To the Graduate Council :

I am submitting herewith a thesis written by Umesh S. Thakur entitled " Artin's Reciprocity Law ." I have examined the final copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Arts, with a major in Mathematics.

Robert M. McConnel, Major Professor

We have read this thesis
and recommend its acceptance :

David F. Anderson

S. B. Mulay

Accepted for the Council :

Vice Provost
and Dean of The Graduate School

STATEMENT OF PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a Master's degree at the University of Tennessee, Knoxville, I agree that the Library shall make it available to borrowers under rules of the Library. Brief quotations from this thesis are allowable without special permission, provided that accurate acknowledgment of the source is made.

Permission for extensive quotation from or reproduction of this thesis may be granted by my major professor, or in his absence, by the Head of Interlibrary Services when, in the opinion of either, the proposed use of the material is for scholarly purposes. Any copying or use of the material in this thesis for financial gain shall not be allowed without my written permission.

Signature Umesh S. Thakur

Date 25th NOV. 1986

ARTIN'S RECIPROCITY LAW

A Thesis

Presented For The

Master Of Arts

Degree

The University Of Tennessee, Knoxville

Umesh S. Thakur

JUNE 1987

ABSTRACT

This thesis tries to determine why Artin's Law of Reciprocity is called a 'reciprocity' law. We will indicate a justification for this term by deducing the law of quadratic and cyclotomic reciprocity from it.

PREFACE

Artin's Law of Reciprocity is considered as a lofty pinnacle in Mathematics. Once you reach the top, a vista of great beauty opens before your eyes. This thesis does not aim at 'conquering' this peak. Instead, it is like a reconnaisance before the top is reached. While working towards this goal I was guided by the Great Masters of the past and the present, and had wonderful time in their company.

I would also like to thank Professor McConnel for the patience with which he tried to explain, my family who gave me encouragement throughout, Professor Mulay for the long talks with him and Dinesh for stimulating discussions. Finally, thanks to Ravi, Shailesh, Veena and Dilip for their help in typing this thesis.

TABLE OF CONTENTS

SECTION

1. INTRODUCTION AND SHORT HISTORY

This thesis presents a discussion of Artin's reciprocity law and its consequences. Specifically, after defining necessary terms and stating the law, we will see how some of the very deep results of number theory follow easily from this law. In particular we will deduce the Law of Quadratic Reciprocity and cyclotomic reciprocity. Also we note that Hilbert's theorem for the Norm residue symbol, the Kronecker-Weber theorem and Dirichlet's theorem about distribution of primes in arithmetical progression can be derived from this law.

Artin reciprocity involves the 'Galois group' of number fields, the 'ray class group' and the 'Frobenius automorphism', all of which will be described in the following sections. It is not immediately clear why Artin Reciprocity is called a reciprocity law or why such terms mentioned above were introduced. Therefore we present a brief account of classical questions of number theory that began with Fermat, continued with Euler, Legendre and reached maturity with the quadratic reciprocity law of Gauss. Then through the insight of Eisenstein, Kronecker, Kummer, Dedekind, Hilbert and Takagi bloomed class field theory. Finally it was Artin who showed that a correspondence in class field theory is 'natural' by his law and most reciprocity laws are special cases of his theorem [1].

In order to understand the origins of reciprocity laws we begin with a very simple question about rational primes p. What odd primes can be written as the sum of squares of two integers a and b, or, if

$p \mid a^2 + b^2$, can we say anything about p? Fermat showed that such a prime has to be of form $p = 4n + 1$ (or $p=2$). He also showed that p has a unique representation as $a^2 + b^2$. Now using the language of modern algebraic number theory, we can say that p splits completely in Q(i), i.e., $p = (a + ib)(a - ib)$ iff $p = 4n + 1$.

Euler and Legendre made progress along this line, but it was Gauss who first gave a proof of the quadratic reciprocity law.

If p and q are odd primes and if (p/q) is the Legendre symbol, then

$$(p/q) = \begin{cases} 1 & \text{if } x^2 \equiv p \pmod q \text{ has a solution for some } x. \\ -1 & \text{if } x^2 \not\equiv p \pmod q \text{ for all } x. \\ 0 & \text{if } p = q. \end{cases}$$

Then Gauss showed that

$$(p/q)(q/p) = (-1)^{(p-1)/2.(q-1)/2} \quad \cdots\cdots\cdots\cdots (1a)$$

$$(-1/p) = (-1)^{(p-1)/2} \quad \cdots\cdots\cdots\cdots (1b)$$

$$(2/p) = (-1)^{(p-1)(p+1)/8} \quad \cdots\cdots\cdots\cdots (1c)$$

We note that (/) is multiplicative, thus if we write $p^* = (-1)^{(p-1)/2} p$, then

$$(q/p) = (p^*/q)$$

and hence the name reciprocity. Another way of looking at this relation is to consider the congruence $x^2 \equiv p \pmod q$. Given any prime q, we can determine all the p's for which the congruence is satisfied by explicit calculations. But if we ask that for a fixed prime p, can we find all the primes q for which the congruence is satisfied, then the answer is far from obvious. It is quadratic reciprocity which tells us

how the solvability of $x^2 \equiv p \pmod q$ and $x^2 \equiv q \pmod p$ are related in terms of a simple congruence relation about p and q. If either $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, then both the congruences are simultaneously solvable or nonsolvable, and, if both p and q are congruent to 3(mod 4), then one of the congruences is solvable while the other is not. Hence ,for the reciprocity laws, we try to find 'simple' congruence relations about the primes [11, 12 ,15] .

