcal{L} \cong \mathcal{L}$ for all $a \in A(\overline{K})$, where τ_a denotes translation by a. We may then define the dual abelian variety as follows:

Definition 6.1 (Dual abelian variety). *A pair $(A^\vee, \mathcal{P})$, where $A^\vee$ is an abelian variety and $\mathcal{P}$ is a line bundle on $A \times A^\vee$, is a (the) dual abelian variety of A if the following holds:*

1. *$\mathcal{P}|_{A\times\{b\}}$ is in $\mathrm{Pic}^0(A_b)$*
2. *$\mathcal{P}|_{\{0\}\times A^\vee}$ is trivial*
3. *$(A^\vee, \mathcal{P})$ is universal among such pairs, that is, the following universal property holds: for all pairs $(T, \mathcal{L})$ consisting of a variety and an invertible sheaf $\mathcal{L}$ on $A \times T$ that satisfies*
   (a) *$\mathcal{L}|_{A\times\{t\}}$ is in $\mathrm{Pic}^0(A_t)$*
   (b) *$\mathcal{L}|_{\{0\}\times T}$ is trivial*
   there is a unique regular map $\alpha : T \to A^\vee$ such that $\mathcal{L} \cong (1 \times \alpha)^*\mathcal{P}$.

Remark 6.2. Of course one should show that the dual abelian variety *exists*! This is done in [**Mum70**]. One can also prove further properties of $A^\vee$, namely, it is functorial in A and is a good duality, in the sense that $(A^\vee)^\vee$ is canonically isomorphic to A itself.

Remark 6.3. An equivalent way of stating the universal property is that

$$\mathrm{Mor}(T, A^\vee) \leftrightarrow \left\{ \begin{array}{c} \text{line bundles } \mathcal{L} \text{ on } A \times T \\ \text{satisfying (a), (b)} \end{array} \right\} / \sim,$$

where the set on the left denotes the space of regular maps $T \to A^\vee$ and $\sim$ is isomorphism of line bundles. Applying this characterisation to $T = \mathrm{Spec}(K)$ we obtain $A^\vee(K) = \mathrm{Pic}^0(A)$.

We describe a standard way to construct maps $A \to A^\vee$:

Definition 6.4 (Mumford's construction). *Let $\mathcal{L}$ be a line bundle on $A_{\overline{K}}$. We define*

$$\begin{array}{rccc} \lambda_{\mathcal{L}} : & A_{\overline{K}} & \to & A^\vee_{\overline{K}} \\ & a & \mapsto & \tau_a^*\mathcal{L} \otimes \mathcal{L}^{-1}, \end{array}$$

where τ_a is translation by a; it follows from the theorem of the square (and the fact that a homologically trivial line bundle is anti-symmetric) that $\lambda_{\mathcal{L}}$ is a homomorphism.

Remark 6.5. Line bundles $\mathcal{L}$ in $\mathrm{Pic}^0(A)$ are precisely those for which $\lambda_{\mathcal{L}}$ is the zero map.

We have already met polarisations in the context of complex abelian varieties (see definition 4.8): we now introduce their algebraic counterparts.

Definition 6.6 (Polarisation, algebraic setting). *A K-**polarisation** of the abelian variety A/K is a K-isogeny $\varphi : A \to A^\vee$ such that **over** $\overline{K}$ φ is of the form $\lambda_{\mathcal{L}}$ for some ample line bundle $\mathcal{L}$. Unfortunately, this is not quite the same as requiring that φ is of the form $\lambda_{\mathcal{L}}$ already over K.*

*A **principal polarisation** is a polarisation which induces an isomorphism $A \cong A^\vee$; notice that principal polarisations need not exist if* $\dim A > 1$. *A pair (A, λ), where A is an abelian variety and λ is a principal polarisation, is usually called a **principally polarised abelian variety**, or **PPAV** for short.*

REMARK 6.7. Let A/K be an abelian variety over an arbitrary field. Then A and $A^\vee$ are isogenous (but not necessarily isomorphic) over K. Proving this is harder than it sounds, and is essentially equivalent to the fact that A is projective. In fact, Mumford's strategy to show that A and $A^\vee$ are isogenous was to prove that $\lambda_{\mathcal{L}}$ is surjective with finite kernel whenever $\mathcal{L}$ is ample; if one chooses $\mathcal{L}$ defined over K, then also the resulting isogeny is defined over K.

One has the following useful fact:

THEOREM 6.8. *Every abelian variety A/K is $\overline{K}$-isogenous to a principally polarisable abelian variety.*

REMARK 6.9. For a proof in the complex case see theorem 4.13. The proof in the general case (see e.g. [**Mum70**, Corollary 1 on page 234]) is conceptually the same but technically more complicated: one needs to rephrase the present elementary argument in the language of section of line bundles, and interpret our quotient Λ'/Λ as a certain subgroup of $\ker \lambda_{\mathcal{L}}$, where $\mathcal{L}$ is the ample line bundle defining the polarisation. For the sake of completeness, let us point out that the finite subgroup $G := \Lambda'/\Lambda$ of A we considered is precisely a maximal subgroup of $\ker(\lambda_h : A \to A^\vee)$ with the property $\Im H|_{G\times G} \subseteq \mathbb{Z}$: one can make sense of this description for abelian varieties over arbitrary algebraically closed fields, and it is using this description that Mumford proves this theorem in full generality.

DEFINITION 6.10 (Dual homomorphism). *Let $A/K, B/K$ be abelian varieties. Given any K-homomorphism $\varphi : A \to B$, there is a dual homomorphism $\varphi^\vee : B^\vee \to A^\vee$ constructed by applying the universal property of $A^\vee$ with $T = B^\vee$ and $\mathcal{L} = (\varphi \times 1)^* \mathcal{P}_{B\times B^\vee}$ (notice that this is a line bundle on $A \times B^\vee$) to obtain a map $B^\vee = T \to A^\vee$. Concretely, at the level of points, $\varphi^\vee$ is simply the pullback of line bundles from B to A:*

$$\begin{array}{rccc} \varphi^\vee : & B^\vee(K) = \mathrm{Pic}^0(B) & \to & A^\vee(K) = \mathrm{Pic}^0(A) \\ & \mathcal{L} & \mapsto & \varphi^*\mathcal{L} \end{array}$$

That $f^\vee$ is itself an isogeny is not obvious; for a proof, see for example [**EMvG**, Theorem 7.5] or [**Mum70**, p. 143].

THEOREM 6.11 (Properties of the dual isogeny). *Let $f : A \to B$ be an isogeny and write N for the kernel of f. Then the dual map $f^\vee : B^\vee \to A^\vee$ is an isogeny, and its finite kernel $K^\vee$ is the dual of K in the sense of Cartier duality. In particular,* $\deg(f^\vee) = \deg(f)$.

REMARK 6.12. Cartier duality over fields of positive characteristic can be quite complicated. Over fields of characteristic zero, however, the Cartier dual is easy to describe: if G is a finite commutative group of order N,

$$G^\vee = \mathrm{Hom}(G(\overline{K}), \mu_N(\overline{K})).$$

More precisely: a finite group scheme $G^\vee$ is described by a finite abstract group H, together with an action of $\mathrm{Gal}\left(\overline{K}/K\right)$ on H. In this case the underlying finite group H is $\mathrm{Hom}(G(\overline{K}), \mu_N(\overline{K}))$, and the Galois action is the natural one.

DEFINITION 6.13 (Rosati involution). *Fix a K-polarisation $\lambda : A \to A^\vee$ of degree d, and recall (remark 5.14) that there is an isogeny $\hat{\lambda} : A^\vee \to A$ such that $\hat{\lambda} \circ \lambda = [d]$. Given an endomorphism $\varphi : A \to A$ we define*

$$\varphi^\dagger = \frac{1}{d}\hat{\lambda} \circ \varphi^\vee \circ \lambda \in \mathrm{End}_K(A) \otimes \mathbb{Q}.$$

REMARK 6.14. The equality $(\varphi^\dagger)^\dagger = \varphi$ holds; it can be proven (see corollary 10.12) by exploiting the relation between the Rosati involution and the Weil pairing.

DEFINITION 6.15 (Weil pairing). *For every n there is a canonical pairing*

$$e_n : A[n] \times A^\vee[n] \to \mathbb{G}_m[n] = \mu_n$$

defined as follows. Let $t \in A[n]$ and $\mathcal{L} \in A^\vee[n]$. By definition we have $nt = 0$ and $\mathcal{L}^{\otimes n} \cong \mathcal{O}$. An application of the theorem of the cube gives $[n]^*\mathcal{L} \cong \mathcal{L}^{\otimes n} \cong \mathcal{O}$, so we may fix an isomorphism $u : \mathcal{O} \to [n]^*\mathcal{L}$. Denote by $\tau_t : A \to A$ the morphism translation-by-t. Pulling back the isomorphism $u : \mathcal{O} \to [n]^*\mathcal{L}$ via τ_t we obtain

$$\tau_t^* u : \tau_t^*\mathcal{O} \to \tau_t^*[n]^*\mathcal{L} \cong ([n] \circ \tau_t)^*\mathcal{L} = [n]^*\mathcal{L}.$$

Recalling that $\tau_t^*\mathcal{O} = \mathcal{O}$, it follows in particular that $u \circ (\tau_t^* u)^{-1}$ is an isomorphism of $[n]^*\mathcal{L}$; an automorphism of a line bundle on the complete variety A can only be multiplication by an element ζ of $H^0(A_{\overline{K}}, \mathcal{O}^\times) = \overline{K}^\times$, and we define $e_n(t, \mathcal{L}) = \zeta$. It is clear from the definition that

$$1 = e_n(nt, \mathcal{L}) = e_n(t, \mathcal{L})^n = \zeta^n,$$

so ζ is in fact an n-th root of unity.

REMARK 6.16. If $A = E$ is an elliptic curve, the identification $E \cong E^\vee$ given by the canonical principal polarisation allows one to define the Weil pairing directly as a map $E[n] \times E[n] \to \mu_n$. In the general case, if $(A, \mathcal{L})$ is a *polarised* abelian variety one may still define a Weil pairing by the formula

$$\begin{array}{rccc} e_n^{\mathcal{L}} : & A[n] \times A[n] & \to & \mu_n \\ & (t_1, t_2) & \mapsto & e_n\left(t_1, \lambda_{\mathcal{L}}(t_2)\right). \end{array}$$

When $\mathcal{L}$ is not a principal polarisation, however, this pairing may have a nontrivial kernel on the right.

THEOREM 6.17 (Properties of the Weil pairing). *The following hold:*

(1) *We have*

$$e_{mn}(P, Q)^m = e_n(mP, mQ) \text{ for } P \in A[mn], Q \in A^\vee[mn],$$

that is, the constructions of the Weil pairing on different torsion groups $A[n]$ are all compatible.

(2) *The Weil pairing is perfect, that is, the kernel on both sides is trivial.*

(3) *The Weil pairing is Galois-equivariant: for any* $\sigma \in \mathrm{Gal}\left(\overline{K}/K\right)$ *and for any pair* $P \in A[n], Q \in A^\vee[n]$ *we have*

$$e_n(\sigma P, \sigma Q) = \sigma(e_n(P,Q)).$$

(4) *For any isogeny* $\varphi : A \to B$ *with kernel contained in* $A[n]$ *we have*

$$\{y \in A^\vee[n] : e_n(x,y) = 0 \quad \forall x \in \ker\varphi\} = \ker\varphi^\vee.$$

(5) *The Weil pairing is compatible with the duality of isogenies, in the sense that if* $f : A \to B$ *is an isogeny then we have*

$$e_n(f(x), y) = e_n(x, f^\vee(y))$$

for all $x \in A[n]$ *and* $y \in B^\vee[n]$.

(6) *For any polarisation* $\mathcal{L}$*, the Weil pairing* $e_n^{\mathcal{L}}$ *introduced above is skew-symmetric on* $A[n]$.

7. Poincaré's total reducibility theorem

THEOREM 7.1. *The following hold:*

(1) *Let* A/K *be an abelian variety and let* B/K *be an abelian subvariety of* A/K*. There exists an abelian subvariety* C *of* A*, also defined over* K*, such that*

$$\begin{array}{ccc} B \times C & \to & A \\ (b,c) & \mapsto & b+c \end{array}$$

is an isogeny. The subvariety C *is often called a* ***complement*** *to* B *in* A.

(2) *Let* A/K *be an abelian variety. There exist* K*-simple abelian* K*-subvarieties* $A_1, \ldots, A_n$ *of* A *such that*

$$\begin{array}{ccc} A_1 \times \cdots \times A_n & \to & A \\ (a_1, \ldots, a_n) & \mapsto & a_1 + \cdots + a_n \end{array}$$

is an isogeny.

SKETCH OF PROOF (FIELDS OF CHARACTERISTIC 0). The second statement follows from (1) by induction (and the fact that a proper abelian subvariety of A has strictly smaller dimension than A). For (1), fix an ample line bundle $\mathcal{L}$ on A and consider the homomorphism of abelian varieties

$$\varphi : A \xrightarrow{\lambda_{\mathcal{L}}} A^\vee \xrightarrow{i^\vee} B^\vee.$$

The connected component of the kernel of φ passing through 0_A is a connected, proper algebraic group, hence an abelian variety[6]. Call it C. One has

$$\dim C \geq \dim\ker(i^\vee) \geq \dim(A^\vee) - \dim(B^\vee) = \dim(A) - \dim(B).$$

We now show that B and C intersect in finitely many points: indeed $(i^\vee \circ \lambda_{\mathcal{L}})|_B = \lambda_{\mathcal{L}|_B}$, which is an isogeny $B \to B^\vee$ (hence has finite kernel) since $\mathcal{L}|_B$ is ample. This implies that $B \times C \xrightarrow{+} A$ is a homomorphism of abelian varieties with finite kernel, hence $\dim(B) +$

[6]since $\mathrm{char}(K) = 0$

$\dim(C) \leq \dim(A)$. Combined with our previous inequality, this yields $\dim(B)+\dim(C) = \dim(A)$, and since $B \times C \xrightarrow{+} A$ has finite kernel it is an isogeny. □

REMARK 7.2. The isogeny in Poincaré's theorem is usually **not** an isomorphism. When $n = 2$ (i.e. there are two simple subvarieties A_1, A_2 of A such that the sum $+ : A_1 \times A_2 \to A$ is an isogeny), the kernel of the sum is essentially the intersection $A_1 \cap A_2$.

8. The Mordell-Weil theorem

Even though we won't make much use of this theorem, no introduction to the arithmetic theory of abelian varieties would be complete without a mention of the famous Mordell-Weil theorem:

THEOREM 8.1 (Mordell-Weil). *Let A/K be an abelian variety over a number field. The group $A(K)$ of its rational points is finitely generated, that is, there exist a number $r \in \mathbb{N}$ and a finite abelian group T such that*

$$A(K) \cong \mathbb{Z}^r \oplus T.$$

*The number r is called the **rank** of A/K.*

9. Jacobians

After the previous general introduction we now turn to more concrete objects; accordingly, we also try to make the exposition more detailed and down-to-earth. We start by considering Jacobians, which are (principally polarised) abelian varieties canonically associated with curves. By a **curve** defined over K we shall usually mean a smooth, projective, geometrically integral K-algebraic variety of dimension 1; thus, for example, the reader should be warned that "the curve $y^2 = f(x)$, defined over $\mathbb{Q}$" will really mean "the unique smooth projective curve over $\mathbb{Q}$ birational to the affine curve $\{y^2 = f(x)\} \subseteq \mathbb{A}^2_{\mathbb{Q}}$".

9.1. Divisors and their classes. Assume that K is a *perfect* field and let C be a curve over K.

DEFINITION 9.1. *The **group of divisors** Div_C is the free abelian group generated by the set $C(\overline{K})$. An element of this group is called a **divisor**, and is nothing but a formal linear combination of $\overline{K}$-rational points with integral coefficients. A divisor is **effective** if all its coefficients are non-negative.*

We shall represent divisors in the form $D = \sum_{i=1}^{k} n_i P_i$, where $k \in \mathbb{N}$, $n_i \in \mathbb{Z}$ and $P_i \in C(\overline{K})$ for $i = 1, \ldots, k$.

So far, this definition only depends on the $\overline{K}$-points of C, hence it is not too suitable to study the arithmetic of C over K: we need to know what it means for a divisor to be defined over K. The definition is straightforward:

DEFINITION 9.2. *The group $\mathrm{Gal}\left(\overline{K}/K\right)$ acts on $C(\overline{K})$ in a natural way, hence it also acts on Div_C. The fixed points for this action form a subgroup, which we denote by $\mathrm{Div}_C(K)$ and whose elements we call **K-rational divisors**.*

REMARK 9.3. If all the points $P_1, \ldots, P_r$ are rational, a divisor $D = \sum n_i P_i$ is certainly K-rational, because $\mathrm{Gal}\left(\overline{K}/K\right)$ acts trivially on the P_i. However, a divisor can be K-rational even if the corresponding P_i are not: consider for example the curve $C: x^2+y^2 = -1/\mathbb{Q}$. The divisor $(0,i)+(0,-i)$ is $\mathbb{Q}$-rational, but the points $(0,i)$ and $(0,-i)$ are not defined over $\mathbb{Q}$.

We also remark that there is an obvious numerical invariant attached to a divisor, namely its **degree**:

DEFINITION 9.4 (Degree of a divisor). *The **degree** of a divisor $D = \sum_{i=1}^{k} n_i P_i$ is*

$$\deg D = \sum n_i \in \mathbb{Z}.$$

We interpret deg *as a group homomorphism* $\mathrm{Div}_C \to \mathbb{Z}$*; its kernel will be denoted by* Div_C^0 *(the subgroup of divisors of degree 0).*

DEFINITION 9.5 (Divisor of a function). *Let $f \in \overline{K}(C) \setminus \{0\}$ be a rational function on C. The divisor of f is*

$$\mathrm{div}(f) = \sum_P v_P(f),$$

where the sum is over all the points of $C(\overline{K})$. Here $v_P(f)$ is the order of vanishing of f at P; if f has a pole of order k at P, then $v_P(f) = -k$.

REMARK 9.6. Any nonzero rational function has only finitely many zeroes and poles, hence the sum defining $\mathrm{div}(f)$ is finite and $\mathrm{div}(f)$ is indeed a divisor.

DEFINITION 9.7 (Principal divisor). *A divisor is said to be **principal** if it is of the form* $\mathrm{div}(f)$ *for some nonzero rational function $f \in \overline{K}(C)$. One checks without difficulty*[7] *that a principal divisor has degree 0 (a rational function has as many zeroes as poles). We denote by* $\mathrm{Princ}_C < \mathrm{Div}_C^0$ *the subgroup of principal divisors.*

DEFINITION 9.8 (Picard group). *We define*

$$\mathrm{Pic}_C = \mathrm{Div}_C \,/\, \mathrm{Princ}_C$$

and

$$\mathrm{Pic}_C^0 = \mathrm{Div}_C^0 \,/\, \mathrm{Princ}_C;$$

equivalently, we observe that $\deg : \mathrm{Div}_C \to \mathbb{Z}$ *descends to* $\deg : \mathrm{Pic}_C \to \mathbb{Z}$*, and we define* Pic_C^0 *to be the kernel of* deg.

DEFINITION 9.9. *Two divisors D_1, D_2 are said to be **linearly equivalent** (written as $D_1 \sim D_2$) if they differ by a principal divisor. We denote by $[D]$ the class of the divisor D in* Pic_C.

[7] if g is a non-constant morphism $C \to \mathbb{P}^1$, one has $\deg(\mathrm{div}(f)) = \deg(g_*(\mathrm{div}(f))) = \deg \mathrm{div}(g_* f)$. Hence it suffices to treat the case $C = \mathbb{P}^1$, which is obvious. Here the push-forward operator on functions g_* is the norm of the field extension $\overline{K}(\mathbb{P}^1) \subseteq \overline{K}(C)$.

NOTATION 9.10. *We shall also write (for example)* $\mathrm{Princ}(\overline{K})$ *or* $\mathrm{Div}_C(\overline{K})$ *when we want to stress that we are considering these as sets (*$\mathrm{Div}_C, \mathrm{Princ}_C$ *have in principle a richer structure).*

By analogy to the definition of $\mathrm{Div}_C(K)$, we now define th group $\mathrm{Princ}_C(K)$ as the $\mathrm{Gal}\left(\overline{K}/K\right)$-invariant subgroup of $\mathrm{Princ}_C(K)$. Notice that $\mathrm{Princ}_C(\overline{K})$ is a Galois submodule of $\mathrm{Div}_C^0(\overline{K})$, which is in turn a Galois submodule of $\mathrm{Div}_C(\overline{K})$. This allows us to take quotients *in the category of Galois modules*, and finally leads to the definition of the K-points of Pic_C^0:

DEFINITION 9.11. *We set*

$$\mathrm{Pic}_C^0(K) = \left(\frac{\mathrm{Div}_C^0(\overline{K})}{\mathrm{Princ}_C(\overline{K})}\right)^{\mathrm{Gal}\left(\overline{K}/K\right)}$$

and

$$\mathrm{Pic}_C(K) = \left(\frac{\mathrm{Div}_C(\overline{K})}{\mathrm{Princ}_C(\overline{K})}\right)^{\mathrm{Gal}\left(\overline{K}/K\right)}.$$

REMARK 9.12. It is not true in general that an element of $\mathrm{Pic}_C(K)$ (that is, a K-rational divisor class) can be represented by a K-rational divisor: in other words, $\mathrm{Pic}_C(K)$ is *not* the same as $\mathrm{Pic}_C(\overline{K})^{\mathrm{Gal}\left(\overline{K}/K\right)}$: see example 9.14 below.

