Galois Cohomology

Contents

Notations, Conventions, and Fundamentals

(a) Throughout, F denotes a commutative unitary ring. The forgetful functor $\mathrm{F}\text{-Mod} \to \mathbb{Z}\text{-Mod}$ (alongside minors variants) is denoted by U.

(b) Given a homomorphism $\phi : A \to B$ of abelian groups, we let $A[\phi]$ denote the kernel of ϕ. For an abelian group A, we let $A_{\mathbb{Q}} := \mathbb{Q} \otimes_{\mathbb{Z}} A$ and $A_{\mathrm{tors}} := \bigcup_{n\in\mathbb{Z}} A[n] \subset A$ denote the maximal torsion subgroup, so there is an exact sequence $0 \to A_{\mathrm{tors}} \to A \to A_{\mathbb{Q}}$. Finally, we let $A^* := \mathrm{Hom}_{\mathrm{Grp}}(A, \mathbb{Q}/\mathbb{Z})$; this is the Pontryagin dual to A when A is finite.

(c) If G is a group and $H \leq G$ a subgroup, we denote by $[G/H]$ a left transversal to H in G, i.e. a subset $[G/H] \subset G$ such that as sets $G = \coprod_{g\in[G/H]} gH$. If G is a profinite group, then by $H \leq_{\mathrm{c}} G$ (resp. $H \leq_{\mathrm{o}} G$) we mean that H is a closed (resp. open) subgroup of G.

(d) Let $\varphi : G' \to G$ be a group homomorphism. We say that the *index*[1] of φ is defined when $[G : \varphi(G')] < \infty$ and $|\ker(\varphi)| < \infty$; in this case, we define the index of φ to be $\mathrm{ind}\,\varphi := [G : \varphi(G')] \cdot |\ker\varphi|^{-1}$. We will use the following result, the proof of which is clear.

Lemma 0.0.1.
(1) When G and G' are finite, for any $\varphi : G' \to G$, the index is always defined and equals $|G|/|G'|$.
(2) If $A^\bullet$ is a complex of finite abelian groups, almost all[2] zero, then

$$\prod_n |A^n|^{(-1)^n} = \prod_n |\mathrm{H}^n(A^\bullet)|^{(-1)^n}.$$

(e) For a scheme X and a point $x \in X$, we denote the residue field of X at x by $\mathrm{k}(x) := \mathscr{O}_{X,x}/\mathfrak{m}_{X,x}$. If X is a R-scheme for a ring R and $R \to S$ a homomorphism, we use the notation $X_S := \mathrm{Spec}\, S \times_{\mathrm{Spec}\, R} X$. By a *variety* over a field K, we mean a separated scheme of finite type over K.

(f) If K is a field, we write $K \to K^{\mathrm{s}} \to K^{\mathrm{a}}$ to denote a fixed choice of separable and algebraic closures of K, and let $G_K := \mathrm{Gal}(K^{\mathrm{s}}/K)$, which is canonical up to inner automorphisms.

(g) If K is a local number field (i.e., nonarchimedean local field with $\mathrm{char}\, K = 0$), we let $K^{\mathrm{nr}} \subset K^{\mathrm{a}}$ be the maximal unramified extension, and $G_K^{\mathrm{nr}} := \mathrm{Gal}(K^{\mathrm{nr}}/K)$. The residue field of K is denoted by k.

(h) If K is a (global) number field, we let $\mathscr{O}_K$ (resp. M_K, resp. M_K^∞, resp. M_K^0) denote its ring of integers (resp. set of places, resp. set of infinite places, resp. set of finite places). For $v \in \mathrm{M}_K$, we denote the corresponding completion of K by K_v. When $v \in \mathrm{M}_K \smallsetminus \mathrm{M}_K^\infty$, we denote the corresponding prime ideal of $\mathscr{O}_K$ (resp. valuation ring of K_v, residue field, size of the residue field) by $\mathfrak{p}_v$ (resp. $\mathscr{O}_v$, k_v, q_v). When v is archimedean, we will let $\mathrm{k}_v := \mathscr{O}_v := K_v$. Given a subset $S \subset \mathrm{M}_K$, we let $\mathscr{O}_{K,S} := \{x \in K : (\forall v \in \mathrm{M}_K^0 \smallsetminus S)\, v(x) \leq 1\}$. The adèle ring (resp. idèle group) of K will be denoted by $\mathbb{A}(K) = \mathbb{A}_K = \prod_{v\in\mathrm{M}_K}(K_v, \mathscr{O}_v)$ (resp. $\mathbb{A}^\times(K) = \mathbb{A}_K^\times = \prod_{v\in\mathrm{M}_K}(K_v^\times, \mathscr{O}_v^\times)$). For $S \subset \mathrm{M}_K$ with $S \supset \mathrm{M}_K^\infty$, we use the notation $\mathbb{A}_{K,S} := \prod_{v\in S} K_v \times \prod_{v\notin S} \mathscr{O}_v$ (resp. $\mathbb{A}_{K,S}^\times := \prod_{v\in S} K_v^\times \times \prod_{v\notin S} \mathscr{O}_v^\times$) to denote the S-adèle ring (resp. S-idèle group) of K, so that $\mathbb{A}_K = \mathrm{colim}_S\, \mathbb{A}_{K,S}$ (resp. $\mathbb{A}_K^\times = \mathrm{colim}_S\, \mathbb{A}_{K,S}^\times$). Also, we use the notation $K_S \subset K^{\mathrm{a}}$ for the maximal extension of K unramified outside of S, and G_S for $\mathrm{Gal}(K_S/K)$.

(i) For a global number field K and $v \in \mathrm{M}_K$, we always fix an extension of v to $K^{\mathrm{s}} = K^{\mathrm{a}}$, which gives an embedding $K^{\mathrm{a}} \to K_v^{\mathrm{a}}$ and the choice of inertia and decomposition groups $\mathrm{I}_v \leq \mathrm{D}_v \leq G_K$ along with isomorphisms $\mathrm{D}_v \xrightarrow{\sim} G_{K_v} =: G_v$ and $\mathrm{D}_v/\mathrm{I}_v \xrightarrow{\sim} G_{\mathrm{k}_v}$.

[1] The terminology is inspired from the theory of elliptic PDEs, although the convention is the opposite of the usual one (inspired by private communication with Dan Freed).

[2] As usual, this means "all but finitely many".

Introduction

The Birch and Swinnerton-Dyer (BSD) Conjecture, one of the six still-open Millenium Prize Problems of the Clay Mathematics Institute, is a tantalizing conjecture relating the local and global arithmetic of an abelian variety over a number field. Although we don't (yet) have a proof, there is a huge amount of experimental and theoretical evidence to support it. One source of theoretical evidence is the theorem due to Cassels in dimension one and Tate in general that the truth value of the BSD conjecture is invariant under a rather weak equivalence relation on abelian varieties called isogeny. It is the goal of this article to present Tate's proof of this result.

An important tool needed for the proof is cohomology. In various branches of topology and geometry, cohomology functions as a powerful linearization tool, i.e., a tool to reduce difficult non-linear problems to (hopefully easier) problems in linear algebra. In differential topology, there is de Rham cohomology; in algebraic topology, simplicial, CW, and singular cohomology; in complex geometry, Dolbeault cohomology; in algebraic geometry, sheaf (and eventually étale, fppf, fpqc, etc.) cohomology.[3] Arithmetic geometry is no exception, and the role of such a linearizing cohomology theory in algebraic number theory and arithmetic geometry is performed by *Galois cohomology*, which is a special kind of (profinite) group cohomology.[4] Galois cohomology is the modern language of a lot of number theory such as local and global class field theory. Further, as with the other cohomology theories mentioned above, it satisfies important duality theorems, which are the key input needed for Tate's result.

In the first chapter, we introduce group cohomology and describe its key properties (functoriality and cup products) as well as how to compute it. We finish by discussing Tate cohomology and the proof of the Tate-Nakayama theorem. In the second chapter, we explain how to extend the results of the first chapter to the profinite setting and describe classical examples of Galois cohomology (Hilbert 90, Brauer groups, etc.). Then we discuss applications of the theory to local and global class field theory, and finally, we sketch the "arithmetic" duality theorems of Tate-Poitou, as well as Tate's theorem on global Euler-Poincaré characteristics, that will be required in what follows. In the final chapter, we rapidly review the theory of abelian varieties over local and global number fields needed to state the strong Birch and Swinnterton-Dyer conjecture. We end by using all the cohomological tools developed to present Tate's proof of its isogeny invariance, tying it all together.

[3] Of course, these are all related in very intricate and important ways.

[4] It is also a special case of, and important historical motivation for, étale cohomology; see [40, §6.1.1]

1 Group Cohomology

We introduce group cohomology as the right derived functor of the functor of invariants and explain its computation using topological models and inhomogeneous cochains. Next, we discuss the (co)restriction, inflation, and conjugation morphisms and the cup product. Finally, we introduce Tate cohomology and prove Tate's theorem on cohomological triviality and as its consequence the Tate-Nakayama Theorem.

We assume familiarity with (the naive approach to) derived functors as δ-functors ([1, Ch. IX], [56, Ch. 2]) and some algebraic topology (at the level of [20]). The material presented is standard and is taken from [6], [8], [13], [15], [28],[29], [36], [37], [43], and [44].

1.1 Introduction and Definitions

Given a commutative unitary ring F and a group G, the category $\mathrm{F}[G]\text{-Mod}$ of left modules over the group algebra $\mathrm{F}[G]$, or equivalently F-linear representations of G, is Grothendieck abelian and has enough projectives (resp. injectives). Therefore, if $\mathscr{A}$ is an abelian category and $\mathscr{F} : \mathrm{F}[G]\text{-Mod} \to \mathscr{A}$ a right-exact (resp. left-exact) additive functor, then the left (resp. right) derived functor $\mathrm{L}_\bullet\mathscr{F}$ (resp. $\mathrm{R}^\bullet\mathscr{F}$) of $\mathscr{F}$, i.e., the universal (co)homological exact δ-functor extending $\mathscr{F}$, exists and is unique up to unique isomorphism of δ-functors extending the identity natural transformation $1_{\mathscr{F}}$. One case of particular interest is when $\mathscr{A} = \mathrm{F}\text{-Mod}$ and $\mathscr{F} = (-)^G$ is the left exact functor obtained by taking G-invariants.[5]

Definition 1.1.1 (Group Cohomology)**.** *The* group cohomology of G in F-modules*, denoted* $\mathrm{H}^\bullet(G, -)$*,*[6] *is the right derived functor of the functor* $(-)^G : \mathrm{F}[G]\text{-Mod} \to \mathrm{F}\text{-Mod}$ *of G-invariants, i.e.,*

$$\mathrm{H}^\bullet(G, -) := \mathrm{R}^\bullet(-)^G : \mathrm{F}[G]\text{-Mod} \to \mathrm{F}\text{-Mod}.$$

Remark 1.1.2.

(a) If $G = \{*\}$ is trivial, then $\mathrm{H}^0(G, -) : \mathrm{F}[G]\text{-Mod} \to \mathrm{F}\text{-Mod}$ is the canonical isomorphism and so $\mathrm{H}^n(G, -) = 0$ for each $n \in \mathbb{Z}_{\geq 1}$. For an arbitrary G, the F-*cohomological dimension* $\mathrm{cd}_{\mathrm{F}}(G)$ of G is the least $d \in \mathbb{Z}_{\geq 0}$, if it exists, such that $\mathrm{H}^n(\mathrm{F}[G], -) = 0$ for all $n > d$; if no such d exists, we write $\mathrm{cd}_{\mathrm{F}}(G) = \infty$. This is a measure of the nontriviality of G; for instance, $\mathrm{cd}_{\mathbb{Z}}(G) = 0$ iff $G = \{*\}$.[7]

(b) For an $A \in \mathrm{F}[G]\text{-Mod}$ and $n \in \mathbb{Z}_{\geq 0}$, the ring homomorphism $\mathrm{H}^n : \mathrm{End}_{\mathrm{F}[G]}(A) \to \mathrm{End}_{\mathrm{F}}(\mathrm{H}^n(G, A))$ is an F-algebra homomorphism, i.e., multiplication by $\lambda \in \mathrm{F}$ on an $\mathrm{F}[G]$-module induces the same map, i.e., multiplication by λ, on cohomology in all degrees; this follows from the δ-functor formalism.

(c) Let us temporarily use $\mathrm{H}^\bullet(\mathrm{F}[G], -)$ to denote the group cohomology of G in F-modules, and let $\mathrm{U}_G : \mathrm{F}[G]\text{-Mod} \to \mathbb{Z}[G]\text{-Mod}$ (resp. $\mathrm{U} : \mathrm{F}\text{-Mod} \to \mathbb{Z}\text{-Mod}$) denote the forgetful functor. The exactness of U_G and U along with the commutativity (up to the obvious natural isomorphism) of

$$\begin{array}{ccc} \mathrm{F}[G]\text{-Mod} & \xrightarrow{\mathrm{U}_G} & \mathbb{Z}[G]\text{-Mod} \\ \downarrow{\scriptstyle (-)^G} & & \downarrow{\scriptstyle (-)^G} \\ \mathrm{F}\text{-Mod} & \xrightarrow{\mathrm{U}} & \mathbb{Z}\text{-Mod} \end{array}$$

tells us that

$$\mathrm{U}\mathrm{H}^\bullet(\mathrm{F}[G], -) \cong \mathrm{R}^\bullet\left(\mathrm{U} \circ (-)^G\right) \cong \mathrm{R}^\bullet\left((-)^G \circ \mathrm{U}_G\right) \cong \mathrm{H}^\bullet(\mathbb{Z}[G], \mathrm{U}_G(-))$$

[5] That this is left exact is clear, but this is also follows from the fact that it is naturally isomorphic to the right adjoint functor $\mathrm{Hom}_{\mathrm{F}[G]}(\mathrm{F}, -)$, where F is equipped with the trivial G-action.

[6] See Remark 1.1.2(c).

[7] Indeed, for general homological algebraic reasons, $\mathrm{cd}_{\mathbb{Z}}(G) = 0$ is equivalent to saying that every $\mathbb{Z}[G]$-module is projective. In particular, the augmentation map $\varepsilon : \mathbb{Z}[G] \to \mathbb{Z}$ given by $g \mapsto 1$ for all $g \in G$ admits a $\mathbb{Z}[G]$-section σ. The element $\gamma := \sigma(1) \in \mathbb{Z}[G]^G$ has $\varepsilon(\sigma(1)) = 1$; the existence of a nonzero such γ implies that G is finite, and then $\gamma = n \cdot \sum_{g \in G} g$ for some $n \in \mathbb{Z}$. Then $1 = \varepsilon(\gamma) = n \cdot |G|$ implies G is trivial.

as δ-functors $\mathrm{F}[G]\text{-Mod} \to \mathbb{Z}\text{-Mod}$, i.e., the cohomology groups $\mathrm{H}^\bullet(G,-)$ "do not depend on F".[8] For instance, if $A \in \mathbb{Z}[G]\text{-Mod}$ has finite exponent $m \in \mathbb{Z}_{\geq 1}$ as an abelian group, then $m \cdot \mathrm{H}^\bullet(G,A) = 0$.

(d) The natural isomorphism $\mathrm{Hom}_{\mathrm{F}[G]}(\mathrm{F},-) \to (-)^G$ of additive functors (foot)noted above extends to a isomorphism of the right derived functors $\mathrm{Ext}^\bullet_{\mathrm{F}[G]}(\mathrm{F},-) \to \mathrm{H}^\bullet(G,-)$. Therefore, we can compute group cohomology using $\mathrm{F}[G]$-projective resolutions of the trivial G-module F (Examples 1.1.4-1.1.5).

(e) When $\mathscr{A} = \mathrm{F}\text{-Mod}$ and $\mathscr{F} = (-)_G$ is the right-exact functor obtained by taking G-coinvariants, with right-exactness coming from the natural isomorphism $\mathscr{F} \cong \mathrm{F} \otimes_{\mathrm{F}[G]} -$, we can define the *group homology* of G in F-modules as $\mathrm{H}_\bullet(G,-) := \mathrm{L}_\bullet(-)_G$. As in (c), we have a δ-isomorphism of left derived functors $\mathrm{Tor}^{\mathrm{F}[G]}_\bullet(F,-) \to \mathrm{H}_\bullet(G,-)$; in particular, group homology can also be computed used $\mathrm{F}[G]$-projective resolutions of F. See also §1.4.

Example 1.1.3. If G is a finite group such that $|G| \in \mathrm{F}^\times$,[9] then $(-)^G : \mathrm{F}[G]\text{-Mod} \to \mathrm{F}\text{-Mod}$ is *exact*, and so $\mathrm{cd}_{\mathrm{F}}(G) = 0$. Indeed, if $B \twoheadrightarrow C$ is an $\mathrm{F}[G]$-module epimorphism and $c \in C^G$, then picking any lift $b \in B$ of c, the element $|G|^{-1}\sum_{g\in G} gb \in B^G$ also maps to c. When F is a field, this argument applied to $B = \mathrm{Hom}_{\mathrm{F}}(V,W)$ and $C = \mathrm{Hom}_{\mathrm{F}}(W,W)$ for a subrepresentation $W \subset V$ proves Maschke's Theorem on complete reducibility.[10] The failure of Maschke's Theorem for a given modular (sub)representation is thus equivalent to the nonvanishing of a first cohomology group.

Next, if G is a finite group and $A \in \mathrm{F}[G]\text{-Mod}$ such that the underlying abelian group of A admits the structure of an F'-module for some commutative unitary ring F' such that $|G| \in (\mathrm{F}')^\times$ (e.g., if $\mathrm{F} = \mathbb{Q}$ and A admits a $\mathbb{Q}$-vector space structure), then by the previous paragraph and Remark 1.1.2(c), $\mathrm{H}^n(G,A) = 0$ for all $n \geq 1$. Also, if $\mathrm{F} \to \mathrm{F}'$ is a flat morphism of rings, then for any group G we have a morphism

$$\mathrm{F}' \otimes_{\mathrm{F}} \mathrm{H}^\bullet(G,-) \to \mathrm{H}^\bullet(G, \mathrm{F}' \otimes_{\mathrm{F}} (-))$$

of δ-functors $\mathrm{F}[G]\text{-Mod} \to \mathrm{F}'\text{-Mod}$, which is an isomorphism when G is finite.[11] Combining these results for the flat morphism $\mathbb{Z} \to \mathbb{Q}$ and using Remark 1.1.2(c) once again shows that if G is a finite group, $A \in \mathrm{F}[G]\text{-Mod}$, and $n \in \mathbb{Z}_{\geq 1}$, then the underlying abelian group $\mathrm{UH}^n(G,A)$ is a torsion group; c.f. Example 1.2.2(a).

Example 1.1.4. (Topological Interpretation) Let G be a (discrete) group and X be (a topological model for) the Eilenberg-MacLane space $\mathrm{K}(G,1)$, or equivalently the classifying space $\mathrm{B}G$. Concretely, X is a pointed path-connected CW complex with contractible universal cover $\widetilde{X}$, equipped with an isomorphism $G \to \pi_1(X)$.[12] Then G acts freely on $\widetilde{X}$ by cellular maps, and by grouping G-translates, the cellular chain complex of $\widetilde{X}$ with F-coefficients is seen to be an $\mathrm{F}[G]$-free resolution of the trivial module F. In particular, for $A \in \mathrm{F}[G]\text{-Mod}$, the group (co)homology $\mathrm{H}_\bullet(G,A)$ (resp. $\mathrm{H}^\bullet(G,A)$) can be identified with the twisted (co)homology $\mathrm{H}_\bullet(X;A)$ (resp. $\mathrm{H}^\bullet(X;A)$) of X with local coefficients in A as defined in [20, §3.H].[13] In particular, if $\mathrm{F} = \mathbb{Z}$ and $A = \mathbb{Z}$ is the trivial $\mathbb{Z}[G]$-module, then by the Hurewicz Theorem ([20, Thm.

[8] In the last isomorphism, to conclude that $\mathrm{R}^\bullet((-)^G \circ \mathrm{U}_G) \cong \mathrm{R}^\bullet(-)^G \circ \mathrm{U}_G$, we are also using that $\mathrm{R}^\bullet(-)^G \circ \mathrm{U}_G$ is effaceable, which can be shown, for instance, by noting that U_G commutes with the particular effacement $A \to \mathscr{C}^1(G,A)$ constructed in Example 1.2.2(b) below. Note that the left adjoint $\mathrm{F} \otimes_{\mathbb{Z}} (-) \cong \mathrm{F}[G] \otimes_{\mathbb{Z}[G]} (-)$ to U_G is not, in general, exact. For an advantage of our (slightly) more general perspective, see Example 1.1.3.

[9] Here $|G|$ denotes the cardinality of G, considered as an element of F via the natural map $\mathbb{Z} \to \mathrm{F}$. The condition that $|G|$ is a unit in F holds, e.g., if F is a field of characteristic 0, or if it is a field of characteristic $p > 0$ for a prime p such that $p \nmid |G|$.

[10] The above proof is, after all, the standard proof of Maschke's Theorem.

[11] Similarly to Footnote 8, here we are using the fact that $\mathrm{F}' \otimes_{\mathrm{F}} (-) : \mathrm{F}[G]\text{-Mod} \to \mathrm{F}'[G]\text{-Mod}$ is exact and commutes with effacement $A \to \mathscr{C}^1(G,A)$ of Example 1.2.2(b) when G is finite!

[12] That such spaces exist is a standard result in algebraic topology ([20, Example 1B.7]).

[13] See the *Introduction* to [6] for some historical comments about the relationship between topological and group (co)homology, and the discovery/invention of group (co)ohomology.

2A.1]), we get a functorial isomorphism $\mathrm{H}_1(G,\mathbb{Z}) \cong G^{\mathrm{ab}}$. This can also be proven purely algebraically; see [15, Lemma 10.20].[14]

Example 1.1.5. (Bar Resolution) For each $n \in \mathbb{Z}_{\geq 0}$, let $\mathrm{F}[G]^{G^n}$ denote the free $\mathrm{F}[G]$-module on the set G^n, where we denote the basis element corresponding to $(g_1, g_2, \ldots, g_n) \in G^n$ by $[g_1|g_2|\cdots|g_n]$. For each $n \in \mathbb{Z}_{\geq 0}$, define the $\mathrm{F}[G]$-module homomorphism $\partial_n : \mathrm{F}[G]^{G^{n+1}} \to \mathrm{F}[G]^{G^n}$ given on the basis by

$$\partial_n[g_1|g_2|\cdots|g_{n+1}] := g_1[g_2|\cdots|g_{n+1}] + \sum_{i=1}^{n}(-1)^i[g_1|g_2|\cdots|g_{i-1}|g_ig_{i+1}|g_{i+2}|\cdots|g_{n+1}] + (-1)^{n+1}[g_1|g_2|\cdots|g_n]$$

for $g_1, \ldots, g_n \in G$. Then a direct check shows that

$$\cdots \xrightarrow{\partial_2} \mathrm{F}[G]^{G^2} \xrightarrow{\partial_1} \mathrm{F}[G]^{G} \xrightarrow{\partial_0} \mathrm{F}[G] \xrightarrow{\varepsilon} \mathrm{F} \to 0 \tag{1.1}$$

is a complex of $\mathrm{F}[G]$-modules, where ε denotes the augmentation map given by $g \mapsto 1$ for all $g \in G$. For each $n \in \mathbb{Z}_{\geq 0}$, define the F-module homomorphism $h_n : \mathrm{F}[G]^{G^n} \to \mathrm{F}[G]^{G^{n+1}}$ on an F-basis by

$$h_n\left(g \cdot [g_1|\ldots|g_n]\right) := [g|g_1|\cdots|g_n]$$

for $g, g_1, \ldots, g_n \in G$. Then for each $n \geq 0$, we have $h_n\partial_n + \partial_{n+1}h_{n+1} = \mathrm{id}_{\mathrm{F}[G]^{G^{n+1}}}$, and so the collection $h = (h_n)_{n\in\mathbb{Z}_{\geq 0}}$ provides an F-module contracting homotopy[15] for the positive-degree part of the complex (1.1), showing that it is an $\mathrm{F}[G]$-free resolution of the trivial module F. This resolution, called the *standard* or *bar* resolution, gives a particularly concrete way of computing group (co)homology. Explicitly, for each $\mathrm{F}[G]$-module A and $n \in \mathbb{Z}_{\geq 0}$, the F-module

$$\mathscr{C}^n(G, A) := \mathrm{Hom}_{\mathrm{F}[G]\text{-Mod}}(\mathrm{F}[G]^{G^n}, A) \cong \mathrm{Hom}_{\mathrm{Set}}(G^n, A)$$

is called the module of *inhomogeneous n-cochains on G with values in A*. For each $n \geq 0$, the pullback by ∂_n gives us an F-module homomorphism $\partial^n := \partial_n^* : \mathscr{C}^n(G,A) \to \mathscr{C}^{n+1}(G,A)$, and the cohomology of the complex $(\mathscr{C}^\bullet(G,A), \partial^\bullet)$ is the group cohomology $\mathrm{H}^\bullet(G,A)$, i.e., if for each $n \in \mathbb{Z}_{\geq 0}$ we let $\mathscr{Z}^n(G,A) := \ker \partial^n$ (resp. $\mathscr{B}^n(G,A) := \mathrm{im}\,\partial^{n-1}$) denote the F-submodule of *inhomogeneous n-cocycles* (resp. *n-coboundaries*), then

$$\mathrm{H}^n(G,A) \cong_{\mathrm{F\text{-}Mod}} \mathscr{Z}^n(G,A)/\mathscr{B}^n(G,A).$$

Finally, given a short exact sequence $0 \to A \to B \to C \to 0$ of $\mathrm{F}[G]$-modules, we get a short exact sequence

$$0 \to \mathscr{C}^\bullet(G,A) \to \mathscr{C}^\bullet(G,B) \to \mathscr{C}^\bullet(G,C) \to 0$$

of complexes of F-modules, and the connecting homomorphisms can be computed using the Snake Lemma.

Remark 1.1.6.

[14] I cannot resist mentioning one further geometrical example. A theorem of Cartan and Hadamard asserts that given $n \in \mathbb{Z}_{\geq 0}$, if X is a connected complete Riemannian n-manifold of non-positive sectional curvature, then its universal cover $\widetilde{X}$ is diffeomorphic to $\mathbb{R}^n$. In particular, if $G = \pi_1(X)$ is the fundamental group of X, then X is a $\mathrm{K}(G,1)$, and so $\mathrm{cd}_{\mathbb{Z}}(G) \leq n$. If X is not closed, then $n \geq 1$ and this can be strengthened to $\mathrm{cd}_{\mathbb{Z}}(G) \leq n-1$. This applies, for instance, when $X = \Sigma_g$ is the oriented surface of genus $g \in \mathbb{Z}_{\geq 2}$, so that $\mathrm{cd}_{\mathbb{Z}}\,\pi_1(\Sigma_g) = 2$, or if X is a hyperbolic knot complement, so that, e.g., the group $G = \langle x, y | y^2x^{-3}\rangle$ has $\mathrm{cd}_{\mathbb{Z}}(G) = 2$ because it is the fundamental group of the trefoil knot complement. Other topological connections and applications can be found in, e.g., [29, Ch. 4].

[15] Note that the maps h_n are, in general, not $\mathrm{F}[G]$-module homomorphisms. Indeed, the complex (1.1) not contractible as a complex of $\mathrm{F}[G]$-modules, else all of group (co)homology would be trivial!

(a) If $n = 1$ and G acts trivially on $A \in \mathrm{F}[G]\text{-Mod}$, then $\mathscr{Z}^1(G, A)$ is the submodule of homomorphisms $G \to A$ and $\mathscr{B}^1(G, A) = 0$, so that $\mathrm{H}^1(G, A) \cong_{\mathrm{F}\text{-Mod}} \mathrm{Hom}_{\mathrm{Grp}}(G, A)$. As an application, note that for a finite group G, considering the short exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ of trivial $\mathbb{Z}[G]$-modules and using Example 1.1.3 gives us isomorphisms of abelian groups

$$\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{H}^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} \mathrm{H}^2(G, \mathbb{Z}).$$

(b) Example 1.1.5 gives another way to see the result of Remark 1.1.2(c). It also immediately shows that if G is a finite group and $A \in \mathbb{Z}[G]\text{-Mod}$ is such that $\mathrm{U}A$ is a finitely generated abelian group, then so is $\mathrm{UH}^n(G, A)$ for each $n \in \mathbb{Z}_{\geq 0}$ (since each $\mathscr{C}^n(G, A)$ is), and hence (along with Example 1.1.3) that $\mathrm{H}^n(G, A)$ is *finite* for each $n \in \mathbb{Z}_{\geq 1}$.

(c) A slight modification of the bar resolution by using *homogeneous* cochains ([15, Ch. 10]) can be seen directly to compute the simplicial cohomology of the *standard simplicial model* for the Eilenberg-MacLane space $\mathrm{K}(G, 1)$ (i.e., the geometric realization of the Kan complex $\mathscr{N}\mathrm{B}G$ which is the nerve of the categorification $\mathrm{B}G$ of G), again illustrating Example 1.1.4. See [6, Ex. I.4.3] and [29, Ch. 4].