Note that $p = a^2 + b^2$ means $(a + ib)(a - ib) = p$ and also $a^2 + b^2 \equiv 0 \pmod p$. The last congruence implies that $(ab')^2 \equiv -1 \pmod p$, where b' is inverse of b in Z_p, thus -1 is quadratic residue in the field Q . But this is true iff $p = 4n + 1$, ($n \varepsilon Z$), as follows from quadratic reciprocity (1b). So we find that the information whether a prime splits in higher field is obtained by a simple congruence relation in the lower field.

Also note that when we write $a^2 + b^2 = (a + ib)(a - ib)$, by the unique factorization property of Z[i], we can determine all the triplets u,v,w which satisfy $u^2 + v^2 = w^2$. Can we handle an equation of the type

$$u^p + v^p = w^p \text{ (p being a prime) ------(2)}$$

in a similar manner? The answer, unfortunately, is no. The main obstacle in factoring (2) is the fact that we are working in the ring $Z[\zeta_p]$, and this ring is not necessarily a unique factorization domain (UFD) [9]. Hence prime integers may not factor uniquely in higher number rings, but Dedekind observed that in such a ring (called a Dedekind domain) any ideal is a product of prime ideals and in this

sense the factorization is unique.

Thus we can write

$$p = P_1^{e_1} P_2^{e_2} \ldots P_g^{e_g} \quad \text{-----(3)}$$

With the help of this factorization we are able to deduce several things. If we consider the splitting of a rational prime p in a field K of degree n over Q, and if

$$f_i = [\mathcal{O}(K)/P_i : Z/(p)],$$

where $\mathcal{O}(K)$ is the ring of integers in the field K, then by using the norm we get

$$n = \sum e_i f_i \quad (1 \leq i \leq g).$$

If K is a Galois extension, then the situation is much better.In this case all the e_i's are same and so are all the f_i's, and hence we get

$$n = efg. \text{ (where } e_i = e \text{ and } f_i = f).$$

The number 'e' is called the ramification index of p and 'f' the inertial degree of p. If $e > 1$, we say that p is ramified in the field K. Next, we utilize a nice theorem which tells us that a prime in Z ramifies in K iff it divides the discriminant of K. The discriminant is a rational integer, so, except for finitely many primes, we have $e = 1$, and thus $n = fg$; hence, if we know anything about either f or g, we get all the information about how such a prime p splits in higher number fields. A prime is said to split completely when we have $f=1$ in the formula above. We can show that $f > 1$ for finitely many primes only. Hilbert introduced the concepts of 'decomposition group', 'inertia group', 'ramification groups' of the Galois group corresponding to the

given algebraic extension of an algebraic number field and the corresponding fields for these groups. He thought that all reciprocity laws had to do with abelian extensions of algebraic number fields. Proceeding along these lines Takagi was able to show that there is a correspondence between abelian Galois extensions K/k and the 'maximal ray ideal group' J (mod f), where f is the conductor. But this correspondence was of a 'formal' nature. Then Artin showed that this correspondence is explicit and canonical in the sense that it is given by the 'Frobenius automorphism', and when this automorphism is the identity, f=1; and hence the prime splits completely.

This is a brief introduction to the Artin reciprocity law. For historic developments which led to the law and the discussion of attempts made to generalize it (nonabelian extensions), we refer the reader to the articles by Hasse [2] and Tate [10]. For general references see [5,6,7] . In the next Section we will define all the necessary terms and precisely state Artin's law. Later sections will reveal the reason for using the term reciprocity and also demonstrate the power of this theorem.

2. DEFINITIONS AND THE RECIPROCITY LAW

In this section we are going to define the terms which will be needed in the subsequent discussion .

As we remarked above, the UFD property does not hold for all number rings. A simple example is that of the ring $Z[\sqrt{-5}]$. In this ring, we can write number 21 in two different ways as $21 = 3.7$ and also $21 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$. We can show that all the numbers 3,7, $(1 + 2\sqrt{-5})$, $(1 - 2\sqrt{-5})$ are irreducible in this ring. Thus in the higher algebraic fields, even if an element can be factored into a product of irreducibles, this factorization need not be unique. But if we introduce the concepts of ideal, prime ideal, etc. , then we get results analogous to ordinary integers [6,14]. Specifically, we define a Dedekind domain R as an integral domain such that

1) Every ideal of R is finitely generated.

2) Every nonzero prime ideal of R is a maximal ideal.

3) R is integrally closed in its field of fractions K.

Every number ring is a Dedekind domain. In a Dedekind domain R, every ideal is uniquely represented as a product of prime ideals.

First we define an algebraic number : It is a complex number α which is a root of a polynomial $a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n = 0$, where a_i's are in Q and $a_0 \neq 0$.

An algebraic integer ω is a complex number that is a root of a polynomial $x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n = 0$, where $a_i \in Z$.

A simple but useful result is that a rational number $r \varepsilon Q$ is an algebraic integer iff $r \varepsilon Z$.

