# NOTES ON ABELIAN VARIETIES [PART I]

TIM DOKCHITSER

## Contents

1. Affine varieties ........................................ 2
2. Affine algebraic groups .................................. 5
3. General varieties ........................................ 9
4. Complete varieties ...................................... 10
5. Algebraic groups ......................................... 13
6. Abelian varieties ......................................... 16
7. Abelian varieties over $\mathbb{C}$ ...................... 17
8. Isogenies and endomorphisms of complex tori ........ 20
9. Dual abelian variety ...................................... 22
10. Differentials ............................................ 24
11. Divisors .................................................. 26
12. Jacobians over $\mathbb{C}$ ................................ 27
1. **Affine varieties**

We begin with varieties defined over an algebraically closed field \( k = \overline{k} \).

By *Affine space* \( \mathbb{A}^n_k \) we understand the set \( k^n \) with Zariski topology: \( V \subset \mathbb{A}^n \) is closed if there are polynomials \( f_i \in k[x_1, \ldots, x_n] \) such that

\[
V = \{ x \in k^n \mid \text{all } f_i(x) = 0 \}.
\]

Every ideal of \( k[x_1, \ldots, x_n] \) is finitely generated (it is Noetherian), so it does not matter whether we allow infinitely many \( f_i \) or not. Clearly, arbitrary intersections of closed sets are closed; the same is true for finite unions: \( \{ f_i = 0 \} \cup \{ g_j = 0 \} = \{ f_ig_j = 0 \} \). So this is indeed a topology.

A closed nonempty set \( V \subset \mathbb{A}^n \) is an *affine variety* if it is irreducible, that is one cannot write \( V = V_1 \cup V_2 \) with closed \( V_i \subsetneq V \). Equivalently, in the topology on \( V \) induced from \( \mathbb{A}^n \), every non-empty open set is dense (Exc 1.1). Any closed set is a finite union of irreducible ones.

**Example 1.1.** A hypersurface \( V : f(x_1, \ldots, x_n) = 0 \) in \( \mathbb{A}^n \) is irreducible precisely when \( f \) is an irreducible polynomial.

**Example 1.2.** The only proper closed subsets of \( \mathbb{A}^1 \) are finite, so \( \mathbb{A}^1 \) and points are its affine subvarieties.

**Example 1.3.** The closed subsets in \( \mathbb{A}^2 \) are \( \emptyset, \mathbb{A}^2 \) and finite unions of points and of irreducible curves \( f(x, y) = 0 \).

With topology induced from \( \mathbb{A}^n \), a closed set \( V \) becomes a topological space on its own right. In particular, we can talk of its subvarieties (irreducible closed subsets). The Zariski topology is very coarse; for example, every two irreducible curves in \( \mathbb{A}^2 \) have cofinite topology, so they are homeomorphic. So to characterise varieties properly, we put them into a category. A map of closed sets

\[
\phi : \mathbb{A}^n \supset V \rightarrow W \subset \mathbb{A}^m
\]

is a *morphism* (also called a *regular map*) if it can be given by \( x \mapsto (f_i(x)) \) with \( f_1, \ldots, f_m \in k[x_1, \ldots, x_n] \). Morphisms are continuous, by definition of Zariski topology. We say that \( \phi \) is an isomorphism if it has an inverse that is also a morphism, and we write \( V \cong W \) in this case.

A morphism \( f : V \rightarrow \mathbb{A}^1 \) is a *regular function* on \( V \), so it is simply a function \( V \rightarrow k \) that can be given by a polynomial in \( n \) variables. The regular functions on \( V \subset \mathbb{A}^n \) form a ring, denoted \( k[V] \), and clearly

\[
k[V] \cong k[x_1, \ldots, x_n]/I, \quad I = \{ f \mid f|_V = 0 \}.
\]

Composing a morphism \( \phi : V \rightarrow W \) with a regular function on \( W \) gives a regular function on \( V \), so \( f \) determines a ring homomorphism \( \phi^* : k[W] \rightarrow k[V] \), the *pullback* of functions. Conversely, it is clear that every \( k \)-algebra homomorphism \( k[W] \rightarrow k[V] \) arises from a unique \( f : V \rightarrow W \). In other words, \( V \rightarrow k[V] \) defines an anti-equivalence of categories

Zariski closed sets \( \rightarrow \) finitely generated \( k \)-algebras with no nilpotents.
In particular, the ring of regular functions determines $V$ uniquely.

Now suppose $V$ is a variety. Then $k[V]$ is an integral domain (Exc 1.3), and the (anti-)equivalence becomes

affine varieties over $k \longrightarrow$ integral finitely generated $k$-algebras.

The field of fractions of $k[V]$ is called the field of rational functions $k(V)$. Generally,

$$\phi : \mathbb{A}^n \supset V \leadsto W \subset \mathbb{A}^m$$

is a rational map if it can be given by a tuple $(f_1, \ldots, f_m)$ of rational functions $f_i \in k(x_1, \ldots, x_n)$ whose denominators do not vanish identically on $V$. In other words, the set of points where $\phi$ is not defined is a proper closed subset of $V$, equivalently $\phi$ is defined on a non-empty (hence dense) open.

So rational functions $f \in k(V)$ are the same as rational maps $V \leadsto \mathbb{P}^1$.

**Example 1.4.** The ring of regular functions on $\mathbb{A}^n$ is $k[\mathbb{A}^n] = k[x_1, \ldots, x_n]$, and $k(\mathbb{A}^n) = k(x_1, \ldots, x_n)$

It is important to note that the image of a variety under a morphism is not in general a variety: $^1$

**Example 1.5.** The first projection $p : \mathbb{A}^2 \to \mathbb{A}^1$ takes $xy = 1$ to $\mathbb{A}^1 \setminus \{0\}$, which is not closed in $\mathbb{A}^1$.

**Example 1.6.** The map $\mathbb{A}^2_{x,y} \xrightarrow{(xy, y)} \mathbb{A}^2_t$ has image $\mathbb{A}^2 \setminus \{x\text{-axis} \} \cup \{(0, 0)\}$.

The first example can be given a positive twist, in a sense that it actually gives $U = \mathbb{A}^1 \setminus \{0\}$ a structure of an affine variety. Generally, for a rational map $\phi : V \leadsto V'$ and $U \subset V$ open, say that $\phi$ is regular on $U$ if it is defined at every point of $U$. (For $U = V$ it coincides with the notion of a regular map as before.) If $\phi$ has a regular inverse $\psi : V' \to V$ with $\psi(V') \subset U$, we can think of $U$ as an affine variety isomorphic to $V'$. In the example above take $V' : xy = 1$ with $\phi(t) = (t, t^{-1})$ and $\psi(x, y) = t$.

**Example 1.7.** If $V \subset \mathbb{A}^n$ is a hypersurface $f(x_1, \ldots, x_n) = 0$, then the complement $U = \mathbb{A}^n \setminus V$ has a structure of an affine variety with the ring of regular functions $k[x_1, \ldots, x_n, 1/f]$.

Many properties of $V$ have a ring-theoretic interpretation. Two very important ones are:

The dimension $d = \dim V$ is the length of a longest chain of subvarieties

$$\emptyset \subset V_0 \subset \cdots \subset V_d \subset V.$$  

(For $k = \mathbb{C}$ this agrees with the usual dimension of a complex manifold.) With $k[V_i] = k[x_1, \ldots, x_n]/P_i$, this becomes the length of a longest chain of prime ideals $k[V] \supset P_0 \supset \cdots \supset P_d = \{0\}$.

$^1$What is true is that the image $f(X) \subset Y$ always contains a dense open subset of the closure $\overline{f(X)}$ ([?] Exc II.3.19b).
which is by definition the ring-theoretic dimension of the ring $k[V]$. For a variety $V$ it is, equivalently, the transcendence degree of the field $k(V)$ over $k$.

**Example 1.8.** $\dim \mathbb{A}^n = \dim k[x_1, \ldots, x_n] = n$.

**Example 1.9.** A hypersurface $H \subset \mathbb{A}^n$ has dimension $n-1$.

Let $V$ be a variety and $x \in V$ a point. A regular function on $V$ may be evaluated at $x$, and the kernel of this evaluation map $k[V] \to k$ is a maximal ideal. (Conversely, every maximal ideal of $k[V]$ is of this form.) The local ring $O_x = O_{V,x}$ is the localisation of $k[V]$ at this ideal. In other words,

$$O_x = \left\{ \frac{f}{g} \in k(V) \mid f, g \in k[V], g(x) \neq 0 \right\}$$

This is a local ring, and its maximal ideal $m_x$ is the set of rational functions that vanish at $x$.

Write $d = \dim V$. We say that $x \in V$ is non-singular if, equivalently,

1. $\dim_k \frac{m_x}{m_x^2} = n - d$. (‘$\geq$’ always holds.)
2. the completion $\hat{O}_x = \lim O_x/m_x^d$ is isomorphic to $k[[t_1, \ldots, t_d]]$ over $k$.
3. If $V$ is given by $f_1 = \ldots = f_n = 0$, the matrix $(\frac{\partial f_i}{\partial x_j}(x))_{i,j}$ has rank $d$.

We say that $V$ is regular (or non-singular) if every point of it is non-singular. Generally, a morphism $f : V \to W$ is smooth of relative dimension $n$ if for all points $f(x) = y$ the pullback of functions $f^* : O_x \leftarrow O_y$ identifies

$$\hat{O}_x \leftarrow f^* \hat{O}_y \cong O_x[[t_1, \ldots, t_n]].$$

So $V$ is regular if and only if $V \to \{\text{pt}\}$ is smooth and, in general, a smooth morphism has regular fibres (preimages of points).

**Example 1.10.** The curves $C_1 : y = x^2$ and $C_2 : y^2 + x^2 = 1$ in $\mathbb{A}^2$ are non-singular, and $C_3 : y^2 = x^3$ and $C_4 : y^2 = x^3 + x^2$ are singular at $(0, 0)$.

It follows from (3) that the set of non-singular points $V_{ns} \subset V$ is open (Exc 1.5), and it turns out it is always non-empty ([? Thm. I.5.3]); in particular, it is dense in $V$.

Finally, there are products in the category of varieties, and they correspond to tensor products of $k$-algebras. In other words, if $V \subset \mathbb{A}^m$ and $W \subset \mathbb{A}^n$ are closed sets (resp. varieties) then so is $V \times W \subset \mathbb{A}^m \times \mathbb{A}^n = \mathbb{A}^{m+n}$, and $k[V \times W] \cong k[V] \otimes_k k[W]$.

Exc 1.1. A topological space is irreducible if and only if every non-empty open set is dense.

Exc 1.2. Zariski topology on $\mathbb{A}^2 = \mathbb{A}^1 \times \mathbb{A}^1$ is not the product topology.

Exc 1.3. Prove that the ring of regular functions $k[V]$ of an affine variety $V$ is an integral domain.

Exc 1.4. Take the curves $C : y^2 = x^3$, $D : y^2 = x^3 + x^2$ and $E : y^2 = x^3 + x$ in $\mathbb{A}^2$, and the point $p = (0, 0)$ on them. Prove that $\hat{O}_{C,p} \cong k[[t^2, t^3]]$, $\hat{O}_{D,p} \cong k[[s, t]]/st$, $\hat{O}_{E,p} \cong k[[t]]$, and that they are pairwise non-isomorphic.
Exc 1.5. Suppose $V$ is given by $f_1 = \ldots = f_n = 0$. Looking at the determinants of the minors of the matrix $\frac{\partial f_i}{\partial x_j}$, prove that the set of singular points of $V$ is closed in $V$.

2. AFFINE ALGEBRAIC GROUPS

In the same way as topological groups (Lie groups, ...) are topological spaces (manifolds, ...) that happen to have a group structure, affine algebraic groups are simply closed affine sets with a group structure.

**Definition 2.1.** A group $G$ is an affine algebraic group over $k$ if it has a structure of a Zariski closed set in some $\mathbb{A}^n_k$, and multiplication $G \times G \to G$ and inverse $G \to G$ are morphisms.

Equivalently, starting with a closed set $V \subset \mathbb{A}^n$ instead, we require

1. A point $e \in V$ (unit element),
2. A morphism $m : V \times V \to V$ (multiplication),
3. A morphism $i : V \to V$ (inverse),

which satisfy the usual group axioms

**Example 2.2.**

1. The additive group $\mathbb{G}_a = \mathbb{A}^1$, group operation $(x, y) \mapsto x + y$.
2. The multiplicative group $\mathbb{G}_m = \mathbb{A}^1 \setminus \{0\}$, group operation $(x, y) \mapsto xy$.

Recall that $\mathbb{A}^1 \setminus \{0\}$ is a variety via its identification with $\{xy = 1\} \subset \mathbb{A}^2$.

