$\mathrm{Cl}(K) \cong Ш(K)$

David Kurniadi Angdinata

Wednesday, 11 March 2020

Abstract

This article gives a short proof of the natural isomorphism between the ideal class group of a number field and a notion of a Tate–Shafarevich group defined from it, primarily adapting the arguments from Sameer Kailasa's 2016 article *on the Tate–Shafarevich group of a number field* while consulting Kevin Buzzard's 2005 article *why is an ideal class group a Tate–Shafarevich group?*.

Let K be a field of characteristic zero. Denote its non-zero elements by $K^\times$, its ring of integers by $\mathcal{O}_K$, its unit group by $\mathcal{O}_K^\times$, its algebraic closure by $\overline{K}$, and its absolute Galois group by G_K. If M is a Galois module of K, denote its n-th Galois cohomology groups by $H^n(K, M)$.

If K is a number field, denote its places by $V(K)$, its non-archimedean places by $V_0(K)$, its ideal group by $I(K)$, its principal ideal group by $P(K)$, and its ideal class group by $\mathrm{Cl}(K)$. If $\mathfrak{p}$ is a place of K, denote its discrete valuation by $v_\mathfrak{p}$, and its completion by $K_\mathfrak{p}$.

If E is an elliptic curve with K-rational points $E(K)$, its Tate–Shafarevich group is defined as

$$Ш(E/K) = \ker\left(H^1(K, E(\overline{K})) \to \prod_{\mathfrak{p} \in V(K)} H^1(K_\mathfrak{p}, E(\overline{K_\mathfrak{p}}))\right).$$

In a similar fashion, if K is a number field, its Tate–Shafarevich group can be defined as

$$Ш(K) = \ker\left(H^1(K, \mathcal{O}_{\overline{K}}^\times) \to \prod_{\mathfrak{p} \in V_0(K)} H^1(K_\mathfrak{p}, \mathcal{O}_{\overline{K_\mathfrak{p}}}^\times)\right).$$

This is a prime example of the folklore heuristic correspondence between rational points of elliptic curves and unit groups of number fields. The following theorem shows its relationship with the ideal class group.

Theorem. *Let K be a number field. Then there is a natural isomorphism* $\mathrm{Cl}(K) \xrightarrow{\sim} Ш(K)$.

Proof. There is a fundamental exact sequence in algebraic number theory given by

$$1 \to \mathcal{O}_K^\times \xrightarrow{i} K^\times \xrightarrow{\bullet\mathcal{O}_K} I(K) \xrightarrow{q} \mathrm{Cl}(K) \to 1.$$

Extracting a short exact sequence from the first two terms, considering their algebraic closures, and applying the Galois cohomology functor, gives a long exact sequence starting with

$$\begin{array}{ccccccccccc} 1 & \longrightarrow & H^0(K, \mathcal{O}_{\overline{K}}^\times) & \xrightarrow{i} & H^0(K, \overline{K}^\times) & \xrightarrow{\bullet\mathcal{O}_{\overline{K}}} & H^0(K, P(\overline{K})) & \xrightarrow{\delta} & H^1(K, \mathcal{O}_{\overline{K}}^\times) & \longrightarrow & H^1(K, \overline{K}^\times) \longrightarrow \dots \\ & & \downarrow\sim & & \downarrow\sim & & \downarrow\sim & & & & \downarrow\sim \\ & & \mathcal{O}_K^\times & & K^\times & & A(\overline{K}) & & & & 1, \end{array}$$

by Hilbert 90, denoting the Galois-invariant principal fractional ideals in $\overline{K}$, or *ambiguous ideals*, by $A(\overline{K})$. Applying the same argument to $K_\mathfrak{p}$ and taking products over all $\mathfrak{p} \in V_0(K)$ gives an exact sequence

$$1 \to \prod_{\mathfrak{p} \in V_0(K)} \mathcal{O}_{K_\mathfrak{p}}^\times \xrightarrow{i} \prod_{\mathfrak{p} \in V_0(K)} K_\mathfrak{p}^\times \xrightarrow{\bullet\mathcal{O}_{\overline{K}}} \prod_{\mathfrak{p} \in V_0(K)} A(\overline{K_\mathfrak{p}}) \xrightarrow{\prod_\mathfrak{p} \delta_\mathfrak{p}} \prod_{\mathfrak{p} \in V_0(K)} H^1(K_\mathfrak{p}, \mathcal{O}_{\overline{K_\mathfrak{p}}}^\times) \to 1,$$