The following remark can be very useful in more advanced contexts, but can be safely skipped on a first reading:

REMARK 9.13. In fancier language, we have an exact sequence of Galois modules

$$0 \to \mathrm{Princ}_C(\overline{K}) \to \mathrm{Div}_C^0(\overline{K}) \to \mathrm{Pic}_C^0(\overline{K}) \to 0,$$

and taking invariants under $\mathrm{Gal}\left(\overline{K}/K\right)$ we get a long exact sequence in cohomology

$$0 \to \mathrm{Princ}_C(K) \to \mathrm{Div}_C^0(K) \to \mathrm{Pic}_C^0(\overline{K})^{\mathrm{Gal}\left(\overline{K}/K\right)} \to H^1(K, \mathrm{Princ}_C(K)),$$

where the last arrow may in general not be surjective. More precisely, since we also have

$$0 \to \overline{K}^\times \to \overline{K}(C)^\times \to \mathrm{Princ}_C(\overline{K}) \to 0,$$

we may again take cohomology to find

$$\begin{array}{lllll} 0 \to & & K^\times \to & K(C)^\times \to & \mathrm{Princ}_C(K) \\ \to & H^1(\Gamma_K, \overline{K}^\times) = 0 \to & H^1(\Gamma_K, \overline{K}(C)^\times) \to & H^1(\Gamma_K, \mathrm{Princ}_C(\overline{K})) & \\ \to & H^2(\Gamma_K, \overline{K}^\times) = \mathrm{Br}(K), & & & \end{array}$$

where we have used Hilbert's theorem 90 ($H^1(K, \overline{K}^\times) = 0$) and which already shows that the obstruction to surjectivity of the natural map $\mathrm{Pic}_C(K) \to \mathrm{Pic}_C(\overline{K})^{\mathrm{Gal}\left(\overline{K}/K\right)}$ should be measured by elements in the Brauer group of K.

To be even more precise (and even fancier), consider the structure map $\pi : C \to \mathrm{Spec}(k)$. By the usual interpretation of divisors as line bundles, one may define the Picard

scheme of C as $H^1(C, \mathbb{G}_m)$; we now see how the Picard schemes of C and $C_{\overline{K}}$ fit in a natural exact sequence. Recall the following form of the spectral sequence of composed functors: for a morphism of schemes $f : Y \to X$ and for a sheaf $\mathcal{F}$ on Y there is a second-page spectral sequence $H^p(X, R^q f_* \mathcal{F}) \Rightarrow H^{p+q}(Y, \mathcal{F})$. Taking the sequence of low-degree terms for the case $Y = C, X = \mathrm{Spec}(K)$ and $\mathcal{F} = \mathbb{G}_m$ yields

$$0 \to H^1(K, \pi_* \mathbb{G}_m) \to H^1(C, \mathbb{G}_m) \to H^0(K, R^1 \pi_* \mathbb{G}_m) \to H^2(K, \pi_* \mathbb{G}_m),$$

or, in more familiar terms,

$$0 \to H^1(K, \overline{K}^\times) \to H^1(C, \mathcal{O}_C^\times) \to H^0(K, H^1(C_{\overline{K}}, \mathcal{O}_C^\times)) \to H^2(K, \overline{K}^\times),$$

that is,

$$0 \to 0 \to \mathrm{Pic}_C(K) \to \mathrm{Pic}_C(\overline{K})^{\mathrm{Gal}(\overline{K}/K)} \to \mathrm{Br}(K).$$

The next term in the exact sequence is the so-called *algebraic Brauer group* of C. Note that we have used the equality $H^1(C, \mathcal{O}_C^\times) = \mathrm{Pic}_C(K)$, which follows from the fact (that we haven't proven) that the Picard group of C can be interpreted as $H^1(C, \mathbb{G}_m)$ also over non-algebraically closed fields.

Example 9.14. We show that there exist curves C over fields K with the property that not all points in $\mathrm{Jac}(C)(K)$ are represented by K-rational divisors. Consider the curve $C : y^2 = -3(x^8 + 1)$. Let $e_1, e_2, e_3, e_4 \in \overline{\mathbb{Q}}$ be the roots of $x^4 - i = 0$ and let $O = \infty_+ + \infty_-$ be the polar divisor[8] of the function x. Then the divisor

$$D = (e_1, 0) + (e_2, 0) + (e_3, 0) + (e_4, 0)$$

is defined over $\mathbb{Q}(i)$, and we now show that its divisor class is defined over $\mathbb{Q}$. Write $D' = \sigma(D) = (e_1', 0) + (e_2', 0) + (e_3', 0) + (e_4', 0)$, where σ is the unique nontrivial element of $\mathrm{Gal}\,(\mathbb{Q}(i)/\mathbb{Q})$ and the e_i' are the roots of $x^4 + i$ in $\overline{\mathbb{Q}}$. Now notice that $2D - 4O$ is principal (since it is the divisor of $x^3 + i$), hence $D \sim 4O - D$; on the other hand, $\mathrm{div}(y) = D + D' - 4O$, so

$$D + D' \sim 4O.$$

Hence $D' \sim 4O - D \sim D$, and the divisor class $[D]$ is defined over $\mathbb{Q}$. Finally, we show that there is no $\mathbb{Q}$-rational divisor whose divisor class is $[D]$. It is easy to see that D is not linearly equivalent to the canonical divisor. Suppose E is a $\mathbb{Q}$-divisor linearly equivalent to D; since $\deg(E) = \deg(D) = 4$ and D is not in the canonical class, Riemann-Roch (over $\mathbb{Q}$) implies that E is in turn $\mathbb{Q}$-linearly equivalent to a $\mathbb{Q}$-rational effective divisor. Hence we may assume that E is effective. The space

$$\mathcal{L}_{\overline{K}}(D) = \{f : \mathrm{div}\, f \geq -D\}$$

has dimension 2 by Riemann-Roch, and one checks easily that it is generated by 1 and $\dfrac{y}{x^4 - i}$. We can therefore write the general (noncostant) member of this space as

$$f_t = \frac{y - t(x^4 - i)}{x^4 - i};$$

[8] i.e. $\sum_{P : v_P(f) < 0} -v_P(f) P$

the general effective divisor linearly equivalent to D is therefore $D + \operatorname{div}(f_t)$. We show that no divisor of such form is $\mathbb{Q}$-rational. Notice first that f_t is finite at infinity, so the polar divisor of f_t is supported on the obvious affine chart of $y^2 = -3(x^8+1)$; we can write $\operatorname{div}(f_t) = (f_t)_0 - (f_t)_\infty$ with $(f_t)_\infty$ supported on our affine chart. Since $\deg(f_t)_\infty = \deg(f_t) = 4$ (with at most finitely many exceptions, that don't lead to solutions) and $(f_t)_\infty \leq D$ we have $(f_t)_\infty = D$. We now study the divisor of zeroes of f_t. The zeroes of f_t are contained in the solutions to the system

$$\begin{cases} y = t(x^4 - i) \\ y^2 = -3(x^8+1), \end{cases}$$

which (replacing the first equation in the second) gives

$$\begin{cases} y = t(x^4-i) \\ t^2(x^4-i)^2 = -3(x^4-i)(x^4+i) \end{cases} \Rightarrow \begin{cases} y = t(x^4-i) \\ (x^4-i)(x^4(t^2+3) + i(3-t^2)) = 0 \end{cases}$$

Since we already know that $(e_i, 0)$ is not a zero of f_t (in fact, it is a pole), the divisors of zeroes of f_t is given by $\sum(x_j, y_j)$, where the x_j are the roots of the equation $x^4(t^2+3) + i(3-t^2) = 0$ and $y_j = t(x_j^4 - 1)$. Assume that $t^2 \neq -3$ (this case being easy to exclude); notice that the y-coordinates of the four points in the support of $(f_t)_0$ are all equal to $t(x_1^4 - i) = -6\frac{it}{t^2+3}$; it follows that the divisor of zeroes of f_t is $\mathbb{Q}$-rational if and only if the following hold:

(1) $\frac{it}{t^2+3}$ is rational;
(2) x_1, x_2, x_3, x_4 are roots of a polynomial with rational coefficients, that is, $\frac{i(t^2-3)}{t^2+3}$ is rational.

A short computation now shows that, writing $t = a + bi$, this is only possible if $(a^2+b^2)^2 = \pm 3$, that is, if and only if ± 3 is a norm in the extension $\mathbb{Q}(i)/\mathbb{Q}$. It is well-known that this is not the case, hence the rational divisor class $[D]$ cannot be represented by a rational divisor. Notice that O is also a rational divisor, hence $[D - 2O]$ is a rational divisor class of degree 0 (that is, a point in $\operatorname{Jac}(C)(\mathbb{Q})$) which is not represented by a rational divisor.

Remark 9.15. After this somewhat long and computational example, let me mention that for many curves one does in fact have $\operatorname{Jac}_C(K) = \operatorname{Jac}_C(\overline{K})^{\operatorname{Gal}(\overline{K}/K)}$: this equality holds for all curves with a rational point, and it also holds for rational divisor classes of degree 1 for curves with a point in every completion of K ([**CM96**]). To prove the equality $\operatorname{Pic}_C(\overline{K})^{\operatorname{Gal}(\overline{K}/K)} = \operatorname{Pic}_C(K)$ in the case $C(K) \neq \emptyset$ one may notice that (with the notation of remark 9.13) a rational point gives a section of $\pi : C \to \operatorname{Spec}(K)$, hence by functoriality a retraction of the canonical map $\operatorname{Pic}_C(K) \to \operatorname{Pic}_C(\overline{K})^{\operatorname{Gal}(\overline{K}/K)}$.

Theorem 9.16 (Jacobian of a curve). *Let C be a nice curve over K. There is an abelian variety J over K such that there is an isomorphism of* $\operatorname{Gal}(\overline{K}/K)$*-modules* $\operatorname{Pic}_C^0 \cong J(\overline{K})$. *This abelian variety J is called the Jacobian variety, or just the Jacobian, of C. The dimension of J agrees with the genus of C.*

REMARK 9.17. Jacobian varieties are principally polarised (even when $C(K) = \emptyset$): when $C(K) \neq \emptyset$ and $g \geq 2$, the (linear equivalence class of a) divisor giving the principal polarisation may be obtained as the image of any map of the form

$$\begin{array}{ccc} \mathrm{Sym}^{g-1}(C) & \to & \mathrm{Jac}(C) \\ (P_1, \ldots, P_{g-1}) & \mapsto & P_1 + \ldots + P_{g-1} - (g-1)O, \end{array}$$

where O is a point in $C(K)$.

Suppose that $C(K)$ is nonempty and fix a point $P \in C(K)$. We can associate with this point an embedding of C in $\mathrm{Jac}(C)$: identifying $\mathrm{Jac}(C) \cong \mathrm{Pic}^0_C(K)$, we may define a map $C \to \mathrm{Pic}^0_C(K) \cong \mathrm{Jac}(C)$ by the formula $Q \mapsto [Q - P]$. We'll see below in example 9.20 that in the case when $C = E$ is an elliptic curve and $P = O$ is the origin of the group law the map $E \to \mathrm{Jac}(E)$ thus defined is an isomorphism.

As is the case for many important objects in algebraic geometry, Jacobians also satisfy a useful universal property:

PROPOSITION 9.18 (Universal property of the Jacobian). *Let C/K be a curve with Jacobian J/K. Fix a rational point $P \in C(K)$ and denote by $i : C \to J$ the corresponding embedding of C into its Jacobian. Then J satisfies the following universal property: for any abelian variety A and for any algebraic morphism $f : C \to A$ such that $f(P) = 0_A$ there is a unique homomorphism of abelian varieties $g : J \to A$ such that the following diagram commutes:*

$$\begin{array}{ccc} C & \xrightarrow{i} & J \\ & \searrow^{f} & \downarrow{\scriptstyle g} \\ & & A \end{array}$$

REMARK 9.19. To be more precise, this is the universal property of the Albanese variety of the pair (C, P) (that is: the Albanese variety is by definition the initial object with respect to maps from (C, P) to abelian varieties that carry P to the neutral element). The point is that – assuming for simplicity that K is perfect – the Albanese variety of (C, P) is naturally isomorphic to the *dual* of Pic^0_C. Finally, one obtains $\mathrm{Alb}(C, P) \cong (\mathrm{Pic}^0_C)^\vee \cong (\mathrm{Pic}^0_C)$, because Jacobians are canonically principally polarised.

To construct the isomorphism $\mathrm{Alb}(C, P) \cong \mathrm{Pic}^0_C$, notice that given a map from C to an abelian variety A carrying P to 0_A we obtain by pullback a map

$$\mathrm{Pic}_A \to \mathrm{Pic}_C,$$

which maps the connected component of the identity of the former into the connected component of the identity of the latter, whence a map

$$\mathrm{Pic}^0_A \to \mathrm{Pic}^0_C,$$

and finally, by duality, a homomorphism

$$(\mathrm{Pic}^0_C)^\vee \to (\mathrm{Pic}^0_A)^\vee.$$

Now our discussion of dual abelian varieties (section 6) implies that $(\mathrm{Pic}^0_A)^\vee \cong (A^\vee)^\vee \cong A$, so all in all from a map of pointed varieties $(C, P) \to (A, 0_A)$ we have constructed a homomorphism $(\mathrm{Pic}^0_C)^\vee \to (\mathrm{Pic}^0_A)^\vee \cong A$. One can then show that the composition

$$C \to (\mathrm{Pic}^0_C)^\vee \to A$$

is the original map we started with.

EXAMPLE 9.20 (An elliptic curve is its own Jacobian). Let E/K be an elliptic curve. We shall show that E is isomorphic to its Jacobian variety by using the classical construction of the group law on an elliptic curve.

We claim that any divisor of degree 0 on E is linearly equivalent to a divisor of the form $P - O$, where O is the origin of the group law on E and P is a point on E. To see this, embed E as a plane cubic in $\mathbb{P}^2$ (with the origin of the group law being the point $[0 : 1 : 0]$). Now any line different from the line at infinity meets E at three points P_1, P_2, P_3 in the affine plane; the divisor of such a line is therefore $P_1 + P_2 + P_3 - 3O$. Now fix two points P, Q lying in the affine part of E (not both on the same vertical line). Then the line through P and Q meets E exactly at a third point R (possibly coincident with P or Q), so the divisor of the rational function corresponding to this line is $P + Q + R - 3O$. It follows that $P + Q \sim 3O - R$. On the other hand, if R and R' lie in the finite plane on the same vertical line, then the line in question is $x - x(R) = 0$, which has zeroes at R, R' and has a double pole at $[0 : 1 : 0]$. It follows that $R + R' \sim 2O$. Combined with $P + Q \sim 3O - R$, this yields $P + Q \sim 3O - R \sim 3O - (2O - R') = O + R'$. On the one hand, this recovers the classical construction of the addition law on elliptic curves; on the other, it gives us an algorithm to transform any divisor of the form $\sum_{i=1}^k P_i$ into one of the form $(k-1)O + Q$. Now consider a general divisor of degree 0, $D = \sum_{i=1}^k P_i - \sum_{j=1}^k Q_j$. We already know how to construct points Q'_j such that $Q_j + Q'_j \sim 2O$, so D is linearly equivalent to $\sum_{i=1}^k P_i + \sum_{j=1}^k (Q'_j - 2O)$; applying our reduction algorithm to $\sum_{i=1}^k P_i + \sum_{j=1}^k Q'_j$, we find that it is linearly equivalent to a divisor of the form $R + (2k-1)O$, where R is a single point on E. Putting everything together, we obtain as desired

$$D \sim R + (2k-1)O - 2kO = R - O.$$

It follows in particular that the map $E \to \mathrm{Pic}^0(E)$ given by $P \mapsto [P - O]$ is surjective, and it's not hard to see that it is injective (if $P - O$ were a principal divisor, $P - O = \mathrm{div}(f)$, then $f : E \to \mathbb{P}^1$ would be a map of degree 1, hence an isomorphism, which is impossible since E has genus 1 while $\mathbb{P}^1$ has genus 0).

REMARK 9.21. I find it very useful to think of the Jacobian of a curve C as *the abelian variety whose regular differentials are the same as those of* C. More precisely, let $i : C \hookrightarrow J$ be the embedding induced by the fixed rational point on C. Then there is a canonical pullback map

$$i^* : H^0(J, \Omega^1_J) \to H^0(C, \Omega^1_C),$$

and the defining property of the Jacobian is essentially that this map is an isomorphism.

PROPOSITION 9.22 (Automorphisms of a curve induce automorphisms of its Jacobian). *Let $\alpha : C \to C$ be an automorphism of a nice curve of genus at least 2. Then α induces a nontrivial automorphism $\alpha : \mathrm{Jac}(C) \to \mathrm{Jac}(C)$; in other words,* $\mathrm{Aut}(C)$ *embeds into* $\mathrm{Aut}(\mathrm{Jac}(C))$.

PROOF. The map induced by α on $\mathrm{Jac}(C)$ is not hard to construct using the universal property; here is a concrete description: the divisor class $[D] = [\sum P_i - \sum Q_j]$, of degree 0, is sent to $[\alpha(D)] := [\sum \alpha(P_i) - \sum \alpha(Q_j)]$. This definition is well posed, because if $D = \mathrm{div}(f)$ is principal then $\alpha(D) = \mathrm{div}(f \circ \alpha)$ is again principal.

Now we show that nontrivial automorphisms of C induce nontrivial automorphisms of $\mathrm{Jac}(C)$. Let Q be a point such that $\alpha(Q) \neq Q, P$ and suppose that $\alpha(i(Q)) = i(Q)$, that is, $[\alpha(Q) - \alpha(P)] = [Q - P]$. Then $D := \alpha(Q) - \alpha(P) + P - Q$ is principal, so it is the divisor of a function $f : C \to \mathbb{P}^1$ of degree 2; by definition, this is only possible if C is hyperelliptic. So if C is not hyperelliptic we are done; if instead C *is* hyperelliptic we distinguish three cases:

(1) C is hyperelliptic and $\alpha(P) = P$. Then $[\alpha(Q) - \alpha(P)] = [Q - P]$ implies $[\alpha(Q) - Q] = 0$, which means that $\alpha(Q) - Q$ is the divisor of a function $f_Q : C \to \mathbb{P}^1$ of degree 1, contradiction.
(2) C is hyperelliptic, $\alpha(P) \neq P$, and there is a 2-to-1 function $x : C \to \mathbb{P}^1$ such that $x(P) = 0$ and $x(\alpha(P)) = \infty$. If α induces the identity on the Jacobian, then for every Q (with at most finitely many exceptions) we have that $\alpha(Q) - \alpha(P) + P - Q$ is the divisor of a function f_Q of degree 2 to $\mathbb{P}^1$. We recall that every hyperelliptic curve of genus at least 2 is hyperelliptic in a unique way; hence f_Q is a rational function of $x : C \to \mathbb{P}^1$, and we may write $f_Q = \frac{a_Q x + b_Q}{c_Q x + d_Q}$ for some constants a_Q, b_Q, c_Q, d_Q. Since $f_Q(P) = 0 = \frac{b_Q}{d_Q}$ we obtain $b_Q = 0$, and since $f_Q(\alpha(P)) = \infty$ we obtain $c_Q = 0$. It follows that $\mathrm{div}(f_Q)$ is independent of Q, but this contradicts the fact that $\mathrm{div}(f_Q) = \alpha(Q) - Q + P - \alpha(P)$.
(3) C is hyperelliptic, $\alpha(P) \neq P$, and for all 2-to-1 functions $x : C \to \mathbb{P}^1$ we have $x(P) = x(\alpha(P))$. This immediately leads to a contradiction, because the functions f_Q (defined as above) are 2-to-1 and take different values at $P, \alpha(P)$.

□

9.2. Jacobians vs general abelian varieties. In the limited scope of the present course there isn't nearly enough time to properly discuss moduli spaces, so we only make a few remarks that might be useful to get a feeling for the general theory. In dimension $g = 1$, all genus 1 curves with a marked point are elliptic curves; they are all principally polarised (we proved this for elliptic curves over $\mathbb{C}$ in example 4.12, but the same holds over any field) and isomorphic to their Jacobian (example 9.20). Hence in dimension 1 the notions of abelian variety, principally polarised abelian variety and Jacobian are all the same.

