The Fundamental Class

Devang Agarwal

Abstract

In this essay, we establish the fundamental exact sequence of class field theory and a fundamental class for number fields, assuming local class field theory and the first and second inequalities. This essay had been made as an end of term project for the course MATH 613D in the 2021 Winter term 1 at UBC.

1 Notation & Preliminaries

$\mathfrak{M}_K$	set of places of a number field K
K_v	completion of a number field K at a place $v \in \mathfrak{M}_K$
L^v	completion of L at a place above a place v of K, where L is finite, Galois over
$\bar{K}$	a fixed separable closure of a field K
G_K	$= \mathrm{Gal}(\bar{K}/K)$, the absolute Galois group of a field K
$G_{L/K}$	$= \mathrm{Gal}(L/K)$, the Galois group of a Galois extension L/K
$\mathrm{Br}(K)$	$= H^2(G_K, \bar{K}^*)$, the Brauer group of a field K
$\mathrm{Br}(L/K)$	$= H^2(G_{L/K}, L^*)$, where L/K is a Galois extension of fields
$\mathbb{I}_K$	the group of idèles of a number field K
$\mathbf{C}_K$	$= \mathbb{I}_K/K^*$, the idèle class group of a number field K
$H^2(L/K)$	$= H^2(G_{L/K}, \mathbf{C}_L)$ for a Galois extension L of a number field K
$H^2(K)$	$= \varinjlim_{L/K} H^2(L/K)$, where the limit is over Galois extensions L of K

The goal of this essay is to compute $\mathrm{Br}(K)$ for a number field K, in the form of the fundamental exact sequence, and to show that $H^2(L/K)$ is cyclic of order $[L:K]$ with a canonical generator (the fundamental class) for every Galois extension L/K. First we state some results that we will need.

Theorem 1.1. *For every abelian extension L/K of number fields, and a finite set S of primes of K containing all infinite primes and those that ramify in L, the map,*

$$\mathfrak{p} \mapsto (\mathfrak{p}, L/K) : I^S \to \mathrm{Gal}(L/K)$$

is surjective, where I^S is the group of fractional ideals coprime to the primes in S, and $(\mathfrak{p}, L/K)$ is the Frobenius element for $\mathfrak{p}$.

Proof. Follows immediately from the first inequality, see Consequence 8.7, Chapter VII in [CFSU67] or Corollary 4.8, Chapter VII in [Mil20]. Alternatively for an analytic proof, see Corollary 3.8, Chapter VI, also in [Mil20]. $\square$

Theorem 1.2. *Let L/K be a cyclic extension of number fields. Then,*

1. $(\mathbb{I}_K : K^* \operatorname{Nm}(\boldsymbol{C}_L))$ *is finite and divides* $[L : K]$
2. $H_1(G_{L/K}, \boldsymbol{C}_L) = 0$
3. $H^2(G_{L/K}, \boldsymbol{C}_L)$ *is finite and divides* $[L : K]$

Proof. This is the second inequality. For a proof, see Theorem 9.1, Chapter VII in [CFSU67] or Theorem 5.1, Chapter VII in [Mil20]. □

Given a Galois extension L/K of number fields, we have the reciprocity map given by

$$\begin{aligned} \phi_{L/K} : \mathbb{I}_K &\to G_{L/K}^{ab} \\ (a_v) &\mapsto \prod_v \phi_v(a_v) \end{aligned}$$

where $\phi_v : K_v^* \to (G_{L/K}^v)^{ab}$ is the local reciprocity map and $G_{L/K}^v$ is the decomposition group of any place w of L above v. We will need the following computation of the reciprocity map for the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.

Lemma 1.3. *For a cyclotomic extension L of a number field K (i.e. $L \subset K(\zeta_n)$ for some n), the reciprocity map sends principal idèles to 1, i.e. $\forall a \in K^*$, $\phi_{L/K}(a) = 1$*

Proof. Follows from an explicit computation of the local reciprocity maps for extensions $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, and compatibility of local reciprocity maps with change of base fields and field norms, see section 10.4, Chapter VII in [CFSU67] or Example 8.2 and Lemma 8.4, Chapter VII in [Mil20] for details. □

Lastly, we require the following results from local class field theory. For proofs, see Chapter VI of [CFSU67].

