The Birch and Swinnerton-Dyer Conjecture for Abelian Varieties over Number Fields

Andrei Jorza

April 4, 2005

Contents

Introduction

The factorization of integer numbers is one of the more important simple mathematical concepts with applications in the real world. It is commonly believed that factorization is hard, but nonetheless, that it is possible to factorize an integer into its prime factors. If we pass from the field of rational numbers $\mathbb{Q}$ to a finite extension K (called *number field*) factorization need not be unique. For example, in the field $\mathbb{Q}(\sqrt{-5})$ the integer 6 can be decomposed into prime numbers in two distinct ways:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

This fact led to one attempt at proving Fermat's Last Theorem, where it was assumed that

$$x^n + y^n = \prod_{i=1}^{n} (x - \zeta^i y),$$

is a unique factorization (where ζ is a primitive n-th root of unity), when in fact this need not be the case. The notion of ideal appeared precisely to explain this phenomenon. If $\mathcal{O}_K$ is the ring of integers of the field K, then $\mathcal{O}_K$ is a Dedekind domain and every integer $\alpha \in \mathcal{O}_K$ can be *uniquely* factorized into a product of prime ideals. To understand how far away a number field K is from having unique factorization into elements of $\mathcal{O}_K$ (and not ideals of $\mathcal{O}_K$), one introduces the class group

$$\mathrm{Cl}(K) = \{\text{fractional ideals}\}/\{\alpha\mathcal{O}_K | \alpha \in K^\times\}.$$

The class group is finite and its size, $h(K)$ is an important arithmetic datum of K.

Seemingly unrelated to the class number is the ζ-function of a number field. Initially studied in connection with the distribution of the prime numbers, the ζ-function of a number field K is

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathbb{N}\mathfrak{a}^s},$$

where the sum runs through all integral ideals $\mathfrak{a}$ of $\mathcal{O}_K$ and $\mathbb{N}\mathfrak{a}$ represents the norm of the ideal $\mathfrak{a}$. The function $\zeta_K(s)$ is absolutely convergent when $\mathrm{Re}s > 1$, has holomorphic continuation to all the complex plane and is related to the class number by the following remarkable formula:

Theorem 0.1 (Analytic Class Number Formula)**.** *Let K be a number field, let R_K be the regulator of K, let h_K be the class number and let w_K be the number of roots of unity in K. If the number field K has r_1 real embeddings $K \hookrightarrow \mathbb{R}$ and r_2 complex embeddings $K \hookrightarrow \mathbb{C}$ then*

$$\frac{1}{(r_1 + r_2 - 1)!} \zeta_K^{(r_1+r_2-1)}(0) = -\frac{h_K R_K}{w_K}.$$

Proof. See [Neu99] VII.5.11. □

This formula is important because it relates an analytic object associated with the number field K (the ζ_K-function) to an arithmetic object (the class group). In particular, it allows an efficient computation of h_K if one has an efficient computation of ζ_K. In 1960, Birch and Swinnerton-Dyer generalized this formula to elliptic curves by noting that if $\mathcal{O}_K^\times$ is the group of units of $\mathcal{O}_K$, then by the Dirichlet Unit Theorem ([Neu99] I.12.12) the group $\mathcal{O}_K^\times$ is finitely generated, has rank $r_1 + r_2 - 1$ and its torsion group is the group of roots of unity, whose size is w_K. In the case of an elliptic curve E defined over $\mathbb{Q}$, the Mordell-Weil group $E(\mathbb{Q})$ is finitely generated with rank r. To the elliptic curve E they associated an L-function $L(E, s)$ that is holomorphic when $\mathrm{Re} s > 3/2$ and which they conjectured to have analytic continuation to the whole complex plane $\mathbb{C}$.

Conjecture 0.2 (Birch and Swinnerton-Dyer)**.** *Let E be an elliptic curve of rank r defined over $\mathbb{Q}$. Then $L(E, s)$ has analytic continuation to a neighborhood of 1, its order of vanishing at 1 is equal to r and*

$$\frac{1}{r!}L^{(r)}(E, 1) = \frac{VR_E|Ш(E/\mathbb{Q})|}{|E(\mathbb{Q})_{\mathrm{tors}}|^2},$$

where $Ш(E/K)$ is the Shafarevich-Tate group, V is the volume and R_E is the regulator of E.

The similarity between Theorem 0.1 and Conjecture 0.2 is remarkable. Instead of the size w_K of the torsion of $\mathcal{O}_K^\times$ we now have $|E(\mathbb{Q})_{\mathrm{tors}}|^2$ and instead of h_K we have the size of the Shafarevich-Tate group (which has a similar behavior to that of $\mathrm{Cl}(K)$). Subsequently, Conjecture 0.2 has been refined and later generalized to abelian varieties over number fields by Tate.

Let A be an abelian variety defined over a number field K. Then the Mordell-Weil group $A(K)$ is finitely generated and has rank $r \geq 0$. Then the conjecture, as generalized by Tate is

Conjecture 0.3. *Let A be an abelian variety of rank r defined over a number field K. Let $L(A, s)$ be the global L-function of A, let $A(K)_{\mathrm{tors}}$ and $A^\vee(K)_{\mathrm{tors}}$ be the torsion subgroups of $A(K)$ and $A^\vee(K)$ respectively. Let R_A be the regulator of A, and let $Ш(A/K)$ be the Shafarevich-Tate group. Then $L(A, s)$ has an analytic continuation to a neighborhood of 1, has order of vanishing r at 1, $Ш(A/K)$ is a finite group and*

$$\frac{L^{(r)}(A, 1)}{r! \int_{A(\mathbb{A}_K)} d\mu_{A,w,\Lambda}} = \frac{R_A|Ш(A/K)|}{|A(K)_{\mathrm{tors}}||A^\vee(K)_{\mathrm{tors}}|},$$

where $\int_{A(\mathbb{A}_K)} d\mu_{A,w,\Lambda}$ corresponds to the term V in Conjecture 0.2.

The first statement of Conjecture 0.2 (that the order of vanishing of $L(E, s)$ at 1 is equal to the rank of E) has been proven in the case when the order of vanishing of $L(E, s)$ at 1 is 0 or 1, but otherwise, little is known about it. However, there are proven theorems about the consistency of the conjectures. Thus, if A is an abelian variety defined over a number field L (a Galois extension of K) then the restriction of scalars $R_{L/K}A$ is an abelian variety defined over K. In 5.8 we show that the conjecture (Conjecture 3.15) holds for one if and

only if it holds for the other. More importantly, if $A \to B$ is an isogeny (i.e., surjection with finite kernel) of abelian varieties defined over a number field K, we show in Theorem 5.22 that (under certain hypotheses) the conjecture holds for A if and only if it holds for B.

We begin with an introduction to algebraic groups where we develop the topologies and Haar measures of locally compact groups. Subsequently, we study the geometric structure of abelian varieties, as well as their measure-theoretic properties. We prove that two forms of the Birch and Swinnerton-Dyer conjecture that appear in the literature are indeed equivalent and proceed to use this equivalence to show certain invariance properties (invariance under restriction of scalars and under isogenies). The theory that goes into the statement of the conjecture is very rich, encompassing analytic (measure-theoretic), geometric and algebraic properties of abelian varieties. As a result, in order to prove the invariance properties, we need to study the algebra of Tate's global duality theory for number fields.

Notation

Let K be a number field, i.e., a finite extension of $\mathbb{Q}$. Let $\mathcal{O}_K$ be the ring of integers of K. Let M_K be the set of places of K, let M_K^0 be the set of finite archimedean places and let M_K^∞ be the set of infinite places. The sets M_K^∞ and M_K^0 correspond to the real and complex embeddings on the one hand and prime ideals of $\mathcal{O}_K$ on the other hand.

For every finite place v, let K_v be the completion of K with respect to the metric defined by the valuation v. The ring $\mathcal{O}_K$ is a Dedekind domain and $\mathcal{O}_v = \{x \in K_v | v(x) \geq 0\}$ is a local ring with maximal ideal $\wp_v = \{x \in K_v | v(x) > 0\}$. We will denote by $k_v = \mathcal{O}_v/\wp_v$ the residue field at v and by $q_v = |k_v|$ (if X is a finite set, $|X|$ represents the cardinality of X).

We will write K_v^{nr} for the maximal unramified extension of K_v. Then $I_v = \mathrm{Gal}(\overline{K}_v/K_v^{nr})$ is the inertia group and $\mathrm{Gal}(\overline{K}_v/K_v)/I_v \cong \mathrm{Gal}(\bar{k}_v/k_v)$. Consider the automorphism $\phi_v : x \mapsto x^{-q_v}$ in $\mathrm{Gal}(\bar{k}_v/k_v) = \mathrm{Gal}(K_v^{nr}/K)$. Choose a lift σ_v of ϕ_v to $\mathrm{Gal}(\overline{K}_v/K_v)$, which we call the arithmetic Frobenius element.

The completions K_v are locally compact, Hausdorff and second countable. Thus, there exists a unique (up to normalization) invariant Haar measure μ_v on K_v. The measure μ_v is uniquely defined by the condition $\int_{\mathcal{O}_v} d\mu_v = 1$. This unique measure corresponds to the normalized metric $|x|_v = q_v^{-v(x)} = \mu_v \circ m_x/\mu_v$ where m_x is the multiplication by x automorphism. Since $\mathcal{O}_v/\wp_v^n$ is an n-dimensional vector space over k_v, using the invariance of the Haar measure we get that $\int_{\wp_v^n} d\mu_v = q_v^{-n}$.

Let S be a finite set of places v of K such that $M_K^\infty \subset S$. Define

$$\mathbb{A}_{K,S} = \prod_{v \in S} K_v \times \prod_{v \notin S} \mathcal{O}_v.$$

If $\mathcal{O}_{K,S} = \{a \in K | a \in \mathcal{O}_v, \forall v \notin S\}$ then $\mathcal{O}_{K,S} \hookrightarrow \mathbb{A}_{K,S}$ is a discrete embedding of topological spaces.

Definition 0.4. The ring of K-rational adèles is the ring

$$\mathbb{A}_K = \varinjlim \mathbb{A}_{K,S},$$

where the direct limit is taken over all finite S as above.

Then $\mathbb{A}_K$ is a locally compact, Hausdorff, second countable topological ring and there exists a discrete embedding $K \hookrightarrow \mathbb{A}_K$. The main reason for dealing with the ring of adèles is that it encodes all the local arithmetic properties of elements of the field K.

Remark 0.5. The topology on $\mathbb{A}_K^\times$ is not the one induced from $\mathbb{A}_K$. In particular, $\mathbb{A}_K^\times \hookrightarrow \mathbb{A}_K$ is not an open embedding.

If S is a finite set of primes, let K_S be the maximal algebraic extension of K that is unramified at each place $v \notin S$ and let $G_S = \mathrm{Gal}(K_S/K)$. If $\overline{\mathcal{O}_K}$ is the ring of integers of $\overline{K}$, set $\mathcal{O}_{\overline{K},S} = \mathcal{O}_{K,S} \otimes_{\mathcal{O}_K} \overline{\mathcal{O}_K}$.

We follow the generally accepted notation $H^r(K, M) = H^r(\mathrm{Gal}(\overline{K}/K), M)$ and $H^r(L/K, M) = H^r(\mathrm{Gal}(L/K), M)$ for Galois cohomology of M.

1 Algebraic Groups

1.1 Group Varieties

Let K be a field and let $\overline{K}$ be an algebraic closure of K. In classical algebraic geometry, an affine variety V is a topological subspace of K^n (for some nonnegative integer n) defined as the zero locus of an ideal $I(V) \subset \overline{K}[x_1, \ldots, x_n]$ of polynomials. In that case, $R = \overline{K}[x_1, \ldots, x_n]/I(V)$ is called the coordinate ring of V. If R is generated over $\overline{K}[x_1, \ldots, x_n]$ by $K[x_1, \ldots, x_n]/(I(V) \cap K[x_1, \ldots, x_n])$, then V is said to be defined over the field K. Similarly, a projective variety V is a topological subspace of $\mathbb{P}K^n$, defined as the zero locus of a homogeneous ideal of polynomials $I(V) \subset \overline{K}[x_0, \ldots, x_n]$ (i.e., a set of homogeneous polynomials of degree at least k in an ideal, for some k). For example, the ideal $I = (xy - 1) \subset \overline{\mathbb{Q}}[x, y]$ defines an affine variety $\mathbb{G}_m$ over $\mathbb{Q}$ because $xy - 1$ generates $I \cap \mathbb{Q}[x, y]$.

Every classical variety V is identified with the set of points $V(\overline{K})$ over $\overline{K}$. If the variety is defined over the field K then there is a subset $V(K) \subset V(\overline{K})$ of K-rational points ($V(K)$ may or may not be empty). For every extension L/K, if the variety V is defined over K, it will also be defined over L. Therefore we have an assignment $L \mapsto V(L)$, where $V(L)$ represents the points on V whose coordinates lie in L. Unfortunately, the context of classical algebraic geometry does not allow a thorough understanding of the functorial properties of this assignment, which are especially important if V is a group variety.

Rather than working in an algebraic closure $\overline{K}$ of K and understanding varieties defined over K in terms of polynomials over $\overline{K}$, we will work in the category $\mathbf{Sch}_K$ of schemes defined over $\operatorname{Spec} K$. More generally, we will look at the category $\mathbf{Sch}_S$ of schemes together with morphisms to a scheme S. The language employed will be that of schemes, but the results are essentially about varieties.

Definition 1.1. Let A be a ring. An *abstract variety* V defined over A is a geometrically integral scheme V that is separated and of finite type over $\operatorname{Spec} A$.

If A is an algebraically closed field, the category defined above is equal to the image in $\mathbf{Sch}_A$ of the category of varieties defined over A ([Har77] II.2.6); the only difference is that if V is, for example, an affine variety with coordinate ring R then V is the subset of closed points of $\operatorname{Spec} R$ as an abstract variety.

Affine varieties defined over a field K can now be realized as affine schemes $\operatorname{Spec} R$ with a morphism to $\operatorname{Spec} K$, R being the coordinate ring of the affine variety defined over K. For example, we have defined the affine variety $\mathbb{G}_m$ over K, given by the vanishing of the polynomial $xy-1 \in \overline{K}[x, y]$. However, the polynomial $xy-1$ that generates the defining ideal has coefficients in $\mathbb{Z}$. Therefore we may define $\mathbb{G}_m = \operatorname{Spec} \mathbb{Z}[x, y]/(xy - 1)$ and base-extend to obtain

$$\operatorname{Spec} K[x, y]/(xy - 1) \cong \mathbb{Z}[x, y]/(xy - 1) \times_{\operatorname{Spec} \mathbb{Z}} \operatorname{Spec} K.$$

If the coordinate ring of a variety V is generated by integer polynomials, it is best to interpret V as an abstract variety over $\mathbb{Z}$, because in that case we can make sense of $V(A)$ for every ring A. As a matter of notation, whenever we have a scheme S and two schemes $V, T \in \mathbf{Sch}_S$,

we write $V_T = V \times_S T$. In particular, if an abstract variety V is defined over a ring A and B is an A-algebra we denote by V_B the base-extension $V_B = V \times_{\operatorname{Spec} A} \operatorname{Spec} B$.

In the context of classical varieties, the assignment $L \mapsto V(L)$ takes a field L to the set of points of V whose coordinates lie in L. In the context of schemes $V \in \mathbf{Sch}_S$, the assignment $Z \mapsto V(Z) = \operatorname{Hom}_{\mathbf{Sch}_S}(Z, V)$ is a functor, called the *functor of points*. Therefore, for each S-scheme Z we obtain a set of points $V(Z)$; in particular, if V is an abstract variety defined over a ring A then we obtain the set $V(B)$ for each A-algebra B. Since $V_B(B) = V(B)$, we will write $V(B)$ for the B-points of V_B.

A subcategory of $\mathbf{Sch}_S$ is that of group schemes. A scheme $G \in \mathbf{Sch}_S$ (let $\pi : G \to S$ be the morphism that defines G over S) is called an *S-group scheme* if there exist a point $e \in G(S)$ and morphisms of S-schemes $m : G \times_S G \to G$ and $i : G \to G$ such that:

1. The following diagram is commutative (i is inversion):

$$\begin{array}{ccc} G & \xrightarrow{\mathrm{id} \times i} & G \times_S G \\ {\scriptstyle i\times\mathrm{id}}\downarrow & \searrow^{e\circ\pi} & \downarrow{\scriptstyle m} \\ G \times_S G & \xrightarrow{m} & G \end{array}$$

2. The following diagram is commutative (associativity):

$$\begin{array}{ccc} G \times_S G \times_S G & \xrightarrow{\mathrm{id} \times m} & G \times_S G \\ {\scriptstyle m\times\mathrm{id}}\downarrow & & \downarrow{\scriptstyle m} \\ G \times_S G & \xrightarrow{m} & G \end{array}$$

In particular, an *algebraic group* is an abstract variety G, defined over a ring A, such that G is a group scheme in $\mathbf{Sch}_A$.

Remark 1.2. Let G be a group scheme defined over a scheme S. Then the functor $Z \mapsto G(Z)$ for $Z \in \mathbf{Sch}_S$ defines a group structure on $G(Z)$ as follows. For $x : Z \to G$ (so $x \in G(Z)$) define inversion $x^{-1} = i \circ x$ and for $x, y : Z \to G \in G(Z)$ define multiplication $x \cdot y = m \circ (x, y)$.

Example 1.3. Since the category of affine schemes is opposite to the category of commutative rings, we may define the morphisms e, m and i on $\operatorname{Spec} R$ on the level of R.

1. The affine line can be realized as a group variety as the additive group $\mathbb{G}_a = \operatorname{Spec} \mathbb{Z}[x]$. Then e corresponds to the linear map that takes x to 1; i corresponds to $u \mapsto -u$ and m corresponds to $u \otimes v \mapsto u + v$. If A is a ring then $\mathbb{G}_a(A) = \operatorname{Hom}(\operatorname{Spec} A, \operatorname{Spec} \mathbb{Z}[x]) = A^+$.

2. Similarly, the multiplicative group is $\mathbb{G}_m = \operatorname{Spec} \mathbb{Z}[x, y]/(xy - 1)$. Then e corresponds to the linear map that takes x to 1; i corresponds to the linear map that interchanges x and y and m corresponds to $u \otimes v \mapsto uv$. If A is a ring then $\mathbb{G}_m(A) = \operatorname{Hom}(\operatorname{Spec} A, \operatorname{Spec} \mathbb{Z}[x, y]/(xy - 1)) = A^\times$.

3. The general linear group variety is

$$\mathrm{GL}_n = \operatorname{Spec} \mathbb{Z}[x_{11}, x_{12}, \ldots, x_{nn}, y]/(\det(x_{ij})y - 1).$$

Then e corresponds to the linear map that takes the matrix $M = (x_{11}, \ldots, x_{nn})$ to the identity; i corresponds to the map that inverts the matrix M and m corresponds to $M \otimes N \mapsto MN$ (matrix product). Note that i is *a priori* only defined over $\mathbb{Q}$. However, over $\mathbb{Z}$ the matrix M has determinant ± 1 so its inverse has integer entries as well. If A is a ring then $\mathrm{GL}_n(A)$ is the usual group of invertible $n \times n$ matrices with entries in A.

Definition 1.4. An *abelian variety* is a complete algebraic group, i.e., it is an algebraic group A defined over a field K, such that A is proper over $\operatorname{Spec} K$.

Lemma 1.5. *Let G be an affine algebraic group defined over a field K. Then there exists a nonnegative integer n and a closed immersion $\varphi : G \hookrightarrow \mathrm{GL}_n$ of $\operatorname{Spec} K$-schemes.*

Proof. See [Wat79] Theorem 3.4. □

If K is a field, not necessarily algebraically closed, the variety

$$S^1 = \operatorname{Spec} K[x, y]/(x^2 + y^2 - 1)$$

is an algebraic group whose multiplication and inversion are the morphisms (on the level of the ring of regular functions)

$$\begin{aligned} m((x, y), (z, t)) &= (xz - yt, xt + yz) \\ i(x, y) &= (x, -y). \end{aligned}$$

If K contains a root of the polynomial $X^2 + 1$ then

$$(x, y) \mapsto (x + \sqrt{-1}y, x - \sqrt{-1}y),$$

gives an isomorphism between S^1 and $(\mathbb{G}_m)_K = \mathbb{G}_m \times_{\operatorname{Spec} \mathbb{Z}} \operatorname{Spec} K$. However, S^1 and $\mathbb{G}_m$ need not be isomorphic over K. Indeed, over $\mathbb{F}_p$, for $p \equiv 3 \pmod 4$ prime (for $p = 2$, S^1 is not even a variety, being nonreduced) the group $(\mathbb{G}_m)_{\mathbb{F}_p}(\mathbb{F}_p) = \mathbb{F}_p^\times$ has $p - 1$ elements, while the group $S^1_{\mathbb{F}_p}(\mathbb{F}_p)$ has $p + 1$ elements, parametrized by $(2u/(1 + u^2), (1 - u^2)/(1 + u^2))$ (the parametrization is well-defined, since $p \equiv 3 \pmod 4$ and thus $1 + u^2$ has no roots mod p). If $\mathbb{G}_m$ and S^1 were isomorphic over $\mathbb{F}_p$, they would have the same number of elements over $\mathbb{F}_p$.

Definition 1.6. An algebraic group G defined over a field K is called a *torus* if there exists an isomorphism of algebraic groups defined over $\overline{K}$ between G and $(S^1)^d = (\mathbb{G}_m)^d$, where $d = \dim G$.

Similarly, a unipotent group is classically defined as a subgroup of a linear group $GL_n(\overline{K})$ consisting of upper-triangular matrices. By Lemma 1.5 we obtain the following definition:

Definition 1.7. An algebraic group G defined over a field K is called *unipotent* if, over $\overline{K}$, there exists a composition series $G = G_0 \supset G_1 \supset \ldots \supset G_k \supset \{e\}$ of algebraic groups such that G_i/G_{i+1} is an algebraic subgroup of $(\mathbb{G}_a)_{\overline{K}}$.

1.2 Restriction of Scalars

Let L/K be a finite field extension and let G be an algebraic group defined over L. Consider the functor of K-schemes $Z \mapsto G(Z_L)$. We would like to construct an algebraic group $R_{L/K}G$ defined over K that represents this functor, i.e., for each K-scheme Z we have $(R_{L/K}G)(Z) = G(Z_L)$.

Definition 1.8. Let G be an algebraic group defined over a finite field extension L/K. If the functor of K-schemes $Z \mapsto G(Z_L)$ is representable, we will denote the group that represents it by $R_{L/K}G$. This group is called the *restriction of scalars* of G from L to K.

Let L/K be a Galois extension and let $\{\sigma_1, \ldots, \sigma_d\}$ be the set of embeddings $L \hookrightarrow \overline{K}$. For a group G defined over L we call a pair (H, ψ) of a K-algebraic group H and morphism $\psi : H \to G$ defined over L a *restriction of scalars pair* if there exists a $\overline{K}$ isomorphism

$$\Psi = (\sigma_1\psi, \ldots, \sigma_d\psi) : H \to \prod_{i=1}^{d} G^{\sigma_d},$$

where the twist G^{σ_i} of G by σ is the fiber product

$$\begin{array}{ccc} G^{\sigma_i} & \xrightarrow{\sigma_i} & G \\ \downarrow & & \downarrow \\ \operatorname{Spec} L & \xrightarrow{\sigma_i} & \operatorname{Spec} L \end{array}$$

Lemma 1.9. *Let L/K be a finite Galois extension. If G is the affine or projective space over L then there exists a restriction of scalars pair for G.*

Proof. See [Wei82] Proposition 1.3.1. □

Lemma 1.10. *Let L/K be a finite Galois extension. Let G be an algebraic group defined over L and let G' be a subgroup of G. If there exists a restriction of scalars pair for G then there exists one for G'.*

Proof. Assume that there exists H an algebraic group defined over K and a morphism $\psi : H \to G$ defined over K such that over $\overline{K}$ there is an induced isomorphism $\Psi : H \to \prod_{i=1}^{d} G^{\sigma_i}$. Let $H' = \Psi^{-1}(\prod_{i=1}^{d} G'^{\sigma_i})$. Since ψ is defined over L for any $\sigma \in \mathrm{Gal}(\overline{K}/L)$ we get that $\sigma\Psi^{-1} = \Psi^{-1}$ and so H' is defined over L. Then $(H', \psi_{H'})$ is a restriction of scalars pair for G'. □

Proposition 1.11. *Let L/K be a finite Galois extension and let G be an algebraic group defined over L. If (H, ψ) is a restriction of scalars pair for G then H represents the functor of K-schemes $Z \mapsto G(Z_L)$, i.e., $H = R_{L/K}G$.*

Proof. Let Z be a K-scheme and suppose that $\tau : Z \to H$ is a morphism defined over K, i.e., $\tau \in H(Z)$. Consider the commutative diagram

$$\begin{array}{ccccc} \operatorname{Spec} L & \longleftarrow & Z_L & \xrightarrow{\phi} & G \\ \downarrow & & \downarrow{\scriptstyle \pi} & \searrow^{\zeta} & \uparrow{\scriptstyle \Psi} \\ \operatorname{Spec} K & \longleftarrow & Z & \xrightarrow{\tau} & H \end{array}$$

where $\pi : Z_L \to Z$ is the projection to the Z factor in the fiber product Z_L and $\phi = \Psi \circ \tau \circ \pi \in G(Z_L)$. Denote by F the natural map that takes τ to ϕ. To prove that H represents $Z \mapsto G(Z_L)$ is it enough to show that $F : H(Z) \to G(Z_L)$ is bijective.

Suppose that $\phi \in G(Z_L)$ and let $\zeta = \Psi^{-1} \circ \phi = (\sigma_1\psi, \ldots, \sigma_d\psi)^{-1} \circ (\sigma_1\phi, \ldots, \sigma_d\phi)$. *A priori* this is a morphism defined over L, but for $\sigma \in \operatorname{Gal}(L/K)$ we have

$$\sigma\zeta = (\sigma\sigma_1\psi, \ldots, \sigma\sigma_d\psi)^{-1} \circ (\sigma\sigma_1\phi, \ldots, \sigma\sigma_d\phi) = \zeta$$

since σ permutes the σ_i. Therefore ζ is defined over K. Consequently, ζ factors through Z so there exists a morphism $\tau : Z \to H$ defined over K such that $\zeta = \tau \circ \pi$. In particular, F is surjective since $F(\tau) = \phi$.

Suppose there exist $\tau_1, \tau_2 \in H(Z)$ such that $F(\tau_1) = F(\tau_2)$. For each $z \in Z$ consider an open affine neighborhood $U = \operatorname{Spec} R_z$ of z. Since the map $R_z \to R_z \otimes_K L$ is injective (R_z is a K-vector space), there exists $z' \in \operatorname{Spec} R_z \otimes_K L$ such that $\pi(z') = z$. Therefore, π is surjective. Then, for each $z \in Z$ there exists a $z' \in Z_L$ such that $\pi(z') = z$ which implies that $\tau_1(z) = \tau_1(\pi(z')) = \tau_2(\pi(z')) = \tau_2(z)$. However, morphisms are not defined by their values on points. Consider an open affine cover of H by $\{U_i\}$ and let $V_i = \tau_1^{-1}(U_i)$ be the open preimage of U_i in Z, under the continuous map τ_1. Let $\{W_{ij}\}$ be an affine open cover of V_i. Since τ_1 and τ_2 take the same values on points, we have $\tau_k(W_{ij}) \subset U_i$ for $k = 1, 2$. Let $W_{ij} = \operatorname{Spec} R_{ij}$ and let $U_i = \operatorname{Spec} T_i$. Since the category of affine schemes is opposite to the category of commutative rings, the following diagrams are equivalent:

$$\begin{array}{ccc} W_{ij} \times_K L & & \\ \downarrow{\scriptstyle \pi} \searrow^{\zeta} & & \\ W_{ij} \underset{\tau_2}{\overset{\tau_1}{\rightrightarrows}} U_i & & \end{array} \qquad\qquad \begin{array}{ccc} R_{ij} \otimes_K L & & \\ \uparrow{\scriptstyle \tilde{\pi}} \swarrow_{\tilde{\zeta}} & & \\ R_{ij} \underset{\tilde{\tau}_1}{\overset{\tilde{\tau}_2}{\leftleftarrows}} T_i & & \end{array}$$

But $\tilde{\pi}$ is an injection so $\tilde{\tau}_1 = \tilde{\tau}_2$ so the morphisms τ_1 and τ_2 are equal, since they agree locally. □

Note that by construction $\dim R_{L/K}G = [L : K] \dim G$. Moreover, if we base extend the restriction of scalars to the algebraic closure, it splits into a product of 'twists' of the original group.

Corollary 1.12. *Let L/K be a Galois extension and let G be an algebraic group defined over L. If G is a torus, unipotent group or abelian variety then $R_{L/K}G$ is a torus, unipotent group or abelian variety, respectively.*

Proof. If G is a torus then $R_{L/K}G$ is isomorphic over $\overline{K}$ to a product of $\mathbb{G}_m$, so $R_{L/K}G$ is a torus. If G is an abelian variety, there exists a closed immersion $H \hookrightarrow \mathbb{P}^m_L$ for some m. Therefore there exists a $\overline{K}$ immersion $R_{L/K}G \cong \prod_\sigma G^\sigma \hookrightarrow \prod \mathbb{P}^m_{\overline{K}} \hookrightarrow \mathbb{P}^N_{\overline{K}}$ where $N = (m+1)^{[L:K]} - 1$ is given by the Segre embedding. But any such immersion is defined over a finite extension M/K (by Lemma 1.13 we could choose $M = L$). Let $\varphi : H_M \hookrightarrow \mathbb{P}^N_M$ be the immersion and let $\mathcal{L} = \varphi^* \mathcal{O}_{\mathbb{P}^N_M}(1)$ be a very ample invertible sheaf on H_M. In that case $\otimes_{\sigma : M \hookrightarrow \overline{K}} \mathcal{L}^\sigma$ is an ample invertible sheaf on H, which proves that H is projective, hence an abelian variety.

If G is unipotent, there exists a composition series $G = G_0 \supset G_1 \supset \cdots \supset G_m \supset \{1\}$ defined over $\overline{K}$ such that $G_i/G_{i+1} \cong (\mathbb{G}_a)_{\overline{K}}$. Then $G_{ij} = G_i^{\sigma_j} \times \prod_{k>j} G_0^{\sigma_k}$ is a $\overline{K}$-composition series for $R_{L/K}G$:

$$R_{L/K}G = G_{0,0} \supset G_{1,0} \supset \cdots \supset G_{d,j} \supset G_{0,j+1} \supset G_{1,j} \supset \cdots \supset G_{m,d} \supset \{1\},$$

with $G_{i,j}/G_{i+1,j} \cong (\mathbb{G}_a)_{\overline{K}}$ if $i < d$ and $G_{d,j}/G_{0,j+1} \cong (\mathbb{G}_a)_{\overline{K}}$ otherwise. □

The following lemma shows that it is enough to base-extend to the field of definition of the group to obtain a decomposition into groups isomorphic over L to G:

Lemma 1.13. *Let L/K be a finite separable extension of fields and let $\mathrm{Gal}(L/K) = \{\sigma_1, \ldots, \sigma_d\}$. For any affine or projective algebraic group G we have*

$$R_{L/K}G \times_{\operatorname{Spec} K} \operatorname{Spec} L \cong \prod_{i=1}^{d} G^{\sigma_i}.$$

Proof. Since we will not be using this result, we direct the reader to [PR94] 2.1.2 for further details. □

Example 1.14. Let L/K be a finite extension of fields and let $(\mathbb{G}_m)_L$ be the one-dimensional split torus over L. Then $R_{L/K}\mathbb{G}_m$ is a $[L : K]$-dimensional torus over K that comes with a distinguished map $\psi : R_{L/K}\mathbb{G}_m \to \mathbb{G}_m$. Define $R^1_{L/K}\mathbb{G}_m$ to be the algebraic group that makes the following sequence (defined over K) exact:

$$1 \to R^1_{L/K}\mathbb{G}_m \to R_{L/K}\mathbb{G}_m \to \mathbb{G}_m \to 1.$$

If we base extend to $\overline{K}$, $R_{L/K}\mathbb{G}_m \times_K \overline{K} \cong \prod_{i=1}^d (\mathbb{G}_m^{\sigma_i})_{\overline{K}}$ and so $R^1_{L/K}\mathbb{G}_m \times_K L = \prod_{\sigma_i \neq 1}^d \mathbb{G}_m^{\sigma_i}$ is clearly an algebraic torus.

Remark 1.15. Restriction of scalars from a field L to a subfield K is an effective process. Given equations defining a group G over L one can find equations for $R_{L/K}G$ over K. For example, the group $(\mathbb{G}_m)_{\mathbb{C}}$ is defined by the equation $xy - 1 = 0$. To obtain equations for $R_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m)_{\mathbb{C}}$ write $x = x_1 + ix_2$ and $y = y_1 + iy_2$ where $\mathbb{C} = \mathbb{R}[1, i]$. Then $xy - 1 = 0$ can be rewritten as $x_1y_1 - x_2y_2 - 1 + i(x_1y_2 + x_2y_1) = 0$ so the group $R_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m)_{\mathbb{C}}$ is defined over $\mathbb{R}$ by the equations $x_1y_1 - x_2y_2 - 1 = 0$ and $x_1y_2 + x_2y_1 = 0$. Then the map ψ takes (x_1, x_2, y_1, y_2) to $(x_1^2 + x_2^2, y_1^2 + y_2^2) = (\mathbb{N}_{\mathbb{C}/\mathbb{R}}x, \mathbb{N}_{\mathbb{C}/\mathbb{R}}y)$ and is generally called the *norm* map. Finally, $R^1_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m)_{\mathbb{C}} = \ker \psi$ is given by the equations $x_1 = y_1, x_2 = -y_2$ and $x_1^2 + x_2^2 = 1$.

1.3 Algebraic Groups over a Nonalgebraically Closed Field K

We have seen in Section 1.1 that the groups S^1 and $\mathbb{G}_m$, not isomorphic over $\mathbb{F}_3$, become isomorphic over $\overline{\mathbb{F}_3}$. Let K be a field and let G be an algebraic group defined over K. More generally, we would like to understand the set of abstract varieties defined over K, which are isomorphic to G over $\overline{K}$.

Definition 1.16. Let L/K be a finite extension of fields and let G be an algebraic group defined over K. An L/K-form of G is a pair (H, ψ) of an abstract variety H defined over K and an isomorphism $H \xrightarrow{\psi} G$ defined over L.

Two L/K-forms of G, (H_1, ψ_1) and (H_2, ψ_2), are said to be K-isomorphic if there exists an isomorphism φ defined over K and a commutative diagram:

$$\begin{array}{ccc} H_1 & \xrightarrow{\varphi} & H_2 \\ & {\scriptstyle\psi_1}\searrow \quad \swarrow{\scriptstyle\psi_2} & \\ & G & \end{array}$$

Define $\mathcal{F}(L/K, G)$ to be the set of L/K-forms of G, modulo K-isomorphisms.

Theorem 1.17. *Let L/K be a finite field extension and let G be an affine or projective algebraic group defined over K. Then there exists a bijection*

$$\mathcal{F}(L/K, G) \to H^1(\mathrm{Gal}(L/K), \mathrm{Aut}_L(G)),$$

where $\mathrm{Aut}_L(G)$ represents the set of (not necessarily origin-preserving) isomorphisms of G onto itself.

Proof. For any $\sigma \in \mathrm{Gal}(L/K)$ consider the diagram (over L)

$$\begin{array}{ccc} G & \xrightarrow{\sigma(\psi)\circ\psi^{-1}} & G \\ & {\scriptstyle\psi^{-1}}\searrow \quad \nearrow{\scriptstyle\sigma(\psi)} & \\ & H & \end{array}$$

where $\sigma(\psi) \circ \psi^{-1} \in \mathrm{Aut}_L(G)$. Then $\sigma \mapsto \sigma(\psi)\psi^{-1}$ is a cocycle since $(\sigma\tau)(\psi)\psi^{-1} = \sigma(\tau\psi)(\tau(\psi))^{-1}\tau(\psi)\psi^{-1}$. (Of course, it is not a coboundary since $\psi \notin \mathrm{Aut}_L(G)$.)

Let Φ be the map that associates to each L/K-form (H, ψ) the cocycle $(\sigma \mapsto \sigma(\psi)\psi^{-1}) \in H^1(L/K, \mathrm{Aut}_L(G))$. We need to show that Φ is well-defined. Assume that $(H, \psi) = (F, \phi)$ in $\mathcal{F}(L/K, G)$. Therefore, there exists a K-isomorphism $f : H \to F$ that makes the diagram

$$\begin{array}{ccc} H & \xrightarrow{f} & F \\ & {\scriptstyle\psi}\searrow \quad \swarrow{\scriptstyle\phi} & \\ & G & \end{array}$$

commutative over L. Then

$$\sigma \mapsto \sigma(\psi)\psi^{-1} = \sigma(\phi f)(\phi f)^{-1} = \sigma(\phi)\sigma(f)f^{-1}\phi^{-1} = \sigma(\phi)\phi^{-1},$$

because f is defined over K.