The bar resolution can be used to give a concrete interpretation of H^1. In what follows, we take $\mathrm{F} = \mathbb{Z}$.

Definition 1.1.7 (Torsors)**.** *Let G be a group and $A \in \mathbb{Z}[G]\text{-Mod}$. By an A-*torsor*, we mean a nonempty G-set X equipped with a simply transitive right action $+ : X \times A \to X$ of A that is compatible with the action of G, i.e., such that for all $x \in X, a \in A$ and $g \in G$, we have $gx + ga = g(x + a)$.*

Torsors are also called *principal homogeneous spaces*. The definition of an isomorphism of A-torsors is clear.

Theorem 1.1.8. *There is a bijection between $\mathrm{H}^1(G, A)$ and the set of isomorphism classes of A-torsors.*

Proof. ([44, §5.2]) Let X be an A-torsor and $x \in X$. For each $g \in G$, there is a unique $a(g) \in A$ satisfying $x + a(g) = gx$, and then the map $a : G \to A$ lies in $\mathscr{Z}^1(G, A)$. Given any other $x' \in X$, there is a $b \in A \cong \mathscr{C}^0(G, A)$ such that $x' = x + b$, and the corresponding map $a' : G \to A$ differs from a by $\partial^0 b \in \mathscr{B}^1(G, A)$. Hence, we get a well-defined class $[a] \in \mathrm{H}^1(G, A)$, and the previous argument also shows it depends only on the isomorphism class of X.

Conversely, if $a \in \mathscr{Z}^1(G, A)$ is a 1-cocycle, define a G-set X_a by taking the underlying set to be A and the a-twisted action of G on the left given by $g \cdot_a x := gx + a(g)$ for $g \in G$ and $x \in X_a$; that this is an action uses precisely the cocycle condition on a. Acting on the right by translations makes X_a into an A-torsor, and two cohomologous cycles define isomorphic A-torsors. This gives a map in the other direction which is easily seen to be the inverse to the first one. □

Remark 1.1.9.

(a) Theorem 1.1.8 gives the set of isomorphism classes of A-torsors the structure of an abelian group.[16] Further, the bijection is functorial in G and A. For instance, if $\phi : A \to B$ a $\mathbb{Z}[G]$-module homomorphism and X is an A-torsor, then the quotient X_B of $X \times B$ modulo the equivalence relation $(x + a, b) \sim (x, \phi(a) + b)$ for $x \in X, a \in A, b \in B$ is a B-torsor, and the map on cohomology groups $\mathrm{H}^1(G, A) \to \mathrm{H}^1(G, B)$ induced by ϕ corresponds to the operation $[X] \mapsto [X_B]$. Similarly, the isomorphism is functorial in G with respect to lifting morphisms defined in the next section.

(b) Similarly, the second cohomology group $\mathrm{H}^2(G, A)$ admits a concrete description: it classifies extensions $1 \to A \to \Gamma \to G \to 0$, where G acts on A by conjugation in Γ via the $\mathbb{Z}[G]$-module structure; this is the theory of "factor sets" ([37, 1.2.4]).[17] When $G = \mathrm{Gal}(L/K)$ is a finite Galois group of order n, extensions $1 \to L^\times \to \Gamma \to G \to 1$ correspond to Azumaya algebras (i.e., central simple algebras) of dimension n^2 over K split by L, and this gives an explicit isomorphism $\mathrm{H}^2(G, L^\times)$ with the Brauer group $\mathrm{Br}(L/K)$ ([15, Part II]).

[16] It is a fun exercise to figure out the corresponding operation on torsors explicitly.

[17] Higher cohomology groups also yield such descriptions (e.g., [37, §I.2, Ex. 2]), but they get increasingly more unwieldy.

(c) There is an an analog of the above group cohomology with coefficients in a nonabelian group A. The above proof applies verbatim in this setting to show that the *pointed set* $\mathrm{H}^1(G, A)$ still classifies A-torsors ([37, 1.2.3]). This is important in the theory of Galois descent ([8, Ch. X], [40, §4.4-4.5], [43, §X.2]).

1.2 Functoriality: (Co)restriction, Inflation, and Conjugation

In this section, we study the functoriality of group cohomology $\mathrm{H}^\bullet(G, A)$ in the group G and the coefficient module A, essentially following [28, Ch. II]. A group homomorphism $\varphi : G' \to G$ induces an F-algebra homomorphism $\varphi : \mathrm{F}[G'] \to \mathrm{F}[G]$, which gives rise to three functors–*induction*, *restriction*, and *coinduction*–

$$\mathrm{F}[G']\text{-Mod} \underset{\mathrm{Res}_\varphi}{\overset{\mathrm{Ind}_\varphi := \mathrm{F}[G]\otimes_{\mathrm{F}[G']} -}{\overset{\longleftarrow}{\underset{\mathrm{Coind}_\varphi := \mathrm{Hom}_{\mathrm{F}[G']\text{-Mod}}(\mathrm{F}[G], -)}{\longrightarrow}}}} \mathrm{F}[G]\text{-Mod}$$

which fit into the tensor-hom adjunctions $\mathrm{Ind}_\varphi \dashv \mathrm{Res}_\varphi \dashv \mathrm{Coind}_\varphi$.[18] In particular, Res_φ is faithfully exact, so that the counit $\varepsilon : \mathrm{Ind}_\varphi \circ \mathrm{Res}_\varphi \to \mathrm{id}_{\mathrm{F}[G]\text{-Mod}}$ (resp. unit $\eta : \mathrm{id}_{\mathrm{F}[G]\text{-Mod}} \to \mathrm{Coind}_\varphi \circ \mathrm{Res}_\varphi$) is a pointwise epimorphism (resp. monomorphism).

Definition 1.2.1 (Lifting Map)**.** *Given a group homomorphism $\varphi : G' \to G$, we define the* lifting along φ

$$\mathrm{Lif}_\varphi^\bullet : \mathrm{H}^\bullet(G, -) \to \mathrm{H}^\bullet(G', \mathrm{Res}_\varphi(-))$$

to be the unique morphism of δ-functors extending the obvious natural transformation $(-)^G \to (-)^{G'} \circ \mathrm{Res}_\varphi$.

Following [29, Def. 1.1.13], we let $\mathrm{F}\text{-}\mathrm{GrpMod}^*$ be the category fibered over $\mathrm{Grp}^{\mathrm{op}}$ whose objects are pairs (G, A) consisting of a group G and an $\mathrm{F}[G]$-module A and morphisms $(G, A) \to (G', A')$ given by pairs (φ, f) where $\varphi : G' \to G$ is a group homomorphism and $f : \mathrm{Res}_\varphi(A) \to A'$ an $\mathrm{F}[G']$-module homomorphism. Then using Definition 1.2.1 and the pushforward along f tells us that for each $n \in \mathbb{Z}_{\geq 0}$, cohomology defines a covariant functor

$$\mathrm{H}^n(-, -) : \mathrm{F}\text{-}\mathrm{GrpMod}^* \to \mathrm{F}\text{-Mod}$$

with $\mathrm{Lif}_\varphi^n = \mathrm{H}^n(\varphi, \mathrm{id})$. If we compute group cohomology using the bar resolution (Example 1.1.5), then for a morphism $(\varphi, f) : (G, A) \to (G', A')$ in $\mathrm{F}\text{-}\mathrm{GrpMod}$ and $n \in \mathbb{Z}_{\geq 0}$, the map $\mathrm{H}^n(\varphi, f) : \mathrm{H}^n(G, A) \to \mathrm{H}^n(G', A')$ is given at the level of inhomogeneous cochains $\mathscr{C}^n(G, A) \to \mathscr{C}^n(G', A')$ by $c \mapsto f \circ c \circ \varphi^n$.[19]

Example 1.2.2. ((Co)restriction) If $\iota : H \hookrightarrow G$ is the inclusion of a subgroup, then the resulting functor $\mathrm{Res}_\iota : \mathrm{F}[G]\text{-Mod} \to \mathrm{F}[H]\text{-Mod}$ and morphism $\mathrm{Lif}_\iota^\bullet : \mathrm{H}^\bullet(G, -) \to \mathrm{H}^\bullet(H, \mathrm{Res}_\iota(-))$ of δ-functors are both called the *restriction* morphisms and denoted Res_H^G. In this case, $\mathrm{F}[G]$ is a free (left or right) $\mathrm{F}[H]$-module, and hence the functors $\mathrm{Ind}_H^G := \mathrm{Ind}_\iota$ and $\mathrm{Coind}_H^G := \mathrm{Coind}_\iota$ are both faithfully exact. Here are a couple of applications of this observation.

[18] If $\varphi : G' \to G$ has finite kernel K and $|K| \in \mathrm{F}^\times$, there is a natural transformation $\Phi : \mathrm{Ind}_\varphi \to \mathrm{Coind}_\varphi$ given on an $\mathrm{F}[G']$-module A by $g \otimes a \mapsto \Phi_{g,a}$, where $\Phi_{g,a}(h) := |K|^{-1} \sum_{g' \in \varphi^{-1}(hg)} g'a$ for $g, h \in G$ and $a \in A$. Dually, if $[G : \varphi(G')] < \infty$, there is a natural transformation $\Psi : \mathrm{Coind}_\varphi \to \mathrm{Ind}_\varphi$ given on an $\mathrm{F}[G']$-module A by $\theta \mapsto \sum_{g \in [G/\varphi(G')]} g \otimes \theta(g^{-1})$ for $\theta \in \mathrm{Coind}_\varphi(A)$. If both hold (i.e., $\mathrm{ind}\,\varphi$ is defined), and for $A \in \mathrm{F}[G']\text{-Mod}$, we let $\mathrm{Avg}^K : A \to A^K \hookrightarrow A$ be the averaging map $a \mapsto |K|^{-1} \sum_{g' \in K} g'a$, then there are natural isomorphisms $\Psi \circ \Phi \cong \mathrm{id}_{\mathrm{F}[G]} \otimes \mathrm{Avg}^K$ and $\Phi \circ \Psi \cong \mathrm{Avg}_*^K$. So, if φ is injective (and identified with the inclusion of a finite index subgroup), then $\mathrm{Avg}^K = \mathrm{id}$ and Φ and Ψ are inverse isomorphisms between the induction and coinduction functors. This is the reason that these two are often conflated for finite group representations.

[19] This is because this operation at the level of inhomogeneous cochains is easily seen to induce a δ-functor morphism, so we are done by the universality.

(a) Since $\mathrm{Res}^G_H : \mathrm{F}[G]\text{-Mod} \to \mathrm{F}[H]\text{-Mod}$ is an exact functor taking injectives to injectives (it admits an exact left adjoint Ind^G_H), we conclude that $\mathrm{H}^\bullet(H, \mathrm{Res}^G_H(-)) \cong \mathrm{R}^\bullet(-)^H : \mathrm{F}[G]\text{-Mod} \to \mathrm{F}\text{-Mod}$.[20] If further $[G:H] < \infty$, then the natural transformation $\mathrm{N}^G_H : (-)^H \to (-)^G$, called the *norm* map and given on $A \in \mathrm{F}[G]\text{-Mod}$ by $A^H \ni a \mapsto \sum_{g \in [G/H]} ga \in A^G$, lifts to a morphism $\mathrm{R}^\bullet \mathrm{N}^G_H$ of δ-functors called the *corestriction* or *transfer morphism*[21]

$$\mathrm{Cor}^G_H := \mathrm{R}^\bullet \mathrm{N}^G_H : \mathrm{H}^\bullet(H, \mathrm{Res}^G_H(-)) \to \mathrm{H}^\bullet(G, -).$$

In this case, $\mathrm{Cor}^G_H \circ \mathrm{Res}^G_H \cong [G:H]$, i.e., the composite of restriction and corestriction is given by multiplication by the $[G:H]$, because both operations are endomorphisms of the derived functor $\mathrm{H}^\bullet(G,-)$ which agree on H^0. In particular, if $n > \mathrm{cd}_{\mathrm{F}}(H)$, then $[G:H] \cdot \mathrm{H}^n(G,-) = 0$. Applying this to the case of G finite and $H = \{*\}$ gives a strengthening of the last result of Example 1.1.3: if G is a finite group, $A \in \mathrm{F}[G]\text{-Mod}$, and $n \in \mathbb{Z}_{\geq 1}$, then $\mathrm{UH}^n(G,A)$ has exponent dividing $|G|$.

(b) (Shapiro's Lemma) If $\varepsilon : \mathrm{Res}^G_H \circ \mathrm{Coind}^G_H \to \mathrm{id}$ denotes the counit morphism, then the map

$$\mathrm{H}^\bullet(\iota, \varepsilon) : \mathrm{H}^\bullet(G, \mathrm{Coind}^G_H(-)) \xrightarrow{\sim} \mathrm{H}^\bullet(H, -)$$

is an isomorphism of δ-functors $\mathrm{F}[H]\text{-Mod} \to \mathrm{F}\text{-Mod}$. Indeed, since Coind^G_H is exact and admits an exact left adjoint Res^G_H, it suffices to demonstrate an isomorphism in H^0; but the counit ε evidently induces an isomorphism $(\mathrm{Coind}^G_H(-))^G \xrightarrow{\sim} (-)^H$. In particular, taking $H = \{*\}$ shows that an $\mathrm{F}[G]$-module coinduced from the trivial subgroup is acyclic. As noted above, the unit $\mathrm{id}_{\mathrm{F}[G]\text{-Mod}} \to \mathrm{Coind}^G_{\{*\}} \circ \mathrm{Res}^G_{\{*\}}$ is a pointwise monomorphism,[22] and hence it is an effacement of the group cohomology functor in positive degrees.[23]

Here's a sample application of these morphisms to the vanishing of cohomology groups which often allows us to reduce to the case of p-groups. In the following corollary, we take $\mathrm{F} = \mathbb{Z}$.

Corollary 1.2.3.

(a) Let G be a group and $H \leq G$ a subgroup of finite index $[G:H]$ not divisible by a prime $p \in \mathbb{Z}$. Then the (p)-localized restriction morphism

$$(\mathrm{Res}^G_H)_{(p)} : \mathrm{H}^\bullet(G,-)_{(p)} \to \mathrm{H}^\bullet(H, \mathrm{Res}^G_H(-))_{(p)}$$

is a pointwise monomorphism in all degrees.

(b) Suppose G is a finite group, $A \in \mathbb{Z}[G]\text{-Mod}$ with $\mathrm{U}A \in \mathbb{Z}\text{-Mod}$ finitely generated, and $n \in \mathbb{Z}_{\geq 1}$. If for each prime p, there is a p-Sylow subgroup $G_p \leq G$ with $\mathrm{H}^n(G_p, \mathrm{Res}^G_{G_p} A) = 0$, then $\mathrm{H}^n(G, A) = 0$.

Proof.

(a) By the formula $\mathrm{Cor}^G_H \circ \mathrm{Res}^G_H = [G:H]$, the (p)-localized corestriction provides a retraction.

(b) By Remark 1.1.6(b), $\mathrm{H}^n(G,A)$ is a finite, and so $\mathrm{H}^n(G,A) \hookrightarrow \bigoplus_p \mathrm{H}^n(G,A)_{(p)}$; now apply (a).

□

Example 1.2.4. (Inflation) Let G be a group, $N \trianglelefteq G$ a normal subgroup, and $\pi : G \twoheadrightarrow G/N$ the quotient map. In this case, there is a natural isomorphism

$$\mathrm{Coind}_\pi \cong (-)^N : \mathrm{F}[G]\text{-Mod} \to \mathrm{F}[G/N]\text{-Mod},$$

[20] For this reason, we will often denote $\mathrm{H}^\bullet(H, \mathrm{Res}^G_H(-))$ simply by $\mathrm{H}^\bullet(H,-)$.

[21] For a formula at the level of cochains, see [28, §II.1] or [37, §1.5].

[22] This can also be seen from the fact that it is given on an $A \in \mathrm{F}[G]\text{-Mod}$ by the embedding $A \hookrightarrow \mathrm{Hom}_{\mathrm{F}\text{-Mod}}(\mathrm{F}[G], \mathrm{Res}^G_{\{*\}} A) \cong_{\mathrm{F}\text{-Mod}} \mathscr{C}^1(G,A)$ given by $a \mapsto (g \mapsto ga)$ for $a \in A$ and $g \in G$.

[23] This gives rise to the technique of *dimension shifting*, and is hence the starting point of some treatments of group cohomology as in [8, Ch. IV]; c.f. the proof of Theorem 1.3.1.

and so $(-)^N$ admits an exact left adjoint, namely Res_π. If $i : \mathrm{Res}_\pi \circ (-)^N \to \mathrm{id}$ is the counit of this adjunction, then the morphism $\mathrm{Inf}_G^{G/N} := \mathrm{H}^\bullet(\pi, i) : \mathrm{H}^\bullet(G/N, (-)^N) \to \mathrm{H}^\bullet(G, -)$ is called the *inflation morphism*. Let us only make the (trivial) observation that if $(G, A) \in \mathrm{F\text{-}GrpMod}$, then the natural map

$$\mathrm{Inf} : \mathrm{colim}_{U \trianglelefteq G} \mathrm{H}^\bullet(G/U, A^U) \to \mathrm{H}^\bullet(G, A)$$

is an isomorphism of F-modules, where the colimit is over normal subgroups $U \trianglelefteq G$ with an inclusion $U \trianglelefteq V \trianglelefteq G$ giving rise to the inflation map $\mathrm{Inf}_{G/U}^{G/V} : \mathrm{H}^\bullet(G/V, A^V) \to \mathrm{H}^\bullet(G/U, A^U)$.

Example 1.2.5. (Conjugation) Let G be a group and $H \leq G$ a subgroup. For each $g \in G$, let ${}^gH := gHg^{-1}$, so for $g, g' \in G$, we have ${}^{gg'}H = {}^g({}^{g'}H)$. For each such H and $g \in G$ and $A \in \mathrm{F}[G]\text{-Mod}$, we have a morphism $g : (-)^H \to (-)^{{}^gH}$ of functors $\mathrm{F}[G]\text{-Mod} \to \mathrm{F\text{-}Mod}$ given by left multiplication by g, which gives rise the *conjugation morphism*[24] of δ-functors (see Example 1.2.2(a))

$$\Psi_{H,g} := \mathrm{R}^\bullet g : \mathrm{H}^\bullet(H, \mathrm{Res}_H^G(-)) \to \mathrm{H}^\bullet({}^gH, \mathrm{Res}_{{}^gH}^G(-)).$$

Again, for $g, g' \in G$, we have $\Psi_{H,gg'} = \Psi_{{}^{g'}H,g} \circ \Psi_{H,g'}$ and also $\Psi_{H,g} = \mathrm{id}$ if $g \in H$. In particular, if $N \trianglelefteq G$ is normal, the map $\Psi_{N,-}$ turns $\mathrm{H}^\bullet(N, \mathrm{Res}_N^G(-))$ into an $\mathrm{F}[G/N]$-module.[25]

For the transitivity of (co)restriction and inflation and various compatibilities for different subgroups, see [28, Ch. II] or [37, §1.5]. One final result relating inflation and restriction we will need is

Theorem 1.2.6 (Inflation-Restriction Sequence)**.** *Let G be a group, $N \trianglelefteq G$ a normal subgroup, and $A \in \mathrm{F}[G]\text{-Mod}$. If $n \in \mathbb{Z}_{\geq 1}$ is such that for all $i = 1, \ldots, n-1$, we have $\mathrm{H}^i(N, A) = 0$, then the sequence*

$$0 \to \mathrm{H}^n(G/N, A^N) \xrightarrow{\mathrm{Inf}_G^{G/N}} \mathrm{H}^n(G, A) \xrightarrow{\mathrm{Res}_N^G} \mathrm{H}^n(N, A)$$

is exact.

Proof. This follows from an explicit check using formulae for $n = 1$, and dimension shifting for $n > 1$ ([37, 1.6.7]). An alternative (and better) proof is afforded by considering the Lyndon-Hochschild-Serre spectral sequence ([37, §2.4]), which is the Grothendieck spectral sequence associated to the composition

$$\mathrm{F}[G]\text{-Mod} \xrightarrow{(-)^N} \mathrm{F}[G/N]\text{-Mod} \xrightarrow{(-)^{G/N}} \mathrm{F\text{-}Mod}.$$

□

1.3 The Cup Product

One final tool in (abstract) group cohomology we will need is the cup product. For this, if $A, B \in \mathrm{F}[G]\text{-Mod}$, then the tensor product $A \otimes_\mathrm{F} B$ can be made into an $\mathrm{F}[G]$-module via the *diagonal action*, i.e., for $a \in A, b \in B$ and $g \in G$, we have $g \cdot (a \otimes b) = ga \otimes gb$. Further, there is a natural map $A^G \otimes_\mathrm{F} B^G \to (A \otimes_\mathrm{F} B)^G$ which for general homological algebra reasons gives rise to a product mapping in group cohomology. We summarize the basic results in

[24] Explicitly for $A \in \mathrm{F}[G]\text{-Mod}$, consider the morphism $(c, g) : (H, \mathrm{Res}_H^G A) \to ({}^gH, \mathrm{Res}_{{}^gH}^G A)$ in $\mathrm{F\text{-}GrpMod}^*$ given by the inverse conjugation $c : {}^gH \to H$ and left-multiplication by $g : \mathrm{Res}_c \circ \mathrm{Res}_H^G A \to \mathrm{Res}_{{}^gH}^G A$. Then $\Psi_{H,g} = \mathrm{H}^\bullet(c, g)$.

[25] In effect, we have described the derived functor $\mathrm{R}^\bullet(-)^N : \mathrm{F}[G]\text{-Mod} \to \mathrm{F}[G/N]\text{-Mod}$ of the functor $(-)^N$ described in Example 1.2.4.

Theorem 1.3.1 (Cup Product)**.** *There is a unique family of homomorphisms, called the* cup product*,*

$$\smile : \mathrm{H}^p(G, A) \otimes_{\mathrm{F}} \mathrm{H}^q(G, B) \to \mathrm{H}^{p+q}(G, A \otimes_{\mathrm{F}} B)$$

defined for all $p, q \in \mathbb{Z}_{\geq 0}$ and $A, B \in \mathrm{F}[G]$-Mod, functorial in F, G, A, and B, such that (a)-(c) hold.

(a) For $A, B \in \mathrm{F}[G]$-Mod, the product agrees with the above map $A^G \otimes_{\mathrm{F}} B^G \to (A \otimes_{\mathrm{F}} B)^G$ for $p = q = 0$.

(b) If $0 \to A' \to A \to A'' \to 0$ is an exact sequence of $\mathrm{F}[G]$-modules, and $B \in \mathrm{F}[G]$-Mod such that the sequence $0 \to A' \otimes_{\mathrm{F}} B \to A \otimes_{\mathrm{F}} B \to A'' \otimes_{\mathrm{F}} B \to 0$ is also exact, then for all $p, q \in \mathbb{Z}_{\geq 0}$ and $a'' \in \mathrm{H}^p(G, A'')$ and $b \in \mathrm{H}^q(G, B)$, we have

$$\delta(a'' \smile b) = \delta(a'') \smile b \in \mathrm{H}^{p+q+1}(G, A' \otimes_{\mathrm{F}} B).$$

(c) If $0 \to B' \to B \to B'' \to 0$ is a an exact sequence of $\mathrm{F}[G]$-modules and if $A \in \mathrm{F}[G]$-Mod such that the sequence $0 \to A \otimes_{\mathrm{F}} B' \to A \otimes_{\mathrm{F}} B \to A \otimes_{\mathrm{F}} B'' \to 0$ is also exact, then for all $p, q \in \mathbb{Z}_{\geq 0}$ and $a \in \mathrm{H}^p(G, A)$ and $b \in \mathrm{H}^q(G, B'')$, we have

$$\delta(a \smile b'') = (-1)^p a \smile \delta(b'').$$

Further, the cup product is associative and graded commutative, compatible with restriction and inflation maps, and satisfies a projection formula *for finite index subgroups $H \leq G$.*[26]

Proof. Uniqueness is proven by *dimension shifting* as follows. For each $A \in \mathrm{F}[G]$-Mod, turn the effacement of Example 1.2.2(b) into a short exact sequence $0 \to A \to \mathscr{C}^1(G, A) \to A'' \to 0$ of $\mathrm{F}[G]$-modules. The map $\mathscr{C}^1(G, A) \to A$ given by $f \mapsto f(1)$ is an F-module retraction of the effacement, so the corresponding sequence of F-modules splits and for any $B \in \mathrm{F}[G]$-Mod, the sequence

$$0 \to A \otimes_{\mathrm{F}} B \to \mathscr{C}^1(G, A) \otimes_{\mathrm{F}} B \to A'' \otimes_{\mathrm{F}} B \to 0$$

is still exact. Then the acyclicity of $\mathscr{C}^1(G, A)$ along with (a) and (b) determines all products for $p \in \mathbb{Z}_{\geq 0}$ and $q = 0$. The same argument with A and B swapped and using (a) and (c) proves the result.

Existence can be proven either using the δ-functor formalism ([28, Ch. IV]), or using projective resolutions ([8, §IV.7] or [13, §3.4]), or very explicitly using inhomogeneous cochains ([15, Ch. 12] or [37, §1.4]). The last approach is exceedingly simple and amenable to concrete computation: for each $p, q \in \mathbb{Z}_{\geq 0}$, we define a map $\smile : \mathscr{C}^p(G, A) \otimes_{\mathrm{F}} \mathscr{C}^q(G, B) \to \mathscr{C}^{p+q}(G, A \otimes_{\mathrm{F}} B)$ by the formula

$$(\sigma \smile \tau)(g_1, \ldots, g_{p+q}) := \sigma(g_1, \ldots, g_p) \otimes g_1 g_2 \cdots g_p \tau(g_{p+1}, \ldots, g_{p+q}) \tag{1.2}$$

for $\sigma \in \mathscr{C}^p(G, A), \tau \in \mathscr{C}^q(G, B)$, and $g_1, \ldots, g_{p+q} \in G$. In this case, it follows from the equality

$$\partial^{p+q}(\sigma \smile \tau) = \partial^p \sigma \smile \tau + (-1)^p \sigma \smile \partial^q \tau \tag{1.3}$$

obtained by direct calculation that the product defined by (1.2) descends to give a product on the cohomology. The remaining properties that need to be checked follow either for formal reasons ([28, Ch. IV]) or using the explicit formulae.[27] □

[26] Explicitly, this says that if $H \leq G$ is a finite index subgroup, then for each $A \in \mathrm{F}[H]$-Mod, $B \in \mathrm{F}[G]$-Mod, $p, q \in \mathbb{Z}_{\geq 0}$, and $x \in \mathrm{H}^p(H, A)$ and $y \in \mathrm{H}^q(G, B)$, we have

$$\mathrm{Cor}(x \smile \mathrm{Res}(y)) = \mathrm{Cor}(x) \smile y.$$

The other claims are similarly clunky to formulate but entirely straightforward (see [8, Prop. IV.9] or [15, Prop. 12.40]).

[27] C.f. [5, Ch. II, Thm. 7.1]. Using Remark 1.1.6(c) and the formula (1.2) (or rather its homogeneous analog), one can show that these cup products agree with those in simplicial cohomology for the standard simplicial model of the Eilenberg-MacLane space $\mathrm{K}(G, 1)$, and hence that they agree with topological cup products when group cohomology is computed as in Example 1.1.4.

1.4 Tate Cohomology

In this section, we follow [8, §IV.6], [36, Part I], and [37, Ch. 1]. When G is a finite group, the group homology and cohomology groups can be spliced together to make the *Tate cohomology groups* $\hat{\mathrm{H}}^\bullet(G,-)$, which are very useful and can be computed from an analog of projective resolutions of F called *complete resolutions*. We need the following notation: given a finite group G, we let $\mathrm{N}_G := \sum_{g\in G} g \in \mathrm{F}[G]\text{-Mod}$ (the "norm of G"), and $\mathrm{I}_G := \ker(\varepsilon)$ where $\varepsilon : \mathrm{F}[G] \to \mathrm{F}$ is given by $g \mapsto 1$ for all $g \in G$ (the "augmentation ideal").

Definition 1.4.1 (Tate Cohomology)**.** *For a finite group G and $A \in \mathrm{F}[G]\text{-Mod}$, the* Tate cohomology groups $\hat{\mathrm{H}}^\bullet(G,A)$ *of G with coefficients in A are defined to be*

$$\hat{\mathrm{H}}^n(G,A) := \begin{cases} \mathrm{H}^n(G,A), & \text{if } n \geq 1, \\ A^G/\mathrm{N}_G\, A, & \text{if } n = 0, \\ A[\mathrm{N}_G]/\mathrm{I}_G A & \text{if } n = -1, \text{ and} \\ \mathrm{H}_{-(n+1)}(G,A), & \text{if } n \leq -2, \end{cases}$$

where as usual $A[\mathrm{N}_G] := \{a \in A : \mathrm{N}_G\, a = 0\}$.

