# History of Reciprocity Law

Haodong Wang

March 10, 2024

## Contents

# 1 Quadratic reciprocity

## 1.1 The Genesis of Quadratic Reciprocity

The mathematician who started studying reciprocity questions was Pierre de Fermat. There were no mathematical journals in Fermat's time, and what we know about his results is contained in his letters to other mathematicians (or on the margins of some books he read). The first result related with quadratic reciprocity was stated in a letter to Mersenne:

*Tout nombre premiere, qui surpasse de l'unité un multiple du quaternaire, est une seul fois la somme de deux carrés.* [42]

This claim that every prime $p \equiv 1 \pmod 4$ is the sum of two squares first appeared (without proof) in a book of S.Stevin [29], and a general criterion for a number to be the sum of two squares is credited to Girard by Grosswald [22]. The fact that no number $\equiv 3 \pmod 4$ is the sum of two squares was already known to Diophantus of Alexandria, and its proof is trivial as soon as one knows about congruences. It's easy to see that if a prime $p$ is the sum of two squares, then each of the following claims holds:

$$p = 2 \text{ or } p \equiv 1 \pmod 4$$

In particular, the converse is also true, and it turns out that the above conditions are in fact equivalent. This is just the assertion of the first supplementary law of quadratic reciprocity.

**Proposition 1.1**

If $p \neq 2$ is a prime, then $p \equiv 1 \pmod 4 \Leftrightarrow X^2 \equiv -1 \pmod p$ is solvable $\Leftrightarrow$ $p$ is a sum of two squares.

It seems that Euler began to read Fermat's work seriously soon after he and Christian Goldbach started their correspondence. In one of his first letters to Euler (no. 2 in [36], from Dec. 1, 1729), Goldbach asked

*P.S Notane Tibi est Fermatii observatio omnes numeros hujus formulae* $2^{2^{x-1}} + 1$, *nempe* 3, 5, 17, *etc. esse primos, quam tamen ipse fatebatur se demonstrare non posse et post eum nemo, quod sciam, demonstravit.* [36]

His subsequent work on divisors of Fermat numbers $2^{2^n} + 1$ and Mersenne numbers $2^q - 1$ or, more generally, on divisors of binary quadratic forms $nx^2 + my^2$, eventually led Euler to the quadratic reciprocity law, although his progress was slow. Using the binomial theorem he could give a proof for Fermat's little theorem, which he stated in the form

*Significante* $p$ *numerum primum formula* $a^{p-1} - 1$ *semper per* $p$ *dividipoterit, nisi* $a$ *per* $p$ *divide queat.*

His first result directly connected with quadratic reciprocity was

**Proposition 1.2 (Euler's criterion)**

For integers $a$ and odd prime $p$ such that $p \nmid a$ we have

$$a^{\frac{p-1}{2}} \equiv \begin{cases} +1 \pmod p & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 \pmod p & \text{if } a \text{ is a quadratic non-residue modulo } p \end{cases}$$

## 1.2 Legendre's works on Quadratic Reciprocity

The quadratic reciprocity law was published in a form that is more familiar to us in 1788 by Legendre [1]. Legendre consider primes $a, A \equiv 1 \pmod 4$ and $b, B \equiv 3 \pmod 4$ and states

| | |
|---|---|
| Théorème I. | Si $b^{\frac{a-1}{2}} \equiv +1$, il s'ensuit $a^{\frac{b-1}{2}} \equiv +1$. |
| Théorème II. | Si $a^{\frac{b-1}{2}} \equiv -1$, il s'ensuit $b^{\frac{a-1}{2}} \equiv -1$. |
| Théorème III. | Si $a^{\frac{A-1}{2}} \equiv +1$, il s'ensuit $A^{\frac{a-1}{2}} \equiv +1$. |
| Théorème IV. | Si $a^{\frac{A-1}{2}} \equiv -1$, il s'ensuit $A^{\frac{a-1}{2}} \equiv -1$. |
| Théorème V. | Si $a^{\frac{b-1}{2}} \equiv +1$, il s'ensuit $b^{\frac{a-1}{2}} \equiv +1$. |
| Théorème VI. | Si $b^{\frac{a-1}{2}} \equiv -1$, il s'ensuit $a^{\frac{b-1}{2}} \equiv -1$. |
| Théorème VII. | Si $b^{\frac{B-1}{2}} \equiv +1$, il s'ensuit $B^{\frac{b-1}{2}} \equiv -1$. |
| Théorème VIII. | Si $b^{\frac{B-1}{2}} \equiv -1$, il s'ensuit $B^{\frac{b-1}{2}} \equiv +1$. |

In 1798, Legendre announced the quadratic reciprocity law in its final form, he introduced the "Legendre symbol" [2] :

*Comme les quantités analogous $N^{\frac{c-1}{2}}$ se rencontreront fréquemment dans le cours de nos recherches, nous emploierons le caractère abrégé $(\frac{N}{c})$ pour exprimer le reste que donne $N^{\frac{c-1}{2}}$ divisé par c, reste qui suivant ce qu'on vient de voir ne peut être que $+1$ ou $-1$.*

After, he continues:

*Quels que soient les nombres permiers m et n, s'il ne sont pas tous deux de la forme $4x-1$, on aura tonjours $(\frac{n}{m}) = (\frac{m}{n})$; et s'ils sont les deux de la forme $4x-1$, on aura $(\frac{n}{m}) = -(\frac{m}{n})$. Ces deux cas géneraux sont compris dans la formule*

$$\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{m}{n}\right)$$

How did Legendre attempt to prove the quadratic reciprocity law? His starting point was the following theorem:

**Theorem 1.1**

Assume that $a, b, c \in \mathbb{Z}$ satisfy the following conditions:

1. $(a, b) = (b, c) = (c, a) = 1$.
2. At least one of $ab, bc, ca$ is negative.
3. The following congruences are solvable:

$$u^2 \equiv -bc \pmod{a}, v^2 \equiv -ca \pmod{b}, w^2 \equiv -ab \pmod{c}$$

Then the diophatine equation

$$ax^2 + by^2 + cz^2 = 0$$

has non-trivial solutions in $\mathbb{Z}$.

Using this result, Legendre could prove Théorème I as follows: Let $a \equiv 1 \pmod 4$ and $b \equiv 3 \pmod 4$ be primes such that $(\frac{b}{a}) = 1$, and assume for contradiction that $(\frac{a}{b}) = -1$. Then $(\frac{-a}{b}) = 1$ because $b \equiv 3 \pmod 4$, and the equation $x^2 + ay^2 - bz^2 = 0$ has non-trivial solutions by Theorem 1.1. Canceling common divisors of $x$, $y$ and $z$ we may assume that at least one of $x$, $y$ or $z$ is odd. But $0 = x^2 + ay^2 - bz^2 \equiv x^2 + y^2 + z^2 \equiv 0 \pmod 4$ implies $x \equiv y \equiv z \equiv 0 \pmod 2$, and this contradiction proves the claim.

Théorème II is a formal consequence of Théorème I, and the proof of Théorème VII proceeds along similar lines: assume that $b \equiv B \equiv 3 \pmod 4$ are primes such that $(\frac{b}{B}) = 1$ and $(\frac{B}{b}) = 1$; then $Bx^2 + by^2 - z^2 = 0$ is solvable in coprime integers $x, y, z$, and reducing a solution modulo 4 yields a contradiction exactly as above.

Legendre's attack on Théorème VIII went like this: assume that $b \equiv B \equiv 3 \pmod 4$ are primes such that $(\frac{b}{B}) = (\frac{B}{b}) = -1$; assume moreover that we can find an auxiliary prime $p \equiv 1 \pmod 4$ such that $(\frac{p}{B}) = (\frac{p}{b}) = -1$. Then, by Théorèm II, we must have $(\frac{B}{p}) = (\frac{b}{p}) = -1$, and therefore $Bx^2 + by^2 - pz^2 = 0$ has a nontrivial solution. As above, this leads to a contradiction modulo 4.

Thus Legendre's proofs of the cases I,II and VII were complete, while the proof of case VIII depends on the existence of a certain prime $p$. The conditions $p \equiv 1 \pmod 4$ and $(\frac{p}{B}) = (\frac{p}{b}) = -1$ are satisfied if $p$ is a prime in a suitable residue class modulo $4bB$; in order to guarantee its existence, Legendre announced the following conjecture proved by Dirichlet:

**Theorem 1.2**

Let $a$ and $b$ be positive integers; if $(a, b) = 1$, then there exist infinitely many primes $\equiv a \pmod b$.

As we will see in the Notes, the role of Dirichlet's theorem in Legendre's attempted proof of the quadratic reciprocity law led to some confusion. As already Gauss has shown in his Disquisitiones [10], Legendre's "proof" of 1785/1788 as given in his Recherches [1] can be formulated in such a way that quadratic reciprocity does become a corollary of Theorem 1.2.

Let us start with Théorème III: suppose that we have $(\frac{a}{A}) = 1$; in order to prove that $(\frac{A}{a}) = 1$, let us assume that $(\frac{A}{a}) = -1$ and try to derive a contradiction. Legendre assumes that there is a prime $\beta \equiv 3 \pmod 4$ such that $(\frac{\beta}{\alpha}) = -1$. Then $(\frac{\alpha}{\beta}) = -1$ by II, hence $(\frac{-\alpha}{\beta}) = 1$ by the first supplementary law, and the assumption $(\frac{A}{a}) = -1$ shows that $A\beta$ is a quadratic residue modulo $a$. Thus the equation $x^2 + ay^2 - A\beta z^2 = 0$ is solvable, and we derive a contradiction exactly as above by looking at it modulo 4.

Case IV is again a formal consequence of Theoreme III, and similarly, VI follows from V. It is therefore sufficient to prove V. So assume that $(\frac{a}{b}) = 1$ and $(\frac{b}{a}) = -1$; by Dirichlet's Theorem 1.2, there is a prime $\alpha \equiv 1 \pmod 4$ such that $(\frac{\alpha}{a}) = (\frac{a}{\alpha}) = -1$. By Théorème IV, this implies $(\frac{a}{\alpha}) = -1$, and then $\alpha x^2 + ay^2 - bz^2 = 0$ is solvable, leading to the now familiar contradiction modulo 4.

The proof above is contained in Legendre's Recherches [1] from 1788, alongside with other proofs that assume the existence of auxiliary primes that do not follow from Dirichlet's theorem. In the later editions of his "Essai" [2], Legendre proved the cases VII and VIII using the theory of Pell's equation and replaced the different auxiliary primes by only one assumption:

**Lemma 1.1 (Legendre's Lemma)**

For each prime $a \equiv 1 \pmod 4$ there exists a prime $\beta \equiv 3 \pmod 4$ such that $(\frac{\alpha}{\beta}) = -1$.

Legendre could not rigorously prove the existence of such a prime $\beta$, but has clearly seen that this claim needed a proof. Legendre stuck to his approach to the proof of the reciprocity law in later editions of his book and each time made fresh attempts to close the gap, but he did not succeed in giving complete proofs for his theorems III- VI (the numbering chosen here is from the first edition).

It should also be remarked that Legendre's Lemma does not follow from Dirichlet's theorem 1.2 without

assuming parts of the quadratic reciprocity law, contrary to many claims made throughout the mathematical literature.

## 1.3 Gauss's work on the quadratic reciprocity

It was Gauss who found the first complete proof of the quadratic reciprocity law. His desire to find similar theorems for reciprocity of higher powers made him look for proofs which would generalize, and by 1818 he had published six proofs; two more were found in his unpublished papers. Proof 1 used induction, Proof 2 used the genus theory of binary quadratic forms. Proofs 4 and 6 use quadratic Gauss sums. Like most of the simplest proofs of the quadratic reciprocity law, proofs 3 and 5 rest on what we now call Gauss's Lemma.

**Lemma 1.2 (Gauss Lemma of Quadratic Residue)**

Let $p$ be an odd prime, and suppose that $a \in (\mathbb{Z}/p\mathbb{Z})^{\times}$; moreover, assume that $A = \{a_1, \cdots, a_{\frac{p-1}{2}}\}$ is a half-system modulo $p$, then

$$\left(\frac{a}{p}\right) = (-1)^{\mu}$$

where

$$\mu = \#\left\{aa_i \in A \,\middle|\, i \in \left\{1, 2, \cdots, \frac{p-1}{2}\right\}\right\}$$

For the proof of the general case Gauss introduces the floor function $\lfloor x \rfloor$, which denotes the greatest integer $\leq x$. It's easy to see that the integer $\mu$ defined in Gauss lemma can be represented as

$$\mu = \sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{ax}{p} \right\rfloor$$

Next one proves that, for odd integers $p, q \in \mathbb{Z}_+$

$$\sum_{x=1}^{\frac{q-1}{2}} \left\lfloor \frac{px}{q} \right\rfloor + \sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

This obviously implies the quadratic reciprocity law:

**Theorem 1.3 (Quadratic Reciprocity)**

For different odd primes $p, q$, we have

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

But not only did Gauss give the first complete proofs of the quadratic reciprocity law, he also extended it to composite values of $p$ and $q$ in [10]. The corresponding extension of the Legendre symbol, however, by making the denominator multiplicative first appears in Jacobi's paper [17]. There Jacobi defined the **Jacobi Symbol** $(\frac{a}{b})$ for odd positive integers $b = p_1 \cdots p_n \in \mathbb{Z}_+$ by

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_n}\right)$$

Clearly $a \equiv x^2 \pmod{b}$ implies $(\frac{a}{b}) = 1$; the converse, however, is not true. Quite surprisingly, the quadratic reciprocity law also holds for the Jacobi symbol:

**Proposition 1.3**

Let $m, n \in \mathbb{Z}_+$ be relatively prime and odd, then

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$$

This was a great improvement on Euler's and Legendre's version of quadratic reciprocity, as far as the computation of residue symbols $(\frac{p}{q})$ was concerned: instead of having to factor the residue of $p$ modulo $q$ before inverting the occurring Legendre symbols one could simply invert the Jacobi symbols and apply a computationally cheap Euclidean algorithm.

For a deduction of the Proposition above from the quadratic reciprocity law it suffices to note that

$$\frac{mn-1}{2} \equiv \frac{m-1}{2} + \frac{n-1}{2} \pmod 2$$

for odd positive integers $m, n \in \mathbb{Z}$; induction on the number of prime factors of $m$ and $n$ then yields the reciprocity law for the Jacobi symbol.

## 1.4 Hilbert's (Quadratic) Reciprocity

Hilbert gave a version of the quadratic reciprocity law that did not involve the Legendre symbol anymore: he used his norm residue symbol instead. The statement that it is valid for all elements $a, b \in \mathbb{Q}^\times$, whereas the quadratic reciprocity law for the Jacobi symbol, even when extended as far as possible, only makes sense when certain restrictions are applied to $a$ and $b$. There are several ways to define the quadratic Hilbert symbol; Hasse [27] gives a construction based on splitting the inversion factor $(\frac{a}{b})(\frac{b}{a})^{-1}$ of the Jacobi symbol into its "$p$-adic contributions", which is very instructive but can hardly be called elegant.

**Definition 1.1 (Quadratic Hilbert' Symbol)**

We will say that a form $ax^2 + by^2 + cz^2$ with $a, b, c \in \mathbb{Q}_p$ **represents** 0 if there exists $x, y, z \in \mathbb{Q}_p$, not all 0, such that $ax^2 + by^2 + cz^2 = 0$. Now we put

$$(m, n)_p = \begin{cases} +1 & \text{if } mx^2 + ny^2 - z^2 \text{ represents } 0 \\ -1 & \text{otherwise} \end{cases}$$

The definition of the Hilbert symbol above also makes sense for the infinite prime: we put $(m, n)_\infty = 1$ if and only if $mx^2 + ny^2 - z^2 = 0$ represents 0 in $\mathbb{R}$. In particular, we have $(m, n)_\infty = -1$ if $m < 0$ and $n < 0$, and $(m, n)_\infty = +1$ otherwise. The properties of the Hilbert symbol that are immediately clear from this definition are the following:

**Proposition 1.4**

For all $m, n \in \mathbb{Q}_p^\times$, the Hilbert symbol satisfies the following relations:

1. $(m, n)_p = (n, m)_p$
2. $(m, n)_p = 1$ if $m$ or $n$ is a square
3. $(-m, m)_p = 1$
4. $(1 - m, m)_p = 1$ if $m \neq 0, 1$.
5. $(a, b)_p(a', b)_p = (aa', b)_p$, $(a, b)_p(a, b')_p = (a, bb')_p$.

Observe that $(\cdot,\cdot)_p$ is a map $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \times \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \to \mathbb{F}_2$, that is: the Hilbert symbol only depends on the square classes of $a$ and $b$. One of these main properties is the bilinearity; this will follows from the fact that the subgroup $N_a = \{z \in \mathbb{Q}_p^\times \mid z = x^2 - ay^2 \text{ for some } x, y \in \mathbb{Q}_p\}$ has index at most 2 in $\mathbb{Q}_p$. The subgroup property is easy to verify: for nonsquares $a \in \mathbb{Q}_p$, the relation $z = x^2 - ay^2$ is equivalent to $z = \mathcal{N}(x + y\sqrt{a})$, where $\mathcal{N}$ denotes the norm of $\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p$. We will use the conclusion directly here and obtain the linearity of $(\cdot,\cdot)_p$ directly. Clearly if $(a,b)_p = 1$, then we have $(aa',b)_p = (a',b)_p$, $(a,bb')_p = (a,b')_p$ directly. Else if $(a,b)_p = (a',b) = -1$, then $b$ must be a non-square, hence $a, a'$ lie in the same coset of $\mathbb{Q}_p/N_b$. Since $N_a$ has order 2, we must have $aa' = c$ for some $c \in N_b$, then the claim follows.

**Proposition 1.5**

Let $p$ be an odd prime, and assume that $m, n \in \mathbb{Q}_p^\times$. Put $m = up^a$, $n = vp^b$ for $a, b \in \mathbb{Z}$ and $u, v \in \mathbb{Z}_p^\times$, then

$$(m,n)_p = \left(\frac{(-1)^{ab}u^b v^{-a}}{p}\right)$$

The proposition follows at once since for all $a, b \in \mathbb{Z}_p^\times$,

$$(p,p)_p = \left(\frac{-1}{p}\right),\ (a,p)_p = \left(\frac{a}{p}\right),\ (a,b)_p = 1$$

Here are the corresponding formulas for the dyadic Hilbert symbol:

$$(2,u)_2 = (-1)^{\frac{u^2-1}{8}},\ (u,v)_2 = (-1)^{\frac{(u-1)(v-1)}{4}}$$

Now we can prove

**Theorem 1.4 (Hilbert's quadratic reciprocity)**

For all $a, b \in \mathbb{Q}^\times$, the product formula

$$\prod_{p \le \infty} (m,n)_p = 1$$

holds. Here the product is extended over all primes, including $p = \infty$.

*Proof.* By bilinearity of the Hilbert symbol, it is sufficient to prove the product formula when $a$ and $b$ are primes or units. Since the formula holds trivially if $a = 1$ and $b = 1$, the only unit we have to consider is $-1$. Thus we have to prove the following formulas:

$$\prod_{p \le \infty} (-1,-1)_p = +1 \tag{1}$$

$$\prod_{p \le \infty} (-1,q)_p = +1 \tag{2}$$

$$\prod_{p \le \infty} (q,q')_p = +1 \tag{3}$$

for all positive primes $q, q'$. The proof for (1) is easy since $(-1,-1)_p = 1$ for all odd primes $p$, and

$$(-1,-1)_2 = (-1,-1)_\infty = -1$$

For (2), if $q = 2$, then $(-1,2)_p = +1$ for all primes $p$; else if $q$ is odd, we have $(-1,q)_q = (-1,q)_2 = -1$ and $(-1,q)_p = 1$ for all $p \neq 2, q$. Finally, contributions to the product in (3), only come from $p \in \{2, q, q'\}$. If $q = q'$ is odd, then

$$(q,q)_q = (q,q)_2 = (\frac{-1}{q})$$

if $q = q' = 2$, then $(2,2)_2 = +1$, and again the product formula holds. Assume therefore that $q \neq q'$. If both primes are odd, then

$$(q,q')_q = \left(\frac{q'}{q}\right), (q,q')_{q'} = \left(\frac{q}{q'}\right), \text{ and } (q,q')_2 = (-1)^{\frac{(q-1)(q'-1)}{4}}$$

If $q \neq q' = 2$, then $(q,2)_q = (q,2)_2 = (-1)^{\frac{q^2-1}{8}}$. Thus the Hilbert reciprocity follows at once. □

Hilbert's proof of his product formula can be found in [19]. In [20], Hilbert showed that the same formula holds for totally complex number fields with odd class number, and eventually conjectured that it can be generalized to arbitrary number fields - which we will discuss later.

# 2 Quartic Reciprocity

## 2.1 Residue Symbols in Number Fields

In this section we define the general power residue symbol in number fields possessing the necessary roots of unity and prove its basic properties.

**Definition 2.1 ($n$-th power residue)**

Let $K$ be a number field, and $n \geq 1$ a natural number. A prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ is said to be prime to $n$ if $\mathfrak{p} \nmid n\mathcal{O}_K$; it is easy to see that $\mathfrak{p}$ is prime to $n$ if and only if $q = \mathcal{N}(\mathfrak{p})$ is prime to $n$. If $K$ contains an $n$-th root of unity $\zeta_n$ and $\mathfrak{p}$ is prime to $n$, then we define the **n-th power residue** $(\alpha/\mathfrak{p})_n$ for all $\alpha \in \mathcal{O}_K$ prime to $\mathfrak{p}$ to be the $n$-th root of unity such that

$$\alpha^{\frac{q-1}{n}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_n \pmod{\mathfrak{p}}$$

and of course we extend the symbol multiplicatively to all ideals

$$\mathfrak{a} = \prod \mathfrak{p}$$

prime to $n$ by setting

$$\left(\frac{\alpha}{\mathfrak{a}}\right)_n = \prod \left(\frac{\alpha}{\mathfrak{p}}\right)_n$$

and let $(\frac{a}{b})_n$ denotes $(\frac{a}{(b)})_n$.

## 2.2 Gauss Sums and Jacobi Sums

Gauss sums over $\mathbb{F}_p$ were introduced by Vandermonde and Lagrange for the purpose of solving algebraic equations; accordingly, they were called *Lagrange resolvants* for a long time. Gauss used them in [10], and determined the sign of the quadratic Gauss sum in [11].

**Definition 2.2 (Gauss Sum)**

For character $\chi : \mathbb{F}_p^\times \to \mathbb{C}$ and $\psi \in \mathbb{F}_p \to \mathbb{C}$, we define the **Gauss sum** with respect to $\chi$ and $\psi$ by

$$G(\chi, \psi) = \sum_{t \in \mathbb{F}_p} \chi(n)\psi(n)$$

We let $G(\chi)$ denotes $G(\chi, \psi_1)$ where $\psi_1 = e^{\frac{2\pi i \cdot}{p}}$. Especially, when $\chi = \left(\frac{\cdot}{p}\right)$ is the quadratic character modulo $p$, we call $G(\chi) = G(\chi, \psi_1)$ the **quadratic Gauss sum** on $\mathbb{F}_p$, usually denoted by $\tau_p$.

We now state another proof of quadratic reciprocity: The main purpose of this proof is to show the following arithmetic properties of $\tau_p$:

**Proposition 2.1**

Let $\tau_p$ be the Gauss sum on $\mathbb{F}_p$, then

*(1).* $\tau_p^2 = (-1)^{\frac{p-1}{2}} p = p^*$.

*(2).* $\tau_p^{q-1} \equiv \left(\frac{q}{p}\right) \bmod q$.

Using the proposition above, the proof of quadratic reciprocity law is now almost trivial: it follows from the congruence

$$\left(\frac{p^*}{q}\right) = (p^*)^{\frac{q-1}{2}} = \tau_p^{q-1} \equiv \left(\frac{q}{p}\right) \pmod{q}$$

But to prove quartic reciprocity, since we need to factorize quartic Gauss sum, it's necessary to calculate the exact value of $\tau_p$ and we will later introduce a concept called **Jacobi sum**, which is first introduced by Jacobi in a letter to Gauss in 1827 [16].

**Definition 2.3 (Jacobi Sum)**

The sum

$$J(\chi_1, \chi_2) = \sum_{t \in \mathbb{F}_p} \chi_1(t)\chi_2(1-t)$$

is called the **Jacobi sum** with respect to the characters

In particular, we have the simple relation

$$G(\chi_1)G(\chi_2) = G(\chi_1\chi_2)J(\chi_1, \chi_2)$$

for all characters such that $\chi_1, \chi_2 \neq 1$, and $\chi_1\chi_2 \neq 1$, which can be found in Gauss's posthumously published [7]. This relation is formally similar to the definition of crossed homomorphisms, which is why Jacobi sums are sometimes called the "factor system" of Gauss sums.

We have known above that $\tau^2 = p^*$. Thus $\tau = \pm p^*$, and it is natural to ask whether we can determine the correct sign. Actually, the problem of determining the correct sign is due to Gauss himself: he needed it for his fourth proof of the quadratic reciprocity law. The result which took him four years to prove (see his letter [9] to Olbers) looks quite innocent:

**Proposition 2.2**

Let $p > 0$ be an odd prime; then

$$\tau_p = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4 \\ i\sqrt{p} & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

Now let

$$\Lambda := \prod_{a=1}^{\frac{p-1}{2}} (\zeta_p^a - \zeta_p^{-a})$$

By classifying $p$ by the residue modulo 4, we obtain that $\Lambda^2 = p^*$, and hence $\Lambda = \pm\tau$. In order to verify the sign of $\tau_p$, we may first obtain that $\Lambda = (\frac{2}{p})\sqrt{p^*}$ and hence it's suffice to show that $\Lambda = (\frac{2}{p})\tau_p$, which can be proved by modulo $(1-\zeta_p)^{\frac{p+1}{2}}$ in $\mathbb{Z}[\zeta_p]$.