To prove that Φ is a bijection, we first need to show injectivity. If $\Phi((H,\psi)) = 0 \in H^1(L/K, \mathrm{Aut}_L(G))$, then there exists $f \in \mathrm{Aut}_L(G)$ such that $\sigma(\psi)\psi^{-1} = \sigma(f)f^{-1}$ for every $\sigma \in \mathrm{Gal}(L/K)$. Then there exists a diagram defined over L

$$\begin{array}{ccc} H & \xrightarrow{f^{-1}\circ\psi} & G \\ & {\scriptstyle\psi}\searrow \quad \swarrow{\scriptstyle f} & \\ & G & \end{array}$$

But $\sigma(f^{-1}\circ\psi) = f^{-1}\circ\psi$ for every $\sigma \in \mathrm{Gal}(L/K)$ so $f^{-1}\circ\psi$ is a K-isomorphism between (H,ψ) and (G,f).

We will only show surjectivity in the case when G is an affine group. (When G is projective, the proof is similar; see [Ser88], Corollary 21.2.) Let $f \in H^1(L/K, \mathrm{Aut}_L(G))$ be a cocycle. We would like to 'twist' G by f to obtain a new variety G_f, an L/K-form of G. Since G is affine, let $G = \mathrm{Spec}\, R$, where $R = \mathcal{O}_G(G)$ is the ring of global sections of the sheaf of regular functions on G.

There is a natural action of $\mathrm{Gal}(L/K)$ on $R \otimes_K L$, given by $\sigma(r \otimes l) = r \otimes \sigma(l)$. To get the twist, we need to create a new K-algebra R_f. For every $\sigma \in \mathrm{Gal}(L/K)$ an automorphism g of G induces an automorphism $\widetilde{g} : R \otimes_K L \to R \otimes_K L$, defined over L. Construct a new action of $\mathrm{Gal}(L/K)$ on $R \otimes_K L$ defined by

$$\sigma * (r \otimes l) = \widetilde{(\sigma \circ f(\sigma))}(r \otimes l) = \sigma(r \otimes l) \circ f(\sigma),$$

for every $r \in R, l \in L$ (if we interpret $r \otimes l$ as a regular function on G_L). This is a well-defined action, since for $\sigma, \tau \in \mathrm{Gal}(L/K)$ we have (f is a cocycle)

$$\begin{aligned} \sigma\tau * (r \otimes l) &= \sigma\tau(r \otimes l) \circ f(\sigma\tau) = \sigma\tau(r \otimes l) \circ \sigma f(\tau) \circ f(\sigma) \\ &= \sigma(\tau(r \otimes l) \circ f(\tau)) \circ f(\sigma) = \sigma * (\tau * (r \otimes l)) \end{aligned}$$

Since R is the fixed part of $R \otimes_K L$ under the natural $\mathrm{Gal}(L/K)$-action, we can analogously define R_f to be the fixed part of $R \otimes_K L$ under the new action $*$. Then R_f has the structure of a K-algebra and $G_f = \mathrm{Spec}\, R_f$ is an affine variety over K. But, $R_f \otimes_K L \cong R \otimes_K L$, which corresponds to an L-isomorphism between G and G_f. If $\psi : G \to G_f$ is an L-isomorphism, then ψ induces an isomorphism $\widetilde{\psi} : R_f \otimes_K L \cong R \otimes_K L$ with the property that $\sigma\widetilde{\psi}(r \otimes l) = \widetilde{\psi}(\sigma * (r \otimes l))$ for $\sigma \in \mathrm{Gal}(L/K)$. But then

$$\sigma(r \otimes l) \circ \sigma(\psi) = \sigma(r \otimes l) \circ f(\sigma) \circ \psi,$$

which implies that $f(\sigma) = \sigma(\psi) \circ \psi^{-1}$, so we get the cocycle we started with. Therefore, Ψ is surjective. □

Passing to direct limit the bijection $\mathcal{F}(L/K, G) \cong H^1(L/K, \mathrm{Aut}_L(G))$, one similarly gets that

$$\mathcal{F}(\overline{K}/K, G) \cong H^1(K, \mathrm{Aut}_{\overline{K}}(G)).$$

Example 1.18 (One-dimensional tori over a finite field $\mathbb{F}_q$). Theorem 1.17 can be used to characterize the forms of $G = (\mathbb{G}_m)_{\mathbb{F}_q}$, the split one-dimensional torus over the finite field $\mathbb{F}_q$.

Since the category of affine schemes is opposite to that of commutative rings, $\mathrm{End}_{\overline{\mathbb{F}}_q}(G)$ is given by $\mathrm{End}_{\overline{\mathbb{F}}_q}(\mathbb{F}_q[x,y]/(xy-1)) \cong \mathbb{Z}$ since x can map to either a power of x or a power of y. Therefore

$$\mathcal{F}(\overline{\mathbb{F}}_q/\mathbb{F}_q, \mathbb{G}_m) \cong H^1(\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q), \mathrm{Aut}(\mathbb{Z})) = \mathrm{Hom}(\widehat{\mathbb{Z}}, \{\pm 1\}),$$

since $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \widehat{\mathbb{Z}}$. Let Frob be the topological generator of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ corresponding to the unit in $\widehat{\mathbb{Z}}$ (recall that $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$). Any continuous cocycle (which must be a homomorphism, because the Galois action is trivial) is determined by the value it assigns to Frob, so $\mathcal{F}(\overline{\mathbb{F}}_q/\mathbb{F}_q, G) = \{\pm 1\}$.

Since for the extension $\mathbb{F}_{q^2}/\mathbb{F}_q$ we still have $H^1(\mathbb{F}_{q^2}/\mathbb{F}_q, \{\pm 1\}) = \{\pm 1\}$, there are two one-dimensional tori over $\mathbb{F}_q$, and they both split over $\mathbb{F}_{q^2}$. To the cocycle that assigns 1 to Frob corresponds $(\mathbb{G}_m)_{\mathbb{F}_q}$. To determine the torus corresponding to the cocycle that assigns -1 to Frob, recall that $R^1_{\mathbb{F}_{q^2}/\mathbb{F}_q}\mathbb{G}_m$ is one-dimensional, since $[\mathbb{F}_{q^2} : \mathbb{F}_q] = 2$. As in Remark 1.15, the group $R^1_{\mathbb{F}_{q^2}/\mathbb{F}_q}\mathbb{G}_m$ is defined by the equations $x_1 = y_1, x_2 = -y_2$ and $x_1^2 - cx_2^2 = 1$, where c is a generator of $\mathbb{F}_q^\times$ (i.e., $\mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{c})$). Therefore, $(\mathbb{G}_m)_{\mathbb{F}_q}$ and $R^1_{\mathbb{F}_{q^2}/\mathbb{F}_q}\mathbb{G}_m$ are not isomorphic over $\mathbb{F}_q$ and $R^1_{\mathbb{F}_{q^2}/\mathbb{F}_q}\mathbb{G}_m$ must be the one-dimensional torus corresponding to the cocycle -1.

1.4 Structure of Algebraic Groups

When we will analyze the reduction of abelian varieties over finite places v of a number field K, we will encounter smooth, connected algebraic groups defined over the residue field k_v at v, which are not necessarily abelian varieties. The following two theorems determine the structure of such groups.

Theorem 1.19 (Chevalley)**.** *Let G be a smooth, connected group defined over a finite field k. Then there exists an exact sequence (defined over k) of smooth connected algebraic groups*

$$1 \to A \to G \to B \to 1,$$

where A is an affine group and B is an abelian variety.

Proof. The proof can be found in [Con02]. The Theorem holds more generally for any perfect field k. □

To complete the characterization of connected smooth groups over finite fields we need to understand general smooth, connected affine groups.

Theorem 1.20. *Let A be an smooth, connected, affine algebraic group defined over a finite field k. Then there exists a maximal torus T of A and a smooth connected unipotent group N, such that*

$$1 \to T \to A \to N \to 1$$

is an exact sequence defined over k.

Proof. See [Wat79], Theorem 9.5. □

1.5 Topologizing $G(R)$

1.5.1 Discrete Valuation Rings

For convenience, all topological groups (or rings) in this section are assumed to be Hausdorff, locally compact and second countable topological spaces. Let R be a topological ring and let K be its fraction field. In the classical context, for every affine variety V defined over K, the set $V(\overline{K})$ comes with a topology inherited from $\overline{K}^n$ for some nonnegative integer n. In the context of abstract varieties, this does not happen. Let **Top** be the category of topological spaces with morphisms continuous functions. We would like a functor $\mathbf{Sch}'_R \to \mathbf{Top}$ that assigns a topology to $X(R)$ for $X \in \mathbf{Sch}'_R$, where $\mathbf{Sch}'_R$ represents schemes locally of finite type in $\mathbf{Sch}_R$. This section is written under the influence of [Con].

Proposition 1.21. *Let $X \in \mathbf{Sch}_R$ be an affine, finite type R-scheme. There exists a topology on $X(R)$ that depends functorially on X and turns $X(R)$ into a Hausdorff, locally compact and second countable topological space. Moreover, the map $X \mapsto$ topology on $X(R)$ is a functor that respects fiber products and takes closed immersions to closed embeddings. If $R^\times$ is open in R then every open immersion of affine, finite type R-schemes $U \hookrightarrow X$ yields an open embedding $U(R) \hookrightarrow X(R)$.*

Proof. Since X is affine of finite type, there exists a closed immersion $i_X : X \hookrightarrow \operatorname{Spec} R[x_1, \ldots, x_n]$ for some n; therefore there exists an ideal I of $R[x_1, \ldots, x_n]$ such that $X \cong \operatorname{Spec} R[x_1, \ldots, x_n]/I$. Then we can endow $X(R)$ with the topology inherited from R^n by identifying $X(R)$ with the subset of points of R^n in the zero-locus of I.

To prove functoriality in X, consider a morphism of affine, finite type R-schemes $f : X \to Y$, a closed immersion $i_Y : Y \hookrightarrow \operatorname{Spec} R[y_1, \ldots, y_m]$ and an identification $Y \cong \operatorname{Spec} R[y_1, \ldots, y_m]/J$, where J is an ideal of $R[y_1, \ldots, y_m]$. The morphism f induces a morphism $\phi : \operatorname{Spec} R[x_1, \ldots, x_n] \to \operatorname{Spec} R[y_1, \ldots, y_m]$ such that $\phi \circ i_X = i_Y \circ f$. Therefore, there exists a map $\psi : R^n \to R^m$ that makes the following diagram commutative:

$$\begin{array}{ccc} R^n & \xrightarrow{\psi} & R^m \\ {\scriptstyle i_X}\uparrow & & \uparrow{\scriptstyle i_Y} \\ X(R) & \xrightarrow[f]{} & Y(R) \end{array}$$

such that ψ is given by polynomial maps. Then ψ is continuous, which shows that the topology on $X(R)$ agrees with the topology on $Y(R)$. In particular, this shows that the topology on $X(R)$ is independent on the closed immersion i_X.

The properties of $X(R)$ of being Hausdorff and second countable are inherited from the topology on R^n. Moreover, if $X \hookrightarrow Y$ is a closed immersion, then by functoriality of topologizing $X(R)$ and $Y(R)$ we may embed X and Y into $R[x_1, \ldots, x_n]$ for the same n. Then the image of $X(R)$ in $Y(R)$ is given by the vanishing of a continuous map (as in the proof of functoriality); since $Y(R)$ is Hausdorff, we get that $X(R) \hookrightarrow Y(R)$ is a closed embedding. Consequently, since $X(R)$ is Hausdorff in R^n, the topological space $X(R)$ is also locally compact.

Let X and Y be affine, finite type schemes over R, and consider closed immersions $X \hookrightarrow \operatorname{Spec} R[x_1, \ldots, x_n], Y \hookrightarrow \operatorname{Spec} R[y_1, \ldots, y_m]$. Then there exists a closed immersion $X \times_R Y \hookrightarrow \operatorname{Spec} R[x_1, \ldots, x_n, y_1, \ldots, y_m]$ and by functoriality the topology on $(X \times_R Y)(R)$ is the same as the topology on $X(R) \times Y(R)$.

It is enough to show the fact that $U(R) \hookrightarrow X(R)$ is an open embedding when $X = \operatorname{Spec} A$ (for $A = R[x_1, \ldots, x_n]/I$) and $U = \operatorname{Spec} A_f$ for some $f \in A$ (since $\operatorname{Spec} A_f$ form a basis for the topology on X). A point in $U(R)$ is a morphism $\psi : \operatorname{Spec} R \to \operatorname{Spec} A_f$ which corresponds to a homomorphism $A_f \to R$. But $U(R) \subset (\operatorname{Spec} A)(R)$ then corresponds to the set of homomorphisms $A \to R$ that send f to an element in $R^\times$. Since $R^\times \subset R$ is open, $U(R)$ is open, as it is the inverse image of an open set. □

Corollary 1.22. *If $R^\times$ is open in R and X is a locally of finite type R-scheme, then we can functorially assign a topology to $X(R)$ that agrees with the topology assigned in Proposition 1.21 when X is affine, of finite type.*

Proof. Let X be a locally of finite type R-scheme. Every point in $X(R)$ is a morphism $\operatorname{Spec} R \to X$ which factors through an affine open $\operatorname{Spec} R \to U \to X$. This means that we can define a topology on $X(R)$ having as a subbasis the topologies on $U(R)$, for each affine open immersion $U \hookrightarrow X$. To see that this agrees with the topology constructed in Proposition 1.21 for X affine, of finite type, let $U \hookrightarrow X$ be an open immersion. But then $U(R) \hookrightarrow X(R)$ is an open embedding for the topology on $X(R)$ previously constructed. Therefore, the two topologies agree when X is affine, of finite type over R. □

Remark 1.23. Since $\mathcal{O}_v^\times$ is open in $\mathcal{O}_v$ (where $\mathcal{O}_v$ is the ring of integers of a finite place v of a number field K) this allows us to topologize $X(\mathcal{O}_v)$ for every finite type scheme X defined over $\operatorname{Spec} \mathcal{O}_v$.

Remark 1.24. If $R^\times$ is open in R and $X \hookrightarrow Y$ is an open immersion of locally of finite type R-schemes, then $X(R) \hookrightarrow Y(R)$ is an open embedding by Proposition 1.21 and the construction of the topology on $X(R)$.

Let R be a discrete valuation ring with fraction field K. Then for every locally of finite type R-scheme X we topologized $X(R)$; since K is a topological R-algebra and $K^\times$ is open in K, we can topologize $X(F) = (X \times_R F)(F)$. The following lemma mirrors the fact that R is compact in K.

Lemma 1.25. *If R is a topological discrete valuation ring and K is its field of fractions, then $X(R) \hookrightarrow X(F)$ is an open embedding. If, moreover, R is nonarchimedean and X is of finite type, then $X(R)$ is a compact topological space.*

Proof. Since an open immersion $X \hookrightarrow Y$ induces an open embedding $X(R) \hookrightarrow Y(R)$ for X and Y locally of finite type R-schemes (Remark 1.24), and since a basis for the topology on $X(R)$ is given by $U(R)$ for affine open immersion $U \hookrightarrow X$, it is enough to check that $X(R) \hookrightarrow X(F)$ is an open embedding on the level of an open cover. So assume X is affine, of finite type over R.

Consider an open immersion $X \hookrightarrow \operatorname{Spec} R[x_1, \ldots, x_n] = \mathbb{A}^n_R$. Then, $X(R) \hookrightarrow \mathbb{A}^n_R(R)$ and $X(K) \hookrightarrow \mathbb{A}^n_R(K)$ are open embeddings, by Proposition 1.21. Therefore, it is enough to check that $\mathbb{A}^n_R(R) \hookrightarrow \mathbb{A}^n_R(K)$ is an open embedding. By Proposition 1.21, the functor that assigns a topology commutes with products over R, so it is enough to check that $\mathbb{A}^1_R(R) \hookrightarrow \mathbb{A}^1_R(K)$ is an open embedding. But this is equivalent to saying that $R \hookrightarrow K$ is an open embedding which is true, since R is a topological discrete valuation ring and K is its field of fractions.

Assume that R is nonarchimedean. Then, for every affine open U, the set $U(R)$ is compact in $U(K)$ since $U(R)$ inherits its topology from R^n and R^n is compact in K^n. If X is of finite type, then we can cover X with finitely many open affines $\{U_1, \ldots, U_s\}$. Since $U_i(R)$ are compact, it is sufficient to prove that $X(R)$ is covered by $U_i(R)$. Let $f : \operatorname{Spec} R \to X$ be a morphism, i.e., $f \in X(R)$. The only way in which f can fail to be in $\bigcup_{i=1}^s U_i(R)$ is if the image of f is not fully contained in any of the U_i. But R is a topological discrete valuation ring, which implies that $\operatorname{Spec} R = \{u, v\}$ where u is the closed point and the v is the generic point of R (if $\mathfrak{m}$ is the maximal ideal of R then $u = \operatorname{Spec} R/\mathfrak{m}$ and $v = \operatorname{Spec} K$). Assume there exist $i \neq j$ such that $f(u) \in U_i \setminus U_j$ and $f(v) \in U_j \setminus U_i$, i.e., that the image of f is not contained in one affine U_i. But then $f^{-1}(U_i)$ and $f^{-1}(U_j)$ are open sets (since f is continuous) and they separate u, v; this cannot be, since u lies in the closure of v. □

1.5.2 Adèlic Points on Varieties

Recall that if K is a number field then $\mathbb{A}_K$ is the (topological) ring of adèles. Since $\mathbb{A}_K$ is a K-algebra, we have $X(\mathbb{A}_K) = \operatorname{Hom}_K(\operatorname{Spec} \mathbb{A}_K, X) = (X \times_K \mathbb{A}_K)(\mathbb{A}_K)$ for every K-scheme X. We would like to topologize this set in a way that is functorial in X, for X an abstract variety defined over K. In the case when X is affine and of finite type, we may use Proposition 1.21 to achieve this goal. Moreover, the following proposition is a generalization of the fact that $K \hookrightarrow \mathbb{A}_K$ is a discrete embedding. In particular, it will show that if X is affine and of finite type over K, then $X(K)$ embeds discretely in $X(\mathbb{A}_K)$.

Proposition 1.26. *Let $R_1 \hookrightarrow R_2$ be a closed and discrete embedding of topological rings. Let X_1 be an affine finite type R_1-scheme and let $X_2 = (X_1)_{R_2}$. Then there exists a closed and discrete embedding $X_1(R_1) \hookrightarrow X_2(R_2) = X_1(R_2)$ (which is well-defined since R_2 has the structure of an R_1-algebra).*

Proof. The closed embedding $R_1 \hookrightarrow R_2$ induces a closed embedding $X_1(R_1) \hookrightarrow X_2(R_2)$, because the embedding $R_1^n \hookrightarrow R_2^n$ is closed for every n. Since R_1 embeds discretely in R_2

we get that R_1^n embeds discretely into R_2^n so the same happens on their subsets $X_1(R_1)$ and $X_2(R_2)$ with their inherited topologies. □

However, as we have seen in Remark 0.5, $\mathbb{A}_K^\times$ is not open in $\mathbb{A}_K$, so we cannot use Corollary 1.22 to topologize $X(\mathbb{A}_K)$, if X is an abelian variety, for example. Even in the case when X is affine of finite type, we would like to topologize $X(\mathbb{A}_K)$ in a manner that is compatible with the previously constructed topologies on $X(K_v)$ and $\mathcal{X}_v(\mathcal{O}_v)$, if $\mathcal{X}_v$ is a model over $\mathcal{O}_{K,S}$ for X.

The main problem with this is that the ring $\mathbb{A}_K$ consists of sequences $(x_v)_v$ such that $x_v \in K_v$ and $x_v \in \mathcal{O}_v$ for all but finitely many places v. However, X is defined over K and $\mathcal{O}_v$ is not a K-algebra, so there is no canonical notion of $\mathcal{O}_v$-valued points of X. If X is defined over K_v by an ideal of polynomials I, then for $\{P_i\}$ a set of generators of I, the rational roots of all P_i will lie in K_v^n for some n. In that case, we could define the $\mathcal{O}_v$-points to be those roots which lie in $\mathcal{O}_v^n$. However, this set depends on the choice of generators of I. A more functorial way to express the choice of equations is the notion of a model.

Definition 1.27. Let K be a field and let R be a subring of K. Let X be a K-scheme. A *model* $\mathcal{X}$ for X over R is an R-scheme such that $\mathcal{X} \times_R K \cong X$.

The above definition simply says that if the model $\mathcal{X}$ has equations with coefficients in R, then X is the variety given by the same equations, but whose coefficients are now interpreted in K. As it stands, the definition of a model is too inclusive to be useful. We will restrict our attention to models which are smooth, separated and of finite type over R. For example, let K be a number field and let $\mathcal{O}_K$ be its ring of integers. If $G = \operatorname{Spec} K[x_1, \ldots, x_n]/(f_1, \ldots, f_d)$ is an affine algebraic group and $m \in \mathbb{Z}$ such that $mf_1, \ldots, mf_d \in \mathcal{O}_K[x_1, \ldots, x_n]$, then $\operatorname{Spec} R[X_1, \ldots, X_n]/(mf_1, \ldots, mf_d)$ is an affine model for G, which is separated and of finite type over $\mathcal{O}_K$.

From now on we will restrict our attention to algebraic groups G defined over a number field K. Let S be a finite set of places of K, such that S contains the set of infinite places, M_K^∞. Recall that $\mathcal{O}_{K,S}$ is the set of $x \in K$, such that $v(x) \geq 0$ for all $v \notin S$ and $\mathbb{A}_{K,S} = \{(x_v)_v \in \mathbb{A}_K | v(x_v) \geq 0, \forall v \notin S\}$, an $\mathcal{O}_{K,S}$-algebra. Choose a model G_S for G over $\mathcal{O}_{K,S}$ such that G_S is smooth, separated and of finite type, as above. (In terms of equations this corresponds to clearing denominators with positive v-valuation for $v \notin S$.) Given that $\varinjlim \mathbb{A}_{K,S} = \mathbb{A}_K$, one can use the following theorem to redefine $G(\mathbb{A}_K)$.

Theorem 1.28. *Let R_i be a direct system of rings and $R = \varinjlim R_i$. If X_i and Y_i are finitely presented R_i-schemes then for $j \geq i$ we have*

$$\varinjlim_j \operatorname{Hom}_{R_j}((X_i)_{R_j}, (Y_i)_{R_j}) \xrightarrow{\cong} \operatorname{Hom}_R((X_i)_R, (Y_i)_R).$$

Proof. See [BLR90], Lemma 1.2.5. □

The previous theorem is a global version of the denominator clearing procedure for the construction of a model for affine varieties over $\mathcal{O}_{K,S}$. Having chosen a separated and finite-type model G_S for G over $\mathcal{O}_{K,S}$, let $G_T = G_S \times_{\mathcal{O}_{K,S}} \mathcal{O}_{K,T}$ for each finite set $T \supset S$. In Theorem

1.28 let $\{T \text{ finite } | T \supset S\}$ be the direct system and let $R_S = \mathcal{O}_{K,S}$. Let $X_S = \operatorname{Spec} \mathbb{A}_{K,S}$ which implies that $X_T = X_S \times_{\mathcal{O}_{K,S}} \mathcal{O}_{K,T} = \operatorname{Spec} \mathbb{A}_{K,T}$. Finally, $\varinjlim R_S = K$, $(X_S)_K = \mathbb{A}_K$ and $(G_S)_K = G$, since G_S is a model for G. Therefore, by Theorem 1.28 we get a bijection

$$\varinjlim_T \operatorname{Hom}_{\mathcal{O}_{K,T}}(\operatorname{Spec} \mathbb{A}_{K,T}, G_T) = \operatorname{Hom}_K(\operatorname{Spec} \mathbb{A}_K, G),$$

or, equivalently,

$$\varinjlim_T G_T(\mathbb{A}_{K,T}) = G(\mathbb{A}_K) \tag{1.1}$$

Remark 1.29. The identification 1.1 can be made precise, as follows. Since $\mathbb{A}_{K,T}$ is a $\mathcal{O}_{K,S}$ algebra ($S \subset T$), we have an identification $G_T(\mathbb{A}_{K,T}) = G_S(\mathbb{A}_{K,T})$ and similarly $G(\mathbb{A}_K) = G_S(\mathbb{A}_K)$. Since $\mathbb{A}_{K,T} \subset \mathbb{A}_K$ there is a natural map $G_S(\mathbb{A}_{K,T}) \to G_S(\mathbb{A}_K)$, which induces a natural map

$$\varinjlim_T G_T(\mathbb{A}_{K,T}) = \varinjlim_T G_S(\mathbb{A}_{K,T}) \longrightarrow G_S(\mathbb{A}_K) = G(\mathbb{A}_K).$$

By Theorem 1.28, this natural map is bijective. In particular, if we had topologies on $G_S(\mathbb{A}_{K,T})$, they would induce a topology on $G(\mathbb{A}_K)$.

We would like to construct (functorially) a topology on $G_S(\mathbb{A}_{K,S})$, for S, a finite set of primes. Recall that G_S is defined over $\operatorname{Spec} \mathcal{O}_{K,S}$, so we are allowed to define $G_{S,v} = G_S \times_{\mathcal{O}_{K,S}} \mathcal{O}_v$, for places $v \notin S$. For the places in S, write $G_v = G_S \times_{\mathcal{O}_{K,S}} K_v$. In order to define a topology on $G_S(\mathbb{A}_{K,S})$, we need to relate the set of points $G_S(\mathbb{A}_{K,S})$ to the sets $G_{S,v}(\mathcal{O}_v)$ and $G_v(K_v)$, for which we have already constructed functorial topologies in Corollary 1.22.

Proposition 1.30. *There exists a bijection*

$$G_S(\mathbb{A}_{K,S}) = \prod_{v \in S} G_v(K_v) \times \prod_{v \notin S} G_{S,v}(\mathcal{O}_v).$$

Proof. See [Con], Theorem 2.10. □

Remark 1.31. This is not a very surprizing result, since the same result for $\mathbb{G}_a$ is the definition of $\mathbb{A}_{K,S}$. The product topology on $\prod_{v \in S} G_v(K_v) \times \prod_{v \notin S} G_{S,v}(\mathcal{O}_v) = G_S(\mathbb{A}_{K,S})$ induces a functorial topology on $G(\mathbb{A}_K)$ that is compatible with the topology constructed in Proposition 1.21 in the case that G is affine.

Proposition 1.32. *Let G be an algebraic group defined over a number field K and let $S \supset M_K^\infty$ be a finite set of primes. If G has a separated and finite-type model G_S over $\mathcal{O}_{K,S}$, then $G(\mathbb{A}_K)$ is a (Hausdorff, second countable, locally compact) topological group.*

Proof. By construction, the topological space $G_S(\mathbb{A}_{K,S})$ is second countable (since it has the product topology of a countable number of second countable spaces). Since G_S is separated, $G_S(\mathbb{A}_{K,S})$ is Hausdorff. By Lemma 1.25, the topological spaces $G_{S,v}(\mathcal{O}_v)$ are compact. Since $G_v(K_v)$ are locally compact, Proposition 1.30 implies that the space $G_S(\mathbb{A}_{K,S})$ is locally compact (using Tychonov's theorem). The result then follows from Remark 1.29. (See [Con], 2.12.) □

Therefore, if G is an algebraic group with a separated and finite-type model G_S over $\mathcal{O}_{K,S}$, then $G(\mathbb{A}_K)$ is a locally compact topological group. If G is an abelian variety, it is projective by Proposition 2.9 and it has a 'Néron' model, which is a smooth, separated and finite-type model over $\mathcal{O}_K$ (by Theorem 2.41). In this case, more can be said about the topology of $G(\mathbb{A}_K)$.

Proposition 1.33. *If A is an abelian variety defined over a number field K, then $A(\mathbb{A}_K)$ is a compact topological group.*

Proof. The proof of this theorem depends on technical results from Section 2.3, but the proposition belongs here from a logical perspective. Let $\mathcal{A}$ be the 'Néron' model for A over $\mathcal{O}_K$, i.e., a smooth, separated and finite-type model for A over $\mathcal{O}_K$. By Corollary 2.53 and Lemma 2.48, there exists a finite set of places S containing the M_K^∞ of infinite places such that $\mathcal{A}_S = (\mathcal{A})_{\mathcal{O}_{K,S}}$ is proper. (In the technical language of Section 2.3, A has good reduction at all places $v \notin S$; for each such place v of good reduction, the fiber of $\mathcal{A}$ over v is an abelian variety, hence proper.)

Let $v \notin S$ and let $\mathcal{A}_v = \mathcal{A} \times_{\mathcal{O}_K} \mathcal{O}_v$. By the valuative criterion of properness (or by the Néron mapping property) we have a bijection $\mathcal{A}_v(\mathcal{O}_v) \xrightarrow{\cong} A(K_v)$. By Lemma 1.25 it will be an open embedding, which implies that the bijection is a homeomorphism. Consequently, if $T \supset S$ is a finite set of places, then there exists a homeomorphism

$$A_S(\mathbb{A}_{K,S}) \longrightarrow A_T(\mathbb{A}_{K,T}),$$

since

$$A_S(\mathbb{A}_{K,S}) \cong A_T(\mathbb{A}_{K,T}) \cong \prod_v A(K_v)$$

by the above. Therefore, to prove that $A(\mathbb{A}_K)$ is compact, it is enough to show that each $A_T(\mathbb{A}_{K,T})$ is compact. Since $A_T(\mathbb{A}_{K,T}) \cong \prod A(K_v)$, by Tychonov's theorem, it is enough to show that each $X(K_v)$ is compact.

Let v be a finite place. Since A is projective, there exists a closed immersion $A_{K_v} \hookrightarrow \mathbb{P}^m_{K_v}$ (where $\mathbb{P}^m = \operatorname{Proj} \mathcal{O}_v[x_1, \ldots, x_m]$), which induces a closed embedding $A(K_v) \hookrightarrow \mathbb{P}^m_{K_v}(K_v)$, since $\mathcal{O}_v^\times$ is open in $\mathcal{O}_v$ (Proposition 1.21). By the valuative criterion of properness, $\mathbb{P}^m_{K_v}(K_v) = \mathbb{P}^m(\mathcal{O}_v)$. Since $\mathbb{P}^m(\mathcal{O}_v)$ can be covered by finitely many sets of the form $U(\mathcal{O}_v)$, where U is affine open, and each $U(\mathcal{O}_v)$ is compact by Lemma 1.25, it follows that $\mathbb{P}^m_{K_v}(K_v)$ is compact. Therefore, $A(K_v)$ is compact as a closed subset of a compact set.

Similarly, if v is real of complex, we need to show that $\mathbb{P}^m\mathbb{R}$ and $\mathbb{P}^m\mathbb{C}$ are compact. But $\mathbb{P}^m\mathbb{R}$ and $\mathbb{P}^m\mathbb{C}$ can be realized as finite CW-complexes, which implies that they are compact ([Hat02], 0.4, 0.6). □

1.6 Defining a Measure on $G(R)$

Let R be a topological discrete valuation ring and let K be its fraction field, of characteristic 0 (for example, $R = \mathcal{O}_v$ and $K = K_v$). Let G be a finite type group scheme of dimension n over K. In particular, G is smooth over F.

Lemma 1.34. *The topological space $G(K)$ has the structure of an n-dimensional topological K-manifold, i.e., for every point $g \in G(K)$ there exists an open neighborhood W of g and a homeomorphism $\psi : W \to \psi(W)$ onto an open set in K^n endowed with the product topology.*

Proof. Every morphism $\operatorname{Spec} K \to G$ factors through some open affine $U \hookrightarrow G$. Since the condition of being a manifold is local, it is enough to check that $U(K)$ is a K-manifold. Consider a closed immersion $h : U \hookrightarrow \operatorname{Spec} K[x_1, \ldots, x_m]$ that induces an isomorphism $U \cong \operatorname{Spec} K[x_1, \ldots, x_m]/I$ for an ideal I generated by polynomials $f_1, \ldots, f_k$. Then U is a smooth affine subvariety of $\mathbb{A}^m_K$ so $U(K)$ is a K-manifold by the implicit function theorem. □

We would like to define a differential structure on $G(K)$ that is compatible with the differential structure on G. Since G is a smooth group variety of dimension n over K, the sheaf of differentials of top degree, $\Omega^n_{G/K}$, is a free $\mathcal{O}_G$-module generated by an invariant differential w ([BLR90], Chapter 4.2, Corollary 3). We would like to use this differential together with the canonical measure μ_v to define a Haar measure on the locally compact topological groups $G(K)$ and $G(R)$. Since both w and a Haar measure on $G(K)$ are left invariant, it is enough to define the measure in a neighborhood of a point $g \in G(K)$. As before, let $U \hookrightarrow X$ be an affine open immersion such that $g \in U(R)$. Let $W \subset U(R)$ be an open neighborhood of g and let $\psi : W \to \psi(W)$ be a homeomorphism onto an open neighborhood of K^n.

Consider a closed immersion $h : U \hookrightarrow \operatorname{Spec} K[x_1, \ldots, x_m] = \mathbb{A}^m_K$. Note that G is smooth at g which implies that exist local generating sections $y_1, \ldots, y_n$ of $\mathcal{O}_G(U)$ at g such that $dy_1, \ldots, dy_n$ generate $(\Omega^1_{G/K})_g$, where $\Omega^1_{G/K}$ is the sheaf of differentials of degree 1 on G. Then by the Jacobi criterion ([BLR90], Chapter 2.2, Proposition 7) we may assume that $dy_1, \ldots, dy_n, dx_{n+1}, \ldots, dx_m$ generate $(\Omega^1_{\mathbb{A}^m_K})_g$ as a $(\mathcal{O}_{\mathbb{A}^m_K})_g$-module. Therefore, via the immersion f, we can identify $f(y_1), \ldots, f(y_n)$ with coordinate functions on $\mathbb{A}^n_K \subset \mathbb{A}^m_K$. This process can be reversed. Let $z_1, \ldots, z_n$ be the standard coordinates on $\mathbb{A}^n_K$. By the above, the pullbacks $y_1 = h^*(z_1), \ldots, y_n = h^*(z_n)$ form local generating sections of $\mathcal{O}_G(U)$. Define $dy_{i,v} = \psi^* dz_i$, i.e., $dy_{i,v}$ are the pullbacks of the standard differentials on K^n, viewed as a K-manifold. The differentials dz_i are the normalized Haar measures on the K-lines defined by the directions z_i; their pullbacks, the differentials $dy_{i,v}$ transport the differential structure from K^n to $G(K)$.

Since $dy_1, \ldots, dy_n$ generate $(\Omega^1_{G/K})_g$, in a small enough open neighborhood $V \subset U$ of g we can write $w = f dy_1 \wedge dy_2 \wedge \ldots \wedge dy_n$ where $f \in (\mathcal{O}_G)_g$ is a rational function in $\mathcal{O}_G(V)$ and is well-defined at g. This implies that one can express f as a power series in the local coordinates $y_1, \ldots, y_n$:

$$f = \sum_{i_1, \ldots, i_n} a_{i_1 i_2 \ldots i_n} (y_1 - y_1(g))^{i_1} \cdots (y_n - y_n(g))^{i_n},$$

that converges in a small enough open neighborhood V.

In a neighborhood of g, define $|w|_v$ to be $|f|_v dy_{1,v} \wedge \ldots \wedge dy_{n,v}$, where $|f|_v$ is the usual norm associated to the rational function f. The following lemma makes implicit use of the

identification of a measure μ with the integral $\int d\mu$ it defines (by the Riesz representation theorem).

Lemma 1.35. *There exists a global invariant Haar measure $\int |w|_v$ on $G(K)$, that is compatible with the local invariant differentials $|w|_v$.*

Proof. It is enough to show that, locally, the differential form $|w|_v$ is functorial in the choice of local coordinates $z_1, \ldots, z_n$. By Fubini's theorem we can do integration on fibers so it is enough to prove functoriality if we only change z_1 to another local coordinate t_1. If $s_1 = h^*(t_1)$, note that $ds_1/dy_1 \in (\mathcal{O}_G)_g$ so we can write

$$w = f dy_1 \wedge dy_2 \wedge \ldots \wedge dy_n = (f ds_1/dy_1) ds_1 \wedge dy_2 \wedge \ldots \wedge dy_n.$$

Therefore, we need to show that

$$|f|_v ds_{1,v} \wedge dy_{2,v} \wedge \ldots \wedge dy_{n,v} = |f ds_1/dy_1|_v dy_{1,v} \wedge \ldots \wedge dy_{n,v},$$

or equivalently, that $ds_{1,v} = |ds_1/dy_1|_v dy_{1,v}$. This result is well-known if v is an infinite place. Assume that v is a finite place.

Since z_1 and t_1 are both local coordinates for K^n at $\psi(g) = 0$, there exists a converging power series (after scaling) $t_1 = z_1 + a_2 z_1^2 + a_3 z_1^3 + \cdots$. Therefore, $dt_1/dz_1 = 1 + 2a_2 z_1 + 3a_3 z_1^2 + \cdots$. If z_1 is close to 0 (around $\psi(g)$), the valuation $v(2a_2 z_1 + 3a_3 z_1^2 + \cdots)$ will be large, since v is nonarchimedean. Then,

$$v(1 + 2a_2 z_1 + 3a_3 z_1^2 + \cdots) = \min(0, v(2a_2 z_1 + 3a_3 z_1^2 + \cdots)) = 0,$$

which implies that $|ds_1/dy_1|_v = |\psi^*(dt_1/dz_1)|_v = 1$ (the last equality follows from the fact that ψ is an isomorphism). Then

$$\begin{aligned} ds_{1,v}/dy_{1,v} &= \psi^*(dt_1)/\psi^*(dz_1) && (1.2)\\ &= \psi^*(dz_1 + a_2 dz_1^2 + \cdots)/\psi^*(dz_1) && (1.3)\\ &= 1 + 2a_2 dz_1 + \cdots = 1 && (1.4)\\ &= |ds_1/dy_1|_v && (1.5) \end{aligned}$$

around g. (The last equality is a reinterpretation of the fact that smooth is equivalent to locally constant in the case of nonarchimedean fields.)

