Abelian varieties over local and global fields

Alexei N. Skorobogatov

March 17, 2016

Contents

1 Geometry

1.1 Definition and basic properties

Let k be a field. A variety over k is a scheme over k which is geometrically integral and of finite type.

Definition 1.1 *An abelian variety over k is a* **proper** *variety A with a distinguished element $0 \in A(k)$ (the origin of the group law) and morphisms $m : A \times A \to A$ (group law) and $[-1] : A \to A$ (the inverse) satisfying the axioms of a group.*

So the set of points $A(k)$ is a group. In this section k is assumed to be algebraically closed.

Some results immediately follow from the definition.

Proposition 1.2 *Any abelian variety is non-singular.*

Proof. This follows from the existence of one non-singular point and the transitive action of A on itself by translations. □

Proposition 1.3 *Any abelian variety is commutative.*

Proof. We need to prove that the action of A on itself by conjugations is trivial. This action fixes $0 \in A$, so it defines an action of A on the local ring $\mathcal{O}$ at 0. Let $\mathfrak{m}$ be the maximal ideal of $\mathcal{O}$. (Then $\mathcal{O}/\mathfrak{m} = k$.) The induced action on the finite-dimensional k-vector space $\mathcal{O}/\mathfrak{m}^n$ defines a homomorphism $A \to \mathrm{GL}(\mathcal{O}/\mathfrak{m}^n)$, which is a morphism from the proper connected variety A to the affine variety $\mathrm{GL}(\mathcal{O}/\mathfrak{m}^n)$. Any such morphism is constant. Hence the induced action on $\mathcal{O}/\mathfrak{m}^n$ is trivial. Since the intersection of all powers of $\mathfrak{m}$ is 0, we see that A acts trivially on $\mathcal{O}$. But $\mathcal{O}$ is a localisation of the ring of regular functions $k[U]$ on some affine neighbourhood $U \subset A$ of 0, in particular, $k[U] \subset \mathcal{O}$, hence the action on $k[U]$ and thus on U is trivial. It follows that the action of A by conjugations is trivial on the irreducible component of A that contains U, but this is just A. □

1.2 Theorem of the cube

Theorem 1.4 (of the cube) *Let X, Y, Z be varieties over k, where X and Y are proper. Then any line bundle on $X \times Y \times Z$ that restricts to trivial line bundles on $x_0 \times Y \times Z$, $X \times y_0 \times Z$ and $X \times Y \times z_0$ must be trivial.*

See [3] for a proof.

The meaning of this theorem is as follows. Let $\mathcal{F}$ be a contravariant functor from varieties to abelian groups. Then we have homomorphisms induced by projections

$$\mathcal{F}(\prod_{i=1, i\neq j}^{n} X_i) \longrightarrow \mathcal{F}(\prod_{i=1}^{n} X_i).$$

Let $U_n \subset \mathcal{F}(\prod_{i=1}^n X_i)$ be the sum of the images of all such homomorphisms induced by the projections that forget one of the factors of $\prod_{i=1}^n X_i$. One would wish to know when $U_n = \mathcal{F}(\prod_{i=1}^n X_i)$.

To answer this question fix a point on each variety X_i and call it x_i. For a non-empty subset $I \subset \{1, \ldots, n\}$ define V_I as the intersection of kernels of the restriction maps defined by assigning to the i-th coordinate the value x_i:

$$V_I = \mathrm{Ker}[\mathcal{F}(\prod_{i\in I} X_i) \longrightarrow \bigoplus_{j\in I} \mathcal{F}((\prod_{i\in I,\ i\neq j} X_i) \times x_j).$$

Write V_n for $V_{\{1,\ldots,n\}}$.

Lemma. *We have* $\mathcal{F}(\prod_{i=1}^n X_i) = U_n \oplus V_n$.
Proof. Let us prove by induction on n that

$$\mathcal{F}(\prod_{i=1}^n X_i) = \mathcal{F}(k) \oplus \bigoplus_{\emptyset \subsetneq I \subseteq \{1,\dots,n\}} V_I.$$

For $n = 1$ the restriction map $\mathcal{F}(X) \to \mathcal{F}(x) = \mathcal{F}(k)$ has a section, so we have

$$\mathcal{F}(X) = \mathcal{F}(k) \oplus \mathrm{Ker}[\mathcal{F}(X) \longrightarrow \mathcal{F}(x)] = U_1 \oplus V_1.$$

Now assume the statement is proved for $n-1$. The group V_n is the kernel of the restriction map

$$\mathcal{F}(\prod_{i=1}^n X_i) \longrightarrow \bigoplus_{j=1}^n \mathcal{F}(\prod_{i=1}^{j-1} X_i \times x_j \times \prod_{i=j+1}^n X_i).$$

Using the inductive assumption one sees that this map factors through

$$\mathcal{F}(\prod_{i=1}^n X_i) \longrightarrow \mathcal{F}(k) \oplus \bigoplus_{\emptyset \subsetneq I \subsetneq \{1,\dots,n\}} V_I.$$

The last map has a natural section whose image is contained in U_n, so this proves our statement and the lemma. $\square$

The functor $\mathcal{F}$ has *order* $n-1$ if $V_n = 0$. This definition makes sense since although V_n depends on the choice of points x_i, U_n doesn't. In this language the theorem of the cube says that the functor Pic from proper varieties to abelian groups is quadratic, that is, has order 2. In concrete terms this means that any line bundle on $X \times Y \times Z$ is a product of line bundles pulled back from $X \times Y$, $Y \times Z$ and $X \times Z$.

Corollary 1.5 *(i) Consider the following morphisms $A \times A \times A \to A$: the sum of all three coordinates s, the sum of two of the coordinates s_{ij} and the projections p_i. For any $L \in Pic(A)$ we have*

$$s^*L \otimes s_{12}^*L^{-1} \otimes s_{23}^*L^{-1} \otimes s_{13}^*L^{-1} \otimes p_1^*L \otimes p_2^*L \otimes p_3^*L = 0 \ \in \ \mathrm{Pic}(A \times A \times A).$$

(ii) $[n]^*L = L^{(n^2+n)/2} \otimes [-1]^*L^{(n^2-n)/2}$.

(iii) ("Theorem of the square") For $x \in A$ let us denote by T_x the translation by x, that is, $T_x(y) = x + y$. Then for any $x, y \in A$ we have $T_{x+y}^*L \otimes L = T_x^*L \otimes T_y^*L$.

Proof. Let us choose 0 as the base point in A. Then (i) immediately follows from the theorem of the cube.

(ii) Consider the morphism $A \to A \times A \times A$ given by $x \mapsto (x, x, -x)$. The pull-back of the formula from (i) gives $L^3 \otimes [-1]^* L = [2]^* L$ which is (ii) for $n = 2$. Now consider the morphism $A \to A \times A \times A$ given by $x \mapsto (2x, x, -x)$. Then the pull-back of the formula from (i) gives $[2]^* L^2 \otimes [-1]^* L = [3]^* L$, which is (ii) for $[3]^* L$. Continue by induction.

(iii) Consider the morphism $A \to A \times A \times A$ given by $z \mapsto (x, y, z)$. Then the pull-back of the formula from (i) gives (iii). □

To each line bundle L on A we attach a map from A to $\mathrm{Pic}(A)$ as follows:

$$\varphi_L(x) = T_x^* L \otimes L^{-1} \ \in \ \mathrm{Pic}(A).$$

Then Corollary 1.5 says that φ_L is a homomorphism. Define

$$K(L) = \mathrm{Ker}(\varphi_L) \ \subset \ A.$$

Exercises Show that $\varphi_{L \otimes M}(x) = \varphi_L(x) + \varphi_M(x)$ and $\varphi_{T_y^* L}(x) = \varphi_L(x)$.

1.3 Quotients and isogenies

We quote another result from algebraic geometry.

Theorem 1.6 (Seesaw principle) *Let X be a* **proper** *variety and let L be a line bundle over $X \times Y$.*

(i) The set of points $y \in Y$ such that L restricts trivially to $X \times y$ is close in Y.

(ii) $L = p_2^* M$ for a line bundle M on Y, where $p_2 : X \times Y \to Y$ is the second projection, if and only if L restricts to a trivial line bundle over $X \times y$ for any $y \in Y$.

(iii) $L = 0$ if and only if L restricts to a trivial line bundle over $X \times y$ for all $y \in Y$ and L restricts to a trivial line bundle over $x \times Y$ for at least one point $x \in X$.

It is clear that (iii) is an immediate consequence of (ii).

Corollary 1.7 *$K(L)$ is closed in A.*

Proof. Recall that L is a line bundle on an abelian variety A. Consider the line bundle $m^* L \otimes p_2^* L^{-1}$ on $A \times A$. It restricts trivialy to $x \times A$ if and only if $x \in K(L)$. So the statement follows from Theorem 1.6 (i). □

Corollary 1.8 *Let $B \subset A$ be the neutral connected component of $K(L)$. Then the line bundle $m^* L \otimes p_1^* L^{-1} \otimes p_2^* L^{-1}$ on $A \times A$ restricts to a trivial line bundle on $B \times B$.*

Proof. Use Theorem 1.6 (iii) for $x = 0$. □

Proposition 1.9 *If L is ample, then $K(L)$ is finite.*

Proof. By Corollary 1.8 the line bundle $m^*L \otimes p_1^*L^{-1} \otimes p_2^*L^{-1}$ is trivial on $B \times B$. Pulling it back via the morphism $B \to B \times B$ given by $x \mapsto (x, -x)$ we see that $L \otimes [-1]^*L$ is trivial on B. However, both L and $[-1]^*L$ are ample, so this is a contradiction unless $B = 0$. □

Remark When L is the line bundle associated with an effective divisor, then $|K(L)| < \infty$ implies that L is ample, see [3, Ch. II, §6, Prop. 1]. One also shows that if $U \subsetneq A$ is an open affine subset, then the sum D of the irreducible components of the closed set $A \setminus U$ is an ample divisor (*ibid.*) In particular, ample divisors on A exist. Thus every abelian variety is projective (and not just proper).

Proposition 1.10 *For each $n \neq 0$ the multiplication by n morphism $[n] : A \to A$ is surjective, so that the group of points A is divisible. The kernel $A[n]$ of $[n]$ is finite.*

Proof. We can clearly assume that $n > 1$. Since A is irreducible, the surjectivity of $[n]$ is equivalent to the condition that $\dim([n]A) = \dim(A)$. Since $[n]$ is a homomorphism, the fibres are cosets and so have the same dimension. Since $\dim([n]A) + \dim([n]^{-1}(0)) = \dim(A)$ the two statements of the proposition are equivalent. Take any ample line bundle L. Then $L^{(n^2+n)/2}$ and $[-1]^*L^{(n^2-n)/2}$ are both ample, $[n]^*L$ is ample by Corollary 1.5 (ii). But $A[n] \subset K([n]^*L)$, we conclude that both these sets are finite by Proposition 1.9. □

Definition 1.11 *A surjective homomorphism of abelian varieties $f : A \to B$ is called an* **isogeny** *if its kernel is finite.*

The *degree* $\deg(f)$ of an isogeny $f : A \to B$ is defined as the degree of the finite extension of function fields $[k(A) : k(B)]$. If E is the separable closure of $k(B)$ in $k(A)$, then

$$\deg_{\text{sep}}(f) = [E : k(B)]$$

is the *separable degree* of f. The separable degree of f is the number of points in each fibre of f. One says that f is separable if $\deg(f) = \deg_{\text{sep}}(f)$. Next,

$$\deg_{\text{insep}}(f) = [k(A) : E]$$

is the *inseparable degree* of f. The inseparable degree is always 1 if $\text{char}(k) = 0$. If $\text{char}(k) = p > 0$, then $\deg_{\text{insep}}(f) = p^m$ for some $m \geq 0$.

The degree of f can be calculated in terms of the induced action of f on divisors: if $g = \dim(A) = \dim(B)$ and D is a divisor on B such that the self-intersection index $(D)_B^g > 0$, then

$$(f^*D)_A^g = \deg(f)(D)_B^g.$$

Proposition 1.12 *The homomorphism $[n] : A \to A$ is an isogeny of degree n^{2g}. If n is prime to the characteristic of k, then $[n]$ is separable. In this case the abelian group $A[n]$ is isomorphic to $(\mathbb{Z}/n)^{2g}$.*

Proof. Take an ample divisor D on A. By passing to $D + [-1]D$ we can assume that D is symmetric, i.e. invariant under the antipodal involution $[-1]$. Then $[n]^*D$ is linearly equivalent to n^2D. Hence $\deg([n]) = n^{2g}$. If n is prime to $\mathrm{char}(k)$, this implies that p does not divide $\deg([n])$, so $[n]$ is separable. For r dividing n we have $A[r] \subset A[n]$. Using this and the fact that $\deg([r]) = r^{2g}$ for any such r we deduce that the abelian group $A[n]$ is isomorphic to $(\mathbb{Z}/n)^{2g}$. $\square$

In particular, if ℓ is a prime not equal to $\mathrm{char}(k)$, then the projective limit

$$T_\ell(A) = \varprojlim A[\ell^n]$$

taken for $n \to \infty$ with respect to the natural surjective maps $A[\ell^n] \to A[\ell^m]$, $n \geq m$, is isomorphic to $\mathbb{Z}_\ell^{2g}$, where $\mathbb{Z}_\ell$ is the ring of ℓ-adic integers. This abelian group is called the ℓ-adic *Tate module* of A.

