Adèles and cohomology

David Ang

Class field theory

Thursday, 4 July 2024

The fundamental exact sequence

Let E/F be a Galois extension. The **Brauer group** of E/F is given by

$$\mathrm{Br}(E/F) \cong H^2(\mathrm{Gal}(E/F), E^\times).$$

The fundamental exact sequence

Let E/F be a Galois extension. The **Brauer group** of E/F is given by

$$\mathrm{Br}(E/F) \cong H^2(\mathrm{Gal}(E/F), E^\times).$$

Theorem (Albert–Brauer–Hasse–Noether)

Let K be a number field. Then there is a short exact sequence

$$0 \to \mathrm{Br}(\overline{K}/K) \to \bigoplus_v \mathrm{Br}(\overline{K_v}/K_v) \to \mathbb{Q}/\mathbb{Z} \to 0.$$

The fundamental exact sequence

Let E/F be a Galois extension. The **Brauer group** of E/F is given by

$$\mathrm{Br}(E/F) \cong H^2(\mathrm{Gal}(E/F), E^\times).$$

Theorem (Albert–Brauer–Hasse–Noether)

Let K be a number field. Then there is a short exact sequence

$$0 \to \mathrm{Br}(\overline{K}/K) \to \bigoplus_v \mathrm{Br}(\overline{K_v}/K_v) \to \mathbb{Q}/\mathbb{Z} \to 0.$$

Why is this the **fundamental exact sequence** of class field theory?

The fundamental exact sequence

Let E/F be a Galois extension. The **Brauer group** of E/F is given by

$$\mathrm{Br}(E/F) \cong H^2(\mathrm{Gal}(E/F), E^\times).$$

Theorem (Albert–Brauer–Hasse–Noether)

Let K be a number field. Then there is a short exact sequence

$$0 \to \mathrm{Br}(\overline{K}/K) \to \bigoplus_v \mathrm{Br}(\overline{K_v}/K_v) \to \mathbb{Q}/\mathbb{Z} \to 0.$$

Why is this the **fundamental exact sequence** of class field theory?

In fact, it suffices to understand

$$0 \to \mathrm{Br}(L/K) \to \bigoplus_v \mathrm{Br}(L_w/K_v) \to \tfrac{1}{\#G}\mathbb{Z}/\mathbb{Z} \to 0,$$

where L/K is a finite cyclic extension with Galois group G.

The idealic reciprocity law

Recall that for a modulus $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ of a number field K,

- $I_K(\mathfrak{m})$ is the ideal group of fractional ideals coprime to $\mathfrak{m}_0$, and
- $P_K(\mathfrak{m})$ is the ray subgroup of principal fractional ideals $\langle\alpha\rangle$ such that $\mathrm{ord}_{\mathfrak{p}}(\alpha - 1) \geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m})$ for all $\mathfrak{p} \mid \mathfrak{m}_0$ and $\sigma(\alpha) > 0$ for all $\sigma \mid \mathfrak{m}_\infty$.

The idealic reciprocity law

Recall that for a modulus $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ of a number field K,

- $I_K(\mathfrak{m})$ is the ideal group of fractional ideals coprime to $\mathfrak{m}_0$, and
- $P_K(\mathfrak{m})$ is the ray subgroup of principal fractional ideals $\langle\alpha\rangle$ such that $\operatorname{ord}_\mathfrak{p}(\alpha - 1) \geq \operatorname{ord}_\mathfrak{p}(\mathfrak{m})$ for all $\mathfrak{p} \mid \mathfrak{m}_0$ and $\sigma(\alpha) > 0$ for all $\sigma \mid \mathfrak{m}_\infty$.

Theorem (global reciprocity)

Let L/K be a finite abelian extension of number fields with Galois group G. Then there is a surjective **global Artin map**

$$\Phi_{L/K} : I_K(\mathfrak{m})/P_K(\mathfrak{m}) \twoheadrightarrow G,$$

with kernel precisely $\operatorname{Nm}(I_L(\mathfrak{m}))$, where $\mathfrak{m}$ consists of all ramified primes.

The idealic reciprocity law

Recall that for a modulus $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ of a number field K,

- $I_K(\mathfrak{m})$ is the ideal group of fractional ideals coprime to $\mathfrak{m}_0$, and
- $P_K(\mathfrak{m})$ is the ray subgroup of principal fractional ideals $\langle\alpha\rangle$ such that $\mathrm{ord}_\mathfrak{p}(\alpha - 1) \geq \mathrm{ord}_\mathfrak{p}(\mathfrak{m})$ for all $\mathfrak{p} \mid \mathfrak{m}_0$ and $\sigma(\alpha) > 0$ for all $\sigma \mid \mathfrak{m}_\infty$.

Theorem (global reciprocity)

Let L/K be a finite abelian extension of number fields with Galois group G. Then there is a surjective **global Artin map**

$$\Phi_{L/K} : I_K(\mathfrak{m})/P_K(\mathfrak{m}) \twoheadrightarrow G,$$

with kernel precisely $\mathrm{Nm}(I_L(\mathfrak{m}))$, where $\mathfrak{m}$ consists of all ramified primes.

Theorem (local reciprocity)

Let L_w/K_v be a finite abelian extension of non-archimedean local fields with Galois group G_v. Then there is a surjective **local Artin map**

$$\phi_{L_w/K_v} : K_v^\times \twoheadrightarrow G_v,$$

with kernel precisely $\mathrm{Nm}(L_w^\times)$.

Idèles

The **idèle group** of K is defined by

$$\mathcal{I}_K := \left\{ (a_v)_v \in \prod_v K_v^\times \;\middle|\; a_v \in \mathcal{O}_v^\times \text{ for almost all } v \right\}.$$

Idèles

The **idèle group** of K is defined by

$$\mathcal{I}_K := \left\{ (a_v)_v \in \prod_v K_v^\times \;\middle|\; a_v \in \mathcal{O}_v^\times \text{ for almost all } v \right\}.$$

It is a topological group under the restricted product topology, where a basis of open sets is given by the open sets of the product

$$\prod_{v \in S} K_v^\times \times \prod_{v \notin S} \mathcal{O}_v^\times,$$

where S is a finite set of places of K containing the archimedean places.

Idèles

The **idèle group** of K is defined by

$$\mathcal{I}_K := \left\{ (a_v)_v \in \prod_v K_v^\times \;\middle|\; a_v \in \mathcal{O}_v^\times \text{ for almost all } v \right\}.$$

It is a topological group under the restricted product topology, where a basis of open sets is given by the open sets of the product

$$\prod_{v \in S} K_v^\times \times \prod_{v \notin S} \mathcal{O}_v^\times,$$

where S is a finite set of places of K containing the archimedean places.

There is a natural diagonal embedding $\Delta : K^\times \hookrightarrow \mathcal{I}_K$, whose image is the **principal idèle subgroup**, and whose cokernel is the **idèle class group**

$$\mathcal{C}_K := \mathcal{I}_K / \Delta(K^\times).$$

The idèlic reciprocity law

Theorem (idèlic reciprocity)

Let L/K be a finite abelian extension of number fields with Galois group G.

The idèlic reciprocity law

Theorem (idèlic reciprocity)

Let L/K be a finite abelian extension of number fields with Galois group G. Then there is a unique continuous surjection $\widetilde{\Psi}_{L/K} : \mathcal{I}_K \twoheadrightarrow G$, such that for all places $w \mid v$, there is a commutative square

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\phi_{L_w/K_v}} & G_v \\ \big\downarrow & & \big\downarrow \\ \mathcal{I}_K & \xrightarrow[\widetilde{\Psi}_{L/K}]{} & G \end{array} .$$

The idèlic reciprocity law

Theorem (idèlic reciprocity)

Let L/K be a finite abelian extension of number fields with Galois group G. Then there is a unique continuous surjection $\widetilde{\Psi}_{L/K} : \mathcal{I}_K \twoheadrightarrow G$, such that for all places $w \mid v$, there is a commutative square

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\phi_{L_w/K_v}} & G_v \\ \big\downarrow & & \big\downarrow \\ \mathcal{I}_K & \xrightarrow[\widetilde{\Psi}_{L/K}]{} & G \end{array} .$$

Furthermore, it descends to a surjective **idèlic Artin map**

$$\Psi_{L/K} : \mathcal{C}_K \twoheadrightarrow G,$$

with kernel precisely $\mathrm{Nm}(\mathcal{C}_L)$.