□

By Lemma 1.25 we can restrict $|w|_v$ to a Haar measure on the locally compact topological group $G(R)$.

1.7 Tamagawa Measures on $G(\mathbb{A}_K)$

Let G be an algebraic group of dimension n defined over a field K. Let S be a finite set of primes such that $S \supset M_K^\infty$. Let G_S be a separated, finite-type model for G over $\mathcal{O}_{K,S}$ and assume that G_S is a group scheme. We would like to explicitly define a Haar measure on the locally compact topological group $G(\mathbb{A}_K)$, that is compatible with the Haar measures $\int |w|_v$ on $G_v(K_v)$ and $G_{S,v}(\mathcal{O}_v)$.

For every place $v \notin S$, if $\pi_v : G_S \times_{\mathcal{O}_{K,S}} \mathcal{O}_v \to G_S$ is projection to the first coordinate, then $w_v = \pi_v^* w$ is a left-invariant differential on $G_{S,v}$ ([Har77], Chapter 2, Proposition 8.10). Similarly we get invariant differentials w_v on G_v for $v \in S$. To each w_v, Lemma 1.35 associates a differential form $|w|_v$ on the topological space $G_{S,v}(\mathcal{O}_{K,S})$ (if $v \notin S$) and $G_v(K_v)$ (if $v \in S$).

Example 1.36.

1. Let $G = \mathbb{G}_a$ be the additive group defined over a field K. Then $\mathbb{G}_a = \operatorname{Spec} K[x]$ and an invariant differential on $\mathbb{G}_a$ is dx which becomes dx_v over all K_v. Then, the normalized measure μ_v is $\int dx_v$.

2. Let $G = \mathbb{G}_m$ be the multiplicative group defined over a number field K. Then $\mathbb{G}_m = \operatorname{Spec} K([x,y]/(xy-1) = \operatorname{Spec} K[x,x^{-1}]$. One choice of (multiplicative) invariant differential form is $x^{-1}dx$ which gives $dx_v/|x|_v$ over the completion K_v.

We would like to create a normalized Haar measure on each of $G_v(K_v)$, $G_{S,v}(\mathcal{O}_v)$ and $G(\mathbb{A}_K)$. However, the group $G(\mathbb{A}_K)$ is an infinite product of groups $G_v(K_v)$ and $G_{S,v}(\mathcal{O}_v)$. Therefore, if the Haar measures $\int |w|_v$ are not normalized, simply taking the product of the measures on $G_{S,v}(\mathcal{O}_v)$ to yield a Haar measure on $G(\mathbb{A}_K)$ might not be well defined.

Definition 1.37. A set $\{(\lambda_v)_v\}$ of positive real numbers is called a set of *convergence factors* for G if

$$\prod_{v \notin S} \left(\int_{G_{S,v}(\mathcal{O}_v)} |w|_v \lambda_v^{-1} \right),$$

converges absolutely.

Remark 1.38. The fact that an infinite product $\prod_{i=1}^\infty x_v$ converges absolutely means that $a_n = \prod_{i=1}^n |x_v|$ is a convergent sequence whose limit is not 0.

In order for this definition to make sense, we need to make sure that the notion of set of convergence factors is independent of the choices of the set S, model G_S and invariant differential w. Invariance with respect to the choice of S follows from the fact that S is a finite set, and so the choice of S does not affect convergence. Moreover, every invariant differential w on G_S is defined up to a scalar $\alpha \in K^\times$. But this changes the product by $(\prod_{v \in S} |\alpha|_v^{-1})|\alpha|_{\mathbb{A}_K} = \prod_{v \in S} |\alpha|_v^{-1}$ since $\alpha \in K^\times$. Therefore, the choice of w is irrelevant.

Let G'_S be another separated and finite-type model for G over $\mathcal{O}_{K,S}$. Then, there exists a K-isomorphism $(G_S)_K \cong G \cong (G'_S)_K$. On the level of equations for G_S and G'_S, the isomorphism is given by polynomials $F = (f_1, \ldots, f_r)$ with coefficients in K. Since the models G_S and G'_S are assumed to be of finite type, there exist finitely many equations that define them. The fact that F is an isomorphism on the generic fiber G implies that F is an

isomorphism from one set of equations to the other, when the coefficients are interpreted in K, rather than in $\mathcal{O}_{K,S}$. But, if M is the least common multiple of all the denominators of all the coefficients of the polynomials f_i, then the f_i have coefficients in $\mathcal{O}_v$ as long as the finite place v does not divide M. Hence, for all but finitely many v, F is an isomorphism on the special fibers $F : (G_S)_v \cong (G'_S)_v$, which implies that the infinite products

$$\prod_{v \notin S} \left(\int_{G_{S,v}(\mathcal{O}_v)} |w|_v \lambda_v^{-1} \right),$$

and

$$\prod_{v \notin S} \left(\int_{G'_{S,v}(\mathcal{O}_v)} |w|_v \lambda_v^{-1} \right),$$

differ at finitely many places. Therefore, the choice of model G_S is irrelevant.

The local measures $\int |w|_v \lambda_v^{-1}$ induce a global measure

$$d\tilde{\mu}_{G,w,(\lambda_v)} = \varinjlim \prod_v \int |w|_v \lambda_v^{-1}$$

on $\mathbb{A}_K$.

Remark 1.39. The definition of a set of convergence factors leaves open the question whether there exists a canonical choice of such a set. We will see that for abelian varieties there exists a canonical choice.

Example 1.40.

1. Let $G = \mathbb{G}_a$ be the additive group. Then a set of convergence factors is $\lambda_v = 1$ for all v, by definition of the normalized measure μ_v. Moreover, $\mathbb{G}_a(K)$ embeds discretely in $\mathbb{G}_a(\mathbb{A}_K)$ and $\mathbb{G}_a(\mathbb{A}_K)/\mathbb{G}_a(K)$ is compact with finite volume

$$\mu_K = \int_{\mathbb{G}_a(\mathbb{A}_K)/\mathbb{G}_a(K)} d\tilde{\mu}_{\mathbb{G}_a,dx,(1)} = \sqrt{|d_K|},$$

where d_K is the discriminant of the number field K ([Wei82], 2.1.3.a). In particular, the global measure $d\tilde{\mu}_{\mathbb{G}_a,dX,(1)}$ induces a global metric on $\mathbb{A}_K$, which is compatible with the local ones $|a|_{\mathbb{A}_K} = \prod_v |a_v|_v$ for every $a = (a_v) \in \mathbb{A}_K^\times$.

2. Let $G = \mathbb{G}_m$. By Example 1.36 we may choose $w_v = dx_v/|x|_v$; then

$$\int_{\mathcal{O}_v^\times} w_v = \int_{\mathcal{O}_v^\times} dX_v = \int_{\mathcal{O}_v} dX_v - \int_{\wp_v} dX_v = \int_{\mathcal{O}_v} (1 - 1/q_v) dX_v = 1 - q_v^{-1}.$$

Therefore we may choose $\lambda_v^{-1} = 1 - q_v^{-1}$.

Remark 1.41. Let $\mathbb{G}_m^1(\mathbb{A}_K) = \{a \in \mathbb{A}_K || a| = 1\}$ be the maximal subgroup of $\mathbb{G}_m(\mathbb{A}_K)$ such that $\mathbb{G}_m^1(\mathbb{A}_K)/\mathbb{G}_m(K)$ is compact. Let $w = dx/x$ and $\lambda_v = (1 - q_v^{-1})^{-1}$. Then

$$\int_{\mathbb{G}_m^1(\mathbb{A}_K)/\mathbb{G}_m(K)} d\tilde{\mu}_{\mathbb{G}_m,w,(\lambda_v)} = \frac{2^{r_1}(2\pi)^{r_2} R_K h_K}{\sqrt{|d_K|} w_K}$$

if K is a number field ([Tat67]).

One of the downsides of the measure $d\tilde{\mu}$ is that it does not have functorial properties. In order to make the global measure compatible with restriction of scalars, we need to make the following adjustment:

Definition 1.42. Let G be an algebraic group and let w be an invariant differential on the model G_S. The Tamagawa measure on G associated with w and the set of convergence factors $\Lambda = \{\lambda_v\}$ is

$$d\mu_{G,w,(\lambda_v)} = \mu_K^{-\dim G} d\tilde{\mu}_{G,w,\Lambda}.$$

1.7.1 Compatibility with Restriction of Scalars

Let L/K be a Galois extension of number fields and let (θ_i) be an integral basis of L over K. Let $d = [L : K]$, $\mathrm{Gal}(L/K) = \{\sigma_1, \ldots, \sigma_d\}$ and let $\Delta = \det(\theta_i^{\sigma_j})$. Consider an algebraic group G of dimension n over L and let $H = R_{L/K}G$ be the restriction of scalars group defined over K. Recall that H comes with an L-morphism $\psi : H \to G$ that induces a $\overline{K}$ isomorphism

$$\Psi = (\sigma_1\psi, \ldots, \sigma_d\psi) : H \xrightarrow{\cong} \prod_i G^{\sigma_i}.$$

Consider an invariant differential w_G of degree n on G and define

$$w_H = \Delta^{-n} \bigwedge_{i=1}^{d} (\psi^{\sigma_i})^*(w_G^{\sigma_i}).$$

The main problem with the definition of w_H is that the factor Δ^{-n} is needed, or else a reordering of $\{\sigma_1, \ldots, \sigma_d\}$ would change the differential w_H.

Lemma 1.43. *The invariant differential w_H is defined over K.*

Proof. By construction, it is defined over L. For every $\sigma \in \mathrm{Gal}(L/K)$ we have

$$w_H^\sigma = \det(\theta_i^{\sigma_j\sigma})^{-n} \bigwedge_i (\psi^{\sigma_i\sigma})^*(w_G^{\sigma_i\sigma}).$$

Since each differential $(\psi^{\sigma_i\sigma})^*(w^{\sigma_i\sigma})$ has degree n, the reordering $\{\sigma\sigma_1, \ldots, \sigma\sigma_d\}$ of $\mathrm{Gal}(L/K)$ changes the sign of $\bigwedge_i (\psi^{\sigma_i\sigma})^*(w^{\sigma_i\sigma})$ by the sign of the permutation to the power n, i.e., exactly the change in sign from Δ^{-n} to $(\Delta^\sigma)^{-n}$. Therefore, $w_H = w_H^\sigma$ for all $\sigma \in \mathrm{Gal}(L/K)$ so w_H is defined over K. □

Let S be a finite set of places of K and let T be the set of places of L lying above the places in S. Consider a separated and finite-type model G_T for G over $\mathcal{O}_{L,T}$ and let H_S be a separated and finite-type model for H over $\mathcal{O}_{K,S}$. The main difference between the setting of this section and that of the previous one is that, instead of starting with an invariant differential on G_S, we start with an invariant differential on G. By [Har77], Proposition 8.10, if $p : G_S \times_{\mathcal{O}_{K,S}} K \to G_S$ is the projection, then $\Omega^n_{G/L} \cong p^*(\Omega^n_{G_T/\mathcal{O}_{L,T}})$. Since $\Omega^n_{G/L}$ is a rank 1 $\mathcal{O}_G$-module, we can scale the differential w_G by a factor of $\alpha \in L^\times$, such that there

exists an invariant differential w_T on G_T with $\alpha w_G = w_T \times_{\mathcal{O}_{L,T}} K$. Remark that the proof of the fact that the notion of set of convergence factors makes sense (Section 1.7) is still valid, since the invariant differential w_T is defined (from w_G) up to a scalar in $K^\times$. Similarly, there exists $\beta \in K^\times$ such that βw_H comes from an invariant differential on H_S. Then, there exists $\gamma \in \mathbb{Q}$ such that $\gamma/\alpha \in \mathcal{O}_{L,T}$ and $\gamma/\beta \in \mathcal{O}_{K,S}$. In this case both γw_G and γw_H come from invariant differentials w_T and w_S on their respective models.

Lemma 1.44. *With the notation above, for each $v \notin S$ we have*

$$\prod_{\eta|v} \int_{G_{T,\eta}(\mathcal{O}_\eta)} |w_T|_\eta = \int_{H_{S,v}(\mathcal{O}_v)} |w_S|_v.$$

Proof. Note that $K_v \otimes_K L = \oplus_{\eta|v} L_\eta$, which implies that $G(K_v \otimes_K L) = \prod_{\eta|v} G_{S,\eta}(L_\eta)$, which is equal to $H(K_v)$ by the restriction of scalars property. Therefore, to prove the lemma, it is enough to show that

$$\bigwedge_{\eta|v} |w_T|_\eta = |w_S|_v,$$

as Haar measures (or invariant differentials) on $G(K_v \otimes_K L) = H(K_v)$. It is enough to check this locally at a point $g \in H(K_v)$, since Haar measures are invariant.

Recall that $G_{T,\eta}(L_\eta)$ and $H_{S,v}(K_v)$ are topological manifolds whose differential structure is transported from L_η^n and K_v^{nd} (n is the dimension of G and nd is the dimension of H) via the local homeomorphisms that define the two groups as topological manifolds (Lemma 1.34).

Moreover, since both Haar measures are on the same topological group, they differ by a constant; therefore, it is enough to evaluate each invariant differential at a basis of the exterior product of top degree of the tangent space (i.e., of the Lie algebra). The Lie algebra is the same for both differentials, but the difference is that for $|w_S|_v$ we consider the Lie algebra as a K_v-vector space, while for $|w_T|_\eta$ we consider the Lie algebra as an L_η-vector space.

Let ϕ_η be a homeomorphism from a neighborhood of h to a neighborhood of the origin in L_η^n. If $x_1, \ldots, x_n$ are local coordinates on L^n, then a basis for the exterior power of top degree of the tangent space of $G(L_\eta)$ is given by $\phi_\eta^*(\partial/\partial x_1) \wedge \ldots \wedge \phi_\eta^*(\partial/\partial x_n)$. Therefore, by construction of $|w_T|_\eta$, its value at the basis $\phi_\eta^*(\partial/\partial x_1) \wedge \ldots \wedge \phi_\eta^*(\partial/\partial x_n)$ is $|\gamma f(g)|_\eta$, where $w_T = f h^*(dx_1 \wedge \ldots \wedge dx_n)$ locally at g and h is a closed immersion of a small affine neighborhood of g into an affine space, and γ is the scaling factor.

Let φ be a homeomorphism from a neighborhood of g to a neighborhood of the origin in K_v^{nd}. The relationship between φ and $\phi = \oplus_\eta \phi_\eta$ is given by the following commutative diagram:

$$\begin{array}{ccc} G(K_v \otimes_K L) & \xrightarrow{\oplus_\eta \phi_\eta} & \oplus_\eta L_\eta^n = L \otimes K_v^n \\ \Psi \uparrow & & \uparrow i \\ H(K_v) & \xrightarrow{\varphi} & K_v^{nd} \end{array}$$

where i is the isomorphism $K_v^{nd} \cong K_v^n \otimes_K L = \oplus_\eta L_\eta^n$. Therefore,

$$|w_T|_\eta = |\gamma|_\eta |f|_\eta \bigwedge_\sigma (\psi^\sigma)^* \phi^* (dx_1 \wedge \ldots \wedge dx_n),$$

However, a basis for the exterior product of top degree of the cotangent space at g is given (by the commutativity of the above diagram) by $dx_i^{\sigma_j}$, while a basis for the exterior product of top degree for the Lie algebra as a K_v-vector space is not $\bigwedge \partial/\partial x_i^{\sigma_j}$. If $x_i = \sum \theta_j y_{ij}$ then such a K_v-basis is $\bigwedge_{i,j} \partial/\partial y_{ij}$. Thus, the value of $|w_S|_v$ at $\bigwedge_{i,j} \partial/\partial y_{ij}$ is

$$|\gamma^d|_v |\Delta|_v^{-n} \left| \prod_\sigma f(g)^\sigma \right|_v \left(\bigwedge_{i,j} \sum_{l=1}^d \theta_l^{\sigma_j} dy_{il} \right) \left(\bigwedge_{i,j} \frac{\partial}{\partial y_{ij}} \right) = |\gamma^d|_v |\Delta|_v^{-n} | \prod_\sigma f(g)^\sigma |_v |D|_v^n,$$

where D is the determinant

$$D = \begin{vmatrix} \theta_1^{\sigma_1} & \theta_1^{\sigma_2} & \ldots & \theta_1^{\sigma_d} \\ \theta_2^{\sigma_1} & \theta_2^{\sigma_2} & \ldots & \theta_2^{\sigma_d} \\ & \vdots & & \\ \theta_s^{\sigma_1} & \theta_s^{\sigma_2} & \ldots & \theta_d^{\sigma_d} \end{vmatrix} = \Delta.$$

The reason why D comes out of the product as $|D|_v$ is equation 1.5, since D is pulled out of the original invariant differential. Since $\prod_{\eta|v} |f(g)|_\eta = |N_{L/K} f(g)|_v = |\prod_\sigma f(g)^\sigma|_v$ and $\prod_\eta |\gamma|_\eta = |N_{L/K}\gamma|_v = |\gamma^d|_v$, the invariant differentials $\wedge_\eta |w_T|_\eta$ and $|w_S|_v$ are the same. □

Proposition 1.45. *Let G be an algebraic group defined over a Galois extension of number fields L/K and let $\psi : H = R_{L/K}G \to G$ be the L-morphism defining the restriction of scalars group H. Let w_G be an invariant differential on G and let $w_H = \Psi^* w_G$ be its pullback under $\Psi : H \to \prod G^{\sigma_i}$ (note that w_H differs from the one previously defined). Let $\gamma \in \mathbb{Q}$ be as before.*

Let $\Lambda_T = \{\lambda_\eta\}$ be a set of convergence factors for w_T with $\lambda_\eta = 1$ for $\eta \in T$, and let $\Lambda_S = \{\lambda'_v\}$ such that $\lambda'_v = \prod_{\eta|v} \lambda_v$. Then Λ_S is a set of convergence factors for w_S and

$$d\mu_{G,\gamma w_G,\Lambda_T} = d\mu_{H,\gamma w_H,\Lambda_S}$$

as Haar measures on the topological groups $G(\mathbb{A}_L) = H(\mathbb{A}_K)$.

Proof. Let Δ be as in Lemma 1.44. Since $\prod_v |\Delta|_v = 1$ by the product formula, the fact that Λ_S is a set of convergence factors follows from Lemma 1.44 because

$$\prod_{\eta|v} \int_{G_{T,\eta}(\mathcal{O}_{L,T})} |w_T|_\eta = |\Delta^n|_v \int_{H_{S,v}(\mathcal{O}_{K,S})} |w_H|_v$$

To check that the two measures are equal, it is enough to evaluate globally. By Lemma 1.44, the nonnormalized Tamagawa measures differ globally by Δ^n (we have changed the formula for w_H by Δ^n). Therefore, the normalized Tamagawa measures differ by

$$(\mu_L/(\mu_K \Delta))^n.$$

But, using multiplicativity of discriminants, $\mu_L^2 = D_L = D_K D_{L/K} = \mu_K^2 \Delta^2$ (where $D_{L/K} = \Delta^2$ is the discriminant) and the result follows. $\square$

2 Abelian Varieties

2.1 Complete Algebraic Groups

Recall (Definition 1.4) that an abelian variety is a complete algebraic group. The main differences between affine algebraic groups and abelian varieties rise from the fact that the latter are projective and abelian.

Lemma 2.1 (Rigidity)**.** *Let X, Y, Z be varieties defined over a field K such that X is complete and $X \times_K Y$ is geometrically irreducible. Let $f : X \times_K Y \to Z$ be a regular map and let $x \in X(K), y \in Y(K), z \in Z(K)$ such that $f(X \times \{y\}) = f(\{x\} \times Y) = z$. Then $f(X \times Y) = z$.*

Proof. The main idea is that the image via a regular map of a complete and connected variety in an affine variety is a point. For a complete proof see [Mum70] II.4. □

We can use this to prove that every abelian variety is abelian as an algebraic group.

Corollary 2.2. *Let A be an abelian variety. Then $m(x, y) = m(y, x)$ for every $x, y \in A$.*

Proof. Consider the commutator map $[x, y] = m(m(x, y), m(i(x), i(y))) : A \times_K A \to A$. Then on $A \times e$ and $e \times A$ we have $[x, y] = e$. By Lemma 2.1 we get $[x, y] = e$ for all $x, y \in A$. Therefore $m(x, y) = m(y, x)$ and A is abelian as a group. □

Remark 2.3. For every K-scheme S, Corollary 2.2 shows that $A(S)$ is an abelian group. From now on we will write $m(x, y) = x + y$ for every $x, y \in A(S)$ and 0 for the identity section $S \to A$. For each integer n write $[n] : A \to A$ to be $[n](x) = x + x + \cdots + x$ where the sum has n terms, if $n \geq 0$ and $[n](x) = -[-n](x)$ if $n < 0$. The morphism $[n]$ is an isogeny if n is not divisible by the characteristic of K (see [Mum70] II.6).

Example 2.4. Let E be an abelian curve, i.e., a one-dimensional abelian variety, defined over a field K of characteristic 0. Let $\mathrm{Div}(E)$ be the group of Weil divisors on E, i.e., the free abelian group generated by the symbols (P) for P points of E. For a rational function $f : E \to \overline{K}$ let $\mathrm{div} f = \sum_{P \in E} (\mathrm{ord}_P f)(P)$, where $\mathrm{ord}_P f$ represents the order of vanishing of f at P (positive if P is a zero of f and negative if P is a pole of f). For a divisor $D = \sum n_P(P) \in \mathrm{Div}(E)$ let $\deg D = \sum n_P$ and let $\ell(D)$ be the dimension as a $\overline{K}$-vector space of $\{f \,|\, \mathrm{ord}_P f \geq -n_P, \forall P \in E\} \cup \{0\}$. (Note that $\deg D$ is well-defined since $\sum n_P P$ is a finite sum.)

Since there exists a non-vanishing invariant differential w on E (unique up to scalars in $K^\times$), the canonical divisor $\mathrm{div} w$ is trivial. Therefore, the Riemann-Roch theorem ([Sil92], Theorem II.5.4) states that

$$\ell(D) - \ell(-D) = \deg D - g + 1,$$

where g is the genus of the curve E. But then for $D = 0$ we get $g = 1$. Therefore E is a smooth algebraic curve of genus 1. Such a curve is called an *elliptic curve*. Elliptic curves have a simple description, as follows from the following proposition.

Proposition 2.5. *Every elliptic curve E defined over a field K has an embedding $\psi : E \hookrightarrow \mathbb{P}^2_K$ of the form $\psi = (x, y, 1)$ (such that $\psi(O) = (0, 1, 0)$), where x and y are rational functions on E such that there exist $a_1, a_2, a_3, a_4, a_6 \in K$ with*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Proof. Since the genus of E is 1, the Riemann-Roch theorem states that for the divisor $D_n = n(O)$ we have $\ell(D_n) - \ell(-D_n) = n$. But $\ell(-D_n) = 0$ by [Sil92] Proposition II.5.2.a so $\ell(D_n) = n$. Therefore there exists a basis $1, x$ for $\mathcal{L}(D_2)$ which can be extended to a basis $1, x, y$ of $\mathcal{L}(D_3)$ ([Sil92], Proposition II.5.8). Then the dimension of $\mathcal{L}(D_6)$ is 6, but it contains the functions $1, x, x^2, x^3, y, xy$ and y^2. The proposition follows from the fact that these must be linearly dependent. □

2.2 Abelian Varieties over Number Fields

2.2.1 Invertible Sheaves on Abelian Varieties

For a K-scheme S and for a scheme $X \in \mathbf{Sch}_S$ let $\mathrm{Pic}_S(X)$ be the group of isomorphism classes of invertible sheaves on X. Let $m : X \times_S X \to X$ be multiplication and let $\pi_i : X \times_S X \to X$ is projection to the i-th factor. Define $\mathrm{Pic}^0_S(X) \subset \mathrm{Pic}_S(X)$ to be the set of isomorphism classes of invertible sheaves $\mathcal{L}$ such that $m^*\mathcal{L} \otimes \pi_1^*\mathcal{L}^{-1} \otimes \pi_2^*\mathcal{L}^{-1}$ is trivial.

Theorem 2.6 (Theorem of the Cube)**.** *Let A, B and C be complete varieties defined over a field K and let $a \in A(K), b \in B(K), c \in C(K)$ be points. Let $\mathcal{L} \in \mathrm{Pic}_K(A \times_K B \times_K C)$. Then $\mathcal{L}$ is trivial if and only if $\mathcal{L}|_{A\times_K B\times_K\{c\}}, \mathcal{L}|_{A\times_K\{b\}\times_K C}$ and $\mathcal{L}|_{\{a\}\times_K B\times_K C}$ are trivial.*

Proof. See [Mum70] Theorem III.1. □

We can specialize Theorem 2.6 to the case when $A = B = C$ is an abelian variety defined over a number field K.

Corollary 2.7. *Let A be an abelian variety and let $\pi_i : A \times_K A \times_K A \to A$ be the projection to the i-th factor. Write $\pi_{ij} = \pi_i + \pi_j$ and $\pi_{123} = \pi_1 + \pi_2 + \pi_3$. Then*

$$\pi_{123}^*\mathcal{L} \otimes \pi_{12}^*\mathcal{L}^{-1} \otimes \pi_{23}^*\mathcal{L}^{-1} \otimes \pi_{13}^*\mathcal{L}^{-1} \otimes \pi_1^*\mathcal{L} \otimes \pi_2^*\mathcal{L} \otimes \pi_3^*\mathcal{L}$$

is trivial.

Proof. Note that $\pi_{123}^*\mathcal{L}|_{A\times_K A\times_K\{0\}} = \pi_{12}^*\mathcal{L}|_{A\times_K A\times_K\{0\}}$, $\pi_{13}^*\mathcal{L}|_{A\times_K A\times_K\{0\}} = \pi_1^*\mathcal{L}|_{A\times_K A\times_K\{0\}}$ and $\pi_{23}^*\mathcal{L}|_{A\times_K A\times_K\{0\}} = \pi_2^*\mathcal{L}|_{A\times_K A\times_K\{0\}}$ while $\pi_3^*\mathcal{L}|_{A\times_K A\times_K\{0\}}$ is trivial. Therefore

$$\pi_{123}^*\mathcal{L} \otimes \pi_{12}^*\mathcal{L}^{-1} \otimes \pi_{23}^*\mathcal{L}^{-1} \otimes \pi_{13}^*\mathcal{L}^{-1} \otimes \pi_1^*\mathcal{L} \otimes \pi_2^*\mathcal{L} \otimes \pi_3^*\mathcal{L}|_{A\times_K A\times_K\{0\}}$$

is trivial and similarly for $A \times_K \{0\} \times_K A$ and $\{0\} \times_K A \times_K A$. The result follows from Theorem 2.6. □

Let A be an abelian variety defined over a field K and let S be a scheme over K. For every $x \in A(S) = \mathrm{Hom}_{\mathbf{Sch}}(S, A)$ we get a map $t_x = m(\mathrm{id}_A \times x) : A \times_K S \to A \times_K S$.

Corollary 2.8. *Let $a, b \in A(K)$ which induce t_a, t_b morphisms on $A \times_K K = A$. If $\mathcal{L} \in \mathrm{Pic}_K(A)$ then $t_{a+b}^*\mathcal{L} \otimes \mathcal{L} = t_a^*\mathcal{L} \otimes t_b^*\mathcal{L}$.*

Proof. Consider the map $f : A \to A \times A \times A$ given by $f(x) = (x, a, b)$ where a and b represent their respective constant images of $\mathrm{Spec}\, K$ (affine) into A (complete). By Corollary 2.7 we have $f^*(\pi_{123}^*\mathcal{L} \otimes \pi_{12}^*\mathcal{L}^{-1} \otimes \pi_{23}^*\mathcal{L}^{-1} \otimes \pi_{13}^*\mathcal{L}^{-1} \otimes \pi_1^*\mathcal{L} \otimes \pi_2^*\mathcal{L} \otimes \pi_3^*\mathcal{L}) = t_{a+b}^*\mathcal{L} \otimes t_a^*\mathcal{L}^{-1} \otimes \mathcal{O}_A \otimes t_b^*\mathcal{L}^{-1} \otimes \mathcal{L} \otimes \mathcal{O}_A \otimes \mathcal{O}_A = t_{a+b}^*\mathcal{L} \otimes t_a^*\mathcal{L}^{-1} \otimes t_b^*\mathcal{L}^{-1} \otimes \mathcal{L}$ is trivial. □

In Proposition 2.5 we saw that elliptic curves are projective. The same is true for abelian varieties as will follow from the existence of an ample invertible sheaf on A (which implies the existence of a very ample invertible sheaf).

Proposition 2.9. *Let A be an abelian variety defined over a field K. Then there exists an ample invertible sheaf $\mathcal{L} \in \mathrm{Pic}_K(A)$. (Therefore, A is projective.)*

Proof. See [Mil86a], Theorem 7.1. □

Example 2.10. Let E be an elliptic curve defined over K. By [HS00] Corollary A.4.2.4 the sheaf $\mathcal{L}(D)$ for $D = (O) \in \mathrm{Div}(E)$ (where O is the identity on E) is ample since $\deg D = 1 > 0$.

Let K be a field of characteristic 0, let S be a K-scheme and let A be an abelian variety defined over K. The existence of an ample invertible sheaf $\mathcal{L}_S$ on $A \times_K S$ allows the construction of an isogeny between $A \times_K S$ and $\mathrm{Pic}_S^0(A \times_K S)$.

Proposition 2.11. *The map $\varphi_{\mathcal{L}_S} : A(S) \to \mathrm{Pic}_S(A \times_K S)$ given by $\varphi_{\mathcal{L}}(x) = t_x^*\mathcal{L}^{-1} \otimes \mathcal{L}$ is a homomorphism whose image lies in $\mathrm{Pic}_S^0(A \times_K S)$. If $S = \mathrm{Spec}\, \overline{K}$ and $\mathcal{L} = \mathcal{L}_S$ then $\varphi_{\mathcal{L}}$ is surjective and has finite kernel.*

Proof. By Corollary 2.8 for every $x, y \in A(S)$ we have $\varphi_{\mathcal{L}_S}(x)\varphi_{\mathcal{L}_S}(y) = t_x^*\mathcal{L}_S \otimes \mathcal{L}_S^{-1} \otimes t_y^*\mathcal{L}_S \times \mathcal{L}_S^{-1} \cong t_{x+y}^*\mathcal{L}_S \otimes \mathcal{L}_S^{-1} = \varphi_{\mathcal{L}_S}(x + y)$ so $\varphi_{\mathcal{L}_S}$ is a homomorphism. When $S = \mathrm{Spec}\, \overline{K}$ note that $\mathcal{L}$ is ample, so the fact that $\varphi_{\mathcal{L}}$ is surjective and with finite kernel follows from [Mum70] Theorem II.8.1. □

Remark 2.12. It is essential that $\mathcal{L}$ be ample. A simple counterexample is provided by Corollary 2.8. Let $\mathcal{L}'$ be any invertible sheaf and let $0 \neq x \in A(S)$. Let $\mathcal{L} = t_x^*\mathcal{L}' \otimes \mathcal{L}'^{-1}$. Then for every $y \in A(S)$ we have $t_y^*\mathcal{L} \otimes \mathcal{L}^{-1} = t_y^*t_x^*\mathcal{L}' \otimes t_y^*\mathcal{L}'^{-1} \otimes t_x^*\mathcal{L}'^{-1} \otimes \mathcal{L}'$ which is trivial by Corollary 2.8. Therefore the image of $\varphi_{\mathcal{L}}$ is constant, hence not surjective. In fact, $\mathcal{L} \in \mathrm{Pic}_K^0(A)$ if and only if $\varphi_{\mathcal{L}}$ is trivial ([Mum70], II.8).

Example 2.13. Let E be an elliptic curve. In Example 2.10 we saw that $\mathcal{L} = \mathcal{L}((O))$ is an ample invertible sheaf on E. Therefore $\varphi_{\mathcal{L}} : E(\overline{K}) \to \mathrm{Pic}_K^0(E)$ given by $\varphi_{\mathcal{L}}(x) = t_x^*\mathcal{L}((O)) \otimes \mathcal{L}((O))^{-1} \cong \mathcal{L}((x)) \otimes \mathcal{L}((O))^{-1} \cong \mathcal{L}((x) - (O))$ is a surjection with finite kernel. If $x \in \ker \varphi_{\mathcal{L}}$ then $(x) - (O) = 0$ in $\mathrm{Pic}^0(E)$, where $\mathrm{Pic}^0(E)$ is now identified with classes of $\mathrm{Div}^0(E)$ modulo elements of the form $\mathrm{div} f$ for rational functions f on E. Therefore $\mathrm{div} f = (x) - (O)$

for some rational function f. Since $\ell((O)) = 1$ by the Riemann-Roch theorem and since $\mathcal{L}((O))$ contains constant functions (since they are holomorphic at infinity), it must be that $f \in \mathcal{L}((O))$ is a constant function or $\ell((O)) > 1$. Therefore $(x) - (O) = \mathrm{div} f = 0$ so $(x) = (O)$ and $\varphi_{\mathcal{L}}$ is bijective. Therefore, we get an isomorphism $E \cong \mathrm{Pic}^0(E)$.

For every abelian variety A defined over a field K of characteristic 0 we have constructed a surjection with finite kernel between $A(S)$ and $\mathrm{Pic}^0_S(A \times_K S)$. This map transports the structure of abelian variety to $\mathrm{Pic}^0_K(A)$.

Theorem 2.14. *The functor $S \mapsto \mathrm{Pic}^0_S(A \times_K S)$ for each $S \in \mathbf{Sch}_{\overline{K}}$ is representable by an abelian variety $A^\vee$ defined over K.*

Proof. See [Mum70] II.8. This proof uses the fact that K has characteristic 0. □

Since $\mathrm{Pic}^0_K(A \times_K \overline{K}) = A^\vee(\overline{K})$ we can rephrase Proposition 2.11 to state that for every ample invertible sheaf $\mathcal{L}$ there is an isogeny $\varphi_{\mathcal{L}}$ from A to $A^\vee$. Such an isogeny is called a *polarization*. The variety $A^\vee$ is called the dual abelian variety. There exists a (unique) invertible sheaf $\mathcal{P}$ (the *Poincaré sheaf*) on $A \times A^\vee$ such that $\mathcal{P}|_{A\times\{a\}}$ is the image of a under the isomorphism $\mathrm{Pic}^0_K(A \times_K \overline{K}) = A^\vee(\overline{K})$ and such that $\mathcal{P}_{\{a\}\times A^\vee}$ is trivial ([Mum70], II.8).

2.2.2 Heights on Projective Spaces

Let $K/\mathbb{Q}$ be a number field. Recall that M_K and M_K^∞ represent the set of places and the set of infinite places of K, respectively. As before, let $K_v, \mathcal{O}_v, \wp_v, k_v$ and q_v be the completion of K at the finite place v, the ring of integers of K_v, the maximal ideal of $\mathcal{O}_v$, the residue field at v and the size of the residue field, respectively. Let $|x|_v = q_v^{-v(x)}$ be the normalized absolute value. For an abelian variety A defined over K the set $A(K)$ is a group. To understand its group structure it is useful to have an ordering of the points in $A(K)$ using a notion of 'height'. To achieve this we will use the fact that A is projective to use the notion of height on projective spaces.

Lemma 2.15. *Define $H_{K,n} : \mathbb{P}^n K \to [0, \infty)$ defined by*

$$H_{K,n}([x_0 : \ldots : x_n]) = \left(\prod_{v \in M_K} \max_i (|x_i|_v) \right)^{1/[K:\mathbb{Q}]}$$

Then there exists $H_n : \mathbb{P}^n \overline{K} \to [0, \infty)$ such that for each number field K we have $H_n|_K = H_{K,n}$.

Proof. Since $[x_0 : \ldots : x_n] \in \mathbb{P}^n(K)$ is defined up to multiplication by $\lambda \in K$, the function $H_{K,n}$ is well-defined up to multiplication by $\prod_v |\lambda|_v = 1$, so the height is well-defined. If L/K is a finite extension, then for each place $v \in M_K$ and $x \in K$ we have $|N_{L/K} x|_v = \prod_{w|v} |x|_w$.

Therefore if $[x_0 : \ldots : x_n] \in \mathbb{P}^n(K) \subset \mathbb{P}^n(L)$ then

$$\begin{aligned} H_{L,n}([x_0 : \ldots : x_n]) &= \left(\prod_{w \in M_L} \max_i (|x_i|_w) \right)^{1/[L:\mathbb{Q}]} \geq \left(\prod_{v \in M_K} \max_i \left(\prod_{w|v} |x_i|_w \right) \right)^{1/[L:\mathbb{Q}]} \\ &= \left(\prod_{v \in M_K} \max_i (|N_{L/K} x_i|_v) \right)^{1/[L:\mathbb{Q}]} = \left(\prod_{v \in M_K} \max_i (|x_i|_v^{[L:K]}) \right)^{1/[L:\mathbb{Q}]} \\ &= H_{K,n}([x_0 : \ldots : x_n]) \end{aligned}$$

Therefore $H_n = \varinjlim_K H_{K,n}$ satisfies the desired properties. □

For each $x = [x_0 : \ldots : x_n] \in K/\mathbb{Q}$ let $h_n(x) = \log H_n(x)$, which makes sense because $H_n(x) > 0$ since not all entries of $x = [x_0 : \ldots : x_n]$ are 0.