Theorem 1.13 *There is a bijection between finite subgroups of an abelian variety A and* **separable** *isogenies $f : A \to B$ (considered up to an isomorphism of B).*

Sketch of proof. The proof is based on a result from algebraic geometry which states the existence and the uniqueness of the quotient variety by the action of a finite group of automorphisms. More precisely, let X be a *quasi-projective* variety and let G be a finite group of automorphisms of X. Then X has a covering by G-invariant open affine subsets $\mathrm{Spec}(R_i)$, where R_i is a k-algebra. There exists a variety Y covered by open affine subsets $\mathrm{Spec}(R_i^G)$ and a morphism $\pi : X \to Y$ whose restriction to each $\mathrm{Spec}(R_i)$ is the natural morphism $\mathrm{Spec}(R_i) \to \mathrm{Spec}(R_i^G)$. The fibres of π are orbits of G. One also proves that the morphism π is finite (this is essentially the statement that each R_i is a finitely generated R_i^G-module), separable and surjective morphism. The finite extension $k(X)/k(Y)$ is a Galois extension with the Galois group G.

If G acts freely on X, in the sense that the stabiliser of each point is trivial, then π is étale (=flat and unramified).

Now if X is a commutative group and $G \subset X$ is a finite subgroup, then the set $Y = X/G$ inherits the group structure from X. The composition law and the operation of taking the inverse are morphisms. Indeed, the composition of Y comes from the morphism $X \times X \to X \to Y$ which sends $G \times G$ to 0 and hence descends to a morphism $Y \times Y \to Y$, and similarly for the inverse. The image of a proper variety is again proper, so any quotient of an abelian variety by a finite subgroup G is again an abelian variety. It is clear that the kernel of the resulting isogeny is G.

If $f : A \to B$ is a separable isogeny, then, by the universal property of the quotient, there is a morphism $A/\mathrm{Ker}(f) \to B$ which is separable and bijective on points. It follows that it induces an isomorphism of function fields. Then it must be an isomorphism. $\square$

1.4 Dual abelian variety

We continue to explore the properties of the map $\varphi_L : A \to \mathrm{Pic}(A)$ which sends $x \in A$ to $T_x^* L \otimes L^{-1} \in \mathrm{Pic}(A)$. Writing the group law of $\mathrm{Pic}(A)$ additively we have $\varphi_{L\otimes M}(x) = \varphi_L(x) + \varphi_M(x)$.

Definition 1.14 *Let* $\mathrm{Pic}^0(A)$ *be the subgroup of* $\mathrm{Pic}(A)$ *such that* $L \in \mathrm{Pic}^0(A)$ *if and only if* φ_L *is the zero homomorphism.*

Corollary 1.5 (iii) gives

$$T_y^*(T_x^* L \otimes L^{-1}) = T_{x+y}^* L \otimes T_y^* L^{-1} \cong T_x^* L \otimes L^{-1},$$

which says that $\varphi_L(x) \in \mathrm{Pic}^0(A)$. In other words, φ_L is actually a map $A \to \mathrm{Pic}^0(A)$. Thus we have an exact sequence of abelian groups

$$0 \to \mathrm{Pic}^0(A) \to \mathrm{Pic}(A) \to \mathrm{Hom}(A, \mathrm{Pic}^0(A)), \tag{1}$$

where the third map sends L to φ_L.

An equivalent definition is:

Proposition 1.15 $L \in \mathrm{Pic}^0(A)$ *if and only if the line bundle* $m^* L \otimes p_1^* L^{-1} \otimes p_2^* L^{-1}$ *on* $A \times A$ *is trivial.*

Proof. Indeed, by the seesaw principle this happens if and only if the restrictions to $A \times x$ are trivial for all $x \in A$ (these are precisely $T_x^* L \otimes L^{-1}$) and the restriction to $0 \times A$ is trivial too (this is obviously true). $\square$

Extensions of commutative algebraic groups. For commutative algebraic groups A, B over k, the abelian group $\mathrm{Ext}^1(A, B)$ is defined as the set of equivalence classes of extensions of A by B:

$$0 \to B \to ? \to A \to 0,$$

where the arrows are morphisms of algebraic groups, i.e. homomorphisms of the groups of k-points which are also morphisms of algebraic varieties. Two extensions are equivalent when they are linked by the maps that are identities on A and B. Pull-back and push-forward of exact sequences show that $\mathrm{Ext}^1(A, B)$ is covariant in B and contravariant in A. Addition in $\mathrm{Ext}^1(A, B)$ is defined by pulling back the sum

of two extensions in $\mathrm{Ext}^1(A\times A, B\times B)$ via the diagonal $A\to A\times A$ and pushing it forward via the composition $B\times B\to B$. The neutral element in $\mathrm{Ext}^1(A,B)$ is the direct product $A\times B$. The key fact is that $\mathrm{Ext}^1(A,B)$ is *an additive bi-functor* from the category of commutative algebraic groups over k to the category of abelian groups, see [7, Ch. VII, §1]. Let us point out that this construction of Ext does not use any cohomology theory. One directly constructs 6-term exact sequences involving Hom and Ext associated to an extension. One also defines $\mathrm{Ext}^n(A,B)$ for $n\geq 2$ using n-fold extensions, using the same notion of equivalent extensions.

Picard group. Line bundles and torsors on a given variety are related in a canonical way: removing the zero section from a line bundle on X produces an étale X-torsor whose structure group is the multiplicative group $\mathbb{G}_m$. More precisely, the Picard group $\mathrm{Pic}(X)$ is the group of invertible coherent sheaves of O_X-modules, so that $\mathrm{Pic}(X)=\mathrm{H}^1_{\mathrm{Zar}}(X,O_X^*)$. Let $\pi: X_{\mathrm{et}}\to X_{\mathrm{Zar}}$ be the continuous morphism of sites induced by the identity on X. We have $(R^1\pi_*)(\mathbb{G}_m)=0$ (Grothendieck's version of Hilbert's theorem 90, see [1]), and the Leray spectral sequence entails a canonical isomorphism

$$\mathrm{Pic}(X)=\mathrm{H}^1_{\mathrm{Zar}}(X,\mathbb{G}_{m,X})\xrightarrow{\sim}\mathrm{H}^1_{\mathrm{et}}(X,\mathbb{G}_{m,X}).$$

Alternatively, to an invertible sheaf $\mathcal{L}$ one directly associates a torsor T for $\mathbb{G}_{m,X}$ defined by $T(U)=\mathrm{Isom}_U(O_U,f^*\mathcal{L})$, where $f: U\to X$ is étale. This gives an equivalence of the category of invertible sheaves of $\mathcal{O}_X$-modules and the category of étale X-torsors for $\mathbb{G}_{m,X}$, see [Arcata], Prop. II.2.3.

Now we go back to the case when our variety is an abelian variety A. A particular kind of A-torsors for $\mathbb{G}_m$ is given by commutative group extensions of A by $\mathbb{G}_m$:

$$0\to\mathbb{G}_m\to ?\to A\to 0.$$

In these terms we can state another equivalent definition:

Proposition 1.16 *$L\in\mathrm{Pic}^0(A)$ if and only if the A-torsor $L\setminus 0$ for $\mathbb{G}_m$ has a group structure of a commutative extension of A by $\mathbb{G}_m$. Associating an A-torsor for $\mathbb{G}_m$ to an extension gives an injective map $\mathrm{Ext}^1(A,\mathbb{G}_m)\to\mathrm{Pic}(A)$ whose image is $\mathrm{Pic}^0(A)$.*

Proof. Let us show that a torsor coming from an extension of A by $\mathbb{G}_m$ defines an element of $\mathrm{Pic}^0(X)$. Let L be the line bundle on A such that this torsor is $L\setminus 0$. By Proposition 1.15 we need to show that the line bundle m^*L on $A\times A$ is isomorphic to $p_1^*L\otimes p_2^*L$. The pull-back m^* defines a homomorphism

$$\mathrm{Ext}^1(A,\mathbb{G}_m)\longrightarrow\mathrm{Ext}^1(A\times A,\mathbb{G}_m)=\mathrm{Ext}^1(A,\mathbb{G}_m)\oplus\mathrm{Ext}^1(A,\mathbb{G}_m),$$

where the equality is due to the fact that $\mathrm{Ext}^1(A,\mathbb{G}_m)$ is an additive functor in the first argument. Thus the line bundle m^*L on $A\times A$ comes from an element of

$\mathrm{Ext}^1(A \times A, \mathbb{G}_m)$ which is the composition of two extensions of A by $\mathbb{G}_m$. Hence $m^*L = p_1^*L_1 \otimes p_2^*L_2$ for some line bundles L_1 and L_2 on A. By restricting to $A \times 0$ and $0 \times A$ we see that $L_1 = L_2 = L$. Thus $L \in \mathrm{Pic}^0(A)$.

This gives a map $\mathrm{Ext}^1(A, \mathbb{G}_m) \to \mathrm{Pic}^0(A)$. Let us prove that this map is injective. If the torsor defined by an extension E is trivial, it has a section $\sigma : A \to E$, which is *a priori* only a morphism of varieties and not necessarily a homomorphism. We need to show that the extension E is trivial, i.e., there is an isomorphism of algebraic groups $E \cong A \times \mathbb{G}_m$. By modifying σ by an element of $\mathbb{G}_m(k)$ we can assume that $\sigma(A)$ contain the origin of the group law of E. Since $\sigma(A)$ is a proper subvariety of E, the subgroup $S \subset E$ generated by $\sigma(A)$ is also proper. Hence $E \cap \mathbb{G}_m$ must be finite. This gives a finite morphism $S \to A$; in particular, $\dim(S) = \dim(A)$. But A is irreducible, so $\sigma(A)$ is an irreducible component of S. An irreducible component of an algebraic group which contains the origin of the group law is a subgroup, hence $S = \sigma(A)$, so σ is in fact a homomorphism. This gives an isomorphism of algebraic groups $E \cong A \times \mathbb{G}_m$.

To show that the map $\mathrm{Ext}^1(A, \mathbb{G}_m) \to \mathrm{Pic}^0(A)$ is surjective one uses the triviality of $m^*L \otimes p_1^*L^{-1} \otimes p_2^*L^{-1}$ on $A \times A$ to define a commutative group structure on $L \setminus 0$, see [7, Ch. VII, §15]. □

Corollary 1.17 *There is a canonical isomorphism of abelian groups*

$$\mathrm{Pic}^0(A) = \mathrm{Ext}^1(A, \mathbb{G}_m), \tag{2}$$

called **the Barsotti–Weil formula**.

Lemma 1.18 *Let S be a variety and let M be a line bundle on $A \times S$. For $s \in S$ write M_s for the restriction $M|_{A \times s}$. Then $M_{s_1} \otimes M_{s_2}^{-1} \in \mathrm{Pic}^0(A)$ for any $s_0, s_1 \in S$.*

Proof. We cover S by open sets, so that it is enough to prove the statement for an open set that can be taken small enough. In particular, we can assume that $M|_{0 \times S} = 0$. By twisting M by a line bundle pulled back from A we can assume that $M|_{A \times s_0} = 0$. To prove that $M_s \in \mathrm{Pic}^0(A)$ it is enough to show that the line bundle $m^*M_s \otimes p_1^*M_s^{-1} \otimes p_2^*M_s^{-1}$ on $A \times A$ is trivial. This bundle is the restriction to $A \times A = A \times A \times s$ of the obvious line bundle on $A \times A \times S$. But this is a trivial line bundle by the theorem of the cube. □

The meaning of this lemma is that the continuous deformations of the trivial line bundle are in $\mathrm{Pic}^0(A)$. Divisors D and D' on a variety X are *algebraically equivalent*, if there is a family of divisors parametrised by a (connected) variety of which D and D' are members. In this language $\mathrm{Pic}^0(A)$ is the group of divisor classes algebraically equivalent to 0.

Proposition 1.19 *For any ample line bundle L on A we have $\varphi_L(A) = \mathrm{Pic}^0(A)$.*

See [3, Ch. II, §8, Thm. 1] for a proof.

This gives an exact sequence of abelian groups

$$0 \longrightarrow K(L) \longrightarrow A \xrightarrow{\varphi_L} \mathrm{Pic}^0(A) \longrightarrow 0.$$

In *characteristic zero* we can use Theorem 1.13 to identify $\mathrm{Pic}^0(A)$ with the group of k-points of an abelian variety, which is well defined up to isomorphism. Then φ_L becomes an isogeny.

Definition 1.20 *The dual abelian variety A^t is the abelian variety whose group of k-points is $\mathrm{Pic}^0(A)$.*

This result can be made more precise in several ways.