The idèlic reciprocity law

Theorem (idèlic reciprocity)

Let L/K be a finite abelian extension of number fields with Galois group G. Then there is a unique continuous surjection $\widetilde{\Psi}_{L/K} : \mathcal{I}_K \twoheadrightarrow G$, such that for all places $w \mid v$, there is a commutative square

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\phi_{L_w/K_v}} & G_v \\ \downarrow & & \downarrow \\ \mathcal{I}_K & \xrightarrow[\widetilde{\Psi}_{L/K}]{} & G \end{array} .$$

Furthermore, it descends to a surjective **idèlic Artin map**

$$\Psi_{L/K} : \mathcal{C}_K \twoheadrightarrow G,$$

with kernel precisely $\mathrm{Nm}(\mathcal{C}_L)$.

Note that $\Psi_{L/K}(a_v) = \mathrm{Fr}_v^{-\mathrm{ord}_v(a_v)}$ for all unramified places v of K.

The idèlic Artin map

Example ($K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_{15})$)

There is an isomorphism of topological groups

$$\begin{array}{cccccccc} \mathcal{I}_{\mathbb{Q}} & \xrightarrow{\sim} & \mathbb{Q}^\times & \times & \mathbb{R}^+ & \times & \prod_p \mathbb{Z}_p^\times \\ (a_\infty, a_2, a_3, a_5, \dots) & \longmapsto & \frac{a_\infty}{|a_\infty|} d & & |a_\infty| & & (\frac{a_2}{d}, \frac{a_3}{d}, \frac{a_5}{d}, \dots) \end{array},$$

where $d := \prod_p p^{\mathrm{ord}_p(a_p)}$.

The idèlic Artin map

Example ($K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_{15})$)

There is an isomorphism of topological groups

$$\begin{array}{ccccccc} \mathcal{I}_{\mathbb{Q}} & \xrightarrow{\sim} & \mathbb{Q}^\times & \times & \mathbb{R}^+ & \times & \prod_p \mathbb{Z}_p^\times \\ (a_\infty, a_2, a_3, a_5, \dots) & \longmapsto & \frac{a_\infty}{|a_\infty|} d & & |a_\infty| & & (\frac{a_2}{d}, \frac{a_3}{d}, \frac{a_5}{d}, \dots) \end{array},$$

where $d := \prod_p p^{\mathrm{ord}_p(a_p)}$. This induces:

$$\mathcal{C}_{\mathbb{Q}} \xrightarrow{\sim} \mathbb{R}^+ \times \prod_p \mathbb{Z}_p^\times$$

The idèlic Artin map

Example ($K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_{15})$)

There is an isomorphism of topological groups

$$\begin{array}{ccccccc} \mathcal{I}_{\mathbb{Q}} & \xrightarrow{\sim} & \mathbb{Q}^{\times} & \times & \mathbb{R}^{+} & \times & \prod_p \mathbb{Z}_p^{\times} \\ (a_\infty, a_2, a_3, a_5, \dots) & \longmapsto & \frac{a_\infty}{|a_\infty|} d & & |a_\infty| & & (\frac{a_2}{d}, \frac{a_3}{d}, \frac{a_5}{d}, \dots) \end{array},$$

where $d := \prod_p p^{\mathrm{ord}_p(a_p)}$. This induces:

$$\mathcal{C}_{\mathbb{Q}} \xrightarrow{\sim} \mathbb{R}^{+} \times \prod_p \mathbb{Z}_p^{\times} \longrightarrow\!\!\!\!\rightarrow \mathbb{Z}_3^{\times} \times \mathbb{Z}_5^{\times}$$

The idèlic Artin map

Example ($K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_{15})$)

There is an isomorphism of topological groups

$$\begin{array}{ccccccc} \mathcal{I}_{\mathbb{Q}} & \xrightarrow{\sim} & \mathbb{Q}^\times & \times & \mathbb{R}^+ & \times & \prod_p \mathbb{Z}_p^\times \\ (a_\infty, a_2, a_3, a_5, \dots) & \longmapsto & \frac{a_\infty}{|a_\infty|} d & & |a_\infty| & & (\frac{a_2}{d}, \frac{a_3}{d}, \frac{a_5}{d}, \dots) \end{array},$$

where $d := \prod_p p^{\mathrm{ord}_p(a_p)}$. This induces:

$$\mathcal{C}_{\mathbb{Q}} \xrightarrow{\sim} \mathbb{R}^+ \times \prod_p \mathbb{Z}_p^\times \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}_3^\times \times \mathbb{Z}_5^\times \longrightarrow\!\!\!\!\!\rightarrow (\mathbb{Z}_3/3\mathbb{Z}_3)^\times \times (\mathbb{Z}_5/5\mathbb{Z}_5)^\times$$

The idèlic Artin map

Example ($K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_{15})$)

There is an isomorphism of topological groups

$$\begin{array}{ccccccc} \mathcal{I}_{\mathbb{Q}} & \xrightarrow{\sim} & \mathbb{Q}^\times & \times & \mathbb{R}^+ & \times & \prod_p \mathbb{Z}_p^\times \\ (a_\infty, a_2, a_3, a_5, \dots) & \longmapsto & \frac{a_\infty}{|a_\infty|} d & & |a_\infty| & & (\frac{a_2}{d}, \frac{a_3}{d}, \frac{a_5}{d}, \dots) \end{array},$$

where $d := \prod_p p^{\mathrm{ord}_p(a_p)}$. This induces:

$$\begin{array}{c} \mathcal{C}_{\mathbb{Q}} \xrightarrow{\sim} \mathbb{R}^+ \times \prod_p \mathbb{Z}_p^\times \twoheadrightarrow \mathbb{Z}_3^\times \times \mathbb{Z}_5^\times \twoheadrightarrow (\mathbb{Z}_3/3\mathbb{Z}_3)^\times \times (\mathbb{Z}_5/5\mathbb{Z}_5)^\times \\ \downarrow \wr \\ (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \end{array}$$

The idèlic Artin map

Example ($K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_{15})$)

There is an isomorphism of topological groups

$$\begin{array}{ccccccc} \mathcal{I}_{\mathbb{Q}} & \xrightarrow{\sim} & \mathbb{Q}^{\times} & \times & \mathbb{R}^{+} & \times & \prod_p \mathbb{Z}_p^{\times} \\ (a_\infty, a_2, a_3, a_5, \dots) & \longmapsto & \frac{a_\infty}{|a_\infty|} d & & |a_\infty| & & \left(\frac{a_2}{d}, \frac{a_3}{d}, \frac{a_5}{d}, \dots\right) \end{array},$$

where $d := \prod_p p^{\mathrm{ord}_p(a_p)}$. This induces:

$$\begin{array}{ccc} \mathcal{C}_{\mathbb{Q}} \xrightarrow{\sim} \mathbb{R}^{+} \times \prod_p \mathbb{Z}_p^{\times} \longrightarrow\!\!\!\!\rightarrow \mathbb{Z}_3^{\times} \times \mathbb{Z}_5^{\times} \longrightarrow\!\!\!\!\rightarrow & (\mathbb{Z}_3/3\mathbb{Z}_3)^{\times} \times (\mathbb{Z}_5/5\mathbb{Z}_5)^{\times} \\ & \downarrow \wr \\ (\mathbb{Z}/15\mathbb{Z})^{\times} \xleftarrow[\sim]{} & (\mathbb{Z}/3\mathbb{Z})^{\times} \times (\mathbb{Z}/5\mathbb{Z})^{\times} \end{array}$$

The idèlic Artin map

Example ($K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_{15})$)

There is an isomorphism of topological groups

$$\begin{array}{ccccccc} \mathcal{I}_{\mathbb{Q}} & \xrightarrow{\sim} & \mathbb{Q}^\times & \times & \mathbb{R}^+ & \times & \prod_p \mathbb{Z}_p^\times \\ (a_\infty, a_2, a_3, a_5, \dots) & \longmapsto & \frac{a_\infty}{|a_\infty|} d & & |a_\infty| & & \left(\frac{a_2}{d}, \frac{a_3}{d}, \frac{a_5}{d}, \dots\right) \end{array},$$

where $d := \prod_p p^{\mathrm{ord}_p(a_p)}$. This induces:

$$\begin{array}{ccc} \mathcal{C}_{\mathbb{Q}} \xrightarrow{\sim} \mathbb{R}^+ \times \prod_p \mathbb{Z}_p^\times \twoheadrightarrow \mathbb{Z}_3^\times \times \mathbb{Z}_5^\times & \twoheadrightarrow & (\mathbb{Z}_3/3\mathbb{Z}_3)^\times \times (\mathbb{Z}_5/5\mathbb{Z}_5)^\times \\ & & \downarrow \wr \\ \mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q}) \xleftarrow{\sim} (\mathbb{Z}/15\mathbb{Z})^\times & \xleftarrow{\sim} & (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \end{array}$$

