ON THE TATE-SHAFAREVICH GROUP OF A NUMBER FIELD

SAMEER KAILASA

Abstract. For an elliptic curve E defined over a field K, the Tate-Shafarevich group $Ш(E/K)$ encodes important arithmetic and geometric information. An important conjecture of Tate and Shafarevich states $Ш(E/K)$ is always finite. Supporting this conjecture is a cohomological analogy between Mordell-Weil groups of elliptic curves and unit groups of number fields. In this note, we follow the analogy to construct, for each number field K, a "Tate-Shafarevich group" $Ш(K)$ and prove that $Ш(K)$ is canonically isomorphic to the ideal class group $\mathrm{Cl}(K)$ (which is finite by a classical result of Dedekind). Prerequisites are some knowledge of algebraic number theory and elliptic curve theory.

Contents

1. Basic Galois Cohomology

For this note, it will suffice to know about the first cohomology group, whose properties we rapidly summarize in this section. Higher cohomology in number theory is discussed in [1].

1.1. **First Cohomology.** Let G be a group and consider a (left) G-module M, i.e. an abelian group M on which G acts. Equip both G and M with the discrete topology.

The invariant submodule M^G of M is

$$M^G := \{x \in M \ : \ g \cdot x = x \ \text{ for all } g \in G\}.$$

Forgetting the G-module structure on M^G, this furnishes a functor $H^0(G, -) : \mathbf{G\text{-}Mod} \to \mathbf{Ab}$ given by $M \mapsto M^G$. The *first cohomology of* G is another functor $H^1(G, -) : \mathbf{G\text{-}Mod} \to \mathbf{Ab}$, described explicitly as follows.

A map $f : G \to M$ is called a *crossed homomorphism* (or 1-*cocycle*) if

$$f(\sigma\tau) = \sigma \cdot f(\tau) + f(\sigma)$$

for all $\sigma, \tau \in G$. Distinguished among the crossed homomorphisms are the *principal crossed homomorphisms* (or *1-coboundaries*), which are those of the form

$$f(\sigma) = \sigma \cdot x - x$$

for some $x \in M$. Let $Z^1(G, M)$ denote the abelian group (under addition) of crossed homomorphisms $G \to M$, and let $B^1(G, M)$ denote the subgroup of principal crossed homomorphisms; then the first cohomology is

$$H^1(G, M) := Z^1(G, M)/B^1(G, M).$$

Example 1.1. When G acts trivially on M, crossed homomorphisms are simply homomorphisms $G \to M$ and principal crossed homomorphisms are trivial, hence $H^1(G, M) = \mathrm{Hom}(G, M)$.

The first cohomology groups realize the first obstruction to exactness of the fixed-point functor H^0 insofar as they fit into the below exact sequence:

Proposition 1.2. *If*

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

is a short exact sequence of G-modules, there is an exact sequence

$$0 \to A^G \xrightarrow{f} B^G \xrightarrow{g} C^G \xrightarrow{\delta} H^1(G, A) \xrightarrow{H^1 f} H^1(G, B) \xrightarrow{H^1 g} H^1(G, C).$$

Description of connecting homomorphism δ: For $c \in C^G$, let $b \in B$ such that $g(b) = c$. Define $\psi : G \to B$ by $\psi(\sigma) = \sigma \cdot b - b$. Since $g(\psi(\sigma)) = \sigma \cdot c - c = 0$, in fact ψ is a map $G \to \mathrm{Ker}(g) = \mathrm{Im}(f)$, so $f^{-1} \circ \psi$ is a crossed homomorphism $G \to A$ and we set $\delta(c) := f^{-1} \circ \psi$. See [4][Proposition B.1.2] for more details. □

1.2. **Inflation/Restriction.** Let $H \leq G$ be a subgroup. The map $Z^1(G, M) \to Z^1(H, M) : f \mapsto f|_H$ descends to a homomorphism $\mathrm{Res} : H^1(G, M) \to H^1(H, G)$, called the *restriction* homomorphism.

Suppose, in addition, that H is a normal subgroup of G. In this case, M^H is naturally a G/H-module and there is a map $\mathrm{Inf} : Z^1(G/H, M^H) \to Z^1(G, M)$ given by $\mathrm{Inf}(f)(\sigma) = f(\sigma H)$. Once again, this descends to an *inflation* homomorphism (abusively denoted) $\mathrm{Inf} : H^1(G/H, M^H) \to H^1(G, M)$.