First of all, one shows that the line bundle $m^*L \otimes p_1^*L^{-1} \otimes p_2^*L^{-1}$ on $A \times A$ descends to $A \times A^t$. In other words, it is the pull-back of a line bundle P on $A \times A^t$:

$$m^*L \otimes p_1^*L^{-1} \otimes p_2^*L^{-1} = (\mathrm{id}, \varphi_L)^*P. \tag{3}$$

To construct P one extends the action of $K(L)$ by translations on A to the action on $A \times A$ which is trivial on the first component. Translations by the points of $K(L)$ preserve L, hence this action of $K(L)$ on A preserves $m^*L \otimes p_1^*L^{-1} \otimes p_2^*L^{-1}$, and thus extends to an action of $K(L)$ on this line bundle. The restriction of $m^*L \otimes p_1^*L^{-1} \otimes p_2^*L^{-1}$ to $0 \times A$ is the trivial bundle canonically isomorphic to the fibre of L^{-1} at 0, ie., this is the direct product $L^{-1}(0) \times A$. The above action of $K(L)$ on $A \times A$ extends to a well defined action of $K(L)$ on $m^*L \otimes p_1^*L^{-1} \otimes p_2^*L^{-1}$ normalised so that the action on the restriction of $m^*L \otimes p_1^*L^{-1} \otimes p_2^*L^{-1}$ to $0 \times A$ is the action on $L^{-1}(0) \times A$ which is trivial on $L^{-1}(0)$ and is the usual action by translations on A. Passing to the quotient by this action we see that $P|_{0 \times A^t} = 0$. The restriction $P|_{A \times \varphi_L(x)}$ is the restriction of $m^*L \otimes p_1^*L^{-1} \otimes p_2^*L^{-1}$ to $A \times x$, and this is $T_x^*L \otimes L^{-1}$. This shows that for $y \in A^t$ the restriction $P|_{A \times y}$ is the line bundle on A given by $y \in A^t = \mathrm{Pic}^0(A)$.

Definition 1.21 *The Poincaré line bundle on $A \times A^t$ is a line bundle P such that $P|_{0 \times A^t} = 0$ and $P|_{A \times y}$ is the line bundle on A given by $y \in A^t = \mathrm{Pic}^0(A)$. One also requires P to satisfy the following universal property. For any variety S and any line bundle M on $A \times S$ such that $M|_{0 \times S} = 0$ and $M|_{A \times s} \in \mathrm{Pic}^0(A)$ for all $s \in S$ the natural map of sets $f : S \to A^t$ defined by $M|_{A \times s} = P|_{A \times f(s)}$ is a morphism of varieties and $M = (1, f)^*P$ is the pull-back of P with respect to the morphism $(1, f) : A \times S \to A \times A^t$.*

With this definition the pair (A^t, P) is unique up to canonical isomorphism.

Secondly, one can adapt the definition of (A^t, P) so that it works in arbitrary characteristic. To a line bundle L on an abelian variety A one associates a *group*

subscheme $K(L) \subset A$ defined as the maximal subscheme of A such that the restriction of $m^*L \otimes p_1^*L^{-1} \otimes p_2^*L^{-1}$ to $K(L) \times A \subset A \times A$ is trivial (see [3, Ch. III, §10, §13]). In terms of the functor of points it is described as follows. Let S be a scheme and write $A_S = A \times S$. An S-point of A is a morphism $f : S \to A$. This point is in $K(L)$ if and only if $T_f^*L \cong L \otimes p_2^*M$ for some line bundle M on S. Here $T_f : A_S \to A_S$ is the morphism $T_f(x, s) = (x + f(s), s)$. The key point is that $K(L)$ need not be reduced.

Then one develops the procedure of forming the quotient by the action of a finite group scheme and defines $A^t = A/K(L)$ for an ample line bundle L. The Poincaré bundle is defined as above and has similar properties.

Let us give an example of application of the universal property of (A^t, P). By applying Lemma 1.18 to the line bundle P on $A \times A^t$ we see that the line bundles in $\mathrm{Pic}^0(A)$ are precisely the continuous deformations of the trivial line bundle on A.

Dual morphism. Let $f : A \to B$ be a morphism of abelian varieties. We have the Poincaré bundles P_A on $A \times A^t$ and P_B on $B \times B^t$. Consider the pull-back $(f, \mathrm{id})^*P_B$ along $(f, \mathrm{id}) : A \times B^t \to B \times B^t$. This is a line bundle on $A \times B^t$ whose restrictions to $A \times x$ are in $\mathrm{Pic}^0(A)$ and whose restriction to $0 \times A^t$ is trivial. We deduce the existence of a morphism $f^t : B^t \to A^t$ such that $(f, \mathrm{id})^*P_B = (\mathrm{id}, f^t)^*P_A$:

$$A \times A^t \xleftarrow{(\mathrm{id}, f^t)} A \times B^t \xrightarrow{(f, \mathrm{id})} B \times B^t.$$

The map $f^t : B^t \to A^t$ is called the *dual morphism* of f. The meaning of this is that f^t sends an element of $B^t = \mathrm{Pic}^0(B)$ corresponding to a line bundle L (a continuous deformation of the trivial bundle) on B to the element of $A^t = \mathrm{Pic}^0(A)$ corresponding to the line bundle f^*L on A.

Duality of finite group schemes. Let G be a finite commutative group k-scheme. The *dual group scheme* of G is definied as a group k-scheme G^D that represents the functor from the category of schemes to the category of abelian groups which associates to a scheme S the group of homomorphisms of commutative group S-schemes $G_S \to \mathbb{G}_{m,S}$. There is a nice description of G^D in terms of its algebra of regular functions $k[G^D]$. The multiplication, the inverse and the neutral elements are morphisms

$$G \times G \to G, \quad G \to G, \quad \mathrm{Spec}(k) \to G.$$

They give rise to k-algebra homomorphisms

$$k[G] \to k[G] \otimes_k k[G], \quad k[G] \to k[G], \quad k[G] \to k.$$

One checks that the fact that G is a group implies that passing to the space of linear functions $k[G]^* = \mathrm{Hom}(k[G], k)$ we obtain a map

$$k[G]^* \otimes_k k[G]^* \to k[G]^*$$

which makes $k[G]^*$ an associative k-algebra with the unit coming from the dual map $k \to k[G]^*$. If G is commutative, then this algebra is commutative, so we can define $G^D = \mathrm{Spec}(k[G]^*)$ so that $k[G^D] = k[G]^* = \mathrm{Hom}(k[G], k)$.

Note that if G is reduced, then G^D has the same cardinality as G. In this case the k-vector space of regular functions on G is the same as the space of maps $G \to k$ which is the dual to the k-vector space freely generated by the elements of G, that is, the group algebra of G. Therefore, the k-algebra $k[G]^*$ is canonically isomorphic to the group algebra of the group of k-points of G: the linear function given by the value of a regular function on G at $g \in G$ is identified with the canonical generator g of the group ring of G. For example, if $G = \mathbb{Z}/p^n$ is a reduced group scheme, then the space of linear functions $k[G] \to k$ is the group algebra of $G = \mathbb{Z}/p^n$ which is $k[t]/(t^{p^n} - 1)$. (The action of a generator of $\mathbb{Z}/p^n$ is encoded by the multiplication by t.) Thus $(\mathbb{Z}/p^n)^D = \mu_{p^n} = \mathrm{Spec}(k[t]/(t^{p^n} - 1))$, and hence $(\mu_{p^n})^D = \mathbb{Z}/p^n$. Note that if $p = \mathrm{char}(k)$, then μ_{p^n} is not reduced.

Exercise Assume that $p = \mathrm{char}(k)$ and define $\alpha_{p^n} = \mathrm{Spec}(k[t]/(t^{p^n}))$. This is a non-reduced subscheme of the additive group k-scheme $\mathbb{G}_a$, whose reduced subscheme is one point 0. One can check that α_{p^n} is a group subscheme of $\mathbb{G}_a$, see [3, §11]. Show that $(\alpha_{p^n})^D = \alpha_{p^n}$.

Proposition 1.22 *Let $f : A \to B$ be an isogeny. Then the dual morphism f^t is an isogeny $B^t \to A^t$ of the same degree $\deg(f)$, called the* **dual isogeny** *of f. Moreover, the finite groups schemes $\mathrm{Ker}(f)$ and $\mathrm{Ker}(f^t)$ are dual to each other.*

Proof. The exact sequence of group schemes

$$0 \longrightarrow K \longrightarrow A \xrightarrow{f} B \longrightarrow 0$$

gives rise to the exact sequence of abelian groups

$$\mathrm{Hom}(A, \mathbb{G}_m) \longrightarrow \mathrm{Hom}(K, \mathbb{G}_m) \longrightarrow \mathrm{Ext}^1(B, \mathbb{G}_m) \longrightarrow \mathrm{Ext}^1(A, \mathbb{G}_m). \tag{4}$$

Here the map $\mathrm{Ext}^1(B, \mathbb{G}_m) \to \mathrm{Ext}^1(A, \mathbb{G}_m)$ is given by the pull-back of extensions along $f : A \to B$ so this is also the dual morphism $f^t : B^t \to A^t$, because both morphisms coincide on k-points: they send L to f^*L. We have $\mathrm{Hom}(A, \mathbb{G}_m) = 0$ since A is proper and $\mathbb{G}_m$ is affine. The sequence (4) holds also after the base change to any base scheme S. This shows that there is an exact sequence of commutative group k-schemes

$$0 \longrightarrow K^D \longrightarrow B^t \xrightarrow{f^t} A^t, \tag{5}$$

where we have used the Barsotti–Weil formula (Corollary 1.17) and the definition of K^D. We see that $\mathrm{Ker}(f^t)$ is finite, so f^t is surjective because $\dim(A^t) = \dim(B^t)$. □

Corollary 1.23 *The dual isogeny of* $[n] : A \to A$ *is* $[n] : A^t \to A^t$. *Thus the finite group schemes* $A[n]$ *and* $A^t[n]$ *are dual to each other.*

Proof. The map $\mathrm{Ext}^1(A, \mathbb{G}_m) \to \mathrm{Ext}^1(A, \mathbb{G}_m)$ induced by the multiplication by n map on A is $[n]$. Thus we see from (4) that in our case the exact sequence (5) takes the form

$$0 \longrightarrow A[n]^D \longrightarrow A^t \xrightarrow{[n]} A^t \longrightarrow 0.$$

Hence $A[n]^D$ is canonically isomorphic to $A^t[n]$. □

We obtain a perfect pairing $A[n] \times A^t[n] \to \mu_n$, called **the Weil pairing**.

Proposition 1.24 *There is a canonical isomorphism* $A \xrightarrow{\sim} (A^t)^t$.

Proof. The Poincaré bundles P_A on $A \times A^t$ and P_{A^t} on $A^t \times (A^t)^t = (A^t)^t \times A^t$ give rise to a unique morphism $c : A \to (A^t)^t$ such that $P_A = (c, \mathrm{id})^* P_{A^t}$. Choose a line bundle L such that $\varphi_L : A \to A^t$ is an isogeny. One checks from the definition of the dual morphism that $\varphi_L^t \, c = \varphi_L$. It follows that c is an isogeny and in particular is surjective. Now applying the snake lemma to the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K(L) & \longrightarrow & A & \xrightarrow{\varphi_L} & A^t & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & K(L)^D & \longrightarrow & (A^t)^t & \xrightarrow{\varphi_L^t} & A^t & \longrightarrow & 0 \end{array}$$

we see that $K(L)$ maps surjectively onto $K(L)^D$. However, by Proposition 1.22 these finite group schemes have the same order, so the map $K(L) \to K(L)^D$ is an isomorphism. Thus $c : A \to (A^t)^t$ is also an isomorphism. □

We always identify A with $(A^t)^t$ via the isomorphism c.

Warning. In view of the canonical identification of $(A^t)^t$ with A we have in fact not one but two Weil pairings:

$$(\,,\,)_A \;:\; A[n] \times A^t[n] \to \mu_n, \qquad (\,,\,)_{A^t} \;:\; A^t[n] \times A[n] \to \mu_n.$$

It seems plausible that they should agree, however this is not quite true because in fact they differ by sign:

$$(x, y)_A = -(y, x)_{A^t},$$

see, e.g. [4, §10.4].

The proof of Proposition 1.24 shows that if $\varphi_L : A \to A^t$ is an isogeny, then $\varphi_L^t : A \to A^t$ is equal to φ_L. Now we show that this holds for any line bundle L.