We can show that the set of algebraic numbers forms a field.It can be shown that the set of algebraic integers forms a ring. This ring is usually denoted by $\mathcal{O}$. An example of an algebraic integer which will be quite useful later is an n-th root of unity satisfying the equation $x^n - 1$. Note that the sum and difference of the roots of unity are also algebraic integers as they form a ring. If α is an algebraic number, then α is a root of a unique monic irreducible polynomial f(x) in Q[x]. If $g(x) \varepsilon Q[x]$, $g(\alpha) = 0$, then $f(x) \mid g(x)$. Such an f(x) is called the minimal polynomial of α. If the degree of f(x) is n, then α is called an algebraic number of degree n. If α,β are the roots of f(x), then α and β are said to be conjugates. Let $Q(\alpha)$ be the set of complex numbers $f(\alpha)/g(\alpha)$ where $f(x), g(x) \varepsilon Q[x]$, $g(\alpha) \neq 0$. $Q(\alpha)$ is obviously a field. Let $Q[\alpha]$ be the ring of polynomials in α with rational coefficients. Then we can show that $Q(\alpha) = Q[\alpha]$. Hence, if α is an algebraic number of degree n, then $[Q(\alpha) : Q] = n$ as $1,\alpha,\alpha^2, \ldots, \alpha^{n-1}$ are linearly independant and span $Q[\alpha]$. Before proceeding further we remark that even though algebraic numbers (integers) were defined originally in the above fashion, we can genaralize these definitions to arbitrary algebraic number fields k and their extension fields K with suitable modifications.

Next we recall a few results from the theory of finite fields. The simplest example is that of Z/(p), where p is a prime; a finite

field with p elements (here (p) is as usual the prime ideal generated by p in the ring Z). If F is a finite field, we denote the nonzero elements of F by F^*. These elements form a multiplicative group. Either by using the structure theorem for finite abelian groups or by using the Moebius inversion formula we can show that F^* is cyclic. As every finite field contains a subfield isomorphic to Z/(p) for some prime p, the number of elements in a finite field is a power of a prime. This prime is called the characteristic of the field. We also know that given an arbitrary field k and an ireducible polynomial f(x) in k[x], we can construct a field K containing k and an element α in K such that $f(\alpha) = 0$. This K is k[x]/(f(x)), and α is x + (f(x)); K is denoted by $k(\alpha)$ over k. For a field F of characteristic p, we have a very important equality, $(a + b)^p = a^p + b^p$ for all a, b in F; in general, $(a + b)^q = a^q + b^q$, where $q = p^n$, n a positive integer.

We again turn our attention to algebraic numbers. The set of all algebraic numbers is the algebraic closure of the rational number field Q in C. It is denoted by A. By an algebraic number field we mean an extension field k of Q of finite degree in C, thus k is a subfield of A. Let $\mathcal{O}$ denote the ring of algebraic integers. It is an integral domain. The ring $D = k \cap \mathcal{O}$ is called a number ring and is an integral domain with field of quotient k. Now we explain how we can write any ideal in a number ring as a product of prime ideals in a unique way. In order to show this we will introduce several simple but important concepts. Let K/Q be an algebraic number field of degree n and $\alpha_1, \alpha_2,$

..., α_n, a basis for K over Q. For $\alpha \varepsilon D$, $\alpha\alpha_i = \sum_j a_{ij}\alpha_j$, where $a_{ij} \varepsilon Q$. We define the norm of α, $N(\alpha)$, as $\det(a_{ij})$. The trace of α, $t(\alpha)$, is defined as $\sum_i a_{ii}$. We see that the norm is multiplicative while the trace is additive. If the extension is Galois, we can show that $N(\alpha) = \alpha^{(1)}.\alpha^{(2)}. . . . \alpha^{(n)}$ and that $t(\alpha) = \alpha^{(1)} + \alpha^{(2)} + . . . + \alpha^{(n)}$, where $\alpha^{(i)} = \sigma_i(\alpha)$, σ_i is an automorphism in the Galois group of K/Q, and $1 \leq i \leq n$. In the case of ideals, we define, for a prime ideal P, N(P) = the number of the elements in the field D/P (this field is finite ,see below). This norm is again multiplicative and we can generalize the definition to any ideal. This is equivalent to an alternate definition, $N(P) = P_1.P_2. . . . P_n$, where $P_i = \sigma_i P$, $\sigma_i \varepsilon Gal(K/Q)$. For any n-tuple $(\alpha_1,\alpha_2, ..., \alpha_n)$ in K, we define the discriminant $\Delta(\alpha_1,\alpha_2, ..., \alpha_n)$ as $\det(t(\alpha_i\alpha_j))$. This concept is going to play a very important role in the subsequent discussion. We list the following properties of the discriminant : If $\Delta(\alpha_1,\alpha_2, ..., \alpha_n) \neq 0$, then $\alpha_1,\alpha_2, ..., \alpha_n$ is a basis for K/Q, and conversely, if K/Q is separable and $\alpha_1,\alpha_2, ..., \alpha_n$ is a basis for K/Q, then $\Delta(\alpha_1,\alpha_2, ..., \alpha_n) \neq 0$. If two bases $\alpha_1,\alpha_2, ..., \alpha_n$ and $\beta_1,\beta_2, . ..,\beta_n$ of K/Q are related by $\alpha_i = \sum_j a_{ij}\beta_j$, then $\Delta (\alpha_1,\alpha_2, ..., \alpha_n) = \det(a_{ij})^2 \times \Delta(\beta_1,\beta_2, . ..,\beta_n)$. If $\alpha_1,\alpha_2, ...,$

$\alpha_n \varepsilon K$ and K/Q is separable, then $\Delta(\alpha_1,\alpha_2,...,\alpha_n) = \det(\alpha_i^{(j)})^2$.

