Comm. Korean Math. Soc. 4 (1989), No. 2, pp. 331~347

GLOBAL CLASS FIELD THEORY SUMMARIZED AND ITS APPLICATION

JA KYUNG KOO, SUNGHAN BAE AND SANG GEUN HAHN

1. Introduction 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 global class field theory such as it can be found in the work of Hasse [**11**], i.e., pre-World-War II class field theory. The second part will resummarize class field theory in a more modern fashion using ideles, i.e., Chevalley's formulation [**6**, **7**, **8**].

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

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

The *arithmetic* of K is the study of the ideal group A_K, subgroups of A_K, factor groups of subgroups of A_K, groups isomorphic to these groups and certain ideals in A_K. 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.)

Received May 15,1989.

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

2. Terminologies Let L be a Galois extension of K of degree n. Let ϑ_K (ϑ_L resp.) be the ring of algebraic integers of K (L resp.). It is known that if $\mathfrak{p}$ is a prime ideal in ϑ_K, then

$$\mathfrak{p}\vartheta_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$$

where $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ are distinct prime ideals in ϑ_L. The integer e is called the *ramification index* of $\mathfrak{p}$. If $\mathfrak{P}|\mathfrak{p}$, then $\vartheta_K/\mathfrak{p}$ is a field which can be thought of as a subfield of $\vartheta_L/\mathfrak{P}$, and $[\vartheta_L/\mathfrak{P} : \vartheta_K/\mathfrak{p}] = f$ is called the *residue class degree* of $\mathfrak{p}$ (or 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 2.1. [**13**, p.136]. *Let L_1 and L_2 be Galois extensions of K and S_1, S_2 be the set 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 $L_1 = L_2$.*

3. 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. 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 3.1. (Kronecker-Weber, 1886-1887). [**13**, p.165]. *Let L be a finite abelian extension of $\mathbf{Q}$. Then there exists a positive integer m such that $L \subset \mathbf{Q}(e^{2\pi i/m})$.*

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 persent now. A summary of class field theory over the rationals is given in [**12**, p. 4-6]. 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, because then $\mathbf{Q}_{2a} = \mathbf{Q}_a$. So we are not eliminating any cyclotomic fields by this restriction. The attainment of the first goal of class field theory is an immediate benefit of the Kronecker-Weber theorem. We say such an m in Th. 3.1. is a ***defining***(or ***admissible***) ***modulus*** of L. The ***conductor*** f_L of L is the greatest common divisor of all defining moduli m of K.

If m is any positive integer, let C_m be the unit group of $\mathbf{Z}/m\mathbf{Z}$. 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 $\mathbf{Q}$.

With 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 $\zeta \to \zeta^a$ (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 3.2. (Artin's Law of Reciprocity). *If L is an abelian extension of $\mathbf{Q}$ with defining modulus m, then the following sequence is exact*

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

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

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

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

THEOREM 3.4. (Decomposition Theorem). *Let m be a defining mod-*

ulus 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 $\mathrm{Spl}(L/K)$ denote the set of all prime ideals of K which split completely in L.

Let $m = f_L$. Then, since $efg = n = [L : \mathbf{Q}]$, $p \in \mathrm{Spl}(L/\mathbf{Q})$ if and only if $e = 1$ and $f = 1$ if and only if $p \nmid f_L$ and $p \in I_{L,f_L}$. This is the realization of

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

4. Classical global class field theory (Classical presentations of class field theory are found in [**11**], [**13**] and [**14**]).

Since the Kronecker-Weber theorem does not hold for an arbitrary ground field K, we need to replace the notions mentioned in §3 with something more general.

A *K-modulus* $\mathfrak{M}$ is a formal product of an ideal $\mathfrak{M}_0 \subset \vartheta_K$ and some real infinite K-primes. All the infinite primes are raised to the first power here. Let p_∞ denote the real infinite $\mathbf{Q}$-prime associated with the identity map on $\mathbf{Q}$. We let $\mathfrak{M} = (m)p_\infty$ when $K = \mathbf{Q}$.