Example 2.16. Consider $x = [1/3, 2 + \sqrt{3}] \in \mathbb{P}^1\overline{\mathbb{Q}}$. Since $2 + \sqrt{3}$ is integral and $(2 + \sqrt{3})(2 - \sqrt{3}) = 1$, it must be a unit. At each place $v \nmid 3$ the valuation $v(1/3) = 0$, while if $v \mid 3$ is a place of $\mathbb{Q}(\sqrt{3})$ then $v(1/3) = -1$. But $\mathbb{Q}(\sqrt{3})$ is totally ramified over $\mathbb{Q}$ at 3 so $|1/3|_v = 9$. Therefore $H_1(x) = 9^{1/2} = 3$.

Remark 2.17. If $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ then $h_n(\sigma(x)) = h_n(x)$.

Lemma 2.18. *If $u, v > 0$ then the set $\{x \in \mathbb{P}^n\overline{\mathbb{Q}} | h_n(x) \leq u, [\mathbb{Q}(x) : \mathbb{Q}] \leq v\}$ is finite.*

Proof. See [HS00] Theorem B.2.3. □

Lemma 2.19 (Kronecker)**.** *Let $K/\mathbb{Q}$ be a number field. Then $h_n(x) = 0$ for $x = [x_0 : \ldots : x_n] \in K$ if and only if x_i/x_j is a root of unity when $x_j \neq 0$.*

Proof. Note that $h_n([x_0^m : \ldots : x_n^m]) = m h_n([x_0 : \ldots : x_n]) = 0$. Since $x_0^m, \ldots, x_n^m$ lie in the finite extension $K(x_0, \ldots, x_n)$, the previous lemma implies that the set $\{[x_0^m : \ldots : x_n^m] | m \geq 1\}$ is finite. Let $r \neq s$ be two exponents such that $[x_0^r : \ldots : x_n^r] = [x_0^s : \ldots : x_n^s]$. If $x_j \neq 0$ then $(x_i/x_j)^{r-s} = 1$ so they are roots of unity. The converse is obvious. □

In order to transport the notion of height from the projective space to an abelian variety we need to prove certain functorial properties of H_n. In particular, it is functorial with taking products and morphisms (up to bounded functions).

Lemma 2.20. *Let $\sigma_{m,n} : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^{mn+m+n}$ be the Segre embedding (taking $([x_i], [y_j])$ to $[x_i y_j]$). Then $h_{mn+m+n}(\sigma_{m,n}(x, y)) = h_m(x) + h_n(y)$.*

Proof. See [HS00] Theorem B.2.4. □

Proposition 2.21. *Let $\psi : \mathbb{P}^n \to \mathbb{P}^m$ be a regular map of degree d. Then $h_m(\psi(x)) = d h_n(x) + O(1)$, where $O(1)$ represents a bounded function.*

Proof. See [HS00] Theorem B.2.5. □

2.2.3 Heights on Abelian Varieties

Let A be an abelian (projective) variety defined over a number field K.

Definition 2.22. For each embedding $\psi : A \to \mathbb{P}^m$ define $h_\psi : A(\overline{K}) \to [0, \infty)$ by $h_\psi(P) = h(\psi(P))$.

Proposition 2.23. *Let $\phi : A \to \mathbb{P}^m$ and $\psi : A \to \mathbb{P}^n$ such that $\phi^*\mathcal{O}_{\mathbb{P}^m}(1)$ and $\psi^*\mathcal{O}_{\mathbb{P}^n}(1)$ (where $\mathcal{O}_{\mathbb{P}^n}(1)$ is the canonical sheaf of $\mathbb{P}^n$) are equal in* $\mathrm{Pic}(A)$. *Then $h_\phi(P) = h_\psi(P) + O(1)$ for all $P \in A(\overline{K})$.*

Proof. See [HS00], Theorem B.3.1. □

This proposition suggests that the height function on A is well defined up to a bounded error term. Consider $\mathcal{H}_A = \mathrm{Hom}(A(\overline{K}), \mathbb{R}) / \mathrm{Hom}_{\mathrm{bounded}}(A(\overline{K}), \mathbb{R})$ to eliminate this ambiguity.

Theorem 2.24 (Height machine)**.** *There exists a unique homomorphism $h_A : \mathrm{Pic}(A) \to \mathcal{H}_A$ such that for every very ample $\mathcal{L}$ on A we have $h_A(\mathcal{L}) = h \circ \phi$ in $\mathcal{H}_A$, where $\phi : A \to \mathbb{P}^m$ is an embedding such that $\mathcal{L} \cong \phi^*\mathcal{O}_{\mathbb{P}^m}(1)$. Moreover, h_A is functorial in A in the sense that if $\psi : A \to B$ is a morphism of abelian varieties over K and $\mathcal{L} \in \mathrm{Pic}(B)$ then $h_A(\psi^*\mathcal{L}) = h_B(\mathcal{L}) \circ \psi$ in $\mathcal{H}_A$.*

Proof. Every $\mathcal{L} \in \mathrm{Pic}(A)$ can be written as $\mathcal{L} = \mathcal{L}_1 \otimes \mathcal{L}_2^{-1}$ for very ample invertible sheaves $\mathcal{L}_1, \mathcal{L}_2$ on A ([HS00], Theorem A.3.2.3). Define $h_A(\mathcal{L}) = h_A(\mathcal{L}_1) - h_A(\mathcal{L}_2)$ for a choice of $\mathcal{L}_1$ and $\mathcal{L}_2$. For any other choice $\mathcal{L} = \mathcal{L}_1' \otimes \mathcal{L}_2'^{-1}$ we have $\mathcal{L}_1 \otimes \mathcal{L}_2' = \mathcal{L}_1' \otimes \mathcal{L}_2$ on A. Let $\phi_i : A \to \mathbb{P}^{m_i}$ and $\phi_i' : A \to \mathbb{P}^{n_i}$ be projective embeddings such that $\mathcal{L}_i = \phi_i^*\mathcal{O}_{\mathbb{P}^{m_i}}(1)$ and $\mathcal{L}_i' = \phi_i'^*\mathcal{O}_{\mathbb{P}^{n_i}}(1)$ for $i = 1, 2$. Then $\mathcal{L}_1 \otimes \mathcal{L}_2' = (\phi_1 \times \phi_2')^*\mathcal{O}_{\mathbb{P}^{m_1} \times \mathbb{P}^{n_2}}$ and $\mathcal{L}_1' \otimes \mathcal{L}_2 = (\phi_1' \times \phi_2)^*\mathcal{O}_{\mathbb{P}^{n_1} \times \mathbb{P}^{m_2}}$. Let $N > \max(m_1 n_2 + m_1 + n_2, n_1 m_2 + n_1 + m_2)$ and let $\sigma : \mathbb{P}^{m_1} \times \mathbb{P}^{n_2} \to \mathbb{P}^N$ and $\sigma' : \mathbb{P}^{n_1} \times \mathbb{P}^{m_2} \to \mathbb{P}^N$ be the Segre embeddings followed by inclusions. By Lemmas 2.20 and 2.21 we get that $h \circ \sigma \circ \phi_1 \times \phi_2' = h \circ \phi_1 + h \circ \phi_2' = h \circ \phi_1' + h \circ \phi_2 = h \circ \sigma \circ \phi_1' \times \phi_2$ in $\mathcal{H}_A$ and so $h_A(\mathcal{L}_1) - h_A(L_2) = h_A(\mathcal{L}_1') - h_A(L_2')$ which means that h_A is a well-defined homomorphism.

For the functoriality property see [HS00], Theorem B.3.2. □

The height machine of an abelian variety is well defined in $\mathcal{H}_A$, i.e., up to a bounded function. A clever trick to remove this dependence on bounded errors is due to Tate. To do this we will have to analyze the properties of the sheaves $\mathcal{L}$. A sheaf $\mathcal{L}$ is called *symmetric* if $[-1]^*\mathcal{L} = \mathcal{L}$ and *antisymmetric* if $[-1]^*\mathcal{L} = \mathcal{L}^{-1}$. Let $\mathcal{L}$ be an ample invertible sheaf on A.

Let $f : A \times_K A \times_K A \to A$ defined by $f = ([n], [1], [-1])$ for an integer n. By Corollary 2.7 we have that $f^*(\pi_{123}^*\mathcal{L} \otimes \pi_{12}^*\mathcal{L}^{-1} \otimes \pi_{23}^*\mathcal{L}^{-1} \otimes \pi_{13}^*\mathcal{L}^{-1} \otimes \pi_1^*\mathcal{L} \otimes \pi_2^*\mathcal{L} \otimes \pi_3^*\mathcal{L}) = [n+1]^*\mathcal{L} \otimes [n-1]^*\mathcal{L} \otimes [n]^*\mathcal{L}^{\otimes 2} \otimes \mathcal{L}^{-1} \otimes [-1]^*\mathcal{L}^{-1}$ is trivial. Therefore, by induction we get that $[n]^*\mathcal{L} = \mathcal{L}^{\otimes n^2}$ if $\mathcal{L}$ is symmetric and $[n]^*\mathcal{L} = \mathcal{L}^{\otimes n}$ if $\mathcal{L}$ is antisymmetric. By Theorem 2.24 we get that $h_A(\mathcal{L}) \circ [n] = h_A([n]^*\mathcal{L}) = h_A(\mathcal{L}^{\otimes n^2}) = n^2 h_A(\mathcal{L})$ in $\mathcal{H}_A$ if $\mathcal{L}$ is symmetric and $h_A(\mathcal{L}) \circ [n] = n h_A(\mathcal{L})$ if $\mathcal{L}$ is antisymmetric. Every invertible sheaf $\mathcal{L}$ can be written as $\mathcal{L} \otimes \mathcal{L} = (\mathcal{L} \otimes [-1]^*\mathcal{L}) \otimes (\mathcal{L} \otimes [-1]^*\mathcal{L}^{-1})$ where $\mathcal{L} \otimes [-1]^*\mathcal{L}$ is symmetric and $\mathcal{L} \otimes [-1]^*\mathcal{L}^{-1}$ is antisymmetric as follows. Therefore, the previous analysis of $h_A(\mathcal{L}) \circ [n]$ can be extended to all invertible sheaves $\mathcal{L}$.

Definition 2.25. The Néron-Tate height is

$$\hat{h}_A(\mathcal{L})(P) = \lim_{n\to\infty} \frac{h_A(\mathcal{L})([2^n]P)}{4^n},$$

if $\mathcal{L}$ is symmetric and

$$\hat{h}_A(\mathcal{L})(P) = \lim_{n\to\infty} \frac{h_A(\mathcal{L})([2^n]P)}{2^n},$$

if $\mathcal{L}$ is antisymmetric.

Theorem 2.26. *The map $\hat{h}_A(\mathcal{L}) : A(\overline{K}) \to \mathbb{R}$ has the property that $\hat{h}_A(\mathcal{L})(P) = h_A(\mathcal{L})(P)$ as functions in $\mathcal{H}_A$. If $\mathcal{L}$ is symmetric then $\hat{h}_A(\mathcal{L})$ is a quadratic function with associated bilinear form $\langle P, Q\rangle_{\mathcal{L}} = (\hat{h}_A(\mathcal{L})(P+Q) - \hat{h}_A(\mathcal{L})(P) - \hat{h}_A(\mathcal{L})(Q))/2$ and if $\mathcal{L}$ is antisymmetric then $\hat{h}_A(\mathcal{L})$ is linear.*

Proof. See [HS00], Theorem B.4.1. □

Proposition 2.27. *Let $\mathcal{L}$ be an ample symmetric invertible sheaf on A. Then $\hat{h}_A(\mathcal{L})(P) \geq 0$ with equality if and only if P is torsion.*

Proof. The proof of this proposition is similar to the proof of Lemma 2.19. See [HS00], Proposition B.5.3. □

In particular, the Poincaré sheaf $\mathcal{P}$ on $A \times_K A^\vee$ is symmetric since $[-1]^*\mathcal{P}$ satisfies the same properties as $\mathcal{P}$ and so must equal $\mathcal{P}$ by uniqueness. Therefore we may define a pairing $\langle , \rangle : A(\overline{K}) \times A^\vee(\overline{K}) \to \mathbb{R}$ by $\langle a, b\rangle = \langle a, \mathcal{B}\rangle_{\mathcal{P}}$ where $\mathcal{B}$ is the image of b under the isomorphism $A^\vee(\overline{K}) \cong \mathrm{Pic}^0_K(A)$. By Proposition 2.27 the kernel of the pairing is the torsion subgroup on each side so we get a nondegenerate pairing

$$\langle , \rangle : A(\overline{K})/A(\overline{K})_{\mathrm{tors}} \times A^\vee(\overline{K})/A^\vee(\overline{K})_{\mathrm{tors}} \to \mathbb{R}.$$

For every isogeny $\psi : A \to B$, there exists a unique dual isogeny $\psi^\vee : B^\vee \to A^\vee$, such that $\psi \circ \psi^\vee$ and $\psi^\vee \circ \psi$ are multiplication by an integer morphisms (see [Sil92] III.6).

Lemma 2.28. *Let $\psi : A \to B$ be an isogeny of abelian varieties defined over a number field K, and let $\psi^\vee : B^\vee \to A^\vee$ be the dual isogeny. If $\langle , \rangle_A$ and $\langle , \rangle_B$ are the Néron-Tate pairings for A and B then, for each $a \in A(K)$ and $b \in B^\vee(K)$, we have*

$$\langle a, \psi^\vee(b)\rangle_A = \langle \psi(a), b\rangle_B.$$

Proof. See [Mil86b] I.7.3. □

2.2.4 Rational Points on Abelian Varieties

For an abelian variety A defined over a number field K the group structure of $A(K)$ is determined by the Mordell-Weil theorem.

Theorem 2.29 (Mordell-Weil)**.** *If A is an abelian variety defined over a number field K then the group $A(K)$ of rational points on A is finitely generated.*

Proof. See [HS00], Theorem C.0.1. We will not prove the theorem here, but mention that it uses the Dirichlet Unit Theorem, which means that it will apply in general only to global fields (i.e., number fields and function fields). □

A corollary of this theorem is that $A(K) \cong A(K)_{\text{tors}} \oplus \mathbb{Z}a_1 \oplus \cdots \oplus \mathbb{Z}a_r$ as abelian groups where r is the *rank* of A and $a_1, \ldots, a_r \in A(K)$. An isogeny $A \to A^\vee$ induces a map $A(K) \to A^\vee(K)$, which is an isomorphism on $A(K)\otimes\mathbb{Q} \to A^\vee(K)\otimes\mathbb{Q}$ since the kernel of the isogeny is a subgroup of $A(K)_{\text{tors}}$. Therefore the rank of $A^\vee$ is r and $A^\vee(K) \cong A^\vee(K)_{\text{tors}} \oplus \mathbb{Z}b_1 \oplus \cdots \oplus \mathbb{Z}b_r$ for $b_1, \ldots, b_r \in A^\vee(K)$.

Definition 2.30. The regulator R_A of the abelian variety A is

$$R_A = \left|\det(\langle a_i, b_j\rangle)_{i,j=1,\ldots,r}\right|.$$

This definition makes sense since the a_i and b_j are defined up to torsion and the pairing $\langle , \rangle$ vanishes on torsion. Moreover, any permutation of the generators a_i and b_j changes the value of the determinant by ± 1 which does not influence the value of R_A.

Definition 2.31. Let ℓ be a prime number. The Tate module of A at ℓ is $T_\ell A = \varprojlim A[\ell^m] = \text{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A)$. Write $V_\ell A = T_\ell A \otimes \mathbb{Q}$.

Remark 2.32. The Tate module $T_\ell A$ and $V_\ell A$ have natural structures of $\text{Gal}(\overline{K}/K)$-modules given by the Galois action on $A[\ell^m]$ for each m. To the abelian variety A we can associate the $\text{Gal}(\overline{K}/K)$-module $A(\overline{K})$, but this is a group whose structure is unknown. The advantage of constructing the Tate module $V_\ell A$ is that it is a $\mathbb{Q}_\ell$-vector space of dimension $2d$, where $d = \dim A$ ([Mum70] II.6) and so it is a representatation of $\text{Gal}(\overline{K}/K)$.

The Tate module has certain functorial properties, illustrated by the following lemma.

Lemma 2.33. *If the sequence of algebraic groups over K*

$$1 \to M \to N \to P \to 1,$$

is exact and multiplication by ℓ is an bijection in M, then there exists an exact sequence of $\text{Gal}(\overline{K}/K)$-modules

$$1 \to T_\ell M \to T_\ell N \to T_\ell P \to 1.$$

Moreover, if M is a unipotent group then $T_\ell N \cong T_\ell P$.

Proof. There is an exact sequence $1 \to M(\overline{K}) \to N(\overline{K}) \to P(\overline{K}) \to 1$ and $T_\ell X = \varprojlim \mathrm{Hom}(\mathbb{Z}/\ell^n\mathbb{Z}, X(\overline{K}))$ for a scheme $X \in \mathbf{Sch}_K$. Therefore we get an exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$1 \to T_\ell M \to T_\ell N \to T_\ell P \to \varprojlim \mathrm{Ext}_{\mathbb{Z}}(\mathbb{Z}/\ell^n\mathbb{Z}, M(\overline{K})).$$

But $\mathrm{Ext}_{\mathbb{Z}}(\mathbb{Z}/\ell^n\mathbb{Z}, M(\overline{K})) \cong M/\ell^n M$ so if multiplication by ℓ is a bijection in M then $\mathrm{Ext}_{\mathbb{Z}}(\mathbb{Z}/\ell^n\mathbb{Z}, M(\overline{K})) = 0$ and we get the exact sequence $1 \to T_\ell M \to T_\ell N \to T_\ell P \to 1$. (For a discussion of Ext, see Section 4.1.)

If M is a unipotent group then there exists a $\overline{K}$ composition series $M = M_0 \supset M_1 \supset \cdots \supset M_n \supset 0$ such that $M_i/M_{i+1} \cong \mathbb{G}_a$. Therefore, multiplication by ℓ is injective, so the torsion $M[\ell^n]$ is trivial so $T_\ell M = 0$ and $T_\ell N \cong T_\ell P$. □

Remark 2.34. Let L/K be an extension of number fields and let A be an abelian variety over L. Then $T_\ell R_{L/K} A \cong \mathrm{Ind}_{\mathrm{Gal}(\overline{L}/L)}^{\mathrm{Gal}(\overline{K}/K)} V_\ell A$ as $\mathrm{Gal}(\overline{K}/K)$-modules since the Tate module takes into account $\overline{K}$ points and $R_{L/K}A(\overline{K}) \cong \prod A^{\sigma_i}(\overline{K})$.

It is essential for the proof of the fact that Conjecture 3.15 is invariant under isogenies, to be able to relate the Tate modules of A and $A^\vee$. The solution is the *Weil pairing*.

Proposition 2.35. *There exists a functorial, nondegenerate,* $\mathrm{Gal}(\overline{K}/K)$*-equivariant bilinear pairing called the Weil pairing*

$$e_\ell : V_\ell A \times V_\ell A^\vee \to \mathbb{Q}_\ell(1) = \varprojlim \mu_{\ell^m},$$

with respect to which there exists an identification

$$A^\vee[\phi^\vee] \cong (A[\phi])^* = \mathrm{Hom}(A[\phi], \mu_\infty),$$

for every isogeny $\phi : A \to B$.

Proof. See [Mil86a] Lemma 16.2. □

2.2.5 The Shafarevich-Tate and Selmer Groups

Computation of the Mordell-Weil group $A(K)$ for a global field K is difficult because the proof of the weak Mordell-Weil theorem is not constructive. One method of analyzing rational points is via the local-to-global principle, i.e., analyzing the points of $A(K_v)$ for each completion K_v of K to obtain information about $A(K)$.

For every isogeny $\phi : A \to A$ the $\mathrm{Gal}(\overline{K}/K)$-cohomology long exact sequence associated with $0 \to A[\phi] \to A \xrightarrow{\phi} A \to 0$ (where $A[\phi] = \ker \phi$) gives

$$0 \to A(K)[\phi] \to A(K) \xrightarrow{\phi} A(K) \to H^1(K, A[\phi]) \to H^1(K, A) \xrightarrow{\phi} H^1(K, A),$$

which gives

$$0 \to A(K)/\phi A(K) \to H^1(\mathrm{Gal}(\overline{K}/K), A[\phi]) \to H^1(\mathrm{Gal}(\overline{K}/K), A)[\phi] \to 0. \tag{2.1}$$

Similar exact sequences for each localization K_v of K gives a commutative diagram

$$\begin{array}{ccc} H^1(K, A[\phi]) & \longrightarrow & H^1(K, A)[\phi] \\ \downarrow{\scriptstyle \text{res}} & \overset{s_\phi}{\searrow} & \downarrow{\scriptstyle \text{res}_\phi} \\ \prod_v H^1(K_v, A[\phi]) & \longrightarrow & \prod_v H^1(K_v, A)[\phi] \end{array}$$

where $\text{res} = \oplus \text{res}_v$ is restriction from $\text{Gal}(\overline{K}/K)$ to $\prod_v \text{Gal}(\overline{K}_v/K_v)$.

Define the *Selmer* group of ϕ to be $\text{Sel}_\phi(A/K) = \ker s_\phi$. Define the *Shafarevich-Tate* group to be $Ш(A/K) = \ker\left(H^1(K, A) \xrightarrow{\text{res}} \prod_v H^1(K_v, A)\right)$. Then $Ш(A/K)[\phi] = \ker \text{res}_\phi$ and the snake lemma gives an exact sequence

$$0 \to A(K)/\phi A(K) \to \text{Sel}_\phi(A/K) \to Ш(A/K)[\phi] \to 0.$$

This exact sequence is useful is computing the Mordell-Weil group $A(K)$ when K is a number field. Namely, if one knows $Ш(A/K)[\phi]$ and one can compute elements of $\text{Sel}_\phi(A/K)$ then this exact sequence yields generators for $A(K)/\phi A(K)$. However, little is known about the Shafarevich-Tate group $Ш(A/K)$.

Lemma 2.36. *The image of the restriction map*

$$H^1(K, A) \to \prod_v H^1(K_v, A)$$

is contained in $\bigoplus_v H^1(K_v, A)$.

Proof. Let f be a cocycle in $H^1(K, A)$. By construction of $\text{Gal}(\overline{K}/K)$-cohomology (i.e., since f is locally constant), there exists a finite extension L/K such that $\text{Res}^{\text{Gal}(\overline{L}/L)}_{\text{Gal}(\overline{K}/K)} f$ is trivial in $H^1(L, A)$. Since the following diagram commutes

$$\begin{array}{ccc} H^1(L, A) & \longrightarrow & \prod_{w|v} H^1(L_w, A) \\ {\scriptstyle \text{Res}^L_K}\uparrow & & \uparrow{\scriptstyle \prod_v \text{res}} \\ H^1(K, A) & \longrightarrow & \prod_v H^1(K_v, A) \end{array}$$

for each $w|v$ the image f_w of f in $H^1(L_w, A)$ is trivial. However, for all but finitely many v the variety A has good reduction at v (see Definition 2.47) and v is unramified in L. Therefore by [LT58] Corollary 1 to Theorem 1, the order of f_v in the torsion group $H^1(K_v, A)$ divides $e_{L_w/K_v} = 1$ (since $w \mid v$ is unramified) which means that f_v is trivial. Therefore, f_v is trivial for almost all places v which implies that the image is in the direct sum. □

Remark 2.37. Since $\mathbb{A}_K \otimes \overline{K}$ has a natural $\text{Gal}(\overline{K}/K)$ action, we can define the Galois cohomology of $A(\mathbb{A}_K \otimes \overline{K})$. Then $Ш(A/K) = \ker(H^1(K, A(\overline{K})) \to H^1(K, A(\mathbb{A}_K \otimes_K \overline{K}))$. (See [PR94] Proposition 6.6.)

The Shafarevich-Tate group $Ш(A/K)$ is functorial in A. Let K be a number field and let $A \xrightarrow{\psi} B$ be an isogeny of abelian varieties defined over K. Then there is a commutative diagram

$$\begin{array}{ccc} Ш(A/K) & \xrightarrow{\psi_{Ш}} & Ш(B/K) \\ \downarrow & & \downarrow \\ H^1(K,A) & \xrightarrow{\psi} & H^1(K,B) \\ {\scriptstyle \mathrm{res}_A}\downarrow & & \downarrow{\scriptstyle \mathrm{res}_B} \\ \oplus_v H^1(K_v,A) & \xrightarrow{\psi} & \oplus_v H^1(K_v,B) \end{array}$$

in which the map $\psi_{Ш}$ is well defined since the kernel of res_A is mapped to the kernel of res_B.

Remark 2.38. The Shafarevich-Tate group is defined in terms of cohomology, seamingly with no relation to geometry. However, we have already seen a connection between geometry and cohomology in Section 1.3. For each $a \in A(\overline{K})$ we have defined a translation automorphism t_a of A, so $A(\overline{K}) \subset \mathrm{Aut}_{\overline{K}}(A)$ which means that $H^1(K, A(\overline{K}))$ is a subset of $H^1(K, \mathrm{Aut}_{\overline{K}}(A))$, a group that parametrizes the isomorphism classes of $\overline{K}$ twisits of A. Our description of $A(\overline{K})$ shows that elements of $H^1(K, A)$ correspond to $\overline{K}$ twisits of A with a simply transitive A-action. Such a twist is called a *principal homogeneous space* for A. A principal homogeneous space corresponds to a trivial cohomology class in $H^1(K, \mathrm{Aut}_{\overline{K}}(A))$ if it has a K-rational point. As such, elements of $Ш(A/K)$ correspond to locally trivial principal homogeneous spaces (i.e., a principal homogeneous space with a rational point over each completion K_v).

2.2.6 The Cassels-Tate Pairing for Ш

In order to relate the Shafarevich-Tate groups of A and $A^\vee$ it is useful to construct a bilinear pairing $Ш(A/K) \times Ш(A^\vee/K) \to \mathbb{Q}/\mathbb{Z}$. The most intuitive way to construct the pairing is to notice that, if X is a principal homogeneous space for A, then $A^\vee(\overline{K}) \cong \mathrm{Pic}^0_{\overline{K}}(A \times_K \overline{K}) \cong \mathrm{Pic}^0_{\overline{K}}(X \times_K \overline{K})$ and use Remark 2.38 where we constructed a locally trivial principal homogeneous space X_f for each cocycle $f \in Ш(A/K)$. This will allow us to relate points in $A^\vee(\overline{K})$ to rational functions on X_f via the exact sequence

$$0 \to \overline{K}(X_f)^\times/\overline{K}^\times \to \mathrm{Div}^0(X_f \times \overline{K}) \to \mathrm{Pic}^0(X_f \times \overline{K}) \to 0 \tag{2.2}$$

where $\overline{K}(X_f)$ is the field of rational functions on X_f. (For three other descriptions of the pairing see [PS99].)

Since $\overline{K}(X_f)$ is a $\mathrm{Gal}(\overline{K}/K)$-module with the action ${}^\sigma h(x) = \sigma h(\sigma^{-1}x)$ on $h \in \overline{K}(X_f)$, we can write the $\mathrm{Gal}(\overline{K}/K)$ and $\mathrm{Gal}(\overline{K}_v/K_v)$-cohomology long exact sequences of the exact sequence ($\mathcal{K} = \overline{K}(X_f)^\times/\overline{K}^\times$)

$$0 \to \overline{K}^\times \to \overline{K}(X_f)^\times \to \mathcal{K} \to 0.$$

Since $H^3(K,\overline{K}^\times)=0$ and $H^3(K_v,\overline{K}_v^\times)=0$ for all places v (by Hilbert's Theorem 90 and [AW67] Theorem 5) we have

$$\begin{array}{ccccccc} H^2(K,\overline{K}^\times) & \longrightarrow & H^2(K,\overline{K}(X_f)^\times) & \xrightarrow{j} & H^2(K,\mathcal{K}) & \longrightarrow & 0 \\ \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & & \\ \prod_v H^2(K_v,\overline{K}_v^\times) & \xrightarrow{i} & \prod_v H^2(K_v,\overline{K}_v(X_f)^\times) & \longrightarrow & \prod_v H^2(K_v,\mathcal{K}) & \longrightarrow & 0 \end{array}$$

In order to remove the relevance of choices in the construction of the pairing we need to show that i is injective. Since X_f is locally trivial, for each place v there exists a point in $X_f(K_v)$, i.e., a section $\operatorname{Spec} K_v \to X_f$. By [Mil86a] Remark 6.11 this implies that i is injective on each component $H^2(K_v,\overline{K}_v^\times)\to H^2(K_v,\overline{K}_v(X_f)^\times)$ and so i is injective.

Since X_f is a principal homogeneous space, there exists a noncanonical isomorphism $X_f\times\overline{K}\approx A\times\overline{K}$ which induces a $\overline{K}$-isomorphism $\mathrm{Pic}^0(X_f\times\overline{K})\approx A^\vee(\overline{K})$. For general twists the isomorphism $X_f\times_K\overline{K}\approx A\times_K\overline{K}$ is defined up to an automorphism of A, but for principal homogeneous spaces it is defined up to an automorphism t_a for $a\in A(\overline{K})$. But t_a acts trivially on $A^\vee(\overline{K})$ since $t_a^*\phi_{\mathcal{L}}=\phi_{\mathcal{L}}$ for a choice of ample invertible sheaf $\mathcal{L}$, by the Corollary 2.8. Therefore, the isomorphism $\mathrm{Pic}^0(X_f\times\overline{K})\approx A^\vee(\overline{K})$ is independent of choices. Moreover, this is an isomorphism of $\mathrm{Gal}(\overline{K}/K)$-modules since for $\sigma\in\mathrm{Gal}(\overline{K}/K)$ we have ${}^\sigma\varphi_{\mathcal{L}}=\varphi_{\mathcal{L}^\sigma}$.

Following Cassels's original idea, we will use the canonical isomorphism of $\mathrm{Gal}(\overline{K}/K)$-modules $\mathrm{Pic}^0(X_f\times\overline{K})\cong A^\vee(\overline{K})$ and the exact sequence 2.2 to define the pairing. The $\mathrm{Gal}(\overline{K}/K)$-cohomology long exact sequence associated with sequence 2.2 gives a boundary map ∂

$$H^1(K,A^\vee(\overline{K}))\cong H^1(K,\mathrm{Pic}^0(X_f\times\overline{K}))\xrightarrow{\partial}H^2(K,\mathcal{K})$$

The rest of the construction of the pairing amounts to abstract nonsense. Let $g\in Ш(A^\vee/K)\subset H^1(K,A^\vee(\overline{K}))$ and let $g'=\partial g$. The map j is surjective so there exists $h'\in H^2(K,\overline{K}(X_f)^\times)$ such that $j(h')=g'$. Let $\prod_v h_v$ be the image of h' in $\prod_v H^2(K_v,\overline{K}_v(X_f)^\times)$ under the restriction maps.

$$\begin{array}{ccccccc} & & & & h' & \xrightarrow{j} & g' \longrightarrow 0 \\ & & & & \downarrow{\scriptstyle \mathrm{res}} & & \\ 0 & \longrightarrow & \prod_v h_v & \xrightarrow{i} & \prod_v h'_v & & \\ & & & \underset{h'_v(p_v)}{\leftarrow} & & & \end{array}$$

For each $\sigma,\tau\in\mathrm{Gal}(\overline{K}_v/K_v)$, we have $h'_v(\sigma,\tau)\in\overline{K}(X_f)^\times$. In order to define the cohomology classes h_v we choose points $p_v\in X_f(\overline{K}_v)$ that are not zeros or poles of $h'_v(\sigma,\tau)$ for any $\sigma,\tau\in\mathrm{Gal}(\overline{K}_v/K_v)$ and then evaluate h'_v at p_v. Define a map $h_v:\mathrm{Gal}(\overline{K}_v/K_v)\times\mathrm{Gal}(\overline{K}_v/K_v)\to\overline{K}_v^\times$ by taking (σ,τ) to $h'_v(\sigma,\tau)(p_v)\in K_v^\times$. Since h'_v is a cocycle and h_v is obtained by evaluation, h_v is also a cocycle in $H^2(K_v,\overline{K}_v^\times)$. By the injectivity of i the choice of the points p_v is irrelevant. Define the pairing

$$\langle f,g\rangle=\sum_v \mathrm{inv}_v(h_v)\in\mathbb{Q}/\mathbb{Z},$$

where inv_v are the invariant maps of local class field theory. This is a finite sum by [Mil86b], Lemma 4.8.

Proposition 2.39 (Cassels-Tate)**.** *The pairing* $\langle , \rangle : Ш(A/K) \times Ш(A^\vee/K) \to \mathbb{Q}/\mathbb{Z}$ *is functorial in* A *and the kernel on each side is the maximal divisible subgroup of* $Ш(A/K)$ *or* $Ш(A^\vee/K)$*.*

Proof. See [Mil86b] Theorem 6.13. □

2.3 Reduction of Abelian Varieties

2.3.1 Motivation

Let A be an abelian variety over a global field K. We would like to study the arithmetic properties of A by analyzing the behavior of A at each finite place v of K. If the abelian variety has a set of defining equations defined over K, one can think of the reduction A_v as the variety defined by the same equations but whose coefficients are taken in k_v, provided that this makes sense (i.e., the v valuations of all coefficients of the equations have to be nonnegative, or we would get division by 0 in k_v).

Example 2.40. Consider $E/\mathbb{Q}$ to be the elliptic curve with Weierstrass equation

$$y^2 + xy + y = x^3 - x^2 - 8x + 11.$$

Then the discriminant of E is $-2^6 3^3 5$ so E_p is an elliptic curve for $p \notin \{2, 3, 5\}$. If $p = 3$ then E_p is a cuspidal curve while if $p \in \{2, 5\}$ then E_p is nodal.

The equations defining the E_p over $\mathbb{F}_p$ together with the curve E over $\mathbb{Q}$ define a scheme E' over $\operatorname{Spec} \mathbb{Z}$, the closure of $\operatorname{Proj} \mathbb{Z}[x, y, z]/(y^2z + xyz + yz^2 - x^3 + x^2z + 8xz^2 - 11z^3)$. By the valuative criterion of properness ([Har77], Theorem 4.7) we have $E'(\mathbb{Z}) = E(\mathbb{Q})$. However, E' is not a group scheme since it is not smooth over $\mathbb{Z}$ (at the primes 2,3,5). Let $\mathcal{E}^0$ be the largest smooth subscheme of E' defined over $\operatorname{Spec} \mathbb{Z}$. Then $E_p = \mathcal{E}^0 \times_{\operatorname{Spec} \mathbb{Z}} \operatorname{Spec} \mathbb{F}_p$. However, $\mathcal{E}^0$ no longer has the property that $\mathcal{E}^0(\mathbb{Z}) = E(\mathbb{Q})$.

2.3.2 Néron Models

To resolve this issue (that $\mathcal{E}^0(\mathbb{Z}) \neq E(\mathbb{Q})$) we want for each abelian variety A defined over a number field (more generally for the fration field of a Dedekind domain) to construct a smooth (group) scheme $\mathcal{A}$ defined over $\mathcal{O}_K$ such that $\mathcal{A}(\mathcal{O}_K) = A(K)$.

Theorem 2.41. *Let* A *be an abelian variety defined over a number field* K*. Then there exists a smooth model* $\mathcal{A}$ *of* A *which is separated and of finite type over* $\operatorname{Spec} \mathcal{O}_K$ *(called the Néron model) such that for every smooth scheme* T *over* $\operatorname{Spec} \mathcal{O}_K$ *the natural map*

$$\operatorname{Hom}(T, \mathcal{A}) \to \operatorname{Hom}(T \times_{\mathcal{O}_K} K, A),$$

is an isomorphism.

This is the surprising property of Néron models (called the Néron mapping property), since surjectivity implies that any morphism defined on the generic fiber A of $\mathcal{A}$ can be uniquely extended to a morphism on $\mathcal{A}$. However, one downside of the Néron model is that it is almost never proper (unlike E' which was proper but not smooth over $\mathbb{Z}$). The following proposition shows that the Néron model is unique.

Proposition 2.42. *Let A be an abelian variety defined over a number field K. Then the Néron model of A over* $\operatorname{Spec}\mathcal{O}_K$ *is unique up to isomorphism.*

Proof. Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be two Néron models of A over $\operatorname{Spec}\mathcal{O}_K$. The for $\{i,j\} = \{1,2\}$ we have

$$\operatorname{Hom}(\mathcal{A}_i, \mathcal{A}_j) = \operatorname{Hom}(\mathcal{A}_i \times_S K, A) = \operatorname{Hom}(A, A).$$

Let ψ_{ij} be the morphism from $\mathcal{A}_i \to \mathcal{A}_j$ that corresponds via the above isomorphism to the identity on A. Then $\psi_i = \psi_{ji} \circ \psi_{ij}$ is a morphism from $\mathcal{A}_i \to \mathcal{A}_i$ that corresponds on the generic fiber to the identity on A. However, the identity on $\mathcal{A}_i$ also has this property. Since

$$\operatorname{Hom}(\mathcal{A}_i, \mathcal{A}_i) = \operatorname{Hom}(A, A),$$

the morphism on $\mathcal{A}_i$ corresponding to the identity on A is unique so $\psi_i = 1$ and similarly $\psi_j = 1$ which proves that $\mathcal{A}_1 \cong_{\mathcal{O}_K} \mathcal{A}_2$. □

Remark 2.43. The Néron model of A is a group scheme. This is a simple consequence of the Néron mapping property since multiplication m and inversion i are morphisms on the generic fiber A of $\mathcal{A}$. Therefore they induce multiplication and inversion morphisms on all of $\mathcal{A}$, with respect to the identity section of $\mathcal{A}$.