The idèlic Artin map

Example ($K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_{15})$)

There is an isomorphism of topological groups

$$
\begin{array}{ccccccc}
\mathcal{I}_{\mathbb{Q}} & \xrightarrow{\sim} & \mathbb{Q}^{\times} & \times & \mathbb{R}^{+} & \times & \prod_{p} \mathbb{Z}_p^{\times} \\
(a_\infty, a_2, a_3, a_5, \ldots) & \longmapsto & \frac{a_\infty}{|a_\infty|} d & & |a_\infty| & & \left(\frac{a_2}{d}, \frac{a_3}{d}, \frac{a_5}{d}, \ldots\right)
\end{array},
$$

where $d := \prod_p p^{\mathrm{ord}_p(a_p)}$. This induces:

$$
\begin{array}{ccccccc}
\mathcal{C}_{\mathbb{Q}} & \xrightarrow{\sim} & \mathbb{R}^{+} \times \prod_p \mathbb{Z}_p^{\times} & \twoheadrightarrow & \mathbb{Z}_3^{\times} \times \mathbb{Z}_5^{\times} & \twoheadrightarrow & (\mathbb{Z}_3/3\mathbb{Z}_3)^{\times} \times (\mathbb{Z}_5/5\mathbb{Z}_5)^{\times} \\
& \searrow^{\Psi_{\mathbb{Q}(\zeta_{15})/\mathbb{Q}}} & & & & & \downarrow \wr \\
& & \mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q}) & \xleftarrow{\sim} & (\mathbb{Z}/15\mathbb{Z})^{\times} & \xleftarrow{\sim} & (\mathbb{Z}/3\mathbb{Z})^{\times} \times (\mathbb{Z}/5\mathbb{Z})^{\times}
\end{array}
$$

The idèlic Artin map

Example ($K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_{15})$)

There is an isomorphism of topological groups

$$\begin{array}{ccccccc} \mathcal{I}_{\mathbb{Q}} & \xrightarrow{\sim} & \mathbb{Q}^\times & \times & \mathbb{R}^+ & \times & \prod_p \mathbb{Z}_p^\times \\ (a_\infty, a_2, a_3, a_5, \dots) & \longmapsto & \frac{a_\infty}{|a_\infty|} d & & |a_\infty| & & (\frac{a_2}{d}, \frac{a_3}{d}, \frac{a_5}{d}, \dots) \end{array},$$

where $d := \prod_p p^{\mathrm{ord}_p(a_p)}$. This induces:

$$\begin{array}{ccccccc} \mathcal{C}_{\mathbb{Q}} & \xrightarrow{\sim} & \mathbb{R}^+ \times \prod_p \mathbb{Z}_p^\times & \twoheadrightarrow & \mathbb{Z}_3^\times \times \mathbb{Z}_5^\times & \twoheadrightarrow & (\mathbb{Z}_3/3\mathbb{Z}_3)^\times \times (\mathbb{Z}_5/5\mathbb{Z}_5)^\times \\ & \searrow^{\Psi_{\mathbb{Q}(\zeta_{15})/\mathbb{Q}}} & & & & & \downarrow \sim \\ & & \mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q}) & \xleftarrow{\sim} & (\mathbb{Z}/15\mathbb{Z})^\times & \xleftarrow{\sim} & (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \end{array}$$

The idèlic Artin map $\Psi_{\mathbb{Q}(\zeta_{15})/\mathbb{Q}} : \mathcal{C}_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q})$ maps the idèle class $[(1, 2, 1, 1, \dots)]$ to the automorphism $\zeta_{15} \mapsto \zeta_{15}^{1/2}$.

The content map

There is a surjective **content map** $\widetilde{c} : \mathcal{I}_K \twoheadrightarrow I_K$ that maps an idèle $(a_v)_v$ to the ideal $\prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(a_{\mathfrak{p}})}$, which descends to a surjection $c : \mathcal{C}_K \twoheadrightarrow I_K / P_K$.

The content map

There is a surjective **content map** $\widetilde{c} : \mathcal{I}_K \twoheadrightarrow I_K$ that maps an idèle $(a_v)_v$ to the ideal $\prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(a_{\mathfrak{p}})}$, which descends to a surjection $c : \mathcal{C}_K \twoheadrightarrow I_K/P_K$.

Lemma

Let G be a finite abelian group, and let $\mathfrak{m}$ be a modulus of a number field K. Then any homomorphism $\Phi_K : I_K(\mathfrak{m}) \to G$ induces a unique continuous homomorphism $\Psi_K : \mathcal{C}_K \to G$ such that

$$\Psi_K((a_v)_v) = \Phi_K(c((a_v)_v)),$$

for any $(a_v)_v \in \mathcal{I}_K$ such that $a_v = 1$ for all $v \mid \mathfrak{m}$.

The content map

There is a surjective **content map** $\widetilde{c} : \mathcal{I}_K \twoheadrightarrow I_K$ that maps an idèle $(a_v)_v$ to the ideal $\prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(a_{\mathfrak{p}})}$, which descends to a surjection $c : \mathcal{C}_K \twoheadrightarrow I_K/P_K$.

Lemma

Let G be a finite abelian group, and let $\mathfrak{m}$ be a modulus of a number field K. Then any homomorphism $\Phi_K : I_K(\mathfrak{m}) \to G$ induces a unique continuous homomorphism $\Psi_K : \mathcal{C}_K \to G$ such that

$$\Psi_K((a_v)_v) = \Phi_K(c((a_v)_v)),$$

for any $(a_v)_v \in \mathcal{I}_K$ such that $a_v = 1$ for all $v \mid \mathfrak{m}$. Furthermore, any continuous homomorphism $\Psi_K : \mathcal{C}_K \to G$ arises in such a way.

The content map

There is a surjective **content map** $\widetilde{c} : \mathcal{I}_K \twoheadrightarrow I_K$ that maps an idèle $(a_v)_v$ to the ideal $\prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(a_{\mathfrak{p}})}$, which descends to a surjection $c : \mathcal{C}_K \twoheadrightarrow I_K/P_K$.

Lemma

Let G be a finite abelian group, and let $\mathfrak{m}$ be a modulus of a number field K. Then any homomorphism $\Phi_K : I_K(\mathfrak{m}) \to G$ induces a unique continuous homomorphism $\Psi_K : \mathcal{C}_K \to G$ such that

$$\Psi_K((a_v)_v) = \Phi_K(c((a_v)_v)),$$

for any $(a_v)_v \in \mathcal{I}_K$ such that $a_v = 1$ for all $v \mid \mathfrak{m}$. Furthermore, any continuous homomorphism $\Psi_K : \mathcal{C}_K \to G$ arises in such a way.

Since Ψ_K is a homomorphism, it is determined by idèles of the form

$$(\dots, 1, 1, \underset{v}{a}, 1, 1, \dots),$$

where a is either a unit or a uniformiser if v is non-archimedean.

Characters of ideals and idèles

Example ($\Phi_{\mathbb{Q}} : I_{\mathbb{Q}}(3\infty) \to \mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$)

Characters of ideals and idèles

Example ($\Phi_{\mathbb{Q}} : I_{\mathbb{Q}}(3\infty) \to \mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$)

For brevity, denote $\{a\} := (\dots, 1, 1, \underset{v}{a}, 1, 1, \dots)$.

Characters of ideals and idèles

Example ($\Phi_{\mathbb{Q}} : I_{\mathbb{Q}}(3\infty) \to \mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$)

For brevity, denote $\{a\} := (\dots, 1, 1, \underset{v}{a}, 1, 1, \dots)$.

- Let $v = p \neq 3, \infty$ and $a = up$.