Let $A_{\mathfrak{M}}$ be the set of all fractional ideals $\mathfrak{A} \in A_K$ such that the unique factorization of $\mathfrak{A}$ and $\mathfrak{M}$ into K-primes has no K-primes in common. Let $K^* = K - \{0\}$. If $\alpha \in K^*$, let (α) be the principal ideal $\alpha\vartheta_K$. If $(\alpha) \in A_{\mathfrak{M}}$, then it turns out that $\alpha = a/b$ for a, $b \in \vartheta_K$ and (a), $(b) \in A_{\mathfrak{M}}$. Let $(\alpha) \in A_{\mathfrak{M}}$. Then "$\alpha \equiv 1 \bmod \mathfrak{M}$" means $a \equiv b \bmod \mathfrak{M}_0$ where $\alpha = a/b$ are as above and $\sigma\alpha > 0$ for each real infinite K-prime $\mathfrak{p}_\sigma$ occuring in $\mathfrak{M}$. We have generalized the notion of congurence. The *ray* mod $\mathfrak{M}$ is the subgroup $R_{\mathfrak{M}}$ of $A_{\mathfrak{M}}$, $R_{\mathfrak{M}} = \{(\alpha) \in A_{\mathfrak{M}} \mid \alpha \equiv 1 \bmod \mathfrak{M}\}$. The *ray class group* mod $\mathfrak{M}$ is the quotient group $C_{\mathfrak{M}} = A_{\mathfrak{M}}/R_{\mathfrak{M}}$ which turns out to be finite. In case $K = \mathbf{Q}$ and $\mathfrak{M} = (m)p_\infty$, $C_{\mathfrak{M}} \cong C_m$ via $\varphi : (\alpha)R_{\mathfrak{M}} \to ab^{-1}$ where $\alpha = \pm ab^{-1}$. Thus $C_{\mathfrak{M}}$ generalizes C_m. If $\mathfrak{M} = 1$, the modulus having no K-primes, then $A_{\mathfrak{M}} = A_K$ and $R_{\mathfrak{M}} = (K^*)$ and so $C_1 = A_K/(K^*)$ the *ideal class group* of K.

Generalizing $I_{L,m}$ is not at all trivial because we do not have the Kroecker-Weber theorem. Let L/K be an abelian extension. Let $\mathfrak{M}$ be a K-modulus. Let $A_{L,\mathfrak{M}}$ be the set of all fractional ideals $\mathcal{U} \in A_L$ such that the unique fractorizations of $\mathcal{U}$ and $\mathfrak{M}_0\vartheta_L$ into L-primes contain no L-primes in common. Let $R_{L,\mathfrak{M}} = \{(\alpha) \in A_{L,\mathfrak{M}} \mid \alpha \equiv 1 \bmod \mathfrak{M}_0\vartheta_L$ and $\tau\alpha > 0$ for all real infinite L – prime $\mathfrak{P}_\tau$ such that $\mathfrak{P}_\tau \mid \mathfrak{p}_\sigma$ where $\mathfrak{p}_\sigma$ occurs in $\mathfrak{M}\}$.

Let $C_{L,\mathfrak{M}} = A_{L,\mathfrak{M}}/R_{L,\mathfrak{M}}$ and let $I_{L/K,\mathfrak{M}} = N_{L/K}(C_{L,\mathfrak{M}})$, a subgroup of $C_{\mathfrak{M}}$. If m is a defining modulus of $L/\mathbf{Q}$ and $\mathfrak{M} = (m)p_\infty$, then it turns out that $I_{L/\mathbf{Q},\mathfrak{M}} \cong I_{L,m}$. So $I_{L/K,\mathfrak{M}}$ generalizes $I_{L,m}$ and, in fact, $I_{L/K,\mathfrak{M}}$ will play the same role in the theory over K as $I_{L,m}$ played in the theory over $\mathbf{Q}$.

To generalize the notion of "the conductor of L" and "a defining modulus of L" we need the following very deep theorem.

THEOREM 4.1. (Weber-Takagi-Chevalley). *Let $\mathfrak{M}$ be a K-modulus. Given abelian extension 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 $\mathfrak{f}_{L/K}|\mathfrak{M}$.*

The unique modulus $\mathfrak{f}_{L/K}$ in the theorem 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.

If $K = \mathbf{Q}$, 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. Let $L = \mathbf{Q}(\sqrt{d})$ where d is a square free integer. Then

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

[**13**, p.198]. In order to replace $\mathbf{Q}_m$ by something more general we need the following theorem proved by Takagi (1920).

THEOREM 4.2. (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) $I_{L/K,\mathfrak{M}}(= N_{L/K}C_{L,\mathfrak{M}}) = I_{\mathfrak{M}}$.

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 Th. 4.2. are satisfied. 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 mod$\mathfrak{M}$. When $\mathfrak{M} = 1$, the ray class field $K(R_{(1)}) = \widetilde{K}$ is called *the Hilbert class field* of K. In this case, $G(\widetilde{K}/K) \cong A_K/(K^*)$. If $K = \mathbf{Q}$, it turns out that $\mathbf{Q}_m$ is the ray class field of $\mathbf{Q}$ mod $\mathfrak{M}$ where $\mathfrak{M} = (m)p_\infty$. So the ray class field mod$\mathfrak{M}$ is what replaces $\mathbf{Q}_m$ in the general theory.