Example 1.4.2 (Cyclic Groups)**.** Let $n \in \mathbb{Z}_{\geq 1}$. If $G = C_n = \langle x | x^n \rangle$, then $\mathrm{F}[G] = \mathrm{F}[x]/(x^n - 1)$ and $\mathrm{N}_G = \sum_{j=0}^{n-1} x^j$. For any $A \in \mathrm{F}[G]\text{-Mod}$, we have

$$\hat{\mathrm{H}}^n(G,A) \cong \begin{cases} A[\mathrm{N}_G]/(1-x)A & \text{if } n \text{ is odd, and} \\ A^G/\mathrm{N}_G\, A & \text{if } n \text{ is even.} \end{cases}$$

This is proven by considering the complete resolution

$$\cdots \xrightarrow{\cdot \mathrm{N}_G} \mathrm{F}[G] \xrightarrow{\cdot(1-x)} \mathrm{F}[G] \xrightarrow{\cdot \mathrm{N}_G} \mathrm{F}[G] \xrightarrow{\cdot(1-x)} \mathrm{F}[G] \xrightarrow{\cdot \mathrm{N}_G} \cdots .$$

Alternatively, one could truncate the above resolution as $\cdots \xrightarrow{\mathrm{N}_G} \mathrm{F}[G] \xrightarrow{\cdot(1-x)} \mathrm{F}[G] \xrightarrow{\varepsilon} \mathrm{F} \to 0$ to get an honest projective (even free) resolution of F, and then use Remarks 1.1.2(d),(e) and Definition 1.4.1. See, e.g., [8, §IV.8]. In particular, the Tate cohomology groups are 2-periodic. Taking $A = \mathrm{F}$ to be the trivial module, we have $\mathrm{H}^2(G,\mathrm{F}) \cong \mathrm{F}/n\mathrm{F}$, so that if $n = |G|$ is not a unit in F, then in particular $\mathrm{cd}_{\mathrm{F}}(G) = \infty$; c.f. Example 1.1.4 and the computation of the (co)homology using the lens space models of $\mathrm{K}(C_n, 1)$ with various coefficient groups, e.g., in [20, Example 2.43 and Exercise 3.1.10].

Remark 1.4.3. Much of the above theory of group cohomology can be extended to Tate cohomology; here we summarize the key points; for proofs, see [8, Ch. IV] or [37, Ch. 1].

(a) A short exact sequence $0 \to A \to B \to C \to 0$ of $\mathrm{F}[G]\text{-Mod}$-modules naturally gives rise to a bi-infinite long exact sequence of F-modules in Tate cohomology:

$$\hat{\mathrm{H}}^\bullet(G,A) \to \hat{\mathrm{H}}^\bullet(G,B) \to \hat{\mathrm{H}}^\bullet(G,C) \xrightarrow{\delta} \hat{\mathrm{H}}^{\bullet+1}(G,A).$$

This follows from splicing together the long exact sequences in homology and cohomology along with easy explicit checks near degrees $n = 0, -1$.

(b) For a subgroup $H \leq G$, there are restriction and corestriction maps

$$\mathrm{Res}^G_H : \hat{\mathrm{H}}^\bullet(G,-) \rightleftarrows \hat{\mathrm{H}}^\bullet(H,-) : \mathrm{Cor}^G_H$$

such that $\mathrm{Cor}^G_H \circ \mathrm{Res}^G_H = [G:H]$. In particular, $\mathrm{U}\hat{\mathrm{H}}^\bullet(G,-)$ has exponent dividing $|G|$.[28]

[28] There is, however, no analog of the inflation map in Tate cohomology (in negative degrees).

(c) ([15, Cor. 12.6]) If $A \in \mathrm{F}\text{-Mod}$, then for any $H \leq G$, we have $\hat{\mathrm{H}}^\bullet(H, \mathrm{Coind}_{\{*\}}^G A) = 0$.[29]
(d) The results of Corollary 1.2.3 remain true in this setting for all $n \in \mathbb{Z}$ (with the same proof).
(e) ([15, Cor. 12.9], "Dimension Shifting") Given an $A \in \mathrm{F}[G]\text{-Mod}$ and $n \in \mathbb{Z}$, there is an $A(n) \in \mathrm{F}[G]\text{-Mod}$ such that $\hat{\mathrm{H}}^\bullet(G, A(n)) \cong \hat{\mathrm{H}}^{\bullet+n}(G, A)$.
(f) There is an extension of the cup product to all degrees in Tate cohomology with similar properties.

In closing this chapter, we mention two important results due Tate which are most directly useful for arithmetic applications. For this we need one definition.

Definition 1.4.4 (Cohomological Triviality)**.** *Let G be a finite group, $A \in \mathrm{F}[G]\text{-Mod}$, and $n \in \mathbb{Z}$. We say that A is*
(a) cohomologically trivial in degree n *if for all subgroups $H \leq G$, we have $\hat{\mathrm{H}}^n(H, A) = 0$, and*
(b) cohomologically trivial *if it is so in each degree $n \in \mathbb{Z}$.*

In 1.4.5-1.4.7, we fix the hypothesis that G is a finite group and $A \in \mathbb{Z}[G]\text{-Mod}$. We follow [36, §1.7].

Theorem 1.4.5 (Tate)**.** *If A is cohomologically trivial in two adjacent degrees, then it is so in all degrees.*

Proof. By Remark 1.4.3(e), we reduce to the case where A is cohomologically trivial in degrees 1 and 2, and we need to show that it is so in degrees 0 and 3. By induction on $|G|$, suppose this is true for all proper $H \leq G$ and reduce to the case $H = G$. By Remark 1.4.3(d), reduce to the case that G is a nontrivial p-group for some prime p. Pick a normal subgroup $N \trianglelefteq G$ of index p, and use Theorem 1.2.6 to get isomorphisms $\mathrm{Inf}_G^{G/N} : \mathrm{H}^n(G/N, A^N) \to \mathrm{H}^n(G, A)$ for $n \in \{1, 2, 3\}$. Now $\mathrm{H}^1(G, A) = 0$ implies $\mathrm{H}^1(G/N, A^N) = 0$ so by Example 1.4.2, $\mathrm{H}^3(G/N, A^N) = 0$ and hence $\mathrm{H}^3(G, A) = 0$. From $\mathrm{H}^2(G, A) = 0$, again by Example 1.4.2 we have $\hat{\mathrm{H}}^0(G/N, A^N) = 0$, so that $A^G = (A^N)^{G/N} = \mathrm{N}_{G/N} A^N$. But $\hat{\mathrm{H}}^0(N, A) = 0$ implies $A^N = \mathrm{N}_N A$, and so $A^G = \mathrm{N}_{G/N}(\mathrm{N}_N A) = \mathrm{N}_G A$, i.e., $\hat{\mathrm{H}}^0(G, A) = 0$. □

We need a small lemma.

Lemma 1.4.6. *Suppose $n \in \mathbb{Z}$ is such that for each subgroup $H \leq G$, the cohomology $\hat{\mathrm{H}}^n(H, A)$ is cyclic of order $|H|$. If $a \in \hat{\mathrm{H}}^n(G, A)$ is a generator, then $\mathrm{Res}_H^G a \in \hat{\mathrm{H}}^n(H, A)$ is a generator for all $H \leq G$.*

Proof. Since $\mathrm{Cor}_H^G \circ \mathrm{Res}_H^G a = [G : H]a$ (Remark 1.4.3(b)), $|H|$ divides the order of $\mathrm{Res}_H^G a$. □

The key result we will use in the next chapter is

Theorem 1.4.7 (Tate-Nakayama)**.** *Suppose that A is cohomologically trivial in degree 1 and for each subgroup $H \leq G$, the group $\mathrm{H}^2(H, A)$ is cyclic of order $|H|$. If $a \in \mathrm{H}^2(G, A)$ is a generator, then for each subgroup $H \leq G$, the cup product induces abelian group isomorphisms*

$$\mathrm{Res}_H^G a \smile - : \hat{\mathrm{H}}^\bullet(H, \mathbb{Z}) \xrightarrow{\sim} \hat{\mathrm{H}}^{\bullet+2}(H, A).$$

In particular, we get an isomorphism $H^{\mathrm{ab}} \to A^H / \mathrm{N}_H A$.

Proof Sketch. ([36, I.7.3], [37, 3.1.4]) By Lemma 1.4.6, we are reduced to the case $H = G$. By dimension shifting (Remark 1.4.3(e)) and naturality of the cup product (Remark 1.4.3(f)), switch to showing instead that when A is cohomologically trivial in degree -1, for each subgroup $H \leq G$, the group $\hat{\mathrm{H}}^0(H, A)$ is cyclic of order $|H|$, and $a \in \hat{\mathrm{H}}^0(G, A)$ is a generator, then $a \smile - : \hat{\mathrm{H}}^\bullet(G, \mathbb{Z}) \to \hat{\mathrm{H}}^\bullet(G, A)$ is an isomorphism.

If we lift a to $\tilde{a} \in A^G$, the corresponding map $\mathbb{Z} \to A$ given by $\tilde{a}$ (which induces the cup product $a \smile -$ in cohomology) need not be injective, but we can remedy this by replacing A by $A \oplus \mathbb{Z}[G]$ and $\tilde{a}$ by $(\tilde{a}, \mathrm{N}_G)$.

[29] Here we continue the notational abuse of Footnote 20. This statement says that coinduced modules are cohomologically trivial (see Definition 1.4.4).

Indeed, the inclusion $A \to A \oplus \mathbb{Z}[G]$ induces an isomorphism in cohomology by Remark 1.4.3(c), and we are using the naturality of cup products (Remark 1.4.3(f)). Having done this, fit $\tilde{a}$ into a short exact sequence $0 \to \mathbb{Z} \xrightarrow{\tilde{a}} A \to B \to 0$ of $\mathbb{Z}[G]$-modules, and for each $H \leq G$ consider the long exact sequence in Tate cohomology of H (Remark 1.4.3(a)). We have $\hat{\mathrm{H}}^{-1}(H, A) = 0$ (hypothesis), $\hat{\mathrm{H}}^{1}(H, \mathbb{Z}) \cong \mathrm{Hom}_{\mathrm{Grp}}(H, \mathbb{Z}) = 0$ (Remark 1.1.6(a) and $|H| < \infty$), and $\hat{\mathrm{H}}^{0}(H, \tilde{a})$ is an isomorphism (Lemma 1.4.6), so that by the long exact sequence, $\hat{\mathrm{H}}^{-1}(H, B) = \hat{\mathrm{H}}^{0}(H, B) = 0$. By Theorem 1.4.5, B is cohomologically trivial and so again by the long exact sequence, the map $a \smile - = \hat{\mathrm{H}}^{\bullet}(G, \tilde{a})$ is an isomorphism.

The last result follows from considering degree $\bullet = -2$; then $\hat{\mathrm{H}}^{-2}(H, \mathbb{Z}) := \mathrm{H}_1(H, \mathbb{Z}) \cong H^{\mathrm{ab}}$ (Example 1.1.4) and $\hat{\mathrm{H}}^{1}(H, A) \cong A^H / \mathrm{N}_H A$ (Definition 1.4.1). □

2 Galois Cohomology

In arithmetic applications, we are often interested in studying the continuous action of a profinite group on a discrete module, the prototypical example being that of *Galois cohomology*, i.e., when the absolute Galois group of a perfect field acts on the (set of algebraic-closure-valued) points of a (commutative) algebraic group. To apply group cohomology to this setting, we need to modify the definition of the "abstract" cohomology groups from the previous chapter to account for the topology, just as is needed for the fundamental theorem of infinite Galois theory. In the first section below, we explain how to do this and define profinite group cohomology; having done this, much of the theory from the previous chapter is seen to extend immediately to the profinite setting. Following this, we define Galois cohomology as a special case of profinite cohomology and study some classical examples. In the third section, we define the notion of a class formation and show how the Tate-Nakayama theorem implies the fundamental theorem of abstract class field theory, illustrating with examples from local and global class field theory. Finally, we outline the local duality theorem of Tate, the Tate-Poitou exact sequence, and Tate's theorem on global Euler-Poincaré characteristics, which will be key ingredients in Tate's proof of the isogeny invariance of the BSD conjecture.

We will assume familiarity with profinite groups ([8, §V.1], [42, Ch. 2]), the basic theory of algebraic groups over a field ([34, Ch. 1-11]), and the basic structure theory for local and global number fields ([7], [8, Ch. I-II], [36, §II.3, III.1-2]). The following is taken from [8], [9], [15], [17], [37], [42], [43], and [44].

2.1 Profinite Cohomology

There are (at least) three ways to extend group cohomology to the profinite setting, namely
(a) using the δ-functor formalism by showing that the category of discrete modules has enough injectives,
(b) using an analog of the bar resolution involving continuous cochains, and
(c) by defining profinite cohomology as a colimit of finite group cohomology.

One must then show that these agree with each other. We now explain how to do this, following [9].

Let F be a fixed (commutative unitary) ring and G be a *profinite* group.[30]

Lemma 2.1.1. *(Discrete G-Sets) Let X be a G-set. The following are equivalent.*
(a) The G-action on X is continuous when X is given the discrete topology.
(b) For any $x \in X$, the stabilizer $G_x \subset G$ is an open subgroup.
(c) We have $X = \bigcup_U X^U$, where the union is over open subgroups $U \subset G$.

Proof. When X is discrete, the action $G \times X \to X$ is continuous iff for each $x, y \in G$, the subset $\{g \in G : gx = y\}$ is open, but this subset is either empty or a coset and translate of the stabilizer G_x. □

Definition 2.1.2 (Discrete G-Modules)**.** *The category $\mathrm{F}[G]\text{-}\mathrm{Mod}^{\mathrm{disc}}$ of* discrete $\mathrm{F}[G]$-modules *is the full additive subcategory of $\mathrm{F}[G]\text{-}\mathrm{Mod}$ comprising modules on which the G-action satisfies the equivalent conditions of Lemma 2.1.1.*

Since $\mathrm{F}[G]\text{-}\mathrm{Mod}^{\mathrm{disc}}$ is evidently closed under taking kernels and cokernels, it is an abelian category and the inclusion functor $\mathrm{F}[G]\text{-}\mathrm{Mod}^{\mathrm{disc}} \to \mathrm{F}[G]\text{-}\mathrm{Mod}$ is exact.

Theorem 2.1.3. *The subcategory $\mathrm{F}[G]\text{-}\mathrm{Mod}^{\mathrm{disc}} \hookrightarrow \mathrm{F}[G]\text{-}\mathrm{Mod}$ is coreflective and so has enough injectives.*

Proof. The *discretization* functor $\mathrm{disc} : \mathrm{F}[G]\text{-}\mathrm{Mod} \to \mathrm{F}[G]\text{-}\mathrm{Mod}^{\mathrm{disc}}$ given on objects by

$$A \mapsto A^{\mathrm{disc}} := \{x \in A : G_x \subset G \text{ is open}\}$$

is right adjoint to the exact inclusion functor. Therefore, if $A \in \mathrm{F}[G]\text{-}\mathrm{Mod}^{\mathrm{disc}}$ and $A \hookrightarrow J$ is an injective envelope in $\mathrm{F}[G]\text{-}\mathrm{Mod}$, then $A \xrightarrow{\sim} A^{\mathrm{disc}} \hookrightarrow J^{\mathrm{disc}}$ is an injective envelope in $\mathrm{F}[G]\text{-}\mathrm{Mod}^{\mathrm{disc}}$. □

[30] Note that some of the initial results only use that G is a topological group.

This theorem allows us to repeat the theory of the previous chapter with minimal modifications; here we briefly mention the salient points.

Definition 2.1.4 (Profinite Cohomology)**.** *The* profinite group cohomology of G in discrete F-modules, *denoted* $\mathrm{H}^\bullet(G,-)$,[31] *is the right derived functor of the left exact functor* $(-)^G : \mathrm{F}[G]\text{-}\mathrm{Mod}^{\mathrm{disc}} \to \mathrm{F}\text{-}\mathrm{Mod}$ *of* G*-invariants, i.e.,*

$$\mathrm{H}^\bullet(G,-) := \mathrm{R}^\bullet(-)^G : \mathrm{F}[G]\text{-}\mathrm{Mod}^{\mathrm{disc}} \to \mathrm{F}\text{-}\mathrm{Mod}.$$

Remark 2.1.5. As in §1.2, profinite cohomology groups are functorial for continuous homomorphisms of profinite groups: if $\varphi : G' \to G$ is a continuous morphism of profinite groups, then we get a functor $\mathrm{Res}_\varphi : \mathrm{F}[G]\text{-}\mathrm{Mod}^{\mathrm{disc}} \to \mathrm{F}[G']\text{-}\mathrm{Mod}^{\mathrm{disc}}$, and as in Definition 1.2.1 we can define $\mathrm{Lif}^\bullet_\varphi$. Similarly, we have analogs of (co)induced modules,[32] (co)restriction maps for closed subgroups $H \leq_{\mathrm{c}} G$,[33] Shapiro's Lemma, inflation maps for closed normal $N \trianglelefteq_{\mathrm{c}} G$, the conjugation morphism, the Lyndon-Hochschild-Serre spectral sequence, the inflation-restriction sequence, cup products, and even Tate cohomology.[34] These can either be developed as in the previous section (see, e.g., [42, Ch. 6]), or as the colimits of the corresponding operations (or results) for the finite case, as we explain below.

For a profinite group G, a discrete $\mathrm{F}[G]$-module A, and $n \in \mathbb{Z}_{\geq 0}$, we let $\mathscr{C}^n_{\mathrm{cts}}(G,A) := \mathrm{Hom}_{\mathrm{Top}}(G^n, A)$ denote the set of continuous maps $G^n \to A$. This is naturally an F-module, called the module of *continuous inhomogeneous* n*-cochains on* G *with values in* A. The same formula from Example 1.1.5 (using Lemma 2.1.1) defines a differential $\partial^\bullet$ making $(\mathscr{C}^\bullet_{\mathrm{cts}}(G,A), \partial^\bullet)$ a complex of F-modules, and we define $\mathscr{Z}^\bullet_{\mathrm{cts}}$, $\mathscr{B}^\bullet_{\mathrm{cts}}$, and $\mathrm{H}^\bullet_{\mathrm{cts}}$ analogously. As previously, each open normal subgroup $U \trianglelefteq_{\mathrm{o}} G$ gives rise to an inflation map $\mathrm{Inf} : \mathscr{C}^\bullet(G/U, A^U) \to \mathscr{C}^\bullet_{\mathrm{cts}}(G,A)$, where, importantly, on the left G/U is *finite* and so we may drop the subscript "cts," and that the image lies in $\mathscr{C}^\bullet_{\mathrm{cts}}(G,A)$ uses that U is open. Gluing these as in Example 1.2.4 yields a map $\mathrm{Inf} : \mathrm{colim}_{U \trianglelefteq_{\mathrm{o}} G} \mathscr{C}^\bullet(G/U, A^U) \to \mathscr{C}^\bullet_{\mathrm{cts}}(G,A)$.

Lemma 2.1.6. *For a profinite* G *and* $A \in \mathrm{F}[G]\text{-}\mathrm{Mod}^{\mathrm{disc}}$*, the inflation map above is an isomorphism of* F*-chain complexes. In particular, it induces an isomorphism* $\mathrm{Inf} : \mathrm{colim}_{U \trianglelefteq_{\mathrm{o}} G} \mathrm{H}^\bullet(G/U, A^U) \xrightarrow{\sim} \mathrm{H}^\bullet_{\mathrm{cts}}(G,A)$.

Proof. The first statement is clear from Lemma 2.1.1, and (co)homology commutes with direct limits. □

Theorem 2.1.7. *For a profinite* G*, there is a natural isomorphism of* δ*-functors* $\mathrm{H}^\bullet(G,-) \cong \mathrm{H}^\bullet_{\mathrm{cts}}(G,-)$.

In other words, derived functor profinite cohomology can be computed via continuous cochains. The δ-functor structure on $\mathrm{H}^\bullet_{\mathrm{cts}}(G,-)$ will be produced in the course of the proof.

Proof. It suffices to show that $\mathrm{H}^\bullet_{\mathrm{cts}}(G,-)$ defines an exact δ-functor extending $(-)^G$ on $\mathrm{F}[G]\text{-}\mathrm{Mod}^{\mathrm{disc}}$, and that it is effaceable in positive degrees. It is definitionally clear that $\mathrm{H}^0_{\mathrm{cts}}(G,-) \cong (-)^G$. Further, if $0 \to A \to B \to C \to 0$ is an exact sequence of discrete $\mathrm{F}[G]$-modules, then the corresponding sequence of chain complexes $0 \to \mathscr{C}^\bullet_{\mathrm{cts}}(G,A) \to \mathscr{C}^\bullet_{\mathrm{cts}}(G,B) \to \mathscr{C}^\bullet_{\mathrm{cts}}(G,C) \to 0$ is also exact, where we are using Lemma 2.1.6 for C and that the quotients G/U for $U \trianglelefteq_{\mathrm{o}} G$ are all finite. Taking long exact sequence in cohomology shows how to give $\mathrm{H}^\bullet_{\mathrm{cts}}(G,-)$ the structure on an exact δ-functor. It remains to show that $\mathrm{H}^n_{\mathrm{cts}}(G,-)$ is

[31] When considering a profinite group G, there is an apparent clash in notation between Definitions 1.1.1 and 2.1.4, and these are in general different ([9, Ex. 2.5]). We define $\mathrm{H}^\bullet(G,-)$ to mean the latter, since there is no reason to consider the "abstract" group cohomology of Definition 1.1.1 for profinite groups G. When G is *finite*, there is no notational clash since every $\mathrm{F}[G]$-module is discrete.

[32] For instance, in the above setting, define for $A \in \mathrm{F}[G']\text{-}\mathrm{Mod}$ the coinduced module $\mathrm{Coind}_\varphi(A)$ to be the module of all *continuous* G'-equivariant set maps $G \to A$. Most other constructions work after inserting the word "continuous" in a suitable place.

[33] For the corestriction map, we also need, as before, H to be of finite index; in this case, that is equivalent to saying H is open. Again, the relation $\mathrm{Cor}^G_H \circ \mathrm{Res}^G_H = [G:H]$ holds.

[34] For this last, see [37, §1.9].

effaceable for $n \in \mathbb{Z}_{\geq 1}$. This follows from Lemma 2.1.6 and the observation that if $J \in \mathrm{F}[G]\text{-}\mathrm{Mod}^{\mathrm{disc}}$ is injective, then for all $U \trianglelefteq_{\mathrm{o}} G$, the module $J^U \in \mathrm{F}[G/U]\text{-}\mathrm{Mod}$ is injective. This last result, in turn, follows from the fact that $(-)^U : \mathrm{F}[G]\text{-}\mathrm{Mod}^{\mathrm{disc}} \to \mathrm{F}[G/U]\text{-}\mathrm{Mod}$ admits an exact left adjoint, namely restriction along the projection $\pi_U : G \twoheadrightarrow G/U$.[35] □

Remark 2.1.8. That profinite group cohomology can be computed using continuous cochains has consequences similar to those of the computation of (abstract) group cohomology using cochains.

(a) Similarly to Remark 1.1.6(a), if a profinite group G acts trivially on an F-module A, then we have $\mathrm{H}^1(G, A) \cong_{\mathrm{F}\text{-}\mathrm{Mod}} \mathrm{Hom}^{\mathrm{cts}}_{\mathrm{Grp}}(G, A)$. If $A = \mathbb{Q}$, then Example 1.1.3 and Lemma 2.1.6 tell us still that $\mathrm{H}^n(G, \mathbb{Q}) = 0$ for $n \in \mathbb{Z}_{\geq 1}$, and again we get an isomorphism $\mathrm{H}^2(G, \mathbb{Z}) \cong \mathrm{Hom}^{\mathrm{cts}}_{\mathrm{Grp}}(G, \mathbb{Q}/\mathbb{Z})$.

(b) Similarly to Remarks 1.1.2(c) and 1.1.6(b), the groups $\mathrm{H}^\bullet(G, -)$ are "independent of F"; consequently, in what follows, we will stick to $\mathrm{F} = \mathbb{Z}$. Further, if $A \in \mathbb{Z}[G]\text{-}\mathrm{Mod}^{\mathrm{disc}}$, then it follows from Example 1.2.2(b) and Lemma 2.1.6 that $\mathrm{H}^n(G, A)$ is a torsion group for each $n \in \mathbb{Z}_{\geq 1}$.

(c) It is easy to see that for an $A \in \mathrm{F}[G]\text{-}\mathrm{Mod}^{\mathrm{disc}}$, the natural map $\mathrm{H}^1_{\mathrm{cts}}(G, A) \to \mathrm{H}^1_{\mathrm{abs}}(G, A)$ is injective, where we use the temporary notation on the right to denote the "abstract" cohomology group (forgetting the topology). Under the identification on Theorem 1.1.8, the subgroup $\mathrm{H}^1(G, A) = \mathrm{H}^1_{\mathrm{cts}}(G, A) \subset \mathrm{H}^1_{\mathrm{abs}}(G, A)$ classifies isomorphism classes of *discrete* A-torsors, i.e., A-torsors X such that X is a discrete G-set in the sense of Lemma 2.1.1 (c.f. Example 2.2.9). Similarly to Remark 1.1.9(b), the second cohomology group $\mathrm{H}^2(G, A)$ classifies profinite extensions of G by A ([42, §6.8]), and there is an analog of the first nonabelian cohomology group to the setting of profinite cohomology (at least in the case of Galois cohomology–see [44, §5.1 and Ch. III]).

(d) In the above approach, we have apparently defined two distinct "inflation" morphisms $\mathrm{Inf} : \mathrm{colim}_{U \trianglelefteq_{\mathrm{o}} G} \mathrm{H}^\bullet(G/U, (-)^U) \to \mathrm{H}^\bullet(G, -)$: one coming from the inflation maps of the δ-functor formalism (Remark 2.1.5), and one coming from combining Lemma 2.1.6 and Theorem 2.1.7. In fact, these two maps agree. For this delicate point, see [9, §4].

2.2 Classical Examples of Galois Cohomology

In this section, we review some basic facts from the theory of algebraic groups (from [12], [34], and [40]), define Galois cohomology, and see some classical examples ([8, §V.2]).

Let K be a field. A *variety* over K (or K-*variety*) is a separated scheme of finite type over K; a morphism of K-varieties is a K-scheme morphism. By an *algebraic group* over K, we mean a group object in the category of K-varieties. We denote by $\mathscr{G}\mathrm{rp}_K$ the category of *commutative* algebraic groups over K; key examples are the additive group $\mathbb{G}_a$, the multiplicative group $\mathbb{G}_m$, for each $n \in \mathbb{Z}_{\geq 1}$ the group μ_n of n^{th} roots of unity, and abelian varieties and kernels of their isogenies (§3.1). We will need

Theorem 2.2.1 (Algebraic Groups)**.** *Let K be a field.*

(a) The category $\mathscr{G}\mathrm{rp}_K$ is abelian.

(b) If L/K is a field extension, the basechange functor $\mathscr{G}\mathrm{rp}_K \to \mathscr{G}\mathrm{rp}_L$ is exact.

(c) If K^{a}/K is an algebraic closure of K, the functor $\mathscr{G}\mathrm{rp}_K \to \mathrm{Ab}$ given by $A \mapsto A(K^{\mathrm{a}})$ is exact.

Proof.

(a) See [12, 4.41], [34, 5.62], or [40, 5.2.12]. We only remark that a quotient map (i.e., epimorphism) in this category is a faithfully flat[36] homomorphism, and that a sequence $1 \to A \to B \to C \to 1$ is exact iff $B \to C$ is a quotient map and A maps isomorphically to its kernel.[37]

[35] That this restriction map maps to *discrete* G/U modules is where we use that U is open!

[36] When the codomain is reduced, surjectivity of the underlying map of topological spaces implies flatness; see [34, 1.70].

[37] The existence of quotients is subtle and the key technical result needed for the proof of this theorem. The construction of quotients in the affine case is classical [34, §5c]. Perhaps the best way to construct quotients in general is to embed $\mathscr{G}\mathrm{rp}_K$

(b) Faithful flatness is stable under base change, and so is the formation of kernels (both are limits).
(c) By (b), assume $K = K^{\mathrm{a}}$. The functor is given by taking closed points, and the assertion is clear.[38]

□

Recall that when X is a scheme locally of finite type over a field K (resp. a commutative algebraic group over K), and L/K a Galois extension with Galois group $G := \mathrm{Gal}(L/K)$, then $X(L)$ is a discrete G-set (resp. discrete $\mathbb{Z}[G]$-module) and $X(K) \xrightarrow{\sim} X(L)^{\mathrm{Gal}(L/K)}$ ([14, §5.2]). In particular, when K is perfect, this applies to $L = K^{\mathrm{s}} = K^{\mathrm{a}}$ with $\mathrm{Gal}(K^{\mathrm{a}}/K) =: G_K$ and we have $X(K) \xrightarrow{\sim} X(K^{\mathrm{a}})^{G_K}$.

