

## CLASS FIELD THEORY SUMMARIZED

DENNIS GARBANATI

**1. Introduction.** A good starting point is a quote from M. J. Herbrand of which the following is a translation.

“There is perhaps no theory in science where at the same time the proofs are so difficult and the results of such perfect simplicity and of such great power.” [11, p. 2].

Hopefully this summary will communicate the simplicity and power of the results of class field theory even though no proofs are presented—a fact which is bound to eliminate to some extent the sharp precision found in a complete course.

The first part of this summary will be a very classical presentation of class field theory such as it can be found in the work of Hasse, i.e., pre-World-War II class field theory. The second part will re-summarize class field theory in a more modern fashion using ideles, i.e., Chevalley’s formulation.

**2. Goals.** What are the goals of class field theory? To answer this we need some definitions.

Let  $K$  be a finite extension of the rationals  $\mathbf{Q}$ . In fact, unless stated otherwise all fields discussed in this summary will be finite extensions of  $\mathbf{Q}$ . Let  $\mathcal{O} = \mathcal{O}_K$  be the ring of algebraic integers of  $K$ . A *fractional ideal*,  $\mathfrak{a}$ , is a nonzero finitely generated  $\mathcal{O}$ -module where the generators are in  $K$ . So we can write  $\mathfrak{a} = (\alpha_1, \dots, \alpha_t)$  where the  $\alpha$ ’s are the generators of  $\mathfrak{a}$ . If  $\mathfrak{b} = (\beta_1, \dots, \beta_s)$ , we define the product  $\mathfrak{a}\mathfrak{b} = (\dots, \alpha_i\beta_j, \dots)$  as the  $\mathcal{O}$ -module generated by the products of the various generators of  $\mathfrak{a}$  and  $\mathfrak{b}$ . Under this multiplication the set of fractional ideals forms a multiplicative group,  $A = A_K$ , with  $\mathcal{O} = (1)$  as the identity element.

Although nobody seems to want to define “the arithmetic of  $K$ ”, the following description seems to work in the present context. The *arithmetic of  $K$*  is the study of  $A$ , subgroups of  $A$ , factor groups of subgroups of  $A$ , groups isomorphic to these groups and certain ideals in  $A$ .

We can now state the three-fold goal of class field theory.

(I) “Describe” all finite abelian extensions of  $K$  in terms of the arithmetic of  $K$ . ( $L$  is an abelian extension of  $K$  if the Galois group  $G(L/K)$  is abelian.)

(II) Canonically realize  $G(L/K)$  in terms of the arithmetic of  $K$  whenever  $G(L/K)$  is abelian.

(III) Describe the decomposition of a prime ideal from  $K$  to  $L$  in terms of the arithmetic of  $K$  whenever  $G(L/K)$  is abelian.

3. **Some terminology.** Let  $L$  be a Galois extension of  $K$  of degree  $n$ . Let  $\mathcal{O}_K(\mathcal{O}_L$  resp.) be the ring of algebraic integers of  $K$  ( $L$  resp.). It is known that if  $\mathfrak{p}$  is a prime ideal in  $\mathcal{O}_K$ , then

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$$

where  $\mathfrak{P}_1, \dots, \mathfrak{P}_g$  are distinct prime ideals in  $\mathcal{O}_L$ . The integer  $e$  is called the *ramification index* of  $\mathfrak{p}$ . (If  $L$  is any finite extension of  $K$ , then

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g},$$

i.e., the powers of the various  $\mathfrak{P}$ 's do not have to coincide.) Let “ $\mathfrak{P}$  divides  $\mathfrak{p}$ ”,  $\mathfrak{P}|\mathfrak{p}$ , mean that  $\mathfrak{P}$  occurs in the factorization (above) of  $\mathfrak{p}$ . If  $\mathfrak{P}|\mathfrak{p}$ , then  $\mathcal{O}_K/\mathfrak{p}$  is a field which can be thought of as a subfield of  $\mathcal{O}_L/\mathfrak{P}$ , and  $f = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$  is called the *residue class degree* of  $\mathfrak{p}$  or the residue class degree of  $\mathfrak{P}$ . It is also known that  $efg = n = [L : K]$ .

We say  $\mathfrak{p}$  *splits completely* from  $K$  to  $L$  if  $g = n$ . Why look at primes which split completely? An answer is given by the following theorem.

**THEOREM 3.1.** [13, p. 136]. *Let  $L_1$  and  $L_2$  be Galois extensions of  $K$  and  $S_1, S_2$  be the sets of primes which split completely from  $K$  to  $L_1, L_2$  resp. Then  $S_1 \subset S_2$  (with finitely many exceptions) if and only if  $L_1 \supset L_2$ . So  $S_1 = S_2$  if and only if  $L_1 = L_2$ .* [13, p. 136].

Thus the primes which split completely “capture” the Galois extension.

4. **The historical setting for class field theory.** Histories of class field theory can be found in [11], [12], pp. 479–518], [5, pp. 266–279], and [7].) Gauss (1777–1855) tried to decide when  $x^2 - a \equiv 0 \pmod p$  has a solution (here  $p \nmid a$  and  $p$  is a prime). He came up with his law of reciprocity— one formulation of which is the following theorem.

**THEOREM 4.1.** (Gauss’ Quadratic Reciprocity). [1, p. 122]. *If  $p$  and  $q$  are odd primes not dividing  $a$  and  $p \equiv q \pmod{4a}$ , then  $x^2 - a \equiv 0 \pmod p$  has a solution if and only if  $x^2 - a \equiv 0 \pmod q$  has a solution.*

In other words, whether or not there is a solution to  $x^2 - a \equiv 0 \pmod p$  depends only on the arithmetic progression mod  $4a$  to which  $p$  belongs. But the following can also be shown.

**THEOREM 4.2.** [4, p. 236]. *Let  $L = \mathbf{Q}(\sqrt{d})$  where  $d$  is a square free integer. Then an odd prime  $p$  splits completely from  $\mathbf{Q}$  to  $L$  if and only if  $x^2 - d \equiv 0 \pmod p$  has a solution and  $p \nmid d$ .*

EXAMPLE 4.1. Let us find all the primes which split completely from  $\mathbf{Q}$  to  $\mathbf{Q}(\sqrt{2})$ . Here  $d = 2$ . Any odd prime is congruent to 1 (which is congruent to 17 mod 8), 3, 5, or 7 mod 8. Now  $x^2 - 2 \equiv 0 \pmod{17}$  has the solution  $x = 6$  and  $x^2 - 2 \equiv 0 \pmod{7}$  has the solution 3. Whereas  $x^2 - 2 \equiv 0 \pmod{3}$  and  $x^2 - 2 \equiv 0 \pmod{5}$  do not have solutions. Since it turns out that 2 does not split completely (cf. Example 6.2), it follows from 4.1 and 4.2 that a prime  $p$  splits completely from  $\mathbf{Q}$  to  $\mathbf{Q}(\sqrt{2})$  if and only if  $p \equiv 1 \equiv 17 \pmod{8}$  or  $p \equiv 7 \pmod{8}$ ; that is,  $p$  is in the arithmetic progression  $1, 1 + 8, 1 + 2 \cdot 8, 1 + 3 \cdot 8, \dots$  or in the arithmetic progression  $7, 7 + 8, 7 + 2 \cdot 8, \dots$ . The field  $\mathbf{Q}(\sqrt{2})$  determines these primes and these primes (3.1) determine this normal extension  $\mathbf{Q}(\sqrt{2})$ .

So Gauss had in essence made a statement about the decomposition of primes and had done so in terms of congruence conditions. He had set the tone for a decomposition theory based on congruences.

Let  $\mathbf{R}, \mathbf{C}, \mathbf{Z}$  resp. denote the reals, the complexes, the rational integers and let gcd denote the greatest common divisor.

Dirichlet (1805–1859) worked with Dirichlet  $L$ -series, i.e.,

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad s \in \mathbf{R}$$

where  $\chi$  is a character, i.e. a homomorphism from the multiplicative group of units of  $\mathbf{Z}/m\mathbf{Z}$  into  $\mathbf{C}$  where  $m$  is some positive integer. If  $\text{gcd}(n, m) > 1$ , then we define  $\chi(n)$  to be 0. Using this analytic tool Dirichlet showed the following theorem.

THEOREM 4.3. (Dirichlet's). *If  $\text{gcd}(a, m) = 1$ , then there are an infinite number of primes  $p$  congruent to  $a \pmod{m}$ .*

Weber's attempt to generalize this result led to some of the results of class field theory.

Riemann (1826–1866) worked with the Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad s \in \mathbf{C}.$$

Thus analytic number theory blossomed under Dirichlet and Riemann and the fruit of their work was ripe for those in pursuit of a class field theory.

Kummer (1810–1893) tried to solve Fermat's last theorem, i.e.  $x^n + y^n = z^n$  has no solution in integers  $x, y$  and  $z$  such that  $xyz \neq 0$  if  $n \geq 3$ . Since this equation can be rewritten as

$$x^n = (z - y)(z - \omega y)(z - \omega^2 y) \cdots (z - \omega^{n-1} y)$$

where  $\omega = e^{2\pi i/n}$ , Kummer was led into some very exciting studies of the

cyclotomic field  $\mathbf{Q}(\omega)$ . In particular, Kummer studied the structure of  $\mathcal{C} = A/(K^*)$ , the ideal class group of  $K$  where  $(K^*)$  denotes the principal fractional ideals of  $A = A_K$  and  $K = \mathbf{Q}(e^{2\pi i/p})$  ( $p$  is an odd prime). The reason he did this is because if the order of this  $\mathcal{C}$ , the class number of  $K$ , is 1, then Fermat's last theorem holds for  $x^p + y^p = z^p$ .

Kummer knew the following result.

**THEOREM 4.4.** [5, p. 87]. *Let  $L = \mathbf{Q}(e^{2\pi i/p})$  where  $p$  is a prime. Let  $q$  be a prime not equal to  $p$ . Let  $f$  be the smallest positive integer such that  $q^f \equiv 1 \pmod{p}$ . Then  $q \mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$  where  $g = (p - 1)/f$  and  $p - 1 = [L : \mathbf{Q}]$ .*

(Kummer did not formulate his ideas in this fashion, however, for the concept of an ideal as we know it came from Dedekind.) Hence if  $q \equiv q' \pmod{p}$ , then  $q$  and  $q'$  decompose in the same way ( $q$  and  $q'$  are primes not equal to  $p$ ).

**EXAMPLE 4.2.** Let  $L = \mathbf{Q}(e^{2\pi i/5})$ . It turns out that 5 does not split completely from  $\mathbf{Q}$  to  $L$  (cf. Example 6.2). So a prime  $q$  splits completely from  $\mathbf{Q}$  to  $L$  if and only if  $q \equiv 1 \pmod{5}$ ; that is,  $q = 11, 31, 41, \dots$

Again we see a decomposition theory stated in terms of congruence conditions.

Dedekind (1831–1916), basing his work on the results established by his predecessors, gave a systematic presentation of algebraic number theory. He introduced the idea of a Dedekind domain  $\mathcal{O}$ , i.e., an integral domain in which each ideal  $\mathfrak{n}$  in  $\mathcal{O}$  is a unique product of powers of prime ideals. The ring of algebraic integers of  $K$ ,  $\mathcal{O}_K$ , is the primary example of such a domain. (It is also true that each fractional ideal  $\mathfrak{n}$  in  $A$  is a unique product of powers of prime ideals. Of course, the powers can be negative.) His book exposed clearly the problem of describing the decomposition of a prime, i.e., of describing the  $e$ 's and  $g$  in

$$p\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}.$$

**5. The beginnings of class field theory.** Kronecker (1821–1891) looked at Abel's work and saw that certain equations in one variable arising from elliptic curves give abelian extensions of imaginary quadratic fields. (An elliptic curve can be thought of as given by  $y^2 = x^3 + Ax + B$  and the point at infinity.) (An equation in one variable  $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$  over  $K$  gives rise to the extension of  $K$  obtained by adjoining all its roots to  $K$ .) He wondered if such a procedure would give all abelian extensions and because of this he set forth the problem of "finding" all abelian extensions of a given algebraic number field. Kronecker had posed one of the major questions of class field theory. Furthermore, he stated the following which was proved completely by Weber (1842–1913).

**THEOREM 5.1.** (Kronecker-Weber, 1886–1887). [13, p. 165]. *Let  $K$  be a finite abelian extension of  $\mathbf{Q}$ . Then there exists a positive integer  $m$  such that  $K \subset \mathbf{Q}(e^{2\pi i/m})$ .*

The quote in §1 from Herbrand certainly applies to this theorem.

Consider  $f(z) = e^{2\pi iz}$ . Let  $\tau: z \rightarrow z + 1$ . Let  $T = \langle \tau \rangle$ . Since  $f(z) = f(\tau z)$ , it turns out that  $f(z)$  is an automorphic function with respect to  $T$ . (Definition of an automorphic function: Let  $\Gamma = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbf{Z} \text{ and } \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1 \right\}$ . Let  $H = \{x + iy \mid x, y \in \mathbf{R} \text{ and } y > 0\}$  be the upper half plane. Let  $\gamma \in \Gamma$  act on  $H$  via  $\gamma(z) = (az + b)/(cz + d)$ ,  $z \in H$ . Let  $T$  be a subgroup of  $\Gamma$ . An *automorphic function for  $T$*  is a meromorphic function on  $H$  such that

(i)  $f(\gamma(z)) = f(z)$  for all  $\gamma \in T$ , and

(ii)  $f(z)$  has a Fourier series of the form

$f(z) = \sum_{n=N}^{\infty} a_n e^{2\pi i n z}$  where  $N$  may possibly be negative.) So there exists an automorphic function such that each abelian extension of  $\mathbf{Q}$  is a subfield of a field obtained by adjoining to  $\mathbf{Q}$  a special value of this automorphic function. Kronecker's Jugendtraum (dream of his youth) was to show that abelian extensions of imaginary quadratic fields are subfields of fields obtained by adjoining to them special values of automorphic functions. Kronecker's Jugendtraum was fulfilled later by Weber (1908) and Fueter (1914) who partially proved this and then by Takagi (1920) who gave a complete proof with class field theory.