Equipped with these properties we can proceed towards the unique factorization property of the ideals in algebraic number fields along the following lines [8] : We can show that for $\beta \varepsilon K$ there is a $b \varepsilon Z$, $b \neq 0$, such that $b\beta \varepsilon D$ and that every ideal A of D contains a basis for K over Q. Hence if $\alpha_1,\alpha_2,...,\alpha_n \varepsilon A$ is a basis for K/Q with

$|\Delta(\alpha_1,\alpha_2,...,\alpha_n)|$ minimal, then $A = Z\alpha_1 + Z\alpha_2 + \ldots + Z\alpha_n$. For a nonzero ideal A of D, $A \cap Z \neq 0$. Hence for any ideal A, D/A has finite cardinality. This follows because $a \varepsilon A \cap Z$, $a \neq 0$, D/(a) has cardinality a^n, (n as above in the basis argument), and finally D/(a) $\rightarrow$ D/A is onto. This immediately tells us that D is a Noetherian ring, and that, when A is a prime ideal, D/A is a finite integral domain and hence a field. Therefore every prime ideal of D is a maximal ideal.

Now we define two ideals A,B in D as equivalent, $A \sim B$, if there are nonzero a, b in D such that (a)A = (b)B. This equivalence relation gives us equivalence classes in the set of ideals of D which are called ideal classes. The number of the ideal classes is called the class number of the field F and is denoted by h. One can show that h is finite. Note that if h = 1, then any two ideals are equivalent,i.e., D is a P.I.D. It also follows easily that, for any ideal A in D, there is an integer $m \leq h$ such that A^m is principal. From this we immediately conclude that if A,B,C are ideals and if AB = AC, then B = C. With this result we can introduce the group structure on the set of ideal classes with D as its unity and this group is called the class group

corresponding to the field F. Also we can show that if B is contained in C, then there is an ideal A such that CA = B. This is not a surprise if we recall that 2 | 4 but (4) is contained in (2); that is, in terms of ideals, 'divide' means 'contains'. By this and the Noetherian property it follows that every ideal in D can be written as as a product of prime ideals. It remains to show that this product is unique. Note that the decreasing chain $P, P^2, \ldots$, where P is a prime ideal, is nonterminating else we will get P = D. Hence for any ideal A, we have a unique nonnegative integer j such that $P^j \supseteq A$ and $P^{j+1} \not\supseteq A$. This number j is denoted by $ord_P A$. It is easy to see that $ord_P P = 1$, $ord_P R = 0$, where R is another prime ideal (recall that prime = maximal in D), and that $ord_P AB = ord_P A + ord_P B$. With the help of this notation we can show the uniqueness of the prime decomposition.

As we noticed above, for P a prime ideal in D, $P \cap Z \neq 0$. This intersection is a prime ideal in Z and so is = (p), where p is a prime in Z. By abuse of notation we denote (p) by p. Again as Q is the ground field, F the field over Q, we call p the prime below and P a prime lying above p. As $P \supset pD$, there is a number $e = ord_P p$ called the ramification index of P. If e = 1, then P is said to be unramified, else it is called ramified. As D/P is a finite field containing Z/pZ, it has p^f elements for some $f \geq 1$, this f is called the degree of P. We can show that, with the above notation, D/P^e has the cardinality p^{ef}. Let $P_1, P_2, \ldots, P_g$ be the primes above p with ramification indices $e_1, e_2, \ldots, e_g$ and degrees $f_1, f_2, \ldots, f_g$ respectively; so we have the relation

$p = P_1^{e_1}P_2^{e_2}\ldots P_g^{e_g}$. Now taking D modulo p, using the Chinese Remainder Theorem, and counting the number of elements in the quotient rings on both the sides we get a remarkable relation between e_i, f_i and n , namely : $n = \sum_{1 \le i \le g} e_i f_i$ (here $n = |D/p|$).

If we let F/Q be a Galois extension with G its Galois group, then for any P_i, P_j lying above p we can find some σ_{ij} in G such that $\sigma_{ij}P_i = P_j$. Also, as $\sigma D = D$ for all σ in G, σP is a prime ideal for P a prime and $D/A \approx \sigma D/\sigma A = D/\sigma A$ for all ideals A. We see that all the f_i's are equal say $f_i = f$, and that all the e_i's are equal say $e_i = e$. Therefore we have arrived at the relation $n = efg$.

In order to analyse the 'behavior' of the prime p while going from Q to the field above, we introduce the <u>decomposition group</u> corresponding to the prime ideal P as $Z(P) = \{ \sigma \in G \mid \sigma P = P\}$. Note that $Z(P)$ has cardinality ef. Consider the Galois extension (D/P)/(Z/pZ) of degree f with Galois group Γ. Now there is a natural homomorphism ϕ from $Z(P)$ onto Γ. This homomorphism has kernel $T(P) = \{ \sigma \in G \mid \sigma a \equiv a(\text{mod } P), a \in D \}$. $T(P)$ is called the <u>inertia group</u> of P. As Γ has cardinality f, $T(P)$ has cardinality e. Corresponding to the decomposition group and inertia group there is a decomposition field and inertia field respectively. In addition to these there are ramification fields. Thus there is a chain of the following type

$$G \supseteq Z(P) \supseteq T(P) \supseteq V_1(P) \supseteq \ldots \supseteq 1$$

in the Galois group G and

$$F \supseteq \ldots \supseteq F(V_1(P)) \supseteq F(T(P)) \supseteq F(Z(P)) \supseteq Q$$

in the field extension F/Q.