Starting with dimension 2 there are non-principally polarised abelian varieties, but any principally polarised abelian variety is a Jacobian (or the product of two elliptic curves

with the product polarisation). Furthermore, it's not hard to prove that every genus 2 curve is hyperelliptic, so we have

$$\left\{ \begin{array}{c} \text{Jacobians of genus 2} \\ \text{hyperelliptic curves} \end{array} \right\} = \{\text{genus 2 Jacobians}\}$$
$$\simeq \left\{ \begin{array}{c} \text{principally polarised} \\ \text{abelian surfaces} \end{array} \right\} \subsetneq \{\text{abelian surfaces}\}.$$

In dimension 3 one has

$$\left\{ \begin{array}{c} \text{Jacobians of genus 3} \\ \text{hyperelliptic curves} \end{array} \right\} \subsetneq \{\text{genus 3 Jacobians}\}$$
$$\simeq \left\{ \begin{array}{c} \text{principally polarised} \\ \text{abelian threefolds} \end{array} \right\} \subsetneq \{\text{abelian threefolds}\},$$

where as before $\simeq$ denotes equality up to the (very thin) subset of principally polarised abelian varieties that are *isomorphic* (and not just *isogenous*) to products of PPAVs of smaller dimension. Finally, from dimension 4 onward, all 4 sets are genuinely distinct. In a suitable sense, which we cannot make precise here, when considering abelian varieties of dimension g the situation is the following:

(1) the moduli space of hyperelliptic curves of genus g has dimension $2g-1$;
(2) the moduli space of curves of genus g (hence of Jacobians, considered together with their principal polarisation[9]) has dimension $3g-3$;
(3) the moduli space of principally polarised abelian varieties of dimension g has dimension $\frac{g(g+1)}{2}$;
(4) there exists a (countably) infinite number of different types of polarisations; recall however that over an algebraically closed field any abelian variety is isogenous to a principally polarised one (theorem 6.8).

It is quite clear from the previous list that Jacobians become more and more sparse in the space of all the PPAVs of a given dimension; however, Jacobians are still very interesting to study, for many reasons, including the following perhaps surprising result which unfortunately we won't have the time to prove (the interested reader can find a proof in [**Mil12**, Theorem 10.1]):

THEOREM 9.23. *Let K be a field. Every abelian variety A/K is the quotient of some Jacobian.*

REMARK 9.24. Notice that in general the dimension of the Jacobian in question will be much larger than that of A.

SKETCH OF PROOF. We may assume $\dim A > 1$. By embedding A in some projective space $\mathbb{P}^N$ and applying Bertini's theorem[10] sufficiently many times, we find a smooth irreducible curve C given by the intersection of A with a linear subspace of $\mathbb{P}^N$. This

[9] it is a theorem of Torelli that one can recover a curve from its polarised Jacobian

[10] this argument, as stated, requires the ground field to be infinite; the result, however, is true over any field

induces a map $J(C) \to A$, which we want to show to be surjective. If it is not, then let A_1 be the image of $J(C)$ in A and let A_2 be a complement. By pulling back C along the map

$$\pi : A_1 \times A_2 \xrightarrow{1\times n} A_1 \times A_2 \xrightarrow{+} A$$

we obtain a curve $\pi^*(C)$ which is not connected (because its projection to C_2 is a finite number of points, and not a single point provided that $n > 1$). This can be shown to be a contradiction. □

9.3. Example: adding points on a Jacobian. We take the curve of this example from [**CF96**]. Consider the curve

$$C : y^2 = x(x-1)(x-2)(x-5)(x-6);$$

C has a single point at infinity, which we denote by ∞; we embed C into $\mathrm{Jac}(C)$ by sending ∞ to $[0] \in \mathrm{Jac}(C)(\mathbb{Q})$.

We now define divisor classes (of degree 0)

$$A = [(0,0) + (1,0) - 2\infty] \quad \text{and} \quad B = [(2,0) + (3,6) - 2\infty]$$

on the Jacobian of C. We show some manipulations involving the points A and B on the Jacobian; in particular, we want to determine a divisor $D_1 + D_2 - 2\infty$ on C that represents the same divisor class as $A + B$.

We first find a function vanishing at all the points in the support of A and B: for example, $f : y - x(x-1)(x-2)$ works. Substituting this into the equation for C we find $x(x-1)(x-2)(x-3)(x^2-x+10) = 0$. Thus the divisor of the function f is

$$(0,0) + (1,0) + (2,0) + (3,6) + C_1 + C_2 - 6\infty = A + B + C_1 + C_2 - 2\infty,$$

where

$$C_1 = \left(\frac{1}{2} + \frac{1}{2}\sqrt{-39}, 15 - 5\sqrt{-39}\right), \quad C_2 = \left(\frac{1}{2} - \frac{1}{2}\sqrt{-39}, 15 + 5\sqrt{-39}\right).$$

Since $[\mathrm{div}\, f] = [0]$ in $\mathrm{Jac}(C)$, we have thus proven

$$[A + B] = [A + B - \mathrm{div}\, f] = [2\infty - C_1 - C_2].$$

Suppose we want to find a representative of the form $[D_1 + D_2 - 2\infty]$: then we need to find a function with divisor $C_1 + C_2 + D_1 + D_2 - 4\infty$. But we already know such a function! Indeed, C_1, C_2 are zeroes of $x^2 - x + 10$ which, being of degree 4 and regular on the affine chart of our curve, satisfies exactly

$$\mathrm{div}(x^2 - x + 10) = C_1 + C_2 + D_1 + D_2 - 4\infty$$

with

$$D_1 = \left(\frac{1}{2} + \frac{1}{2}\sqrt{-39}, -15 + 5\sqrt{-39}\right), \quad D_2 = \left(\frac{1}{2} - \frac{1}{2}\sqrt{-39}, -15 - 5\sqrt{-39}\right).$$

Hence $A+B = [D_1+D_2-2\infty]$ on $\mathrm{Jac}(C)$; notice that once we find $A+B = [2\infty-C_1-C_2]$ we also obtain the same conclusion by observing that the hyperelliptic involution induces

$-\mathrm{id}$ on the Jacobian (exercise 1.9), which means that (denoting by $\overline{P}$ the point $(x,-y)$ when $P=(x,y)$) we have

$$\iota(\overline{P}) = -\iota(P) \Leftrightarrow [\overline{P} - \infty] = [\infty - P].$$

Applying this in our particular example we obtain

$$A + B = [2\infty - C_1 - C_2] = [-2\infty + \overline{C_1} + \overline{C_2}] = [D_1 + D_2 - 2\infty].$$

10. Torsion points, the Tate module

In this course we are mainly interested in the *torsion points* of abelian varieties. Recall the definition of the group of n-torsion points of an abelian variety:

Definition 10.1 (See definition 5.12). *Let A be an abelian variety over the field K and let n be a positive integer. We define $A[n]$ to be the kernel of $[n] : A(\overline{K}) \to A(\overline{K})$. We call $A[n]$ the **group of n-torsion points of** A.*

Remark 10.2. The more scheme-theoretically minded reader will notice that $A[n]$ can in fact be defined as a group scheme over K: indeed $[n] : A \to A$ is an isogeny defined over K, hence its kernel is a subgroup scheme of A defined over K. This point of view leads to more natural (or at least more intrinsic) definitions, but we shall not pursue it further here. It is however very fruitful from an arithmetic point of view to try and understand the scheme $A[n]$ when A is defined over a more general base scheme than simply a field.

Theorem 10.3. *Let K be a field of characteristic zero and A/K be a g-dimensional abelian variety. Then $A[n]$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g}$ as an abstract group.*

We give a quick and dirty argument; for a more conceptual one, see the proof of theorem 10.5 below.

Proof. All we care about (equations defining the abelian variety, the multiplication map, the inverse, etc) are defined over a finitely generated extension of $\mathbb{Q}$. Any such extension can be embedded in $\mathbb{C}$, hence it is enough to consider the case $K = \mathbb{C}$, which we saw in Proposition 4.5. □

Remark 10.4. The reduction to the case $K = \mathbb{C}$ in the above proof is often quoted as the *Lefschetz principle*: quoting from Wikipedia, *true statements of the first order theory of fields about $\mathbb{C}$ are true for any algebraically closed field K of characteristic zero.*

More generally, one has

Theorem 10.5. *Let K be a field and A/K be a g-dimensional abelian variety. Let n be an integer which is prime to the characteristic of K: then $A[n]$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g}$ as an abstract group.*

Proof. For any divisor n' of n, the isogeny $[n']$ is finite, étale[11], and of degree $(n')^{2g}$. Hence $\ker[n']$ consists of $(n')^{2g}$ distinct geometric points (it is an étale group scheme of

[11] since $(n, \mathrm{char}(K)) = 1$ by assumption

rank $(n')^{2g}$); since this holds for every divisor n' of n, the only possible group structure for $A[n]$ is $(\mathbb{Z}/n\mathbb{Z})^{2g}$. □

EXAMPLE 10.6. Theorem 10.3 is very much **false** in positive characteristic. For example, if $E/\mathbb{F}_p$ is an elliptic curve, then $E[p]$ can never have order p^2: the group $E[p]$ can either be trivial, in which case we say that E is **supersingular**, or it can have order p, in which case we say that E is **ordinary**.

The reason of the failure of $E[p]$ to have order p^2 is to be found in the fact that $[p]$ can be written as $\mathrm{Ver} \circ \mathrm{Frob}$, where the Frobenius morphism Frob is purely inseparable of degree p (more generally, for a g-dimensional abelian variety one has $[p] = \mathrm{Ver} \circ \mathrm{Frob}$ with Frob purely inseparable of degree p^g).

Here Ver is the Verschiebung operator, defined as follows: let G be a finite commutative group scheme over a field of characteristic p. Then we have a Cartier dual G^*, with an associated Frobenius morphism $\mathrm{Frob}_{G^*} G^* \to (G^*)^{(p)} = (G^p)^*$. Verschiebung is the dual of Frob_{G^*}, so it is a group scheme homomorphism from G^p to G.

DEFINITION 10.7 (Tate module). *Let A/K be an abelian variety and let ℓ be a prime number different from* $\mathrm{char}(K)$. *The* ***ℓ-adic Tate module of*** *A is*

$$T_\ell(A) = \varprojlim_{n \to \infty} A[\ell^n],$$

where the transition morphisms are given by multiplication by ℓ.

REMARK 10.8. Concretely, an element of $T_\ell(A)$ is an infinite sequence $\{a_0, a_1, a_2, \ldots\}$ of torsion points of A such that

(1) $a_i \in A[\ell^i]$ for all $i \geq 0$;
(2) $\ell a_{i+1} = a_i$ for all $i \geq 0$.

REMARK 10.9. We have already seen that $A[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$ (the isomorphism is not canonical, however); by passing to the limit in n we obtain that there is a (non-canonical) isomorphism $T_\ell(A) \cong \mathbb{Z}_\ell^{2g}$.

DEFINITION 10.10. *It is sometimes useful to consider the* ***adelic Tate module****: by definition, it is the projective limit of the system of n torsion points along the transition maps given by $A[km] \xrightarrow{[k]} A[m]$. We have*

$$\hat{T}(A) = \varprojlim_{n:(n,\mathrm{char}(K))=1} A[n] = \prod_{\substack{\ell \text{ prime} \\ \ell \neq \mathrm{char}(K)}} T_\ell(A)$$

Another useful variant of the Tate module is the so-called ***rational Tate module*** $V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

REMARK 10.11. As a consequence of theorem 6.17 part (1) one sees immediately that passing to the limit over those n of the form ℓ^k we may construct a perfect bilinear Weil pairing

$$\langle \cdot, \cdot \rangle_\ell : T_\ell(A) \times T_\ell(A^\vee) \to \varprojlim_n \mu_n = \mathbb{Z}_\ell(1).$$

By composing with an isogeny corresponding to a polarisation $\mathcal{L}$ we also obtain a skew-symmetric pairing

$$\langle \cdot, \cdot \rangle_{\ell,\mathcal{L}} : T_\ell(A) \times T_\ell(A) \to \mathbb{Z}_\ell(1)$$

which is a non-degenerate bilinear form on $V_\ell(A)$.

COROLLARY 10.12. *The Rosati map satisfies* $(\varphi)^{\dagger\dagger} = \varphi$.

PROOF. Let φ be an endomorphism of A and fix a prime ℓ which does not divide the degree of φ. We have

$$\langle \varphi(P), Q \rangle_{\ell,\mathcal{L}} = \langle \varphi(P), \lambda_{\mathcal{L}}(Q) \rangle_\ell = \langle P, \varphi^\vee \circ \lambda_{\mathcal{L}}(Q) \rangle_\ell = \langle P, \varphi^\dagger(Q) \rangle_{\ell,\mathcal{L}}.$$

It follows that $\varphi \mapsto \varphi^\dagger$ is the adjunction map for the non-degenerate bilinear form $\langle \cdot, \cdot \rangle_{\ell,\mathcal{L}}$, hence it is involutive. □

CHAPTER 2

Galois representations

The purpose of this lecture is to (re)describe the family of compatible Galois representation attached to an abelian variety over a number field and to provide the reader with a bag of tricks that might be useful in determining properties of these Galois representations.

1. The Galois representation

It is customary to study Galois representations *one prime at a time*: while this is not strictly necessary, it often makes matters easier. For this reason, in what follows we shall fix a prime ℓ and only consider modulo-ℓ and ℓ-adic representations. From now on, A is a fixed abelian variety over a field K (which will usually be either a number field or a finite field).

The crucial remark is that the coordinates of the points in the finite set $A[\ell^n]$ are algebraic, so that there is a natural action of the absolute Galois group $\mathrm{Gal}\left(\overline{K}/K\right)$ on the points of $A[\ell^n]$. It is clear that when Galois acts on a point in $A(\overline{K})$ we get a new point in $A(\overline{K})$, and that the fixed points of this action are precisely the K-points of A (in particular, 0_A is fixed under the Galois action).

More precisely, we notice that Galois also acts on the finite set $A[\ell^n]$. Since the equations that define A and the group law have coefficients in K, one sees easily that

$$[n]\sigma(P) = \sigma([n]P)$$

for all $\sigma \in \mathrm{Gal}\left(\overline{K}/K\right)$, $P \in A(\overline{K})$ and $n \in \mathbb{Z}$. In particular, if P is a n-torsion point, then so is $[n]P$: it follows that $\mathrm{Gal}\left(\overline{K}/K\right)$ acts on $A[\ell^n]$. Moreover, since $\sigma(P+Q) = \sigma(P)+\sigma(Q)$, the Galois action is compatible with the obvious structure of $\mathbb{Z}/\ell^n\mathbb{Z}$-module of $A[\ell^n]$. Combining the previous remarks, we see that the following definition is well-posed:

Definition 1.1 (Galois representation attached to A). *Let A/K be an abelian variety over a field, let ℓ be a prime number*[1]*, and let n be a positive integer. There is a natural action of* $\mathrm{Gal}\left(\overline{K}/K\right)$ *on $A[\ell^n]$, or, which is the same, a natural representation*

$$\rho_{\ell^n} : \mathrm{Gal}\left(\overline{K}/K\right) \to \mathrm{Aut}_{\mathbb{Z}/\ell^n\mathbb{Z}}\left(A[\ell^n]\right).$$

Remark 1.2. The representations ρ_{ℓ^n} are continuous: this amounts to saying that they factor through a finite quotient of $\mathrm{Gal}\left(\overline{K}/K\right)$, and this is clear, because ρ_{ℓ^n} becomes trivial upon extending the base field to $K(A[\ell^n])$, the field obtained from K by adjoining the coordinates of all the ℓ^n torsion points. Notice that – since there are only finitely many

[1] in all our applications, ℓ will be different from the characteristic of K

torsion points and each of them has algebraic coordinates – the field $K(A[\ell^n])$ is a finite extension of K.

REMARK 1.3. Understanding the representations ρ_{ℓ^n} can be quite complicated when ℓ is equal to the characteristic p of K: we shall steer clear of these difficulties and focus on the case $\ell \neq p$.

The general problem we would like to solve is that of describing (as precisely and as concretely as possible) the image of the Galois representations ρ_{ℓ^n}. In order to dispense with the dependence on n, it is often useful to pass to the limit $n \to \infty$ and work with the so-called **ℓ-adic representation**

$$\rho_{\ell^\infty} : \mathrm{Gal}\left(\overline{K}/K\right) \to \mathrm{Aut}(T_\ell A).$$

This representation is again continuous and will be our main object of study. We shall use the informal term **image of Galois** to refer to either the groups

$$G_{\ell^n} := \rho_\ell(\mathrm{Gal}\left(\overline{K}/K\right)) \subseteq \mathrm{Aut}(A[\ell^m])$$

or their ℓ-adic counterpart,

$$G_{\ell^\infty} := \rho_{\ell^\infty}(\mathrm{Gal}\left(\overline{K}/K\right)) \subseteq \mathrm{Aut}(T_\ell(A)).$$

These groups do of course depend on ℓ but – in a sense that will be made precise later – they are conjectured to be *very similar* to each other.

NOTATION 1.4. *Let A/K be an abelian variety of dimension g and let $\ell \neq \mathrm{char}(K)$ be a prime number. We fix once and for all $\mathbb{Z}_\ell$-basis of $T_\ell(A)$ (recall from remark 10.9 that $T_\ell(A)$ is free of rank $2g$ over $\mathbb{Z}_\ell$); upon reduction modulo ℓ, this basis also induces a $\mathbb{F}_\ell$-basis of the $2g$-dimensional vector space $A[\ell]$. With this choice, the groups G_ℓ and G_{ℓ^∞} can respectively be identified with subgroups of $\mathrm{GL}_{2g}(\mathbb{F}_\ell)$ and $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$; in what follows we shall make this identification without further comment.*

2. Algebraic cycles constrain the action of Galois

A guiding principle in the study of Galois representation is that

if the image of Galois is small, there must be a good reason!

We now try to explain what this principle means in practice. Recall that an **algebraic cycle** is, roughly speaking, a formal linear combination of (irreducible reduced closed) subvarieties.

2.1. Weil pairing: the image of Galois is contained in GSp. Let A be principally polarised, so that we may identify A with $A^\vee$. The ℓ-adic Weil pairing

$$\langle \cdot, \cdot \rangle_\ell : T_\ell A \times T_\ell A \to \mathbb{Z}_\ell(A)$$

is Galois-equivariant, that is, for all $\sigma \in \mathrm{Gal}\left(\overline{K}/K\right)$ and for all $t_1, t_2 \in T_\ell(A)$ we have

$$\langle \sigma(t_1), \sigma(t_2) \rangle_\ell = \sigma(\langle t_1, t_2 \rangle_\ell).$$

This means in particular that G_{ℓ^∞} (respectively G_ℓ) is contained in the subgroup of $\mathrm{Aut}(T_\ell(A))$ (resp. of $\mathrm{Aut}(A[\ell])$) consisting of those automorphisms M that satisfy

$$\langle Mv, Mw\rangle_\ell = \lambda(M)\langle v, w\rangle_\ell,$$

for some $\lambda(M) \in \mathbb{Z}_\ell^\times$ (respectively $\mathbb{F}_\ell^\times$). This group deserves a name:

Definition 2.1 (General symplectic group). *Let $(V, \langle\cdot,\cdot\rangle)$ be a finite-rank free module over the ring R endowed with a skew-symmetric bilinear form $\langle\cdot,\cdot\rangle$. The **general symplectic group** of $(V, \langle\cdot,\cdot\rangle)$ is the subgroup of $\mathrm{GL}(V)$ given by*

$$\mathrm{GSp}(V, \langle\cdot,\cdot\rangle) = \{M \in \mathrm{GL}(V) \mid \exists \lambda(M) \in R^\times : \langle Mv, Mw\rangle = \lambda(M)\langle v, w\rangle \ \forall v, w \in V\}$$

*The map $M \mapsto \lambda(M)$ is a homomorphism from $\mathrm{GSp}(V, \langle\cdot,\cdot\rangle)$ to $R^\times$; its kernel is by definition the **symplectic group** of $(V, \langle\cdot,\cdot\rangle)$. By abuse of notation we will usually denote $\mathrm{GSp}(V, \langle\cdot,\cdot\rangle)$ by $\mathrm{GSp}(V)$.*

Remark 2.2. Given our implicit choice of basis of $T_\ell(A)$ we shall usually consider G_{ℓ^∞} as being a subgroup of $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$.

Example 2.3 (Elliptic curves). As with other higher-dimensional phenomena, the fact that G_{ℓ^∞} is contained in $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ rather than just $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$ is not easy to notice when $g = 1$. Indeed, it is immediate to check that for $V = \mathbb{Z}_\ell^2$ equipped the standard symplectic form $\langle \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \rangle = x_1y_2 - y_1x_2$ one has $\mathrm{GSp}_2(V) = \mathrm{GL}_2(V)$: in the case of elliptic curves the existence of the Weil pairing does not impose any restriction on the image of Galois.

