HISTORY OF CLASS FIELD THEORY

KEITH CONRAD

1. Introduction

Class field theory is the description of abelian extensions of global fields and local fields. The label "class field" refers to a field extension satisfying a technical property that is historically related to ideal class groups, and one of the main theorems is that class fields are the same as abelian extensions.

Three themes in number theory at the end of the 19th century led to class field theory: relations between abelian extensions and ideal class groups, density theorems for primes (and L-functions), and reciprocity laws. We will outline how class field theory developed from these initial ideas through the work of Kronecker, Weber, Hilbert, Takagi, Artin, Hasse, and Chevalley. One point concerning chronology: while we usually attribute results to mathematicians in years according to the appearance of the published papers, the actual work was often done earlier (*e.g.*, Takagi's fundamental paper in 1920 was based on work he had carried out several years earlier, with its publishing outside of Japan being delayed by World War I).

Some general surveys on the development of class field theory are [3], [4] (a more detailed version of [3], but not as accessible), [6], [8], [9], and the beginning of Part 2 of [10]. At the start of each section, particular references for that material are indicated. References to original papers are not given here, but can be found by consulting the cited sources.

Concerning notation, generally L/K will be an extension of number fields, with rings of integers $\mathcal{O}_L$ and $\mathcal{O}_K$, and E/F will be an extension of local fields. The set of primes in K which split completely in L is $\mathrm{Spl}(L/K)$. Given a place v on K and a place w lying over it in L, $D(w|v)$ and $I(w|v)$ are the associated decomposition and inertia groups.[1]

I thank Peter Roquette, Jean-Pierre Serre, and counselors at the PROMYS program (particularly Dustin Clausen) for their comments.

2. Beginnings (Kronecker)

References: [12], [13], [19].

In 1853, Kronecker announced what is now called the Kronecker–Weber theorem.

Theorem 2.1 (Kronecker–Weber)**.** *Every finite abelian extension of* $\mathbf{Q}$ *lies in a cyclotomic field* $\mathbf{Q}(\zeta_m)$ *for some* m.

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 which went unnoticed for about 90 years. The first correct proof was Hilbert's in 1896. It's worth saying something about the strategy of the proof because of its relation to Hilbert's

---

[1]In the literature these are also denoted $Z(w|v)$ and $T(w|v)$ from the German: Zerlegungsgruppe and Trägheitsgruppe.

later ideas on class field theory. Hilbert starts with an abelian extension $L/\mathbf{Q}$ and uses his recently developed theory of higher ramification groups to show L lies in a succession of fields of the form $F_n(\zeta_n)$ where F_n is a subfield of L (so F_n is necessarily abelian over $\mathbf{Q}$) such that the ramification in $F_n/\mathbf{Q}$ can be made smaller in exchange for adjoining appropriate roots of unity. Eventually F_n is an abelian unramified extension of $\mathbf{Q}$, so $F_n = \mathbf{Q}$ since $\mathbf{Q}$ has no proper unramified extensions (abelian or not). At this point we have $L \subset \mathbf{Q}(\zeta_n)$ and the proof is complete. If $\mathbf{Q}$ had a proper abelian unramified extension, Hilbert's proof would not have worked.

Abelian extensions of $\mathbf{Q}(i)$ were constructed by Abel (1829), using special values of the lemniscatic elliptic function $\mathrm{sl}(z)$, whose period lattice is essentially $\mathbf{Z}[i]$. (Abel was following up on suggestions of Gauss in the *Disquisitones Arithmeticae* that there is a theory of arc division on the lemniscate which 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 any imaginary quadratic field using special values of elliptic and modular functions. In a letter to Dedekind in 1880, Kronecker's described his "Jugendtraum" (dream of youth)[2] as the hope that every finite abelian extension of an imaginary quadratic field lies in one of the extensions he had found. As a particular example, he expected that every finite abelian extension of $\mathbf{Q}(i)$ lies in a field $\mathbf{Q}(i, \mathrm{sl}(\omega/m))$, where $\omega \approx 2.622$ is the lemniscatic analogue of π. This is similar to the Kronecker-Weber theorem, with $\mathrm{sl}(\omega/m)$ analogous to $\zeta_m = e^{2\pi i/m}$.

An important case of Kronecker's work uses the j-function: if K is imaginary quadratic and we write $\mathcal{O}_K = \mathbf{Z} + \mathbf{Z}\tau_1$, where τ_1 is in the upper half-plane, Kronecker showed the number $j(\tau_1)$ is algebraic over K and its K-conjugates are of the form $j(\tau_1), \ldots, j(\tau_h)$ where the lattices $\mathbf{Z} + \mathbf{Z}\tau_i$ 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 ideal $\mathfrak{b}$ act on $j(\tau_i)$ using multiplication in the class group: if $\mathfrak{b}(\mathbf{Z} + \mathbf{Z}\tau_i) = \mathbf{Z} + \mathbf{Z}\tau_{i'}$ in $\mathrm{Cl}(K)$ then set $\sigma_{\mathfrak{b}}(j(\tau_i)) = j(\tau_{i'})$. This action of fractional ideals on the j-values descends to an action of the ideal class group on the j-values.

Example 2.2. Let $K = \mathbf{Q}(\sqrt{-31})$. The class number is 3 and ideals representing the different ideal classes are (1), $\mathfrak{p}_2$, $\bar{\mathfrak{p}}_2$, where $\mathfrak{p}_2 = 2\mathbf{Z} + (\frac{1+\sqrt{-31}}{2})\mathbf{Z}$ and $\bar{\mathfrak{p}}_2$ is the conjugate ideal of $\mathfrak{p}_2$. Scaling each ideal to be a lattice of the form $\mathbf{Z} + \mathbf{Z}\tau$ for τ in the upper half-plane, three values of τ are $\frac{1+\sqrt{-31}}{2}, \frac{1+\sqrt{-31}}{4}$, and $\frac{-1+\sqrt{-31}}{4}$. The values of the j-function at these three numbers are the roots of the cubic polynomial

$$X^3 + 39491307X^2 - 58682638134X + 1566028350940383.$$

Its discriminant is $-31 \cdot (3^{19} \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 23 \cdot 29)^2$, so its splitting field over $\mathbf{Q}$ is $\mathbf{Q}(\gamma, \sqrt{-31})$, where $\gamma = j(\frac{1+\sqrt{-31}}{2}) \approx -39492793.9115$. The extension $K(\gamma)/K$ is a cubic Galois extension generated by a special value of the j-function.

Kronecker called $K(j(\tau))$, where $\mathcal{O}_K = \mathbf{Z} + \mathbf{Z}\tau$, 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:

---

[2]Kronecker was 56 at the time, and was in his 30s when he worked on the Kronecker–Weber theorem and relations between modular functions and imaginary quadratic fields.

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.

In addition to the construction of abelian extensions, Kronecker set off another path to class field theory in an 1880 paper on densities of primes and factorization of polynomials. For a polynomial $f(X) \in \mathbf{Z}[X]$, Kronecker considered the number n_p of roots of $f(X) \bmod p$ in $\mathbf{F}_p$ as p varies. For example, if $f(X) = X^2 + 1$ then $n_2 = 1$ and $n_p = 0$ or 2 for odd p, depending on p modulo 4. So on average, n_p is 1.

Theorem 2.3 (Kronecker, 1880). *If $f(X)$ has r irreducible factors in $\mathbf{Z}[X]$ then the average value of n_p is r:*

$$\lim_{s \to 1^+} \frac{\sum_p n_p/p^s}{\sum_p 1/p^s} = r.$$

The use of a density with Dirichlet series rather than as $\lim_{x \to \infty}(\sum_{p \le x} n_p)/\#\{p \le x\}$ is no surprise: the Prime Number theorem was still 16 years in the future, so a rigorous notion of density at the time could not use denominator $\#\{p \le x\}$.

Corollary 2.4. *Let $K/\mathbf{Q}$ be a Galois extension. The set of primes which split completely in K has density $1/[K : \mathbf{Q}]$.*

Proof. Write $K = \mathbf{Q}(\alpha)$ for an algebraic integer α. Let $f(X) \in \mathbf{Z}[X]$ be the minimal polynomial of α over $\mathbf{Q}$. Because the roots of $f(X)$ are polynomials in α with rational coefficients, if $f(X) \bmod p$ has a root then it splits completely (for all but finitely many p), which means $n_p = \deg f = [K : \mathbf{Q}]$ if $n_p \ne 0$. Letting A be the set of primes p such $n_p = [K : \mathbf{Q}]$, Kronecker's theorem says in this case

$$\lim_{s \to 1^+} \frac{\sum_{p \in A} 1/p^s}{\sum_p 1/p^s} = \frac{1}{[K : \mathbf{Q}]},$$

so the (Dirichlet) density of the p where $f(X) \bmod p$ splits completely is $1/[K : \mathbf{Q}]$. Since $f(X) \bmod p$ splits completely if and only if p splits completely in K (with finitely many exceptions), the primes which split completely in K have density $1/[K : \mathbf{Q}]$. $\qquad\square$

Example 2.5. Kronecker used Corollary 2.4 to prove irreducibility of the nth cyclotomic polynomial by the following analytic method. Let $K = \mathbf{Q}(\zeta_n)$, which is Galois over $\mathbf{Q}$ since all nth roots of unity are powers of ζ_n. Let $f(X)$ be the minimal polynomial of ζ_n in $\mathbf{Z}[X]$. For all but finitely many p, p splits completely in K if and only if $f(X)$ splits completely in $\mathbf{F}_p[X]$, which is equivalent to there being a primitive nth root of unity in $\mathbf{F}_p$. That means $n|(p-1)$, or $p \equiv 1 \bmod n$. By Dirichlet's theorem, this set of primes has density $1/\varphi(n)$. So Corollary 2.4 tells us $[K : \mathbf{Q}] = \varphi(n)$. Since ζ_n is a root of the nth cyclotomic polynomial $\Phi_n(X)$, which has degree $\varphi(n)$, this proves $f(X) = \Phi_n(X)$, so $\Phi_n(X)$ is irreducible in $\mathbf{Q}[X]$.

Kronecker's paper included two influential conjectures on sets of primes. The first one asked for the density of the set of primes p such that $f(X) \bmod p$ has a fixed number of roots in $\mathbf{F}_p$, where $f(X) \in \mathbf{Z}[X]$. When the number of roots is $\deg f$ then $f(X) \bmod p$ splits completely and Kronecker found that density. He was unable to prove the existence of these densities in general, but he conjectured they exist and described some properties the densities should have. The existence of these densities was first established by Frobenius, and in his work on this problem Frobenius introduced (1896) the Frobenius element of a

prime ideal[3] and conjectured what later became the Chebotarev density theorem. We will see the importance of this result when we discuss Artin's work on class field theory.

Kronecker's second conjecture was that a Galois extension of $\mathbf{Q}$ is characterized by the set of primes in $\mathbf{Q}$ which split completely in the extension (*e.g.*, $\mathbf{Q}(i)$ is the only Galois extension of $\mathbf{Q}$ in which the split primes are $p \equiv 1 \bmod 4$). He considered this idea as an arithmetic "boundary value theorem," just as Cauchy's integral formula determines a complex analytic function inside a disc from its values on the boundary. For a finite extension L/K, denote the set of primes in K that split in L as $\mathrm{Spl}(L/K)$, so Kronecker had proved $\mathrm{Spl}(L/K)$ has Dirichlet density $1/[L:K]$ when L/K is Galois. (Strictly, he proved this only for $K = \mathbf{Q}$, but the argument is similar for any number field, replacing a sum over prime numbers in the density with a sum over prime ideals of K.) Kronecker's conjecture was proved by M. Bauer in 1903 for Galois extensions of any number field, not just $\mathbf{Q}$.

Theorem 2.6 (Bauer)**.** *Let L_1 and L_2 be finite Galois extensions of a number field K. Then $L_1 \subset L_2$ if and only if $\mathrm{Spl}(L_2/K) \subset \mathrm{Spl}(L_1/K)$. In particular, $L_1 = L_2$ if and only if $\mathrm{Spl}(L_1/K) = \mathrm{Spl}(L_2/K)$.*

Proof. If $L_1 \subset L_2$ then easily $\mathrm{Spl}(L_2/K) \subset \mathrm{Spl}(L_1/K)$. Conversely, if $\mathrm{Spl}(L_2/K) \subset \mathrm{Spl}(L_1/K)$, consider the extension $L_1 L_2/K$. It is Galois, and $\mathrm{Spl}(L_1 L_2/K) = \mathrm{Spl}(L_1/K) \cap \mathrm{Spl}(L_2/K)$. From the hypothesis, $\mathrm{Spl}(L_1/K) \cap \mathrm{Spl}(L_2/K) = \mathrm{Spl}(L_2/K)$, so $\mathrm{Spl}(L_1 L_2/K) = \mathrm{Spl}(L_2/K)$. Computing the Dirichlet density of both sides, we get $1/[L_1 L_2 : K] = 1/[L_2 : K]$ by Corollary 2.4. Thus $L_1 L_2 = L_2$, so $L_1 \subset L_2$. □

Changing a set of primes by a finite amount does not affect its density, so Bauer's theorem is true with the inclusion and equality of sets of split primes being true up to finitely many exceptions. For example, the only Galois extension of $\mathbf{Q}$ whose split primes are $\{p \equiv 1 \bmod 4\}$ up to finitely many exceptional primes is $\mathbf{Q}(i)$. Allowing finitely many exceptional primes in Bauer's theorem is important when we use it in the context of Weber's definition of a class field below.