Proposition 1.3. *Let M be a left G-module and $H \trianglelefteq G$ a normal subgroup. Then the sequence*

$$0 \to H^1(G/H, M^H) \xrightarrow{\text{Inf}} H^1(G, M) \xrightarrow{\text{Res}} H^1(H, M)$$

is exact.

Proof. See [4][Proposition B.2.4]. □

1.3. **Infinite Galois Groups.** Let K be a perfect field. The absolute Galois group $\text{Gal}(\overline{K}/K)$ is the inverse limit

$$\text{Gal}(\overline{K}/K) = \varprojlim \text{Gal}(L/K)$$

over finite extensions L/K, via the inverse system defined by restriction maps $\text{Gal}(L'/K) \to \text{Gal}(L/K)$ for each finite tower $L'/L/K$. Equipping each finite $\text{Gal}(L/K)$ with the discrete topology induces a limit topology on $\text{Gal}(\overline{K}/K)$, known as the *Krull topology*, for which a basis of open sets about the identity consists of all finite index normal subgroups.

A $\text{Gal}(\overline{K}/K)$-module M is called *continuous* if the action of $\text{Gal}(\overline{K}/K)$ is continuous with respect to the Krull topology, i.e. the map $\text{Gal}(\overline{K}/K) \times M \to M$ is continuous. Equivalently, M is continuous if for every $x \in M$, the stabilizer subgroup $\{\sigma \in \text{Gal}(\overline{K}/K) : \sigma \cdot x = x\}$ has finite index.

Galois cohomology is defined for continuous $\text{Gal}(\overline{K}/K)$-modules M in terms of a direct system formed by inflation maps. If $L'/L/K$ is a finite tower of Galois extensions, then $M^{\text{Gal}(\overline{K}/L')}$ is a $\text{Gal}(L'/K)$-module, hence there is the injective inflation homomorphism

$$H^1(\text{Gal}(L/K), M^{\text{Gal}(\overline{K}/L)}) \hookrightarrow H^1(\text{Gal}(L'/K), M^{\text{Gal}(\overline{K}/L')})$$

(these cohomology groups being defined as in Section 1.1 since finite Galois groups are taken with the discrete topology). Accordingly, one defines

$$H^1(\text{Gal}(\overline{K}/K), M) := \varinjlim H^1(\text{Gal}(L/K), M^{\text{Gal}(\overline{K}/L)})$$

where the direct limit is over finite Galois extensions of K.

This does not coincide exactly with the original definition of cohomology for discrete groups: instead, the direct limit is seen to consist precisely of equivalence classes of *continuous* 1-cocycles, i.e. those that are continuous when viewed as maps $\text{Gal}(\overline{K}/K) \to M$. But otherwise, the homological properties of H^1 remain unchanged, e.g. the analogues of Propositions 1.2 and 1.3 remain true for Galois cohomology.

In what follows, we abbreviate $H^1(\text{Gal}(\overline{K}/K), M)$ as $H^1(K, M)$ and refer simply to "$\text{Gal}(\overline{K}/K)$-modules," omitting the adjective "continuous."

1.4. **Two Useful Facts.** We record two important facts about group cohomology that will be cited later in this note.

Fact 1: G acts trivially on $H^1(G, M)$. For any group G, there is a natural G-action on $H^1(G, M)$: for a 1-cocycle f, set

$$[\tau \cdot f](\sigma) = f(\sigma\tau) - f(\tau).$$

This effectively transfers the action of G on itself by inner automorphisms to H^1.

Proposition 1.4. *The natural G-action described above is trivial.*

Proof. Note that

$$[\tau \cdot f - f](\sigma) = f(\sigma\tau) - f(\tau) - f(\sigma) = \sigma \cdot f(\tau) - f(\tau),$$

which is a 1-coboundary. □

Fact 2: Hilbert's Theorem 90. This theorem computes the cohomology group $H^1(K, \overline{K}^\times)$ for any perfect field K.