Remark 2.4. This restriction on the image of Galois should be though of as being an avatar of the existence of a polarisation, which in turn is an algebraic cycle on $A \times A^\vee$. Indeed, let $\Gamma \subset A \times A^\vee$ be the graph of the principal polarisation $\lambda_\mathcal{L}$. Since $\lambda_\mathcal{L}$ is a homomorphism of abelian varieties we have $\lambda_\mathcal{L}(A[\ell^n]) \subseteq A^\vee[\ell^n]$, and when we consider the action of $\sigma \in \mathrm{Gal}\left(\overline{K}/K\right)$ on $P \in A[\ell^n]$ we obtain

$$\sigma(P, \lambda_\mathcal{L}(P)) \in \sigma(\Gamma) = \Gamma,$$

so that $(\sigma(P), \sigma(\lambda_\mathcal{L}(P))$ is again a point of Γ. This imposes a nontrivial restriction on the action of σ, which manifests itself in the containment $G_{\ell^\infty} \subseteq \mathrm{GSp}(T_\ell(A))$.

Remark 2.5. We notice that we have the useful formula

$$\lambda(\rho_{\ell^\infty}(\sigma)) = \chi_\ell(\sigma),$$

where λ is the multiplier $\mathrm{GSp}(T_\ell(A)) \to \mathbb{Z}_\ell^\times$ and χ_ℓ is the cyclotomic character. This is true essentially by definition: indeed we know that

$$\langle \rho_{\ell^\infty}(\sigma)(P), \rho_{\ell^\infty}(\sigma)(Q)\rangle_\ell = \rho_{\ell^\infty}(\sigma)\left(\langle P, Q\rangle_\ell\right),$$

and on the other hand the action of Galois on the root of unity $\langle P, Q\rangle_\ell$ is by definition the cyclotomic character. It is also useful to notice that (in full generality) we have an equality between the group homomorphisms $\mathrm{GSp}_{2g}(V) \to R^\times$ given by λ^g and by det.

REMARK 2.6. It is interesting to understand what happens if A carries no principal polarisation: see exercise 1.10.

2.2. Endomorphisms. By the same reasoning as in remark 2.4, one sees that the existence of nontrivial K-endomorphisms of A automatically leads to restrictions for the image of Galois: indeed, if $\varphi : A \to A$ is an endomorphism of A defined over K, for any torsion point $P \in A[\ell^n]$ and for every $\sigma \in \mathrm{Gal}\left(\overline{K}/K\right)$ we have

$$\sigma(\varphi(P)) = \varphi(\sigma(P)),$$

an equality which should be interpreted as saying that the knowledge of the action of $\sigma(P)$ is enough to determine the action of σ on $\varphi(P)$. Clearly this is (in general) a nontrivial restriction on the possible automorphisms of $T_\ell(A)$ which can lie in the image of Galois.

REMARK 2.7. This discussion applies in particular to the endomorphisms $[n]$ of A, but all that can be deduced from the existence of these endomorphisms is the fact that σ acts $\mathbb{Z}_\ell$-linearly on $T_\ell(A)$; this fact is already subsumed by our very notation, since we are considering the image of Galois as a subgroup of $\mathrm{GL}(T_\ell(A))$.

REMARK 2.8. As in remark 2.4, the restrictions on the image of Galois coming from the existence of nontrivial endomorphisms can be interpreted as the existence of suitable algebraic cycles, namely the graph of the endomorphism itself in $A \times A$.

A special case is that of *decomposable* abelian varieties: if A is isomorphic to $B \times C$, then $T_\ell(A)$ decomposes as $T_\ell(B) \oplus T_\ell(C)$, and the image of Galois will – in a suitable basis – act through block-diagonal matrices. If A is only isogenous to a product $B \times C$ the same is true after tensoring with $\mathbb{Q}_\ell$: more precisely, while it is not true in general[2] that $T_\ell(A) \cong T_\ell(B) \oplus T_\ell(C)$, it *is* true that $V_\ell(A) \cong V_\ell(B) \oplus V_\ell(C)$ (recall that $V_\ell(A)$ is the rational Tate module $T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$); this means that the action of Galois may be put in block-diagonal form after a change of basis that may involve denominators.

REMARK 2.9. Notice that if A is isogenous to a product $B \times C$ then A cannot be simple, and in particular it admits nontrivial endomorphisms. Indeed we have the following maps at our disposal:

(1) an isogeny $A \to B \times C$, by assumption;
(2) isogenies $A \to A^\vee$, $A^\vee \to A$, $B \to B^\vee$, by remark 6.7.
(3) an isogeny $B^\vee \times C^\vee \to A^\vee$, by duality

We then obtain a homomorphism

$$A \to B \times C \xrightarrow{\pi_1} B \to B^\vee \xrightarrow{\iota_1} B^\vee \times C^\vee \to A^\vee \to A$$

whose image is easily seen to have dimension equal to $\dim(B) \neq 0, \dim A$ (hence in particular this endomorphism cannot be of the form $[n]$).

[2]the problematic ℓ are those that divide the degree of the isogeny

2.3. 0-dimensional cycles: torsion points and isogenies. Suppose that $A(K)_{\text{tors}}$ is nontrivial, and let $P \in A(K)_{\text{tors}}$ be a point of order ℓ^k. Then we have $\sigma(P) = P$, that is, the group G_{ℓ^n} is contained in the group of automorphisms of $A[\ell^n]$ that fix P.

More generally, if there is a nontrivial isogeny $f : A \to A'$ of degree N defined over K, then $\ker f$ is a Galois-stable subgroup of $A[N]$. If $\ell^n \mid N$, this implies in particular that G_{ℓ^n} stabilises a $\mathbb{Z}/\ell^n\mathbb{Z}$-free submodule of rank 1 in $A[\ell^n]$, thus imposing another restriction on G_{ℓ^n}.

2.4. Tate's conjecture. Given its extreme importance we take a moment to state Tate's conjecture on homomorphisms (now a theorem of Faltings [**Fal83**] for number fields; Tate himself proved in [**Tat66**] the version for finite fields):

THEOREM 2.10 (Faltings, Tate). *Let A, B be abelian varieties defined over a common field K (either a number field or a finite field). There is a natural isomorphism*

$$\mathrm{Hom}_K(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \cong \mathrm{Hom}_{\mathrm{Gal}\left(\overline{K}/K\right)}(V_\ell(A), V_\ell(B)),$$

where $\mathrm{Hom}_{\mathrm{Gal}\left(\overline{K}/K\right)}(V_\ell(A), V_\ell(B))$ denotes the group of $\mathbb{Q}_\ell$-linear homomorphisms

$$g : V_\ell(A) \to V_\ell(B)$$

that satisfy

$$\sigma(g(v)) = g(\sigma(v)) \quad \forall v \in V_\ell(A), \forall \sigma \in \mathrm{Gal}\left(\overline{K}/K\right).$$

REMARK 2.11. Thanks to the work of many people over the years (with particularly important contributions by Zarhin), Tate's conjecture is now a theorem over any field finitely generated over its prime field.

REMARK 2.12. This is an incredibly powerful result: it reduces the problem of studying maps between abelian varieties (which might seem to be highly non-linear objects) to that of understanding certain *linear* objects. It is not unreasonable to consider this theorem as a sophisticated version of analytic uniformisation: over $\mathbb{C}$ we have a vector space, namely $H_1(A(\mathbb{C}), \mathbb{C})$, containing a lattice, namely $H_1(A(\mathbb{C}), \mathbb{Z})$, and maps between abelian varieties can be described as linear maps between $\mathbb{C}$-vector spaces that behave in a certain way with respect to the respective lattices. Here the lattice $H_1(A(\mathbb{C}), \mathbb{Z})$ is replaced by the $\mathbb{Z}_\ell$-lattice $T_\ell(A)$, the ambient vector space by $V_\ell(A)$, and the action of Galois ensures that the maps in question are defined over the correct ground field.

When K is a finite field, $\mathrm{Gal}\left(\overline{K}/K\right)$ is (pro)cyclic, generated by Frobenius, so the Galois action on $V_\ell(A), V_\ell(B))$ is completely determined from the characteristic polynomial of Frobenius (see definition 5.5). This leads to the following

THEOREM 2.13 (Tate). *Let A, B be abelian varieties over a finite field K. Let $p_A(t)$, $p_B(t)$ be the corresponding characteristic polynomials of Frobenius. Given any extension L of $\mathbb{Q}$, write $p_A(t) = \prod_f f(t)^{a_f}$ and $p_B(t) = \prod_f f(t)^{b_f}$ for the factorisation of $p_A(t), p_B(t)$ in $L[t]$. Define*

$$r(p_A, p_B) = \sum_f \deg(f) a_f b_f.$$

Then:

(1) $r(p_A, p_B)$ *is independent of* L*;*
(2) $\operatorname{rank} \operatorname{Hom}_{\operatorname{Gal}\left(\overline{K}/K\right)}(A, B) = r(p_A, p_B)$.

Combining this fact with Honda-Tate theory [**Wat69**] [**WM71**] one obtains:

THEOREM 2.14. *Let* A *be a non-zero abelian variety defined over* $\mathbb{F}_p$ *where* p *is a prime. Assume that* $p_A(t)$ *is not divisible by* $t^2 - p$*. If* $p_A(x) = \prod_{i=1}^{s} Q_i(t)^{m_i}$*, where the* $Q_i(t)$ *are distinct monic irreducible polynomials in* $\mathbb{Z}[t]$*, then* A *is isogenous to* $\prod_{i=1}^{s} A_i^{m_i}$*, where* A_i *is a simple abelian variety over* $\mathbb{F}_p$ *satisfying* $p_{A_i}(t) = Q_i(t)$*.*

Finally, theorem 2.13 (applied to $B = A$) gives:

THEOREM 2.15. *Let* K *be a finite field and assume that* A/K *is a simple* K*-abelian variety of dimension* g*. Then*

$$\operatorname{rank} \operatorname{End}_K(A) = \deg(p_A) = 2g.$$

In this case, since the Frobenius of K *induces an automorphism of* K *with characteristic polynomial* $p_A(t)$*, we see that* $\operatorname{End}_K(A) \otimes \mathbb{Q} \cong \frac{\mathbb{Q}[t]}{(p_A(t))}$*; this is a CM field of degree* $2g$*.*

3. The Mumford-Tate conjecture and independence of ℓ

I feel compelled to at least mention the Mumford-Tate conjecture, and this sounds like the appropriate moment to do so. Roughly speaking, the Mumford-Tate conjecture asserts that *all* the restrictions on G_{ℓ^∞} should come from algebraic cycles; its precise form is a little complicated to state, so I will limit myself to giving the following very vague version:

CONJECTURE 3.1 (Mumford-Tate-Serre). *Let* A *be an abelian variety over a number field* K*. There is an algebraic subgroup* $\operatorname{MT}(A)$ *of* $\operatorname{GL}_{2g,\mathbb{Q}}$*, defined over* $\mathbb{Q}$*, with the following properties:*

(1) $\operatorname{MT}(A)$ *depends only on the geometry of* A*, that is, it only depends on* $A(\mathbb{C})$ *(for any embedding* $K \hookrightarrow \mathbb{C}$*);*
(2) *there is a finite extension of* K *such that the following hold:*
   (a) *seeing* $\operatorname{GL}(T_\ell(A)) \cong \operatorname{GL}_{2g}(\mathbb{Z}_\ell)$ *inside* $\operatorname{GL}_{2g}(\mathbb{Q}_\ell)$*, the group* $\rho_{\ell^\infty}(\operatorname{Gal}\left(\overline{K'}/K'\right))$ *is contained in* $\operatorname{MT}(A)(\mathbb{Q}_\ell)$
   (b) $\rho_{\ell^\infty}(\operatorname{Gal}\left(\overline{K'}/K'\right))$ *is open (for the* ℓ*-adic topology) inside* $\operatorname{MT}(A)(\mathbb{Q}_\ell)$*.*

REMARK 3.2. Even though the full conjecture remains open, various parts of it (and several special cases) have been proven: there is a precise description of the group $\operatorname{MT}(A)$ (which does indeed depend only on $A(\mathbb{C})$, and which by work of Deligne does not depend on the embedding of K in $\mathbb{C}$); part (2a) has also been proven by Deligne, and for part (2b) one does at least know that $\rho_{\ell^\infty}(\operatorname{Gal}\left(\overline{K'}/K'\right))$ is open (in the ℓ-adic topology) in its Zariski closure. What we don't know is whether this Zariski closure is all of $\operatorname{MT}(A)(\mathbb{Q}_\ell)$!

REMARK 3.3. The Mumford-Tate conjecture gives a precise meaning to the following vague intuitions:

(1) independence of ℓ: indeed, it says that the different G_{ℓ^∞} are all interpolated by a single $\mathbb{Q}$-algebraic group
(2) the image of Galois is as large as it can be, once the obvious restrictions have been taken into account: loosely speaking, all the restrictions on G_{ℓ^∞} should come from algebraic cycles, and $\mathrm{MT}(A)$ is defined so as to capture the existence of all algebraic cycles. Therefore part (2b) of the conjecture says that the image of Galois is – up to some finite index – as large as it can be, given the geometric restrictions encoded by $\mathrm{MT}(A)$.

4. The Good, the Bad, and the Semistable (reduction)

This is a technical section, which will be needed in the following when we'll need to work with Frobenius elements and their characteristic polynomials.

Definition 4.1 (Good and bad reduction). *Let A/K be an abelian variety over a number field and let v be a place of K. Recall that we denote by $\mathcal{O}_{K,v}$ the completion of the ring of integers of K at the place v. We say that A has **good reduction** at v if $A \to \mathrm{Spec}(K)$ extends to an abelian scheme $\mathcal{A}$ over $\mathrm{Spec}(\mathcal{O}_{K,v})$ (whose generic point we identify with $\mathrm{Spec}(K)$), otherwise we say that A has **bad reduction** at v. We say that A has good reduction (without specifying a place v) if it has good reduction at all places of K.*

Notation 4.2. *Let A/K be an abelian variety over a number field, and let v be a place of good reduction for A. We shall simply write $A(\mathbb{F}_v)$ to mean $\mathcal{A}(\mathbb{F}_v)$, where $\mathcal{A} \to \mathrm{Spec}(\mathcal{O}_{K,v})$ is an abelian scheme extending A_{K_v}.*

We shall also need some more technical definitions:

Definition 4.3 (Néron model). *Let A/K be an abelian variety over a number field (or a local field). The **Néron model** of A is a smooth separated but in general not proper group scheme $\mathcal{A} \to \mathrm{Spec}(\mathcal{O}_K)$ with the following property, called the **Néron mapping property**: if X is a smooth separated scheme over $\mathcal{O}_K$ then any K-morphism of the generic fibres $X_K \to A_K$ can be extended to a unique R-morphism from X to $\mathcal{A}$.*

It is a deep theorem (due in its original form to Néron [**Nér64**], and in full generality to Raynaud [**Ray66**]) that (semi)abelian varieties over the fraction field of a Dedekind domain admit a Néron model. Once we have a Néron model we may use it to define the notion of semistable reduction:

Definition 4.4 (Semistable reduction). *Let A/K be an abelian variety with Néron model $\mathcal{A}/\mathcal{O}_K$. We say that A has **semistable reduction** at v if the connected component of the identity of $\mathcal{A} \times_{\mathcal{O}_K} \mathbb{F}_v$ is an extension of an abelian variety by a torus. We say that A has semistable reduction if it does at every place v of K.*

Remark 4.5. In other words, A has semistable reduction at v if the special fiber at v of $\mathcal{A}$ fits into an exact sequence

$$0 \to T \to \mathcal{A}_v^0 \to B \to 0,$$

where T is a torus and B an abelian variety. For A *not* to have semistable reduction essentially means that T (which always exists as a linear algebraic group) has some factors isomorphic to $\mathbb{G}_a$.

For future use we note that one may attach a further numerical invariant to a place of semistable reduction:

DEFINITION 4.6 (Toric rank). *Let A/K have semistable reduction at v. Write*

$$0 \to T \to \mathcal{A}_v^0 \to B \to 0$$

for the canonical exact sequence involving the identity component of the special fiber of $\mathcal{A}$ at v. The ***toric rank*** *of A at v is simply $\dim(T)$; it is equal to 0 precisely when A has good reduction at v.*

Finally, we deal with the change of reduction type induced by an extension of the ground field:

DEFINITION 4.7 (Potentially good/semistable reduction). *Let L/K be a finite extension of fields. We say that A* ***acquires good reduction over*** *L (respectively* ***acquires semistable reduction over*** *L) at v if $A \times_K L$ has good (respectively semistable) reduction at all places of $\mathcal{O}_L$ lying above v.*

Finally, we say that A has ***potentially good*** *(respectively* ***potentially semistable****) reduction at v if there exists some extension L/K such that A acquires good (semistable) reduction at v over L.*

REMARK 4.8. When working with elliptic curves one often uses the term **multiplicative reduction** to refer to what we're calling semistable reduction. In higher dimensions, however, the distinction is important.

The reader familiar with elliptic curves might also want to think about the following possible definition of multiplicative reduction: an elliptic curve has multiplicative reduction at v if and only if the group of the smooth points in the reduction is isomorphic (possibly after a quadratic extension) to $\mathbb{G}_m$.

REMARK 4.9. Good, bad and semistable reduction are really local problems: these definitions could (and in fact *should*) be given in the context of abelian varieties defined over local fields. In that setting, given an abelian variety $A \to \mathrm{Spec}(K)$ where $K = \mathrm{Frac}(R)$ is the field of fractions of a DVR R, we say that A has good reduction if there exists an abelian scheme $\mathcal{A} \to \mathrm{Spec}(R)$ whose generic fiber is A.

The two fundamental theorems one should always have in mind are the following:

THEOREM 4.10 (Finiteness of the set of places of bad reduction). *Let A/K be an abelian variety over a number field. Then A has good reduction at all but finitely many places of K.*

PROOF. Follows from the general principle known as *spreading out*. More specifically, since $A \to \mathrm{Spec}(K)$ is defined over the generic point of $\mathrm{Spec}(\mathcal{O}_K)$, it can be extended (as a variety, not necessarily as an abelian scheme) to some open subset of $\mathrm{Spec}(\mathcal{O}_K)$. The same

holds for the multiplication, inverse, and unit maps; since the intersection of open subsets is open, this implies that we can find a common open subscheme S of $\mathrm{Spec}(\mathcal{O}_K)$ over which A, m, i, and the unit section all extend. Given that the maps satisfy the commutative diagrams that encode the property of being a group *generically*, they also satisfy the same properties over S: this means precisely that there is an abelian scheme $\mathcal{A} \to S$ with generic fibre A. The places of bad reduction of A are then contained in the finite set $\mathrm{Spec}(\mathcal{O}_K) \setminus S$.

In layman's terms, the argument is simply the following: choose any set of equations for A and for the morphisms that give A its group structure. Let T be the set of primes of $\mathcal{O}_K$ that divide the denominator of at least one coefficient of at least one equation of the given presentation (there are only finitely many of them); on $\mathrm{Spec}(\mathcal{O}_K) \setminus T$ the given equations already define an abelian scheme. □

THEOREM 4.11 (Semistable reduction theorem, local case (Grothendieck [**GRR72**])). *Let A/K be an abelian variety over a local field. Then A has potentially semistable reduction.*

COROLLARY 4.12 (Semistable reduction theorem, global case). *Let A be an abelian variety over a number field. Then A has potentially semistable reduction at all the places of K.*

We also quote another result for which, as demonstrated by figure 1, it is not easy to find a good reference:

THEOREM 4.13. *Let A/K be an abelian variety; we consider the reduction properties of A either over R (if $K = \mathrm{Frac}(R)$ is local) or at a fixed place of K (if K is a number field).*

1. *Suppose that A has good reduction. Then A has semistable reduction.*
2. *Suppose that A has good reduction. Then for any field extension L/K the abelian variety A_L also has good reduction (at all the places of L above v, when K is a number field)*
3. *Suppose that A has bad semistable reduction. Then for any field extension L/K the abelian variety A_L has bad semistable reduction (at all the places of L above v, when K is a number field)*

We finish this paragraph by giving some useful information on the reduction type of a Jacobian:

THEOREM 4.14 (Bad reduction of a Jacobian). *Let C/K be a smooth projective geometrically irreducible curve of genus $g \geq 2$. The Jacobian J of C, considered as an abelian variety over K, has good reduction at v whenever C does*[3] *(but the converse implication does not hold: it is possible for J to have good reduction at v even when C has bad reduction there). Moreover, J has semistable reduction at v whenever C admits a semistable model over $\mathcal{O}_{K,v}$, that is, there is a model $\mathcal{C}$ over $\mathcal{O}_{K,v}$ whose special fiber has only ordinary double points as singularities.*

[3] in the obvious sense: C extends to a smooth curve over $\mathrm{Spec}(\mathcal{O}_{K,v})$

FIGURE 1. Good riddance indeed

We also have the following theorem, which is very useful when working with Jacobians:

THEOREM 4.15 ([**BLR90**, Example 8 p. 246]). *Suppose C/K is a curve with semistable reduction at v and let $J = \mathrm{Jac}(C)$. Then J has semistable reduction at v, and its toric rank is equal to the rank of $H^1(X(\mathcal{C}_{\mathbb{F}_v}), \mathbb{Z})$, where $X(\mathcal{C}_{\mathbb{F}_v})$ is the dual graph[4] of the special fibre of a semistable model $\mathcal{C}$ of C.*

EXAMPLE 4.16 (Hyperelliptic curves with toric rank 1). Let $C : y^2 = f(x)$ be a hyperelliptic curve over $\mathbb{Q}$. Suppose that some prime $p \neq 2$ divides the discriminant of $f(x)$ exactly once: then $\mathrm{Jac}(C)$ has bad semistable reduction of toric rank 1 at p. Indeed, the hypothesis implies that the equation $y^2 = f(x)$ gives a semistable model of C over $\mathbb{Z}_p$, with special fibre $y^2 = (x-a)^2 g(x)$, where $g(x)$ has not multiple roots modulo p and $(g(x), x-a) = 1$. This implies that dual graph is a single vertex with a loop (the only irreducible component intersects itself), so that the homology group $H^1(X(\mathcal{C}_{\mathbb{F}_p}), \mathbb{Z})$ has rank 1.