## 2.3 Proof of Quartic Reciprocity by Gauss Sums

In this section we will use Gauss sums to prove the quartic reciprocity. The main ingredient will be the prime factorization of quartic Gauss sums. As the proof above, for $p \equiv 1 \pmod 4$, let $p = \mathcal{N}(\nu)$ for some Gaussian integer $\nu$ and $\nu \equiv 1 \pmod{2+2i}$, we may now consider the quartic Gauss sum with respect to $\chi = (\frac{\cdot}{\nu})_4$.

$$G = G(\chi) = \sum_{k=1}^{p-1} \chi(k)\zeta_p^k$$

with respect to the quartic character $\chi(r) \equiv r^{\frac{p-1}{4}} \pmod \nu$. Then by some basic calculation, we may identify that

$$G(\chi)^4 = J(\chi,\chi)^2 G(\chi^2)^2$$

Since we have already proved that $G(\chi^2)^2 = \mathcal{N}(\nu)^*$, in order to calculate $G(\chi)^4$, it remains to calculate the square of the Jacobi sum $J(\chi,\chi)$. Since

$$J(\chi,\chi) \equiv \sum_{t\in\mathbb{F}_p} t^{\frac{p-1}{4}}(1-t)^{\frac{p-1}{4}} \equiv 0 \pmod \nu$$

and

$$J(\chi,\chi) = \chi^2\left(\frac{p+1}{2}\right) + 2\sum_{t=1}^{\frac{p-1}{2}} \chi(t)\chi(1-t) \equiv 1 \pmod 2$$

with the assumption $\nu \equiv 1 \pmod{2+2i}$, we may induce that $J^2(\chi,\chi) = \nu^2$ and hence $G(\chi)^4 = \nu^3\overline{\nu}$. Before proving the quartic reciprocity law, we firstly focus on a special case:

**Lemma 2.1**

If $\nu \in \mathbb{Z}[i]$, $p \in \mathbb{Z}$ are relatively prime, where $\nu \equiv 1 \pmod{2+2i}$, $p \equiv 1 \pmod 4$, then

$$\left(\frac{\nu}{p}\right)_4 = \left(\frac{p}{\nu}\right)_4, \quad \left(\frac{i}{p}\right)_4 = (-1)^{\frac{p-1}{4}}$$

Especially, when $\nu \in \mathbb{Z}$, we have moreover

$$\left(\frac{\nu}{p}\right)_4 = \left(\frac{p}{\nu}\right)_4 = 1$$

*Proof.* Assume $p = \mu\overline{\mu}$ for some $\mu \in \mathbb{Z}[i]$, $\mu \equiv 1 \pmod{2+2i}$. For the proof of

$$\left(\frac{\nu}{p}\right)_4 = \left(\frac{p}{\nu}\right)_4$$

we may assume that $\nu$ is prime in $\mathbb{Z}[i]$ and that $p$ is prime in $\mathbb{Z}$. We will distinguish the following case:

*Case 1*: $\nu \in \mathbb{Z}$.

In this case, since $\nu$ is prime in $\mathbb{Z}[i]$, we have that $\nu < 0$, $-\nu \equiv 3 \pmod 4$ is prime in $\mathbb{Z}$, and hence

$$\left(\frac{\nu}{p}\right)_4 = \left(\frac{\nu}{\mu}\right)_4\left(\frac{\nu}{\overline{\mu}}\right)_4 = \left(\frac{\nu}{\mu}\right)_4\overline{\left(\frac{\nu}{\mu}\right)_4} = 1$$

and

$$\left(\frac{p}{\nu}\right)_4 \equiv p^{\frac{q^2-1}{4}} \equiv (p^{\frac{q+1}{4}})^{q-1} \equiv 1 \pmod q$$

Hence we obtain that $\left(\frac{p}{\nu}\right)_4 = \left(\frac{\nu}{p}\right)_4 = 1$.

*Case 2*: $\nu \notin \mathbb{Z}$, $p \equiv 3 \pmod 4$:

In this case we define $q = \mathcal{N}(\nu)$, $\chi = \left(\frac{\cdot}{\nu}\right)_4$ and find

$$\begin{aligned} G(\chi)^p &\equiv \left(\sum_{t\in\mathbb{F}_q} \chi(t)\psi(t)\right)^p \equiv \sum_{t\in\mathbb{F}_q} \chi(t)^p\psi(pt) \\ &\equiv \chi(p)\sum_{t\in\mathbb{F}_q} \overline{\chi}(pt)\psi(pt) \equiv \chi(p)G(\overline{\chi}) \pmod p \end{aligned}$$

hence $G(\chi)^p \equiv \chi(p)G(\overline{\chi}) \pmod p$. Multiplying through by $G(\chi)$ yields

$$G(\chi)^{p+1} \equiv q\left(\frac{p}{\nu}\right)_4 \pmod p$$

Since $G(\chi)^4 = \mu^3\overline{\mu}$, where $\mu \equiv 1 (\mathrm{mod}\ 2+2i)$ and $\mathcal{N}(\mu) = p$, we obtain that

$$G(\chi)^{p+1} \equiv (\nu^3\overline{\nu})^{\frac{p+1}{4}} \equiv (\nu^{p+3})^{\frac{p+1}{4}} \equiv \nu^{p+1}\left(\frac{\nu}{p}\right)_4 \equiv q\left(\frac{\nu}{p}\right)_4 \pmod p$$

Comparing both congruences gives $\left(\frac{\nu}{p}\right)_4 = \left(\frac{p}{\nu}\right)_4$.

*Case 3*: $\nu \notin \mathbb{Z}$, $p = \mathcal{N}(\mu) \equiv 1 (\mathrm{mod}\ 4)$ for some $\mu \equiv 1 \pmod{2+2i}$

Let $q$ denotes $\mathcal{N}(\nu)$, $\chi$ denotes $\left(\frac{\cdot}{\nu}\right)_4$ and find

$$\begin{aligned} G(\chi)^p &\equiv \left(\sum_{t\in\mathbb{F}_q} \chi(t)\psi(t)\right)^p \equiv \sum_{t\in\mathbb{F}_q} \chi(t)^p\psi(pt) \\ &\equiv \overline{\chi}(p)\sum_{t\in\mathbb{F}_q} \chi(pt)\psi(pt) \equiv \overline{\chi}(p)G(\chi) \pmod p \end{aligned}$$

and we find

$$G(\chi)^{p-1} = \nu^{\frac{3(p-1)}{4}}\overline{\nu}^{\frac{p-1}{4}} \equiv \overline{\left(\frac{\nu}{\mu}\right)_4}\left(\frac{\overline{\nu}}{\mu}\right)_4 \equiv \overline{\left(\frac{p}{\nu}\right)_4} \pmod \mu$$

Hence $\left(\frac{\nu}{p}\right)_4 \equiv \left(\frac{\nu}{\mu}\right)_4\left(\frac{\nu}{\overline{\mu}}\right)_4 \equiv \left(\frac{\nu}{\mu}\right)_4\overline{\left(\frac{\overline{\nu}}{\mu}\right)_4} \equiv \left(\frac{p}{\nu}\right)_4 \pmod \mu$. Now we aim to prove that

$$\left(\frac{i}{p}\right)_4 = (-1)^{\frac{p-1}{4}}$$

Since $\frac{m-1}{4} + \frac{n-1}{4} \equiv \frac{mn-1}{4} \pmod 4$ for all integers $m, n \equiv 1 (\mathrm{mod}\ 4)$, it's sufficient to prove the supplementary law only for prime $p$:

*Case 1:* $p < 0$, $-p \equiv 3 \pmod 4$ is prime: then $\left(\frac{i}{p}\right)_4 = (i^{p+1})^{\frac{p-1}{4}} = (-1)^{\frac{p-1}{4}}$

*Case 2:* $p > 0$, $p = \mathcal{N}(\mu) \equiv 1 \pmod 4$, then $\left(\frac{i}{p}\right)_4 = \left(\frac{i}{\mu}\right)_4\left(\frac{i}{\overline{\mu}}\right)_4 = i^{\frac{p-1}{4}}i^{\frac{p-1}{4}} = (-1)^{\frac{p-1}{4}}$. □

And now we are able to prove the quartic reciprocity:

**Theorem 2.1 (Quartic Reciprocity)**

For relatively prime $\alpha, \beta \equiv 1 \pmod{2+2i}$, we have

$$\left(\frac{\alpha}{\beta}\right)_4 \left(\frac{\beta}{\alpha}\right)_4^{-1} = (-1)^{\frac{bd}{4}} = (-1)^{\frac{\mathcal{N}(\alpha)-1}{4}\frac{\mathcal{N}(\beta)-1}{4}}$$

*Proof.* Choose $\alpha = a + bi$ and $\beta = c + di$ in such a way that $a \equiv c \equiv 1 \pmod 4$, and assume that $(a, b) = (c, d) = 1$; note that we may do this without loss of generality and invert them with the above Lemma. Now we use the congruences $ci \equiv d \pmod\beta$, $c\alpha = ac + bci \equiv ac + bd \pmod\beta$ and find

$$\left(\frac{\alpha}{\beta}\right)_4 = \left(\frac{c}{\beta}\right)_4^{-1} \left(\frac{c\alpha}{\beta}\right)_4 = \left(\frac{c}{\beta}\right)_4^{-1} \left(\frac{ac+bd}{\beta}\right)_4$$

Similar we get

$$\left(\frac{\beta}{\alpha}\right)_4 = \left(\frac{a}{\alpha}\right)_4^{-1} \left(\frac{ac+bd}{\alpha}\right)_4, \text{ i.e. } \left(\frac{\beta}{\alpha}\right)_4^{-1} = \left(\frac{a}{\alpha}\right)_4 \left(\frac{ac+bd}{\overline{\alpha}}\right)_4$$

Multiplying both equations yields

$$\left(\frac{\alpha}{\beta}\right)_4 \left(\frac{\beta}{\alpha}\right)_4^{-1} = \left(\frac{c}{\beta}\right)_4^{-1} \left(\frac{ac+bd}{\beta}\right)_4 \left(\frac{a}{\alpha}\right)_4 \left(\frac{ac+bd}{\overline{\alpha}}\right)_4$$

Applying Lemma 2.1 gives

$$\left(\frac{c}{\beta}\right)_4 = \left(\frac{\beta}{c}\right)_4 = \left(\frac{di}{c}\right)_4 = \left(\frac{i}{c}\right)_4$$

and correspondingly $\left(\frac{a}{\alpha}\right)_4 = \left(\frac{i}{a}\right)_4$. Moreover we find

$$\left(\frac{ac+bd}{\overline{\alpha}\beta}\right)_4 = \left(\frac{\overline{\alpha}\beta}{ac+bd}\right)_4 = \left(\frac{ac+bd+(ad-bc)i}{ac+bd}\right)_4 = \left(\frac{i}{ac+bd}\right)_4$$

Together this shows

$$\left(\frac{\alpha}{\beta}\right)_4 \left(\frac{\beta}{\alpha}\right)_4^{-1} = \left(\frac{i}{c}\right)_4^{-1} \left(\frac{i}{a}\right)_4 \left(\frac{i}{ac+bd}\right)_4$$

The symbols on the right hand side are easily computed using the supplementary law in Lemma 2.1; in fact

$$\left(\frac{i}{c}\right)_4^{-1} \left(\frac{i}{a}\right)_4 \left(\frac{i}{ac+bd}\right)_4 = (-1)^{\frac{a-1-c+1+ac+bd-1}{4}} = (-1)^{\frac{bd}{4}}$$

because of the congruence $a - c + ac \equiv 1 \pmod 8$. □

Unfortunately we do not know when Gauss really discovered the quartic reciprocity law; we are quite sure that this must have happened long before the publication of some of his results in 1828 and 1832. The complete reciprocity law is stated in one of Gauss's note books [5] and must have been known to him not much later than 1813. This agrees with what Gauss says in a letter to Dirichlet (May 30, 1828):

*Die ganze Untersuchung, deren Stoff ich schon seit 23 Jahren vollstädig bestize, die Beweise der Haupttheoreme aber (zu welchen das in der ersten Commentatio noch nicht zu rechnen ist) seit etwa* 14 *Jahren*

It is therefore reasonable to assume that Gauss discovered rational criteria for cubic and quartic reciprocity starting in 1805, but found the full reciprocity laws along with their proofs only shortly before 1814. Although

parts of his investigations dealing with quartic reciprocity were eventually published in 1828 [13] (where he derived the quartic character of 2) and 1832 [14] (where he gave criteria for the quartic residuacity of small primes as well as for the integers $\pm 6$, stated the quartic reciprocity law, and derived the quartic character for $1+i$), the promised third part containing the proof of the quartic reciprocity law never appeared. We don't even know which method Gauss used for a proof: in his publication [12] containing his fifth and sixth proof of the quadratic reciprocity law, he mentions that these proofs were motivated by his research on cubic and quadratic residues, so we might guess that the proof of his quartic reciprocity law was based on either Gauss's Lemma or on quartic Gauss sums. A proof using Gauss sums was found in Gauss's paper [8], but Bachmann said that this might have been written after the publication of Eisenstein's papers.

The first published proofs, however, are due to Eisenstein [24]. Most of the proofs published after 1850 are variations of those Eisenstein has given, exceptions are Kaplan's proof in [43], which starts by computing the number of solutions of the congruence $x_1^4 + \cdots + x_q^4 \equiv q \pmod{p}$, and the geometric proof of the quartic reciprocity law, sketches of which were found in Gauss's posthumous papers [6].

## 2.4 Abel's Construction of Elliptic Functions and Eisenstein's Analytic Proofs

In this section we will have a closer look at Eisenstein's analytic proofs for the reciprocity laws for quadratic and quartic residues. In the historical survey which he put at the beginning of his paper [21], Kummer praises them with the following words:

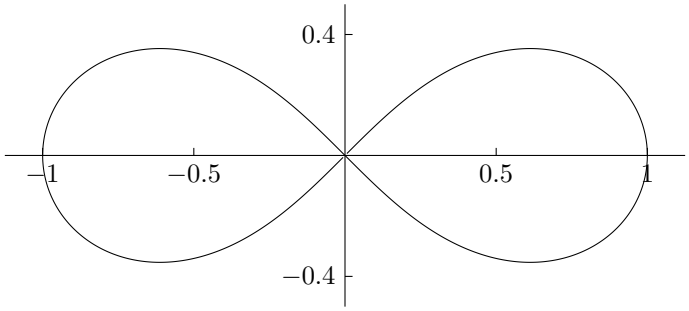
*Für einen der schönsten Beweise dieses von den ausgezeichnetsten Mathematikern viel bewiesenen Theorems wird aber derjenige mit Recht gehalten, welchen Eisenstein in Grelle's Journal, Bd. 29, pag. 177, gegeben hat. In diesem wird das Legendresche Zeichen $(\frac{p}{q})$ durch Kreisfunktionen so ausgedrückt, daß bei der Vertauschung von p und q dieser Ausdruck, his auf eine leicht zu bestimmende Änderung im Vorzeichen, ungeändert bleibt.* [...] *Wenn dieser Eisensteinsche Beweis schon wegen seiner vorzüglichen Eleganz beachtenswerth ist, so wird der Werth desselben noch dadurch erhöht, daß er, wie Eisenstein selbst gezeigt hat, ohne besondere Schwierigkeit auch auf die biquadratischen und kubischen Reciprocitätsgesetze angewendet werden kann, wenn anstatt der Kreisfunktionen elliptische Funktionen mit bestimmten Moduln angewendet werden.*

In fact Eisenstein's proofs of the quartic reciprocity laws using elliptic functions are much simpler than those using Gauss sums, at least from a computational point of view. Most proofs of the quadratic reciprocity law using cyclotomic methods probably have their counterparts in the lemniscate theory; so far only a few of these proofs have been uncovered, however.

The key to Eisenstein's proof of quartic reciprocity is the study of a certain elliptic function which can already be found in the work Abel (and which had been studied before by Gauss, who chose not to publish most of his results in this area), namely the lemniscatic sine $\mathrm{sl}(z)$; as the name suggests, $\mathrm{sl}(z)$ is related to the usual sine. We will throw some light on this relation by sketching Abel's construction of $\mathrm{sl}\, z$.

Let us first say a few words about the lemniscate. Geometrically it can be described as follows: let $F_1$ and $F_2$ be points in $\mathbb{R}^2$ with distance $|F_1F_2| = 2c$; then the lemniscate is the set of points $P$ such that $|PF_1| \cdot |PF_2| = c^2$. If we choose $F_1 = (-c, 0)$ and $F_2 = (c, 0)$, we get the equation $(x^2+y^2)^2 = 2c^2(x^2-y^2)$. In polar coordinates, lemniscates are described by $r^2 = a^2 \cos 2\theta$ with $a^2 = 2c^2$, as a straightforward computation shows. We will only consider the lemniscate corresponding to $a = 1$; then, from the equations

$r^4 = x^2 - y^2$ and $r^2 = x^2 + y^2$, we get the parameterization $2x^2 = r^2 + r^4$, $2y^2 = r^2 - r^4$.




For computing the arclength of the lemniscate (say for the part lying in the first quadrant and corresponding to the interval $r \in [0, 1]$) we need the derivatives

$$\dot{x} = \frac{\mathrm{d}x}{\mathrm{d}r} \text{ and } \dot{y} = \frac{\mathrm{d}y}{\mathrm{d}r}$$

From $x\dot{x} = r + 2r^3$ and $y\dot{y} = r - 2r^3$ we get (after some computing) $\dot{x}^2 + \dot{y}^2 = (1 - r^4)^{-1}$; in particular, the arclength of the lemniscate in the first quadrant is given by

$$\int_0^1 \frac{\mathrm{d}r}{\sqrt{1 - r^4}}$$

Abel's construction of elliptic functions begins with the integral

$$z = \int_0^w \frac{\mathrm{d}x}{\sqrt{1 - x^2}} \qquad\qquad z = \int_0^w \frac{\mathrm{d}x}{\sqrt{1 - x^4}}$$

Then $z = z(w)$ is a well-defined differentiable function on the open interval $(-1, 1)$. The transformation $\phi : [0, 1] \to [0, 1]$ given by

$$x \mapsto \frac{2t}{1 + t^2} \qquad\qquad x \mapsto \sqrt{\frac{2t^2}{1 + t^4}}$$

shows that

$$\int_0^1 \frac{\mathrm{d}x}{\sqrt{1 - x^2}} = 2\int_0^1 \frac{\mathrm{d}t}{1 + t^2} \qquad\qquad \int_0^1 \frac{\mathrm{d}x}{\sqrt{1 - x^4}} = \sqrt{2}\int_0^1 \frac{\mathrm{d}t}{\sqrt{1 + t^4}}$$

converges. A numerical computation yields

$$\pi = 2\int_0^1 \frac{\mathrm{d}x}{\sqrt{1 - x^2}} = 3.141592\ldots \qquad\qquad \varpi = 2\int_0^1 \frac{\mathrm{d}x}{\sqrt{1 - x^4}} = 2.62205\ldots$$

Since the function $z = z(w)$ is strictly increasing on $[-1, 1]$, we can define its inverse function by

$$w = \sin z \qquad\qquad w = \mathrm{sl}\, z$$

These functions are differentiable, and a simple computation yields

$$\frac{\mathrm{d}}{\mathrm{d}z} \sin z = \sqrt{1 - \sin^2 z} = \cos z \qquad\qquad \frac{\mathrm{d}}{\mathrm{d}z} \mathrm{sl}\, z = f(z)F(z)$$

where $f(z) = \sqrt{1 - \mathrm{sl}^2 z}$ and $F(z) = \sqrt{1 + \mathrm{sl}^2 z}$. In all three cases, we choose the plus sign on sufficient small intervals $[0, \varepsilon]$. Note that $\sin z$ and $\mathrm{sl}\, z$ must have derivative $+1$ in $z = 0$, because the integrands in their definition have value 1 at $z = 0$. Now straightforward computations show

$$\frac{\mathrm{d}}{\mathrm{d}z} \cos z = -\sin z \qquad\qquad \begin{aligned} \frac{\mathrm{d}}{\mathrm{d}z} f(z) &= -\mathrm{sl}(z)F(z) \\ \frac{\mathrm{d}}{\mathrm{d}z} F(z) &= \mathrm{sl}(z)f(z) \end{aligned}$$

Next let us derive the addition theorems; to this end we put

$$\widetilde{\omega} = \pi \qquad\qquad \widetilde{\omega} = \varpi$$

and $I = [-\frac{\widetilde{\omega}}{2}, \frac{\widetilde{\omega}}{2}]$. Then we put $D = \{(\alpha, \beta) \in \mathbb{R}^2 \mid \alpha, \beta, \alpha + \beta \in I\}$ and define a function $g : D \to \mathbb{R}$ by $g(\alpha, \beta) =$

$$\sin\alpha\cos\beta + \cos\alpha\sin\beta \qquad\qquad \frac{\mathrm{sl}(\alpha)f(\beta)F(\beta) + \mathrm{sl}(\beta)f(\alpha)F(\alpha)}{1 + \mathrm{sl}^2(\alpha)\,\mathrm{sl}^2(\beta)}$$

Introducing the new variables $\gamma = \frac{\alpha+\beta}{2}$ and $\delta = \frac{\alpha-\beta}{2}$ we find $\partial g/\partial\delta = 0$; this shows that $g(\gamma, \delta)$ does not depend on $\delta$. Evaluating $g$ at $\delta = \gamma$ gives

$$g(\gamma) = \sin 2\gamma \qquad\qquad g(\gamma) = \mathrm{sl}\, 2\gamma$$

After reintroducing $\alpha$ and $\beta$ we find the addition formulae for $\sin x$ and $\mathrm{sl}\, x$. Substituting $\beta = \frac{1}{2}\widetilde{\omega}$ in the addition formulae gives us a relation that allows us to define the lemniscate cosine $\mathrm{cl}\, z$:

$$\sin\left(\alpha + \frac{\pi}{2}\right) = \cos\alpha \qquad\qquad \mathrm{sl}\left(\alpha + \frac{\varpi}{2}\right) = \frac{f(\alpha)}{F(\alpha)} = \mathrm{cl}\,\alpha$$

Note that we can use these identities to extend the domain of definition for $\sin z$ and $\mathrm{sl}\, z$. Repeating this argument we find that we can extend $\sin z$ and $\mathrm{sl}\, z$ to differentiable functions on $\mathbb{R}$. It is clear that the addition formulae continue to hold for all $\alpha, \beta \in \mathbb{R}$. Moreover we find that $\sin z$ is $2\pi$-periodic, and that $\mathrm{sl}\, z$ is $2\varpi$. Differentiation shows that the same is true for $\cos z$ and $f(z), F(z)$ respectively. Finally we note the following relations:

$$\sin^2 z + \cos^2 z = 1 \qquad\qquad \mathrm{sl}^2 z + \mathrm{cl}^2 z + \mathrm{sl}^2 z\,\mathrm{cl}^2 z = 1$$

The identity for $\sin z$ and $\cos z$ follows directly from the definition of $\cos z$; in the lemniscatic case we get $\mathrm{sl}^2 z + \mathrm{cl}^2 z + \mathrm{sl}^2 z\,\mathrm{cl}^2 z = (1 + \mathrm{sl}^2 z)^{-1}((1 + \mathrm{sl}^2 z)\,\mathrm{sl}^2 z + (1 - \mathrm{sl}^2 z) + (1 - \mathrm{sl}^2 z)\,\mathrm{sl}^2 z) = 1$ as claimed. We will now evaluate these functions at certain real $z$; we will need these values later when we compute the zeros and poles of $\mathrm{sl}\, z$:

| $z$ | $\sin z$ | $\cos z$ | $\mathrm{sl}\, z$ | $f(z)$ | $F(z)$ |
|---|---|---|---|---|---|
| $m\varpi$ | $0$ | $(-1)^m$ | $0$ | $(-1)^m$ | $1$ |
| $(m + \frac{1}{2})\varpi$ | $(-1)^m$ | $0$ | $(-1)^m$ | $0$ | $\sqrt{2}$ |

Our next goal is to turn the duplication formulas into 'division formulas', i.e. we want to express $\mathrm{sl}(\frac{\alpha}{2})$, say, in terms of $\mathrm{sl}(\alpha)$, $f(\alpha)$ and $F(\alpha)$. By calculate directly, we have

$$\sin\frac{\alpha}{2} = \sqrt{\frac{1 - \cos\alpha}{2}} \qquad\qquad \mathrm{sl}\,\frac{\alpha}{2} = \sqrt{\frac{1 - f(\alpha)}{1 + F(\alpha)}}$$

Abel's next step is defining $\sin z$ and $\mathrm{sl}\, z$ for $z \in i\mathbb{R}$, that is, on the imaginary axis. This is simple for $\mathrm{sl}\, z$, because replacing $z$ by $iz$ in the definition of $\mathrm{sl}\, z$ shows that we should define $\sin(iz) = i\sinh(z)$, where the real function $w = \sinh(z)$ is defined by inverting the integral

$$z = \int_0^w \frac{\mathrm{d}x}{\sqrt{1 + x^2}}$$

Using the addition formula we can extend $\sin z$ and $\mathrm{sl}\, z$ to functions $\mathbb{C} \to \mathbb{P}^1_{\mathbb{C}}$ on the entire complex plane. One checks that $\sin z$ is holomorphic in $\mathbb{C}$, whereas $\mathrm{sl}\, z$ is meromorphic. Furthermore, the addition formulae continue to hold for all $\alpha, \beta \in \mathbb{C}$. Replacing $z$ by $iz$ in the definition of $f$ and $F$ shows that $f(iz) = F(z)$ and $F(iz) = f(z)$. We can also compute a small table of values:

| $z$ | $\operatorname{sl} z$ | $f(z)$ | $F(z)$ |
|---|---|---|---|
| $m\varpi + ni\varpi$ | $0$ | $(-1)^m$ | $(-1)^n$ |
| $(m+\frac{1}{2})\varpi + ni\varpi$ | $(-1)^{m+n}$ | $0$ | $(-1)^n\sqrt{2}$ |
| $m\varpi + (n+\frac{1}{2})i\varpi$ | $(-1)^{m+n}i$ | $(-1)^n\sqrt{2}$ | $0$ |
| $(m+\frac{1}{2})\varpi + (n+\frac{1}{2})i\varpi$ | $\infty$ | $\infty$ | $\infty$ |

In order to see that $\operatorname{sl} z$ has simple poles at $z = (m+\frac{1}{2})\varpi + (n+\frac{1}{2})i\varpi$, we observe

$$\operatorname{sl}((1+i)\alpha) = \frac{(1+i)\operatorname{sl}(\alpha)f(\alpha)F(\alpha)}{f(\alpha)^2F(\alpha)^2} = (1+i)\frac{\operatorname{sl}(\alpha)}{f(\alpha)F(\alpha)}$$

Putting $\alpha = \frac{\varpi}{2}$ shows that $\operatorname{sl} z$ has simple poles at $z = (m+\frac{1}{2})\varpi + (n+\frac{1}{2})i\varpi$. Our next step is to show that $\operatorname{sl} z = 0$ has no zeros and poles other than those given in the table above. Suppose that $\operatorname{sl} z = 0$ for $\alpha + \beta i$, $\alpha, \beta \in \mathbb{R}$. Then the addition formula shows that

$$0 = \operatorname{sl}(z) = \frac{\operatorname{sl}(\alpha)f(\beta)F(\beta) + i\operatorname{sl}(\beta)f(\alpha)F(\alpha)}{1 - \operatorname{sl}^2(\alpha)\operatorname{sl}^2(\beta)}$$

now there are only two possibilities:

1. $\operatorname{sl}^2(\alpha)\operatorname{sl}^2(\beta) = 1$: this implies that $\operatorname{sl}^2(\alpha) = \operatorname{sl}^2(\beta) = 1$. This happens if and only if $\alpha = (m+\frac{1}{2})\varpi$ and $\beta = (n+\frac{1}{2})\varpi$; in this case, we have already shown that $\operatorname{sl}(z)$ has a simple pole.
2. $\operatorname{sl}^2(\alpha)\operatorname{sl}^2(\beta) \neq 1$: then $\operatorname{sl}(\alpha)f(\beta)F(\beta) = \operatorname{sl}(\beta)f(\alpha)F(\alpha) = 0$, but since $1 \leq F(z) \leq \sqrt{2}$ for $z \in \mathbb{R}$, this is equivalent to $\operatorname{sl}(\alpha)f(\beta) = \operatorname{sl}(\beta)f(\alpha) = 0$. Since $\operatorname{sl}(\alpha)$ and $f(z)$ cannot have common zeros by the definition of $f$, this implies that either $\operatorname{sl}(\alpha) = \operatorname{sl}(\beta) = 0$ or $f(\alpha) = f(\beta) = 0$. From our knowledge of the zeros of sl and $f$ on the real line we conclude that either $\alpha = m\varpi$, $\beta = n\varpi$ or $\alpha = (m+\frac{1}{2})\varpi$ and $\beta = (n+\frac{1}{2})\varpi$; we have excluded the second alternative in part *1*, hence the first possibility must hold.