Theorem 1.4. *For every non archimedean local field K there exist an isomorphism,* $\operatorname{inv}_K : \operatorname{Br}(K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ *such that we have the following commutative diagram for every finite extension L/K of local fields with degree n,*

$$\begin{array}{ccccccc} 0 & \longrightarrow & \operatorname{Br}(L/K) & \xrightarrow{\text{Inf}} & \operatorname{Br}(K) & \xrightarrow{\text{Res}} & \operatorname{Br}(L) \\ & & \downarrow{\scriptstyle \operatorname{inv}_{L/K}} & & \downarrow{\scriptstyle \operatorname{inv}_K} & & \downarrow{\scriptstyle \operatorname{inv}_L} \\ 0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \hookrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{\times n} & \mathbb{Q}/\mathbb{Z} \end{array}$$

This diagram has exact rows and all vertical maps are isomorphisms.
For archimedean local fields we have $\operatorname{inv}_{\mathbb{R}} : \operatorname{Br}(\mathbb{R}) \xrightarrow{\sim} \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, *and* $\operatorname{inv}_{\mathbb{C}} : \operatorname{Br}(\mathbb{C}) \xrightarrow{\sim} (0)$ *and the following diagram,*

$$\begin{array}{ccccccc} 0 & \longrightarrow & \operatorname{Br}(\mathbb{C}/\mathbb{R}) & \xrightarrow{\text{Inf}} & \operatorname{Br}(\mathbb{R}) & \xrightarrow{\text{Res}} & \operatorname{Br}(\mathbb{C}) \\ & & \downarrow{\scriptstyle \operatorname{inv}_{\mathbb{C}/\mathbb{R}}} & & \downarrow{\scriptstyle \operatorname{inv}_{\mathbb{R}}} & & \downarrow{\scriptstyle \operatorname{inv}_{\mathbb{C}}} \\ 0 & \longrightarrow & \frac{1}{2}\mathbb{Z}/\mathbb{Z} & \hookrightarrow & \frac{1}{2}\mathbb{Z}/\mathbb{Z} & \xrightarrow{\times 2} & 0 \end{array}$$

Theorem 1.5. *For a Galois extension L/K of local fields, let $\chi \in \mathrm{Hom}(G_{L/K}, \mathbb{Q}/\mathbb{Z}) \cong H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z})$ be a character of its Galois group. If $\delta : H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^2(G_{L/K}, \mathbb{Z})$ denotes the isomorphism obtained from the connecting map of the long exact sequence for $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$, and $\bar{\alpha}$ denotes the class of $\alpha \in K^*$ in $H^0_T(G_{L/K}, L^*)$, then we have,*

$$\chi(\phi_{L/K}(a)) = \mathrm{inv}_{L/K}(\bar{a} \cup \delta\chi)$$

2 Splitting of Brauer Classes

Let L/K be an algebraic field extension. We say an element $\alpha \in \mathrm{Br}(K)$ is split by L if it is mapped to zero under $\mathrm{Res} : \mathrm{Br}(K) \to \mathrm{Br}(L)$. Now assume L/K to be Galois. By Hilbert's theorem 90, $H^1(G_K, K^*) = 0$ for all fields K, so by the restriction-inflation sequence of group cohomology, we have an exact sequence,

$$0 \to \mathrm{Br}(L/K) \xrightarrow{\mathrm{inf}} \mathrm{Br}(K) \xrightarrow{\mathrm{Res}} \mathrm{Br}(L)$$

So we may identify $\mathrm{Br}(L/K)$ with the subgroup of Brauer classes of $\mathrm{Br}(K)$ split by the extension L/K. Theorem 1.4 tells us that for local fields, this depends just on the degree of the extension.
Now let L/K be a finite Galois extension of number fields. Then we have the exact sequence,

$$0 \to L^* \to \mathbb{I}_L \to \mathbf{C}_L \to 0$$

of $G_{L/K}$-modules. From theorem 1.2, we know that $H^1(G_{L/K}, \mathbf{C}_L) = 0$, so taking the long exact sequence gives us,

$$0 \to \mathrm{Br}(L/K) \to H^2(G_{L/K}, \mathbb{I}_L) \to H^2(L/K) \to H^3(G_{L/K}, L^*) \tag{1}$$