5. Characteristic polynomials of Frobenius

Characteristic polynomials of Frobenius constitute one of the main tools in study of the Galois representations attached to abelian varieties, both from a theoretical point of view and for practical purposes. Before discussing them, however, we need to recall some basic terminology from algebraic number theory.

Let v be a place of K. Fix a place $\overline{v}$ of $\overline{K}$ extending v (or, equivalently, an embedding $\overline{K} \hookrightarrow \overline{K_v}$). The choice of $\overline{v}$ induces identifications of $\mathrm{Gal}\left(\overline{K_v}/K_v\right)$ with the *decomposition group* $D_v = D(\overline{v}/v)$, which contains the canonical inertia subgroup $I_v = I(\overline{v}/v)$. Different choices of $\overline{v}$ are conjugated under Galois, hence in particular all the possible decomposition and inertia groups above v are conjugated under Galois.

[4]this is the multi-graph having a vertex for every irreducible component of $\mathcal{C} \times_{\mathcal{O}_{K,v}} \mathbb{F}_v$ and an edge (possibly a loop) between components C_i and C_j if C_i and C_j meet at a double point

DEFINITION 5.1. *Let A/K be an abelian variety and let v be a place of K. Let ℓ be a prime number. We say that the representation ρ_{ℓ^n} (or ρ_{ℓ^∞}) is* ***unramified at*** *v if for some (hence all) choices of an inertia subgroup $I_v = I(\overline{v}/v)$ we have $\rho_{\ell^n}(I_v) = \{1\}$ (resp. $\rho_{\ell^\infty}(I_v) = \{1\}$).*

REMARK 5.2. The definition is independent of the choice of $\overline{v}$. This follows immediately from the fact that all inertia subgroups at v are conjugated.

Luckily, ρ_{ℓ^∞} is unramified at most places of K (recall from theorem 4.10 that every abelian variety A/K has good reduction at all but finitely many places of K):

THEOREM 5.3. *For every ℓ and n, the representations ρ_{ℓ^n} and ρ_{ℓ^∞} attached to A are unramified away from ℓ and from the places of bad reduction of A.*

This result is a consequence of the smooth proper base change theorem in étale cohomology, so we omit its proof. The statement itself, however, is really quite crucial in many applications!

The property of being unramified is extremely important. It leads in particular to the following definition:

DEFINITION 5.4. *Let v be a place of K at which A has good reduction. Then D_v/I_v is pro-cyclic, generated by an element which we call (improperly) the* ***Frobenius at*** *v. We also denote by Frob_v any lift of this element to $\mathrm{Gal}\left(\overline{K}/K\right)$: notice that Frob_v is well-defined only up to I_v and to the conjugation action of $\mathrm{Gal}\left(\overline{K}/K\right)$.*

Let now ℓ be a prime not divisible by ℓ. By theorem 5.3 we have that $\rho_{\ell^\infty}(I_v) = \{1\}$, which implies that $\rho_{\ell^\infty}(\mathrm{Frob}_v)$ is well-defined up to conjugation. Finally, since the characteristic polynomial of an endomorphism depends only on its conjugacy class, we may define

$$f_{v,\ell}(t) := \det\left(t\,\mathrm{Id} - \rho_{\ell^\infty}(\mathrm{Frob}_v)\right),$$

which is a well-defined polynomial in $\mathbb{Z}_\ell[t]$, independent of all the choices we made in defining Frob_v.

There is an obvious analogue of this definition in the case of finite fields:

DEFINITION 5.5. *Let A/K be an abelian variety over a finite field of characteristic p. Choose a prime $\ell \neq p$: the* ***characteristic polynomial of Frobenius*** *is defined as*

$$p_A(t) = \det(\rho_{\ell^\infty}(\mathrm{Frob}) - t\,\mathrm{Id}) \in \mathbb{Z}[t].$$

5.1. Compatibility. The extreme usefulness of these characteristic polynomials of Frobenius lies in the following (very deep) result, which combines input from many people but which was ultimately proved by Deligne [**Del74**]:

THEOREM 5.6 (Compatibility and the Weil conjectures). *The following hold:*

(1) *The polynomials $f_{v,\ell}(t)$ have integral coefficients and do not depend on the choice of v (provided that $v \nmid \ell$)*

(2) *the roots of* $f_{v,\ell}(t) \in \mathbb{Z}[t] \subset \mathbb{C}[t]$ *come in* g *conjugate pairs* $\tau_1, \overline{\tau_1}, \ldots, \tau_g, \overline{\tau_g}$. *Every* τ_i *is a* ***Weil number****: its absolute value is* $\#F_v^{1/2}$ *under any embedding of* $\overline{\mathbb{Q}}$ *in* $\mathbb{C}$.

In the light of this theorem it makes sense to introduce the following definition:

DEFINITION 5.7. *Notation as above. We set*

$$f_v(t) := f_{v,\ell}(t)$$

for any prime ℓ *not divisible by* v.

We can at least check that this is compatible with what we discussed in remark 2.5:

REMARK 5.8. Let $\sigma := \rho_{\ell\infty}(\mathrm{Frob}_v)$ (for an arbitrary determination of Frob_v). The constant term of $f_v(t)$ is given by $\det(\sigma)$, which according to remark 2.5 is equal to $\lambda(\sigma)^g = \chi_\ell(\mathrm{Frob}_v)^g = (\#\mathbb{F}_v)^g$. On the other hand, by theorem 5.6 we know that the constant term of f_v is equal to the product

$$\prod_{i=1}^{g} \tau_i\overline{\tau_i} = \prod_{i=1}^{g} |\tau_i|^2 = \prod_{i=1}^{g} \#\mathbb{F}_v = (\#\mathbb{F}_v)^g.$$

6. Characteristic polynomials of Frobenius for Jacobians

We finally come to our first properly explicit/computational topic. How does one go about determining $f_v(t)$ when A is the Jacobian of some nice curve? The answer is again provided by work of Weil (and Deligne):

THEOREM 6.1 (Zeta functions of curves over finite fields). *Let* $C/\mathbb{F}_q$ *be a smooth projective curve over the finite field with* $q = p^n$ *elements. Define the local zeta function by the formula*

$$Z(C,s) = \exp\left(\sum_{m=1}^{\infty} \frac{\#C(\mathbb{F}_{q^m})}{m} q^{-ms}\right).$$

Then the following hold:

(1) $Z(C,s)$ *is a rational function of* $t = q^{-s}$
(2) *we can write*

$$Z(C,s) = \frac{P_C(t)}{(1-t)(1-qt)}$$

for a certain polynomial $P_C(t)$ *of degree* $2g$ *with integer coefficients.*
(3) *the roots of* $P_C(t) \in \mathbb{Z}[t] \subset \mathbb{C}[t]$ *come in* g *conjugate pairs* $\tau_1, \overline{\tau_1}, \ldots, \tau_g, \overline{\tau_g}$. *Every* τ_i *is a Weil number of weight* -1, *that is, under every embedding in* $\mathbb{C}$ *it has absolute value* $q^{-1/2}$, *and* $\tau_i\overline{\tau_i} = q^{-1}$.

The usefulness of this theorem (and the connection to our computational problems) comes from the following additional result:

THEOREM 6.2. *Let C/K be a nice curve having good reduction at v. Then $f_v(t)$ agrees with $t^{2g}P_{C_{\mathbb{F}_v}}(1/t)$, where $C_{\mathbb{F}_v}$ is the curve over $\mathbb{F}_v$ deduced from (a smooth $\mathcal{O}_{K,v}$-model of) C by reduction modulo v.*

REMARK 6.3. By expanding formally the definition of $Z(C,s)$ and matching coefficients between this representation and the representation $Z(C,s) = \frac{P_C(t)}{(1-t)(1-qt)}$ one sees that the $g = g(C)$ numbers $\#C(\mathbb{F}_q), \dots, \#C(\mathbb{F}_{q^g})$ are sufficient to uniquely determine the polynomial $P_C(t)$. Moreover, the symmetry condition (τ is a root then so is $\frac{1}{q\tau}$) ensures that writing $P_C(t) = \sum_{i=0}^{2g} a_i t^i$ the coefficients a_i satisfy $a_{g+i} = q^i a_{g-i}$.

EXAMPLE 6.4. Let us see how this works in practice for the curve $C : y^2 = x^5 + x + 2$ defined over $\mathbb{F}_p$ for $p = 7$. It is useful to write N_m for $\#C(\mathbb{F}_{p^m})$. One may compute directly (that is, using some computer algebra system) that $N_1 = 10$ and $N_2 = 46$ (don't forget that there is a point at infinity!).

Now write $P_C(t) = p^2t^4 - pa_1t^3 + a_2t^2 - a_1t + 1$ (the shape of the polynomial follows from Remark 6.3, and the minus sign in front of the coefficient a_1 is for consistency with some familiar formulas in the case of elliptic curves, see below). Expanding the ratio $\dfrac{P_C(t)}{(1-t)(1-pt)}$ formally as a power series in t we obtain

$$Z(C,s) = 1 + t(-a_1 + p + 1) + t^2\left(-a_1p - a_1 + a_2 + p^2 + p + 1\right) + O\left(t^3\right),$$

while from the defining formula for $Z(C,s)$ we get

$$\begin{aligned} Z(C,s) &= \exp\left(N_1t + \frac{N_2}{2}t^2 + O(t^3)\right) \\ &= 1 + N_1t + \frac{1}{2}N_2t^2 + \frac{1}{2}N_1^2t^2 + O(t^3) \end{aligned}$$

from which we get the formulas

$$a_1 = p + 1 - N_1, \quad a_2 = \frac{1}{2}(N_2 + N_1^2) - (p+1)N_1 + p.$$

While the formula for a_2 might not be very enlightening, the formula for a_1 should be familiar: it's precisely the definition of the so-called **trace of Frobenius** (very often denoted by a_p) for elliptic curves!

More generally, we have:

PROPOSITION 6.5. *We have the following general formula: writing $P_C(t) = \prod_{i=1}^{2g}(\alpha_i t - 1)$, for every $m \geq 1$ we have*

$$\#C(\mathbb{F}_{q^m}) = q^m + 1 - \sum_{i=1}^{2g} \alpha_i^m.$$

REMARK 6.6 (Number of $\mathbb{F}_q$-rational points of the Jacobian). If we are interested in the arithmetic of the Jacobian itself (rather than the arithmetic of C), another formula which often comes in handy is the equality

$$\#\operatorname{Jac}(C)(\mathbb{F}_q) = P_C(1).$$

The quickest proof of this equality I know goes through the Lefschetz trace formula: the number of fixed points of Frobenius is equal to the alternating sum of traces of Frob on $H^i_{\acute{e}t}(J, \mathbb{Q}_\ell)$, that is,

$$\begin{aligned}
\#J(\mathbb{F}_q) &= \#J(\overline{\mathbb{F}_q})^{\mathrm{Frob}} \\
&= \sum_{i=0}^{2g} (-1)^i \operatorname{tr}\left(\mathrm{Frob} \;\middle|\; H^i_{\acute{e}t}(J, \mathbb{Q}_\ell)\right) \\
&= \sum_{i=0}^{2g} (-1)^i \operatorname{tr}\left(\mathrm{Frob} \;\middle|\; \Lambda^i H^1_{\acute{e}t}(J, \mathbb{Q}_\ell)\right) \\
&= \sum_{i=0}^{2g} (-1)^i \sum_{\substack{H \subseteq \{1,\ldots,2g\} \\ |H|=i}} \prod_{h \in H} \alpha_h \\
&= P_C(1).
\end{aligned}$$

7. Torsion in the Jacobian

We may now ask a very concrete computational question:

QUESTION 7.1. *Let $C/\mathbb{Q}$ be a nice curve of genus g with Jacobian J. How does one compute the torsion of $J(\mathbb{Q})$?*

To my knowledge, the answer is fully known only for $g \leq 2$, and work is being done on the $g = 3$ case. The reason for these restrictions is described in the following remark:

REMARK 7.2 (Torsion of the Jacobian, global approach). There is a notion of canonical height on Jacobians. If one denotes by $\hat{h}$ this canonical height and by h some naïve height on divisors, then $|h - \hat{h}|$ is bounded by an absolute constant $c = c(J)$, and furthermore one knows that $\hat{h}([D]) = 0$ if and only if $[D]$ is a torsion point. Therefore a possible approach to computing $J(\mathbb{Q})_{\mathrm{tors}}$ is as follows: one determines c from the equations of C, and then enumerates all points on the Jacobian up to *naïve* height c. This finite (and computable) set of divisor classes contains all the torsion points in $J(\mathbb{Q})$. This leaves us with two problems:

(1) enumerating divisors: this is computationally challenging when the genus increases. As a first approximation, consider that a divisor class on J of height bounded by c can be represented by a divisor $D = [P_1 + \ldots + P_g - g\infty]$, where ∞ is a fixed rational point[5] and the naïve height of each of the P_i is bounded by c.

[5]of course the situation is even more complicated if there is no rational point at all!

Since the height in question is typically a *logarithmic* measure of size, one needs to enumerate all rational points with numerator and denominator up to e^c, and then take all possible multi-sets of size at most g built from these points. It is not hard to image how this computation might quickly become unfeasible.

We note however that in order to test whether a given divisor is a torsion point one needs an *a priori* bound on its torsion order. This is typically obtained by the techniques we shall see in the following example (namely computing in $J(\mathbb{F}_p)$ for some small prime p).

(2) More importantly, explicit values for the constant c have only been worked out for small values of g: the theory is very well understood for $g = 1$ (elliptic curves) and there are satisfactory answers also for $g = 2$ [**MS16**], but for $g \geq 3$ no complete answer is known (see however [**Sto17**] for recent progress on the $g = 3$ case).

However, given a concrete curve C one may often gain a fairly good idea of what the torsion subgroup of $\mathrm{Jac}(C)(\mathbb{Q})$ looks like by studying the action of Galois on torsion points:

EXAMPLE 7.3. Let C be the curve over $\mathbb{Q}$ defined by $y^2 + (x^2 + x + 1)y = -x^6$ and let J be its Jacobian. We determine the torsion in $J(\mathbb{Q})$.

(1) We check that C has bad reduction only at $83, 139$
(2) By point-counting we determine that for $p = 3$ the characteristic polynomial of Frobenius is $f_3(t) = t^4 - t^3 - 3t + 9$, while for $p = 5$ we have $f_5(t) = t^4 - t^3 + 4t^2 - 5t + 25$.
(3) Assume that $P \in J(\mathbb{Q})$ is a torsion point of order N, and let ℓ^k be a prime power dividing N. Then the representation ρ_{ℓ^k} has a fixed point, which means that (for all primes $p \neq \ell$ at which C has good reduction, $p \neq \ell$) the characteristic polynomial of the Frobenius at p must have 1 as a root modulo ℓ^k. This means in particular that ℓ^k is either a power of 3 or it divides $f_3(1) = 6$, hence $\ell^k \in \{2, 3^k\}$. For the same reason, ℓ^k is either a power of 5 (which we have already ruled out) or it divides $f_5(1) = 24$. Combining these two pieces of information we obtain $\ell^k \in \{2, 3\}$.
(4) This already shows that $J(\mathbb{Q})_{\mathrm{tors}}$ is killed by 6. By using exercise 1.8, we check that there is no 2-torsion in $J(\mathbb{Q})$. This implies that $J(\mathbb{Q})_{\mathrm{tors}}$ is either trivial or has order 3.
(5) Checking more characteristic polynomials of Frobenius, a factor of 3 keeps popping up, so we suspect there might be 3-torsion in the Jacobian after all.
(6) We notice two obvious rational points on C, namely $P_1 = (0, 0)$ and $P_2 = (0, -1)$. From these two points we obtain a point in $J(\mathbb{Q})$, namely $[D]$ where D is the divisor $P_2 - P_1$. Notice that $[D] \neq 0$ for an argument we have already used many times: if $[D] = 0$, then $D = \mathrm{div}(g)$ with $g : C \to \mathbb{P}^1$ of degree 1, which is not possible since C and $\mathbb{P}^1$ are not isomorphic.
(7) We show that $3[D] = 0$: this will imply $J(\mathbb{Q})_{\mathrm{tors}} = \{0, [D], [2D]\}$. We need to find a function which vanishes at $(0, -1)$ of order 3. Such a function will necessarily be of the form $f = a(x)y + b(x)$ with $a(x), b(x)$ rational functions; replacing in the equation for C we find that the x-coordinates of the zeroes of f in the affine

patch are to be found among the solutions to

$$\begin{cases} y = -b(x)/a(x) \\ \left(\frac{-b(x)}{a(x)}\right)^2 + (x^2+x+1)\left(\frac{-b(x)}{a(x)}\right) = -x^6. \end{cases}$$

Since $-x^6$ vanishes at $(0,-1)$ with high order, we'd like the left-hand side to do the same. Hence we may try setting it equal to 0, which gives

$$\frac{b(x)}{a(x)} = (x^2+x+1),$$

that is, $f = a(x)(y+x^2+x+1)$. Since we have already observed that f vanishes only at points with $x=0$, for these points we have either $a(0)=0$ or $y=-1$. Since we want f to only vanish at P_2, it suffices to choose $a(0)\neq 0$. The simplest choice $a(x)=1$ leads to

$$\operatorname{div}(f) = 6P_2 - 3(\infty_1+\infty_2),$$

where ∞_1, ∞_2 are the two points at infinity on C; this doesn't quite work yet. Thus we now need to choose $a(x)$ so that $\operatorname{div}(a) = 3(\infty_1+\infty_2) - 3P_1 - 3P_2$, that is, $a(x)$ needs to have zeroes at infinity and poles precisely where x vanishes. It is then immediate to deduce that we need to take $a(x) = \frac{1}{x^3}$, which does indeed have a pole of order 3 at both P_1, P_2 and a triple zero at each point at infinity. Putting everything together, we have that

$$3D = \operatorname{div}\left(\frac{y+x^2+x+1}{x^3}\right) = \operatorname{div}\left(\frac{x^3}{y}\right)$$

and therefore $3[D] = 0 \in J(\mathbb{Q})$.

Having treated this example with a minimal amount of theory, we point out that in fact one has finer tools to compare the torsion in $\operatorname{Jac}(C)(\mathbb{Q})$ with the finite groups $\operatorname{Jac}(C)(\mathbb{F}_p)$:

THEOREM 7.4 (Torsion injects in the reductions). *Let A/K be an abelian variety over a number field. Let v be a place of K of characteristic p and let suppose that A has good reduction at v. Finally, let $A(K)'_{\text{tors}}$ denote the subgroup of $A(K)_{\text{tors}}$ whose points have order prime to p. Then the natural reduction map*

$$A(K)'_{\text{tors}} \to A(\mathbb{F}_v)$$

is injective.

SKETCH OF PROOF. It suffices to do this one prime at a time, namely, it suffices to show that for $\ell \neq p$ we have an injection $A(K)[\ell^\infty] \to A(\mathbb{F}_v)$, where $A(K)[\ell^\infty]$ denotes the ℓ-primary component of $A(K)_{\text{tors}}$. By the Mordell-Weil theorem 8.1 the group $A(K)_{\text{tors}}$ is finite, so we can choose $n \gg 0$ such that $A(K)[\ell^\infty] = A(K)[\ell^n]$. Let $\mathcal{A} \to \operatorname{Spec}(\mathcal{O}_{K,v})$ be an abelian scheme extending $A \to \operatorname{Spec}(K_v)$; the extension $\mathcal{A}$ exists since A has good reduction at v.