Although Bauer's theorem tells us that a Galois extension L/K is determined (as an extension of K) by the primes in K which split completely in L, this doesn't give us a simple rule for describing the set of split primes. When L/K is abelian, class field theory will give a simple rule for $\mathrm{Spl}(L/K)$ in terms of generalized congruences.

3. Splitting Laws (Weber)

Reference: [1].

In his 1891 book on elliptic functions and algebraic numbers, H. Weber introduced the label "class field" for the species of Kronecker, so at first a class field was just a particular abelian (conjecturally unramified) extension of an imaginary quadratic field, whose Galois group is isomorphic to the ideal class group of the base field. In 1897, Weber extended the concept of ideal class group: for any number field K and nonzero ideal $\mathfrak{m}$ in $\mathcal{O}_K$, let $I_{\mathfrak{m}}$ be the group of fractional ideals in K relatively prime to $\mathfrak{m}$ and let $P_{\mathfrak{m}}^+$ be the group of principal fractional ideals (α/β) where α and β are nonzero integers in K such that

- (α) and (β) are relatively prime to $\mathfrak{m}$,
- $\alpha \equiv \beta \bmod \mathfrak{m}$.

---

[3]The construction of Frobenius elements was made by Frobenius in 1880 and independently found by Dedekind, according to correspondence between them in 1882.

- α/β is totally positive (that is, under all real embeddings of K, if there are any, α/β has positive image).

Example 3.1. An ideal is in $P_{(1)}^+$ if it has a totally positive generator. In $\mathbf{Q}(\sqrt{2})$, the ideal $(\sqrt{2})$ is in $P_{(1)}^+$ even though $\sqrt{2}$ is not totally positive, since another generator $\sqrt{2}(1+\sqrt{2})$ is totally positive. In $\mathbf{Q}(\sqrt{3})$, $(\sqrt{3}) \notin P_{(1)}^+$ since $\sqrt{3}u$ is not totally positive for any $u \in \mathbf{Z}[\sqrt{3}]^\times$: all units in $\mathbf{Z}[\sqrt{3}]$ have norm 1, so $\sqrt{3}u$ has norm -3 and therefore can't be totally positive.

The index $[I_\mathfrak{m} : P_\mathfrak{m}^+]$ is finite. Any intermediate group

$$P_\mathfrak{m}^+ \subset H \subset I_\mathfrak{m}$$

is called an *ideal group with modulus* $\mathfrak{m}$ and the quotient $I_\mathfrak{m}/H$ is called a *generalized ideal class group*. If $\mathfrak{m} = (1)$ and P is the group of principal fractional ideals, then $P_{(1)}^+ \subset P \subset I_{(1)}$ and $I_{(1)}/P$ is the ideal class group. When $K = \mathbf{Q}$ and $\mathfrak{m} = m\mathbf{Z}$, $I_\mathfrak{m}/P_\mathfrak{m}^+ \cong (\mathbf{Z}/m\mathbf{Z})^\times$ (send each fractional ideal $(a/b)\mathbf{Z}$, with positive generator a/b, to the congruence class $ab^{-1} \bmod m$).

Considering $I_\mathfrak{m}/H$ as a generalization of $(\mathbf{Z}/m\mathbf{Z})^\times$, Weber sought an analogue of Dirichlet's theorem (1837) that every congruence class in $(\mathbf{Z}/m\mathbf{Z})^\times$ contains infinitely many primes: does each coset of $I_\mathfrak{m}/H$ contain infinitely many prime ideals? To solve this, Weber adapted Dirichlet's method, whose key tool was L-functions of characters $\chi \colon (\mathbf{Z}/m\mathbf{Z})^\times \to \mathbf{C}^\times$, defined by

$$L(s,\chi) = \prod_{(p,m)=1} \frac{1}{1 - \chi(p)p^{-s}} = \sum_{(n,m)=1} \frac{\chi(n)}{n^s}$$

for $\mathrm{Re}(s) > 1$. The series converges (conditionally) for $\mathrm{Re}(s) > 0$ when χ is nontrivial, and the heart of Dirichlet's argument is the proof that $L(1,\chi) \neq 0$ for all nontrivial χ. Weber introduced an L-function for characters $\psi \colon I_\mathfrak{m}/H \to \mathbf{C}^\times$:

$$(3.1) \qquad L(s,\psi) = \prod_{\mathfrak{p} \nmid \mathfrak{m}} \frac{1}{1 - \psi(\mathfrak{p})\,\mathrm{N}\mathfrak{p}^{-s}} = \sum_{(\mathfrak{a},\mathfrak{m})=1} \frac{\psi(\mathfrak{a})}{\mathrm{N}\mathfrak{a}^s}$$

for $\mathrm{Re}(s) > 1$. For nontrivial ψ, the series is convergent slightly to the left of 1 (specifically, it converges for $\mathrm{Re}(s) > 1 - 1/[K : \mathbf{Q}]$), so it makes sense to talk about $L(1,\psi)$.

Theorem 3.2 (Weber). *For a nonzero ideal $\mathfrak{m}$ in $\mathcal{O}_K$ and ideal group H with modulus $\mathfrak{m}$, assume there is a Galois extension L/K such that $\mathrm{Spl}(L/K) \subset H$ with finitely many exceptions. Then*

$$(3.2) \qquad [I_\mathfrak{m} : H] \leq [L : K].$$

If $\mathrm{Spl}(L/K) = H$ with finitely many exceptions then $[I_\mathfrak{m} : H] = [L : K]$ and there are infinitely many primes in each coset of $I_\mathfrak{m}/H$.

Weber's proof depends on showing $L(1,\psi) \neq 0$ for nontrivial ψ, and this is established using orthogonality relations on characters of $I_\mathfrak{m}/H$ and the fact that the Dedekind zeta-function of any number field (namely K and the hypothesized extension L) has a simple pole at $s = 1$.

Definition 3.3 (Weber, 1908). For a nonzero ideal $\mathfrak{m}$ in $\mathcal{O}_K$ and ideal group H with modulus $\mathfrak{m}$, the *class field* over K for H is a Galois extension L/K such that for primes $\mathfrak{p} \nmid \mathfrak{m}$ in K,

$$(3.3) \qquad \mathfrak{p} \text{ splits completely in } L \iff \mathfrak{p} \in H.$$

A class field over K, for Weber, is an extension of K whose set of split primes are (up to finitely many exceptions) the prime ideals in an ideal group. We have to allow finitely many exceptions because an ideal group with modulus $\mathfrak{m}$ contains no prime dividing $\mathfrak{m}$ (they are not in $I_\mathfrak{m}$) and some of the prime factors of $\mathfrak{m}$ may split in the extension.

Theorem 3.2 tells us what class fields can be good for: their existence implies the infinitude of primes in cosets of generalized ideal class groups. Bauer's theorem (allowing finitely many exceptional primes) tells us the class field L/K for H is unique *if* it exists.

Example 3.4. The extension $\mathbf{Q}(i)/\mathbf{Q}$ is the class field for $P_{(4)}^+$ since p splits in $\mathbf{Q}(i)$ if and only if $p \equiv 1 \bmod 4$ (where p is a positive prime).

Example 3.5. The extension $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ is the class field for $\{P_8^+, -P_{(8)}^+\}$, since p splits in $\mathbf{Q}(\sqrt{2})$ if and only if $p \equiv \pm 1 \bmod 8$.

Weber needed the existence of class fields to prove his extension of Dirichlet's theorem to generalized ideal class groups. For certain ideal groups H from imaginary quadratic K, Weber could prove the existence of a class field L/K and an isomorphism of $\mathrm{Gal}(L/K)$ with $I_\mathfrak{m}/H$, but the existence of class fields for ideal groups over number fields beyond $\mathbf{Q}$ and imaginary quadratics was left open.

4. Unramified Extensions (Hilbert)

References: [12], [17], [20].

Hilbert's ideas 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 fields. One of his goals was to develop reciprocity laws in number fields, building on his conception (1897) of the quadratic reciprocity law over $\mathbf{Q}$ as a product formula: $\prod_v (a, b)_v = 1$ for any a and b in $\mathbf{Q}^\times$, where $(a, b)_v$ is the v-adic Hilbert symbol:

$$(a, b)_v = \begin{cases} 1, & \text{if } a = x^2 - by^2 \text{ is solvable in } \mathbf{Q}_v, \\ -1, & \text{otherwise.} \end{cases}$$

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 constraints on a and b. There are several new aspects being used in this version of quadratic reciprocity: emphasis on norms rather squares, p-adic equations[4] rather than congruences modulo p, and the infinite places on an equal footing with the finite places. Ultimately all three ideas will appear in class field theory, and none are present in Weber's work.

The Hilbert symbol makes sense on any number field K (replacing completions of $\mathbf{Q}$ with completions of K in the definition), 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 which 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 $\mathbf{Q}(\zeta_p)$ (1859) was restricted to regular primes ($p \nmid h(\mathbf{Q}(\zeta_p))$), which Hilbert could

---

[4]Hilbert wrote congruences modulo arbitrarily high powers of p, as the p-adics did not yet exist, although they were just on the verge of existence: Hensel's first paper on them appeared in 1897.

interpret as avoiding the cases when $\mathbf{Q}(\zeta_p)$ has an abelian unramified extension of degree p. Hilbert's proof of the Kronecker-Weber theorem succeeded in part because $\mathbf{Q}$ has no (abelian) unramified extensions larger than $\mathbf{Q}$. It is perhaps this experience which drove Hilbert's interest in *unramified* abelian extensions, as an obstacle in proofs. Thinking about analogies between number fields and Riemann surfaces (*e.g.*, 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.

Conjecture 4.1 (Hilbert, 1898)**.** *For any number field K there is a unique finite extension K'/K such that*

(1) *K'/K is Galois and $\operatorname{Gal}(K'/K) \cong \operatorname{Cl}(K)$,*
(2) *K'/K is unramified at all places, and every abelian extension of K with this property is a subfield of K',*
(3) *for any prime $\mathfrak{p}$ of K, the residue field degree $f_{\mathfrak{p}}(K'/K)$ is the order of $\mathfrak{p}$ in $\operatorname{Cl}(K)$,*
(4) *every ideal of K is principal in K'.*

Condition (3) implies that a prime in K splits in K' if and only if it is principal in K, so K' is a class field over K in Weber's sense for the ideal group of all principal fractional ideals in K. The field K' 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.[5]

Example 4.2. The extensions

$$
\begin{array}{cccc}
\mathbf{Q}(\sqrt{6}, \sqrt{-2}) & \mathbf{Q}(\sqrt{-23}, \alpha) & \mathbf{Q}(\sqrt{-31}, \beta) & \mathbf{Q}(\sqrt{-14}, \sqrt{2\sqrt{2}-1}) \\
\Big|\,2 & \Big|\,3 & \Big|\,3 & \Big|\,4 \\
\mathbf{Q}(\sqrt{6}) & \mathbf{Q}(\sqrt{-23}) & \mathbf{Q}(\sqrt{-31}) & \mathbf{Q}(\sqrt{-14})
\end{array}
$$

are all examples of Hilbert class fields over the base fields, with $\alpha^3 - \alpha - 1 = 0$ and $\beta^3 + \beta + 1 = 0$. In particular, each of these extensions has degree equal to the class number of the base field and the Galois group of the extension is isomorphic to the ideal class group of the base field. The third example is the same as $\mathbf{Q}(\sqrt{-31}, \gamma)$ in Example 2.2, since $\beta := -16480503\gamma^2 + 11239722\gamma - 24150771$ is a root of $X^3 + X + 1$.

Hilbert proved the existence of the Hilbert class field when $h(K) = 2$ (and $[K : \mathbf{Q}] = 2$). In 1907, Hilbert's student Furtwängler proved the first two parts of Hilbert's conjecture in general, and used this to prove the quadratic reciprocity law in all number fields in 1913. He proved the third part in 1911. The fourth part, which extends an observation of Kronecker for imaginary quadratic fields, was proved by Furtwängler (1930) after Artin reduced it to a purely group-theoretic statement related to the iterated Hilbert class field $K'' = (K')'$, which is a Galois extension of K that is usually not abelian.