Hilbert's 12-th problem presented at the International Congress of Mathematicians at Paris in 1900 asks for a generalization of Kronecker's Jugendtraum. This is still a major open problem but Shimura has made a good deal of progress on this problem.

To Kronecker and Weber class field theory meant "finding" all abelian extensions of  $K$  and generalizing Dirichlet's theorem. Although they conjectured and proved some of the key results of class field theory, it was Hilbert who saw the big picture—who saw class field theory as a theory of abelian extensions.

Hilbert's Zahlbericht (1887) gave a systematic account of the work done in algebraic number theory up to that time. Chapter III was on quadratic fields, Chapter IV on cyclotomic fields and Chapter V on Kummer fields (i.e., fields of the form  $K(\sqrt[n]{\alpha})$  where  $e^{2\pi i/n} \in K$ ). All of these fields are abelian extensions. Hilbert was, indeed, blessed by a great deal of knowledge about abelian extensions. With this background and especially with the background of his own work on relative quadratic extensions, Hilbert presented some conjectures in 1898–1899 which capture the broad outlines of class field theory in an ungeneralized form, i.e., Hilbert's conjectures concern the existence and properties of what is now

called the Hilbert class field of  $K$  as it relates to the ideal class group  $\mathcal{C}$  of  $K$ . (The Hilbert class field of  $K$  is the maximal abelian unramified extension of  $K$ .)

In 1900 Hilbert went on to present two key problems in class field theory: problem 12 (already discussed) and problem 9 (i.e., generalize Gauss' law of quadratic reciprocity).

It was Furtwangler who established the validity of most of Hilbert's conjectures on the Hilbert class field by 1907. One of the conjectures—the Principal Ideal Theorem—he was not able to prove until 1930.

However, it was basically Weber during the period 1891–1909, Takagi during the period 1920–1922, Artin in 1927 and Hasse during the period 1926–1930 who gave the world class field theory in its general “classical” form which we present now.

**6. Class field theory over  $\mathbf{Q}$ .** (A summary of class field theory over the rationals is given in [10, p. 4–6].) The statements of class field theory are particularly simple and concrete when the ground field  $K$  is the rationals  $\mathbf{Q}$ . So we start there. But first we adopt a convention. Let  $\mathbf{Q}_m = \mathbf{Q}(e^{2\pi i/m})$  where  $m$  is a positive integer. We shall always assume that  $m$  is not of the form  $2a$  where  $a$  is odd. Why? Because then  $\mathbf{Q}_{2a} = \mathbf{Q}_a$ . (If  $a$  is odd and  $\zeta = e^{2\pi i/a}$ , then  $-\zeta$  is a primitive  $2a$ -th root of 1.) So we are not eliminating any cyclotomic fields by this restriction.

The attainment of the first goal of class field theory (i.e., describing all abelian extensions of  $\mathbf{Q}$  in terms of the arithmetic of  $\mathbf{Q}$ ) is an immediate benefit of the major theorem of class field theory over  $\mathbf{Q}$ , namely, the Kronecker-Weber theorem which says that if  $L$  is any finite abelian extension of  $\mathbf{Q}$ , then there exists a positive integer  $m$  such that  $L \subset \mathbf{Q}_m$ . We say such an  $m$  is a *defining* or *admissible modulus* of  $L$ .

Throughout this section unless stated otherwise  $L$  is an abelian extension of  $\mathbf{Q}$ .

**DEFINITION 6.1.** The *conductor* of  $L$ , denoted  $f_L$ , is the smallest defining modulus of  $L$ .

**EXAMPLE 6.1.** The three most commonly investigated abelian extensions of  $\mathbf{Q}$  are: (1)  $L = \mathbf{Q}_m$  and here  $f_L = m$ ; (2)  $L = \mathbf{Q}(\zeta + \zeta^{-1})$  where  $\zeta = e^{2\pi i/m}$  and here  $f_L = m$ ; and (3)  $L = \mathbf{Q}(\sqrt{d})$  for which we have the following theorem.

**THEOREM 6.1.** [13, p. 198]. *Let  $L = \mathbf{Q}(\sqrt{d})$  where  $d$  is a square free integer. Then*

$$f_L = \begin{cases} |d| & \text{if } d \equiv 1 \pmod{4} \\ |4d| & \text{if } d \equiv 2 \text{ or } 3 \pmod{4}. \end{cases}$$

where  $| \cdot |$  denotes absolute value.

Note that  $f_{\mathbf{Q}(\sqrt{2})} = 8$  and  $f_{\mathbf{Q}_5} = 5$ . These were the numbers used in Example 4.1 and Example 4.2 for determining which primes split completely in  $L = \mathbf{Q}(\sqrt{2})$  and  $L = \mathbf{Q}_5$ . At the end of this section it will be clear why this happened.

It can be shown that  $\mathbf{Q}_{m_1} \cap \mathbf{Q}_{m_2} = \mathbf{Q}_{\gcd(m_1, m_2)}$  from which the following is immediate (from the definition of  $f_L$ ).

**THEOREM 6.2.** *If  $m$  is a defining modulus of  $L$ , then  $f_L | m$ .*

If  $m$  is any positive integer let  $C_m$  be the multiplicative group of  $\mathbf{Z}/m\mathbf{Z}$ , i.e., the integers relatively prime to  $m$  under multiplication. Let  $m$  be a defining modulus of  $L$ . Since  $G(\mathbf{Q}_m/\mathbf{Q}) \cong C_m$ ,  $L$  is the fixed field of some subgroup of  $C_m$  which we denote by  $I_{L, m}$ . Thus we have that

(I) Each abelian extension  $L$  of  $\mathbf{Q}$  is given in terms of the arithmetic of  $\mathbf{Q}$ .

Whit  $m$  as before let  $\gcd(a, m) = 1$ . Then  $a \in C_m$ . Let  $(L/a)$ , the Artin symbol, be the automorphism on  $L$  given by restricting  $\zeta \rightarrow \zeta^a$  (where  $\zeta = e^{2\pi i/m}$ ) to  $L$ . Then  $(L/ \ )$  maps  $C_m$  onto  $G(L/\mathbf{Q})$  and has kernel  $I_{L, m}$ , i.e., we have the following theorem.

**THEOREM 6.3.** (Artin's Law of Reciprocity). *If  $L$  is an abelian extension of  $\mathbf{Q}$  with defining modulus  $m$ , then the following sequence is exact*

$$1 \longrightarrow I_{L, m} \hookrightarrow C_m \xrightarrow{(L/ \ )} G(L/\mathbf{Q}) \longrightarrow 1.$$

Thus  $(L/ \ )$  induces an isomorphism between  $C_m/I_{L, m}$  and  $G(L/\mathbf{Q})$ . Another way to put this is

(II)  $G(L/\mathbf{Q})$  has been canonically realized in terms of the arithmetic of  $\mathbf{Q}$ .

**DEFINITION.** Let  $L$  be a Galois extension of  $K$ . If the ramification index  $e$  of  $\mathfrak{p}$  equals 1, then we say  $\mathfrak{p}$  is *unramified in  $L$* . If  $e > 1$ , then  $\mathfrak{p}$  *ramifies in  $L$* .

If  $a \in \mathbf{Z}$  let  $(a)$  be the principal ideal  $a\mathbf{Z}$ . If  $p$  is a prime number, we identify  $p$  and the prime ideal  $(p)$ .

**THEOREM 6.4.** (Conductor-Ramification Theorem). *If  $L$  is an abelian extension of  $\mathbf{Q}$ , then  $p$  ramifies in  $L$  if and only if  $p | f_L$ .*

Again the quote from Herbrand applies to this result. This theorem has the following as an immediate corollary.

**THEOREM 6.5.** *If  $L \neq \mathbf{Q}$  is an abelian extension of  $\mathbf{Q}$ , then at least one prime  $p$  ramifies in  $L$ .*

**EXAMPLE 6.2.** By Example 6.1  $p$  ramifies in  $\mathbf{Q}_m$  if and only if  $p|m$ . By Theorem 6.1  $p$  ramifies in  $\mathbf{Q}(\sqrt{2})$  if and only if  $p = 2$ . This is the reason

2 did not split completely in Example 4.1 and 5 did not split completely in Example 4.2.

H. Hasse gave a more precise version of 6.4 for which we need the following definitions. Let  $L$  be a Galois extension of  $K = \mathbf{Q}$  where  $G(L/\mathbf{Q}) = \{\sigma_1, \dots, \sigma_n\}$ . An *integral basis* of  $L$  is a set  $\{\alpha_1, \dots, \alpha_n\} \subset \mathcal{O}_L$  where each  $\alpha \in \mathcal{O}_L$  can be written uniquely in the form  $\alpha = b_1\alpha_1 + \dots + b_n\alpha_n$  where  $b_i \in \mathbf{Z}$ .

DEFINITION. If  $\alpha_1, \dots, \alpha_n$  is an integral basis of  $L$  (an integral basis always exists), then the *discriminant* of  $L$  is defined to be  $d_L = \det(\sigma_i\alpha_j)^2$  where  $\sigma_i\alpha_j$  is the  $(i, j)$ -th entry in the  $n \times n$ -matrix  $(\sigma_i\alpha_j)$ .

The following was well known before class field theory.

THEOREM 6.6. *A prime  $p$  of  $\mathbf{Q}$  ramifies in  $L$  if and only if  $p|d_L$ .*

Let  $\hat{C}_m$  be the set of characters on  $C_m$ , i.e., homomorphisms from  $C_m$  into the complex numbers  $\mathbf{C}$ . If  $\gcd(a, m) > 1$ , then let  $\chi(a) = 0$  for any  $\chi \in \hat{C}_m$ .

DEFINITION. A positive integer  $c$  is a *defining modulus* of  $\chi \in \hat{C}_m$  if  $a \equiv 1 \pmod c$  implies  $\chi(a) = 1$ .

DEFINITION. The *conductor* of  $\chi \in \hat{C}_m$ , denoted  $f_\chi$ , is the smallest defining modulus of  $\chi$ .

If  $m$  is a defining modulus of  $L$ , let

$$X_{L,m} = \{\chi \in \hat{C}_m \mid \chi(h) = 1 \text{ for all } h \in I_{L,m}\},$$

the *character group of  $L$  mod  $m$* .

It can now be seen from Theorem 6.6 that the following result of Hasse is a more precise version of Theorem 6.4.

THEOREM 6.7. (Conductor-Discriminant Formula) *Let  $m$  be a defining modulus of  $L$ . Then*

$$f_L = \text{lcm} \{f_\chi \mid \chi \in X_{L,m}\}$$

and

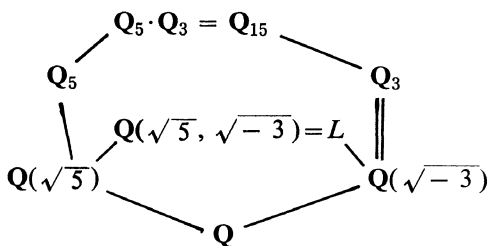
$$|d_L| = \prod_{\chi \in X_{L,m}} f_\chi$$

(lcm = least common multiple).

In particular  $f_L | d_L$  and so we always have the tower  $\mathbf{Q} \subset L \subset \mathbf{Q}_{f_L} \subset \mathbf{Q}_{|d_L|}$ .

EXAMPLE 6.3. Let  $L = \mathbf{Q}(\sqrt{5}, \sqrt{-3})$ . We will show  $|d_L| = 5^2 \cdot 3^2$  and  $f_L = 5 \cdot 3$ . By Theorem 6.1 we have





Now  $G(\mathbf{Q}_5/\mathbf{Q}) \cong C_5$  which is cyclic generated by say  $a_1$  and  $G(\mathbf{Q}_3/\mathbf{Q}) \cong C_3$  which is also cyclic generated by say  $a_2$ . Then

$$C_{15} \cong G(\mathbf{Q}_{15}/\mathbf{Q}) \cong G(\mathbf{Q}_5/\mathbf{Q}) \times G(\mathbf{Q}_3/\mathbf{Q}) \cong \langle a_1 \bmod 5 \rangle \times \langle a_2 \bmod 3 \rangle.$$

Define characters  $\chi_1$  and  $\chi_2$  on  $\langle a_1 \bmod 5 \rangle \times \langle a_2 \bmod 3 \rangle$  as follows:  $\chi_1(a_1) = \sqrt{-1}$ ,  $\chi_1(a_2) = 1$  and  $\chi_2(a_1) = 1$ ,  $\chi_2(a_2) = -1$ . Then we can take  $\langle \chi_1 \rangle \times \langle \chi_2 \rangle$  to be the character group of  $C_{15}$ . Since  $G(\mathbf{Q}_5/\mathbf{Q}(\sqrt{5})) = \langle a_1^2 \bmod 5 \rangle$  and  $\mathbf{Q}(\sqrt{-3}) = \mathbf{Q}_3$ , we get  $G(\mathbf{Q}_{15}/L) = \langle a_1^2 \bmod 5 \rangle \times \langle 1 \bmod 3 \rangle$ . Thus  $X_{L,15} = \langle \chi_1^2 \rangle \times \langle \chi_2 \rangle$ . Now the following proposition can be shown.

**PROPOSITION.** *The defining moduli of  $\chi \in \hat{C}_m$  are precisely the multiples of  $f_\chi$ .*

Thus since 5 is a defining modulus of  $\mu = \chi_1^2$ ,  $f_\mu = 1$  or 5. But clearly 1 is not a defining modulus of  $\chi_1^2$ . So  $f_\mu = 5$ . Similarly  $f_{\chi_2} = 3$ ,  $f_{\mu\chi_2} = 15$  and  $f_{\chi_0} = 1$  where  $\chi_0 = 1$  is the principal character. Therefore by the Conductor—Discriminant formula  $|d_L| = 5^2 \cdot 3^2$  and  $f_L = 5 \cdot 3$ .

Let  $m$  be a defining modulus of  $L$ . If  $p \nmid m$  then by Theorem 6.2  $p \nmid f_L$  and so  $p$  does not ramify in  $L$  (Conductor-Ramification theorem). We can now state the generalization of Example 4.1 and Theorem 4.4.