We know that $A[\ell^n]$ is an étale group scheme over K_v (remark 5.7), but in fact it is also étale over $\mathcal{O}_{K,v}$, because $\ell \neq p$ is invertible in $\mathcal{O}_{K,v}$. It follows that $\mathcal{A}[n]$ has precisely

ℓ^{2ng} points over the maximal unramified extension $\mathcal{O}_v^{\mathrm{nr}}$ of $\mathcal{O}_{K,v}$ (that is, the integral closure of $\mathcal{O}_{K,v}$ inside the maximal unramified extension of K_v). Similarly, $\mathcal{A}[n]$ has ℓ^{2ng} rational points over $\overline{\mathbb{F}_v}$. By Hensel's lemma (and étaleness), each point in $\mathcal{A}[n]\left(\overline{\mathbb{F}_v}\right)$ lifts to a unique point in $\mathcal{A}[n]\left(\mathcal{O}_v^{\mathrm{nr}}\right)$, which implies that the reduction map

$$\mathcal{A}[\ell^n](\mathcal{O}_v^{\mathrm{nr}}) \to \mathcal{A}[\ell^n](\overline{\mathbb{F}_v})$$

is a bijection (since it is surjective between sets of the same cardinality). In particular, by restricting to $\mathcal{O}_{K,v} \subseteq \mathcal{O}_v^{\mathrm{nr}}$ we obtain an injective map

$$A[\ell^n](K_v) = \mathcal{A}[\ell^n](\mathcal{O}_{K,v}) \to \mathcal{A}[\ell^n](\mathbb{F}_v),$$

where the first equality follows from the properness of $\mathcal{A}$ and the obvious fact that

$$A[\ell^n](K_v) = A(K_v)[\ell^n], \quad \mathcal{A}[\ell^n](\mathcal{O}_{K,v}) = \mathcal{A}(\mathcal{O}_{K,v})[\ell^n].$$

□

REMARK 7.5. In fact, it is even true that $A(\mathbb{Q})_{\mathrm{tors}} \to A(\mathbb{F}_p)$ is injective, provided that $p \geq 3$ is a prime of good reduction of A.

8. The existence of transvections; Chris Hall's trick

Frobenius elements are very useful to control the image of Galois, but (due to the fundamental results of Faltings) they only provide *semisimple* elements in $\mathrm{Aut}(V_\ell A)$. It is sometimes useful to have a source of unipotent elements to work with: in this direction a very useful trick was introduced by Chris Hall in [**Hal11**]. We state it in its simplest form:

THEOREM 8.1. *Let A/K be an abelian variety with Néron model $\mathcal{A}$. Suppose there exists a place v of K at which A has semistable reduction of toric rank 1 (see definition 4.6). Let ℓ be a prime which does not divide the Tamagawa number*[6] *of A at v. Then G_{ℓ^∞} contains a **transvection**, that is, an automorphism M such that the image of $M - I$ is a saturated*[7] *$\mathbb{Z}_\ell$-module of rank 1.*

9. Raynaud's theorem: the action of the inertia at ℓ

As we have seen, Frobenius polynomials capture essentially all the information concerning our Galois representations when we restrict to the decomposition group of a place at which the representation is *unramified*. Even when the underlying abelian variety has good reduction everywhere, however, this is not the full story, because of the action of the inertia at primes of characteristic ℓ. This is a very rich subject (and the starting point of p-adic Hodge theory), so we content ourselves with describing a single (very useful) result due to Raynaud [**Ray74**]:

THEOREM 9.1. *Suppose A/K has good reduction at v (a place of K characteristic ℓ) and consider the action of the inertia subgroup at v on $A[\ell]$. Let W be a Jordan-Hölder simple constituent of the $I(v)$-module $A[\ell]$. Then:*

[6] write $\mathcal{A}$ for the Néron model of A and consider the exact sequence $0 \to \mathcal{A}^0 \to \mathcal{A} \to \Phi \to 0$. The Tamagawa number of A at v is $\Phi(\mathbb{F}_v)$.

[7] that is, if kv belongs to the image of $M - I$ then v belongs to the image of $M - I$

(1) *the wild inertia subgroup acts trivially, so that the action of* $I(v)$ *factors through the tame inertia group* I_v^t
(2) *if* $\dim(W) = n$*, one can endow* W *with the structure of a* $\mathbb{F}_{\ell^n}$*-vector space of dimension* 1 *in such a way that the action of* I_v^t *is given by a character* ψ
(3) *there are exponents* $e_1, \dots, e_n$ *such that:*
   (a) $\psi = \varphi_1^{e_1} \dots \varphi_n^{e_n}$*, where the* φ_i *are the* n *fundamental characters of level* n*;*
   (b) $e_i \leq e = e(v|\ell)$*, the absolute ramification index of* v *over* ℓ*.*

10. The isogeny theorem

As a final tool in the study of Galois representations we mention an incredibly powerful and deep result due to Masser and Wüstholz [**MW93**] (subsequently improved by Gaudron and Rémond [**GR14**]):

THEOREM 10.1 (Isogeny theorem). *There is an (explicit) function* $f(g, d, h)$ *with the following property. For every number field* K *of degree at most* d *and for every pair of* g*-dimensional abelian varieties* A/K*,* B/K *such that there exists a* K*-isogeny between* A *and* B*, there exists a* K*-isogeny* $\psi : A \to B$ *of degree bounded by* $f(g, d, h(A))$*, where* $h(A)$ *is the* ***semistable Faltings height of*** A[8]*.*

[8]we shall not define this notion here; we only remark that $h(A)$ is a measure of the arithmetic complexity of A, and in the case of an elliptic curve E it agrees (up to bounded error) with $\frac{1}{12}h(j(E))$, where $j(E)$ is the usual j-invariant and h denotes the logarithmic Weil height

CHAPTER 3

Endomorphism algebras, complex multiplication, and examples

1. Endomorphism algebras

The purpose of this section is to recall the following theorem of Albert, which is often very helpful to determine the endomorphism algebra of an abelian variety:

THEOREM 1.1 (Albert classification, [**Alb34**], [**Alb35**], [**Mum70**, Page 202]). *Let $A/\mathbb{C}$ be a simple abelian variety and let $D := \mathrm{End}^0_{\mathbb{C}}(A) = \mathrm{End}_{\mathbb{C}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. Denote by L be the center of D (a number field) and by L_0 the subfield of L fixed by the Rosati involution. Let furthermore $e = [L : \mathbb{Q}], e_0 = [L_0 : \mathbb{Q}], d^2 = \dim_L(D)$ and $g = \dim(A)$. Then L_0 is a totally real field, $[L : L_0]$ is either one or two, and if $[L : L_0] = 2$, then L is a CM field. Moreover, in this case it is always possible to choose a polarisation λ in such a way that the corresponding Rosati involution is complex conjugation.*

The following are the only possibilities for D (the fourth column displays numerical constraints that e_0, e, d and g must satisfy):

Type	**e**	**d**		**Description**
I(e_0)	e_0	1	$e_0 \mid g$	$D = L$, a totally real field of degree e_0 over $\mathbb{Q}$
II(e_0)	e_0	2	$2e_0 \mid g$	D is a quaternion algebra over the totally real field L, split at all the infinite places ('totally indefinite quaternion algebra')
III(e_0)	e_0	2	$2e_0 \mid g$	D is a quaternion algebra over the totally real field L, inert at all the infinite places ('totally definite quaternion algebra')
IV(e_0, d)	$2e_0$	any	$e_0 d^2 \mid g$	L is a CM field and D is a division ring of degree d over L

REMARK 1.2. There is a similar result in positive characteristic; the only difference is that some of the numerical restrictions become less stringent.

We don't discuss the proof of this theorem (which depends on the properties of the Rosati involution – mainly its positivity – and on a careful study of its action on D), but quickly explain where the numerical restrictions come from:

PROPOSITION 1.3. *Let $A/\mathbb{C}$ be a simple abelian variety of dimension g and let D be its endomorphism algebra. The degree $[D : \mathbb{Q}]$ divides $2g$.*

PROOF. D acts faithfully on the $2g$-dimensional $\mathbb{Q}$-vector space $H_1(A(\mathbb{C}), \mathbb{Q})$. In characteristic zero, if V is a representation of a division algebra $R/\mathbb{Q}$ we have

$$\dim_{\mathbb{Q}}(R) \mid \dim_{\mathbb{Q}}(V).$$

□

REMARK 1.4. A result of Shimura [**Shi63**] implies that most of the algebras in the Albert classification actually appear as endomorphism algebras of complex abelian varieties. More precisely, given an integer g and an algebra D whose invariants (e, d) satisfy the restrictions in Albert's theorem, there is a simple abelian variety $A/\mathbb{C}$ such that $\mathrm{End}^0(A) \cong D$, unless D is of type III (resp. IV) and the quotient $g/(2e)$ (resp. $\frac{g}{e_0 d^2}$) is either 1 or 2 (see [**Mum70**], page 203). Even for these exceptional cases, Shimura proved a complete classification result [**Shi63**, §4].

EXAMPLE 1.5. If A is a simple abelian surface over $\mathbb{C}$ with endomorphism algebra D, the center of D does not contain an imaginary quadratic field and D is not of type III.

REMARK 1.6. A specialisation argument shows that Shimura's theorem still holds if one replaces $\mathbb{C}$ by $\overline{\mathbb{Q}}$.

When working with endomorphism algebras it is sometimes useful to consider the so-called *reduced degree*:

DEFINITION 1.7. *Given a semisimple $\mathbb{Q}$-algebra D of finite dimension, write $D \cong \bigoplus D_i$ with every D_i simple. Denoting by K_i the center of D_i (K_i is then a number field), there exist integers d_i such that $[D_i : K_i] = d_i^2$; the* ***reduced degree*** *of D is*

$$[D : \mathbb{Q}]_{\mathrm{red}} = \sum_i d_i [K_i : \mathbb{Q}].$$

PROPOSITION 1.8. *Let $A/\mathbb{C}$ be a simple abelian variety of dimension g. Then the inequality $[\mathrm{End}_{\mathbb{C}}(A) : \mathbb{Q}]_{\mathrm{red}} \leq 2g$ holds, with equality if and only if $\mathrm{End}_{\mathbb{C}}(A)$ is a CM field of degree $2g$. More generally, if $A/\mathbb{C}$ is any abelian variety, then we have $[\mathrm{End}_{\mathbb{C}}(A) : \mathbb{Q}]_{\mathrm{red}} \leq 2g$. If equality holds, $\mathrm{End}_{\mathbb{C}}(A)$ is a product of matrix algebras over fields.*

DEFINITION 1.9. *An abelian variety A (not necessarily simple) for which equality is attained (that is, $[\mathrm{End}_{\mathbb{C}}(A) : \mathbb{Q}]_{\mathrm{red}} = 2g$) is called a* ***CM abelian variety****.*

1.1. Behaviour under reduction, ordinarity. We quickly discuss the relationship between the endomorphism algebra of an abelian variety over a number field K and that of any of its reductions. The crucial fact is the following:

THEOREM 1.10 ([**ST61**, Proposition 6.1]). *Let A be an abelian variety over a number field K and let v be a place of good reduction for A. The natural map*

$$\mathrm{End}(A) \otimes \mathbb{Q} \to \mathrm{End}(A_v) \otimes \mathbb{Q}$$

is injective.

It is also interesting to understand how the endomorphisms of an abelian variety over a finite field change upon extension of the ground field. We shall need a definition:

DEFINITION 1.11 (Ordinary abelian variety). *Let A be an abelian variety over a field K of characteristic p. We say that A is **ordinary** if $A[p](\overline{K})$ has order $p^{\dim A}$.*

We give a concrete characterisation of ordinarity for abelian varieties of small dimension; for the following two results, see [**Gon98**] and [**WM71**, § III]:

PROPOSITION 1.12. *Let A/K be an abelian variety over a field of characteristic p. Then:*

1. *if $\dim A = 1$ (i.e. A is an elliptic curve), then A is ordinary if and only if it is not supersingular, that is, if and only if the trace of Frobenius is not 0.*
2. *if $\dim A = 2$, write $f(t) = t^4 + pat^3 + bt^2 + at + p^2$ for the characteristic polynomial of Frobenius. Then A is ordinary if and only if $p \nmid b$.*

In general, A is ordinary if and only if $\pi_A + q/\pi_A$ is prime to p, where $|\mathbb{F}| = q = p^h$ and $\pi_A \in \mathbb{C}$ is any root of the characteristic polynomial of the Frobenius of A.

THEOREM 1.13. *Let A be an abelian variety over a finite field $\mathbb{F}$. Suppose that A is ordinary and simple: then $\mathrm{End}_{\mathbb{F}}(A) = \mathrm{End}_{\overline{\mathbb{F}}}(A)$.*

1.2. Examples. Let's now give an example of how, in some cases, one may use the Albert classification to quickly establish the structure of $\mathrm{End}(\mathrm{Jac}(C))$:

EXAMPLE 1.14 (Maximal complex multiplication). Consider the curves $C_p : y^2 = x^p + 1$ and their Jacobians J_p. It is apparent that (over $\overline{\mathbb{Q}}$) there is an action of ζ_p on C_p, which induces an embedding $\mathbb{Z}[\zeta_p]^\times \hookrightarrow \mathrm{End}_{\overline{\mathbb{Q}}}(J_p)^\times$. Let A be a simple factor of J_p over $\overline{\mathbb{Q}}$ on which ζ_p acts nontrivially. Then $D := \mathrm{End}^0_{\overline{\mathbb{Q}}}(A)$ is a division algebra that contains $\mathbb{Z}[\zeta_p]$, hence contains $\mathbb{Q}(\zeta_p)$. Notice that $\dim A \leq \dim J_p = g(C_p) = \frac{p-1}{2}$ and that A contains the subalgebra $\mathbb{Q}(\zeta_p)$, of dimension $p-1 = 2g(C_p)$. By proposition 1.3 we obtain $\dim(A) \geq \frac{p-1}{2}$, hence $A = J_p$, which is therefore absolutely simple. Moreover, one sees easily by going through Albert's list that D must coincide with $\mathbb{Q}(\zeta_p)$:

1. D cannot be of type I, because $\mathbb{Q}(\zeta_p)$ does not embed in a totally real number field;
2. D cannot be of type II or III: if it were, the embedding $\mathbb{Q}(\zeta_p) \hookrightarrow D$ would give $[D : \mathbb{Q}] \geq p - 1$, and on the other hand $[D : \mathbb{Q}] = 4e_0 \mid 2g = p - 1$, which would imply $D = \mathbb{Q}(\zeta_p)$, which is a contradiction since $\mathbb{Q}(\zeta_p)$ is commutative and D is not.
3. therefore D is of type IV. As before, one has $[D : \mathbb{Q}] \geq p - 1$ and $[D : \mathbb{Q}] = 2e_0 d^2 \leq 2g = p - 1$, whence $D = \mathbb{Q}(\zeta_p)$ as claimed.

Finally, since $\mathbb{Z}[\zeta_p]$ is a maximal order in $\mathbb{Q}(\zeta_p)$, we obtain $\mathrm{End}_{\mathbb{C}}(J_p) = \mathbb{Z}[\zeta_p]$.

EXAMPLE 1.15 (Picard curves). Consider a genus 3 curve of the form

$$C : y^3 = f(x),$$

where $f(x)$ is a separable polynomial of degree 4. Then there is an action of ζ_3 on C, and therefore also on $J = \mathrm{Jac}(C)$. Assume that J is geometrically irreducible: what can its geometric endomorphism algebra look like? It's certainly not type II or III in the Albert classification, because these only arise for even g. It's not an algebra of type I either, because the field $\mathbb{Q}(\zeta_3)$ cannot be embedded in a totally real number field. So it is of type IV, and since $g = 3$ we must have $d = 1$ and $e_0 \in \{1, 3\}$. Hence the endomorphism algebra of J is a CM field: more precisely, it is either quadratic imaginary (in which case it is $\mathbb{Q}(\zeta_3)$: this is the general case), or a sextic CM field given by the compositum of $\mathbb{Q}(\zeta_3)$ with a totally real cubic field.

Example 1.16 (Curve of genus 3 whose Jacobian maps to the square of an elliptic curve). Consider the genus-3 curve

$$C : \ y^2 = x^8 + 3x^4 + 1$$

and its Jacobian J. Then $\mathrm{Aut}(C)$ contains (at least) the hyperelliptic involution and the two isomorphisms $\alpha_2 : (x, y) \mapsto (ix, y)$ and $\alpha_3 : (x, y) \mapsto (1/x, y/x^4)$. Notice that

$$\alpha_2\alpha_3(x, y) = (i/x, y/x^4) \neq (-i/x, y/x^4) = \alpha_3\alpha_2(x, y),$$

so that $\mathrm{Aut}(C)$ is not commutative. However, we know that $\mathrm{Aut}(C)$ embeds in $\mathrm{End}(J)^\times$; suppose now that J is geometrically simple. Then Albert's classification implies that $D := \mathrm{End}^0_{\mathbb{C}}(J)$ is a field, which contradicts the fact that $D^\times$ contains the non-commutative group $\mathrm{Aut}(C)$. Hence we recover from Albert's classification the fact (obvious by just staring at the equation of the curve for three or more seconds!) that J cannot be simple. But looking at the endomorphism ring tells us more: indeed it's immediate to see that C admits at least two independent maps towards elliptic curves, so J is (geometrically) isogenous to the product of three elliptic curves E_1, E_2, E_3. Suppose that the E_i are pairwise non-isogenous (geometrically): then $D \cong \prod_{i=1}^3 \mathrm{End}^0_{\mathbb{C}}(E_i)$, which is commutative since the endomorphism ring of an elliptic curve is always commutative in characteristic zero. Again we find a contradiction with the fact that $\mathrm{Aut}(C)$ embeds in $D^\times$! It follows that at least two of the three elliptic curves are geometrically isogenous.

Finally, we prove that 2 of these 3 elliptic curves are isogenous, but the third one is not. We compute that $f_3(t) = (t^2 - 2t + 3)(t^2 + 3)(t^2 + 2t + 3)$, which means (by theorem 2.14) that $J_{\mathbb{F}_3}$ is isogenous to the product of three elliptic curves $\tilde{E}_1, \tilde{E}_2, \tilde{E}_3$, precisely one of which (say $\tilde{E}_2$) is supersingular. Since supersingularity is a geometric property (and it depends only on the isogeny class), we find that even over $\overline{\mathbb{F}_3}$ the curves $\tilde{E}_1$ and $\tilde{E}_2$ cannot become isogenous. This in turn implies that over $\overline{\mathbb{Q}}$ (or even over $\mathbb{C}$) not all the elliptic curves E_i are isogenous. Thus the decomposition of $J_{\overline{\mathbb{Q}}}$ up to isogeny is $E_1^2 \times E_2$, with E_1, E_2 not isogenous.

As a final remark, notice that $\tilde{E}_1$ and $\tilde{E}_3$ are (up to isogeny) quadratic twists of each other, hence, after a quadratic extension of $\mathbb{F}_p$, they become isogenous. This is consistent with the decomposition $J_{\overline{\mathbb{Q}}} \sim E_1^2 \times E_2$.

Example 1.17 (A simple, not absolutely simple abelian surface). Consider the Jacobian J of the curve $C : \ y^2 = x^5 - 3x^4 + 3x^2 + x$ (LMFDB). A quick computation reveals that

the characteristic polynomial of the Frobenius at 7 is t^4-10t^2+49, which is irreducible over $\mathbb{Q}$; this immediately implies that J is $\mathbb{F}_7$-irreducible, hence also $\mathbb{Q}$-irreducible. However, we notice that $\mathrm{Aut}_{\mathbb{Q}(i)}(C)$ contains $\alpha : (x,y) \mapsto \left(\frac{-1}{x}, \frac{iy}{x^3}\right)$, which induces an automorphism α on J. Notice that $\alpha \neq -\mathrm{id}$ on J since $-\mathrm{id}$ is induced by the hyperelliptic involution (exercise 1.9), so $\beta_1 := \alpha - \mathrm{Id}$ and $\beta_2 := \alpha + \mathrm{Id}$ are both nontrivial endomorphisms. Since their product is zero (but neither is trivial), one sees immediately that β_1, β_2 have kernels of positive dimension. The identity components E_1, E_2 of these kernels are abelian subvarieties of J, which is therefore not simple: since J is a surface, E_1, E_2 are forced to be of dimension 1 (hence elliptic curves), which proves that $J_{\mathbb{Q}(i)} \sim E_1 \times E_2$.

EXAMPLE 1.18 (Real multiplication by $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$). We take this example from [**KM16**]. Consider the curve

$$C : \ u^2 = h(t) := t^5 - t^4 + t^3 + t^2 - 2t + 1$$

with Jacobian J. Define Z to be the curve

$$Z : \begin{cases} u^2 = h(t) \\ t^2x^2 - x - t + 1 = 0 \end{cases}$$

The obvious map $\varphi : Z \to C$ given by $(t,u,x) \mapsto (t,u)$ is a 2-to-1 cover, but there is also a further map $Z \to C$ given by

$$\psi : (u,t,x) \mapsto \left(x, \frac{u}{t^3}\left(1 - x(t+1)\right)\right).$$

One may check that $T := \psi_*\varphi^*$ is an endomorphism of J with minimal polynomial $T^2 - T - 1$, hence it generates a subring of $\mathrm{End}^0_{\mathbb{Q}}(J)$ isomorphic to $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

We now show that $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ is the full ring of endomorphisms of $J_{\overline{\mathbb{Q}}}$.

First we compute $f_3(t) = t^4+3t^3+7t^2+9t+9$ and $f_5(t) = t^4+2t^3+6t^2+10t+25$; as $f_3(t)$ is irreducible over $\mathbb{Q}$, this implies that $J_{\mathbb{Q}}$ is simple. Further manipulations of $f_3(t)$ (see exercise 2.15) show that J is geometrically simple, and that its geometric endomorphism ring is commutative. It follows from theorem 1.1 that $D := \mathrm{End}^0_{\mathbb{Q}}(J)$ is a field, and we already know that it contains $\mathbb{Q}(\sqrt{5})$. Hence there are only two possibilities: either $D = \mathbb{Q}(\sqrt{5})$, or D is a quartic CM field.