The connection between the above groups and fields is given by $Z(P) \leftrightarrow F(Z(P))$, $T(P) \leftrightarrow F(T(P))$ and $V_i(P) \leftrightarrow F(V_i(P))$, where $V_i(P) = \{ \sigma \in G | \sigma a \equiv a \pmod{P^{i+1}}, i>0, a \in D\}$ are the higher ramification groups and correspondingly there are ramification fields. With the help of these fields we can determine in which relative extensions does the prime ramify, where does it remain inert , and over what extension does it split completely. By inert we mean $e = 1$, $g = 1$, and split completely means $e = 1$, $f = 1$

Next we give some examples. First consider ring $D = Z[i]$. The integers of this ring are of the type $\alpha = a + ib$, where $a,b \in Z$. The norm, $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2$, and if u is a unit then $N(u) = \pm 1$. If π is irreducible, then there exists $p \in Z$ such that $\pi \mid p$; further, if $\alpha \in D$, $N(\alpha)$ is prime, then α is irreducible . It is clear that 2, which is a prime integer in the ring Z, can be written as $2 = -i(1 + i)^2$, so $1 + i$ is irreducible in the ring D, and as $n = 2$ here , $g = 1$, $f = 1$ and $e = 2$, i. e., 2 ramifies totally in Q(i). We can show that if $p \equiv 1 \pmod 4$, then there exists an irreducible π such that $p = \pi\bar{\pi}$,and if $q \equiv 3 \pmod 4$,then q is irreducible in D. Note that $2 \mid \Delta(1,i) = 4$. Another example is that of the ring $Z[\omega]$, where ω is an imaginary cube root of unity. In this ring $N(\alpha) = \alpha\bar{\alpha} = a^2-ab+b^2$, where $\alpha = a + \omega b$. Analogous to Z[i] we have the following results: If p, q are primes in Z and if $q \equiv 2 \pmod 3$,then

q is prime in D, if $p \equiv 1 \pmod 3$, then $p = \pi\bar{\pi}$, π a prime in D, and $3 = -\omega^2(1-\omega)^2$, $1-\omega$ a prime in D. Our last example is the ring $Z[\zeta_p]$, ζ_p being primitive p-th root of unity. We can show that $1-\zeta_p$ is a prime element in this ring and that p ramifies in this ring with $p = (1-\zeta_p)^{p-1}$. The discriminant in this ring is a power of p. The ramified primes in all the previous examples did divide the discriminants of the respective rings, and this behaviour is explained by the theorem which says that only those primes ramify which divide the discriminant. Above examples also give the idea that the unramified primes lie in an arithmetic progression with modulus of ramified primes. This concept will later generalize to 'ray class'.

Considering the relation between decomposition group, inertia group etc., we find that $Z(P) \simeq \Gamma$ if $|T(P)|=1$, and in this case Γ is a cyclic group generated by an automorphism of order $f = |Z(P)|$. This automorphism is given by $a \rightarrow a^p$, $a \in F$. The corresponding element in $Z(P)$ is denoted by σ_p and is called the Frobenius automorphism associated with P. We also denote the Frobenius automorphism by $Frob_p$. It is also convenient to write a^{σ_P} (or a^{Frob_P}) instead of $\sigma_P a$ ($Frob_P a$ respectively).

Note that the Frobenius automorphism has order f. Thus if the prime P is unramified and if σ_p is the identity, then we know that p splits completly where P|p. If we consider the conjugate of $P, \tau P$, $\tau \in G$, then $\tau^{-1} \sigma_p \tau = \sigma_{\tau P}$, so, if Gal F/Q is abelian, then σ_p is the same for all

the conjugates and this common value is called the Artin residue symbol σ_p. The way we defined this symbol tells us that to determine how p splits in the higher field we need not go to the higher field itself but can consider some simplier condition in the lower field (compare with the remark at the middle of page 6).

We now define the terms needed to state Artin's theorem [3,4] . Let J_1 be the group of fractional ideals in the field k. By fractional ideal we mean an ideal of the type (1/b)A, where $b \neq 0$, $b \varepsilon D$, and A is some ideal in D. Let J_m be the set of fractional ideals relatively prime to m , where m is an ordinary integral ideal. Thus $J_m = \{ a/b \mid a/b \varepsilon J_1, (m,ab) = 1 \}$. Let $J^1_{m\sim}$, a unit ray ideal group mod $m\sim$, be defined as $J^1_{m\sim} = \{ a/b \mid (m,ab) = 1, a/b \equiv 1 \bmod^{\times} m\sim \}$ where $a/b \equiv 1 \bmod^{\times} m\sim$ means $a/b = (\alpha)/(\beta)$, $((\alpha)(\beta),m) = 1$, $\alpha \equiv \beta \bmod m$, and $\alpha^{(j)}/\beta^{(j)} > 0$ for the conjugates $k^{(j)}$ represented by infinite primes in $m\sim$. An infinite prime means an embedding of k into real or complex field, and in the case of complex embeddings we have by convention $\alpha^{(j)} > 0$ (please refer to Section 4 for discussion of infinite primes). The reason for choosing fractional ideals is similar to the equivalence among the ideals and we can define an equivalence relation on them and get ideal classes, while 'infinite prime ' helps us in choosing the 'correct ' element (this is similar to choosing a 'primary ' element in case of cubic, biquadratic reciprocity laws).