We also have an isomorphism $H^2(G_{L/K}, \mathbb{I}_L) \cong \bigoplus_{v \in \mathfrak{M}_k} \mathrm{Br}(L^v/K_v)$, where the map is given by a sum of restrictions to decomposition groups followed by maps induced by $L^* \hookrightarrow (L^v)^*$ for an arbitrary choice of a place of L above each place of K. Replacing $H^2(G_{L/K}, \mathbb{I}_L)$ by $\bigoplus_{v \in \mathfrak{M}_k} \mathrm{Br}(L^v/K_v)$ and taking direct limits over all Galois extensions L over K, we obtain,

$$0 \to \mathrm{Br}(K) \to \oplus_v \mathrm{Br}(K_v) \to \varinjlim_{L/K} H^2(L/K) \tag{2}$$

Combining this with a similar sequence for L and the previous sequence, we get the diagram,

$$\begin{array}{ccccccc} & & 0 & & 0 & & 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{Br}(L/K) & \longrightarrow & \bigoplus_v \mathrm{Br}(L^v/K_v) & \longrightarrow & H^2(L/K) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{Br}(K) & \longrightarrow & \bigoplus_v \mathrm{Br}(K_v) & \longrightarrow & H^2(K) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{Br}(L) & \longrightarrow & \bigoplus_v \left(\bigoplus_{w|v} \mathrm{Br}(L_w)\right) & \longrightarrow & H^2(L/K) \end{array} \tag{3}$$

with exact rows and columns (columns are exact due to restriction-inflation). Now let $\boldsymbol{\alpha} \in \mathrm{Br}(K)$, with image $(\alpha_v) \in \bigoplus_v \mathrm{Br}(K_v)$. Then $\boldsymbol{\alpha} \in \mathrm{Br}(L/K)$ iff $\boldsymbol{\alpha}$ maps to zero in $\mathrm{Br}(L)$ or equivalently (α_v) maps to zero in $\bigoplus_v \left(\bigoplus_{w|v} \mathrm{Br}(L_w)\right)$. Interpreting this via invariant maps of theorem 1.4, we obtain,

Lemma 2.1. *With notation as above, $\boldsymbol{\alpha} \in \mathrm{Br}(K)$ is split by L iff for all places v of K, $[L^v : K_v]\,\mathrm{inv}_{K_v}(\alpha_v) = 0$ in $\mathbb{Q}/\mathbb{Z}$, if v is finite, and in $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ is v is real. (There is nothing to check for complex places).*

3 Cyclic cyclotomic extensions

In local class field theory, we see that unramified extensions of local fields play an important role due to them not only being well-behaved due to their similarities with finite field extensions, but at the same being being a large enough class of extensions to be able to split the entire Brauer group of a local field. In the global setting, cyclotomic extensions form a large class of better understood extensions, meanwhile being cyclic makes computation of cohomology easier due to periodicity of the cohomology groups, so we try to find useful families of cyclic, cyclotomic extensions and show that these extensions can split all Brauer classes of a number field.

Consider the cyclotomic extension $\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}$. For now we assume $p \neq 2$. We have the following isomorphisms,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}) \cong (\mathbb{Z}/p^r\mathbb{Z})^* \cong \Delta_p \times \mathbb{Z}/p^{r-1}\mathbb{Z}$$