Proposition 1.5. *Let L/K be a finite Galois extension of fields. Then*

$$H^1(\mathrm{Gal}(L/K), L^\times) = 0.$$

Proof. Let $f : \mathrm{Gal}(L/K) \to L^\times$ be a crossed homomorphism. By Artin's Theorem on linear independence of characters ([3][Sec. 14.2, Thm. 7]), there is some $x \in L^\times$ such that

$$y := \sum_{\sigma \in \mathrm{Gal}(L/K)} f(\sigma)\sigma(x) \neq 0.$$

For $\tau \in \mathrm{Gal}(L/K)$, it follows

$$\tau(y) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \tau(f(\sigma))\tau(\sigma(x)) = f(\tau)^{-1} \sum_{\sigma \in \mathrm{Gal}(L/K)} f(\tau\sigma)\tau(\sigma(x)) = f(\tau)^{-1} y,$$

hence $f(\tau) = y/\tau(y) = \tau(y^{-1})/y^{-1}$, i.e. f is principal. □

Corollary 1.6 (Hilbert's Theorem 90)**.** *If K is a perfect field, then $H^1(K, \overline{K}^\times) = 0$.*

2. Torsors and Ш for Elliptic Curves

For the rest of this note, assume K is a number field. If E is an elliptic curve defined over K, then $E(\overline{K})$ is a $\mathrm{Gal}(\overline{K}/K)$-module whose fixed points are precisely the K-rational points $E(K)$. In this situation, $H^1(K, E(\overline{K}))$ permits a geometric interpretation as the *principal homogenous spaces* (a.k.a. *torsors*) of E/K, smooth curves on which E acts freely and transitively by morphisms over K. Following this interpretation, we define a subgroup $Ш(E, K) \subset H^1(K, E(\overline{K}))$ called the *Tate-Shafarevich group*, whose elements represent curves that fail the Hasse local-global principle.

2.1. Torsors and the Weil-Châtelet Group.

Let E/K be an elliptic curve; in particular, E has a K-rational point. A smooth curve X/K is a *K-torsor under E* if

- $E(\overline{K})$ acts on $X(\overline{K})$ by morphisms over K (i.e. for each $P \in E(\overline{K})$, the map $X(\overline{K}) \to X(\overline{K}) : x \mapsto P \cdot x$ is a morphism over K),
- for any x, $y \in X(\overline{K})$, there is a unique $Q \in E(\overline{K})$ such that $Q \cdot x = y$ (i.e., $E(\overline{K})$ acts freely and transitively on $X(\overline{K})$).

We may think of K-torsors under E as "twists" of E which carry all information of the group structure on E but lack a distinguished identity element.

Two K-torsors under E are *equivalent* if they permit a curve isomorphism over K that is also an isomorphism of $E(\overline{K})$-modules. Certainly, E/K is itself a K-torsor under E via the group law; denoting this torsor as $\mathbb{E}$, we say a torsor is *trivial* if it is equivalent to $\mathbb{E}$.

Let $\mathrm{WC}(E/K)$ denote the set of equivalence classes of K-torsors under E; this is called the *Weil-Châtelet* group of E/K and its group structure arises from identification with a cohomology group, as will be described shortly.

Proposition 2.1. *Let X/K be a K-torsor under E. Then X is trivial iff X has a K-rational point.*

Proof. If $x_0 \in X$ is a K-rational point, then the isomorphism $\mathbb{E} \to X : P \mapsto P \cdot x_0$ is defined over K and respects the torsor action. Conversely, if X is trivial and $f : \mathbb{E} \to X$ is the corresponding isomorphism, then $f(P)$ is a K-rational point of X when P is a K-rational point of $\mathbb{E}$. □

Remark 2.2. For any smooth curve X/K, there is an elliptic curve $J(X)/K$ called the *Jacobian of* X under which X is a K-torsor. In particular, *every* curve is a torsor for *some* elliptic curve.

If X/K is a K-torsor under E/K, consider the "subtraction" map $X \times X \to E$ defined by

$$y - x := \{\text{unique } P \in E \text{ such that } y = P \cdot x\};$$

in fact, one can show this is a morphism over K.

Proposition 2.3. *Let X/K be a K-torsor under E. For any choice of $x_0 \in X$, the map*

$$\mathrm{Gal}(\overline{K}/K) \to E(\overline{K}) : \sigma \mapsto \sigma(x_0) - x_0$$

is a 1-cocycle, which we denote $f(X, x_0)$. The natural map

$$\mathrm{WC}(E/K) \to H^1(K, E(\overline{K})) : \{X/K\} \mapsto \{f(X, x_0)\}$$

is a bijection.