A ray ideal group J is a subgroup of some J_m for which some

$m\sim$ exists such that $J_m \supseteq J \supseteq J^1{}_{m\sim}$, and we say J is defined modulo $m\sim$. The quotient $H\{J\} = J_m/J$ is called the ray class group of J. When $f\sim$ is a conductor (the conductor is defined as follows : For D a domain and D' a subdomain, the conductor m of D' is the maximal ideal of D such that $D' \supseteq m\,D$), we consider the maximal ray ideal group J mod $f\sim$. We can now state the 'Weber- Takagi correspondence' which says that there is an isomorphism between abelian Galois extensions K/k and maximal ray ideal group J mod $f\sim$ given by $K \leftrightarrow J$ such that { P a prime ideal splits completely in K/k } $\leftrightarrow$ {P ε J }. We will be considering k = Q. The Artin symbol, defined above for the prime p, is extended as follows: If $a = p_i^{e_i}$, where p_i's are unramified, then we define

$\sigma_a = \prod (\sigma_{p_i})^{e_i}$. This gives a homomorphic mapping of $J_{f\sim}$ into G, which is called the Artin mapping $\mathcal{A}: a \rightarrow \sigma_a$. This homomorphism is onto with kernel J i.e., p ε J iff σ_p = identity. Thus there exists an isomorphism between ideal classes c ε $J_{f\sim}/J$ and elements σ ε G given by $c \rightarrow \sigma_c$. This is the Artin Reciprocity Law. It tells us that **if an unramified prime p splits completely in the abelian Galois extension F/Q , then σ_p= identity**, and this is what we meant by a simple relation in p. To show that the Artin map is surjective,we consider Tchebotarev density theorem. Let S be the set of all the prime numbers, and let R be any subset of S, define d(R,x) = card {p ε R | p < x}/card{p ε S | p < x},for any real x>1. If $\lim_{x\rightarrow\infty}$ d(R,x) = d(R), then

the set R is said to have density d(R). Now we state the Tchebotarev Density Theorem (in the weak form) : Let f(x) be an irreducible polynomial in Z[X] with splitting field K and suppose [K:Q]=n. Then the set of primes p for which f(x) splits completely modulo p has density 1/n. We claim that G_Z ,the decomposition group of all unramified primes P for F/Q, is all of G,else we will have G_Z properly contained in G. Hence by Galois correspondence there is a corresponding subfield F_z of F containing Q. This means all the unramified primes p in Q split completely in F_z/Q. The density theorem says that 1/[F:Q]=1/[F_z:Q], but this is not possible as F_z is strictly contained in F and so [F:Q] > [F_z:Q]. Thus the Artin map is surjective.

3. DERIVATION OF LEGENDRE SYMBOL AND CYCLOTOMIC RECIPROCITY

We consider a quadratic extension of Q, i.e., let $F = Q(\sqrt{d})$,where d is a square free rational integer.In this field $D = Z + Z\sqrt{d}$ if $d \equiv 2,3 \pmod 4$ or if $d \equiv 1 \pmod 4$, then $D = Z + Z((-1 + \sqrt{d})/2)$. As $[F:Q] = 2$, by Galois theory, the Galois group corresponding to this extension is of degree 2. Let $G = \{I,C\}$,C being the conjugate mapping in D. From the result $n = efg$, either $e = 2, f = 1 = g$; or $e = 1, f = 2, g = 1$; or $e = 1 = f$, $g = 2$. Also we have the following congruences (in this discussion we consider the prime p to be odd): $r^p \equiv r \pmod p$ for any rational number r; $(\sqrt{d})^p = d^{(p-1)/2}\sqrt{d} \equiv (d/p)\sqrt{d} \pmod p$ (by the definition of the Legendre symbol and Fermat theorem). Using this for $\alpha = (a + b\sqrt{d})/2$ (where a,b are chosen suitably depending on d), $\alpha^p \equiv (a + b(d/p)\sqrt{d})/2 \pmod p$. As $(d/p) = \pm 1$, so $\alpha^p = \alpha$ or α^C.Thus the Artin symbol $\sigma_p = I$ or C depending on $(d/p) = 1$ or -1.Hence assuming $p \nmid 2d$,(p does not ramify as d is the discriminant),we can identify the Artin symbol σ_p to be (d/p). We next find the kernel for the Artin correspondence, which is a ray ideal group. In the quadratic case, as the ideals in Z are principal ideals generated by the integers, the ray ideal group consists of $r \in Q$ which are relatively prime to 2d and for which $(d/r) = 1$. (Note : So far we have defined the Legendre symbol with only a prime in the denominator, but we can generalize this notation to composite numbers as follows : $(a/p.q) = (a/p)(a/q)$; p,q being the primes).

Now we derive the cyclotomic reciprocity law using Artin reciprocity. Let $F = Q(\zeta_m)$, where $\zeta_m = (e^{2\pi i/m})$ is a primitive m-th root of unity. We will denote ζ_m by ζ. Recall that $Gal(F/Q) = Z_m^*$,the set of elements relatively prime to m modulo m, and for $\sigma \in G$, $\sigma\zeta = \zeta^k$,$(k,m)=1$ for some k. Recall the result from Section 2 : $Z(P)/T(P) \approx \Gamma$, $\Gamma =$ Gal[F/P:Q/p], for unramified primes $e = 1$ ($e = \text{ord } T(P)$), and we have $Z(P) \approx \Gamma$, so f is the order of Γ which is the order of the Frobenius element. Recall that in the finite field F_{q^n}, $\sigma: x \to x^q$ is the Frobenius automorphism and $\sigma, \sigma^2, ..., \sigma^n$ are all the distinct elements in $Gal(F_{q^n}/F_q)$, so $G = \langle\sigma\rangle$ and σ is the Frobenius element. Thus we have $x^{Frob_P} \equiv x^q (\text{mod}P)$,$(q = NP)$. In particular, for unramified primes, f=1 and so $Frob_P$ = identity. Consider $p \nmid m$ (so that p is unramified as the discriminant has factors only from m). From above we have $x^{Frob_P} \equiv x^p (\text{mod}P)$, (here $p = NP$) for x in D . We will show that the above congruence is actually an equality by showing $\zeta^{Frob_P} = \zeta^p$. Observe that ζ^{Frob_P} is some root of unity which is $\equiv \zeta^p$ (modP), so it suffices to show that all the roots of unity are distinct mod P. If $\zeta^i \equiv \zeta^j$ mod P, $i \neq j$, $1 \leq j < i < m$, then $\zeta^{i-j} \equiv 1$ (modP) and so $P \mid (1-\zeta^{i-j})$. We also have $m = f(1)$, where $f(x) = x^{m-1} + x^{m-2} + ... + 1 = (x-\zeta)(x-\zeta^2)...(x-\zeta^{m-1})$,and hence $P \mid (1-\zeta^{i-j}) \Rightarrow p \mid f(1) = m$ (by considering all the conjugates of P), which is a contradiction as $p \nmid m$. Thus we have the following equivalent facts: p is unramified $\Leftrightarrow$ f=1(= order of $Frob_p$ in the Galois group) $\Leftrightarrow$ $\zeta^p = \zeta \Leftrightarrow \zeta^{p-1} = 1$, and, as ζ is an m-th root of unity, so