One checks (using proposition 1.12) that J is ordinary at 3 and 5, which implies (by theorems 1.13 and 2.15) that $\mathrm{End}^0_{\overline{\mathbb{F}_3}}(J) = \mathrm{End}_{\mathbb{F}_3}(J) = \mathbb{Q}[t]/(f_3(t)) =: F_3$ and $\mathrm{End}^0_{\overline{\mathbb{F}_5}}(J) = \mathrm{End}_{\mathbb{F}_5}(J) = \mathbb{Q}[t]/(f_5(t)) =: F_5$. It follows that if D were a quartic CM field, the three fields F_3, F_5 and D should all coincide. It is easy to see (for example computing discriminants) that this does not happen, so D cannot be a CM field. Finally, since $D = \mathbb{Q}(\sqrt{5})$ and $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ is the unique maximal order of D, we deduce as desired that $\mathrm{End}_{\overline{\mathbb{Q}}}(J) = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

2. Complex multiplication

In this final paragraph we quickly review the theory of complex multiplication from the point of view of Galois representations.

In this section A will be a g-dimensional abelian variety defined over a number field[1] K of CM type (see definition 1.9). The general principle is that *everything about CM abelian varieties is well understood*, but of course turning this vague (and optimistic) statement into actual computations can be challenging at times! See for example Exercise 2.14.

The most important results (due variously to Shimura, Taniyama, Weil, Serre and Tate, and nicely explained in [**ST68**]) are as follows.

(1) A has potential good reduction at all places of K.
(2) from now on, suppose that A/K has complex multiplication defined over K – that is, $\mathrm{End}_{\overline{K}}(A) = \mathrm{End}_K(A)$. Let $E := \mathrm{End}^0_K(A)$ be the field of complex multiplication and let $R = \mathrm{End}_K(A)$. Then $V_\ell(A)$ is a free $E_\ell := E \otimes \mathbb{Q}_\ell$-vector space of dimension 1, and $T_\ell(A)$ is a free $R_\ell := R \otimes \mathbb{Z}_\ell$-module of rank 1 provided that ℓ does not divide the index of R inside the maximal order of E. Moreover, an element of E_ℓ carries $T_\ell(A)$ to itself if and only if it is contained in R_ℓ.
(3) Using this, we may identify the Galois representation
$$\rho_{\ell^\infty} : \mathrm{Gal}\left(\overline{K}/K\right) \to \mathrm{Aut}(T_\ell(A))$$
with a representation
$$\rho_{\ell^\infty} : \mathrm{Gal}\left(\overline{K}/K\right) \to R_\ell^\times.$$
(4) For each place v of K there is a homomorphism
$$\varphi_v : I(v) \to \mu(E)$$
from the inertia group at v to the group of roots of unity in E. The fixed field of its kernel is the minimal extension of K over which A acquires good reduction at the places above v; in particular, φ_v is trivial if A has good reduction at v.
(5) let n_v be the minimal integer such that φ_v is trivial on the n_v-th ramification group $I(v)^{(n_v)}$ (in the upper numbering). Then the exponent of the conductor of A at v is equal to $2\dim(A)n_v$.
(6) there is a map ψ_ℓ, which we describe below, such that for every idèle $a \in I_K$ we have
$$\rho_{\ell^\infty}(a) = \varepsilon(a)\psi_\ell(a_\ell^{-1}),$$
where a_ℓ is the component of ℓ along the places of characteristic ℓ.
(7) ε agrees with φ_v upon restriction to $U_v(K)$, the group of units of the ring of integers of the completion K_v.

In order to describe the map ψ_ℓ we need to introduce some further concepts specific to CM abelian varieties:

Definition 2.1 (CM field). *A **CM field** is a totally imaginary quadratic extension E of a totally real number field E_0.*

Definition 2.2 (CM type). *Let E be a CM field and let $G := \mathrm{Hom}(E, \overline{\mathbb{Q}})$ be the set of field embeddings of E in $\overline{\mathbb{Q}}$. The elements of G come naturally in pairs, since if $\varphi : E \hookrightarrow \overline{\mathbb{Q}}$*

[1] it is a theorem that *complex* abelian varieties of CM type can be defined over a number field

is an embedding, then so is $\overline{\varphi}$ (obtained by post-composing φ with complex conjugation[2]*); moreover, since E is totally imaginary, φ and $\overline{\varphi}$ are distinct. A* ***CM type*** *for E is a subset Φ of G such that $\Phi \cup \overline{\Phi} = G$ and $\Phi \cap \overline{\Phi} = \emptyset$.*

DEFINITION 2.3 (CM type of an absolutely simple CM abelian variety). *Let A/K be an absolutely simple abelian variety, admitting complex multiplication (over $\overline{K}$) by the field E. The tangent space at the identity of $A_{\overline{K}}$ is a $\overline{K}$-module and an E-module, and the two actions are compatible: it follows that this tangent space is a $(E \otimes \overline{K})$-bimodule, so it decomposes as $T_{\mathrm{id}} A_{\overline{K}} \cong \prod_{\varphi \in \Phi} \overline{K}_\varphi$, where $\overline{K}_\varphi$ is a 1-dimensional $\overline{K}$-vector space on which E acts through the embedding $\varphi : E \hookrightarrow \overline{K}$, and Φ is a subset of $\mathrm{Hom}(E, \overline{K})$ of cardinality g. The set Φ of embeddings that appear in this decomposition is a CM type for E, and we say that A admits complex multiplication by the CM type (E, Φ).*

EXAMPLE 2.4. Consider for example the Jacobian J of the curve $C : \ y^2 = x^5 + 1$. Identifying the tangent space V to J at the identity to the dual of $H^0(J, \Omega^1_J) \cong H^0(C, \Omega^1_C) = \langle \frac{dx}{y}, \frac{x\,dx}{y} \rangle$, one sees that the action of ζ_5 on V is given by

$$\zeta^* \frac{dx}{y} = \zeta \frac{dx}{y}, \quad \zeta^* \frac{x\,dx}{y} = \zeta^2 \frac{dx}{y},$$

hence (taking the duality into account) the two nontrivial embeddings $\mathbb{Q}(\zeta_5) \hookrightarrow \overline{\mathbb{Q}}$ that appear in the CM type of A are those characterised by $\zeta_5 \mapsto \zeta_5^{-1}, \zeta_5 \mapsto \zeta_5^{-2}$.

DEFINITION 2.5 (Reflex type). *The* ***reflex type*** *of a CM type Φ on the CM field E is a pair (E^*, Φ^*) defined as follows.*

1. *the field E^* is the fixed field of $\{\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) : \sigma\Phi = \Phi\}$*
2. *the type Φ^* is obtained as follows. Let L be the Galois closure of E, $G = \mathrm{Gal}(L/\mathbb{Q})$ and $H = \mathrm{Gal}(L/E)$. Then one may identify $\mathrm{Hom}(E, \overline{\mathbb{Q}})$ with the quotient $H \setminus G$, and the CM type Φ for E lifts naturally to a CM type Φ_L for L. Let Φ_L^* be the CM type given by $\{\phi^{-1} : \phi \in \Phi_L\}$. Then Φ_L^* is induced from a unique CM type Φ^* on E^*, called the* ***reflex type****.*

THEOREM 2.6. *Let A/K be an abelian variety of CM type, with CM defined over K. Then the reflex field E^* is contained in K.*

The proof is essentially immediate: if the action of complex multiplication is defined over K, then $\mathrm{Gal}\left(\overline{K}/K\right)$ preserves the characters showing up in $T_0(A)$ (considered as a representation of the CM field E), hence for every $\sigma \in \mathrm{Gal}\left(\overline{K}/K\right)$ we have $\sigma\Phi = \Phi$, that is, $\mathrm{Gal}\left(\overline{K}/K\right)$ fixes the reflex field of (E, Φ).

DEFINITION 2.7. *Given a CM field E and a CM type Φ, we define the* ***reflex norm associated with*** *Φ to be the map*

$$\begin{array}{rccc} N_\Phi : & (E^*)^\times & \to & E^\times \\ & x & \mapsto & \prod_{\phi \in \Phi^*} \phi(x) \end{array}$$

[2] *complex conjugation* is not well-defined on $\overline{\mathbb{Q}}$, but it can be shown that any determination of complex conjugation will induce the same automorphism on the Galois closure of a CM field

One can show that N_Φ is well-defined, in the sense that $N_\Phi((E^*)^\times)$, which is a priori only a subset of $\overline{\mathbb{Q}}^\times$, is in fact contained in $E^\times$.

EXAMPLE 2.8. We continue with the field $E = \mathbb{Q}(\zeta_5)$ and the CM type corresponding to the embeddings $\zeta_5 \mapsto \zeta_5^3$, $\zeta_5 \mapsto \zeta_5^4$. Since $E/\mathbb{Q}$ is Galois, one sees that the reflex field is E itself, while the reflex type is given by the two embeddings that send $\zeta_5 \mapsto \zeta_5$, $\zeta_5 \mapsto \zeta_5^2$. The reflex norm is therefore

$$N_\Phi(a_0 + a_1\zeta_5 + a_2\zeta_5^2 + a_3\zeta_5^3) = (a_0 + a_1\zeta_5 + a_2\zeta_5^2 + a_3\zeta_5^3)(a_0 + a_1\zeta_5^2 + a_2\zeta_5^4 + a_3\zeta_5)$$

We are finally ready to describe the map ψ_ℓ which, by the results described above, is (essentially) the representation $\rho_{\ell\infty}$:

DEFINITION 2.9. *We define ψ_ℓ to be the composition of N_{K/E^*} with the reflex norm $N_\Phi : E^* \to E$. Here N_{K/E^*} is the norm from $K \otimes \mathbb{Q}_\ell$ to $E^* \otimes \mathbb{Q}_\ell$, which makes sense because by theorem 2.6 the field E^* is contained in K, and N_Φ is the reflex norm corresponding to the CM type of A.*

We finish with one last example: the determination of the reflex type in a non-Galois case.

EXAMPLE 2.10. Consider the field $E = \mathbb{Q}[x]/(x^4+13x^2+41)$. This is a quartic CM field with totally real subfield equal to $\mathbb{Q}(\sqrt{5})$. The extension $E/\mathbb{Q}$ is not Galois, and its Galois closure L is given by $\mathbb{Q}\left(\pm i\sqrt{\frac{1}{2}\left(13 \pm \sqrt{5}\right)}\right)$. The Galois group of L over $\mathbb{Q}$ is isomorphic do D_4 and is generated by two elements, s of order 2 (with fixed field E), and r of order 4 (with fixed field $\mathbb{Q}(\sqrt{205})$). Complex conjugation in $\mathrm{Gal}(L/\mathbb{Q})$ is given by r^2, whose fixed field (i.e. the maximal totally real subfield of L) is generated by a root of $x^4 - 15x^3 + 48x^2 - 15x + 1$. A CM type for E is given by a subset of $\mathrm{Hom}(E, L) = \mathrm{Gal}(L/\mathbb{Q})/\mathrm{Gal}(L/E) = \langle r, s\rangle/\langle s\rangle$. We consider the CM type $\Phi = \{\mathrm{id}\,\mathrm{Gal}(L/E), r\,\mathrm{Gal}(L/E)\}$. There are 4 elements in $\mathrm{Gal}(L/\mathbb{Q})$ that map to Φ under restriction, namely $\Phi_L = \{\mathrm{id}, s, r, rs\}$. Their inverses are given by $\Phi_L^* = \{\mathrm{id}, s, r^{-1}, rs\}$. We now describe the reflex field: we need to study the group

$$\mathrm{Gal}(L/E^*) = \{g \in \mathrm{Gal}(L/\mathbb{Q}) : g\Phi_L = \Phi_L\}.$$

Notice that $\mathrm{Gal}(L/E^*)$ is contained in Φ_L (indeed, for every $g \in \mathrm{Gal}(L/E^*)$ we must have $g \cdot \mathrm{id} \in \Phi_L$, hence $g \in \Phi_L$). It's clear that r, s do not belong to $\mathrm{Gal}(L/E^*)$, but rs does: indeed $rs \cdot \{\mathrm{id}, s, r, rs\} = \{rs, r, rsr, \mathrm{id}\} = \{rs, r, s, \mathrm{id}\}$. It follows that the reflex field E^* is the field fixed by rs (which is isomorphic to $\mathbb{Q}[x]/(x^4 + 19x^2 + 80)$), with CM type induced by Φ_L^*. Notice that

$$\begin{aligned}\mathrm{Hom}(E^*, L) &= \mathrm{Gal}(L/\mathbb{Q})/\mathrm{Gal}(L/E^*) = \langle r, s\rangle/\langle rs\rangle \\ &= \{\mathrm{id}\,\mathrm{Gal}(L/E^*), r\,\mathrm{Gal}(L/E^*), r^2\,\mathrm{Gal}(L/E^*), r^3\,\mathrm{Gal}(L/E^*)\}'\end{aligned}$$

and recall that the reflex type is given by those elements of this set that are restrictions of elements in Φ_L^*. It's immediate to see that id and rs belong to the same coset under the action of $\mathrm{Gal}(L/E^*)$, and the same is true for s and $r^{-1} = srs$, hence the reflex type Φ^* is given by $\Phi^* = \{\mathrm{id}\,\mathrm{Gal}(L/E^*), r^{-1}\,\mathrm{Gal}(L/E^*)\} = \{\mathrm{id}\,\mathrm{Gal}(L/E^*), r^3\,\mathrm{Gal}(L/E^*)\}$.

CHAPTER 4

Exercises

The division of exercises in "level 1" and "level 2" is entirely subjective. You are encouraged to look at all the exercises and spend some time thinking about a strategy; then choose your favourite problems and try to put your strategy in practice, possibly with the help of a computer.

1. Level 1 problems

EXERCISE 1.1 (Commutativity of abelian varieties, slightly different proof). Using the fact that the map $x \mapsto x^{-1}$ is algebraic, show that an abelian variety is commutative.

EXERCISE 1.2 (Uniqueness in Poincaré's theorem). Assume that $\mathrm{Aut}_K(A)$ is a finite group. Prove that the decomposition in Poincaré's theorem is unique (that is, there exist **unique** simple abelian subvarieties $A_1, \ldots, A_n$ of A such that the sum is an isogeny $A_1 \times \cdots \times A_n \to A$). Show with an example that uniqueness of the decomposition does not hold in general.

EXERCISE 1.3. Let $A \to B$ be a surjective homomorphism of abelian varieties. Prove that B is isogenous to a subvariety of A. Let $A \to B$ be an injective homomorphism: prove that there is a surjective homomorphism $B \to A$ (hence, up to isogeny, "homomorphisms of abelian varieties go in both directions").

EXERCISE 1.4. Prove the claim made in remark 4.11; more precisely, show that the kernel of $\lambda_H : A \to A^\vee$ has order $d(H)^2$.

EXERCISE 1.5. Prove that an abelian variety over $\mathbb{C}$ can never be embedded as a hypersurface in projective space unless it is an elliptic curve. Find an abelian surface (that is, an abelian variety of dimension 2) which can be embedded in $\mathbb{P}^8$.

Hint. It can be useful to apply the Lefschetz theorem.

EXERCISE 1.6. Show that the polarisation introduced in example 4.12 is indeed canonical (that is, it does not depend on our choice of representatives $1, \tau$ for the lattice).

EXERCISE 1.7. Compute the order of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ and compare it with that of $\mathrm{GL}_{2g}(\mathbb{F}_\ell)$.

EXERCISE 1.8. Let C/K be the hyperelliptic curve $y^2 = f(x)$, where $f(x)$ is a separable monic polynomial of degree 5 and K is a field not of characteristic 2. Describe a $\mathbb{F}_2$-basis for the $\mathbb{F}_2$-vector space $\mathrm{Jac}(C)[2](\overline{K})$. How does the answer change if $f(x)$ is not monic? How does it change if it has degree 6?

Hint. See exercise 2.3.

EXERCISE 1.9. Let C be the curve given by $y^2 = f(x)$ (with $f(x)$ separable of degree 5), and let ∞ be the point at infinity of C. Embed C into its Jacobian J via $P \mapsto [P - \infty]$. Let ι be the involution $\iota(x, y) = (x, -y)$ of C; as we have seen (proposition 9.22), ι induces an automorphism of J. Prove that this automorphism is multiplication by -1.

EXERCISE 1.10. Assume that A carries a polarisation of degree d (not necessarily equal to 1). What can be said on the image of Galois? Is it still contained in the general symplectic group?

Hint. A useful way to think about problems where isogenies are involved is the following: *in the category of abelian varieties up to isogeny*, A and $A^\vee$ are isomorphic. At the level of Tate modules, this implies (among other things) that $V_\ell(A)$ and $V_\ell(A^\vee)$ are isomorphic (notice that these are $\mathbb{Q}_\ell$-vector spaces and not $\mathbb{Z}_\ell$-modules, though!). In particular, a polarisation of *any* degree induces an alternating form on $V_\ell(A)$. And now you should try to work out what this implies for the Weil pairing $T_\ell(A) \times T_\ell(A^\vee) \to \mathbb{Z}_\ell(1)$...

EXERCISE 1.11. Find a genus 2 curve $C/\mathbb{Q}$ whose Jacobian has good reduction away from 2. Is it possible that $\mathbb{Q}(J[2]) = \mathbb{Q}$?

EXERCISE 1.12. Play the following game with a partner. Ask them to query the LMFDB for genus 2 curves with Sato-Tate group $G_{3,3}$ and with $\overline{\mathbb{Q}}$-simple Jacobian[1]. They choose such a curve C and tell you the equation; you need to guess the algebra $\mathrm{End}^0_{\mathbb{Q}}(\mathrm{Jac}(C))$. You are only allowed to compute characteristic polynomials of Frobenius – but of course you may use your favourite computer algebra system.

EXERCISE 1.13. Let $C/\mathbb{Q}$ be a curve of genus 2 with good reduction at p. Find a formula for the characteristic polynomial of the Frobenius at p in terms of $\#C(\mathbb{F}_p)$ and $\#C(\mathbb{F}_{p^2})$. Same question with $C/\mathbb{Q}$ of genus 3, using $\#C(\mathbb{F}_{p^3})$ as well as $\#C(\mathbb{F}_p)$, $\#C(\mathbb{F}_{p^2})$.

EXERCISE 1.14. Using remark 7.5, determine the torsion subgroup of $J(\mathbb{Q})$, where J is the Jacobian of $y^2 = x^5 + 1$.

EXERCISE 1.15. Prove that the group of rational points of the Jacobian of $y^2 = x^5 - x + 1$ has rank at least 1.

EXERCISE 1.16. Assuming theorem 6.1 prove proposition 6.5.

EXERCISE 1.17. Consider the curves $C_a : y^2 = x^5 - 2x^4 - x^3 - ax^2 + x$ for $a \in [1, 100] \cap \mathbb{N}$. Determine for which values of a in this range the abelian variety $J_a = \mathrm{Jac}(C_a)$ is $\mathbb{Q}$-simple.

EXERCISE 1.18. How many different CM types does a CM field E possess?

2. Level 2 problems

EXERCISE 2.1 (B. Poonen). If A is a g-dimensional principally polarised abelian variety over K with $\mathrm{End}_K(A) = \mathbb{Z}$, and G is a finite subgroup of A whose order n is not a g-th power, then $B := A/G$ is an abelian variety that admits no principal polarization. Show that the assumption on $\mathrm{End}_K(A)$ is necessary.

[1] these conditions are equivalent to the geometric endomorphism algebra of the Jacobian being a real quadratic field and to all the endomorphisms being defined over $\mathbb{Q}$

EXERCISE 2.2 (Serre's lifting lemma). In this exercise we describe a useful lemma, originally due to Serre, which allows one to deduce ℓ-adic information from mod-ℓ data.

(1) Let $\ell \geq 5$ and G be a closed subgroup of $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$. Suppose that the reduction of G modulo ℓ contains $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$: prove that G contains $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$. If we further assume that the reduction of G modulo ℓ is all of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, can we deduce that $G = \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$?
(2) Deduce that if $A/\mathbb{Q}$ is a principally polarised abelian variety such that $\mathrm{Im}\,\rho_\ell$ contains $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$, then $\mathrm{Im}\,\rho_{\ell^\infty} = \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$.
(3) Can you find similar statements that apply to other subgroups of GL_{2g}?

EXERCISE 2.3. Let K be a field of characteristic different from 2 and let $C : y^2 = \prod_{i=1}^{2g+1}(x - \alpha_i)$ be a hyperelliptic curve defined over K (with $\alpha_i \in \overline{K}$). Let $P_i = (\alpha_i, 0)$ and let ∞ denote the unique point at infinity of C. Show that $\{[P_i - \infty]\}_{i=1}^{2g}$ is a basis of $\mathrm{Jac}(C)[2]$. Compute, for all i, j, the Weil pairing between $[P_i - \infty]$ and $[P_j - \infty]$.