Remark 2.44. If $\mathcal{E}$ is the Néron model of the elliptic curve E in Example 2.40 then $\mathcal{E}^0$ is the connected component of the identity section of $\mathcal{E}$. Analogously, if A is an abelian variety defined over a number field K and $\mathcal{A}$ is its Néron model defined over $\mathcal{O}_K$, let $\mathcal{A}^0$ be the subscheme of $\mathcal{A}$ that is the connected component of the identity section.

2.3.3 The reduction of an Abelian Variety at a Finite Place

Let A be an abelian variety over a number field K and let $\mathcal{A}^0$ be the connected component of the identity of the Néron model $\mathcal{A}$ of A over $\mathcal{O}_K$. For each finite place $v \in M_K^0$ define the special fiber of the reduction of A at v to be $\tilde{\mathcal{A}}_v = \mathcal{A} \times_{\mathcal{O}_K} k_v$, where k_v is the residue field at v. (Recall from Section 1.7 that $\mathcal{A}_v$ is defined to be $\mathcal{A}_v = \mathcal{A} \times_{\mathcal{O}_K} \mathcal{O}_v$.) The special fiber $\tilde{\mathcal{A}}_v$ is a smooth group scheme, but it need not be connected. Let $\tilde{\mathcal{A}}_v^0$ be the connected component of the identity in the fiber $\tilde{\mathcal{A}}_v$ (in which case $\tilde{\mathcal{A}}_v^0 = \mathcal{A}^0 \times_{\mathcal{O}_K} k_v$).

Proposition 2.45. *For a finite place v let Φ_v be the component group of the special fiber, i.e., the algebraic group defined by the exact sequence*

$$1 \to \tilde{\mathcal{A}}_v^0 \to \tilde{\mathcal{A}}_v \to \Phi_v \to 1.$$

Then the group Φ_v is a finite group scheme.

Proof. The groups $\tilde{\mathcal{A}}_v$ are varieties over the finite fields k_v, so they have finitely many components. □

Definition 2.46. Let v be a finite place. The positive integer $c_v = |\Phi_v(k_v)|$ is called the Tamagawa number at v.

There is no known general method of computing the Tamagawa number. In the case of elliptic curves, there exists a complete algorithm due to Tate (see [Tat75, Cre97]). For algorithms that compute the Tamagawa numbers of certain special abelian varieties (other than elliptic curves), see [CS01, KS00].

By Theorem 1.19 there exist (over k_v) an abelian variety B and an affine algebraic group G such that

$$1 \to G \to \tilde{\mathcal{A}}_v^0 \to B \to 1$$

is exact. By Theorem 1.20 there exist a unipotent group N and a torus T such that

$$1 \to N \to G \to T \to 1$$

is exact.

Definition 2.47. If $G = 1$ then A is said to have *good* reduction at v. Otherwise, A is said to have *bad* reduction at v. Moreover, if $N = 1$ then A is said to have *semistable* reduction at v; in this case, if T is a split torus then A has *split semistable* reduction at v.

Lemma 2.48. *If v is a place of good reduction for A then $c_v = 1$.*

Proof. We will show that if A has good reduction at v then $\tilde{\mathcal{A}}_v^0 = \tilde{\mathcal{A}}_v$ (then $\Phi_v = 1$ and so $c_v = 1$). The scheme $\mathcal{A}_1 = \mathcal{A} \times_{\mathcal{O}_K} \mathcal{O}_v$ is a subscheme of $\mathcal{A}$ so restriction from $\mathcal{A}$ to $\mathcal{A}_1$ extends any morphism on $\mathcal{A}$ to a morphism on $\mathcal{A}_1$. Therefore, for every smooth $\mathcal{O}_v$-scheme T we have $\mathrm{Hom}_{\mathbf{Sch}}(T, \mathcal{A}_1) = \mathrm{Hom}_{\mathbf{Sch}}(T \times_{\mathcal{O}_v} K_v, A)$ which implies that $\mathcal{A}_1$ is the Néron model of A over $\operatorname{Spec} \mathcal{O}_v$ ([BLR90], Proposition 1.2.4). Let $\mathcal{A}_2$ be the subscheme of $\mathcal{A}$ which consists of the generic fiber A and the abelian variety $\tilde{\mathcal{A}}_v^0$. Then $\mathcal{A}_2$ is a smooth and proper scheme over $\mathcal{O}_v$ (since the fibers A and $\tilde{\mathcal{A}}_v^0$ are proper;[Har77] 4.8.f) so by [BLR90] Proposition 1.2.8 the scheme $\mathcal{A}_2$ is the Néron model of its generic fiber A. Therefore Proposition 2.42 guarantees that $\mathcal{A}_1 \cong \mathcal{A}_2$ which implies that $\tilde{\mathcal{A}}_v = \tilde{\mathcal{A}}_v^0$. □

Example 2.49. Let E be an elliptic curve. Then $\dim_K \mathcal{E}_v^0 = 1$ which implies that either $\dim_K B = 1$ (in which case $G = 1$ and E has good reduction at v) or $\dim_K B = 0$ (in which case $\dim_K G = 1$ and E has bad reduction at v). Assume that E has bad reduction at v.

1. If $\dim_K N = 1$ and $T \cong 1$ then $N \cong \mathbb{G}_a$ and E is said to have additive reduction at v.
2. Otherwise, $\dim_K T = 1$ and $N \cong 1$ in which case $T \cong \mathbb{G}_m$ over $\overline{k}_v$ and E is said to have multiplicative reduction. In Example 1.18 we saw that T is either $\mathbb{G}_m$ or $R^1_{\mathbb{F}_{q_v^2}/\mathbb{F}_{q_v}} \mathbb{G}_m$. If $T = \mathbb{G}_m$ then E is said to have split multiplicative reduction. If $T = R^1_{\mathbb{F}_{q_v^2}/\mathbb{F}_{q_v}} \mathbb{G}_m$ then E is said to have nonsplit multiplicative reduction.

2.4 The Néron-Ogg-Shafarevich Criterion

Let A be an abelian variety of dimension d defined over a number field K. Recall that there is an action of the decomposition group $\mathrm{Gal}(\overline{K}_v/K_v) \subset \mathrm{Gal}(\overline{K}/K)$ and inertia group I_v on the Tate module $T_\ell A$. We have chosen a lift σ_v of the Frobenius element of $\mathrm{Gal}(\overline{k}_v/k_v) = \mathrm{Gal}(\overline{K}_v/K_v)^{I_v}$ to $\mathrm{Gal}(\overline{K}_v/K_v)$. Therefore, the action of σ_v on $T_\ell A$ depends on the choice of σ_v. However, the action of σ_v on $T_\ell A^{I_v}$ is independent of choices since σ_v is well-defined up to conjugation by an element of I_v. The following lemma shows that we can interpret the inertia-invariant subrepresentation of $T_\ell A$ as the Tate module of the special fiber of the Néron model, which is more manageable. Let $\mathcal{A}$ be the Néron model of A over $\mathcal{O}_K$.

Lemma 2.50. *If ℓ is coprime to char k_v and to the index of $\tilde{\mathcal{A}}_v^0$ in $\tilde{\mathcal{A}}_v$, then there exists an isomorphism of $\mathrm{Gal}(\overline{K}_v/K_v)$-modules*

$$T_\ell \tilde{\mathcal{A}}_v^0 = T_\ell \tilde{\mathcal{A}}_v = (T_\ell A)^{I_v}.$$

Proof. Let K_v^{nr} be the maximal unramified extension of K_v, i.e., $K_v^{\mathrm{nr}} = K_v^{I_v}$. Since $A(\overline{K})^{I_v} = A(K_v^{\mathrm{nr}})$ we get that $A[\ell^n]^{I_v} = A(K_v^{\mathrm{nr}})[\ell^n]$. For each finite unramified extension L/K the scheme $\mathrm{Spec}\,\mathcal{O}_L$ is smooth over $\mathrm{Spec}\,\mathcal{O}_K$ so the Néron mapping property implies that $\mathcal{A}_v(\mathcal{O}_L) = A(L)$. By passing to the limit we get

$$\mathcal{A}_v(\mathcal{O}_v^{\mathrm{nr}}) = A(K_v^{\mathrm{nr}}),$$

where $\mathcal{O}_v^{\mathrm{nr}}$ is the ring of integers of K_v^{nr}

Since $\mathcal{A}_v$ is a smooth scheme over $\mathrm{Spec}\,\mathcal{O}_v$ and $\mathcal{O}_v^{\mathrm{nr}}$ is henselian, the reduction map

$$\mathcal{A}_v(\mathcal{O}_v^{\mathrm{nr}}) \xrightarrow{r} \tilde{\mathcal{A}}_v(\overline{k}_v),$$

is surjective (because the residue field of $\mathcal{O}_v^{\mathrm{nr}}$ is $\overline{k}_v$). Moreover, the $\mathrm{Ext}_{\mathbb{Z}}(\mathbb{Z}/\ell^n\mathbb{Z})$-long exact sequence of

$$0 \to \ker r \to \mathcal{A}_v(\mathcal{O}_v^{\mathrm{nr}}) \to \tilde{\mathcal{A}}_v(\overline{k}_v) \to 0,$$

gives

$$0 \to (\ker r)[\ell^n] \to \mathcal{A}_v(\mathcal{O}_v^{\mathrm{nr}})[\ell^n] \to \tilde{\mathcal{A}}_v(\overline{k}_v)[\ell^n] \to \mathrm{Ext}(\mathbb{Z}/\ell^n\mathbb{Z}, \ker r).$$

Since $\ker r$ is divisible ([Mum70] II.6.2) the group $\mathrm{Ext}(\mathbb{Z}/\ell^n\mathbb{Z}, \ker r)$ is trivial so the map $\mathcal{A}_v(\mathcal{O}_v^{\mathrm{nr}})[\ell^n] \xrightarrow{r} \tilde{\mathcal{A}}_v(\overline{k}_v)[\ell^n]$ is surjective. Moreover, Remark 2.60 implies that, since ℓ^n and char k_v are coprime, the surjection $\mathcal{A}_v(\mathcal{O}_v^{\mathrm{nr}})[\ell^n] \to \tilde{\mathcal{A}}_v(\overline{k}_v)[\ell^n]$ is also injective. By passing to the limit as $n \to \infty$ we get $T_\ell A^{I_v} = T_\ell \tilde{\mathcal{A}}_v$.

By Lemma 2.33 there is an exact sequence $1 \to T_\ell \tilde{\mathcal{A}}_v^0 \to T_\ell \tilde{\mathcal{A}}_v \to T_\ell \Phi_v$. Since ℓ is coprime to the index of $\tilde{\mathcal{A}}_v^0$ in $\tilde{\mathcal{A}}_v$, the module $T_\ell \Phi_v$ is trivial, which implies that $T_\ell \tilde{\mathcal{A}}_v^0 = T_\ell \tilde{\mathcal{A}}_v$. □

Theorem 2.51 (Néron-Ogg-Shafarevich)**.** *For A to have good reduction at a place v it is sufficient that $I_v \subset \mathrm{Gal}(\overline{K}_v/K_v)$ act trivially on $T_\ell A$, for some ℓ coprime to char k_v and the index of $\tilde{\mathcal{A}}_v^0$ in $\tilde{\mathcal{A}}_v$.*

Proof. In Section 2.3.3 we have seen that there exist algebraic groups G, N, T and B defined over k_v, such that T is a torus, N is unipotent, B is an abelian variety and there exist exact sequences

$$1 \to T \to G \to N \to 1 \tag{2.3}$$

$$1 \to G \to \tilde{\mathcal{A}}_v^0 \to B \to 1$$

An immediate consequence is that $d = \dim \mathcal{A}_v^0 = \dim A = \dim N + \dim T + \dim B$. Moreover, since the unipotent group U is divisible, Lemma 2.33 applied to the exact sequences 2.3 gives (since $T_\ell T \cong T_\ell G$)

$$1 \to T_\ell T \to T_\ell \tilde{\mathcal{A}}_v^0 \to T_\ell B \to 1.$$

But Lemma 2.50 allows us to replace $T_\ell \tilde{\mathcal{A}}_v^0$ with $T_\ell A^{I_v}$. Therefore

$$1 \to T_\ell T \to (T_\ell A)^{I_v} \to T_\ell B \to 1,$$

which implies that $\dim T_\ell \tilde{\mathcal{A}}^0 = \dim T_\ell T + \dim T_\ell B$. The rest of the proof ammounts to dimension count. By Remark 2.32, we have $\dim T_\ell B = 2 \dim B$ since B is an abelian variety. Moreover, since T is a torus, there exists a $\overline{k}_v$-isomorphism $T \cong \mathbb{G}_m^{\dim T}$. Therefore, $T_\ell T = T_\ell \mathbb{G}_m^{\dim T} = (T_\ell \mathbb{G}_m)^{\dim T}$ which implies that $\dim T_\ell T = \dim T$.

Since I_v acts trivially on $T_\ell A$ we get that $\dim T_\ell \mathcal{A}_v^0 = \dim T_\ell A = 2 \dim A = 2 \dim N + 2 \dim T + 2 \dim B$; but this is also equal to $2 \dim B + \dim T$ which implies that $2 \dim N + \dim T = 0$. Since N and T are connected, they must be trivial, so A has good reduction at v. □

One implication of Theorem 2.51 is that if $T_\ell A$ is unramified at v for some ℓ, coprime to char k_v and the index of $\tilde{\mathcal{A}}_v^0$ in $\tilde{\mathcal{A}}_v$, then it is unramified for all ℓ coprime to char k_v and the index of $\tilde{\mathcal{A}}_v^0$ in $\tilde{\mathcal{A}}_v$.

Remark 2.52. The conclusion of Theorem 2.51 still holds if we only assume ℓ to be coprime to char k_v, since in the proof of the theorem it is enough that ℓ^n becomes larger than the index of $\tilde{\mathcal{A}}_v^0$ in $\tilde{\mathcal{A}}_v$ as $n \to \infty$ (which follows from Proposition 2.45). Moreover, if A has good reduction at v, then for infinitely many ℓ, the Tate module $V_\ell A$ is unramified at v. The details of the proof of this more general version can be found in [ST68], Theorem 1.

Corollary 2.53. *1. If A is an abelian variety defined over a global field K then for all but finitely many places v the variety A has good reduction at v.*

2. Let $\psi : A \to B$ be an isogeny of abelian varieties. If A has good reduction at v then so does B.

Proof. 1. Choose a prime ℓ. Since $T_\ell A$ is a finitely generated $\mathrm{Gal}(\overline{K}/K)$-module, the inertia I_v acts trivially on $T_\ell A$ for all but finitely many places v. Therefore, Remark 2.52 proves that there is good reduction outside a finite set of places (where $T_\ell A$ has bad reduction or where $\ell \mid$ char k_v).

2. Via ψ the $\mathbb{Z}_\ell$-module $T_\ell A$ has image a submodule of $T_\ell B$ of finite index. Therefore, if I_v acts trivially on $T_\ell B$, it will act trivially on $T_\ell A$.

□

2.5 Abelian Varieties over Finite Fields

Let A be an abelian variety of dimension d defined over a finite field $\mathbb{F}_q$. Let π_q be the Frobenius isogeny of the abelian variety (acting as the identity on the topological space underlying the variety as a scheme and acting on functions by $f \mapsto f^q$). If $\mathrm{End}(A)$ represents the ring of endomorphisms of A (i.e., isogenies preserving the identity of A), write $\mathrm{End}(A)^0 = \mathrm{End}(A) \otimes \mathbb{Q}$.

Lemma 2.54. *There exists a monic polynomial $P_q \in \mathbb{Z}[x]$ of degree $2d$ such that for all $m, n \in \mathbb{Z}$ we have $n^{2d} P_q(m/n) = \deg([m] + [n] \circ \pi_q) = |\ker([m] + [n] \circ \pi_q)|$. Moreover, P_q is the characteristic polynomial of Frob_q acting on $V_\ell A$ and the minimal polynomial of π_q in $\mathbb{Q}(\pi_q)/\mathbb{Q}$ (where $\mathbb{Q}(\pi_q) \subset \mathrm{End}^0(A)$.*

Proof. See [Mil86a], Proposition 12.4. and Proposition 12.9. □

Write $P_q(x) = \prod_{i=1}^{2d}(x - \alpha_i)$, with $\alpha_i \in \mathbb{C}$. To understand the behavior of the roots α_i of P_q we need to understand the relationship between A and $A^\vee$. Fix $\mathcal{L}$ an ample invertible sheaf on A and let $\phi = \phi_{\mathcal{L}}$ be the polarization associated with $\mathcal{L}$ (i.e., an isogeny $\phi_{\mathcal{L}} : A \to A^\vee$). We define the *Rosati involution* $\dagger$ on $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$ by $\psi^\dagger = \phi^{-1} \circ \psi^\vee \circ \phi$ acting on A.

Lemma 2.55. *The following relation holds in* $\mathrm{End}^0(A)$

$$\pi_q^\dagger \circ \pi_q = [q].$$

Proof. This is equivalent to $\phi^{-1} \circ \pi_q^\vee \circ \phi \circ \pi_q = [q]$ or $\pi_q^\vee \circ \phi \circ \pi_q = [q] \circ \phi$ (since $[q]$ commutes with ϕ by construction). But for each $x \in A(\overline{K})$ we have $(\pi_q^\vee \circ \phi \circ \pi_q)(x) = \pi_q^*(t^*_{\pi_q(x)}\mathcal{L} \otimes \mathcal{L}^{-1}) = t_x^*(\pi_q^*\mathcal{L}) \otimes \pi_q^*\mathcal{L}$. Since π_q^* acts by raising to the power q we get

$$(\pi_q^\vee \circ \phi \circ \pi_q)(x) = t_x^*\mathcal{L}^q \otimes \mathcal{L}^{-q} = [q] \circ (t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}) = [q] \circ \phi.$$

□

Proposition 2.56. *Let $\pi \in \mathrm{End}^0(A)$ such that $\pi^\dagger \circ \pi = [m]$, where m is a positive integer. Let R be the set of roots of the minimal polynomial of π over $\mathbb{Q}$. Then for every root $\alpha \in R$, we have $|\alpha| = \sqrt{m}$ and $x \mapsto m/x$ is a permutation of R.*

Proof. See [Mum70] IV.21.II. □

Corollary 2.57 (Riemann Hypothesis)**.** *The roots $\alpha_1, \ldots, \alpha_{2d}$ of the minimal polynomial of π_q have absolute value $\sqrt{q}$ and can be reordered such that $\alpha_{2d-i}\alpha_i = q$ for all i.*

Proof. Follows from Lemma 2.55 and Proposition 2.56. □

2.6 The Tamagawa Measure of Abelian Varieties

Let A be an abelian variety of dimension d over a number field K and let $\mathcal{A}$ be its Néron model over $\operatorname{Spec}\mathcal{O}_K$. We have seen in Section 1.7 how to use a nowhere vanishing invariant differential form w on $\mathcal{A}$ and a set of convergence factors $\{\lambda_v\}$ to define a measure $d\mu_{A,w,\{\lambda_v\}}$. However, this measure depends on the (noncanonical) choice of factors λ_v. We will use the results of Section 3.1.1 to prove that there is a canonical choice of convergence factors given by $\lambda_v = 1$, if v is an infinite place, and $\lambda_v = L_v(A, 1)$, if v is a finite place. This result holds for tori as well, but we will prove a stronger statement in the case of abelian varieties over number fields.

2.6.1 The Formal Group of an Abelian Variety

In order to analyze the Haar measures, it is enough to look locally. This is best understood in the context of formal groups. Abelian varieties are commutative groups so their global analytic behavior is determined in a local neighborhood of the identity element e, by translations. A powerful tool of analyzing such a local neighborhood of e is the notion of formal neighborhood of e, which is a formal group for algebraic groups. However, instead of looking at the formal group of A, we will look at the formal group of $\mathcal{A}$, since $\mathcal{A}$ has much better arithmetic properties than A.

We will identify the point $e \in A(K_v)$ with the (closed) point which is the image of the map $e : \operatorname{Spec} K_v \to A$ (since A is complete every morphism from an affine scheme into A is constant). The group $\mathcal{A}_v$ is defined over $\operatorname{Spec}\mathcal{O}_v$. Let $\mathcal{O}_{\mathcal{A}_v,e}$ be the local regular ring of $\mathcal{A}_v$ at e and let $\mathfrak{m}_{\mathcal{A}_v,e}$ be the maximal ideal of $\mathcal{O}_{\mathcal{A}_v,e}$. Let $\widehat{\mathcal{O}}_{\mathcal{A}_v,e} = \varprojlim \mathcal{O}_{\mathcal{A}_v,e}/\mathfrak{m}^n_{\mathcal{A}_v,e}$ be the completion of $\mathcal{O}_{\mathcal{A}_v,e}$. Since $\mathcal{A}_v$ is smooth of relative dimension d, the ring $\mathcal{O}_{\mathcal{A}_v,e}$ is regular so there exist indeterminates $x_1, \ldots, x_d$ such that $\widehat{\mathcal{O}}_{\mathcal{A}_v,e} \cong \mathcal{O}_v[\![x_1, \ldots, x_d]\!]$. Similarly, we have $\widehat{\mathcal{O}}_{\mathcal{A}_v\times\mathcal{A}_v,e\times e} \cong \mathcal{O}_v[\![y_1, \ldots, y_d, z_1, \ldots, z_d]\!]$, where $x_i \circ \pi_1 = y_i$, $x_i \circ \pi_2 = z_i$, and π_k is projection to the k-th factor.

The multiplication morphism $m : \mathcal{A}_v \times \mathcal{A}_v \to \mathcal{A}_v$ induces a morphism $m^* : \mathcal{O}_v[\![x_1, \ldots, x_d]\!] \to \mathcal{O}_v[\![y_1, \ldots, y_d, z_1, \ldots, z_d]\!]$. Write $F_i = m^*(x_i)$ which will be power series in y_i and z_j.

Proposition 2.58. *If $F = (F_1, \ldots, F_d)$ then for $y = (y_1, \ldots, y_d), z = (z_1, \ldots, z_d)$ we have*

1. $F(y, z) \equiv y + z \pmod{\mathfrak{m}_{A_v,e}}$.
2. $F(x, F(y, z)) = F(F(x, y), z)$.
3. $F(y, z) = F(z, y)$.
4. $F(0, z) = z, F(y, 0) = y$.

Proof. All the above follow from the formal properties of m except for the first property. The first property follows from the fact that $\mathcal{A}$ has a differential operator which takes m to the map $m_* : K_v[\![y_1, \ldots, y_d, z_1, \ldots, z_d]\!] \to K_v[\![x_1, \ldots, x_d]\!]$ given by $m_*(y, z) = y + z$. □

Let $\widehat{\mathcal{A}}_v$ be the formal group of $\mathcal{A}_v$. Similarly to the case of the group $\mathcal{A}_v$ itself, the space $\Omega = \sum \mathcal{O}_v[\![x_1, \ldots, x_d]\!]dx_i$ is generated by d independent invariant differentials $\eta_i = \sum \phi_{ij}(x)dx_j$. The fact that η_i are invariant and they generate Ω implies that they are a unique scalar multiple of

$$\begin{pmatrix} 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \end{pmatrix} \left(\frac{\partial F_p}{\partial x_q}\right)^{-1} dx.$$

We have constructed a formal group $\widehat{\mathcal{O}}_{\mathcal{A}_v,e}$ as the formal completion of $\mathcal{A}_v$ along the identity section. The de Rham cohomology of $K_v[\![x_1, \ldots, x_n]\!]$ is trivial, so there exist power series $\log_i$ such that $d\log_i = \eta_i$ for every i. The $\log_i$ form the logarithm map $\log = (\log_1, \ldots, \log_n) : \widehat{\mathcal{A}}_v \to \mathbb{G}_a^n$, which is an isomorphism of formal groups (see [Fre93], Theorem 1). On a small enough neighborhood of the identity where the series converge, log is a homeomorphism. The formal Lie algebra of $\widehat{\mathcal{A}}_v$ is the Lie algebra structure $\mathfrak{A}_v$ of $\mathbb{G}_a^n$, given by $[x, y] = F_2(x, y) - F_2(y, x)$, where F_2 represents the homogeneous part of degree 2 of F.

2.6.2 Behavior at Finite Places

Let $\Omega_{\mathcal{A}}$ be the projective $\mathcal{O}_K$-module of global invariant differentials on the Néron model $\mathcal{A}$ with $\mathcal{O}_K$-basis $\eta_1, \ldots, \eta_d$. Then $\wedge^d\Omega_{\mathcal{A}}$ is a rank one $\mathcal{O}_K$-module (with $\mathcal{O}_K$-basis $\eta_1 \wedge \ldots \wedge \eta_d$), which is a rank one submodule of $H^0(A, \Omega^d_{A/K})$, the module of invariant differentials on the abelian variety A (Section 1.7.1). Therefore, for every global invariant differential $w \in H^0(A, \Omega_{A/K})$, there exists a fractional ideal $\mathfrak{a}_w$ of $\mathcal{O}_K$, such that $w\mathfrak{a}_w = \eta_1 \wedge \ldots \wedge \eta_d\mathcal{O}_K = \wedge^d\Omega_{\mathcal{A}}$. Let $v_w = |\mathfrak{a}_w|_v$ for every finite place v.

Lemma 2.59. *If v is a finite place, then*

$$\int_{\mathcal{A}_v(\mathcal{O}_v)} |w|_v = q_v^{-d} v_w |\tilde{\mathcal{A}}_v(k_v)|.$$

Proof. Let $\mathcal{A}_v(\mathcal{O}_v)_1$ be the kernel of the reduction map $\mathcal{A}_v(\mathcal{O}_v) \to \mathcal{A}_v(\mathcal{O}_v/\wp_v)$. For every polynomial which defines a smooth variety, Hensel's lemma implies that one can lift roots of the polynomials in $\mathcal{O}_v/\wp_v$ to roots in $\mathcal{O}_v$. Therefore, since $\mathcal{A}_v$ is smooth, the map $\mathcal{A}_v(\mathcal{O}_v) \to \mathcal{A}_v(\mathcal{O}_v/\wp_v) = \tilde{\mathcal{A}}_v(k_v)$ is surjective by Hensel's lemma. Therefore $\mathcal{A}_v(\mathcal{O}_v)/\mathcal{A}_v(\mathcal{O}_v)_1 \cong \tilde{\mathcal{A}}_v(k_v)$.

Consider invariant differentials $w_1, \ldots, w_n$ such that $w = w_1 \wedge \ldots \wedge w_n$. The differentials w_i and η_i induce invariant differentials $\widehat{w}_i$ and $\widehat{\eta}_i$ on the formal group $\widehat{\mathcal{A}}_v$ of $\mathcal{A}_v$ at the identity section. Let $\mathfrak{A}_v$ be the formal Lie algebra of $\widehat{\mathcal{A}}_v$. Let $\log_i = \int \widehat{\eta}_i$ be the logarithm maps associated with the differentials $\widehat{\eta}_i$ such that $\log_i(0) = 0$. Then $\log = (\log_1, \ldots, \log_n)$ defines a homeomorphism between the neighborhood $\wp_v^N \times \ldots \times \wp_v^N$ of $(0, \ldots, 0) \in K_v^n$ for large enough N and a neighborhood U_N of e in $\mathcal{A}_v(\mathcal{O}_v)$ (note that $U_1 = \mathcal{A}_v(\mathcal{O}_v)_1$, see [HS00], Theorem 2.6). In fact, the logarithm map log induces a formal group isomorphism between $\widehat{\mathcal{A}}_v$ and $\mathbb{G}_a^n$ via $(a, b) \mapsto \log^{-1}(\log a + \log b)$; the map $\log^{-1}$ is well-defined since $\widehat{\eta}_1, \ldots, \widehat{\eta}_d$ is an $\mathcal{O}_K$-basis for the module of invariant differentials (see [Fre93], Theorem 1).

Since the differential w is translation invariant we have

$$\int_{\mathcal{A}(\mathcal{O}_v)} |w|_v d\mu_v = [\mathcal{A}(\mathcal{O}_v) : \mathcal{A}(\mathcal{O}_v)_1] \int_{\mathcal{A}(\mathcal{O}_v)_1} |w|_v d\mu_v = |\tilde{\mathcal{A}}_v(k_v)| \int_{\widehat{\mathcal{A}}_v(\wp_v)} |\widehat{w}|_v.$$

The log function allows us to compute

$$\int_{\widetilde{\mathcal{A}}_v(\wp_v^N)} |\widehat{w}|_v = \int_{\wp_v^N \mathfrak{A}_v} |\log_* \widehat{w}|_v,$$

and so we get that

$$\int_{\mathcal{A}(\mathcal{O}_v)} |w|_v d\mu_v = [\mathcal{A}(\mathcal{O}_v) : \mathcal{A}(\mathcal{O}_v)_1][\wp_v^n : (\wp_v^N)^n] \int_{\wp_v^N \mathfrak{A}_v} |\log_* \widehat{w}|_v.$$

But $\log_* \widehat{w}$ is an invariant differential on $\wp_v^N \mathfrak{A}_v$ so it must be a scalar multiple of $dx_1 \wedge \ldots \wedge dx_n$. To evaluate this scalar factor, we need to evaluate $\log_* \widehat{w}$ at the basis $\partial/\partial x_1 \wedge \ldots \wedge \partial/\partial x_d$. Then

$$\begin{aligned}
|\log_*(\widehat{w}_1 \wedge \ldots \wedge \widehat{w}_d)|_v \left(\frac{\partial}{\partial x_1} \wedge \ldots \wedge \frac{\partial}{\partial x_d} \right) &= |\widehat{w}_1 \wedge \ldots \wedge \widehat{w}_d|_v \log^* \left(\frac{\partial}{\partial x_1} \wedge \ldots \wedge \frac{\partial}{\partial x_d} \right) \\
&= |\widehat{w}_1 \wedge \ldots \wedge \widehat{w}_d|_v \left(\log_1^* \frac{\partial}{\partial x_1} \wedge \ldots \wedge \log_d^* \frac{\partial}{\partial x_d} \right) \\
&= |\widehat{w}_1 \wedge \ldots \wedge \widehat{w}_d|_v \left(\frac{\partial}{\log_1' \partial t_1} \wedge \ldots \wedge \frac{\partial}{\log_d' \partial t_d} \right) \\
&= \left| \frac{\widehat{w}_1}{\widehat{\eta}_1} \wedge \ldots \wedge \frac{\widehat{w}_d}{\widehat{\eta}_d} \right|_v \left(\frac{\partial}{\partial t_1} \wedge \ldots \wedge \frac{\partial}{\partial t_d} \right) \\
&= v_w
\end{aligned}$$

by definition of the v_w. Therefore

$$\int_{\mathcal{A}(\mathcal{O}_v)} |w|_v = [\mathcal{A}(\mathcal{O}_v) : \mathcal{A}(\mathcal{O}_v)_1] q_v^{n(N-1)} v_w \int_{\wp_v^N \mathfrak{A}_v} dx_1 \wedge \ldots \wedge dx_n = q_v^{-n} v_w |\tilde{\mathcal{A}}_v(k_v)|.$$

□

Remark 2.60. Since $\mathcal{A}_v(\mathcal{O}_v)_1$ is isomorphic via the logarithm map to $U_1 \cong \prod \wp_v$, the m-torsion $\mathcal{A}_v(\mathcal{O}_v)_1[m]$ is trivial is m is coprime to char k_v.

Corollary 2.61. *If A has good reduction at v then*

$$\left(\int_{\mathcal{A}_v(\mathcal{O}_v)} |w|_v \right) L_v(A, 1) = v_w.$$

Proof. By Proposition 3.10 we have that $L_v(A,1)^{-1} = q_v^d / |\tilde{\mathcal{A}}_v^0(k_v)|$ and since A has good reduction at v we know that $\tilde{\mathcal{A}}_v^0 = \tilde{\mathcal{A}}_v$. But from Proposition 2.59

$$\int_{\mathcal{A}_v(\mathcal{O}_v)} |w|_v d\mu_v = q_v^{-d} v_w |\tilde{\mathcal{A}}_v(k_v)|.$$

By combining these two results we get the statement of the lemma. □

Remark 2.62. By the Néron mapping property, there exists a homeomorphism of topological spaces $\mathcal{A}_v(\mathcal{O}_v) \cong A(K_v)$. If w is an invariant differential on $\mathcal{A}$, then w induces a Haar measure $|w|_v$ on $\mathcal{A}_v(\mathcal{O}_v)$. However, the same is obtained if we consider the invariant differential $w_K = w \times_{\mathcal{O}_K} K$ on A, which induces a Haar measure $|w_K|_v$ on $A(K_v)$. The main reasons for the introduction of the fractional ideals $\mathfrak{a}_{w_K}$ is precisely to allow the computation of the (same) integral over $A(K_v) = \mathcal{A}_v(O_v)$ by using a differential on $\mathcal{A}$ or a differential on A.

Example 2.63. Consider the elliptic curve E defined by the Weierstrass equation

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

and let $p \neq 37$. If $\mathcal{E}$ is the Néron model of E over $\mathbb{Z}$, then $\mathcal{E}_p$ consists of two fibers, each of which is an abelian variety, and is defined over $\mathbb{Z}_p$ by the (projectivized) equation $Y^2Z + YZ^2 = X^3 - XZ^3$. An invariant differential on $\mathcal{E}_p$ is given by $w = dx/(2y+1)$. Since the Weierstrass model we chose for the elliptic curve E is minimal, in the sense that the differential w comes from an invariant differential on $\mathcal{E}$, we may compute its power series expansion in the formal group $\widehat{\mathcal{E}}_p$. A detailed description of how to find the formal group law on $\widehat{\mathcal{E}}_p$ and how to compute a power series expansion for w is given in [Sil92] IV.1.1. Using the computer program MAGMA, we obtained the following power series expansion

$$\begin{aligned} \widehat{w}(t)/dt &= 1 + 2t^3 - 2t^4 + 6t^6 - 12t^7 + 6t^8 + 20t^9 - 60t^{10} + 60t^{11} + 50t^{12} - 280t^{13} + \\ &\quad +420t^{14} - 28t^{15} - 1190t^{16} + 2520t^{17} - 1596t^{18} - 4284t^{19} + 13608t^{20} + \cdots \end{aligned}$$

Integrating, we obtain

$$\begin{aligned} \log(t) &= t + \frac{1}{2}t^4 - \frac{2}{5}t^5 + \frac{6}{7}t^7 - \frac{3}{2}t^8 + \frac{2}{3}t^9 + 2t^{10} - \frac{60}{11}t^{11} + 5t^{12} + \frac{50}{13}t^{13} - 20t^{14} \\ &\quad +28t^{15} - \frac{7}{4}t^{16} - 70t^{17} + 140t^{18} - 84t^{19} - \frac{1071}{5}t^{20} + 648t^{21} + \cdots \end{aligned}$$

Since the coefficients of w are integers, the power series log converges whenever $v_p(t) > 0$. For the derivation $\partial/\partial x$ on the formal Lie algebra ($x = \log t$) we have

$$\log_*(\widehat{w})\left(\frac{\partial}{\partial x}\right) = w\left(\log^*\left(\frac{\partial}{\partial x}\right)\right) = w\left(\frac{1}{\log'(t)}\frac{\partial}{\partial t}\right) = dt\left(\frac{\partial}{\partial t}\right) = 1.$$

Therefore, the invariant differential $\log_* \widehat{w}$ is the standard derivation on the formal Lie algebra, so $(v_p)_w = 1$.

2.6.3 Behavior at Infinite Places

The problem of computing the integrals

$$\int_{A(K_v)} |w|_v,$$

when v is a real or complex place, can be done using the analytic theory of tori. For every complex embedding $\sigma_v : K \hookrightarrow \mathbb{C}$ let A^{σ_v} be the abelian variety defined by the fiber product

$$\begin{array}{ccc} A^{\sigma_v} & \longrightarrow & A \\ \downarrow & & \downarrow \\ \operatorname{Spec}\mathbb{C} & \xrightarrow{\sigma_v} & \operatorname{Spec} K \end{array}$$

Over $\mathbb{C}$, the abelian variety A^{σ_v} is abelian so $A^{\sigma_v}(\mathbb{C})$ is a complex analytic abelian Lie group. Therefore, it is topologically a complex torus and the homology group $H_1(A^{\sigma_v}(\mathbb{C}), \mathbb{Z})$ is a free $\mathbb{Z}$-module of rank $2d$ generated by $\gamma_1, \ldots, \gamma_{2d}$, where d is the dimension of the abelian variety A ([Mum70], I.1). Similarly, if v is a real place, then $H_1(A^{\sigma_v}(\mathbb{R}), \mathbb{Z})$ is the subset of $H_1(A^{\sigma_v}(\mathbb{C}), \mathbb{Z})$ fixed by complex conjugation (the nontrivial element of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$) (assume that $H_1(A^{\sigma_v}(\mathbb{R}), \mathbb{Z})$ is generated by $\gamma_1, \ldots, \gamma_d$). If we write $w = w_1 \wedge \ldots \wedge w_d$, then we may compute

$$\int_{A^{\sigma_v}(\mathbb{C})} |w|_v = \begin{vmatrix} \int_{\gamma_1} w_1 & \ldots & \int_{\gamma_1} \overline{w}_1 & \ldots \\ \int_{\gamma_2} w_1 & \ldots & \int_{\gamma_2} \overline{w}_1 & \ldots \\ & \vdots & & \\ \int_{\gamma_{2d}} w_1 & \ldots & \int_{\gamma_{2d}} \overline{w}_1 & \ldots \end{vmatrix}$$

for a complex place v and

$$\int_{A^{\sigma_v}(\mathbb{R})} |w|_v = \begin{vmatrix} \int_{\gamma_1} w_1 & \ldots & \int_{\gamma_1} w_d \\ & \vdots & \\ \int_{\gamma_d} w_1 & \ldots & \int_{\gamma_d} w_d \end{vmatrix}$$

for a real place v. Since these formulae have no immediate arithmetic significance, we will not prove them here (see, for example, [Gro82], pp.223).