---

[5]Hilbert's notion of class field concerned abelian extensions unramified at all prime ideals, but ramification at infinity was not forbidden. For instance, $\mathbf{Q}(\sqrt{3})$ has class number 1 but $\mathbf{Q}(\sqrt{3}, i)/\mathbf{Q}(\sqrt{3})$ is unramified at all prime ideals in $\mathbf{Z}[\sqrt{3}]$; there is ramification at infinity. So Hilbert's conjecture was actually about the "Hilbert class field in the narrow sense," whose Galois group is isomorphic to the narrow ideal class group where fractional ideals are identified only if their ratio is a principal ideal having a *totally positive* generator. The narrow class number of $\mathbf{Q}(\sqrt{3})$, for instance, is 2. We stated Hilbert's conjecture in terms of unramifiedness even at the archimedean places since that's what the label Hilbert class field means today.

5. Class Field Theory Proved (Takagi)

References: [5], [7], [14]

T. Takagi studied in Germany during 1898–1901, partly with Hilbert in Göttingen. In his 1903 thesis, Takagi proved the Jugendtraum for base field $\mathbf{Q}(i)$ using values of the lemniscatic function, as Kronecker had envisioned. His proof was an adaptation to $\mathbf{Q}(i)$ of Hilbert's proof of the Kronecker–Weber theorem. In 1914, R. Fueter proved that for any imaginary quadratic field K, viewed as a subfield of $\mathbf{C}$, every *odd* degree abelian extension of K inside of $\mathbf{C}$ is a subfield of some $K(e^{2\pi i r}, j(\tau))$, where $r \in \mathbf{Q}$ and $\tau \in K$ (with $\operatorname{Im}(\tau) > 0$). 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 $e^{2\pi i z}$ at rational numbers and the j-function at numbers in K. Fueter also gave a counterexample for extensions of even degree: $\mathbf{Q}(\sqrt[4]{1+2i})$ has degree 4 over $\mathbf{Q}(i)$ and is a cyclic extension, but it lies in no field of the form $\mathbf{Q}(i, e^{2\pi i r}, j(\tau))$ for $r \in \mathbf{Q}$ and $\tau \in \mathbf{Q}(i)$.

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 (the only place where algebraic number theory was under serious study) 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 them.

Takagi began with a new definition of a class field, using norms of ideals rather than splitting laws and also incorporating infinite places into the modulus. (Note the influence of Hilbert's ideas on norms and infinite places.)

Definition 5.1. 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 in K and set the *norm* of $\mathfrak{P}$ in K to be

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

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

This notion of norm is compatible with the ring-theoretic norm on principal fractional ideals: $\mathrm{N}_{L/K}(x\mathcal{O}_L) = \mathrm{N}_{L/K}(x)\mathcal{O}_K$ for $x \in L^\times$. Throughout class field theory, groups of norm-values play a key role.

The link between Weber's and Takagi's viewpoints is that when L/K is Galois and $\mathfrak{p}$ is unramified in L, $\mathfrak{p}$ splits in L (Weber) if and only if $\mathfrak{p}$ is the norm of some ideal from L (Takagi).

Definition 5.2. A K-*modulus* is a formal product $\mathfrak{m} = \mathfrak{m}_f \mathfrak{m}_\infty$, where $\mathfrak{m}_f$ (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 $\mathfrak{m}_f$.

Let $I_\mathfrak{m}$ be the fractional ideals relatively prime to $\mathfrak{m}$ and $P_\mathfrak{m}$ be the principal fractional ideals (α/β) where α and β are nonzero integers in K such that

- (α) and (β) are relatively prime to $\mathfrak{m}$,
- $\alpha \equiv \beta \bmod \mathfrak{m}_f$,
- $v(\alpha/\beta) > 0$ for all real embeddings $v | \mathfrak{m}_\infty$.

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

$$\mathrm{N}_\mathfrak{m}(L/K) := \{\mathfrak{a} \text{ in } K : \mathfrak{a} = \mathrm{N}_{L/K}(\mathfrak{A}) \text{ for a fractional ideal } \mathfrak{A} \text{ in } L, \mathfrak{a} \text{ is rel. prime to } \mathfrak{m}\}.$$

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

What is the purpose of the group $H_{\mathfrak{m}}(L/K)$? We want to create an ideal group using norms of ideals, but $\mathrm{N}_{\mathfrak{m}}(L/K)$ need not contain $P_{\mathfrak{m}}$. Multiplying by $P_{\mathfrak{m}}$ gives us a group that contains $P_{\mathfrak{m}}$ and thus becomes an ideal group. Put differently, the subgroup of $I_{\mathfrak{m}}/P_{\mathfrak{m}}$ generated by cosets of $\mathrm{N}_{\mathfrak{m}}(L/K)$ is $H_{\mathfrak{m}}(L/K)/P_{\mathfrak{m}}$, so this 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.

What is the connection between Weber's and Takagi's ideal groups? For a general number field K and nonzero ideal $\mathfrak{m}$, Weber's $P_{\mathfrak{m}}^{+}$ equals Takagi's $P_{\mathfrak{m}\infty}$, where ∞ is the product of all real places of the number field. Takagi has a more general construction than Weber since Takagi allows varying sign conditions in his modulus. (Weber had largely worked over imaginary quadratic fields, where there are no real places, so he had no motivation to be sensitive to varying sign conditions.)

When $\mathfrak{m}$ is a K-modulus and L/K is Galois, the primes of K not dividing $\mathfrak{m}$ which split in L lie in $\mathrm{N}_{\mathfrak{m}}(L/K) \subset H_{\mathfrak{m}}(L/K)$, so $\mathrm{Spl}(L/K) \subset H_{\mathfrak{m}}(L/K)$ except perhaps for primes dividing $\mathfrak{m}$. Therefore Theorem 3.2 (whose proof works with any K-modulus in place of the nonzero ideals in $\mathcal{O}_K$) implies

(5.1) $$[I_{\mathfrak{m}} : H_{\mathfrak{m}}(L/K)] \le [L : K].$$

Definition 5.3 (Takagi). A Galois extension of number fields L/K is called a *class field* when (5.1) is an equality for some K-modulus $\mathfrak{m}$. Any such $\mathfrak{m}$ is called an *admissible* modulus for L/K.

For all $\mathfrak{m}$ the left side of (5.1) is no larger than the right side, so admissibility is a kind of optimal property. For some extensions there could be an inequality for all $\mathfrak{m}$ (that is, there may be no admissible modulus at all).

Example 5.4. We saw in Example 3.4 that $\mathbf{Q}(i)/\mathbf{Q}$ is a class field in Weber's sense. Now we will show it is a class field in Takagi's sense, with admissible modulus 4∞. Since $\mathrm{N}_{4\infty}(\mathbf{Q}(i)/\mathbf{Q}) \subset P_{4\infty}$ (essentially because an odd sum of two integral squares is 1 mod 4), $H_{4\infty}(\mathbf{Q}(i)/\mathbf{Q}) = P_{4\infty}$, and $[I_{4\infty} : P_{4\infty}] = \#(\mathbf{Z}/4\mathbf{Z})^{\times} = 2 = [\mathbf{Q}(i) : \mathbf{Q}]$, so the upper bound is reached.

To define a class field, Weber picks any ideal group H and seeks a corresponding (class) field L/K, which should exist and be abelian, while Takagi picks any L/K and sees if there is an ideal group H making (5.1) an equality (which may not happen).

It is useful to know the relations among all admissible moduli for an extension L/K. Any multiple of an admissible modulus is admissible.[6] To prove this, if $\mathfrak{m}|\mathfrak{m}'$ then $I_{\mathfrak{m}'} \subset I_{\mathfrak{m}}$, $P_{\mathfrak{m}'} \subset P_{\mathfrak{m}}$, and $\mathrm{N}_{\mathfrak{m}'}(L/K) \subset \mathrm{N}_{\mathfrak{m}}(L/K)$, so $H_{\mathfrak{m}'}(L/K) \subset H_{\mathfrak{m}}(L/K)$. The natural map $I_{\mathfrak{m}'}/H_{\mathfrak{m}'} \to I_{\mathfrak{m}}/H_{\mathfrak{m}}$ is onto,[7] so (5.1) with modulus $\mathfrak{m}'$ implies $[I_{\mathfrak{m}'} : H_{\mathfrak{m}'}] = [L : K]$ if $[I_{\mathfrak{m}} : H_{\mathfrak{m}}] = [L : K]$. For any two admissible K-moduli, their least common multiple is admissible. Going the other way, the greatest common factor of two admissible moduli is

---

[6]Using Weber's definition of a class field for an ideal group, call an ideal $\mathfrak{m}$ in $\mathcal{O}_K$ *admissible* for L/K if there is an ideal group with modulus $\mathfrak{m}$ in Weber's sense whose class field in Weber's sense is L. The notions of admissible for Weber and Takagi ultimately turn out to coincide, but it's a good exercise to check directly from the definition that any multiple of an admissible modulus in Weber's sense is admissible.

[7]This means any coset in $I_{\mathfrak{m}}/H_{\mathfrak{m}}$ contains an ideal relatively prime to $\mathfrak{m}'$ when $\mathfrak{m}|\mathfrak{m}'$. It generalizes the fact that if $m|n$ then the natural map $(\mathbf{Z}/n\mathbf{Z})^{\times} \to (\mathbf{Z}/m\mathbf{Z})^{\times}$ is onto.

admissible (this is somewhat more delicate to show, since not every factor of 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 multiples of it. The least admissible modulus for L/K is called the *conductor* of L/K and is denoted $\mathfrak{f}_{L/K}$ from the German word Führer.[8]

Example 5.5. The extension $\mathbf{Q}(i)/\mathbf{Q}$ has admissible modulus 4∞, but neither 2∞ nor 4 are admissible for $\mathbf{Q}(i)/\mathbf{Q}$ since $[I_{2\infty} : P_{2\infty}]$ and $[I_4 : P_4]$ equal 1 rather than 2, so the conductor of $\mathbf{Q}(i)/\mathbf{Q}$ is 4∞.

Theorem 5.6 (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 class field L/K, then* $\mathrm{Gal}(L/K) \cong I_{\mathfrak{m}}/H$.
   (3) (*Completeness*) *Any finite abelian extension 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 $L_1 \subset L_2 \Longleftrightarrow H_2 \subset H_1$.*
   (5) (*Conductor*) *The places of K appearing in the conductor $\mathfrak{f}_{L/K}$ 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 any prime $\mathfrak{p} \nmid \mathfrak{m}$ is unramified in L and the residue field degree $f_{\mathfrak{p}}(L/K)$ equals the order of $\mathfrak{p}$ in $I_{\mathfrak{m}}/H$.*

Some parts of this theorem had been proved earlier by Weber (comparison, and in some cases isomorphism).

Here are some immediate consequences 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 reprove all of Hilbert's conjectures on the Hilbert class field except for the last conjecture on principalization. Moreover, the comparison and conductor theorems show the Hilbert class field of K contains all other abelian unramified extensions of K. Thus the Hilbert class field is the maximal abelian everywhere unramified extension of K. The comparison and completeness theorems imply that any finite abelian extension of K is inside the class field over K of some $P_{\mathfrak{m}}$. This is a generalization of the Kronecker–Weber theorem, since the class field over $\mathbf{Q}$ of $P_{m\infty}$ is $\mathbf{Q}(\zeta_m)$. (The naive generalization of the Kronecker-Weber theorem to all numbers fields is completely false: when $K \neq \mathbf{Q}$, there are abelian extensions of K which are not contained in a cyclotomic extension of K.) At the end of his paper, Takagi proved Kronecker's Jugendtraum for all imaginary quadratic fields.

Now we make some comments on the different parts of Takagi's theorem.

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

---

[8]This technical meaning for Führer used to be translated as *leader* in the early 1930s. See the review of Fueter's book on complex multiplication in the 1931 Bulletin of the Amer. Math. Society, page 655.