EXERCISE 2.4. Prove that the Jacobian of the curve $y^2 = x^8 + 3x^6 + x^4 + 3x^2 + 1$ splits up to isogeny as the product of three elliptic curves (try to keep your computations to a minimum).

EXERCISE 2.5. Let $J/\mathbb{Q}$ be the Jacobian of the curve $y^2 = x^5 + x + 1$. Determine $\#J(\mathbb{Q})_{\mathrm{tors}}$. Same question for the Jacobian of the curve $y^2 + y(x^3 + 1) = -x - 1$.

EXERCISE 2.6. Consider the curve $X_1(13) : y^2 + (x^3 + x + 1)y = x^5 + x^4$. Using information from the LMFDB if necessary, determine the size of the image of the Galois representation ρ_{19} attached to the Jacobian of $X_1(13)$. Can you also determine the image of ρ_{19} up to conjugacy?

Hint. This is a hard exercise; here is one way of doing it (which assumes all the information from the LMFDB):

(1) show that the order of G_{19} divides $6 \cdot 19 \cdot 18$
(2) prove that $\#G_{19}$ is divisible by $6 \cdot 18$
(3) observe that if $19 \nmid \#G_{19}$, then all the 19-torsion of J is defined over $\mathbb{Q}(\zeta_{13}, \zeta_{19})$
(4) use information coming from the reduction of J at $p = 1483$ to decide whether or not $19 \mid \#G_{19}$.

Note. This is a famous curve! Knowing the structure of $J(\mathbb{Q})_{\mathrm{tors}}[19]$ allowed Tate and Mazur [**MT74**] to prove that there are no elliptic curves over $\mathbb{Q}$ admitting a rational 13-torsion point.

EXERCISE 2.7. Consider a general hyperelliptic curve $C : y^2 = f(x)$ over $\mathbb{Q}$.

(1) Prove that C has good reduction at all primes that don't divide $2\,\mathrm{disc}(f(x))$.
(2) Show that for every prime p there exists an abelian surface $A/\mathbb{Q}$ with good reduction away from $2p$.

EXERCISE 2.8. Consider the curves

$$C_1 : y^2 + (x^3 + x^2 + x + 1)y = -12x^6 - 15x^5 + 9x^4 + 31x^3 + 9x^2 - 15x - 12$$

and

$$C_2 : y^2 + y = -x^6 - 9x^5 - 22x^4 + 3x^3 + 37x^2 - 24x + 4.$$

Let J_1, J_2 be the corresponding Jacobians. One can show that $J_1(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$ and $J_2(\mathbb{Q}) \cong \mathbb{Z}/15\mathbb{Z}$. However, for any prime p of good reduction of C_1, one has $\#J_1(\mathbb{F}_p) \equiv 0 \pmod 5$. Can you make a guess as to why this happens?

EXERCISE 2.9. Let $C/\mathbb{Q}$ be a genus 2 curve with good reduction away from 2.

(1) Prove that $J = \mathrm{Jac}(C)$ admits a rational 2-torsion point.
(2) What is the minimal order of $J(\mathbb{Q})_{\mathrm{tors}}$ for such a curve?

Hint. It might be possible to solve this problem without the help of a computer, but `https://hobbes.la.asu.edu/NFDB/` will probably come in handy.

EXERCISE 2.10. Let J be the Jacobian of the curve $C : y^2 = x^5 - x^4 - x^3 - x^2 + x - 1$. It is known that $\mathrm{End}_{\overline{\mathbb{Q}}}(J)$ is $\mathbb{Z}[\sqrt{2}]$. Prove that for $p \equiv 1, 3 \pmod 8$ the characteristic polynomial of the Frobenius at p is of the form $t^4 + 2at^2 + p^2$ for some integer a (it may be useful to consult [**FKRS12**]).

EXERCISE 2.11. Consider the Jacobian $J/\mathbb{Q}$ of the curve $y^2 + y = x^5 - 2x^4 + 2x^3 - x^2$. Determine for which primes ℓ there is a $\mathbb{Q}$-rational isogeny of degree ℓ from J to another abelian variety.

Hint. Here is a possible way to attack this problem:

(1) Assume that $J[\ell]$ admits a cyclic submodule $H \cong \mathbb{F}_\ell$ which is stable under Galois. This induces a character $\psi : \mathrm{Gal}\left(\overline{K}/K\right) \to \mathrm{Aut}(H) \cong \mathbb{F}_\ell^\times$ which is unramified outside ℓ and the primes of bad reduction of J.
(2) Show that $\psi = \varepsilon\chi_\ell^i$, where ε is ramified at most at the primes of bad reduction of J and $i \in 0, 1$ (you will need theorem 9.1).
(3) It follows (why?) that the conductor of ρ_ℓ is divisible by $\mathrm{cond}(\varepsilon)^2$.
(4) In the case at hand, this implies that ε is trivial.
(5) Hence we have that for every p of good reduction the characteristic polynomial of $\rho_\ell(\mathrm{Frob}_p)$ (which is just the reduction modulo ℓ of $f_p(t)$) has a root of the form $\chi_\ell(\mathrm{Frob}_p)^i$ for some $i = 0, 1$. Moreover, $\chi_\ell(\mathrm{Frob}_p)^i \equiv p^i \pmod \ell$.
(6) This should be enough to reduce the problem to a finite list of cases.

EXERCISE 2.12. Let A/K be an abelian variety over a field of characteristic 0. Let $R = \mathrm{End}_K(A)$, $D = \mathrm{End}_K^0(A)$, and let S be an order in D that contains R. Prove that A is K-isogenous to a K-abelian variety B such that $\mathrm{End}_K(B) = S$.

EXERCISE 2.13 (Silverberg [**Sil92**]). Let A, B be abelian varieties over a field K of characteristic 0. Let $N \geq 3$ be a positive integer and let $L = K(A[N], B[N])$. The purpose of this exercise is to show that the action of $\mathrm{Gal}\left(\overline{L}/L\right)$ on $\mathrm{Hom}_K(A, B)$ is trivial, or, in other words, that all the $\overline{K}$-homomorphisms from A to B are defined over L. Let $\Lambda := \mathrm{Hom}_{\overline{K}}(A, B)$.

You will need the following lemma: for every r and $N \geq 3$, $\mathrm{GL}_r(\mathbb{Z}) \to \mathrm{GL}_r(\mathbb{Z}/N\mathbb{Z})$ is injective on finite subgroups.

(1) Suppose G is a finite group, Λ is a $\mathbb{Z}[G]$-module which is a finitely generated free $\mathbb{Z}$-module, and N is an integer greater than 2. If $\sigma \in G$ and $(\sigma - 1)\Lambda \subseteq N\Lambda$, then $g(\lambda) = \lambda$ for every $\lambda \in \Lambda$.
(2) Let $H = \{\sigma \in \mathrm{Gal}\left(\overline{K}/K\right) : \sigma(\lambda) = \lambda \quad \forall \lambda \in \Lambda\}$ and
$$H_N := \{\sigma \in \mathrm{Gal}\left(\overline{K}/K\right) : (\sigma - 1)(\lambda) \in N\Lambda \quad \forall \lambda \in \Lambda\}.$$
Let F_N be the fixed field of H_N. Prove that $H_N = H$ and that every element of Λ is defined over H_N.
(3) Let K_N be the fixed field of
$$\{\sigma \in \mathrm{Gal}\left(\overline{K}/K\right) : \sigma(\lambda) = \lambda \quad \forall \lambda \in \mathrm{Hom}(A[N], B[N])\}.$$
Prove that F_N is contained in K_N.
(4) Deduce the theorem.

Exercise 2.14. Let $C/\mathbb{Q}$ be the curve given by the equation $y^2 = x^5 + 1$ and let $J/\mathbb{Q}$ be its Jacobian. Determine, for every prime $p > 5$ with $p \not\equiv 1 \pmod 5$, the number of $\mathbb{F}_p$-points of J. Equivalently, determine the number of $\mathbb{F}_p$- and $\mathbb{F}_{p^2}$-points of the curve $y^2 = x^5 + 1$.

Hint. This can be a hard problem. Here is a sketch of solution:

(1) Reduce to working over $K = \mathbb{Q}(\zeta_5)$
(2) the only places of bad reduction of C are 2 and 5, hence the only places of bad reduction of C/K are contained in $\{2, 1 - \zeta_5\}$
(3) the conductor of C over $\mathbb{Q}(\zeta_5)$ is $2^4(1 - \zeta_5)^4$. This implies that φ_v (for $v = 2$ or $v = 1 - \zeta_5$) is trivial on the principal units.
(4) if $p \equiv -1 \pmod 5$ is written in the form $p = (a + b\omega)(a + b\omega^\sigma)$, where $\omega = \frac{-1+\sqrt{5}}{2}$ and σ is the generator of $\mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$, then $(a + b\omega) \equiv \pm 2 \pmod{1 - \zeta_5}$
(5) let c be the idèle whose v-component is 1 for all v, except for $v = a + b\omega$, where it takes the values $a+b\omega$. Then $\rho_\ell(c) = \rho_\ell(c')$, where c' is the idèle with v-component equal to $\frac{1}{a+b\omega}$ for $v \neq a + b\omega$ and $c'_{a+b\omega} = 1$. Now you are reduced to computing $\psi_\ell(a + b\omega)$ and $\varphi_v(\frac{1}{a+b\omega})$ for all v
(6) for $v = 2$, the algebraic number $a + b\omega$ has order dividing 3 in the residue field $\mathbb{F}_v$, hence its image via φ_v is trivial
(7) finally, for $v = 1 - \zeta_5$, the image in $\mathbb{F}_v \cong \mathbb{F}_5$ of $\frac{1}{a+b\omega}$ is ± 2, which is a generator of $\mathbb{F}_5^\times$. This should tell you the value of $\varphi_v(a + b\omega)$.
(8) putting everything together, you should now have a simple formula for the trace of Frob_p^2.

Exercise 2.15. In this exercise we consider the situation of example 1.18.

(1) Prove that T has minimal polynomial $T^2 - T - 1$ as claimed.
(2) Let A/K be an abelian surface such that $\mathrm{End}_K(A)$ is a (nonsplit) quaternion algebra. Prove that the reduction of A at any place of K (where it has good reduction) is the square of an elliptic curve. Use this fact to deduce that $\mathrm{End}_{\overline{\mathbb{Q}}}(J)$ is commutative.

(3) Prove that J is geometrically simple.
(4) Let A be the Jacobian of Z. Can you determine $\mathrm{End}_{\overline{\mathbb{Q}}}(A)$?
(5) Challenge (that has little to do with Galois representations): decompose $\mathrm{Jac}(Z) \sim \prod A_i^{n_i}$ up to isogeny over $\mathbb{Q}$, with the A_i absolutely simple. Choosing a suitable isogeny allows you to assume that each A_i is a Jacobian over $\mathbb{Q}$. Can you find equations for all the corresponding curves?

Hint (for parts (2) and (3)). Given an abelian surface $A/\mathbb{Q}$ there exists a Galois extension $L/\mathbb{Q}$ over which all the endomorphisms of A are defined and such that $\mathrm{Gal}(L/\mathbb{Q})$ has exponent dividing 12 (see [**FKRS12**], or deduce this fact from exercise 2.13).

Hint (for part (4)). It can be computationally difficult to determine characteristic polynomials of Frobenius for Z; here are the first three (there is bad reduction at 2):

(1) $p = 3$, $f_3(t) = (t^2 - t + 3)(t^2 + t + 3)(t^4 + 3t^3 + 7t^2 + 9t + 9)^2$
(2) $p = 5$, $f_5(t) = (t^2 - t + 5)(t^2 + t + 5)(t^4 + 2t^3 + 6t^2 + 10t + 25)^2$
(3) $p = 7$, $f_7(t) = (t^2 - 4t + 7)(t^2 + 2t + 7)(t^4 + 7t^3 + 25t^2 + 49t + 49)^2$

3. Projects

EXERCISE 3.1. Zarhin has proven [**Zar00**] the following remarkable theorem:

THEOREM 3.2 (Zarhin). *Let $f(x)$ be a separable polynomial of degree $n \geq 5$ with coefficients in a number field K. Let C be the hyperelliptic curve $y^2 = f(x)$, and suppose that the Galois group of $f(x)$ over K is either A_n or S_n. Then for the Jacobian J of C we have $\mathrm{End}_{\overline{K}}(J) = \mathbb{Z}$.*

The aim of this project is to find similar criteria which give information on $\mathrm{End}_{\overline{K}}(J)$ (or $\mathrm{End}_K(J)$) in terms of properties of the Galois group G of $f(x)$: here are two possible extensions for you to think about.

(1) are there assumptions on G (weaker than G containing A_n, of course) that ensure that J is geometrically irreducible?
(2) fix a (small) value of g and a proper subgroup H of A_n. Is there a polynomial $f_H(x)$ of degree n with Galois group H and such that the Jacobian J_H of $y^2 = f_H(x)$ has (geometrically) nontrivial endomorphism ring? If the answer is yes, then you have found an abelian variety with an 'interesting' Galois representation (nontrivial endomorphisms and prescribed structure on $J_H[2]$). If the answer is no, you have found a strengthening of Zarhin's theorem.

EXERCISE 3.3 (small torsion of non-hyperelliptic Jacobians). The purpose of this exercise is to investigate the geometry of torsion points of small order on Jacobians of non-hyperelliptic curves.

(1) Let C be a genus-3 non hyperelliptic curve, presented as a smooth plane quartic $F(X, Y, Z) = 0$. Can you describe the 2-torsion in $J = \mathrm{Jac}(C)$ in terms of the geometry of F? [This is known, but I'm not sure where to find it in the literature].

(2) Can you find a similar geometric description for a non-hyperelliptic genus 4 curve presented as the intersection of a quadric and a cubic in $\mathbb{P}^3$? [I haven't tried to solve this exercise].
(3) Can you find further interesting classes of curves C for which some of the groups $\mathrm{Jac}(C)[\ell]$ are easy to describe in geometric terms?

EXERCISE 3.4 (A surjectivity criterion in genus 2). As described in Sara's lectures on elliptic curves, there is a surjectivity criterion for Galois representations attached to elliptic curves (due to Serre) which reads as follows:

THEOREM 3.5 (Serre). *Let E be an elliptic curve over a number field K. Let $p \geq 5$ be a prime number and let G_p be the image of the representation ρ_p attached to E. Suppose that G_p contains:*

(1) *an element g such that $\mathrm{tr}(g) \neq 0$ and $\mathrm{tr}(g)^2 - 4\det(g)$ is a nonzero square in $\mathbb{F}_p^\times$*
(2) *an element g' such that $\mathrm{tr}(g') \neq 0$ and $\mathrm{tr}(g')^2 - 4\det(g')$ is not a square in $\mathbb{F}_p^\times$*
(3) *an element g'' such that $u := \mathrm{tr}(g'')^2/\det(g'')$ satisfies $u \neq 0, 1, 2, 4$ and $u^2 - 3u + 1 \neq 0$*

Then G_p contains $\mathrm{SL}_2(\mathbb{F}_p)$. In particular, if p is unramified in K, then $G_p = \mathrm{GL}_2(\mathbb{F}_p)$.

Can you find a similar criterion for abelian surfaces (the classification of proper subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ given in [**Lom16**] might be useful)?

EXERCISE 3.6 (Prime values of some quadratic polynomials). Consider the elliptic curve $E : y^2 = x^3 + x$ over the field $\mathbb{Q}$. Let $p \equiv 1 \pmod 4$ be a prime number; it is well-known that p can be written as $p = a^2 + b^2$ in an essentially unique[2] way.

(1) Compute the trace of the Frobenius at p in terms of a and b.
(2) Notice that whenever the trace of the Frobenius at p is ± 2 the prime number p is of the form $x^2 + 1$ (and recall that it is not known whether there exist infinitely many primes of this form).
(3) Google the Lang-Trotter conjecture (a good reference for the purposes of this project is [**BJ09**]). Combined with the previous remarks, what does the Lang-Trotter conjecture imply on the distribution of primes p of the form $x^2 + 1$?
(4) Can you derive the same prediction from analytic number theory, without resorting to the theory of elliptic curves?
(5) Apply the same argument to other CM elliptic curves over $\mathbb{Q}$. What are the corresponding predictions about the prime values taken by certain quadratic polynomials?
(6) Can you support these predictions by analytic arguments and/or with numerical experiments?
(7) ($\star$) Can you find a higher-dimensional analogue of these heuristics? (That is, can you make similar predictions by looking at CM abelian varieties of dimension 2 or more?)

[2]that is, up to exchanging a and b and to a choice of signs

Bibliography

[Alb34] A. A. Albert. A solution of the principal problem in the theory of Riemann matrices. *Ann. Math. (2)*, 35(3):500–515, July 1934.

[Alb35] A. A. Albert. On the construction of Riemann matrices. II. *Ann. Math. (2)*, 36(2):376–394, April 1935.

[BJ09] Stephan Baier and Nathan Jones. A refined version of the Lang-Trotter conjecture. *Int. Math. Res. Not. IMRN*, (3):433–461, 2009.

[BL04] C. Birkenhake and H. Lange. *Complex Abelian Varieties*. Springer, 2004.

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.

[CF96] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2*, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996.

[CM96] Daniel Coray and Constantin Manoil. On large Picard groups and the Hasse principle for curves and $K3$ surfaces. *Acta Arith.*, 76(2):165–189, 1996.

[Con04] Brian Conrad. Polarisations. Notes available at `http://math.stanford.edu/~conrad/vigregroup/vigre04/polarization.pdf`, 2004.

[Del74] Pierre Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.

[EMvG] B. Edixhoven, B. Moonen, and B. van Geemen. *Abelian varieties*. Draft. Available at `https://www.math.ru.nl/~bmoonen/research.html#bookabvar`.

[Fal83] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[FKRS12] Francesc Fité, Kiran S. Kedlaya, Víctor Rotger, and Andrew V. Sutherland. Sato-Tate distributions and Galois endomorphism modules in genus 2. *Compos. Math.*, 148(5):1390–1442, 2012.

[Fon85] J-M. Fontaine. Il n'y a pas de variété abélienne sur $\mathbf{Z}$. *Invent. Math.*, 81(3):515–538, 1985.

[Gon98] Josep González. On the p-rank of an abelian variety and its endomorphism algebra. *Publ. Mat.*, 42(1):119–130, 1998.

[GR14] É. Gaudron and G. Rémond. Polarisations et isogénies. *Duke Math. J.*, 163(11):2057–2108, 2014.

[GRR72] A. Grothendieck, M. Raynaud, and D.S. Rim. *Groupes de monodromie en géométrie algébrique. I.* Lecture Notes in Mathematics, Vol. 288. Springer-Verlag, Berlin-New York, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim.

[Hal11] C. Hall. An open-image theorem for a general class of abelian varieties. *Bull. Lond. Math. Soc.*, 43(4):703–711, 2011. With an appendix by Emmanuel Kowalski.

[KM16] A. Kumar and R. E. Mukamel. Real multiplication through explicit correspondences. *LMS J. Comput. Math.*, 19(suppl. A):29–42, 2016.

[Lom16] D. Lombardo. Explicit surjectivity for Galois representations attached to abelian surfaces and GL_2-varieties. *Journal of Algebra*, 460C:26–59, 2016.

[Mil12] Milne, J.S. Abelian varieties. *Available online at* `http://www.jmilne.org/math/CourseNotes/AV.pdf`, 2012.

[MS16] Jan Steffen Müller and Michael Stoll. Canonical heights on genus-2 Jacobians. *Algebra Number Theory*, 10(10):2153–2234, 2016.

[MT74] B. Mazur and J. Tate. Points of order 13 on elliptic curves. *Invent. Math.*, 22:41–49, 1973/74.

[Mum70] D. Mumford. Abelian varieties. In *Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research*, 1970.

[MW93] D. Masser and G. Wüstholz. Isogeny estimates for abelian varieties, and finiteness theorems. *Ann. of Math. (2)*, 137(3):459–472, 1993.

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

[Ray66] Michel Raynaud. Modèles de Néron. *C. R. Acad. Sci. Paris Sér. A-B*, 262:A345–A347, 1966.

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

[Shi63] G. Shimura. On analytic families of polarized Abelian varieties and automorphic functions. *Ann. of Math*, 78(1):149–192, 1963.

[Sil92] A. Silverberg. Fields of definition for homomorphisms of abelian varieties. *J. Pure Appl. Algebra*, 77(3):253–262, 1992.

[ST61] Goro Shimura and Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan*. The Mathematical Society of Japan, Tokyo, 1961.

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

[Sta18] The Stacks project authors. The stacks project. `http://stacks.math.columbia.edu`, 2018.

[Sto17] M. Stoll. An explicit theory of heights for hyperelliptic Jacobians of genus three. *ArXiv e-prints*, January 2017.

[Tat66] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[Wat69] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969.

[WM71] W. C. Waterhouse and J. S. Milne. Abelian varieties over finite fields. In *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, pages 53–64. Amer. Math. Soc., Providence, R.I., 1971.

[Zar00] Yu. G. Zarhin. Hyperelliptic Jacobians without complex multiplication. *Math. Res. Lett.*, 7(1):123–132, 2000.