At this point we know that $\operatorname{sl}, \operatorname{cl}, f$ and $F$ are meromorphic functions on $\mathbb{C}$ with periods $2\varpi$ and $2i\varpi$; now we claim that $\operatorname{sl} z$ actually have $(1+i)\varpi$ and $(1-i)\varpi$ as periods. The verification consists in a few simple computations:

$$\begin{aligned}
\operatorname{sl}(\alpha+\varpi) &= -\operatorname{sl}(\alpha) & \qquad \operatorname{sl}(\alpha+i\varpi) &= -\operatorname{sl}(\alpha)\\
f(\alpha+\varpi) &= -f(\alpha) & \qquad f(\alpha+i\varpi) &= f(\alpha)\\
F(\alpha+\varpi) &= F(\alpha) & \qquad F(\alpha+i\varpi) &= -F(\alpha)
\end{aligned}$$

and now the addition formula yields $\operatorname{sl}(\alpha+(1+i)\varpi) = \operatorname{sl}(\alpha+(1-i)\varpi) = \operatorname{sl}(\alpha)$ as claimed. We record a few more computations

$$\begin{aligned}
\operatorname{sl}\left(\alpha+\frac{\varpi}{2}\right) &= \frac{f(\alpha)}{F(\alpha)} & \qquad \operatorname{sl}\left(\alpha+\frac{i\varpi}{2}\right) &= \frac{if(\alpha)F(\alpha)}{1-\operatorname{sl}^2(\alpha)}\\
f\left(\alpha+\frac{\varpi}{2}\right) &= -\frac{\sqrt{2}\operatorname{sl}(\alpha)F(\alpha)}{1+\operatorname{sl}^2(\alpha)} & \qquad f\left(\alpha+\frac{i\varpi}{2}\right) &= \frac{\sqrt{2}f(\alpha)}{1-\operatorname{sl}^2(\alpha)}\\
F\left(\alpha+\frac{\varpi}{2}\right) &= \frac{\sqrt{2}F(\alpha)}{1+\operatorname{sl}^2(\alpha)} & \qquad F\left(\alpha+\frac{i\varpi}{2}\right) &= \frac{i\sqrt{2}\operatorname{sl}(\alpha)f(\alpha)}{1-\operatorname{sl}^2(\alpha)}
\end{aligned}$$

As a corollary, we note the relations

$$\operatorname{sl}(\alpha)\operatorname{sl}\left(\alpha+\frac{1+i}{2}\varpi\right) = -i \qquad \operatorname{sl}(\alpha)\operatorname{sl}\left(\alpha+\frac{1-i}{2}\varpi\right) = i$$

which shows that the zeros of $\operatorname{sl} z$ and the poles of $\operatorname{sl}(z+\frac{1+i}{2}\varpi)$ coincide. It is often convenient to work with the function $\phi(z) = \operatorname{sl}((1-i)\varpi)$ whose period lattice is $\mathbb{Z}[i]$.

For instance, we assume the following proposition holds, which we will prove in appendix A. Here we will show how to deduce the quartic reciprocity law from these properties.

**Proposition 2.3**

The elliptic function $\phi(z) = \mathrm{sl}((1-i)\varpi z)$ has the following properties:

1. $\phi$ has period lattice $\mathbb{Z}[i]$ and simple zeros at $z \equiv 0, \frac{1+i}{2} \pmod{\mathbb{Z}[i]}$ simple poles at $z \equiv \frac{1}{2}, \frac{i}{2} \pmod{\mathbb{Z}[i]}$, and takes finite values everywhere else.
2. $\phi(iz) = i \cdot \phi(z)$, $\phi(\frac{1+i}{4}) = 1$, and $\phi(z)\phi(z - \frac{1}{2}) = i$.
3. Let $\nu \in \mathbb{Z}[i]$, assume that $(2, \nu) = 1$, and define a fourth root of unity $\varepsilon$ such that $\nu \equiv \varepsilon \pmod{2-2i}$. Then
$$\phi(\nu z) = \varepsilon \prod_{\alpha} \phi\left(z - \frac{\alpha}{\nu}\right)$$
where $\alpha$ runs through a complete residue system modulo $\nu$.

In Section 1.3 we have introduced Gauss's Lemma for quadratic residues; its generalization to general power residues is no problem. Let $K$ be a number field containing the $n$th roots of unity $\mu_n = \{1, \zeta, \cdots, \zeta^{n-1}\}$. For any ideal $\mathfrak{a}$ coprime to $n$, the homomorphism $\mu_n \to (\mathcal{O}_K/\mathfrak{a})^\times$ is injective. Any set $A = \{\alpha_1, \cdots, \alpha_m\}$ of representatives in $\mathcal{O}_K$ of the classes in $(\mathcal{O}_K/\mathfrak{a})^\times/\mu_n$ is called a $\frac{1}{n}$-**system** modulo $\mathfrak{a}$. The general form of Gauss's Lemma is

**Lemma 2.2 (Gauss's Lemma)**

Let $A = \{a_1, \cdots, a_m\}$ denote a $\frac{1}{n}$-system modulo $\mathfrak{p}$; then we have $\alpha\alpha_i \equiv \zeta^{a(i)}\alpha_{\pi(i)} \pmod{\mathfrak{p}}$ for some permutation $\pi$ of $\{1, 2, \cdots, m\}$, and
$$\left(\frac{\alpha}{\mathfrak{p}}\right) = \zeta^\mu, \text{ where } \mu = \sum_{i=1}^{m} a(i)$$

And the proof is exactly as in the quadratic case. At the heart of Eisenstein's approach to the lower reciprocity laws lies the following special form of Gauss's Lemma:

**Lemma 2.3**

Let $F$ be a number field containing a primitive $n$-th root of unity $\zeta_n$, suppose that $\mathfrak{p} = \pi\mathcal{O}_F$ is a principal prime ideal in $\mathcal{O}_F$ above $p$ such that $\mathfrak{p} \nmid n$, and let $f : F \to \mathbb{C}$ be an $\mathcal{O}_F$-periodic such that

1. $f(\zeta_n z) = \zeta_n f(z)$ for all $z \in F \backslash \mathcal{O}_F$.
2. $f(\frac{\alpha}{\pi}) \neq 0$ for all $\alpha \in \mathcal{O}_F \backslash \mathfrak{p}$.

Then, for any $\frac{1}{n}$-system $A$ modulo $\mathfrak{p}$, we have
$$\left(\frac{\gamma}{\mathfrak{p}}\right)_n = \prod_{\alpha \in A} \frac{f(\gamma\alpha/\pi)}{f(\alpha/\pi)}$$

Using these properties of the elliptic function $\phi$, giving a proof of the quartic reciprocity law is child's play.

*Eisenstein's proof of Quartic Reciprocity.* Let $\mu, \nu \equiv 1 \pmod{2+2i}$ be primes in $\mathbb{Z}[i]$, and let $A$ and $B$ denote $\frac{1}{4}$-systems modulo $\mu$ and modulo $\nu$, respectively. Applying Lemma 2.3 to the $\mathbb{Z}[i]$-periodic function

$\phi$ we get

$$\left(\frac{\nu}{\mu}\right)_4 = \prod_{\alpha\in A} \frac{\phi(\nu\alpha/\mu)}{\phi(\alpha/\mu)}$$

Now we define

$$P(x,y) = \prod_{j=1}^{4} \phi(x + i^j y)$$

using 2.3 and $P(x,y) = -P(y,x)$ we find

$$\left(\frac{\nu}{\mu}\right)_4 = \prod_{\alpha\in A}\prod_{\beta\in B} P\left(\frac{\alpha}{\mu}, \frac{\beta}{\nu}\right)$$

and, symmetrically

$$\left(\frac{\mu}{\nu}\right)_4 = \prod_{\beta\in B}\prod_{\alpha\in A} P\left(\frac{\beta}{\nu}, \frac{\alpha}{\mu}\right)$$

But the product over all $\alpha \in A$ and $\beta \in B$ has $\frac{\mathcal{N}(\mu)-1}{4} \cdot \frac{\mathcal{N}(\nu)-1}{4}$ factors, hence

$$\left(\frac{\nu}{\mu}\right)_4 = (-1)^{\frac{\mathcal{N}(\mu)-1}{4}\cdot\frac{\mathcal{N}(\nu)-1}{4}} \left(\frac{\mu}{\nu}\right)_4$$

and this is the quadratic reciprocity law in $\mathbb{Z}[i]$. □

The mathematical career of G. Eisenstein began in 1844 with the publication of proofs of the quadratic and cubic reciprocity laws in the 27th volume of Grelle's Journal. Though this was the first published proof of the cubic reciprocity law, it was known to Jacobi at least since 1837 when he lectured on number theory and cyclotomy [15] in Königsberg. Jacobi never bothered to publish his proofs, though his results appeared in [17], published in 1837. After Eisenstein's proofs had appeared, he had this article reprinted in 1846 as [18], having added the following footnote:

*Diese aus vielfach verbreiteten Nachschriften der oben erwähnten Vorlesung (an der Königsberger Universität) auch den Herren Dirichlet und Kummer seit mehreren Jahren bekannten Beweise sind neuerdings von Hrn. Dr. Eisenstein im 27ten Bande des Crelleschen Journals auf S. 53 publicirt worden. Der S. 41 des 28ten Bandes von Hrn. Eisenstein gegebene Beweis des quadratischen Reziprocitätsgesetzes ist der nämliche, welchen ich im Jahre 1827 Legendre mitgeteilt und dieser in die 3te Ausgabe seiner Zahlentheorie aufgenommen hat.*

Eisenstein defends himself against this attack in vol. 35 of Grelle's Journal and remarks that the proof which Jacobi claims for himself is,

*abgesehen von einer rein äußerlichen Unterschiedenheit kein anderer als der sechste Gaußische Beweis*

from 1818. Actually, Cauchy [38] published quite a similar proof in 1829; it was reprinted [39] in 1840, together with the remark

*La démonstration que je viens d'en donner, et que j'ai dejà exposée dans le Bulletin de M. Férussac de septembre 1829, est plus rigoureuse que celle qu'avait obtenu M. Legendre et plus courte que celles auxquelles M. Gauss était d'abord parvenu*

and the following footprint

*Dans la troisième édition de la Théorie des nombres, qui a paru en 1830, M. Legendre présente cette démonstration comme étant la plus simple de toutes et l'attribute à M. Jacobi, sans indiquer aucun Ouvrage òu ce géomètre l'ait pubilée, et dont la date soit anterieure au mois de septembre 1829.*

In a postscriptum to another article, however, he is much more cautious:

*La note placée au bas de la page 179, et relative à la loi de réprocité qui existe entre deux nombres premiers, se réduit à cette observation très simple, que la démonstration empurtée par M. Legendre à M. Jacobi ne parait pas avoir été pubilée par l'un au l'autre des ces deux géomètres avant 1830. Je suis loin de vouloir en conclure que cette démonstration n'ait pu être découverte par M. Jacobi à une epoque antérieure.*

It has gone unnoticed so far that Borchardt, then editor of Crelle's Journal, seems to have advised Jacobi before he wrote his footnote: in a letter to Lipschitz [4], Borchardt writes

*Dirichlet hat sich auf persönliche Reclamationen nie eingelassen, Jacobi dagegen hat z.B. Eisenstein gegenüber die Hand auf sein Eigentum gelegt, und zwar in der von mir angerathenen Form.*

Jacobi's accusations seem to have been a severe blow for Eisenstein; this transpires from almost every line on the first three pages of Eisenstein's paper [26]:

*Durch die Bemerkung Jacobi's über welchen ich mich am Schlusse meiner letzten Abhandlung über Elliptische Functionen bei Gelegenheit neuer Beweise der Reciprocitätsgesetze ausgesprochen habe, wurde ich indessen dergestalt von den Untersuchungen dieser Art abgeschreckt, dsß ich dieselben bis auf die neueste Zeit habe liegen ich dieselben bis auf die neueste Zeit habe liegen ...*

When Dirichlet wanted to explain in 1849 (see [35]) why Eisenstein's output of papers had diminished lately he said that "Eisenstein has learned the art of self-criticism in which he had been lacking before"; it seems as if this was only half the truth.

Eisenstein's proof of the quadratic reciprocity law using the sine function is taken from [25]; the same article contains proofs (or at least sketches) of the cubic and quartic reciprocity laws using Abel's elliptic functions. The third proof of the quadratic reciprocity law given here is due to Liouville [30]. Abel's construction of elliptic functions can be found in his collected works [40].

# 3 Higher Reciprocity and Class Field Theory

## 3.1 Statement of the Reciprocity Laws

Jacobi was working on a generalization of the cubic and quartic reciprocity law using cyclotomy, but it turned out that the failure of unique factorization was a major stumbling block. Only after Kummer had introduced his ideal numbers (with the intention of applying the theory to find a general reciprocity law) did it become possible to do arithmetic in cyclotomic fields $\mathbb{Q}(\zeta_p)$. Eisenstein, who had before favored the language of forms, quickly acknowledged the superiority of Kummer's approach and succeeded in finding a special case of the general reciprocity law called

**Eisenstein's Reciprocity Law**: *Let $\ell$ be an odd prime and suppose that $\alpha \in \mathbb{Z}[\zeta_\ell]$ congruence to a rational integer modulo $(1-\zeta_\ell)^2$, then*

$$\left(\frac{\alpha}{a}\right)_\ell = \left(\frac{a}{\alpha}\right)_\ell$$

*for all integers $a \in \mathbb{Z}$ prime to $\ell$.*

The quintic case had to wait for Kummer, who created the theory of ideal numbers along the way and finally produced a reciprocity theorem valid in all regular cyclotomic fields.

In order to define a residue symbols for ideals coprime to $\ell$ in the case of regular primes $\ell$ we observe that $\mathfrak{a}^h(K)$ is principal. Kummer showed that we can choose $\alpha$ primary, that is, in such a way that the congruences

$$\alpha\overline{\alpha} \equiv a \pmod{\ell},\ \alpha \equiv b \pmod{(1-\zeta_\ell)^2}$$

hold for some integers $a$ and $b$. Moreover he proved that the residue symbol $(\frac{\alpha}{\mathfrak{b}})_\ell$ does not depend on the choice of $\alpha$, as long as $\alpha$ is primary. Provided that $(\ell, h) = 1$, we can now define the residue symbol $(\frac{\mathfrak{a}}{\mathfrak{b}})_\ell$ by

$$\left(\frac{\mathfrak{a}}{\mathfrak{b}}\right)_\ell^h = \left(\frac{\alpha}{\mathfrak{b}}\right)_\ell$$

**Kummer's Reciprocity Law**: *Let $K = \mathbb{Q}(\zeta_\ell)$ and suppose that $\ell$ is regular, i.e., that $\ell$ is regular, i.e., that $\ell$ does not divide the class number $h$ $K$. Then*

$$\left(\frac{\mathfrak{a}}{\mathfrak{b}}\right)_\ell = \left(\frac{\mathfrak{b}}{\mathfrak{a}}\right)_\ell$$

*where $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime integral ideals prime to $\ell$.*

Kummer also gave explicit formulas for the supplementary laws that look rather complicated at first sight.

Hilbert did the next step forward by returning to the quadratic case: he discovered that there is a quadratic reciprocity law in every number field with odd class numbers, and he outlined how to include fields with even class field with even class number as well. Moreover, Hilbert showed that the quadratic reciprocity laws in algebraic number fields could be given a very simple form by using the norm residue symbol, and conjectured the following generalization: **Hilbert's Reciprocity Law***Let $k$ be an algebraic number field containing the $m$-th roots of unity; then for all $\mu, \nu \in k^\times$, we have*

$$\prod_v (\mu, \nu)_v = 1$$

*Here $(\cdot,\cdot)_v$ is Hilbert's $m$-th power norm residue symbol with respect to the valuation $v$, and the product is extended over all valuations $v$ of $k$.*

In this formulation of a reciprocity law, the power residue symbol does not even occur: in order to derive the classical formulation from Hilbert's one essentially has to compute certain Hilbert symbols which is rather straightforward though extremely technical. Actually, even the definition of the norm residue symbol is far from being obvious when $m > 2$.

Hilbert's conjectured reciprocity law was a part of the program he devised when he formulated the ninth problem in his famous address at the Congress of Mathematicians in Paris:

*Beweis des allgemeinsten Reziprozitätsgesetezes. Für einen beliebigen Zahlkörper soll das Reziprozitätsgesetzes der $\ell$-ten Potenzreste bewiesen werden, wenn $\ell$ eine Potenz von 2 oder eine Potenz einer ungeraden Primzahl ist. Die Aufstellung des Gesetzes, sowie die wesentlichen Hilfsmittel zum Beweis desselben werden sich, wie ich glaube, ergeben, wenn man die von mir entwickelte Theorie des Körpers der $\ell$-ten Einheitswurzeln und meine Theorie des relativ-quadratischen Körpers in gehöriger Weise verallgemeinert.*

The first sentence of this problem asks for a generalization of Kummer's reciprocity law to fields $\mathbb{Q}(\zeta_\ell)$ for irregular primes $\ell$. This was accomplished by Furtwängler, who succeeded in showing the existence of the Hilbert class field and used it to prove a quite general reciprocity law. Takagi created a sensation when he found that Furtwängler's results were just a special case of what we call class field theory today. As an application of his theory, Takagi derived a reciprocity law for $\ell$-th power in $\mathbb{Q}(\zeta_\ell)$ that contained Kummer's results for regular primes $\ell$ as a special case.

Between 1923 and 1926, Artin and Hasse were looking for simpler formulations of Takagi's reciprocity law in the hope that this would help them finish Hilbert's quest for the "most general reciprocity law" in number fields. One of the less complicated formulas they found is the following:

**The Weak Reciprocity Law of Hasse**: *Let $\ell$ be an odd prime, $K = \mathbb{Q}(\zeta_\ell)$, and suppose that $\alpha, \beta \in \mathcal{O}_K$ satisfy $(\alpha, \beta) = 1$, $\alpha \equiv 1 \ (mod\ \ell)$, and $\beta \equiv 1 \ (mod\ \lambda)$. Let* Tr *denote the trace for $K/\mathbb{Q}$. Then*

$$\left(\frac{\alpha}{\beta}\right)_\ell \left(\frac{\beta}{\alpha}\right)_\ell^{-1} = \zeta^{\mathrm{Tr}(\frac{\alpha-1}{\ell}\cdot\frac{\beta-1}{\lambda})}$$

*Here $\lambda = 1 - \zeta_\ell$.*

Hasse considered this as an approximation to the full reciprocity law since the assumption that $\alpha \equiv 1 \pmod{\ell}$ is quite strong. Artin and Hasse succeeded in giving more exact formulations, but the price they had to pay was the introduction of $\ell$-adic logarithm into their formulas.

The next break-through was Artin's discovery that all the reciprocity laws of Gauss, Kummer, Hilbert, and Takagi could be subsumed into a **general reciprocity law**. The connection between these laws is, not of the kind that springs to one's eye at first glance. Using the idèle class group $C_k$ of a number field $k$, Artin's reciprocity law takes the following simple form:

**Artin's Reciprocity Law**: *Let $k$ be an algebraic number field and let $K/k$ be a finite extension. Then the global norm residue symbol $(\frac{K/k}{\cdot})$ induces an isomorphism*

$$C_k/\mathcal{N}_{K/k}(C_K) \simeq \mathrm{Gal}(K/k)^{\mathrm{ab}}$$

*where $G^{\mathrm{ab}}$ is $G$ made abelian.*

In this ideal theoretic formulation, Artin's reciprocity law basically states that the power residue symbol $(\frac{\alpha}{\mathfrak{p}})_m$ only depends on the residue class of $\alpha$ modulo some multiple of $\mathfrak{p}$; in the case $m = 2$, this is

basically Euler's formulation of the quadratic reciprocity law, while for prime values of $m$ already Eisenstein had shown how to derive the reciprocity law from such a statement.

Immediately after Artin had proved his own four-year old conjecture in 1927 (using methods of Chebotarev), Hasse devoted the second part of his Zahlbericht to the derivation of the known explicitly reciprocity laws from Artin's. Moreover, Artin's reciprocity law allowed Hasse to define a norm residue symbol $(\frac{\mu,K/k}{\mathfrak{p}})$ for any number field $k$ and an abelian extension $K/k$, not only for those $k$ containing the appropriate roots of unity; moreover he noticed that a product formula similar to Hilbert's holds. Finally, in the special case $\zeta_m \in k$ and $K = k(\sqrt[m]{\nu})$, Hasse found

$$\left(\frac{\mu, K/k}{\mathfrak{p}}\right) = \left(\frac{\mu, \nu}{\mathfrak{p}}\right)$$

Hasse's investigation of the norm residue symbol (which is of a central importance in the second part of his Bericht) eventually suggested the existence of a "local class field theory", that is a theory of abelian extensions of local fields. This allowed him to find the local counterpart of Artin's reciprocity law and prove it by deducing it from the global result:

**Local Reciprocity**: *Let $k$ be a local field and let $K/k$ be a finite extension. Then the local norm residue symbol induces an isomorphism*

$$k^\times / \mathcal{N}_{K/k}(K^\times) \simeq \mathrm{Gal}(K/k)^{\mathrm{ab}}$$

Hasse immediately suggested that to look for direct proofs for the local case and build global class field theory on the simpler local one. This program was carried out essentially by him, F.K. Schmidt and Chevalley.

The classical formulation of class field theory in terms of ideal groups was abandoned by Chevalley who introduced idèles in order to describe the class field theory of infinite extensions. It soon became clear that idèle could also be used to reverse the classical approach and to deduce the global class field theory from the (easier) local one. Another revolution was the cohomological formulation of class field theory; using Tate's cohomology groups, the reciprocity law takes the following form:

**Tate's Formulation of Artin's Reciprocity Law**: Let $K/k$ be a normal extension, and let $u_{K/k} \in H^2(\mathrm{Gal}(K/k), C_K)$ be the fundamental class of $K/k$. Then the cup product with $u_{K/k}$ induces, for every $q \in \mathbb{Z}$, an isomorphism

$$u_{K/k} \cup : H^q(\mathrm{Gal}(K/k), \mathbb{Z}) \to H^{q+2}(\mathrm{Gal}(K/k), C_K)$$

We will later explain the background neccessary for understanding Tate's formulation, here we only note that the special case $q = -2$ is nothing but Artin's reciprocity law, since $H^{-2}(\mathrm{Gal}(K/k, \mathbb{Z})) \simeq \mathrm{Gal}(K/k)^{\mathrm{ab}}$ and $H^0(\mathrm{Gal}(K/k), C_K) = C_k / \mathcal{N}_{K/k}(C_K)$.

If, at this point, you have the feeling that we've come a long way, you might be surprised to hear that Weil [3] claimed that there was hardly any progress at all from Gauss to Artin:

*on peut dire que tout ce qui a été fait en arithmétique depuis Gauss jusqu'à ces dernières années consiste en variations sur la loi de réciprocité: on est parti de celle de Gauss; on aboutit, couronnement de tous les travaux de Kummer, Dedekind, Hilbert, à colle d'Artin, et c'est la même.*

In a way, Artin's reciprocity law closed the subject (except for the subsequent work on explicit formulas, not to mention the dramatic progress into non-abelian class field theory that is connected in particular with the names of Shimura and Langlands or the recent generalization of class field theory to "higher dimensional" local fields), and the decline of interest in the classical reciprocity laws was a natural consequence.

## 3.2 The Origin of Class Field Theory

In 1853, Kronecker announced what is now called the Kronecker-Weber Theorem.

**Theorem 3.1 (Kronecker-Weber Theorem)**

Every finite abelian extension of $\mathbb{Q}$ lies in a cyclotomic field $\mathbb{Q}(\zeta_n)$ for some $n \in \mathbb{Z}_+$.