Proposition 1.25 *Let* L *be any line bundle on* A. *Then the morphism* $\varphi_L : A \to A^t$ *is self-dual.*

Proof. By Proposition 1.24 the dual morphism $\varphi_L^t \in \mathrm{Hom}(A, A^t)$. Thus we have morphisms

$$A^t \times A \overset{(\varphi_L^t, \mathrm{id})}{\longleftarrow} A \times A \overset{(\mathrm{id}, \varphi_L)}{\longrightarrow} A \times A^t.$$

By (3) and the definition of the dual morphism we have canonical isomorphisms of line bundles on $A \times A$:

$$(\varphi_L^t, \mathrm{id})^* P_{A^t} = m^* L \otimes p_1^* L^{-1} \otimes p_2^* L^{-1} = (\mathrm{id}, \varphi_L)^* P_A.$$

The canonical isomorphism $A \xrightarrow{\sim} (A^t)^t$ of Proposition 1.24 identifies P_A and P_{A^t} when we swap the factors in $A \times A^t$. Since $m^* L \otimes p_1^* L^{-1} \otimes p_2^* L^{-1}$ is invariant under swapping the factors in $A \times A$, we see that everything is invariant under the swapping the factors, hence $\varphi_L^t = \varphi_L$. $\square$

Write $\mathrm{Hom}_{\mathrm{self-dual}}(A, A^t)$ for the subgroup of self-dual morphisms $A \to A^t$. Then (1) gives rise to an exact sequence of abelian groups

$$0 \to A^t \to \mathrm{Pic}(A) \to \mathrm{Hom}_{\mathrm{self-dual}}(A, A^t) \to 0. \tag{6}$$

See [4, Thm. 13.7] for the proof of the surjectivity of the third arrow in this sequence. The *Néron–Severi group* of a variety X over an algebraically closed field is defined as the quotient of $\mathrm{Pic}(X)$ by the subgroup of classes of divisors agebraically equivalent to zero. We see that the Néron–Severi group of an abelian variety A has a nice interpretation

$$\mathrm{NS}\,(A) = \mathrm{Hom}_{\mathrm{self-dual}}(A, A^t).$$

Elliptic curves. An elliptic curve is an abelian variety of dimension 1. Let $O \in E$ be the origin of the group law on an elliptic curve E. The line bundle $L = \mathcal{O}(O)$ is ample and the associated morphism φ_L sends $x \in E$ to $T_x^* L \otimes L^{-1} = \mathcal{O}([-x] - [O])$. This map is injective, hence $E = E^t$. Thus the Weil pairing is a non-degenerate bilinear pairing

$$(,) \ : \ E[n] \times E[n] \to \mu_n.$$

From the Warning above we know that it is skew-symmetric: $(x, y) = -(y, x)$ for all $x, y \in E[n]$. Moreover, it is known that the Weil pairing is alternating, that is, $(x, x) = 0$ for any $x \in E[n]$. (The second property is stronger when n is even!)

2 Abelian varieties over non-closed fields

2.1 Galois cohomology

Let G be a group. For a G-module M we have cohomology groups $\mathrm{H}^n(G, M)$ which are derived functors of the functor from the category of G-modules to abelian groups given by $M \mapsto M^G$.

Exercise 1. If G is a cyclic group of order n with generator g, then $\mathrm{H}^{2n+1}(G,M)$, where $n=0,1,2,\ldots$, is the quotient of the kernel of the norm map $\mathrm{N}: M\to M$ by $(g-\mathrm{id})M$, where $\mathrm{N}=\sum_{i=0}^{n-1} g^i$. Similarly, $\mathrm{H}^{2n}(G,M)$ is the quotient of M^G by $\mathrm{N}M$, where $n=1,2,\ldots$ (Check that $\ldots\to\mathbb{Z}[G]\to\mathbb{Z}[G]\to\ldots$, where the arrows are alternating N and $g-1$, is a projective resolution of the G-module $\mathbb{Z}$.)

We also have $\mathrm{Ext}^n_G(M,N)$ which can be thought of either the right derived functors of $N\mapsto \mathrm{Hom}_G(M,N)$ or the left derived functors of $M\mapsto \mathrm{Hom}_G(M,N)$. Equivalently, $\mathrm{Ext}^n_G(M,N)$ can be defined as the set of equivalence classes of n-fold extensions of G-modules M by N. These groups can be computed using the spectral sequence

$$\mathrm{H}^p(G,\mathrm{Ext}^q_{\mathbb{Z}}(M,N))\Rightarrow \mathrm{Ext}^{p+q}_G(M,N).$$

From the definition in terms of extensions we get pairings

$$\mathrm{Ext}^p_G(L,M)\times\mathrm{Ext}^q_G(M,N)\to\mathrm{Ext}^{p+q}_G(L,N)$$

defined by splicing extensions. This means composing the surjective (penultimate) map in the first extension with the injective (second) map in the second extension. From the right derived functor definition we see that $\mathrm{Ext}^n_G(\mathbb{Z},N)=\mathrm{H}^n(G,N)$. In particular, we obtain pairings

$$\mathrm{H}^p(G,M)\times\mathrm{Ext}^q_G(M,N)\to\mathrm{H}^{p+q}(G,N). \tag{7}$$

Cohomology of profinite groups Let G be a profinite group, i.e. the inverse limit $\varprojlim G_i$ of a projective system of finite groups G_i, equipped with the topology for which the kernels of projections $G\to G_i$ form a basis of open sets. A G-module M is a continuous discrete G-module if the action $G\times M\to M$ is continuous when M is given discrete topology. This means that the stabiliser of each element of M is an open subgroup of G, or, equivalently, $M=\cup_U M^U$ where $U\subset G$ are open subgroups. The cohomology groups $\mathrm{H}^n(G,M)$, defined as the derived functors of $M\to M^G$, can be calculated as a direct limit of cohomologies of finite groups:

$$\mathrm{H}^n(G,M)=\varinjlim \mathrm{H}^n(G/U,M^U),$$

where $U\subset G$ ranges over all open normal subgroups of G. If $U\subset U'$, then $\mathrm{H}^n(G/U',M^{U'})\to\mathrm{H}^n(G/U,M^U)$ is an inflation homomorphism. Since G/U is finite, we see that for $n\geq 1$ every element of $\mathrm{H}^n(G,M)$ has finite order, that is, $\mathrm{H}^n(G,M)$ *is a torsion group.*

Exercise 2. Prove that if M is finite, then $\mathrm{H}^n(\hat{\mathbb{Z}},M)=0$ for $n\geq 2$. (To fix ideas let $n>0$ be even. We have $\hat{\mathbb{Z}}/m\hat{\mathbb{Z}}=\mathbb{Z}/m$ and $\mathrm{H}^n(\mathbb{Z}/m,M^{m\hat{\mathbb{Z}}})=M^{\hat{\mathbb{Z}}}/\mathrm{N}_m M^{m\hat{\mathbb{Z}}}$, where $\mathrm{N}_m=\sum_{i=0}^{m-1} g^i$ and g is a topological generator of $\hat{\mathbb{Z}}$. The inflation homomorphism

$$\mathrm{H}^n(\mathbb{Z}/m,M^{m\hat{\mathbb{Z}}})\longrightarrow\mathrm{H}^n(\mathbb{Z}/mr,M^{mr\hat{\mathbb{Z}}})$$

is the map

$$M^{\hat{\mathbb{Z}}}/\mathrm{N}_m M^{m\hat{\mathbb{Z}}} \longrightarrow M^{\hat{\mathbb{Z}}}/\mathrm{N}_{mr} M^{mr\hat{\mathbb{Z}}}$$

given by N_r which induces the multiplication by r. So this map is zero if r is divisible by $|M|$, so the direct limit is the zero group.)

Cohomology of commutative algebraic groups Let k be a *perfect* field with an algebraic closure $\bar{k}$ and the Galois group $\Gamma = \mathrm{Gal}(\bar{k}/k)$. If G is a commutative group scheme over a field k, then we write $\mathrm{H}^n(k, G)$ for the continuous cohomology group $\mathrm{H}^n(\Gamma, G(\bar{k}))$, where the Galois group Γ has its natural profinite topology and $G(\bar{k})$ is given discrete topology. In particular, $\mathrm{H}^0(k, G) = G(k)$. The group $\mathrm{H}^1(k, G)$ classifies k-torsors for G up to isomorphism.

Question: *When does a self-dual isogeny $\varphi : A \to A^t$ of abelian varieties over k come from a line bundle on A, i.e., when $\varphi = \varphi_L$ for some $L \in \mathrm{Pic}(A)$?* (Variant: if such a line bundle exists, *can we choose it to be symmetric with respect to the action of* $[-1]$?) The first question can be restated as the question about the differential $\partial(\varphi)$ attached to (6). Over some easy non-closed fields it has a positive answer. For example, Lang's theorem says that over any finite field k we have $\mathrm{H}^1(k, A) = 0$.

The second question is a question about the differential attached to the subsequence of (6) obtained by taking invariants with respect to the induced action of $[-1]$ on A:

$$0 \to A^t[2] \to \mathrm{Pic}(\overline{A})^{[-1]^*} \to \mathrm{Hom}_{\mathrm{self-dual}}(\overline{A}, \overline{A}^t) \to 0. \tag{8}$$

This sequence is exact because $\mathrm{H}^1(\mathbb{Z}/2, A^t) = 0$. Let us denote by c_φ the image of φ under the differential

$$\mathrm{Hom}_{\mathrm{self-dual}}(\overline{A}, \overline{A}^t)^\Gamma \longrightarrow \mathrm{H}^1(k, A^t[2]).$$

Poonen and Stoll showed that when k is a number field, the class c_φ plays an important role in deciding whether the order of the n-torsion subgroup of Ш(A) is a square or twice a square.

Let us define Ext-groups in the category of commutative group schemes over k. The group $\mathrm{Ext}^n_k(A, B)$ is the group of equivalence classes of n-fold extensions, as was explained above in the case of an algebraically closed field. In that case we obtained $\mathrm{Ext}^n(A, B) = \mathrm{Ext}^n_{\bar{k}}(A, B)$; this group also has the structure of a Γ-module. The pairings

$$\mathrm{H}^p(k, A) \times \mathrm{Ext}^q_k(A, B) \to \mathrm{H}^{p+q}(k, B) \tag{9}$$

are defined by forgetting the algebraic group structure, that is, by composing the forgetful map $\mathrm{Ext}^q_k(A, B) \to \mathrm{Ext}^q_\Gamma(A(\bar{k}), B(\bar{k}))$ with the pairing between Ext-groups in the category of discrete Γ-modules (7).

Proposition 2.1 *Let k be a perfect field.*

(i) *(J.S. Milne) There is a spectral sequence*

$$\mathrm{H}^p(k, \mathrm{Ext}^q(A, B)) \Rightarrow \mathrm{Ext}_k^{p+q}(A, B).$$

(ii) *(F. Oort) If A is an abelian variety over k, then $\mathrm{Ext}^n(A, \mathbb{G}_m) = 0$ for $n \geq 2$.*

(iii) *(F. Oort) If N is a finite group scheme of order coprime to the characteristic of k, then $\mathrm{Ext}^n(N, \mathbb{G}_m) = 0$ for $n \geq 1$.*

Corollary 2.2 *Let k be a perfect field and let $n \geq 0$. For any abelian variety A we have $\mathrm{Ext}_k^{n+1}(A, \mathbb{G}_m) = \mathrm{H}^n(k, A^t)$. For any finite group k-scheme N of order coprime to the characteristic of k we have $\mathrm{Ext}_k^n(N, \mathbb{G}_m) = \mathrm{H}^n(k, N^D)$.*

Proof This is immediate using Milne's spectral sequence, $\mathrm{Hom}(A, \mathbb{G}_m) = 0$ and the Barsotti–Weil formula (Corollary 1.17). □

Thus we obtain pairings

$$\mathrm{H}^n(k, A) \times \mathrm{Ext}_k^{2-n}(A, \mathbb{G}_m) = \mathrm{H}^n(k, A) \times \mathrm{H}^{1-n}(k, A^t) \to \mathrm{H}^2(k, \mathbb{G}_m) = \mathrm{Br}(k), \quad (10)$$

where $n = 0$ or 1, and

$$\mathrm{H}^n(k, N) \times \mathrm{Ext}_k^{2-n}(N, \mathbb{G}_m) = \mathrm{H}^n(k, N) \times \mathrm{H}^{2-n}(k, N^D) \to \mathrm{H}^2(k, \mathbb{G}_m) = \mathrm{Br}(k), \quad (11)$$

where $n = 0, 1, 2$. For example, for $N = N^D = \mathbb{Z}/2$ we are not getting anything interesting when $n = 0$ or $n = 2$, but for $n = 1$ we get a pairing

$$k^*/k^{*2} \times k^*/k^{*2} \longrightarrow \mathrm{Br}(k)[2],$$

given by the symbol $(a, b) \in \mathrm{Br}(k)$ which is the class of the quaternion algebra $k \oplus ik \oplus jk \oplus ijk$, where $i^2 = a$, $j^2 = b$ and $ij = -ji$.