Proof. See [4][Theorem X.3.6]. □

2.2. **The Tate-Shafarevich Group ....** Based on the above geometric interpretation of $H^1(K, E(\overline{K}))$ as torsors under E, one can reformulate the Hasse local-global principle in cohomological terms. A smooth curve X/K *fails the local-global principle* if it has a rational point over each completion K_v (for v a place of K) but no K-rational point. Since the presence of rational points on X is equivalent to triviality as an element of H^1, we can recast this failure as follows.

Let M_K denote the set of places of K. For each $v \in M_K$, fix an embedding $\lambda_v : \overline{K} \hookrightarrow \overline{K_v}$ and consider the induced embedding

$$\lambda_v^\times : \mathrm{Gal}(\overline{K_v}/K_v) \hookrightarrow \mathrm{Gal}(\overline{K}/K).$$

This furnishes a restriction map

$$H^1(K, E(\overline{K})) \to H^1(K_v, E(\overline{K_v}))$$

which, in fact, does not depend on the choice of embedding λ. Indeed, any other embedding $\Lambda : \overline{K} \hookrightarrow \overline{K_v}$ is of the form $\Lambda = \lambda \circ \sigma$ for some $\sigma \in \mathrm{Gal}(\overline{K}/K)$, and since the natural $\mathrm{Gal}(\overline{K}/K)$-action on $H^1(K, E(\overline{K}))$ is trivial, it follows both embeddings induce the same map on cohomology.

Consequently, a smooth curve X/K fails the local-global principle iff it is in the kernel of the canonical restriction map

$$H^1(K, J(X)(\overline{K})) \to H^1(K_v, J(X)(\overline{K_v}))$$

for every $v \in M_K$ (where $J(X)$ is the Jacobian of X). Following this observation, we define the *Tate-Shafarevich group* of an elliptic curve E/K to be

$$Ш(E/K) := \bigcap_{v \in M_K} \mathrm{Ker}(H^1(K, E(\overline{K})) \to H^1(K_v, E(\overline{K_v}))).$$

Hence, $Ш(K)$ is precisely the group of K-torsors under E that fail the local-global principle.

Example 2.4. Consider the curve X defined over $\mathbb{Q}$ by the equation $3x^3 + 4y^3 + 5z^3 = 0$. Selmer proved this curve has points in $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p, but no points in $\mathbb{Q}$. Hence, X corresponds to a nontrivial element of $Ш(J(X)/\mathbb{Q})$.

In addition to possessing this appealing arithmetic-geometric description, $Ш(K)$ plays an important computational role. Consider the exact sequence

$$0 \to E(\overline{K})[n] \hookrightarrow E(\overline{K}) \xrightarrow{[n]} E(\overline{K}) \to 0,$$

where $[n]$ denotes multiplication by n and $E(\overline{K})[n]$ is the n-torsion in $E(\overline{K})$; note that $[n] : E(\overline{K}) \to E(\overline{K})$ is surjective since $\overline{K}$ is algebraically closed. Taking cohomology gives a long exact sequence

$$0 \to E(K)[n] \to E(K) \xrightarrow{[n]} E(K) \to H^1(K, E(\overline{K})[n])$$
$$\to H^1(K, E(\overline{K})) \xrightarrow{[n]} H^1(K, E(\overline{K})),$$

which may be consolidated into the short exact sequence

$$0 \to E(K)/[n]E(K) \to H^1(K, E(\overline{K})[n]) \xrightarrow{\gamma} H^1(K, E(\overline{K}))[n] \to 0.$$

Denoting by $\mathrm{Sel}^{(n)}(E/K)$ the preimage of $Ш(E/K)[n] \subset H^1(K, E(\overline{K}))[n]$ under γ gives another short exact sequence

$$0 \to E(K)/[n]E(K) \to \mathrm{Sel}^{(n)}(E/K) \xrightarrow{\gamma} Ш(E/K)[n] \to 0.$$

The *n-Selmer group* $\mathrm{Sel}^{(n)}(E/K)$ is, in fact, finite and computable. This is discussed in, for instance, Silverman's [4][Ch. X]. Consequently, knowledge of $Ш(E/K)$ can be leveraged into knowledge of generators for $E(K)/[n]E(K)$. In fact, Silverman describes an explicit algorithm to compute generators of $E(K)/[n]E(K)$ that terminates in finite time if the following conjecture is true.