In this notation, multiplication becomes $(x_1, y_1), (x_2, y_2) \mapsto (x_1 x_2, y_1 y_2)$.

This example naturally generalises to $\text{GL}_n$ ($\text{GL}_1$ being $\mathbb{G}_m$):

**Example 2.3.** Write $M_n = \mathbb{A}^{n^2}$ for the set of $n \times n$-matrices over $k$, and $I_n \in M_n$ for the identity matrix. The classical groups

\[
\begin{align*}
\text{GL}_n &= \{A \in M_n \mid \det A \neq 0\}, \\
\text{SL}_n &= \{A \in M_n \mid \det A = 1\}, \\
\text{O}_n &= \{A \in M_n \mid A^t A = I_n\}, \\
\text{Sp}_{2n} &= \{A \in M_{2n} \mid A^t \Omega A = \Omega\} \quad (\Omega = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}).
\end{align*}
\]

are affine algebraic groups. This is clear for $G = \text{SL}_n, \text{O}_n, \text{Sp}_{2n}$, because the defining conditions are polynomial in the variables, so $G \subset \mathbb{A}^{n^2}$ is closed. As for $\text{GL}_n$, it is the complement to the hypersurface $\det(a_{ij}) = 0$, hence affine by Example 1.7 (cf. also Exc 2.1).

A homomorphism of affine algebraic groups is a morphism that is also a group homomorphism, an isomorphism is a homomorphism that has an inverse, and subgroups and normal subgroups will always refer the ones that are closed in Zariski topology. If $H \subset G$ is any ‘abstract’ subgroup, its Zariski closure is a subgroup in this sense (Exc 2.2).

\[\text{So } V \xrightarrow{(e, \text{id})} V \times V \xrightarrow{m} V \text{ is identity and same for } (\text{id}, e) \text{ (unit), } m \circ (m \times \text{id}) = m \circ (\text{id} \times m)\]

as maps $V \times V \times V \to V$ (associativity), and $V \xrightarrow{\text{diag}} V \times V \xrightarrow{(\text{id}, e)} V \times V \xrightarrow{m} V$ is constant $e$ (inverse).
It is clear that the product of two algebraic groups is an algebraic group, and that the kernel of a homomorphism $\phi : G_1 \to G_2$ is an algebraic group. It is also true that the image $\phi(G_1)$ is an algebraic group (Exc 2.3).

**Example 2.4.** The classical groups $G = SL_n, O_n, Sp_n$ are subgroups of $GL_n$, and the embeddings $G \hookrightarrow GL_n$ and the determinant map $G \to \mathbb{G}_m$ are homomorphisms.

For $g \in G$, the left translation-by-$g$ map $l_g : G \to G$ is an isomorphism. Because these maps act transitively on $G$, every point of $G$ \'looks the same\'. For instance, the irreducible components $G_{i, \text{ns}} \subset G_i$ is non-empty, $G_i$ is non-singular (use left translations again).

In particular, the connected component of identity $G^0 \subset G$ is a non-singular variety. It is a normal subgroup of $G$, and its left cosets are the connected components of $G$ (Exc 2.7). So $G/G^0$ is finite and $G = G^0 \times \Delta$ for some finite group $\Delta$. Thus it suffices to understand connected groups; the classical matrix groups are connected (Exc 2.8).

**Example 2.5.** Every finite group $G$ is an affine algebraic group, via the regular representation $G \subset \text{Aut} \ k[G] = GL_n$.

In particular, every finite affine algebraic group is a closed subgroup of some $GL_n$. (In fact, any faithful $k$-representation of $G$, not just the regular representation, defines such an embedding.) Somewhat surprisingly, it turns out that this is true for all affine algebraic groups:

**Theorem 2.6.** Every affine algebraic group $G$ is a closed subgroup of $GL_n$ for some $n$.

We will prove this, if only to illustrate that questions about affine varieties are really questions about $k$-algebras. First, some preliminaries are necessary.

An action of $G$ on a variety $V$ is a group action $\alpha : G \times V \to V$ which is a morphism. If $V = k^n$ and the action is linear (i.e. $\alpha_g : V \to V$ is in $GL_n(k)$ for all $g \in G$), we say that $V$ is a representation of $G$. Equivalently, it is a homomorphism $G \to GL_n$ of algebraic groups.

To prove the theorem, we need to find $\Sigma : G \to GL(V)$ whose corresponding ring map $\Sigma^* : k[GL(V)] \to A$ is surjective. (Then $\Sigma$ is an isomorphism of $G$ onto $\Sigma(G)$.) Putting aside the question of surjectivity, where can we possibly find a non-trivial representation in the first place?

Let us reformulate this on the level of the ring $A = k[G]$. Write\(^3\)

$$m^* : A \to A \otimes A, \quad i^* : A \to A, \quad e^* : A \to k$$

\(^3\)A $k$-algebra $A$ with such maps $m^*, i^*$ and $e^*$ that satisfy the axioms $(e^* \otimes id) \circ m^* = id$, $(id \otimes m^*) \circ m^* = (m^* \otimes id) \circ m^*$ and $(i^* \otimes id) \circ m^* = e^*$ (dual to the previous footnote) is called a Hopf algebra, and the maps comultiplication, counit and coinverse respectively.
for the ring maps corresponding to the multiplication \( m : G \times G \to G \), the inverse \( i : G \to G \) and the identity \( e : \{ \text{pt} \} \to G \). To give a representation \( \Sigma : G \to \text{GL}(V) \) is equivalent to specifying a \( k \)-linear map
\[
\sigma : V \to V \otimes A
\]
such that \((\text{id} \otimes e^*) \circ \sigma = \text{id} \) and \((\text{id} \otimes m^*) \circ \sigma = (\sigma \otimes \text{id}) \circ \sigma \). We say that \( \sigma \) makes \( V \) into an \( A \)-comodule.

There is only one obvious \( A \)-comodule, and that is \( V = A = k[G] \) itself with \( \sigma = m^* \), the co-multiplication map. The only problem is that \( k[G] \) is an infinite-dimensional \( k \)-vector space\(^4\), so what we need is the following

**Lemma 2.7.** Every finite-dimensional \( k \)-subspace \( W \subset A \) is contained in a finite-dimensional subcomodule \( V \subset A \) (so \( m^*(V) \subset V \otimes A \)).

**Proof.** A sum of subcomodules is again one, so we may assume \( V = \langle w \rangle \) is one-dimensional. Write \( m^*(w) = \sum_{i=1}^n v_i \otimes a_i \) with \( a_1, \ldots, a_n \) linearly independent over \( k \) and complete them to a \( k \)-basis \( \{a_i\}_{i \in I} \) of \( A \). We claim that \( V = \langle w, v_1, \ldots, v_n \rangle \) is a comodule.

Indeed, suppose \( m^*(a_i) = \sum c_{ijk} a_j \otimes a_k \). Then
\[
\sum m^*(v_i) \otimes a_i = (m^* \otimes \text{id})m^*(w) = (\text{id} \otimes m^*)m^*(w) = \sum v_i \otimes c_ij k a_j \otimes a_k
\]
in \( V \otimes A \). Comparing the coefficients of \( a_k \), we get \( m^*(v_k) = \sum v_i \otimes c_i j k a_j \), so \( m^*(V) \subset V \otimes A \). \( \square \)

**Proof of Theorem 2.6.** Pick some \( k \)-algebra generators of \( A = k[G] \), and let \( W \subset A \) be their \( k \)-span. Take an \( A \)-comodule \( W \subset V \subset A \) as in the lemma, and let \( v_1, \ldots, v_n \) be a \( k \)-basis of \( V \). The image of
\[
\Sigma^* : k[\text{GL}(V)] = k[x_{11}, \ldots, x_{nn}, 1/\det] \to A
\]
contains \( \sum_i e^*(v_i) \Sigma^*(x_{ij}) = (e^* \otimes \text{id})m^*(v_j) = v_j \), so \( \Sigma^* \) is surjective. \( \square \)

Note that the proof is completely explicit.

**Example 2.8.** Take \( G = \mathbb{G}_a \). Then \( A = k[G] = k[t] \) is generated by \( t \), so take \( W = \langle t \rangle \). The comultiplication
\[
m^* : k[t] \to k[t] \otimes k[t] \quad (\cong k[t_1, t_2])
\]
maps \( t \mapsto t \otimes 1 + 1 \otimes t = t_1 + t_2 \), so \( m^*(W) \not\subset W \otimes A \). In other words, \( W \) is not a comodule. But \( V = \langle 1, t \rangle \) is one (cf. proof of Lemma 2.7), and the corresponding embedding \( \mathbb{G}_a \to \text{GL}_2 \) is
\[
t \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.
\]

In view of Theorem 2.6, affine algebraic groups are also called *linear algebraic groups*. The statement of the theorem can even be refined so that a given \( H < G \) can be picked out as a stabiliser of some linear subspace:

\(^4\)unless \( G \) is finite, in which case the construction recovers Example 2.5
Theorem 2.9 (Chevalley). Let $H < G$ be a (closed) subgroup of an affine algebraic group $G$. There is a linear representation $G \to \text{GL}(V)$ and a linear subspace $W \subset V$ whose stabiliser is $H$.

**Proof.** Exc 2.10. 

Extending this further, one proves that if $H < G$ is normal, it is possible to find $V$ such that $H$ is precisely the kernel of $\phi : G \to \text{Aut} V$ (see [?], §16.3). The image $\phi(G)$ is then an algebraic group, so factor groups exist for algebraic groups. (In positive characteristic this factor group is not unique, because there are injective homomorphisms of algebraic groups that are not isomorphisms, see Exc 2.12; the question whether the quotient $G/H$ exists in the sense of category theory is subtle, see [?] §15–16.)

Exc 2.1. Write down explicitly the multiplication map and the inverse for $\text{GL}_2 \subset \mathbb{A}^5$.

Exc 2.2. Suppose $G$ is an algebraic group and $H \subset G$ is a subgroup in the 'abstract group sense'. Then its (Zariski) closure $\bar{H} \subset G$ is a subgroup in the algebraic group sense.

Exc 2.3. Show that the image of an algebraic group homomorphism is an algebraic group. (The image of a variety under a morphism is not always a variety, see Exc 3.5.)

Exc 2.4. (Closed orbit lemma) Suppose $G \times V \to V$ is an action of $G$ on a variety $V$, and let $U = Gv$ be an orbit. Then the closure $\bar{U} \subset V$ is a variety, $U \subset \bar{U}$ is open and non-singular, and $\bar{U} \setminus U$ is a union of orbits (of strictly smaller dimension). In particular, the orbits of minimal dimension are closed.

Exc 2.5. Let $G$ be an algebraic group and write $\text{Aut} G$ for the set of isomorphisms $G \to G$ (as algebraic groups). Determine $\text{Aut} G$ for $G = \mathbb{G}_a$ and $G = \mathbb{G}_m$. Does $\text{Aut} G$ have a structure of an algebraic group in these cases, and is it true that its action on $G$ is an algebraic group action?

Exc 2.6. If $G$ is connected and $H \triangleleft G$ is finite, then $H \subset Z(G)$, in particular $H$ is abelian.

Exc 2.7. Prove that the connected component of identity $G^0 \subset G$ is a normal subgroup and its left cosets are the connected components of $G$.

Exc 2.8. Show that the classical groups $\text{GL}_n, \text{SL}_n, \text{O}_n$ and $\text{Sp}_{2n}$ are connected.

Exc 2.9. Do Example 2.8 for $G = \mathbb{G}_m$.

Exc 2.10. Prove Theorem 2.9 (Modify the proof of Theorem 2.6.)

Exc 2.11. A character of $G$ is a 1-dimensional representation of $G$, equivalently a homomorphism $G \to \mathbb{G}_m$. Prove that characters are in 1-1 correspondence with invertible elements $x \in k[G]^\times$ such that $m^*(x) = x \otimes x$. What does the product of characters correspond to? Compute the character group for $G = \mathbb{G}_m$ and $G = \mathbb{G}_a$.

Exc 2.12. Let $G \subset \mathbb{A}^n$ be an affine algebraic group of dimension $> 0$ over $k = \overline{\mathbb{F}}_p$. Suppose $G$ is given by the equations $f_1(x_1, \ldots, x_n) = 0$. For a polynomial $f$ write $f^{(p)}$ for the polynomial whose coefficients are those of $f$ raised to the $p$th power. Prove that $G^{(p)} = \{ x | f^{(p)}(x) = 0 \}$ is also an algebraic group, and that the Frobenius map $F(x) = x^p$ is a homomorphism from $G$ to $G^{(p)}$. Prove that $F$ is bijective but not an isomorphism of algebraic groups.
3. General varieties

Recall that to define a topological ($C^\infty$, analytic, ...) manifold one takes a topological space covered by open sets $V = \bigcup V_i$, such that

1. Each $V_i$ is identified with a standard open ball in $\mathbb{R}^n$ (or $\mathbb{C}^n$).
2. The transition functions between charts $V_i \supset V_i \cap V_j \to V_j \cap V_i \subset V_j$ are continuous ($C^\infty$, analytic,...).
3. $V$ is Hausdorff and second countable.