THEOREM 4.3. (Takagi, 1920). *Given L/K abelian, there exists a K-modulus $\mathfrak{M}$ such that $L \subset K(R_{\mathfrak{M}})$.*

THEOREM 4.4. *The conductor $\mathfrak{f}_{L/K}$ is the "smallest" K-modulus $\mathfrak{M}$ such that $L \subset K(R_{\mathfrak{M}})$. "Smallest" means that if $L \subset K(R_{\mathfrak{M}})$ then $\mathfrak{f}_{L/K}|\mathfrak{M}$. Also $\mathfrak{M}$ is a defining modulus of L/K if and only if $L \subset K(R_{\mathfrak{M}})$.*

Thus we have found all abelian extensions of K, i.e., they are the subfields of the ray class fields of K. But the construction problem is another and is still one of the major open problems in number theory, so called "the Hilbert's 12-th problem". (For more on this topic see [3], [15], [17], [18] and [19]).

We shall now canonically realize $G(L/K)$-Artin's law of reciprocity. Let $\mathfrak{M}$ be a defining modulus of L/K. Let $\mathfrak{p}$ be a finite K-prime such that $\mathfrak{p} \nmid \mathfrak{M}$. Then there exists a unique automorphism in $G(L/K)$, denoted $\left(\frac{L/K}{\mathfrak{p}}\right)$, such that

$$\left(\frac{L/K}{\mathfrak{p}}\right)\alpha \equiv \alpha^{N_{K/\mathbf{Q}}\mathfrak{p}} \bmod \mathfrak{p}\vartheta_L$$

for all $\alpha \in \vartheta_L$. The *Artin symbol* is the natural extension of this map as follows. If $\mathfrak{A} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_s^{a_s}$ $(a_i \in \mathbf{Z})$, then

$$\left(\frac{L/K}{\mathfrak{A}}\right) = \left(\frac{L/K}{\mathfrak{p}_1}\right)^{a_1} \cdots \left(\frac{L/K}{\mathfrak{p}_s}\right)^{a_s}.$$

It can be shown that if $(\alpha) \in R_{\mathfrak{M}}$ then $\left(\frac{L/K}{(\alpha)}\right) = 1$ 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 $c = \mathfrak{A}R_{\mathfrak{M}}$, then let $\left(\frac{L/K}{c}\right) = \left(\frac{L/K}{\mathfrak{A}}\right)$.

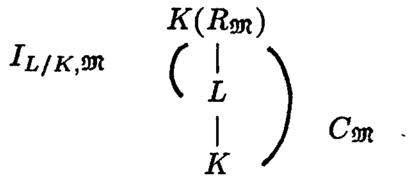
If $K = \mathbf{Q}$ and $\mathfrak{M} = (m)p_\infty$ is a defining modulus of L/Q, it is not difficult to show that $\left(\frac{L/K}{c}\right) = (L/\varphi(c))$ where φ is the map given in $C_{\mathfrak{M}} \cong C_m$ and $(L/\ )$ is the map defined in Th. 3.2. Thus this definition of the Artin symbol is a generalization of that given before theorem 3.2. In 1927 Artin proved the following theorem.

THEOREM 4.5 (Artin's Law of Reciprocity). *The following sequence is exact*

$$1 \longrightarrow I_{L/K,\mathfrak{M}} \longrightarrow C_{\mathfrak{M}} \xrightarrow{\left(\frac{L/K}{\ }\right)} G(L/K) \longrightarrow 1.$$

COROLLARY 4.6. *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 $G(K(R_{\mathfrak{M}})/L) \cong I_{L/K,\mathfrak{M}}$.*

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



THEOREM 4.7. (Takagi's Conductor-Ramification Theorem, 1920). *A K-prime $\mathfrak{p}$ ramifies in L if and only if $\mathfrak{p} | \mathfrak{f}_{L/K}$.*

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

THEOREM 4.8. *The Hilbert class field $\widetilde{K}$ of K is the maximal unramified abelian extension of K.*

THEOREM 4.9. (Takagi's Decomposition Theorem, 1920). *Let $\mathfrak{M}$ be a defining modulus of L/K. Let $\mathfrak{p}$ be a finite K-prime such that $\mathfrak{p} \nmid \mathfrak{M}$.*

Let $\bar{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{M}}$ *in* $C_{\mathfrak{M}}$. *Then the order of* $\bar{\mathfrak{p}}I_{L/K,\mathfrak{M}}$ *in* $C_{\mathfrak{M}}/I_{L/K,\mathfrak{M}}$ *is* f, *the residue class degree of* $\mathfrak{p}$.

COROLLARY 4.10. *Let* $\mathfrak{p}$ *be a* K*-prime. Then* $\mathfrak{p} \in \mathrm{Spl}(\widetilde{K}/K)$ *if and only if* $\mathfrak{p} \in (K^*)$.

COROLLARY 4.11. *Let* L/K *be abelian and* $\mathfrak{p}$ *a finite* K*-prime. Then* $\mathfrak{p} \in \mathrm{Spl}(L/K)$ *if and only if* $\mathfrak{p} \nmid \mathfrak{f}_{L/K}$ *and* $\left(\frac{L/K}{\mathfrak{p}}\right) = 1$.

5. Post World War II Class Field Theory (Presentation of class field theory using ideles can be found in [**2**], [**5**], [**9**], [**10**], [**14**] and [**16**].)