Characters of ideals and idèles

Example ($\Phi_{\mathbb{Q}} : I_{\mathbb{Q}}(3\infty) \to \mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$)

For brevity, denote $\{a\} := (\ldots, 1, 1, \underset{v}{a}, 1, 1, \ldots)$.

- Let $v = p \neq 3, \infty$ and $a = up$. Then $\{up\}_3 = \{up\}_\infty = 1$, so

$$\Psi_{\mathbb{Q}}(\{up\}) = \Phi_{\mathbb{Q}}(c(\{up\})) = \Phi_{\mathbb{Q}}(p^{\mathrm{ord}_p(up)}) = \Phi_{\mathbb{Q}}(p) = (\zeta_3 \mapsto \zeta_3^p).$$

Characters of ideals and idèles

Example ($\Phi_{\mathbb{Q}} : I_{\mathbb{Q}}(3\infty) \to \mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$)

For brevity, denote $\{a\} := (\ldots, 1, 1, \underset{v}{a}, 1, 1, \ldots)$.

- Let $v = p \neq 3, \infty$ and $a = up$. Then $\{up\}_3 = \{up\}_\infty = 1$, so

$$\Psi_{\mathbb{Q}}(\{up\}) = \Phi_{\mathbb{Q}}(c(\{up\})) = \Phi_{\mathbb{Q}}(p^{\mathrm{ord}_p(up)}) = \Phi_{\mathbb{Q}}(p) = (\zeta_3 \mapsto \zeta_3^p).$$

- Let $v = \infty$.

Characters of ideals and idèles

Example ($\Phi_{\mathbb{Q}} : I_{\mathbb{Q}}(3\infty) \to \mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$)

For brevity, denote $\{a\} := (\dots, 1, 1, \underset{v}{a}, 1, 1, \dots)$.

- Let $v = p \neq 3, \infty$ and $a = up$. Then $\{up\}_3 = \{up\}_\infty = 1$, so

$$\Psi_{\mathbb{Q}}(\{up\}) = \Phi_{\mathbb{Q}}(c(\{up\})) = \Phi_{\mathbb{Q}}(p^{\mathrm{ord}_p(up)}) = \Phi_{\mathbb{Q}}(p) = (\zeta_3 \mapsto \zeta_3^p).$$

- Let $v = \infty$. Then $\Psi_{\mathbb{Q}}(\{a\}) = \Psi_{\mathbb{Q}}(\Delta(\frac{a}{|a|}) \cdot \{a\}) = 1$, since

$$\Delta(\tfrac{a}{|a|}) \cdot \{a\} = (\dots, \tfrac{a}{|a|}, \tfrac{a}{|a|}, \underset{\infty}{\tfrac{a}{|a|}a}, \tfrac{a}{|a|}, \tfrac{a}{|a|}, \dots),$$

and $\mathbb{R}^+$ is connected while $\mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$ is discrete.

Characters of ideals and idèles

Example ($\Phi_{\mathbb{Q}} : I_{\mathbb{Q}}(3\infty) \to \mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$)

For brevity, denote $\{a\} := (\ldots, 1, 1, \underset{v}{a}, 1, 1, \ldots)$.

- Let $v = p \neq 3, \infty$ and $a = up$. Then $\{up\}_3 = \{up\}_\infty = 1$, so

$$\Psi_{\mathbb{Q}}(\{up\}) = \Phi_{\mathbb{Q}}(c(\{up\})) = \Phi_{\mathbb{Q}}(p^{\mathrm{ord}_p(up)}) = \Phi_{\mathbb{Q}}(p) = (\zeta_3 \mapsto \zeta_3^p).$$

- Let $v = \infty$. Then $\Psi_{\mathbb{Q}}(\{a\}) = \Psi_{\mathbb{Q}}(\Delta(\frac{a}{|a|}) \cdot \{a\}) = 1$, since

$$\Delta(\tfrac{a}{|a|}) \cdot \{a\} = (\ldots, \tfrac{a}{|a|}, \tfrac{a}{|a|}, \underset{\infty}{\tfrac{a}{|a|}a}, \tfrac{a}{|a|}, \tfrac{a}{|a|}, \ldots),$$

  and $\mathbb{R}^+$ is connected while $\mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$ is discrete.
- Let $v = 3$ and $a = 3$.

Characters of ideals and idèles

Example ($\Phi_{\mathbb{Q}} : I_{\mathbb{Q}}(3\infty) \to \mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$)

For brevity, denote $\{a\} := (\ldots, 1, 1, \underset{v}{a}, 1, 1, \ldots)$.

- Let $v = p \neq 3, \infty$ and $a = up$. Then $\{up\}_3 = \{up\}_\infty = 1$, so

$$\Psi_{\mathbb{Q}}(\{up\}) = \Phi_{\mathbb{Q}}(c(\{up\})) = \Phi_{\mathbb{Q}}(p^{\mathrm{ord}_p(up)}) = \Phi_{\mathbb{Q}}(p) = (\zeta_3 \mapsto \zeta_3^p).$$

- Let $v = \infty$. Then $\Psi_{\mathbb{Q}}(\{a\}) = \Psi_{\mathbb{Q}}(\Delta(\frac{a}{|a|}) \cdot \{a\}) = 1$, since

$$\Delta(\tfrac{a}{|a|}) \cdot \{a\} = (\ldots, \tfrac{a}{|a|}, \tfrac{a}{|a|}, \underset{\infty}{\tfrac{a}{|a|}a}, \tfrac{a}{|a|}, \tfrac{a}{|a|}, \ldots),$$

  and $\mathbb{R}^+$ is connected while $\mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$ is discrete.

- Let $v = 3$ and $a = 3$. Then $\Psi_{\mathbb{Q}}(\{3\}) = \Psi_{\mathbb{Q}}(\Delta(\frac{1}{3}) \cdot \{3\}) = 1$, since

$$\Delta(\tfrac{1}{3}) \cdot \{3\} = (\ldots, \tfrac{1}{3}, \tfrac{1}{3}, \underset{3}{1}, \tfrac{1}{3}, \tfrac{1}{3}, \ldots),$$

  and $\Psi_{\mathbb{Q}}(\{1\}) = 1$.

Characters of ideals and idèles

Example ($\Phi_{\mathbb{Q}} : I_{\mathbb{Q}}(3\infty) \to \mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$)

For brevity, denote $\{a\} := (\ldots, 1, 1, \underset{v}{a}, 1, 1, \ldots)$.

- Let $v = 3$ and $a = 2$.

Characters of ideals and idèles

Example ($\Phi_{\mathbb{Q}} : I_{\mathbb{Q}}(3\infty) \to \mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$)

For brevity, denote $\{a\} := (\dots, 1, 1, \underset{v}{a}, 1, 1, \dots)$.

- Let $v = 3$ and $a = 2$. It suffices to find a prime $p \in \mathbb{Z}$ such that

$$\Delta(p) \cdot \{2\} = (\dots, p, p, \underset{3}{2p}, \underset{p}{1}, p, p, \dots) \cdot (\dots, 1, 1, \underset{p}{p}, 1, 1, \dots),$$

  and that $2p \to 1$ in $\mathbb{Z}_3$, so that $\Psi_{\mathbb{Q}}(\{2p\}) = 1$ by continuity.

Characters of ideals and idèles

Example ($\Phi_{\mathbb{Q}} : I_{\mathbb{Q}}(3\infty) \to \mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$)

For brevity, denote $\{a\} := (\ldots, 1, 1, \underset{v}{a}, 1, 1, \ldots)$.

- Let $v = 3$ and $a = 2$. It suffices to find a prime $p \in \mathbb{Z}$ such that

  $$\Delta(p) \cdot \{2\} = (\ldots, p, p, \underset{3}{2p}, \underset{p}{1}, p, p, \ldots) \cdot (\ldots, 1, 1, \underset{p}{p}, 1, 1, \ldots),$$

  and that $2p \to 1$ in $\mathbb{Z}_3$, so that $\Psi_{\mathbb{Q}}(\{2p\}) = 1$ by continuity. Then

  $$\Psi_{\mathbb{Q}}(\{2\}) = \Phi_{\mathbb{Q}}(p) = (\zeta_3 \mapsto \zeta_3^p) = (\zeta_3 \mapsto \zeta_3^2),$$

  which does not depend on p.