**THEOREM 6.8. (Decomposition Theorem).** *Let  $m$  be a defining modulus of  $L$ . If  $p \nmid m$  then the order of  $pI_{L,m}$  in  $C_m/I_{L,m}$  is  $f$ , the residue class degree of  $p$ .*

Let  $L$  be a Galois extension of  $K$ . Let  $\text{Spl}(L/K)$  denote the set of all prime ideals of  $K$  which split completely in  $L$ .

Let  $m = f_L$ . Then, since  $efg = n = [L: \mathbf{Q}]$ ,  $p \in \text{Spl}(L/\mathbf{Q})$  if and only if  $e = 1$  and  $f = 1$  if and only if  $p \nmid f_L$  and  $p \in I_{L,f_L}$ . If we let  $I_{L,f_L} = \{a_1, \dots, a_s\}$  where the  $a_i$  are integers (necessarily relatively prime to  $f_L$ ), then  $p \in \text{Spl}(L/\mathbf{Q})$  if and only if  $p \equiv a_i \pmod{f_L}$  for some  $i$ ,  $1 \leq i \leq s$ . Thus the primes which split completely are given by congruence conditions. This is the realization of

(III) Describing the decomposition of a prime (III) in terms of the arithmetic of  $\mathbf{Q}$ .

DEFINITION. If  $p$  is an odd prime,  $a \in \mathbf{Z}$ , and  $p \nmid a$ , the *Legendre symbol*  $(a/p)$  is given by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv a \pmod{p} \text{ has a solution} \\ -1 & \text{if } x^2 \equiv a \pmod{p} \text{ has no solution.} \end{cases}$$

If  $b$  is an odd positive integer where  $b = p_1^{a_1} \dots p_s^{a_s}$  and  $\gcd(a, b) = 1$ , the *Jacobi symbol*  $(a/b)$  is given by

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{a_1} \dots \left(\frac{a}{p_s}\right)^{a_s}.$$

Let  $L = \mathbf{Q}(\sqrt{d})$ . Identify  $G(L/\mathbf{Q})$  and the multiplicative group of order 2 generated by  $-1$  by mapping the generator of  $G(L/\mathbf{Q})$  to  $-1$ . Under this identification if  $p$  is an odd prime not dividing  $f_L$ , then  $(L/p) = (d/p)$ . This follows from Theorem 4.2, the Decomposition theorem and Artin's law of reciprocity which say  $(d/p) = 1$  if and only if  $p \in \text{Spl}(L/\mathbf{Q})$  if and only if  $(L/p) = 1$ . Since  $(L/\cdot)$  is a homomorphism, if  $b$  is an odd positive integer and  $\gcd(d, b) = 1$ , then  $(L/b) = (d/b)$ . Thus the Artion symbol is a generalization of the Jacobi symbol which is a generalization of the Legendre symbol.

REMARK 6.1. Not only does the Artin symbol generalize the Legendre symbol but Gauss' law of quadratic reciprocity (4.1) can be deduced from Artin's law of reciprocity (6.3) as follows. Let  $p$  and  $q$  be odd primes not dividing  $a$  and let  $p \equiv q \pmod{4a}$ . Then the following six statements are equivalent.

- 1)  $x^2 \equiv a \pmod{p}$  has a solution.
- 2)  $x^2 \equiv d \pmod{p}$  has a solution where  $a = d \cdot \text{square}$  and  $d$  is square free.
- 3)  $p \in \text{Spl}(\mathbf{Q}(\sqrt{d})/\mathbf{Q})$ . (By Theorem 4.2.)
- 4)  $(\mathbf{Q}(\sqrt{d})/p) = 1$ . (By 6.8 and Artin's law of reciprocity.)
- 5)  $(\mathbf{Q}(\sqrt{d})/q) = 1$ . (Since  $p \equiv q \pmod{4a} \Rightarrow p \equiv q \pmod{4d} \Rightarrow p \equiv q \pmod{f_{\mathbf{Q}(\sqrt{d})}} \Rightarrow (\mathbf{Q}(\sqrt{d})/p) = (\mathbf{Q}(\sqrt{d})/q)$  by the definition of  $(\mathbf{Q}(\sqrt{d})/p)$ .)
- 6)  $x^2 \equiv a \pmod{q}$  has a solution.

EXAMPLE 6.4. Let  $L = \mathbf{Q}(\sqrt{5}, \sqrt{-3})$ . We will show  $p \in \text{Spl}(L/\mathbf{Q})$  if and only if  $p \equiv 1 \pmod{15}$  or  $p \equiv 4 \pmod{15}$ . Let  $a_1 = 3$  and  $a_2 = 2$ . Then as in Example 6.3 under the natural isomorphism we have

$$\begin{aligned} G(\mathbf{Q}_{15}/\mathbf{Q}) &\cong \langle a_1 \pmod{5} \rangle \times \langle a_2 \pmod{3} \rangle \\ &= \langle 3 \pmod{5} \rangle \times \langle 2 \pmod{3} \rangle \end{aligned}$$

and

$$G(\mathbf{Q}_{15}/L) \cong \langle 3^2 \pmod{5} \rangle \times \langle 1 \pmod{3} \rangle.$$

Therefore

$$I_{L, f_L} = G(\mathbf{Q}_{15}/L) = \langle 4 \pmod{15} \rangle.$$

The result follows from 6.8.

**7. Classical global class field theory.** (Classical presentations of class field theory are found in [9], [13], and [14].) In order to state the results of class field theory for an arbitrary ground field  $K$  we need to

- (a) replace  $m$  with something more general,
- (b) generalize the concept of congruence,
- (c) replace  $C_m$  with something more general,
- (d) generalize  $I_{L, m}$ ,
- (e) generalize “the conductor of  $L$ ” and “a defining modulus of  $L$ ”,  
and
- (f) replace  $\mathbf{Q}_m$  with something more general.

The insight needed to do this is to say the least nontrivial because the Kronecker-Weber theorem simply does not hold for an arbitrary ground field  $K$ .

In this section  $K$  is always an arbitrary finite extension of  $\mathbf{Q}$ .

(a) In dealing with  $\mathbf{Q}$  one can get away with avoiding a discussion of infinite primes but they must be introduced now. Let  $\sigma_1, \dots, \sigma_t$  be the isomorphisms from  $K$  into  $\mathbf{C}$  which fix  $\mathbf{Q}$  where  $t = [K: \mathbf{Q}]$ . With each  $\sigma$  such that  $\sigma K \subset \mathbf{R}$  we associate a formal symbol  $\mathfrak{p}_\sigma$  referred to as a real infinite  $K$ -prime. If  $\sigma K \not\subset \mathbf{R}$ , then  $\bar{\sigma}$  ( $\sigma$  followed by complex conjugation) is another isomorphism from  $K$  into  $\mathbf{C}$ . With each such pair  $\{\sigma, \bar{\sigma}\}$  associate a formal symbol  $\mathfrak{p}_\sigma = \mathfrak{p}_{\bar{\sigma}}$  referred to as a complex infinite  $K$ -prime. In this context a prime ideal of  $\mathcal{O}_K$  is also called a finite  $K$ -prime. So “a  $K$ -prime” will refer to a finite or infinite  $K$ -prime.

Let  $L$  be a Galois extension of  $K$ . Let  $\mathfrak{P}$ (resp.  $\mathfrak{p}$ ) be an infinite  $L$ -prime (resp.  $K$ -prime). Then  $\mathfrak{P} | \mathfrak{p}$  means that if  $\mathfrak{P} = \mathfrak{P}_\tau$  and  $\mathfrak{p} = \mathfrak{p}_\sigma$ , then  $\tau$  is an extension of  $\sigma$  to  $L$ .

**DEFINITION.** A *modulus* of  $K$  (or  $K$ -modulus), denoted  $\mathfrak{m}$ , is a formal product of an ideal  $\mathfrak{m}_0 \subset \mathcal{O}_K$  and a set of real infinite  $K$ -primes. Thus  $\mathfrak{m} = \mathfrak{m}_0 \cdot$  some real infinite  $K$ -primes. All the infinite primes are raised to the first power here.

Let  $\mathfrak{p}_\infty$  denote the real infinite prime on  $\mathbf{Q}$  associated with the identity map on  $\mathbf{Q}$ .

(b) Let  $A_\mathfrak{m}$  be the set of all fractional ideals  $\mathfrak{a} \in A = A_K$  such that the unique factorization of  $\mathfrak{a}$  and  $\mathfrak{m}$  into  $K$ -primes contains no  $K$ -prime in common. Let  $K^* = K - \{0\}$ . If  $\alpha \in K^*$ , let  $(\alpha)$  be the principal ideal  $\alpha \mathcal{O}_K$ . If  $(\alpha) \in A_\mathfrak{m}$ , then it turns out that  $\alpha = a/b$  where  $a, b \in \mathcal{O}_K$  and  $(a), (b) \in A_\mathfrak{m}$ .

DEFINITION. Let  $(\alpha) \in A_m$ . Then  $\alpha \equiv 1 \pmod m$  means  $a \equiv b \pmod{m_0}$  where  $\alpha = a/b$  are as above and  $\sigma\alpha > 0$  for each infinite  $K$ -prime  $p_\sigma$  occurring in  $m$ .

This is a well defined concept, i.e., it makes no difference how  $\alpha$  is written as the quotient of two algebraic integers. We have generalized the notion of congruence.

(c) Let  $R_m$ , the ray mod  $m$ , be the subgroup of  $A_m$ ,  $R_m = \{(\alpha) \in A_m \mid \alpha \equiv 1 \pmod m\}$ .

Let  $K = \mathbf{Q}$  and let  $m = (m)p_\infty$ . If  $(\alpha) \in A_m$ , then  $\alpha = \pm ab^{-1}$  where  $a$  and  $b$  are positive integers relatively prime to  $m$ . Let  $A_m \rightarrow C_m$  via  $(\alpha) \rightarrow ab^{-1}$ . The kernel of this map is  $R_m$ . So this map induces an isomorphism  $\phi$  given in the following proposition.

PROPOSITION 7.1. *Let  $K = \mathbf{Q}$  and  $m = (m)p_\infty$ . Then  $A_m/R_m \cong C_m$  via  $\phi: (\alpha)R_m \rightarrow ab^{-1}$  where  $\alpha = \pm ab^{-1}$  as above.*

Let  $C_m = A_m/R_m$ . Thus  $C_m$  generalizes  $C_m$  and, in fact,  $C_m$  will play the same role in the theory over  $K$  that  $C_m$  played in the theory over  $\mathbf{Q}$ . Note that if  $m = 1$ , then  $A_m = A$  and  $R_m = (K^*)$  and so  $C_m = \mathcal{C}$ , the ideal class group of  $K$ . Thus  $C_m$  is a generalization of the integers mod  $m$  under multiplication and also of the ideal class group which makes it a very interesting object.

(d) Generalizing  $I_{L,m}$  is not at all trivial since we do not have the Kronecker-Weber Theorem. Let  $L/K$  be a Galois extension. Let  $\mathfrak{P}$  and  $\mathfrak{p}$  be prime ideals of  $L$  and  $K$  (resp.) such that  $\mathfrak{P} \mid \mathfrak{p}$ . Let  $f$  be the residue class degree of  $\mathfrak{P}$ . Define the norm of  $\mathfrak{P}$  via  $N_{L/K}\mathfrak{P} = \mathfrak{p}^f$ . Extend this definition to all fractional ideals  $\mathfrak{A} \in A_L$  of  $L$  via

$$N_{L/K} \mathfrak{A} = \prod_{i=1}^s (N_{L/K} \mathfrak{P}_i)^{a_i}$$

where

$$\mathfrak{A} = \prod_{i=1}^s \mathfrak{P}_i^{a_i}.$$

Let  $m$  be a  $K$ -modulus. Let  $A_{L,m}$  be the set of all fractional ideals  $\mathfrak{A} \in A_L$  such that the unique factorizations of  $\mathfrak{A}$  and  $m_0\mathcal{O}_L$  into  $L$ -primes contain no  $L$ -primes in common. Let  $R_{L,m} = \{(\alpha) \in A_{L,m} \mid \alpha \equiv 1 \pmod{m_0\mathcal{O}_L} \text{ and } \tau\alpha > 0 \text{ for all real } \mathfrak{P}_\tau \text{ such that } \mathfrak{P}_\tau \mid p_\sigma \text{ where } p_\sigma \text{ occurs in } m\}$ .

It can be shown that  $N_{L/K}(R_{L,m}) \subset R_m$ . Let  $C_{L,m} = A_{L,m}/R_{L,m}$ . Then we extend the definition of  $N_{L/K}$  to  $C_{L,m}$ , i.e., if  $\mathfrak{A} \in A_{L,m}$ , then  $N_{L/K}(\mathfrak{A}R_{L,m}) = N_{L/K} \mathfrak{A} \cdot R_m$ . Let  $I_{L/K,m} = N_{L/K}(C_{L,m})$ , a subgroup of  $C_m$ .

If  $m$  is a defining modulus of  $L$  (an abelian extension of  $\mathbf{Q}$ ) and if  $m = (m)p_\infty$ , then it turns out that  $I_{L,\mathbf{Q},m} \cong I_{L,m}$ . So  $I_{L/K,m}$  generalizes  $I_{L,m}$

and, in fact,  $I_{L/K, \mathfrak{m}}$  will play the same role in the theory over  $K$  as  $I_{L, \mathfrak{m}}$  played in the theory over  $\mathbf{Q}$ .

Convention: Unless stated otherwise  $L$  is an abelian extension of  $K$ .

(e) To generalize the notion of “the conductor of  $L$ ” and “a defining modulus of  $L$ ” we need the following very deep theorem.

**THEOREM 7.2.** *Let  $\mathfrak{m}$  be a  $K$ -modulus. Given  $L/K$  there exists a unique  $K$ -modulus  $\mathfrak{f}_{L/K}$  such that  $(C_{\mathfrak{m}} : I_{L/K, \mathfrak{m}}) = [L : K]$  if and only if  $\mathfrak{f}_{L/K} | \mathfrak{m}$ .*

**DEFINITION.** The unique modulus  $\mathfrak{f}_{L/K}$  given in Theorem 7.2 is called the *conductor* of  $L/K$  and any  $K$ -modulus  $\mathfrak{m}$  such that  $\mathfrak{f}_{L/K} | \mathfrak{m}$  is called a *defining modulus* of  $L/K$ .