where the $\mathfrak{p}$-components of the connecting homomomorphisms $\delta_\mathfrak{p}$ are surjections sending ambiguous ideals $x_\mathfrak{p}\mathcal{O}_{\overline{K_\mathfrak{p}}} \in A(\overline{K_\mathfrak{p}})$ to 1-cocycles, which in turn send automorphisms $\sigma \in G_K$ to units $\sigma(x_\mathfrak{p})/x_\mathfrak{p} \in \mathcal{O}_{\overline{K_\mathfrak{p}}}^\times$.

Combining the three exact sequences gives a diagram with exact rows

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathcal{O}_K^\times & \xrightarrow{\quad i \quad} & K^\times & \xrightarrow{\bullet\mathcal{O}_K} & I(K) & \xrightarrow{\quad q \quad} & \mathrm{Cl}(K) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \sim} & & \downarrow{\scriptstyle \sim} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \\
1 & \longrightarrow & \mathcal{O}_{\overline{K}}^\times & \xrightarrow{\quad i \quad} & K^\times & \xrightarrow{\bullet\mathcal{O}_{\overline{K}}} & A(\overline{K}) & \xrightarrow{\quad \delta \quad} & H^1(K, \mathcal{O}_{\overline{K}}^\times) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \Delta} & & \downarrow{\scriptstyle \Delta} & & \downarrow{\scriptstyle \Delta_\alpha} & & \downarrow{\scriptstyle \Delta_\beta} & & \\
1 & \longrightarrow & \prod_{\mathfrak{p} \in V_0(K)} \mathcal{O}_{K_\mathfrak{p}}^\times & \xrightarrow{i} & \prod_{\mathfrak{p} \in V_0(K)} K_\mathfrak{p}^\times & \xrightarrow{\bullet\mathcal{O}_{\overline{K}}} & \prod_{\mathfrak{p} \in V_0(K)} A(\overline{K_\mathfrak{p}}) & \xrightarrow{\prod_\mathfrak{p} \delta_\mathfrak{p}} & \prod_{\mathfrak{p} \in V_0(K)} H^1(K_\mathfrak{p}, \mathcal{O}_{\overline{K_\mathfrak{p}}}^\times) & \longrightarrow & 1.
\end{array}$$

To make this diagram commute, it is necessary to define the relevant vertical maps.

- The maps $\sim$ are identity maps, and the maps Δ are diagonal embeddings.
- The map $\alpha : I(K) \to A(\overline{K})$ is an injection sending a fractional ideal $I \in I(K)$ to the ambiguous ideal above $I_{\mathcal{O}_{\overline{K}}} \in A(\overline{K})$. This is principal since $\overline{K}$ contains the Hilbert class field of K, and Galois-invariant since I and $\mathcal{O}_{\overline{K}}$ are Galois-invariant.
- The map $\beta : \mathrm{Cl}(K) \to H^1(K, \mathcal{O}_{\overline{K}}^\times)$ is an injection sending an ideal class $[I] \in \mathrm{Cl}(K)$ to the composition $\delta(\alpha(I)) \in H^1(K, \mathcal{O}_{\overline{K}}^\times)$, which is independent of the representative fractional ideal $I \in I(K)$. This by definition gives $Ш(K) = \ker \Delta_\beta$.

To prove the isomorphism $\mathrm{Cl}(K) \xrightarrow{\sim} Ш(K)$, it is sufficient to prove $\operatorname{im} \beta = \ker \Delta_\beta$.

$\subseteq$ Let $f \in \operatorname{im} \beta$ be a 1-cocycle. By surjectivity, there is an ideal class $[I] \in \mathrm{Cl}(K)$ such that $f = \beta([I])$. Now let $\mathfrak{p} \in V_0(K)$ be a place. By the Chinese remainder theorem, there is a fractional ideal $J \in [I]$ such that $J + \mathfrak{p} = \mathcal{O}_K$, so $v_\mathfrak{p}(J_{\mathcal{O}_{\overline{K}}}) = 0$. By principality, there is an ambiguous ideal $x_\mathfrak{p} \mathcal{O}_{\overline{K}} \in A(\overline{K})$ such that $J_{\mathcal{O}_{\overline{K}}} = x_\mathfrak{p} \mathcal{O}_{\overline{K}}$, so $v_\mathfrak{p}(x_\mathfrak{p} \mathcal{O}_{\overline{K}}) = 0$, or $x_\mathfrak{p} \in \mathcal{O}_{\overline{K_\mathfrak{p}}}^\times$. Considering Δ_β over all places $\mathfrak{p} \in V_0(K)$,