Conjecture 2.5 (Tate-Shafarevich)**.** *If K is a number field and E/K an elliptic curve, then $Ш(E/K)$ is finite.*

The conjecture has been proved in some special cases, for instance when E has analytic rank at most 1 (the zero of its L-function at $s = 1$ has order at most 1). However, the general proof remains out of reach. A particularly compelling piece of evidence in favor of the conjecture comes from an analogy between elliptic curves and unit groups of number fields.

2.3. ... **of a Number Field.** Let $\mathcal{O}_{\overline{K}}$ denote the ring of algebraic integers in $\overline{K}$. There is of course a $\mathrm{Gal}(\overline{K}/K)$-action on $\mathcal{O}_{\overline{K}}^\times$ whose fixed points are precisely the unit group $\mathcal{O}_K^\times$. By Dirichlet's Unit Theorem, $\mathcal{O}_K^\times$ is finitely generated as an abelian group, which we can think of as an analogue of the Mordell-Weil Theorem (by which the group $E(K)$ of an elliptic curve is finitely generated).

The same cohomological procedure as in the section above gives an analogue of the Tate-Shafarevich group in the context of unit groups. For each non-archimedean $v \in M_K$, let $\mathcal{O}_{\overline{K_v}}$ denote the valuation ring in $\overline{K_v}$, and for each archimedean $v \in M_K$, let $\mathcal{O}_{\overline{K_v}} = \overline{K_v}$. Then, accordingly, one may define

$$Ш(K) := \bigcap_{v \in M_K} \mathrm{Ker}(H^1(K, \mathcal{O}_{\overline{K}}^\times) \to H^1(K_v, \mathcal{O}_{\overline{K_v}}^\times)).$$

In fact, since $H^1(K_v, \overline{K_v}^\times) = 0$ by Hilbert's Theorem 90, $Ш(K)$ may be defined purely in terms of the non-archimedean places.

Remarkably, it turns out $Ш(K)$ is canonically isomorphic to $\mathrm{Cl}(K)$, the ideal class group of K. This result is folklore, but it seems few detailed proofs have been recorded in the literature (one may be found in [5][Prop. 1.1]). We dedicate the remainder of this note to proving this fact, following an argument of Karl Schaefer. A couple of interesting questions, some of them wildly open, arise from this situation:

- Finiteness of $\mathrm{Cl}(K)$ is classically proven using the geometry of numbers (i.e., Minkowski's Theorem on lattice points). Is there a corresponding geometry of numbers approach to proving $Ш(E/K)$ is finite?
- Is there a cohomological proof that $\mathrm{Cl}(K)$ is finite using the isomorphism with $Ш(K)$?
- In the elliptic curve case, $Ш(E/K)$ is an artifact of the failure of a local-global principle. Is there a similar local-global principle whose failure is detected by $\mathrm{Cl}(K)$? Naïvely, $\mathrm{Cl}(K)$ measures the failure of locally principal ideals to be globally principal; but this is a somewhat unsatisfying interpretation since all ideals in a local field are principal.

3. Proof that $Ш(K) \cong \mathrm{Cl}(K)$

Associated with a number field K is the exact sequence

$$1 \to \mathcal{O}_K^\times \to K^\times \to I_K \to \mathrm{Cl}(K) \to 1,$$

where I_K denotes the group of fractional ideals in K. To bring cohomology into the picture, consider the short exact sequence

$$1 \to \mathcal{O}_{\overline{K}}^\times \to \overline{K}^\times \to \overline{K}^\times/\mathcal{O}_{\overline{K}}^\times \to 1,$$

in which we may identify $\overline{K}^\times/\mathcal{O}_{\overline{K}}^\times$ with the subgroup $\mathrm{Prin}(\overline{K}) \subset I_{\overline{K}}$ of principal fractional ideals in $\overline{K}$. Taking fixed points under the $\mathrm{Gal}(\overline{K}/K)$-action yields

$$1 \to \mathcal{O}_K^\times \to K^\times \to H^0(K, \mathrm{Prin}(\overline{K})) \to H^1(K, \mathcal{O}_{\overline{K}}^\times) \to H^1(K, \overline{K}^\times) \cong 1,$$

with triviality of the last cohomology group being due to Hilbert's Theorem 90. The elements of $\mathrm{Amb}(\overline{K}) := H^0(K, \mathrm{Prin}(\overline{K}))$ are the Galois-invariant principal ideals in $\overline{K}$, called *ambiguous* principal ideals.