Let K be a finite extension of $\mathbf{Q}$ and let $C_K = \mathbf{J}_K/K^*$, the *idele class group*. Let L be a Galois extension of K. There is a natural embedding $\mathbf{J}_K \hookrightarrow \mathbf{J}_L$, i.e., $j \to \hat{j}$ where $\hat{j}_{\mathfrak{P}} = j_{\mathfrak{p}}$ for $\mathfrak{P}|\mathfrak{p}$. Think "$\mathbf{J}_K \subset \mathbf{J}_L$". If $\sigma \in G = G(L/K)$, there is a unique topological isomorphism also denoted by σ mapping $L_{\sigma^{-1}\mathfrak{P}}$ onto $L_{\mathfrak{P}}$ which extends $\sigma \in G(L/K)$. ($|\alpha|_{\sigma^{-1}\mathfrak{P}} = |\sigma\alpha|_{\mathfrak{P}}$ for $\alpha \in L$, i.e., $|\ |_{\sigma^{-1}\mathfrak{P}}$ is defined via $|\ |_{\mathfrak{P}}$. So if $\mathfrak{P} = \mathfrak{P}_\tau$ is infinite, then $|\alpha|_{\sigma^{-1}\mathfrak{P}_\tau} = |\sigma\alpha|_{\mathfrak{P}_\tau} = |\tau\sigma(\alpha)|$ on $\mathbf{C}$, i.e., $\sigma^{-1}\mathfrak{P}_\tau = \mathfrak{P}_{\tau\sigma}$ gives the action of σ^{-1} on the infinite L-prime $\mathfrak{P}_\tau$.) To turn $\mathbf{J}_L$ into a G-module we define the $\mathfrak{P}$-component of $\sigma\hat{j}$ where $\hat{j} \in \mathbf{J}_L$ as follows $(\sigma\hat{j})_{\mathfrak{P}} = \sigma(\hat{j}_{\sigma^{-1}\mathfrak{P}})$. One also naturally embeds C_K in C_L via $jK^* \to jL^*$ where $j \in \mathbf{J}_K$. Think "$C_K \subset C_L$". Make C_L a G-module via $\sigma(\hat{j}L^*) = \sigma\hat{j} \cdot L^*$ and define the norm map $N_{L/K} : C_L \to C_K$ via

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

due to the fact that C_K is the fixed G-submodule of C_L.

Let D_K be the connected component of the identity in the topological group C_K. Then D_K is characterized algebraically as the set of all infinitely divisible elements of C_K, i.e., if $a \in D_K$ then for any positive integer n there is $b \in C_L$ such that $a = b^n$. Also $D_K = \bigcap_L N_{L/K}C_L$ 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. Since $N_{L/K}D_L \subset D_K$, we can extend $N_{L/K}$ to $N_{L/K} : C'_L \to C'_K$

where $N_{L/K}(aD_L) = N_{L/K}a \cdot D_K$. Let $I'_{L/K} = N_{L/K}C'_L$. If L/K is abelian, then $I'_{L/K}$ is an open subgroup of C'_K.

THEOREM 5.1. (Existence Theorem). *Let I' be an open subgroup of C'_K. Then there exists a unique finite abelian extension L of K such that $I'_{L/K}(= N_{L/K}C'_L) = I'$.*

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 $N_{L/K}C'_L = I'$.

Let $i, j \in \mathbf{J}_K$ and let $\mathfrak{M}$ be a K-modulus. Then "$j \equiv i \bmod \mathfrak{M}$" means $\mathrm{ord}_\mathfrak{p}(ji^{-1} - 1)_\mathfrak{p} \geq \mathrm{ord}_\mathfrak{p} \mathfrak{M}$ for all finite K-primes $\mathfrak{p}|\mathfrak{M}$ and $(ji^{-1})_\mathfrak{p} \in (K^*_\mathfrak{p})^2$ for all infinite K-primes $\mathfrak{p}|\mathfrak{M}$. Write "$j \equiv i \overline{\bmod \mathfrak{M}}$" if it is also true that $(ji^{-1})_\mathfrak{p} \in U_\mathfrak{p}$, the unit group of $K_\mathfrak{p}$, if $\mathfrak{p} \nmid \mathfrak{M}$. Let $J_\mathfrak{M} = \{j \in \mathbf{J}_K \mid j \equiv 1 \overline{\bmod \mathfrak{M}}\}$. Let $I_\mathfrak{M} = J_\mathfrak{M} \cdot K^*/K^*$, the *congruence subgroup* of C_K mod $\mathfrak{M}$. It can be shown that $C_K/I_1 \cong A_K/(K^*)$.