The proof of 7.2 consists of proving the following two statements.

(a)  $(C_{\mathfrak{m}} : I_{L/K, \mathfrak{m}}) \leq [L : K]$  for every  $K$ -modulus  $\mathfrak{m}$ —the first inequality of class field theory proved by Weber (1897–1898) using Dirichlet  $L$ -series. (Chevalley using purely arithmetic means proved (a) which in the new terminology is called the second inequality.)

(b)  $(C_{\mathfrak{m}} : I_{L/K, \mathfrak{m}}) \geq [L : K]$  for some  $K$ -modulus  $\mathfrak{m}$ —the second inequality of class field theory proved by Takagi in 1920.

Let  $L$  be an abelian extension of  $\mathbf{Q}$ . Then it can be shown that

$$\mathfrak{f}_{L/\mathbf{Q}} = \begin{cases} (f_L) & \text{if } L \subset \mathbf{R} \\ (f_L)p_{\infty} & \text{if } L \not\subset \mathbf{R} \end{cases}$$

So  $\mathfrak{f}_{L/\mathbf{Q}}$  is a generalization of  $f_L$ .

In order to replace  $\mathbf{Q}_{\mathfrak{m}}$  by something more general we need the following theorem proved by Takagi (1920).

**THEOREM 7.3. (Existence Theorem).** *Given a  $K$ -modulus  $\mathfrak{m}$  and a subgroup  $I_{\mathfrak{m}}$  of  $C_{\mathfrak{m}}$  there exists a unique abelian extension  $L$  of  $K$  such that*

- (a)  $\mathfrak{m}$  is a defining modulus of  $L/K$ , and
- (b)  $I_{L/K, \mathfrak{m}} = N_{L/K} C_{L, \mathfrak{m}} = I_{\mathfrak{m}}$ .

**DEFINITION.** Let  $I_{\mathfrak{m}}$  be a subgroup of  $C_{\mathfrak{m}}$  and  $L$  an abelian extension of  $K$ . We say  $L$  is the *class field* of  $I_{\mathfrak{m}}$  if (a) and (b) of 7.3 are satisfied.

**DEFINITION.** Let  $I_{\mathfrak{m}} = \{1\} \subset C_{\mathfrak{m}}$ . Then the class field of  $I_{\mathfrak{m}}$ , denote  $K(R_{\mathfrak{m}})$ , is called the *ray class field* of  $K \bmod \mathfrak{m}$ .

There is a particular ray class field which is of fundamental importance, the Hilbert class field of  $K$ , denoted  $\tilde{K}$ . Why? Because, as we shall see later,  $G(\tilde{K}/K) \cong C$ , the ideal class group of  $K$ .

**DEFINITION.** [13, p. 191]. *The Hilbert class field of  $K$  is the ray class field  $K(R_{(1)})$ , i.e.,  $\tilde{K} = K(R_{(1)})$ .*

If  $K = \mathbf{Q}$ , it turns out that  $\mathbf{Q}_{\mathfrak{m}}$  is the ray class field of  $\mathbf{Q} \bmod \mathfrak{m}$  where  $\mathfrak{m} = (m)p_{\infty}$ . So the ray class field mod  $\mathfrak{m}$  is what replaces  $\mathbf{Q}_{\mathfrak{m}}$  in the general

theory. But the analogy is even more stunning as the following theorems indicate.

**THEOREM 7.4.** *Given  $L/K$  there exists a  $K$ -modulus  $m$  such that  $L \subset K(R_m)$ .*

**THEOREM 7.5.** *The conductor  $f_{L/K}$  is the “smallest”  $K$ -modulus  $m$  such that  $L \subset K(R_m)$ . “Smallest” means that if  $L \subset K(R_m)$ , then  $f_{L/K} | m$ . Also  $m$  is a defining modulus of  $L/K$  if and only if  $L \subset K(R_m)$ .*

Thus we have “found” all abelian extensions of  $K$ , i.e., they are the subfields of the ray class fields of  $K$ , but we have not “constructed” them. However, if  $K = \mathbf{Q}(\sqrt{-d})$  ( $d$  square free) is an imaginary quadratic field, then one can show in fact, that each abelian extension  $L$  of  $K$  is a subfield of  $K(R_{(N)})$  for some positive integer  $N$ . Furthermore, by the fundamental theorem of complex multiplication one can produce a finite set of automorphic functions whose values at  $(1 + \sqrt{d})/2$  if  $d \equiv 1 \pmod{4}$  or at  $\sqrt{-d}$  if  $d \equiv 2$  or  $3 \pmod{4}$  when adjoined to  $K$  yield  $K(R_{(N)})$ . Thus in this case it is possible to “construct” the abelian extensions of  $K$ —Kronecker’s Jugendtraum is fulfilled. (For more on this topic see [15], [3] and [18].)

Getting back to the Existence Theorem the following is historically interesting. Since  $C_m \cong A_m/R_m$  if  $m = (m)p_\infty$ , one way of stating Dirichlet’s theorem is that each coset of  $A_m/R_m$  contains an infinite number of primes. As mentioned before, Weber had set himself to the task of generalizing Dirichlet’s theorem. He pointed out in 1897–1898 that the generalization given below would follow from the Existence theorem which, it is safe to say, he was convinced was true but could not prove.

**THEOREM 7.6.** (Dirichlet’s Theorem Generalized). *Let  $I_m$  be a subgroup of  $C_m$ . Then  $I_m = H_m/R_m$  where  $A_m \supset H_m \supset R_m$ . There are an infinite number of primes in each coset of  $A_m/H_m$ .*

There is a more precise way of stating this result using the concept of density. (For more on this topic see [16, pp. 322–361].)

**DEFINITION.** Let  $M$  be any set of finite  $K$ -primes. Let  $\mathcal{Q}$  be the set of all finite  $K$ -primes. Let  $\#(\ )$  denote “the number of elements of”. The natural density  $d(M)$  of  $M$  is the following limit (if it exists)

$$d(M) = \lim_{x \rightarrow \infty} \frac{\#\{p \in M \mid N_{K/\mathbf{Q}} p \leq x\}}{\#\{p \in \mathcal{Q} \mid N_{K/\mathbf{Q}} p \leq x\}}.$$

If  $K = \mathbf{Q}$ , then

$$d(M) = \lim_{x \rightarrow \infty} \frac{\#\{p \in M \mid p \leq x\}}{\#\{p \mid p \text{ is a prime and } p \leq x\}}.$$

A finite set of  $K$ -primes obviously has a natural density of zero.

**THEOREM 7.7. (Prime Ideal Theorem).**

$$1 = \lim_{x \rightarrow \infty} \frac{\#\{p \in \mathcal{O} \mid N_{K/\mathbf{Q}} p \leq x\}}{\frac{x}{\log x}}.$$

(The prime number theorem is the prime ideal theorem in the case where  $K = \mathbf{Q}$ .) So we can redefine the natural density to be

$$d(M) = \lim_{x \rightarrow \infty} \frac{\#\{p \in M \mid N_{K/\mathbf{Q}} p \leq x\}}{\frac{x}{\log x}}.$$

The more precise version of Theorem 7.6 now reads as follows.

**THEOREM 7.8.** *Let  $m$  be a  $K$ -modulus. Using the notation of Theorem 7.6, let  $M$  be the set of  $K$ -primes in any fixed coset of  $A_m/H_m$ . Then*

$$d(M) = \frac{1}{\#(A_m/H_m)}.$$

So a more precise version of Dirichlet's theorem is the following theorem.

**THEOREM 7.9.** *Let  $m = (m)p_\infty$ , a  $\mathbf{Q}$ -modulus. Let  $M$  be the set of primes in any fixed coset of  $A_m/R_m \cong C_m$ . Then*

$$d(M) = \frac{1}{\#(C_m)} = \frac{1}{\varphi(m)}$$

where  $\varphi$  is the Euler phi function.

We shall now canonically realize  $G(L/K)$ —Artin's law of reciprocity. Let  $m$  be a defining modulus of  $L/K$ . Let  $p$  be a finite  $K$ -prime such that  $p \nmid m$ . Then it can be shown that there exists a unique automorphism in  $G(L/K)$ , denoted  $(L/K/p)$ , such that

$$(*) \quad \left(\frac{L/K}{p}\right)\alpha \equiv \alpha^{N_{K/\mathbf{Q}}p} \pmod{p\mathcal{O}_L}$$

for all  $\alpha \in \mathcal{O}_L$ . The *Artin symbol* is the natural extension of this map as follows. If

$$\alpha = p_1^{a_1} \cdots p_s^{a_s}, \quad a_i \in \mathbf{Z},$$

then

$$\left(\frac{L/K}{\alpha}\right) = \left(\frac{L/K}{p_1}\right)^{a_1} \cdots \left(\frac{L/K}{p_s}\right)^{a_s}$$

The following proposition is immediate from the uniqueness of the map given by (\*).

PROPOSITION 7.10. *Let  $M \supset L \supset K$  and let  $\mathfrak{m}$  be a defining modulus of  $M/K$  and  $L/K$ . If  $\alpha \in A_{\mathfrak{m}}$ , then  $(L/K/\alpha)$  is  $(M/K/\alpha)$  restricted to  $L$ .*

It can be shown that if  $(\alpha) \in R_{\mathfrak{m}}$ , then  $(L/K/(\alpha)) = 1$  and so we can define the Artin symbol on  $C_{\mathfrak{m}} = A_{\mathfrak{m}}/R_{\mathfrak{m}}$  as follows. If  $c \in C_{\mathfrak{m}}$  and  $c = \alpha R_{\mathfrak{m}}$ , then let  $(L/K/c) = (L/K/\alpha)$ .

Let  $K = \mathbf{Q}$  and let  $\mathfrak{m} = (m)p_{\infty}$  be a defining modulus of  $L$ . It is not difficult to show that  $(L/K/c) = (L/\psi(c))$  where  $\psi$  is the map given in Proposition 7.1 and  $(L/ )$  is the map defined before 6.3. Thus this definition of the Artin symbol is a generalization of that given before Theorem 6.3.

In 1927 Artin proved the following theorem.

THEOREM 7.11. (Artin's Law of Reciprocity). *The following sequence is exact:*

$$1 \longrightarrow I_{L/K, \mathfrak{m}} = N_{L/K}(C_{L, \mathfrak{m}}) \hookrightarrow C_{\mathfrak{m}} \xrightarrow{(L/K)} G(L/K) \longrightarrow 1.$$

COROLLARY 7.12. *Let  $\mathfrak{m}$  be a defining modulus of  $L/K$ . Then  $L \subset K(R_{\mathfrak{m}})$ ,  $G(K(R_{\mathfrak{m}})/K) \cong C_{\mathfrak{m}}$ , and  $G(K(R_{\mathfrak{m}})/L) \cong I_{L/K, \mathfrak{m}}$ .*

PROOF. Theorem 7.5 yields  $L \subset K(R_{\mathfrak{m}})$ . Since  $(L/K): I_{L/K, \mathfrak{m}} \rightarrow 1 \in G(L/K)$  and  $(L/K)$  is  $(K/R_{\mathfrak{m}})/K$  restricted to  $L$  (7.10),  $(K(R_{\mathfrak{m}})/K)$  maps  $I_{L/K, \mathfrak{m}}$  into  $G(K(R_{\mathfrak{m}})/L)$ . This map is an isomorphism because  $\text{Ker}(K(R_{\mathfrak{m}})/K) = 1$  and is onto by a simple order argument.

Artin's law of reciprocity thus allows us to give a Galois interpretation to class field theory, i.e., the following picture gives the basics.

$$I_{L/K, \mathfrak{m}} = N_{L/K}(C_{L, \mathfrak{m}}) \left( \begin{array}{c} K(R_{\mathfrak{m}}) \\ | \\ L \\ | \\ K \end{array} \right) C_{\mathfrak{m}}$$

COROLLARY 7.13. *If  $\tilde{K}$  is the Hilbert class field of  $K$ , then  $G(\tilde{K}/K) \cong C$ , the ideal class group of  $K$ .*

PROOF. Let  $L = \tilde{K}$  and  $\mathfrak{m} = 1$  in 7.11.

Because of this corollary extensive investigation has been made on certain subfields of  $\tilde{K}$  which contain  $K$  because such research leads to results about  $\mathcal{C}$ —results desired ever since Kummer studied  $\mathcal{C}$  in connection with Fermat's last theorem. (See Appendix II for a list of some articles on this topic.)

The Galois interpretation of class field theory afforded by 7.11 will rather easily yield the following theorem.

THEOREM 7.14. *Let  $\mathfrak{m}$  be a defining modulus of  $L_1/K$  and  $L_2/K$ . Then (a)  $\mathfrak{m}$  is a defining modulus of  $L_1L_2/K$  and  $L_1 \cap L_2/K$ ,*



(b)  $I_{L_1L_2/K, m} = I_{L_1/K, m} \cap I_{L_2/K, m}$ ,  $I_{L_1 \cap L_2/K, m} = I_{L_1/K, m} \cdot I_{L_2/K, m}$   
 and

(c) (The ordering theorem proved by Weber in 1897-98)  $L_1 \subset L_2$  if and only if  $I_{L_1/K, m} \supset I_{L_2/K, m}$ .

DEFINITION. Let  $L$  be a Galois extension of  $K$ . Let  $\mathfrak{p}_\sigma$  be an infinite  $K$ -prime and  $\mathfrak{P}_\tau$  an infinite  $L$ -prime such that  $\mathfrak{P}_\tau | \mathfrak{p}_\sigma$ . Then  $\mathfrak{p}_\sigma$  is ramified in  $L$  if  $\sigma K \subset \mathbf{R}$  and  $\tau L \not\subset \mathbf{R}$ . Otherwise  $\mathfrak{p}_\sigma$  is unramified in  $L$ . (Note that if  $\tau$  and  $\tau'$  are two extensions of  $\sigma$ , then  $\tau' = \tau\rho$  where  $\rho \in G(L/K)$ , and so this definition is independent of the choice of the extension of  $\sigma$ .)