Kronecker's proof, by his own admittance, had difficulties with extensions of 2-power degree. The first accepted proof was by Weber in 1886, but it also had an error at 2 that went unnoticed for about 90 years. The first correct proof was Hilbert's in 1886. It's worth saying something about the strategy of the proof because of its relation to Hilbert's later ideas on class field theory. Hilbert starts with an abelian extension $L/\mathbb{Q}$ and uses his recently developed theory of higher ramification groups to show $L$ lies in a succession of that the ramification in $F_n/\mathbb{Q}$ can be made smaller in exchange for adjoining appropriate roots of unity. Eventually $F_n$ is an abelian unramified extension of $\mathbb{Q}$, so $F_n = \mathbb{Q}$ since $\mathbb{Q}$ has no proper unramified extensions. At this point we have $L \subseteq \mathbb{Q}(\zeta_n)$ and the proof is complete.

Abelian extensions of $\mathbb{Q}(i)$ were constructed by Abel (1829) with special values of the lemniscate sine function $\mathrm{sl}((1+i)\varpi z)$, and as we mentioned before, it has period lattice is essentially $\mathbb{Z}[i]$. (Abel was following up on suggestion of Gauss in the *Disquisitones Arithmeticae* [10] that there is a theory of arc division on the lemniscate that parallels the theory of arc division on the circle using roots of unity) Extending Abel's work, Kronecker was able to generate abelian extensions of imaginary quadratic fields using special values of elliptic and modular functions. In a letter to Dedekind in 1880, Kronecker's described his "Jugendtraum" as the extensions he has found. As a particular example, he expected that every finite abelian extension of $\mathbb{Q}(i)$ lies in a field $\mathbb{Q}(i, \mathrm{sl}(\varpi/m))$. This is similar to the Kronecker-Weber theorem, with $\mathrm{sl}(\varpi/m)$ analogous to $\zeta_m = \exp(2\pi i/m)$.

An important case of Kronecker's work uses the $j$-function: if $K$ is imaginary quadratic and we write $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\tau_1$, where $\tau_1$ is in the upper half plane, Kronecker showed $j(\tau_1)$ is algebraic over $K$ and its $K$-conjugates are $j(\tau_1), \cdots, j(\tau_h)$ where the lattices $\mathbb{Z} + \mathbb{Z}\tau_j$ are fractional ideals in $K$ representing the different ideal classes of $K$. Kronecker proved the field $K(j(\tau_1))$ is a Galois extension of $K$ whose Galois group is isomorphic to the ideal class group of $K$. How can the ideal class group of $K$ be identified with the Galois group of $K(j(\tau_1)/K)$? Let a fractional $\mathfrak{a}$ act on $j(\tau_1)$ using multiplication in the class group: if $\mathfrak{a}(\mathbb{Z}+\mathbb{Z}\tau_j) = \mathbb{Z}+\mathbb{Z}\tau_{j'}$ in $\mathrm{Cl}(K)$ then set $\sigma_{\mathfrak{a}}(j(\tau_j)) = \tau_{j'}$. This action of fractional ideals on $j$-values descends to an action of the ideal class group on the $j$-values.

Kronecker called $K(j(\tau))$, where $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\tau$, the "species" associated to $K$, continuing the co-opting of taxonomic terminology in number theory (earlier examples being class, order, and genus). In examples, Kronecker observed the species of $K$ is not just an extension of $K$ with Galois group isomorphic to the ideal class group, but has two other properties: it is unramified over $K$ and every ideal of $K$ becomes principal in it. Hilbert will include these properties as part of his general conjectures on Hilbert class fields.

Hilbert's idea about abelian extensions of number fields developed from his careful study of three families of examples: quadratic and cyclotomic extensions of general number fields and Kummer extensions of cyclotomic field. One of his goal was to develop reciprocity laws in number fields, building on his conception (1897) of the quadratic reciprocity law over $\mathbb{Q}$ as a product formula:

$$\prod_v (a, b)_v = 1$$

for all $a, b \in \mathbb{Q}^\times$, where $(a, b)_v$ denotes the Hilbert's symbol. This is equivalent to quadratic reciprocity, but nicer in two respects: the prime 2 is on the same footing as the other primes and there are no positivity or

relative primality contraints on $a$ and $b$. The Hilbert symbol makes sense on all number fields $K$, so Hilbert proposed a quadratic reciprocity law on $K$:

$$\prod_v (a,b)_v = 1$$

for $a$ and $b$ in $K^\times$ with $v$ running over all the places of $K$. Hilbert's proof of this formula broke down for number fields that admit a quadratic extension unramified at all primes. This doesn't mean the result is wrong for those fields, only that the proof doesn't work. An obstruction like this had happened before: Kummer's $p$-th power reciprocity law in $\mathbb{Q}(\zeta_p)$ was restricted to regular primes $p$, which Hilbert could interpret as avoiding the cases when $\mathbb{Q}(\zeta_p)$ has an abelian unramified extension of degree $p$. Hilbert's proof of the Kronecker-Weber theorem succeeded in part because $\mathbb{Q}$ has no abelian unramified extension larger than $\mathbb{Q}$. It is perhaps this experience that drove Hilbert's interest in **unramified abelian extensions**, as an obstacle in proofs. Thinking about analogies between number fields and Riemann surfaces (prime ideals correspond to points and unramified extensions of number fields correspond to unbranched coverings of Riemann surfaces), Hilbert was led to the following conjecture:

**Theorem 3.2 (Hilbert, 1898)**

For each number field $K$, there is a unique finite extension $H/K$ such that

1. $H/K$ is Galois and $\mathrm{Gal}(H/K) \simeq \mathrm{Cl}(K)$.
2. $H/K$ is unramified at all places, and every abelian extension of $K$ with this property is a subfield of $H$.
3. For each prime $\mathfrak{p}$ of $K$, the residue field degree $f_\mathfrak{p}$ is the order of $\mathfrak{p}$ in $\mathrm{Cl}(K)$.
4. Every ideal of $K$ is principal in $H$.

Condition *3* implies that a prime in $K$ splits in $H$ if and only if it is principal in $K$, so $H$ is a class field over $K$ in Weber's sense for the ideal group of all principal fractional ideals in $K$. The field $H$ is called the **Hilbert class field** of $K$, but Hilbert just called it a "class field". Kronecker's species of an imaginary quadratic field is its Hilbert class field.

T. Takagi studied in Germany during 1898-1901, partly with Hilbert in Göttingen. In his 1903 thesis, Takagi proved the Jugendtraum for base field $\mathbb{Q}(i)$ using values of the lemniscate function, as Kronecker had envisioned. His proof was an adaption to $\mathbb{Q}(i)$ of Hilbert's proof of the Kronecker-Weber theorem. In 1914, R. Fueter proved that for each imaginary quadratic field $K$, viewed as a subfield of $\mathbb{C}$, every odd-degree abelian extension of $K$ inside of $\mathbb{C}$ is a subfield of some $K(e^{2\pi i\tau}, j(\tau))$, where $r \in \mathbb{Q}$ and $\tau \in K$. In other words, all odd degree abelian extensions of $K$ are inside fields generated over $K$ by special values of two analytic functions at algebraic numbers: the exponential function $e^{2\pi iz}$ at rational numbers and the $j$-function at numbers in $K$. Fueter also gave a counterexample for extensions of even degree: $\mathbb{Q}(\sqrt[4]{1+2i})$ has degree 4 over $\mathbb{Q}(i)$ and is a cyclic extension, but it lies in no field of the form $\mathbb{Q}(i, e^{2\pi i\tau}, j(\tau))$ for $r \in \mathbb{Q}$ and $r \in \mathbb{Q}(i)$.

Takagi read the work of Furtwängler on the Hilbert class field and Fueter on the Jugendtraum over imaginary quadratic fields. When World War I broke out in 1914, scientific contact between Germany and Japan ceased. Working in isolation, Takagi combined the work of Furtwängler and Fueter with an inductive procedure to prove the existence of class fields in full generality, and nearly everything else that was expected about then. Takagi began with a new definition of class fields, using norms and ideals, not splitting laws, and using infinite places in the modulus.

**Definition 3.1**

For a finite extension of number fields $L/K$ and a prime $\mathfrak{P}$ of $L$, let $\mathfrak{p} = \mathfrak{P} \cap K$ be the prime below it and set the **norm** of $\mathfrak{P}$ in $K$ to be

$$\mathcal{N}_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})}$$

Extend the norm by multiplicativity to all fractional ideals in $L$.

The link between Weber's and Takagi's viewpoints is that for Galois $L/K$ and $\mathfrak{p}$ in $K$ unramified in $L$, $\mathfrak{p}$ splits in $L$ (Weber) if and only if $\mathfrak{p}$ is the norm of a prime in $\mathcal{O}_L$.

**Definition 3.2 ($K$-modulus)**

A $K$-**modulus** is a formal product $\mathfrak{m} = \mathfrak{m}_{\mathrm{f}}\mathfrak{m}_\infty$, where $\mathfrak{m}_{\mathrm{f}}$ (the "finite part") is a nonzero ideal in $\mathcal{O}_K$ and $\mathfrak{m}_\infty$ is a formal product of real embeddings of $K$. A fractional ideal of $K$ is called **relatively prime** to $\mathfrak{m}$ when it is relatively prime to $\mathfrak{m}_{\mathrm{f}}$.

Let $I_m$ be the fractional ideals relatively prime to $\mathfrak{m}$ and $P_{\mathfrak{m}}$ be the principal fractional ideals having some generator $\alpha/\beta$ for nonzero $\alpha, \beta \in \mathcal{O}_K$ such that

1. $(\alpha)$ and $(\beta)$ are relatively prime to $\mathfrak{m}$.
2. $\alpha \equiv \beta \pmod{\mathfrak{m}_{\mathrm{f}}}$.
3. $v(\alpha/\beta) > 0$ for all real embeddings $v \mid \mathfrak{m}_\infty$.

For a $K$-modulus $\mathfrak{m}$, an intermediate group $H$ where $P_{\mathfrak{m}} \subseteq H \subseteq I_{\mathfrak{m}}$ is called an **ideal group with modulus** $\mathfrak{m}$. For a finite extension $L/K$, set

$$\mathcal{N}_{\mathfrak{m}}(L/K) := \mathcal{N}_{L/K}(J_L) \cap \{\mathfrak{a} \mid \mathfrak{a} \text{ is relatively prime to } \mathfrak{m}\}$$

and

$$H_{\mathfrak{m}}(L/K) := P_{\mathfrak{m}}\,\mathcal{N}_{\mathfrak{m}}(L/K)$$

In fact, the purpose of the group $H_{\mathfrak{m}}(L/K)$ is to create an ideal group using norms of ideals, but $\mathcal{N}_{\mathfrak{m}}(L/K)$ need not contain $P_{\mathfrak{m}}$ and thus becomes an ideal group. Put differently, the subgroup of $I_{\mathfrak{m}}/P_{\mathfrak{m}}$ generated by cosets of $\mathcal{N}_{\mathfrak{m}}(L/K)$ is $H_{\mathfrak{m}}(L/K)/P_{\mathfrak{m}}$, so the quotient group is the "norm subgroup" of $I_{\mathfrak{m}}/P_{\mathfrak{m}}$ that Takagi is focusing on. It eventually turns out that every subgroup of $I_{\mathfrak{m}}/P_{\mathfrak{m}}$ is such a norm subgroup for some finite abelian extension of $K$.

When $K$ is a $K$-modulus and $L/K$ is Galois, the primes of $K$ not dividing $\mathfrak{m}$ that split in $L$ lie in $\mathcal{N}_{\mathfrak{m}}(L/K) \subseteq H_{\mathfrak{m}}(L/K)$, so $\mathrm{Spl}(L/K) \subseteq H_{\mathfrak{m}}(L/K)$ except perhaps for primes dividing $\mathfrak{m}$. Weber's work has shown that

$$[I_{\mathfrak{m}} : H_{\mathfrak{m}}(L/K)] \leq [L : K] \tag{4}$$

**Definition 3.3 (Takagi)**

A Galois extension of number fields $L/K$ is called a **class field** when (4) has equality for a $K$-modulus $\mathfrak{m}$. Call such $\mathfrak{m}$ an **admissible modulus** of $L/K$.

To define a class field, Weber picks an ideal group $H$ and seeks a corresponding (class) field $L/K$, which should exist and be abelian, while Takagi picks an $L/K$ and sees if there is an ideal group $H$ making (4) an equality. For two admissible $K$-moduli, their least common multiple is admissible. Going the other way, the greatest common factor of two an admissible modulus is admissible, so we can speak about the least

admissible modulus: there is a $K$-modulus that is admissible for $L/K$ and the admissible moduli for $L/K$ are precisely the multiple of it. The least admissible modulus for $L/K$ is called the **conductor** of $L/K$ and is denoted $\mathfrak{C}_{L/K}$ from the German word Führer.

**Theorem 3.3 (Takagi, 1920)**

Let $K$ be a number field:

1. (Existence) To each ideal group $H$ there is a class field over $K$.
2. (Isomorphism) If $H$ is an ideal group with modulus $\mathfrak{m}$ and has a class field $L/K$, then $\mathrm{Gal}(L/K) \simeq I_{\mathfrak{m}}/H$.
3. (Completeness) Each finite abelian extensions of $K$ is a class field.
4. (Comparison) If $H_1$ and $H_2$ are ideal groups with common modulus $\mathfrak{m}$ and they have class fields $L_1$ and $L_2$, then $L_1 \subseteq L_2 \Leftrightarrow H_2 \subseteq H_1$.
5. (Conductor) For every finite abelian extension $L/K$, the places of $K$ appearing in the conductor $\mathfrak{C}_{L/K}$ are the ramified places for $L/K$.
6. (Decomposition) If $H$ is an ideal group with modulus $\mathfrak{m}$ and class field $L/K$, then each prime $\mathfrak{p} \nmid \mathfrak{m}$ is unramified in $L$ and the residue field degree $f_{\mathfrak{p}}(L/K)$ equals the order $\mathfrak{p}$ in $I_{\mathfrak{m}}/H$.

All but the last parts in Hilbert's conjecture 3.2 is a immediate consequence of Takagi's theorem. Taking $\mathfrak{m} = (1)$ and $H = P_{(1)}$, $I_{\mathfrak{m}}/H$ is the ideal class group of $K$, so the existence, isomorphism, and decomposition theorems imply the first and third parts of conjecture 3.2, let $H/K$ be a finite abelian extension unramified at all places of $K$.

Takagi proved the existence theorem from a counting argument, starting with the cyclic case. To this day, all proofs of class field theory use a reduction to the cyclic case. The complicated index calculations Takagi used in this proof were later streamlined by Herbrand.

The isomorphism and completeness theorems say the technically defined class fields over $K$ are the same as the finite abelian extensions of $K$. Takagi at first didn't believe the completeness theorem was really possible, i.e., that every finite abelian extension is a class field. He wrote that trying to explain why this idea should be wrong almost led him to a nervous breakdown. At that time nobody else in Japan was studying algebraic number theory, so Takagi had no local colleagues who could check his work. Takagi did not prove the isomorphism theorem with an explicit isomorphism, but only obtained it indirectly. Artin later contributed the essential ingredient to class field theory by writing down a natural and explicit isomorphism from the Galois group to the ideal group.

In Takagi's proof of the completeness theorem, he used (4) and an inequality that is reverse for abelian $L/K$:

$$I_{\mathfrak{m}} : H_{\mathfrak{m}}(L/K) \geq [L : K] \tag{5}$$

for some $\mathfrak{m}$. Note (4) is valid for all Galois extensions, while (5) is stated only for abelian extensions. Takagi proved 5 only for cyclic extensions of prime degree, which sufficed for his inductive proof. Later Hasse found a proof of 5 that did not need a restriction to prime degree. Unlike the proof of **??**, which uses Weber's $L$-functions, the proof of **??** is purely algebraic and its ideas go back to work of Gauss on quadratic forms.

The comparison theorem resembles Galois theory as long as we focus on class fields with a common admissible modulus $\mathfrak{m}$. Their corresponding ideal groups with modulus $\mathfrak{m}$ are the subgroups between $P_{\mathfrak{m}}$ and

$I_{\mathfrak{m}}$. However, if we consider all class fields at once, then we run into a comparison problem: the admissible modulus for the two abelian extensions of $\mathbb{Q}$ by Galois theory only after embedding then in a common cyclotomic field, so it's not a far-out idea at all. If we want a bijection between all ideal groups in $K$ and all class fields over $K$, in the spirit of Galois theory, we need to identify together the ideal groups for $K$ defined with moduli $\mathfrak{m}$ and $\mathfrak{m}'$, call $H$ and $H'$ equivalent if there is a modulus $\mathfrak{m}''$ divisible by both $\mathfrak{m}$ and $\mathfrak{m}'$ such that the natural homomorphisms $I_{\mathfrak{m}''} \to I_{\mathfrak{m}}/H$ and $I_{\mathfrak{m}''} \to I'_{\mathfrak{m}}/H'$ have the same kernel, which says $H \cap I_{\mathfrak{m}} = H' \cap I_{\mathfrak{m}''}$. Two ideal groups in $K$ that are equivalent in this sense have the same class field over $K$, and ideal groups in $K$ that are equivalent in this sense have the same class field over $K$, and the correspondence between class fields over $K$ and ideal groups in $K$ up to equivalence is a bijection. This notion of equivalent ideal groups goes back to Weber, and is awkward.

When we pass to the language of ideles later, all equivalent ideal groups will merge into a single subgroup of the ideles, making class field theory simpler.

The conductor theorem suggests the conductor and discriminant of an abelian extension are related, since their prime factors agree.

**Theorem 3.4 (Hasse, Führerdiskriminantenproduktformel)**

Let $L/K$ be abelian and $\mathfrak{m}$ be an admissible modulus for $L/K$. For a character $\chi$ of $I_{\mathfrak{m}}/H_{\mathfrak{m}}$, let $L_\chi$ be the class field to $\ker \chi$ and set $\mathfrak{C}_\chi$ to be the conductor of $L_\chi/K$. Then the discriminant of $L/K$ is given by formulas

$$\Delta_{L/K} = \prod_{\chi} \mathfrak{C}_{\chi,\mathrm{f}}$$

where $\chi$ runs over all characters of $I_{\mathfrak{m}}/H_{\mathfrak{m}}$ and $\mathfrak{C}_{\chi,\mathrm{f}}$ is the finite part of $\mathfrak{C}_\chi$.

The theorem expresses the discriminant of an abelian extension $L/K$ in terms of conductors of cyclic subextensions $L_\chi/K$. Hasse's proof used complex analysis, specifically the decomposition of $\zeta_L(s)$ into a product of Weber $L$-functions for the characters of $I_{\mathfrak{m}}/H_{\mathfrak{m}}$. In addition to writing $\Delta_{L/K}$ as a product of the finite parts of the $\mathfrak{C}_\chi$, Hasse showed the conductor $\mathfrak{C}_{L/K}$ is their least common multiple.

With Takagi's class field theory in hand, the next natural step was to search for an analogue for non-abelian Galois extensions. Takagi raised this issue himself when he reported on his work at the 1920 ICM. Artin thought out a lot about this problem: what is non-abelian class field theory? He was also thinking about the question of whether $\zeta_K(s)$ "divides" $\zeta_L(s)$ when $K \subseteq L$, in the sense that the ratio $\zeta_L(s)/\zeta_K(s)$ should be an entire function. Hecke showed in 1917 that the zeta-function of each number field is analytic in the complex plane except for a simple pole at $s = 1$, so $\zeta_L(s)/\zeta_K(s)$ is meromorphic on $\mathbb{C}$. The issue is whether the multiplicity of each zero of $\zeta_L(s)/\zeta_K(s)$ is meromorphic on $\mathbb{C}$. The issue is whether the multiplicity of each zero of $\zeta_K(s)$ is bounded above by its multiplicity as a zero of $\zeta_L(s)$ so the ratio of zeta-functions doesn't acquire poles.

Although we can consider here all extensions of number fields $L/K$, the only general theorem that was known was for **abelian extensions**: The ratio $\zeta_L(s)/\zeta_K(s)$ can be expressed as a product of Weber $L$-functions of non-trivial characters are entire functions, so the ratio $\zeta_L(s)/\zeta_K(s)$ is entire when $L/K$ is abelian. Artin wanted to treat the case when $L/K$ is a non-abelian Galois extension, and in this work he discovered $L$-functions of representations of Galois groups, which involves Frobenius elements of prime ideals in an essential way.

When a Galois group is abelian, its representations are essentially just the (1-dimensional) characters of that abelian group and Artin's definition looks like the following:

**Definition 3.4 (Artin $L$-function)**

Let $L/K$ be a finite abelian extension with Galois group $G$. For a character $\chi : G \to S^1$ and $\Re(s) > 1$, set

$$L(s,\chi) = \prod_{\mathfrak{p} \text{ unramified}} \frac{1}{1 - \chi\big(\big(\frac{L/K}{\mathfrak{p}}\big)\big)\,\mathcal{N}(\mathfrak{p}^{-s})}$$

where the Euler product is taken over the primes of $K$ that unramified in $L$.

Here's the situation: Artin created $L$-functions for characters of (possibly non-abelian) Galois groups of number fields, Weber had $L$-functions for characters of generalized ideal class groups, and for an abelian extension of number fields $L/K$, Takagi had an isomorphism

$$I_{\mathfrak{m}}/H_{\mathfrak{m}} \simeq \mathrm{Gal}(L/K) \tag{6}$$

for all admissible $K$-moduli $\mathfrak{m}$. But Takagi did not find a specific isomorphism between these groups; an isomorphism was only obtained in an arbitrary way. For the isomorphic groups in (6), Weber and Artin had $L$-functions of their characters, so it was natural to ask for an explicit isomorphism $\varphi : I_{\mathfrak{m}}/H_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ identifying the $L$-functions: $L_A(s,\chi) = L_W(s,\chi\circ\varphi)$ for every character $\chi : \mathrm{Gal}(L/K) \to S^1$, where we $L_A$ and $L_W$ denotes the Artin and Weber constructions of $L$-functions. Takagi showed each $\mathfrak{p} \nmid \mathfrak{m}$ is unramified in $L$, and if we use the conductor of $L/K$ as a modulus then the Weber's $L$-function is a product over all unramified primes, just like the Artin $L$-functions. In any event, starting at the Euler factor on $\mathfrak{p}$ in both the Artin and Weber $L$-functions suggested to Artin an isomorphism $\varphi$ from $I_{\mathfrak{m}}/H_{\mathfrak{m}}$ to $\mathrm{Gal}(L/K)$: let $\varphi(\mathfrak{p}) = (\frac{L/K}{\mathfrak{p}})$ for $\mathfrak{p} \nmid \mathfrak{m}$ and extend $\varphi$ to all of $I_{\mathfrak{m}}/H_{\mathfrak{m}}$ by multiplicativity.

There is certainly no problem in multiplicativity extending a function on prime ideals not dividing $\mathfrak{m}$ to all ideals in $I_{\mathfrak{m}}$, since primes not dividing $\mathfrak{m}$ generate $I_{\mathfrak{m}}$ without multiplicative relations between them, but the catch is whether we truly have a function on $I_{\mathfrak{m}}/H_{\mathfrak{m}}$: if primes $\mathfrak{p}$ and $\mathfrak{q}$ lie in the same coset of $I_{\mathfrak{m}}/H_{\mathfrak{m}}$, is it true that $(\frac{L/K}{\mathfrak{p}}) = (\frac{L/K}{\mathfrak{q}})$? This is not obvious though. In the special case that $L/K$ is abelian of prime degree $\ell$ and $\mu_\ell \subseteq K$, Takagi showed a result of this kind in 1922, which must have encouraged Artin that he was on the right track.

**Definition 3.5 (Artin map)**

For an abelian extension $L/K$ and $K$-modulus $\mathfrak{m}$ divide by all primes ramifying in $L$, the **Artin map** $\varphi_{L/K,\mathfrak{m}} : I_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ is given by $\varphi_{L/K,\mathfrak{m}}(\mathfrak{p}) = (\frac{L/K}{\mathfrak{p}})$ at primes $\mathfrak{p}$ not dividing $\mathfrak{m}$ and extends to $I_{\mathfrak{m}}$ by multiplicativity. For each ideal $\mathfrak{a}$ relatively prime to $\mathfrak{m}$, $\varphi_{L/K,\mathfrak{m}}(\mathfrak{a})$ is called the **Artin symbol** at $\mathfrak{a}$.

**Theorem 3.5 (Artin reciprocity law, 1927)**

When $\mathfrak{m}$ is a $K$-modulus divisible by the places of $K$ that ramify in $L$, the Artin map $\varphi_{L/K,\mathfrak{m}} : I_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ is surjective and its kernel contains $H_{\mathfrak{m}}(L/K)$, so $I_{\mathfrak{m}} \simeq \mathrm{Gal}(L/K)$ by the Artin map.

We will derive the main law of quadratic reciprocity from Artin reciprocity. For an odd prime $p$, let $p^* = (-1)^{\frac{p-1}{2}}p$, so $p^* \equiv 1 \pmod 4$. The Artin map $I_{p\infty} \to \mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q})$ sends each odd prime ideal $(q) \neq (p)$ to $(\frac{\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}}{q})$. Since the least admissible $\mathbb{Q}$-modulus for $\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$ has finite part $|d_{\mathbb{Q}(\sqrt{p^*})}| = p$, so $p\infty$ is admissible and therefore the kernel of the Artin map contains $P_{p\infty}$ by the Artin reciprocity law. Identifying $I_{p\infty}/P_{p\infty}$ with $(\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$ with the effect $q \bmod p \mapsto (\frac{p^*}{q})$ for odd primes $q \neq p$. Its nontrivial since the Artin map is onto. The only homomorphism from $(\mathbb{Z}/p\mathbb{Z})^\times$ onto $\{\pm 1\}$ is the Legendre symbol $(\frac{\cdot}{p})$, so $(\frac{p^*}{q}) = (\frac{q}{p})$.

## 3.3 Local and Idelic Class Field Theory

Hasse was interested in class field theory since shortly after his thesis (1923). In the thesis he classified quadratic forms with rational coefficients in terms of the simpler classification of quadratic forms over real and $p$-adic numbers, expressed concisely as a "local-global principal". His proofs used Dirichlet's theorem on primes and the quadratic reciprocity law in the guise of Hilbert's product formula. Hasse extended this work (1924) to quadratic forms with coefficients in a number field, using Weber's generalization of Dirichlet's theorem and the Hilbert-Fürtwangler quadratic reciprocity law in number fields.