where $\Delta_p \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Here the first isomorphism is natural and second depends only on a choice of a primitive root modulo p^r. Let L_{p^r} be the fixed field of Δ_p, then $\mathrm{Gal}(L_{p^r}/\mathbb{Q}) \cong \mathbb{Z}/p^{r-1}\mathbb{Z}$ and $[\mathbb{Q}(\zeta_{p^r}) : L_{p^r}] = (p-1)$. Furthermore, under the above sequence of isomorphisms, complex conjugation corresponds to the residue class of $[-1]$ in $(\mathbb{Z}/p^r\mathbb{Z})^*$ which in turn gets mapped to the element $(\frac{p-1}{2}, 0)$ of $\Delta_p \times \mathbb{Z}/p^{r-1}\mathbb{Z}$, and hence fixes L_{p^r}. Therefore the extension L_{p^r} is totally real.
Now consider $\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}$ for $r \geq 3$. Here we have isomorphisms,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}) \cong (\mathbb{Z}/2^r\mathbb{Z})^* \cong \langle[-1]\rangle \times \langle[5]\rangle \cong \langle[-5^{2^{r-3}}]\rangle \times \langle[5]\rangle$$

where [_] denotes residue classes in $(\mathbb{Z}/2^r\mathbb{Z})^*$. Let L_{2^r} be the fixed field of $\Delta_2 := \langle[-5^{2^{r-3}}]\rangle$. Then it has Galois group $\text{Gal}(L_{2^r}/\mathbb{Q}) \cong \langle[5]\rangle \cong \mathbb{Z}/2^{r-2}\mathbb{Z}$ and $[\mathbb{Q}(\zeta_{2^r}) : L_{2^r}] = 2$. Moreover, since complex conjugation, $[-1]$ does not fix L_{2^r}, this extensions is totally complex.
Therefore we have a family of extensions L_{p^r} of $\mathbb{Q}$ for every prime p and $r \geq 3$ satisfying:

- The extensions $L_{p^r}/\mathbb{Q}$ are cyclic with degree, a power of p. Moreover, $[L_{p^r} : \mathbb{Q}] \to \infty$ as $r \to \infty$. (the degree is p^{r-1} if $p \neq 2$ and is 2^{r-2} if $p = 2$)
- $L_{p^r} \subset \mathbb{Q}(\zeta_{p^r})$, with $[\mathbb{Q}(\zeta_{p^r}) : L_{p^r}] \leq p$ (we know this degree is $p-1$ for $p \neq 2$ and is 2 if $p = 2$)

We now look at local degrees $[(L_{p^r})^l : \mathbb{Q}_l]$.
If $l = p$, we know that p is totally ramified in $\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}$ and hence in $L_{p^r}/\mathbb{Q}$, so the local degree $[(L_{p^r})^p : \mathbb{Q}_p] = [L_{p^r} : \mathbb{Q}] \to \infty$ as $r \to \infty$.
Meanwhile if $l \neq p$, then l does not ramify in $\mathbb{Q}(\zeta_{p^r})$, and hence in L_{p^r}, so the local degrees of both the extensions at l is going to be equal to the residue degree at l. The residue field extension of $\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}$ at l is generated by the p^r-th roots of unity over $\mathbb{F}_l$ and hence has degree, the smallest integer d for which $\mathbb{F}_{l^d}$ contains roots of $x^{p^r} - 1$, i.e. the smallest integer satisfying $p^r \mid l^d - 1$, i.e. d is the order of l modulo p^r. Therefore, $[(L_{p^r})^l : \mathbb{Q}_l] = [\mathbb{Q}(\zeta_{p^r})^l : \mathbb{Q}_l]/[\mathbb{Q}(\zeta_{p^r})^l : (L_{p^r})^l] \geq d/p$ since $[\mathbb{Q}(\zeta_{p^r})^l : (L_{p^r})^l] \mid [\mathbb{Q}(\zeta_{p^r}) : L_{p_r}] \leq p$. Clearly, $d \to \infty$ as $r \to \infty$, and hence even in this case $[(L_{p^r})^l : \mathbb{Q}_l] \to \infty$ as $r \to \infty$. So we have all the ingredients needed to prove the following,

Lemma 3.1. *For any finite set S of finite places of a number field K, and a positive integer m, there exists a totally complex, cyclic, cyclotomic extension L/K such that for all $v \in S$, $m \mid [L^v : K_v]$.*