Example 3.1. Note that $\mathrm{Amb}(\overline{K}) \neq \mathrm{Prin}(K)$, although every ideal in $\overline{K}$ extended from a principal ideal in K is certainly ambiguous. For instance, when $K = \mathbb{Q}$, the ideal $i\mathcal{O}_{\overline{Q}}$ is Galois-invariant since $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ swaps i and $-i$, but $i\mathcal{O}_{\overline{Q}}$ does not come from an ideal of $\mathbb{Q}$.

If $x\mathcal{O}_{\overline{K}}$ is ambiguous (where $x \in \overline{K}^\times$), then for each $\sigma \in \mathrm{Gal}(\overline{K}/K)$, one has

$$\sigma(x)\mathcal{O}_{\overline{K}} = \sigma\left(x\mathcal{O}_{\overline{K}}\right) = x\mathcal{O}_{\overline{K}}.$$

Hence $\sigma(x)/x \in \mathcal{O}_{\overline{K}}^\times$, by which it follows $\sigma \mapsto \sigma(x)/x$ is a 1-cocycle. This precisely describes the boundary map $\delta : \mathrm{Amb}(\overline{K}) \to H^1(K, \mathcal{O}_{\overline{K}}^\times)$.

Our approach to showing $Ш(K) \cong \mathrm{Cl}(K)$ will be to "lift" this boundary map to an inclusion $\mathrm{Cl}(K) \to H^1(K, \mathcal{O}_{\overline{K}}^\times)$ whose image is $Ш(K)$. In other words, we shall

construct injections α and β such that the diagram below commutes, and such that $\mathrm{Im}(\beta) = Ш(K)$:

$$(\star) \qquad \begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & K^\times & \longrightarrow & I_K & \longrightarrow & \mathrm{Cl}(K) & \longrightarrow & 1 \\ & & \downarrow \mathrm{Id} & & \downarrow \mathrm{Id} & & \downarrow \alpha & & \downarrow \beta & & \\ 1 & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & K^\times & \longrightarrow & \mathrm{Amb}(\overline{K}) & \xrightarrow{\delta} & H^1(K, \mathcal{O}_{\overline{K}}^\times) & \longrightarrow & 1 \end{array}$$

Remark 3.2. Prior to what follows, we fix for each prime $\mathfrak{p} \subset \mathcal{O}_K$ an embedding $\overline{K} \hookrightarrow \overline{K_\mathfrak{p}}$. There is a unique extension of the $\mathfrak{p}$-adic valuation on $K_\mathfrak{p}$ to $\overline{K_\mathfrak{p}}$; we somewhat abusively denote this extension $v_\mathfrak{p}$. For each finite extension L/K, the choice of embedding $\overline{K} \hookrightarrow \overline{K_\mathfrak{p}}$ yields a preferred prime $\mathfrak{q} \subset \mathcal{O}_L$ corresponding to the restriction of $v_\mathfrak{p}$ to the image of L in $L \hookrightarrow \overline{K} \hookrightarrow \overline{K_\mathfrak{p}}$. Details may be found in [2][Ch. II, § 8].

Lemma 3.3. *For any $I \in I_K$, there exists a finite extension L/K such that $I\mathcal{O}_L$ is principal.*

Proof. If n is the class number of K, then I^n is principal; write $I^n = \alpha\mathcal{O}_K$ (where $\alpha \in K^\times$) and set $\beta := \alpha^{1/n}$. Taking $L = K(\beta)$, we have

$$(I\mathcal{O}_L)^n = I^n\mathcal{O}_L = \alpha\mathcal{O}_L = (\beta\mathcal{O}_L)^n.$$

Hence, by unique prime factorization of ideals in L, it follows $I\mathcal{O}_L = \beta\mathcal{O}_L$. □

Corollary 3.4. *If $I \in I_K$, then $I\mathcal{O}_{\overline{K}}$ is principal.*

Lemma 3.5. *For any $I \in I_K$, every ideal class in* $\mathrm{Cl}(K)$ *contains an ideal relatively prime to I.*

Proof. Consider an ideal class $[J]^{-1} \in \mathrm{Cl}(K)$. By the Chinese Remainder Theorem, there is $\alpha \in \mathcal{O}_K$ such that

- for each prime $\mathfrak{p}$ dividing I but not J, we have $v_\mathfrak{p}(\alpha) = 0$
- for each prime $\mathfrak{p}$ dividing J, we have $v_\mathfrak{p}(\alpha) = v_\mathfrak{p}(J)$.