**Definition 3.6**

Let $L/K$ be an abelian extension, $\alpha \in K^\times$, and $v$ a place of $K$. Define $(\alpha, L/K)_v \in \mathrm{Gal}(L/K)$ by the following procedure: Write $\mathrm{Gal}(L/K) \simeq I_\mathfrak{m}/H_\mathfrak{m}$, with $\mathfrak{m}$ an admissible modulus for $L/K$. When $v$ is finite, choose $\alpha_0 \in K^\times$ such that $\alpha_0$ is close to $\alpha$ at $v$ and $\alpha_0$ is close to 1 at the place in $\mathfrak{m}$:

$$v\left(\frac{\alpha_0}{\alpha} - 1\right) \geq v(\mathfrak{m}),\ w(\alpha_0 - 1) \geq w(\mathfrak{m}),\ u(\alpha_0) > 0$$

where $w$ runs over finite places in $\mathfrak{m}$ and $u$ runs over real places in $\mathfrak{m}$. If $v$ is not in $\mathfrak{m}$, include the additional condition on $(\alpha_0)$. Define

$$(\alpha, L/K)_v = \varphi_{L/K,\mathfrak{m}}(\mathfrak{a})^{-1} \tag{7}$$

For infinite $v$ where $K_v$ is real, $L_v$ is complex, and $\alpha < 0$ in $K_v$, set $(\alpha, L/K)_v$ to be the complex conjugation in $\mathrm{Gal}(L_v/K_v) \subseteq \mathrm{Gal}(L/K)$. For other infinite $v$, set $(\alpha, L/K)_v$ to be the identity.

Of course Hasse needed to check $(\alpha, L/K)_v$ is independent of the choice of $\alpha_0$: if $\beta_0$ has the same properties as $\alpha_0$, then $(\alpha_0/\beta_0) \in P_\mathfrak{m}$, so $\varphi_{L/K,\mathfrak{m}}((\frac{\alpha_0}{\beta_0})) = 1$ by the Artin reciprocity law. Therefore Hasse's symbol $(\alpha, L/K)_v$ is well-defined, but we have to bring in some heavy machinery to show it. When $L = K(\sqrt{\beta})$ and we identify $\mathrm{Gal}(L/K)$ with $\{\pm 1\}$, $(\alpha, L/K)_v$ equals the quadratic Hilbert symbol $(\alpha, \beta)_v$, so Hasse's construction generalizes the Hilbert symbol.

Pick a prime $\mathfrak{p}$ not dividing any admissible modulus $\mathfrak{m}$ for $L/K$. For $\alpha \in K^\times$, let $k = v_\mathfrak{p}(\alpha)$. Choose $\alpha_0$ so that $w(\alpha_0 - 1) \geq w(\mathfrak{m})$ for all $w \mid \mathfrak{m}_\mathrm{f}$, $w(\alpha_0) > 0$ for all $w \mid \mathfrak{m}_\infty$, and $v_\mathfrak{p}(\alpha_0/\alpha - 1) \geq 1$. Then $(\alpha_0) = \mathfrak{p}^k\mathfrak{a}$ where $\mathfrak{a}$ is relatively prime to $\mathfrak{p}$ and to $\mathfrak{m}$. Then $(\alpha, L/K)_\mathfrak{p} = \varphi_{L/K} = \varphi_{L/K,\mathfrak{m}}(\mathfrak{a})^{-1} = \varphi_{L/K,\mathfrak{m}}((\alpha_0)\mathfrak{p}^{-k})^{-1}$. By Artin reciprocity, $(\alpha_0)$ is in the kernel of the Artin map, so

$$(\alpha, L/K)_\mathfrak{p} = \varphi_{L/K,\mathfrak{m}}((\alpha_0)\mathfrak{p}^{-k})^{-1} = \left(\frac{L/K}{\mathfrak{p}}\right)^{v_\mathfrak{p}(\alpha)}$$

That the exponent on the right is $v_\mathfrak{p}(\alpha)$ rather than $-v_\mathfrak{p}(\alpha)$ comes from the exponent $-1$ in the definition of $(\alpha, L/K)_\mathfrak{p}$. We see that $(\alpha, L/K)_\mathfrak{p}$ has a simple definition in terms of Frobenius elements when $\mathfrak{p} \nmid \mathfrak{m}$. In particular, $(\alpha, L/K)_v = 1$ for all but finitely many $v$ since all but finitely many $v$ don't divide $\mathfrak{m}$ and $v_\mathfrak{p}(\alpha) = 0$ for all but finitely many $\mathfrak{p}$.

**Theorem 3.6 (Hasse)**

For each finite abelian extension of number fields $L/K$ and $\alpha \in K^\times$, we have

$$\prod_v (\alpha, L/K)_v = 1$$

Just as Hasse's definition of $(\alpha, L/K)_v$ depended on the Artin reciprocity law, so too his proof of Theorem 3.6 used the Artin reciprocity law.

Hasse's study of $(\alpha, L/K)_v$ for finite $v$ indicated that it should depend only on the local behavior of $K$ and $L$ at $v$, despite its roundabout global definition in terms of the Artin map at ideal in $K$ that is relative prime to $v$. For example $(\alpha, L/K)$ lies in the common decomposition group $D(w \mid v)$ for all places $w \mid v$ for all places $w \mid v$ on $L$, and this decomposition group is naturally identified with the Galois group of completions $\mathrm{Gal}(L_w/K_v)$. This led Hasse to the discovery of class field theory for local fields. The first version of local class field theory was worked out by Hasse and Schmidt in 1930 and used global class field theory in an essential way: an abelian extension of local fields is realized as the completion of an abelian extension of number fields, and the global Artin map for that extension of number fields is used to define a local Artin map.

Here is how it goes. Starting with an abelian extension $E/F$ of a (characteristic 0) local field $F$, write $F = K_v$ for some number field $K$ and finite place $v$ on $K$. Takagi's class field theory implies there is an abelian extension $L/K$ such that $E = LK_v$. For $\alpha \in K^\times$, the symbol $(\alpha, L/K)_v$ belongs to $D(w \mid v)$, which is naturally identified with $\mathrm{Gal}(L_w/K_v) = \mathrm{Gal}(E/F)$. Hasse defined $(\alpha, E/F) \in \mathrm{Gal}(E/F)$ to be the element in $\mathrm{Gal}(E/F)$ by $\alpha \mapsto (\mapsto, E/F)$. This function is a homomorphism and is $v$-adically locally constant, so it extends to all $\alpha \in K_v^\times = F^\times$, giving a homomorphism $(-, E/F) : F^\times \to \mathrm{Gal}(E/F)$ called the **local Artin map**. In particular, if $E/F$ is unramified and $\pi$ is a prime in $F$ then $(\pi, E/F)$ is the local Frobenius element in $\mathrm{Gal}(E/F)$. If we had not used the exponent $-1$ to define $(-, L/K)_v$, then $(\pi, E/F)$ would be the inverse of the Frobenius when $E/F$ unramified.

Compatibility properties of the global Artin map show $(-, E/F)$ is independent of the number fields $K$ and $L$ and the place $v$ on $K$ used to construct it. It turns out that $(-, E/F)$ has kernel equal to the norm subgroup $\mathcal{N}_{E/F}(E^\times) \subseteq F^\times$. This is a local analogue of $\mathcal{N}_{\mathfrak{m}}(L/K)$ being part of the kernel of the global Artin map $\varphi_{L/K,\mathfrak{m}}$, but in the local case the norm subgroup is the full kernel.

**Theorem 3.7**

For an abelian extension of local fields $E/F$ with characteristic 0, the local Artin map $\alpha \mapsto (\alpha, E/F)$ is a homomorphism from $F^\times$ onto $\mathrm{Gal}(E/F)$ with kernel $\mathcal{N}_{E/F}(E^\times)$, so $F^\times/\mathcal{N}_{E/F}(E^\times) \simeq \mathrm{Gal}(E/F)$. Associating to $E$ the group $\mathcal{N}_{E/F}(E^\times)$ gives a one-to-one inclusion-reversing correspondence between finite abelian extensions of $F$ and subgroups of finite index in $F^\times$. The image of $\mathcal{O}_F^\times$ in $\mathrm{Gal}(E/F)$ under the local Artin map is the inertia group $I(E/F)$, so

$$e(E/F) = (\mathcal{O}_F^\times \mathcal{N}_{E/F}(E^\times) : \mathcal{N}_{E/F}(E^\times)) = (\mathcal{O}_F^\times : \mathcal{N}_{E/F}(\mathcal{O}_E^\times))$$

Then $f(E/F) = (F^\times : \mathcal{O}_F^\times \mathcal{N}_{E/F}(E^\times))$ is the order of $\pi$ in $F^\times/\mathcal{O}_F^\times \mathcal{N}_{E/F}(E^\times)$ for each prime $\pi$ of $F$.

If $H \subseteq F^\times$ is a subgroup of finite index, call $E$ the **class field** to $H$ over $F$ when $\mathcal{N}_{E/F}(E^\times) = H$. Theorem 3.7 shows Takagi's theorems about class fields over number fields have analogues for class fields over local fields. The only missing part is the local analogue of the conductor. For this, we need a local substitute for the ideal group $P_{\mathfrak{m}}$. It is the subgroups $U_n = 1 + \pi^n \mathcal{O}_F$ for $n \geq 1$ and $U_0 = \mathcal{O}_F^\times$. Every ideal group in a number field contains some $P_{\mathfrak{m}}$ and every subgroup of $F^\times$ with finite index, say $d$, contains all $d$th powers and thus contains some $U_n$ by Hensel's Lemma. When a subgroup of $F^\times$ contains some $U_n$, it contains $U_{n'}$ for all $n' \geq n$, so there is a $U_n$ inside it with minimal $n \geq 0$. Specifically, when $E/F$ is abelian, let $U_n \subseteq \mathcal{N}_{E/F}(E^\times)$ with $n$ as small as possible.

The **conductor** of $E/F$ is defined to be the ideal $\pi^n \mathcal{O}_F$, so the conductor is $\mathcal{O}_F$ of and only if $E/F$ is unramified. When $E/F$ is ramified, its conductor is a proper ideal of $\mathcal{O}_F$. The global conductor-discriminant formula (Theorem 3.6) has a local analogue:

**Theorem 3.8**

Let $E/F$ be an abelian extension of local fields with characteristic 0. For a character $\chi$ of $\mathrm{Gal}(E/F)$, let $\mathfrak{C}_\chi$ be the conductor of the class field to $\ker\chi$. Then

$$\Delta_{E/F} = \prod_\chi \mathfrak{C}_\chi$$

where the product runs over all characters of $\mathrm{Gal}(E/F)$.

E. Noether felt that there should be a self-contained derivation of local class field theory, and global class field theory should be derived from local class eld theory. F. K. Schmidt announced a local development of local class field theory for tamely ramified extensions, but he did not publish it. The main problem in building local class field theory is defining a local Artin map. This isn't difficult for an unramified extension, since there is a Frobenius element in the local Galois group just as in the global case at unramified primes. But a local construction of the local Artin map for ramified abelian extensions of local fields is not at all easy. In 1933, Hasse found a local description of the local Artin map for cyclic extensions, and Chevalley extended this to abelian extensions. Their construction came from developments in noncommutative ring theory, which is surprising since class field theory is about commutative Galois groups and commutative fields. The particular noncommutative rings that matter are cyclic algebras.

The mathematical structure of cyclic algebras (which after all were entirely in terms of the number fields themselves) in proofs of class field theory, leaving behind only cohomological formalism. This is how cohomology entered local and global class field theory in period 1950-1952 in work of Hochschild, Nakayama, Weil, Artin and Tate.

With local class field theory having been set up on its own terms, a remaining task was to derive the theorems of global class field theory from those of local class field theory. The new concept that allowed this is the idele group of a number field. It was first defined by Chevalley for the purpose of describing global class field theory from local class field theory.

**Definition 3.7 (Idele group)**

The **idele group** $\mathbb{I}_K$ of a number field is the set of sequences $(x_v)_v$, indexed by the places $v$ of $K$, such that $x_v \in K_v^\times$ for all $v$ and $x_v \in \mathcal{O}_v^\times$ for all but finitely many $v$, where $\mathcal{O}_v$ is the ring of integers of $K_v$.

An element of $\mathbb{I}_K$ is called an idele. Chevalley first called it an "élément idéal", abbreviated later (at Hasse's suggestion) to idèle. Under componentwise multiplication, the ideles are a group, and they lie between the direct sum of the $K_v^\times$'s and the direct product of the $K_v$'s. We embed $K^\times \hookrightarrow \mathbb{I}_K$ singly.

To each idele $x \in \mathbb{I}_K$ we have a fractional ideal

$$\iota(x) = \prod_{v\nmid\infty} \mathfrak{p}_v^{v(x_v)}$$

where the right side is a finite product. The image of a principal idele is the principal ideal of the same element of $K^\times$. The archimedean components of $x$ play no role in $\iota(x)$.

Using this passage from ideles to ideals, each generalized ideal class group of $K$ can be realized as a quotient

group of $\mathbb{I}_K$ as follows. Pick a $K$-modulus $\mathfrak{m}$. Starting with an idele $x \in J_K$, pick $\alpha_0 \in K^\times$ so that for $v$ in $\mathfrak{m}$ we have

$$v\left(\frac{x_v}{\alpha_0} - 1\right) \geq v(\mathfrak{m})$$

when $v \mid \mathfrak{m}_{\mathrm{f}}$, and

$$\frac{x_v}{v(\alpha_0)} > 0$$

when $v \mid \mathfrak{m}_\infty$. The idele $x/\alpha_0$ has corresponding ideal $\iota(x/\alpha_0)$ in $I_\mathfrak{m}$. If $\beta_0 \in K^\times$ has the same properties as $\alpha_0$ then the ideals $\iota(x/\alpha_0)$ is well-defined in terms of $x$ as an element of $I_\mathfrak{m}/P_\mathfrak{m}$. Sending $x$ to $\iota(x/\alpha_0)$ is a homomorphism from $\mathbb{I}_K$ onto $I_\mathfrak{m}/P_\mathfrak{m}$. If $x = (\alpha, \cdots)$ is a principal idele, we can use $\alpha_0 = \alpha$, so the image is 1, which means the $K$ can be viewed as quotients of the single group $\mathbb{I}_K$, or even of $\mathbb{I}_K/K^\times$. If we multiply an archimedean component of $x$ by a positive real number then the new idele $x'$ has the same image as $x$ in $I_\mathfrak{m}/P_\mathfrak{m}$, because $x$ and $x'$ admit the same choices for $\alpha_0$ in the above inequalities, and $\iota(x'/\alpha_0) = \iota(x/\alpha_0)$ since forming fractional ideals from ideles doesn't involve the archimedean components. Therefore generalized ideal class groups are all quotients of $\mathbb{I}_K^1/K^\times$, where $\mathbb{I}_K^1$ is the group of ideles with idelic norm 1.

As an indication of the simplicity coming from this viewpoint, lets return to the equivalence relation put on ideal groups in $K$ to make the correspondence between class fields and (equivalence classes of) ideal groups a bijection. An ideal group $H$ with modulus $\mathfrak{m}$ can be converted into a subgroup of $\mathbb{I}_K$ containing $K^\times$: take the inverse image of $H/P_\mathfrak{m}$ under the map $\mathbb{I}_K \to I_\mathfrak{m}/P_\mathfrak{m}$. Two ideal groups $H$ and $H'$ are equivalent ($H \cap I_{\mathfrak{m}''} = H' \cap I_{\mathfrak{m}''}$ for some multiple $\mathfrak{m}''$ of the moduli for $H$ and $H'$) exactly when they correspond to the same group of ideles.

Now we introduce an idelic version of the Artin map. When $L/K$ is an abelian extension of number fields and $\mathfrak{m}$ is an admissible for this extension, the composite map

$$\varphi_{L/K} : \mathbb{I}_K \longrightarrow I_\mathfrak{m}/P_\mathfrak{m} \xrightarrow{\varphi_{L/K,\mathfrak{m}}} \mathrm{Gal}(L/K)$$

is a surjective homomorphism and is independent of the choice of admissible $\mathfrak{m}$. This composite map is the **idelic Artin map**, we need norms on ideles. Define $\mathcal{N}_{L/K} : \mathbb{I}_L \to \mathbb{I}_K$ by $\mathcal{N}_{L/K}(y) = (x)$ where

$$x_v = \prod_{w \mid v} \mathcal{N}_{L_w/K_v}(y_w)$$

for all places $v$ of $K$. Then the kernel of $\varphi_{L/K}$ is $K^\times \mathcal{N}_{L/K}(\mathbb{I}_L)$, which is an idelic counterpart to $\varphi_{L/K,\mathfrak{m}}$ having kernel $P_\mathfrak{m}\mathcal{N}_\mathfrak{m}(L/K)$ for admissible $\mathfrak{m}$.

To formulate class field theory as a one-to-one correspondence using ideles, we need a topology on $\mathbb{I}_K$. The topology Chevalley put on $\mathbb{I}_K$ is not Hausdorff. It was later replaced by the restricted product topology, where a basic open neighborhood of 1 in $\mathbb{I}_K$ is a set

$$\prod_v U_v$$

with $U_v$ an open neighborhood of 1 in $K_v^\times$ for all $v$ and $U_v = \mathcal{O}_v^\times$ for all but finitely many $v$. With this topology, $\mathbb{I}_K$ is a locally compact topological group. Using the product topology, $\mathbb{I}_K$ is a locally compact (Hausdorff) topological group. Using the product topology, $\mathbb{I}_K$ would not be locally compact, which is why the product topology is not a good choice.

**Theorem 3.9**

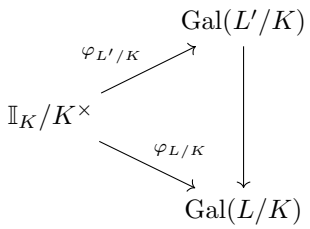
For an abelian extension of number fields $L/K$, the **idelic Artin map** $x \mapsto \varphi_{L/K}(x)$ is a homomorphism from $\mathbb{I}_K$ onto $\mathrm{Gal}(L/K)$ with kernel $K^\times \mathcal{N}_{L/K}(\mathbb{I}_L)$. So $\mathbb{I}_K/K^\times \mathcal{N}_{L/K}(\mathbb{I}_L) \simeq \mathrm{Gal}(L/K)$. Associating to $L$ the group $K^\times \mathcal{N}_{L/K}(\mathbb{I}_L)$ gives a one-to-one inclusion-reversing correspondence between finite abelian extensions of $K$ and open subgroups of finite index in $\mathbb{I}_K$ that contain $K^\times$. For each place $v$ of $K$, pick a place $w$ in $L$ lying over $v$. The composite map

$$K_v^\times \longrightarrow \mathbb{I}_K \longrightarrow \mathrm{Gal}(L/K)$$

Using subgroups of $\mathbb{I}_K/K^\times$ in Theorem 3.9 instead of subgroups of $\mathbb{I}_K$ containing $K^\times$, finite abelian extensions of $K$ correspond one-to-one with "norm subgroups" of $\mathbb{I}_K/K^\times$. The isomorphism $\mathbb{I}_K/K^\times \mathcal{N}_{L/K} \simeq \mathrm{Gal}(L/K)$ is analogous to $I_\mathfrak{m}/P_\mathfrak{m}\mathcal{N}_\mathfrak{m}(L/K) \simeq \mathrm{Gal}(L/K)$.

The idelic class field theory still has a flaw: while the idelic Artin map $\varphi_{L/K}$ is independent of the admissible modulus used in its construction, we are still using an admissible modulus to define it, so a proof of 3.9 has to fall back on the ideal-theoric global class field theory. We will see how this flaw get sorted out below. But first we use the idelic viewpoint to get a workable substitute for the definition that lets us pass to infinite abelian extensions.

When $K' \subseteq L \subseteq L'$ is a tower of finite abelian extension of $K$ and $\mathfrak{m}$ is an admissible $K$-modulus for $L'$ (and thus also for $L$), the diagram




commutes: the source group $\mathbb{I}_K/K$ does not change as $L'$ grows, so we can pass to an inverse limit compatibly to get a homomorphism

$$\varphi_K : \mathbb{I}_K/K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

mapping to the Galois group of the maximal abelian extension of $K$. Since the map is onto at finite levels, it has dense image. To show the image is $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ consider $\varphi_K$ on the subgroup $\mathbb{I}_K^1/K^\times$, which is compact. Shrinking $\mathbb{I}_K/K^\times$ to $\mathbb{I}_K^1/K^\times$ maintains surjectivity of the idelic Artin maps $\mathbb{I}_K \to \mathrm{Gal}(L/K)$ - this goes back to the fact that each generalized ideal class group is a quotient not just of $\mathbb{I}_K$, but of $\mathbb{I}_K^1$ - so the image of $\varphi_K : \mathbb{I}_K^1/K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}, K)$ is dense. The image is also compact, and thus closed, so the image is $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. The kernel of $\varphi_K$ is the connected component of the identity in $J_K/K^\times$, so $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ is the largest totally disconnected quotient group of $\mathbb{I}_K/K^\times$.

Finally, we arrive at a description of the idelic Artin map $\varphi_{L/K}$ that doesn't require admissible moduli and illustrates the local-global principle.

**Theorem 3.10**

For a finite abelian extension of number fields $L/K$ and $x \in \mathbb{I}_K$

$$\varphi_{L/K}(x) = \prod_v (x_v, L_w/K_v) \tag{8}$$

where $w$ is an arbitrary place in $L$ over $v$ and the local Artin symbol $(x_v, L_w/K_v) \in \mathrm{Gal}(L_w/K_v)$ is viewed in $D(w \mid v)$.

On the right side of (8), all but finitely many factors are trivial since for all but finitely many $v$, $L_w/K_v$ is unramified, $x_v \in \mathcal{O}_v^\times$, and $\mathcal{O}_v^\times \subseteq \mathcal{N}_{L_w/K_v}(L_w^\times)$ for unramified $v$. The hard step in the proof of (8) is showing the right side is trivial on $K^\times$. This is **exactly** Hasse's product formula 3.6, which is equivalent to the Artin reciprocity law, whose hard step classically was the proof that the global Artin map is trivial on $P_{\mathfrak{m}}$. So we see that all the new notation doesn't make class field theory easier, or change what the hard step is, but the formalism surrounding the difficulties is much more elegant. Reproving Theorem 3.9 by using the right side of (8) as a new definition of the idelic Artin map lets global class field theory be derived from local class field theory.

## 3.4 Algebraic Approach to Hilbert's Reciprocity

Assume that $K$ contains a primitive $n$th root of 1. Thus $\mu_n = \{e^{\frac{2\pi i k}{n}} \mid 1 \le k \le n\} \simeq \mathbb{Z}/n\mathbb{Z}$ obtain an structure of $G$-module. In particular, $\mu_n \otimes_{\mathbb{Z}} \mu_n \simeq \mu_n$, and so $H^2(G, \mu_n \otimes_{\mathbb{Z}} \mu_n) \simeq H^2(G, \mu_n)$. There is a canonical isomorphism

$$H^2(G, \mu_n) \otimes_{\mathbb{Z}} \mu_m \xrightarrow{\sim} H^2(G, \mu_n \otimes_{\mathbb{Z}} \mu_n)$$

which can be defined as $x, y \mapsto x \cup y$. On combining this with the isomorphism $H^2(G, \mu_n) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ given by the invariant map, we obtain an isomorphism

$$H^2(G, \mu_n \otimes_{\mathbb{Z}} \mu_n) \simeq \mu_n$$

Thus we have a cup product pairing

$$\begin{array}{ccccc} H^1(G, \mu_n) & \times & H^1(G, \mu_n) & \longrightarrow & H^2(G, \mu_n \otimes_{\mathbb{Z}} \mu_n) \\ \wr & & \wr & & \wr \\ K^\times/(K^\times)^n & & K^\times/(K^\times)^n & & \mu_n \end{array}$$

by definition of $H^1$. For $a, b \in K^\times$, their image in $\mu_n$ under this paring is denoted $(a, b)$. The pairing is called the **Hilbert symbol**.

**Theorem 3.11**

The Hilbert symbol has the following properties:

*(1).* It is bi-multiplicative, i.e.

$$(aa', b) = (a, b)(a', b),\ \ (a, bb') = (a, b)(a, b')$$

*(2).* It is skew-symmetric, i.e.

$$(b, a) = (a, b)^{-1}$$

*(3).* It is non-degenerate, i.e.

$$(a, b) = 1 \text{ for all } b \in K^\times/(K^\times)^n \Rightarrow a \in (K^\times)^n$$

$$(a, b) = 1 \text{ for all } a \in K^\times/(K^\times)^n \Rightarrow b \in (K^\times)^n$$

*(4).* $(a, b) = 1$ if and only if $b$ is a norm from $K[a^{\frac{1}{n}}]$.

We may now deduce the following proposition from Theorem 3.11:

**Proposition 3.1**

Let $K$ be a local field containing a primitive $n$th root of 1. Any element of $K^\times$ that is a norm from every cyclic extension of $K$ of degree dividing $n$ is an $n$th power.

*Proof.* If $b$ is norm from $K[a^{\frac{1}{n}}]$ for all $a$, then $(a, b) = 1$ for all $a$, and hence $b \in (K^\times)^n$. □

The Hilbert symbol is related to the local Artin map by the formula

$$\varphi_K(b)(a^{\frac{1}{n}}) = (a, b)a^{\frac{1}{n}}$$

where $\varphi_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ is the local Artin map. For $K$ global, let $\phi_K : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ denotes the global (idelic) Artin map with respect to the field $K$. Since $\phi|_{K^\times}$ is trivial, we have

$$\prod_v (a, b)_v = \prod_v \frac{\phi_{K_v}(b)(a^{\frac{1}{n}})}{a^{\frac{1}{n}}}$$

Meanwhile, by 3.10, we have that

$$\phi_K(b) = \prod_v \phi_{K_v}(b) = \mathrm{id}$$

Hilbert's reciprocity law follows at once.

# A Appendix: Basic Properties of Lemniscate Sine Function

In section 2.4 we have seen how Abel constructed elliptic functions (i.e. doubly-periodic meromorphic functions on $\mathbb{C}$). Today's courses on complex analysis build the theory of elliptic functions around Liouville's theorems; here we will review the basic theorems and then show how to derive Abel's results on $\operatorname{sl} z$ from them.