2.2 Local fields

As a warming-up for the duality over local fields let us first consider the case when k is a *finite* field. Then $\Gamma \cong \hat{\mathbb{Z}}$ is the completion of the infinite cyclic group generated by the Frobenius. If M is a $\hat{\mathbb{Z}}$-module with a topological generator g, then

$$\mathrm{H}^0(\hat{\mathbb{Z}}, M) = M^{\hat{\mathbb{Z}}}, \quad \mathrm{H}^1(\hat{\mathbb{Z}}, M) = M/(g - \mathrm{id}) = M_{\hat{\mathbb{Z}}}$$

are the groups of invariants and co-invariants, respectively. Note that there is an exact sequence

$$0 \to M^{\hat{\mathbb{Z}}} \to M \xrightarrow{g-\mathrm{id}} M \to M_{\hat{\mathbb{Z}}} \to 0,$$

hence if M is finite, then $|M^{\hat{\mathbb{Z}}}| = |M_{\hat{\mathbb{Z}}}|$.

Assume that M is finite and define the dual module as $M^* = \mathrm{Hom}(M, \mathbb{Z}/m)$, where $m = |M|$. Then

$$\mathrm{H}^0(\hat{\mathbb{Z}}, M^*) = \mathrm{Hom}_{\hat{\mathbb{Z}}}(M, \mathbb{Z}/m) = \mathrm{Hom}(M_{\hat{\mathbb{Z}}}, \mathbb{Z}/m),$$

so there is a perfect duality of finite abelian groups

$$M_{\hat{\mathbb{Z}}} \times (M^*)^{\hat{\mathbb{Z}}} \longrightarrow \mathbb{Z}/m.$$

This can be thought of as a duality

$$\mathrm{H}^r(\hat{\mathbb{Z}}, M) \times \mathrm{H}^{1-r}(\hat{\mathbb{Z}}, M^*) \longrightarrow \mathrm{H}^1(\hat{\mathbb{Z}}, \mathbb{Z}/m) = \mathbb{Z}/m,$$

where $r = 0$ or 1. In Exercise 2 above we have seen that if M is finite, then $\mathrm{H}^r(\hat{\mathbb{Z}}, M) = 0$ for $r \geq 2$.

Definition 2.3 *We call a field k* **local** *if k is the field of fractions of a complete discrete valuation ring with the finite residue field.*

Let k_{nr} be the maximal unramified extension of k. Let $\mathcal{O}_k$ be the ring of integers of k, let $\mathfrak{m}$ be the maximal ideal of R and let $\kappa = \mathcal{O}_k/\mathfrak{m}$ be the residue field. The Galois group $\mathrm{Gal}(k_{\mathrm{nr}}/k)$ is canonically isomorphic to $\mathrm{Gal}(\bar{\kappa}/\kappa) \cong \hat{\mathbb{Z}}$.

Recall the cohomological interpretation of the Brauer group of the field k:

$$\mathrm{Br}(k) = \mathrm{H}^2(k, \mathbb{G}_m) = \mathrm{H}^2(\Gamma, \bar{k}^*).$$

Lang's theorem says that $\mathrm{Br}(k_{\mathrm{nr}}) = 0$. This, Hilbert's theorem 90 $\mathrm{H}^1(k_{\mathrm{nr}}, \bar{k}^*) = 0$, and the Hochschild–Serre spectral sequence

$$\mathrm{H}^p(\hat{\mathbb{Z}}, \mathrm{H}^q(k_{\mathrm{nr}}, \bar{k}^*)) \Rightarrow \mathrm{H}^{p+q}(\Gamma, \bar{k}^*)$$

imply $\mathrm{H}^2(\Gamma, \bar{k}^*) = \mathrm{H}^2(\hat{\mathbb{Z}}, k_{\mathrm{nr}}^*)$. We obtain

$$\mathrm{Br}(k) = \mathrm{H}^2(\hat{\mathbb{Z}}, k_{\mathrm{nr}}^*) \xrightarrow{\mathrm{val}} \mathrm{H}^2(\hat{\mathbb{Z}}, \mathbb{Z}) \xleftarrow{\sim} \mathrm{H}^1(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z},$$

where all arrows are isomorphisms, see [6, Ch. XII]. This gives the *local invariant* isomorphism

$$\mathrm{inv} : \mathrm{Br}(k) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}.$$

Theorem 2.4 (local Tate duality with finite coefficients) *Let M be a finite discrete Γ-module whose order is coprime to the characteristic of k. The paring*

$$\mathrm{H}^r(\Gamma, M) \times \mathrm{H}^{2-r}(\Gamma, M^D) \longrightarrow \mathrm{Br}(k) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

is a perfect duality of finite groups. We have $\mathrm{H}^r(\Gamma, M) = 0$ for $r \geq 3$.

The proof is based on local class field theory, more precisely, on the duality theorem relative to a class formation. See [2, §I.2].

Example Take $k = \mathbb{Q}_p$, where p is a prime, and $M = M^D = \mathbb{Z}/2$. Then this pairing is given by the Hilbert symbol $(a, b)_p \in \{\pm 1\}$, where $a, b \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. The resulting class in $\mathrm{Br}(\mathbb{Q}_p)$ is the class of the quaternion algebra $\mathbb{Q}_p \oplus i\mathbb{Q}_p \oplus j\mathbb{Q}_p \oplus ij\mathbb{Q}_p$, where $i^2 = a$, $j^2 = b$ and $ij = -ji$. Cyclic algebras can be used to prove this theorem in the case when $M = \mathbb{Z}/m$ and $M^D = \mu_m$.

Remark A Γ-module M is called *unramified* if the inertia subgroup $I = \mathrm{Gal}(\bar{k}/k_{\mathrm{nr}}) \subset \Gamma = \mathrm{Gal}(\bar{k}/k)$ acts trivialy on M, that is, $M^I = M$. In this case we define the *unramified cohomology group* $\mathrm{H}^n_{\mathrm{nr}}(\Gamma, M) = \mathrm{H}^n(\Gamma/I, M)$. The most important of these is $\mathrm{H}^1_{\mathrm{nr}}(\Gamma, M)$ which coincides with the image of the injective inflation map $\mathrm{H}^1(\Gamma/I, M) \to \mathrm{H}^1(\Gamma, M)$.

Now assume that M is finite. Since $\Gamma/I \cong \hat{\mathbb{Z}}$, the order of $\mathrm{H}^1_{\mathrm{nr}}(\Gamma, M)$ is equal to the order of $\mathrm{H}^0_{\mathrm{nr}}(\Gamma, M) = M^\Gamma$. We have seen in Exercise 2 above that $\mathrm{H}^n(\hat{\mathbb{Z}}, M) = 0$ for $n \geq 2$. Let $\bar{\mu}$ be the group of roots of unity of order coprime to p. Then $\bar{\mu}^I = \bar{\mu}$, and thus $M^D = \mathrm{Hom}(M, \bar{\mu})$ is also unramified. We claim that $\mathrm{H}^1_{\mathrm{nr}}(\Gamma, M)$ and $\mathrm{H}^1_{\mathrm{nr}}(\Gamma, M^D)$ are *exact annihilators* of each other for the local duality pairing

$$\mathrm{H}^1(\Gamma, M) \times \mathrm{H}^1(\Gamma, M^D) \to \mathrm{H}^2(\Gamma, \bar{k}^*) = \mathbb{Q}/\mathbb{Z}.$$

Indeed, these subgroups annihilate each other because their pairing factors through $\mathrm{H}^2_{\mathrm{nr}}(\Gamma, \bar{\mu}) = \mathrm{H}^2(\hat{\mathbb{Z}}, \bar{\mu}) = 0$, which is zero since $\bar{\mu}$ is unramified. The orders of these subgroups are equal to $|\mathrm{H}^0(\Gamma, M)|$ and $|\mathrm{H}^0(\Gamma, M^D)|$, respectively. By the local duality with finite coefficients we have $|\mathrm{H}^0(\Gamma, M^D)| = |\mathrm{H}^2(\Gamma, M)|$. Now the calculation of the Euler–Poincaré characteristic in Proposition 2.5 below shows that

$$|\mathrm{H}^0(\Gamma, M)| \cdot |\mathrm{H}^0(\Gamma, M^D)| = |\mathrm{H}^1(\Gamma, M)|,$$

so our claim is proved.

Proposition 2.5 *For a finite Γ-module M of order m coprime to the characteristic of k the Euler–Poincaré characteristic of M equals*

$$\chi(M) = \frac{|H^0(\Gamma, M)| \cdot |H^2(\Gamma, M)|}{|H^1(\Gamma, M)|} = \frac{1}{|\mathcal{O}_k : m\mathcal{O}_k|}.$$

Proof. We only prove this under the additional assumption $(m, p) = 1$, where p is the characteristic of the residue field $\kappa = \mathcal{O}_k/\mathfrak{m}$. Let $I \subset \Gamma$ be the inertia subgroup and let $I_p \subset I$ be the maximal pro-p-subgroup. Since $(m, p) = 1$ we have $\mathrm{H}^n(I_p, M) = 0$ for $n > 0$. Since I_p is normal in I, and I/I_p is isomorphic to the product of $\mathbb{Z}_\ell$ for all primes $\ell \neq p$, the Hochschild–Serre spectral sequence

$$\mathrm{H}^m(I/I_p, \mathrm{H}^n(I_p, M)) \Rightarrow \mathrm{H}^{m+n}(I, M)$$

gives similarly to Exercise 2 above that $\mathrm{H}^n(I, M) = 0$ for $n \geq 2$.

Now $\Gamma/I = \mathrm{Gal}(k_{\mathrm{nr}}/k) = \hat{\mathbb{Z}}$. We have $\mathrm{H}^0(\Gamma, M) = \mathrm{H}^0(\hat{\mathbb{Z}}, M^I)$. The Hochschild–Serre spectral sequence

$$\mathrm{H}^m(\hat{\mathbb{Z}}, \mathrm{H}^n(I, M)) \Rightarrow \mathrm{H}^{m+n}(\Gamma, M)$$

gives an exact sequence

$$0 \to \mathrm{H}^1(\hat{\mathbb{Z}}, M^I) \to \mathrm{H}^1(\Gamma, M) \to \mathrm{H}^0(\hat{\mathbb{Z}}, \mathrm{H}^1(I, M)) \to \mathrm{H}^2(\hat{\mathbb{Z}}, M^I) = 0,$$

where the zero in the right hand side is due to Exercise 2. We also obtain $\mathrm{H}^2(\Gamma, M) = \mathrm{H}^1(\hat{\mathbb{Z}}, \mathrm{H}^1(I, M))$. But if N is a finite $\hat{\mathbb{Z}}$-module, then the orders of finite groups $\mathrm{H}^0(\hat{\mathbb{Z}}, N)$ and $\mathrm{H}^1(\hat{\mathbb{Z}}, N)$ are equal. This implies that if m is invertible in $\mathcal{O}_k$, then $\chi(M) = 1$. (See [2, Thm. I.2.8] for the proof in the general case.) $\square$

2.3 Duality for abelian varieties over local fields

Recall that an abelian group G has *cofinite type* if it is a torsion group (every element has finite order) and $G[n]$ is finite for all n. Here is the main result of this section.

Theorem 2.6 (local Tate duality for abelian varieties) *Let k be a local field of characteristic zero and let A be an abelian variety over k. For $n \geq 2$ we have $\mathrm{H}^n(k, A) = 0$. For $n = 0, 1$ the canonical pairing*

$$\mathrm{H}^n(k, A) \times \mathrm{H}^{1-n}(k, A^t) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

gives rise to an isomorphism of compact groups

$$A(k) \tilde{\longrightarrow} \mathrm{Hom}(\mathrm{H}^1(k, A^t), \mathbb{Q}/\mathbb{Z})$$

and an isomorphism of discrete groups of cofinite type

$$\mathrm{H}^1(k, A) \tilde{\longrightarrow} \mathrm{Hom}(A^t(k), \mathbb{Q}/\mathbb{Z}).$$

As a preparation for the proof we prove a statement valid over an arbitrary ground field. Let n be coprime to the characteristic of k. The exact sequence

$$1 \to A[n] \to A \to A \to 1 \tag{12}$$

gives an exact sequence

$$0 \to A(k)/n \to \mathrm{H}^1(k, A[n]) \to \mathrm{H}^1(k, A)[n] \to 0. \tag{13}$$

Recall that by the non-degeneracy of the Weil pairing we have $A^t[n] = A[n]^D$, see Corollary 1.23.

Lemma 2.7 *The subgroups $A(k)/n \subset \mathrm{H}^1(k, A[n])$ and $A^t(k)/n \subset \mathrm{H}^1(k, A^t[n]) = \mathrm{H}^1(k, A[n]^D)$ are orthogonal with respect to the pairing (11):*

$$\mathrm{H}^1(k, A[n]) \times \mathrm{H}^1(k, A[n]^D) \to \mathrm{Br}(k).$$

In particular, if E is an elliptic curve, then $E(k)/n$ is a subspace of $\mathrm{H}^1(k, E[n])$ such that the restriction of the Weil pairing to it is trivial.

Proof. We shall construct several commutative diagrams that will be crucial in the proof of the duality theorem for abelian varieties over a local field (Theorem 2.6 below).