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 (finite abelian groups have enough numerical invariants to make this possible, *e.g.*, two cyclic groups are abstractly isomorphic as soon as we know they have the same size). 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 (5.1) and an inequality that is its reverse for abelian L/K:

$$(5.2) \qquad\qquad [I_{\mathfrak{m}} : H_{\mathfrak{m}}(L/K)] \geq [L : K]$$

for some $\mathfrak{m}$. Note (5.1) is valid for all Galois extensions, while (5.2) is stated only for abelian extensions (and in fact is not true for any other extensions). Takagi proved (5.2) only for cyclic extensions of prime degree, which sufficed for his inductive proof. Later Hasse found a proof of (5.2) that did not need a restriction to prime degree. Unlike the proof of (5.1), which uses Weber's L-functions, the proof of (5.2) 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 $\mathfrak{m}$. (These are the fields between K and the class field over K for $P_{\mathfrak{m}}$.) Their corresponding ideal groups with modulus $\mathfrak{m}$ are the subgroups between $P_{\mathfrak{m}}$ and $I_{\mathfrak{m}}$. However, if we start to consider *all* class fields at once, then we run into a comparison problem: the admissible moduli for two class fields might not be the same, so we have to pass to a common admissible modulus for the two extensions before we can compare them by their ideal groups. This is like comparing two abelian extensions of $\mathbf{Q}$ by Galois theory only after embedding them 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 that have the same class field. When does this happen? If H and H' are ideal groups for K defined with moduli $\mathfrak{m}$ and $\mathfrak{m}'$ (that is, $P_{\mathfrak{m}} \subset H \subset I_{\mathfrak{m}}$ and $P_{\mathfrak{m}'} \subset H \subset I_{\mathfrak{m}'}$), 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 which 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 5.7 (Hasse). *Let L/K be abelian and $\mathfrak{m}$ be an admissible modulus for L/K. For any character χ of $I_{\mathfrak{m}}/H_{\mathfrak{m}}$, let L_{χ} be the class field to $\ker \chi$ and set $\mathfrak{f}_{\chi}$ to be the conductor of L_{χ}/K. Then the discriminant of L/K is given by the formulas*

$$\mathrm{disc}(L/K) = \prod_{\chi} \mathfrak{f}_{\chi,f},$$

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

This is the conductor-discriminant formula (or Führerdiskriminantenproduktformel). It expresses the discriminant of an abelian extension L/K in terms of conductors of cyclic subextensions L_{χ}/K (the Galois group of L_{χ}/K is isomorphic to the image of χ, which is a

cyclic group). 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 $\mathrm{disc}(L/K)$ as a product of the finite parts of the $\mathfrak{f}_\chi$, Hasse showed the conductor $\mathfrak{f}_{L/K}$ is their least common multiple (retaining the infinite places).

Example 5.8. When $[L : K] = 2$, $\mathrm{disc}(L/K)$ is the finite part of $\mathfrak{f}_{L/K}$. In particular, if $L = \mathbf{Q}(\sqrt{d})$ for squarefree d, the conductor of L has finite part $|d|$ or $4|d|$, which proves $4|d|\infty$ is an admissible modulus for $\mathbf{Q}(\sqrt{d})$.

The decomposition theorem shows a prime $\mathfrak{p} \nmid \mathfrak{m}$ splits in L if and only if $\mathfrak{p} \in H$, so Weber's and Takagi's notions of class field agree. Takagi's definition in terms of norms rather than prime splitting just happens to be more convenient than Weber's as a starting point to prove theorems.

The decomposition theorem also tells us a special property of abelian extensions: the primes which split in the extension are described by "congruence conditions." For instance, the primes p splitting in $\mathbf{Q}(\sqrt{6})$ satisfy $p \equiv 1, 5, 19, 23 \bmod 24$. (This follows from quadratic reciprocity.) These congruence classes are a subgroup of the units mod 24. To see what this turns into for a general abelian extension L/K, we appeal to the completeness theorem: L is a class field over K for some modulus $\mathfrak{m}$, so a prime $\mathfrak{p}$ of K not dividing $\mathfrak{m}$ splits completely in L if and only if $\mathfrak{p}$ lies in $H_\mathfrak{m}$ (since $\mathfrak{p}$ is unramified in L and the order of $\mathfrak{p}$ in $I_\mathfrak{m}/H_\mathfrak{m}$ is its residue field degree). Therefore the primes not dividing $\mathfrak{m}$ which are in $\mathrm{Spl}(L/K)$ are those in the subgroup $H_\mathfrak{m}/P_\mathfrak{m}$ of $I_\mathfrak{m}/P_\mathfrak{m}$, and lying in a subgroup should be thought of as generalized congruence conditions. Since class fields over K are the same thing as abelian extensions, splitting in an abelian extension is described by congruences. Amazingly, the converse is also true by class field theory. To show this, we extend Bauer's theorem.

Lemma 5.9 (Bauer, 1916). *Let L_1 and L_2 be finite extensions of a number field K, with L_2/K Galois. Then $L_1 \subset L_2$ if and only if $\mathrm{Spl}(L_2/K) \subset \mathrm{Spl}(L_1/K)$.*

Proof. Let $\widetilde{L}_1/K$ be the Galois closure of L_1/K. Since L_2/K is Galois, $L_1 \subset L_2$ if and only if $\widetilde{L}_1 \subset L_2$. Also a prime splits completely in an extension if and only if it splits completely in the Galois closure, so $\mathrm{Spl}(L_1/K) = \mathrm{Spl}(\widetilde{L}_1/K)$. Now we can invoke Bauer's theorem given earlier (Theorem 2.6) for a pair of Galois extensions. $\qquad\square$

Theorem 5.10. *Let L/K be a finite extension of number fields and assume there is a K-modulus $\mathfrak{m}$ and a finite set S of primes in K containing all $\mathfrak{p}|\mathfrak{m}$ such that whether or not a prime $\mathfrak{p} \notin S$ splits in L is determined by the coset of $\mathfrak{p}$ in $I_\mathfrak{m}/P_\mathfrak{m}$. Then L/K is an abelian extension.*

Proof. Let $R_\mathfrak{m}$ be the class field over K of $P_\mathfrak{m}$, so a prime in K not dividing $\mathfrak{m}$ splits in $R_\mathfrak{m}$ if and only if it is in $P_\mathfrak{m}$. Consider the composite extension $LR_\mathfrak{m}/K$. The set of primes in K splitting in a finite extension of K is infinite, so there is a prime $\mathfrak{q} \notin S$ which splits in $LR_\mathfrak{m}$. Since $\mathfrak{q}$ splits in $R_\mathfrak{m}$ and doesn't divide $\mathfrak{m}$, $\mathfrak{q} \in P_\mathfrak{m}$. For any prime $\mathfrak{p} \notin S$ which splits in $R_\mathfrak{m}$, $\mathfrak{p} \in P_\mathfrak{m}$ (by the definition of $R_\mathfrak{m}$), so $\mathfrak{p} = \mathfrak{q}$ in $I_\mathfrak{m}/P_\mathfrak{m}$ and therefore $\mathfrak{p}$ splits in L by hypothesis. Hence the primes of $\mathrm{Spl}(R_\mathfrak{m}/K) \subset \mathrm{Spl}(L/K)$ except perhaps for primes dividing $\mathfrak{m}$, so $L \subset R_\mathfrak{m}$ by Lemma 5.9. (Here we need that $R_\mathfrak{m}/K$ is Galois.) Since $R_\mathfrak{m}/K$ is abelian, the subextension L/K is abelian. $\qquad\square$

Corollary 5.11. *For a number field $L/\mathbf{Q}$ and $m \in \mathbf{Z}^+$, the following conditions are equivalent:*

(1) *for any positive prime p not dividing m, the splitting of p in $L/\mathbf{Q}$ is determined by a congruence condition on p mod m,*

(2) $L \subset \mathbf{Q}(\zeta_m)$.

Both Weber and Takagi defined class fields as Galois extensions with a certain additional property (using prime splitting or group indices). In 1929, A. Scholz showed the Galois property can be dropped, as a non-Galois extension L/K has $[I_{\mathfrak{m}} : H_{\mathfrak{m}}(L/K)] < [L : K]$ for all K-moduli $\mathfrak{m}$, so L/K can't be a class field. Thus (5.1) holds for all finite extensions, while (5.2) is still only true for abelian extensions. (The largest size of $[I_{\mathfrak{m}} : H_{\mathfrak{m}}(L/K)]$ as $\mathfrak{m}$ varies is $[\widetilde{L} : K]$, where $\widetilde{L}$ is the maximal abelian extension of K in L.)

6. Canonical Isomorphism (Artin)

References: [11], [13]

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 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 $K \subset L$, 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 any 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 $\mathbf{C}$. The issue is whether the multiplicity of any 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 any poles.

Although we can consider here any extension of numbers 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 nontrivial characters (of an ideal group with class field L/K) and Weber L-functions of nontrivial characters are entire functions, so L/K 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 characters of the group and Artin's definition looks like the following.

Definition 6.1 (Artin, 1923). Let L/K be a finite abelian extension with Galois group G. For a character χ of G and $\mathrm{Re}(s) > 1$, set

$$L(s, \chi) = \prod_{\mathfrak{p} \text{ unram.}} \frac{1}{1 - \chi(\mathrm{Frob}_{\mathfrak{p}}(L/K)) \, \mathrm{N}\mathfrak{p}^{-s}},$$

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

The Frobenius element of a prime ideal is defined initially for unramified primes in the top field. As a function of unramified primes in the bottom field, Frobenius elements are only well-defined up to conjugation, so in an *abelian* Galois group they are still well-defined elements.

For Artin's L-function to have a clean *functional equation*, which we won't discuss here, there should be Euler factors in the L-function at the ramified primes too. For example, if χ is the trivial character of $\mathrm{Gal}(L/K)$ then $L(s, \chi)$ ought to be $\zeta_K(s)$, but in the above definition Euler factors at ramified $\mathfrak{p}$ are missing. Since there is not a well-defined Frobenius

element at ramified primes in a Galois extension, it is not at all clear how to make a correct definition for Euler factors at these primes based on the way Euler factors in the L-function are defined at the unramified primes. In 1923, Artin was able to find the right Euler factors for his L-functions at ramified primes only by a roundabout way *using* class field theory. In 1930 he found a definition of the correct Euler factors at the ramified primes using inertia groups without class field theory.[9] The provisional definition of $L(s, \chi)$ above, using only the unramified primes, will suffice for us.

Here's the situation: Artin has L-functions for characters of Galois groups, Weber has L-functions for characters of generalized ideal class groups, and for any abelian extension L/K, Takagi proved there is an isomorphism

$$(6.1) \qquad\qquad I_{\mathfrak{m}}/H_{\mathfrak{m}} \cong \mathrm{Gal}(L/K)$$

for all admissible K-moduli $\mathfrak{m}$ (which are the multiples of the least admissible modulus $\mathfrak{f}_{L/K}$). But Takagi did not find any specific isomorphism between these groups; an isomorphism was only obtained in an indirect way. Since the Weber and Artin L-functions are defined on characters of isomorphic groups, it is natural to ask for an explicit isomorphism $\varphi\colon I_{\mathfrak{m}}/H_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ that identifies the L-functions: $L_A(s, \chi) = L_W(s, \chi \circ \varphi)$ for every character χ of $\mathrm{Gal}(L/K)$, where we write L_A and L_W for the Artin and Weber constructions of L-functions. Recall from (3.1) Weber's L-function of a character ψ of $I_{\mathfrak{m}}/H_{\mathfrak{m}}$:

$$L(s, \psi) = \prod_{\mathfrak{p} \nmid \mathfrak{m}} \frac{1}{1 - \psi(\mathfrak{p}) \, \mathrm{N}\mathfrak{p}^{-s}}.$$

Takagi showed any $\mathfrak{p} \nmid \mathfrak{m}$ is unramified in L, and if we use the conductor of L/K as a modulus then the Weber L-function is a product over all unramified primes, just like the Artin L-function. In any event, staring at the Euler factor of $\mathfrak{p}$ in both the Artin and Weber L-functions suggested to Artin an isomorphism φ from $I_{\mathfrak{m}}/H_{\mathfrak{m}}$ to $\mathrm{Gal}(L/K)$: let $\varphi(\mathfrak{p}) = \mathrm{Frob}_{\mathfrak{p}}(L/K)$ for $\mathfrak{p} \nmid \mathfrak{m}$ and extend φ to all of $I_{\mathfrak{m}}/H_{\mathfrak{m}}$ by multiplicativity.

There is certainly no problem in multiplicatively 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 any 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 $\mathrm{Frob}_{\mathfrak{p}}(L/K) = \mathrm{Frob}_{\mathfrak{q}}(L/K)$? This is not obvious! In the special case that L/K is abelian of prime degree ℓ and $\mu_\ell \subset K$, Takagi showed a result of this kind in 1922, which must have encouraged Artin that he was on the right track.

Definition 6.2. For an abelian extension L/K and K-modulus $\mathfrak{m}$ divisible by the primes which ramify in L, the *Artin map* $\varphi_{L/K, \mathfrak{m}}\colon I_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ is given by $\varphi_{L/K, \mathfrak{m}}(\mathfrak{p}) = \mathrm{Frob}_{\mathfrak{p}}(L/K)$ at primes not dividing $\mathfrak{m}$ and is extended to $I_{\mathfrak{m}}$ by multiplicativity. For any ideal relatively prime to $\mathfrak{m}$, $\varphi_{L/K, \mathfrak{m}}(\mathfrak{a})$ is called the *Artin symbol* at $\mathfrak{a}$.