$$\begin{aligned}
\Delta_\beta(f) &= \Delta_\beta(\beta([I])) = \Delta_\beta(\beta([J])) = \Delta_\beta(\delta(\alpha(J))) = \Delta_\beta(\delta(J_{\mathcal{O}_{\overline{K}}})) \\
&= \Delta_\beta(\delta(x_\mathfrak{p} \mathcal{O}_{\overline{K}})) = \Delta_\beta(\sigma \mapsto \sigma(x_\mathfrak{p})/x_\mathfrak{p}) = 1.
\end{aligned}$$

Hence $f \in \ker \Delta_\beta$.

$\supseteq$ Let $f \in \ker \Delta_\beta$ be a 1-cocycle. By diagram chasing at f, there is an element $(x_\mathfrak{p})_\mathfrak{p} \in \prod_\mathfrak{p} K_\mathfrak{p}^\times$ in the commutative diagram

$$\begin{array}{ccccc}
 & & x\mathcal{O}_{\overline{K}} & \xrightarrow{\quad \delta \quad} & f \\
 & & \downarrow{\scriptstyle \Delta_\alpha} & & \downarrow{\scriptstyle \Delta_\beta} \\
(x_\mathfrak{p})_\mathfrak{p} & \xrightarrow{\bullet\mathcal{O}_{\overline{K}}} & (x\mathcal{O}_{\overline{K_\mathfrak{p}}})_\mathfrak{p} & \xrightarrow{\prod_\mathfrak{p} \delta_\mathfrak{p}} & 1,
\end{array}$$

such that $x_\mathfrak{p} \mathcal{O}_{\overline{K_\mathfrak{p}}} = x\mathcal{O}_{\overline{K_\mathfrak{p}}}$ for all places $\mathfrak{p} \in V_0(K)$, or $v_\mathfrak{p}(x_\mathfrak{p}) = v_\mathfrak{p}(x)$. By taking limits, it suffices to consider a finite extension $K \subseteq L$. By the unique factorisation of prime ideals and transitivity of the Galois group G_K/G_L,

$$\begin{aligned}
\delta(x\mathcal{O}_L) &= \delta\left(\prod_{\mathfrak{p} \in V_0(K)} \left(\prod_{\mathfrak{q} \in V_0(L),\ \mathfrak{q} \mid \mathfrak{p}} \mathfrak{q}\right)^{v_\mathfrak{p}(x)}\right) = \delta\left(\prod_{\mathfrak{p} \in V_0(K)} \left(\prod_{\mathfrak{q} \in V_0(L),\ \mathfrak{q} \mid \mathfrak{p}} \mathfrak{q}\right)^{v_\mathfrak{p}(x_\mathfrak{p})}\right) \\
&= \delta\left(\prod_{\mathfrak{p} \in V_0(K)} \mathfrak{p}_{\mathcal{O}_L}^{\frac{v_\mathfrak{p}(x_\mathfrak{p})}{e_\mathfrak{p}}}\right) = \delta\left(\alpha\left(\prod_{\mathfrak{p} \in V_0(K)} \mathfrak{p}^{\frac{v_\mathfrak{p}(x_\mathfrak{p})}{e_\mathfrak{p}}}\right)\right) = \beta\left(q\left(\prod_{\mathfrak{p} \in V_0(K)} \mathfrak{p}^{\frac{v_\mathfrak{p}(x_\mathfrak{p})}{e_\mathfrak{p}}}\right)\right),
\end{aligned}$$

where $e_\mathfrak{p}$ are the respective local ramification indices of $K_\mathfrak{p} \subseteq L_\mathfrak{q}$. Hence $f \in \operatorname{im} \beta$.

Hence $\operatorname{im} \beta = \ker \Delta_\beta$ and thus $\mathrm{Cl}(K) \cong Ш(K)$. $\square$