THEOREM 7.15. (Conductor-Ramification Theorem, Takagi, 1920). *A  $K$ -prime  $\mathfrak{p}$  ramifies in  $L$  if and only if  $\mathfrak{p} | \mathfrak{f}_{L/K}$ .*

DEFINITION. Let  $L/K$  be Galois. Then  $L$  is an unramified extension of  $K$  if no  $K$ -prime, finite or infinite, ramifies in  $L$ .

THEOREM 7.16. *The Hilbert class field  $\tilde{K}$  of  $K$  is the maximal abelian unramified extension of  $K$ , i.e., if  $L$  is an unramified abelian extension of  $K$ , then  $L \subset \tilde{K}$  which itself is an unramified extension of  $K$ .*

PROOF. Since  $\tilde{K} = K(R_{(1)})$ ,  $\mathfrak{f}_{\tilde{K}/K} = (1)$  by 7.5. If  $L$  is an unramified extension of  $K$ , then  $\mathfrak{f}_{L/K} = (1)$ . By 7.5,  $L \subset K(R_{(1)}) = \tilde{K}$ .

EXAMPLE 7.1. Let  $K = \mathbf{Q}\sqrt{-3 \cdot 5}$ . We will show  $\tilde{K}' = \mathbf{Q}(\sqrt{-3}, \sqrt{5})$ . Let  $K' = \mathbf{Q}(\sqrt{-3}, \sqrt{5})$ . Since  $K$  and  $K'$  are both non-real abelian extensions of  $\mathbf{Q}$ , no infinite  $K$ -prime ramifies in  $K'$ . By Theorems 6.1, 6.4, and Example 6.3 the finite  $\mathbf{Q}$ -primes which ramify in  $K$  are the same as those which ramify in  $K'$ , namely, 3 and 5. The ramification index of 3 in  $K$  is two. Thus since 3 does not ramify in  $\mathbf{Q}(\sqrt{5})$ , 3 ramifies in  $K'$  with ramification index 2. Similarly, the ramification indices of 5 in  $K$  and  $K'$  are the same. So  $K'$  is an unramified extension of  $K$  and hence  $K' \subset \tilde{K}$  by 7.16. Now the following result can be deduced without using class field theory from facts about Dirichlet  $L$ -series.

THEOREM 7.17. *Let  $K = \mathbf{Q}(\sqrt{d})$  where  $d < -2$ . Suppose  $f_K$  is odd. Let  $(a/|d|)$  be the Jacobi symbol. Then*

$$\#(\mathcal{E}) = \frac{1}{2 - \left(\frac{2}{|d|}\right)} \cdot \sum_{0 < a < f_K/2} \left(\frac{a}{|d|}\right)$$

$$\gcd(a, f_K) = 1$$

(A similar but slightly more complicated result holds if  $f_K$  is even [4, p. 346].) Thus if  $K = \mathbf{Q}(\sqrt{-3 \cdot 5})$ , then  $f_K = 15$  by 6.1 and  $(2/|d|) = (2/15) = (2/3)(2/5) = 1$ . Therefore  $\#(\mathcal{E}) = (1/15) + (2/15) + (4/15) + (7/15) = 1 + 1 + 1 - 1 = 2$  and so  $K' = K$ .

THEOREM 7.18. (Decomposition, Takagi, 1920). *Let  $\mathfrak{p}$  be a defining modulus*

of  $L/K$  Let  $\mathfrak{p}$  be a finite  $K$ -prime such that  $\mathfrak{p} \nmid m$ . Let  $\bar{\mathfrak{p}} = \mathfrak{p}R_m \in C_m$ . Then the order of  $\bar{\mathfrak{p}}I_{L/K,m}$  in  $C_m/I_{L/K,m}$  is  $f$ , the residue class degree of  $\mathfrak{p}$ .

**COROLLARY 7.19.** *Let  $\mathfrak{p}$  be a finite  $K$ -prime. Then  $\mathfrak{p} \in \text{Spl}(\tilde{K}/K)$  if and only if  $\mathfrak{p} \in (K^*)$ .*

**PROOF.** By 7.18,  $\mathfrak{p} \in \text{Spl}(\tilde{K}/K)$  if and only if  $\bar{\mathfrak{p}} \in I_{\tilde{K}/K,(1)} = \{1\}$  if and only if  $\bar{\mathfrak{p}} = R_{(1)} = (K^*)$ .

**COROLLARY 7.20.** *Let  $L/K$  be abelian and  $\mathfrak{p}$  a finite  $K$ -prime. Then  $\mathfrak{p} \in \text{Spl}(L/K)$  if and only if  $\mathfrak{p} \nmid f_{L/K}$  and  $(L/K/\mathfrak{p}) = 1$ .*

**PROOF.** By 7.15 and 7.18,  $\mathfrak{p} \in \text{Spl}(L/K)$  if and only if  $\mathfrak{p} \nmid f_{L/K}$  and  $\mathfrak{p} \in I_{K/L, f_{L/K}}$ , which is true by 7.11 if and only if  $\mathfrak{p} \nmid f_{L/G}$  and  $(L/K/\mathfrak{p}) = 1$ .

**DEFINITION.** Let  $m$  be a  $K$ -modulus. If  $\alpha, \beta \in A_m$  then  $\alpha \equiv \beta \pmod m$  means  $\alpha\beta^{-1}$  is a principle fractional ideal with generator  $\alpha$  such that  $\alpha \equiv 1 \pmod m$ .

**DEFINITION.** Let  $L/K$  be a Galois extension.  $\text{Spl}(L/K)$  is given by congruence conditions if there exists a  $K$ -modulus  $m$  and  $\alpha_1, \dots, \alpha_r \in A_m$  such that  $\mathfrak{p} \in \text{Spl}(L/K)$  if and only if  $\mathfrak{p} \equiv \alpha_i \pmod m$  for some  $i$  with finitely many exceptions (i.e., there are a finite number of  $\mathfrak{p}$ 's such that  $\mathfrak{p} \in \text{Spl}(L/K)$  and yet  $\mathfrak{p} \not\equiv \alpha_i \pmod m$  for any  $i$ ).

Let  $L/K$  be abelian with defining modulus  $m$  and let  $I_{L/K,m} = \{\alpha_1 R_m, \dots, \alpha_r R_m\}$ . With finitely many exceptions, by 7.18,  $\mathfrak{p} \in \text{Spl}(L/K)$  if and only if  $\mathfrak{p} \in I_{L/K,m}$  if and only if  $\mathfrak{p} \equiv \alpha_i \pmod m$  for some  $i$ . (If  $\mathfrak{p} \nmid f_{L/K}$  and  $\mathfrak{p} \mid m$ , then  $\mathfrak{p}$  could be an exception.) So if  $L/K$  is abelian then  $\text{Spl}(L/K)$  is given by congruence conditions. But the converse is also true.

**THEOREM 7.21.** *Let  $L/K$  be a Galois extension and let  $\text{Spl}(L/K)$  be given by congruence conditions mod  $m$ . Then  $L$  is a subfield of  $K(R_m)$  and so  $L/K$  is abelian.*

**PROOF.** Let  $\text{Spl}(L/K) = \{\mathfrak{p} \mid \mathfrak{p} \equiv \alpha_i \pmod m \text{ for some } i\}$  with finitely many exceptions. On the other hand we know that by 7.18  $\text{Spl}(K(R_m)/K) = \{\mathfrak{p} \mid \mathfrak{p} \in R_m\}$  with finitely many exceptions. Now suppose  $\alpha_i \notin R_m$  for all  $i$ . Then

$$\{\mathfrak{p} \mid \mathfrak{p} \equiv \alpha_i \pmod m\} \cap \{\mathfrak{p} \mid \mathfrak{p} \in R_m\}$$

is empty. Therefore

$$\text{Spl}(L \cdot K(R_m)/K) = \text{Spl}(L/K) \cap \text{Spl}(K(R_m)/K)$$

has only a finite number of elements which contradicts the following theorem.

**THEOREM 7.22.** *Let  $M/K$  be a Galois extension. Then*

$$d(\text{Spl}(M/K)) = \frac{1}{[M:K]}.$$

Therefore for some  $i, \alpha_i \in R_m$  and so  $\text{Spl}(K(R_m)/K \subset \text{Spl}(L/K)$  with finitely many exceptions. By Theorem 3.1,  $L \subset K(R_m)$ .

REMARK. As Remark 6.1 illustrates, Artin's law of reciprocity is the solution for abelian extensions to Hilbert's 9-th problem (generalize Gauss' law of quadratic reciprocity). Of course, the problem still remains of finding a reciprocity law for non-abelian extensions  $L/K$ —a law which will characterize those  $K$ -primes  $\mathfrak{p}$  which split completely in  $L$  as the law of quadratic reciprocity does for quadratic fields (Example 4.1) and Artin's law of reciprocity does for arbitrary abelian extensions (Corollary 7.20). However, Theorem 7.21 tells us that congruence conditions will not in general characterize  $\text{Spl}(L/K)$ . Something else is needed. Indeed, the development of a nonabelian class field theory is certainly one of the major problems in mathematics and such a reciprocity law is desired as a key constituent in such a theory.

Let  $L/K$  be a Galois extension. If  $\alpha \in L$ , let  $\text{Tr}_{L/K} \alpha = \sum_{\sigma \in G} \sigma \alpha$  where  $G = G(L/K)$ . Let

$$\mathcal{O}'_L = \{\alpha \in L \mid \text{Tr}_{L/K}(\alpha \mathcal{O}_L) \subset \mathcal{O}_K\}.$$

Then it can be shown that  $\mathcal{O}'_L \in A_L$  is a fractional ideal and  $(\mathcal{O}'_L)^{-1}$  is an ideal in  $\mathcal{O}_L$ .

DEFINITION. The different of  $L/K$  is  $D_{L/K} = (\mathcal{O}'_L)^{-1}$ . The discriminant of  $L/K$  is  $d_{L/K} = N_{L/K}(D_{L/K})$ .

Let  $\hat{C}_m$  be the set of characters on  $C_m$ . If  $\mathfrak{m}$  is a defining modulus of  $L/K$ , let

$$X_{L/K, \mathfrak{m}} = \{\chi \in C_m \mid \chi(I_{L/K, \mathfrak{m}}) = 1\},$$

the character group of  $L/K \bmod \mathfrak{m}$ . If  $\chi \in X_{L/K, \mathfrak{m}}$ , let  $I_\chi = \text{Ker } \chi$ . Let  $L_\chi$  be the subfield of  $K(R_m)$  fixed by  $I_\chi$ . Then we have the following picture.

$$C_m \left( \begin{array}{c} K(R_m) \\ | \\ L \\ | \\ L_\chi \\ | \\ K \end{array} \right)_{I_{L/K, \mathfrak{m}}} I_\chi$$

Let  $f_\chi$  be the conductor of  $L_\chi/K$  and let  $(f_\chi)_0$  be the finite part of  $f_\chi$ .

THEOREM 7.23. (Conductor-Discriminant Formula). Let  $\mathfrak{m}$  be a defining modulus of  $L/K$ . Then

$$f_{L/K} = \text{lcm}\{f_\chi | \chi \in X_{L/K,m}\}$$

and

$$d_{L/K} = \prod_{\chi \in X_{L/K,m}} (f_\chi)_0.$$

**THEOREM 7.24. (Norm Limitation Theorem).** *Let  $L/K$  be a finite Galois extension. Let  $L_0$  be the maximal abelian extension of  $K$  in  $L$ . Then*

$$N_{L/K}C_{L,m} = N_{L_0/K}C_{L_0,m}$$

where  $m$  is a defining modulus of  $L_0/K$ .

**THEOREM 7.25. (Translation Theorem).** *Let  $L/K$  be a finite abelian extension. Let  $L$  be the class field of  $I_{L/K,m}$  where  $m$  is a defining modulus of  $L/K$ . Let  $F$  be an arbitrary extension of  $K$ . Then  $L \cdot F$  is the class field over  $F$  of  $\{c \in C_{F,m} | N_{F/K} c \in I_{L/K,m}\}$ .*

We end the statements of class field theory with Furtwangler’s result of 1930 (Hilbert’s conjecture of 1898–1899) which he was able to prove after Artin had reduced the problem (via his reciprocity law) to purely group theoretic considerations.

**THEOREM 7.26. (Principal Ideal Theorem).** *Each fractional ideal  $\mathfrak{a} \in A_K$  is principal in  $\tilde{K}$ , i.e.,  $\alpha \mathcal{O}_{\tilde{K}} = \mathfrak{a} \mathcal{O}_{\tilde{K}}$  where  $\alpha \in \tilde{K}$ .*

This does not say that each ideal in  $\mathcal{O}_{\tilde{K}}$  is principal. Instead, “the class tower problem” arises which was posed by Furtwangler and restated as a major unsolved problem in Hasse’s Bericht (1926) [9]. Let  $K_0 = K$  and let  $K_i$  be the Hilbert class field of  $K_{i-1}$  for  $i \geq 1$ . Does there exist a  $j$  such that  $K_j = K_{j-1}$  or is the class field tower  $K_0 \subset K_1 \subset K_2 \subset \dots$  infinite? If  $K_j = K_{j-1}$ , then the ideal class group of  $K_{j-1}$  is 1 and so each ideal of  $K_{j-1}$  is principal. Golod and Shafarevich in 1964 showed there exist infinite class field towers [8]. In particular, any imaginary quadratic field  $Q(\sqrt{d})$  where at least six primes divide  $d$  has an infinite class field tower [5, pp. 231–249].

An appropriate conclusion would be an application to a diophantine problem which we now present. Thanks go to George Cooke for the ideas here.

Given a prime  $p$  do there exist  $x, y \in \mathbf{Z}$  such that

$$p = x^2 + xy + 4y^2$$

has a solution? We will show that there is a solution if and only if  $p \equiv 1 \pmod{15}$  or  $p \equiv 4 \pmod{15}$ .