Theorem 6.3 (Artin, 1927). *When $\mathfrak{m}$ is a K-modulus divisible by the places of K which ramify in L, the Artin map $\varphi_{L/K, \mathfrak{m}}\colon I_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ is surjective and its kernel contains $\mathrm{N}_{\mathfrak{m}}(L/K)$. When $\mathfrak{m}$ is admissible for L/K, the kernel of the Artin map is $P_{\mathfrak{m}} \mathrm{N}_{\mathfrak{m}}(L/K) = H_{\mathfrak{m}}(L/K)$, so $I_{\mathfrak{m}}/H_{\mathfrak{m}}(L/K) \cong \mathrm{Gal}(L/K)$ by the Artin map.*

This is the *Artin reciprocity law*. The isomorphism in the reciprocity law makes Takagi's isomorphism theorem (which had no specific isomorphism in it) explicit and it also explains

---

[9]The ramified primes also appear in Artin's definition of the conductor for his L-function, which is a constant in its functional equation.

the decomposition theorem since $\mathrm{Frob}_{\mathfrak{p}}(L/K)$ has order $f_{\mathfrak{p}}(L/K)$ in $\mathrm{Gal}(L/K)$. Artin conjectured the reciprocity law in 1923, but at the time could only prove it in special cases, such as cyclotomic and Kummer extensions. Several years later, Artin read Chebotarev's field-crossing method with cyclotomic extensions in the proof of the Chebotarev density theorem and used the same idea to prove the reciprocity law in general.

By far the most difficult part of the Artin reciprocity law to prove is that the kernel of $\varphi_{L/K,\mathfrak{m}}$ for admissible $\mathfrak{m}$ contains $P_{\mathfrak{m}}$: for $(\alpha) \in P_{\mathfrak{m}}$, $\varphi_{L/K,\mathfrak{m}}((\alpha)) = 1$.

Example 6.4. For a squarefree integer d, the Galois group of the extension $\mathbf{Q}(\sqrt{d})/\mathbf{Q}$ has size 2, so it can be (uniquely) identified with $\{\pm 1\}$. By Example 5.8, $4|d|\infty$ is an admissible modulus for $\mathbf{Q}(\sqrt{d})/\mathbf{Q}$. When $p \nmid 4d$, the Artin map $I_{4|d|\infty} \to \mathrm{Gal}(\mathbf{Q}(\sqrt{d})/\mathbf{Q}) \cong \{\pm 1\}$ sends $p\mathbf{Z}$ to $(\frac{d}{p})$, so for $(a, 4d) = 1$ the Artin map sends $a\mathbf{Z}$ to $(\frac{d}{a})$: the Jacobi symbol is a special instance of the Artin map. The Artin reciprocity law in this case says for $a > 0$ with $a \equiv 1 \bmod 4d$ (a sign condition and a congruence condition) that $(\frac{d}{a}) = 1$. This equality is also a consequence of Jacobi reciprocity, and is nearly equivalent to it.

Example 6.5. We will derive the main law of quadratic reciprocity from Artin reciprocity. For an odd prime p, let $p^* = (-1)^{(p-1)/2}p$, so $p^* \equiv 1 \bmod 4$. (The sign on p^* is chosen so 2 doesn't ramify in $\mathbf{Q}(\sqrt{p^*})$.) The Artin map $I_{p\infty} \to \mathrm{Gal}(\mathbf{Q}(\sqrt{p^*})/\mathbf{Q})$ sends any odd prime ideal $(q) \neq (p)$ to $\mathrm{Frob}_q(\mathbf{Q}(\sqrt{p^*})/\mathbf{Q})$. By Example 5.8, the least admissible $\mathbf{Q}$-modulus for $\mathbf{Q}(\sqrt{p^*})/\mathbf{Q}$ has finite part $|\operatorname{disc}(\mathbf{Q}(\sqrt{p^*})/\mathbf{Q})| = |p^*| = p$, 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 $(\mathbf{Z}/p\mathbf{Z})^\times$ and $\mathrm{Gal}(\mathbf{Q}(\sqrt{p*})/\mathbf{Q})$ with $\{\pm 1\}$ makes the Artin map a homomorphism $(\mathbf{Z}/p\mathbf{Z})^\times \to \{\pm 1\}$ with the effect $q \bmod p \mapsto (\frac{p^*}{q})$ for odd (positive) primes $q \neq p$. It's nontrivial since the Artin map is onto. The only homomorphism from $(\mathbf{Z}/p\mathbf{Z})^\times$ onto $\{\pm 1\}$ is the Legendre symbol $(\frac{\cdot}{p})$, so $(\frac{p^*}{q}) = (\frac{q}{p})$. Replacing p^* with $(-1)^{(p-1)/2}p$ and using the formula $(\frac{-1}{q}) = (-1)^{(q-1)/2}$, we get $(-1)^{(p-1)/2 \cdot (q-1)/2}(\frac{p}{q}) = (\frac{q}{p})$.

Remark 6.6. Since only p and (perhaps) ∞ ramify in $\mathbf{Q}(\sqrt{p^*})/\mathbf{Q}$, this extension has admissible modulus $p^r\infty$ for some $r \geq 1$. The Artin map $I_{p^r\infty} \to \mathrm{Gal}(\mathbf{Q}(\sqrt{p^*})/\mathbf{Q})$ is trivial on $P_{p^r\infty}$ by Artin reciprocity, so view it as a surjective homomorphism $(\mathbf{Z}/p^r\mathbf{Z})^\times \to \{\pm 1\}$. The group $(\mathbf{Z}/p^r\mathbf{Z})^\times$ is cyclic, so its only homomorphism onto $\{\pm 1\}$ is $a \bmod p^r \mapsto (\frac{a}{p})$ and the proof ends as before: we do not need to know *a priori* that $r = 1$ is possible.

7. Local Class Field Theory (Hasse)

References: [2], [16]

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 principle". 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–Furtwängler quadratic reciprocity law in number fields.

In 1923/1924, Hasse gave a course on class field theory. At Hilbert's suggestion, the notes for this course developed into a comprehensive report surveying the whole subject as it was known at that time. The first installment of Hasse's *Klassenkörperbericht* appeared in 1926.

This made class field theory much more accessible, but note the year: it was missing the crown jewel of class field theory, Artin's reciprocity law (1927). A second part of Hasse's report came out in 1930, incorporating the reciprocity law and showing how it implies all known power reciprocity laws that had been found up to that time.

One flaw in class field theory as described so far is the tendency to avoid dealing with ramified primes. The groups $I_\mathfrak{m}$ for admissible moduli $\mathfrak{m}$ don't include ramified primes, and Frobenius elements are not well-defined at ramified primes, so there is no way to extend the Artin map to ramified prime ideals. However, the Hilbert-Furtwängler version of quadratic reciprocity with the Hilbert symbol $(a,b)_v$ uses all places, ramified and unramified. Hasse generalized this symbol in his report and obtained a product formula for it. Instead of using a symbol with values that are roots of unity, Hasse's symbol has values in a Galois group.

Definition 7.1. 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.[10]

Write $\mathrm{Gal}(L/K) \cong I_\mathfrak{m}/H_\mathfrak{m}$, with $\mathfrak{m}$ an admissible modulus for L/K. When v is finite, choose $\alpha_0 \in K^\times$ such that α_0 is close to α at v and α_0 is close to 1 at the places in $\mathfrak{m}$ (excluding v if v is in $\mathfrak{m}$):

$$\mathrm{ord}_v\left(\frac{\alpha_0}{\alpha} - 1\right) \geq \mathrm{ord}_v(\mathfrak{m}), \quad \mathrm{ord}_w(\alpha_0 - 1) \geq \mathrm{ord}_w(\mathfrak{m}), \quad u(\alpha_0) > 0,$$

where w runs over finite places in $\mathfrak{m}$ (excluding v) and u runs over real places in $\mathfrak{m}$. If v is not in $\mathfrak{m}$, include the additional condition $((\alpha_0/\alpha), v) = 1$. (For instance, take $\mathrm{ord}_v(\alpha_0/\alpha - 1) \geq 1$.) Factoring the fractional ideal (α_0) into a product of prime ideals, let $\mathfrak{a}$ be its v-free part, so $(\mathfrak{a}, \mathfrak{m}) = 1$ from the conditions on α_0. Define[11]

$$(7.1) \qquad\qquad\qquad (\alpha, L/K)_v = \varphi_{L/K,\mathfrak{m}}(\mathfrak{a})^{-1}.$$

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 $\mathrm{Gal}(L_v/K_v) \subset \mathrm{Gal}(L/K)$. 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 α_0: if β_0 has the same properties as α_0, then $(\alpha_0/\beta_0) \in P_\mathfrak{m}$, so $\varphi_{L/K,\mathfrak{m}}((\alpha_0/\beta_0)) = 1$ 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! (The symbol also has to be shown to be independent of the choice of admissible modulus $\mathfrak{m}$, which is fairly straightfoward to do by comparing the construction at $\mathfrak{m}$ with that at the conductor $\mathfrak{f}_{L/K}$.) 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.

Example 7.2. We compute $(-1, \mathbf{Q}(i)/\mathbf{Q})_v$. (The exponent -1 in (7.1) won't matter here, since values of the symbol are their own inverses.) An admissible modulus for $\mathbf{Q}(i)/\mathbf{Q}$ is 4∞. We identify $\mathrm{Gal}(\mathbf{Q}(i)/\mathbf{Q})$ with $\{\pm 1\}$. Since $-1 < 0$ in $\mathbf{R}$, $(-1, \mathbf{Q}(i)/\mathbf{Q})_\infty = -1$. For $p = 2$, we can use $\alpha_0 = 3$, so $(-1, \mathbf{Q}(i)/\mathbf{Q})_2 = \mathrm{Frob}_3(\mathbf{Q}(i)/\mathbf{Q}) = (\frac{-1}{3}) = -1$. For an odd prime p, we can use $\alpha_0 = 1$, so $(-1, \mathbf{Q}(i)/\mathbf{Q})_p = 1$.

Example 7.3. In a similar way, $(3, \mathbf{Q}(i)/\mathbf{Q})_v = -1$ at $v = 2$ and $v = 3$, and $(3, \mathbf{Q}(i)/\mathbf{Q})_v = 1$ at other v (including $v = \infty$).

---

[10]This procedure generalizes an approach of Hilbert to define Hilbert symbols at ramified places. See [20].

[11]Hasse's definition of $(\alpha, L/K)_v$ did not have the exponent -1. We include it to fit normalizations that show up later.

Example 7.4. Pick a prime $\mathfrak{p}$ not dividing an admissible modulus $\mathfrak{m}$ for L/K. For $\alpha \in K^\times$, let $k = \mathrm{ord}_\mathfrak{p}(\alpha)$. Choose α_0 so that $\mathrm{ord}_w(\alpha_0 - 1) \geq \mathrm{ord}_w(\mathfrak{m})$ for all $w|\mathfrak{m}_f$, $w(\alpha_0) > 0$ for all $w|\mathfrak{m}_\infty$, and $\mathrm{ord}_\mathfrak{p}(\alpha_0/\alpha - 1) \geq 1$. Then $(\alpha_0) = \mathfrak{p}^k \mathfrak{a}$ where $\mathfrak{a}$ is relatively prime to $\mathfrak{p}$ and to $\mathfrak{m}$. Then $(\alpha, L/K)_\mathfrak{p} = \varphi_{L/K,\mathfrak{m}}(\mathfrak{a})^{-1} = \varphi_{L/K,\mathfrak{m}}((\alpha_0)\mathfrak{p}^{-k})^{-1}$. By Artin reciprocity, (α_0) is in the kernel of the Artin map, so

$$(\alpha, L/K)_\mathfrak{p} = \varphi_{L/K,\mathfrak{m}}(\mathfrak{p})^k = \mathrm{Frob}_\mathfrak{p}(L/K)^{\mathrm{ord}_\mathfrak{p}(\alpha)}.$$

That the exponent on the right is $\mathrm{ord}_\mathfrak{p}(\alpha)$ rather than $-\mathrm{ord}_\mathfrak{p}(\alpha)$ 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 $\mathrm{ord}_\mathfrak{p}(\alpha) = 0$ for all but finitely many $\mathfrak{p}$.