The Hausdorff condition is necessary to avoid unpleasanties like glueing $\mathbb{R}$ with $\mathbb{R}$ along $\mathbb{R} - \{0\}$:

\[
\begin{array}{ccc}
\bullet & & \bullet \\
\bullet & & \bullet \\
\end{array}
\]

The two origins cannot be separated by open sets, so the resulting space is not Hausdorff although both charts are. We do not want this.

We now copy this definition to glue affine varieties together, and we only allow finitely many charts.

An algebraic set $V$ is a topological space covered by finitely many open sets $V = V_1 \cup \ldots \cup V_n$ (affine charts), such that

1. Each $V_i$ has a structure of an affine variety.
2. The transition maps $V_i \supset V_i \cap V_j \to V_j \cap V_i \subset V_j$ are isomorphisms\(^5\).
3. $V$ is closed in $V \times V$ ($V$ is separated).\(^6\)

An (algebraic) variety is an irreducible algebraic set; in particular, varieties are connected.

The separatedness condition (3) is equivalent to Hausdorffness for topological spaces, but makes sense for varieties. (Because open sets are usually dense in Zariski topology, varieties are never Hausdorff). See Excs 3.1–3.4.

Here is the main example:

**Example 3.1.** Projective space $\mathbb{P}^n = \mathbb{P}^n_k$ is a set of tuples $[x_0 : \ldots : x_n]$ with $x_i \in k$ and not all 0, modulo the relation that $[ax_0 : \ldots : ax_n]$ defines the same point for all $a \in k^\times$.

A subset $V \subset \mathbb{P}^n$ is closed if there are homogeneous polynomials $f_i$ in $x_0, \ldots, x_n$ such that

\[
V = \{x \in \mathbb{P}^n | \text{ all } f_i(x) = 0\}.
\]

As $f_i$ are homogeneous, the condition $f_i(x) = 0$ is independent of the choice of a tuple representing $x$.

To give $\mathbb{P}^n$ a structure of a variety, cover it $\mathbb{P}^n = \mathbb{A}^n_{(0)} \cup \ldots \cup \mathbb{A}^n_{(n)}$ with

\[
\mathbb{A}^n_{(j)} = \{[x_0 : \ldots : x_{j-1} : 1 : x_{j+1} : \ldots : x_n] \} \subset \mathbb{P}^n
\]

\(^5\)That is, rational functions $\phi_{ij} : V_i \to V_j$, defined everywhere on $V_i \cap V_j \subset V_i$ and mapping it to $V_j \cap V_i \subset V_j$.

\(^6\)The topology on $V \times V$ comes from Zariski topology on affine varieties $V_i \times V_j$ that cover it.
The transition maps between charts are indeed morphisms
\[ \mathbb{A}^n \setminus \{x_k = 0\} \to \mathbb{A}^n \setminus \{x_j = 0\}, \quad (x_i) \mapsto (x_i \frac{x_j}{x_k}), \]
so \( \mathbb{P}^n \) becomes an algebraic variety. Closed irreducible subsets of \( \mathbb{P}^n \) are called projective varieties; see Exc 3.7.

**Example 3.2.** If \( X \) is an affine variety and \( V \subset X \) an open set, then \( V \) is general not an affine variety. However, it can always be covered by finitely many affine subvarieties of \( X \), so it is a variety. Generally, both open and irreducible closed subsets of a variety are varieties (Exc 3.6).

A morphism \( X \to Y \) of algebraic sets is a continuous map which is a morphism when restricted to affine charts. A rational map \( X \leadsto Y \) is a morphism from a dense open set. As before, regular and rational functions on \( X \) as morphisms \( X \to \mathbb{A}^1 \) and rational maps \( X \leadsto \mathbb{P}^1 \), respectively. The former form a ring \( k[X] \), and the latter a field \( k(X) \) if \( X \) is a variety. However, unless \( X \) is affine, \( k(X) \) is usually much larger than the field of fractions of \( k[X] \) (Exc 3.8).

We refer to 1-dimensional varieties as curves and 2-dimensional varieties as surfaces. A 0-dimensional variety is a point.

Exc 3.1. Every variety \( X \) is compact, and \( X \) is not Hausdorff unless \( X \) is a point.
Exc 3.2. A topological space \( X \) is Hausdorff if and only if the diagonal \( X \subset X \times X \) is closed in the product topology.
Exc 3.3. (‘Valuative criterion of separatedness’) Suppose \( V \) satisfies (1) and (2) in the definition of an algebraic set. Then it satisfies (3) if and only if for every curve \( C \) and a non-singular point \( P \in C \), any morphism \( C \setminus \{P\} \to X \) has at most one extension to a morphism \( C \to X \).
Exc 3.4. If \( f, g : X \to V \) are morphisms of varieties, the set of points \( x \in X \) where \( f(x) = g(x) \) is closed in \( X \). In fact, for a fixed \( V \) this holds for all \( X, f, g \) if and only if \( V \) is separated.
Exc 3.5. Show that the image of \( \mathbb{A}^2 \) under \( (xy, x) : \mathbb{A}^2 \to \mathbb{A}^2 \) is not a variety.
Exc 3.6.
(a) Prove that \( \mathbb{A}^2 \setminus \{0\} \) is not isomorphic to an affine variety.
(b) Suppose \( X \) is an affine variety and \( \emptyset \neq V \subset X \) open. Then \( V \) can be covered by finitely many affine subvarieties of \( X \), so it is a variety.
(c) Prove that both open and irreducible closed subsets of a variety are varieties.
Exc 3.7. Prove that \( \mathbb{A}^n \) and \( \mathbb{P}^n \) are varieties, that is satisfy the separatedness condition. In particular, affine varieties and projective varieties are actually varieties.
Exc 3.8. Show that \( k[\mathbb{P}^1] = k \) and \( k(\mathbb{P}^1) \cong k(t) \).
Exc 3.9. Prove that every curve has cofinite topology.

4. Complete varieties

The nicest manifolds are the compact ones, but Zariski compactness is not the right notion for varieties — from finite-dimensionality it follows easily that every affine variety is compact (Exc 3.1).
A variety $X$ is **complete** if for every variety $Y$, the projection $X \times Y \to Y$ maps closed sets to closed sets\(^7\).

For $k = \mathbb{C}$ this is the same as requiring $X$ to be compact in the usual topology. Also, in the same way as separatedness is a reformulation of being Hausdorff, completeness is equivalent to compactness for topological spaces (Exc 4.1).

Any topological space can be compactified, and the same is true in our setting:

**Theorem 4.1** (Nagata). *Every variety can be embedded in a complete variety as a dense open subset.*

Here are two alternative definitions of completeness that are a bit more natural. Both say that $X$ is as large as possible in some sense, and has no missing points. For the proof of equivalence, see Exc 4.2.

**Lemma 4.2.** For a variety $X$ the following conditions are equivalent:

1. (‘Universally closed’) $X$ is complete.
2. (‘Maximality’) If $X \subset Y$ is open with $Y$ a variety, then $X = Y$.
3. (‘Valuative criterion’) For every curve $C$ and a non-singular point $P \in C$, any morphism $C \setminus \{P\} \to X$ extends to a morphism\(^8\) $C \to X$.

**Example 4.3.** $\mathbb{A}^1$ is not complete:

1. fails because under $\mathbb{A}^1 \times \mathbb{A}^1 \to \mathbb{A}^1$, the set $xy = 1$ projects to $\mathbb{A}^1 \setminus \{0\}$.
2. fails because $\mathbb{A}^1$ may be embedded in $\mathbb{P}^1$ as a dense open subset.
3. fails because $\mathbb{A}^1 \setminus \{0\} \to \mathbb{A}^1$ does not extend to $\mathbb{A}^1 \to \mathbb{A}^1$.

Here are some important consequences of completeness:

**Lemma 4.4.** Suppose $X$ is a complete variety.

1. Every closed subvariety $Z \subset X$ is complete.
2. For any morphism $f : X \to Y$ the image $f(X)$ is complete and closed in $Y$.
3. $k[X] = k$, in other words $X$ has no non-constant regular functions.
4. If $X$ is affine, then $X$ is a point.

**Proof.** (a) Clear from the definition.
(b) $f(X)$ is the same as $p_2$ of the “graph of $f$” $(x, f(x)) \subset X \times Y$.
(c) The image of $X$ under the composition $X \xrightarrow{f} \mathbb{A}^1 \to \mathbb{P}^1$ is connected, closed and misses $\infty$, so it must be a point.
(d) Affine varieties are characterised by $k[X]$.

The main example of a complete variety is $\mathbb{P}^n$ (Exc 4.4). By (a), all projective varieties are therefore complete, and these are the only complete

---

\(^7\)One says that $\pi : X \to \{\text{pt}\}$ is ‘universally closed’ ($\pi \times \text{id}_Y$ is a closed map for all $Y$).

\(^8\)Necessarily unique as $X$ is a variety and is therefore separated
varieties we will ever encounter. Incidentally, note that this proves Nagata’s theorem for affine varieties: embed $V \subset \mathbb{A}^n \subset \mathbb{P}^n$ and take the closure $\overline{V}$ of $V$ in $\mathbb{P}^n$ (the intersection of all closed subsets of $\mathbb{P}^n$ containing $V$). Then $V \subset \overline{V}$ is dense open and $\overline{V}$ is a projective variety, hence complete.

Here is one standard illustration of the power of completeness:

**Lemma 4.5.** Suppose $C_1$ and $C_2$ are complete non-singular curves.

(i) Any morphism $C_1 \setminus \{P_1, \ldots, P_n\} \to C_2$ extends uniquely to $C_1 \to C_2$.

(ii) Every non-constant map $f : C_1 \to C_2$ is surjective.

*Proof.* (i) use 4.2 (3); uniqueness follows from separatedness of $C_2$. (ii) $\text{Im } f$ is closed, so it is either a point or the whole of $C$. □

What (i) says is that every rational map $C_1 \to C_2$ extends to a unique morphism, so for non-singular complete curves there is no real distinction between rational maps and morphisms. From here it is not hard to get that $C \mapsto k(C)$ defines an equivalence of categories

\[
\begin{array}{ccc}
\text{complete non-singular} & \to & \text{Finitely generated field extensions} \\
\text{curves over } k & & K/k \text{ of transcendence degree 1}
\end{array}
\]

In higher dimensions this is not true — for instance $\mathbb{P}^2$ and $\mathbb{P}^1 \times \mathbb{P}^1$ have the same field of rational functions, but are not isomorphic (Exc 4.8).

When $k = \mathbb{C}$, complete non-singular curves are the same as (compact) Riemann surfaces. In particular, every Riemann surface is algebraizable (arises from such a curve), but this is not true for higher-dimensional compact complex manifolds. Nevertheless, for complete varieties there is a very close connection between the usual complex topology and Zariski topology:

**Theorem 4.6** (Chow). Let $X, Y$ be complete varieties over $\mathbb{C}$.

(1) Every analytic subset\(^{11}\) of $X$ is closed in Zariski topology.

(2) Every holomorphic map $f : X \to Y$ is induced by a morphism of varieties.

Chow proved (1) for $X = \mathbb{P}^n$ and the rest of the assertions follow relatively easily (using Chow’s lemma for (1) and applying (1) to the graph of $f$ in (2); see [?] §1.3).

In particular, the only meromorphic functions on a complete variety over $\mathbb{C}$ are rational functions (take $Y = \mathbb{P}^1$).

\(^{9}\) In fact, complete curves and surfaces are always projective, and it is quite non-trivial to construct a non-projective complete 3-dimensional variety [?].

\(^{10}\) Thus Nagata’s theorem for arbitrary varieties becomes a question of arranging the completions of affine charts so that they can be glued together. This may be done using ‘blowing-ups’ and ‘blowing-downs’, see [?].

\(^{11}\) Locally (in the usual complex topology) a zero set of holomorphic functions...
Exc 4.3. Let $C$ be a curve and $P \in C$ a non-singular point. Show that the local ring $O_{C,P} \subset k(C)$ of functions defined at $P$ is a discrete valuation ring.

Exc 4.4. Use Exc 4.3 and the ‘valuative criterion’ to show that $\mathbb{P}^n$ is complete.

Exc 4.5. Determine $k[\mathbb{P}^n]$ and $k(\mathbb{P}^n)$.