Let A be an abelian variety defined over a number field K. The *period* of the abelian variety A associated to the invariant differential w is

$$P_{A,w} = \left(\prod_{v \in M_K^\infty} \int_{A^{\sigma_v}(K_v)} |w|_v \right) \prod_{v \in M_K^0} v_w.$$

If we change the invariant differential w by a scalar $\alpha \in K^\times$, then $v_{\alpha w} = |\alpha|_v v_w$ for each finite place v. Moreover, for each infinite place v we have

$$\int_{A^{\sigma_v}(K_v)} |\alpha w|_v = |\alpha|_v \int_{A^{\sigma_v}(K_v)} |w|_v.$$

Therefore,

$$P_{A,\alpha w} = \prod_v |\alpha|_v P_{A,w}.$$

But, since $\alpha \in K^\times$, we have $\prod_v |\alpha|_v = 1$, so $P_{A,w}$ is independent of w. Therefore, the real number $P_{A,w}$ is called the *period* of A and is denoted by P_A.

2.6.4 The Tamagawa Measure of $A(\mathbb{A}_K)$

Let A be an abelian variety of dimension d defined over a number field K and let w be an invariant differential on w. Let $\Lambda = \{\lambda_v\}$ to be a set of convergence factors, such that $\lambda_v = 1$ if v is an infinite place and $\lambda_v = L_v(A, 1)$ (see Corollary 2.61) if v is a finite place. Let S be a finite set of places that includes all the infinite places, all the places where A has bad reduction and all the places v such that $v_w \neq 1$. Recall that c_v is the Tamagawa number at the finite place v (Definition 2.46) and that P_A is the period of A.

Proposition 2.64. *If D_K is the discriminant of the number field K then*

$$\int_{A(\mathbb{A}_K)} d\mu_{A,w,\Lambda} = \frac{P_A \prod_{v \in M_K^0} c_v}{\sqrt{|D_K|}^d}.$$

Proof. By Proposition 1.33, the integral makes sense, since $A(\mathbb{A}_K)$ is a compact topological group. Moreover, the proof of Proposition 1.33 showed that if S is a finite set of places that includes the infinite places and all the places v where A has bad reduction, then the natural inclusion

$$A(\mathbb{A}_{K,S}) \to A(\mathbb{A}_K),$$

is a homeomorphism. Therefore, we may integrate on $A(\mathbb{A}_{K,S}) = \prod_{v \in S} A(K_v) \times \prod_{v \notin S} \mathcal{A}_v(\mathcal{O}_v)$ instead of $A(\mathbb{A}_K)$ (by Proposition 1.30) and use the measure $d\mu_{A,w,\Lambda}$ on $A(\mathbb{A}_{K,S})$:

$$\begin{aligned}
\int_{A(\mathbb{A}_K)} d\mu_{A,w,\Lambda} &= \int_{A(\mathbb{A}_{K,S})} d\mu_{A,w,\Lambda} \\
&= (\sqrt{|D_K|})^{-d} \int_{\prod_{v \in S} A(K_v) \times \prod_{v \notin S} \mathcal{A}_v(\mathcal{O}_v)} \left(\prod_{v \in M_K^\infty} |w|_v \right) \left(\prod_{v \in M_K^0} |w|_v L_v(A,1)^{-1} \right) \\
&= (\sqrt{|D_K|})^{-d} \left(\prod_{v \in M_K^\infty} \int_{A(K_v)} |w|_v \right) \left(\prod_{v \in M_K^0} \int_{\mathcal{A}_v(\mathcal{O}_v)} |w|_v L_v(A,1)^{-1} \right)
\end{aligned}$$

But, by Proposition 2.59 we have

$$\int_{\mathcal{A}_v(\mathcal{O}_v)} |w|_v = q_v^{-d} v_w |\tilde{\mathcal{A}}_v(k_v)| = q_v^{-d} v_w c_v |\tilde{\mathcal{A}}_v^0(k_v)|,$$

which by Proposition 3.10 is equal to $v_w c_v L_v(A, 1)$. Therefore, we get that

$$\int_{A(\mathbb{A}_K)} d\mu_{A,w,\Lambda} = (\sqrt{|D_K|})^{-d} \left(\prod_{v \in M_K^\infty} \int_{A(K_v)} |w|_v \right) \prod_v v_w c_v = \frac{P_A \prod_{v \in M_K^0} c_v}{\sqrt{|D_K|}^d}.$$

□

3 The Birch and Swinnerton-Dyer Conjecture

3.1 L-functions Attached to Abelian Varieties

Let A be an abelian variety of dimension d defined over a number field K. We would like to construct certain L-functions associated with the $\mathrm{Gal}(\overline{K}/K)$-representation $V_\ell A$. On the one hand, these L-functions will give a canonical set of convergence factors for the Tamagawa measure on $A(\mathbb{A}_K)$; on the other hand, we will construct a global L-function whose asymptotic behavior is part of the Birch and Swinnerton-Dyer conjecture.

3.1.1 The Local L-function

Let $\mathcal{A}$ be the Néron model of A over $\mathcal{O}_K$. Let v be a finite place of K and let ℓ be a prime number coprime to $\mathrm{char}\, k_v$ and the index of $\tilde{\mathcal{A}}_v^0$ in $\tilde{\mathcal{A}}_v$. Recall that $V_\ell A = T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = \mathrm{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A)$ which is a $\mathbb{Q}_\ell$ vector space of dimension $2d$. Let σ_v be a lift to $\mathrm{Gal}(\overline{K}_v/K_v)$ of the geometric Frobenius element in $\mathrm{Gal}(K_v^{nr}/K_v)$, and let $I_v \subset \mathrm{Gal}(\overline{K}_v/K_v)$ be the inertia at v. The group $\mathrm{Gal}(\overline{K}_v/K_v)$ acts on $\mathrm{Hom}(V_\ell A, \mathbb{Q}_\ell)$ by $(f^\sigma)(v) = f(\sigma^{-1}v)$.

However, the action of σ_v on $\mathrm{Hom}(V_\ell A, \mathbb{Q}_\ell)$ depends on the choice of lift σ_v. We can eliminate the dependence on choices if we restrict to the subrepresentation $\mathrm{Hom}(V_\ell A, \mathbb{Q}_\ell)^{I_v}$. Then, for every other choice of lift σ_v', there exists $\tau \in I_v$ such that $\sigma_v' = \tau\sigma_v\tau^{-1}$, and the actions of σ_v and σ_v' on $\mathrm{Hom}(V_\ell A, \mathbb{Q}_\ell)^{I_v}$ are identical. The action of σ_v can be represented as a $(2d) \times (2d)$ matrix whose characteristic polynomial is

$$\chi_v(X) = \det(1 - \sigma_v X | \,\mathrm{Hom}(V_\ell A, \mathbb{Q}_\ell)^{I_v}).$$

Remark 3.1. A priori, the coefficients of the characteristic polynomial $\chi_v(X)$ lie in $\mathbb{Z}_\ell$, but they lie in $\mathbb{Z}$ and they do not depend on ℓ. This is essential in defining a *complex* valued, holomorphic function $L_v(A, s)$. This surprizing fact follows from the Weil conjectures ([Mil86a], Theorem 19.1)

We define the local L-function at v to be

$$L_v(A, s) = \chi_v(q_v^{-s})^{-1}.$$

To understand the local factors $L_v(A, s)$ we look at the reduction of the abelian variety at each finite place v. Let $\mathcal{A}$ be the Néron model of A over $\mathrm{Spec}\, \mathcal{O}_K$, let $\tilde{\mathcal{A}}_v$ be the special fiber of $\mathcal{A}$ over $\mathrm{Spec}\, k_v$ and let $\tilde{\mathcal{A}}_v^0$ is the connected component of the identity in $\tilde{\mathcal{A}}_v$. By Theorems 1.19 and 1.20 there exist smooth connected algebraic groups G, N, T and B such that G is affine, N is unipotent, T is a torus and B is an abelian variety, such that there exist exact sequences

$$1 \longrightarrow G \longrightarrow \tilde{\mathcal{A}}_v^0 \longrightarrow B \longrightarrow 1 \tag{3.1}$$

$$1 \longrightarrow T \longrightarrow G \longrightarrow U \longrightarrow 1$$

By Lemma 2.33, the fact that G is affine and N is unipotent implies that, on the level of Tate modules we have an exact sequence

$$1 \to V_\ell T \to V_\ell \tilde{\mathcal{A}}_v^0 \to V_\ell B \to 1. \tag{3.2}$$

For any $\mathrm{Gal}(\overline{K}_v/K_v)$-module M, let $M(n)$ be the $\mathrm{Gal}(\overline{K}_v/K_v)$-module whose underlying set is M, but whose action is $\tau\sigma_v^k(m) = \tau(q_v^{kn}m)$, where $\tau \in I_v$ and $\sigma_v \in \mathrm{Gal}(K_v^{\mathrm{nr}}/K_v)$ is the Frobenius. Then $M(n)$ is called the n-twist of M. For example, if $\mathbb{Q}_\ell$ is the trivial module, then $\mathbb{Q}_\ell(1) = \varprojlim \mu_{\ell^n}$.

Lemma 3.2. *There exists an isomorphism of* $\mathrm{Gal}(\overline{K}/K)$*-module* $\mathrm{Hom}(V_\ell A, \mathbb{Q}_\ell) \cong V_\ell A^\vee(-1) \cong V_\ell A(-1)$.

Proof. Recall that the Weil pairing

$$e_\ell : V_\ell A \times V_\ell A^\vee \to \varprojlim_n \mu_{\ell^n} \otimes \mathbb{Q}_\ell = \mathbb{Q}_\ell(1),$$

is a perfect $\mathrm{Gal}(\overline{K}/K)$-invariant pairing which induces an isomorphism of $\mathrm{Gal}(\overline{K}/K)$-modules

$$\mathrm{Hom}(V_\ell A, \mathbb{Q}_\ell(1)) \cong V_\ell A^\vee \Longrightarrow \mathrm{Hom}(V_\ell A, \mathbb{Q}_\ell) \cong V_\ell A^\vee(-1).$$

But A and $A^\vee$ are isogenous so $V_\ell A \cong V_\ell A^\vee$, which implies that $\mathrm{Hom}(V_\ell A, \mathbb{Q}_\ell) \cong V_\ell A(-1)$, as $\mathrm{Gal}(\overline{K}/K)$-modules. □

Using the exact sequence 3.2, the previous lemma allows us to compute the local $L_v(A, s)$ in terms of the analogously defined L-factors for the torus T and abelian variety B.

Proposition 3.3. *If A, T and B are defined as above, then*

$$\chi_v(A, X) = \det(1 - \sigma_v X | V_\ell B(-1)) \det(1 - \sigma_v X | V_\ell T(-1)).$$

Proof. Twisting the exact sequence 3.2 by (-1) we get

$$1 \to V_\ell T(-1) \to V_\ell \tilde{\mathcal{A}}_v^0(-1) \to V_\ell B(-1) \to 1.$$

But, by Lemma 2.50, there exists an isomorphism of $\mathrm{Gal}(\overline{K}/K)$-modules $V_\ell A^{I_v} = V_\ell \tilde{\mathcal{A}}_v^0$; since I_v acts trivially on the twist (-1), we obtain $V_\ell A^{I_v}(-1) = V_\ell \tilde{\mathcal{A}}_v^0(-1)$. Therefore,

$$1 \to V_\ell T(-1) \to V_\ell A^{I_v}(-1) \to V_\ell B(-1) \to 1,$$

which implies that

$$\det(1 - \sigma_v X | V_\ell A^{I_v}(-1)) = \det(1 - \sigma_v X | V_\ell B(-1)) \det(1 - \sigma_v X | V_\ell T(-1)),$$

and the proposition follows. □

Lemma 3.4. *Let $1 \to M \to N \to P \to 1$ be an exact sequence of algebraic groups defined over k_v, such that M is affine. Then*

$$|M(k_v)||P(k_v)| = |N(q_v)|.$$

Proof. There exists an exact sequence $1 \to M(\overline{k}_v) \to N(\overline{k}_v) \to P(\overline{k}_v) \to 1$. The $\mathrm{Gal}(\overline{k}_v/k_v)$-cohomology long exact sequence is

$$1 \to M(k_v) \to N(k_v) \to P(k_v) \to H^1(k_v, M).$$

Since M is affine, by Theorem 1.20, to show that $H^1(k_v, M) = 0$ it is enough to show that $H^1(k_v, \mathbb{G}_a)$ and $H^1(k_v, \mathbb{G}_m)$ are both trivial. But this is the statement of Hilbert's theorem 90. Therefore, $1 \to M(k_v) \to N(k_v) \to P(k_v) \to 1$ and the conclusion follows. □

Lemma 3.5. *For the abelian variety B we have $\chi_v(B, q_v^{-1}) = |B(k_v)|q^{-d_B}$ and*

$$|\chi_v(B, q_v^{-s})| \geq \left|1 - q_v^{1/2-s}\right|^{2\dim B}.$$

Proof. Let $b = \dim_{k_v} B$. By Lemma 2.54, $\chi_v(B, X) = \det(1 - \sigma_v X | \operatorname{Hom}(V_\ell B, \mathbb{Q}_\ell))$ is a degree $2b$-poynomial $\chi_v(B, X) = \prod_{i=1}^{2b}(1 - \alpha_i X)(1 - \overline{\alpha}_i X)$ with $|\alpha_i| = \sqrt{q_v}$. Therefore,

$$|\chi_v(B, q_v^{-s})| \geq \prod_{i=1}^{2b} |1 - q_v^{1/2-s}| = \left|1 - q_v^{1/2-s}\right|^{2b}.$$

But $\alpha_i/q_v = 1/\overline{\alpha}_i$ which implies that

$$\chi_v(B, q_v^{-1}) = \prod(1 - 1/\overline{\alpha}_i)(1 - 1/\alpha_i) = \prod(1 - \alpha_i)(1 - \overline{\alpha}_i)/\prod \alpha_i \overline{\alpha}_i.$$

Since $\chi_v(B, 1) = \prod(1 - \alpha_i)(1 - \overline{\alpha}_i)$ counts the number of fixed points of the Frobenius $\pi_B = \pi_{q_v}$ (acting on B, as in Section 2.5), we have $\chi_v(B, 1) = |B(k_v)|$. Therefore $\chi_v(B, q_v^{-1}) = |B(k_v)|q^{-\dim B}$. □

We would like to do the same computation for the torus T. Let $\widehat{T} = \operatorname{Hom}(T, \mathbb{G}_m)$ be the character group of the torus T. The action of $\mathrm{Gal}(\overline{k}_v/k_v)$ on $\widehat{T}$ is given by $({}^\sigma f)(g) = \sigma f(\sigma^{-1}(g))$, for $f : T \to \mathbb{G}_m$ and $g \in T$.

Lemma 3.6. *We have $\chi_v(T, X) = \det(1 - \sigma_v X | V_\ell T(-1)) = \det(1 - F_v X | \widehat{T} \otimes \mathbb{Q}_\ell)$, where $F_v = \sigma_v^{-1}$.*

Proof. The evaluation pairing $V_\ell T \times (\widehat{T} \otimes \mathbb{Q}_\ell) \to \mathbb{Q}_\ell(1)$ is perfect and $\mathrm{Gal}(\overline{k}_v/k_v)$-invariant. Therefore, there exists an isomorphism of $\mathrm{Gal}(\overline{k}_v/k_v)$-modules $V_\ell T(-1) \cong \operatorname{Hom}(V_\ell T, \mathbb{Q}_\ell(1)) \cong \widehat{T} \otimes \mathbb{Q}_\ell$. The result follows from the fact that the Galois action on Hom is given by $f^\sigma(x) = f(\sigma^{-1}x)$. □

Lemma 3.7. *We have* $\chi_v(T, q_v^{-1}) = |T(k_v)|/q_v^{\dim T}$.

Proof. Let $t = \dim T$. The lemma is equivalent to the fact that $\det(q_v - F_v|\widehat{T} \otimes \mathbb{Q}_\ell) = |T(k_v)|$. Since T is a torus, there exists a $\overline{k}_v$-isomorphism $\phi : T \xrightarrow{\cong} \mathbb{G}_m^t$. From the fact that $T \cong \widehat{\widehat{T}}$ we deduce (by taking Galois invariants) that the map $T(k_v) \longrightarrow \mathrm{Hom}_{\mathrm{Gal}(\overline{k}_v/k_v)}(\widehat{T}, \mathbb{G}_m)$ given by $x \mapsto (\psi_x : \xi \mapsto \xi(x))$ is an isomorphism ($T \cong \widehat{\widehat{T}}$). Therefore,

$$x \in T(k_v) \Longleftrightarrow \psi_x \in \mathrm{Hom}_{\mathrm{Gal}(\overline{k}_v/k_v)}(\widehat{T}, \mathbb{G}_m)$$

which, via $\widehat{\phi} : \widehat{\mathbb{G}}_m^t \to \widehat{T}$, is equivalent to $\psi_x \circ \widehat{\phi} \in \mathrm{Hom}_{\mathrm{Gal}(\overline{k}_v/k_v)}(\widehat{\mathbb{G}}_m^t, \mathbb{G}_m)$.

The idea is to use linear algebra to compute the characteristic polynomial of F_v and for this we need to pass from the $\mathbb{Z}$-module $\mathrm{Hom}_{\mathrm{Gal}(\overline{k}_v/k_v)}(\widehat{\mathbb{G}}_m^t, \mathbb{G}_m)$ to a vector space. One way to achieve this is to tensor with $\mathbb{Q}_\ell$. The condition that $x \in T(k_v)$ is equivalent to

$$\psi_x \circ \widehat{\phi} \otimes 1 \in \mathrm{Hom}_{\mathrm{Gal}(\overline{k}_v/k_v)}(\widehat{\mathbb{G}}_m^t \otimes \mathbb{Q}_\ell, \mathbb{G}_m \otimes \mathbb{Q}_\ell).$$

Since $\mathrm{Gal}(\overline{k}_v/k_v)$ is topologically generated by F_v it is enough to check that $\psi_x \circ \widehat{\phi} \otimes 1$ is fixed by F_v.

In Theorem 1.17 we defined a cocycle $h_\sigma : \sigma \mapsto \sigma(\psi)\psi^{-1} \in H^1(k_v, \mathrm{Aut}_{\overline{k}_v}(\mathbb{G}_m^t))$. Let ξ_i be the standard basis of $\widehat{\mathbb{G}}_m^t$, i.e., $\xi_i(x_1, \ldots, x_d) = x_i$ for all i. Since h_{F_v} is an automorphism of $\mathbb{G}_m^t$, the map $\widehat{h}_{F_v}$ defines an automorphism of $\widehat{\mathbb{G}}_m^t$ so $\widehat{h}_{F_v} \otimes 1 \in \mathrm{Aut}(\widehat{\mathbb{G}}_m^t \otimes \mathbb{Q}_\ell)$. Then

$$\det(q_v - F_v|\widehat{T} \otimes \mathbb{Q}_\ell) = \det(q_v - \widehat{h}_{F_v} \otimes 1).$$

In terms of the standard basis on $\widehat{\mathbb{G}}_m^t$ we can write $\widehat{h}_{F_v}(\xi_i) = \sum_j h_{ij}\xi_j$ with $h_{ij} \in \mathbb{Z}$. The condition that F_v fixes $\psi_x \circ \widehat{\phi} \otimes 1$ is equivalent to $\widehat{h}_{F_v} \otimes 1$ fixing $\psi_x \circ \widehat{\phi} \otimes 1$, i.e., for every $\xi \in \widehat{\mathbb{G}}_m^t$ we have

$$F_v((\psi_x \circ \widehat{\phi} \otimes 1)(\xi \otimes 1)) = (\psi_x \circ \widehat{\phi} \otimes 1)(\widehat{h}_{F_v}\xi \otimes 1).$$

This can be checked at each basis element ξ_i in which case we need

$$F_v((\psi_x \circ \widehat{\phi})(\xi_i) \otimes 1) = (\psi_x \circ \widehat{\phi})(\sum_j h_{ij}\xi_j) \otimes 1 = \prod_j (\psi_x \circ \widehat{\phi})(\xi_j)^{h_{ij}} \otimes 1.$$

Write $\phi(x) = (x_1, \ldots, x_d) \in \mathbb{G}_m^t$. The advantages of the formula above is that it takes the problem of finding points in $T(k_v)$ to finding points on $\mathbb{G}_m^t$. Note that $(\psi_x \circ \widehat{\phi})(\xi_i) = x_i$ (because $\xi_i(\phi(x)) = x_i$) which implies that $\prod_j (x_j \otimes 1)^{h_{ij}} = (x_i \otimes 1)^{q_v}$.

Therefore, to count $T(k_v)$ we only need to count $(x_1, \ldots, x_n) \in \mathbb{G}_m^t$ such that $\prod_j (x_j \otimes 1)^{h_{ij}} = (x_i \otimes 1)^{q_v}$ for all i. Observe that $\mathbb{G}_m^t \otimes \mathbb{Q}_\ell$ is a $\mathbb{Q}_\ell$-vector space; by diagonalizing the matrix $q_v I_t - (h_{ij})$, the number of such solutions is equal to the determinant of the matrix $q_v I_d - (h_{ij})$ ([Ono61], 1.2.6). □

Lemma 3.8. *If N is a nilpotent group defined over k_v then $|U(k_v)| = q_v^{\dim U}$.*

Proof. By [Gro64], Exp. 17, Lemma 2.3, the group N has a composition series with successive quotients isomorphic to $\mathbb{G}_a$. But $|\mathbb{G}_a(k_v)| = q_v$ so by Lemma 3.4 we get that $|N(k_v)| = \prod_{i=1}^{\dim N} |\mathbb{G}_a(k_v)| = q_v^{\dim N}$. □

Example 3.9. Let E be an elliptic curve and let v be a finite place. If v is a place of good reduction and if B is the reduced elliptic and $\det(1 - \pi_B q_v^{-s}) = 1 - a_v q_v^{-s} + q_v^{1-2s}$, giving the usual L_v-factor at primes of good reduction for elliptic curves. If E has additive reduction at v, then Proposition 3.3 shows that $L_v(E, s) = 1$.

Assume that E has multiplicative reduction at v. Then the toric part of the reduction is 1-dimensional so by Example 1.18, T is either $\mathbb{G}_m$ or $R^1_{l_v/k_v}\mathbb{G}_m$, where l_v/k_v is a degree 2 extension. If E has split reduction then $\mathbb{T} \cong \mathbb{G}_m$ and the L_v-factor is given by $\det(1 - F_v q_v^{-s} | \widehat{\mathbb{G}}_m)^{-1} = (1 - q_v^{-s})^{-1}$. If E has nonsplit reduction then $\mathbb{T} \cong R^1_{l_v/k_v}\mathbb{G}_m$ and so L_v is given by $\det(1 - F_v q_v^{-s} | \widehat{R}^1_{l/k}\mathbb{G}_m)^{-1} = (1 + q_v^{-s})^{-1}$.

Proposition 3.10. *For all finite places v of K we have $L_v(A, 1) = q_v^{\dim \tilde{A}_v^0} / |\tilde{A}_v^0(k_v)|$.*

Proof. By Lemma 3.4 and the two exact sequences 3.1 we have $|\tilde{\mathcal{A}}_v^0(k_v)| = |N(k_v)||T(k_v)||B(k_v)|$. Combining the results from Lemmas 3.5, 3.7 and 3.8 we get

$$\begin{aligned} \frac{|\tilde{A}_v^0(k_v)|}{q_v^{\dim \tilde{A}_v^0}} &= \frac{|B(k_v)||T(k_v)||U(k_v)|}{q_v^{\dim B + \dim T + \dim U}} \\ &= \chi_v(B, q_v^{-1})\chi_v(T, q_v^{-1}) = \chi_v(A, q_v^{-1}) \\ &= L_v(A, 1)^{-1} \end{aligned}$$

□

3.1.2 Global L-function

The local $L_v(A, s)$ factors encode information at each finite place v. In order to get global information about the abelian variety A, we define the global L-function to be

$$L(A, s) = \prod_v L_v(A, s),$$

where the product is taken over all finite places v. One could define local L-factors at the infinite places, using variants of the Euler Γ-function. However, such factors are useful for possible functional equations satisfied by the global L-function, and do not encode relevant arithmetic data (for a discussion of the local L-factors at infinite places, see [Tay02]).

Lemma 3.11. *The function $L(A, s)$ converges absolutely to a holomorphic function for* $\mathrm{Re}\, s > 3/2$.

Proof. For all but finitely many places v, the abelian variety A has good reduction, so the analytic behavior of L is determined by the product of the local $L_v(A, s)$, such that A has

good reduction at v. By Lemma 3.5 we have $|\chi_v(A, q_v^{-s})| \geq |1 - q_v^{1/2-s}|^{2d}$ for all v of good reduction for A. Therefore, the analytic behavior of $L(A, s)$ is the same as that of

$$\prod_v |1 - q_v^{1/2-s}|^{-2d} = \zeta_K(s - 1/2)^{2d}.$$

Therefore, $L(A, s)$ is holomorphic when $\mathrm{Re} s > 3/2$. □

The basic conjecture regarding the L-function is

Conjecture 3.12. *If K is a number field and A is an abelian variety over K then there exists an analytic continuation of $L(A, s)$ to the whole plane $\mathbb{C}$.*

Remark 3.13. In the case when K is a function field then it is known that $L(A, s)$ is meromorphic on $\mathbb{C}$. In the case of number fields K, the conjecture is proven for elliptic curves defined over $K = \mathbb{Q}$, a fact that follows from the Modularity Theorem ([BCDT00]).

3.2 The Conjecture

The Birch and Swinnerton-Dyer conjecture relates the behavior of the global L-function and the arithmetic properties of the abelian variety.

Conjecture 3.14 (Birch and Swinnerton-Dyer, weak form)**.** *Let A be an abelian variety defined over a number field K and let $L(A, s)$ be the global L-function of A. Then the order of vanishing of L at 1 is equal to r, the rank of A.*

Birch and Swinnerton-Dyer went further and conjectured what the coefficient of the first term in the Taylor expansion of $L(A, s)$ around 1 should be:

Conjecture 3.15 (Birch and Swinnerton-Dyer, strong form)**.** *Let A be an abelian variety of rank r defined over a number field K. Let $L(A, s)$ be the global L-function of A, let $A(K)_{\mathrm{tors}}$ and $A^\vee(K)_{\mathrm{tors}}$ be the torsion subgroups of $A(K)$ and $A^\vee(K)$ respectively. Let R_A be the regulator of A, and let $Ш(A/K)$ be the Shafarevich-Tate group. Then $Ш(A/K)$ is a finite group and*

$$\frac{L^{(r)}(A, 1)}{r! \int_{A(\mathbb{A}_K)} d\mu_{A,w,\Lambda}} = \frac{R_A |Ш(A/K)|}{|A(K)_{\mathrm{tors}}||A^\vee(K)_{\mathrm{tors}}|}.$$

This statement of the conjecture is not effective from a computational perspective. By Proposition 2.64 we may rewrite the formula as

$$\frac{1}{r!} L^{(r)}(A, 1) = \frac{P_A R_A |Ш(A/K)| \prod_{v \in M_K^0} c_v}{\sqrt{|D_K|}^d |A(K)_{\mathrm{tors}}||A^\vee(K)_{\mathrm{tors}}|}.$$

This statement of the conjecture is extremely useful because it gives a computationally effective method of computing the size of $Ш(E/K)$ in the case of elliptic curves E defined over $\mathbb{Q}$, which in turn gives an upper bound on the running time of an algorithm that

computes generators for the Mordell-Weil group $E(\mathbb{Q})$ (algorithms for computing each of the other quantities in the formula are discussed in [Cre97]).

Conjecture 3.14 was proven in the case of elliptic curves of analytic rank 0 or 1 (i.e., order of vanishing of the L-function 0 or 1) by combining the Modularity theorem ([BCDT00]), the work of Gross and Zagier ([GZ86]) and that of Kolyvagin on Euler systems ([Gro91]). In most other cases, little is known. However, there are theorems about the consistency of the conjecture. If $A \to B$ is an isogeny, then Conjecture 3.15 is true for A if and only if it is true for B. To prove such a theorem one cannot use the above form of the conjecture, since the Néron model of an abelian variety (and implicitly the Tamagawa numbers at finite places) does not behave well under isogenies.

What does behave well under isogeny is the set of places where an abelian variety has good reduction (Corollary 2.53). So choose S a finite set of places that includes the set of infinite places, the places of bad reduction and the places where $v_w \neq 1$. We will define a new set of convergence factors for the Tamagawa measure on $A(\mathbb{A}_K)$ by $\Lambda_S = \{\lambda_v\}$ such that $\lambda_v = 1$ if $v \in S$ and $\lambda_v = L_v(A,1)$ if $v \notin S$. Thus we obtain a measure $d\mu_{A,w,\Lambda_S}$ such that

$$\int_{A(\mathbb{A}_K)} d\mu_{A,w,\Lambda} = \left(\prod_{v \in S \cap M_K^0} L_v(A,1) \right) \int_{A(\mathbb{A}_K)} d\mu_{A,w,\Lambda_S}.$$

Let $L_S(A,s) = \prod_{v \notin S} L_v(A,s)$, which has the same analytic behavior as $L(A,s)$ since we simply took out a finite product of nonvanishing, holomorphic functions.

Proposition 3.16. *Conjecture 3.15 is equivalent to*

$$\frac{L_S^{(r)}(A,1)}{r! \int_{A(\mathbb{A}_{K,S})} d\mu_{A,w,\Lambda_S}} = \frac{R_A |Ш(A/K)|}{|A(K)_{\text{tors}}||A^\vee(K)_{\text{tors}}|}.$$

Proof. Since $A(\mathbb{A}_{K,S}) = A(\mathbb{A}_K)$, it is enough to show that $L^{(r)}(A,1) = \left(\prod_{v \in S \cap M_K^0} L_v(A,1) \right) L_S^{(r)}(A,1)$.

We have

$$\begin{aligned} L^{(r)}(A,1) &= \left(\left(\prod_{v \in S \cap M_K^0} L_v(A,s) \right) L_S(A,s) \right)^{(r)} |_{s=1} \\ &= \sum_{i=0}^{r} \left(\prod_{v \in S \cap M_K^0} L_v(A,s) \right)^{(i)} (L_S(A,s))^{(r-i)} |_{s=1} \end{aligned}$$

But Conjecture 3.14 implies that the order of vanishing of $L_S(A,s)$ at 1 is r so $(L_S)^{(r-i)}(A,1) = 0$ if $r \neq 0$ and the proposition follows immediately. □

Conjectures 3.15 and 3.16 do not generally appear together in the literature. With the machinery already developed, the proof was straightforward. However, it required the prior careful analysis of the structure of the local L-factors and of the local integrals.

4 Global Number Theory

The fact that Conjecture 3.15 encodes so much arithmetic data implies that any proof involving the conjecture would require a large number of global number theoretic results. In order to prove that the conjecture is invariant under isogenies, one needs to use global Tate-Poitou duality and the global Euler-Poincare characteristic. First, we develop the necessary machinery to be able to manipulate long exact sequences of Ext. Then we derive the global results we will use to prove the invariance under isogeny.

4.1 Derived Functors

The absolute Galois group of a number field K, $\mathrm{Gal}(\overline{K}/K)$, is rather mysterious. It is a topological profinite group, i.e., it is Hausdorff, compact and totally disconnected. However, its structure is not fully understood. In fact, most information about $\mathrm{Gal}(\overline{K}/K)$ can be obtained not by studying its structure, but by studying representations of it, i.e., continuous maps

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(V)$$

for some (finite dimensional) vector space V. More generally, if G is a group, $\mathbb{Z}[G]$, the free group whose generators are elements of G, is a noncommutative ring that can act on a set M. If the action of G on M is continuous, we say that M is a continuous $\mathbb{Z}[G]$-module, or simply, a continuous G-module. Let $\mathbf{Mod}_G$ be the category of continuous G-modules.

The most efficient strategy in studying the representations of a group G is to associate to each representation an invariant. For example, a covariant functor F from $\mathbf{Mod}_G$ to the category of abelian groups is an example of such an invariant. More often than not, the functor F is not exact in the sense that given an exact sequence $1 \to M \to N \to P \to 1$ of continuous G-modules, the corresponding sequence $1 \to F(M) \to F(N) \to F(P)$ is not right exact.

Example 4.1. Let $G = \{-1, 1\}$ acting by multiplication on the sets $M = N = \mathbb{Z}$ and $P = \mathbb{Z}/2\mathbb{Z}$. Consider the functor F from $\mathbf{Mod}_G$ to the category of abelian groups, $F(X) = X^G$, taking a module X to the G-invariant submodule. Then $F(\mathbb{Z}) = \{0\}$, since G acts by inverting the sign. However, $F(\mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$ since $-1 = 1$ in $\mathbb{Z}/2\mathbb{Z}$. Therefore the exact sequence $1 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 1$ becomes $1 \to 1 \to 1 \to \mathbb{Z}/2\mathbb{Z}$, which is not exact.

Definition 4.2. The k-th *right derived functor* of F is a functor R^rF from $\mathbf{Mod}_G$ to the category of abelian groups such that for every exact sequence $1 \to M \to N \to P \to 1$ of continuous G-modules, we get a long exact sequence

$$1 \to F(M) \to F(N) \to F(P) \to R^1F(M) \to R^1F(N) \to R^1F(P) \to R^2F(M) \to \cdots$$

Example 4.3. If G is a group and F is the functor that takes $X \in \mathbf{Mod}_G$ to X^G, then $R^rF(X)$ is none other than the usual group cohomology $H^r(G, X)$.

If the functor F is contravariant, meaning that a map $M \to N$ induces a map $F(N) \to F(M)$ (in the other direction), then one can define the notion of *left derived functor* in the same way.

Let G be a group. Then, the functor $F(X) = X^G$ can be rewritten as the functor $F(X) = \mathrm{Hom}_G(\mathbb{Z}, X)$, i.e., G-invariant homomorphisms from the trivial G-module $\mathbb{Z}$ to the G-module X. More generally, for a continuous G-module M, the functor $F_M(X) = \mathrm{Hom}_G(M, X)$ taking X to G-invariant homomorphisms from M to X is covariant.

Definition 4.4. Let $\mathrm{Ext}^r_G(M, -)$ be the k-th derived functor of F_M.

Remark 4.5. If $M = \mathbb{Z}$ has trivial G-action, then $\mathrm{Ext}^r_G(M, X) = H^r(G, X)$, since $\mathrm{Hom}_G(\mathbb{Z}, X)$ and X^G are the same functor. The quickest way to compute $\mathrm{Ext}^r_G(M, N)$ is to use injective resolutions. Let

$$N^* : 1 \to N^0 \to N^1 \to N^2 \to \cdots$$

be an injective resolution of N. Since $\mathrm{Hom}_G(M, -)$ is covariant, we obtain a resolution

$$1 \to \mathrm{Hom}_G(M, N^0) \xrightarrow{i_1} \mathrm{Hom}_G(M, N^1) \xrightarrow{i_2} \mathrm{Hom}_G(M, N^2) \to \cdots .$$

Then $\mathrm{Ext}^*_G(M, -)$ is simply the cohomology of the complex $\mathrm{Hom}_G(M, N^*)$, i.e., $\mathrm{Ext}^r = \ker i_r / \mathrm{Im} i_{r-1}$. A quick corollary of this fact is that if M, N and P are continuous G-modules, then

$$\mathrm{Ext}^r_G(M, N \oplus P) = \mathrm{Ext}^r_G(M, N) \oplus \mathrm{Ext}^r_G(M, P)$$

Example 4.6. As an application of the previous remark, we will show that if M and N are abelian groups then for every $r \geq 2$ we have $\mathrm{Ext}^r_{\{1\}}(M, N) = 0$. Indeed, let N^1 be an injective module such that $0 \to N \to N^1$. If N^2 is the cokernel of the inclusion, then it is also injective (see [Wei94] Lemma 3.3.1) so we get an injective resolution $0 \to N \to N^1 \to N^2 \to 0$. Therefore, $\mathrm{Ext}^r_{\{1\}}(M, N)$ is the cohomology of the complex

$$0 \to \mathrm{Hom}(M, N^1) \to \mathrm{Hom}(M, N^2) \to 0.$$

Since there are only two nonzero groups in the complex, all cohomology groups in dimension $r \geq 2$ vanish.