Definition 2.2.2 (Galois Cohomology)**.** *Let K be a field and A a commutative algebraic group over K.*
(a) Given a Galois extension L/K, the (relative) Galois cohomology *groups of A relative to L/K are the profinite cohomology groups $\mathrm{H}^\bullet(L/K, A) := \mathrm{H}^\bullet(\mathrm{Gal}(L/K), A(L))$.*
(b) The (absolute) Galois cohomology *groups of A are $\mathrm{H}^\bullet(K, A) := \mathrm{H}^\bullet(K^{\mathrm{s}}/K, A)$ for a fixed choice of separable closure $K \to K^{\mathrm{s}}$.*

Remark 2.2.3.
(a) For L/K finite Galois, we have analogously the *Tate-Galois cohomology groups* $\hat{\mathrm{H}}^\bullet(L/K, A)$.
(b) By Theorem 2.2.1(c), when K is perfect, a short exact sequence $0 \to A \to B \to C \to 0$ in $\mathscr{G}\mathrm{rp}_K$ yields a long exact sequence in Galois cohomology $\mathrm{H}^\bullet(K, A) \to \mathrm{H}^\bullet(K, B) \to \mathrm{H}^\bullet(K, C) \xrightarrow{\delta} \mathrm{H}^{\bullet+1}(K, A)$. From now on, we (tacitly) assume that our base field K is perfect, so that $K^{\mathrm{s}} = K^{\mathrm{a}}$.[39]
(c) In Definition 2.2.2(b), we have made a choice of separable closure $K \to K^{\mathrm{s}}$ of K and hence of $G_K = \mathrm{Gal}(K^{\mathrm{s}}/K)$. However, a different choice would change G_K by an inner automorphism, and so, by Example 1.2.5, the Galois cohomology group is well-defined up to an *canonical isomorphism*.[40]
(d) Suppose K is a number field and $v \in \mathrm{M}_K$ a place, and fix an extension of v to $K^{\mathrm{s}} = K^{\mathrm{a}}$, obtaining an embedding $K^{\mathrm{a}} \hookrightarrow K_v^{\mathrm{a}}$ and decomposition and inertia groups D_v and I_v respectively. For each $A \in \mathscr{G}\mathrm{rp}_K$, the map $G_{K_v} \cong \mathrm{D}_v \hookrightarrow G_K$ along with the pushforward $A(K^{\mathrm{a}}) \to A(K_v^{\mathrm{a}}) = A_v(K_v^{\mathrm{a}})$, where $A_v := A_{K_v}$ is the basechange of A to K_v, gives rise to a homomorphism of the Galois cohomology groups called the *local restriction map* $\mathrm{Res}_v : \mathrm{H}^\bullet(K, A) \to \mathrm{H}^\bullet(K_v, A_v)$. The resulting morphism $\mathrm{Res}_v : \mathrm{H}^\bullet(K, -) \to \mathrm{H}^\bullet(K_v, (-)_v)$ is a morphism of δ-functors $\mathscr{G}\mathrm{rp}_K \to \mathrm{Ab}$ by Theorem 2.2.1(b). In this setting, given an $A \in \mathscr{G}\mathrm{rp}_K$ and $\xi \in \mathrm{H}^\bullet(K, A)$, we say that the class ξ is *unramified* at v if ξ maps to zero under the composite restriction $\mathrm{H}^\bullet(K, A) \xrightarrow{\mathrm{Res}_v} \mathrm{H}^\bullet(K_v, A_v) \xrightarrow{\mathrm{Res}_{\mathrm{I}_v}^{\mathrm{D}_v}} \mathrm{H}^\bullet(\mathrm{I}_v, A_v(K_v^{\mathrm{a}}))$. More generally, given any $S \subset \mathrm{M}_K$, we define the subgroup $\mathrm{H}^\bullet(K, A; S)$ to consist of cohomology classes which are unramified at all $v \notin S$. Even though the subgroups D_v and I_v depend on the choice of extensions of v to K^{a}, they are well-defined up to conjugation, and hence by considerations analogous to those in (c), restriction morphism Res_v, the notion of "unramified class," and the group $\mathrm{H}^\bullet(K, A; S)$ are well-defined, independent of any choices.

---

into the category $\mathrm{Shv}(\mathrm{Spec}(K)_{\mathrm{fl}}, \mathrm{Ab}) =: \mathscr{A}\mathrm{b}_K$ of abelian sheaves on the big flat (i.e., fppf) site $\mathrm{Spec}(K)_{\mathrm{fl}}$, which is evidently abelian, and then to show that the quotient in this category is also representable by an algebraic group ([40, 5.2.12], [12, 4.41]). For a more accesible and low-tech approach, see [34, Appendix B].

[38] This uses standard facts such as surjective (resp. locally finite type morphisms) are stable under base change, a nonempty locally finite type scheme over the field K^{a} has a K^{a}-point, etc.

[39] This suffices for all our applications; in what follows we will only be interested in fields of characteristic zero or finite fields. This assumption is not necessary for all that follows, but it does simplify the exposition somewhat.

[40] Here's one way to phrase this. Suppose $K \to K^{\mathrm{s}'}$ is another choice of separable closure (or equivalently algebraic closure–recall that K is perfect), and let $G'_K = \mathrm{Gal}(K^{\mathrm{s}'}/K)$ be the corresponding absolute Galois group. Then there is a K-isomorphism $\phi : K^{\mathrm{s}} \xrightarrow{\sim} K^{\mathrm{s}'}$ which induces an isomorphism $c_\phi : G'_K \xrightarrow{\sim} G_K$ by $\sigma \mapsto \phi^{-1}\sigma\phi$. This gives rise to an isomorphism of the cohomology groups $\mathrm{H}^\bullet(c_\phi, A(\phi)) : \mathrm{H}^\bullet(G_K, A(K^{\mathrm{s}})) \xrightarrow{\sim} \mathrm{H}^\bullet(G'_K, A(K^{\mathrm{s}'}))$, and the point being made is that the isomorphism $\mathrm{H}^\bullet(c_\phi, A(\phi))$ is independent of the choice of ϕ, i.e., if $\psi : K^{\mathrm{s}} \xrightarrow{\sim} K^{\mathrm{s}'}$ is another K-isomorphism, then $\mathrm{H}^\bullet(c_\phi, A(\phi)) = \mathrm{H}^\bullet(c_\psi, A(\psi))$. Indeed, both of these define morphisms of δ-functors (in A) which evidently agree in degree zero.

Example 2.2.4. If L/K is a finite Galois extension, then $\hat{\mathrm{H}}^\bullet(L/K, \mathbb{G}_a) = 0$. Indeed, the *Normal Basis Theorem* of field theory is equivalent to saying that $\mathbb{G}_a(L)$ is a free $\mathbb{Z}[\mathrm{Gal}(L/K)]$ module of rank 1, and so (co)induced from the trivial group; now apply Remark 1.4.3(c). In particular, $\mathrm{H}^n(K, \mathbb{G}_a) = 0$ for $n \in \mathbb{Z}_{\geq 1}$.

Example 2.2.5 (Artin-Schreier Theory)**.** Let K be a field of $\mathrm{char}\, K = p > 0$ and consider the homomorphism $\wp : \mathbb{G}_a \to \mathbb{G}_a$ given by $x \mapsto x^p - x$. There is an exact sequence[41] $0 \to \mathbb{Z}/p \to \mathbb{G}_a \xrightarrow{\wp} \mathbb{G}_a \to 0$ in $\mathscr{G}\mathrm{rp}_K$ which along with Remark 2.2.3(c), Example 2.2.4, and Remark 2.1.8(a) gives us isomorphisms $K/\wp(K) \xrightarrow{\delta} \mathrm{H}^1(K, \mathbb{Z}/p) \cong \mathrm{Hom}^{\mathrm{cts}}_{\mathrm{Grp}}(G_K, \mathbb{Z}/p)$, recovering classical Artin-Schreier Theory.

Example 2.2.6. (Hilbert 90) If L/K is a finite Galois extension, then $\mathrm{H}^1(L/K, \mathbb{G}_m) = 0$; this follows from Dedekind's Theorem on the independence of characters ([15, Thm. 11.1]). In particular, $\mathrm{H}^1(K, \mathbb{G}_m) = 0$.

Example 2.2.7. (Brauer Groups) When L/K is a finite Galois extension, we observed in Remark 1.1.9(b) that $\mathrm{H}^2(L/K, \mathbb{G}_m) \cong \mathrm{Br}(L/K)$.[42] This result, along with some naturality considerations ([15, Ch. 7]), gives us a functorial isomorphism $\mathrm{H}^2(K, \mathbb{G}_m) \cong \mathrm{Br}(K)$.

Example 2.2.8 (Kummer Theory)**.** For each $n \in \mathbb{Z}_{\geq 1}$, the sequence $1 \to \mu_n \to \mathbb{G}_m \xrightarrow{[n]} \mathbb{G}_m \to 1$ is exact in $\mathscr{G}\mathrm{rp}_K$, so from Remark 2.2.3(c) and Example 2.2.6 we get the isomorphism $\delta : K^\times/(K^\times)^n \xrightarrow{\sim} \mathrm{H}^1(K, \mu_n)$. When K contains all n^{th} roots of unity, i.e. $\mu_n(K) \xrightarrow{\sim} \mu_n(K^{\mathrm{a}})$, then we have the $\mathbb{Z}[G_K]$-module isomorphism $\mu_n \cong \mathbb{Z}/n$, and hence, using Remark 2.1.8(a), $\mathrm{H}^1(K, \mu_n) \cong \mathrm{H}^1(K, \mathbb{Z}/n) \cong \mathrm{Hom}^{\mathrm{cts}}_{\mathrm{Grp}}(G_K, \mathbb{Z}/n)$. Combining these results (and considering finite subgroups on both sides) recovers classical Kummer Theory ([15, 11.7]). The same sequence, combined with Example 2.2.7, also gives us the isomorphism $\mathrm{H}^2(K, \mu_n) \xrightarrow{\sim} \mathrm{Br}(K)[n]$.

Even if the above definitions and results cannot be applied *verbatim* to a few other important settings, the ideas *can*. Here are a couple of examples of this phenomenon.

Example 2.2.9 (Weil-Châtelet Group)**.** ([40, §5.12]) Let $A \in \mathscr{G}\mathrm{rp}_K$. Analogously to Definition 1.1.7, we define an *A-torsor*, or *principal homogeneous space for A over K*, to be a nonempty K-variety X with a simply transitive right algebraic group action of A on X defined over K, i.e., a K-scheme morphism $+ : X \times A \to X$ satisfying the axioms of a group action on R-points for each K-algebra R, such that $A(K^{\mathrm{a}})$ acts transitively on $X(K^{\mathrm{a}})$ and that for some $x \in X(K^{\mathrm{a}})$, the orbit map $A_{K^{\mathrm{a}}} \to X_{K^{\mathrm{a}}}$ given by $a \mapsto x + a$ is an isomorphism. Two A-torsors X and X' are isomorphic if there is a K-scheme isomorphism $X \to X'$ compatible with the action of A, and an A-torsor X is isomorphic to the "trivial" A-torsor A iff $X(K) \neq \emptyset$. Let $\mathrm{WC}(A)$ denote the set of isomorphism classes of A-torsors; this is called the *Weil-Châtelet group* of A.

Analogously to Theorem 1.1.8, there is a bijection[43] $\mathrm{H}^1(K, A) \xrightarrow{\sim} \mathrm{WC}(A)$, and essentially the same proof works: for an A-torsor X, pick an $x \in X(K^{\mathrm{a}})$ and consider for each $g \in G_K$ the unique $a(g) \in A(K^{\mathrm{a}})$ such that $x + a(g) = gx$. Then $a : G_K \to A(K^{\mathrm{a}})$ is a *continuous* 1-cocycle, and we get a well-defined cohomology class $[a] \in \mathrm{H}^1(K, A)$. Conversely, given a continuous 1-cocycle $a \in \mathscr{Z}^1_{\mathrm{cts}}(G_K, A(K^{\mathrm{a}}))$, one

[41] Here, for $n \in \mathbb{Z}_{\geq 1}$, $\mathbb{Z}/n$ denotes the constant group scheme, the K^{a} points of which form the trivial $\mathbb{Z}[G_K]$-module $\mathbb{Z}/n$.

[42] As an application of the theory developed so far, one can prove *Wedderburn's Theorem* that every finite division algebra is a field. Indeed, let Δ be a finite division algebra, and let $K := Z(\Delta)$ be its center, so that K is a finite field; we need to show that $[\Delta] = 0$ in $\mathrm{Br}(K)$. From the general theory of Azumaya algebras ([15, 6.36]; this also follows from this example combined with Remark 2.2.3), there is a finite extension L/K such that $[\Delta] \in \mathrm{Br}(L/K) \subset \mathrm{Br}(K)$. Since L/K is Galois, this examples tells us $\mathrm{Br}(L/K) \cong \mathrm{H}^2(\mathrm{Gal}(L/K), L^\times)$. Since L/K is further cyclic, we get from Example 1.4.2 that $\mathrm{H}^2(\mathrm{Gal}(L/K), L^\times) \cong K^\times/\mathrm{N}^L_K(K^\times)$. One can now show directly by a counting argument that this is trivial (i.e., that the norm map on finite fields is surjective, see [15, 7.24]), or use the consequence of Example 1.4.2 that if A is a finite $\mathbb{Z}[G]$-module for a finite cyclic group G, then $|\mathrm{H}^1(G, A)| = |\mathrm{H}^2(G, A)|$, which combined with Example 2.2.6 gives the result.

[43] This justifies the terminology. For a geometric description of the group law, see [40, Ex. 5.12.16] or [57, Prop. 5].

can construct an A-torsor X_a inverting this operation.[44] Therefore, elements of the first cohomology group $\mathrm{H}^1(K, A)$ can be thought of as K-isomorphism classes of principal homogeneous spaces for A over K, and this bijection is functorial in K and A as in Remark 1.1.9.

Example 2.2.10. Let K be a local number field, and let $K^{\mathrm{nr}} \subset K^{\mathrm{a}}$ and $G_K \twoheadrightarrow G_K^{\mathrm{nr}}$ be as in Notation and Conventions. Fix an extension of the discrete valuation v on K to K^{a}, and for each subextension $K \subset L \subset K^{\mathrm{a}}$, let $\mathscr{O}_L$ denote the valuation ring of L. For each Galois subextension L/K of K^{a}, we define $\mathrm{H}^\bullet(L/K, \mathscr{O}^\times) := \mathrm{H}^\bullet(\mathrm{Gal}(L/K), \mathscr{O}_L^\times)$. When $L \subset K^{\mathrm{nr}}$ (i.e., L/K is unramified), one can show that $\mathrm{H}^n(L/K, \mathscr{O}^\times) = 0$ for $n \in \mathbb{Z}_{\geq 1}$.[45] It then follows from the exact sequence $1 \to \mathscr{O}_{K^{\mathrm{nr}}}^\times \to \mathbb{G}_m(K^{\mathrm{nr}}) \xrightarrow{v} \mathbb{Z} \to 1$ of discrete $\mathbb{Z}[G_K^{\mathrm{nr}}]$-modules, combined with Example 2.2.7 and Remark 2.1.8(a) that we have isomorphisms

$$\mathrm{Br}(K^{\mathrm{nr}}/K) \cong \mathrm{H}^2(K^{\mathrm{nr}}/K, \mathbb{G}_m) \xrightarrow{\sim} \mathrm{H}^2(G_K^{\mathrm{nr}}, \mathbb{Z}) \cong \mathrm{Hom}_{\mathrm{Grp}}^{\mathrm{cts}}(G_K^{\mathrm{nr}}, \mathbb{Q}/\mathbb{Z}).$$

Reduction gives us an isomorphism $G_K^{\mathrm{nr}} \to G_{\mathrm{k}} \cong \hat{\mathbb{Z}}$, where k is the residue field of K and the last group is topologically generated by the Frobenius autmorphism; this tells us that the last group above is isomorphic to $\mathrm{Hom}_{\mathrm{Grp}}^{\mathrm{cts}}(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Q}/\mathbb{Z}$ with the isomorphism given by evaluation at the Frobenius automorphism. This, combined with the fact that $\mathrm{Br}(K^{\mathrm{nr}}/K) = \mathrm{Br}(K)$ (or equivalently that every Azumaya K algebra is split by an unramified extension; see [15, 8.2] or [43, Ch. XII]) gives us an isomorphism $\mathrm{Inv}_K : \mathrm{Br}(K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ called the *Hasse invariant*.[46] This computation is the prototypical example of the cohomological approach to class field theory, as we will explain in the next section.

2.3 Class Formations and Class Field Theory

In this section, we define class formations and discuss the fundamental theorem of abstract class field theory and its consequences. We then give plenty of examples coming from local and global number fields. We follow the exposition in [36, Parts II-III] and [43, Ch. XI]; references for examples will be mentioned there.

Given any profinite group G, one can set up a formal analogy between G and an absolute Galois group by indexing the set of all open subgroups G_L of G by "fields" L. The "field" K with $G_K = G$ is the "basefield". When $G_L \subset G_K$, we formally write $K \subset L$, and define the "degree" of the "extension" L/K to be $[G_K : G_L]$. We say that the "extension" L/K is Galois iff $G_L \trianglelefteq G_K$, and in this case define the relative Galois group to be $G(L/K) := G_K/G_L$. See [36, §II.1] for more details, which are entirely straightforward; we will henceforth drop all quotation marks.

Suppose further that $A \in \mathbb{Z}[G]\text{-}\mathrm{Mod}^{\mathrm{disc}}$. Then we define for each field K of G the invariant submodule $A(K) := A^{G_K}$; the discreteness of A is equivalent to $A = \bigcup_K A(K)$. For each field K, we define the cohomology group $\mathrm{H}^\bullet(K, A) := \mathrm{H}^\bullet(G_K, \mathrm{Res}_{G_K}^G A)$ so that $\mathrm{H}^0(G_K, A) = A(K)$. Similarly, if $K \subset L$ is a Galois extension of fields of G, then $A(L)$ is a $G(L/K)$-module with $A(L)^{G(L/K)} = A(K)$ and we let $\hat{\mathrm{H}}^\bullet(L/K, A) := \hat{\mathrm{H}}^\bullet(G(L/K), A(L))$. As in the previous sections, we have inflation, restriction, and corestriction maps (and the latter two also for Tate cohomology in negative degrees). The profinite inflation-restriction sequence (Theorem 1.2.6 and Remark 2.1.5) tells us that if L/K is a Galois extension and $n \in \mathbb{Z}_{\geq 1}$ such that $\mathrm{H}^i(L, A) = 0$ for $i = 1, \ldots, n-1$, then there is an exact sequence

[44] This is somewhat nontrivial. The idea is to embed $A(K^{\mathrm{a}})$ into $\mathrm{Aut}_{K^{\mathrm{a}}}(A)$ via translations and then to consider the resulting map $\mathrm{H}^1(G_K, A(K^{\mathrm{a}})) \to \mathrm{H}^1(G_K, \mathrm{Aut}_{K^{\mathrm{a}}}(A)) \cong \mathrm{Twist}(A/K)$ to the set of twists of A (where we use Galois descent to make the last identification). The resulting twist is essentially the corresponding A-torsor. See [49, §X.3] for the case of elliptic curves and [40, §4.4-4.5] for an explanation of how to generalize the first proof; see also [40, §5.12].

[45] One reduces to the case of finite Galois L/K by Lemma 2.1.6. There, it is a consequence of the fact that $\mathscr{O}_L^\times$ admits a filtration $(U_L^n)_{n \in \mathbb{Z}_{\geq 1}}$ by unit groups with successive subquotients $\mathscr{O}_L^\times/U_L^1 \cong \mathbb{G}_m(\mathrm{k}_L)$ and $U_L^n/U_L^{n+1} \cong \mathbb{G}_a(\mathrm{k}_L)$ for $n \geq 1$. One then uses the corresponding cohomology exact sequences, Example 2.2.4, Footnote 42, and either the completeness of $\mathscr{O}_L^\times$ (in abitrary characteristic) or that $U_L^n \cong \mathbb{G}_a(\mathscr{O}_L)$ (in characteristic zero, using the exponential) for $n \gg 0$ along with divisibility and finiteness considerations (Remark 1.1.6(b)) to deduce the result; see [8, Lemma VI.1.2.3] or [36, II.4.3].

[46] For a direct construction of this map using Azumaya algebras, see [15, Ch. 8].

$$0 \to \mathrm{H}^n(L/K, A) \to \mathrm{H}^n(K, A) \to \mathrm{H}^n(L, A). \tag{2.1}$$

In particular, $\mathrm{H}^1(K, A) = \bigcup_{L/K} \mathrm{H}^1(L/K, A)$ and the same holds for H^2 if A is cohomologically trivial in degree 1. Motivated by Example 2.2.10, this leads us naturally to

Definition 2.3.1 (Class Formations)**.** *A* class formation *is a pair (G, A), where G is a profinite group and A is a discrete $\mathbb{Z}[G]$-module satisfying conditions (a)-(c).*

(a) A is cohomologically trivial in degree 1, i.e., for each field K of G, we have $\mathrm{H}^1(K, A) = 0$.[47]

(b) For each field K of G, there is an injection $\mathrm{Inv}_K : \mathrm{H}^2(K, A) \hookrightarrow \mathbb{Q}/\mathbb{Z}$ that is natural with respect to extensions: if L/K is any extension of fields of G, then the following diagram commutes:

$$\begin{array}{ccc} \mathrm{H}^2(K, A) & \xrightarrow{\mathrm{Inv}_K} & \mathbb{Q}/\mathbb{Z} \\ \big\downarrow{\scriptstyle \mathrm{Res}} & & \big\downarrow{\scriptstyle [L:K]} \\ \mathrm{H}^2(L, A) & \xrightarrow{\mathrm{Inv}_K} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

(c) For each Galois L/K, the relative invariant map $\mathrm{Inv}_K^L : \mathrm{H}^2(L/K, A) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ obtained from (2.1) and (b) is an isomorphism of groups.

Remark 2.3.2. If each $\mathrm{Inv}_K : \mathrm{H}^2(K, A) \hookrightarrow \mathbb{Q}/\mathbb{Z}$ is an isomorphism, then condition (c) is automatic.

Given a class formation (G, A), for each Galois extension L/K of fields of G, we let $\varphi_K^L \in \mathrm{H}^2(L/K, A)$ denote the generator such that $\mathrm{Inv}_K^L \varphi_K^L = [L : K]^{-1}$; this is called the *Frobenius* or the *fundamental class*. The importance of this class lies in

Theorem 2.3.3 (Fundamental Theorem of Abstract Class Field Theory)**.** *Let (G, A) be a class formation. For each Galois extension L/K of fields of G, the cup product induces abelian group isomorphisms*

$$\varphi_K^L \smile - : \hat{\mathrm{H}}^\bullet(L/K, \mathbb{Z}) \xrightarrow{\sim} \hat{\mathrm{H}}^{\bullet+2}(L/K, A).$$

In particular, we get an isomorphism $G(L/K)^{\mathrm{ab}} \to A(K)/\mathrm{N}_K^L A(L)$.

Proof. This is just Theorem 1.4.7, which also explains the notation. □

We say that a subgroup of $A(K)$ is a *norm subgroup* if it is of the form $\mathrm{N}_K^L A(L)$ for some finite Galois L/K. Importantly, this definition would be unchanged if L is further required to be abelian, since $\mathrm{N}_K^L A(L) = \mathrm{N}_K^{L^{\mathrm{ab}}} A(L^{\mathrm{ab}})$.[48] The whole point of setting up the machinery in this way is that the fundamental classes φ_K^L, and hence the isomorphisms of Theorem 2.3.3, are compatible over varying L/K ([36, II.1.6-11]). This compatibility has, along with Theorem 2.3.3, the following consequences, the proofs of which are entirely straightforward.

Corollary 2.3.4. *The map $L \mapsto \mathrm{N}(L) := \mathrm{N}_K^L A(L)$ gives an antitone Galois connection between the lattice of abelian extensions L of K and the lattice of norm subgroups of $A(K)$. In particular, we have for any abelian extensions L, L' of K that $\mathrm{N}(LL') = \mathrm{N}(L) \cap \mathrm{N}(L')$ and $\mathrm{N}(L \cap L') = \mathrm{N}(L) \cdot \mathrm{N}(L')$. Finally, any subgroup of $A(K)$ containing a norm subgroup is a norm subgroup.*

[47] By virtue of (2.1), this is equivalent to $\mathrm{H}^1(L/K, A) = 0$ for each Galois L/K.

[48] Here L^{ab} is the maximal abelian subextension of K in L; equivalently, $G_{L^{\mathrm{ab}}}$ is the closed subgroup of G_K generated by G_L and $[G_K, G_K]$. By Theorem 2.3.3, $A(K)/\mathrm{N}_K^L A(L) \cong G(L/K)^{\mathrm{ab}} \cong G(L^{\mathrm{ab}}/K) \cong G(L^{\mathrm{ab}}/K)^{\mathrm{ab}} \cong A(K)/\mathrm{N}_K^{L^{\mathrm{ab}}} A(L^{\mathrm{ab}})$, which along with the inclusion $\mathrm{N}_K^L A(L) \subset \mathrm{N}_K^{L^{\mathrm{ab}}} A(L^{\mathrm{ab}})$ implies the equality.

In the above setting, the induced map $A(K) \to G(L/K)^{\mathrm{ab}}$ fitting into the exact sequence

$$0 \to \mathrm{N}(L) \to A(K) \xrightarrow{(-,L/K)} G(L/K)^{\mathrm{ab}} \to 0$$

of abelian groups is called the *norm residue symbol* and is denoted $(-, L/K)$. By the compatibility assertion, these glue to give rise to a universal symbol $(-,K) : A(K) \to G_K^{\mathrm{ab}} = \lim_L G(L/K)^{\mathrm{ab}}$. The image of this map is denoted by W_K^{ab} and is called the *(abelianized) Weil group*.

Corollary 2.3.5. *There is an exact sequence*

$$0 \to \bigcap_L \mathrm{N}(L) \to A(K) \xrightarrow{(-,K)} W_K^{\mathrm{ab}} \to 0,$$

and $W_K^{\mathrm{ab}} \leq G_K^{\mathrm{ab}}$ is dense.

See [36, §II.1], which also contains an explicit formula for the norm residue symbol in terms of cup products. In particular, Corollary 2.3.4 says that the lattice of abelian extensions of K in G can be described explicitly via the group $A(K)$ which is is in some sense "internal" to K; this is the content of local and global class field theory (LCFT/GCFT).

Remark 2.3.6. To make Corollary 2.3.4 useful, one needs to give an intrinsic characterization of the norm subgroups of $A(K)$. This is often done in the arithmetic setting by giving a natural topology to $A(K)$ under which the norm subgroups are exactly the closed subgroups of finite index; this is the content of the relevant *Existence Theorem*. In this case, it is also often true that $\bigcap_L \mathrm{N}_L = 0$, and hence that the universal symbol $(-,K)$ gives an isomorphism between $A(K)$ and the dense subgroup $W_K^{\mathrm{ab}} \leq G_K^{\mathrm{ab}}$.

Example 2.3.7. (Archimedean LCFT) Take $G = G_{\mathbb{R}} \cong C_2$ and $A = \mathbb{G}_m(\mathbb{C})$; that this is a class formation follows from either of Examples 1.4.2 or 2.2.6. The only fields are $\mathbb{R} \subset \mathbb{C}$, the only norm subgroup of $\mathbb{G}_m(\mathbb{R}) = \mathbb{R}^\times$ is $\mathrm{N}_{\mathbb{R}}^{\mathbb{C}}\,\mathbb{G}_m(\mathbb{C}) = \mathbb{R}^{>0}$, and Corollary 2.3.5 is the sequence $0 \to \mathbb{R}^{>0} \to \mathbb{R}^\times \xrightarrow{\mathrm{sgn}} \{\pm 1\} \to 0$.

Example 2.3.8. (Abstract Unramified Nonarchimedean LCFT) Take $G = \hat{\mathbb{Z}}$ and $A = \mathbb{Z}$ the trivial G-module. Here there is a unique field K_n for each integer $n \in \mathbb{Z}_{\geq 1}$. That this pair is a class formation follows from considering the long exact cohomology sequence associated to $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ and its naturality; see Remark 2.1.8(a). The Fundamental Theorem (Theorem 2.3.3) is just the 2-periodicity of Example 1.4.2. Corollary 2.3.4 is saying that the lattices of finite index subgroups of $\mathbb{Z}$ and $\hat{\mathbb{Z}}$ are isomorphic, namely both to $(\mathbb{Z}_{\geq 1}, |)$. In Corollary 2.3.5, $\bigcap_L \mathrm{N}(L) = 0$, and for each $n \in \mathbb{Z}_{\geq 1}$, the the Artin map $(-, K_n) : A(K_n) \to G_{K_n}^{\mathrm{ab}}$ is the inclusion $n\mathbb{Z} \hookrightarrow n\hat{\mathbb{Z}}$, which is an isomorphism onto a dense subgroup.