**Definition A.1 (Divisor)**

Let $f$ be an elliptic function with period lattice $\Lambda$, we define the **divisor** of an elliptic function as a formal sum

$$\operatorname{div} f := (f) := \sum_{p \in \mathbb{C}/\Lambda} v_p(f) \cdot (p)$$

where $v_p(f)$ denotes the order of $f$ at the point $p$. Any finite formal sum

$$D = \sum_{p \in \mathbb{C}/\Lambda} n_p \cdot (p)$$

is called a **divisor** on $\mathbb{C}/\Lambda$; $D$ is called **principal** if there exists an elliptic function $f$ on $\mathbb{C}/\Lambda$ such that $D = (f)$. The **degree** of $D$ is defined to be the integer

$$\deg(D) = \sum_{p \in \mathbb{C}/\Lambda} n_p$$

which can be viewed as the difference between the number of zeros and the number of poles if $D = (f)$.

Using some basic results of complex analysis we find

**Proposition A.1**

1. Elliptic functions without poles are constant. In particular, if $f$ and $g$ are elliptic functions such that $(f) = (g)$, then $f = c \cdot g$ for some $c \in \mathbb{C}\backslash\{0\}$.
2. Elliptic functions have only finitely many poles in $\mathbb{C}/\Lambda$, and the sum of their residues is 0. In particular, elliptic functions have at least two poles.
3. $\deg((f)) = 0$.

*Proof.* *1.* Liouville's theorem states that the only bounded holomorphic function on $\mathbb{C}$ are constants. If $f$ is an elliptic function without a pole, then $f$ is bounded on $\mathbb{C}/\Lambda$ and hence on $\mathbb{C}$: therefore it must be constant. Since $(f) = (g)$ implies that $f/g$ is an elliptic function without poles, it must be constant.

*2.* The residue theorem induces the conclusion at once by integrating $f$ along the boundary of the parallelogram fundamental domain of $\mathbb{C}/\Lambda$ (WLOG, we may assume $f$ is holomorphic on the boundary since $f$ only has finite poles).

*3.* It follows at once by taking $g = f'/f$ in *2.* □

Next comes to the construction of Weierstraß' $\sigma$ functions. We want the $\sigma$ function to be a function with simple zeros in $\lambda \in \Lambda$; the function

$$z \prod_{\lambda \neq 0} (1 - z\lambda^{-1})$$

would be such a function: unfortunately it does not converge. Weierstraß' idea was to multiply the factors in this product by functions without zeros that would make the product convergent:

$$\sigma(z) = \sigma(z, \Lambda) = z \prod_{\lambda \in \Lambda \setminus \{0\}} \left(1 - \frac{z}{\lambda}\right) \exp\left(\frac{z}{\lambda} + \frac{z^2}{2\lambda^2}\right)$$

We now introduce an efficient tool for constructing elliptic functions with prescribed poles and zeros:

**Theorem A.1 (Abel's Theorem)**

Let $D$ be a given divisor on $\mathbb{C}/\Lambda$ of degree zero, then there exists an elliptic function $f$ with divisor $D$ if and only if

$$\sum_{p \in \mathbb{C}/\Lambda} D_p \cdot p \equiv 0 \pmod{\Lambda}$$

where $D_p$ is the composition of $D$ at the point $p$.

*Proof.* If $D$ is a divisor of degree 0 such that

$$\sum_{p \in \mathbb{C}/\Lambda} D_p \cdot p \equiv 0 \pmod{\Lambda}$$

Then the properties of the $\sigma$-function show that

$$\prod_{p \in \mathbb{C}/\Lambda} \sigma(z-p)^{D_p}$$

is an elliptic function with period lattice $\Lambda$ and divisor $(D)$, here we choose $p$ as a representative element in $\mathbb{C}$ with respect to $\mathbb{C}/\Lambda$. The converse can be easily shown by Riemann-Roch theorem. □

This theorem allows us to construct the elliptic function $\operatorname{sl} z$ at a single stroke: we simply choose the divisor $D = (0) + (\frac{1+i}{2}) - (\frac{1}{2}) - (\frac{i}{2})$ on the lattice $\Lambda = \mathbb{Z}[i]$; since the condition in theorem A.1 is satisfied, there must be an elliptic function $\phi$ with $(\phi) = D$. In fact there are infinitely many, all differing by a constant factor $c \neq 0$. By demanding $\phi(\frac{1+i}{4}) = 1$ we get a uniquely determined elliptic function $\phi(z)$. We claim in fact that $\phi(iz) = i\phi(z)$. In fact, since $\phi(iz)$ is an elliptic function with the same divisor as $\phi$, the quotient $\phi(iz)/\phi(z)$ must be a constant function. Developing $\phi(z)$ into a Taylor series at $z = 0$ we find that $\phi(iz)$ $i\phi(z)$ near 0. Finally we claim that $\phi(z)\phi(z - \frac{1}{2}) = i$. Since $\phi(z)$ and $\phi(z - \frac{1}{2})$ have inverse divisors, their product must be constant. Therefore it is sufficient to evaluate it at $z = \frac{1+i}{4}$; we find $\phi(\frac{1+i}{4})\phi(\frac{-1+i}{4}) = i\phi(\frac{1+i}{4})^2 = i$, proposition 2.3 *1,2* follows.

Now it remains to prove *3* in proposition 2.3. To this end, observe that the function $\psi(z) = \phi(\nu z)$ has the divisor

$$(\psi) = \sum \left(\frac{\alpha}{\nu}\right) + \left(\frac{\alpha}{\nu} + \frac{1+i}{2}\right) - \left(\frac{\alpha}{\nu} + \frac{1}{2}\right) + \left(\frac{\alpha}{\nu} + \frac{i}{2}\right)$$

where the sums are over a complete set of residues $\alpha$ modulo $\nu$. Moreover, $\phi(z - \frac{\alpha}{\nu})$ has the divisor

$$\left(\frac{\alpha}{\nu}\right) + \left(\frac{\alpha}{\nu} + \frac{1+i}{2}\right) - \left(\frac{\alpha}{\nu} + \frac{1}{2}\right) + \left(\frac{\alpha}{\nu} + \frac{i}{2}\right)$$

hence $\phi(\nu z)$ and $\prod \phi(z - \frac{\alpha}{\nu})$ differ at most by a constant factor $\delta_\nu$. In order to compute $\delta_n u$ we put $\gamma = \frac{1+i}{4}$; using property *2* we find

$$\phi\left(\gamma + \frac{\alpha}{\nu}\right)\phi\left(\gamma - \frac{i\alpha}{\nu}\right) = -i\phi\left(\gamma + \frac{\alpha}{\nu}\right)\phi\left(i\gamma + \frac{\alpha}{\nu}\right) = -i\phi\left(\gamma + \frac{\alpha}{\nu}\right)\phi\left(\gamma + \frac{\alpha}{\nu} + \frac{1}{2}\right) = 1$$

Since there exists a 'half system' $M$ of residue classes such that exactly one of $\alpha$ and $-\alpha$ is in $M$, we conclude that

$$\prod \phi\left(\gamma + \frac{\alpha}{\nu}\right) = 1$$

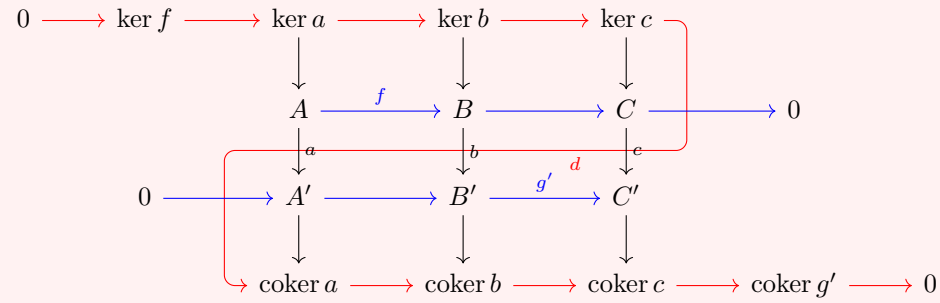
Thus $\delta_\nu = \phi(\nu\gamma)$. But now $\phi(\nu\gamma) = \phi(\varepsilon_\nu\gamma + (\nu - \varepsilon_\nu)\gamma) = \phi(\varepsilon_\nu\gamma) = \varepsilon_\nu\phi(\gamma) = \varepsilon_\nu$, *3* holds.

# B Cohomology of groups

## B.1 Preliminaries from Homological Algebra

**Lemma B.1 (The Extended Snake Lemma)**

The exact commutative diagram in blue gives rise to the exact sequence in red




**Lemma B.2 (Kernel-Cokernel Lemma)**

Every pair of homomorphisms

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

of abelian groups gives rise to an exact sequence

$$0 \longrightarrow \ker f \longrightarrow \ker g \circ f \xrightarrow{f} \operatorname{coker} f \longrightarrow \operatorname{coker} g \circ f \longrightarrow \operatorname{coker} g \longrightarrow 0$$

**Definition B.1 (Category)**

A **category** $\mathscr{C}$ consists of a nonempty class $\mathrm{Obj}(\mathscr{C})$ of objects, a set $\mathrm{Hom}(A, B)$ for each pair of objects $A$, $B$ (called the set of **morphisms** from $A$ to $B$), and a map

$$(\alpha, \beta) \mapsto \beta \circ \alpha : \mathrm{Hom}(A, B) \times \mathrm{Hom}(B, C) \mapsto \mathrm{Hom}(A, C)$$

for each triple of objects $A$, $B$ and $C$, satisfying the following conditions:

*(1).* composition of morphisms is associative.

*(2).* for each object $A$, $\mathrm{Hom}(A, A)$ has an element $\mathrm{id}_A$ that is left and right identity for composition.

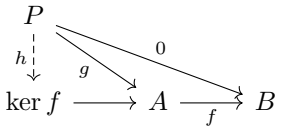
It is to be understood that the set $\mathrm{Hom}(A, B)$ are disjoint, so that a morphism determines its source and target.

A **covariant functor** $F : \mathscr{C} \to \mathscr{D}$ is **left-adjoint** to the functor $G : \mathscr{D} \to \mathscr{C}$ if there is a natural isomorphism

$$\mathrm{Hom}_{\mathscr{D}}(F(A), B) \simeq \mathrm{Hom}_{\mathscr{C}}(A, G(B))$$

If the sets $\mathrm{Hom}(A, B)$ are endowed with the structures of abelian groups in such a way that the composition maps are bi-additive, and every finite collection of objects in $\mathscr{C}$ has a direct sum, then $\mathscr{C}$ (together with the structures) is called an **additive category**. The **kernel** $\ker f$ of a morphism $f : A \to B$ is defined by the following universal property: For all objects $P$ with morphisms $g : P \to A$ such that $f \circ g = 0$, there exists

unique morphism $h : P \to \ker f$ such that the following diagram commutes.




and the definition of cokernel is the dual of the one of kernel. The kernel of the cokernel $B \to \operatorname{coker} f$ is called the **image** of $f$, and the cokernel of the kernel $\ker f \to A$ is called the **coimage** of $A$. If $\mathscr{C}$ is an additive category in which every morphism has both a kernel and a cokernel, and the induced morphism $\operatorname{coim} f \to \operatorname{im} f$ is always an isomorphism, then $\mathscr{C}$ is called an **abelian category**. An object $I$ of $\mathscr{C}$ is **injective** if $\operatorname{Hom}(\cdot, I)$ is an exact functor. An abelian category $\mathscr{C}$ is said to have **enough injectives** if every object admits an injective homomorphism into an an injective object.

**Definition B.2 (Resolution)**

Let $\mathscr{C}$ be an abelian category with enough injectives, and let $F : \mathscr{C} \to \mathscr{D}$ be a left exact functor from $\mathscr{C}$ to a second abelian category $\mathscr{D}$. Let $M$ be an object of $\mathscr{C}$. A **resolution** of $M$ is a long exact sequence

$$0 \longrightarrow M \longrightarrow I^0 \xrightarrow{d^0} I_1 \xrightarrow{d^1} \cdots \xrightarrow{d^{r-1}} I^r \xrightarrow{d^r} I^{r+1} \xrightarrow{d^{r+1}} \cdots$$

If the $I^r$'s are injective objects of $\mathscr{C}$, then it is called an **injective resolution**. We sometimes denote this complex by $M \to I^\bullet$.

Two morphisms $\alpha^\bullet, \beta^\bullet : I^\bullet \to J^\bullet$ of complexes are said to be **homotopic** if there exists a family of morphisms $k^r : I^r \to J^{r-1}$ such that

$$\alpha^r - \beta^r = e^{r-1} \circ k^r + k^{r+1} \circ d^r$$

for all $r$.

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & I^{r-1} & \xrightarrow{d} & I^r & \xrightarrow{d} & I^{r+1} & \longrightarrow & \cdots \\
 & & \downarrow & \swarrow_{k} & \downarrow & \swarrow_{k} & \downarrow & & \\
\cdots & \longrightarrow & J^{r-1} & \xrightarrow[e]{} & J^r & \xrightarrow[e]{} & J^{r+1} & \longrightarrow & \cdots
\end{array}$$

Especially, we call $\alpha^\bullet : I^\bullet \to J^\bullet$ a **homotopy equivalence** if and only if there exists $\beta : J^\bullet \to I^\bullet$ such that $\alpha^\bullet \circ \beta^\bullet$ is homotopic to $\mathrm{id}_J^\bullet$ and $\beta^\bullet \circ \alpha^\bullet$ is homotopic to $\mathrm{id}_I^\bullet$. If there exists a homotopy equivalence from $I^\bullet$ to $J^\bullet$, then $I^\bullet$ and $J^\bullet$ are said to be **homotopy equivalent**.

**Proposition B.1**

Homotopic homomorphisms $\alpha^\bullet, \beta^\bullet : I^\bullet \to J^\bullet$ define the same morphisms on cohomology.

**Proposition B.2**

Let $M \to I^\bullet$ and $N \to J^\bullet$ be two injective resolutions of objects $M$ and $N$ of $\mathscr{C}$, then every morphism $\alpha : M \to N$ extends to a morphism

$$\begin{array}{ccc}
M & \longrightarrow & I^\bullet \\
{\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\alpha^\bullet} \\
N & \longrightarrow & J^\bullet
\end{array}$$

and any two extensions $\alpha^\bullet$ and $\beta^\bullet$ of $\alpha$ to $I^\bullet \to J^\bullet$ are homotopic. Especially, if $N = M$ and $\alpha = \mathrm{id}_M$, then $\alpha^\bullet$ define an homotopy equivalence.

For each object $A \in \mathrm{Obj}(\mathscr{C})$ with injective resolution $A \to I^\bullet$ and a left-exact covariant functor $F : \mathscr{C} \to \mathscr{D}$, we define the **right-derived functors** of $F$ by

$$(R^q F)(A) = H^q(F(I^\bullet))$$

Notice that each two injective resolutions $A \to I^\bullet$ and $A \to J^\bullet$ of $A$ are homotopy equivalent, hence $F(A) \to F(I^\bullet)$ and $F(A) \to F(J^\bullet)$ are homotopy equivalent, hence define the same cohomology, $R^q F$ is well-defined.

**Proposition B.3**

Let

$$0 \longrightarrow A' \xrightarrow{f} A \xrightarrow{g} A'' \longrightarrow 0$$

be an exact sequence in the category $\mathscr{C}$, $J^\bullet$ and $K^\bullet$ are injective resolutions of $A'$ and $A''$ respectively. Under these conditions there exists an injective resolution $I^\bullet$ of $A$ satisfying the following conditions:

*(a).* There exists the morphisms of complexes $f^\bullet$ and $g^\bullet$ such that

$$0 \longrightarrow J^\bullet \xrightarrow{f^\bullet} I^\bullet \xrightarrow{g^\bullet} K^\bullet \longrightarrow 0$$

is exact.

*(b).* For any $n \geq 0$, $I^n \simeq J^n \oplus K^n$. We denote by $i_J^n, i_K^n$ the canonical injections and by $p_J^n, p_K^n$ the canonical projections.

*(c).* The diagram

$$\begin{array}{ccccc} A' & \xrightarrow{f} & A & \xrightarrow{g} & A'' \\ \downarrow & & \downarrow & & \downarrow \\ J^\bullet & \longrightarrow & I^\bullet & \longrightarrow & K^\bullet \end{array}$$

is commutative.

*(d).* $f^\bullet = i_J^\bullet$, $g^\bullet = p_K^\bullet$.

The proposition indicates that each exact sequence can be extended into a commutative diagram

with exact rows and exact columns and $I^\bullet = J^\bullet \oplus K^\bullet$, hence we have commutative diagram

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & F(J^0) & \longrightarrow & F(I^0) & \longrightarrow & F(K^0) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & F(J^1) & \longrightarrow & F(I^1) & \longrightarrow & F(K^1) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & \vdots & & \vdots & & \vdots & & \end{array}$$

with exact rows, which gives rise to a long exact sequence

$$\begin{array}{l} 0 \longrightarrow R^0F(J^\bullet) \longrightarrow R^0F(I^\bullet) \longrightarrow R^0F(K^\bullet) \\ \qquad\qquad \hookrightarrow R^1F(J^\bullet) \longrightarrow R^1F(I^\bullet) \longrightarrow \cdots \end{array} \tag{9}$$

and a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & B' & \longrightarrow & B & \longrightarrow & B'' & \longrightarrow & 0 \end{array}$$

gives rise to a commutative diagram

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & R^{r-1}F(A'') & \longrightarrow & R^rF(A') & \longrightarrow & R^rF(A) & \longrightarrow & R^rF(A'') & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & R^{r-1}F(B'') & \longrightarrow & R^rF(B') & \longrightarrow & R^rF(B) & \longrightarrow & R^rF(B'') & \longrightarrow & \cdots \end{array} \tag{10}$$

In fact, the right derived functors of $F$ are uniquely determined (up to a unique isomorphism of functors) by the following three properties:

1. $R^0F = F$.
2. $R^F(I) = 0$ for $r > 0$ when $I$ is injective.
3. The properties (9) and (10).

**Definition B.3 (The Ext groups)**

If $\mathscr{C}$ has enough injectives, then we can define the right derived functors of the left exact functor $\mathrm{Hom}(A, \cdot)$. Denote the $r$th right derived functor by $\mathrm{Ext}^r(A, \cdot)$. To compute $\mathrm{Ext}^r(A, B)$, we choose an injective resolution $B \to I^\bullet$ of $B$, and set

$$\mathrm{Ext}^r(A, B) = H^r(\mathrm{Hom}(A, I^\bullet))$$

If $\mathscr{C}$ has enough projectives, then we can define the right derived functors of the left exact contravariant functor $\mathrm{Hom}(\cdot, B)$. Denote the $r$th right derived functor by $\mathrm{Ext}^r(\cdot, B)$. To compute $\mathrm{Ext}^r(A, B)$, we choose a projective resolution $P_\bullet \to A$ of $A$, and we set

$$\mathrm{Ext}^r(A, B) = H^r(\mathrm{Hom}(P_\bullet, B))$$

**Proposition B.4**

If $\mathscr{C}$ has enough injectives and enough projectives, then the two definition of $\mathrm{Ext}^r(A, B)$ coincide.

## B.2 Cohomology

If $M$ and $N$ are $G$-modules, then the set $\mathrm{Hom}_{\mathbf{Ab}}(M, N)$ of homomorphisms becomes a $G$-module with the structure

$$\begin{aligned} (\varphi + \varphi')(m) &= \varphi(m) + \varphi'(m) \\ (g\varphi)(m) &= g(\varphi(g^{-1}m)) \end{aligned}$$

For $H$ a subgroup of $G$ and an $H$-module $M$, we define $\mathrm{Ind}_H^G(M)$ to be the set of maps $\varphi : G \to M$ such that $\varphi(hg) = h\varphi(g)$ for all $h \in H$. Then $\mathrm{Ind}_H^G(M)$ becomes a $G$-module with the operations

$$(\varphi + \varphi')(x) = \varphi(x) + \varphi'(x)$$
$$(g\varphi)(x) = \varphi(xg)$$

A homomorphism $\alpha : M \to M'$ of $H$-modules defines a homomorphism

$$\varphi \mapsto \alpha \circ \varphi : \mathrm{Ind}_H^G(M) \to \mathrm{Ind}_H^G(M')$$

of $G$-modules.

**Lemma B.3**

*(1).* For every $G$-module $M$ and $H$-module $N$,

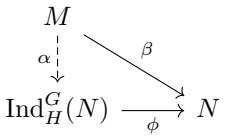
$$\mathrm{Hom}_G(M, \mathrm{Ind}_H^G(N)) \simeq \mathrm{Hom}_H(M, N)$$

*(2).* The functor

$$\mathrm{Ind}_H^G : \mathbf{Mod}_H \to \mathbf{Mod}_G$$

is exact

Let $\phi$ denote the map $\mathrm{Ind}_H^G(N) \to N$, $\varphi \mapsto \varphi(1_G)$, the lemma shows that $\mathrm{Ind}_H^G(N)$ has the following universal property: For any $H$-homomorphism $\beta : M \to N$, there exist a unique $G$-homomorphism $\alpha : M \to \mathrm{Ind}_H^G(N)$ such that $\phi \circ \alpha = \beta$.




For a $G$-module $M$, define

$$M^G = \{m \in M \mid gm = m \text{ for all } g \in G\}$$

The functor $(-)^G$ is left exact since it is isomorphic to $\mathrm{Hom}_G(\mathbb{Z}, -)$. Let $\mathrm{Ind}^G$ denote $\mathrm{Ind}_{\{1\}}^G$, we call $M$ is an **induced** $G$-module if $M = \mathrm{Ind}^G(M_0)$ for some abelian group $M_0$.

**Lemma B.4 (Shapiro's Lemma)**

Let $H$ be a subgroup of $G$. For every $H$-module $N$, there is a canonical isomorphism

$$H^r(G, \mathrm{Ind}_H^G(N)) \xrightarrow{\sim} H^r(H, N)$$

for all $r \geq 0$.

**Remark B.1**

Consider an exact sequence

$$0 \longrightarrow M \longrightarrow J \longrightarrow N \longrightarrow 0$$

of $G$-modules. If $H^r(G, J) = 0$ for all $r > 0$, then the cohomology sequence becomes the exact sequence

$$0 \longrightarrow M^G \longrightarrow J^G \longrightarrow N^G \longrightarrow H^1(G, M) \longrightarrow 0$$

and the collection of isomorphisms

$$H^r(G, N) \xrightarrow{\sim} H^{r+1}(G, M) \text{ for } r \geq 1$$

Let $P_r$ be the free $\mathbb{Z}$-module with basis the $(r+1)$-tuples $(g_0, g_1, \cdots, g_r)$ of elements of $G$, endowed the action of $G$ such that

$$g(g_0, \cdots, g_r) = (gg_0, \cdots, gg_r)$$

Note that $P_r$ is also free as a $\mathbb{Z}[G]$-module, with basis $\{(1, g_1, \cdots, g_r) \mid g_i \in G\}$. Define a homomorphism $d_r : P_r \to P_{r-1}$ by the rule

$$d_r(g_0, \cdots, g_r) = \sum_{i=0}^{r} (-1)^i (g_0, \cdots, \hat{g}_i, \cdots, g_r)$$

where the symbol $\hat{\cdot}$ means that $\cdot$ is omitted. Let $P_\bullet$ be

$$\cdots \longrightarrow P_r \xrightarrow{d_r} P_{r-1} \longrightarrow \cdots \longrightarrow P_0$$

One checks easily that $d_{r-1} \circ d_r = 0$, and so this is a complex.

**Lemma B.5**

The complex $P_\bullet \longrightarrow \mathbb{Z} \longrightarrow 0$ is exact.

An element of $\mathrm{Hom}(P_r, M)$ can be identified with a function $\varphi : G^{r+1} \to M$, and $\varphi$ is fixed by $G$, i.e.

$$\varphi(gg_0, \cdots, gg_r) = g(\varphi(g_0, \cdots, g_r)) \text{ for all } g, g_1, \cdots, g_r \in G$$

Thus $\mathrm{Hom}_G(P_r, M)$ can be identified with the set $\tilde{C}^r(G, M)$ of $\varphi$ satisfying this condition. Such $\varphi$ are called **homogeneous $r$-cochains of $G$ with values in $M$**. The boundary map $d^r : \tilde{C}^r(G, M) \to \tilde{C}^{r+1}(G, M)$ induced by $d_{r+1}$ is

$$(\tilde{d}^r \varphi)(g_0, \cdots, g_{r+1}) = \sum_{i=0}^{r} (-1)^i \varphi(g_0, \cdots, \hat{g}_i, \cdots, g_{r+1})$$

Proposition **??** says that

$$H^r(G, M) \simeq \ker(\tilde{d}^r) / \mathrm{im}(\tilde{d}^{r-1})$$

A homogeneous cochain $\varphi : G^{r+1} \to M$ is determined by its values on the elements $(1, g_1, \cdots, g_1 \cdots g_r)$. We are therefore led to introduce the group $C^r(G, M)$ of **inhomogeneous $r$-cochains of $G$ with values in $M$** consisting of all maps $\varphi : G^r \to M$. We set $G^0 = \{1\}$, so that $C^0(G, M) = M$. Define

$$d^r : C^r(G, M) \to C^{r+1}(G, M)$$

by

$$(d^r \varphi)(g_1, \cdots, g_{r+1}) = g_1 \varphi(g_2, \cdots, g_{r+1}) + \sum_{j=1}^{r} (-1)^j \varphi(g_1, \cdots, g_j g_{j+1}, \cdots, g_{r+1}) + (-1)^{r+1} \varphi(g_1, \cdots, g_r)$$

Define $Z^r(G,M) = \ker(d^r)$ (group of $r$-cocycles) and $B^r(G,M) = \mathrm{im}(d^{r-1})$ (group of $r$-coboundaries).