Remark 4.7. If $M = \mathbb{Z}$, the previous remark shows that we may compute the cohomology groups $H^r(G, -)$ by using injective resolutions. Such a computation could also be taken as a definition. However, in that case, the fact that $H^r(G, -)$ is the r-th derived functor of $F(X) = X^G$ would no longer be clear. To show that the cohomology of the complex $\mathrm{Hom}_G(\mathbb{Z}, N^*)$ does indeed give the derived functors of $\mathrm{Hom}_G(\mathbb{Z}, N)$, we need the following general fact about cohomology (see [Wei94] 1.3). Consider a commutative diagram with

exact columns, such that the rows are complexes, i.e., $d \circ d = 0$

$$\begin{array}{ccccccc}
 & 0 & & 0 & & 0 & \\
 & \downarrow & & \downarrow & & \downarrow & \\
\xrightarrow{d} & A_{k-1} & \xrightarrow{d} & A_k & \xrightarrow{d} & A_{k+1} & \xrightarrow{d} \\
 & \downarrow & & \downarrow & & \downarrow & \\
\xrightarrow{d} & B_{k-1} & \xrightarrow{d} & B_k & \xrightarrow{d} & B_{k+1} & \xrightarrow{d} \\
 & \downarrow & & \downarrow & & \downarrow & \\
\xrightarrow{d} & C_{k-1} & \xrightarrow{d} & C_k & \xrightarrow{d} & C_{k+1} & \xrightarrow{d} \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & 0 & & 0 & & 0 &
\end{array}$$

We may construct the cohomologies of each complex $H^r = \ker d / \mathrm{Im} d$. Then H^r is a derived functor in the sense that there exists a long exact sequence

$$1 \to H^0(A) \to H^0(B) \to H^0(C) \to H^1(A) \to \cdots$$

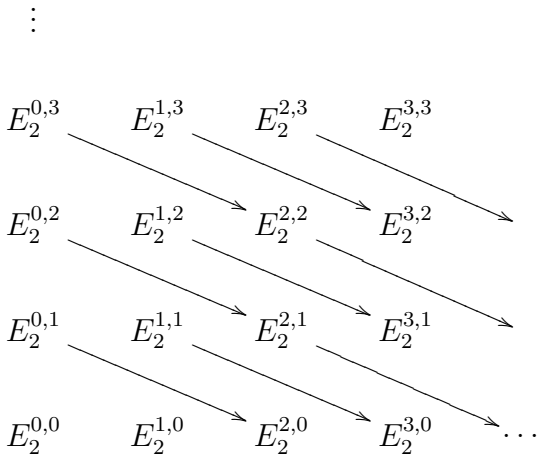
A similar functor to $\mathrm{Hom}_G(M, -)$ is the functor $- \otimes_{\mathbb{Z}[G]} N$ for a continuous G-module N. However, this functor is contravariant. Define $\mathrm{Tor}_k^G(-, N)$ to be the k-th *left* derived functor of the functor $- \otimes_{\mathbb{Z}[G]} N$. Again, Tor can be computed in a similar fashion to Ext, but now by choosing a projective resolution $\cdots \to N^2 \to N_1 \to N_0 = N \to 0$ and taking $\mathrm{Tor}_r^G(M, N)$ to be the homology of the complex $M \otimes_{\mathbb{Z}[G]} N_*$.

If H is a normal and closed subgroup of G then G/H is a topological profinite group and we may naturally endow $\mathrm{Ext}_H^r(M, N)$ with the structure of G/H module by letting $\sigma \in G/H$ act on $f \in \mathrm{Hom}_H(M, N)$ by $\sigma f : m \mapsto \sigma f(\sigma^{-1} m)$. If M is finite, then $\mathrm{Ext}_H^r(M, N)$ is a continuous module. Otherwise, define $\widehat{\mathrm{Ext}}_H^r(M, N) = \cup_{H \subset U \subset G} \mathrm{Ext}_H^r(M, N)^U$ to be the continuous submodule of $\mathrm{Ext}_H^r(M, N)$.

For every continuous H-module N, we define the *induction* $\mathrm{Ind}_H^G N = \{f : G \to N | f(hg) = h(f(g)), \forall h \in H\}$ to be a set with a G-action given by ${}^g f(x) = f(xg)$. The induction is a continuous G-module and for every G-module M we have $\mathrm{Hom}_G(M, \mathrm{Ind}_H^G N) = \mathrm{Hom}_H(M, N)$ (Frobenius reciprocity). Since the two functors are equal, their right derived functors must be equal as well, hence there exists an isomorphism $\mathrm{Ext}_G^r(M, \mathrm{Ind}_H^G N) \cong \mathrm{Ext}_H^r(M, N)$.

As usual for derived functors, there exists a Grothendieck spectral sequence for the $\mathrm{Ext}_G^r(M, N)$. Spectral sequences are an extremely useful tool for determining right derived functors, such as Ext^* and H^*. A spectral sequence is consists of a set of abelian groups $E_r^{p,q}$ for $r \geq 2$ and $(p, q) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ and derivations $d : E_r^{p,q} \to E_r^{p+r, q-r+1}$ (derivation simply means that $d \circ d = 0$) such that $E_{r+1}^{p,q}$ can be obtained as the cohomology group of the complex $E_r^{p+kr, q-k(r-1)}$. For each p and q, there exists r_0 such that if $r > r_0$ then $E_r^{p,q} = E_{r-1}^{p,q}$. This occurs when the derivations that go in and out of $E_r^{p,q}$ are the 0 maps

(so $r_0 = p + q$ works). Denote this constant sequence of groups by $E^{p,q}$. To say that there exists a spectral sequence $E_2^{p,q} \Longrightarrow E^{p+q}$ simply means that for each $n \geq 0$, there exists a composition series of E^n with successive quotients equal to $E^{p,n-p}$. While a full description of spectral sequences and their techniques of computation would diverge too much from the purpose of this section, it is worthwhile to mention the similarity between the Grothendieck spectral sequence $R^iF \circ R^jG \Longrightarrow R^{i+j}F \circ G$ and the classical Leibniz rule for differentiation $d^n(fg) = \sum_{i=0}^{n} d^i(f)d^{n-i}(g)$. It is much easier to deal with spectral sequences visually



Thus, the fact that $E_2^{p,q} \Longrightarrow E^{p+q}$ can be interpreted as: for r sufficiently large, E^n has a composition series whose successive quotients are elements $E_r^{p,q}$ on the diagonal $p + q = n$. For certain groups $E_2^{p,q}$ it is particularly easy to compute E^{p+q}, since it may happen that all $E_2^{p,q} = 0$ for $q > 0$ (as it does in Lemma 4.11).

Proposition 4.8. *Let H be a normal closed subgroup of G, let N, P be G-modules and let M be a G/H-module such that $\mathrm{Tor}_{\mathbb{Z}}^1(M, N) = 0$. Then there exists a spectral sequence*

$$\mathrm{Ext}_{G/H}^r(M, \widehat{\mathrm{Ext}}_H^s(N, P)) \Longrightarrow \mathrm{Ext}_G^{r+s}(M \otimes_{\mathbb{Z}} N, P).$$

Proof. See [Mil86a], Theorem 0.3. □

4.2 Duality

All G-modules are assumed to be continuous. Let μ_∞ represent the group of roots of unity. For a $\mathrm{Gal}(L/K)$-module M we will write $M^* = \mathrm{Hom}(M, \mu_\infty)$ and $M^\vee = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z})$ and $\widehat{M} = \mathrm{Hom}(M, \mathbb{G}_m)$ for the Pontryjagin dual of M. If M is a G-module, each of $M^*, M^\vee$ and $\widehat{M}$ can be turned into a G-module, by letting ${}^\sigma f(x) = \sigma f(\sigma^{-1}x)$, where the action of G on the image space is determined on a case-by-case basis. (For example, if $G = \mathrm{Gal}(\overline{K}/K)$ then the G-action on $\mathbb{G}_m$ is simply the action of $\mathrm{Gal}(\overline{K}/K)$ on $\overline{K}^\times$.)

Let K be a number field. Duality in the context of arithmetic has been inspired by duality theorems (such as Poincare duality) in the care of smooth compact manifolds.

4.2.1 Local Duality

Let v be a finite place of K and let M be a $\mathrm{Gal}(\overline{K}_v/K_v)$-module. Then $H^r(K_v, M) = 0$ for $r \geq 3$ and there exists a pairing

$$H^r(K_v, M) \times H^{2-r}(K_v, M^*) \xrightarrow{\cup} H^2(K_v, M \otimes M^*) \to \mathbb{Q}/\mathbb{Z}$$

given by $\langle f, g \rangle_v = \mathrm{inv}_v(f \cup g)$, where inv_v are the invariant maps of local class field theory. For proofs of the following two theorems, see [NSW00] Theorem 7.2.6.

Theorem 4.9 (Local Tate Duality)**.** *The pairing*

$$\langle , \rangle_v : H^r(K_v, M) \times H^{2-r}(K_v, M^*) \to \mathbb{Q}/\mathbb{Z}$$

is perfect.

If v is complex, the groups $H^r(K_v, -)$ are trivial. If v is real, $H^r(K_v, -)$ are finite for finite $\mathrm{Gal}(\overline{K}_v/K_v)$-modules. There is a pairing

$$\langle , \rangle_{\mathbb{R}} : H^r(K_v, M) \times H^{2-r}(K_v, M^*) \to \mathbb{Q}/\mathbb{Z},$$

given by the $\cup$ product (since $H^2(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^\times) \cong \mathbb{Z}/2\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$). The pairing defined for these cohomology groups is degenerate when $r = 0, 2$. For every infinite place v, write $\widehat{H}^r(K_v, M) = M^{\mathrm{Gal}(\overline{K}_v/K_v)}/N_{\overline{K}_v/K_v} M$ if $r = 0$ and $\widehat{H}^r(K_v, M) = H^r(K_v, M)$ if $r > 0$. To ease notation we will write $\widehat{H}^0(K_v, M) = H^0(K_v, M)$ whenever v is a finite place.

Theorem 4.10. *The pairing*

$$\langle , \rangle_v : \widehat{H}^r(K_v, M) \times \widehat{H}^{2-r}(K_v, M^*) \to \mathbb{Q}/\mathbb{Z}$$

is nondegenerate.

If we continue the analogy with the case of topological duality, Theorem 4.9 implies that local fields behave like complex curves. This is not the case for number fields, as we shall see in the next section.

4.2.2 Global Duality

Let K be a number field and let S be a finite set of places that includes all infinite places. Let K_S be the maximal algebraic extension of K that is unramified at all places $v \notin S$ and let $G_S = \mathrm{Gal}(K_S/K)$. We will denote the finite sum $\oplus_{v \in S} K_v^\times \otimes \overline{K}^\times$ by I^S and we will write $C_S = I^S/\mathcal{O}^\times_{\overline{K},S}$. Then, there exists an exact sequence

$$0 \to \mathcal{O}^\times_{\overline{K},S} \to I^S \to C_S \to 0.$$

The construction of the 9-term global duality long exact sequence in Theorem 4.15 requires global class field theory and an analysis of the Ext long exact sequences that arise from the

short exact sequence $0 \to \mathcal{O}_{\overline{K},S} \to I^S \to C_S \to 0$. The particular case of interest for global duality is the case of $\mathrm{Gal}(K_S/K)$-modules M such that no place of S divides $|M|$. Before we write down the $\mathrm{Ext}_{G_S}(M,-)$-long exact sequence for the short sequence above, we would like to compute the Ext-groups separately. Since the proofs of these computations are somewhat lengthy, technical and unrevealing, we will only prove the first lemma, as an example of the general method of proof using spectral sequences.

Lemma 4.11. *Let M be a finite $\mathrm{Gal}(K_S/K)$-module and let $\widehat{M} = \mathrm{Hom}(M, \mathcal{O}^\times_{\overline{K},S})$, where the $\mathrm{Gal}(K_S/K)$-action on $\mathcal{O}^\times_{\overline{K},S}$ is given by the action of G_S on $\mathcal{O}^\times_{\overline{K},S}$. If S contains all the infinite places and all the places dividing $|M|$ then*

$$\mathrm{Ext}^r_{G_S}(M, \mathcal{O}^\times_{\overline{K},S}) = H^r(G_S, \widehat{M})$$

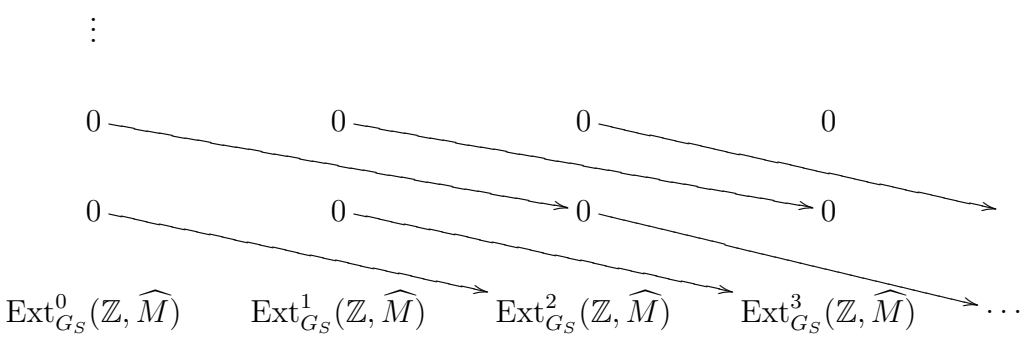
for $r \geq 0$.

Proof. The proof is nothing more than an exercise in interpreting the spectral sequence in Proposition 4.8. If we apply Proposition 4.8 to the closed subgroup 1 of G_S and the trivial G_S-module $\mathbb{Z}$ (in which case the hypothesis of Proposition 4.8 is satisfied) we get

$$E_2^{r,s} = \mathrm{Ext}^r_{G_S}(\mathbb{Z}, \widehat{\mathrm{Ext}}^s_1(M, \mathcal{O}^\times_{\overline{K},S})) \Longrightarrow \mathrm{Ext}^{r+s}_{G_S}(M, \mathcal{O}^\times_{\overline{K},S}).$$

Since M is finite we can replace $\widehat{\mathrm{Ext}}$ by Ext. Then $H^r(G_S, \mathrm{Ext}^s_1(M, \mathcal{O}^\times_{\overline{K},S})) = \mathrm{Ext}^r_{G_S}(\mathbb{Z}, \mathrm{Ext}^s_1(M, \mathcal{O}^\times_{\overline{K},S}))$.

Since $\mathbb{Z}[1] = \mathbb{Z}$, the groups $\mathrm{Ext}^s_1(M, \mathcal{O}^\times_{\overline{K},S})$ are trivial for $r \geq 2$, by Example 4.6. Moreover, we have assumed that no place of S divides $|M|$. Thus, $|M| \in \mathcal{O}^\times_{\overline{K},S}$ and for every $\ell \mid |M|$ the roots of unity μ_ℓ are included in K_S. Consequently, raising to power ℓ is a surjection on $\mathcal{O}^\times_{\overline{K},S}$. Therefore, $\mathrm{Ext}^1(\mathbb{Z}/\ell\mathbb{Z}, \mathcal{O}^\times_{\overline{K},S}) = \mathcal{O}_{\overline{K},S}/(\mathcal{O}_{\overline{K},S})^\ell = 0$ ([Wei94] 3.3.2). Since M is a finite abelian group, this implies that $\mathrm{Ext}^1(M, \mathcal{O}^\times_{\overline{K},S}) = 0$ (by the structure theorem for finitely generated abelian groups). Finally, $\mathrm{Ext}^0(M, \mathcal{O}^\times_{\overline{K},S}) = \widehat{M}$ by definition. Thus, the spectral sequence $E_2^{r,s} \Longrightarrow E^{r+s}$ is



and so

$$H^r(G_S, \widehat{M}) \cong \mathrm{Ext}^r_{G_S}(\mathbb{Z}, \widehat{M}) \cong \mathrm{Ext}^r_{G_S}(M, \mathcal{O}^\times_{\overline{K},S}),$$

since on each diagonal in the spectral sequence, only one term is nonzero. □

Lemma 4.12. *Let M be a finite G_S-module and let $\widehat{M} = \mathrm{Hom}(M, \overline{K}^\times)$ with the usual Galois action. Then*

$$\mathrm{Ext}^r_{G_S}(M, I^S) = \oplus_{v\in S} H^r(K_v, \widehat{M})$$

Proof. See [Mil86b], Lemma 4.13. (Note that in our case, S is a finite set, so the computation is significantly simpler than in [Mil86b]).

□

Lemma 4.13. *Assume that M is a finite G_S-module such that S contains all the places dividing $|M|$. Then, for $r \in \{1, 2\}$, we have*

$$\mathrm{Ext}^r_{G_S}(M, C_S) \cong H^{2-r}(G_S, M)^\vee.$$

Proof. See [Mil86b] Theorem 4.6.a. This lemma is where global class field theory is used. □

Consider the exact sequence of G_S-modules $0 \to \mathcal{O}^\times_{\overline{K},S} \to I^S \to C_S \to 0$. The $\mathrm{Ext}_{G_S}(M, -)$-long exact sequence associated to it is

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Ext}^0_{G_S}(M, \mathcal{O}^\times_{\overline{K},S}) & \longrightarrow & \mathrm{Ext}^0_{G_S}(M, I^S) & \longrightarrow & \mathrm{Ext}^0_{G_S}(M, C_S) \\
 & & & \searrow & & & \\
 & & \mathrm{Ext}^1_{G_S}(M, \mathcal{O}^\times_{\overline{K},S}) & \longrightarrow & \mathrm{Ext}^1_{G_S}(M, I^S) & \longrightarrow & \mathrm{Ext}^1_{G_S}(M, C_S) \\
 & & & \searrow & & & \\
 & & \mathrm{Ext}^2_{G_S}(M, \mathcal{O}^\times_{\overline{K},S}) & \longrightarrow & \mathrm{Ext}^2_{G_S}(M, I^S) & \longrightarrow & \mathrm{Ext}^2_{G_S}(M, C_S)
\end{array}$$

By Lemmas 4.11, 4.12 and 4.13, this exact sequence becomes

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^0(G_S, M) & \xrightarrow{i_M} & \oplus_{v\in S} H^0(K_v, M) & \longrightarrow & \mathrm{Ext}^0_{G_S}(M, C_S) \\
 & & & \searrow & & & \\
 & & H^1(G_S, M) & \xrightarrow[f_M]{} & \oplus_{v\in S} H^1(K_v, M) & \xrightarrow{g_M} & H^1(G_S, M^*)^\vee \\
 & & & \searrow & & & \\
 & & H^2(G_S, M) & \longrightarrow & \oplus_{v\in S} H^2(K_v, M) & \xrightarrow{j_M} & H^0(G_S, M^*)^\vee
\end{array} \tag{4.1}$$

Remark 4.14. By Theorems 4.9 and 4.10, there exists an isomorphism

$$\oplus_{v\in S} H^1(K_v, M) \cong \oplus_{v\in S} H^1(K_v, M^*)^\vee.$$

Similarly, there exists an isomorphism

$$\oplus_{v\in S} \widehat{H}^0(K_v, M) \cong \oplus_{v\in S} H^2(K_v, M^*)^\vee.$$

Theorem 4.15 (Tate-Poitou)**.** *The maps $i_M : H^0(G_S, M) \to \oplus_{v\in S}\widehat{H}^0(K_v, M)$ and $j_{M^*} : \oplus_{v\in S}H^2(K_v, M^*) \to H^0(G_S, M)^\vee$ are dual to each other. The maps $f_M : H^1(G_S, M) \to \oplus_{v\in S}H^1(K_v, M)$ and $g_{M^*} : H^1(G_S, M)^\vee \to \oplus_{v\in S}H^1(K_v, M^*)$ are dual to each other. Moreover, they induce an exact sequence*

$$0 \longrightarrow H^0(G_S, M) \longrightarrow \oplus_{v\in S}\widehat{H}^0(K_v, M) \longrightarrow H^2(G_S, M^*)^\vee$$
$$H^1(G_S, M) \longrightarrow \oplus_{v\in S}H^1(K_v, M) \longrightarrow H^1(G_S, M^*)^\vee$$
$$H^2(G_S, M) \longrightarrow \oplus_{v\in S}H^2(K_v, M) \longrightarrow H^0(G_S, M^*)^\vee \longrightarrow 0$$

Proof. By algebraic dual we mean $\mathrm{Hom}(-, \mathbb{Q}/\mathbb{Z})$. First, by the previous remark, it makes sense to require that i_M and j_{M^*} be dual, and that f_M and g_{M^*} be dual, since their domains and ranges are dual. These two facts follow from [Mil86b], Theorem 4.10.

Since j_{M^*} is the algebraic dual of i_M, which is injective, the homomorphism j_{M^*} is surjective. Therefore, the long exact sequence 4.1 implies that we have an exact sequence

$$\oplus_{v\in S}H^1(K_v, M) \xrightarrow{g_M} H^1(G_S, M^*)^\vee$$
$$H^2(G_S, M) \longrightarrow \oplus_{v\in S}H^2(K_v, M) \xrightarrow{j_M} H^0(G_S, M^*)^\vee \longrightarrow 0$$

Consider the algebraic dual of the previous exact sequence, with M changed to M^*. By Remark 4.14, we get

$$0 \longrightarrow H^0(G_S, M) \xrightarrow{j^\vee_{M^*}} \oplus_{v\in S}\widehat{H}^0(K_v, M) \longrightarrow H^2(G_S, M^*)^\vee$$
$$H^1(G_S, M) \xrightarrow[g^\vee_{M^*}]{} \oplus_{v\in S}H^1(K_v, M)$$

But $f_M = g^\vee_{M^*}$ so if we put the two sequences next to each other, the new sequence will be exact at $\oplus_{v\in S}H^1(K_v, M)$, since

$$H^1(G_S, M) \xrightarrow[f_M]{} \oplus_{v\in S}H^1(K_v, M) \xrightarrow{g_M} H^1(G_S, M^*)^\vee$$

is exact in the middle by the exact sequence 4.1. This new 9-term long exact sequence is the one we needed to construct. □

4.2.3 Global Euler-Poincare Characteristic

For a finite $\mathrm{Gal}(K_S/K)$ module M write

$$\chi_S(M) = \frac{|H^0(G_S, M)||H^2(G_S, M)|}{|H^1(G_S, M)|}.$$

Theorem 4.16 (Tate)**.** *We have*

$$\chi_S(M) = \prod_{v \in M_K^\infty} \frac{|\widehat{H}^0(K_v, M^*)|}{|M|_v} = \prod_{v \in M_K^\infty} \frac{|\widehat{H}^0(K_v, M^*)|}{|H^0(K_v, M)|}.$$

Proof. The proof of this theorem is extremely technical and would take us too far afield. For a proof, see [Mil86a] or [NSW00]. □

In particular, if we replace M by M^*, since $|M| = |M^*|$ we get

$$\chi_S(M^*) = \prod_{v \in M_K^\infty} \frac{|\widehat{H}^0(K_v, M)|}{|H^0(K_v, M)|}.$$

5 Invariance Properties of the Birch and Swinnerton-Dyer Conjecture

5.1 Invariance Under Restriction of Scalars

Let L/K be a Galois extension of number fields and let A be an abelian variety defined over L. Then, by Corollary 1.12, $B = R_{L/K}A$ is also an abelian variety, isomorphic over $\overline{K}$ to $\prod A^{\sigma_i}$ as σ_i ranges over embeddings $\sigma_i : L \hookrightarrow \overline{K}$. We would like to show that Conjecture 3.15 holds for A if and only if it holds for B. For this, we need to analyze separately each of the quantities in the statement of the conjecture. In fact, it is more convenient to work with Conjecture 3.16 (which is equivalent to Conjecture 3.15).

To begin with, let S be a finite set of places of K that includes all infinite places, all places of bad reduction of B, all places lying under places of bad reduction for A and all places that ramify in L. Let T be the set of places of L that lie above places in S. There exist canonical choices of models for A and B over $\mathcal{O}_{L,T}$ and $\mathcal{O}_{K,S}$ respectively, i.e., the Néron models $\mathcal{A}$ and $\mathcal{B}$. Let w_A be an invariant differential on A and let w_B its corresponding invariant differential on B, as in Proposition 1.45. Moreover, fix the canonical sets of convergent factors $\Lambda_T = \{\lambda_w\}$, such that $\lambda_w = 1$ is $w \in T$ and $\lambda_w = L_w(A, 1)$ if $w \notin T$, and $\Lambda_S = \{\lambda'_v\}$ such that $\lambda'_v = 1$ if $v \in S$ and $\lambda'_v = L_v(B, 1)$ if $v \notin S$.

By Theorem 2.51, for each $v \notin S$ a place of K and w a place of L lying above v, there exists ℓ (sufficiently large) such that the Tate modules $V_\ell A$ and $V_\ell B$ are unramified at w and v respectively. By Remark 2.34, we have $V_\ell B \cong \mathrm{Ind}_{\mathrm{Gal}(\overline{L}/L)}^{\mathrm{Gal}(\overline{K}/K)} V_\ell A$. Therefore $V_\ell B = \{f : \mathrm{Gal}(\overline{K}/K) \to V_\ell A | f(hg) = hf(g), \forall h \in \mathrm{Gal}(\overline{L}/L)\}$ with $\mathrm{Gal}(\overline{K}/K)$ action given by ${}^{\sigma}f(g) = f(g\sigma)$. In order to get the local L-factors we need $(V_\ell A)^{I_w} = V_\ell A$ and $(V_\ell B)^{I_v} = V_\ell B$, where I_v and I_w are the inertia groups. Since v is unramified in L, we have $I_w = \mathrm{Gal}(\overline{K}_v/LK_v^{\mathrm{nr}}) = I_v \subset \mathrm{Gal}(\overline{L}/L)$.

Lemma 5.1. *With the above notation we have*

$$\det(1 - \sigma_v^{-1}X | \mathrm{Ind}_{\mathrm{Gal}(\overline{L}_w/L_w)}^{\mathrm{Gal}(\overline{K}_v/K_v)} V_\ell A) = \det(1 - \sigma_w^{-1}X^{[L_w:K_v]} | V_\ell A),$$

(where σ_w is a lift of the Frobenius ϕ_w to $Gal(\overline{L}_w/L_w)$).

Proof. Since $w \mid v$ is unramified by construction of S, the extension L_w/K_v is cyclic of order $n_w = [L_w : K_v]$ generated by σ_v^{-1}. Then

$$\mathrm{Ind}_{\mathrm{Gal}(\overline{L}_w/L_w)}^{\mathrm{Gal}(\overline{K}_v/K_v)} V_\ell A = \mathbb{Q}[\mathrm{Gal}(\overline{K}_v/K_v)] \otimes_{\mathbb{Q}[\mathrm{Gal}(\overline{L}_w/L_w)]} V_\ell A = \mathbb{Q}[\mathrm{Gal}(L_w/K_v)] \otimes V_\ell A$$

in the following sense: if $v_1, \ldots, v_{2d}$ form a $\mathbb{Q}_l$-basis for $V_\ell A$ ($d = \dim A$), then a $\mathbb{Q}_l$-basis for $\mathrm{Ind}_{\mathrm{Gal}(\overline{L}_w/L_w)}^{\mathrm{Gal}(\overline{K}_v/K_v)} V_\ell A$ is given by the $\mathrm{Gal}(\overline{L}_w/L_w)$-equivariant maps f_{ij} taking σ_v^{-i} to v_j and all the other powers of σ_v^{-1} to 0. In that case $f_{ij}^{\sigma_v^{-1}} = f_{i-1,j}$ for $i > 0$; $f_{0,j}^{\sigma_v^{-1}}$ takes $\sigma_v^{-(n_w-1)}$ to $\sigma_w^{-1}v_j$ and everything else to 0, so $f_{0,j}^{\sigma_v^{-1}}$ is a linear combination of $f_{n_w-1,j}$-s that corresponds on the σ_w^{-1} action on $V_\ell A$.

Let $H = (h_{ij})$ be the matrix of the action of σ_w^{-1} on the basis $\{v_1, \dots, v_{2d}\}$. Then, the matrix of σ_v^{-1} on $\operatorname{Ind}_{\mathrm{Gal}(\overline{L}_w/L_w)}^{\mathrm{Gal}(\overline{k}_v/k_v)} V_\ell A$ is

$$\begin{pmatrix} 0_{2d} & 0_{2d} & \dots & 0_{2d} & H \\ I_{2d} & 0_{2d} & \dots & 0_{2d} & 0_{2d} \\ 0_{2d} & I_{2d} & \dots & 0_{2d} & 0_{2d} \\ & & \vdots & & \\ 0_{2d} & 0_{2d} \dots & 0_{2d} & I_{2d} & 0_{2d} \end{pmatrix}$$

Interpretted as a matrix with entries $0, 1$ and the variable H, the characteristic polynomial is simply $I_{2d} - X^{n_w} H$. Therefore, the characteristic polynomial of the $2dn_w \times 2dn_w$ matrix is the determinant of $I_{2d} - X^{n_w} H$, i.e., the determinant $\det(1 - \sigma_w^{-1} X^{n_w} | V_\ell A)$. □

Lemma 5.2. *Let V be a $\mathrm{Gal}(\overline{L}/L)$ module (e.g., $V = V_\ell A$). If v is a finite place of K such that L and V are unramified at v, then*

$$\operatorname{Ind}_{\mathrm{Gal}(\overline{L}/L)}^{\mathrm{Gal}(\overline{K}/K)} V \cong \oplus_{w|v} \operatorname{Ind}_{\mathrm{Gal}(\overline{L}_w/L_w)}^{\mathrm{Gal}(\overline{K}_v/K_v)} V,$$

as $\mathrm{Gal}(\overline{K}_v/K_v)$-modules.

Proof. Since L/K is Galois, if $w_1, \dots, w_e$ are the places of L lying above v, then $\mathrm{Gal}(L/K)$ acts tranzitively on $\{w_1, \dots, w_e\}$, so there exist $\sigma_i \in \mathrm{Gal}(L/K)$ such that $\sigma_i w_1 = w_i$. Moreover, v is unramified in L, so all the decomposition groups $D_i = \mathrm{Gal}(L_{w_i}/K_v)$ are isomorphic, which means that $\{\sigma_1, \dots, \sigma_e\}$ form a set of representatives for $\mathrm{Gal}(L_{w_1}/K_v) \setminus \mathrm{Gal}(L/K)$. We need to show that

$$\mathbb{Q}[\mathrm{Gal}(\overline{K}/K)] \otimes_{\mathbb{Q}[\mathrm{Gal}(\overline{L}/L)]} V \cong \oplus_{w|v} \mathbb{Q}[\mathrm{Gal}(\overline{K}_v/K_v)] \otimes_{\mathbb{Q}[\mathrm{Gal}(\overline{L}_w/L_w)]} V$$

or $\mathbb{Q}[\mathrm{Gal}(L/K)] \otimes V \cong \oplus_{w|v} \mathbb{Q}[\mathrm{Gal}(L_w/K_v)] \otimes V$. This is equivalent to $\operatorname{Ind}_1^{\mathrm{Gal}(L/K)} V = \oplus_{w_i} \operatorname{Ind}_1^{D_i} V$.

Note that $\sigma \in D_1$ if and only if $\sigma_i \sigma \sigma_i^{-1} \in D_i$, so $\operatorname{Ind}_1^{D_i} V = (\operatorname{Ind}_1^{D_1} V)^{\sigma_i}$ (if ρ gives the Galois action on W, then $\rho'(x) = \rho(\sigma x \sigma^{-1})$ is the Galois action on W^σ). Therefore, we need to show that $\operatorname{Ind}_1^{\mathrm{Gal}(L/K)} V = \oplus_{\sigma_j} (\operatorname{Ind}_1^{D_1} V)^{\sigma_j}$. Consider the map $\Theta : \operatorname{Ind}_1^{\mathrm{Gal}(L/K)} V \to \oplus_{\sigma_i} (\operatorname{Ind}_1^{D_1} V)^{\sigma_i}$ that takes the function $f : \mathrm{Gal}(L/K) \to V$ (i.e., $f \in \operatorname{Ind}_1^{\mathrm{Gal}(L/K)} V$) to $\oplus_{\sigma_i} f_i$, where $f_i(x) = f(x\sigma_i)$ goes from $D_1 \to V$. Since $\{\sigma_1, \dots, \sigma_e\}$ form representatives for $D_1 \setminus \mathrm{Gal}(L/K)$, the map Θ is injective. Moreover, for $\oplus f_i \in \oplus_{\sigma_i} (\operatorname{Ind}_1^{D_1} V)^{\sigma_i}$, the function $f : \mathrm{Gal}(L/K) \to V$ given by $f(x) = f_i(x\sigma_i^{-1})$, for $x \in D_1 \sigma_i$, maps to $\oplus f_i$, via Θ. Therefore, the two sides are isomorphic.

□

Lemma 5.3. *For each $v \notin S$ a place of K and $w \mid v$ a place of L we have*

$$L_v(B, s) = \prod_{w|v} L_w(A, s).$$

Proof. Having assumed that the Tate modules $V_\ell A$ and $V_\ell B$ are unramified at w and v respectively, for ℓ large enough, we have

$$\begin{aligned} L_v(B,s)^{-1} &= \det(1-\sigma_v q_v^{-s}|\operatorname{Hom}(V_\ell B,\mathbb{Q}_\ell)) \\ &= \det(1-\sigma_v^{-1}q_v^{-s}|V_\ell B) \\ &= \det(1-\sigma_v^{-1}q_v^{-s}|\oplus_{w|v}\operatorname{Ind}_{\mathrm{Gal}(\overline{L}_w/L_w)}^{\mathrm{Gal}(\overline{K}_v/K_v)} V_\ell A) \\ &= \prod_{w|v}\det(1-\sigma_v^{-1}q_v^{-s}|\operatorname{Ind}_{\mathrm{Gal}(\overline{L}_w/L_w)}^{\mathrm{Gal}(\overline{K}_v/K_v)} V_\ell A) \\ &= \prod_{w|v}\det(1-\sigma_w^{-1}q_v^{-n_w s}|V_\ell A) \\ &= \prod_{w|v}\det(1-\sigma_w q_w^{-s}|\operatorname{Hom}(V_\ell A,\mathbb{Q}_\ell)) = \prod_{w|v} L_w(A,s) \end{aligned}$$

The second equality comes from the fact that the action of σ on $f : V_\ell B \to \mathbb{Q}_\ell$ is given by $f^\sigma(x) = f(\sigma^{-1}x)$. The third equality comes from Lemma 5.2 while the fifth equality comes from Lemma 5.1. □

In particular, for the canonical choices of sets of convergent factors Λ_T and Λ_S, by the previous lemma we have that $\prod_{w|v}\lambda_w = \lambda'_v$. In particular, the conditions of Proposition 1.45 are satisfied and $A(\mathbb{A}_{L,T}) = B(\mathbb{A}_{K,S})$ (by the restriction of scalars property) so

$$\int_{A(\mathbb{A}_{L,T})} d\mu_{A,w_A,\Lambda_T} = \int_{B(\mathbb{A}_{K,S})} d\mu_{B,w_B,\Lambda_S}.$$

We now turn to the question of rank and torsion subgroups for A and B. The following lemma shows that $R_{L/K}A^\vee = B^\vee$.

Lemma 5.4. *By definition of restriction of scalars there exists an L-morphism $\psi : B \to A$. If $\pi_i : \prod_{\sigma:L\hookrightarrow\overline{K}} A^\sigma \to A^{\sigma_i}$ is projection to the i-th factor, then the map $\mathrm{Pic}^0(A) \to \mathrm{Pic}^0(B)$ given by $R_{L/K} : \mathcal{L} \mapsto \otimes\psi^*\pi_i^*(\mathcal{L}^{\sigma_i}) \in \mathrm{Pic}^0(B)$ is an isomorphism.*

Proof. See [Mil72]. □

Corollary 5.5. *There exist equalities of groups $A(L) = B(K)$ and $A^\vee(L) = B^\vee(K)$. Moreover, the ranks of A and B are equal, $|A(L)_{\mathrm{tors}}| = |B(K)_{\mathrm{tors}}|$ and $|A^\vee(L)_{\mathrm{tors}}| = |B^\vee(K)_{\mathrm{tors}}|$.*

Proof. The fact that $A(L) = B(K)$ and $A^\vee(L) = B^\vee(K)$ follow from the definition of restriction of scalars. The last statements are simple corollaries of these two equalities. □

The Néron-Tate height pairing on A is a map $\langle,\rangle_A : A(\overline{L}) \times \mathrm{Pic}^0(A) \to \mathbb{R}$. Therefore, to analyze how the regulator behaves under restriction of scalars we need to look at the functorial properties of the Néron-Tate height pairing. By construction of heights on projective spaces, we see that $\langle,\rangle_{B\times_K L} = [L:K]\langle,\rangle_B$.

Lemma 5.6. *The regulators R_A and R_B of A and B are equal.*

Proof. Let $\langle , \rangle_A$ and $\langle , \rangle_B$ be the Néron-Tate height pairing on A and B respectively. Let $a_1, \ldots, a_r \in A(L)$ be a $\mathbb{Z}$-basis for $A(L)$ and let $b_1, \ldots, b_r$ be a $\mathbb{Z}$-basis for $A^\vee(L)$. Then let $a'_j = \psi^{-1}(\prod a_j^{\sigma_i}) \in B(K)$ and let $b'_j = R_{L/K} b_j \in B^\vee(K)$.