Exc 4.6. Suppose $C$ is a curve.
(a) Show that there is a non-singular complete curve $\tilde{C}$ birationally isomorphic to $C$. In other words, there are rational maps $\phi : C \to \tilde{C}$ and $\psi : \tilde{C} \to C$ with $\phi \psi = \text{id}$ and $\psi \phi = \text{id}$. Show that any two such $\tilde{C}$ are isomorphic.
(b) If $C$ is complete, then $\psi$ is a surjective morphism.
(c) If $C$ is non-singular, then $\phi$ is an injective morphism identifying $C$ with an open set of the form $\tilde{C} \setminus \{P_1, \ldots, P_n\}$.

Exc 4.7. Explain why Lemma 4.5 fails if one of the words ‘complete’, ‘non-singular’ or ‘curves’ is omitted.

Exc 4.8. Show that $\mathbb{P}^2$ and $\mathbb{P}^1 \times \mathbb{P}^1$ have the same field of rational functions but are not isomorphic. (You may want to use that a non-singular curve $C \subset \mathbb{P}^2$ defined by a homogenous equation $f(x_0, x_1, x_2) = 0$ of degree $d$ has genus $g = (d - 1)(d - 2)/2$.)

Exc 4.9. Prove that the complete variety in Nagata’s theorem is not necessarily unique.

Exc 4.10. Show that for complex varieties that are not complete Chow’s theorem may fail.

Exc 4.11. Prove that a compact complex manifold has at most one algebraic structure.

5. Algebraic Groups

As before, $k = \bar{k}$ is an algebraically closed base field. We define algebraic groups from varieties exactly as in the affine case (Def. 2.1).

Definition 5.1. A group $G$ is an algebraic group if it has a structure of an algebraic set, and multiplication $G \times G \to G$ and inverse $G \to G$ are morphisms.

As before, homomorphisms refer to morphisms that are group homomorphisms, isomorphisms are isomorphisms of both groups and varieties, and subgroups and normal subgroups always refer to closed ones.

Example 5.2. Affine algebraic groups $\mathbb{G}_m, \mathbb{G}_a, \text{GL}_n, ...$ are algebraic groups.

Example 5.3. Elliptic algebraic curves and their products are algebraic groups.

Example 5.4. The multiplication-by-$m$ map $[m] : G \to G$ is a homomorphism for any commutative algebraic group $G$ and $m \in \mathbb{Z}$ (Exc 5.1).

Basic properties of algebraic groups carry over immediately from the affine case: an algebraic group $G$ is a semidirect product $G = G^0 \rtimes \Delta$ of its connected component of identity $G^0$ and a finite discrete group $\Delta$. Again, $G^0$ is a non-singular variety. Kernels and images of algebraic group homomorphisms exist, and so do factor groups in the same ‘naive’ sense as before.

Example 5.5. Algebraic groups often occur naturally as automorphism groups of varieties (see Exc 5.2 though). For example, suppose $C$ is a complete non-singular curve of genus $g$.

$(g = 0) \quad C \cong \mathbb{P}^1$, and $\text{Aut } C \cong \text{PGL}_2 = \text{GL}_2 / \mathbb{G}_m$ is a Möbius group (Exc 5.3).
(g = 1) Choosing a point $O \in C$ makes $C$ into an elliptic curve, and from the theory of elliptic curves it follows that $\text{Aut} C \cong C \rtimes \text{Aut}(C, O)$ with $\text{Aut}(C, O)$ finite of order $\leq 24$ (usually just $\{\text{id}, [-1]\}$.)

(g $\geq 2$) $\text{Aut} C$ is finite.

**Proposition 5.6.** The only one-dimensional connected algebraic groups are $\mathbb{G}_a$, $\mathbb{G}_m$ and elliptic curves.

**Proof.** Write $G = C \setminus \{P_1, \ldots, P_n\}$ with $C$ a non-singular complete curve (Exc 4.6), and take $x \in G$. The left translation map $l_x : y \mapsto xy$ on $G$ extends to an automorphism $l_x : C \rightarrow C,$

because $C$ is non-singular and complete. So $C$ has infinitely many automorphisms that are (a) fixed point free on $G$, and (b) preserve the set of ‘missing points’ $\{P_1, \ldots, P_n\}$.

Write $g$ for the genus of $C$, and $e \in G$ for the identity element.

$g \geq 2$: $\text{Aut} C$ is finite, so this is impossible.

$g = 1$: If $n \geq 1$ then $|\text{Aut}(C, P_1)| \leq 24$, so $n = 0$ and $G$ is complete. For $x \in G$ there is a unique fixed point free map taking the identity element $e$ to $x$, which must be $l_x$ in every group law on $G$ which has $e$ as the identity element. So the group law must be the same one as the standard one on an elliptic one.

$g = 0$: Now $C \cong \mathbb{P}^1$ and $\text{Aut} C \cong \text{PGL}_2(k)$ is the group of Möbius transformations. These are uniquely determined by what they do to 3 given points, in particular $\text{Aut} G \neq \{1\}$ implies $n \leq 2$.

$n = 0$: Then $l_x : \mathbb{P}^1 \rightarrow \mathbb{P}^1$ has no fixed points, which is impossible.

$n = 1$: Change the coordinate on $\mathbb{P}^1$ to move $P_1$ to $\infty$ and $e$ to 0. The fixed point free automorphisms of $\mathbb{P}^1 \setminus \{\infty\}$ are translations

$$z \mapsto z + a,$$

again there is a unique one taking $0$ to a given $a \in G$, and $G = \mathbb{G}_a$.

$n = 2$: Similarly, move $P_1 \mapsto 0$, $P_2 \mapsto \infty$ and $e \mapsto 1$. The automorphisms of $\mathbb{P}^1 \setminus \{0, \infty\}$ are $z \mapsto az$ and $z \mapsto a/z$. Only the former ones are fixed point free, and there is a unique one taking $e \rightarrow x$ for a given $x$. So the group law is unique, $G = \mathbb{G}_m$. \hfill \Box

Suppose $G$ is an algebraic group over $k$. Recall that if $G$ is an affine variety, $G$ is also called a linear algebraic group.

**Definition 5.7.** An abelian variety is a complete connected algebraic group.

---

12Hurwitz (1893) showed that $|\text{Aut}(C)| \leq 84(g - 1)$ over $\mathbb{C}$, and the bound is sharp for infinitely many $g$ (Macbeath 1961). Schmid (1938) proved finiteness when $\text{char} k = p > 0$ and noted that Hurwitz’ bound fails for small $p$. It still holds when $p > g + 1$, except for $y^p - y = x^2$ which has $g = \frac{p-1}{2}$ and $|\text{Aut}(C)| = 8g(g + 1)(2g + 1)$ (Roquette 1970).
We have seen that 1-dimensional algebraic groups are either linear \((G_a, \mathbb{G}_m)\) or abelian varieties (elliptic curves). Much more generally, these two extremes build all algebraic groups:

**Theorem 5.8** (Barsotti-Chevalley). Every connected algebraic group \(G\) fits into an exact sequence

\[
1 \rightarrow H \rightarrow G \rightarrow A \rightarrow 1
\]

with \(H \triangleleft G\) the unique largest linear connected subgroup of \(G\), and \(A\) an abelian variety.

**Remark 5.9.** With the theory of linear groups thrown in, the classification can be extended. There is a unique filtration of \(G\) of the form

\[
G = G_0 \rightarrow G_1 \rightarrow G_2 \rightarrow G_3 \rightarrow 1
\]

with \(G_i\) connected and normal in \(G_{i-1}\). Here:
- A **torus** is an algebraic group isomorphic to \(\mathbb{G}_m \times \cdots \times \mathbb{G}_m\);
- A **unipotent group** is a subgroup of upper-triangular matrices with ones on the diagonal;
- A **solvable group** is one admitting a filtration \(1 = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_k = G\) with \(H_i/H_{i-1}\) commutative;
- A **semisimple** group is one whose radical \(G_2\) (the unique maximal connected linear solvable normal subgroup) is trivial; a semisimple group admits a finite covering \(G_1 \times \cdots \times G_n \rightarrow G\) with \(G_i\) almost simple (finite centre \(C\) and \(G/C\) simple). Every almost simple group is isomorphic to either \(\text{SL}_{m+1}\) (type \(A_n\)), \(\text{Sp}_{2n}\) (type \(C_n\)), \(E_6, E_7, E_8, F_4, G_2\) (exceptional groups) or isogenous to an orthogonal group (types \(B_n, D_n\)).

See [?] Ch. X for a more extended summary and references.

**Example 5.10.** \(G = \text{GL}_n\). Then \(G = G_1, G_2 = Z(G) = \mathbb{G}_m\) and \(G/G_2 = \text{PGL}_n\) is simple.

**Example 5.11.** Is it not hard to deduce that the only connected commutative linear groups are \(U \cong (\mathbb{G}_m)^m \times (\mathbb{G}_a)^n\). So every commutative connected algebraic group \(G\) has the form \(G = A \times U\) with \(A\) an abelian variety, \(U\) as above and acting trivially on \(A\).

Exc 5.1. Prove that the multiplication-by-\(m\) map \([m] : G \rightarrow G\) is a homomorphism for any commutative algebraic group \(G\) and \(m \in \mathbb{Z}\).

Exc 5.2. Give an example of a variety \(V\) such that \(\text{Aut} \ V\) has no natural structure of an algebraic group.

Exc 5.3. Show that every automorphism of \(\mathbb{P}_k^1\) is of the form \(t \mapsto \frac{at+b}{ct+d}\). Deduce that \(\text{Aut} \, \mathbb{P}_k^1 \cong \text{PGL}_2(k) = (\text{GL}_2(k)/k^*)\).

Exc 5.4. Show that there are no non-constant algebraic group homomorphisms from an abelian variety to a linear algebraic group.
6. Abelian varieties

Suppose $k = \bar{k}$ as before. Recall that an abelian variety $A/k$ is an algebraic group over $k$, which is a complete variety. Let us validate ‘abelian’ and prove that abelian varieties are always commutative. This must clearly rely on completeness, and we follow Mumford’s approach using rigidity:

**Lemma 6.1 (Rigidity).** Suppose $f : V \times W \to U$ is a map of varieties, $V$ is complete, and

$$f(\{v_0\} \times W) = f(V \times \{w_0\}) = \{u_0\}$$

for some points $v_0, w_0$ and $u_0$. Then $f$ is constant, $f(V \times W) = \{u_0\}$.

**Proof.** Let $U_0$ be an open affine neighbourhood of $u_0$ and $Z = f^{-1}(U - U_0)$. This is a closed set, and so is its image under the projection $p_2 : V \times W \to W$, as $V$ is complete.

As $w_0 \notin p_2(Z)$, the complement $W_0 = W - p_2(Z)$ is open dense in $W$. But for all $w \in W_0$ the image $f(V \times \{w\}) \subset U_0$ must be a point, as $V \times \{w\}$ is complete and $U_0$ is affine. In other words, $f(V \times \{w\}) = f((v_0, w)) = u_0$. So $f^{-1}(u_0)$ contains a dense open $V \times W_0$; as $f^{-1}(u_0)$ is also closed, it must be the whole space, so $f$ is constant. □

**Corollary 6.2.** If $U, V, W$ are varieties, $V$ is complete, $U$ is an algebraic group, and $f_1, f_2 : V \times W \to U$ are morphisms that agree on $\{v_0\} \times W$ and on $V \times \{w_0\}$, then they agree everywhere.

**Proof.** The map $x \mapsto f_1(x)f_2(x)^{-1}$ is constant by the rigidity lemma. □

**Corollary 6.3.** Abelian varieties are commutative.

**Proof.** The maps $xy$ and $yx$ from $X \times X$ to $X$ agree on $X \times \{e\}$ and $e \times X$, so they must agree everywhere by the previous corollary. □

From now on let us write the group operation on abelian varieties as addition, and denote the identity element by $0$.

**Corollary 6.4.** If $A, B$ are abelian varieties, then every morphism of varieties $f : A \to B$ that takes $0$ to $0$ is a homomorphism of abelian varieties.

**Proof.** The morphisms $f(x) + f(y)$ and $f(x + y)$ from $A \times A$ to $B$ agree on $\{0\} \times A$ and on $A \times \{0\}$, so they are equal. □

**Corollary 6.5.** Every morphism $f : A \to B$ between abelian varieties is a composition of a translation on $B$ and a homomorphism $A \to B$.

---

13 Over $k = \mathbb{C}$, this works as follows: if $w$ is close to $w_0$, then $f(V \times \{w\})$ is close to $u_0$, by the compactness of $V$ and continuity of $f$. So $f(V \times \{w\})$ is contained in some open ball around $u_0$. But there are no non-constant analytic maps from $V$ to an open ball (maximum principle), so $f(V \times \{w\})$ is a point for such $w$, namely $f((v_0, w)) = u_0$. This proves that the set of such $w$ is open; but it is also closed, so $f$ is constant.
In fact, in the two preceding corollaries $B$ could be any algebraic group. Rigidity has another curious consequence: in defining an abelian variety we could have dropped the associativity condition, as it also follows automatically from rigidity! (Exc 6.1) For instance, for elliptic curves this gives a quick proof of the associativity of the group law, that only relies on $E$ being complete.