Let L/K be abelian. $\mathfrak{M}$ is called a *defining modulus* of L/K if $I_\mathfrak{M} \subset N_{L/K}C_L$. Let $\mathfrak{M}$ be a defining modulus of L/K. The *global norm residue symbol* $(\ ,L/K) : \mathbf{J}_K \to G(L/K)$ is defined as follows. Let $j \in \mathbf{J}_K$. Then there exists $\alpha \in K^*$ such that $j \equiv \alpha \bmod \mathfrak{M}$. Define

$$(j, L/K) = \prod_{\substack{\mathfrak{p}\nmid\mathfrak{M} \\ \mathfrak{p}\text{ finite}}} \left(\frac{L/K}{\mathfrak{p}}\right)^{\mathrm{ord}_\mathfrak{p}(j\alpha^{-1})_\mathfrak{p}}$$

where $\left(\frac{L/K}{\mathfrak{p}}\right)$ is an Artin symbol. This is well defined and it can be shown that if $\alpha \in K^*$ then $(\alpha, L/K) = 1$. Hence we can define $(\ ,L/K)$ on C_K by $(jK^*, L/K) = (j, L/K)$. Moreover, if $jK^* \in D_K$ then $(jK^*, L/K) = 1$. So we can define $(\ ,L/K)$ on $C'_K = C_K/D_K$ via $(\bar{j}, L/K) = (j, L/K)$ where $\bar{j} = jK^* \cdot D_K \in C'_K$.

THEOREM 5.2. (Artin's Law of Reciprocity). *Let L be a finite abelian extension of K. Then*

$$1 \longrightarrow I'_{L/K} \longrightarrow C'_K \xrightarrow{(\ ,L/K)} G(L/K) \longrightarrow 1$$

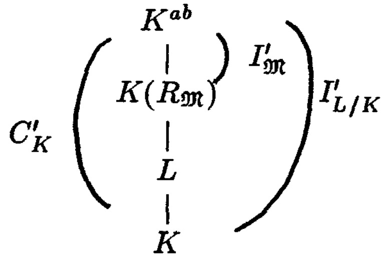
is exact.

Define $(\ ,K): C'_K \to G(K^{ab}/K)$ by

$$(\bar{\jmath}, K) = \varprojlim_L (\bar{\jmath}, L/K) \in \varprojlim_L G(L/K) = G(K^{ab}/K)$$

where L runs over all finite abelian extensions of K. One can show using Th. 5.2. that $(\ ,K)$ gives an isomorphism from C'_K onto $G(K^{ab}/K)$. (This is true for a finite extension K of $\mathbf{Q}$, not for function fields over finite constant field.) So C'_K will replace $\{C_{\mathfrak{M}} \mid \mathfrak{M}$ is a K-modulus$\}$. Furthermore this map gives an isomorphism $G(K^{ab}/L) \cong N_{L/K}C'_L = I'_{L/K}$ and so $I'_{L/K}$ will replace $\{I_{L/K,\mathfrak{M}} \mid \mathfrak{M}$ is a defining modulus of $L/K\}$.

Since $D_K = \bigcap\limits_{\substack{\mathfrak{M} \\ K\text{-modulus}}} I_{\mathfrak{M}}$, let $I'_{\mathfrak{M}} = I_{\mathfrak{M}}/D_K (\subset C'_K)$. Let $\mathfrak{M}$ be a K-modulus. Then it can be shown that $I'_{K(R_{\mathfrak{M}})/K} = N_{K(R_{\mathfrak{M}})/K} C'_{K(R_{\mathfrak{M}})} = I'_{\mathfrak{M}}$. If $\mathfrak{M}$ is a defining modulus of L/K, then $I'_{\mathfrak{M}} \subset I'_{L/K}$ and we have the following Galois interpretation.



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

THEOREM 5.3. (Conductor-Ramification Theorem). *A K-prime $\mathfrak{p}$ ramifies in L if and only if $\mathfrak{p} | \mathfrak{f}_{L/K}$.*

If $\mathfrak{p}$ is a prime ideal, let $j(\mathfrak{p})$ be the element of $\mathbf{J}_K$ whose $\mathfrak{q}$-th component is given by

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

where $\mathfrak{q}$ is a K-prime and π is a unifomizing parameter of $K_{\mathfrak{p}}$. $j(\mathfrak{p})$ is called "the idele of $\mathfrak{p}$". Let $\overline{j(\mathfrak{p})} = j(\mathfrak{p})K^* \cdot D_K$ in C'_K.

THEOREM 5.4. (Decomposition Theorem). *Let L/K be abelian. Suppose $\mathfrak{p}$ is a finite K-prime which does not ramify in L. Then the order of $\overline{j(\mathfrak{p})I'_{L/K}}$ in $C'_K/I'_{L/K}$ is the residue class degree f of $\mathfrak{p}$.*

COROLLARY 5.5. $\mathfrak{p} \in \mathrm{Spl}(L/K)$ *if and only if* $\mathfrak{p} \nmid \mathfrak{f}_{L/K}$ *and* $(j(\mathfrak{p}), L/K) = 1$.