Characters of ideals and idèles

Example ($\Phi_{\mathbb{Q}} : I_{\mathbb{Q}}(3\infty) \to \mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$)

For brevity, denote $\{a\} := (\ldots, 1, 1, \underset{v}{a}, 1, 1, \ldots)$.

- Let $v = 3$ and $a = 2$. It suffices to find a prime $p \in \mathbb{Z}$ such that

$$\Delta(p) \cdot \{2\} = (\ldots, p, p, \underset{3}{2p}, \underset{p}{1}, p, p, \ldots) \cdot (\ldots, 1, 1, \underset{p}{p}, 1, 1, \ldots),$$

and that $2p \to 1$ in $\mathbb{Z}_3$, so that $\Psi_{\mathbb{Q}}(\{2p\}) = 1$ by continuity. Then

$$\Psi_{\mathbb{Q}}(\{2\}) = \Phi_{\mathbb{Q}}(p) = (\zeta_3 \mapsto \zeta_3^p) = (\zeta_3 \mapsto \zeta_3^2),$$

which does not depend on p. Now $\frac{1}{2} = 2 + \sum_{i=1}^{\infty} 3^i$ in $\mathbb{Z}_3$, so set

$$p := 2 + \sum_{i=1}^{15} 3^i = 21523361,$$

which is prime in $\mathbb{Z}$, and $2p = 1 + 3^{16} \to 1$ in $\mathbb{Z}_3$.

Group cohomology

Let G be a finite group, and let M be a G-module. Recall that group cohomology $H^i(G, -)$ is the right derived functor of $(-)^G$, where

$$M^G := \{m \in M \mid g \cdot m - m = 0 \text{ for all } g \in G\}.$$

Group cohomology

Let G be a finite group, and let M be a G-module. Recall that group cohomology $H^i(G, -)$ is the right derived functor of $(-)^G$, where

$$M^G := \{m \in M \mid g \cdot m - m = 0 \text{ for all } g \in G\}.$$

The low-dimensional cohomology groups can be made explicit.

Group cohomology

Let G be a finite group, and let M be a G-module. Recall that group cohomology $H^i(G, -)$ is the right derived functor of $(-)^G$, where

$$M^G := \{m \in M \mid g \cdot m - m = 0 \text{ for all } g \in G\}.$$

The low-dimensional cohomology groups can be made explicit.

- $H^0(G, M)$ is just M^G.

Group cohomology

Let G be a finite group, and let M be a G-module. Recall that group cohomology $H^i(G, -)$ is the right derived functor of $(-)^G$, where

$$M^G := \{m \in M \mid g \cdot m - m = 0 \text{ for all } g \in G\}.$$

The low-dimensional cohomology groups can be made explicit.

- $H^0(G, M)$ is just M^G.
- $H^1(G, M)$ consists of 1-cocycles $f : G \to M$ such that

$$g \cdot f(h) - f(gh) + f(g) = 0, \qquad g, h \in G,$$

  modulo 1-coboundaries given by $g \mapsto g \cdot m - m$ for some $m \in M$.

Group cohomology

Let G be a finite group, and let M be a G-module. Recall that group cohomology $H^i(G,-)$ is the right derived functor of $(-)^G$, where

$$M^G := \{m \in M \mid g \cdot m - m = 0 \text{ for all } g \in G\}.$$

The low-dimensional cohomology groups can be made explicit.

- $H^0(G,M)$ is just M^G.
- $H^1(G,M)$ consists of 1-cocycles $f : G \to M$ such that

  $$g \cdot f(h) - f(gh) + f(g) = 0, \qquad g,h \in G,$$

  modulo 1-coboundaries given by $g \mapsto g \cdot m - m$ for some $m \in M$.
- $H^2(G,M)$ consists of 2-cocycles $f : G \times G \to M$ such that

  $$g \cdot f(h,k) - f(gh,k) + f(g,hk) - f(g,h) = 0, \qquad g,h,k \in G,$$

  modulo 2-coboundaries given by $(g,h) \mapsto g \cdot f(h) - f(gh) + f(g)$ for some $f : G \to M$.

The long exact sequence

A short exact sequence of G-modules $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ induces a long exact sequence of cohomology groups

$$\cdots \to H^1(G, B) \xrightarrow{\overline{g}} H^1(G, C) \xrightarrow{\delta} H^2(G, A) \xrightarrow{\overline{f}} H^2(G, B) \to \ldots .$$

The long exact sequence

A short exact sequence of G-modules $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ induces a long exact sequence of cohomology groups

$$\cdots \to H^1(G,B) \xrightarrow{\overline{g}} H^1(G,C) \xrightarrow{\delta} H^2(G,A) \xrightarrow{\overline{f}} H^2(G,B) \to \ldots .$$

For a 1-cocycle $f \in H^1(G,C)$, the 2-cocycle $\delta(f) \in H^2(G,A)$ is given by $(g,h) \mapsto g \cdot \widetilde{f}(h) - \widetilde{f}(gh) + \widetilde{f}(g)$, where $\widetilde{f} : G \to B$ is any lift of f.

The long exact sequence

A short exact sequence of G-modules $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ induces a long exact sequence of cohomology groups

$$\cdots \to H^1(G, B) \xrightarrow{\overline{g}} H^1(G, C) \xrightarrow{\delta} H^2(G, A) \xrightarrow{\overline{f}} H^2(G, B) \to \dots.$$

For a 1-cocycle $f \in H^1(G, C)$, the 2-cocycle $\delta(f) \in H^2(G, A)$ is given by $(g, h) \mapsto g \cdot \widetilde{f}(h) - \widetilde{f}(gh) + \widetilde{f}(g)$, where $\widetilde{f} : G \to B$ is any lift of f.

Example ($G = \{1, \sigma, \sigma^2\}$ trivial on $0 \to \mathbb{Z} \xrightarrow{\iota} \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$)

The long exact sequence

A short exact sequence of G-modules $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ induces a long exact sequence of cohomology groups

$$\cdots \to H^1(G,B) \xrightarrow{\overline{g}} H^1(G,C) \xrightarrow{\delta} H^2(G,A) \xrightarrow{\overline{f}} H^2(G,B) \to \ldots.$$

For a 1-cocycle $f \in H^1(G,C)$, the 2-cocycle $\delta(f) \in H^2(G,A)$ is given by $(g,h) \mapsto g \cdot \widetilde{f}(h) - \widetilde{f}(gh) + \widetilde{f}(g)$, where $\widetilde{f} : G \to B$ is any lift of f.

Example ($G = \{1, \sigma, \sigma^2\}$ trivial on $0 \to \mathbb{Z} \xrightarrow{\iota} \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$)

Let $f \in H^1(G, \mathbb{Q}/\mathbb{Z})$ be given by $\sigma \mapsto [\frac{1}{3}]$.

The long exact sequence

A short exact sequence of G-modules $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ induces a long exact sequence of cohomology groups

$$\cdots \to H^1(G,B) \xrightarrow{\overline{g}} H^1(G,C) \xrightarrow{\delta} H^2(G,A) \xrightarrow{\overline{f}} H^2(G,B) \to \dots.$$

For a 1-cocycle $f \in H^1(G,C)$, the 2-cocycle $\delta(f) \in H^2(G,A)$ is given by $(g,h) \mapsto g \cdot \widetilde{f}(h) - \widetilde{f}(gh) + \widetilde{f}(g)$, where $\widetilde{f} : G \to B$ is any lift of f.

Example ($G = \{1, \sigma, \sigma^2\}$ trivial on $0 \to \mathbb{Z} \xrightarrow{\iota} \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$)

Let $f \in H^1(G, \mathbb{Q}/\mathbb{Z})$ be given by $\sigma \mapsto [\frac{1}{3}]$. Let $\widetilde{f} : G \to \mathbb{Q}$ be the lift of f given by $\sigma \mapsto \frac{1}{3}$.

The long exact sequence

A short exact sequence of G-modules $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ induces a long exact sequence of cohomology groups

$$\cdots \to H^1(G,B) \xrightarrow{\overline{g}} H^1(G,C) \xrightarrow{\delta} H^2(G,A) \xrightarrow{\overline{f}} H^2(G,B) \to \dots.$$

For a 1-cocycle $f \in H^1(G,C)$, the 2-cocycle $\delta(f) \in H^2(G,A)$ is given by $(g,h) \mapsto g \cdot \widetilde{f}(h) - \widetilde{f}(gh) + \widetilde{f}(g)$, where $\widetilde{f} : G \to B$ is any lift of f.