Step 1 Let N and M be (discrete) G-modules, and let

$$0 \to C \to B \to A \to 0 \tag{14}$$

be an exact sequence of G-modules. The differentials in the two long exact sequences of Ext-groups (with respect to the first and to the second argument, respectively)

$$\mathrm{Ext}^q_G(C, M) \xrightarrow{\partial_1} \mathrm{Ext}^{q+1}_G(A, M), \quad \mathrm{Ext}^p_G(N, A) \xrightarrow{\partial_2} \mathrm{Ext}^{p+1}_G(N, C)$$

are (up to sign) obtained by splicing with the class of (14). Thus the pairings

$$\mathrm{Ext}^{p+1}_G(N, C) \times \mathrm{Ext}^q_G(C, M) \longrightarrow \mathrm{Ext}^{p+q+1}_G(N, M)$$

and

$$\mathrm{Ext}^p_G(N, A) \times \mathrm{Ext}^{q+1}_G(A, M) \longrightarrow \mathrm{Ext}^{p+q+1}_G(N, M)$$

are compatible in the obvious sense: $\partial_2(x) \cup y = x \cup \partial_1(y)$.

Step 2 We apply Step 1 with (12) playing the role of (14), for $p + q + 1 = 2$, $M = \mathbb{G}_m$ and $N = \mathbb{Z}$. From the conclusion of Step 1 we deduce the commutativity of the right hand square of the following diagram with exact rows, where $r = 1$ or $r = 0$, possibly up to sign:

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{Ext}^r_k(A, \mathbb{G}_m)/n & \to & \mathrm{Ext}^r_k(A[n], \mathbb{G}_m) & \to & \mathrm{Ext}^{r+1}_k(A, \mathbb{G}_m)[n] & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \mathrm{H}^{2-r}(k, A)[n]^* & \to & \mathrm{H}^{2-r}(k, A[n])^* & \to & (\mathrm{H}^{1-r}(k, A)/n)^* & \to & 0 \end{array} \tag{15}$$

Here for an abelian group L we denote $L^* = \mathrm{Hom}(L, \mathrm{Br}(k))$. The left hand square commutes by functoriality.

Step 3 Now we take $r = 1$ and apply Corollary 2.2. We obtain a commutative (up to sign) diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \to & A^t(k)/n & \to & \mathrm{H}^1(k, A^t[n]) & \to & \mathrm{H}^1(k, A^t)[n] & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \mathrm{H}^1(k, A)[n]^* & \to & \mathrm{H}^1(k, A[n])^* & \to & (A(k)/n)^* & \to & 0 \end{array} \tag{16}$$

The horizontal maps in the top sequence come from $[n] : A^t \to A^t$ because this is the dual morphism to $[n] : A \to A$ (we defined the dual morphism via $\mathrm{Ext}(\cdot, \mathbb{G}_m)$, see Proposition 1.22 and Corollary 1.23).

Now the statement of the lemma immediately follows from the commutativity of (16) and the exactness of its rows. □

Proof of Theorem 2.6.

Step 1 The middle vertical map in diagram (16) is an isomorphism by Theorem 2.4. Hence the map $A^t(k)/n \to \mathrm{H}^1(k, A)[n]^*$ is injective. The topological groups $A(k)$ and $A^t(k)$ are extensions of a finite group by a subgroup isomorphic to $(\mathcal{O}_k)^{\dim(A)}$, hence $A^t(k) = \varprojlim A^t(k)/n$ is canonically isomorphic to its own profinite completion. Thus passing to the limit in n we obtain that the map $A^t(k) \to \mathrm{H}^1(k, A)^*$ is injective.

We note that the representation of $A(k)$ as an extension of a finite abelian group by $(\mathcal{O}_k)^{\dim(A)}$ implies

$$|A(k)/n| = |A(k)[n]| \cdot |\mathcal{O}_k : n\mathcal{O}_k|^{\dim(A)}. \tag{17}$$

(Use the snake lemma.)

Step 2 Using Corollary 2.2 the commutative diagram (15) for $r = 0$ can be written as follows:

$$\begin{array}{ccccccccc} & & & & A^t[n](k) & = & A^t[n](k) & & \\ & & & & \downarrow & & \downarrow & & \\ 0 & \to & \mathrm{H}^2(k, A)[n]^* & \to & \mathrm{H}^2(k, A[n])^* & \to & (\mathrm{H}^1(k, A)/n)^* & \to & 0 \end{array}$$

The middle vertical map is again an isomorphism by Theorem 2.4. Since the right hand vertical map is injective by Step 1, we see that $\mathrm{H}^2(k, A)[n] = 0$. This holds for any $n \geq 2$, thus $\mathrm{H}^2(k, A) = 0$. One deduces that $\mathrm{H}^m(k, A) = 0$ for $m \geq 2$. (Indeed, $\mathrm{H}^m(k, A)$ is a torsion group, but $\mathrm{H}^m(k, A)[n]$ is a quotient of $\mathrm{H}^m(k, A[n])$ which is zero for $m \geq 3$ by the last statement of Theorem 2.4.)

Step 3 Let us show that $A^t(k) \to \mathrm{H}^1(k, A)^*$ is surjective. By what was said in Step 1 this will follow if we show that the injective map $A^t(k)/n \to \mathrm{H}^1(k, A)[n]^*$ is also surjective, for all n. We prove that these groups have the same order. This follows from (17) and Proposition 2.5. On the one hand, we have

$$|A^t(k)/n| = |A^t(k)[n]| \cdot |\mathcal{O}_k : n\mathcal{O}_k|^g = |\mathrm{H}^2(k, A[n])| \cdot |\mathcal{O}_k : n\mathcal{O}_k|^g,$$

where the second equality follows from the local Tate duality with finite coefficients for $A[n]$ and $A^t[n] = A[n]^D$. On the other hand,

$$|\mathrm{H}^1(k, A)[n]| = \frac{|\mathrm{H}^1(k, A[n])|}{|A(k)/n|} = \frac{|\mathrm{H}^1(k, A[n])|}{|A(k)[n]| \cdot |\mathcal{O}_k : n\mathcal{O}_k|^g} = |\mathrm{H}^2(k, A[n])| \cdot |\mathcal{O}_k : n\mathcal{O}_k|^g,$$

because $|A[n]| = n^{2g}$ and $|\mathcal{O}_k : n^{2g}\mathcal{O}_k| = |\mathcal{O}_k : n\mathcal{O}_k|^{2g}$.

Step 4 The map in the last stement of the theorem is surjective by the diagram (16). To show that it is an isomorphism we need to prove that the orders of $\mathrm{H}^1(k, A^t)[n]$ and $A(k)/n$ are equal. This is the same calculation as in Step 3 with A^t in place of A. $\square$

Complements. **1** We have proved that all vertical maps in diagram (16) are isomorphisms. This implies that $A(k)/n$ and $A^t(k)/n$ are the *exact annihilators* for the pairing

$$\mathrm{H}^1(k, A[n]) \times \mathrm{H}^1(k, A[n]^D) \to \mathbb{Z}/n$$

discussed in Lemma 2.7.

2 If an abelian variety A over a local field k has good reduction and n is coprime to the residual characteristic p of k, then the Galois module $A[n]$ is unramified. (Since $(n, p) = 1$ the multiplication by n is an étale morphism of the Néron model $\mathcal{A} \to \mathcal{A}$; its kernel is identified with $A[n]^I$. The special fibre of the Néron model is an abelian variety of the same dimension as A, hence its n-torsion subgroup has the same cardinality as $A[n]$, hence $A[n]^I = A[n]$.) Moreover, $A(k)/n = \mathrm{H}^1_{\mathrm{nr}}(k, A[n])$. This can be seen as follows. Let $P \in A(k)$. The set of $\bar{k}$-points Q in A such that $nQ = P$ is a k-torsor for $A[n]$ whose class is the image of P in $\mathrm{H}^1(k, A[n])$. Since A has good reduction, this torsor is unramified, i.e. it is the generic fibre of a $\mathrm{Spec}(\mathcal{O}_k)$-torsor for $\mathcal{A}[n]$. Thus its class in $\mathrm{H}^1(k, A[n])$ comes from

$$\mathrm{H}^1(\mathrm{Spec}(\mathcal{O}_k), \mathcal{A}[n]) = \mathrm{H}^1_{\mathrm{nr}}(k, A[n]) \subset \mathrm{H}^1(k, A[n]).$$

2.4 Global fields

Let k be a global field, i.e. a finite extension of $\mathbb{Q}$ or $\mathbb{F}_p(t)$. Let $\bar{k}$ be a separable closure of k and let $\Gamma = \mathrm{Gal}(\bar{k}/k)$. We write k_v for a completion of k. This is a local field or $k_v = \mathbb{R}$ or $\mathbb{C}$.

One van choose a valuation w of $\bar{k}$ that extends the valuation v of k. Let $D_w \subset \Gamma$ be the decomposition group of w, i.e. the stabiliser of w in Γ. Let $\bar{k}_w$ be the union of completions of finite extensions of k at w. By Krasner's lemma every finite extension of k_v has the form $k_v[x]/(f(x))$ for an irreducible polynomial $f(x)$ with coefficients in k, so is a completion of a finite extension of k. Thus $\bar{k}_w$ is a separable closure of k_v and the decomposition group D_w is identified with $\Gamma_v = \mathrm{Gal}(\bar{k}_w/k_v)$. (Choosing w is equivalent to choosing an embedding of $\bar{k}$ into a given separable closure of k_v.) This identification allows us to define the restriction maps

$$\mathrm{H}^n(\Gamma, M) \longrightarrow \mathrm{H}^n(\Gamma_v, M)$$

simply by restricting to the subgroup $D_w \cong \Gamma_v$ of Γ. We shall abuse notation and write $\bar{k}_v$ for the algebraic closure $\bar{k}_w$.

If G is an algebraic k-group, then $\mathrm{H}^1(k,G)$ classifies k-torsors for G up to isomorphism. In this case the restriction map $\mathrm{H}^1(k,G) \to \mathrm{H}^1(k_v,G)$ sends the class of a torsor X to the class of $X \times_k k_v$. In particular, the class of X is in the kernel of the restriction map to k_v if and only if $X(k_v) \neq \emptyset$.

Let A be an abelian variety over k. We define the Shafarevich–Tate group

$$Ш(A) = \cap_v \mathrm{Ker}[\mathrm{H}^1(k,A) \to \mathrm{H}^1(k_v,A)],$$

where v ranges over all places of k. Define the n-Selmer group as

$$\mathrm{Sel}_n(A) = \cap_v \mathrm{Ker}[\mathrm{H}^1(k,A[n]) \to \mathrm{H}^1(k_v,A)],$$

then there is an obvious exact sequence

$$0 \to A(k)/n \to \mathrm{Sel}_n(A) \to Ш(A)[n] \to 0.$$

It can be proved that $\mathrm{Sel}_n(A)$ is finite for any n, see [2, Remark I.6.7]. Thus $Ш(A)[n]$ is finite too. A conjecture of Shafarevich and Tate says that $Ш(A)$ is finite for any abelian variety A over any global field.

There is a bilinear Cassels–Tate pairing

$$\langle , \rangle : \quad Ш(A) \times Ш(A^t) \to \mathbb{Q}/\mathbb{Z}$$

which is defined as follows. Any class of $Ш(A)$ is represented by a k-torsor X for A such that X has a k_v-point P_v for each completion k_v.