6. Remarks Gauss (1777-1855) tried to decide when $x^2 - a \equiv 0 \bmod p$ has a solution ($p \nmid a$ and p is a prime). He came up with his law of reciprocity—one formulation of which is the following theorem.

THEORME 6.1. (Gauss' Quadratic Reciprocity). [1, p.122]. *If p and q are odd primes not dividing a and $p \equiv q \bmod 4a$, then $x^2 - a \equiv 0 \bmod p$ has a solution if and only if $x^2 - a \equiv 0 \bmod q$ has a solution.*

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

THEOREM 6.2. [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 $x^2 - d \equiv 0 \bmod p$ has a solution and $p \nmid d$.*

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

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

If b is an odd prime 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

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

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 Th. 6.2., the Decomposition theorem and Artin's law of reciprocity which say $(d/p) = 1$ if and only if $p \in \mathrm{Spl}(L/\mathbf{Q})$ if and only if $(L/p) = 1$. Since $(L/\ )$ is a homomorphism, if b is an odd positive integer and $\gcd(d, b) = 1$ then $(L/b) = (d/b)$. Therefore the Artin symbol is a generalization of the Jacobi symbol which is a generalization of the Legendre Symbol.

Not only does the Artin symbol generalize the Legendre Symbol but Gauss' law of quadratic reciprocity (Th. 6.1) can be deduced from Artin's law of reciprocity (Th. 3.2) as follows. Let p and q be odd primes not dividing a and let $p \equiv q \bmod 4a$. Then the following six statements are equivalent.

(1) $x^2 \equiv a \bmod p$ has a solution.
(2) $x^2 \equiv d \bmod p$ has a solution where $a = d \cdot$ square and d is square free.
(3) $p \in \mathrm{Spl}(\mathbf{Q}(\sqrt{d})/\mathbf{Q})$. (By Th. 6.2.)
(4) $(\mathbf{Q}(\sqrt{d})/p) = 1$. (By Th 3.4 and Artin's law of reciprocity.)
(5) $(\mathbf{Q}(\sqrt{d})/q) = 1$. (Since $p \equiv q \bmod 4a \Rightarrow p \equiv q \bmod 4d \Rightarrow p \equiv q \bmod f_{\mathbf{Q}(\sqrt{d})} \Rightarrow (\mathbf{Q}(\sqrt{d})/p) = (\mathbf{Q}(\sqrt{d})/q)$ by the definition of $(\mathbf{Q}(\sqrt{d})/p)$.)
(6) $x^2 \equiv a \bmod q$ has a solution.

7. Application An appropriate conclusion would be an application to a Diophantine problem which we now present. Given a prime p do there exist x, $y \in \mathbf{Z}$ such that $p = x^2 + xy + 9y^2$ has a solution? We will show that there is a solution if and only if $p \equiv 1, 4, 9, 11, 16$ or $29 \bmod 35$.

Let $K = \mathbf{Q}(\sqrt{-35})$. Then ϑ_K has an integral basis 1 and $(1+\sqrt{-35})/2$, i.e.,

$$\vartheta_K = \mathbf{Z} \oplus \mathbf{Z}\left(\frac{1+\sqrt{-35}}{2}\right).$$

Also

$$\begin{aligned} x^2 + xy + 9y^2 &= \left(x + \frac{1+\sqrt{-35}}{2}y\right)\left(x + \frac{1-\sqrt{-35}}{2}y\right) \\ &= N_{K/\mathbf{Q}}\left(x + \frac{1+\sqrt{-35}}{2}y\right). \end{aligned}$$

Thus the question is : For which p is there an element of ϑ_K whose norm is p? To answer this we need the following general definitions and theorem.

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

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

The form F_K is homogeneous of degree n with coefficients in $\mathbf{Z}$.

THEOREM 7.1. *Let K be a totally imaginary abelian extension of $\mathbf{Q}$ with $[K : \mathbf{Q}] = n$. Suppose $p \nmid f_K$. Let $F_K(x_1, \ldots, x_n)$ be the norm form associated with K. Then $F_K(x_1, \ldots, x_n) = p$ has a solution with $x_i \in \mathbf{Z}$ if and only if $p \in \mathrm{Spl}(\widetilde{K}/\mathbf{Q})$.*

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

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

Hence $F_K(x_1, \ldots, x_n) = p$ has a solution if and only if $N_{K/\mathbf{Q}}\alpha = p$ for some $\alpha \in \vartheta_K$ if and only if there is a principal prime ideal $\mathfrak{p}$ of K having norm p. On the other hand $p \in \mathrm{Spl}(K/\mathbf{Q})$ if and only if there is a K-prime $\mathfrak{p}$ having norm p ; and $\mathfrak{p}$ is principal by Cor. 4.10 if and only if $\mathfrak{p} \in \mathrm{Spl}(\widetilde{K}/K)$.

We will show that the Hilbert Class field $\widetilde{K}$ of K is $\mathbf{Q}(\sqrt{5}, \sqrt{-7})$.