Example ($G = \{1, \sigma, \sigma^2\}$ trivial on $0 \to \mathbb{Z} \xrightarrow{\iota} \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$)

Let $f \in H^1(G, \mathbb{Q}/\mathbb{Z})$ be given by $\sigma \mapsto [\frac{1}{3}]$. Let $\widetilde{f} : G \to \mathbb{Q}$ be the lift of f given by $\sigma \mapsto \frac{1}{3}$. Then $\delta(f) \in H^2(G,\mathbb{Z})$ is given by

$$(g,h) \mapsto \begin{cases} 1 & (g,h) = (\sigma,\sigma^2), (\sigma^2,\sigma), (\sigma^2,\sigma^2) \\ 0 & \text{otherwise} \end{cases}.$$

The long exact sequence

A short exact sequence of G-modules $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ induces a long exact sequence of cohomology groups

$$\cdots \to H^1(G,B) \xrightarrow{\overline{g}} H^1(G,C) \xrightarrow{\delta} H^2(G,A) \xrightarrow{\overline{f}} H^2(G,B) \to \dots.$$

For a 1-cocycle $f \in H^1(G,C)$, the 2-cocycle $\delta(f) \in H^2(G,A)$ is given by $(g,h) \mapsto g \cdot \widetilde{f}(h) - \widetilde{f}(gh) + \widetilde{f}(g)$, where $\widetilde{f} : G \to B$ is any lift of f.

Example ($G = \{1, \sigma, \sigma^2\}$ trivial on $0 \to \mathbb{Z} \xrightarrow{\iota} \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$)

Let $f \in H^1(G, \mathbb{Q}/\mathbb{Z})$ be given by $\sigma \mapsto [\frac{1}{3}]$. Let $\widetilde{f} : G \to \mathbb{Q}$ be the lift of f given by $\sigma \mapsto \frac{1}{3}$. Then $\delta(f) \in H^2(G,\mathbb{Z})$ is given by

$$(g,h) \mapsto \begin{cases} 1 & (g,h) = (\sigma,\sigma^2),(\sigma^2,\sigma),(\sigma^2,\sigma^2) \\ 0 & \text{otherwise} \end{cases}.$$

Note that $\mathbb{Q}$ is torsion-free and divisible, so $H^i(G,\mathbb{Q}) = 0$ for all $i > 0$. In particular, there is an isomorphism $\delta : H^1(G,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^2(G,\mathbb{Z})$.

Tate's theorem

Theorem (Tate)

Let M be a G-module, such that for all subgroups $H \leq G$,

T1 $H^1(H, M) = 0$, *and*

T2 $H^2(H, M)$ *is cyclic of order* $\#H$.

Then there is an explicit isomorphism $G^{ab} \xrightarrow{\sim} M^G/\mathrm{Nm}(M)$.

Tate's theorem

Theorem (Tate)

Let M be a G-module, such that for all subgroups $H \leq G$,

T1 $H^1(H, M) = 0$, *and*

T2 $H^2(H, M)$ *is cyclic of order* $\#H$.

Then there is an explicit isomorphism $G^{ab} \xrightarrow{\sim} M^G/\mathrm{Nm}(M)$.

This is the key result in abstract class field theory.

Tate's theorem

Theorem (Tate)

Let M be a G-module, such that for all subgroups $H \leq G$,

T1 $H^1(H, M) = 0$, *and*

T2 $H^2(H, M)$ *is cyclic of order* $\#H$.

Then there is an explicit isomorphism $G^{ab} \xrightarrow{\sim} M^G/\mathrm{Nm}(M)$.

This is the key result in abstract class field theory.

- If $G = \mathrm{Gal}(L_w/K_v)$ and $M = L_w^\times$, this gives the local reciprocity law

$$\mathrm{Gal}(L_w/K_v) \xrightarrow{\sim} K_v^\times/\mathrm{Nm}(L_w^\times).$$

Tate's theorem

Theorem (Tate)

Let M be a G-module, such that for all subgroups $H \leq G$,

T1 $H^1(H, M) = 0$, *and*

T2 $H^2(H, M)$ *is cyclic of order* $\#H$.

Then there is an explicit isomorphism $G^{ab} \xrightarrow{\sim} M^G/\mathrm{Nm}(M)$.

This is the key result in abstract class field theory.

- If $G = \mathrm{Gal}(L_w/K_v)$ and $M = L_w^\times$, this gives the local reciprocity law

$$\mathrm{Gal}(L_w/K_v) \xrightarrow{\sim} K_v^\times/\mathrm{Nm}(L_w^\times).$$

- If $G = \mathrm{Gal}(L/K)$ and $M = \mathcal{C}_L$, this gives the global reciprocity law

$$\mathrm{Gal}(L/K) \xrightarrow{\sim} \mathcal{C}_K/\mathrm{Nm}(\mathcal{C}_L).$$

Cohomology of unramified units

Theorem (local class field theory)

Let L_w/K_v *be a finite unramified extension of non-archimedean local fields with Galois group* G_v*. Then* $H^i(G_v, \mathcal{O}_w^\times) = 0$ *for all* $i > 0$*.*

Cohomology of unramified units

Theorem (local class field theory)

Let L_w/K_v be a finite unramified extension of non-archimedean local fields with Galois group G_v. Then $H^i(G_v, \mathcal{O}_w^\times) = 0$ for all $i > 0$.

The short exact sequence $1 \to \mathcal{O}_w^\times \to L_w^\times \xrightarrow{\mathrm{ord}_w} \mathbb{Z} \to 0$ induces:

$$\overset{0}{\cancel{H^1(G_v, \mathcal{O}_w^\times)}} \longrightarrow H^2(G_v, L_w^\times) \underset{\sim}{\xrightarrow{\mathrm{ord}_w^*}} H^2(G_v, \mathbb{Z}) \longrightarrow \overset{0}{\cancel{H^2(G_v, \mathcal{O}_w^\times)}}$$

Cohomology of unramified units

Theorem (local class field theory)

Let L_w/K_v be a finite unramified extension of non-archimedean local fields with Galois group G_v. Then $H^i(G_v, \mathcal{O}_w^\times) = 0$ for all $i > 0$.

The short exact sequence $1 \to \mathcal{O}_w^\times \to L_w^\times \xrightarrow{\mathrm{ord}_w} \mathbb{Z} \to 0$ induces:

$$
\begin{array}{ccccccc}
 & & & & \overset{0}{\cancel{H^2(G_v, \mathbb{Q})}} & & \\
 & & & & \uparrow & & \\
\overset{0}{\cancel{H^1(G_v, \mathcal{O}_w^\times)}} & \longrightarrow & H^2(G_v, L_w^\times) & \xrightarrow[\sim]{\mathrm{ord}_w^*} & H^2(G_v, \mathbb{Z}) & \longrightarrow & \overset{0}{\cancel{H^2(G_v, \mathcal{O}_w^\times)}} \\
 & & & & \delta\uparrow\wr & & \\
 & & & & H^1(G_v, \mathbb{Q}/\mathbb{Z}) & & \\
 & & & & \uparrow & & \\
 & & & & \underset{0}{\cancel{H^1(G_v, \mathbb{Q})}} & &
\end{array}
$$

Cohomology of unramified units

Theorem (local class field theory)

Let L_w/K_v be a finite unramified extension of non-archimedean local fields with Galois group G_v. Then $H^i(G_v, \mathcal{O}_w^\times) = 0$ for all $i > 0$.

The short exact sequence $1 \to \mathcal{O}_w^\times \to L_w^\times \xrightarrow{\mathrm{ord}_w} \mathbb{Z} \to 0$ induces:

$$\begin{array}{ccccccc}
 & & & & \overset{0}{\cancel{H^2(G_v,\mathbb{Q})}} & & \\
 & & & & \uparrow & & \\
\overset{0}{\cancel{H^1(G_v,\mathcal{O}_w^\times)}} & \longrightarrow & H^2(G_v, L_w^\times) & \xrightarrow[\sim]{\mathrm{ord}_w^*} & H^2(G_v,\mathbb{Z}) & \longrightarrow & \overset{0}{\cancel{H^2(G_v,\mathcal{O}_w^\times)}} \\
 & & & & \delta\uparrow\wr & & \\
 & & & & H^1(G_v,\mathbb{Q}/\mathbb{Z}) & \xrightarrow[\sim]{f\mapsto f(1)} & \frac{1}{\#G_v}\mathbb{Z}/\mathbb{Z} \\
 & & & & \uparrow & & \\
 & & & & \underset{0}{\cancel{H^1(G_v,\mathbb{Q})}} & &
\end{array}$$

Cohomology of unramified units

Theorem (local class field theory)

Let L_w/K_v be a finite unramified extension of non-archimedean local fields with Galois group G_v. Then $H^i(G_v, \mathcal{O}_w^\times) = 0$ for all $i > 0$.