Let us write $\overline{A}$ for $A \times_k \bar{k}$ and similarly for $\overline{X}$. We defined $\mathrm{Pic}^0(\overline{A})$ as the subgroup of $\mathrm{Pic}(\overline{A})$ consisting of the elements that are stable under the translations of all points of $A(\bar{k})$, see Definition 1.14. Later we proved that $\mathrm{Pic}^0(\overline{A})$ coincides with the subgroup of $\mathrm{Pic}(\overline{A})$ formed by the classes of divisors algebraically equivalent to 0 (this follows from Lemma 1.18 and the existence of the Poincaré line bundle). This subgroup can be defined for any variety, in particular, for X. The torsor X is constructed by twisting A by a cocycle $\Gamma \to A(\bar{k})$, where $A(\bar{k})$ acts on $\overline{A} = A(\bar{k})$ by translations. The induced action on $\mathrm{Pic}^0(\overline{A}) = A^t(\bar{k})$ is trivial, therefore we obtain an isomorphism of Γ-modules $\mathrm{Pic}^0(\overline{X}) \cong A^t(\bar{k})$. Hence any class in $Ш(A^t)$ can be realised as an (everywhere locally trivial) element $\xi \in \mathrm{H}^1(\Gamma, \mathrm{Pic}^0(\overline{X}))$. There is an exact sequence of Γ-modules

$$0 \to \bar{k}(X)^*/\bar{k}^* \to \mathrm{Div}(\overline{X}) \to \mathrm{Pic}(\overline{X}) \to 0.$$

Let $\mathrm{Div}^0(\overline{X}) \subset \mathrm{Div}(\overline{X})$ be such that the following sequence is exact:

$$0 \to \bar{k}(X)^*/\bar{k}^* \to \mathrm{Div}^0(\overline{X}) \to \mathrm{Pic}^0(\overline{X}) \to 0.$$

The differential $\partial(\xi) \in \mathrm{H}^2(\Gamma, \bar{k}(X)^*/\bar{k}^*)$ comes from an element $\phi \in \mathrm{H}^2(\Gamma, \bar{k}(X)^*)$ because $\mathrm{H}^3(\Gamma, \bar{k}^*) = 0$. This ϕ is well defined up to an element in the image of

$$\mathrm{H}^2(\Gamma, \bar{k}^*) \longrightarrow \mathrm{H}^2(\Gamma, \bar{k}(X)^*).$$

Since ξ restricts to 0 in $\mathrm{H}^1(\Gamma_v, \mathrm{Pic}^0(\overline{X}_v))$, we see that $\partial(\xi)$ goes to $0 \in \mathrm{H}^2(\Gamma_v, \bar{k}_v(X)^*/\bar{k}_v^*)$, hence ϕ restricts to an element in the image of

$$\mathrm{H}^2(\Gamma_v, \bar{k}_v^*) \longrightarrow \mathrm{H}^2(\Gamma_v, \bar{k}_v(X)^*),$$

for each completion k_v. Let $c_v \in \mathrm{H}^2(\Gamma_v, \bar{k}_v^*) = \mathrm{Br}(k_v)$ be such an element. We can think of c_v as the "value" of ϕ at $P_v \in X(k_v)$. (By a small deformation of P_v we can avoid the zeros and poles of ϕ.) The collection (c_v) is well defined up to a global element, hence $\sum_v \mathrm{inv}_v(c_v) \in \mathbb{Q}/\mathbb{Z}$ is well defined. This is the value of the Cassels–Tate pairing of $[X] \in Ш(A)$ and $\xi \in Ш(A^t)$. (See [2, Remark I.6.11]. A definition that uses choices of cocycles instead of torsors can be found in [2, Prop. I.6.9]. For more definitions and the proof that they are all equivalent, see [5].)

The main result about the Cassels–Tate pairing is this.

Theorem 2.8 *The left and right kernels of $\langle , \rangle : Ш(A) \times Ш(A^t) \to \mathbb{Q}/\mathbb{Z}$ are the divisible subgroups of $Ш(A)$ and $Ш(A^t)$, respectively.*

Conjecturally, these divisible subgroups should be zero.

Recall the exact sequence of Γ-modules (8):

$$0 \to A^t[2] \to \mathrm{Pic}(\overline{A})^{[-1]^*} \to \mathrm{Hom}_{\mathrm{self-dual}}(\overline{A}, \overline{A}^t) \to 0.$$

We have $\mathrm{NS}(\overline{A}) = \mathrm{Hom}_{\mathrm{self-dual}}(\overline{A}, \overline{A}^t)$, so that $\mathrm{NS}(\overline{A})^\Gamma = \mathrm{Hom}_{\mathrm{self-dual}}(A, A^t)$. Let us denote by c_λ the image of a self-dual morphism $\lambda : A \to A^t$ (defined over k) under the differential

$$\mathrm{Hom}_{\mathrm{self-dual}}(\overline{A}, \overline{A}^t)^\Gamma \longrightarrow \mathrm{H}^1(k, A^t[2]).$$

Any such λ that equals φ_L for some ample line bundle on $\overline{A}$ is called a *polarisation* of A. A polarisation is *principal* if it is an isomorphism $A \xrightarrow{\sim} A^t$.

Theorem 2.9 (Poonen–Stoll) *Let A be an abelian variety over a global field k and let $\lambda \in \mathrm{NS}(\overline{A})^\Gamma$. Then $c_\lambda \in \mathrm{Sel}_2(A^t)$.*

Proof. This is a local fact: we need to show that $\partial(\lambda)$ in $\mathrm{H}^1(k, A^t)$ is zero when k is a local field or $k = \mathbb{R}$. Here ∂ is the differential in the long exact sequence of Galois cohomology associated to the exact sequence

$$0 \to A^t \to \mathrm{Pic}(\overline{A}) \to \mathrm{NS}(\overline{A}) \to 0.$$

We shall use the fact that $\partial(\lambda)$ goes to 0 under the map $\mathrm{H}^1(\Gamma, A^t) \to \mathrm{H}^1(\Gamma, \mathrm{Pic}(\overline{A}))$.

The proof of the theorem uses local duality for abelian varieties. The local duality pairing

$$\mathrm{H}^1(k, A^t) \times A(k) \to \mathrm{Br}(k),$$

or, equivalently, the pairing

$$\mathrm{H}^1(k, A^t) \times \mathrm{Ext}^1_k(A^t, \mathbb{G}_m) \to \mathrm{Br}(k),$$

is defined via the pairing

$$\mathrm{H}^1(\Gamma, A^t) \times \mathrm{Ext}^1_\Gamma(A^t, \bar{k}^*) \to \mathrm{Br}(k),$$

which is the pairing

$$\mathrm{H}^1(\Gamma, \mathrm{Pic}^0(\overline{A})) \times \mathrm{Ext}^1_\Gamma(\mathrm{Pic}^0(\overline{A}), \bar{k}^*) \to \mathrm{Br}(k).$$

By local duality (Theorem 2.6) our statement immediately follows from the obvious fact that the last pairing is compatible with the pairing

$$\mathrm{H}^1(\Gamma, \mathrm{Pic}(\overline{A})) \times \mathrm{Ext}^1_\Gamma(\mathrm{Pic}(\overline{A}), \bar{k}^*) \to \mathrm{Br}(k)$$

and, crucially, that any extension of A^t by $\mathbb{G}_m$ in the category of commutative algebraic k-groups gives (via the forgetful functor) an extension of Γ-modules $\mathrm{Pic}^0(\overline{A})$ by $\bar{k}^*$ which is a pull-back of some extension of $\mathrm{Pic}(\overline{A})$ by $\bar{k}^*$.

Let $P \in A(k)$ be the point corresponding to our extension

$$0 \to \mathbb{G}_m \to ? \to A^t \to 0$$

in the category of commutative algebraic k-groups via the canonical identification of A with $(A^t)^t$. Let $\mathcal{O}_{0,P}$ be the semilocal ring of $\{0, P\}$ in $\overline{A}$, where 0 is the origin of the group law. This is the subring of $\bar{k}(A)$ consisting of the functions regular at 0 and P. Let $\mathrm{Div}_{0,P}(\overline{A})$ be the group of divisors on $\overline{A}$ whose supports are disjoint from $\{0, P\}$. We have an exact sequence of Γ-modules

$$0 \to \mathcal{O}^*_{0,P}/\bar{k}^* \to \mathrm{Div}_{0,P}(\overline{A}) \to \mathrm{Pic}(\overline{A}) \to 0.$$

Its push-forward via the map $\mathcal{O}^*_{0,P}/\bar{k}^* \to \bar{k}^*$ that sends a function f to $f(P)/f(0)$ is an extension of $\mathrm{Pic}(\overline{A})$ by $\bar{k}^*$. We claim that the pull-back of this extension to $\mathrm{Pic}^0(\overline{A})$ is an extension of Γ-modules A^t by $\bar{k}^*$ obtained from our extension (?). This can be checked by comparing the associated systems of rational factors as in [7, VII.3 Thm. 6 and the remark after it]. We omit this verification. □

Proposition 2.10 (Poonen–Stoll) *Let $\tilde{c}_\lambda$ be the image of c_λ in $Ш(A)$. For all $x \in Ш(A)$ we have $\langle x, \lambda_* x - \tilde{c}_\lambda \rangle = 0$.*

Proof. This follows straight from the definition of the Cassels–Tate pairing. Let X be a k-torsor for A representing x. Choose $P \in X(\bar{k})$. Then x is the class of the

cocycle $g \mapsto gP - P \in A(\bar{k})$ where $g \in \Gamma$. Next, suppose that $\lambda = \varphi_D$ where D is a divisor on $\overline{A}$. Then $\lambda_* x$ is a k-torsor for A^t represented by the cocycle

$$g \mapsto [T^*_{gP-P} D] - [D] \in A^t(\bar{k}) = \mathrm{Pic}^0(\overline{A}).$$

However, λ also equals $\varphi_{{}^g D}$ because λ is the class of D in $\mathrm{NS}\,(\overline{A})$ and λ is Γ-invariant. Thus $\lambda_* x$ can be also represented by the cocycle

$$g \mapsto [T^*_{gP-P}({}^g D)] - [{}^g D] \in A^t(\bar{k}) = \mathrm{Pic}^0(\overline{A}).$$

The isomorphism of $\bar{k}$-varieties $\overline{A} \xrightarrow{\sim} \overline{X}$ that sends a to $a + P$ induces a canonical isomorphism of Γ-modules $\mathrm{Pic}^0(\overline{A}) \cong \mathrm{Pic}^0(\overline{X})$. Alternatively, we can take an isomorphism $a \to a + gP$. Using it we see that $\lambda_* x$ is represented by the cocycle

$$g \mapsto [T^*_{-P}({}^g D)] - [T^*_{-gP}({}^g D)] \in \mathrm{Pic}^0(\overline{X}).$$

(The sign is due to the fact that T^*_x acts on divisors by $-x$, so $a \to a+gP$ corresponds to T^*_{-gP}.) On the other hand, $\tilde{c}_\lambda$ is represented by the cocycle

$$g \mapsto [{}^g D] - [D] \in A^t(\bar{k}) = \mathrm{Pic}^0(\overline{A})$$

identified with the cocycle

$$g \mapsto [T^*_{-P}({}^g D)] - [T^*_{-P} D] \in \mathrm{Pic}^0(\overline{X}).$$

Thus $\lambda_* x - \tilde{c}_\lambda$ is the class of the cocycle

$$g \mapsto [T^*_{-P} D] - [{}^g T^*_{-P} D].$$

It lifts to a cocycle $g \mapsto T^*_{-P} D - {}^g T^*_{-P} D$ with coefficients in $\mathrm{Div}^0(\overline{X})$ because $[D] - [{}^g D] \in \mathrm{Pic}^0(\overline{A})$ and hence $[T^*_{-P} D] - [{}^g T^*_{-P} D] \in \mathrm{Pic}^0(\overline{X})$. It follows that $\partial(\lambda_* x - \tilde{c}_\lambda) = 0$ in the notation used in the definition of the Cassels–Tate pairing. This implies that $\phi \in \mathrm{H}^2(\Gamma, \bar{k}(X)^*)$ comes from an element of $\mathrm{Br}(k)$. The sum of local invariants of a global element is zero, hence $\langle x, \lambda_* x - \tilde{c}_\lambda \rangle = 0$. $\square$

This proposition immediately implies that the bilinear form $\langle x, \lambda_* x \rangle$ on $Ш\,(A)$ is antisymmetric. The proof of the following statement is elementary.

Corollary 2.11 (Poonen–Stoll) *Let A be an abelian variety with a* **principal polarisation** *λ. Define $c \in Ш\,(A)$ as $\lambda_*^{-1}(\tilde{c}_\lambda)$. Define $\langle x, y \rangle_\lambda = \langle x, \lambda_* y \rangle$. Then assuming that $Ш\,(A)$ is finite we have the following alternative.*

If $\langle c, c \rangle_\lambda = 0$, then there is a finite abelian group T such that

$$Ш\,(A) \cong T \times T.$$

If $\langle c, c \rangle_\lambda = 1/2$, then there is a finite abelian group T such that

$$Ш\,(A) \cong \mathbb{Z}/2 \times T \times T.$$

Remark Let E be an elliptic curve. If $O \in E$ is the origin of the group law, then the line bundle $L = \mathcal{O}(O)$ is ample. At the end of Chapter 1 we have seen that the associated isogeny φ_L is an isomorphism $\lambda : E \xrightarrow{\sim} E^t$, so E is canonically principally polarised. Moreover, the polarisation λ comes from a symmetric divisor O defined over k.

For an elliptic curve $\mathrm{Pic}^0(\overline{E})$ is the kernel of the surjective map $\mathrm{Pic}(\overline{E}) \to \mathbb{Z}$ given by the degree. Hence $\mathrm{NS}\,(\overline{E}) \cong \mathbb{Z}$ and we have the exact sequence

$$0 \to E[2] \to \mathrm{Pic}(\overline{E})^{[-1]^*} \to \mathbb{Z} \to 0.$$

The polarisation λ represents a generator of $\mathbb{Z}$. It comes from $[O] \in (\mathrm{Pic}(\overline{E})^{[-1]^*})^\Gamma$, hence the associated long exact sequence of Galois cohomology groups shows that $c_\lambda = 0$. Thus in the case of elliptic curves we are always in the first case of the alternative of Corollary 2.11. This proves

Corollary 2.12 *Let E be an elliptic curve over a number field. If $Ш(E)$ is finite, then the Cassels–Tate pairing on $Ш(E)$ is alternating and $|Ш(E)|$ is a square.*

This does not generalise to curves of higher genus!