Let  $K = \mathbf{Q}(\sqrt{-15})$ . Then it can be shown that 1 and  $1 + \sqrt{-15}/2$  is an integral base of  $\mathcal{O}_K$ , i.e.,

$$\mathcal{O}_K = \mathbf{Z} \oplus \mathbf{Z} \left( \frac{1 + \sqrt{-15}}{2} \right).$$

Also

$$\begin{aligned} x^2 + xy + 4y^2 &= \left( x + \frac{1 + \sqrt{-15}}{2} y \right) \left( x + \frac{1 - \sqrt{-15}}{2} y \right) \\ &= N_{K/\mathbf{Q}} \left( x + \frac{1 + \sqrt{-15}}{2} y \right). \end{aligned}$$

Thus the question is: For which  $p$  is there an element of  $\mathcal{O}_K$  whose norm is  $p$ ? To answer this we have the following general definitions and theorem.

DEFINITION. Let  $K/\mathbf{Q}$  be a Galois extension of degree  $n$ . Let  $\alpha_1, \dots, \alpha_n$  be an integral base of  $K$ . The *norm form associated with  $K$*  (which is independent of the integral basis chosen) is

$$F_K(x_1, \dots, x_n) = N_{K/\mathbf{Q}} \left( \sum_{i=1}^n x_i \alpha_i \right).$$

The form  $F_K$  is homogeneous of degree  $n$  with coefficients in  $\mathbf{Z}$ . (Concerning the following theorem it can be shown that  $\bar{K}/\mathbf{Q}$  is a Galois extension and so  $\text{Spl}(\bar{K}/\mathbf{Q})$  makes sense as we have defined it).

THEOREM 7.27. *Let  $K$  be an imaginary abelian extension of  $\mathbf{Q}$ . Suppose  $p \nmid f_K$ . Let  $F_K(x_1, \dots, x_n)$  be the norm form associated with  $K$ . Then  $p = F_K(x_1, \dots, x_n)$  has a solution with  $x_i \in \mathbf{Z}$  if and only if  $p \in \text{Spl}(\bar{K}/\mathbf{Q})$ .*

PROOF. If  $\sigma$  is complex conjugation, then we can write  $G(K/\mathbf{Q}) = \langle \tau_1, \dots, \tau_{n/2}, \sigma\tau_1, \dots, \sigma\tau_{n/2} \rangle$ . Let  $\alpha \in K^*$ . Then

$$N_{K/\mathbf{Q}} \alpha = \prod_{i=1}^{n/2} (\tau_i \alpha) \cdot \sigma(\tau_i \alpha) > 0.$$

Thus  $p = F_K(x_1, \dots, x_n)$  has a solution if and only if  $p = N_{K/\mathbf{Q}} \alpha$  for some  $\alpha \in \mathcal{O}_K$  if and only if  $(p) = (N_{K/\mathbf{Q}} \alpha)$  if and only if there is a principal prime ideal  $\mathfrak{p}$  of  $K$  having norm  $p$ . On the other hand  $p \in \text{Spl}(K/\mathbf{Q})$  if and only if there is a  $K$ -prime  $\mathfrak{p}$  having norm  $p$ ; and  $\mathfrak{p} \in \text{Spl}(\bar{K}/K)$  if and only if  $\mathfrak{p}$  is principal by 7.19.

Returning to the original problem it follows that if  $K = \mathbf{Q}(\sqrt{-15})$  and  $p \nmid f_K = 15$  by Theorem 6.1, then  $p = x^2 + xy + 4y^2$  has a solution by Theorem 7.27 if and only if  $p \in \text{Spl}(\bar{K}/\mathbf{Q})$ , which is equivalent to  $p \in \text{Spl}(\mathbf{Q}(\sqrt{-3}, \sqrt{5})/\mathbf{Q})$  by Example 7.1, which in turn by Example 6.4 is equivalent to  $p \equiv 1 \pmod{15}$  or  $p \equiv 4 \pmod{15}$ . Now suppose  $p = 3$ . Since  $3 \notin I_{\mathbf{Q}(\sqrt{5})/\mathbf{Q}, (5)} = G(\mathbf{Q}_5/\mathbf{Q}(\sqrt{5})) = \langle 3^2 \pmod{5} \rangle$ , the residue class degree

of 3 for  $\mathbf{Q}(\sqrt{5})/\mathbf{Q}$  is 2 by Theorem 6.8. Since 3 does not ramify in  $\mathbf{Q}(\sqrt{5})$ , 3 ramifies in  $\mathbf{Q}(\sqrt{-3}, \sqrt{5}) = \tilde{K}$  with ramification index  $e = 2$ . Therefore, the residue class degree of 3 for  $\mathbf{Q}(\sqrt{-3}, \sqrt{5})/\mathbf{Q}$  is  $f = 2$ . Since  $\text{egf} = [\tilde{K} : \mathbf{Q}] = 4$ , we get  $g = 1$  and so if  $\mathfrak{p}$  is a  $K$ -prime and  $\mathfrak{p}|p$ , then  $\mathfrak{p} \notin \text{Spl}(\tilde{K}/K)$ . Therefore  $\mathfrak{p} \notin (K^*)$ . Since  $N_{K/\mathbf{Q}} \mathfrak{p} = (3)$ ,  $3 = x^2 + xy + 4y^2$  does not have a solution. A similar argument shows that  $5 = x^2 + xy + 4y^2$  does not have a solution. (Also note that if  $5 = x^2 + xy + 4y^2 = [x + xy + (y/2)^2] - (y/2)^2 + 4y^2$  has a solution, then  $20 = (2x + y)^2 + 15y^2$  has a solution which is not the case.)

**8. Post World War II class field theory.** (Presentation of class field theory using ideles can be found in [5], [6], [7], and [14].) Suppose  $I_{L_1/K, m_1}$  and  $I_{L_2/K, m_2}$  are given and we want to know if  $L_1 \subset L_2$ . We cannot directly apply the ordering theorem because we do not have a common defining modulus. Instead, the following ploy is used. Let  $I_{L_1/K, m_1} = H_{m_1}/R_{m_1}$  where  $H_{m_1}$  is a subgroup of  $A_{m_1}$  containing  $R_{m_1}$ . The following proposition can be shown.

**PROPOSITION.** *Let  $m_1$  be a defining modulus of  $L/K$ . Let  $m_1|m$ . Let  $I_{L/K, m_1} = H_{m_1}/R_{m_1}$ . Then*

$$I_{L/K, m} = (H_{m_1} \cap A_m)/R_m.$$

So, if  $m_1|m$  and  $m_2|m$ , then by 7.14  $L_1 \supset L_2$  if and only if  $I_{L_1/K, m} \subset I_{L_2/K, m}$  which is equivalent to  $H_{m_1} \cap A_m \subset H_{m_2} \cap A_m$  where  $I_{L_2/K, m_2} = H_{m_2}/R_{m_2}$ . Thus in order to compare  $L_1$  and  $L_2$  we have to compare  $H_{m_1} \cap A_m$  and  $H_{m_2} \cap A_m$ . Such considerations are aesthetically unpleasing. The modern approach does away with the defining moduli in the statements of most of the theorems. The price that one pays for this convenience is charged when  $C_m$  and  $I_{L/K, m}$ , which are finite groups, are replaced by infinite groups  $C'_K$  and  $I'_{L/K}$ .

Let  $K^{ab}$  be the maximal abelian extension of  $K$ , an infinite extension of  $K$ . Looking at the following picture and realizing that all abelian

$$I_{L/K, m} \left( \begin{array}{c} K^{ab} \\ | \\ K(R_m) \\ | \\ L \\ | \\ K \end{array} \right) C_m$$

extensions of  $K$  are subfields of ray class fields suggests replacing  $\{C_m|m \text{ is a } K\text{-modulus}\}$  or, more precisely,  $\varinjlim C_m \cong G(K^{ab}/K)$  by something else isomorphic to  $G(K^{ab}/K)$  and  $\{I_{L/K, m}|m \text{ is a defining modulus of } L/K\}$  or, more precisely,  $\varinjlim I_{L/K, m} \cong G(K^{ab}/L)$  (where  $\varinjlim$  is taken

over  $m$  as  $m$  runs through the defining moduli of  $L/K$ ) by something else isomorphic to  $G(K^{ab}/L)$ .

Let  $K_{\mathfrak{p}}$  be the completion of  $K$  at  $\mathfrak{p}$  and  $K_{\mathfrak{p}}^* = K_{\mathfrak{p}} - \{0\}$ . If  $\mathfrak{p}$  is finite,  $K_{\mathfrak{p}}$  is the completion of  $K$  with respect to the valuation  $|\alpha| = \rho^{\text{ord}_{\mathfrak{p}}\alpha}$  where  $0 < \rho < 1$ , and if  $\alpha \mathcal{O}_K = \prod_{\mathfrak{p}} \mathfrak{p}^{\alpha(\mathfrak{p})}$ , then  $\text{ord}_{\mathfrak{p}}\alpha = a(\mathfrak{p})$ . If  $\mathfrak{p}_{\sigma} = \mathfrak{p}$  is infinite, then  $K_{\mathfrak{p}}$  is the completion of  $K$  with respect to  $|\alpha|_{\mathfrak{p}} = |\sigma\alpha|$  where  $|\cdot|$  denotes ordinary absolute value on  $\mathbb{C}$ . Let  $U_{\mathfrak{p}}$  be the unit group of  $K_{\mathfrak{p}}$  if  $\mathfrak{p}$  is finite, and  $K_{\mathfrak{p}}^*$  if  $\mathfrak{p}$  is infinite. Let  $S$  be any finite set of  $K$ -primes. Let

$$J_K^S = \prod_{\mathfrak{p} \in S} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p} \notin S} U_{\mathfrak{p}} \subset \prod_{\mathfrak{p}} K_{\mathfrak{p}}^*.$$

Let  $J_K = \bigcup_S J_K^S$  where  $S$  runs through all finite sets of  $K$ -primes.  $J_K$  is called the idele (from ideale elemente) group. If  $j \in J_K$ , let  $j_{\mathfrak{p}} \in K_{\mathfrak{p}}^*$  be the  $\mathfrak{p}$ -component of  $j$ . There is a natural embedding  $K^* \rightarrow J_K$ , i.e.,  $\alpha \rightarrow j$  where  $j_{\mathfrak{p}} = \alpha$  for all  $\mathfrak{p}$ . So think of  $K^*$  as a subset of  $J_K$ . Let  $C_K = J_K/K^*$ , the idele class group.

Let  $L$  be a Galois extension of  $K$ . There is a natural embedding  $J_K \hookrightarrow J_L$ , i.e.,  $j \rightarrow \hat{j}$  where  $\hat{j}_{\mathfrak{p}} = j_{\mathfrak{p}}$  and  $\mathfrak{p}$  is divisible by  $\mathfrak{P}$ . Think “ $J_K \subset J_L$ ”. If  $\sigma \in G = G(L/K)$ , there is a unique topological isomorphism also denoted  $\sigma$  mapping  $L_{\sigma^{-1}\mathfrak{P}}$  onto  $L_{\mathfrak{P}}$  which extends  $\sigma \in G(L/K)$ . ( $|\cdot|_{\sigma^{-1}\mathfrak{P}}$  is defined via  $|\cdot|_{\mathfrak{P}}$  by mapping  $\alpha \in L$  to  $\sigma\alpha$  and then applying  $|\cdot|_{\mathfrak{P}}$ , i.e.,  $|\alpha|_{\sigma^{-1}\mathfrak{P}} = |\sigma\alpha|_{\mathfrak{P}}$ . So if  $\mathfrak{P} = \mathfrak{P}_{\tau}$  is infinite, then  $|\alpha|_{\sigma^{-1}\mathfrak{P}_{\tau}} = |\sigma\alpha|_{\mathfrak{P}_{\tau}} = |\tau\sigma(\alpha)|$ , i.e.,  $\sigma^{-1}\mathfrak{P}_{\tau} = \mathfrak{P}_{\tau\sigma}$  gives the action of  $\sigma^{-1}$  on the infinite prime  $\mathfrak{P}_{\tau}$ .) To turn  $J_L$  into a  $G$ -module we define the  $\mathfrak{P}$ -component of  $\sigma j$  where  $j \in J_L$  as follows  $(\sigma j)_{\mathfrak{P}} = \sigma(j_{\sigma^{-1}\mathfrak{P}})$ .

One also naturally embeds  $C_K$  in  $C_L$  via  $jK^* \rightarrow jL^*$  where  $j \in J_K$ . Think “ $C_K \subset C_L$ ”. Make  $C_L$  a  $G$ -module via  $\sigma(jL^*) = \sigma j \cdot L^*$  and define the norm map  $N_{L/K}: C_L \rightarrow C_K$  via

$$N_{L/K}(jL^*) = \prod_{\sigma \in G} \sigma(jL^*).$$

TOPOLOGY. Let  $K_{\mathfrak{p}}^*$  and  $U_{\mathfrak{p}}$  have the valuation topology. Then

$$J_K^S = \prod_{\mathfrak{p} \in S} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p} \notin S} U_{\mathfrak{p}}$$

is a topological group with the product topology. So we get in a canonical way (since  $S \subset S'$  implies  $J_K^S \subset J_K^{S'}$ ) a topology on  $J_K = \bigcup_S J_K^S$ , the idele topology. (A set is open if and only if its intersection with  $J_K^S$  is open in  $J_K^S$  for all  $S$ .) A neighborhood basis of 1 in  $J_K$  is, in fact,

$$\prod_{\mathfrak{p} \in S} W_{\mathfrak{p}} \times \prod_{\mathfrak{p} \notin S} U_{\mathfrak{p}}$$

where  $W_{\mathfrak{p}}$  runs through a neighborhood basis of 1 in  $K_{\mathfrak{p}}^*$  and  $S$  runs through all finite sets of  $K$ -primes. It turns out that  $K^*$  is a closed subgroup of the topological group  $J_K$  and so  $C_K = J_K/K^*$  is a topological group.