The short exact sequence $1 \to \mathcal{O}_w^\times \to L_w^\times \xrightarrow{\mathrm{ord}_w} \mathbb{Z} \to 0$ induces:

$$
\begin{array}{ccccccc}
 & & & & \overset{0}{\cancel{H^2(G_v, \mathbb{Q})}} & & \\
 & & & & \uparrow & & \\
\overset{0}{\cancel{H^1(G_v, \mathcal{O}_w^\times)}} & \longrightarrow & H^2(G_v, L_w^\times) & \xrightarrow[\sim]{\mathrm{ord}_w^*} & H^2(G_v, \mathbb{Z}) & \longrightarrow & \overset{0}{\cancel{H^2(G_v, \mathcal{O}_w^\times)}} \\
 & & & & \delta\uparrow\sim & & \\
 & & & & H^1(G_v, \mathbb{Q}/\mathbb{Z}) & \xrightarrow[\sim]{f \mapsto f(1)} & \frac{1}{\# G_v}\mathbb{Z}/\mathbb{Z} \\
 & & & & \uparrow & & \\
 & & & & \underset{0}{\cancel{H^1(G_v, \mathbb{Q})}} & &
\end{array}
$$

In particular, T2 holds for $L_w^\times$.

The local invariant map

The **local invariant map** is $\mathrm{inv}_v : H^2(G_v, L_w^\times) \to \frac{1}{\#G_v}\mathbb{Z}/\mathbb{Z}$.

The local invariant map

The **local invariant map** is $\mathrm{inv}_v : H^2(G_v, L_w^\times) \to \frac{1}{\#G_v}\mathbb{Z}/\mathbb{Z}$.

Example ($K_v = \mathbb{Q}_2$ and $L_w = \mathbb{Q}_2(\zeta_7)$)

Note that $G_v = \{1, \sigma, \sigma^2\}$, so that $\frac{1}{\#G_v}\mathbb{Z}/\mathbb{Z} = \{[0], [\frac{1}{3}], [\frac{2}{3}]\}$.

The local invariant map

The **local invariant map** is $\mathrm{inv}_v : H^2(G_v, L_w^\times) \to \frac{1}{\#G_v}\mathbb{Z}/\mathbb{Z}$.

Example ($K_v = \mathbb{Q}_2$ and $L_w = \mathbb{Q}_2(\zeta_7)$)

Note that $G_v = \{1, \sigma, \sigma^2\}$, so that $\frac{1}{\#G_v}\mathbb{Z}/\mathbb{Z} = \{[0], [\frac{1}{3}], [\frac{2}{3}]\}$.
They correspond to the three 1-cocycles $f_0, f_1, f_2 \in H^1(G_v, \mathbb{Q}/\mathbb{Z})$ given by

$$f_0 : \sigma \mapsto [0], \qquad f_1 : \sigma \mapsto [\tfrac{1}{3}], \qquad f_2 : \sigma \mapsto [\tfrac{2}{3}].$$

The local invariant map

The **local invariant map** is $\mathrm{inv}_v : H^2(G_v, L_w^\times) \to \frac{1}{\# G_v}\mathbb{Z}/\mathbb{Z}$.

Example ($K_v = \mathbb{Q}_2$ and $L_w = \mathbb{Q}_2(\zeta_7)$)

Note that $G_v = \{1, \sigma, \sigma^2\}$, so that $\frac{1}{\# G_v}\mathbb{Z}/\mathbb{Z} = \{[0], [\frac{1}{3}], [\frac{2}{3}]\}$.
They correspond to the three 1-cocycles $f_0, f_1, f_2 \in H^1(G_v, \mathbb{Q}/\mathbb{Z})$ given by

$$f_0 : \sigma \mapsto [0], \qquad f_1 : \sigma \mapsto [\tfrac{1}{3}], \qquad f_2 : \sigma \mapsto [\tfrac{2}{3}].$$

After choosing a lift and applying δ,

- $\delta(f_0)$ is the trivial 2-cocycle,
- $\delta(f_1)$ maps (g, h) to 1 iff $(g, h) = (\sigma, \sigma^2), (\sigma^2, \sigma), (\sigma^2, \sigma^2)$, and
- $\delta(f_2)$ maps (g, h) to 1 iff $(g, h) = (\sigma, \sigma^2), (\sigma^2, \sigma), (\sigma, \sigma)$.

The local invariant map

The **local invariant map** is $\mathrm{inv}_v : H^2(G_v, L_w^\times) \to \frac{1}{\#G_v}\mathbb{Z}/\mathbb{Z}$.

Example ($K_v = \mathbb{Q}_2$ and $L_w = \mathbb{Q}_2(\zeta_7)$)

Note that $G_v = \{1, \sigma, \sigma^2\}$, so that $\frac{1}{\#G_v}\mathbb{Z}/\mathbb{Z} = \{[0], [\frac{1}{3}], [\frac{2}{3}]\}$.
They correspond to the three 1-cocycles $f_0, f_1, f_2 \in H^1(G_v, \mathbb{Q}/\mathbb{Z})$ given by

$$f_0 : \sigma \mapsto [0], \qquad f_1 : \sigma \mapsto [\tfrac{1}{3}], \qquad f_2 : \sigma \mapsto [\tfrac{2}{3}].$$

After choosing a lift and applying δ,

- $\delta(f_0)$ is the trivial 2-cocycle,
- $\delta(f_1)$ maps (g, h) to 1 iff $(g, h) = (\sigma, \sigma^2), (\sigma^2, \sigma), (\sigma^2, \sigma^2)$, and
- $\delta(f_2)$ maps (g, h) to 1 iff $(g, h) = (\sigma, \sigma^2), (\sigma^2, \sigma), (\sigma, \sigma)$.

Since $\mathbb{Q}_2(\zeta_7)^\times \cong \mathbb{Z}_2[\zeta_7]^\times \times 2^{\mathbb{Z}}$,

- $\mathrm{inv}_2^{-1}[0]$ is the trivial 2-cocycle,
- $\mathrm{inv}_2^{-1}[\frac{1}{3}]$ maps (g, h) to 2 iff $(g, h) = (\sigma, \sigma^2), (\sigma^2, \sigma), (\sigma^2, \sigma^2)$, and
- $\mathrm{inv}_2^{-1}[\frac{2}{3}]$ maps (g, h) to 2 iff $(g, h) = (\sigma, \sigma^2), (\sigma^2, \sigma), (\sigma, \sigma)$.

Cohomology of idèle classes

Theorem (global class field theory)

Let L/K be a finite extension of number fields with Galois group G. Then $H^1(G, \mathcal{C}_L) = 0$ and $H^2(G, \mathcal{C}_L)$ is finite.

Cohomology of idèle classes

Theorem (global class field theory)

Let L/K be a finite extension of number fields with Galois group G. Then $H^1(G, \mathcal{C}_L) = 0$ and $H^2(G, \mathcal{C}_L)$ is finite. Furthermore,

1. *(second inequality)* $\#H^2(G, \mathcal{C}_L) \leq \#G$, *and*
2. *(first inequality)* $\#H^2(G, \mathcal{C}_L) \geq \#G$ *if G is cyclic.*

Cohomology of idèle classes

Theorem (global class field theory)

Let L/K be a finite extension of number fields with Galois group G. Then $H^1(G, \mathcal{C}_L) = 0$ and $H^2(G, \mathcal{C}_L)$ is finite. Furthermore,

1. *(second inequality)* $\#H^2(G, \mathcal{C}_L) \leq \#G$, *and*
2. *(first inequality)* $\#H^2(G, \mathcal{C}_L) \geq \#G$ *if G is cyclic.*

In particular, T1 holds for $\mathcal{C}_L$, and T2 holds for $\mathcal{C}_L$ if G is cyclic.