Theorem 7.5 (Hasse, 1930)**.** *For any finite abelian extension of number fields L/K and $\alpha \in K^\times$, $\prod_v (\alpha, L/K)_v = 1$.*

Just as Hasse's definition of $(\alpha, L/K)_v$ depended on the Artin reciprocity law, so too his proof of Theorem 7.5 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 (that is, on the completion of K at v and of L at any place over v), despite its roundabout global definition in terms of the Artin map at an ideal in K that is relatively prime to v. For example, $(\alpha, L/K)_v$ lies in the common decomposition group $D(w|v)$ for all places $w|v$ on L, and this decomposition group is naturally identified with the Galois group of completions $\mathrm{Gal}(L_w/K_v)$. (The definition we gave for $(\alpha, L/K)_v$ for infinite v is directly in terms of the completion at v and it is the generator of the decomposition group $\mathrm{Gal}(L_w/K_v)$ as a subgroup of $\mathrm{Gal}(L/K)$.) 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 F. K. 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's 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. (Every local field of characteristic 0 contains a dense number field, so such K and v exist, in many ways in fact.) Takagi's class field theory implies there is an abelian extension L/K such that $E = LK_v$. (It is generally *not* true that one can arrange for $[L : K] = [E : F]$, even when E/F is cyclic. The Grunwald-Wang theorem describes when it is possible.) For $\alpha \in K^\times$, the symbol $(\alpha, L/K)_v$ belongs to $D(w|v)$, 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 $\mathrm{Gal}(E/F)$ corresponding to $(\alpha, L/K)_v$. So we have a function $K^\times \to \mathrm{Gal}(E/F)$ by $\alpha \mapsto (\alpha, E/F)$. 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 $(-, E/F)\colon F^\times \to \mathrm{Gal}(E/F)$ called the *local Artin map*. In particular, if E/F is unramified and π is a prime in F then Example 7.4 implies $(\pi, E/F)$ is the local Frobenius element in $\mathrm{Gal}(E/F)$ (just like the global Artin map associates to an unramified prime ideal its Frobenius element). 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 is 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 $\mathrm{N}_{E/F}(E^\times) \subset F^\times$. This is a local analogue

of $\mathrm{N}_{\mathfrak{m}}(L/K)$ 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 7.6. *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 $\mathrm{N}_{E/F}(E^{\times})$, so $F^{\times}/\mathrm{N}_{E/F}(E^{\times}) \cong \mathrm{Gal}(E/F)$. Associating to E the group $\mathrm{N}_{E/F}(E^{\times})$ 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

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

Then $f(E/F) = \frac{[E:F]}{e(E/F)} = [F^{\times} : \mathcal{O}_F^{\times} \mathrm{N}_{E/F}(E^{\times})]$ is the order of π in $F^{\times}/\mathcal{O}_F^{\times} \mathrm{N}_{E/F}(E^{\times})$ for any prime π of F.

When E/F is not abelian, $[F^{\times} : \mathrm{N}_{E/F}(E^{\times})] < [E : F]$.

If $H \subset F^{\times}$ is a subgroup of finite index, call E the *class field* to H over F when $\mathrm{N}_{E/F}(E^{\times}) = H$. Theorem 7.6 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 groups $P_{\mathfrak{m}}$. 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 $P_{\mathfrak{m}}$ (by definition) and every subgroup of $F^{\times}$ with finite index, say d, contains all dth powers and thus contains some U_n by Hensel's lemma.[12] 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 $U_n \subset \mathrm{N}_{E/F}(E^{\times})$ 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 $\mathcal{O}_F$ if 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 5.7) has a local analogue:

Theorem 7.7. *Let E/F be an abelian extension of local fields with characteristic 0. For a character χ of $\mathrm{Gal}(E/F)$, let $\mathfrak{f}_\chi$ be the conductor of the class field to $\ker \chi$. Then $\mathrm{disc}(E/F) = \prod_\chi \mathfrak{f}_\chi$, where the product runs over all characters of $\mathrm{Gal}(E/F)$.*

This theorem from local class field theory helps to compute the conductor in global class field theory. For an abelian extension of number fields L/K, its conductor can be computed locally: for a prime $\mathfrak{p}$ of K and $\mathfrak{P}|\mathfrak{p}$ in L, choose the least $n_{\mathfrak{p}} \geq 0$ such that $1 + \pi_{\mathfrak{p}}^{n_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}} \subset \mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(L_{\mathfrak{P}}^{\times})$. The finite part of $\mathfrak{f}_{L/K}$ is $\prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$. (The infinite part is the product of the real places of K that extend to complex places of L.) So a K-modulus $\mathfrak{m}$ is admissible for an abelian extension L/K when, for each prime power $\mathfrak{p}^{e_{\mathfrak{p}}}$ fully dividing $\mathfrak{m}$, $1 + \pi_{\mathfrak{p}}^{e_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}} \subset \mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(L_{\mathfrak{P}}^{\times})$ and $\mathfrak{m}$ is divisible by all real places of K that ramify in L.

Example 7.8. In Example 5.4, we showed 4∞ is the conductor of $\mathbf{Q}(i)/\mathbf{Q}$ by a global argument using norms. Now we will check 4∞ is the conductor of $\mathbf{Q}(i)/\mathbf{Q}$ by local arguments at each place. Since only 2 and ∞ ramify in $\mathbf{Q}(i)$, the least admissible modulus is $2^r\infty$ for some $r \geq 1$. The least value of r is the least $r \geq 1$ such that $1 + 2^r\mathbf{Z}_2 \subset \mathrm{N}_{\mathbf{Q}_2(i)/\mathbf{Q}_2}(\mathbf{Q}_2(i)^{\times})$. This norm group is the group of nonzero sums of two squares in $\mathbf{Q}_2^{\times}$. Since -1 is not a sum of two squares in $\mathbf{Q}_2$, $r \neq 1$. Any $x \equiv 1 \bmod 4\mathbf{Z}_2$ satisfies $x \equiv 1 \bmod 8\mathbf{Z}_2$ or $x \equiv 5 \bmod 8\mathbf{Z}_2$.

---

[12]This step uses characteristic 0. The pth powers in a characteristic p local field don't contain a neighborhood of 1. The relevant subgroups of $F^{\times}$ for local class field theory in all characteristics are the open subgroups of finite index, but openness follows from finite index in characteristic 0.

In the first case x is a 2-adic square, so also a sum of two squares. In the second case, $x/5$ is a 2-adic square, so x is a sum of two squares since 5 is. Therefore we can use $r = 2$.

Since finite abelian extensions of a local field F of characteristic 0 correspond to finite-index subgroups of $F^\times = \pi^{\mathbf{Z}} \times \mathcal{O}_F^\times \cong \mathbf{Z} \times \mathcal{O}_F^\times$, $\mathrm{Gal}(F^{ab}/F)$ is the profinite completion of $F^\times \cong \mathbf{Z} \times \mathcal{O}_F^\times$, which is $\widehat{\mathbf{Z}} \times \mathcal{O}_F^\times$.

Example 7.9. Taking $F = \mathbf{Q}_p$, the local Kronecker–Weber theorem says every finite abelian extension of $\mathbf{Q}_p$ is inside a cyclotomic extension of $\mathbf{Q}_p$:

$$\mathbf{Q}_p^{ab} = \bigcup_{n \geq 1} \mathbf{Q}_p(\mu_n) = \bigcup_{(n,p)=1} \mathbf{Q}_p(\mu_n) \cdot \bigcup_{r \geq 1} \mathbf{Q}_p(\mu_{p^r}),$$

where the first union is the maximal unramified extension of $\mathbf{Q}_p$, whose Galois group over $\mathbf{Q}_p$ is isomorphic to $\widehat{\mathbf{Z}}$. The second union has Galois group $\mathbf{Z}_p^\times$ over $\mathbf{Q}_p$. Therefore $\mathrm{Gal}(\mathbf{Q}_p^{ab}/\mathbf{Q}_p) \cong \widehat{\mathbf{Z}} \times \mathbf{Z}_p^\times$, which agrees with local class field theory.

E. Noether insisted that there should be a self-contained derivation of local class field theory, and global class field theory should be derived from local class field theory. F. K. Schmidt (1930) 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 (Example 7.4). 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 definition of a cyclic algebra goes back to Dickson (1906) and generalizes the construction of Hamilton's quaternions $\mathbf{H}$. Note that

$$
\begin{aligned}
\mathbf{H} &= \mathbf{R} + \mathbf{R}i + \mathbf{R}j + \mathbf{R}k \\
&= (\mathbf{R} + \mathbf{R}i) + (\mathbf{R} + \mathbf{R}i)j \\
&= \mathbf{C} + \mathbf{C}j,
\end{aligned}
$$

with $j^2 = -1$ and $jz = \overline{z}j$. These rules tells us how to multiply two quaternions when written in the form $z + wj$ for complex numbers z and w. The structure here involves complex conjugation, acting as an element of $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$. Dickson replaced $\mathbf{C}/\mathbf{R}$ with any cyclic extension.

Definition 7.10 (Dickson)**.** Let L/K be a cyclic extension of fields with degree n, $\alpha \in K^\times$, and let σ be a generator of $\mathrm{Gal}(L/K)$. The direct sum

$$L \oplus Lx \oplus Lx^2 \oplus \cdots \oplus Lx^{n-1},$$

where

- $x^n = \alpha$,
- $x\gamma = \sigma(\gamma)x$ for all $\gamma \in L$,

is called a *cyclic algebra* over K.

Here K can be any field, not just a number field, there is no obvious link between cyclic algebras and class field theory. Dickson called these "algebras of type D," but the hint didn't have a long-term influence (unlike Banach's "espaces du type (B)".) They are no longer called Dickson algebras.

Example 7.11. The quaternions are $(\mathbf{C}/\mathbf{R}, c, -1)$, and $(\mathbf{C}/\mathbf{R}, c, 1) \cong \mathrm{M}_2(\mathbf{R})$.

Example 7.12. The quaternions with rational coefficients equal $(\mathbf{Q}(i)/\mathbf{Q}, c, -1)$. They are also $(\mathbf{Q}(\sqrt{-5})/\mathbf{Q}, c, -6)$, which is not obvious! The same cyclic algebra arising from different cyclic extensions is like different polynomials having the same splitting field.

Theorem 7.13. *With notation as above,*

(1) $(L/K, \sigma, \alpha)$ *has center* K, K*-dimension* n^2, *and is a simple* K*-algebra (no 2-sided ideals besides* (0) *and* (1)*),*
(2) $(L/K, \sigma, 1) \cong \mathrm{M}_n(K)$ *as* K*-algebras,*
(3) $(L/K, \sigma, \alpha) \cong (L/K, \sigma, \beta)$ *as* K*-algebras if and only if* $\alpha/\beta \in \mathrm{N}_{L/K}(L^\times)$,
(4) *for* $(t, n) = 1$, $(L/K, \sigma^t, \alpha) \cong (L/K, \sigma, \alpha^u)$, *where* $tu \equiv 1 \bmod n$.

Theorem 7.13(3) resembles the equivalence $(\alpha, E/F) = (\beta, E/F) \Longleftrightarrow \alpha/\beta \in \mathrm{N}_{E/F}(E^\times)$ in local class field theory. This suggests (but does not say how!) that cyclic algebras could be a route to a purely local definition of the local Artin symbol $(\alpha, E/F)$, and that is exactly what happened. We need to know what the cyclic algebras over a local field look like. Hasse showed they can always be put into a standard form using *unramified* extensions.

Theorem 7.14 (Hasse, 1931). *Every cyclic algebra over a local field* F *of characteristic* 0 *with* F*-dimension* n^2 *is a cyclic algebra of the form*

$$(F_n/F, \mathrm{Frob}, \pi^a),$$

where F_n *is the unramified extension of* F *with degree* n, Frob *is the canonical generator of* $\mathrm{Gal}(F_n/F)$, π *is a prime in* F, *and* $a \in \mathbf{Z}$.

The norm subgroup $\mathrm{N}_{F_n/F}(F_n^\times)$ from the unramified extension of degree n is $\pi^{n\mathbf{Z}} \times \mathcal{O}_F^\times$, so Theorem 7.13(3) tells us two things:

(1) $(F_n/F, \mathrm{Frob}, \pi^a) \cong (F_n/F, \mathrm{Frob}, \pi^b)$ as F-algebras if and only if $a \equiv b \bmod n$,
(2) $(F_n/F, \mathrm{Frob}, \pi^a)$ is independent of π,

Therefore the class $a \bmod n$ is a well-defined invariant of the F-algebra $(F_n/F, \mathrm{Frob}, \pi^a)$. By Theorem 7.13, this invariant is $0 \bmod n$ precisely when the algebra is isomorphic to $\mathrm{M}_n(F)$.