Example 2.3.9. (Unramified Nonarchimedean LCFT; [36, §II.4]) If K is a local number field, then Example 2.2.10 tells us that $(G_K^{\mathrm{nr}}, \mathbb{G}_m(K^{\mathrm{nr}}))$ is a class formation relative to the invariant map constructed there. Indeed, axiom (a) of Definition 2.3.1 is Example 2.2.6, axiom (b) is Examples 2.2.7 and 2.2.10 along with the naturality of the Hasse invariant ([15, 8.10], [36, II.4.6], [43, XIII.3.7]), and (c) is Remark 2.3.2. Every unramified extension L/K of K is already abelian (and, indeed, cyclic), and the norm subgroup corresponding to the unique (up to isomorphism) unramified extension of degree $n \in \mathbb{Z}_{\geq 1}$ is exactly $\pi^{n\mathbb{Z}}\mathcal{O}_K^\times = v_K^{-1}(n\mathbb{Z}) \subset K^\times$, where π is any uniformizer and v_K the valuation ([36, II.4.9]). The lattice of Corollary 2.3.4 is $(\mathbb{Z}_{\geq 1}, |)$. The exact sequence of Corollary 2.3.5 is $0 \to \mathcal{O}_K^\times \to K^\times \xrightarrow{v_K} \mathbb{Z} \to 0$, and $W_K^{\mathrm{ab}} \leq G_K^{\mathrm{ab}}$ is $\mathbb{Z} \leq \hat{\mathbb{Z}}$. This example is ultimately the same as the previous one.

The power of this abstract set-up is that is can be extended to the ramified setting with very little work.

Example 2.3.10. (Nonarchimedean LCFT; [8, Ch. VI], [17, Ch. 9], [36, Ch. II], [37, Ch. VII]) If K is a local number field, then $(G_K, \mathbb{G}_m(K^{\mathrm{a}}))$ is a class formation. Again, axiom (a) is Example 2.2.6, (b) comes from the observation made in Example 2.2.10 that $\mathrm{Br}(K) = \mathrm{Br}(K^{\mathrm{nr}}/K)$ along with naturality as in Example 2.3.9, and (c) is Remark 2.3.2. It follows easily from Kummer Theory (Example 2.2.8) that for each $m \in \mathbb{Z}_{\geq 1}$, if K contains a primitive m^{th} root of unity and $L := K[(K^\times)^{1/m}]$, then L/K is an abelian extension with norm subgroup $\mathrm{N}(L) = (K^\times)^m$, and hence in general that the norm subgroups are exactly the closed subgroups of finite index ([36, II.6.2]). In particular, $\bigcap_L \mathrm{N}(L) = 0$ ([36, II.3.6]), and hence the universal symbol–the *Artin map*–$(-, K) : K^\times \to W_K^{\mathrm{ab}}$ is an isomorphism, and induces an isomorphism $\widehat{K^\times} \to G_K^{\mathrm{ab}}$. If $\mathrm{pr} : G_K^{\mathrm{ab}} \to G_{\mathrm{k}} \cong \hat{\mathbb{Z}}$ is the reduction map, where k is the residue field and in the latter isomorphism the topological generator is the Frobenius Fr, then $W_K^{\mathrm{ab}} = \mathrm{pr}^{-1}(\mathbb{Z})$. Under this isomorphism, the filtration $(U_K^n)_{n \in \mathbb{Z}_{\geq 0}}$ of $K^\times$ by unit groups corresponds to the filtration by the higher ramification groups in the upper numbering, and the Artin map $(-, K)$ can be constructed incredibly explicitly using the Lubin-Tate theory of formal $\mathcal{O}$-modules ([8, Ch. VII], [36, §II.7]).

For a concrete example, let p be a prime and $K = \mathbb{Q}_p$. For each $n \in \mathbb{Z}_{\geq 1}$, let $\zeta_n \in \mathbb{Q}_p^{\mathrm{a}}$ be a primitive n^{th} root of unity; then the cyclotomic extension $L_n := \mathbb{Q}_p[\zeta_n]/\mathbb{Q}_p$ is abelian. It is easy to check that for any $n \in \mathbb{Z}_{\geq 0}$, we have $\mathrm{N}(L_{p^n}) = p^{\mathbb{Z}}(\mathbb{Z}_p^\times)^n$. Further, the unique unramified extension of degree $m \in \mathbb{Z}_{\geq 1}$ in $\mathbb{Q}_p^{\mathrm{a}}$ is exactly L_{p^m-1}, and so by Example 2.3.9, $\mathrm{N}(L_{p^m-1}) = p^{m\mathbb{Z}}\mathbb{Z}_p^\times$. By Corollary 2.3.4, $\mathrm{N}(L_{p^n(p^m-1)}) = p^{m\mathbb{Z}}(\mathbb{Z}_p^\times)^n$, and hence $\mathrm{N}(L_{p^m(p^m-1)}) = (\mathbb{Q}_p^\times)^m$. It follows from Corollary 2.3.4 and the discussion above that every finite abelian extension of $\mathbb{Q}_p$ is contained in a cyclotomic extension, which is the local Kronecker-Weber Theorem (c.f. [7, §8.4]).[49] In particular, $\mathbb{Q}_p^{\mathrm{ab}} = L_\infty$ can be written as the compositum of $\mathbb{Q}_p[\zeta_{p^\infty}] = L_{p^\infty} := \mathrm{colim}_n L_{p^n}$ and $\mathbb{Q}_p^{\mathrm{nr}} = \mathrm{colim}_m L_{p^m-1}$. Of these, the first is totally ramified and the second unramified, so that the two are linearly disjoint in $\mathbb{Q}_p^{\mathrm{a}}$. One can show very directly that for each $n \in \mathbb{Z}_{\geq 0}$, we have $\mathrm{Gal}(L_{p^n}) \cong (\mathbb{Z}/p^n)^\times$; further, these isomorphisms glue to give an isomorphism $\mathrm{Gal}(\mathbb{Q}_p[\zeta_{p^\infty}]/\mathbb{Q}_p) \cong \mathbb{Z}_p^\times$. Further, $G_{\mathbb{Q}_p}^{\mathrm{nr}} \cong G_{\mathbb{F}_p} \cong \hat{\mathbb{Z}}$, topologically generated by the Frobenius automorphism Fr_p. Under these isomorphisms, the composite

$$\mathbb{Z} \times \mathbb{Z}_p^\times \xrightarrow{\sim} p^{\mathbb{Z}}\mathbb{Z}_p^\times = \mathbb{Q}_p^\times \xrightarrow{(-,\mathbb{Q}_p)} G_{\mathbb{Q}_p}^{\mathrm{ab}} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{nr}}/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}_p[\zeta_{p^\infty}]/\mathbb{Q}_p) \cong \hat{\mathbb{Z}} \times \mathbb{Z}_p^\times$$

is the usual embedding,[50] which is of course an isomorphism onto its dense image.

To extend CFT to the global setting is much more work; we only outline the key ideas involved.

Example 2.3.11. (GCFT; [2], [8, Ch. VII], [17, Ch. 13], [36, Part III], [37, Ch. VIII]) Let K be a (global) number field and $\mathbb{A}^\times(K) = \prod_{v \in \mathrm{M}_K}(K_v, \mathcal{O}_v)$ (resp. $C(K)$) be its idèle group (resp. idèle class group), so there is a short exact sequence $1 \to \mathbb{G}_m(K) \xrightarrow{\Delta} \mathbb{A}^\times(K) \to C(K) \to 1$. For each finite extension L/K, there is an L-algebra isomorphism $L \otimes_K \mathbb{A}(K) \to \mathbb{A}(L)$ extending the map $K \to L$ which induces an injective homomorphism $\mathbb{A}^\times(K) \to \mathbb{A}^\times(L)$; if L/K is also Galois, then $\mathrm{Gal}(L/K)$ evidently acts on $\mathbb{A}^\times(K)$ (resp. $C(L)$) with $(\mathbb{A}^\times(L))^{\mathrm{Gal}(L/K)} = \mathbb{A}^\times(K)$ (resp. $C(L)^{\mathrm{Gal}(L/K)} = C(K)$[51]). We define the *total idèle group* to be $\mathbb{A}^\times := \mathbb{A}^\times(K^{\mathrm{a}}) := \mathrm{colim}_{L/K} \mathbb{A}^\times(L)$ and the total class group C to fit into the short exact sequence of discrete $\mathbb{Z}[G_K]$-modules

$$0 \to \mathbb{G}_m \to \mathbb{A}^\times \to C \to 0, \tag{2.2}$$

where $\mathbb{G}_m$ here means $\mathbb{G}_m(K^{\mathrm{a}})$. The key result then is that (G_K, C) is a class formation; this is nontrivial to prove, but the idea is to break $\mathbb{A}^\times$ into its local components by showing that restriction gives and

[49] This is only a stone's throw away from the global Kronecker-Weber Theorem. The ingredients needed are the theorem on "arithmetic monodromy" along with the input from the Minkowski geometry of numbers that the only everywhere unramified extension of $\mathbb{Q}$ is $\mathbb{Q}$ itself, or equivalently that $\mathbb{Q}$ is its own Hilbert class field. See [7, §10.12] or [15, Ch. 14].

[50] Depending on your choice of isomorphism $\mathrm{Gal}(\mathbb{Q}_p[\zeta_{p^\infty}]/\mathbb{Q}_p) \cong \mathbb{Z}_p^\times$ (and in particular if you make the obvious one), you may have to postcompose with the automorphism $u \mapsto u^{-1}$ of $\mathbb{Z}_p^\times$.

[51] This follows from the previous result and Example 2.2.6.

isomorphism $\mathrm{H}^\bullet(K, \mathbb{A}^\times) \cong \bigoplus_{v \in \mathrm{M}_K} \mathrm{H}^\bullet(K_v, \mathbb{G}_m)$, and then to use Example 2.3.10 and the long exact cohomology sequence associated with (2.2). The corresponding Existence Theorem says that the norm subgroups of $C(K)$ are exactly the closed subgroups of finite index.[52] One can show further that universal symbol $(-, K) : C(K) \to G_K^{\mathrm{ab}}$ is surjective (so that $W_K^{\mathrm{ab}} = G_K^{\mathrm{ab}}$), and the kernel $\bigcap_L \mathrm{N}(L)$ is the connected component $C(K)^\circ = D(K)$ of the identity in $C(K)$, which is rather complicated.[53] Corollary 2.3.5 therefore gives an isomorphism $\pi_0 C(K) := C(K)/D(K) \xrightarrow{\sim} G_K^{\mathrm{ab}}$.

The relationship between the local and global CFT is that the global symbol $(-, K)$ is essentially a product of the local symbols $(-, K_v)$ ([8, §VII.6]).

Example 2.3.12. (GCFT with Restricted Ramification; [37, §VIII.3]) Let K be a (global) number field and $S \subset \mathrm{M}_K$ a finite set containing M_K^∞. Let $U_{K,S} \subset C(K)$ be the image of $\prod_{v \notin S} \{1\} \times \prod_{v \in S} U_v^1$, where $U_v^1 \subset \mathscr{O}_v^\times$ is the 1-unit group; this is a compact subgroup of $C(K)$. We define the *S-idèle group* of K to be $C_S(K) := C(K)/U_{K,S}$. As in Example 2.3.11, for each field extension L/K of K with $L \subset K_S$–the maximal unramified-outside-S extension of K–, we have an injective comparison map $C_S(K) \to C_S(L)$; further, if L/K is Galois, then $C_S(L)$ is a $\mathbb{Z}[\mathrm{Gal}(L/K)]$-module with $C_S(L)^{\mathrm{Gal}(L/K)} = C_S(K)$. We then define the total S-class group C_S to be $C_S = \mathrm{colim}_L C_S(L) = C(K_S)/U_S$, where $U_S = \mathrm{colim}_L U_{L,S} \subset C(K_S)$. Then (G_S, C_S) is a class formation. The corresponding Existence Theorem says that the norm subgroups of $C_S(K)$ are exactly the open subgroups (which automatically have finite index). The universal symbol $C_S(K) \to G_S^{\mathrm{ab}}$ is surjective, and the kernel $\bigcap_L N(L)$ is the image $D_S(K)$ of $D(K)$ in the quotient $C_S(K)$.

For many more examples, see [32, §I.1] and the references mentioned there.

2.4 Arithmetic Duality Theorems and Theorems of Tate-Poitou and Tate

The analogs of the famous and powerful duality theorems of algebraic topology (e.g., Poincaré-Verdier, Alexander) and algebraic geometry (Grothendieck-Serre) in the arithmetic world are due to Tate and Poitou from the 1960s ([39], [53]). Since the proofs are highly technical and would lead us too far,[54] in this final section of this chapter, we content ourselves with providing the statements of the key results which we will need in the final chapter. The exposition is taken from [32, Ch. I].

For this, we will need one notion: Cartier duality. For a field K of characteristic zero and a $\mathbb{Z}[G_K]$-module Φ, we define its *Cartier dual* to be $\Phi^{\mathrm{D}} := \mathrm{Hom}_{\mathrm{Grp}}(\Phi, \mathbb{G}_m(K^{\mathrm{a}}))$ with the G_K-action given by intertwining: for $\alpha \in \Phi$, $\psi \in \Phi^{\mathrm{D}}$, and $\sigma \in G_K$, we define $\sigma\psi$ by

$$(\sigma\psi)(\alpha) = \sigma\left(\psi(\sigma^{-1}\alpha)\right). \tag{2.3}$$

Then Φ^{D} is a finite discrete $\mathbb{Z}[G_K]$-module if Φ is, and in this case the natural evaluation map $\Phi \to \Phi^{\mathrm{DD}}$ is an isomorphism of such objects. Because of (2.3), the natural bilinear map given by evaluation

$$\Phi \otimes_{\mathbb{Z}} \Phi^{\mathrm{D}} \to \mathbb{G}_m(K^{\mathrm{a}})$$

is a morphism of $\mathbb{Z}[G_K]$-modules, where the left side is given the diagonal action (§1.3). Consequently, by Theorem 1.3.1 and the pushforward map, for each $p, q \in \mathbb{Z}_{\geq 0}$, we get a bilinear map

$$\mathrm{H}^p(K, \Phi) \times \mathrm{H}^q(K, \Phi^{\mathrm{D}}) \to \mathrm{H}^{p+q}(K, \mathbb{G}_m). \tag{2.4}$$

First suppose that K is a local number field. Then by Examples 2.2.7 and 2.2.10, we have the isomorphism $\mathrm{Inv}_K : \mathrm{H}^2(K, \mathbb{G}_m) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$. Combining with (2.4), we have defined the pairing in

[52] In passing, we remark this proves immediately, as in Example 2.3.10, the Kronecker-Weber Theorem for K.

[53] It is isomorphic as a topological group to $(S^1)^{r_2} \times ((\mathbb{R} \times \hat{\mathbb{Z}})/\mathbb{Z})^r \times \mathbb{R}$ for some integers $r_2, r \in \mathbb{Z}_{\geq 0}$.

[54] Haberland and Milne wrote entire books ([16] and [32] respectively) on them!

Theorem 2.4.1. *(Local Tate Duality) In the above setting, for $p = 0, 1, 2$, there is a bilinear pairing*

$$\langle -, - \rangle : \mathrm{H}^p(K, \Phi) \times \mathrm{H}^{2-p}(K, \Phi^{\mathrm{D}}) \to \mathbb{Q}/\mathbb{Z}$$

with the following properties.

(a) The pairing is nondegenerate, i.e., the induced map $\mathrm{H}^p(K, \Phi^{\mathrm{D}}) \to \mathrm{H}^{2-p}(K, \Phi)^*$ is an isomorphism.

(b) The pairing is natural, i.e., if $\phi : \Phi \to \Psi$ is a $\mathbb{Z}[G_K]$-module homomorphism, then

$$\langle \phi_*(-), - \rangle = \langle -, \phi_*^{\mathrm{D}}(-) \rangle,$$

where $\phi_* = \mathrm{H}^p(\mathrm{id}, \phi) : \mathrm{H}^p(K, \Phi) \to \mathrm{H}^p(K, \Psi)$ is the induced map in cohomology (similarly for ϕ_*^{D}). Further, the groups $\mathrm{H}^1(K, \Phi)$ and $\mathrm{H}^1(K, \Phi^{\mathrm{D}})$ are finite.

Proof. See [16, Prop. 1.2.1], [17, Thm. 10.9], [32, Cor. I.2.3], or [37, Thm. 7.2.6]. □

Remark 2.4.2. In the case of an archimedean local field K (i.e., $K = \mathbb{R}, \mathbb{C}$), there is a similar, but even simpler result which uses only Example 1.4.2–provided that H^0 is interpreted as the Tate cohomology group. Given the paucity of proofs in this section, we explain this at least. The case $K = \mathbb{C}$ is trivial. Now, let us consider the case $K = \mathbb{R}$ with Galois group $G_{\mathbb{R}} \cong C_2 = \langle x | x^2 \rangle$ so $\mathbb{Z}[C_2] = \mathbb{Z}[x]/(x^2 - 1)$. For each $\mathbb{Z}[C_2]$-module Φ, we denote the action of x on Φ by a bar. In this notation, the induced action on $\Phi^{\mathrm{D}} = \mathrm{Hom}_{\mathrm{Grp}}(\Phi, \mathbb{C}^\times) = \Phi^*$ is given by $\bar{\lambda}(\alpha) = \overline{\lambda(\bar{\alpha})}$ for $\alpha \in \Phi$ and $\lambda \in \Phi^{\mathrm{D}}$. Then, by considering Example 1.4.2 and unpacking the definitions (using, e.g., formula (1.2)), Theorem 2.4.1 in this setting says exactly that the bilinear maps

$$\Phi^{C_2}/\,\mathrm{N}_{C_2}\,\Phi \times (\Phi^{\mathrm{D}})^{C_2}/\,\mathrm{N}_{C_2}\,\Phi^{\mathrm{D}} \to \{\pm 1\} \text{ and } \Phi[1+x]/(1-x)\Phi \times \Phi^{\mathrm{D}}[1+x]/(1-x)\Phi^{\mathrm{D}} \to \{\pm 1\}$$

induced by evaluation are nondegenerate. We'll do the first one; the second can be handled either analogously or by dimension shifting (Remark 1.4.3(e)). For the first one, observe that by naturality (the immediate analog of Theorem 2.4.1(b)), if we have a short exact sequence $0 \to \Phi' \to \Phi \to \Phi'' \to 0$ of finite $\mathbb{Z}[C_2]$-modules and the result is true for Φ' and Φ'', then it is true for Φ. Therefore, by induction on the size of Φ and considering $\Phi' := \Phi^{C_2}$, we are reduced to checking two cases: when the action is trivial, and when $\Phi^{C_2} = 0$. In the first case, the induced action on Φ^{D} is given by complex conjugation on the codomain, and the claim being made is the natural pairing

$$\Phi/2\Phi \times \mathrm{Hom}_{\mathrm{Grp}}(\Phi, \{\pm 1\}) \to \{\pm 1\}$$

is nondegenerate. This claim is clear, for instance by considering the structure theorem for finite abelian groups. In the second case, the action is necessarily given by negation; furthermore, the 2-primary component $\Phi_{(2)}$ of Φ is zero. But then Φ is a $\mathbb{Z}[1/2][C_2]$-module and so all groups in question are zero (by say Examples 1.1.3 and 1.4.2), and the result holds trivially. See also [32, Thm. I.2.13(a)] for a different argument, and note that the theorem is *not* true when we take ordinary group cohomology in place of the Tate cohomology.

Next suppose that K be a number field, $S \subset \mathrm{M}_K$ be a finite set containing M_K^∞, and K_S the maximal unramified-outside-S extension of K in K^{a} with $G_S := \mathrm{Gal}(K_S/K)$. Let Φ be a finite discrete $\mathbb{Z}[G_S]$-module with order $|\Phi|$ a unit in $\mathscr{O}_{K,S}$. In this case, the Cartier dual $\Phi^{\mathrm{D}} := \mathrm{Hom}_{\mathrm{Grp}}(\Phi, \mathbb{G}_m(K^{\mathrm{a}}))$ has the property that $\Phi^{\mathrm{D}} = \mathrm{Hom}_{\mathrm{Grp}}(\Phi, \mathbb{G}_m(K_S))$, and consequently a formula analogous to (2.3) makes it a finite discrete $\mathbb{Z}[G_S]$-module. As before, we have the isomorphism of $\mathbb{Z}[G_S]$-modules $\Phi \to \Phi^{\mathrm{DD}}$, and a natural bilinear map $\Phi \otimes_{\mathbb{Z}} \Phi^{\mathrm{D}} \to \mathbb{G}_m(K_S)$.

Analogously to Remark 2.2.3(d)–but even more simply–we have for each $v \in S$ the restriction maps $\mathrm{Res}_v : \mathrm{H}^\bullet(G_S, \Phi) \to \mathrm{H}^\bullet(K_v, \Phi)$. In what follows, we use $\hat{\mathrm{H}}^0(K_v, \Phi)$ to denote the usual cohomology group $\mathrm{H}^0(K_v, \Phi)$ for $v \in \mathrm{M}_K^0$ and the Tate cohomology group $\hat{\mathrm{H}}^0(K_v, \Phi)$ for $v \in \mathrm{M}_K^\infty$; in the latter case case, we postcompose the above restriction map with the surjection $\mathrm{H}^0(K_v, \Phi) \twoheadrightarrow \hat{\mathrm{H}}^0(K_v, \Phi)$ (Definition 1.4.1) to get restriction maps $\mathrm{Res}_v : \mathrm{H}^0(G_S, \Phi) \to \hat{\mathrm{H}}^0(K_v, \Phi)$ for all $v \in S$. The key result of this section is then

Theorem 2.4.3 (Poitou-Tate Duality)**.** *In the above setting, there is an exact sequence*

$$0 \to \mathrm{H}^0(G_S, \Phi) \to \bigoplus_{v \in S} \hat{\mathrm{H}}^0(K_v, \Phi) \to \mathrm{H}^2(G_S, \Phi^{\mathrm{D}})^* \to \mathrm{H}^1(G_S, \Phi) \to \bigoplus_{v \in S} \mathrm{H}^1(K_v, \Phi) \to \mathrm{H}^1(G_S, \Phi^{\mathrm{D}})^*.$$

Proof. See [16, Thm. 1], [17, Thm. 17.13], [32, Thm. I.4.10], or [37, Thm. 8.6.10]. We only describe (most of the) maps. The first (nontrivial) map is the sum of the local restriction map Res_v. The second map is the $\mathbb{Q}/\mathbb{Z}$-dual to the composite

$$\mathrm{H}^2(G_S, \Phi^{\mathrm{D}}) \xrightarrow{\oplus_{v \in S} \mathrm{Res}_v} \bigoplus_{v \in S} \mathrm{H}^2(K_v, \Phi) \xrightarrow{\sim} \bigoplus_{v \in S} \hat{\mathrm{H}}^0(K_v, \Phi^{\mathrm{D}}),$$

where the last isomorphism comes from Theorem 3.3.1 (and Remark 2.4.2 for $v \in \mathrm{M}_K^\infty$). The maps in the second half of the sequence are obtained identically, leaving only the map $\mathrm{H}^2(G_S, \Phi^{\mathrm{D}})^* \to \mathrm{H}^1(G_S, \Phi)$. This comes from a global duality theorem, and we omit its description (which we will not need anyway). For a description of this map, an extension of this sequence to two more terms, and the proof of exactness, see the references mentioned above. The references also explain the case of possibly infinite S, where care must be taken to introduce suitable restricted products and topologies (which, fortunately, may be safely ignored when S is finite). □

Corollary 2.4.4. *In the above setting, the groups $\mathrm{H}^n(G_S, \Phi)$ for $n = 0, 1$ are finite, and similarly for Φ^{D}.*

Proof. The case $n = 0$ follows from Theorem 2.4.3 and the finiteness of S and $\hat{\mathrm{H}}^0(K_v, \Phi)$ for $v \in S$; indeed, the last is a subquotient of Φ (Definition 1.4.1). The case $n = 1$ needs work; see [32, Cor. I.4.15]. □

The final result we will state without proof is

Theorem 2.4.5 (Tate's Theorem on Global Euler-Poincaré Characteristics)**.** *In the above setting, we have*

$$\frac{|\mathrm{H}^0(G_S, \Phi^{\mathrm{D}})| \cdot |\mathrm{H}^2(G_S, \Phi^{\mathrm{D}})|}{|\mathrm{H}^1(G_S, \Phi^{\mathrm{D}})|} = \prod_{v \in \mathrm{M}_K^\infty} \frac{|\hat{\mathrm{H}}^0(K_v, \Phi)|}{|\mathrm{H}^0(K_v, \Phi)|}.$$

Proof. See [16, Thm. 2], [32, Thm. I.5.1, Rem. I.5.2(a)], or [37, Thm. 8.7.4]. □

3 Isogeny Invariance of the Birch and Swinnerton-Dyer Conjecture

In this last chapter, we first review some fundamentals related to abelian varieties and abelian varieties over number fields, and use this to state the weak and strong Birch and Swinnerton-Dyer (BSD) conjectures for such varieties. Then, after discussing three pairings associated to abelian varieties over (local and global) number fields, we conclude by using the cohomological techniques developed so far to give a detailed sketch of the proof due to Cassels (for elliptic curves) and Tate (for arbitrary abelian varieties) that the truth value of the BSD conjecture for a given abelian variety over a number field is constant in its isogeny class.

We will assume familiarity with standard algebraic geometry (at the level of [14], [19], [30, Ch. I], [40, Ch. 2-3], or [55]) and the basic theory of elliptic curves ([49]). In §3.3, some familiarity will be assumed with the big flat site $\mathrm{Spec}(K)_{\mathrm{fl}}$ and sheaves on it ([30, Ch. I-II]), and in §3.4 we will also need some input from the theory of analytic manifolds ([22, Ch.. 2],[45, Part II, Ch. III-IV]) and Haar measures on locally compact abelian groups ([10]). The material presented has been taken principally from from [12], [21], [23], [27], [31], and [32], and we generally follow the thread of exposition in [23, §5.2] and [32, §I.7].

3.1 A Crash Course on Abelian Varieties

The basic theory of abelian varieties is amply covered in [12], [31], [33] and [35]; here we summarize the key points needed.[55] Specifically, we review isogenies, Tate modules, characterstic polynomials of self-isogenies, and dual abelian varieties.

As above, let K be a field and $K \to K^{\mathrm{s}} \to K^{\mathrm{a}}$ a fixed choice of separable and algebraic closures of K, with $G_K := \mathrm{Gal}(K^{\mathrm{s}}/K)$. The definition of an algebraic group is reviewed in §2.2, and we emphasize that all products of K-schemes are taken over K.

Definition 3.1.1. *(Abelian Variety) An* abelian variety *over a field K is a proper smooth geometrically connected algebraic group over K.*

Theorem 3.1.2. *An abelian variety is a commutative algebraic group and a projective variety.*

Proof. Commutativity is a consequence of the Rigidity Theorem for complete varieties (see [31, 2.4]). Projectivity is proven in [31, 7.1]. For a different approach, see [40, 5.7.3]. □

For an abelian variety A over a field K, we will always denote its identity element by $0_A \in A(K) \subset A$.

Theorem/Definition 3.1.3 (Isogenies)**.** *Let A, B be abelian varieties over K and $\phi : A \to B$ be a K-scheme morphism. The following are equivalent.*

(a) We have $\dim A = \dim B$, $\phi(0_A) = 0_B$, and the induced map $\phi(K^{\mathrm{a}}) : A(K^{\mathrm{a}}) \to B(K^{\mathrm{a}})$ is surjective.
(b) We have $\dim A = \dim B$, and ϕ is a morphism of K-group schemes with finite kernel $A[\phi] := \ker(\phi)$.
(c) The map ϕ is finite faithfully flat homomorphism of K-group schemes.

A morphism ϕ satisfying these equivalent conditions is called an isogeny over K*, or a K-*isogeny*. For an isogeny ϕ, we define the* degree *of ϕ to be* $\deg(\phi) := [K(A) : \phi^*(K(B))] = |A[\phi]|$.[56]

Conditions (a) and (b) are easy to check, while (c) says that an isogeny is a quotient map (c.f. Theorem 2.2.1) with finite kernel. Unlike the case of elliptic curves, it is *not* true in general for higher dimensional abelian varieties that a sum of isogenies is an isogeny, even when nonzero.

Proof.

[55] Consequently, proofs of the following results can often be found in all four references. For brevity, we will only quote one.

[56] In the last expression, $|A[\phi]|$ is the rank of the kernel as a finite group scheme ([34, Ch. 11]). In particular, if $\ker(\phi)$ is reduced, then $\deg(\phi) = |\ker \phi(K^{\mathrm{a}})|$ is the set-theoretic cardinality of the kernel of $\phi(K^{\mathrm{a}})$.

(a) $\Leftrightarrow$ (b) By the Rigidity Theorem, a K-scheme morphism $\phi : A \to B$ satisfies $\phi(0_A) = 0_B$ iff it is a homomorphism of K-group schemes ([31, 2.2]). By Chevalley's Theorem, surjectivity of $f(K^{\mathrm{a}})$ is equivalent to that of f ([55, Ex. 7.4.E]), and this is in turn equivalent to the finiteness of the kernel by the theorem on fibre dimension and the properness of A ([14, Cor. 14.121] or [19, Ex. 3.22]).

(b) $\Leftrightarrow$ (c) See [31, 8.1].

In this case, $f_*\mathcal{O}_A$ is a locally free $\mathcal{O}_B$-module ([31, 8.1]), and then the equality of the two terms in the definition of $\ker(f)$ follows by taking the ranks at the generic point $\eta_B \in B$ and the identity $0_B \in B$. $\square$

Theorem/Definition 3.1.4 (Separable Isogenies)**.** *Let $\phi : A \to B$ be a K-isogeny of abelian varieties over K. The following are equivalent:*

(a) The field extension $\phi^* : K(B) \to K(A)$ is separable.