Proof. We first reduce to $K = \mathbb{Q}$. Let L be a totally complex, cyclic, cyclotomic extension of $\mathbb{Q}$ such that for all $p \in \{p \in \mathfrak{M}_\mathbb{Q} | \exists v \in S, p \mid v\}$, $m[K : \mathbb{Q}] \mid [L^p : K_p]$. $K.L$ is clearly totally complex. Since $L \subset \mathbb{Q}(\zeta_n)$ for some n, $K.L \subset K(\zeta_n)$ and is hence cyclotomic over K. Moreover, $\text{Gal}((K.L)/K) \cong \text{Gal}(L/K \cap L) \subset \text{Gal}(L/\mathbb{Q})$ and is hence cyclic. Finally, for $v \in S$ above a rational prime p, we have,

$$m[K : \mathbb{Q}] \mid [(K.L)^p : \mathbb{Q}_p] = [(K.L)^v : K_v][K^p : \mathbb{Q}_p] \mid [(K.L)^v : K_v][K : \mathbb{Q}]$$

and therefore $m \mid [(K.L)^v : K_v]$. So $K.L$ has the required properties.
Now we assume $K = \mathbb{Q}$. From our discussion before the lemma, for each prime p dividing m, the extension $L_{p^{r_p}}/\mathbb{Q}$ is cyclic, cyclotomic with p-power degree and for large enough r_p, the local degrees $[(L_{p_{r_p}})^l : \mathbb{Q}_l]$ are going to be powers of p larger than $p^{v_p(m)}$ for every $l \in S$. If $2 \mid m$, let L be the composite of such extensions for every prime p dividing m, else also include L_8 in the composite. Then $L/\mathbb{Q}$ is clearly cyclotomic, it is also cyclic since its a composite of prime-power cyclic extensions for distinct primes, and its totally complex since it contains L_{2^r} for some r which is totally complex. Lastly, $m \mid \text{lcm}_{p|m}([(L_{p^{r_p}})^l : \mathbb{Q}_l]) \mid [L^l : \mathbb{Q}_l]$, so the extension $L/\mathbb{Q}$ has all the required properties. □

Going back to the situation in lemma 2.1, since $\boldsymbol{\alpha} \in \text{Br}(K) = (\alpha_v) \in \bigoplus_v \text{Br}(K_v)$, almost all α_v are zero. Let S be the set of finite places where α_v is non-zero and m be the lcm of the denominators of all the nonzero α_v. Then using the last lemma along with 2.1 we obtain,

Corollary 3.1.1.

$$\mathrm{Br}(K) = \bigcup_{\substack{L/K \\ \textit{cyclic, cyclotomic}}} \mathrm{Br}(L/K)$$

By essentially the same argument, we also have,

Corollary 3.1.2.

$$\bigoplus_v \mathrm{Br}(K_v) = \bigcup_{\substack{L/K \\ \textit{cyclic, cyclotomic}}} \bigoplus_v \mathrm{Br}(L^v/K_v)$$

4 The Fundamental Exact Sequence

In section 2, we saw that $\mathrm{Br}(K)$ sits injectively inside $\bigoplus_v \mathrm{Br}(K_v)$. We understand $\mathrm{Br}(K_v)$ very well (theorem 1.4), so to understand $\mathrm{Br}(K)$ it will suffice to compute the image of $\mathrm{Br}(K)$ in the direct sum. In the last section, we saw that every class in $\mathrm{Br}(K)$ actually lives inside $\mathrm{Br}(L/K)$ for a cyclic cyclotomic extension L/K, so it further suffices to find the image of $\mathrm{Br}(L/K)$ in $\bigoplus_v \mathrm{Br}(L^v/K_v)$. Since $G_{L/K}$ is cyclic, we know that $H^3(G_{L/K}, \mathbf{C}_L) \cong H^1(G_{L/K}, \mathbf{C}_L) = 0$ (theorem 1.2). So the exact sequence 1 of section 2 becomes,

$$0 \to \mathrm{Br}(L/K) \to \bigoplus_v \mathrm{Br}(L^v/K_v) \to H^2(L/K) \to 0$$

To compute $H^2(L/K)$ we will use the following,

Lemma 4.1. *For a cyclic cyclotomic extension L/K, if $\alpha \in \mathrm{Br}(L/K)$, then $\sum_v \mathrm{inv}_{L^v/K_v}(\alpha) = 0$.*