Cohomology of idèle classes

Theorem (global class field theory)

Let L/K be a finite extension of number fields with Galois group G. Then $H^1(G,\mathcal{C}_L)=0$ and $H^2(G,\mathcal{C}_L)$ is finite. Furthermore,

1. *(second inequality) $\#H^2(G,\mathcal{C}_L)\le \#G$, and*
2. *(first inequality) $\#H^2(G,\mathcal{C}_L)\ge \#G$ if G is cyclic.*

In particular, T1 holds for $\mathcal{C}_L$, and T2 holds for $\mathcal{C}_L$ if G is cyclic.

The short exact sequence $1\to L^\times \xrightarrow{\Delta} \mathcal{I}_L \to \mathcal{C}_L \to 0$ induces

$$\overset{0}{\cancel{H^1(G,\mathcal{C}_L)}} \to H^2(G,L^\times) \xrightarrow{\overline{\Delta}} H^2(G,\mathcal{I}_L) \to H^2(G,\mathcal{C}_L).$$

Cohomology of idèle classes

Theorem (global class field theory)

Let L/K be a finite extension of number fields with Galois group G. Then $H^1(G, \mathcal{C}_L) = 0$ and $H^2(G, \mathcal{C}_L)$ is finite. Furthermore,

1. *(second inequality) $\#H^2(G, \mathcal{C}_L) \leq \#G$, and*
2. *(first inequality) $\#H^2(G, \mathcal{C}_L) \geq \#G$ if G is cyclic.*

In particular, T1 holds for $\mathcal{C}_L$, and T2 holds for $\mathcal{C}_L$ if G is cyclic.

The short exact sequence $1 \to L^\times \xrightarrow{\Delta} \mathcal{I}_L \to \mathcal{C}_L \to 0$ induces

$$\overset{0}{\cancel{H^1(G, \mathcal{C}_L)}} \to H^2(G, L^\times) \xrightarrow{\overline{\Delta}} H^2(G, \mathcal{I}_L) \to H^2(G, \mathcal{C}_L).$$

Thus there are inequalities

$$\#\mathrm{coker}(\overline{\Delta}) \leq \#H^2(G, \mathcal{C}_L) \leq \#G,$$

where the right inequality is an equality if G is cyclic.

The idèlic invariant map

Corollary

Let L/K be a finite extension of number fields with Galois group G.

The idèlic invariant map

Corollary

Let L/K be a finite extension of number fields with Galois group G.

1. *There are canonical isomorphisms $H^i(G, \mathcal{I}_L) \cong \bigoplus_v H^i(G_v, L_w^\times)$ for all $i > 0$. In particular, there is an* **idèlic invariant map**

$$\sum_v \mathrm{inv}_v : H^2(G, \mathcal{I}_L) \to \tfrac{1}{\mathrm{lcm}_v(\# G_v)}\mathbb{Z}/\mathbb{Z}.$$

The idèlic invariant map

Corollary

Let L/K be a finite extension of number fields with Galois group G.

1. *There are canonical isomorphisms $H^i(G, \mathcal{I}_L) \cong \bigoplus_v H^i(G_v, L_w^\times)$ for all $i > 0$. In particular, there is an* **idèlic invariant map**

$$\sum_v \mathrm{inv}_v : H^2(G, \mathcal{I}_L) \to \frac{1}{\mathrm{lcm}_v(\# G_v)}\mathbb{Z}/\mathbb{Z}.$$

2. *If $a \in H^2(G, L^\times)$, then $\sum_v \mathrm{inv}_v(a) = 0$.*

The idèlic invariant map

Corollary

Let L/K be a finite extension of number fields with Galois group G.

1. *There are canonical isomorphisms* $H^i(G, \mathcal{I}_L) \cong \bigoplus_v H^i(G_v, L_w^\times)$ *for all* $i > 0$. *In particular, there is an* **idèlic invariant map**

$$\sum_v \operatorname{inv}_v : H^2(G, \mathcal{I}_L) \to \tfrac{1}{\operatorname{lcm}_v(\#G_v)}\mathbb{Z}/\mathbb{Z}.$$

2. *If* $a \in H^2(G, L^\times)$, *then* $\sum_v \operatorname{inv}_v(a) = 0$.
3. *If* G *is cyclic, then* $\sum_v \operatorname{inv}_v$ *surjects onto* $\frac{1}{\#G}\mathbb{Z}/\mathbb{Z}$.

The idèlic invariant map

Corollary

Let L/K be a finite extension of number fields with Galois group G.

1. *There are canonical isomorphisms $H^i(G, \mathcal{I}_L) \cong \bigoplus_v H^i(G_v, L_w^\times)$ for all $i > 0$. In particular, there is an* **idèlic invariant map**

$$\sum_v \mathrm{inv}_v : H^2(G, \mathcal{I}_L) \to \tfrac{1}{\mathrm{lcm}_v(\# G_v)}\mathbb{Z}/\mathbb{Z}.$$

2. *If $a \in H^2(G, L^\times)$, then $\sum_v \mathrm{inv}_v(a) = 0$.*
3. *If G is cyclic, then $\sum_v \mathrm{inv}_v$ surjects onto $\frac{1}{\# G}\mathbb{Z}/\mathbb{Z}$.*

Proof.

1. Follows from the cohomology of unramified units.
2. Follows from the product formula and explicit description of inv_v.
3. Follows from Chebotarev's density theorem and surjectivity of inv_v.

□

Back to the fundamental exact sequence

In summary, if G is cyclic, there is a chain complex

$$0 \to H^2(G, L^\times) \xrightarrow{\overline{\Delta}} H^2(G, \mathcal{I}_L) \xrightarrow{\sum_v \mathrm{inv}_v} \frac{1}{\#G}\mathbb{Z}/\mathbb{Z} \to 0,$$

which is exact except possibly at the middle.

Back to the fundamental exact sequence

In summary, if G is cyclic, there is a chain complex

$$0 \to H^2(G, L^\times) \xrightarrow{\overline{\Delta}} H^2(G, \mathcal{I}_L) \xrightarrow{\sum_v \mathrm{inv}_v} \tfrac{1}{\#G}\mathbb{Z}/\mathbb{Z} \to 0,$$

which is exact except possibly at the middle. However, it is also exact by

$$\#G \leq \#\mathrm{coker}(\overline{\Delta}) \leq \#H^2(G, \mathcal{C}_L) = \#G.$$

Back to the fundamental exact sequence

In summary, if G is cyclic, there is a chain complex

$$0 \to H^2(G, L^\times) \xrightarrow{\overline{\Delta}} H^2(G, \mathcal{I}_L) \xrightarrow{\sum_v \mathrm{inv}_v} \tfrac{1}{\#G}\mathbb{Z}/\mathbb{Z} \to 0,$$

which is exact except possibly at the middle. However, it is also exact by

$$\#G \le \#\mathrm{coker}(\overline{\Delta}) \le \#H^2(G, \mathcal{C}_L) = \#G.$$

On the other hand, recall that

$$\mathrm{Br}(L/K) = H^2(G, L^\times), \qquad \mathrm{Br}(L_w/K_v) = H^2(G_v, L_w^\times).$$

Back to the fundamental exact sequence

In summary, if G is cyclic, there is a chain complex

$$0 \to H^2(G, L^\times) \xrightarrow{\overline{\Delta}} H^2(G, \mathcal{I}_L) \xrightarrow{\sum_v \mathrm{inv}_v} \tfrac{1}{\#G}\mathbb{Z}/\mathbb{Z} \to 0,$$

which is exact except possibly at the middle. However, it is also exact by

$$\#G \leq \#\mathrm{coker}(\overline{\Delta}) \leq \#H^2(G, \mathcal{C}_L) = \#G.$$

On the other hand, recall that

$$\mathrm{Br}(L/K) = H^2(G, L^\times), \qquad \mathrm{Br}(L_w/K_v) = H^2(G_v, L_w^\times).$$

This proves that the sequence

$$0 \to \mathrm{Br}(L/K) \xrightarrow{\overline{\Delta}} \bigoplus_v \mathrm{Br}(L_w/K_v) \xrightarrow{\sum_v \mathrm{inv}_v} \tfrac{1}{\#G}\mathbb{Z}/\mathbb{Z} \to 0$$

is exact.