**Proposition B.5**

The sequence of maps

$$C^0(G,M) \xrightarrow{d^0} C^1(G,M) \xrightarrow{d^1} \cdots \xrightarrow{d^{r-1}} C^r(G,M) \xrightarrow{d^r} C^{r+1}(G,M) \longrightarrow \cdots$$

is a complex and there is a canonical isomorphism

$$H^r(G,M) \simeq Z^r(G,M)/B^r(G,M)$$

The isomorphism is clear if for $\varphi \in \tilde{C}^r(G,M)$ we take $\varphi' \in C^r(G,M)$ such that

$$\varphi'(g_1, \cdots, g_r) = \varphi(1, g_1, \cdots, g_1 \cdots g_r)$$

Let $M$ be an abelian group. An **extension of $G$ by $M$** is an exact sequence of groups

$$1 \longrightarrow M \longrightarrow E \longrightarrow G \longrightarrow 1$$

We set

$$\sigma m = s(\sigma) \cdot m \cdot s(\sigma)^{-1}$$

where $s(\sigma)$ is any element of $E$ mapping to $\sigma$. Now choose a section $s$ to $\pi$, i.e., a map $s : G \to E$ such that $\pi \circ s = \mathrm{id}$. Then $s(\sigma)s(\sigma')$ and $s(\sigma\sigma')$ both map to $\sigma\sigma' \in G$, and so they differ by an element $\varphi(\sigma,\sigma') \in M$:

$$s(\sigma)s(\sigma') = \varphi(\sigma,\sigma') \cdot s(\sigma\sigma')$$

From

$$s(\sigma)(s(\sigma')s(\sigma'')) = (s(\sigma)s(\sigma'))s(\sigma'')$$

we deduce that

$$\sigma\varphi(\sigma',\sigma'') = \varphi(\sigma,\sigma') \cdot \varphi(\sigma\sigma',\sigma'')$$

i.e., $\varphi \in Z^2(G,M)$. Assume $s'$ is a second section, then let $\varphi'(\sigma,\sigma') = s'(\sigma)s'(\sigma')s'^{-1}(\sigma\sigma')$, we have

$$\begin{aligned}\varphi'(\sigma,\sigma')\varphi^{-1}(\sigma,\sigma') &= s'(\sigma)s'(\sigma')s'^{-1}(\sigma\sigma')s(\sigma\sigma')s^{-1}(\sigma')s^{-1}(\sigma) \\ &= \sigma(s'(\sigma')s^{-1}(\sigma)) \cdot (s'(\sigma)s^{-1}(\sigma))^{-1} \cdot (s'(\sigma)s^{-1}(\sigma)) \\ &= \sigma(\phi(\sigma')) \cdot \phi^{-1}(\sigma\sigma') \cdot \phi(\sigma) = d^1\phi(\sigma,\sigma')\end{aligned}$$

where $\phi(\sigma) = s'(\sigma)s^{-1}(\sigma)$, and so the class of $\varphi$ in $H^2(G,M)$ is independent of the choice of $s$. Every such $\varphi$ arises from an extension. In this way, $H^2(G,M)$ classifies the isomorphism classes of extension of $G$ by $M$ with a fixed action of $G$ on $M$.

**Proposition B.6 (Hilbert's Theorem 90)**

Let $L/K$ be a finite Galois extension with Galois group $G$. Then $H^1(G, L^\times) = 0$.

*Proof.* Let $\varphi \in Z^1(G, L^\times)$ be a crossed homomorphism. In multiplicative notation, this means that

$$\varphi(\sigma\tau) = \sigma\varphi(\tau) \cdot \varphi(\sigma)$$

and it remains to find a $c \in L^\times$ such that $\varphi(\sigma) = \sigma c/c$. For $a \in L^\times$, let

$$b = \sum_{\sigma \in G} \varphi(\sigma) \cdot \sigma a$$

Suppose $b \neq 0$, then

$$\tau b = \sum_{\sigma \in G} \tau\varphi(\sigma) \cdot \tau\sigma a = \varphi(\tau)^{-1} \cdot b$$

Hence

$$\varphi(\tau) = \frac{b}{\tau b} = \frac{\tau b^{-1}}{b^{-1}}$$

which shows that $\varphi \in Z^1(G, M)$. It remains to show that $b \neq 0$ for some $a$, which is direct since every finite set $\{f_i\}$ of distinct homomorphisms $G \to L^\times$ is linearly independent over $L$. □

**Corollary B.1 (Hilbert's Theorem 90)**

Let $L/K$ be a cyclic extension with Galois group generated by $\sigma$. If $\mathcal{N}_{L/K}(a) = 1$, then $a$ is of the form $\sigma b/b$.

*Proof.* Notice that

$$\varphi \in Z^1(G, L^\times) \longleftrightarrow \varphi(\sigma^n) = \prod_{i=0}^{n-1} \sigma^i\varphi(\sigma) \text{ and } \mathcal{N}_{L/K}(\varphi(\sigma)) = 1 \longleftrightarrow \varphi \in B^1(G, L^\times)$$

which indicates that $\mathcal{N}_{L/K}(a) = 1 \Leftrightarrow a = \sigma b/b$ for some $b \in L^\times$. □

**Proposition B.7**

Let $L/K$ be finite Galois extension with Galois group $G$, then $H^r(G, L) = 0$ for all $r > 0$.

*Proof.* There exists an $\alpha \in L$ such that $\{\sigma\alpha \mid \sigma \in G\}$ is a basis for $L$ as a $K$-vector space, and it defines an isomorphism of $G$-modules

$$\begin{array}{ccc} K[G] & \longrightarrow & L \\ \displaystyle\sum_{\sigma \in G} a_\sigma \sigma & \longrightarrow & \displaystyle\sum_{\sigma \in G} a_\sigma \sigma\alpha \end{array}$$

Hence $H^r(G, L) \simeq H^r(G, K[G]) \simeq H^r(G, \operatorname{Ind}^G K) = 0$. □

## B.3 Homology

Let $M$ be a $G$-module with projective resolution

$$\cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} M \longrightarrow 0$$

of $M$. The complex

$$\cdots \longrightarrow (\mathbb{Z}[G]/I_G) \otimes_{\mathbb{Z}[G]} P_2 \xrightarrow{d_2} (\mathbb{Z}[G]/I_G) \otimes_{\mathbb{Z}[G]} P_1 \xrightarrow{d_1} (\mathbb{Z}[G]/I_G) \otimes_{\mathbb{Z}[G]} P_0 \longrightarrow 0$$

need no longer be exact, where $I_G = \langle g - 1_G \rangle$, and we set

$$H_r(G, M) = \ker(d_r)/\operatorname{im}(d_{r+1})$$

Similarly, these groups have the following properties:

*(1).* $H_0(G, M) = M_G$.

*(2).* If $P$ is projective, then $H_r(G, P) = 0$ for all $r > 0$.

*(3).* Let $P_\bullet \to M$ and $Q_\bullet \to N$ be projective resolutions of $M$ and $N$. Any homomorphism $\alpha : M \to N$ of $G$-modules extends to a morphism of complexes

$$\begin{array}{ccc} P_\bullet & \longrightarrow & M \\ {\scriptstyle \alpha_\bullet}\downarrow & & \downarrow{\scriptstyle \alpha} \\ Q_\bullet & \longrightarrow & N \end{array}$$

and the homomorphisms $H_r(\alpha_\bullet)$ are independent of the choice of $\alpha_\bullet$.

*(4).* A short exact sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

of $G$-modules gives rise to a long exact sequence

$$\cdots \longrightarrow H_r(G, M) \longrightarrow H_r(G, M'') \longrightarrow H_{r-1}(G, M') \longrightarrow \cdots \longrightarrow H_0(G, M'') \longrightarrow 0$$

Moreover, the association "short exact sequence $\longmapsto$ long exact sequence" is functorial, i.e., a morphism of short exact sequences induces a morphism of long exact sequences.

**Remark B.2**

The family of functors $(H_r(G, \cdot))$ are uniquely determined by the above properties.

The **argumentation map** is

$$\mathbb{Z}[G] \to \mathbb{Z}, \ \sum n_g g \mapsto \sum n_g$$

Its kernel $I_G$ is called the **argumentation ideal**. Consider the exact (**argumentation**) sequence:

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0$$

The $G$-module $\mathbb{Z}[G]$ is projective, and so $H_1(G, \mathbb{Z}[G]) = 0$. Therefore we obtain an exact sequence of homology groups

$$0 \longrightarrow H_1(G, \mathbb{Z}) \longrightarrow I_G/I_G^2 \longrightarrow \mathbb{Z}[G]/I_G \longrightarrow \mathbb{Z} \longrightarrow 0$$

The middle map is induced by the inclusion $I_G \hookrightarrow \mathbb{Z}[G]$, and so is zero. Therefore the sequence shows that

$$H_1(G, \mathbb{Z}) \simeq I_G/I_G^2$$

**Proposition B.8**

There is a canonical isomorphism

$$H_1(G, \mathbb{Z}) \simeq G^{\mathrm{ab}}$$

## B.4 The Tate groups

**Definition B.4 (Norm map)**

For a $G$-module $M$, the **norm map** $\mathcal{N}_G : M \to M$ is defined to be

$$m \mapsto \sum_{g \in G} gm$$

then $I_G M \subseteq \ker \mathcal{N}_G, \operatorname{im} \mathcal{N}_G \subseteq M^G$.

Therefore we get an exact commutative diagram

$$\begin{array}{ccccccccc} & & & & M & \xrightarrow{\mathcal{N}_G} & M & & \\ & & & & \downarrow & & \uparrow & & \\ 0 & \longrightarrow & \ker(\mathcal{N}_G)/I_G M & \longrightarrow & M/I_G M & \longrightarrow & M^G & \longrightarrow & M^G/\mathcal{N}_G(M) \longrightarrow 0 \end{array}$$

The bottom row can be rewritten

$$0 \longrightarrow \ker(\mathcal{N}_G)/I_G M \longrightarrow H_0(G,M) \longrightarrow H^0(G,M) \longrightarrow M^G/\mathcal{N}_G(M) \longrightarrow 0$$

Tate defined

$$H_T^r(G,M) = \begin{cases} H^r(G,M) & r > 0 \\ M^G/\mathcal{N}_G(M) & r = 0 \\ \ker(\mathcal{N}_G(M)) & r = -1 \\ H_{-r-1}(G,M) & r < -1 \end{cases}$$

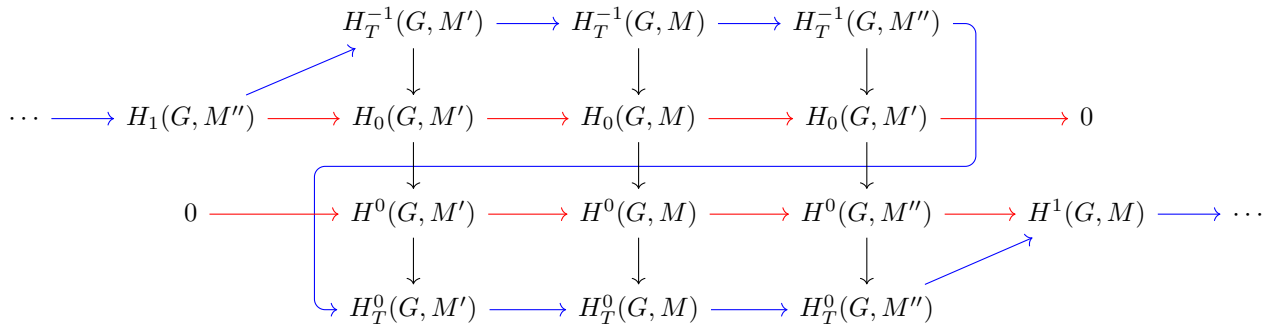
Thus, the exact sequence now becomes

$$0 \longrightarrow H_T^{-1}(G,M) \longrightarrow H_0(G,M) \xrightarrow{\mathcal{N}_G} H^0(G,M) \longrightarrow H_T^0(G,M) \longrightarrow 0$$

The above groups $H_T^r(G,M)$ are know as the **Tate cohomology groups**. Often $H_T^r(G,M)$ is denoted as $\hat{H}^r(G,M)$. For any short exact sequence of $G$-modules

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

we get a diagram




On applying the extended snake lemma 2.1 to the middle part of the diagram, we get a long exact sequence

$$\cdots \longrightarrow H_T^r(G,M') \longrightarrow H_T^r(G,M) \longrightarrow H_T^r(G,M'') \longrightarrow H_T^{r+1}(G,M) \longrightarrow \cdots$$

**Proposition B.9**

If $M$ is induced, then $H_T^r(G,M) = 0$ for all $r \in \mathbb{Z}$.

Let $H$ be a subgroup of $G$. We now obtain the **restriction homomorphisms**

$$\text{Res} : H^r(G,M) \to H^r(H,M)$$

which are constructed as follows: Let $M \to \text{Ind}_H^G(M)$ be the homomorphism sending $m$ to the map $g \mapsto gm$, which defines on cohomology with the isomorphism in Shapiro's Lemma **??**,

$$H^r(G,M) \to H^r(G, \text{Ind}_H^G(M)) \xrightarrow{\sim} H^r(H,M)$$

is the **restriction** map. Similarly, for every $G$-module $M$, there is a canonical homomorphism of $G$-modules

$$\varphi \mapsto \sum_{\bar{s}\in G/H} s\varphi(s^{-1}) : \mathrm{Ind}_H^G(M) \to M$$

the map on cohomology which it defines, when composed with the isomorphism in Shapiro's lemma, gives Cor,

$$H^r(H, M) \xrightarrow{\sim} H^r(G, \mathrm{Ind}_H^G(M)) \to H^r(G, M)$$

**Proposition B.10**

Let $H$ be a subgroup of $G$ of finite index. The composite

$$\mathrm{Cor} \circ \mathrm{Res} : H^r(G, M) \to H^r(G, M)$$

is multiplication by $(G : H)$.

**Corollary B.2**

If $(G : 1) = m$, then $mH^r(G, M) = 0$ for $r > 0$.

*Proof.* Multiplication by $m$ factors through $H^r(\{1\}, M) = 0$,

$$H^r(G, M) \xrightarrow{\mathrm{Res}} H^r(\{1\}, M) \xrightarrow{\mathrm{Cor}} H^r(G, M)$$

□

**Corollary B.3**

Let $G_p$ denotes a Sylow $p$-subgroup of $G$, then the $p$-primary component of $H^r(G, M)$ and $H^r(G_p, M)$ are the same, where the $p$-primary component of an abelian group is the subgroup consisting of all elements killed by some power of $p$.

**Lemma B.6**

For every finite group $G$,

*(1).* $H_T^r(G, \mathbb{Q}) = 0$ for all $r \in \mathbb{Z}$.

*(2).* $H_T^0(G, \mathbb{Z}) = \mathbb{Z}/(G : 1)\mathbb{Z}$ and $H^1(G, \mathbb{Z}) = 0$.

*(3).* There is a canonical isomorphism

$$\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^2(G, \mathbb{Z})$$

*Proof. (1).* The group $\mathbb{Q}$ is uniquely divisible, i.e., for all nonzero integers $m$, multiplication by $m : \mathbb{Q} \to \mathbb{Q}$ is an isomorphism. Therefore the map $H_T^r(m) : H_T^r(G, \mathbb{Q}) \to H_T^r(G, \mathbb{Q})$ is both zero and an isomorphism, which is possible only if $H_T^r(G, \mathbb{Q}) = 0$.
*(2).* Because $G$ acts trivially on $\mathbb{Z}$ and the norm map is multiplication by $(G : 1)$. Hence $H_T^0(G, \mathbb{Z}) = \mathbb{Z}/(G : 1)\mathbb{Z}$. Moreover, $H^1(G, \mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Z}) = 0$ since $\mathbb{Z}$ is torsion-free.
*(3).* The cohomology sequence of

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

is an exact sequence

$$H^1(G, \mathbb{Q}) \longrightarrow H^1(G, \mathbb{Q}/\mathbb{Z}) \longrightarrow H^2(G, \mathbb{Z}) \longrightarrow H^2(G, \mathbb{Q})$$

where $H^1(G,\mathbb{Q}) = H^2(G,\mathbb{Q}) = 0$, hence $H^2(G,\mathbb{Z}) \simeq H^1(G,\mathbb{Q}/\mathbb{Z}) \simeq \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$. □

**Proposition B.11**

Let $G$ be a cyclic group of finite order. The choice of a generator for $G$ determines isomorphisms

$$H_T^r(G,M) \xrightarrow{\sim} H_T^{r+2}(G,M)$$

for all $G$-modules $M$ and all $r \in \mathbb{Z}$.

*Proof.* Let $\sigma$ generates $G$, then the sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\sum g} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0$$

is exact. Thus

$$0 \longrightarrow M \longrightarrow \mathbb{Z}[G] \otimes_{\mathbb{Z}} M \xrightarrow{f} \mathbb{Z}[G] \otimes_{\mathbb{Z}} M \longrightarrow M \longrightarrow 0$$

is an exact sequence of $G$-modules, which splits into two exact sequence of $G$-modules:

$$0 \longrightarrow M \longrightarrow \mathbb{Z}[G] \otimes_{\mathbb{Z}} M \longrightarrow \mathrm{im}\, f \longrightarrow 0$$

and

$$0 \longrightarrow \mathrm{im}\, f \longrightarrow \mathbb{Z}[G] \otimes_{\mathbb{Z}} M \longrightarrow M \longrightarrow 0$$

By Remark **??**, the sequence defines isomorphism

$$H_T^r(G,M) \xrightarrow{\sim} H_T^{r+1}(G,\mathrm{im}\, f) \xrightarrow{\sim} H_T^{r+2}(G,M)$$

for all $r$. □

Let $G$ be a finite cyclic group, and let $M$ be a $G$-module. When the cohomology groups $H^r(G,M)$ are finite, we define the **Herbrand quotient** of $M$ to be

$$h(M) = \frac{|H_T^0(G,M)|}{|H_T^1(G,M)|}$$

**Proposition B.12**

Let $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ be an exact sequence of $G$-modules. If any two of the Herbrand quotients $h(M'), h(M), h(M'')$ are defined, then so also is the third, and

$$h(M) = h(M')h(M'')$$

*Proof.* We can truncate the long exact cohomology sequence as follows:

$$0 \longrightarrow K \longrightarrow H_T^0(M') \longrightarrow H_T^0(M) \longrightarrow H_T^0(M'') \longrightarrow H^1(M') \longrightarrow H^1(M) \longrightarrow H^1(M'') \longrightarrow K' \longrightarrow 0$$

where $K = \mathrm{coker}(H_T^{-1}(M) \longrightarrow H_T^{-1}(M'')) \simeq \mathrm{coker}(H_T^1(M) \longrightarrow H_T^1(M)) = K'$. The two statements are now obvious. □

**Proposition B.13**

If $M$ is a finite module, then $h(M) = 1$.

*Proof.* Consider the exact sequences

$$0 \longrightarrow M^G \longrightarrow M \xrightarrow{g-1} M \longrightarrow M_G \longrightarrow 0$$

and

$$0 \longrightarrow H_T^{-1}(M) \longrightarrow M_G \xrightarrow{\mathcal{N}_G} M^G \longrightarrow H_T^0(M) \longrightarrow 0$$

where $g$ is any generator of $G$. From the first sequence we find that $\#M^G = \#M_G$, and hence from the second that $\#H_T^{-1}(M) = \#H_T^0(M)$. □

**Corollary B.4**

Let $\alpha : M \to N$ be a homomorphism of $G$-modules with finite kernel and cokernel. If either $h(M)$ or $h(N)$ is defined, then so is the other, and they are equal.

*Proof.* Suppose $h(N)$ is defined, and consider the exact sequences

$$0 \longrightarrow \alpha(M) \longrightarrow N \longrightarrow \operatorname{coker}\alpha \longrightarrow 0$$

$$0 \longrightarrow \ker\alpha \longrightarrow M \longrightarrow \alpha(M) \longrightarrow 0$$

We find that $h(M) = h(\alpha(M)) = h(N)$. □

Let $H$ be a normal subgroup of $G$, let $\alpha$ be the quotient map $G \to G/H$, and let $\beta$ be the inclusion $M^H \hookrightarrow M$. In this case, we obtain the **inflation homomorphisms**.

$$\mathrm{Inf} : H^r(G/H, M^H) \longrightarrow H^r(G, M)$$

**Proposition B.14 (The inflation-restriction exact sequence)**

Let $H$ be a normal subgroup of $G$, and let $M$ be a $G$-module. Let $r$ be an positive integer. If $H^j(H, M) = 0$ for all $0 < j < r$, then the sequence

$$0 \longrightarrow H^r(G/H, M^H) \xrightarrow{\mathrm{Inf}} H^r(G, M) \xrightarrow{\mathrm{Res}} H^r(H, M)$$

is exact.

**Theorem B.1**

Let $G$ be a finite group, and let $M$ be a $G$-module. If

$$H^1(H, M) = H^2(H, M) = 0$$

for all subgroups $H$ of $G$, then $H_T^r(G, M) = 0$ for all $r \in \mathbb{Z}$.

*Proof.* If $G$ is cyclic, this follows from the periodicity of the cohomology. Assume now that $G$ is solvable. We shall prove the theorems in the case by induction on the order of $G$. Since $G$ is solvable, it contains a proper normal subgroup $H$ such that $G/H$ is cyclic, and $(H, M)$ satisfies the hypothesis of the theorem, $H^r(H, M) = 0$ for all $r$. Therefore (By proposition **??**) we have exact sequences

$$0 \longrightarrow H^r(G/H, M^H) \longrightarrow H^r(G, M) \longrightarrow H^r(H, M)$$

for all $r \geq 1$. Because $H^1(G, M) = H^2(G, M) = 0$, $H^1(G/H, M^H) = H^2(G/H, M^H) = 0$, and because $G/H$ is cyclic, this implies that $H^r(G/H, M^H) = 0$ for all $r$. Therefore $H^r(G, M) = 0$ for all $r > 0$. We next

show that $H^0(G,M)=0$. Let $x\in M^G$. Because $H^0(G/H,M^H)=0$, there exists a $y\in M^H$ such that $\mathcal{N}_{G/H}(y)=x$, and because $H^0(H,M)=0$, there exists a $y\in M^H$ such that $\mathcal{N}_{G/H}(y)=x$, and because $H^0(H,M)=0$, there exists a $z\in M$ such that $\mathcal{N}_H(z)=y$. Now

$$\mathcal{N}_G(z)=(\mathcal{N}_{G/H}\circ\mathcal{N}_H)(z)=x$$

Thus $H^r(G,M)=0$ for all $r\geq 0$. To proceed further, we use the exact sequence

$$0\longrightarrow M'\longrightarrow \mathbb{Z}[G]\otimes_{\mathbb{Z}} M\longrightarrow M\longrightarrow 0$$

Therefore $H^r(H,M)\simeq H^{r+1}(H,M')$ for all $r$ and $H$. In particular, $M'$ satisfies the hypothesis of the theorem, and so $H^r(G,M')=0$ for $r\geq 0$. In particular

$$H^0(G,M')=H^{-1}(G,M)=0$$

The argument, when repeated, gives that $H^{-2}(G,M)=0$, etc. This proves the theorem when $G$ is solvable. Now consider the case of an arbitrary finite group $G$. If $G$ and $M$ satisfy the hypothesis of the theorem, so also do $G_p$ and $M$, where $G_p$ is the Sylow $p$-subgroup of $G$. Therefore $H^r(G_p,M)=0$ for all $r$ and $p$, the $p$-primary component of $H^r(G,M)$ is zero for all $r$ and $p$. This implies that $H^r(G,M)=0$ for all $r$. □

**Theorem B.2 (Tate's theorem)**

Let $G$ be a finite group and let $C$ be a $G$-module. Suppose that for all subgroups $H$ of $G$

*(1).* $H^1(H,C)=0$

*(2).* $H^2(H,C)$ is a cyclic group of order $(H:1)$.

Then, for all $r$, there is an isomorphism

$$H_T^r(G,\mathbb{Z})\xrightarrow{\sim} H_T^{r+2}(G,C)$$

depending only on the choice of generator for $H^2(G,C)$.

*Proof.* Let $\gamma$ generates $H^2(G,C)$. Since $\mathrm{Cor}\circ\mathrm{Res}=(G:H)$, $\mathrm{Res}(\gamma)$ generates $H^2(G,C)$ for any subgroup $H$ of $G$. Let $\varphi$ be a cocycle representing $\gamma$. Define $C(\varphi)$ to be the direct sum of $C$ with the free abelian group having as basis symbols $x_\sigma$, one for each $\sigma\in G$, $\sigma\neq 1$, and extend the action of $G$ to an action on $C(\varphi)$ by setting

$$\sigma x_\tau=x_{\sigma\tau}-x_\sigma+\varphi(\sigma,\tau)$$

The symbol $x_1$ is to be interpreted as $\varphi(1,1)$. This does define an action of $G$ on $C(\varphi)$ because

$$\rho\sigma x_\tau=x_{\rho\sigma\tau}-x_{\rho\sigma}+\varphi(\rho\sigma,\tau)$$

whereas

$$\rho(\sigma x_\tau)=\rho(x_{\sigma\tau}-x_\sigma+\varphi(\sigma,\tau))=x_{\rho\sigma\tau}-x_\rho+\varphi(\rho,\sigma\tau)-(x_{\rho\sigma}-x_\rho+\varphi(\rho,\sigma))+\rho\varphi(\sigma,\tau)$$

These agree because $\varphi$ satisfies the cocycle condition

$$\rho\varphi(\sigma,\tau)+\varphi(\rho,\sigma\tau)=\varphi(\rho\sigma,\tau)+\varphi(\rho,\sigma)$$

Note that $\varphi$ is the coboundary of the 1-cochain $\sigma\mapsto x_\sigma$, and so $\gamma$ maps to zero in $H^2(G,C(\varphi))$. For this reason, $C(\varphi)$ is called the **splitting module** for $\gamma$. Now let $\alpha: C(\varphi)\to\mathbb{Z}[G]$ to be the additive map such that

$$\alpha(c)=0 \text{ for all } c\in C,\ \alpha(x_\sigma)=\sigma-1$$

Clearly

$$0 \longrightarrow C \longrightarrow C(\varphi) \xrightarrow{\alpha} I_G \longrightarrow 0$$

is an exact sequence of $G$-modules. Its cohomology sequence reads

$$0 \longrightarrow H^1(H, C(\varphi)) \longrightarrow H^1(H, I_G) \longrightarrow H^2(H, C) \longrightarrow H^2(H, C(\varphi)) \longrightarrow 0$$

The zeros at the ends us that $H^1(H, C) = H^2(H, I_G) = H^1(H, \mathbb{Z}) = 0$. The map $H^2(H, C) \to H^2(H, C(\varphi))$ is zero because $H^2(H, C)$ is generated by $\mathrm{Res}(\gamma)$ in $H^2(G, C(\varphi))$, which is zero. It remains to show that $H^1(H, I_G) \simeq H^2(H, C)$, which is clear since $\#H^1(H, I_G) = \#H^0(H, \mathbb{Z}) = \#H^2(H, C) = (H : 1)$ and the map $H^1(H, I_G) \to H^2(H, C)$ is surjective. Hence $H^r(G, C(\varphi)) = 0$ by theorem **??**, and we obtain an exact sequence

$$0 \longrightarrow C \longrightarrow C(\varphi) \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0$$

with the property that $H^r(G, C(\varphi)) = H^r(G, \mathbb{Z}[G])$ for all $r$. Therefore, the double boundary map is an isomorphism

$$H^r(G, \mathbb{Z}) \xrightarrow{\sim} H^{r+2}(G, C)$$

□

## B.5 The Cohomology of Profinite groups

Let $G$ be a **profinite** group. This means that $G$ is a compact topological group for which the open normal subgroups form a fundamental system of neighborhoods of 1.