**Remark 6.6.** It is possible to extend Corollary 6.5 slightly: any rational map $\phi : G \rightarrow A$ from a connected algebraic group to an abelian variety is a composition of a translation with a homomorphism $G \rightarrow A$ (in particular, $\phi$ a morphism).

**Exc 6.1.** Suppose $V$ is a complete variety, $e \in V(k)$ a point, and we have a morphism $*: V \times V \rightarrow V$ and an isomorphism $i : V \rightarrow V$. If $x*e = e*x = x$ and $x*i(x) = i(x)*x = e$, then $*$ is associative, so $V$ is an abelian variety.

**Exc 6.2.** Prove that for an abelian variety $A$, every rational map $\mathbb{P}^1 \rightarrow A$ is a constant morphism (hint: 6.6). Deduce that every rational map $\mathbb{P}^n \rightarrow A$ is also constant.

### 7. Abelian varieties over $\mathbb{C}$

If the base field $k = \overline{k}$ has characteristic 0, by Lefschetz principle (e.g. [?]) §VI.6) understanding varieties over $k$ essentially reduces to understanding those over $\mathbb{C}$.

Suppose $k = \mathbb{C}$ and $X/\mathbb{C}$ is a $g$-dimensional abelian variety. As $X$ is regular and complete, in classical topology (also referred to as Euclidean or strong topology) it is a compact complex manifold with a group structure. In other words, it is a compact complex-analytic Lie group of $\mathbb{C}$-dimension $g$.

**Theorem 7.1.** Let $X/\mathbb{C}$ be a $g$-dimensional abelian variety. As complex Lie groups, $X \cong \mathbb{C}^g/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}^g$ of rank $2g$.

**Proof.** Suppose $X$ is any complex Lie group, and write $V = T_eX$ for the tangent space at identity. From the theory of Lie groups, for every $v \in V$ there is a unique analytic group homomorphism ("one-parameter subgroup") $\phi_v : \mathbb{C} \rightarrow X$

with $d\phi_v(0) = v$, and $\phi_v(\cdot) : V \times \mathbb{C} \rightarrow X$ analytic. Define the exponential map exp : $V \rightarrow X$ by exp$v = \phi_v(1)$. It is analytic, and we have

1. $\phi_v(t) = \exp(tv)$, $[\phi_v(st) = \phi_v(s) \circ \phi_v(t)]$ by uniqueness of $\phi_v$; now put $s = 1$.

2. If $X$ is commutative then exp : $V \rightarrow X$ is a group homomorphism. [As $X$ is abelian, $\psi : t \mapsto \exp(tx) \exp(ty)$ is a homomorphism $\mathbb{C} \rightarrow X$. But $d\psi(1) = x + y$, so $\psi = \phi_{x+y}$ again by uniqueness; now put $t = 1$.] Now if $X$ is an abelian variety, then exp : $V \rightarrow X$ is surjective because exp$(V) \subset X$ is an open subgroup (Exc 7.1). Finally, ker exp $\subset V$ is a discrete subgroup with compact quotient, so it is a lattice of maximal rank. □
Corollary 7.2. Let $X$ be a $g$-dimensional abelian variety over $\mathbb{C}$, and write $X[n]$ for the $n$-torsion subgroup of $X$ (all $x$ with $nx = 0$). Then\(^{14}\)

$$X[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g} \quad (n \geq 1).$$

Proof. $X \cong \mathbb{C}^{2g}/\Lambda$, so $X[n] \cong \frac{1}{n}\Lambda/\Lambda \cong (\frac{1}{n}\mathbb{Z}/\mathbb{Z})^{2g}$ as a group. $\square$

The proof of Theorem 7.1 does not use compactness of $X$ until the last line, so all conclusions except $\Lambda = \ker \exp$ having maximal rank remain valid for all commutative Lie groups over $\mathbb{C}$:

Example 7.3. For $X = G_a$, $\exp : \mathbb{C} \to \mathbb{C} = G_a$ is identity, and $\Lambda = \{1\}$.

Example 7.4. For $X = G_m$, $\exp : \mathbb{C} \to \mathbb{C}^* = G_m$ is the usual exponential function $z \mapsto e^z$, and $\Lambda = 2\pi i\mathbb{Z}$ is a lattice of rank one; in other words, $G_m \cong \mathbb{C}/\mathbb{Z}$ as an analytic Lie group.

Example 7.5. (Elliptic curves) If $\Lambda \subset \mathbb{C}$ is a lattice, the parametrisation

$$\mathbb{C}/\Lambda \xrightarrow{(\wp, \wp', 1)} E : y^2 = 4x^3 - g_2x - g_3 \subset \mathbb{P}^2$$

is given by the elliptic functions $g_2 = g_2(\Lambda)$, $g_3 = g_3(\Lambda)$ and $\wp(z) = \wp(\Lambda, z)$:

$$g_2 = 60 \sum_{w \in \Lambda, w \neq 0} \frac{1}{w^4}, \quad g_3 = 140 \sum_{w \in \Lambda, w \neq 0} \frac{1}{w^6}, \quad \wp(z) = \frac{1}{z^2} + \sum_{w \in \Lambda, w \neq 0} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2}\right).$$

Note that $\wp(z)$ is a transcendental function, in other words the morphism $A^1_{\mathbb{C}} = \mathbb{C} \to E$ is by no means algebraic.\(^{15}\)

The three examples combine to an analytic analogue of the classification of 1-dimensional algebraic groups (Prop. 5.6): a connected 1-dimensional commutative complex Lie group is either $G_a = \mathbb{C}$, $G_m = \mathbb{C}/\mathbb{Z}$ or an elliptic curve $E = \mathbb{C}/\mathbb{Z} \tau_1 \oplus \mathbb{Z} \tau_2$.

A compact analytic Lie group of the form $\mathbb{C}^g/\Lambda$ is called a ($g$-dimensional) complex torus. By the example above, every 1-dimensional complex torus is an elliptic curve. Unfortunately, this fails for $g > 1$: not every complex torus is an abelian variety. The ones that are varieties are called algebraizable, and we give a criterion below.

Everything else goes well though:

Theorem 7.6. Suppose $A = \mathbb{C}^g/\Lambda$ and $A' = \mathbb{C}^g/\Lambda'$ are abelian varieties.

1. Abelian subvarieties $U \subset A$ are in one-to-one correspondence with the $\mathbb{C}$-subspaces $V \subset \mathbb{C}^g$ for which $\text{rk}_\mathbb{Z}(V \cap \Lambda) = 2\dim V$.
2. $\text{Hom}_{\text{AV}}(A, A') = \{M \in \text{Mat}_{g \times g}(\mathbb{C}) \mid MA \subset A'\}$.
3. $A \cong A'$ if and only if $MA = A'$ for some $M \in \text{GL}_g(\mathbb{C})$.

Proof. (3) is a special case of (2). Half of (2) is also easy: a homomorphism

---

\(^{14}\)By Lefschetz principle, the same holds over any $k = \bar{k}$ of characteristic $0$ (Exc 7.2)

\(^{15}\)E.g. its kernel $\Lambda$ is not Zariski closed; in fact, there are no non-constant morphisms $A^1 \to E$ by Exc 6.2.
\( \phi : A \to A' \) induces a \( \mathbb{C} \)-linear map on the tangent spaces at \( e \),

\[
d\phi : \mathbb{C}^g \to \mathbb{C}^{g'}
\]

and \( \exp \circ d\phi = \phi \circ \exp \) by the uniqueness of \( \exp \), so \( \phi(\Lambda) \subset \Lambda' \). Applying this to the inclusion \( U \subset A \) gives half of (1) as well.

The other half of (1) and (2) is a special case of Chow's theorem 4.6. □

**Corollary 7.7.** If \( A = \mathbb{C}^g / \Lambda \) and \( A' = \mathbb{C}^{g'} / \Lambda' \) are abelian varieties, then \( \text{Hom}_{AV}(A, A') \) is a free \( \mathbb{Z} \)-module of rank \( \leq 2gg' \).

**Proof.** Let \( L \subset \Lambda \) be a rank \( g \) sublattice which spans \( \mathbb{C}^g \) over \( \mathbb{C} \). Then \( \text{Hom}_{AV}(A, A') \hookrightarrow \text{Hom}_{\mathbb{Z}}(L, \Lambda') \) from 7.6 (2).

This bound is best possible for all \( g \) and \( g' \) (Exc 8.3).

**Example 7.8.** If \( E = \mathbb{C} / \Lambda \) is an elliptic curve, then \( \text{End} E = \text{Hom}(E, E) \) is either \( \mathbb{Z} \) or has rank 2. In the latter case, it is an order in an imaginary quadratic field (Exc 7.3) and we say that \( E \) has complex multiplication.

Another immediate corollary of Chow’s theorem is a description of rational functions on an abelian variety \( A = \mathbb{C}^g / \Lambda \):

Rational functions on \( A = \text{Meromorphic functions on } A = \Lambda\text{-periodic meromorphic functions on } \mathbb{C}^g \).

It turns out that algebraicity of a complex torus amounts to requiring that it has ‘enough’ meromorphic functions, and has the following explicit description:

**Theorem 7.9.** (Lefschetz) Let \( \Lambda \subset \mathbb{C}^g \) be a \( \mathbb{Z} \)-lattice of rank \( 2g \). For \( X = \mathbb{C}^g / \Lambda \) the following conditions are equivalent:

1. \( X \) is an abelian variety.
2. \( X \) is a projective variety.
3. \( X \) has \( g \) algebraically independent meromorphic functions.
4. There is a positive-definite Hermitian form \( H : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C} \) such that \( E = \text{Im} H \) takes values in \( \mathbb{Z} \) on \( \Lambda \times \Lambda \).

A form \( H \) as in (4) is called a Hermitian Riemann form, and \( E = \text{Im} H \) an alternating Riemann form. Note that

\[
E : \Lambda \times \Lambda \to \mathbb{Z}
\]

is alternating and \( E(iu, iv) = E(u, v) \) (use that \( H \) is Hermitian). Conversely, such a \( E \) recovers \( H \) by \( H(u, v) = E(iu, v) + iE(u, v) \), see Exc 7.4.

**Example 7.10.** (Elliptic curves) For 1-dimensional complex tori \( X = \mathbb{C} / \Lambda \) the conditions are always satisfied:

1. Every compact Riemann surface in algebraizable.
2. The field of meromorphic functions is generated by \( \wp(z) \) and \( \wp'(z) \) with one relation (Example 7.5).
3. Rescale the lattice so that \( \Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau \). Then \( H(z, w) = \frac{1}{\text{Im} \tau} zw \) is a Hermitian Riemann form.
For $g > 1$, a general lattice $\Lambda \subset \mathbb{C}^g$ does not admit any alternating Riemann forms: if $\{e_i\}$ is a $\mathbb{Z}$-basis of $\Lambda$, an alternating form $E : \Lambda \times \Lambda \to \mathbb{Z}$ is determined by $E(e_i, e_j) \in \mathbb{Z}$. The condition $E(iu, iv) = E(u, v)$ forces linear relations with real coefficients upon them, and these will have no non-zero integer solutions in general. Thus, ‘most’ tori are not algebraizable.

Exc 7.1. If $G$ is a connected topological group and $U \subset G$ an open subgroup, then $U = G$.

Exc 7.2. Use Lefschetz principle to show that $A$ is determined by $E$. Thus, if $G$ is a zero integer solutions in general. Thus, ‘most’ tori are not algebraizable.

Exc 7.3. Suppose $E = C/(Z + \tau Z)$ is an elliptic curve with End $E \neq \mathbb{Z}$. Show that $K = \mathbb{Q}(\tau)$ is an imaginary quadratic field, and End $E \hookrightarrow K$ is naturally a subring which has rank 2 over $\mathbb{Z}$ (so it is an order of $K$).

Exc 7.4. Show that $H \mapsto \text{Re } H$ defines a 1-1 correspondence between Hermitian forms $H$ on $\mathbb{C}^g$ and real-valued alternating forms $E$ on $\mathbb{C}^g$ satisfying $E(iu, iv) = E(u, v)$.

Exc 7.5. Let $E : \mathbb{Z}^{2g} \times \mathbb{Z}^{2g} \to \mathbb{Z}$ be an alternating non-degenerate form. There is a basis for $\mathbb{Z}^{2g}$ in which $E$ has the shape $(0 \ M \ 0)$, where $M$ is a diagonal matrix with positive integer entries on the diagonal.

Exc 7.6. Write down an explicit example of a non-algebraizable complex torus.