$m \mid (p-1)$,i.e, $p \equiv 1 \pmod m$.The last congruence is what we were looking for, as it reduces the question of the splitting of the prime in the cyclotomic extension to a simple criterion about congruence modulo m.If we assume f=2, then $(Frob_p)^2$=identity, and so $\zeta = (\zeta^{Frob_p})^{Frob_p} = (\zeta^p)^{Frob_p} = (\zeta^{Frob_p})^p = (\zeta^p)^p$. Hence $\zeta^{p \cdot p} = \zeta$, i.e., $p^2 \equiv 1 \pmod m$. In general for f = t, we have $p^t \equiv 1 \pmod m$.

4. HILBERT NORM RESIDUE SYMBOL AND THE QUADRATIC RECIPROCITY LAW

The concept of a valuation on the field F originated from that of the absolute value. There are various approaches to define a valuation.We follow that of Weiss [13].

Valuation of the field F is a function f: $F \to R_+ \cup \{0\}$ satisfying

(1) $f(a) = 0 \Leftrightarrow a = 0$,

(2) $f(ab) = f(a).f(b)$,

(3) There exists a real constant C such that $f(a) \leq 1 \Rightarrow f(1+a) \leq C$ for all a in F.

If $f(0) = 0$ and $f(a) = 1$ for all $a \neq 0$ in F, then f is called a trivial valuation.Some easy consequences of the definition are $f(1)=1$, $f(a^{-1}) = 1/f(a)$, $f(a/b)=f(a)/f(b)$, $f(-1) = 1$ and for any root of unity z in F, $f(z) = 1$. We can show that (3) is equivalent to $f(a+b) \leq C.\max\{f(a),f(b)\}$, where C is a constant. Just as absolute value gives us a metric topology on the set, similarly valuation gives us a topological structure on the field. This turns out to be the Hausdorff topology with the basis given by $U_\delta(a,F) = \{b \in F \mid f(a-b) < \delta\}$ Two valuations are equivalent if they determine the same topology on F. This equivalence relation gives us equivalence classes of valuations on F called the prime divisors of F. A norm of a valuation f, $\| f \|$, is defined to be : $\| f \| = \inf C$ (C in (3) above). A prime divisor P of F is called archimedian when $\| f \| > 1$ for all f in P; it is called nonarchimedian if $\| f \| = 1$ for all f in P. An example of an archimedian

valuation is the absolute value valuation on R or C.

When working on Q we introduce the exponential valuation $v(a) = -\log f(a)$ or $f(a) = e^{-v(a)}$. Thus $v : F \to R \cup \{\infty\}$, $v(a) = \infty \Leftrightarrow a = 0$, $v(ab) = v(a)+v(b)$, $v(a+b) \geq \min\{v(a), v(b)\}$. If $v_p(F^*) = Z$, (where v_p is the valuation corresponding to the prime divisor p), v_p is called a normalized exponential valuation on P. The absolute value valuation, which is Archimedian, is called the infinite prime of Q and denoted by ∞.

For a prime integer p, a nonarchimedian valuation is defined as $v_p : Q^* \to Z$ by $v_p(a) = i$, where $a = (r/s).p^i$, $i \in Z$, $p \nmid rs$, and $v_p(0) = \infty$. Finally we define p-adic valuation $f_p(a) = (1/p)^{v_p(a)}$, $a \in Q$. The set of nontrivial prime divisors is $M = \{\infty, 2, 3, 5, 7, \ldots\}$. One can prove the following results : $f_p(a) = 1$ for almost all p in M, $a \in Q - \{0\}$, and that

$$\Pi_{p \in M} f_p(a) = 1.$$

We comment here that all the arithmetic that we did in Q can be carried to Q_p, the completion of Q at p, and as for primes in a field below/above, we can talk about the primes in the respective rings for Q and Q_p. We can also introduce the concept of ideals here. The merit of this approach is observed when dealing with Diophantine problems which become easier to work when in Q_p. For example, the Hasse principle says that for the quadratic forms, the solvability in the integers is equivalent to solvability in both finite and infinite prime divisors.

Now we introduce ' Hilbert's Norm Residue Symbol' : (a,b/p).

Hilbert's Norm Residue Symbol : (a,b/p), a,b, ε Z , p a prime (finite or infinite) is defined as

(a,b/p)=1, if a is the norm of an element of $Q_p(\sqrt{b})$,

(where the norm of $x + y\sqrt{b}$ is $N(x + y\sqrt{b}) = x^2-by^2$)

= -1 otherwise.