(b) The morphism ϕ is étale.

(c) The kernel $A[\phi]$ is an étale group scheme over K.

An isogeny ϕ is said to be separable *if it satisfies these equivalent conditions.*

Proof. See [12, Prop. 5.6]. $\square$

Example 3.1.5. Let A be an abelian variety over a finite field K. The Frobenius moprhism $\mathrm{Fr} : A \to A$ is an isogeny, but it is not separable.[57] The proof is identical to the one given in [12, Prop. 5.15] for $K = \mathbb{F}_p$.

If ϕ is a separable isogeny, then from (c) it follows that $A[\phi](K^s) \xrightarrow{\sim} A[\phi](K^{\mathrm{a}}) \xrightarrow{\sim} A(K^{\mathrm{a}})[\phi(K^{\mathrm{a}})]$.

Theorem 3.1.6. *Let A be an abelian variety of dimension $g := \dim A$ over K and $n \in \mathbb{Z}$ with $n \neq 0$.*

(a) The morphism $[n] : A \to A$ is an isogeny of degree n^{2g}.

(b) If $n \neq 0$ in K, then $[n]$ is separable and $A[n](K^{\mathrm{s}}) \cong (\mathbb{Z}/n)^{2g}$.

Proof.

(a) See [31, 8.2]. The idea is to choose a symmetric ample line bundle $\mathscr{L} \to A$ (here, symmetric means $[-1]^*\mathscr{L} \cong \mathscr{L}$; by Theorem 3.1.2, there is some ample $\mathscr{L} \to A$, and then $\mathscr{L} \otimes [-1]^*\mathscr{L}$ is symmetric and ample), and then to show that the restriction of $[n]^*\mathscr{L}$ to $A[n]$ is both trivial (clear) and ample (using the Theorem of the Cube and $n \neq 0$) to conclude that $A[n]$ is finite. Then we can apply Theorem/Definition 3.1.3(b). To compute the degree, one can either use intersection theory ([31, 8.2]) or Hilbert polynomials ([54, 0BFG]).

(b) If $\mathrm{char}\, K = 0$, then every isogeny is separable; if $\mathrm{char}\, K = p > 0$ but $p \nmid n$, then p does not divide $n^{2g} = [K(A) : \phi^*(K(B))]$, so the extension $\phi^* : K(B) \to K(A)$ is separable. The kernel $A[n]$ is an étale group scheme of rank n^{2g}, and so $A[n](K^{\mathrm{s}})$ an abelian group of order n^{2g} and exponent n. This is true for each divisor of n; conclude by structure theorem for finitely generated abelian groups.

$\square$

Theorem/Definition 3.1.7 (Isogenous Abelian Varieties)**.** *The relation $\sim_K$ on abelian varieties over K given by $A \sim_K B$ if there is a K-isogeny $f : A \to B$ is an equivalence relation. Two abelian varieties A and B are said to be* isogenous *(over K) if $A \sim_K B$.*

Proof. Reflexivity and transitivity are clear, and symmetry follows from the more precise statement that if $\phi : A \to B$ is an isogeny of degree $n \in \mathbb{Z}_{\geq 1}$, then there is an isogeny $\psi : B \to A$ such that $\psi \circ \phi = [n]$. This itself follows from the factorization theorem for algebraic group quotients ([12, 5.12-13] or [34, 5.13]). $\square$

Next, we briefly discuss Tate modules. For this, suppose that ℓ is a prime other than $\mathrm{char}\, K$. Given an abelian variety A over K, we have from Theorem 3.1.6 a sequence of G_K-modules

$$\cdots \to A[\ell^3](K^{\mathrm{s}}) \xrightarrow{\cdot \ell} A[\ell^2](K^{\mathrm{s}}) \xrightarrow{\cdot \ell} A[\ell](K^{\mathrm{s}}) \xrightarrow{\cdot \ell} 0. \tag{3.1}$$

[57] In fact, it is *purely inseparable* ([12, Props. 5.6(ii) and 5.15]).

Definition 3.1.8 (Tate Module)**.** *In the above setting, we define the* Tate module $\mathrm{T}_\ell A$ *to be the profinite G_K-module which is the inverse limit of (3.1), i.e.,* $\mathrm{T}_\ell A := \lim_{n\geq 0} A[\ell^n](K^{\mathrm{s}})$.

Since each $A[\ell^n](K^{\mathrm{s}})$ is a $\mathbb{Z}/\ell^n$-module, the Tate module $\mathrm{T}_\ell(A)$ is naturally a $\mathbb{Z}_\ell[G_K]$-module. Let $\mathrm{V}_\ell A := \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \mathrm{T}_\ell A \in \mathbb{Q}_\ell[G_K]$-Mod. The corresponding continuous morphism

$$\rho_\ell : G_K \to \mathrm{Aut}_{\mathbb{Z}_\ell\text{-Mod}}(\mathrm{T}_\ell A) \xrightarrow{\mathbb{Q}_\ell \otimes -} \mathrm{GL}(\mathrm{V}_\ell A)$$

is called the *ℓ-adic representation* associated to A and carries a lot of information about A (see, e.g., Lemma 3.1.9 and [27, Cor. IV.3.4]). Again using Theorem 3.1.6, we have that $\mathrm{T}_\ell A \cong_{\mathbb{Z}_\ell\text{-Mod}} \mathbb{Z}_\ell^{2g}$ (although not canonically), where $g := \dim A$, so ρ_ℓ has degree $2g$. The construction of the Tate module is functorial: to each K-group scheme homomorphism $\phi : A \to B$, we get an associated $\mathbb{Z}_\ell[G_K]$-module homomorphism $\mathrm{T}_\ell\phi : \mathrm{T}_\ell A \to \mathrm{T}_\ell B$ (and similarly for V_ℓ).

Lemma 3.1.9. *Let $\phi : A \to B$ be a K-isogeny and ℓ as above. The map $\mathrm{V}_\ell\phi : \mathrm{V}_\ell A \to \mathrm{V}_\ell B$ is an isomorphism of $\mathbb{Q}_\ell[G_K]$-modules.*

Proof. As in the proof of Theorem/Definition 3.1.7, pick an isogeny $\psi : B \to A$ such that $\psi \circ \phi = [n]$, where $n := \deg(\phi)$. By the functoriality of V_ℓ, we have $\mathrm{V}_\ell\psi \circ \mathrm{V}_\ell\phi = \mathrm{V}_\ell[n]$, and evidently $\mathrm{V}_\ell[n] = n$ is multiplication by n on the $\mathbb{Q}_\ell$-vector space $\mathrm{V}_\ell A$. Therefore, $\mathrm{V}_\ell\phi$ is injective, and hence an isomorphism for dimension reasons.[58] Finally, $\mathrm{V}_\ell\phi$ is G_K-equivariant because ϕ is a K-morphism. □

Now suppose that $\phi : A \to A$ is a K-isogeny of an abelian variety to itself;[59] then $\mathrm{V}_\ell\phi$ is a $\mathbb{Q}_\ell$-vector space endomorphism of $\mathrm{V}_\ell\phi$.

Definition 3.1.10 (Characteristic Polynomial)**.** *In the above setting, we define the* characteristic polynomial P_ϕ *of ϕ to be that of the endomorphism* $\mathrm{V}_\ell\phi$*, i.e.,* $P_\phi(x) := \det(x\,\mathrm{id} - \mathrm{V}_\ell\phi)$.

Remark 3.1.11. The polynomial $P_\phi(x)$ admits two other characterizations: as the characteristic polynomial of ϕ acting on the étale cohomology $\mathrm{H}^1_{\text{ét}}(A, \mathbb{Q}_\ell)$–because of the duality between the Tate module and the étale cohomology group ([31, §15])–and as the unique polynomial such that $P_\phi(n) = \deg(\phi - [n])$ for all $n \in \mathbb{Z}$ ([31, §12]).[60] It follows that $P_\phi(x) \in \mathbb{Z}[x]$ is a polynomial of degree $2g$ independent of ℓ.[61]

The final notion that we will need is that of the dual abelian variety.

Theorem/Definition 3.1.12 (Dual Variety)**.** *Let A be an abelian variety over K. The* dual variety *to A is a pair $(A^\vee, \mathscr{P})$, where $A^\vee$ is an abelian variety over K and $\mathscr{P}$ a line bundle on $A \times A^\vee$, such that*

(a) $\mathscr{P}|_{\{0\}\times A}$ is trivial[62] and for all $a \in A^\vee$ the bundle $\mathscr{P}|_{A\times\{a\}}$ lies in $\mathrm{Pic}^0(A_{\mathrm{k}(a)})$,[63] and

(b) $(A^\vee, \mathscr{P})$ is universal with respect to these properties: for every K-scheme T and line bundle $\mathscr{L} \to A\times T$ such that $\mathscr{L}|_{\{0\}\times T}$ is trivial and for all $t \in T$ the bundle $\mathscr{L}|_{A\times\{t\}}$ lies in $\mathrm{Pic}^0(A_{\mathrm{k}(t)})$, there is a unique K-morphism $f : T \to A^\vee$ such that $\mathscr{L} \cong (\mathrm{id}_A \times f)^*\mathscr{P}$.

[58] Alternatively, the same argument with ψ tells us that $\mathrm{V}_\ell A$ and $\mathrm{V}_\ell B$ have the same dimension as well.

[59] An "endoisogeny"?

[60] By the way, this gives another way to see the result of Lemma 3.1.9, since $P_\phi(0) = \deg(\phi) \neq 0$.

[61] For the beautiful story relating characteristic polynomials, zeta functions, the Weil conjectures, the Lefschetz fixed point theorem from topology, and the historic motivation for étale cohomology, see [31, §19] and [40, Ch. 7].

[62] Here $0 = 0_A \in A(K)$ is the identity element of A. A trivialization $\mathscr{O}_A \xrightarrow{\sim} \mathscr{P}|_{\{0\}\times A}$ is called a *rigidification*. It is unique only up to scaling, and we get a better universal property by fixing rigidifications, but we won't get into this.

[63] Recall that for each smooth geometrically integral variety X over a field K, we use $\mathrm{Pic}^0(X)$ to denote the group of isomorphism classes of line bundles on X which are algebraically equivalent to zero. For equivalent characterizations when $X = A$ is an abelian variety–the only case we will need–see [31, 9.2-3].

The line bundle $\mathscr{P}$ (sometimes denoted $\mathscr{P}_A$) is called the *Poincaré bundle (or sheaf)* on $A \times A^\vee$. Often, $A^\vee$ is called the dual variety to A. By (b), the pair $(A^\vee, \mathscr{P})$ is determined uniquely up to unique isomorphism if it exists.

Remark 3.1.13.

(a) Taking $T = \operatorname{Spec} L$ for a field L/K in (b), we see that $A^\vee(L) \cong \operatorname{Pic}^0(A_L)$, functorially in L. In particular, when K is perfect, taking $L = K^{\mathrm{a}}$ tells us that the closed points of $A^\vee$ are in bijection with G_K-orbits in $\operatorname{Pic}^0(A_{K^{\mathrm{a}}})$.

(b) Taking $T = \operatorname{Spec} K[\varepsilon]$ (where $K[\varepsilon] := K[x]/(x^2)$) and using the exact sequence

$$0 \to \mathrm{H}^1(A, \mathscr{O}_A) \to \operatorname{Pic}(A_{K[\varepsilon]}) \to \operatorname{Pic}(A)$$

of groups coming from deformation theory, it follows that $\mathrm{T}_0 A^\vee \xrightarrow{\sim} \mathrm{H}^1(A, \mathscr{O}_A)$ ([12, 6.6]); in particular, since $\dim_K \mathrm{H}^1(A, \mathscr{O}_A) = \dim_K \mathrm{T}_0 A = \dim A$ for any abelian variety A ([35, §4]), we conclude that $\dim A^\vee = \dim A$.

(c) Taking $T = A^\vee \times A$ and $\mathscr{L} := \mathrm{sw}^* \mathscr{P}_A$, where $\mathrm{sw} : A^\vee \times A \to A \times A^\vee$ is the swap map, gives a unique K-morphism $\mathrm{ev} : A \to A^{\vee\vee}$ such that $\mathrm{sw}^* \mathscr{P}_A \cong (\mathrm{id}_{A^\vee} \times \mathrm{ev})^* \mathscr{P}_{A^\vee}$. One can then show that ev is an isomorphism, justifying the name "dual variety" ([12, 7.9], [31, 9.5], [38, §III.20]).

(d) Let $\phi : A \to B$ be a K-isogeny. Taking $T = A \times B^\vee$ shows that there is a unique K-morphism $\phi^\vee : B^\vee \to A^\vee$ such that $(\phi \times \mathrm{id}_{B^\vee})^* \mathscr{P}_B \cong (\mathrm{id}_A \times \phi^\vee)^* \mathscr{P}_A$ as line bundles on $A \times B^\vee$. One can show that $\phi^\vee$ is also an isogeny, called the *dual isogeny*; indeed, one shows more specifically that $B^\vee[\phi^\vee]$ is the Cartier dual $A[\phi]^{\mathrm{D}}$ ([34, §11c]) to $A[\phi]$, and is hence finite ([31, §11], [35, §15]; c.f. §3.3).

(e) It is nontrivial to construct the dual variety, and there are several approaches. One is to use the general construction of the Picard scheme $\operatorname{Pic}_{X/K}$, and then take $A^\vee := \operatorname{Pic}^0_{X/K}$ to be the connected component of the identity; one must then show that $A^\vee$ is smooth, or equivalently reduced ([12, 6.18]). Over $K = \mathbb{C}$, the exponential exact sequence gives us an isomorphism $\exp : \mathrm{H}^1(A^{\mathrm{an}}, \mathscr{O}_{A^{\mathrm{an}}}) / \mathrm{H}^1(A^{\mathrm{an}}, \mathbb{Z}) \to A^\vee(\mathbb{C})$ ([31, 9.4(c)]). A third approach is to take $A^\vee := \mathscr{E}\mathrm{xt}^1(A, \mathbb{G}_m)$ on the big flat site $\operatorname{Spec}(K)_{\mathrm{fl}}$, in which case $\phi^\vee = \mathscr{E}\mathrm{xt}^1(\phi, \mathbb{G}_m)$, but then one must show this sheaf is representable ([31, §11], §3.3). A fourth, concrete, approach is to construct $A^\vee$ directly as a quotient of A ([31, §10]); this has the advantage that is also automatically proves Lemma 3.1.14 below.

(f) When $\dim A = 1$, i.e., A is an elliptic curve, we have $A \cong A^\vee$ as abelian varieties; indeed, this is often used in the proof of the associativity of the group law on A (e.g., [49, §III.3]). This simplifies many of the formulae appearing in the conjectures (e.g., Conjecture 3.4.4) in the case of elliptic curves.

Lemma 3.1.14. *If A is an abelian variety over K, then $A \sim_K A^\vee$.*

Proof. This is often stated as the existence of a *polarization* on A; see [31, §9, 10, 13]. □

3.2 Abelian Varieties over Number Fields

In this section, we summarize basic results about abelian varieties over number fields. Firstly, we discuss good and bad reduction of abelian varieties, introduce the Selmer and Tate-Shafarevich groups, and discuss the Mordell-Weil Theorem. Finally, we state the Birch and Swinnerton-Dyer conjecture, and prove the isogeny invariance of the weak form of it; the strong form is then treated in the last section, after discussing three technical tools needed for it in the next one. The following material has been adapted from [21, Part C], [27, Ch. III], [31], [32, §I.6-7], and [49, Ch. VII-VIII].

In this section, K denotes a number field and we use the notation established in Notation, Conventions, and Fundamentals. For each prime $\mathfrak{p}$ of $\mathscr{O}_K$, we denote by $\mathscr{O}_{K,\mathfrak{p}}$ the localization of $\mathscr{O}_K$ at $\mathfrak{p}$.

Definition 3.2.1. *(Good and Bad Reduction) Let A be an abelian variety over K and $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ (corresponding to a $v \in \mathrm{M}_K^0$). We say that A has* good reduction *at $\mathfrak{p}$ (or v) if there is an abelian scheme*[64] *$\mathscr{A}$ over $\operatorname{Spec} \mathcal{O}_{K,\mathfrak{p}}$ and a K-scheme isomorphism $\mathscr{A}_K \cong_{K\text{-Sch}} A$ of the generic fiber of $\mathscr{A}$ with A. Otherwise, we say that A has* bad reduction *at $\mathfrak{p}$.*

Lemma 3.2.2. *Let A be an abelian variety over K. There is a finite subset $S \subset \mathrm{M}_K$ containing M_K^∞ and an abelian scheme $\mathscr{A}$ over $\mathcal{O}_{K,S}$ along with an isomorphism $\mathscr{A}_K \cong_{K\text{-Sch}} A$. In particular, an abelian variety A over K has good reduction at almost all (i.e., all but finitely many places) of K.*

Proof Sketch. This is the standard technique of *spreading out*. To produce $\mathscr{A}$, use [40, Thm. 3.2.1(i)-(ii)] and the fact that proper morphisms, smooth morphisms, and morphisms with geometrically connected fibers spread out. Then apply [40, Theorem 3.2.1(iii)] to the product $m : A \times A \to A$ and inversion $i : A \to A$ morphisms to turn the spread out scheme $\mathscr{A}$ into an abelian scheme; see also [40, Remark 5.7.24].[65] □

Remark 3.2.3. A theorem due to Chow and Lang asserts that when A has good reduction at $\mathfrak{p}$ and $\mathscr{A}$ as in Definition 3.2.1, then the isomorphism class of the abelian variey $\mathscr{A}_{\mathrm{k}(\mathfrak{p})}$ over $\mathrm{k}(\mathfrak{p})$ does not depend on the choice of $\mathscr{A}$, and is called the *reduction* of A at $\mathfrak{p}$ (or v) and denoted $\tilde{A}_\mathfrak{p}$ or $\tilde{A}_v$. The modern approach to this theorem is via Néron models: there is a smooth separated finite type scheme $\mathscr{N}$ over $\mathcal{O}_K$ such that for every smooth $\mathcal{O}_K$-scheme $\mathscr{T}$ with generic fiber $T := \mathscr{T}_K$, the natural map $\mathscr{A}(\mathscr{T}) \to A(T)$ is an isomorphism. One can use this to show that A has good reduction at $\mathfrak{p}$ iff $\mathscr{N}_{\mathrm{k}(\mathfrak{p})}$ is an abelian variety, and then any reduction of A at $\mathfrak{p}$ is isomorphic to $\mathscr{N}_{\mathrm{k}(\mathfrak{p})}$. This shows also that A spreads out over $\mathcal{O}_{K,S}$ where S is the set of all primes of bad reduction. The definitive account can be found in [4].

Now suppose that A is an abelian variety with good reduction at a place $v \in \mathrm{M}_K^0$, so that the reduction $\tilde{A}_v$ is an abelian variety over the finite field k_v. The Frobenius morphism $\mathrm{Fr}_v : \tilde{A}_v \to \tilde{A}_v$ is an isogeny (Example 3.1.5); let $P_v(x) \in \mathbb{Z}[x]$ denote its characteristic polynomial (Definition 3.1.10 and Remark 3.1.11).

Remark 3.2.4. The polynomial $P_v(x)$ has the property that if we write $P_v(x) = \prod_{i=1}^{2g}(x - \alpha_i)$ for algebraic integers α_i and $g = \dim A$, then $|\alpha_i| = q_v^{1/2}$ for each i (where $q_v := |\mathrm{k}_v|$) and for each $n \in \mathbb{Z}_{\geq 1}$, we have $\tilde{A}_v(\mathrm{k}_{v,n}) = \prod_{i=1}^{2g}(1 - \alpha_i^n)$, where $\mathrm{k}_{v,n}$ is the degree n extension of k_v ([31, §19]). It follows that $\tilde{A}_v(\mathrm{k}_v) = P_v(1) = q_v^{-g} P_v(q_v)$ and that for each $s \in \mathbb{C}$, we have $|q_v^{-2gs} P_v(q_v^s)| \geq |1 - q_v^{1/2-s}|^{2g}$.

Definition 3.2.5. *Let A be an abelian variety over K and $S \subset \mathrm{M}_K$ a finite set containing M_K^∞ and all the places of bad reduction for A. With the above notation, we define the associated L-*function *to be*

$$L_S(A, s) := \prod_{v \notin S} q_v^{2gs} P_v(q_v^s)^{-1}.$$

It follows from Remark 3.2.4 that the product is dominated by $\zeta_K(s - 1/2)^{2g}$ and hence converges to give a holomorphic function on $\operatorname{Re} s > 3/2$; see Conjecture 3.2.15.

Theorem 3.2.6. *Let $\phi : A \to B$ be a K-isogeny of abelian varieties over K, and let $S \subset \mathrm{M}_K$ be a finite set containing M_K^∞, all places of bad reduction for A and B*[66]*, and all places whose residue characteristic divides $\deg(\phi)$. Let $K_S \subset K^{\mathrm{a}}$ be the maximal unramified-outside-S extension of K. Then $A[\phi](K_S) \twoheadrightarrow A[\phi](K^{\mathrm{a}})$ and $\phi(K_S) : A(K_S) \to B(K_S)$ is surjective.*

[64] An *abelian scheme* over a base scheme S is a proper smooth S-scheme $\mathscr{A} \to S$ with geometrically connected fibers ([31, §20]). This implies that for each point $s \in S$, the fiber $\mathscr{A}_s$ is an abelian variety over the residue field $\mathrm{k}(s)$; in particular, if, as above, S is integral with generic point $\eta \in S$ and function field $K = \mathrm{k}(\eta)$, then the generic fiber $\mathscr{A}_K := \mathscr{A}_\eta$ is an abelian variety over K. The notion of an abelian scheme is the spreading out of the notion of an abelian variety to arbitrary base schemes.

[65] The rough idea is that the same defining equations for A suffice also to define $\mathscr{A}$, as long as we stay away from the primes dividing the denominators of the coefficients appearing in these equations.

[66] It can be shown using Néron models (Remark 3.2.3) and the Néron-Ogg-Shafarevich criterion that isogenous abelian varieties have bad reduction at the same set of primes ([46, §1, Thm. 1, Cor. 2]), but we won't need this.

Proof Sketch. There are two approaches. One could argue by showing that for each $p \in B(K_S)$, the schematic inverse image $\phi^{-1}(p)$ splits over K_S (and then use this for $p = 0_B$ to deduce the first statement), and this can be proven by spreading out: by Remark 3.2.3, A, B spread out to abelian schemes $\mathscr{A}, \mathscr{B}$ over $\mathcal{O}_{K,S}$ and ϕ to a finite flat morphism $\mathscr{A} \to \mathscr{B}$ which is étale thanks to the hypotheses on S. Then p spreads out to a section of $\mathscr{B}$ over $\mathcal{O}_{K,S}$ and hence $\phi^{-1}(p)$ to a finite étale subscheme of $\mathscr{A}$ over $\mathcal{O}_{K,S}$, which can then be shown to split ([31, §20], [32, Lemma I.6.1]). The second approach notes that for each $v \notin S$, reduction gives an exact sequence $0 \to A_1(K_v^{\mathrm{nr}}) \to A(K_v^{\mathrm{nr}}) \to \tilde{A}_v(\mathrm{k}_v^{\mathrm{a}}) \to 0$, where exactness at the right comes from Hensel's Lemma, and the first group $A_1(K_v^{\mathrm{nr}})$ can be interepreted as the group of $\mathfrak{m}_v^{\mathrm{nr}}$-points of a formal group over $\mathcal{O}_v$ ([21, Thm. C.2.6]), and similarly for B. Then one can show that $A_1(K_v^{\mathrm{nr}}) \to B_1(K_v^{\mathrm{nr}})$ and $\tilde{A}_v(\mathrm{k}_v^{\mathrm{a}}) \to \tilde{B}_v(\mathrm{k}_v^{\mathrm{a}})$ are surjective (by the assumption on residue characteristic and Theorem 2.2.1(c) respectively), whence so is $\phi(K_v^{\mathrm{nr}}) : A(K_v^{\mathrm{nr}}) \to B(K_v^{\mathrm{nr}})$. Combining these for all $v \notin S$ yields the result. □

It follows from Theorem 3.2.6 that if A is an abelian variety over K and ℓ a prime, then for any place $v \in \mathrm{M}_K^0$ of good reduction and such that $\ell \neq 0$ in k_v, the ℓ-adic representation $\mathrm{V}_\ell A$ of G_K is unramified at v, i.e., the inertia group I_v acts trivially on $\mathrm{V}_\ell A$.[67] Now the quotient $\mathrm{D}_v/\mathrm{I}_v \cong G_{\mathrm{k}_v} \cong \hat{\mathbb{Z}}$ is topologically generated by the Frobenius endomorphism Fr_v, and so we get a well-defined action of Fr_v on $\mathrm{V}_\ell A$.

Lemma 3.2.7. *In the above setting, $P_v(x)$ equals the characteristic polynomial of Fr_v acting on $\mathrm{V}_\ell A$.*

Proof. Reduction gives $\mathrm{D}_v/\mathrm{I}_v \cong G_{\mathrm{k}_v}$-isomorphisms $\mathrm{T}_\ell(A) \to \mathrm{T}_\ell(\tilde{A}_v)$; see [27, §III.3] and [31, §19]. □

Next, suppose that $\phi : A \to B$ be a K-isogeny of abelian varieties over K. By Theorem/Definition 3.1.3(c), we have a short exact sequence

$$0 \to A[\phi] \to A \to B \to 0 \tag{3.2}$$

in $\mathscr{G}\mathrm{rp}_K$. Considering a piece of the associated long exact sequence in Galois cohomology, and for each $v \in \mathrm{M}_K$ the corresponding sequence over K_v (Remark 2.2.3(d)), we obtain the commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \operatorname{coker}\phi(K) & \longrightarrow & \mathrm{H}^1(K, A[\phi]) & \longrightarrow & \mathrm{WC}(A)[\phi_*] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \displaystyle\bigoplus_{v\in\mathrm{M}_K} \operatorname{coker}\phi(K_v) & \longrightarrow & \displaystyle\bigoplus_{v\in\mathrm{M}_K} \mathrm{H}^1(K_v, A_v[\phi_v]) & \longrightarrow & \displaystyle\bigoplus_{v\in\mathrm{M}_K} \mathrm{WC}(A_v)[\phi_{v,*}] & \longrightarrow & 0,
\end{array}$$

where we have used Example 2.2.9 to write $\mathrm{H}^1(K, A)$ as $\mathrm{WC}(A)$, the notation $\phi_* : \mathrm{WC}(A) \to \mathrm{WC}(B)$ denotes the induced map of Weil-Châtelet Groups (and similarly for each K_v), the vertical maps are given by the sum of the local restriction maps, and we are using

Lemma 3.2.8. *For each $\xi \in \mathrm{H}^1(K, A[\phi])$ (resp. $\mathrm{WC}(A)$), we have $\mathrm{Res}_v \xi = 0$ for almost all v.*

Proof. See [32, Lemma I.6.3]. □

Definition 3.2.9. *In the above setting, we define the ϕ-*Selmer group *and Tate-Shafarevich group of A to be, respectively,*

$$\mathrm{Sel}^\phi(A) := \ker\left(\mathrm{H}^1(K, A[\phi]) \to \bigoplus_{v\in\mathrm{M}_K} \mathrm{WC}(A_v)\right) \text{ and } Ш(A) := \ker\left(\mathrm{WC}(A) \to \bigoplus_{v\in\mathrm{M}_K} \mathrm{WC}(A_v)\right).$$

[67] This characterizes places v of good reduction, see [46, §1, Thm. 1]. (This is the criterion of Footnote 66.)

According to Example 2.2.9, the elements of the Tate-Shafarevich group $Ш(A)$ can be interpreted as (K-isomorphism classes) of principal homogeneous spaces for A which are everywhere locally trivial, i.e., admit a K_v-rational point for each $v \in \mathrm{M}_K$, and is therefore a quantitative measure of the obstruction to the local-to-global principal for abelian varieties. From the above definitions, we immediately obtain the short exact sequence of groups

$$0 \to B(K)/\phi(A(K)) \to \mathrm{Sel}^{\phi}(A) \to Ш(A)[\phi_*] \to 0. \tag{3.3}$$

The key finiteness result in the whole story is

Theorem 3.2.10. *If $\phi : A \to B$ is a K-isogeny of abelian varieties over K, then $\mathrm{Sel}^{\phi}(A)$ is finite.*

Proof. Identical to the proof for elliptic curves in [49, Theorem X.4.2]. The idea is to construct a finite S with $\mathrm{M}_K^{\infty} \subset S \subset \mathrm{M}_K$ such that (in the notation of Remark 2.2.3(d)), we have $\mathrm{Sel}^{\phi}(A) \subset \mathrm{H}^1(K, A[\phi]; S)$, and then to show that the latter group is finite. Here are some more details.