8. ISOGENIES AND ENDOMORPHISMS OF COMPLEX TORI

Recall that by 7.6(2), homomorphisms $\phi : \mathbb{C}^g/\Lambda \to \mathbb{C}^g'/\Lambda'$ of abelian varieties are just $\mathbb{C}$-linear maps $\mathbb{C}^g \to \mathbb{C}^g'$ mapping $\Lambda$ to $\Lambda'$. Let us call the latter homomorphisms of complex tori even when they are not algebraizable. (Equivalently, it is a homomorphism as analytic Lie groups.)

**Definition 8.1.** A homomorphism $\phi : X \to X'$ of complex tori is an isogeny of degree $m$ if it is surjective with kernel of size $m$. We write $\deg \phi = m$, and we say that the two tori are isogenous (denoted $X \sim X'$).

Equivalently, $\phi$ is a homomorphism which is a covering map of degree $m$ in the topological sense. If $\phi : \mathbb{C}^g/\Lambda \to \mathbb{C}^g'/\Lambda'$ is such an isogeny, then $g = g'$ and we identify $\mathbb{C}^g = \mathbb{C}^{g'}$ via $\phi$, it gives inclusion of lattices $\phi : \Lambda \hookrightarrow \Lambda'$, identifying $\Lambda$ with a sublattice of index $m$ in $\Lambda'$.

Here are some immediate properties of isogenies:

- For isogenies $X \xrightarrow{\phi} X' \xrightarrow{\psi} X''$ of complex tori, $\deg(\psi \circ \phi) = \deg \phi \cdot \deg \psi$. [Consider $\Lambda \hookrightarrow \Lambda' \hookrightarrow \Lambda''$.]
- The multiplication-by-$m$ map $[m] : \mathbb{C}^g/\Lambda \to \mathbb{C}^g/\Lambda$ is an isogeny of degree $m^{2g}$ [cf. 7.2].
- There is an isogeny $X \to X'$ if and only if there is one $X' \to X$. [If $\Lambda \subset \Lambda'$ has index $m$, then $m \Lambda' \subset \Lambda$.]

Thus, being isogenous is an equivalence relation. Specifically, for a degree $m$ isogeny $\phi : X \to X'$ we constructed a unique isogeny $\tilde{\phi} : X' \to X$ (of degree $m^{2g-1}$) with $\tilde{\phi} \phi = [m]$, called the conjugate isogeny. For elliptic curves $\phi^z = \phi$, but this fails in higher dimensions (wrong degree).

- For isogenies $X \xrightarrow{\phi} X' \xrightarrow{\psi} X''$ of complex tori, $\tilde{\psi} \phi = \tilde{\phi} \circ \tilde{\psi}$. 

A complex torus isogenous to an abelian variety is an abelian variety. 

[Restrict the Riemann form to $\Lambda \subset \Lambda'$]

The endomorphism ring $\text{End}\, A$ of a complex abelian variety $A$ is finitely generated and free as a $\mathbb{Z}$-module (7.7), and we call $\text{End}^0\, A = \text{End}\, A \otimes_{\mathbb{Z}} \mathbb{Q}$ the *endomorphism algebra of* $A$. Its units are isogenies $A \to A$.

We call $A$ *simple* if it has no abelian subvarieties apart from $\{0\}$ and $A$.

**Lemma 8.2.**

1. $A$ is simple if and only if $\text{End}^0\, A$ is a division algebra.
2. If $A$ and $A'$ are simple, then either $A \sim A'$ or $\text{Hom}(A, A') = 0$.
3. If $A \sim A'$ then $\text{End}^0\, A \cong \text{End}^0\, A'$.

**Proof.** (1, 2) Exc 8.5. (3) If $\phi : A \to A'$ is an isogeny of degree $m$, the maps

\[ \alpha : f \mapsto \phi f \phi : \text{End}\, A \to \text{End} A' \quad \text{and} \quad \beta : f \mapsto \tilde{\phi} f \phi : \text{End} A' \to \text{End} A \]

compose to $\alpha \beta = [m] \in \text{End} A$ and $\beta \alpha = [m] \in \text{End} A'$. Because $[m]$ becomes a unit after $\otimes \mathbb{Q}$, $\alpha$ and $\beta$ are isomorphisms on the level of $\text{End}^0$. □

**Theorem 8.3** (Poincare reducibility). Suppose $A' \subset A$ is an abelian subvariety of a complex abelian variety. Then there is an abelian subvariety $A'' \subset A$ such that $A = A' + A''$ and $A' \cap A''$ is finite; $A$ is isogenous to $A' \times A''$.

**Proof.** Exc 8.6. □

Thus, every non-simple abelian variety is isogenous to a product $A' \times A''$ of abelian varieties of smaller dimension. Continuing this process, we get

**Corollary 8.4** (Complete reducibility). Every complex abelian variety is isogenous to a product simple abelian varieties,

\[ A \sim A_1^{n_1} \times \cdots \times A_k^{n_k}. \]

For such an $A$,

\[ \text{End}^0\, A \cong \text{Mat}_{n_1 \times n_1}(D_1) \times \cdots \times \text{Mat}_{n_k \times n_k}(D_k), \quad D_i = \text{End}^0(A_i), \]

in particular it is a semisimple $\mathbb{Q}$-algebra (product of matrix algebras over division algebras).

A formal way of saying this is that the category of ‘abelian varieties up to isogeny’ (objects = abelian varieties, morphisms = $\text{Hom}_{\text{AV}} \otimes_{\mathbb{Z}} \mathbb{Q}$) is a *semisimple* $\mathbb{Q}$-linear category (Homs are $\mathbb{Q}$-vector spaces and every object is a direct sum of simple objects).

It remains to understand algebraically which division rings may actually occur as endomorphism algebras of simple abelian varieties. For this we first need to reformulate the algebraizability condition (existence of a Riemann form).

\[ ^{16}\text{The same argument also gives an alternative proof that subtori of abelian varieties are abelian varieties (half of Thm. 7.6(2)), avoiding the use of Chow's theorem.} \]
Exc 8.1. Show that the elliptic curves \( E_n = \mathbb{C}/(\mathbb{Z} + n\mathbb{Z}) \) for \( n \geq 1 \) are pairwise isogenous. Determine \( \text{End} E_n \) and \( \text{End}^0 E_n \).

Exc 8.2. ‘A generic complex torus has endomorphism ring \( \mathbb{Z} \).’ Explain.

Exc 8.3. For any \( g, g' \geq 1 \) give an example of complex abelian varieties with \( \text{dim} A = g \), \( \text{dim} A' = g' \) and \( \text{dim} \text{Hom}(A, A') = 2gg' \). Give also an example with \( \text{Hom}(A, A') = \{0\} \).

Exc 8.4. Give an example of an abelian variety which is isogenous to a product of two (positive-dimensional) abelian varieties, but is itself not such a product.

Exc 8.5. Prove that \( A \) is a simple abelian variety if and only if \( \text{End}^0 A \) is a division algebra. Show that if \( A \) and \( A' \) are simple abelian varieties, then either \( A \sim A' \) or \( \text{Hom}(A, A') = 0 \).

Exc 8.6. Prove the Poincare reducibility theorem (8.3). Hint: Take the orthogonal complement \( V \) of \( \Lambda' \subset \Lambda \) with respect to the Hermitian Riemann form \( H \), and let \( \Lambda'' = V \cap \Lambda \).

9. Dual abelian variety

Let \( X = V/\Lambda \) be a complex torus of dimension \( g \) (so \( V \cong \mathbb{C}^g \)). Define

\[
V^* = \{ f \in \text{Hom}_\mathbb{R}(V, \mathbb{C}) \mid f(\alpha v) = \bar{\alpha} f(v), \text{ all } \alpha \in \mathbb{C}, v \in V \},
\]

\[
\Lambda^* = \{ f \in V^* \mid \text{Im} f(v) \in \mathbb{Z} \text{ all } v \in \Lambda \}.
\]

Because \( (v, f) \mapsto \text{Im} f(v) \) is a non-degenerate \( \mathbb{R} \)-linear pairing \( V \times V^* \to \mathbb{R} \), \( \Lambda^* \subset V^* \) is again a lattice of rank \( 2g \). Call \( X^* = V^*/\Lambda^* \) the dual torus of \( V/\Lambda \).

Clearly,

- \( X^{**} = X \) canonically;
- a homomorphism \( f : X \to Y \) induces \( f^* : Y^* \to X^* \). Moreover, \( f \) is an isogeny if and only if \( f^* \) is; if they are, then \( \deg f = \deg f^* \);
- \( (\psi \circ \phi)^* = \phi^* \circ \psi^* \) for homomorphisms \( X \xrightarrow{\phi} X' \xrightarrow{\psi} X'' \);
- \( [m]^* = [m] \) for the multiplication-by-\( m \) map \( [m] : X \to X \),

the properties expected from a decent duality.

If \( X = V/\Lambda \) is an abelian variety, then a Hermitian Riemann form on \( X \) defines a \( \mathbb{C} \)-linear isomorphism \( \lambda_H : v \mapsto H(v, \cdot) \) from \( V \) to \( V^* \) which maps \( \Lambda \) to \( \Lambda^* \), because \( \text{Im} H \) is integer-valued on \( \Lambda \times \Lambda \) by definition. So

\[
\lambda_H : X \to X^*
\]

is an isogeny.\(^{17}\) Such as isogeny \( \lambda : X \to X^* \) induced by a positive-definite Hermitian form \( H \) is called a polarisation on \( X \), and Lefschetz’ Theorem 7.9 asserts that abelian varieties are precisely those tori that admit a polarisation. Note also that \( \lambda^* = \lambda \) (identifying \( X^{**} \) with \( X \)).

We call \( \lambda \) a principal polarisation if it has degree 1, in other words if it is an isomorphism \( X \xrightarrow{\sim} X^* \). By Exc 7.5, a principal polarisation comes from a Riemann form \( (\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}) \) in some basis of \( \Lambda \) (\( I \) is the \( g \times g \) identity matrix). Not every abelian variety admits a principal polarisation, but it is always isogenous to one that does (Exc 9.2).

**Example 9.1.** On an elliptic curve \( X = \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau) \), any Riemann form is an integer multiple of the standard one \( H(z, w) = \frac{1}{\text{Im} \tau} z\overline{w} \). An elliptic curve

\(^{17}\) whose degree is \( \sqrt{\det E} \), where \( E = \text{Im} H \) (Exc 9.1)
is principally polarised via $\lambda_H : X \to X^*$, and every other polarisation has the form $[n] \lambda_H$ for some non-zero $n$.

Now we return to the question of understanding the endomorphism algebra $\text{End}^0 A$ of an abelian variety $A$. Fix a polarisation $\lambda : A \to A^*$. As it is an isogeny, it induces a ring isomorphism $\text{End}^0 A \to \text{End}^0 A^*$ via $\phi \mapsto \lambda \phi \lambda^{-1}$. But also the duality map

$$f \mapsto f^* : \text{End} A \to \text{End}(A^*),$$

induces an anti-isomorphism $\text{End}^0 A \to \text{End}^0 A^*$. Combining the two gives an anti-involution on $\text{End}^0 A$:

**Definition 9.2.** The anti-involution $\iota : \phi \mapsto \phi^\iota = \lambda \phi^* \lambda^{-1}$ on $\text{End}^0 A$ is called the Rosati involution induced by the polarisation $\lambda$.

Note that $\iota([m]) = \lambda[m]^* \lambda^{-1} = \lambda[m] \lambda^{-1} = [m] \lambda \lambda^{-1} = [m]$ (isogenies commute with addition), so $\iota$ acts trivially on $\mathbb{Q} \subset \text{End}_0 A$.

**Example 9.3.** If $E$ is a non-CM elliptic curve, then $\text{End}^0 E = \mathbb{Q}$ and the Rosati involution induced by any $\lambda$ is the identity map $\iota : \mathbb{Q} \to \mathbb{Q}$.

**Example 9.4.** If $E$ is a CM elliptic curve, then the Rosati involution induced by any $\lambda$ is the complex conjugation on $\text{End}^0 E \cong \mathbb{Q}((\sqrt{-d}))$ (check).