Jacobians of curves Let C be a smooth, projective and geometrically integral curve of genus g. The Jacobian of C is the abelian variety $J = \mathrm{Pic}^0_{C/k}$ over k whose group of $\bar{k}$-points is $\mathrm{Pic}^0(\overline{C})$. It is canonically principally polarised, so there is an isomorphism $\lambda : J \xrightarrow{\sim} J^t$.

The set of divisor classes on $C \times_k \bar{k}$ of degree n is denoted by $\mathrm{Pic}^n(\overline{C})$. This is the group of $\bar{k}$-points of an algebraic variety over k denoted by $\mathrm{Pic}^n_{C/k}$. The Jacobian J acts on $\mathrm{Pic}^n_{C/k}$ by translations, making $\mathrm{Pic}^n_{C/k}$ a k-torsor for J. Note that $\mathrm{Pic}^n_{C/k}$ may or may not have k-points, but if there is a divisor on C of degree n defined over k, then $\mathrm{Pic}^n_{C/k}(k) \neq \emptyset$.

Exercise Show that the converse is not true by taking C to be a conic without k-points and $n = 1$.

If v is a place of k of large residual characteristic, then $C(k_v) \neq \emptyset$. (Indeed, C has good reduction outside finitely many places. Then the reduction $\tilde{C}$ is a smooth projective curve over a finite field $\mathbb{F}_q$. When q is large enough compared to the genus of C, there are $\mathbb{F}_q$-points on $\tilde{C}$ by the Hasse–Weil formula $|\tilde{C}(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}$. A smooth $\mathbb{F}_q$-point on $\tilde{C}$ lifts to a k_v-point on C by Hensel's lemma.) Thus X has k_v-points for almost all places v.

The canonical class K_C is represented by the divisors of rational forms on C which are divisors over k. Hence K_C is a k-point of $\mathrm{Pic}^{2g-2}_{C/k}$. The inverse image of K_C under the multiplication by 2 map

$$[2] : \mathrm{Pic}^{g-1}_{C/k} \longrightarrow \mathrm{Pic}^{2g-2}_{C/k}$$

is a finite k-scheme Θ whose $\bar{k}$-points are divisor classes $x \in \mathrm{Pic}(\overline{C})$ such that $2x = K_C$. This is clearly a k-torsor for $J[2]$, called the *torsor of theta-characteristics*. We have the following crucial fact.

Lemma 2.13 *$c_\lambda = [\Theta]$, hence $\tilde{c}_\lambda = [\mathrm{Pic}^{g-1}_{C/k}] \in \mathrm{H}^1(k, J)$.*

If $X = \mathrm{Pic}^n_{C/k}$ has points in each completion of k, then $[X] \in Ш(J)$. By Theorem 2.9 and Lemma 2.13 we have

$$\tilde{c}_\lambda = [\mathrm{Pic}^{g-1}_{C/k}] \in Ш(J),$$

so this always holds for $n = g - 1$. Poonen and Stoll prove that $\langle [X], [X] \rangle_\lambda = N/2$, where N is the number of places v for which C has no divisor of degree n defined over k_v. Applying this to $\tilde{c}_\lambda = [\mathrm{Pic}^{g-1}_{C/k}]$ we obtain the following explicit form of Corollary 2.11:

Corollary 2.14 *If $Ш(J)$ is finite, then $|Ш(J)|$ is a square if and only if the number of places v such that C does not have a divisor of degree $g-1$ defined over k_v is even. Otherwise, $|Ш(J)|$ is twice a square.*

An explicit example is the following genus 2 curve over $\mathbb{Q}$ which has $Ш(J) \cong \mathbb{Z}/2$:

$$y^2 = -3(x^2+1)(x^2-6x+1)(x^2+6x+1).$$

The calculation uses the fact that J is isogenous to a product of CM elliptic curves which makes it possible to apply a theorem of Rubin.

Remark Corollary 2.14 does not generalise to abelian varities without which are not principally polarised! Indeed, for many small odd primes p (including $p = 3$) William Stein [9] constructed an abelian variety A over $\mathbb{Q}$ such that $Ш(A)$ is finite of order pn^2 for some $n \in \mathbb{Z}$.

More precisely, take E^{p-1} to be the kernel of the homomorphism $E^p \to E$ which sends $(M_1, \ldots, M_p)$ to $M_1 + \ldots + M_p$. Then $\mathbb{Z}/p$ acts on E^{p-1} by cyclic shifts. The group $\mathrm{H}^1(k, \mathbb{Z}/p) = \mathrm{Hom}(\Gamma, \mathbb{Z}/p)$ consists of characters of the Galois group $\Gamma \to \mathbb{Z}/p$. The non-trivial characters bijectively correspond to the cyclic extensions $K/\mathbb{Q}$ of degree $[K : \mathbb{Q}] = p$. Thus we can twist E^{p-1} by such extensions. Let ℓ be a prime such that $\ell \equiv 1 \bmod p$ and let $K \subset \mathbb{Q}(\mu_\ell)$ be the unique subfield of degree $[K : \mathbb{Q}] = p$. Let A be the twist of E^{p-1} by K. Equivalently, A is the kernel of the natural map $\mathrm{R}_{K/\mathbb{Q}}(E_K) \to E$, where $\mathrm{R}_{K/\mathbb{Q}}$ is the Weil restriction of scalars. The resulting exact sequence

$$0 \to A \to \mathrm{R}_{K/\mathbb{Q}}(E_K) \to E \to 0$$

gives us a map $E(\mathbb{Q}) \to \mathrm{H}^1(\mathbb{Q}, A)$. William Stein, in the situation that he considers, obtains from this map an injective map

$$E(\mathbb{Q})/p \hookrightarrow Ш(A)[p^\infty]$$

and proves that its cokernel is the kernel of a surjective map

$$Ш(E_K)[p^\infty] \to Ш(E)[p^\infty].$$

Thus Corollary 2.12 and the standard conjecture that the Shafarevich–Tate groups are finite imply that $|Ш(A)|$ cannot be a square when E has odd rank over $\mathbb{Q}$ and the image of the Galois action on $E[p]$ is the full group $\mathrm{GL}(\mathbb{F}_p)$.

For an explicit example one can take E to be the elliptic curve

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

of conductor 37. Calculations (based on deep results of Rubin, Kolyvagin, Kato) show that for every odd $p \le 25000$, $p \ne 37$, there exists a prime ℓ as above such that $Ш(A)$ has order pn^2 for some $n \ge 1$.

2.5 Brauer–Manin obstruction

The (cohomological) Brauer group of a scheme X is defined by Grothendieck as the étale cohomology group $\mathrm{H}^2(X, \mathbb{G}_m)$. Let X be a proper geometrically integral variety over a field k. Let $\bar{k}$ be a separable closure of k, $\Gamma = \mathrm{Gal}(\bar{k}/k)$ and $\overline{X} = X \times_k \bar{k}$. By Hilbert's theorem 90 the spectral sequence

$$\mathrm{H}^p(\Gamma, \mathrm{H}^q(\overline{X}, \mathbb{G}_m)) \Rightarrow \mathrm{H}^{p+q}(X, \mathbb{G}_m)$$

gives rise to the exact sequence

$$0 \to \mathrm{Pic}(X) \to \mathrm{Pic}(\overline{X})^\Gamma \to \mathrm{Br}(k) \to \mathrm{Ker}[\mathrm{Br}(X) \to \mathrm{Br}(\overline{X})] \to \mathrm{H}^1(\Gamma, \mathrm{Pic}(\overline{X})). \quad (18)$$

Let k be a number field. Then $\mathrm{H}^3(\Gamma, \bar{k}^*) = 0$, and hence the last arrow in this exact sequence is surjective.

Suppose that X has points everywhere locally, i.e., $X(k_v) \ne \emptyset$ for each place v. Take $P_v \in X(k_v)$ for each v. By functoriality an element $A \in \mathrm{Br}(X)$ gives rise to $A(P_v) \in \mathrm{Br}(k_v)$. We have the local invariant homomorphism $\mathrm{inv}_v : \mathrm{Br}(k_v) \to \mathbb{Q}/\mathbb{Z}$, see Section 2.2.

Lemma 2.15 *Let $A \in \mathrm{Br}(X)$. For almost all places v we have $\mathrm{inv}_v(A(P_v)) = 0$ for any $P_v \in X(k_v)$.*

Sketch of proof. This uses the properness of X. There is a finite set of places S of k and a proper morphism $\mathcal{X} \to \mathrm{Spec}(\mathcal{O}_S)$ whose generic fibre is X such that A extends to an element of $\mathrm{Br}(\mathcal{X})$. By the valuative criterion of properness each point P_v extends to an $\mathcal{O}_v$-point of $\mathcal{X}$. It follows that $A(P_v) \in \mathrm{Br}(k_v)$ comes from an element of $\mathrm{Br}(\mathcal{O}_v)$, but this group is zero, see [6, Ch. XII] or [1, IV.1]. □

Thus we can consider the (finite) sum

$$\sum_v \mathrm{inv}_v(A(P_v)) \in \mathbb{Q}/\mathbb{Z}. \tag{19}$$

It defines the *Brauer–Manin pairing*:

$$\prod_v X(k_v) \ \times \ \mathrm{Br}(X) \ \longrightarrow \ \mathbb{Q}/\mathbb{Z}.$$

Definition 2.16 *The Brauer–Manin set* $\prod_v X(k_v)^{\mathrm{Br}}$ *is the subset of* $\prod_v X(k_v)$ *consisting of the elements orthogonal to* $\mathrm{Br}(X)$ *under the Brauer–Manin pairing.*

The Albert–Brauer–Hasse–Noether theorem from global class field theory says that the diagonal embedding of $\mathrm{Br}(k)$ into the direct sum of $\mathrm{Br}(k_v)$ fits into the exact sequence

$$0 \to \mathrm{Br}(k) \to \oplus_v \mathrm{Br}(k_v) \to \mathbb{Q}/\mathbb{Z} \to 0,$$

where the third map the sum of local invariants. Thus the diagonal image of $X(k)$ in $\prod_v X(k_v)$ is contained in $\prod_v X(k_v)^{\mathrm{Br}}$. One says that the Brauer–Manin obstruction is the only obstruction to the Hasse principle for a given class of varieties if $\prod_v X(k_v)^{\mathrm{Br}}$ is non-empty if and only if $X(k)$ is.

Theorem 2.17 (Manin) *Let A be an abelian variety over a number field k such that $Ш(A)$ is finite. Then the Brauer–Manin obstruction is the only obstruction to the Hasse principle for k-torsors for A.*

This implies that the well known failure of the Hasse principle for plane cubic curves (e.g. Selmer's counterexample $3x^3 + 4y^3 + 5z^3 = 0$) can be explained through the Brauer–Manin obstruction.

Sketch of proof. The idea is to link (19) to the Cassels–Tate pairing. Let X be a k-torsor for A with points everywhere locally. Then $[X] \in Ш(A)$. For each place v fix a point $P_v \in X(k_v)$ in such a way that $(P_v) \in \prod_v X(k_v)^{\mathrm{Br}}$. The exact sequence (18) shows that

$$Ш(A^t) \subset \mathrm{H}^1(\Gamma, \mathrm{Pic}^0(\overline{A})) = \mathrm{H}^1(\Gamma, \mathrm{Pic}^0(\overline{X}))$$

naturally maps to a subgroup in $\mathrm{Coker}[\mathrm{Br}(k) \to \mathrm{Br}(X)]$. Using our explicit description of the Cassels–Tate pairing it is possible to check that if $A \in \mathrm{Br}(X)$ comes from a class $\xi \in Ш(A^t)$, then (up to sign)

$$\sum_v \mathrm{inv}_v(A(P_v)) = \langle [X], \xi \rangle$$

(see [8, Ch. 6] for details). By the finiteness of $Ш(A)$ the left kernel of the Cassels–Tate pairing is zero. Thus if the Brauer–Manin set of X is not empty, then $[X] = 0$ so that X is a trivial torsor isomorphic to A. In particular, $X(k) \neq \emptyset$. $\square$

References

[1] J. Milne. *Étale cohomology*. Princeton University Press, 1980. 8, 31

[2] J. Milne. *Arithmetic Duality Theorems*. Kea Books, 2006. 19, 20, 24, 25

[3] D. Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics **5**. Oxford University Press, 1970. 2, 5, 10, 11, 12

[4] A. Polishchuk. *Abelian varieties, theta functions and the Fourier transform*. Cambridge University Press, 2003. 13, 14

[5] B. Poonen and M. Stoll. The Cassels–Tate pairing on polarized abelian varieties. *Ann. Math.* **150** (1999) 1109–1149. 25

[6] J.-P. Serre. *Corps locaux*. Hermann, 1968. 18, 31

[7] J.-P. Serre. *Groupes algébriques et corps de classes*. Hermann, 1959. 8, 9, 26

[8] A. Skorobogatov. *Torsors and rational points*. Cambridge University Press, 2001. 32

[9] W.A. Stein. Shafarevich–Tate groups of nonsquare order. *Modular curves and abelian varieties*, 277–289, Progr. Math. **224** Birkhäuser, 2004. 29