Let  $D_K$  be the connected component of 1 in the topological group  $C_K$ . It can be shown that  $D_K$  is characterized algebraically as the set of all infinitely divisible elements of  $C_K$ , i.e.,

$$D_K = \bigcap_{n=1}^{\infty} C_K^n,$$

i.e., if  $a \in D_K$ , then given any positive integer  $n$  there is a  $b \in C_L$  such that  $a = b^n$ . Also  $D_K$  can be characterized externally via  $D_K = \bigcap_L N_{L/K} C_L$  where  $L$  runs through all finite abelian extensions of  $K$ . It can be shown that  $D_K$  is a closed subgroup of  $C_K$  and so  $C'_K = C_K/D_K$  is a topological group. It can also be shown that  $G(K^{ab}/K) \cong C'_K$ . (This is true for a finite extension  $K$  of  $\mathbf{Q}$ , not for function fields.) So  $C'_K$  will replace  $\{C_m | m \text{ is a } K\text{-modulus}\}$ .

Since  $N_{L/K} D_L \subset D_K$ , we can extend  $N_{L/K}$  to  $N_{L/K}: C'_L \rightarrow C'_K$  where  $N_{L/K}(aD_L) = N_{L/K} a \cdot D_K$ . Let  $I'_{L/K} = N_{L/K} C'_L$ . It can be shown that  $G(K^{ab}/L) \cong I'_{L/K}$  and so  $I'_{L/K}$  will replace  $\{I_{L/K,m} | m \text{ is a defining modulus of } L/K\}$ .

If  $L$  is a finite abelian extension of  $K$ , then  $I'_{L/K} = N_{L/K} C'_L$  is an open subgroup of  $C'_K$ . On the other hand we have the following theorem.

**THEOREM 8.1. (Existence Theorem).** *Let  $I'$  be an open subgroup of  $C'_K$ . Then there exists a unique finite abelian extension  $L$  of  $K$  such that  $I'_{L/K} = N_{L/K} C'_L = I'$ .*

**DEFINITION.** Let  $I'$  be an open subgroup of  $C'_K$  and  $L$  a finite abelian extension of  $K$ . Then  $L$  is the *class field of  $I'$*  if  $N_{L/K} C'_L = I'$ .

**DEFINITION.** Let  $j, i \in J_K$  and let  $m$  be a  $K$ -modulus. Then  $j \equiv i \pmod m$  means  $\text{ord}_p(ji^{-1} - 1)_p \geq \text{ord}_p m$  for all finite  $p$  occurring in  $m$  and  $(ji^{-1})_p \in K_p^{*2}$  for all infinite  $p$  occurring in  $m$ . Write  $j \equiv i \pmod m$  if it is also true that  $(ji^{-1})_p \in U_p$  if  $p \nmid m$ .

Let  $J_m = \{j \in J_K | j \equiv 1 \pmod m\}$ . Let  $I_m = J_m \cdot K^*/K^* \subset C_K$ .

**DEFINITION.** Let  $L$  be a finite abelian extension of  $K$ . Then  $m$  is a *defining modulus* of  $L/K$  if  $I_m \subset N_{L/K} C_L$ .

**DEFINITION.** Let  $m$  be a defining modulus of  $L/K$ . The *global norm residue symbol*

$$(\ , L/K): J_K \rightarrow G(L/K)$$

is defined as follows. Let  $j \in J_K$ . Then there exists  $\alpha \in K^*$  such that  $j \equiv \alpha \pmod m$ . (This follows from a "glorified" Chinese Remainder Theorem.) Define  $(j, L/K)$  via  $(j, L/K) = \prod \{(L/K/p)^n | n = \text{ord}(j\alpha^{-1})_p, p \text{ finite } K\text{-prime, } p \nmid m\}$ .



This is well defined and it can be shown easily from this definition that if  $\beta \in K^*$ , then  $(\beta, L/K) = 1$ . Thus we can define  $(\cdot, L/K)$  on  $C_K$  via  $(jK^*, L/K) = (j, L/K)$ . It can also be shown that if  $jK^* \in D_K$ , then  $(jK^*, L/K) = 1$ . So we can define  $(\cdot, L/K)$  on  $C'_K = C_K/D_K$  via  $(\bar{j}, L/K) = (j, L/K)$  where  $\bar{j} = jK^* \cdot D_K \in C'_K$ . Artin's law of reciprocity now reads as follows.

**THEOREM 8.2.** (Artin's law of reciprocity). *Let  $L$  be a finite abelian extension of  $K$ . Then*

$$1 \rightarrow N_{L/K}C'_L = I'_{L/K} \rightarrow C'_K \xrightarrow{(\cdot, L/K)} G(L/K) \rightarrow 1$$

is exact.

Define  $(\cdot, K): C'_K \rightarrow G(K^{ab}/K)$  via  $(\bar{j}, K) = \varinjlim (\bar{j}, L/K) \in \varinjlim G(L/K) = G(K^{ab}/K)$  where  $\varinjlim$  is taken over  $L$  as  $L$  runs over all finite abelian extensions of  $K$ .

It is not difficult to show using 8.2 that  $(\cdot, K)$  gives an isomorphism from  $C'_K$  into  $G(K^{ab}/K)$ . This isomorphism is onto if  $K$  is a finite extension of  $\mathbb{Q}$  which we are assuming. Furthermore  $(\cdot, K)$  gives an isomorphism from  $N_{L/K}C'_L$  onto  $G(K^{ab}/L)$  and so we have the following Galois interpretation for the objects  $C'_K$  and  $I'_{L/K}$ .

$$I'_{L/K} = N_{L/K}C'_L \left( \begin{array}{c} K^{ab} \\ | \\ L \\ | \\ K \end{array} \right) C'_K$$

It can be shown that  $D_K = \bigcap_m I_m$  where  $m$  runs over all  $K$ -moduli. So we can let  $I'_m = I_m/D_K \subset C'_K$ . Let  $m$  be a  $K$ -modulus. Then it can be shown that  $I'_{K(R_m)/K} = N_{K(R_m)/K}C'_{K(R_m)} = I'_m$ . If  $m$  is a defining modulus of  $L/K$ , then  $I'_m \subset I'_{L/K}$  and we have the following picture

$$C'_K \left( \begin{array}{c} I'_m \left( \begin{array}{c} K^{ab} \\ | \\ K(R_m) \\ | \\ L \\ | \\ K \end{array} \right) \\ | \\ I'_{L/K} \end{array} \right)$$

**EXAMPLE 8.1.** The following is a computation of  $(j, L/K)$  when  $K = \mathbb{Q}$  and  $L = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$ . Let  $j$  be given by  $j_3 = 3^2 \cdot 2, j_5 = 11, j_{13} = 13, j_p = 1$  if  $p \neq 3, 13$  or  $5$ . (In particular  $j_{p_\infty} = 1$ .) Since  $\mathfrak{f}_{L/K} = (15)p_\infty$ , the first step in computing  $(j, L/\mathbb{Q})$  is to find an  $\alpha \in \mathbb{Q}^*$  such that  $j \equiv \alpha \pmod{(15)p_\infty}$ , i.e., find an  $\alpha \in \mathbb{Q}^*$  such that

$$\text{ord}_3(j\alpha^{-1} - 1)_3 = \text{ord}_3(3^2 \cdot 2\alpha^{-1} - 1) \geq \text{ord}_3(15)p_\infty = 1$$

and  $\text{ord}_5(11\alpha^{-1} - 1) \geq 1$  and  $(j\alpha^{-1})_{p_\infty} = \alpha^{-1} \in \mathbf{Q}_{p_\infty}^{*2}$  i.e.,  $\alpha > 0$ . Because of the first inequality  $\alpha = 3^2x$  where  $x \in \mathbf{Z}$ . So we must find an  $x \in \mathbf{Z}$  such that  $2 \equiv x \pmod 3$ ,  $1 \equiv 11 \equiv 9x \equiv 4x \pmod 5$  and  $x > 0$ . A solution is  $x = 14$ . Thus let  $\alpha = 3^2 \cdot 2 \cdot 7$ . Then

$$\begin{aligned} (j, L/Q) &= \left(\frac{L}{13}\right)^{\text{ord}_{13}(j\alpha^{-1})_{13}} \left(\frac{L}{2}\right)^{\text{ord}_2(j\alpha^{-1})_2} \left(\frac{L}{7}\right)^{\text{ord}_7(j\alpha^{-1})_7} \\ &= \left(\frac{L}{13}\right) \left(\frac{L}{2}\right)^{-1} \left(\frac{L}{7}\right)^{-1} \end{aligned}$$

where  $(L/p)$  is given before 6.3. (One can easily show for example that  $(L/2)^{-1} = (L/2)$  sends  $\sqrt{-3}$  to  $-\sqrt{-3}$  and  $\sqrt{5}$  to  $-\sqrt{5}$  and thus one obtains a more concrete realization of  $(L/2)$ .)

For those familiar with cohomology we present here a definition of  $(j, L/K)$  without using a defining modulus. Let  $G = G(L/K)$ . Let  $u_{L/K} \in H^2(G, C_L) = A/B$  where  $A = \{x: G \times G \rightarrow C_L | x(\sigma\tau, \rho) + x(\sigma, \tau) = \sigma x(\tau, \rho) + x(\sigma, \tau\rho)\}$  and  $B = \{x: G \times G \rightarrow C_L | x(\sigma, \tau) = \sigma y(\tau) - y(\sigma\tau) + y(\sigma)$  for some  $y: G \rightarrow C_L\}$ . Let  $u_{L/K} \cup$  denote the map from  $G$  into  $C_K/N_{L/K}C_L$  which acts on  $\sigma \in G$  via

$$(u_{L/K} \cup)\sigma = \sum_{\tau \in G} u_{L/K}(\tau, \sigma) \cdot N_{L/K}C_L.$$

(This map comes from the cup product given in the following picture

$$H^2(G, C_L) \times H^{-2}(G, \mathbf{Z}) \xrightarrow{\cup} H^0(G, C_L) = C_K/N_{L/K}C_L$$

via

$$(u_{L/K}, \bar{\sigma}) \xrightarrow{\cup} u_{L/K} \cup \bar{\sigma}$$

where  $\bar{\sigma}$  is the image of  $\sigma$  under a canonical isomorphism from  $G$  onto  $H^{-2}(G, \mathbf{Z})$ .) There is a canonical way of picking  $u_{L/K}$  which makes a

$$G \xrightarrow{u_{L/K} \cup} C_K/N_{L/K}C_L$$

bijection. This canonically chosen  $u_{L/K}$  is called the *fundamental class*. Appendix I explains how  $u_{L/K}$  is chosen. If  $u_{L/K}$  is the fundamental class,  $(, L/K): C_K \rightarrow G$  is given by the inverse of the map  $u_{L/K} \cup$ . This in turn determines the map  $(, L/K): J_K \rightarrow G$  via  $(j, L/K) = (jK^*, L/K)$ .

Returning to the statement of results, the Galois interpretation afforded by Artin's law of reciprocity gives the following theorem.

**THEOREM 8.3. (Ordering Theorem).** *Let  $L_1$  and  $L_2$  be finite abelian extensions of  $K$ . Then  $L_1 \subset L_2$  if and only if  $I'_{L_1/K} \supset I'_{L_2/K}$ .*

If  $\mathfrak{p}$  is a prime ideal let  $j(\mathfrak{p})$  be the element of  $J_K$  where the  $q$ -th component is given by

$$j(\mathfrak{p})_q = \begin{cases} \pi & \text{if } q = \mathfrak{p} \\ 1 & \text{if } q \neq \mathfrak{p} \end{cases}$$

where  $q$  is a  $K$ -prime and  $\pi$  is a prime of  $K_{\mathfrak{p}}$ . Let  $\overline{j(\mathfrak{p})}$  be the corresponding element of  $C'_K$ , i.e.,  $\overline{j(\mathfrak{p})} = j(\mathfrak{p})K^* \cdot D_K$ .

**THEOREM 8.4. (Decomposition Theorem).** *Let  $L$  be a finite abelian extension of  $K$ . Suppose  $\mathfrak{p}$  is a prime ideal of  $K$  which does not ramify in  $L$ . Then the residue class degree  $f$  of  $\mathfrak{p}$  is the order of  $\overline{j(\mathfrak{p})}I'_{L/K}$  in  $C'_K$ .*

**DEFINITION.** The conductor  $\mathfrak{f}_{L/K}$  of  $L/K$  is the greatest common divisor of the defining moduli of  $L/K$ .

**THEOREM 8.5. (Conductor-Ramification Theorem).** *A  $K$ -prime  $\mathfrak{p}$  ramifies in  $L$  if and only if  $\mathfrak{p} | \mathfrak{f}_{L/K}$ .*

### APPENDIX I

**The determination of the fundamental class  $u_{L/K}$ .** (The cohomology groups here are all Tate cohomology groups.) Let  $K$  be a finite extension of  $\mathbf{Q}$  and let  $L$  be a finite Galois extension of  $K$  with  $G = G(L/K)$ . We seek to canonically define a bijection

$$\text{inv}_{L/K}: H^2(G, C_L) \rightarrow \frac{1}{n} \mathbf{Z}/\mathbf{Z}$$

called the invariant map. Once  $\text{inv}_{L/K}$  is defined, the fundamental class  $u_{L/K}$  is defined as follows.

**DEFINITION.**  $u_{L/K}$  is the unique element of  $H^2(G, C_L)$  such that  $\text{inv}_{L/K} u_{L/K} = 1/n + \mathbf{Z}$ .

**A. The local invariant map.** Let  $\mathfrak{p}$  be a  $K$ -prime and  $\mathfrak{P}$  and  $L$ -prime such that  $\mathfrak{P} | \mathfrak{p}$ . Let  $\mathcal{O}_{\mathfrak{P}}$  be the ring of integers of  $L_{\mathfrak{P}}$  and  $\mathfrak{P}$  the prime ideal of  $\mathcal{O}_{\mathfrak{P}}$ . Let  $\overline{L}_{\mathfrak{P}} = \mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$ , the residue class field of  $L_{\mathfrak{P}}$ . Define  $\overline{K}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$  similarly. Let  $q = \#(\overline{K}_{\mathfrak{p}})$ .