Now suppose $A$ is simple, so $D = \text{End}^0 A$ is a finite-dimensional division algebra over $\mathbb{Q}$. Denote by $\text{Tr} = \text{Tr}_{D/\mathbb{Q}}$ the trace from $D$ to $\mathbb{Q}$. It is easy to see what the positive-definiteness of the Riemann form corresponds to:

**Lemma 9.5.** The quadratic form $\phi \mapsto \text{Tr}(\phi \phi^\iota)$ is positive definite on $\text{End}^0 A$.

Division algebras with these properties can be classified completely:

**Theorem 9.6** (Albert). Let $D$ be a finite-dimensional division algebra over $\mathbb{Q}$ with a positive-definite anti-involution $\iota$. Write $K$ for the centre of $D$, and $K_0$ for the subfield of $K$ of $\iota$-invariants. Then $K$ is a field, $K_0$ is a totally real field, and the pair $(D, \iota)$ belongs to one of the following types:

* Type I: $D = K = K_0$ and $\iota$ is identity.
* Type II: $K = K_0$, $D$ is a quaternion algebra over $K$, and there is an isomorphism $D \otimes_{\mathbb{Q}} \mathbb{R} \cong \text{Mat}_{2 \times 2}(\mathbb{R}) \times \cdots \times \text{Mat}_{2 \times 2}(\mathbb{R})$, taking $\iota$ to the involution $(x_1, \ldots, x_e) \mapsto (x_1^t, \ldots, x_e^t)$.
* Type III: $K = K_0$, $D$ is a quaternion algebra over $K$, and there is an isomorphism $D \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{H} \times \cdots \times \mathbb{H}$ taking $\iota$ to $(\iota_H, \ldots, \iota_H)$ with $\iota_H(x) = \text{Tr}_{\mathbb{H}/\mathbb{R}}(x) - x$, the usual involution on the standard (Hamiltonian) quaternions $\mathbb{H}$.

---

18 i.e. it preserves addition and changes the order in multiplication
19 = trace of the left multiplication by $\alpha \in D$ as a $\mathbb{Q}$-linear endomorphism of $D(\cong \mathbb{Q}^e)$
Type IV: $K/K_0$ is a totally imaginary quadratic extension, $D$ is a division algebra over $K$ (of some rank $d^2$) whose Brauer invariants above any fixed finite place of $K_0$ sum to 0, and there is an isomorphism

$$D \otimes_{\mathbb{Q}} \mathbb{R} \cong \text{Mat}_{d \times d}(\mathbb{C}) \times \cdots \times \text{Mat}_{d \times d}(\mathbb{C}),$$

taking $i$ to the involution $(x_1, \ldots, x_{e_0}) \mapsto (\overline{x}_1, \ldots, \overline{x}_{e_0}).$

Let $D$ be a division algebra as in the theorem, and denote $e_0 = [K_0 : \mathbb{Q}]$, $e = [K : \mathbb{Q}]$, $d^2 = \text{dim}_K D$. Can $D$ actually occur as the endomorphism algebra of some abelian variety $A = \mathbb{C}^g / \Lambda$? One restriction is that $d^2 e = \text{dim}_Q D/2g$, since $D$ should act $\mathbb{Q}$-linearly on $\Lambda \otimes \mathbb{Q} \cong \mathbb{Q}^{2g}$.

Conversely, suppose $g \geq 1$ an integer with $\text{dim}_Q D/2g$. It turns out that except when $D$ has Type III with $g/2e \in \{1, 2\}$ or Type IV with $g/e_0d^2 \in \{1, 2\}$ there always is a simple complex abelian variety of dimension $g$ with endomorphism algebra $D$ (see [?]). In the exceptional cases there are explicit additional conditions guaranteeing the existence (see [?]).

Exc 9.1. Show that the degree of the polarisation induced by a Hermitian Riemann form $H$ satisfies $(\deg H)^2 = |\det E|$ (the $2g \times 2g$-determinant of $E = \text{Im} H$ on $\Lambda \times \Lambda$).

Exc 9.2. Give an example of an abelian variety that has no principal polarisation. Show, however, that every abelian variety over $\mathbb{C}$ is isogenous to a principally polarized one.

10. DIFFERENTIALS

Let $X$ be a variety over a field $k = \overline{k}$. The rational $k$-differentials on $X$ are formal finite sums $\omega = \sum f_i dg_i$ with $f_i, g_i \in k(X)$, modulo the relations

$$d(f + g) = df + dg, \quad d(fg) = fdg + gdf, \quad da = 0 \quad (a \in k).$$

If $\text{char} k = 0$, $\text{dim} X = n$ and $t_1, \ldots, t_n \in k(X)$ are algebraically independent, every differential can be written uniquely as $g_1 dt_1 + \cdots + g_n dt_n$ with $g_i \in k(X)$

(Exc 10.1), so their space is $\cong k(X)^n$ as a $k$-vector space.

Example 10.1. $X = \mathbb{P}^1$ has differentials $f(x)dx$ for $f \in k(X) = k(x)$.

Example 10.2. On the curve $C : y^2 = x^3 + 1$ every differential can be written uniquely as $f(x, y)dx$, and also as $h(x, y)dy$ with $f, h \in k(C)$.

(Use that $0 = d(y^2 - x^3 - 1) = 2ydy - 3x^2dx$ to transform between the two).

A differential $\omega$ is regular at $P \in X$ if it has a representation $\omega = \sum_i f_i dg_i$ with $f_i, g_i$ regular at $P$.\footnote{If $P \in X$ is a non-singular point, there is an easy test: pick the algebraically independent functions $g_1, \ldots, g_d \in k(X)$ so that $g_i - g_i(P)$ generate $m_P/m_P^2$, and write $\omega = \sum_i f_i dg_i$. Then $\omega$ is regular at $P$ if and only if all the $f_i$ are (Exc 10.2).} If $\omega$ is regular everywhere, we call it a regular differential, and we write $\Omega_X$ for the $k$-vector space of those. A morphism $\phi : X \to Y$ naturally induces a $k$-linear map

$$\phi^* : \Omega_Y \to \Omega_X, \quad \sum_i f_i dg_i \mapsto \sum_i (\phi^* f_i) d(\phi^* g_i),$$
the pullback of differentials. For complete varieties \( \dim_k \Omega_X \) is finite; if, moreover, \( X \) is projective then regular differentials are the same as holomorphic differentials\(^{21}\).

**Example 10.3.** \( \mathbb{P}^1 \) (and, generally, \( \mathbb{P}^n \)) has no non-zero regular differentials.

**Example 10.4.** The curve \( C : y^2 = x^3 + 1 \) has \( \Omega_C = k \frac{dx}{y} \), of \( k \)-dimension 1.

**Example 10.5.** An abelian variety \( A = \mathbb{C}^g/\Lambda \) has \( \Omega_A = \langle \frac{dz_1}{y}, \ldots, \frac{dz_g}{y} \rangle \), where \( z_i \) are the standard coordinates. In fact, \( \dim_k \Omega_A = \dim A \) for an abelian variety over any \( k \), and all \( \omega \in \Omega_A \) are invariant under translations on \( A \).\(^{22}\)

**Definition 10.6.** The genus \( g \) of a complete non-singular curve \( X \) is \( \dim_k \Omega_X \).

Thus, \( \mathbb{P}^1 \) has genus 0 and \( y^2 = x^3 + 1 \subset \mathbb{P}^2 \) genus 1. Generally:

**Example 10.7.** (Plane curves) A curve given by a non-singular homogeneous equation \( f(x, y, z) \subset \mathbb{P}^2 \) has genus \( g = \frac{(d-1)(d-2)}{2} \), \( d = \deg f \).

**Example 10.8.** (Hyperelliptic curves, \( \text{char } k \neq 2 \)) Let \( f(x) \) be a polynomial of degree \( 2g + 1 \) or \( 2g + 2 \) with no multiple roots, for some \( g \geq 0 \). The two affine charts
\[
y^2 = f(x) \quad \text{and} \quad Y^2 = X^{2g+2} f\left(\frac{1}{X}\right)
\]
glue via \( Y = \frac{y}{x^{g+1}}, \ X = \frac{1}{x} \) to a curve \( C \). The curve is complete, non-singular and admits a degree 2 map \( C \to \mathbb{P}^1 \) (via \( (x, y) \mapsto x \)). Such a curve is called hyperelliptic, and every hyperelliptic curve has a model as above (use that \( [k(C) : k(x)] = 2 \)). The reflection automorphism
\[
(x, y) \mapsto (x, -y) : \quad C \to C
\]
is called the hyperelliptic involution. Here
\[
\Omega_C = \left\langle \frac{dx}{y}, \frac{xdx}{y}, \ldots, \frac{x^{g-1}dx}{y} \right\rangle,
\]
so \( C \) has genus \( g \). (See Exc 10.4).

It is consequence of Riemann-Roch theorem that for \( g \leq 2 \) every complete non-singular curve is hyperelliptic, and genus 3 curves are either hyperelliptic or non-singular plane quartics.

Exc 10.1. Suppose \( X \) is an \( n \)-dimensional variety, \( t_1, \ldots, t_n \in k(X) \) are algebraically independent and the (finite) extension \( k(X)/k(t_1, \ldots, t_n) \) is separable (e.g. \( \text{char } k = 0 \)). Then every rational differential on \( X \) can be written uniquely as \( g_1 dt_1 + \ldots + g_n dt_n \) with \( g_i \in k(X) \).

\(^{21}\)These are special cases of finite-dimensionality of the space of global sections of a coherent sheaf on a complete variety, and of Serre’s ‘Géométrie Algébrique Géométrie Analytique’ (GAGA) principle for complex projective varieties.

\(^{22}\)Otherwise the action by translations would give a non-constant morphism \( A \to \text{GL}(\Omega_A) \).
Exc 10.2. Suppose $X$ is a variety, $P \in X$ a non-singular point, and $g_1, \ldots, g_{\dim X} \in k(X)$ are algebraically independent functions so that $g_i - g_i(P)$ generate the $k$-vector space $m_P/m_P^2$. ($m_P \subset O_{X,P}$ is the maximal ideal.) Then $\omega = \sum f_idg_i$ is regular at $P$ if and only if all the $f_i$ are.

Exc 10.3. Prove that $\mathbb{P}^n$ has no non-zero regular differentials.

Exc 10.4. Suppose $\text{char } k \neq 2$. Let $C : y^2 = f(x)$ with $f(x) \in k[x]$ of degree $2g + 1$ or $2g + 2$ with no multiple roots. Prove that $\Omega_C = \langle \frac{dx}{y}, \frac{x^2dx}{y}, \ldots, \frac{x^{2g-1}dx}{y} \rangle$.

11. DIVISORS

Let $C$ be a complete non-singular curve over $k = \bar{k}$. A divisor on $C$ is a finite formal linear combination of points,

$$D = \sum_{i=1}^{r} n_i(P_i), \quad n_i \in \mathbb{Z}, \quad P_i \in C.$$ 

The degree of $D$ is $\sum n_i$.

If $f \in k(C)^\times$ is a non-zero rational function, define the divisor of $f$

$$(f) = \sum_{P \in C} \text{ord}_P(f)(P).$$

(Recall that the local rings $O_{C,P}$ are discrete valuation rings, and $\text{ord}_P$ denotes the corresponding valuation on $k(X)$.) Divisors of the form $(f)$ are called principal, and it is not hard to see that they have degree 0. Clearly they form a subgroup, and the quotient groups

$$\text{Pic } C = \frac{\text{divisors on } C}{\text{principal divisors}}, \quad \text{Pic}^0 C = \frac{\text{divisors of degree 0 on } C}{\text{principal divisors}}$$

are called the Picard group of $C$ and the degree 0 Picard group of $C$. Two divisors are called linearly equivalent if they have the same class in $\text{Pic } C$.

There is an obvious (split) exact sequence

$$0 \to \text{Pic}^0 C \to \text{Pic } C \xrightarrow{\text{deg}} \mathbb{Z} \to 0.$$

**Example 11.1.** On $C = \mathbb{P}^1$ any divisor $D = \sum_{a \in \mathbb{P}^1} n_a(a)$ of degree 0 is principal,

$$D = (f), \quad f = \prod_{a \neq \infty} (x - a)^{n_a}.$$ 

So $\text{Pic}^0 \mathbb{P}^1 = \{0\}$ and $\text{Pic } \mathbb{P}^1 = \mathbb{Z}$.

**Example 11.2.** On an elliptic curve $E$ with origin $O$ every divisor of degree 0 is linearly equivalent to a divisor of the form $(P) - (O)$ for a unique $P \in E$. Thus $\text{Pic}^0 E \cong E$ and $\text{Pic } E \cong E \times \mathbb{Z}$ as abelian groups.

A morphism of non-singular complete curves $\phi : C \to C'$ induces a map

$$\phi^* : \{\text{divisors on } C'\} \to \{\text{divisors on } C\},$$
the pullback of divisors. For a point \(D = (P)\),
\[
\phi^*(P) = \sum_{f(Q) = P} e_Q(Q),
\]
the sum taken over the pre-images \(Q\) of \(P\), and the coefficient \(e_Q\) the ramification index\(^{23}\) of \(f\) at \(Q\). It is easy to check that
\[
\deg \phi^* D = \deg \phi \deg D \quad \text{and} \quad \phi^*(f) = (f \circ \phi) \quad \text{for} \quad f \in k(D)^	imes,
\]
in particular \(\phi^*\) takes divisors of degree 0 to divisors of degree 0 and principal divisors to principal divisors. So it induces maps
\[
\phi^* : \text{Pic} C' \to \text{Pic} C \quad \text{and} \quad \text{Pic}^0 C' \to \text{Pic}^0 C.
\]

**Example 11.3.** Let \(C : y = x^2 \subset \mathbb{P}^2\) and \(D = \mathbb{P}^1\), with \(\phi : (x, y) \mapsto y\). Then \(\phi^*(a) = (\sqrt{a}, a) + (-\sqrt{a}, a)\) for non-zero \(a\), and \(\phi^*(0) = 2(0, 0)\).