(1) Let $S \subset \mathrm{M}_K$ be a finite set as in Theorem 3.2.6. Given any $\xi \in \mathrm{Sel}^{\phi}(A)$ and $v \in \mathrm{M}_K$, by considering a suitable lift in $\mathscr{Z}^1_{\mathrm{cts}}(G_v, A_v[\phi_v])$, there is a $p_v \in A(K_v^{\mathrm{a}})$ so that for all $\sigma \in G_v$, we have $\xi(\sigma) = p_v^{\sigma} - p_v$. In particular, this holds for all $\sigma \in \mathrm{I}_v$. Considering the reduction morphism $A(K_v^{\mathrm{a}}) \to \tilde{A}_v(\mathrm{k}_v^{\mathrm{a}})$ and noting that I_v acts trivially on the latter by definition tells us that when $\sigma \in \mathrm{I}_v$, $\xi(\sigma)$ belongs to the kernel of the reduction morphism. But again, considering the formal group law structure on $A_1(K_v^{\mathrm{a}})$ (as in the proof of Theorem 3.2.6) along with the hypothesis that the residue characteristic of v does not divide $\deg(\phi)$ tells us that $A_v[\phi_v](K_v^{\mathrm{a}})$ injects into $\tilde{A}_v(\mathrm{k}_v^{\mathrm{a}})$, and hence $\xi(\sigma) = 0$ for all $\sigma \in \mathrm{I}_v$.

(2) If M is a finite discrete G_K-module and S a finite set with $\mathrm{M}_K^{\infty} \subset S \subset \mathrm{M}_K$, then $\mathrm{H}^1(G_K, M; S)$ is finite. Indeed, by Lemma 2.1.1 and the fundamental theorem of infinite Galois theory, there is a finite Galois L/K such that G_L acts trivially on M. Then by the profinite inflation-restriction sequence (Theorem 1.2.6 and Remark 2.1.5) and the finiteness of $\mathrm{H}^1(L/K, M^{G_L})$ (Remark 1.1.6(b)), we may replace K by L and hence are reduced to the case where G_K acts trivially on M. Then, by Remark 2.1.8(a), $\mathrm{H}^1(G_K, M) = \mathrm{Hom}^{\mathrm{cts}}_{\mathrm{Grp}}(G_K, M)$. If M has exponent $m \in \mathbb{Z}_{\geq 1}$, and $K_{S,m}$ is the maximal abelian extension of K of exponent m unramified outside of S, then under the above identification, $\mathrm{H}^1(G_K, M; S)$ lies in the image of $\mathrm{Hom}(\mathrm{Gal}(K_{S,m}/K), M) \to \mathrm{Hom}^{\mathrm{cts}}_{\mathrm{Grp}}(G_K, M)$. Finiteness follows from the fact that $K_{S,m}/K$ is finite; this is proven using the two fundamental finiteness results from algebraic number theory: the finiteness of the class group $\mathrm{Cl}(K)$ and the finite generation of the S-unit group $\mathscr{O}_{K,S}^{\times}$.[68]

□

Here are two important corollaries.

Corollary 3.2.11. *Let A be an abelian variety over a number field K, and let $n \in \mathbb{Z}_{\geq 1}$.*

(a) (Weak Mordell-Weil) The group $A(K)/nA(K)$ is finite.

(b) The group $Ш(A)[n]$ of n-torsion in the Tate-Shafarevich group is finite.

Proof. Both claims follow from Theorems 3.1.6 and 3.2.10 and the sequence (3.3). □

For a phrasing of the above proof of Corollary 3.2.11(a) in the language of étale cohomology, see [30, Thm. III.4.22]. Corollary 3.2.11(b) is a piece of evidence towards the currently open conjecture that for each abelian variety A over K, the whole Tate-Shafarevich group $Ш(A)$ is finite; see Conjecture 3.4.4

Corollary 3.2.12. *Let $A \sim_K B$ be isogenous abelian varieties over a number field K. If one of $Ш(A)$ or $Ш(B)$ is finite, then so is the other. Therefore, for any A over K, the group $Ш(A)$ is finite iff $Ш(A^{\vee})$ is.*

[68] These results are themselves equivalent to certain adèlic and idèlic compactness results.

Proof. By Theorem/Definition 3.1.7, we may assume $Ш(B)$ is finite and show that $Ш(A)$ is. Let $\phi : A \to B$ be a K-isogeny. From Theorem 3.2.10 and (3.3), the kernel $Ш(A)[\phi_*]$ is finite; we conclude by considering the exact sequence $0 \to Ш(A)[\phi_*] \to Ш(A) \xrightarrow{\phi_*} Ш(B)$. The second statement follows from the first combined with Remark 3.1.13(c) and Lemma 3.1.14. □

The other key ingredient in the proof of the full Mordell-Weil Theorem–the finite generation of $A(K)$–is the theory of heights.[69] Recall ([49, §VIII.5]) that for each $n \in \mathbb{Z}_{\geq 0}$, there is a unique $G_{\mathbb{Q}}$-invariant function $h : \mathbb{P}^n(\mathbb{Q}^{\mathrm{a}}) \to \mathbb{R}$ such that if $K \subset \mathbb{Q}^{\mathrm{a}}$ is a number field and $p = [x_0 : \cdots : x_n] \in \mathbb{P}^n(K) \subset \mathbb{P}^n(\mathbb{Q}^{\mathrm{a}})$ is chosen with all $x_i \in K$, then

$$h(p) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in \mathrm{M}_K} [K_v : \mathbb{Q}_v] \log \max_{i=0}^{n} |x_i|_v,$$

where $\mathbb{Q}_v \subset K_v$ is the completion of $\mathbb{Q}$ in K_v. Given an abelian variety A and a very ample line bundle $\mathscr{L} \to A$, we consider the corresponding embedding $\varphi_{\mathscr{L}} : A \to \mathbb{P}\mathrm{H}^0(A, \mathscr{L})^\vee \cong \mathbb{P}^n_K$ for some $n \in \mathbb{Z}_{\geq 1}$ and the resulting height function $h_{\mathscr{L}} : A(K^{\mathrm{a}}) \to \mathbb{R}$ given by postcomposing with h on $\mathbb{P}^n(K^{\mathrm{a}}) = \mathbb{P}^n(\mathbb{Q}^{\mathrm{a}})$. One can then show that if $\mathscr{L}$ is symmetric, then $h_{\mathscr{L}}$ is (up to a bounded function) a quadratic form on $A(K^{\mathrm{a}})$,[70] and so by using Corollary 3.2.11(a) and descent via this height function,[71] we obtain exactly as for elliptic curves,

Theorem 3.2.13 (Mordell-Weil)**.** *For any abelian variety A over K, the group $A(K)$ is finitely generated.*

See [47]. In particular, we define the *rank* of A to be the rank of $A(K)$, i.e., $\mathrm{rk}(A) := \dim_{\mathbb{Q}} A(K)_{\mathbb{Q}}$.

Lemma 3.2.14. *Let $\phi : A \to B$ be a K-isogeny of abelian varieties over a number field K. Then the map $\phi(K)_{\mathbb{Q}} : A(K)_{\mathbb{Q}} \to B(K)_{\mathbb{Q}}$ is $\mathbb{Q}$-linear isomorphism. In particular, A and B have the same rank, say $r \in \mathbb{Z}_{\geq 0}$. Moreover, if $a_1, \ldots, a_r \in A(K)$ give a $\mathbb{Q}$-basis for $A(K)_{\mathbb{Q}}$, then so do $\phi(a_1), \ldots, \phi(a_r) \in B(K)$.*

Proof. Identical to the proof of Lemma 3.1.9, using the functor $-(K)_{\mathbb{Q}}$ this time. □

We are now ready to formulate

Conjecture 3.2.15 (Weak Birch and Swinnerton-Dyer)**.** *Let A be an abelian variety over a number field K and $S \subset \mathrm{M}_K$ a finite set containing M_K^∞ and all places of bad reduction for A. Then $L_S(A, s)$ can be analytically continued to a neighborhood of $s = 1$, and $\mathrm{ord}_{s=1} L_S(A, s) = \mathrm{rk}(A)$.*

Note that the quantity $\mathrm{ord}_{s=1} L_S(A, s)$ is independent of the choice of S–as predicted by the conjecture–thanks to Remark 3.2.4. The strength of the conjecture lies in the connection it proposes between the global arithmetic of K (manifested in $\mathrm{rk}(A)$) and the local arithmetic of K (manifested in the analytic object $L_S(A, s)$ made up of local factors coming from the reductions $\tilde{A}_v$). We are immediately ready to prove

Theorem 3.2.16. *Let $A \sim_K B$ be isogenous abelian varieties over a number field K. If the weak BSD conjecture (Conjecture 3.2.15) is true for one of A or B, then it is true for both.*

Proof. Let $S \subset \mathrm{M}_K$ be a finite set as in Theorem 3.2.6; then $L_S(A, s) = L_S(B, s)$ thanks to Lemma 3.1.9, Lemma 3.2.7, and the observation that $\mathrm{V}_\ell\phi \circ \mathrm{V}_\ell\mathrm{Fr}_{v,A} = \mathrm{V}_\ell\mathrm{Fr}_{v,B} \circ \mathrm{V}_\ell\phi$ for all suitable ℓ. The result follows from Lemma 3.2.14. □

[69] Unfortunately, we do not have the space to develop the theory of heights, an important topic in diophantine geometry.

[70] As for elliptic curves, one can normalize by defining the *Néron-Tate canonical height* $\hat{h}_{\mathscr{L}}(p) := \lim_{n \to \infty} 2^{-2n} h_{\mathscr{L}}(2^n p)$, which is an actual quadratic form.

[71] Here we are using Theorem 3.1.2 to obtain the existence of *some* very ample line bundle.

3.3 Three Pairings associated with Abelian Varieties

In this section, we describe the local Tate pairing, the Cassels-Tate pairing, and the Néron-Tate canonical height pairing, which will serve as important tools in the final section. For an overview of these pairings, and the description of two more–the Weil e_ϕ pairing and the Tate-Lichtenbaum pairing–see [48].[72]

Recall (Footnote 37) that there is a fully faithful embedding $\mathrm{Grp}_K \hookrightarrow \mathrm{Shv}(\mathrm{Spec}(K)_{\mathrm{fl}}, \mathrm{Ab}) =: \mathscr{A}\mathrm{b}_K$ of the category of commutative algebraic groups over a field K into the category of abelian sheaves over the big flat (i.e., fppf) site $\mathrm{Spec}(K)_{\mathrm{fl}}$, and we identify $\mathscr{G}\mathrm{rp}_K$ with its (essential) image ([38, Ch. III]). In $\mathscr{A}\mathrm{b}_K$, there is an internal sheaf $\mathscr{H}\mathrm{om}$ operation, and for $G \in \mathscr{A}\mathrm{b}_K$, we define its *Cartier dual* to be $G^{\mathrm{D}} := \mathscr{H}\mathrm{om}(G, \mathbb{G}_m)$. For instance, when $G \in \mathscr{G}\mathrm{rp}_K$, then by definition $G^{\mathrm{D}}(K) = \mathrm{Hom}_{\mathscr{G}\mathrm{rp}_K}(G, \mathbb{G}_m)$ is the character group of G.[73] The endofunctor $(-)^{\mathrm{D}} = \mathscr{H}\mathrm{om}(-, \mathbb{G}_m)$ of $\mathscr{A}\mathrm{b}_K$ is left exact (and $\mathscr{A}\mathrm{b}_K$ has enough injectives–[30, Prop. III.1.1]), so we may define its derived functor $\mathscr{E}\mathrm{xt}^\bullet(-, \mathbb{G}_m) := \mathrm{R}^\bullet\mathscr{H}\mathrm{om}(-, \mathbb{G}_m)$. Now for a general G and $n \in \mathbb{Z}_{\geq 0}$, the sheaf $\mathscr{E}\mathrm{xt}^n(G, \mathbb{G}_m)$ may not come from an algebraic group, i.e., lie in the essential image of $\mathscr{G}\mathrm{rp}_K$,[74] but here are three important scenarios–the only ones we'll need–when it does:

(a) when $n = 0$ and G is finite; this is the usual formulation of Cartier duality ([34, §11c]), and
(b) when $n = 0, 1$ and $G = A$ is an abelian variety. The case $n = 0$ is clear: $A^{\mathrm{D}} = 0$ by the properness of A. The case $n = 1$ is of the dual abelian variety $A^\vee = \mathscr{E}\mathrm{xt}^1(A, \mathbb{G}_m)$ ([38, §III.18]).

Given a K-isogeny $\phi : A \to B$ of abelian varieties, the derived functor $\mathrm{R}^\bullet(-)^{\mathrm{D}}$ gives the exact sequence

$$0 = A^{\mathrm{D}} \to A[\phi]^{\mathrm{D}} \xrightarrow{\delta} \mathscr{E}\mathrm{xt}^1(B, \mathbb{G}_m) \xrightarrow{\mathscr{E}\mathrm{xt}^1(\phi, \mathbb{G}_m)} \mathscr{E}\mathrm{xt}^1(A, \mathbb{G}_m),$$

yielding the promised isomorphism $B^\vee[\phi^\vee] \cong A[\phi]^{\mathrm{D}}$ of Remark 3.1.13(d) ([38, §III.19]). From this, we get (see [34, §11c]) a natural bilinear morphism of K-group schemes

$$A[\phi] \times B^\vee[\phi^\vee] \to \mathbb{G}_m,$$

which, if $\deg(\phi) = n$, factors through μ_n. When K is perfect, this in turn yields G_K-invariant bilinear pairings

$$A[\phi](K^{\mathrm{a}}) \times B^\vee[\phi^\vee](K^{\mathrm{a}}) \to \mu_n(A^{\mathrm{a}}).$$

As in §2.4, precomposing with cup products in Galois cohomology gives for each $p, q \in \mathbb{Z}_{\geq 0}$ a bilinear map

$$\mathrm{H}^p(K, A[\phi]) \times \mathrm{H}^q(K, B^\vee[\phi^\vee]) \to \mathrm{H}^{p+q}(K, \mu_n). \tag{3.4}$$

These products then give rise to a wealth of different pairings, natural in A and B. For instance, taking $p = q = 0$ gives the Weil e_ϕ pairing, which can be shown to be nondegenerate and has important uses ([31, §16], c.f. [49, §III.8]). Another pairing obtained from this is the local Tate pairing.

Theorem/Definition 3.3.1. *(Local Tate Pairing) For an abelian variety A over a local number field K and for $p = 0, 1$, there is a bilinear pairing*

$$\langle -, - \rangle : \mathrm{H}^p(K, A) \times \mathrm{H}^{1-p}(K, A^\vee) \to \mathbb{Q}/\mathbb{Z}$$

with the following properties.

(a) The pairing is nondegenerate, i.e., induces an isomorphism $A^\vee(K) \xrightarrow{\sim} \mathrm{WC}(A)^*$.[75]

[72] Evidently, John Tate made a lot of contributions to this area, c.f. Footnote 1 of [48].

[73] Note also that when G is geometrically reduced, we have $G^{\mathrm{D}}(K^{\mathrm{a}}) = \mathrm{Hom}_{\mathscr{G}\mathrm{rp}_{K^{\mathrm{a}}}}(G_{K^{\mathrm{a}}}, \mathbb{G}_m) \cong \mathrm{Hom}_{\mathrm{Grp}}(G(K^{\mathrm{a}}), \mathbb{G}_m(K^{\mathrm{a}}))$, establishing the agreement with the notion introduced in §2.4. The last isomorphism here is using [19, Prop. II.2.6].

[74] See, e.g., [34, Ex. 1-1] for $G = \mathbb{G}_a$ and $n = 0$.

[75] Here we are using, of course, Example 2.2.9. We also get an isomorphism $\mathrm{WC}(A^\vee) \xrightarrow{\sim} A(K)^*$. Finally, the same thing holds for the dual variety.

(b) The pairing is natural, i.e., if $\phi : A \to B$ is a K-isogeny, then $\langle \phi_*(-), - \rangle = \langle -, \phi^\vee_*(-) \rangle$.

Proof Sketch. ([48, §8]) We do the case $p = 0$; the other case is obtained by biduality (Remark 3.1.13(c)). For $n \in \mathbb{Z}_{\geq 1}$, using Theorem 3.1.6, take $A = B$, $\phi = [n]$, and $p = q = 1$ in (3.4) to get a bilinear map

$$\mathrm{H}^1(K, A[n]) \times \mathrm{H}^1(K, A^\vee[n]) \to \mathrm{H}^2(K, \mu_n).$$

Using Examples 2.2.7, 2.2.8, and 2.2.10, write this last group as $\mathrm{Br}(K)[n] \cong (\mathbb{Q}/\mathbb{Z})[n] = \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Precompose on the left with the connecting map $\delta : A(K)/nA(K) \to \mathrm{H}^1(K, A[n])$ of Galois cohomology, and show that the image pairs trivially with $A^\vee(K)/nA^\vee(K)$ obtained similarly to descend on the right to the quotient $\mathrm{H}^1(K, A^\vee)[n] = \mathrm{WC}(A^\vee)[n]$, resulting in a pairing

$$A(K)/nA(K) \times \mathrm{WC}(A^\vee)[n] \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

Taking a suitable limit as $n \to \infty$ gives the pairing. See [32, Cor. I.3.4] for an approach along these lines using the Barsotti-Weil formula, or [32, Rem. I.3.5] or [52] for Tate's original construction. □

Remark 3.3.2. In the above setting, one can show that $\mathrm{H}^p(K, A) = 0$ for $p \geq 2$ (see [32, Cor. I.3.4] or combine Props. 15 and 16 of [44, §II.5.3]). Also, there are natural topologies on the groups in (a) such that the isomorphisms are topological isomorphisms.

Another cohomological pairing we will need to use is the Cassels-Tate pairing.

Theorem/Definition 3.3.3 (Cassels-Tate)**.** *For an abelian variety A over a (global) number field K, there is a bilinear pairing*

$$\langle -, - \rangle_{\mathrm{CT}} : Ш(A) \times Ш(A^\vee) \to \mathbb{Q}/\mathbb{Z}$$

with the following properties.

(a) If $Ш(A)$ and $Ш(A^\vee)$ are finite (see Corollary 3.2.12), then the pairing is nondegenerate.[76]

(b) The pairing is natural, i.e., if $\phi : A \to B$ is a K-isogeny, then $\langle \phi_*(-), - \rangle_{\mathrm{CT}} = \langle -, \phi^\vee_*(-) \rangle_{\mathrm{CT}}$.

Proof. Unsurprising, the pairing is cohomological, although the construction is more involved. See [32, I.6.9], [41], or [48, §10]; the second reference has four constructions, and shows why they all agree. □

Remark 3.3.4.

(a) If A admits a principal polarization by a K-rational divisor, then the resulting bilinear pairing $Ш(A)$, is alternating. This can be used to show that, in this setting (which holds always for elliptic curves and Jacobians), the Tate-Shafarevich group, if finite, must have order a perfect square; this is consistent with experimentatal observations. See again [8, Ch. XII] and [41].

(b) There is a common generalization of Thms. 2.3.3, 3.3.1, and 3.3.3, via motivic cohomology ([18]).

The final pairing needed is not cohomological, but rather arithmetic in nature.

Theorem/Definition 3.3.5 (Néron-Tate Canonical Height Pairing)**.** *For an abelian variety A over a (global) number field K, there is a bilinear pairing*

$$\langle -, - \rangle_{\mathrm{NT}} : A(K^{\mathrm{a}}) \times A^\vee(K^{\mathrm{a}}) \to \mathbb{R}$$

with the following properties.

(a) The induced pairing on the quotients by the torsion subgroups is nondegenerate.

(b) The pairing is natural, i.e., if $\phi : A \to B$ is a K-isogeny, then $\langle \phi(K^{\mathrm{a}})(-), - \rangle_{\mathrm{NT}} = \langle -, \phi^\vee(K^{\mathrm{a}})(-) \rangle_{\mathrm{NT}}$.

[76] Perhaps more generally, the pairing is nondegenerate on the non-divisible quotients of $Ш(A)$ and $Ш(A^\vee)$.

Proof. See [21, Thm. B.5.8] or [25, Ch. 5]. The idea is that, in the notation explained above, we have $\langle -,- \rangle_{\mathrm{NT}} = \hat{h}_{\mathscr{P}}$, where $\mathscr{P}$ is the Poincaré bundle on $A \times A^\vee$. □

The height pairing allows us to define an important invariant of an abelian variety over a number field.

Definition 3.3.6 (Regulator)**.** *Let A be an abelian variety over a (global) number field K. We define the* regulator *of K to be*

$$\mathrm{Reg}(A) := |\det[\langle a_i, a'_j \rangle]_{i,j=1}^r|,$$

where $r := \mathrm{rk}(A) = \mathrm{rk}(A^\vee)$ is the common rank of A and $A^\vee$ (Lemmas 3.1.14 and 3.2.14), and $a_1, \ldots, a_r \in A(K)$ (resp. $a'_1, \ldots, a'_r \in A^\vee(K)$) is any choice of elements whose images form a $\mathbb{Z}$-basis for the free quotient $A(K)_{\mathrm{free}} := A(K)/A(K)_{\mathrm{tors}}$ (resp. $A^\vee(K)_{\mathrm{free}}$).

By the bilinearity of the canonical height pairing, the regulator is well-defined independent of the choices of the a_i and a'_j, and it is nonzero by Theorem/Definition 3.3.5(a). It is an interesting measure of the arithmetic complexity of A, and a key term appearing in the strong BSD conjecture, which we discuss now.

3.4 Main Proof

The more precise form of the Birch and Swinnerton-Dyer conjecture also predicts the first coefficient of $L_S(A, s)$ in its Taylor expansion around $s = 1$ (analogously to the analytic class number formula for the Dedekind zeta function ζ_K). Evidently, this depends on S, and so we need some normalization to eliminate this dependence. This is done as follows.

For a number field K and $v \in \mathrm{M}_K$, normalize the Haar measure on the locally compact topological abelian group $\mathbb{G}_a(K_v)$ to satisfy $\mu_v(\mathscr{O}_v) = 1$ when v is nonarchimedean and to be the usual Lebesgue measure otherwise; with this normalization, for any compact $S \subset K_v$ and $\lambda \in K_v^\times$, we have $\mu_v(\lambda S) = |\lambda|_v \mu_v(S)$. These normalizations give rise to the product measure μ, called the Tamagawa measure ([8, §X.3.1]), on the additive group $\mathbb{G}_a(\mathbb{A}_K)$ of the adèle ring $\mathbb{A}_K$, with the property that the compact quotient $\mathbb{G}_a(\mathbb{A}_K)/\mathbb{G}_a(K)$ has Tamagawa measure $|\mu| = 2^{-r_2}|\mathrm{disc}(K)|^{1/2}$, where r_2 is the number of complex places of K and $\mathrm{disc}(K)$ is the discriminant of the number field K ([26, Prop. XIV.6.6]). Next, suppose that A is an abelian variety of dimension $g \in \mathbb{Z}_{\geq 1}$ over a number field K, and suppose $\omega \in \Gamma(A, \Omega^g_{A/K})$ is a nonzero invariant top differential (take the g^{th} exterior power in [12, Prop. 3.15]). For each place v of K, the set of K_v-points $A(K_v) = A_v(K_v)$ of A is a smooth compact analytic group over K_v ([22, Ch. 2], [45, Part II, Ch. III-IV]), and the choice of ω (considered as an element of $\Gamma(A_v, \Omega^g_{A_v/K_v})$) along with μ_v determines a Haar measure $|\omega|_v \mu_v^g$ on $A(K_v)$ ([22, §7.4]). The volume of $A(K_v)$ with respect to this measure is called the *v-adic period of A*, and is denoted $\mu_v(A, \omega) := \int_{A(K_v)} |\omega|_v \mu_v^g$.

Remark 3.4.1. If $v \in \mathrm{M}_K^0$ is a place of good reduction for A and ω is chosen to reduce to a nonzero differential on $\tilde{A}_v$,[77] the exact sequence $0 \to A_1(K_v) \to A(K_v) \to \tilde{A}_v(\mathrm{k}_v) \to 0$ along with the isomorphism $A_1(K_v) \cong \mathfrak{m}_v^g$ from the formal group law (c.f. the proof of Theorem 3.2.6) can be used to show that $\mu_v(A, \omega) = q_v^{-g} |\tilde{A}_v(\mathrm{k}_v)|$ (see [23, §2.6.2]).

We can now define a modified L-function.

[77] Here's what this means explicitly. Let $\mathscr{A}$ be a model of A over $\mathrm{Spec}\, \mathscr{O}_{K,\mathfrak{p}_v}$ as in Definition 3.2.1. Then pullback by the basechange morphism $A \to\!\!\to \mathscr{A}$ (resp. $\tilde{A}_v \to \mathscr{A}$) gives us a K-linear map $K \otimes_{\mathscr{O}_{K,\mathfrak{p}_v}} \Gamma(\mathscr{A}, \Omega^g) \to \Gamma(A, \Omega^g_{A/K})$ (resp. k_v-linear map $\mathrm{k}_v \otimes_{\mathscr{O}_{K,\mathfrak{p}_v}} \Gamma(\mathscr{A}, \Omega^g) \to \Gamma(\tilde{A}_v, \Omega^g_{\tilde{A}_v/\mathrm{k}_v})$), where $\Gamma(\mathscr{A}, \Omega^g) := \Gamma(\mathscr{A}, \Omega^g_{\mathscr{A}/\mathscr{O}_{K,\mathfrak{p}_v}})$ The hypothesis is saying that there is an element $\bar{\omega} \in \Gamma(\mathscr{A}, \Omega^g)$ that maps to ω under the first map and whose image under the second map is nonzero. As in Lemma 3.2.2, this is the case for almost all v. One could also work globally with the Néron model (Remark 3.2.3) to make this definition; c.f. [23, §2.6.2], where our definition is equivalent to his $v_\omega = 1$.

Definition 3.4.2. *Let A be an abelian variety over a number field K, and $S \subset \mathrm{M}_K$ a finite set as in Definition 3.2.5. In the above notation, define the associated* modified L-function *to be*

$$L_S^*(A,s) := L_S(A,s) \cdot |\mu|^g \cdot \prod_{v \in S} \mu_v(A,\omega)^{-1},$$

where $\omega \in \Gamma(A, \Omega^g_{A/K})$ is any a nonzero invariant differential reducing to a nonzero differential (see Footnote 77) on $\tilde{A}(v)$ for all $v \notin S$.

Remark 3.4.3. The function $L_S^*(A,s)$ is independent of the choice of ω: if ω' is another form with the same properties, then–since the space of invariant g-forms is 1-dimensional–there is a $\lambda \in K^\times$ such that $\omega' = \lambda\omega$. The hypotheses on ω and ω' ensure that $|\lambda|_v = 1$ for all $v \notin S$, so that the product formula gives $\prod_{v\in S} |\lambda|_v = 1$, and hence $\prod_{v\in S} \mu_v(A,\omega') = \prod_{v\in S} |\lambda|_v \prod_{v\in S} \mu_v(A,\omega) = \prod_{v\in S} \mu_v(A,\omega)$. Moreover–and this is the point of this definition–assuming Conjecture 3.2.15 for an abelian variety A, the Taylor coefficient $\lim_{s\to 1}(s-1)^{-\mathrm{rk}(A)} L_S^*(A,s)$ is independent of the choice of S; this follows from Remarks 3.2.4 and 3.4.1.

We are now ready to state

Conjecture 3.4.4. *(Strong Birch and Swinnerton-Dyer) Let A be an abelian variety over a number field K, and $S \subset \mathrm{M}_K$ a finite set of places containing M_K^∞ and all places of bad reduction for A. Then $Ш(A)$ is finite, $L_S^*(A,s)$ admits an analytic continuation to a neighborhood of $s = 1$, and*

$$\lim_{s\to 1} \frac{L_S^*(A,s)}{(s-1)^{\mathrm{rk}(A)}} = \frac{|Ш(A)| \cdot \mathrm{Reg}(A)}{|A(K)_{\mathrm{tors}}| \cdot |A^\vee(K)_{\mathrm{tors}}|}.$$

Remark 3.4.5.

(a) For the agreement with the usual way the BSD conjecture is stated for elliptic curves–e.g., as in [49, Conjecture C.16.5])–see Remark 3.1.13(f) and [27, §III.6].

(b) The (inverse) correction factor $|\mu|^{-g} \prod_{v\in S} \mu_v(A,\omega)$ is the volume of $A(\mathbb{A}_{K,S})$ for a suitable Tamagawa measure on it ([23, Prop. 3.16]; c.f. [8, §X.3]). There is also a way to define a complete L-function $L(A,s)$ with local factors also at infinite places and places of bad reduction of A (see [27, §III.5]), and to state the conjecture in terms of this $L(A,s)$, the correct (inverse) correction factor needed then is the volume of $A(\mathbb{A}_K)$ with respect to the Tamagawa measure ([23, Prop. 2.64 and Conj. 3.15]).