Let $\widehat{C}_m$ be the character group of the unit group C_m of $\mathbf{Z}/m\mathbf{Z}$. If $\gcd(a, m) > 1$, then let $\chi(a) = 0$ for any $\chi \in \widehat{C}_m$. A positive integer b is a *defining modulus* of $\chi \in \widehat{C}_m$ if $a \equiv 1 \bmod b$ implies $\chi(a) = 1$. The *conductor* f_χ of $\chi \in \widehat{C}_m$ is the smallest defining modulus of χ. If m is a defining modulus of a number field L, let

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

the *character group* of L mod m.

THEOREM 7.2. (Hasse Conductor-Discriminant Formula) *Let m be a defining modulus of L. Then*

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

and

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

(lcm = least common multiple, d_L = discriminant of L).

Let $L = \mathbf{Q}(\sqrt{5}, \sqrt{-7})$. Then we have the following diagram :

$$\begin{tikzcd}
 & & \mathbf{Q}_5 \cdot \mathbf{Q}_7 = \mathbf{Q}_{35} \arrow[lld, dash] \arrow[rrd, dash] \arrow[dd, dash] & & \\
\mathbf{Q}_5 \arrow[dd, dash] & & & & \mathbf{Q}_7 \arrow[dd, dash] \\
 & & \mathbf{Q}(\sqrt{5}, \sqrt{-7}) = L \arrow[lld, dash] \arrow[rrd, dash] & & \\
\mathbf{Q}(\sqrt{5}) \arrow[rrd, dash] & & & & \mathbf{Q}(\sqrt{-7}) \arrow[lld, dash] \\
 & & \mathbf{Q} & &
\end{tikzcd}$$

Now $G(\mathbf{Q}_5/\mathbf{Q}) \cong C_5$ which is cyclic generated by say a_1 and $G(\mathbf{Q}_7/\mathbf{Q}) \cong C_7$ which is also cyclic generated by say a_2. Then $C_{35} \cong G(\mathbf{Q}_{35}/\mathbf{Q}) \cong G(\mathbf{Q}_5/\mathbf{Q}) \times G(\mathbf{Q}_7/\mathbf{Q}) \cong \langle a_1 \bmod 5\rangle \times \langle a_2 \bmod 7\rangle$. Define characters χ_1 and χ_2 on $\langle a_1 \bmod 5\rangle \times \langle a_2 \bmod 7\rangle$ as follows: $\chi_1(a_1) = \sqrt{-1}$, $\chi_1(a_2) = 1$ and $\chi_2(a_1) = 1$, $\chi_2(a_2) = \frac{1}{2} + \frac{\sqrt{3}}{2}i$. Then we can take $\langle \chi_1\rangle \times \langle \chi_2\rangle$ to be the character group of C_{35}. Since $G(\mathbf{Q}_5/\mathbf{Q}(\sqrt{5})) \cong \langle a_1^2 \bmod 5\rangle$ and $G(\mathbf{Q}_7/\mathbf{Q}(\sqrt{-7})) \cong \langle a_2^2 \bmod 7\rangle$, we get $G(\mathbf{Q}_{35}/L) \cong \langle a_1^2 \bmod 5\rangle \times \langle a_2^2 \bmod 7\rangle$. Hence $X_{L,35} = \langle \chi_1^2\rangle \times \langle \chi_2^3\rangle$ by Th. 3.2. Now the following proposition can be shown.

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

Thus since 5 is a defining modulus of χ_1^2, $f = 1$ or 5. But clearly 1 is not a defining modulus of χ_1^2. So $f_{\chi_1^2} = 5$. Similarly $f_{\chi_2^3} = 7$, $f_{\chi_1^2\chi_2^3} = 35$

and $f_{\chi_0} = 1$ where $\chi_0 = 1$ is the principal character. Therefore by Th. 7.2 $|d_L| = 5^2 \cdot 7^2$ and $f_L = 5 \cdot 7$.

We are ready to show that $\tilde{K} = \mathbf{Q}(\sqrt{5}, \sqrt{-7})$. Let $L = \mathbf{Q}(\sqrt{5}, \sqrt{-7})$. Since K and L are both non-real abelian extensions of $\mathbf{Q}$, no infinite K-prime ramifies in L. By Th. 3.3, considering the conductors $f_K = 35$ (see §4) and $f_L = 35$, the finite $\mathbf{Q}$-primes which ramify in K are the same as those which ramify in L, namely, 5 and 7. The ramification index of 5 in$K$ is 2. Thus since 5 does not ramify in $\mathbf{Q}(\sqrt{-7})$, 5 ramifies in L with ramification index 2. Similarly, the ramification indices of 7 in K and L are the same. Therefore L is an unramified extension of K and so $L \subset \tilde{K}$ by Th. 4.8. Now the following result can be deduced without using class field theory from facts about Dirichlet L-series.