Proof. Note that by $\mathrm{inv}_{L^v/K_v}(\alpha)$, we actually mean $\mathrm{inv}_{L^v/K_v}(j_v \circ \mathrm{Res}^{G^v_{L/K}}_{G_{L/K}} \circ i(\alpha))$, where i and j_v are the maps induced by the inclusion $L^* \hookrightarrow \mathbb{I}_L$ and the projection $j_v : \mathbb{I}_L \to (L^v)^*$ on the cohomologies respectively, and $j_v \circ \mathrm{Res}^{G^v_{L/K}}_{G_{L/K}} : H^2(G_{L/K}, \mathbb{I}_L) \to \mathrm{Br}(L^v/K_v)$ is the projection under the isomorphism $H^2(G_{L/K}, \mathbb{I}_L) \cong \bigoplus_v \mathrm{Br}(L^v/K_v)$.

For now let L/K be an arbitrary finite Galois extension. As in the hypothesis for theorem 1.5, let $\chi \in H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z})$ be a character and $\delta\chi \in H^2(G_{L/K}, \mathbb{Z})$ be its image under the boundary isomorphism $\delta : H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^2(G_{L/K}, \mathbb{Z})$. Furthermore, for every place v of K, let $\chi_v = \mathrm{Res}^{G^v_{L/K}}_{G_{L/K}} \chi \in H^1(G^v_{L/K}, \mathbb{Q}/\mathbb{Z})$ and $\delta_v : H^1(G^v_{L/K}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^2(G^v_{L/K}, \mathbb{Z})$ be the boundary isomorphism. Then we have the following diagram,

$$\begin{array}{ccccc} H^0_T(G_{L/K}, L^*) & \longrightarrow & H^0_T(G_{L/K}, \mathbb{I}_L) & \xrightarrow{\phi_{L/K}} & G_{L/K} \\ \Big\downarrow{\scriptstyle \cup\delta\chi} & & \Big\downarrow{\scriptstyle \oplus_v j_v \circ \mathrm{Res}^{G^v_{L/K}}_{G_{L/K}} \circ (\cup\delta\chi)} & & \Big\downarrow{\scriptstyle \chi} \\ \mathrm{Br}(L/K) & \longrightarrow & \bigoplus_v \mathrm{Br}(L^v/K_v) & \xrightarrow{\sum_v \mathrm{inv}_{L^v/K_v}} & \mathbb{Q}/\mathbb{Z} \end{array}$$

The left square commutes due to the functoriality of the cup-product, meanwhile if

$\boldsymbol{\alpha} = (\alpha_v) \in H^0_T(G_{L/K}, \mathbb{I}_L) = \bigoplus_v H^0_T(G^v_{L/K}, (L^v)^*) = \bigoplus_v K_v^*/\operatorname{Nm}(L^v)^*$, then,

$$\begin{aligned}
\chi(\phi_{L/K}(\boldsymbol{\alpha})) &= \sum_v \chi(\phi_{L^v/K_v}(\alpha_v)) \\
&= \sum_v \chi_v(\phi_{L^v/K_v}(\alpha_v)) \\
&= \sum_v \operatorname{inv}_{L^v/K_v}(\alpha_v \cup \delta_v\chi_v) \quad \text{(by theorem 1.5)} \\
&= \sum_v \operatorname{inv}_{L^v/K_v}(j_v(\boldsymbol{\alpha}) \cup \delta_v\chi_v) \\
&= \sum_v \operatorname{inv}_{L^v/K_v}(j_v(\boldsymbol{\alpha} \cup \delta_v\chi_v)) \\
&= \sum_v \operatorname{inv}_{L^v/K_v}(j_v \circ \operatorname{Res}^{G^v_{L/K}}_{G_{L/K}}(\boldsymbol{\alpha} \cup \delta\chi)) \quad \text{(restriction commutes with cup products and boundary maps)}
\end{aligned}$$