Then $\alpha\mathcal{O}_K = JJ_1$ for some fractional ideal J_1, where J_1 is relatively prime to I. Since $[J_1] = [J]^{-1}$, the conclusion follows. □

Theorem 3.6. *There is a canonical isomorphism $Ш(K) \cong \mathrm{Cl}(K)$.*

Proof. By Lemma 3.3, for $I \in I_K$, the ideal $I\mathcal{O}_{\overline{K}}$ is principal. Certainly $I\mathcal{O}_{\overline{K}}$ is ambiguous, since $\mathrm{Gal}(\overline{K}/K)$ fixes K; hence, this furnishes a map $\alpha : I_K \to \mathrm{Amb}(\overline{K})$ given by $I \mapsto I\mathcal{O}_{\overline{K}}$. In fact, since $I\mathcal{O}_{\overline{K}} \cap \mathcal{O}_K = I$, this α is an injection. Furthermore, one can easily verify $\beta : \mathrm{Cl}(K) \to H^1(K, \mathcal{O}_{\overline{K}}^\times)$ given by $\beta([I]) := \delta(\alpha(I))$ is well-defined and injective.

In the diagram $(\star\star)$ below, $Ш(K) = \mathrm{Ker}(\tilde{\beta})$, hence we must show $\mathrm{Im}(\beta) = \mathrm{Ker}(\tilde{\beta})$.

$$
(\star\star)\qquad
\begin{array}{ccccccc}
K^\times & \longrightarrow & I_K & \longrightarrow & \mathrm{Cl}(K) & \longrightarrow & 1 \\
\downarrow & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \\
K^\times & \longrightarrow & \mathrm{Amb}(\overline{K}) & \xrightarrow{\delta} & H^1(K, \mathcal{O}_{\overline{K}}^\times) & \longrightarrow & 1 \\
\downarrow & & \downarrow{\scriptstyle \tilde{\alpha}} & & \downarrow{\scriptstyle \tilde{\beta}} & & \\
\prod_{\mathfrak{p}} K_{\mathfrak{p}}^\times & \longrightarrow & \prod_{\mathfrak{p}} \mathrm{Amb}(\overline{K_{\mathfrak{p}}}) & \xrightarrow{\tilde{\delta}} & \prod_{\mathfrak{p}} H^1(K_{\mathfrak{p}}, \mathcal{O}_{\overline{K_{\mathfrak{p}}}}^\times) & \longrightarrow & 1
\end{array}
$$

Consider $[I] \in \mathrm{Cl}(K)$. Given a prime $\mathfrak{p} \subset \mathcal{O}_K$, by Lemma 3.5 there is $J \in [I]$ relatively prime to $\mathfrak{p}$. If $\alpha(J) = x\mathcal{O}_{\overline{K}}$, then $v_{\mathfrak{p}}(x) = 0$, so $x \in \mathcal{O}_{\overline{K_{\mathfrak{p}}}}^\times$ under the fixed embedding $\overline{K} \hookrightarrow \overline{K_{\mathfrak{p}}}$. Consequently, the restriction of the cocycle $\sigma \mapsto \sigma(x)/x$ to $\mathrm{Gal}(\overline{K_{\mathfrak{p}}}/K_{\mathfrak{p}})$ is a coboundary. Since this is true for every prime $\mathfrak{p}$, it follows $\tilde{\beta}(\beta([I])) = 0$, hence $\mathrm{Im}(\beta) \subseteq Ш(K)$.

Suppose $f \in Ш(K)$. Take $t\mathcal{O}_{\overline{K}} \in \mathrm{Amb}(\overline{K})$ such that $\delta(t\mathcal{O}_{\overline{K}}) = f$. To show $f \in \mathrm{Im}(\beta)$, it will suffice to prove $t\mathcal{O}_{\overline{K}} \in \mathrm{Im}(\alpha)$.