Now we can give a local definition of $(\alpha, E/F)$, first for cyclic E/F and then for abelian E/F. Let $n = [E : F]$, with F a local field of characteristic 0. For $\alpha \in F^\times$ and σ a generator of $\mathrm{Gal}(E/F)$, consider the cyclic algebra

$$A = (E/F, \sigma, \alpha).$$

Let the invariant of A be $a \bmod n$. If we change σ, we usually get a new (that is, non-isomorphic) cyclic algebra, so a will usually change too. Although A depends on the choice of generator σ of $\mathrm{Gal}(E/F)$, the power

$$\sigma^a \in \mathrm{Gal}(E/F)$$

is independent of σ, and is the local Artin symbol defined before: $(\alpha, E/F) = \sigma^a$.[13] If E/F is abelian rather than cyclic, write $E = E_1 \cdots E_r$ with cyclic E_i/F. Then $\mathrm{Gal}(E/F)$ embeds

---

[13]If the definition of a cyclic algebra had $\gamma x = x\sigma(\gamma)$ instead of $x\gamma = \sigma(\gamma)x$ then $(\alpha, E/F) = \sigma^{-a}$.

into $\prod_i \mathrm{Gal}(E_i/F)$, with the image being the sequences which agree on the overlaps $E_i \cap E_j$. For $\alpha \in F^\times$, the symbols $(\alpha, E_i/F)$ agree on the overlaps $E_i \cap E_j$, so they come by restriction from a single element of $\mathrm{Gal}(E/F)$, and this is precisely the local Artin symbol $(\alpha, E/F)$ defined before. By proving *ab ovo* that this construction of $(\alpha, E/F)$ is independent of the choice of cyclic subextensions E_i/F, local class field theory can be developed without global class field theory.

Like Takagi in the global case, this approach to local class field theory does not give an explicit construction of class fields over local fields, but such a construction was achieved later (1965) by Lubin and Tate using formal groups.

We now turn to the case of number fields and get a definition of Hasse's $(\alpha, L/K)_v$ for finite v without recourse to the global Artin map. (For infinite v we already presented a direct local definition of $(\alpha, L/K)_v$.) Let L/K be a cyclic extension of number fields, with degree n. Pick a generator σ of $\mathrm{Gal}(L/K)$. For any $\alpha \in K^\times$, $A := (L/K, \sigma, \alpha)$ is a cyclic K-algebra. When v is a finite place of K, the tensor product $K_v \otimes_K A$ is a cyclic K_v-algebra with K_v-dimension n^2.[14] Let it have invariant $a_v \bmod n$. Then $(\alpha, L/K)_v = \sigma^{a_v}$. The definition of $(\alpha, L/K)_v$ for abelian L/K proceeds as in the local case by writing L as a composite of cyclic extensions of K.

Example 7.15. Consider $\mathbf{Q}(i)/\mathbf{Q}$ with Galois group $\{1, c\} \cong \{\pm 1\}$. We want to compute $(-1, \mathbf{Q}(i)/\mathbf{Q})_v$ using the new definition of these symbols. (They were computed before in Example 7.2 with Hasse's original definition.)

Here $n = [\mathbf{Q}(i) : \mathbf{Q}] = 2$ and our only choice for σ is $c = -1$. The cyclic algebra $(\mathbf{Q}(i)/\mathbf{Q}, c, -1)$ is the rational quaternions $\mathbf{H}(\mathbf{Q})$, and $\mathbf{Q}_v \otimes_\mathbf{Q} \mathbf{H}(\mathbf{Q}) \cong \mathbf{H}(\mathbf{Q}_v)$.[15] When $v = \infty$, $\mathbf{H}(\mathbf{Q}_v) = \mathbf{H}(\mathbf{R})$ is the real quaternions, whose invariant is $1 \bmod 2$, so $(-1, \mathbf{Q}(i)/\mathbf{Q})_\infty = c^1 = c = -1$. The 2-adic quaternions are $\mathbf{H}(\mathbf{Q}_2) = (\mathbf{Q}_2(i)/\mathbf{Q}_2, c, -1)$, but this is *not* in the normalized form of Theorem 7.14 for two reasons: $\mathbf{Q}_2(i)/\mathbf{Q}_2$ is ramified and the parameter -1 is not an integral power of 2. It turns out that $\mathbf{H}(\mathbf{Q}_2) \cong (\mathbf{Q}_2(\sqrt{-3})/\mathbf{Q}_2, c, 2)$, which is in standard form, so $a_2 \equiv 1 \bmod 2$. Therefore $(-1, \mathbf{Q}(i)/\mathbf{Q})_2 = c^{a_2} = c = -1$.

For odd primes p, $-1 = x^2 + y^2$ for some x and y in $\mathbf{Q}_p$ (since $-1 \equiv x^2 + y^2 \bmod p$ is solvable and we can lift to a p-adic solution with Hensel's Lemma). Therefore[16] $\mathbf{H}(\mathbf{Q}_p) \cong \mathrm{M}_2(\mathbf{Q}_p)$, whose invariant is $0 \bmod 2$, so $(-1, \mathbf{Q}(i)/\mathbf{Q})_p = 1$.

Armed with the new local definition of $(\alpha, L/K)_v$, Hasse (1933) proved Theorem 7.5 without global class field theory and could derive the Artin reciprocity law from Theorem 7.5. Since Hasse originally used the Artin reciprocity law to prove Theorem 7.5, Theorem 7.5 is equivalent[17] to the Artin reciprocity law. But unlike the Artin reciprocity law, all the places of K occur in Theorem 7.5, so we are getting closer to a more balanced formulation of the reciprocity law.

---

[14] The base extension of a cyclic algebra to a larger base field might not be a cyclic algebra according to the definition we gave, *e.g.*, $\mathbf{C} \otimes_\mathbf{R} \mathbf{H} \cong \mathrm{M}_2(\mathbf{C})$ apparently isn't a cyclic $\mathbf{C}$-algebra since $\mathbf{C}$ doesn't have a quadratic field extension with which to create a $\mathbf{C}$-algebra of dimension 4. In the definition of a cyclic algebra $(L/K, \sigma, \alpha)$, we could relax the hypothesis that L/K is a cyclic *field* extension to L being a separable K-algebra of dimension n admitting a K-automorphism σ of order n whose fixed set is K. Then, for instance, $\mathrm{M}_n(K) \cong (K^n/K, \sigma, 1)$ where σ is the cyclic shift of the coordinates of K^n. This makes $\mathrm{M}_n(K)$ a cyclic algebra over K whether or not K has a degree n cyclic field extension and the base extension of a cyclic algebra is a cyclic algebra.

[15] For a field K, let $\mathbf{H}(K) = K + Ki + Kj + Kk$ with the usual rules of multiplication on the basis.

[16] For any field K of characteristic not 2, $\mathbf{H}(K) \cong \mathrm{M}_2(K)$ if and only if -1 is a sum of two squares in K.

[17] Proving Theorem 7.5 without class field theory is hard, since it is the Artin reciprocity law in disguise.

The mathematical structure underlying cyclic algebras (and more general crossed product algebras, which are the analogue of cyclic algebras using general Galois extensions in place of cyclic extensions) is group cohomology. After World War II, developments in class field theory led to the stripping away of the algebras (which after all were defined entirely in terms of the number fields themselves) in proofs of class field theory as far as possible, leaving behind only cohomological formalism. This is how cohomology entered local and global class field theory in the period 1950–1952 in work of Hochschild, Nakayama, Weil, Artin, and Tate.

8. Idelic Class Field Theory (Chevalley)

Reference: [8]

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 which 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 for infinite extensions, but several years later he used ideles in a new way to get global class field theory from local class field theory.

Let's see why the classical description of the Artin map, in terms of ideals, is not well-suited to describe infinite abelian extensions of a number field. When $K \subset L \subset L'$ is a tower of finite abelian extensions of K, and a K-modulus $\mathfrak{m}$ is admissible for L' (and thus also for L), the diagram

(8.1)

$$
\begin{array}{ccc}
 & & \mathrm{Gal}(L'/K) \\
 & \overset{\varphi_{L'/K,\mathfrak{m}}}{\nearrow} & \Big\downarrow \text{res.} \\
I_{\mathfrak{m}} & & \\
 & \underset{\varphi_{L/K,\mathfrak{m}}}{\searrow} & \\
 & & \mathrm{Gal}(L/K)
\end{array}
$$

commutes. But as L' grows, the domain $I_{\mathfrak{m}}$ of the Artin map has to change since the modulus needs to become more highly divisible by primes to keep up with the ensuing ramification. (This resembles the slightly annoying feature of Takagi's comparison theorem: ideal groups must be defined to the same K-modulus.) We want to replace $I_{\mathfrak{m}}$ with an object that doesn't involve a modulus, so the behavior of (8.1) as L' grows is cleaner.

Definition 8.1 (Chevalley, 1936). The *idele group* J_K of a number field K 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 J_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 ($x_v = 1$ for all but finitely many v) and the direct product of the $K_v^\times$'s ($x_v \in K_v^\times$ with no constraints). We embed $K^\times \hookrightarrow J_K$ diagonally, the image being called the *principal ideles* (analogue of principal ideals). We also embed $K_v^\times \hookrightarrow J_K$ singly (on the v-coordinate, with 1's elsewhere).

To each idele $\mathbf{x} \in J_K$ we have a fractional ideal

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

where the right side is a finite product since $x_v \in \mathcal{O}_v^\times$ for all but finitely many v. The image of a principal idele is the principal ideal of the same element of $K^\times$.

Using this passage from ideles to ideals, any generalized ideal class group of K can be realized as a quotient group of J_K as follows. Pick a K-modulus $\mathfrak{m}$. Starting with an idele $\mathbf{x} \in J_K$, pick $\alpha_0 \in K^\times$ (by the approximation theorem) so that for v in $\mathfrak{m}$ we have

$$\mathrm{ord}_v(x_v/\alpha_0 - 1) \geq \mathrm{ord}_v(\mathfrak{m})$$

when $v|\mathfrak{m}_f$, and

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

when $v|\mathfrak{m}_\infty$. (This is the analogue of Hasse's choice of auxiliary α_0 in the definition of the symbol $(\alpha, L/K)_v$.) The idele $\mathbf{x}/\alpha_0 = (\dots, x_v/\alpha_0, \dots)$ has corresponding ideal $\iota(\mathbf{x}/\alpha_0)$ in $I_\mathfrak{m}$. If $\beta_0 \in K^\times$ has the same properties as α_0 then the ideals $\iota(\mathbf{x}/\alpha_0)$ and $\iota(\mathbf{x}/\beta_0)$ differ by the principal ideal (β_0/α_0), which lies in $P_\mathfrak{m}$, so $\iota(\mathbf{x}/\alpha_0)$ is well-defined in terms of $\mathbf{x}$ as an element of $I_\mathfrak{m}/P_\mathfrak{m}$. Sending $\mathbf{x}$ to $\iota(\mathbf{x}/\alpha_0)$ is a homomorphism from J_K onto $I_\mathfrak{m}/P_\mathfrak{m}$. If $\mathbf{x} = (\alpha, \alpha, \dots)$ is a principal idele, we can use $\alpha_0 = \alpha$, so the image is 1, which means the map $J_K \to I_\mathfrak{m}/P_\mathfrak{m}$ kills all principal ideles. Therefore all generalized ideal class groups of K can be viewed as quotients of the single group J_K, or even of $J_K/K^\times$.

As an indication of the simplicity coming from this viewpoint, let's 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 J_K containing $K^\times$: take the inverse image of $H/P_\mathfrak{m}$ under the map $J_K \to I_\mathfrak{m}/P_\mathfrak{m}$. Two ideal groups H and H' are equivalent (meaning $H \cap I_{\mathfrak{m}''} = H' \cap I_{\mathfrak{m}''}$ 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 K-modulus for this extension, the composite map

$$\varphi_{L/K} \colon J_K \longrightarrow I_\mathfrak{m}/P_\mathfrak{m} \xrightarrow{\varphi_{L/K,\mathfrak{m}}} \mathrm{Gal}(L/K)$$

is a surjective homomorphism and (by properties of the Artin map $\varphi_{L/K,\mathfrak{m}}$) is *independent* of the choice of admissible $\mathfrak{m}$. This composite map is the *idelic Artin map*, and $\varphi_{L/K}(K^\times) = 1$ from the construction. To describe the full kernel of the idelic Artin map, norms on ideles are needed. Define $\mathrm{N}_{L/K} \colon J_L \to J_K$ by $\mathrm{N}_{L/K}(\mathbf{y}) = \mathbf{x}$ where $x_v = \prod_{w|v} \mathrm{N}_{L_w/K_v}(y_w)$ for all places v of K. The kernel of $\varphi_{L/K}$ is $K^\times \mathrm{N}_{L/K}(J_L)$, which is the idelic counterpart to $P_\mathfrak{m} \mathrm{N}_\mathfrak{m}(L/K)$.

To formulate class field theory as a one-to-one correspondence using ideles, we need a topology on J_K. The topology Chevalley put on J_K was not Hausdorff (*e.g.*, the closure of 1 was the connected component of J_K.) It was later replaced by the restricted product topology, where a basic open neighborhood of 1 in J_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. (The product topology would have $U_v = K_v^\times$ for all but finitely many v.) With this topology, J_K is a locally compact topological group. (Using the product topology, J_K is *not* locally compact, which is why the product topology is not the right choice.)