(c) By the bilinearity of the height pairing, Conjecture 3.4.4 for an abelian variety A over K is equivalent to the assertion that

$$\lim_{s\to 1} \frac{L_S^*(A,s)}{(s-1)^r} = \frac{|Ш(A)| \cdot |\det[\langle a_i, a_j'\rangle_{\mathrm{NT}}]_{i,j=1}^r|}{[A(K) : \sum_{i=1}^r \mathbb{Z}a_i] \cdot [A^\vee(K) : \sum_{j=1}^r \mathbb{Z}a_j']},$$

where $r := \mathrm{rk}(A) = \mathrm{rk}(A^\vee) \in \mathbb{Z}_{\geq 0}$, and $a_1, \ldots, a_r \in A(K)$ (resp. $a_1', \ldots, a_r' \in A^\vee(K)$) is *any* family of elements which gives a $\mathbb{Q}$-basis for $A(K)_\mathbb{Q}$ (resp. $A^\vee(K)_\mathbb{Q}$).

The goal for the rest of this essay is to prove

Theorem 3.4.6 (Cassels-Tate)**.** *Let $A \sim_K B$ be isogenous abelian varieties over a number field K. If the strong BSD conjecture (Conjecture 3.4.4) is true for one of A or B, it is true for both.*

It is rather remarkable that none of the terms which appear individually in the Taylor coefficient in Conjecture 3.4.4–the size of the Tate-Shafarevich group, the regulator, or the sizes of the torsion subgroups–are in general the same for isogenous abelian varieties. Accordingly, Theorem 3.4.6 serves as very powerful theoretical evidence for Conjecture 3.4.4. We closely follow the proof of [32, Thm. I.7.3].

Proof. We proceed with a series of reductions. To prove the theorem, by Theorem/Definition 3.1.7, we may assume Conjecture 3.4.4 to be true for B and show it for A, given a K-isogeny $\phi : A \to B$. Let $\phi^\vee : B^\vee \to A^\vee$ by the dual isogeny (Remark 3.1.13(d)). By Corollary 3.2.12, the finiteness of $Ш(B)$ implies also that of $Ш(B^\vee)$, $Ш(A)$, and $Ш(A^\vee)$.

Now suppose that $\omega_B \in \Gamma(B, \Omega^g_{B/K})$ is a nonzero invariant differential and let $\omega_A := \phi^*\omega_B$. Let $S \subset \mathrm{M}_K$ be a finite set containing M_K^∞ and all places of bad reduction for A and B (c.f. Footnote 66), all places whose residue characteristic divides $\deg(\phi)$, and all places where ω_A and ω_B do not reduce to a nonzero differential form upon reduction (Footnote 77). Let $r \in \mathbb{Z}_{\geq 0}$ denote the common rank of A, B, $A^\vee$, and $B^\vee$, and let $a_1, \dots, a_r \in A(K)$ (resp. $b'_1, \dots, b'_r \in B^\vee(K)$) be any family of elements giving a $\mathbb{Q}$-basis of the $A(K)_\mathbb{Q}$ (resp. $B^\vee(K)_\mathbb{Q}$); then if we let $b_i := \phi(a_i)$ (resp. $a'_i := \phi^\vee(b'_i)$), then $b_1, \dots, b_r \in B(K)$ (resp. $a'_1, \dots, a_r \in A(K^\vee)$) also gives a $\mathbb{Q}$-basis of $B(K)_\mathbb{Q}$ (resp. $A^\vee(K)_\mathbb{Q}$), by Lemma 3.2.14. By Theorem 3.2.16 and Remarks 3.4.3 and 3.4.5(c), it remains to show that

$$\prod_{v \in S} \frac{\mu_v(B, \omega_B)}{\mu_v(A, \omega_A)} = \frac{|Ш(A)|}{|Ш(B)|} \cdot \frac{|\det[\langle a_i, a'_j\rangle_{\mathrm{NT}}]_{i,j=1}^r|}{|\det[\langle b_i, b'_j\rangle_{\mathrm{NT}}]_{i,j=1}^r|} \cdot \frac{[B(K) : \sum_{i=1}^r \mathbb{Z}b_i] \cdot [B^\vee(K) : \sum_{j=1}^r \mathbb{Z}b'_j]}{[A(K) : \sum_{i=1}^r \mathbb{Z}a_i] \cdot [A^\vee(K) : \sum_{j=1}^r \mathbb{Z}a'_j]}. \tag{3.5}$$

By Theorem/Definition 3.3.5(b), we have for each $i, j = 1, \dots, r$ that

$$\langle a_i, a'_j\rangle_{\mathrm{NT}} = \langle a_i, \phi^\vee(b'_j)\rangle_{\mathrm{NT}} = \langle \phi(a_i), b'_j\rangle_{\mathrm{NT}} = \langle b_i, b'_j\rangle_{\mathrm{NT}}, \tag{3.6}$$

eliminating the middle term on the right of (3.5). By the Snake Lemma applied to the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \sum_{i=1}^r \mathbb{Z}a_i & \longrightarrow & A(K) & \longrightarrow & A(K)/\sum_{i=1}^r \mathbb{Z}a_i & \longrightarrow & 0 \\ & & \downarrow \cong & & \downarrow \phi(K) & & \downarrow & & \\ 0 & \longrightarrow & \sum_{i=1}^r \mathbb{Z}b_i & \longrightarrow & B(K) & \longrightarrow & B(K)/\sum_{i=1}^r \mathbb{Z}b_i & \longrightarrow & 0, \end{array}$$

we get that

$$\frac{[B(K) : \sum_{i=1}^r \mathbb{Z}b_i]}{[A(K) : \sum_{i=1}^r \mathbb{Z}a_i]} = \frac{|\operatorname{coker}\phi(K)|}{|\ker\phi(K)|} =: \operatorname{ind}\phi(K), \tag{3.7}$$

and similarly for the duals.[78] Similarly, the ratio of periods can be interpreted as an index: for $v \in \mathrm{M}_K$,

$$\mu_v(B, \omega_B) \cdot \mu_v(A, \omega_A)^{-1} = \operatorname{ind}\phi(K_v). \tag{3.8}$$

Indeed, $\omega_A = \phi^*\omega_B$ tells us that the counting measure, $|\omega_A|_v\mu_v^g$, $|\omega_B|_v\mu_v^g$, and the counting measure again respectively are compatible Haar measures in the exact sequence of compact abelian groups

$$0 \to \ker\phi(K_v) \to A(K_v) \to B(K_v) \to \operatorname{coker}\phi(K_v) \to 0,$$

and so we are done by Fubini's Theorem.[79] Combining (3.5), (3.6), (3.7), (3.8), the finiteness of $Ш(A)$ and $Ш(B)$, and Lemma 0.0.1(1), we are reduced to showing that

$$\operatorname{ind} Ш(\phi) \cdot \prod_{v \in S} \operatorname{ind}\phi(K_v) = \frac{\operatorname{ind}\phi(K)}{\operatorname{ind}\phi^\vee(K)}, \tag{3.9}$$

[78] Note that $\operatorname{coker}\phi(K)$ is finite thanks to Theorem 3.2.10 and the sequence (3.3). Alternatively, (3.7) *proves* this.

[79] Here we are using that the $\ker\phi(K_v)$ and $\operatorname{coker}\phi(K_v)$ are finite (the latter uses an argument similar to, but even easier than, the one in Footnote 78). The particular version of Fubini's Theorem used is a straightforward generalization of the "quotient integral formula" for compatible Haar measures (e.g., [10, Thm. 1.5.3]) to longer exact sequences of locally compact abelian groups.

where $Ш(\phi) = \phi_* : Ш(A) \to Ш(B)$ is the induced map of Tate-Shafarevich groups.[80] Finally, the nondegeneracy and naturality of the Cassels-Tate pairing (Theorem/Definition 3.3.3) tells us that $\ker Ш(\phi^\vee) = (\operatorname{im} Ш(\phi))^\perp$, the orthogonal complement being with respect to $\langle -, - \rangle_{\mathrm{CT}}$, so again by nondegeneracy, $|\ker Ш(\phi^\vee)| = |\operatorname{coker} Ш(\phi)|$, and hence

$$\operatorname{ind} Ш(\phi) = |\ker Ш(\phi^\vee)| \cdot |\ker Ш(\phi)|^{-1}. \tag{3.10}$$

Let $\Phi := A[\phi](K_S) = A[\phi](K^{\mathrm{a}}) = A_v[\phi_v](K_v^{\mathrm{a}})$ (the equalities coming from Theorem 3.2.6), considered variously as a G_S, G_K or G_v-module for $v \in \mathrm{M}_K$, and Φ^{D} be its Cartier dual (in the sense of §2.4), so that by Remark 3.1.13(d) and Footnote 73, we have $\Phi^{\mathrm{D}} = B^\vee[\phi^\vee](K_S)$, etc. We need two lemmas.

Lemma 3.4.7. *There is a commutative diagram of finite abelian groups*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{H}^0(G_S, \Phi) & \longrightarrow & \bigoplus_{v\in S} \hat{\mathrm{H}}^0(K_v, \Phi) & \longrightarrow & \mathrm{H}^2(G_S, \Phi^{\mathrm{D}})^* & & \\
 & & & & & \swarrow & & & \\
0 & \longrightarrow & \operatorname{coker} \phi(K) & \longrightarrow & \mathrm{H}^1(G_S, \Phi) & \longrightarrow & \mathrm{H}^1(G_S, A)[\phi_*] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha'} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha''} & & \\
0 & \longrightarrow & \bigoplus_{v\in S} \operatorname{coker} \phi(K_v) & \longrightarrow & \bigoplus_{v\in S} \mathrm{H}^1(K_v, \Phi) & \longrightarrow & \bigoplus_{v\in S} \mathrm{WC}(A_v)[\phi_{v,*}] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \beta'} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \beta''} & & \\
0 & \longrightarrow & \mathrm{H}^1(G_S, B^\vee)[\phi_*^\vee]^* & \longrightarrow & \mathrm{H}^1(G_S, \Phi^{\mathrm{D}})^* & \longrightarrow & \operatorname{coker} \phi^\vee(K)^* & \longrightarrow & 0
\end{array}$$

such that the rows and columns are complexes, and the rows and (extended) middle column are exact.[81]

Proof Sketch. The (extended) middle column comes from Theorem 2.4.3. The first row that is not a part of it arises from taking the long exact sequence in G_S-cohomology of the exact sequence of discrete $\mathbb{Z}[G_S]$-modules $0 \to \Phi \to A(K_S) \xrightarrow{\phi(K_S)} B(K_S) \to 0$ coming from Theorem 3.2.6, the second row is obtained similarly, and the third row is obtained by $\mathbb{Q}/\mathbb{Z}$-dualizing the corresponding row for $\phi^\vee$, where we are using Remark 3.1.13(d) and the finiteness result Corollary 2.4.4. The maps $\alpha, \alpha', \alpha''$ are the sums of corresponding restriction maps. For each $v \in S$, the $\mathbb{Q}/\mathbb{Z}$-duality between $B_v(K_v)$ and $\mathrm{WC}(B_v^\vee)$ (Theorem/Definition 3.3.1) induces by naturality (3.3.1(b)) a duality between $\operatorname{coker} \phi(K_v)$ and $\mathrm{WC}(B^\vee)[\phi_{v,*}^\vee]$, and the map β' is the $\mathbb{Q}/\mathbb{Z}$-dual to the composite

$$\mathrm{H}^1(G_S, B^\vee)[\phi_*^\vee] \xrightarrow{\sum \mathrm{Res}_v} \bigoplus_{v\in S} \mathrm{WC}(B^\vee)[\phi_{v,*}^\vee] \xrightarrow{\sim} \bigoplus_{v\in S} \operatorname{coker} \phi(K_v)^*.$$

Similarly, β'' is the $\mathbb{Q}/\mathbb{Z}$-dual to the composite

$$\operatorname{coker} \phi^\vee(K) \xrightarrow{\sum \mathrm{Res}_v} \bigoplus_{v\in S} \operatorname{coker} \phi^\vee(K_v) \xrightarrow{\sim} \bigoplus_{v\in S} \mathrm{WC}(A_v)[\phi_{v,*}]^*.$$

The commutativity of the diagram follows from the definition of the maps α and β in Theorem 2.4.3 and the duality maps of Theorem/Definition 3.3.1, and this proves also that the outer columns are complexes. □

[80] The formulation (3.9) of Theorem 3.4.6 has the pleasant reinterpretation that the ratio of the indices of the global maps $\phi(K)$ and $\phi^\vee(K)$ is given by the product of the local contributions $\operatorname{ind} \phi(K_v)$ and the contribution $\operatorname{ind} Ш(\phi)$ coming from the failure of the local-to-global principle.

[81] Here we are using the shorthand notation $\mathrm{H}^1(G_S, A) := \mathrm{H}^1(G_S, A(K_S))$ and similarly for B and the duals.

Lemma 3.4.8. *There is an exact sequence*

$$0 \to \ker Ш(\phi) \to \mathrm{H}^1(G_S, A)[\phi_*] \to \bigoplus_{v \in S} \mathrm{WC}(A_v)[\phi_{v,*}]$$

and similarly for the duals.

Proof Sketch. A sequence $X \xrightarrow{f} Y \xrightarrow{g} Z$ of morphisms of abelian groups yields an exact sequence $0 \to \ker f \to \ker gf \xrightarrow{f} \ker g$. Applying this to

$$\mathrm{WC}(A)[\phi_*] \xrightarrow{\sum \mathrm{Res}_v} \bigoplus_{v \in \mathrm{M}_K} \mathrm{WC}(A_v)[\phi_{v,*}] \xrightarrow{\mathrm{pr}} \bigoplus_{v \notin S} \mathrm{WC}(A_v)[\phi_{v,*}]$$

tells us that we need to identify the kernel of the map $\mathrm{WC}(A) \to \bigoplus_{v \notin S} \mathrm{WC}(A_v)$ with $\mathrm{H}^1(G_S, A)$. The profinite inflation-restriction sequence (Theorem 1.2.6 and Remark 2.1.5) tells us that the inflation map $\mathrm{H}^1(G_S, A) \to \mathrm{H}^1(K, A)$ is injective, giving us a subgroup. It remains to identify this subgroup with the kernel, and this is done exactly as in [32, Prop. I.6.5].[82] □

Given these lemmas, we are ready to finish the proof of Theorem 3.4.6. From Lemma 3.4.7 and the Snake Lemma, there is an exact sequence

$$0 \to \ker \alpha' \to \ker \alpha \to \ker \alpha'' \to \ker \beta' / \operatorname{im} \alpha' \to 0. \tag{3.11}$$

By Lemma 0.0.1(2) applied to (3.11), the first column, and the lowest row of Lemma 3.4.7, we get

$$\operatorname{ind} Ш(\phi) \cdot \prod_{v \in S} |\operatorname{coker} \phi(K_v)| \cdot \frac{|\operatorname{coker} \phi^\vee(K)|}{|\operatorname{coker} \phi(K)|} = \frac{|\mathrm{H}^1(G_S, \Phi^{\mathrm{D}})|}{|\ker \alpha|}, \tag{3.12}$$

where we have also used (3.10) and from (the proofs of) Lemmas 3.4.7 and 3.4.8 that $\ker \alpha'' = \ker Ш(\phi)$ and $\operatorname{coker} \beta' = \ker Ш(\phi^\vee)^*$. Next, Lemma 0.0.1(2) applied to the extended middle column of Lemma 3.4.7 yields (along with the fact that $\mathrm{H}^0(G_S, \Phi) = \ker \phi(K)$ and $\mathrm{H}^0(G_S, \Phi^{\mathrm{D}}) = \ker \phi^\vee(K)$, and similarly for the local factors) that

$$\prod_{v \in S} \frac{1}{|\ker \phi(K_v)|} \cdot \frac{|\ker \phi(K)|}{|\ker \phi^\vee(K)|} = \frac{|\ker \alpha|}{|\mathrm{H}^0(G_S, \Phi^{\mathrm{D}})| \cdot |\mathrm{H}^2(G_S, \Phi^{\mathrm{D}})|} \cdot \prod_{v \in \mathrm{M}_K^\infty} \frac{|\hat{\mathrm{H}}^0(K_v, \Phi)|}{|\mathrm{H}^0(K_v, \Phi)|}. \tag{3.13}$$

Finally, multiplying (3.12) and (3.13) shows that the required equality (3.9) is equivalent to Theorem 2.4.5. □

[82] Including full details in this proof would need us to develop the theory of abelian varieties over local number fields more fully than we have space for. The key technical input needed here is that $\mathrm{H}^1(\mathrm{k}_v, A(K_v^{\mathrm{nr}})) = 0$, which uses the fact that A has good reduction at v, that Weil-Châtelet groups over finite fields are trivial ([27, Thm. III.4.3]), and an argument with Hensel's lemma similar to the one in Footnote 45; alternatively, one could use Néron models, as is done in [32, Prop. I.3.8].

Conclusion

In this essay, we began by defining abstract (§1) and profinite group cohomology (§2.1), and Galois cohomology (§2.2). Next, we discussed how the Tate-Nakayama theorem combined with Galois cohomology gives class field theory (§2.3). Finally, we discussed how the artithmetic duality theorems of Tate and Poitou (§2.4) combined with a few other duality theorems for abelian varieties over local and global number fields (§3.3) can be used to prove the Cassels-Tate theorem on the isogeny invariance of the strong Birch and Swinnerton-Dyer conjecture (§3.4). Needless to say, there is much more to be said about each of these topics. We end this essay by giving a brief (and necessarily incomplete) overview of some further directions in which the material of this essay can be taken.

In group cohomology, one important topic we did not have space to discuss was the Lyndon-Hochschild-Serre spectral sequence, which is a powerful computational tool ([28, Ch. VI], [56, §6.8]). Further, by Example 1.1.4 and Remark 1.1.6(c), there is at least as much to be said about group cohomology as there is about the topological cohomology of Eilenberg-MacLane spaces (of which there is a lot). For instance, if G is a free group, then $\mathrm{K}(G,1)$ is a bouquet of circles, and so $\mathrm{cd}_{\mathbb{Z}}(G) \leq 1$; the converse–that any (finitely generated or torsion free) group of cohomological dimension at most 1 is free–is a deep theorem due to Stallings [50] and Swan [51], which resolved important conjectures in group theory. For an application of group cohomology (or more precisely its close analog, *bounded* group cohomology) to amenability and geometric group theory, see [29, Ch. 2]. For several other topics in group cohomology such as finiteness conditions and Euler characteristics of groups, see [6].

Another interesting result that can be proved using Galois cohomology is the Golod-Shafarevich theorem on the existence of infinite class field towers of number fields ([8, Ch. IX]). For the much more that remains to be said about the Galois cohomology of local and global number fields and global class field theory, see [2] and [37]. Besides its applications to class field theory (and those mentioned in §2.2), Galois cohomology is an essential tool for studying rationality questions via Galois descent ([40, Ch. 4,5]). When applied to algebraic groups such as orthogonal groups, this has applications to the classification of quadratic forms over number fields ([3, Ch. IV], [8, Ch. X], [44, Ch. III]). Further, as noted above (Footnote 4), Galois cohomology is also one special case of, and a starting point for, the theory of étale cohomology, the importance of which for modern arithmetic geometry cannot be overstated ([30], [40, Ch. 6-9]). For several other applications of Galois cohomology, see [3], [13], or [44]. We also want to mention that class field theory (Theorem 2.3.3), local Tate duality (Theorem/Definition 2.4.1), and the duality from the Cassels-Tate pairing (Theorem/Definition 3.3.3) can be simultaneously generalized by duality theorems and a Poitou-Tate type exact sequence (Theorem 2.4.3) in motivic cohomology ([18]).

Finally, in addition to providing important theoretical evidence for the Birch and Swinnerton-Dyer conjecture, the Cassels-Tate theorem has other applications and supports other conjectures in number theory. One direct application is to the partial resolution of the parity conjecture by the brothers Dokchitser. If A is an abelian variety over a number field K and $L(A,s)$ its complete L-function (Remark 3.4.5(b)), then it is conjectured that L admits a functional equation in which s and $2-s$ play symmetric roles (analogous to the one satisfied by ζ-functions). A consequence of this result asserts that, in this case, $(-1)^{\mathrm{rk}(A)} = w(A)$, where $w(A)$ is a *root number* of A, which is again computed from local data–this is the *parity conjecture*. It is a weaker form of Conjecture 3.2.15, which is still "responsible for a wide range of [otherwise] unexplained arithmetic phenomena" ([24]). Roughly a decade ago, the brothers Tim and Vlad Dokchitser resolved the parity conjecture for elliptic curves (assuming the finiteness of the Tate-Shafarevich group), and one key ingredient in their proof is the Cassels-Tate theorem for all abelian varieties ([11, Lemma 1.2]). Besides explaining all the "parity phenomena," this result brings us one step closer to the still-elusive full Birch and Swinnerton-Dyer conjectures.

References

[1] Aluffi, P. *Algebra: Chapter 0*, vol. 104 of *Graduate Studies in Mathematics*. American Mathematical Society, 2009.

[2] Artin, E., and Tate, J. *Class Field Theory*. AMS Chelsea Publishing, 1990.

[3] Berhuy, G. *An Introduction to Galois Cohomology and Applications*, vol. 377 of *London Mathematical Society Lecture notes series*. Cambridge University Press, 2010.

[4] Bosch, S., Lütkebohmert, W., and Raynaud, M. *Néron Models*. No. 21 in Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge. Springer-Verlag Berlin Heidelberg GmbH, 1990.

[5] Bredon, G. E. *Sheaf Theory*, second ed. No. 170 in Graduate Texts in Mathematics. Springer, 1997.

[6] Brown, K. S. *Cohomology of Groups*. No. 87 in Graduate Texts in Mathematics. Springer, 1982.

[7] Cassels, J. W. S. *Local Fields*, vol. 3 of *London Mathematical Society Student Texts*. Cambridge University Press, 1986.

[8] Cassels, J. W. S., and Fröhlich, A., Eds. *Algebraic Number Theory*. Academic Press, 1967.

[9] Conrad, B. Profinite Group Cohomology. Available at `https://math.stanford.edu/~conrad/210BPage/handouts/profcohom.pdf`.

[10] Deitmar, A., and Echterhoff, S. *Principles of Harmonic Analysis*, second ed. Universitext. Springer, 2014.

[11] Dokchitser, T. Notes on the parity conjecture. In *Elliptic Curves, Hilbert Modular Forms and Galois Deformations*. Springer Basel, 2013, p. 201–249. Available at `http://dx.doi.org/10.1007/978-3-0348-0618-3_5`.

[12] Edixhoven, B., van der Geer, G., and Moonen, B. Abelian Varieties. Available at `http://van-der-geer.nl/~gerard/AV.pdf`.

[13] Gille, P., and Szamuely, T. *Central Simple Algebras and Galois Cohomology*, vol. 101 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 2006.

[14] Görtz, U., and Wedhorn, T. *Algebraic Geometry I: Schemes*, second ed. Springer Studium Mathematik - Master. Springer, 2020.

[15] Guillot, P. *A Gentle Course in Local Class Field Theory*. Cambridge University Press, 2018.

[16] Haberland, K. *Galois Cohomology of Algebraic Number Fields*. VEB Deutscher Verlag der Wissenschaften, 1978.

[17] Harari, D. *Galois Cohomology and Class Field Theory*. Universitext. Springer, 2020.

[18] Harari, D., and Szamuely, T. Arithmetic duality theorems for 1-motives, 2004. Available online at `https://arxiv.org/abs/math/0304480`.

[19] Hartshorne, R. *Algebraic Geometry*. No. 52 in Graduate Texts in Mathematics. Springer, 1977.

[20] Hatcher, A. *Algebraic Topology*. Cambridge University Press, 2002. Available online at `https://pi.math.cornell.edu/~hatcher/AT/AT+.pdf`.

[21] Hindry, M., and Silverman, J. H. *Diophantine Geometry: An Introduction*. No. 201 in Graduate Texts in Mathematics. Springer, 2000.

[22] Igusa, J. *An Introduction to the Theory of Local Zeta Functions*, vol. 14 of *Studies in Advanced Mathematics*. American Mathematical Society/International Press, 2000.

[23] Jorza, A. The Birch and Swinnterton-Dyer Conjecture for Abelian Varieties over Number Fields, 2005. Available at `https://www3.nd.edu/~ajorza/notes/bsd.pdf`.

[24] Kellock, L. C., and Dokchitser, V. Root numbers and parity phenomena, 2023. Available at `https://arxiv.org/abs/2303.07883`.

[25] Lang, S. *Fundamentals of Diophantine Geometry*. Springer Science+Business Media New York, 1983.

[26] Lang, S. *Algebraic Number Theory*. No. 110 in Graduate Texts in Mathematics. Springer, 1986.

[27] Lang, S., Ed. *Number Theory III*, vol. 60 of *Encyclopedia of Mathematical Sciences*. Springer-Verlag, 1991.

[28] Lang, S. *Topics in Cohomology of Groups*. No. 1625 in Lecture Notes in Mathematics. Springer, 1996.

[29] Löh, C. Group Cohomology, 2019. Available at `https://loeh.app.uni-regensburg.de/teaching/grouphom_ss19/lecture_notes.pdf`.

[30] Milne, J. S. *Étale Cohomology*, vol. 33 of *Princeton Mathematical Series*. Princeton University Press, 1980.

[31] Milne, J. S. Abelian Varieties. In *Arithmetic Geometry*, G. Cornell and J. H. Silverman, Eds. Springer-Verlag, 1986, ch. V.

[32] Milne, J. S. *Arithmetic Duality Theorems*, second ed. BookSurge, LLC, 2006. Available online at `https://www.jmilne.org/math/Books/ADTnot.pdf`.

[33] Milne, J. S. Abelian Varieties (v2.00), 2008. Available at `www.jmilne.org/math/`.

[34] Milne, J. S. *Algebraic Groups: The Theory of Group Schemes of Finite Type over a Field*, vol. 170 of *Cambridge sudies in advanced mathematics*. Cambridge University Press, 2017.

[35] Mumford, D. *Abelian Varieties*. Tata Institute of Fundamental Research and Hindustan Book Agency, Reprint 2014.

[36] Neukirch, J. *Class Field Theory -The Bonn Lectures-*. Springer, 2013. Edited by Alexander Schmidt.

[37] Neukirch, J., Schmidt, A., and Wingberg, K. *Cohomology of Number Fields*, second ed., vol. 323 of *Die Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 2008.

[38] Oort, F. *Commutative Group Schemes*. No. 15 in Lecture Notes in Mathematics. Springer, 1966.

[39] Poitou, G. *Cohomologie galoisienne des modules finis: séminaire de l'Institut de mathématiques de Lille*. 1967.

[40] Poonen, B. *Rational Points on Varieties*, vol. 186 of *Graduate Studies in Mathematics*. American Mathematical Society, 2010.

[41] Poonen, B., and Stoll, M. The Cassels-Tate pairing on polarized abelian varieties. *The Annals of Mathematics 150*, 3 (Nov. 1999), 1109. Available online at `https://arxiv.org/abs/math/9911267`.

[42] Ribes, L., and Zalesskii, P. *Profinite Groups*. No. 40 in Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge. Springer-Verlag Berlin Heidelberg GmbH, 2000.

[43] Serre, J.-P. *Local Fields*. No. 67 in Graduate Texts in Mathematics. Springer, 1979.

[44] Serre, J.-P. *Galois Cohomology*. Springer Monographs in Mathematics. Springer, 2002.

[45] Serre, J.-P. *Lie Algebras and Lie Groups*, 2nd ed. No. 1500 in Lecture Notes in Mathematics. Springer, 2006.

[46] Serre, J.-P., and Tate, J. Good Reduction of Abelian Varieties. *Annals of Mathematics 88*, 3 (1968), 492–517.

[47] Silverman, J. H. The Theory of Height Functions. In *Arithmetic Geometry*, G. Cornell and J. H. Silverman, Eds. Springer-Verlag, 1986, ch. VI.

[48] Silverman, J. H. A Survey of Local and Global Pairings on Elliptic Curves and Abelian Varieties. In *Pairing-Based Cryptography - Pairing 2010* (2010), M. Joye, A. Miyaji, and A. Otsuka, Eds., Springer Berlin Heidelberg, pp. 377–396.

[49] Silverman, J. H. *The Arithmetic of Elliptic Curves*, second ed. No. 106 in Graduate Texts in Mathematics. Springer, 2016.

[50] Stallings, J. R. On torsion-free groups with infinitely many ends. *Annals of Mathematics 88*, 2 (1968), 312–334.

[51] Swan, R. G. Groups of cohomological dimension one. *Journal of Algebra 12* (1969), 585–610.

[52] Tate, J. WC-groups over p-adic fields. In *Séminaire Bourbaki : années 1956/57 - 1957/58, exposés 137-168*, no. 4 in Séminaire Bourbaki. Société mathématique de France, 1958, pp. 265–277. talk:156.

[53] Tate, J. Duality theorems in Galois cohomology over number fields. *Proc. Int. Congr. Stockholm* (1962).

[54] The Stacks Project Authors. *Stacks Project*. `https://stacks.math.columbia.edu`, 2018.

[55] Vakil, R. *The Rising Sea: Foundations of Algebraic Geometry*. Princeton University Press, 2025. Available online at `https://math.stanford.edu/~vakil/216blog/`.

[56] Weibel, C. A. *An Introduction to Homological Algebra*, vol. 38 of *Cambridge studies in advanced mathematics*. Cambridge University Press, 1994.

[57] Weil, A. On Algebraic Groups and Homogeneous Spaces. *American Journal of Mathematics 77*, 3 (1955), 493–512.