Since $\tilde{\delta}(\tilde{\alpha}(t\mathcal{O}_{\overline{K}})) = \tilde{\beta}(\delta(t\mathcal{O}_{\overline{K}})) = 0$, exactness of the bottom row in $(\star\star)$ implies that for each prime $\mathfrak{p}$, there is $t_{\mathfrak{p}} \in K_{\mathfrak{p}}^\times$ such that $t_{\mathfrak{p}}\mathcal{O}_{\overline{K_{\mathfrak{p}}}} = \tilde{\alpha}(t\mathcal{O}_{\overline{K}}) = t\mathcal{O}_{\overline{K_{\mathfrak{p}}}}$. In particular, $v_{\mathfrak{p}}(t) = v_{\mathfrak{p}}(t_{\mathfrak{p}})$.

Take L to be a finite Galois extension of K such that $t \in L$, and consider the prime factorization of $t\mathcal{O}_L$:

$$t\mathcal{O}_L = \prod_{\mathfrak{p} \subset \mathcal{O}_K} \prod_{\mathfrak{q} \mid \mathfrak{p}} (\mathfrak{q}\mathcal{O}_L)^{a_{\mathfrak{q}}}.$$

Since $t\mathcal{O}_{\overline{K}}$ is ambiguous and $\mathrm{Gal}(L/K)$ acts transitively on the primes in L above a fixed prime $\mathfrak{p}$ in K, we must have $a_{\mathfrak{q}} = a_{\mathfrak{q}'}$ whenever $\mathfrak{q}, \mathfrak{q}' \subset \mathcal{O}_L$ both lie over $\mathfrak{p} \subset \mathcal{O}_K$. Accordingly, set $a_{\mathfrak{p}} := a_{\mathfrak{q}}$ for any $\mathfrak{q} | \mathfrak{p}$.

Denote by $e_{\mathfrak{p}}$ the ramification index of $\mathfrak{p}$ in L/K, and let $\mathfrak{q} \subset \mathcal{O}_L$ be the preferred prime over $\mathfrak{p}$ furnished by the fixed embedding $\overline{K} \hookrightarrow \overline{K_{\mathfrak{p}}}$. By definition, $a_{\mathfrak{q}} = v_{\mathfrak{p}}(t) = v_{\mathfrak{p}}(t_{\mathfrak{p}})$, which is a multiple of the ramification degree of $L_{\mathfrak{q}}/K_{\mathfrak{p}}$ (since $t_{\mathfrak{p}} \in K_{\mathfrak{p}}$); this is precisely $e_{\mathfrak{p}}$, hence $a_{\mathfrak{p}}/e_{\mathfrak{p}} \in \mathbb{Z}$ for all primes $\mathfrak{p}$. It follows that

$$t\mathcal{O}_L = \prod_{\mathfrak{p} \subset \mathcal{O}_K} \left(\prod_{\mathfrak{q} \mid \mathfrak{p}} \mathfrak{q}\mathcal{O}_L \right)^{a_{\mathfrak{p}}} = \prod_{\mathfrak{p} \subset \mathcal{O}_K} (\mathfrak{p}\mathcal{O}_L)^{a_{\mathfrak{p}}/e_{\mathfrak{p}}}.$$

Thus, we conclude $t\mathcal{O}_{\overline{K}} = \alpha(I)$, where $I = \prod_{\mathfrak{p} \subset \mathcal{O}_K} \mathfrak{p}^{a_{\mathfrak{p}}/e_{\mathfrak{p}}} \in I_K$.

□

Acknowledgments. Sincerest thanks to Karl Schaefer, who patiently explained to me much of the mathematics in this article and described his proof of the main result. Thanks also to Peter May, for his patience and support during a trying time.

References

[1] J. Neukirch. *Cohomology of Number Fields.* 2e, Springer-Verlag 2007.
[2] J. Neukirch. *Algebraic Number Theory.* Springer-Verlag 1991.
[3] D. Dummit, S. Foote. *Abstract Algebra* 3e, Wiley and Sons 2004.

[4] J. Silverman. *The Arithmetic of Elliptic Curves* 2e, Springer GTM 2009.
[5] R. Schoof, L. Washington. Visibility of ideal classes, *J. Number Theory* Vol. 130, Issue 12, December 2010.
[6] C. Delaunay. Heuristics on class groups and on Tate-Shafarevich groups: The magic of the Cohen-Lenstra heuristics. Post-doctoral expository document.