Thus (a,b/p) =1 means $a = x^2- by^2$ has a solution $x,y \varepsilon Q_p$, where Q_p is the p-adic completion of Q. Next, we discuss a few elementary properties of the norm residue symbol. First we have $(a^2, b/p) = 1$, as $a^2 = x^2-by^2$ has $x = a$, $y = 0$ as a solution . We can show that (a,b/p) = (b,a/p) by noticing that (a,b/p)= 1 iff there exist $x, y \varepsilon Q_p$ such that $ax^2+by^2 = 1$. As $ax^2+by^2 = 1$ is symmetric, (a,b/p) = (b,a/p). We also have (a, -a/p) =1, as $a = N(\sqrt{-a})$, and (a,(1-a)/p)=1 as $a.1^2+(1-a).1^2=1$. Also for $p \neq \infty$, we have $(a_1a_2,b/p) = (a_1,b/p)(a_2,b/p)$. We consider the folowing results:

(1) (a,b/p) =1, for p odd and relatively prime to a and b,

(2) (a,p/p) = (a/p) where (a/p) is the Legendre symbol for p odd and a relatively prime to p.

Note the (a,p/p) =1 means $ax^2+py^2=1$ for some $x,y \varepsilon Q_p$, i.e. , $ax^2 \equiv 1 \pmod p$, i.e., $z^2 \equiv a \pmod p$, where $z = x^{-1}$, and this means (a/p)=1. Conversely if (a/p) = -1, but (a,p/p) =1,then $a = x^2-py^2$ for some $x,y \varepsilon Q_p$, i.e., $x^2 \equiv a \pmod p$. One can also prove

(3) $(a,b/2) = (-1)^{(a-1)/2.(b-1)/2}$,

(4) $(a,2/2) = (-1)^M$, where $M = (a^2-1)/8$

With these results we will deduce quadratic reciprocity using Hilbert's product formula: $\prod_{\text{all } p}(a,b/p)=1$ for all $a,b \in Z^*$. From the above discussion we have to consider the cases when a,b are -1,2, p and q, where p and q are odd primes. By (1) above almost all the terms (a,b/p) are 1. For any p, (-1,-1/p) =1 because (u,v/p) =1 for u and v units. From the properties of the symbol we have
(-1,2/p) = (-1,1-(-1)/p) =1; (2,2/p) = (2,-2/p)(2,-1/p) = 1;
(-1,p/∞)=1; (-1,p/p)= (-1/p) by (2).

Hence $\prod_{\text{all } p}(a,b/p)=1$ for a =-1, b = p gives, (-1,p/2)(-1,p/p)=1, i.e., (-1,p/2) = (-1/p), thus $(-1/p) = (-1)^{(p-1)/2}$. Next consider a =2, b=q ≠2, so $\prod_{\text{all } p}(2,q/p)=(2,q/\infty)(2,q/2)(2,q/q)=1$, and, as (2,q/∞)=1, (2,q/q)=(2/q) and $(2,q/2) = (-1)^M$. Hence we get $(2/q)=(-1)^M$ where $M = (q^2-1)/8$.

Finally let a =p, b=q be odd primes. Then $\prod_{\text{all primes } r}(p,q/r) =$ (p,q/2)(p,q/p)(p,q/q)(p,q/∞)=1, and so $(p/q)\,(q/p)=(-1)^{(p-1)/2.(q-1)/2}$, which is the quadratic reciprocity law. The product formula above is equivalent to the Artin Reciprocity Law [7], and hence we have derived quadratic reciprocity law using Artin Reciprocity Law.

REFERENCES

REFERENCES

1) E. Artin, *The Collected Papers of Emil Artin* , Addison Wesley, Reading Mass., 1965. ,

2) J.W.S. Cassels and A. Frohlich (eds.), *Algebraic Number Theory* Thompson Book Co., Washington D.C.,1967.

3) H. Cohn, *A Classical Invitation To Algebraic Numbers And Class Fields* , Springer- Verlag, New York,1976.

4) H. Cohn, *Introduction To The Construction of Class Fields* , Cambridge Univ. Press, New York,1985.

5) Encyclopedic Dictionary Of Mathematics, M. I. T. Press, Cambridge, Mass., 1977.

6) E. Hecke, *Lectures on The Theory Of Algebraic Numbers* , Springer- Verlag, New York, 1981.

7) L.J. Goldstein, *Analytic Number Theory*, Prentice Hall, Princeton,1971.

8) K.Ireland and M. Rosen, *A Classical Introduction To Modern Number Theory*, Springer- Verlag, New York,1982.

9) D.A. Marcus, *Number Fields*, Springer- Verlag, New York, 1977.

10) J. Tate, Problem 9 :The General Reciprocity Law , in Mathematical Developments Arising From The Hilbert Problems , Proc. Of Symposia In Pure Math., Vol 28, 311-322, Amer. Math. Soc., Providence, R.I.,1976.

11) A. Weil, *Oeuvres Scientifiques* ,Collected Papers, 3-volumes, Springer- Verlag, New York, 1980.

12) A. Weil, *Number Theory*, Birkhauser, Boston,1983.

13) E. Weiss, *Algebraic Number Theory*, McGraw Hill, New York, 1963.

14) H. Weyl, *Algebraic Theory Of Numbers* , Princeton Univ. Press, Princeton,1940.

15) B.F. Wyman, What Is A Reciprocity Law ?, Amer. Math. Monthly, 79 (1972), 571-586.

VITA

Umesh Thakur is a native of Ratnagiri, India. He did his school education at B.P.M. High School, Khar, Bombay. He graduated from Ruia College, Matunga, Bombay with a Bachelor's Degree. He received a M.Sc. in mathematics from The University of Bombay in 1980. He joined the University of Tennessee in 1981.