12. **Jacobians over \(\mathbb{C}\)**

Generalising Examples 11.1 and 11.2, it turns out that for any complete non-singular curve \(C\) of genus \(g\) the group \(\text{Pic}^0 C\) has a natural structure of a principally polarized abelian variety of dimension \(g\), the Jacobian of \(C\).

Over the complex numbers this is classical theory of Abel and Jacobi. Thus, suppose \(k = \mathbb{C}\) (so \(C\) is a compact Riemann surface), and choose

1. a basis \(\omega_1, \ldots, \omega_g\) of the space of regular differentials \(\Omega_C\) and
2. a basis \(\gamma_1, \ldots, \gamma_{2g}\) of the first homology group \(H_1(C, \mathbb{Z})\).

Fix a point \(P_0 \in C\) and look at the map
\[
C \to \mathbb{C}^g, \quad P \mapsto \left(\int_{P_0}^P \omega_1, \ldots, \int_{P_0}^P \omega_g\right).
\]
This is not well-defined because the integrals are path-dependent; changing a path by a loop with a class in \(\sum n_i \gamma_i \in H_1(C, \mathbb{Z})\) modifies the integral by \(\sum n_i \lambda_i\), where
\[
\lambda_i = \left(\int_{\gamma_i} \omega_1, \ldots, \int_{\gamma_i} \omega_g\right), \quad (i = 1, \ldots, 2g).
\]
(The integrals \(\int_{\gamma_i} \omega_j\) are called the periods of \(C\)). Letting
\[
\Lambda = \mathbb{Z} \lambda_1 + \ldots + \mathbb{Z} \lambda_{2g} \subset \mathbb{C}^g \quad \text{("period lattice"),}
\]
the integration map \(C \to \mathbb{C}^g/\Lambda\) is now well-defined. Extending it by linearity defines the *Abel-Jacobi map*
\[
(12.1) \quad \{\text{divisors on } C\} \to \mathbb{C}^g/\Lambda.
\]
It turns out that \((H_1(C, \mathbb{Z}) =) \Lambda \hookrightarrow \mathbb{C}^g \quad (= \Omega_C)\) is a lattice, and we have

\[^{23}\text{Defined by } e_Q = \frac{\text{ord}_Q \phi^* f}{\text{ord}_P f}\text{ for any } f \in k(C')\text{ with } \text{ord}_P f \neq 0.\]
Theorem 12.2 (Abel–Jacobi). The map (12.1) a bijection \( \text{Pic}^0 C \to \mathbb{C}^g/\Lambda \). \(^{24}\)

The lattice \( \Lambda = H_1(C,\mathbb{Z}) \) carries a natural non-degenerate alternating form \( E : \Lambda \times \Lambda \to \mathbb{Z} \) of determinant 1, the intersection pairing for homology classes\(^{25}\); one checks that after embedding \( \Lambda \hookrightarrow \mathbb{C}^g \), the form satisfies \( E(iu, iv) = E(u, v) \) for \( u, v \in \mathbb{C}^g \). So \( E \) is a Riemann form and gives \( \mathbb{C}^g/\Lambda \) the structure of a principally polarized abelian variety, the Jacobian \( \text{Jac} C \) of \( C \).

Example 12.3. Let \( C \) be the genus 2 hyperelliptic curve \( y^2 = x^6 - 1 \) over \( \mathbb{C} \). Here \( \Omega_C = \langle dx/y, xdx/y \rangle \), and we let \( \alpha_1, \alpha_2, \beta_1, \beta_2 \) be the standard ‘symplectic’ basis of \( H_1(C,\mathbb{Z}) \) as in Figure 1; thus \( E(\alpha_j, \beta_j) = 1 = -E(\beta_j, \alpha_j) \), and the rest are 0.

To represent \( C \) as a Riemann surface, make 3 cuts in \( C \) between the roots of \( x^6 - 1 \) (6th roots of unity), see Figure 2. There are two continuous branches of \( \sqrt{x^6 - 1} \) on the complement, in other words every point \( (x, y) \in C \) with \( x \notin \{ \text{cuts} \} \) lies on one of the two sheets. Glueing them together gives \( C \), which is topologically a surface as in Figure 3 (the cuts become joining circles), visibly of genus 2.

The period lattice \( \Lambda \subset \mathbb{C}^2 \) is spanned by 4 vectors

\[
\left( \int_{\gamma} \frac{dx}{y}, \int_{\gamma} \frac{x}{y} \right) = \left( \int_{\gamma} \frac{dz}{\sqrt{z^6 - 1}}, \int_{\gamma} \frac{z}{\sqrt{z^6 - 1}} \right), \quad \gamma \in \{ \alpha_1, \alpha_2, \beta_1, \beta_2 \},
\]

\(^{24}\)Abel showed that the degree 0 divisors in the kernel of (12.1) are precisely the divisors of meromorphic functions, and Jacobi proved surjectivity.

\(^{25}\)To define \( E(\gamma, \gamma') \) pick closed loops representing \( \gamma \) and \( \gamma' \) that intersect each other transversally in a finite set of points. Then follow \( \gamma \), and count the number of times \( \gamma' \) meets it from the left minus the ones from the right (\( C \) is oriented). This is bilinear and alternating by construction, and also non-degenerate of determinant 1 (look at the standard generators of \( H_1(C,\mathbb{Z}) \), loops going ‘once around the holes’ as in Figure 1).
the plane integrals taken over the four loops in Figure 4, and the dotted lines indicate ‘the other sheet’, i.e. $-\sqrt{z^6-1}$ in the denominator instead. This is the same as changing the sign and integrating in the opposite direction. By continuity we can deform all 4 integrals to twice the integrals along the line segments as in Figure 5 (the third one with minus).

Figure 5

The 2 components for the 4 basis vectors of $\Lambda$ are therefore

$$\int_{j/6}^{(j+1)/6} 2\pi i \frac{e^{2\pi i tk}}{\sqrt{e^{12\pi it}}-1}, \quad j \in \{0, 4, 1, 3\}, k \in \{1, 2\},$$

again with minus for the third integral. Evaluated numerically, they are

$$\text{constant} \times \left( \frac{1}{\zeta}, \frac{1}{i}, \frac{-\zeta}{i} \right), \quad \zeta = e^{2\pi i/3}.$$

Move the first 2 vectors to $\left( \begin{smallmatrix} 1 \\ 0 \end{smallmatrix} \right)$ and $\left( \begin{smallmatrix} 0 \\ 1 \end{smallmatrix} \right)$ with an element of $\text{GL}_2(\mathbb{C})$, we get

$$\text{Jac } C \cong \mathbb{C}^2/\Lambda, \quad \Lambda = \langle (\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}), (\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}), \frac{i}{\sqrt{3}}(\begin{smallmatrix} 2 \\ -1 \end{smallmatrix}), \frac{i}{\sqrt{3}}(\begin{smallmatrix} -1 \\ 2 \end{smallmatrix}) \rangle.$$

Note that $\Lambda$ contains an index 12 sublattice

$$2\langle (\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}), (\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}), (\begin{smallmatrix} \zeta \\ 0 \end{smallmatrix}), (\begin{smallmatrix} 0 \\ \zeta \end{smallmatrix}) \rangle, \text{ so}$$

$\text{Jac } C \sim E \times E$ (via the corresponding 12-isogeny), where $E = \mathbb{C}/\mathbb{Z} + \zeta\mathbb{Z}$ is the unique elliptic curve over $\mathbb{C}$ with an automorphism of order 6,

$$E : y^2 = x^3 + 1.$$

In particular, $\text{End}^0(\text{Jac } C) \cong \text{GL}_2(\mathbb{Q}(\zeta))$.

Now we go back to an arbitrary complete non-singular curve $C$ over $\mathbb{C}$ with a fixed base point $P_0 \in \mathbb{C}$. We have defined a map

$$P \mapsto \left( \int_{P_0}^P \omega_1, \ldots, \int_{P_0}^P \omega_9 \right) : \quad C \rightarrow \mathbb{C}^g/\Lambda = \text{Jac } C,$$

which is clearly holomorphic, and therefore a morphism by Chow’s theorem. (Recall that both compact Riemann surfaces and abelian varieties over $\mathbb{C}$ are projective varieties.) Seeing the Jacobian as $\text{Pic}^0$, the map is

$$C \rightarrow \text{Pic}^0 C, \quad P \mapsto (P) - (P_0),$$

and it is an embedding unless $C \cong \mathbb{P}^1$. 

---

**NOTES ON ABELIAN VARIETIES [PART I]**

29
The Jacobian of $C$ is functorial in two ways. A non-constant map of curves

$$\phi : C \mapsto C'$$

induces maps $\phi_* : \text{Jac } C \to \text{Jac } C'$ and $\phi^* : \text{Jac } C' \to \text{Jac } C$, given on the level of divisors by the usual pushforward and pullback of divisors

$$\phi_*(Q) = \phi Q, \quad \phi^*(P) = \sum_{f(Q) = P} \epsilon_Q(Q),$$

restricted to $\text{Pic}^0 = \text{Jac}$. Clearly $\phi_* \circ \phi^* = [\deg \phi]$, in particular $\phi_*$ is onto, and $\ker \phi^*$ is finite. On the level of ambient spaces,

$$\phi^* : \Omega_{C'}/H_1(C', \mathbb{Z}) = \mathbb{C}^g/\Lambda' \to \mathbb{C}^g/\Lambda = \Omega_C/H_1(C, \mathbb{Z})$$

is induced by the usual pullback of differentials $\phi^* : \Omega_{C'} \to \Omega_C$.

**Example 12.4.** Let us use these purely functorial properties to compute (up to isogeny) the Jacobian of

$$C : y^2 = ax^6 + bx^4 + cx^2 + d.$$

Supposing the right-hand side has no multiple roots, $C$ is a genus 2 hyperelliptic curve. It admits two non-constant maps to elliptic curves,

$$\phi : C \to E_1 : y^2 = ax^3 + bx^2 + cx + d$$

$$\psi : C \to E_2 : y^2 = dx^3 + cx^2 + bx + a$$

given by $(x, y) \mapsto (x^2, y)$ and $(x, y) \mapsto \left(\frac{1}{x^2}, \frac{y}{x^3}\right)$ respectively. The pullback gives morphisms of abelian varieties with finite kernels

$$\phi^* : E_1 \to \text{Jac } C, \quad \psi^* : E_2 \to \text{Jac } C.$$

By Poincare reducibility theorem, $\text{Jac } C \sim E_1 \times E_2$ if $E_1 \not\sim E_2$. If $E_1 \sim E_2$, the claim is still true, because

$$\phi^* \frac{dx}{y} = \frac{d(x^2)}{y} = \frac{2xdx}{y},$$

$$\psi^* \frac{dx}{y} = \frac{d(1/x^2)}{y/x^3} = -\frac{2dx}{y}$$

are linearly independent, so $\phi^*$ and $\psi^*$ map the lattices of $E_1$ and $E_2$ into different complex subspaces of $\mathbb{C}^2$, and the two image lattices generate that of $\text{Jac } C$ up to finite index.

Conversely, any genus 2 curve whose Jacobian is not simple is isomorphic to one of the form $y^2 = ax^6 + bx^4 + cx^2 + d$ (Exc 12.2).

Exc 12.1. Suppose $C : y^2 = f(x)$ with $f \in \mathbb{C}[x]$ of even degree $2g + 2$ with distinct roots $\alpha_i$. (Any genus $g$ hyperelliptic curve over $\mathbb{C}$ has such an equation.) For $j = 2, \ldots, 2g + 2$ fix any path in $\mathbb{C}$ from $\alpha_1$ to $\alpha_j$ that does not pass through the $\alpha_k$ and any continuous branch of $\sqrt{f(z)}$ along the path. Generalising Example 12.3, show that the vectors

$$\left( \int_{\alpha_1}^{\alpha_j} \frac{ds}{\sqrt{f(s)}}, \int_{\alpha_1}^{\alpha_j} \frac{sds}{\sqrt{f(s)}}, \ldots, \int_{\alpha_1}^{\alpha_j} \frac{s^{g-1}ds}{\sqrt{f(z)}} \right), \quad j = 2, \ldots, 2g + 2$$

generate the period lattice of $C$.

Exc 12.2. Suppose $C$ is a hyperelliptic genus 2 curve whose Jacobian is not simple. Then $C \cong y^2 = ax^6 + bx^4 + cx^2 + d$. (You may use Torelli’s theorem — see below.)