**Definition B.5 (Discrete $G$-module)**

A $G$-module for which the map

$$G \times M \to M$$

is continuous when $M$ is endowed with the discrete topology, i.e., the topology in which every subject is open, are called a **discrete** $G$-module. Equivalent conditions:

- $M = \bigcup M^H$, where $H$ runs through the open subgroups of $G$.
- The stabilizer in $G$ of any element of $M$ is open.

In future, all cohomology groups will be defined using continuous cochains.

**Proposition B.15**

The maps $\mathrm{Inf} : H^r(G/H, M^H) \to H^r(G, M)$ realize $H^r(G, M)$ as the direct limit of the groups $H^r(G/H, M^H)$ as $H$ runs through the open normal subgroups $H$ of $G$:

$$\varinjlim H^r(G/H, M^H) = H^r(G, M)$$

**Corollary B.5**

For every profinite group $G$ and discrete $G$-module $M$, $H^r(G, M)$ is a torsion group for all $r > 0$.

**Proposition B.16**

Let $G$ be a profinite group, and $M = \varinjlim M_i$, where $M_i \subseteq M$, then $H^r(G, M) = \varinjlim H^r(G, M_i)$.

# C Algebraic approach to Local Class Field Theory

## C.1 The Cohomology of Unramified Extensions

**Proposition C.1**

Let $L/K$ be a finite unramified extension with Galois group $G$, and let $U_L$ be the group of units in $L$. Then

$$H_T^r(G, U_L) = 0 \text{ for all } r$$

*Proof.* Notice that since $L/K$ is unramified, we have that

$$\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(\kappa(L)/\kappa(L))$$

is cyclic, and there exists some $\pi \in K$ such that $L^\times = U_L \cdot \pi^{\mathbb{Z}} \simeq U_L \times \mathbb{Z}$ which is also a decomposition of $G$-modules. Therefore $H^r(G, U_L) \simeq H^r(G, L^\times)$. Since $H^1(G, L^\times) = 0$ by Hilbert's theorem 90 **??**, this shows that $H^1(G, U_L) = 0$. It remains to show that $H^0(G, U_L) = 0$, which is accomplished by the next proposition. □

**Proposition C.2**

Let $L/K$ be a finite unramified extension. Then the norm map $\mathcal{N}_{L/K} : U_L \to U_K$ is surjective.

We first need some lemmas.

**Lemma C.1**

For all $r$, $H^r(G, \kappa(L)^\times) = 0$. In particular, $\kappa(L)^\times \to \kappa(K)^\times$ is surjective.

*Proof.* Since $\kappa(L)^\times$ is finite, $h(\kappa(L)^\times) = 1$, and the conclusion is clear since $H^1(G, \kappa(L)^\times) = 0$. □

*Proof of proposition* **??**. There are commutative diagrams

$$\begin{array}{ccc} U_L & \longrightarrow & \kappa(L)^\times \\ \downarrow{\scriptstyle \mathcal{N}} & & \downarrow{\scriptstyle \mathcal{N}} \\ U_K & \longrightarrow & \kappa(K)^\times \end{array} \qquad \begin{array}{ccc} U_L^{(m)} & \longrightarrow & \kappa(L) \\ \downarrow{\scriptstyle \mathcal{N}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ U_K^{(m)} & \longrightarrow & \kappa(K) \end{array}$$

Consider $u \in U_K$. Because the norm map $\kappa(L)^\times \to \kappa(K)^\times$ is surjective, there exists a $v_0 \in U_L$ such that $\mathcal{N}(v_0)$ and $u$ have the same image in $\kappa(K)^\times$. Similarly, we may find $v_m \in U_L^{(m)}$ such that $u/\mathcal{N}(v_0 v_1 \cdots v_m) \in U_K^{(m+1)}$, and hence

$$u = \mathcal{N}(v_0 v_1 \cdots)$$

□

Now we denote $H^2(\mathrm{Gal}(L/K), L^\times)$ by $H^2(L/K)$, the following composition of maps

$$\mathrm{inv}_{L/K} : \quad H^2(L/K) \xrightarrow{\sim} \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{f \mapsto f(\sigma)} \mathbb{Q}/\mathbb{Z}$$

is called the **invariant map**

$$\mathrm{inv}_{L/K} : H^2(L/K) \to \mathbb{Q}/\mathbb{Z}$$

**Theorem C.1**

There exists a unique isomorphism

$$\mathrm{inv}_K : H^2(K^{\mathrm{un}}/K) \to \mathbb{Q}/\mathbb{Z}$$

with the property that, for every $L \subseteq K^{\mathrm{un}}$ of degree $n$ over $K$, $\mathrm{inv}_K$ induces the isomorphism

$$\mathrm{inv}_{L/K} : H^2(L/K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

Here $e$ is the ramification index for $L/K$ and $f$ is the residue class degree. The first square is obtained from the commutative square

$$\begin{array}{ccc} K^{\mathrm{un}\,\times} & \xrightarrow{v_K} & \mathbb{Z} \\ \downarrow & & \downarrow e \\ L^{\mathrm{un}\,\times} & \xrightarrow{v_L} & \mathbb{Z} \end{array}$$

This is an immediate consequence of the above discussion.

**Proposition C.3**

Let $L$ be a finite extension of $K$ of degree $n$, and let $K^{\mathrm{un}}$ and $L^{\mathrm{un}}$ be the largest unramified extensions of $K$ and $L$. Then the following diagram commutes:

$$\begin{array}{ccc} H^2(K^{\mathrm{un}}/K) & \xrightarrow{\mathrm{Res}} & H^2(L^{\mathrm{un}}/L) \\ \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_L} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array}$$

*Proof.* Let $\Gamma_K = \mathrm{Gal}(K^{\mathrm{un}}/K)$ and $\Gamma_L = \mathrm{Gal}(L^{\mathrm{un}}/L)$, and consider the diagram

$$\begin{array}{ccccccc} H^2(K^{\mathrm{un}}/K) & \xrightarrow{\sim} & H^2(\Gamma_K, \mathbb{Z}) & \xrightarrow{\sim} & H^1(\Gamma_K, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{g \mapsto g(\sigma_K)} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle e\,\mathrm{Res}} & & \downarrow{\scriptstyle e\,\mathrm{Res}} & & \downarrow{\scriptstyle ef} \\ H^2(K^{\mathrm{un}}/K) & \xrightarrow{v_L} & H^2(\Gamma_L, \mathbb{Z}) & \xrightarrow{\sim} & H^1(\Gamma_K, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{g \mapsto g(\sigma_L)} & \mathbb{Q}/\mathbb{Z} \end{array}$$

Here $e$ is the ramification index for $L/K$ and $f$ is the residue class degree. The first square is obtained from the commutative square

$$\begin{array}{ccc} K^{\mathrm{un}\,\times} & \xrightarrow{v_K} & \mathbb{Z} \\ \downarrow & & \downarrow e \\ L^{\mathrm{un}\,\times} & \xrightarrow{v_L} & \mathbb{Z} \end{array}$$

The third square is

$$\begin{array}{ccc} \mathrm{Hom}(\Gamma_K, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{g \mapsto g(\sigma_K)} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle g \mapsto g|_{\Gamma_L}} & & \downarrow{\scriptstyle f} \\ \mathrm{Hom}(\Gamma_L, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{g \mapsto g(\sigma_L)} & \mathbb{Q}/\mathbb{Z} \end{array}$$

The Frobenius element $\sigma_K$ and $\sigma_L$ are determined by the fact that they induce $x \mapsto x^q$ and $x \mapsto x^{q^f}$ respectively on the residue fields, where $q = |\kappa(K)|$ and $q^f = |\kappa(L)|$. It is now clear that the square commutes, and since $n = ef$, this proves the proposition. □

Let $L$ be a finite unramified extension of $K$ with Galois group $G$, and let $n = [L : K]$. The **local fundamental class** $u_{L/K}$ is the element of $H^2(L/K)$ mapped to the generator $\frac{1}{n}$ of $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ by the invariant map $\mathrm{inv}_{L/K} : H^2(L/K) \xrightarrow{\sim} \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. The pair $(G, L^\times)$ satisfies the hypothesis of Tate's theorem **??**, and so cup-product with the fundamental class $u_{L/K}$ defines an isomorphism

$$H^r(G, \mathbb{Z}) \to H^{r+2}(G, L^\times)$$

for all $r \in \mathbb{Z}$. For $r = -2$, this becomes

$$\begin{array}{ccc} H^{-2}(G, \mathbb{Z}) & \xrightarrow{\sim} & H^0(G, L^\times) \\ \| & & \| \\ G & & K^\times / \mathcal{N}(L^\times) \end{array}$$

We now compute this map explicitly. A prime element $\pi \in K$ is also a prime element of $L$, and defines a decomposition

$$L^\times = U_L \cdot \pi^{\mathbb{Z}} \simeq U_L \times \mathbb{Z}$$

of $G$-modules. Thus

$$H^r(G, L^\times) \simeq H^r(G, U_L) \oplus H^r(G, \pi^{\mathbb{Z}})$$

Choose a generator $\sigma$ of $G$, and let

$$f \in H^1(G, \mathbb{Q}/\mathbb{Z}) \simeq \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$$

**Proposition C.4**

Under the composite

$$\begin{array}{ccc} H^{-2}(G, \mathbb{Z}) & \xrightarrow{\sim} & H^0(G, L^\times) \\ \| & & \| \\ G & & K^\times / \mathcal{N}(L^\times) \end{array}$$

of the above maps, the Frobenius element $\sigma \in G$ maps to the class of $\pi$ in $K^\times / \mathcal{N}(L^\times)$.

## C.2 The Cohomology of Ramified extensions

Because of Hilbert's Theorem 90 **??**, there exists an exact sequence

$$0 \longrightarrow H^2(L/K) \xrightarrow{\mathrm{Inf}} H^2(E/K) \xrightarrow{\mathrm{Res}} H^2(E/L)$$

for any tower of Galois extensions $E \supseteq L \supseteq K$. The next theorem extends theorem **??** to ramified extensions.

**Theorem C.2**

For every local field $K$, there is a canonical isomorphism

$$\mathrm{inv}_K : H^2(K^{\mathrm{al}}/K) \to \mathbb{Q}/\mathbb{Z}$$

Let $L$ be a Galois extension of $K$ of degree $n < \infty$, then the diagram

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

commutes, and therefore defines an isomorphism

$$\mathrm{inv}_{L/K} : H^2(L/K) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

**Lemma C.2**

If $L/K$ is Galois of finite degree $n$, then $H^2(L/K)$ contains a subgroup canonically isomorphic to $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$.

*Proof.* Consider the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \ker(\mathrm{Res}) & \longrightarrow & H^2(K^{\mathrm{un}}/K) & \xrightarrow{\mathrm{Res}} & H^2(L^{\mathrm{un}}/L) \\ & & \downarrow & & \downarrow{\scriptstyle \mathrm{Inf}} & & \downarrow{\scriptstyle \mathrm{Inf}} \\ 0 & \longrightarrow & H^2(L/K) & \longrightarrow & H^2(K^{\mathrm{al}}/K) & \xrightarrow{\mathrm{Res}} & H^2(K^{\mathrm{al}}/L) \end{array}$$

Since the two inflation maps are injective, so also is the first vertical map, but **??** shows that the kernel of the map on the top row is canonically isomorphic to $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$. □

**Lemma C.3**

Let $L$ be a finite Galois extension of $K$ with Galois group $G$. Then there exists an open subgroup $V$ of $\mathcal{O}_L$, stable under $G$, such that $H^r(G, V) = 0$ for all $r > 0$.

*Proof.* Let $\{x_\tau \mid \tau \in G\} \subseteq \mathcal{O}_L$ be a normal basis of $L$ over $K$, then $V = \sum \mathcal{O}_K x_\tau$ is stable under $G$ with finite index with respect to $\mathcal{O}_L$. Finally

$$V \simeq \mathcal{O}_K[G] \simeq \mathrm{Ind}^G \mathcal{O}_K$$

as $G$-modules, and so $H^r(G, V) = 0$ for all $r > 0$. □

**Lemma C.4**

Let $L$ be a finite Galois extension of $K$ with Galois group $G$. Then there exists an open subgroup $V$ of $U_L$, stable under $G$, such that $H^r(G, V) = 0$ for all $r > 0$.

**Corollary C.1**

Let $L/K$ be cyclic, then $h(U_L) = 1$ and $h(L^\times) = n$.

**Lemma C.5**

Let $L$ be a finite Galois extension of order $n$, then $H^2(L/K)$ has order $n$.

*Proof.* We know that the order of $H^2(L/K)$ is divisible by $n$, and that it equals $n$ when $L/K$ is cyclic. We prove the lemma by induction on $[L:K]$. Because the group $\mathrm{Gal}(L/K)$ is solvable, there exists a Galois extension $K'/K$ with $L \supsetneq K' \supsetneq K$. From the exact sequence

$$0 \longrightarrow H^2(K'/K) \longrightarrow H^2(L/K) \longrightarrow H^2(L/K')$$

we see that

$$|H^2(L/K)| \leq |H^2(K'/K)| \cdot |H^2(L/K)| = n$$

□

*Proof (of 3.2).* We've seen that for every finite Galois extension $L$ of $K$, the subgroup $H^2(L/K)$ of $H^2(K^{\mathrm{al}}/K)$ is contained in $H^2(K^{\mathrm{un}}/K)$, this proves that the inflation map $H^2(K^{\mathrm{un}}/K) \to H^2(K^{\mathrm{al}}/K)$ is an isomorphism. Compose the inverse of this with the invariant map $\mathrm{inv}_K : H^2(K^{\mathrm{un}}/K) \to \mathbb{Q}/\mathbb{Z}$ of Theorem 3.2. □

Let $L$ be a finite Galois extension of $K$ with Galois group $G$. As in the unramified case, we define the **fundamental class** $u_{L/K}$ of $L/K$ to be the element $u_{L/K}$ of $H^2(L/K)$ such that

$$\mathrm{inv}_{L/K}(u_{L/K}) = \frac{1}{[L:K]} \pmod{\mathbb{Z}}$$

or, equivalently, such that

$$\mathrm{inv}_K(u_{L/K}) = \frac{1}{[L:K]} \pmod{\mathbb{Z}}$$

**Lemma C.6**

Let $L \supseteq E \supseteq K$ with $L/K$ finite and Galois. Then

$$\mathrm{Res}(u_{L/K}) = u_{L/E}$$
$$\mathrm{Cor}(u_{L/E}) = [E:K]u_{L/K}$$

Moreover, if $E/K$ is also Galois, then

$$\inf(u_{E/K}) = [L:E]u_{L/K}$$

## C.3 The Local Artin Map

The pair $(G, \mathrm{L}^\times)$ satisfies the hypothesis of Tate's theorem **??**, and so we have proved the following result

**Theorem C.3**

For every finite Galois extension of local fields $L/K$ and $r \in \mathbb{Z}$, the homomorphism

$$H^r(\mathrm{Gal}(L/K), \mathbb{Z}) \to H^{r+2}(\mathrm{Gal}(L/K), L^\times)$$

defined by $x \mapsto x \cup u_{L/K}$ is an isomorphism. When $r = -2$, this becomes an isomorphism

$$G^{\mathrm{ab}} \simeq K^\times / \mathcal{N}_{L/K}(L^\times)$$

For $r = -2$, the map in the theorem becomes

$$\mathrm{Gal}(L/K)^{\mathrm{ab}} \xrightarrow{\sim} K^\times / \mathcal{N}_{L/K}(L^\times)$$

We denote the inverse map by

$$\phi_{L/K} : K^\times / \mathcal{N}_{L/K}\, L^\times \to \mathrm{Gal}(L/K)^{\mathrm{ab}}$$

and call it the **local Artin map**.

**Lemma C.7**

Let $L \supseteq E \supseteq K$ be local fields with $L/K$ Galois. Then the following diagrams commute:

$$\begin{array}{ccc} E^\times & \xrightarrow{\phi_{L/E}} & \mathrm{Gal}(L/E)^{\mathrm{ab}} \\ \downarrow{\scriptstyle \mathcal{N}_{E/K}} & & \downarrow \\ K^\times & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \end{array} \qquad \begin{array}{ccc} E^\times & \xrightarrow{\phi_{L/E}} & \mathrm{Gal}(L/E)^{\mathrm{ab}} \\ \uparrow & & \uparrow \\ K^\times & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \end{array}$$

Let $L \supseteq E \supseteq K$ be local fields with both $L$ and $E$ Galois over $K$. Then the following diagram commutes

$$\begin{array}{ccc} K^\times & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \\ & {\scriptstyle \phi_{E/K}} \searrow & \downarrow \\ & & \mathrm{Gal}(E/K)^{\mathrm{ab}} \end{array}$$

**Theorem C.4**

For every local field $K$, there exists a homomorphism (the so-called local Artin map)

$$\phi_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

with the following properties:

*(1).* For every prime element $\pi$ of $K$, $\phi_K(\pi)|_{K^{\mathrm{un}}} = \mathrm{Frob}_K$.

*(2).* For every finite extension $L$ of $K$, $\mathcal{N}_{L/K}(L^\times)$ is contained in the kernel of $a \mapsto \phi_K(a)|_L$, and $\phi_K$ induces an isomorphism

$$\phi_{L/K} : K^\times / \mathcal{N}_{L/K}(L^\times) \xrightarrow{\sim} \mathrm{Gal}(L/K)$$

# References


[1] A.M. Legendre, *Recherches d'analyse indéterminée*, Historie de l'Academie Royale des Sciences de Paris (1785), 465-559, Paris 1788; cf. p. 6, 7.

[2] A.M. Legendre, *Essai sur la théorie des nombres*, 1st ed. Paris 1798, 2nd ed. Paris 1808, 3rd ed. Paris 1830; German transl. (Zahlentheorie) of the 3rd. ed., Leipzig 1886; Quatrieme edition conforme ala troisieme, nouveau tirage corrige, Paris 1955; cf. p. 6, 18.

[3] A. Weil, *Une lettre et un extrait de lettre à Simone Weil*, Œurve I (1926-1951), 244-255; cf. p. xi. 22.

[4] C. Borchardt, *Letter to R. Lipschitz*, Dec. 21, 1875; in: Dokumente zur Geschichte der Mathematik, Bd. 2. DMV Vieweg & Sohn, 1986.

[5] C.F. Gauss, *Fragmente zur Theorie der aus einer Cubikwurzel zu bildenden ganzen algebraischen Zahlen*, Werke X, 1, 53 - 55, cf. p. 199, 204.

[6] C.F. Gauss, *Hauptmomente des Beweises für die biquadratischen Reste*, Werke X, 1, 56-57; cf. p. 201.

[7] C.F. Gauss, *Disquisitionum circa aequationes puras*, Nachlaß, Werke II.

[8] C.F. Gauss, *Beweis des Reziprozitätssatzes für die biquadratischen Reste, der auf die Kreisteilung gegründet ist*, Werke X, 1, 65 - 69; cf. p. 200.

[9] C.F. Gauss, *Letter to W. Olbers, Sept. 3, 1805.*

[10] C.F. Gauss, *Disquisitiones Arithmeticae*, Werke I; French transl. 1807; Paris 1910, FdM 42 (1911), 236; 1953, Zbl 51.03003; German transl. Springer 1889, reprint Chelsea 1965, MR 32 #5488; Russian transl. Moscow 1959, MR 23 #A2352; English transl. New Haven, London 1966, Zbl 136.32301; reprint Springer Verlag 1986, Zbl 585.10001; Spanish transl. Bogota 1995, Zbl 899.01034; cf. p. 6, 12, 14, 22, 100, 101, 137, 223, 227, 268, 342.

[11] C.F. Gauss, *(4th Proof) Summatio serierum quarundam singularium*, Comment. Soc. regiae sci. Göttingen 1811; Werke II, p. 9-45; cf. p. 21, 137, 413.

[12] C.F. Gauss, *(5th Proof) Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et amplicationes novae*, 1818; Werke II, 47-64, in particular p. 51; cf. p. 21, 200, 413.

[13] C.F. Gauss, *Theoria residuorum biquadraticorum, Commentatio prima*, Comment. Soc. regiae sci. Göttingen 6 (1828), 27 ff; Werke II, 65-92; cf. p. 15, 101, 154, 170, 174,202,200.

[14] C.F. Gauss, *Theoria residuorum biquadraticorum, Commentatio secunda*, Comment. Soc. regiae sci. Gottingen 7 (1832), 93-148; Werke II, 93-148; cf. p. 15, 203, 200.

[15] C.G.J. Jacobi, *Lecture Notes*, Königsberg 1837 (H.Pieper, ed.), in preparation; cf. p. vii, xv, 12, 24, 170, 200, 227, 270.

[16] C.G.J. Jacobi, *Letter to Gauss*, Gesammelte Werke VII, 393-400; cf. p. 138, 144, 313.

[17] C.G.J. Jacobi, *Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie*, Berliner Akad. Ber. 1837, 127-136; Werke VI, 245-274; cf. p. 10, 138, 138, 224, 225, 270, 313, 413.

[18] C.G.J. Jacobi, *Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie*, J. Reine Angew. Math. 30 (1846), 166-182; cf. p. 270.

[19] D. Hilbert, *Die Theorie der algebraischen Zahlen* (Zahlbericht), Jahresber. DMV 4 (1897), 175-546; FdM 28 (1897), 157-162; French transl.: Toulouse Ann. (3) 1 (1905), 257-328; FdM 41 (1911), 244; English transl.: Springer Verlag 1998; Roumanian trans!: Bukarest 1998; cf. p. 86, 101, 103, 358.

[20] D. Hilbert, *Über die Theorie der relativ-quadratischen Zahlkörper*, Jber. DMV 6 (1899), 88-94; cf. p. 70.

[21] E.E. Kummer, *Über die allgemeinen Reziprozitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist*, Berliner Akad. Abh. (1859), 19-159; Coli. Papers I, 699-839; cf. p. 19, 22, 235, 273

[22] E. Grosswald, *Representations of integers as sums of squares*, SpringerVerlag 1985.

[23] F. Lemmermeyer (2000) *Reciprocity Laws*, Addison-Wesley Professional.

[24] G. Eisenstein, *Lois de réciprocité*, J. Reine Angew. Math. 28 (1844), 53-67; Math. Werke I, 126-140; cf. p. 201.

[25] G. Eisenstein, *Application de l'algèbre à l'arithmétique transcendante*, J. Reine Angew. Math. 29 (1845), 177-184; Math. Werke I, 291-298; cf. p. 201, 275, 413.

[26] G. Eisenstein, *Zur Theorie der quadratischen Zerfällung der Primzahlen* $8n+3$, $7n+2$ *und* $7n+4$, J. Reine Angew. Math. 37 (1848), 97-126; Werke II, 506-535.

[27] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Jahresber. DMV, Ergänzungsband Würzburg 1965; Zbl 138.03202; MR 33 #4045a, #4045b; MR 42 #1795; cf. p. 395.

[28] H. Weyl, *David Hilbert and His Mathematical Work*, Bull. Amer. Math. Soc. 50 (1944), 612-654.

[29] J. Hoffman (1960) *Über die zahlentheoretischen Methoden Fermats and Eulers, ihre Zusammenhänge und ihre Bedeutung*, Archive for History of Exact Sciences 1 (1960/62), 122-159.

[30] J. Liouville, *Sur la loi de réciprocité dans la théorie des résidus quadratiques*, C. R. Acad. Sci. Paris 24 (1847), 577-578; cf. p. 275.

[31] J.S. Milne (2020) *Class Field Theory*, Available at www.jmilne.org/math/.

[32] J.W.S. Cassels, A. Fröhlich, *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*. Thompson, Washington, D.C.

[33] K. Conrad, *History of Class Field Theory*

[34] K. Iwasawa, *On papers of Takagi in Number Theory*, in Teiji Takagi Collected Papers, 2nd ed., Springer-Verlag, Tokyo, 1990, 342-351.

[35] K.-R. Biermann, *Johann Peter Gustav Lejeune Dirichlet- Dokumente für sein Leben und Wirken*, Aka.demie-Verlag Berlin, 1959

[36] L. Euler, *Leonhard Euler und Christian Goldbach: Briefwechsel 1729 - 1764*, Abh. Deutsche Akad. Wiss. Berlin, Akademie-Verlag 1965.

[37] L. Euler, *Theorematum quorundam ad numeros primos spectantium demonstratio*, Novi Comm. Acad. Sci. Petropol. 8 (1736), 1741, 141-146 Opera Omnia I-2, p. 33-37.

[38] M. Cauchy, *Sur la théorie des nombres*, Bull. de Férussac 12 (1829), 205-221 Œurves S. 2, II, 88-107; cf. p. 138, 270, 413.

[39] M. Cauchy, *Mémorie sur la theorie des nombres*, Œurves de Cauchy, Sér. I, III, 5-??; cf. 202, 270, 313, 291.

[40] N.H. Abel, *Œuvres complètes de Niels Henrik Abel*, Johnson Reprint Corporation, 1965.

[41] N. Schappacher, *On the History of Hilbert's 12th Problem: A Comedy Errors, in "Matériaux pour l'historie des mathématiques au vingtième siècle"*, Soc. Math. France, Paris, 1998, 243-273.

[42] P. de Fermat *Œurve*.

[43] P. Kaplan, *Une démonstration géométrique de la loi de réciprocité quadratique*, Proc. Japan Acad. 45 (1969), 779-780; Zbl 216.03703; MR 42 # 4474; cf. p. 416.