The isomorphism $B \cong \prod A^{\sigma_i}$ is defined over L and by the properties of the Néron-Tate pairing we have

$$\begin{aligned}
\langle a'_i, R_{L/K} b_j \rangle_B &= [L:K]^{-1} \langle a'_i, R_{L/K} b_j \rangle_{B \times_K L} = [L:K]^{-1} \sum_{k=1}^{n} \langle a'_i, \psi^* \pi_k^*(b_j^{\sigma_k}) \rangle_{A^{\sigma_k}} \\
&= [L:K]^{-1} \sum_{k=1}^{n} \langle \pi_k \psi(a'_i), b_j^{\sigma_k} \rangle_{A^{\sigma_k}} = [L:K]^{-1} \sum_{k=1}^{n} \langle a_i, b_j \rangle_A \\
&= (n/[L:K]) \langle a_i, b_j \rangle_A = \langle a_i, b_j \rangle_A
\end{aligned}$$

by functoriality of the height pairing and the fact that L/K is Galois.

Therefore $R_B = |\det \langle a'_i, b'_j \rangle_B| = |\det \langle a_i, b_j \rangle_A| = R_A$. □

Lemma 5.7. *The Shafarevich-Tate groups* $Ш(A/L)$ *of* A *over* L *and* $Ш(B/K)$ *of* B *over* K *have the same cardinality. In fact, there exists a canonical isomorphism between them.*

Proof. We have

$$H^1(K, B(\overline{K})) = H^1(K, \prod A^{\sigma_i}(\overline{L})) = H^1(K, \mathrm{Ind}_{\mathrm{Gal}(\overline{L}/L)}^{\mathrm{Gal}(\overline{K}/K)} A(\overline{L})),$$

which by Shapiro's lemma equals $H^1(L, A(\overline{L}))$. Therefore, the kernels, $Ш(B/K)$ and $Ш(A/L)$, of the two restriction maps

$$\begin{array}{ccc}
H^1(K, B(\overline{K})) & \longrightarrow & \oplus_v H^1(K_v, B(\overline{K}_v)) \\
\downarrow \cong & & \downarrow \\
H^1(L, A(\overline{L})) & \longrightarrow & \oplus_w H^1(L_w, A(\overline{L}_w))
\end{array}$$

must be isomorphic, by the snake lemma. □

We have shown that each quantity that appears in Conjecture 3.16 is invariant under restriction of scalars.

Corollary 5.8. *Conjecture 3.15 is true for* A *if and only if it is true for* $B = R_{L/K} A$.

5.2 Invariance Under Isogeny

Let K be a number field and let $A \xrightarrow{\psi} B$ be an isogeny of abelian varieties defined over K. Then there exists a finite group scheme $A[\psi] = \ker \psi$ that fits into an exact sequence $0 \to A[\psi] \to A \xrightarrow{\psi} B \to 0$. In particular this implies that $0 \to A[\psi](\overline{K}) \to A(\overline{K}) \to B(\overline{K}) \to 0$ and by taking cohomology we get that $0 \to A[\psi](K) \to A(K) \to B(K) \to H^1(\mathrm{Gal}(\overline{K}/K), A[\psi])$. But $A[\psi]$ is a finite $\mathrm{Gal}(\overline{K}/K)$-module so $A(K)$ and $B(K)$ differ by at most torsion, so the algebraic ranks of A and B are equal. Thus, the following proposition will prove that Conjecture 3.14 is invariant under isogeny.

Proposition 5.9. *For every finite set of places S we have $L_S(A,s) = L_S(B,s)$.*

Proof. By Lemma 2.33, for ℓ large enough to be coprime to the size of $A[\psi]$, we have $V_\ell A \cong V_\ell B$. Therefore, each of the local L_v-factors in the definition of $L_S(A,s)$ and $L_S(B,s)$ are the same, and the conclusion follows. □

Corollary 5.10. *There exists an analytic continuation of $L_S(A,s)$ to a neighborhood of 1 if and only if there exists one for $L_S(B,s)$.*

It is also the case that if Conjecture 3.15 holds for one of A and B then it will hold for the other. To make sense of the conjecture, one needs choices of invariant differentials. Let $\mathcal{A}$ and $\mathcal{B}$ be the Néron models of A and B over $\mathcal{O}_K$. Choose w an invariant differential on B, which induces an invariant differential w on $\mathcal{B}$. Then $\psi^* w$ is an invariant differential on A and induces an invariant differential on $\mathcal{A}$ (if necessary, replace w by γw for $\gamma \in \mathbb{Q}$ to achieve this goal). The proof of the invariance of the Birch and Swinnerton-Dyer conjecture under restriction of scalars was essentially easy since the Shafarevich-Tate group does not change under restriction of scalars and the L-functions behave in a straightforward manner. On the other hand, in the case of the isogeny invariance, the situation is reversed. Since the places of bad reduction are very hard to control via isogeny, instead of working with Conjecture 3.15 we will deal with Conjecture 3.16. Choose S finite containing M_K^∞, all places of bad reduction for A and B, all places where v_w or $v_{\psi^* w}$ is not 1 and all places that divide $|A[\psi]|$. Moreover, choose $\Lambda_S = \{\lambda_v\}$ such that $\lambda_v = 1$ for $v \in S$ and $\lambda_v = L_v(A,1) = L_v(B,1)$ for $v \notin S$. We will denote by K_S the maximal algebraic extension of K that is unramified at places $v \notin S$, and by $G_S = \mathrm{Gal}(K_S/K)$.

The key to the proof of the fact that Conjecture 3.16 is invariant under isogeny is expressing all the quantities in the conjecture in terms of the isogeny ψ. But, before we can proceed, we need to assume the finiteness of the groups $Ш(A/K)$ and $Ш(B/K)$ in Conjecture 3.16. One can prove that if A and B are isogenous, then one of the two groups is finite if and only if the other one is finite ([Mil86a] Lemma 7.1.b). However, the proof would divert us from the techniques required to prove the invariance of Conjecture 3.16 under isogeny. Therefore, we will assume that *both* groups $Ш(A/K)$ and $Ш(B/K)$ are finite.

We can now proceed to analyze the changes under isogeny of each of the quantities in the conjecture. The functorial properties of the Néron-Tate pairing suggest that the regulator of A should be equal to the regulator of B.

Lemma 5.11. *The regulators R_A of A and R_B of B are equal.*

Proof. Let r denote the ranks of A and B. Consider $a_1, \ldots, a_r$ a $\mathbb{Z}$-basis of $A(K)$ and $b_1, \ldots, b_r$ a $\mathbb{Z}$-basis of $B^\vee(K)$. Let $a_i' = \psi(a_i)$ and $b_i' = \psi^\vee(b_i)$ for $i = 1, \ldots, r$. Then

$$|\det(\langle a_i, b_j' \rangle)| = |\det(\langle a_i, \psi^\vee(b_j) \rangle)| = |\det(\langle \psi(a_i), b_j \rangle)| = |\det(\langle a_i', b_j \rangle)|,$$

by functoriality of the Néron-Tate height pairing (Proposition 2.35). □

However, it is no longer the case that the torsion subgroups are equal. Determining the relationship between the torsion subgroups is a simple application of the snake lemma.

Lemma 5.12. *We have*

$$\frac{|A(K)_{\mathrm{tors}}||A^\vee(K)_{\mathrm{tors}}|}{|B(K)_{\mathrm{tors}}||B^\vee(K)_{\mathrm{tors}}|} = \frac{|\ker\psi|}{|\operatorname{coker}\psi|}\frac{|\operatorname{coker}\psi^\vee|}{|\ker\psi^\vee|}.$$

Proof. On the level of torsion, we have a commutative diagram induces by the isogeny ψ

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \sum \mathbb{Z}a_i & \longrightarrow & A(K) & \longrightarrow & A(K)_{\mathrm{tors}} & \longrightarrow & 0 \\ & & \psi\downarrow\cong & & \psi\downarrow & & \psi_{\mathrm{tors}}\downarrow & & \\ 0 & \longrightarrow & \sum \mathbb{Z}b_i & \longrightarrow & B(K) & \longrightarrow & B(K)_{\mathrm{tors}} & \longrightarrow & 0 \end{array}$$

In this case the snake lemma gives an exact sequence $1 \to \ker\psi \to \ker\psi_{\mathrm{tors}} \to 1 \to \operatorname{coker}\psi \to \operatorname{coker}\psi_{\mathrm{tors}} \to 1$. Therefore $|A(K)_{\mathrm{tors}}|/|B(K)_{\mathrm{tors}}| = |\ker\psi|/|\operatorname{coker}\psi|$. The analogous procedure in the case of the dual isogeny $\psi^\vee : B^\vee \to A^\vee$ gives that $|A^\vee(K)_{\mathrm{tors}}|/|B^\vee(K)_{\mathrm{tors}}| = |\ker\psi^\vee|/|\operatorname{coker}\psi^\vee|$ and the lemma follows. □

The only two terms in Conjecture 3.16 that we have not yet discussed are the global integral and the Shafarevich-Tate group. For each $v \notin S$, both A and B have good reduction at v. Therefore, Corollary 2.61 implies that for our choice of (canonical) convergence factors we have

$$\int_{A(\mathbb{A}_{K,S})} d\mu_{A,w,\Lambda_S} = \left(\prod_{v\in S}\int_{A(K_v)}|w|_v\right)\left(\prod_{v\notin S}\int_{\mathcal{A}_v(\mathcal{O}_v)}|w|_v L_v(A,1)^{-1}\right) = \prod_{v\in S}\int_{A(K_v)}|w|_v$$

and similarly for B. Therefore, to analyze the behavior of the global integrals, it is sufficient to prove the following lemma.

Lemma 5.13. *If $v \in S$, then*

$$\int_{A(K_v)}|\psi^* w|_v = \frac{|\ker\psi_v|}{|\operatorname{coker}\psi_v|}\int_{B(K_v)}|w|_v,$$

where $\psi_v : A(K_v) \to B(K_v)$.

Proof. The Haar measure $|\psi^* w|_v$ on $A(K_v)$ is induced from the Haar measure $|w|_v$ on $\psi_v(A(K_v)) \cong A(K_v)/\ker\psi_v$. Therefore, in the exact sequence of topological groups

$$1 \to A(K_v)[\psi] \to A(K_v) \to \psi_v(A(K_v)) \to 1$$

(note that the fact that ψ is surjective does not imply that ψ_v is surjective), the Haar measure $|\psi^* w|_v$ on $A(K_v)$ induces the discrete measure μ on the finite set $A(K_v)[\psi]$ and the Haar measure $|w|_v$ on the topological groups $\psi_v(A(K_v)) \subset B(K_v)$. Therefore (by Fubini's theorem)

$$\int_{A(K_v)}|\psi^* w|_v = \int_{A(K_v)[\psi_v]}\left(\int_{A(K_v)}|w|_v\right)d\mu = |\ker\psi_v|\int_{A(K_v)}|w|_v.$$

Similarly, the exact sequence $1 \to \psi_v(A(K_v)) \to B(K_v) \to \operatorname{coker}\psi_v \to 1$ shows that the Haar measure $|w|_v$ on $B(K_v)$ induces the discrete measure μ on the finite set $\operatorname{coker}\psi_v$ and the Haar measure $|w|_v$ on $\psi_v(A(K_v))$. Therefore,

$$\int_{B(K_v)} |w|_v = \int_{\operatorname{coker}\psi_v} \left(\int_{\psi_v(A(K_v))} |w|_v \right) d\mu = |\operatorname{coker}\psi_v| \int_{\psi_v(A(K_v))} |w|_v.$$

By dividing the two formulas, we get the formula in the lemma. □

We have expressed all changes in the quantities that appear in Conjecture 3.16 in terms of the isogenies ψ and $\psi^\vee$. This suggests that we should look for a similar formula in the case of the Shafarevich-Tate groups. In Section 2.2.5 we have seen how the isogeny $\psi : A \to B$ induces a map $\psi_{Ш} : Ш(A/K) \to Ш(B/K)$. We need to look at the dual map $\psi_{Ш}^\vee : Ш(B^\vee/K) \to Ш(A^\vee/K)$. Thus, Proposition 2.39 becomes essential in our analysis, since it related $Ш(A/K)$ to $Ш(A^\vee/K)$.

Lemma 5.14. *If $\psi : A \to B$ is an isogeny, then*

$$\frac{|Ш(A/K)|}{|Ш(B/K)|} = \frac{|\ker\psi_{Ш}|}{|\ker\psi_{Ш}^\vee|}.$$

Proof. Since we have assumed that the groups $Ш(A/K)$ and $Ш(B/K)$ are finite, Proposition 2.39 implies the existence of nondegenerate pairings in the following commutative diagram (because all divisible subgroups are infinite):

$$\begin{array}{ccccc}
\ker\psi_{Ш} & & & & \operatorname{coker}\psi_{Ш}^\vee \\
\downarrow & & & & \uparrow \\
Ш(A/K) & \times & Ш(A^\vee/K) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\
{\scriptstyle\psi_{Ш}}\downarrow & & \uparrow{\scriptstyle\psi_{Ш}^\vee} & & \\
Ш(B/K) & \times & Ш(B^\vee/K) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\
\downarrow & & \uparrow & & \\
\operatorname{coker}\psi_{Ш} & & \ker\psi_{Ш}^\vee & &
\end{array}$$

Let $g \in \ker\psi_{Ш}^\vee$. The $\psi_{Ш}^\vee(g) = 0$ and, for every $f \in Ш(A/K)$, we have $\langle f, \psi_{Ш}^\vee(g)\rangle = 0$. But the diagram is commutative, so $\langle \psi_{Ш}(f), g\rangle = 0$ for every f. Therefore, for every $f' \in \operatorname{Im}\psi_{Ш}$ we have $\langle f', g\rangle = 0$ so $g \in (\operatorname{Im}\psi_{Ш})^\perp$, where for $X \subset Ш(B/K)$ we denote by $X^\perp$ the annihilator of X in the pairing:

$$X^\perp = \{g \in Ш(B^\vee/K) | \langle x, g\rangle = 0, \forall x \in X\}$$

Conversely, if $g \in (\operatorname{Im}\psi_{Ш})^\perp$ then for every $f \in Ш(A/K)$ we have $\langle \psi_{Ш}(f), g\rangle = 0$ so $\langle f, \psi_{Ш}^\vee(g)\rangle = 0$. But the pairing is nondegenerate, so $g \in \ker\psi_{Ш}^\vee$. Therefore, $\ker\psi_{Ш}^\vee = (\operatorname{Im}\psi_{Ш})^\perp$. But the pairing $\langle , \rangle$ is nondegenerate, so $(\operatorname{Im}\psi_{Ш})^\perp \approx Ш(B/K)/\operatorname{Im}\psi_{Ш} = \operatorname{coker}\psi_{Ш}$. Therefore,

$$|\operatorname{coker}\psi_{Ш}| = |\ker\psi_{Ш}^\vee|.$$

Consequently, the exact sequence $1 \to \ker \psi_{ш} \to Ш(A/K) \to Ш(B/K) \to \operatorname{coker} \psi_{ш} \to 1$ shows that

$$\frac{|Ш(A/K)|}{|Ш(B/K)|} = \frac{|\ker \psi_{ш}|}{|\operatorname{coker} \psi_{ш}|} = \frac{|\ker \psi_{ш}|}{|\ker \psi_{ш}^{\vee}|}.$$

□

Before we can go on to prove the fact that Conjecture 3.16 is invariant under isogeny, we need to construct a commutative diagram involving the maps ψ and $\psi^{\vee}$, as well as the long exact sequence in Theorem 4.15.

Lemma 5.15. *Let A be an abelian variety defined over a number field K. For each place v of K there exists an isomorphism $A^{\vee}(K_v) \cong H^1(K_v, A)^{\vee}$ (where $X^{\vee} = \operatorname{Hom}(X, \mathbb{Q}/\mathbb{Z})$, except for $A^{\vee}$, which is the dual variety).*

Proof. See [Mil86b] Corollary 3.4. □

We constructed S such that S contains all places of bad reduction for A and B and all the places that divide the order of $A[\psi]$. Therefore, [Mil86a], Lemma 6.1 implies that there exists an exact sequence $1 \to A(K_S)[\psi] \to A(K_S) \xrightarrow{\psi} B(K_S) \to 1$ (we will not prove this statement here, since it would be a too large departure from the subsequent line of the argument). By taking G_S-cohomology, we get an exact sequence

$$1 \to A(K)[\psi] \to A(K) \xrightarrow{\psi} B(K) \to H^1(G_S, A[\psi]) \to H^1(G_S, A) \xrightarrow{\psi} H^1(G_S, B).$$

Just as in the case of the exact sequence 2.1, we get the short exact sequence

$$1 \to \operatorname{coker} \psi \to H^1(G_S, A[\psi]) \to H^1(G_S, A)[\psi] \to 1.$$

Writing the same exact sequence for the dual isogeny $\psi^{\vee} : B^{\vee} \to A^{\vee}$ we get a short exact sequence

$$1 \to \operatorname{coker} \psi^{\vee} \to H^1(G_S, B^{\vee}[\psi^{\vee}]) \to H^1(G_S, B)[\psi^{\vee}] \to 1.$$

Similarly, for each $v \in S$ the short exact sequence $1 \to A[\psi] \to A \to B \to 1$ yields a short exact sequence

$$1 \to \operatorname{coker} \psi_v \to H^1(K_v, A[\psi]) \to H^1(K_v, A)[\psi] \to 1.$$

Putting these exact sequences together, we get that there exists a natural commutative diagram whose vertical morphisms are restriction maps

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{coker} \psi & \longrightarrow & H^1(G_S, A[\psi]) & \longrightarrow & H^1(G_S, A)[\psi] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \oplus \operatorname{res}_v} & & \downarrow{\scriptstyle f = \oplus \operatorname{res}_v} & & \downarrow{\scriptstyle \oplus \operatorname{res}_v} & & \\ 0 & \longrightarrow & \oplus_{v \in S} \operatorname{coker} \psi_v & \longrightarrow & \oplus_{v \in S} H^1(K_v, A[\psi]) & \longrightarrow & \oplus_{v \in S} H^1(K_v, A)[\psi] & \longrightarrow & 0 \end{array} \tag{5.1}$$

Moreover, the 9-term long exact sequence in Theorem 4.15 implies the existence of an exact sequence

$$H^1(G_S, A[\psi]) \xrightarrow{f} \oplus_{v \in S} H^1(K_v, A[\psi]) \xrightarrow{g} H^1(G_S, A[\psi]^*)^{\vee}.$$

Lemma 5.16. *The diagrams*

$$\begin{array}{ccc} \oplus_{v\in S}\operatorname{coker}\psi_v & \longrightarrow & \oplus_{v\in S}H^1(K_v,A[\psi]) \\ & & \downarrow{\scriptstyle g} \\ H^1(G_S,B^\vee)[\psi^\vee]^\vee & \longrightarrow & H^1(G_S,A[\psi]^*)^\vee \end{array} \qquad \begin{array}{ccc} \oplus_{v\in S}H^1(K_v,B^\vee)[\psi^\vee] & \longleftarrow & \oplus_{v\in S}H^1(K_v,A[\psi]^*) \\ {\scriptstyle \oplus\operatorname{res}_v}\uparrow & & \uparrow{\scriptstyle f} \\ H^1(G_S,B^\vee)[\psi^\vee] & \longleftarrow & H^1(G_S,A[\psi]^*) \end{array}$$

are dual to each other with respect to $\mathbb{Q}/\mathbb{Z}$.

Proof. Recall that there exists an exact sequence

$$A(K_v)\to B(K_v)\to \operatorname{coker}\psi_v\to 1.$$

If we dualize with respect to $\mathbb{Q}/\mathbb{Z}$ we get that $1\to(\operatorname{coker}\psi_v)^\vee\to B(K_v)^\vee\xrightarrow{\psi^\vee}A(K_v)^\vee$; by Lemma 5.15, this is the same as

$$1\to(\operatorname{coker}\psi_v)^\vee\to H^1(K_v,B^\vee)^\vee\longrightarrow H^1(K_v,A^\vee)^\vee.$$

Therefore, we get a map $(\operatorname{coker}\psi_v)^\vee\xrightarrow{\cong}H^1(K_v,B^\vee)[\psi^\vee]^\vee$. Moreover, by Theorem 4.10 there exists an isomorphism $\oplus_{v\in S}H^1(K_v,A[\psi])\cong\oplus_{v\in S}H^1(K_v,A[\psi]^*)^\vee$. Therefore, the groups in the two diagrams are pairwise dual with respect to $\mathbb{Q}/\mathbb{Z}$.

We still need to show that the maps are also dual. The lower horizontal maps are dual to each other by definition. By Theorem 4.15 the maps f and g are also dual to each other. The upper horizontal maps are dual to each other by Proposition 2.35, since $A[\psi]^*\cong A^\vee[\psi^\vee]$. □

Lemma 5.17. *There exists a commutative diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{coker}\psi & \longrightarrow & H^1(G_S,A[\psi]) & \longrightarrow & H^1(G_S,A)[\psi] & \longrightarrow & 0 \\ & & {\scriptstyle \alpha=\oplus\operatorname{res}_v}\downarrow & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \beta=\oplus\operatorname{res}_v} & & \\ 0 & \longrightarrow & \oplus_{v\in S}\operatorname{coker}\psi_v & \longrightarrow & \oplus_{v\in S}H^1(K_v,A[\psi]) & \longrightarrow & \oplus_{v\in S}H^1(K_v,A)[\psi] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle v} & & \\ 0 & \longrightarrow & H^1(G_S,B^\vee)[\psi^\vee]^\vee & \longrightarrow & H^1(G_S,A[\phi]^*)^\vee & \longrightarrow & (\operatorname{coker}\psi^\vee)^\vee & \longrightarrow & 0 \end{array}$$

Proof. The top part of the diagram is the commutative diagram 5.1. By Lemma 5.16, we can define the vertical map $u:\oplus_{v\in S}\operatorname{coker}\psi_v\to H^1(G_S,B^\vee)[\psi^\vee]^\vee$ to be the $\mathbb{Q}/\mathbb{Z}$-dual of the map $\oplus\operatorname{res}_v:H^1(G_S,B^\vee)[\psi^\vee]\to\oplus_{v\in S}(\operatorname{coker}\psi_v)^\vee$. Similarly, we may define a map $v:\oplus_{v\in S}H^1(K_v,A)[\psi]\to(\operatorname{coker}\psi^\vee)^\vee$ that makes the diagram commute. Note that each column is a complex, and the central column is exact. □

Lemma 5.18. *There exists a cohomology exact sequence*

$$0\to\ker\alpha\to\ker f\to\ker\beta\to\ker u/Im\alpha\to 0.$$

Proof. In Remark 4.7 we described the long exact sequence of cohomology of cochain complexes. In Lemma 5.17, each column is a complex. Let c_1, c_2, c_3 be the complexes representing the three columns. Then $H^0(c_1) = \ker\alpha$, $H^0(c_2) = \ker f$, $H^0(c_3) = \ker\beta$, $H^1(c_1) = \ker u/\mathrm{Im}\alpha$ and $H^1(c_2) = \ker g/\mathrm{Im}f = 0$ since c_2 is exact. Then, the exact sequence of the lemma is just the beginning of the cohomology long exact sequence in Remark 4.7. □

Lemma 5.19. *We have an equality*

$$\frac{|\ker\psi|}{\prod_{v\in S}|\ker\psi_v|}\frac{|H^2(G_S, A[\psi]^*)|}{|\ker f|}\prod_{v\in M_K^\infty}\frac{|H^0(K_v, A[\psi])|}{|\widehat{H}^0(K_v, A[\psi])|} = 1.$$

Proof. The first six terms of the long exact sequence of Theorem 4.15 are

$$0 \longrightarrow H^0(G_S, A[\psi]) \longrightarrow \oplus_{v\in S}\widehat{H}^0(K_v, A[\psi]) \longrightarrow H^2(G_S, A[\psi]^*)^\vee$$
$$H^1(G_S, A[\psi]) \xrightarrow{f} \oplus_{v\in S}H^1(K_v, A[\psi]) \longrightarrow H^1(G_S, A[\psi]^*)^\vee$$

These induce an exact sequence

$$0 \longrightarrow H^0(G_S, A[\psi]) \longrightarrow \oplus_{v\in S}\widehat{H}^0(K_v, A[\psi]) \longrightarrow H^2(G_S, A[\psi]^*)^\vee \longrightarrow \ker f \longrightarrow 0$$

Since, $H^0(K, A[\psi]) = A(K)[\psi] = \ker\psi$ and $H^0(K_v, A[\psi]) = A(K_v)[\psi] = \ker\psi_v$ and the sequence is exact, the relation follows. □

The only objects that we still haven't described are $\psi_{\text{ш}}$ and $\psi_{\text{ш}}^\vee$.

Lemma 5.20. *There is an isomorphism*

$$\ker\psi_{\text{ш}} \cong \ker\left(H^1(G_S, A)[\psi] \xrightarrow{\beta} \oplus_{v\in S}H^1(K_v, A)[\psi]\right)$$

Proof. See [Mil86b], Lemma 7.1.b. □

Remark 5.21. From now on we will be implicitly using that if $A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} \cdots \xrightarrow{f_k} A_{k+1}$ is a complex, then

$$\prod_{i=1}^{k+1}(-1)^{i-1}|A_i| = \prod_{i=1}^{k+1}(-1)^{i-1}|\ker f_i/\mathrm{Im}f_{i-1}|.$$

Having determined the relationship between the various maps $\psi, \psi^\vee, \psi_v$ and $\psi_v^\vee$, we can now state and prove the fact that Conjecture 3.15 is invariant under isogeny. The rest of the proof is abstract nonesense, using the commutative diagram in Lemma 5.17.

Theorem 5.22. *Let $\psi : A \to B$ be an isogeny of abelian varieties defined over a number field K. Suppose that $L(A, s)$ has analytic continuation to a neighborhood of 1 and suppose that $Ш(A/K)$ and $Ш(B/K)$ are finite. If Conjecture 3.15 holds for A, then it holds for B as well.*

Proof. We have already chosen a finite set of places S, invariant differentials w and $\psi^* w$ on B and A, and a set of convergence factors Λ_S. By Lemma 5.9, the function $L(B,s)$ also has analytic continuation to a neighborhood of 1, since its analytic behavior is the same as that of $L_S(B,s) = L_S(A,s)$. Rather than working with Conjecture 3.15 we will work with conjecture 3.16. If r is the rank of A and B, by Lemma 5.13 we get that

$$\frac{L_S^{(r)}(A,1)/\int_{A(\mathbb{A}_{K,S})} d\mu_{A,\psi^* w,\Lambda_S}}{L_S^{(r)}(B,1)/\int_{B(\mathbb{A}_{K,S})} d\mu_{B,w,\Lambda_S}} = \prod_{v\in S} \frac{|\operatorname{coker}\psi_v|}{|\ker\psi_v|}.$$

Moreover, by Lemmas 5.11, 5.12 and 5.14

$$\frac{R_A|Ш(A/K)|/(|A(K)_{\text{tors}}||A^\vee(K)_{\text{tors}}|)}{R_B|Ш(B/K)|/(|B(K)_{\text{tors}}||B^\vee(K)_{\text{tors}}|)} = \frac{|\ker\psi_{ш}|}{|\ker\psi_{ш}^\vee|}\frac{|\operatorname{coker}\psi|}{|\ker\psi|}\frac{|\ker\psi^\vee|}{|\operatorname{coker}\psi^\vee|}$$

To show that the conjecture is invariant under isogeny it is enough to show that

$$\frac{|\ker\psi_{ш}|}{|\ker\psi_{ш}^\vee|}\frac{|\operatorname{coker}\psi|}{|\ker\psi|}\frac{|\ker\psi^\vee|}{|\operatorname{coker}\psi^\vee|} = \prod_{v\in S}\frac{|\operatorname{coker}\psi_v|}{|\ker\psi_v|}.$$

By Lemma 5.20 we have $\ker\psi_{ш} = \ker\beta$ and, similarly, $\ker\psi_{ш}^\vee = \operatorname{coker} u$.

Therefore, it is enough to show that

$$\frac{|\ker\beta|}{|\operatorname{coker} u|}\frac{|\operatorname{coker}\psi|}{\prod_{v\in S}|\operatorname{coker}\psi_v|}\frac{\prod_{v\in S}|\ker\psi_v|}{|\ker\psi|}\frac{|\ker\psi^\vee|}{|\operatorname{coker}\psi^\vee|} = 1.$$

Moreover, the column c_1 gives

$$\frac{|\operatorname{coker}\psi|}{\prod_{v\in S}|\operatorname{coker}\psi_v|}|H^1(G_S,B^\vee)[\psi^\vee]^\vee| = \frac{|\ker\alpha|}{|\ker u/\mathrm{Im}\alpha|}|\operatorname{coker} u|.$$

Therefore, it is enough to show that

$$\frac{|\ker\beta|}{|\operatorname{coker} u|}\frac{|\ker\alpha||\operatorname{coker} u|}{|\ker u/\mathrm{Im}\alpha||H^1(G_S,B^\vee)[\psi^\vee]^\vee|}\frac{\prod_{v\in S}|\ker\psi_v|}{|\ker\psi|}\frac{|\ker\psi^\vee|}{|\operatorname{coker}\psi^\vee|} = 1.$$

By Lemma 5.19 it is enough to show that

$$\frac{|\ker\beta|}{|\operatorname{coker} u|}\frac{|\ker\alpha||\operatorname{coker} u|}{|\ker u/\mathrm{Im}\alpha||H^1(G_S,B^\vee)[\psi^\vee]^\vee|}\frac{|H^2(G_S,A[\psi]^*)|}{|\ker f|}\frac{|\ker\psi^\vee|}{|\operatorname{coker}\psi^\vee|}\prod_{v\in M_K^\infty}\frac{|H^0(K_v,A[\psi])|}{|\widehat{H}^0(K_v,A[\psi])|} = 1.$$

But the exact sequence in Lemma 5.18 gives that

$$\frac{|\ker\alpha|}{|\ker f|}\frac{|\ker\beta|}{|\ker u/\mathrm{Im}\alpha|} = 1.$$

Therefore, it is enough to show that

$$\frac{|H^2(G_S, A[\psi]^*)|}{|H^1(G_S, B^\vee)[\psi^\vee]^\vee|} \frac{|\ker \psi^\vee|}{|\operatorname{coker} \psi^\vee|} \prod_{v \in M_K^\infty} \frac{|H^0(K_v, A[\psi])|}{|\widehat{H}^0(K_v, A[\psi])|} = 1.$$

By Proposition 2.35, we have

$$|\ker \psi^\vee| = |A^\vee[\psi^\vee]| = |A[\psi]^*| = |H^0(G_S, A[\psi]^*)|.$$

Moreover, we can compute $|\operatorname{coker} \psi^\vee|$ from the lowest row in the commutative diagram in Lemma 5.17. We get

$$|\operatorname{coker} \psi^\vee| = \frac{|H^1(G_S, A[\psi]^*)|}{|H^1(G_S, B^\vee)[\psi^\vee]^\vee|}.$$

Therefore it is enough to show that

$$\frac{|H^2(G_S, A[\psi]^*)||H^0(G_S, A[\psi]^*)|}{|H^1(G_S, A[\psi]^*)|} = \prod_{v \in M_K^\infty} \frac{|\widehat{H}^0(K_v, A[\psi])|}{|H^0(K_v, A[\psi])|},$$

which follows from Theorem 4.16 applied to $M = A[\psi]^*$. □

References

[AW67] M. F. Atiyah and C. T. C. Wall, *Cohomology of groups*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 94–115.

[BCDT00] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises*, `http://www.math.harvard.edu/HTML/Individuals/Richard_Taylor.html`.

[Blo80] S. Bloch, *A note on height pairings, Tamagawa numbers, and the Birch and Swinnerton-Dyer conjecture*, Invent. Math. **58** (1980), no. 1, 65–76.

[Blo00] Spencer J. Bloch, *Higher regulators, algebraic K-theory, and zeta functions of elliptic curves*, CRM Monograph Series, vol. 11, American Mathematical Society, Providence, RI, 2000.

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990.

[Cas62] J. W. S. Cassels, *Arithmetic on curves of genus* 1. *IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. **211** (1962), 95–112.

[CF86] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, London, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], 1986.

[Con] Brian Conrad, *Finiteness of class numbers for algebraic groups*, http://www.math.lsa.umich.edu/ bdconrad/papers/cosetfinite.pdf.

[Con02] ———, *A modern proof of Chevalley's theorem on algebraic groups*, J. Ramanujan Math. Soc. **17** (2002), no. 1, 1–18.

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

[CS86] G. Cornell and J. H. Silverman (eds.), *Arithmetic geometry*, Springer-Verlag, New York, 1986, Papers from the conference held at the University of Connecticut, Storrs, Conn., July 30–August 10, 1984.

[CS01] Brian Conrad and William A. Stein, *Component groups of purely toric quotients*, Math. Res. Lett. **8** (2001), no. 5-6, 745–766.

[Del79] P. Deligne, *Valeurs de fonctions L et périodes d'intégrales*, Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979, pp. 313–346.

[Fre93] Margaret N. Freije, *The formal group of the Jacobian of an algebraic curve*, Pacific J. Math. **157** (1993), no. 2, 241–255.

[Gro64] A. Grothendieck, *Schémas en groupes. II: Groupes de type multiplicatif, et structure des schémas en groupes généraux*, Springer-Verlag, Berlin, 1962/1964.

[Gro82] Benedict H. Gross, *On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication*, Number theory related to Fermat's last theorem (Cambridge, Mass., 1981), Progr. Math., vol. 26, Birkhäuser Boston, Mass., 1982, pp. 219–236.

[Gro91] B. H. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic (Durham, 1989), Cambridge Univ. Press, Cambridge, 1991, pp. 235–256.

[GZ86] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320. MR 87j:11057

[Har77] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[Hat02] Allen Hatcher, *Algebraic topology*, Cambridge University Press, Cambridge, 2002.

[HS00] Marc Hindry and Joseph H. Silverman, *Diophantine geometry*, Springer-Verlag, New York, 2000, An introduction.

[KS00] D. R. Kohel and W. A. Stein, *Component Groups of Quotients of $J_0(N)$*, Proceedings of the 4th International Symposium (ANTS-IV), Leiden, Netherlands, July 2–7, 2000 (Berlin), Springer, 2000.

[Lan83] Serge Lang, *Abelian varieties*, Springer-Verlag, New York, 1983, Reprint of the 1959 original.

[Lan91] S. Lang, *Number theory. III*, Springer-Verlag, Berlin, 1991, Diophantine geometry.

[Lan94] ———, *Algebraic number theory*, second ed., Springer-Verlag, New York, 1994.

[LT58] S. Lang and J. Tate, *Principal homogeneous spaces over abelian varieties*, Amer. J. Math. **80** (1958), 659–684.

[Man71] J. I. Manin, *Cyclotomic fields and modular curves*, Russian Math. Surveys **26** (1971), no. 6, 7–78.

[Maz73] Barry Mazur, *Notes on étale cohomology of number fields*, Ann. Sci. École Norm. Sup. (4) **6** (1973), 521–552 (1974).

[Mil72] J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177–190.

[Mil80] ———, *Étale cohomology*, Princeton University Press, Princeton, N.J., 1980.

[Mil86a] ———, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.

[Mil86b] ———, *Arithmetic duality theorems*, Academic Press Inc., Boston, Mass., 1986.

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

[Neu99] Jürgen Neukirch, *Algebraic number theory*, vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[NSW00] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, vol. 323, Springer-Verlag, Berlin, 2000.

[Ono61] Takashi Ono, *Arithmetic of algebraic tori*, Ann. of Math. (2) **74** (1961), 101–139.

[Ono63] ———, *On the Tamagawa number of algebraic tori*, Ann. of Math. (2) **78** (1963), 47–73.

[Ono68] ———, *On Tamagawa numbers*, Proc. Internat. Congr. Math. (Moscow, 1966), Izdat. "Mir", Moscow, 1968, pp. 509–512.

[PR94] Vladimir Platonov and Andrei Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press Inc., Boston, MA, 1994.

[PS99] B. Poonen and M. Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149.

[Ros86] M. Rosen, *Abelian varieties over* $\mathbf{C}$, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 79–101.

[Ser88] J-P. Serre, *Algebraic groups and class fields*, Springer-Verlag, New York, 1988, Translated from the French.

[Ser92] Jean-Pierre Serre, *Lie algebras and Lie groups*, second ed., Lecture Notes in Mathematics, vol. 1500, Springer-Verlag, Berlin, 1992, 1964 lectures given at Harvard University.

[Sil92] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

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

[Spr79] T. A. Springer, *Reductive groups*, Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 1, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979, pp. 3–27.

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

[Tat63] J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, pp. 288–295.

[Tat67] J. T. Tate, *Fourier analysis in number fields, and Hecke's zeta-functions*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 305–347.

[Tat75] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1975, pp. 33–52. Lecture Notes in Math., Vol. 476.

[Tat95] ———, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1995, pp. Exp. No. 306, 415–440.

[Tay02] R. Taylor, *Galois representations*, Proceedings of the International Congress of Mathematicians, Vol. I (Beijing, 2002) (Beijing), Higher Ed. Press, 2002, pp. 449–474.

[Wat79] William C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics, vol. 66, Springer-Verlag, New York, 1979.

[Wei82] André Weil, *Adeles and algebraic groups*, Progress in Mathematics, vol. 23, Birkhäuser Boston, Mass., 1982.

[Wei94] Charles A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994.