Suppose  $L_{\mathfrak{P}}/K_{\mathfrak{p}}$  is unramified. It can be shown that  $G(\overline{L}_{\mathfrak{P}}/\overline{K}_{\mathfrak{p}})$  is cyclic with generator  $\bar{x} \rightarrow \bar{x}^q$  where  $\bar{x} \in \overline{L}_{\mathfrak{P}}$  and also  $G(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \cong G(\overline{L}_{\mathfrak{P}}/\overline{K}_{\mathfrak{p}})$  via  $\sigma \rightarrow \bar{\sigma}$  where  $\bar{\sigma}(x + \mathfrak{P}) = \sigma x + \mathfrak{P}$  for  $x \in \mathcal{O}_{\mathfrak{P}}$ . The automorphism  $\sigma_{\mathfrak{P}} \in G(L_{\mathfrak{P}}/K_{\mathfrak{p}})$  which in  $\overline{L}_{\mathfrak{P}}$  induces  $\bar{x} \rightarrow \bar{x}^q$  is called the Frobenius automorphism of  $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ . Let  $G_{\mathfrak{P}} = G(L_{\mathfrak{P}}/K_{\mathfrak{p}})$  and let  $n_{\mathfrak{P}} = [L_{\mathfrak{P}}: K_{\mathfrak{p}}]$ . The following maps can all be shown to be bijections.

(a)  $\overline{\text{ord}}_{\mathfrak{P}}: H^2(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*) \rightarrow H^2(G_{\mathfrak{P}}; \mathbf{Z})$  where  $\overline{\text{ord}}_{\mathfrak{P}}$  is the map induced by  $\text{ord}_{\mathfrak{P}}: L_{\mathfrak{P}}^* \rightarrow \mathbf{Z}$ . (If  $L_{\mathfrak{P}}/K_{\mathfrak{p}}$  is unramified,  $\overline{\text{ord}}_{\mathfrak{P}}$  is a bijection because

$H^q(G_{\mathfrak{P}}, U_{\mathfrak{P}}) = 1$  for all  $q$  where  $U_{\mathfrak{P}}$  is the unit group of  $\mathcal{O}_{\mathfrak{P}}$ .)

(b)  $\delta: \hat{G}_{\mathfrak{P}} = H^1(G_{\mathfrak{P}}, \mathbf{Q}/\mathbf{Z}) \rightarrow H^2(G_{\mathfrak{P}}, \mathbf{Z})$  where  $\hat{G}_{\mathfrak{P}}$  is the character group of  $G_{\mathfrak{P}}$  and  $\delta$  is the “connecting homomorphism” arising from the exact sequence  $1 \rightarrow \mathbf{Z} \rightarrow \mathbf{Q} \rightarrow \mathbf{Q}/\mathbf{Z} \rightarrow 1$ . (If  $A$  is a  $G$ -module, then

$$H^1(G, A) = \frac{\{x: G \rightarrow A \mid x(\sigma\tau) = \sigma x(\tau) + x(\sigma)\}}{\{x: G \rightarrow A \mid x(\sigma) = \sigma(a) - a \text{ for some } a \in A\}}.$$

(c)  $\phi: \hat{G}_{\mathfrak{P}} \rightarrow 1/n_{\mathfrak{P}}\mathbf{Z}/\mathbf{Z}$  where  $\phi: \chi \rightarrow \chi(\sigma_{\mathfrak{P}})$ . Let  $1^{1/n_{\mathfrak{P}}}$  be a primitive  $n_{\mathfrak{P}}$ -th root of 1. Then  $\langle 1^{1/n_{\mathfrak{P}}} \rangle \cong 1/n_{\mathfrak{P}}\mathbf{Z}/\mathbf{Z}$ . So we can think of a character  $\chi$  as mapping an element of  $G_{\mathfrak{P}}$  into either  $\langle 1^{1/n_{\mathfrak{P}}} \rangle$  or  $1/n_{\mathfrak{P}}\mathbf{Z}/\mathbf{Z}$ .)

DEFINITION 1. Suppose  $L_{\mathfrak{P}}/K_p$  is unramified. Let  $\text{inv}_{\mathfrak{P}}$  be the isomorphism from  $H^2(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*)$  onto  $1/n_{\mathfrak{P}}\mathbf{Z}/\mathbf{Z}$  given by

$$\text{inv}_{\mathfrak{P}}: H^2(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*) \xrightarrow{\text{ord}_{\mathfrak{P}}} H^2(G_{\mathfrak{P}}, \mathbf{Z}) \xrightarrow{\delta^{-1}} \hat{G}_{\mathfrak{P}} \xrightarrow{\phi} \frac{1}{n_{\mathfrak{P}}}\mathbf{Z}/\mathbf{Z}.$$

Let  $N \supset M \supset K_p$  be finite Galois extensions of  $K_p$ . Let  $\tilde{G} = G(N/K_p)$ ,  $g = G(N/M)$ , and  $G = \tilde{G}/g = G(M/K_p)$ . It can be shown that  $\text{Inf}: H^2(G, M^*) \rightarrow H^2(\tilde{G}, N^*)$  is an injection and so we can think of  $H^2(G, M^*)$  as a subset of  $H^2(\tilde{G}, N^*)$ . (Let  $\mu: G \times G \rightarrow M^*$ . Define the inflation map,  $\text{Inf}: H^2(G, M^*) \rightarrow H^2(\tilde{G}, N^*)$ , by the following prescription:  $\text{Inf } \mu: \tilde{G} \times \tilde{G} \rightarrow N^*$  via  $\text{Inf } \mu(\sigma_1, \sigma_2) = \mu(\sigma_1g, \sigma_2g)$ .) If  $M$  and  $M'$  are finite Galois extensions of  $K_p$  with  $G = G(M/K_p)$ ,  $G' = G(M'/K_p)$ , then write  $H^2(G, M^*) = H^2(G', M'^*)$  if  $H^2(G, M^*)$  and  $H^2(G', M'^*)$  are the same subsets of  $H^2(\tilde{G}, N^*)$  where  $N = MM'$  and  $\tilde{G} = G(N/K_p)$ .

Let  $L_{\mathfrak{P}}/K_{\mathfrak{P}}$  be an arbitrary Galois extension. Then there exists an unramified Galois extension  $M$  of  $K_p$  such that  $[L_{\mathfrak{P}}: K_p] = [M: K_p]$ . It can be shown that when this happens then  $H^2(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*) = H^2(G, M^*)$ .

DEFINITION 2. Let  $L_{\mathfrak{P}}/K_p$  be a Galois extension. Let  $M$  be an unramified extension of  $K_p$  such that  $[L_{\mathfrak{P}}: K_p] = [M: K_p]$ . Let  $\text{inv}_{\mathfrak{P}}$  be the bijection

$$\text{inv}_{\mathfrak{P}}: H^2(G_{\mathfrak{P}}: L_{\mathfrak{P}}^*) = H^2(G, M^*) \rightarrow \frac{1}{n_{\mathfrak{P}}}\mathbf{Z}/\mathbf{Z}$$

where  $H^2(G, M^*) \rightarrow 1/n_{\mathfrak{P}}\mathbf{Z}/\mathbf{Z}$  is given in Definition 1.

**B. The global invariant map.** Since

$$H^2(G, J_L) \cong \coprod_{\mathfrak{p}} H^2(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*)$$

where  $\mathfrak{P}$  is any prime on  $L$  dividing  $\mathfrak{p}$ , if  $c \in H^2(G, J_L)$ , we can write  $c = \sum_{\mathfrak{p}} c_{\mathfrak{p}}$  where  $c_{\mathfrak{p}} \in H^2(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*)$ .

Let  $L$  be a cyclic extension of  $K$  with  $G = G(L/K)$  and let  $n = [L: K]$ .

Then it can be shown that the canonical map  $\beta: H^2(G, J_L) \rightarrow H^2(G, C_L)$  is onto.

DEFINITION 3. Let  $L$  be a finite cyclic extension of  $K$ . If  $\bar{c} \in H^2(G, C_L)$ , let  $c \in H^2(G, J_L)$  such that  $\beta(c) = \bar{c}$ . Let  $c = \sum_{\mathfrak{p}} c_{\mathfrak{p}}$ . Then the invariant map is the bijection

$$\text{inv}_{L/K}: H^2(G, C_L) \rightarrow \frac{1}{n} \mathbf{Z}/\mathbf{Z}$$

given by

$$\text{inv}_{L/K}(\bar{c}) = \sum_{\mathfrak{p}} \text{inv}_{\mathfrak{p}} c_{\mathfrak{p}}$$

where  $\mathfrak{p}$  is any prime on  $L$  dividing  $\mathfrak{p}$ .

As in the local case if  $L$  and  $L'$  are two finite Galois extensions of  $K$ , write  $H^2(G, C_L) = H^2(G', C_{L'})$  if

$$\text{Im}[\text{Inf}: H^2(G, C_L) \rightarrow H^2(\tilde{G}, C_N)] = \text{Im}[\text{Inf}: H^2(G', C_{L'}) \rightarrow H^2(\tilde{G}, C_N)]$$

where  $N = LL'$  and  $\tilde{G} = G(N/K)$ .

Let  $L$  be an arbitrary finite Galois extension of  $K$ . Then there is a cyclic extension of  $L'$  of  $K$  such that  $[L: K] = [L': K]$ . When this happens it can be shown that  $H^2(G, C_L) = H^2(G', C_{L'})$ .

DEFINITION 4. Let  $L/K$  be a finite Galois extension. Let  $L'$  be a cyclic extension of  $K$  such that  $[L: K] = [L': K]$ . Let  $\text{inv}_{L/K}$  be the bijection

$$\text{inv}_{L/K}: H^2(G, C_L) = H^2(G', C_{L'}) \rightarrow \frac{1}{n} \mathbf{Z}/\mathbf{Z}$$

where  $H^2(G', C_{L'}) \rightarrow 1/n \mathbf{Z}/\mathbf{Z}$  is given in Definition 3.

DEFINITION 5. The fundamental class is  $u_{L/K} = \text{inv}_{L/K}^{-1}(1/n + \mathbf{Z})$ .

## APPENDIX II

### Some References on subfields of the Hilbert class field.

H. Bauer, *Über die kubischer Klassenkörper zyklischer kubischer Zahlkörper*, Dissertation, Karlsruhe Universität (1970).

T. Callahan, *The 3-class group of non-abelian cubic fields*, I, II, *Mathematika* **21**(1974), 72–89, 161–188.

A. Fröhlich, *On the absolute class-group of abelian fields*, *J. London Math. Soc.* **29**(1954), 211–217.

———, *On a method for the determination of class number factors in number fields*, *Mathematika* **4**(1957), 113–121.

Y. Furuta, *The genus field and genus number in algebraic number fields*, Nagoya Math. J. **29**(1967), 281–285.

———, *Über die Zentrale Klassenzahl eines Relativ-Galoisschen Zahlkörpers*, J. Number Theory **3**(1971), 318–322.

———, *On nilpotent factors of congruent ideal class groups of Galois extensions*, Nagoya Math. J. **62**(1976), 13–28.

G. Gras, *Sur les  $\ell$ -classes d'ideaux dans les extensions cycliques relatives de degré premier  $\ell$* , Ann. Inst. Fourier, Grenoble, **3**(1973), 1–48; **4**(1973), 1–44.

H. Hasse, *Über die Klassenzahl Abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952.

———, *An algorithm for determining the structure of the 2-Sylow subgroup of the divisor class group of a quadratic number field*, Symposium Mathematica **XV**(1975), 341–352.

K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg **20**(1956), 257–258.

H. Leopoldt, *Zur Geschlechtertheorie in abelschen Zahlkörpern*, Math. Nachr. **9**(1953), 351–362.

———, *Zur Struktur der  $\ell$ -Klassengruppe galoisscher Zahlkörper*, J. Reine Angew. Math. **199**(1958), 165–174.

L. Redei and H. Reichardt, *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. **170**(1934), 69–74.

A. Yokoyama, *On class numbers of finite algebraic number fields*, Tôhoku Math. J. (2) **17**(1965), 349–357.

W. Zink, *Über die Klassengruppe einer absolut zyklischen Erweiterung*, Dissertation, Humbolt-Universität zu Berlin.

#### REFERENCES

1. W. Adams and L. Goldstein, *Introduction to Number Theory*, Prentice-Hall, Inc., Englewood Cliffs, 1976.
2. E. Artin and J. Tate, *Class Field Theory*, W. A. Benjamin, Inc., New York, 1967.
3. Borel, A., Chowla, S., Herz, C., Iwasawa, K., Serre, J.-P., *Seminar on Complex Multiplication*, Springer-Verlag, New York, 1966.
4. Z. Borevich and I. Shafarevich, *Number Theory*, Academic Press, New York, 1966.
5. J. Cassels and A. Frohlich, *Algebraic Number Theory*, Thompson Book Company, Inc., Washington, D.C., 1967.
6. L. Goldstein, *Analytic number Theory*, Prentice-Hall, Inc., Englewood Cliffs, 1971.
7. ———, *The theory of numbers*, Enciclopedia Del Novecento Instituto Della Enciclopedia Italiana Pisa, Italy.
8. E. Golod and I. Shafarevich, *On the tower class fields*, Izv. Akad. Nauk. SSSR Ser. Math. **28** (1964), 261–272.
9. H. Hasse, *Bericht über neuere Untersuchungen and Probleme aus der Theorie der algebraischen Zahlkörper*, I, Ia, II, Jahresber. der Deutsch Math. Ver., 1926, 1927, 1930.

10. ———, *Über die Klassenzahl Abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952.
11. M. Herbrand, *Memorial des sciences mathématiques*, fasc. LXXV, Gauthier-Villars, Paris, 1936.
12. S. Iyanaga (Ed.), *The Theory of Numbers*, North-Holland Publishing Company, New York, 1975.
13. G. Janusz, *Algebraic Number Fields*, Academic Press, New York, 1973.
14. S. Lang, *Algebraic Number Theory*, Addison-Wesley Publishing Company, Inc., Reading, 1970.
15. ———, *Elliptic Functions*, Addison-Wesley Publishing Company, Inc., Reading, 1973.
16. W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Polish Scientific Publishers, Warsaw, 1974.
17. J. Neukirch, *Klassenkörpertheorie*, Mathematisches Institut der Universität Bonn.
18. G. Shimura, *Automorphic Functions and Number Theory*, Springer-Verlag, New York, 1968.
19. A. Weil, *Basic Number Theory*, Springer-Verlag, New York, 1967.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MARYLAND, COLLEGE PARK, MD 20742