Theorem 8.2. *For an abelian extension of number fields L/K, the idelic Artin map $\mathbf{x} \mapsto \varphi_{L/K}(\mathbf{x})$ is a homomorphism from J_K onto $\mathrm{Gal}(L/K)$ with kernel $K^\times \mathrm{N}_{L/K}(J_L)$, so $J_K/K^\times \mathrm{N}_{L/K}(J_L) \cong \mathrm{Gal}(L/K)$. Associating to L the group $K^\times \mathrm{N}_{L/K}(J_L)$ gives a one-to-one inclusion-reversing correspondence between finite abelian extensions of K and open subgroups of finite index in J_K which contain $K^\times$.*

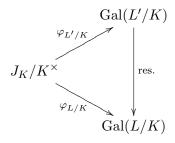*For a place v of K, the composite*

$$L_w^\times \xrightarrow{\;\mathrm{N}_{L_w/K_v}\;} K_v^\times \xrightarrow{\hspace{2cm}} J_K \xrightarrow{\;\varphi_{L/K}\;} \mathrm{Gal}(L/K)$$

has image the decomposition group $D(w|v)$ and the image of $\mathcal{O}_w^\times$ is the inertia group $I(w|v)$.

If we work with subgroups of $J_K/K^\times$, rather than subgroups of J_K containing $K^\times$, then we can say that the finite abelian extensions of K correspond in a one-to-one manner with "norm subgroups" of $J_K/K^\times$. The isomorphism $J_K/K^\times \mathrm{N}_{L/K}(J_L) \cong \mathrm{Gal}(L/K)$ is analogous to $I_{\mathfrak{m}}/P_{\mathfrak{m}} \mathrm{N}_{\mathfrak{m}}(L/K) \cong \mathrm{Gal}(L/K)$.

The idelic class field theory still has a hidden flaw: while the idelic Artin map $\varphi_{L/K}$ is independent of the admissible modulus used in its construction, we nevertheless are using an admissible modulus to define it, so a proof of Theorem 8.2 has to fall back on the ideal-theoretic global class field theory. We will see how this flaw gets sorted out below. But first we use the idelic viewpoint to get a workable substitute for (8.1) that lets us pass to infinite abelian extensions.

When $K \subset L \subset L'$ 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

$$
\begin{array}{ccc}
 & & \mathrm{Gal}(L'/K) \\
 & \overset{\varphi_{L'/K}}{\nearrow} & \big| \\
J_K/K^\times & & \big| \;\mathrm{res.} \\
 & \underset{\varphi_{L/K}}{\searrow} & \big\downarrow \\
 & & \mathrm{Gal}(L/K)
\end{array}
$$

commutes and can be used in place of (8.1): the source group $J_K/K^\times$ does not change as L' grows, so we can pass to an inverse limit compatibly to get a homomorphism

$$(-, K)\colon J_K/K^\times \to \mathrm{Gal}(K^{ab}/K)$$

mapping to the Galois group of the maximal abelian extension of K. Since the map is onto at finite levels, it has dense image. Using a compactness theorem, this homomorphism is surjective and its kernel is equal to the connected component of the identity in $J_K/K^\times$. So $\mathrm{Gal}(K^{ab}/K)$ is the largest totally disconnected quotient group of $J_K/K^\times$.[18]

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.

---

[18]From the viewpoint of infinite Galois theory, $\mathrm{Gal}(K^{ab}/K)$ is the inverse limit of the ideal groups $I_{\mathfrak{m}}/P_{\mathfrak{m}}$, partially ordered by reverse divisibility of the K-moduli $\mathfrak{m}$. Weber's equivalence relation on ideal groups, when using Takagi's K-moduli and not just ideals, says ideal groups are equivalent when they correspond to the same subgroup of the inverse limit.

Theorem 8.3. *For a finite abelian extension of number fields L/K and $\mathbf{x} \in J_K$,*

$$(8.2) \qquad\qquad \varphi_{L/K}(\mathbf{x}) = \prod_v (x_v, L_w/K_v),$$

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

On the right side of (8.2), 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 $\mathcal{O}_v^{\times} \subset \mathrm{N}_{L_w/K_v}(L_w^{\times})$ for unramified v. The hard step in the proof of (8.2) is showing the right side is trivial on $K^{\times}$. This is *exactly* Hasse's old product formula (Theorem 7.5), 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 any easier, or change what the hard step is, but the formalism surrounding the difficulties is much more elegant. Reproving Theorem 8.2 by using the right side of (8.2) as a new definition of the idelic Artin map lets global class field theory be derived from local class field theory.

The two classical inequalities (5.1) and (5.2) are still important in the idelic development of class field theory. The idelic version of (5.1) says $[J_K : K^{\times} \mathrm{N}_{L/K}(J_L)] \leq [L : K]$ for any finite extension L/K, while the idelic version of (5.2) says $[J_K : K^{\times} \mathrm{N}_{L/K}(J_L)] \geq [L : K]$ when L/K is abelian (and the inequality is false if L/K is not abelian). The original proof of (5.1) used Weber L-functions, so complex analysis was needed. In 1940, Chevalley found a purely algebraic proof of (5.1) in its idelic form. His argument used Pontryagin duality on $J_K/K^{\times}$ to derive (5.2) in its idelic form without L-functions and using this he could prove (5.1) in its idelic form for abelian extensions. Because of the new logical dependencies, with (5.2) being used to prove (5.1), the order of appearance of the two inequalities in the development of class field theory had to be reversed, which led to a name change. From 1920 to 1940, (5.1) was called the first inequality of class field theory and (5.2) was called the second inequality of class field theory. After 1940, (5.1) was called the second inequality and (5.2) was called the first inequality.

9. FUNCTION FIELDS

References: [15], [18]

The development of arithmetic in function fields over finite fields, beyond $\mathbf{F}_q(x)$, began with Artin's 1921 thesis, which explored the arithmetic of quadratic extensions of $\mathbf{F}_q(x)$ and their zeta-functions for odd q. (The thesis itself only treated the case when $q = p$ is prime, but Artin recognized that with no essential changes any finite constant field can be used.) Artin used these quadratic extensions to prove a quadratic reciprocity law for $\mathbf{F}_q(x)$ in odd characteristic, adapting an argument of Kummer for the classical quadratic reciprocity law that used parity properties of class numbers of quadratic fields. In 1925, F. K. Schmidt began the development of arithmetic in a general finite extension of $\mathbf{F}_q(x)$, including an (easy) n-th power reciprocity law when the constant field of the extension contains the nth roots of unity. Later Schmidt (1931) sketched a partial development of class field theory for function fields in characteristic p when the degrees of the extensions are not divisible by p, following closely the ideas of Takagi. However, Schmidt was not able to treat the existence theorem as Takagi had done for number fields.

In 1934, Hasse proved the Artin reciprocity law[19] in the function field case, using cyclic algebras, as he had done a year before in the number field case. Theorem 7.14 is true for characteristic p local fields by the same argument as for characteristic 0 local fields, leading to a local class field theory in characteristic p. Its theorems are identical to the characteristic 0 local class field theory, except one needs to be explicit about using *open* subgroups of finite index. Hasse's product formula (Theorem 7.5) is true in the function field case, where it turns out to be a consequence of the residue theorem for function fields. In 1935, Witt proved the existence theorem (for the first time) when the field degree is divisible by p. This completed the basic statements of class field theory for function fields.

Chevalley's idelic viewpoint makes sense for both number fields and function fields, so permits a simultaneous development of both cases. However, a dichotomy between the two cases occurs in class field theory for *infinite* abelian extensions. For a function field K, as for a number field, the idelic Artin map $J_K/K^{\times} \to \mathrm{Gal}(K^{ab}/K)$ has a dense image, but now the map is injective rather than surjective. Its image can be characterized as the elements of $\mathrm{Gal}(K^{ab}/K)$ which, on the algebraic closure of the constant field of K, are integral powers of the Frobenius automorphism.

In the 1950s, Lang developed class field theory for function fields over a finite field using algebraic geometry, at first for unramified abelian extensions and then for ramified abelian extensions. He proved an analogue of Artin's reciprocity isomorphism geometrically without the intervention of inequalities like (5.1) and (5.2). Lang used Rosenlicht's generalized Jacobian varieties (an analogue of Weber's generalized ideal class groups) to show the abelian extensions he described geometrically, together with constant field extensions, account for all finite abelian extensions in the function field case.

These approaches to class field theory over a function field do not give explicit class fields that are cofinal in all finite abelian extensions, which would be analogous to the cyclotomic fields over $\mathbf{Q}$ (Kronecker–Weber theorem). Even in the number field case, the explicit construction of class fields is a very hard problem, except over $\mathbf{Q}$ and imaginary quadratic fields. Hayes (1974), building on work of Carlitz (1938), constructed an explicit class field theory over rational function fields. That is, Hayes wrote down a collection of explicit finite abelian extensions of $\mathbf{F}_q(x)$ such that any finite abelian extension of $\mathbf{F}_q(x)$ is inside one of these fields.[20] Drinfeld (1974) used Drinfeld modules (called "elliptic modules" by him, from the analogy with complex multiplication on elliptic curves) to achieve the same goal for any function field in one variable over a finite field, not just the rational function field. Roughly, what makes the function field case different from the number field case from the viewpoint of explicit class field theory is that in characteristic p there are far more additive functions.

References

[1] G. Frei, *Heinrich Weber and the Emergence of Class Field Theory*, in "The History of Modern Mathematics, vol. 1: Ideas and their Reception," (J. McCleary and D. E. Rowe, ed.) Academic Press, Boston, 1989, 424–450.

[2] G. Frei, *How Hasse was led to the Theory of Quadratic Forms, the Local-Global Principle, the Theory of the Norm Residue Symbol, the Reciprocity Laws, and to Class Field Theory*, in "Class Field Theory – its Centenary and Prospect," Math. Soc. Japan, Tokyo, 2001, 31–62.

[3] H. Hasse, *History of Class Field Theory*, in "Algebraic Number Theory," J. W. S. Cassels and A. Fröhlich (ed.), Academic Press, New York, 1967, 266–279.

---

[19]Hasse only treated the reciprocity law for cyclic extensions, which is the main case.

[20]To verify his explicit class field theory worked, Hayes used the abstract class field theory.

[4] H. Hasse, "Class Field Theory," Lecture Notes # 11, Dept. Math. Univ. Laval, Quebec, 1973.

[5] K. Iwasawa, *On papers of Takagi in Number Theory*, in "Teiji Takagi Collected Papers," 2nd ed., Springer-Verlag, Tokyo, 1990, 342–351.

[6] S. Iyanaga, "The Theory of Numbers," North-Holland, Amsterdam, 1975.

[7] S. Iyanaga, *On the life and works of Teiji Takagi*, in "Teiji Takagi Collected Papers," 2nd ed., Springer-Verlag, Tokyo, 1990, 354–371.

[8] S. Iyanaga, *Travaux de Claude Chevalley sur la théorie du corps de classes: Introduction*, Japan. J. Math. **1** (2006), 25–85.

[9] M. Katsuya, *The Establishment of the Takagi–Artin Class Field Theory*, in "The Intersection of History and Mathematics," (C. Sasaki, M. Sugiura, J. W. Dauben ed.), Birkhauser, Boston, 1995, 109–128.

[10] S. Lang, "Algebraic Number Theory," 2nd ed., Springer-Verlag, New York, 1994.

[11] H. W. Lenstra and P. Stevenhagen, *Chebotarev and his Density Theorem*, Math. Intelligencer **18** (1996), 26–37.

[12] T. Masahito, *Three Aspects of the Theory of Complex Multiplication*, "The Intersection of History and Mathematics," (C. Sasaki, M. Sugiura, J. W. Dauben ed.), Birkhauser, Boston, 1995, 91–108.

[13] K. Miyake, *A Note on the Arithmetic Background to Frobenius' Theory of Group Characters*, Exposition. Math. **7** (1989), 347–358.

[14] K. Miyake, *Teiji Takagi, Founder of the Japanese School of Modern Mathematics*, Japan. J. Math. **2** (2007), 151–164.

[15] P. Roquette, *Class Field Theory in Characteristic p, its Origin and Development*, in "Class Field Theory – its Centenary and Prospect," Math. Soc. Japan, Tokyo, 2001, 549–631.

[16] P. Roquette, "The Brauer-Hasse-Noether Theorem in Historical Perspective," Springer-Verlag, Berlin, 2005.

[17] N. Schappacher, *On the History of Hilbert's* 12*th Problem: A Comedy of Errors*, in "Matériaux pour l'histoire des mathématiques au XX$^\text{e}$ siècle," Soc. Math. France, Paris, 1998, 243–273.

[18] J-P. Serre, "Algebraic Groups and Class Fields," Springer-Verlag, 1988.

[19] S. Vladut, "Kronecker's Jugendtraum and Modular Functions," Gordon and Breach, New York, 1991.

[20] H. Weyl, *David Hilbert and His Mathematical Work*, Bull. Amer. Math. Soc. **50** (1944), 612–654.