That is, the right square also commutes. Now let L/K be cyclic, cyclotomic and pick χ to be a generating character. Then we know that both the $\cup\delta\chi$ in the diagram are isomorphisms (theorem 5, chapter IV in [CFSU67]) in particular the one on the left is surjective. But from theorem 1.3, we know that the composition on the top row is zero, therefore the composition on the bottom row is also zero, proving what we claimed. $\square$

Consider the following diagram,

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \operatorname{Br}(L/K) & \longrightarrow & \bigoplus_v \operatorname{Br}(L^v/K_v) & \longrightarrow & H^2(L/K) & \longrightarrow & 0 \\
 & & & & & \searrow^{\sum_v \operatorname{inv}_{L^v/K_v}} & \big\downarrow{\scriptstyle \operatorname{inv}_{L/K}} & & \\
 & & & & & & \frac{1}{n_{L/K}}\mathbb{Z}/\mathbb{Z} & \longrightarrow & 0
\end{array}$$

where $n_{L/K} = \operatorname{lcm}_v[L^v : K_v]$ Here, the horizontal sequence is exact, the bent sequence is a complex from the lemma above, and the angled map is surjective. This induces a surjective map $\operatorname{inv}_{L/K}$ from $H^2(L/K)$ to $\frac{1}{n_{L/K}}\mathbb{Z}/\mathbb{Z}$. But theorem 1.1 tells us that there exists a finite unramified place v such that $(\mathfrak{p}_\mathfrak{v}, L/K)$ is the generator of the Galois group, and hence $[L^v : K_v] = f_v = [L : K]$, which gives us $[L : K] \mid n_{L/K} \mid [L : K]$, i.e. $n_{L/K} = [L : K]$. But then from theorem 1.2, we have that order of $H^2(L/K) \leq [L : K]$. Therefore, $\operatorname{inv}_{L/K}$ is an isomorphism. Going back to $\operatorname{Br}(K)$, consider the commutative diagram,

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Br}(L/K) & \longrightarrow & \bigoplus_v \mathrm{Br}(L^v/K_v) & \xrightarrow{\mathrm{inv}^1_{L/K}} & \frac{1}{n_{L/K}}\mathbb{Z}/\mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Br}(K) & \longrightarrow & \bigoplus_v \mathrm{Br}(K_v) & \xrightarrow{\mathrm{inv}^1_{K}} & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0
\end{array}$$

where $\mathrm{inv}^1_{L/K} = \sum_v \mathrm{inv}_{L^v/K_v}$ and $\mathrm{inv}^1_K = \sum_v \mathrm{inv}_{K_v}$. From the above discussion, the top row is exact for cyclic, cyclotomic extensions L/K, while the columns are always exact. Let $\alpha \in \mathrm{Br}(K)$. Then $\alpha \in \mathrm{Br}(L/K)$ for some cyclic, cyclotomic extension of K due to corollary 3.1.1, and thus $\sum_v \mathrm{inv}_{K_v}(\alpha) = \sum_v \mathrm{inv}_{L^v/K_v}(\alpha) = 0$, so the bottom row is a complex. Moreover, if $(\alpha_v) \in \bigoplus_v \mathrm{Br}(K_v)$ such that $\sum_v \mathrm{inv}_{K_v}(\alpha_v) = 0$, due to corollary 3.1.2, $(\alpha_v) \in \bigoplus_v \mathrm{Br}(L^v/K_v)$ for some cyclic, cyclotomic extension L/K, but then $\sum_v \mathrm{inv}_{L^v/K_v}(\alpha_v) = \sum_v \mathrm{inv}_{K_v}(\alpha_v) = 0$, which by exactness of the top row, gives us an element $\alpha \in \mathrm{Br}(L/K) \subset \mathrm{Br}(K)$ such that $\alpha = (\alpha_v)$. Therefore the bottom sequence is exact at the centre. Exactness at the left was shown in section 2, meanwhile exactness at the right is obvious, so we get,

Theorem 4.2 (Fundamental Exact Sequence of Global Class Field Theory)**.** *For every number field K, the sequence,*

$$0 \to \mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v) \xrightarrow{\mathrm{inv}^1_K} \mathbb{Q}/\mathbb{Z} \to 0$$

is exact.