THEOREM 7.3. *Let $K = \mathbf{Q}(\sqrt{d})$ where $d < -2$. Suppose f_K is odd. Let $(a/|d|)$ be the Jacobi symbol. Then the class number of K is*

$$h_K = \frac{1}{2 - \left(\frac{2}{|d|}\right)} \sum_{\substack{0<x<\frac{f_k}{2} \\ \gcd(x,f_k)=1}} \left(\frac{x}{|d|}\right).$$

(A similar but slightly more complicated result holds if f_K is even [4, p.346].)

Thus if $K = \mathbf{Q}(\sqrt{-35})$, then $f_K = 35$ and $(2/|d|) = (2/35) = (2/5)(2/7) = -1$. Therefore $h_K = 1/3\{(1/35) + (2/35) + (3/35) + (4/35)+(6/35)+(8/35)+(9/35)+(11/35)+(12/35)+(13/35)+(16/35)+(17/35)\} = 1/3\{1-1+1+1-1-1+1+1+1+1+1+1\} = 2$ and so the order of $G(\tilde{K}/K)$ is 2, which implies $[\tilde{K} : K] = 2$. Since $[L : \mathbf{Q}] = 4$ and $L \subset \tilde{K}$, $L = \tilde{K}$.

When $L = \mathbf{Q}(\sqrt{5}, \sqrt{-7})$, we will show that $p \in \mathrm{Spl}(L/\mathbf{Q})$ if and only if $p \equiv 1, 4, 9, 11, 16$ or $29 \bmod 35$. Let $a_1 = 3$ and $a_2 = 5$. As in the example given just before Proposition, under the natural isomorphism we have $G(\mathbf{Q}_{35}/\mathbf{Q}) \cong \langle a_1 \bmod 5\rangle \times \langle a_2 \bmod 7\rangle = \langle 3 \bmod 5\rangle \times \langle 5 \bmod 7\rangle$ and $G(\mathbf{Q}_{35}/L) \cong G(\mathbf{Q}_5/\mathbf{Q}(\sqrt{5})) \times G(\mathbf{Q}_7/\mathbf{Q}(\sqrt{-7})) \cong \langle 3^2 \bmod 5\rangle \times \langle 5^2 \bmod 7\rangle$. Therefore $I_{L,f_L} = G(\mathbf{Q}_{35}/L) \cong \langle 4 \bmod 35\rangle$. The result follows from Th. 3.4.

Returning to the original problem if follows that if $K = \mathbf{Q}(\sqrt{-35})$ and $p \nmid f_K = 35$ then, by Th. 7.1, $p = x^2 + xy + 9y^2$ has a solution if and only if $p \in \mathrm{Spl}(\widetilde{K}/\mathbf{Q})$, which is equivalent to $p \in \mathrm{Spl}(\mathbf{Q}(\sqrt{5}, \sqrt{-7})/\mathbf{Q})$, which in turn is equivalent to $p \equiv 1, 4, 9, 11, 16$ or $29 \bmod 35$. Now suppose $p = 5$. If $5 = x^2 + xy + 9y^2 = \left(x + xy + \left(\frac{y}{2}\right)^2\right) - \left(\frac{y}{2}\right)^2 + 9y^2$ has a solution, then $20 = (2x + y)^2 + 35y^2$ has a solution which is not the case. A similar argument shows that $7 = x^2 + xy + 9y^2$ does not have a solution.

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. Fröhlich, "Algebraic Number Theory," Thompon Book Company, Inc., Washington, D.C., 1967.

[6] C. Chevalley, *La théorie du symbole de restes normiques*, J. reine angew. Math. **169** (1933a), 140–157.

[7] ————, *Sur la théorie du corps de classes dans les corps finis et les corps locaux*, J. Fac. Sci. Tokyo Univ. **2** (1933b), 365–476.

[8] ————, *La théorie du corps de classes*, Ann. Math. **41** (1940), 394-417.

[9] L. Goldstein, "Analytic Number Theory," Prentice-Hall, Inc., Englewood Cliffs, 1971.

[10] ————, "The theory of numbers," Enciclopedia Del. Novecento Instituto Della Enciclopedia Italiana Pisa, Italy.

[11] 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).

[12] ————, "Über die Klassenzahl Abelzcher Zahlkörper," Akademie-Verlag, Berlin, 1952.

[13] G. Janusz, "Algebraic Number Fields," Adademic-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] J. Neukirch, "Class Field Theory," Springer-Verlag, New York, 1986.

[17] G. Shimura and Taniyama, "Complex Multiplication of Abelian Varieties and its Application to Number Theory," Math. Soc. Japan, Tokyo, 1960.

[18] G. Shimura, "Automorphic Functions and Number Theory," Springer-Verlag, New York, 1968.

[19] ―――――, *Class fields over real quaratic fields and Hecke operators*, Ann. Math. **95** (1972), 130–190.

Department of Mathematics
Korea Institute of Technology
Taejon, 305-701 Korea