Moreover, the commutativity of the right square in theorem 1.4 combined with the fact that sum of local degrees is the global degree gives us:

Lemma 4.3. *For any finite extension $[L : K]$ of number fields of degree n, we have the following commutative diagram,*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Br}(K) & \longrightarrow & \bigoplus_v \mathrm{Br}(K_v) & \xrightarrow{\mathrm{inv}^1_{K}} & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \times n} & & \\
0 & \longrightarrow & \mathrm{Br}(L) & \longrightarrow & \bigoplus_v \left(\bigoplus_{w|v} \mathrm{Br}(L_w)\right) & \xrightarrow{\mathrm{inv}^1_{L}} & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0
\end{array}$$

Comparing the bottom rows of the diagram 3 with the fundamental exact sequences K and L, we obtain unique injective maps $\mathrm{inv}^2_K : \mathbb{Q}/\mathbb{Z} \to H^2(K)$ for all number fields K satisfying,

$$\begin{array}{ccc}
\bigoplus_v \mathrm{Br}(K_v) & \longrightarrow & H^2(K) \\
{\scriptstyle \mathrm{inv}^1_K}\downarrow & \nearrow_{\mathrm{inv}^2_K} & \\
\mathbb{Q}/\mathbb{Z} & &
\end{array}$$

and then the diagram in the last lemma gives us,

$$
\begin{array}{ccccc}
 & & 0 & & 0 \\
 & & \downarrow & & \downarrow \\
0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & H^2(L/K) \\
 & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{\mathrm{inv}_K^2} & H^2(K) \\
 & & \downarrow{\scriptstyle \times n} & & \downarrow \\
0 & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{\mathrm{inv}_L^2} & H^2(L)
\end{array}
$$

with exact rows and columns. But we know from theorem 1.2 that $H2(L/K)$ has order atmost n, so the map inv_K^2 restricted to $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ is an isomorphism onto $H^2(L/K)$. Denote its inverse by $\mathrm{inv}_{L/K} : H^2(L/K) \xrightarrow{\sim} \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Taking direct limit of $\mathrm{inv}_{L/K}$ over all Galois extensions L/K we find that the map inv_K^2 is also an isomorphism, again denoting its inverse by $\mathrm{inv}_K : H^2(K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$. For any finite Galois extension L/K of number fields, let $u_{L/K} = \mathrm{inv}_{L/K}^{-1}\left(\frac{1}{[L:K]}\right)$. Then it generates $H^2(L/K)$ and is called the **fundamental class**. Note that $u_{L/K} = \mathrm{inv}_{L/K}^{-1}\left(\frac{1}{[L:K]}\right) = \mathrm{inv}_K^{-1}\left(\frac{1}{[L:K]}\right)$, so if we have a tower of extensions $E \supset L \supset K$, and $\mathrm{Res} : H^2(K) \to H^2(L)$ is the restriction map, then $\mathrm{inv}_L(\mathrm{Res}(u_{E/K})) = [L : K]\,\mathrm{inv}_K(u_{E/K}) = \frac{1}{[]E:L]}$, which means $u_{E/L} = \mathrm{Res}(u_{E/K})$. So we have shown the following,

Theorem 4.4. *For every finite Galois extension of number fields L/K, $H^2(L/K)$ is cyclic of order $[L : K]$ with a canonical generator given by the fundamental class $u_{L/K}$, compatible under restrictions.*

Although one can prove the reciprocity law in a more direct fashion using our discussion on cyclic cyclotomic extensions, with the fundamental class established, we can also now use Tate's theorem to obtain an isomorphism,

$$\mathrm{Gal}(L/K)^{ab} \to \mathbf{C}_K / \mathrm{Nm}\,\mathbf{C}_L$$

which can be shown to be the inverse to the Artin map.

References

[CFSU67] J. W. S. Cassels, A. Fröhlich, London Mathematical Society, and International Mathematical Union. Algebraic number theory: Proceedings of an instructional conference organized by the london mathematical society (a nato advanced study institute) with the support of the international mathematical union. New York;London;, 1967. Academic Press.

[Mil20] J.S. Milne. Class field theory (v4.03), 2020. Available at www.jmilne.org/math/.